FireSIGHT System 사용 설명서

버전 5.4.1
2015년 1월 22일

Cisco Systems, Inc.
www.cisco.com
Cisco는 전 세계에 200여 개 이상의 지사가 있습니다.
주소, 전화 번호 및 팩스 번호는 Cisco 웹사이트
www.cisco.com/go/offices에서 확인하십시오.

동봉된 제품의 소프트웨어 라이센스 및 제한 보증은 제품과 함께 제공되는 정보 패킷에 설명되어 있으며 본 참조 문서에 통합되어 있습니다. 소프트웨어 라이센스 또는 제한 보증을 찾을 수 없는 경우 CISCO 담당자에게 사본을 요청하십시오.

Cisco의 TCP 헤더 압축은 UNIX 운영 체제의 UCB 퍼블릭 도메인 버전의 일부로서 University of California, Berkeley(UCB)에서 개발된 프로그램을 적용하여 구현합니다. All rights reserved. Copyright © 1981, Regents of the University of California.

여기에 언급된 기타 모든 보증에도 불구하고 이러한 공급자의 모든 문서 및 소프트웨어는 모든 결함이 포함된 "있는 그대로" 제공됩니다. CISCO 및 위에 언급된 모든 공급업체는 상품성, 특정 목적에의 적합성, 타인의 권리 비침해 또는 처리, 사용, 거래 행위로 발생하는 문제에 대한 묵시적 보증을 포함하여(단, 이에 한하지 않음) 묵시적이든 명시적이든 모든 종류의 보증을 부인합니다.

Cisco 또는 해당 공급업체는 피해의 가능성에 대해 언급한 경우라도 이 설명서의 사용 또는 사용 불능으로 인해 발생하는 이익 손실, 데이터 손실 또는 손상을 포함하여(단, 이에 한하지 않음) 간접, 특별, 중대 또는 부수적 손해에 대해 어떠한 경우라도 책임을 지지 않습니다.

Cisco 및 Cisco 로고는 미국 및 기타 국가에서 Cisco Systems, Inc. 및/또는 계열사의 상표입니다. Cisco 상표 목록을 확인하려면 www.cisco.com/go/trademarks로 이동하십시오. 언급된 타사 상표는 해당 소유주의 재산입니다. "파트너"라는 용어의 사용이 Cisco와 다른 회사 간의 파트너 관계를 의미하지는 않습니다. (1110R)

이 문서에 사용된 모든 IP(인터넷 프로토콜) 주소와 전화 번호는 실제 주소와 전화 번호가 아닙니다. 이 문서에 포함된 예제, 명령 표시 출력, 네트워크 토폴로지 다이어그램 및 다른 그림은 이해를 돕기 위한 자료일 뿐이며, 실제 IP 주소나 전화 번호가 사용되었다면 이는 의도하지 않은 우연의 일치입니다.

목 차

58장

1장

Cisco FireSIGHT 시스템 소개

Cisco FireSIGHT® System은 네트워크 보안 및 트래픽 관리 제품들로 구성된 통합 제품군으로, 특별히 구축된 플랫폼에 또는 소프트웨어 솔루션으로서 구축됩니다.

시스템은 조직의 보안 정책(네트워크 보호를 위한 지침)을 따르는 방식으로 네트워크 트래픽을 처리하는 데 도움이 되도록 설계됩니다. 보안 정책에는 직원의 조직 시스템 이용 지침을 제공하는 AUP(Acceptable Use Policy)도 포함됩니다.

일반적인 구축에서는 네트워크 세그먼트에 설치된, 여러 트래픽 센싱 관리되는 *디바이스*가 분석을 위해 트래픽을 모니터링하고 관리하는 *방어 센터*®에 보고합니다. 인라인으로 구축된 디바이스는 트래픽의 흐름에 영향을 줄 수 있습니다.

팁

디바이스와 방어 센터의 여러 모델이 있습니다. 관리되는 디바이스에는 물리적 및 가상 FirePOWER 어플라이언스, Cisco NGIPS for Blue Coat X-Series 및 Cisco ASA with FirePOWER Services(ASA FirePOWER)가 포함됩니다. 방어 센터는 물리적 또는 가상 어플라이언스로서 구축할 수도 있습니다. 필요 시 어플라이언스 모델은 시리즈 및 제품군으로 더 그룹화됩니다. 시스템 기능은 종종 모델과 라이센스에 달려 있습니다.

방어 센터는 관리, 분석 및 보고 작업을 수행하는 데 사용할 수 있는 웹 인터페이스가 포함된 중앙 집중식 관리 콘솔을 제공합니다. 관리되는 물리적 디바이스에는 또한 초기 설정과 기본 분석 및 컨피그레이션 작업을 수행하기 위해 사용할 수 있는 웹 인터페이스도 있습니다. 관리되는 가상 디바이스, Cisco NGIPS for Blue Coat X-Series, 및 ASA FirePOWER 디바이스에는 FireSIGHT 시스템 웹 인터페이스가 없습니다. 이러한 디바이스의 경우, 관리하는 방어 센터를 사용하여 완료할 수 없는 작업을 수행하려면 CLI를 사용해야 합니다.

이 가이드에서는 FireSIGHT 시스템의 기능에 대한 정보를 제공합니다. 각 장의 설명 텍스트, 다이어그램 및 절차는 사용자 인터페이스를 탐색하고, 시스템 성능을 최대화하고, 복잡한 문제를 해결하는 데 도움이 되는 자세한 정보를 제공합니다.

다음 항목은 FireSIGHT 시스템을 소개하고, 주요 구성 요소를 설명하고, 이 가이드의 사용 방법을 이해하도록 도와줍니다.

관리되는 디바이스 소개

네트워크 세그먼트에 설치된 관리되는 디바이스는 분석용 트래픽을 모니터링합니다. 수동적으로 구축된 관리되는 디바이스는 호스트, 운영 체제, 애플리케이션, 사용자, 전송된 파일(악성코드 포함), 취약성 등 조직의 자산에 대한 자세한 정보를 수집합니다. FireSIGHT 시스템은 이러한 정보를 분석용으로 상호 연결하여, 사용자들이 방문하는 웹사이트와 사용하는 애플리케이션을 모니터링하고, 트래픽 패턴을 평가하고, 침입 및 기타 공격에 대한 알림을 수신할 수 있도록 지원합니다.

인라인으로 구축된 시스템은 네트워크에서 트래픽이 들어오고 나가고 통과하는 방법을 세부적으로 지정할 수 있는 *액세스 제어*를 사용하여 트래픽의 흐름에 영향을 미칠 수 있습니다. 네트워크 트래픽에 대해 수집하는 데이터 및 여기에서 가져오는 모든 정보를 사용하여 다음을 기반으로 트래픽을 필터링 및 제어할 수 있습니다.

- 소스와 목적지, 포트, 프로토콜 등 간단하고 쉽게 결정되는 전송 및 네트워크 레이어 특성
- 평판, 위험, 비즈니스 연관성, 사용된 애플리케이션 또는 방문한 URL 등의 특성을 비롯하여 트래픽에 대한 최신 컨텍스트 정보
- 조직의 Microsoft Active Directory LDAP 사용자(서로 다른 사용자에게 여러 액세스 레벨 허용 가능)
- 암호화된 트래픽의 특성(추가 분석을 위해 이 트래픽을 해독할 수도 있음)
- 암호화되지 않은 또는 해독된 트래픽에 금지된 파일, 탐지된 악성코드 또는 침입 이벤트가 포함되었는지 여부

각 유형의 트래픽 검사와 제어는 유연성과 성능을 최대화할 수 있는 방식으로 발생합니다. 예를 들어 평판 기반의 블랙리스트 추가는 단순한 소스 및 목적지 데이터를 사용하므로 프로세스 초기에 금지된 트래픽을 차단할 수 있는 반면, 침입과 익스플로잇의 탐지 및 차단은 최후의 방어 수단입니다.

액세스 제어 외에도 Series 3 디바이스의 네트워크 관리 기능을 사용하면 스위치드 및 라우티드 환경에서 디바이스를 작동하고, NAT(network address translation)를 수행하고, 구성한 가상 라우터 간 안전한 VPN(virtual private network) 터널을 구축할 수 있습니다. 또한 우회 인터페이스, 집계 인터페이스, 빠른 경로(fast-path) 규칙, 엄격한 TCP 적용 등을 구성할 수 있습니다.

자세한 내용은 다음 링크를 참고하십시오.

- 1-2페이지의 Series 2 및 Series 3 관리되는 디바이스
- 1-3페이지의 64비트 관리되는 가상 디바이스
- 1-3페이지의 Cisco NGIPS for Blue Coat X-Series
- 1-4페이지의 Cisco ASA with FirePOWER Services

Series 2 및 Series 3 관리되는 디바이스

모든 Cisco FirePOWER 7000 Series 및 8000 Series 디바이스를 포함하는 Series 3 디바이스는 FireSIGHT 시스템을 위해 특별히 구축된 물리적 디바이스의 세 번째 시리즈입니다. Series 3 디바이스는 처리량이 다양하지만, 대부분 동일한 기능을 공유하고 있습니다. 일반적으로 8000 Series 디바이스는 7000 Series보다 강력하며 빠른 경로 규칙, 링크 집계 및 스태킹 등의 추가 기능도 지원합니다.

방어 센터 및 Series 3 디바이스 모두 브랜딩 전환 과정 중에 있습니다. 방어 센터를 FireSIGHT Management Center라고도 하며, Series 3 디바이스를 FirePOWER 디바이스라고도 합니다. 방어 센터의 제품 식별 번호는 DC보다는 FS로 시작될 수 있습니다. 마찬가지로, Series 3의 제품 식별 번호는 3D보다는 FP로 시작될 수 있습니다. 다른 모델 번호는 변경되지 않습니다. 예를 들어 DC4000 및 FS4000은 동일한 방어 센터를 가리킵니다.

Series 2는 관리되는 물리적 디바이스의 두 번째 시리즈입니다. Series 2 디바이스에는 보호 라이센스와 관련된 대부분의 기능, 즉, 침입 탐지 및 방지, 파일 제어, 간단한 네트워크 기반 액세스 제어가 탑재되어 있습니다. 또한 3D9900은 빠른 경로 규칙, 스태킹 및 탭 모드를 지원합니다.

그러나 리소스 및 아키텍처 제한 때문에 Series 2 디바이스는 보호 라이센스에서 허용하는 기능의 일부만 지원합니다. Series 2 디바이스는 아카이브 파일 내에 중첩된 파일에 대해 보안 인텔리전스 필터링 또는 파일 제어를 수행할 수 없습니다. 또한 Series 2 디바이스는 FireSIGHT 라이센스 방어 센터가 있더라도 지오로케이션 기반 액세스 제어를 수행할 수 없습니다. Series 2 디바이스에서는 다른 라이센스 기능을 활성화할 수 **없습니다**.

Cisco에서는 더 이상 새로운 Series 2 어플라이언스를 출고하지 않지만, 시스템의 이전 버전을 실행하는 Series 2 디바이스를 버전 5.4.1로 업데이트하거나 이미지로 다시 설치할 수 있습니다. 이미지로 다시 설치할 경우 어플라이언스의 거의 **모든** 컨피그레이션과 이벤트 데이터가 손실됩니다. 자세한 내용은 *FireSIGHT 시스템 설치 가이드*을/를 참조하십시오.

팁 버전 4.10.3 구축에서 버전 5.2 구축으로 특정 컨피그레이션 및 이벤트 데이터를 마이그레이션한 다음 버전 5.4.1로 업데이트할 수 있습니다. 자세한 내용은 버전 5.2에 대한 *FireSIGHT 시스템 마이그레이션 가이드*을/를 참조하십시오.

64비트 관리되는 가상 디바이스

VMware vSphere Hypervisor 또는 vCloud Director 환경을 사용하여 64비트 가상 디바이스를 ESXi 호스트로서 구축할 수 있습니다. 또한 지원되는 모든 ESXi 버전에서 VMWare Tools를 활성화할 수 있습니다. 지원되는 버전 목록은 *FireSIGHT 시스템 Virtual Installation Guide*를 참조하십시오. VMWare Tools의 전체 기능에 대한 자세한 내용은 VMWare 웹사이트(http://www.vmware.com/)를 참조하십시오.

가상 어플라이언스는 e1000(1Gbit/s) 인터페이스를 사용합니다. 또는 VMWare vSphere Client를 사용하면 기본 센싱 및 관리 인터페이스를 vmxnet3(10Gbit/s) 인터페이스와 교체할 수 있습니다. 또한 VMWare vSphere Client를 사용하면 가상 방어 센터에 추가 관리 인터페이스를 생성할 수 있습니다. 자세한 내용은 *FireSIGHT 시스템 Virtual Installation Guide*를 참조하십시오.

가상 어플라이언스는 설치 및 적용된 라이센스와 상관없이, 시스템의 하드웨어 기반 기능(이중화, 리소스 공유, 스위칭, 라우팅 등)을 지원하지 않습니다. 또한 가상 디바이스에는 FireSIGHT 시스템 웹 인터페이스가 없습니다.

Cisco NGIPS for Blue Coat X-Series

Blue Coat X-Series플랫폼에서 Cisco NGIPS for Blue Coat X-Series를 설치할 수 있습니다. 이 소프트웨어 기반 어플라이언스는 가상의 관리되는 디바이스와 유사한 방식으로 작동합니다. 설치 및 적용된 라이센스와 상관없이 Cisco NGIPS for Blue Coat X-Series에서는 다음 FireSIGHT 시스템 기능을 지원하지 않습니다.

- Cisco NGIPS for Blue Coat X-Series는 AMP(advanced malware protection), 애플리케이션 제어, 사용자 제어, 시스템 하드웨어 기반 기능(클러스터 스태킹, 스위칭, 라우팅, VPN, NAT 등)을 비롯하여 악성코드 또는 제어 라이센스에서 허용하는 기능을 지원하지 않습니다.
- 암호화된 트래픽(SSL 검사)을 해독하거나 검사하는 데 Cisco NGIPS for Blue Coat X-Series를 사용할 수 없습니다.
- Cisco NGIPS for Blue Coat X-Series를 사용하여 발송지 또는 대상지의 국가 또는 대륙을 기준으로 네트워크 트래픽을 필터링할 수 없습니다(위치 기반 액세스 제어).

- 방어 센터 웹 인터페이스를 사용하여 Cisco NGIPS for Blue Coat X-Series 인터페이스를 사용할 수 없습니다.
- 방어 센터를 사용하여 Cisco NGIPS for Blue Coat X-Series 프로세스를 종료하거나 다시 시작하거나 다른 방식으로 관리할 수 없습니다.
- 방어 센터를 사용하여 Cisco NGIPS for Blue Coat X-Series에서 백업을 만들거나 여기로 백업을 복원할 수 없습니다.
- Cisco NGIPS for Blue Coat X-Series에 상태 또는 시스템 정책을 적용할 수 없습니다. 여기에는 시간 설정 관리가 포함됩니다.

Cisco NGIPS for Blue Coat X-Series에는 웹 인터페이스가 없습니다. 하지만, X-Series 플랫폼에는 고유한 CLI(Command Line Interface)가 있습니다. 이 CLI를 사용하여 시스템을 설치하고 다음과 같이 다른 플랫폼별 관리 작업을 수행할 수 있습니다.

- X-Series 플랫폼의 로드 밸런싱 및 이중화 이점(Cisco 물리적 디바이스 클러스터링과 비교)을 활용할 수 있는 VAP(Virtual Appliance Processor) 그룹 만들기
- 인터페이스의 MTU(Maximum Transmission Unit) 구성을 포함한 수동 및 인라인 센싱 인터페이스 구성
- 프로세스 관리
- NTP 설정을 포함한 시간 설정 관리

Cisco ASA with FirePOWER Services

Cisco ASA with FirePOWER Services(ASA FirePOWER 디바이스)는 관리되는 디바이스와 작동 방식이 유사합니다. 이러한 구축 환경에서 ASA 디바이스는 액세스 제어, 침입 감지 및 방지, 검색, AMP를 위해 FireSIGHT 시스템에 시스템 정책을 제공하고 트래픽을 전달합니다.

설치 및 적용된 라이센스와 상관없이 ASA FirePOWER 디바이스에서는 다음 FireSIGHT 시스템 기능을 지원하지 않습니다.

- ASA FirePOWER 디바이스는 FireSIGHT 시스템 시스템의 하드웨어 기반 기능, 즉, 클러스터링, 스태킹, 스위칭, 라우팅, VPN, NAT 등을 지원하지 않습니다. 하지만 ASA 플랫폼은 이러한 기능을 제공하지 않으며, 해당 기능은 ASA CLI 및 ASDM을 이용하여 구성할 수 있습니다. 자세한 내용은 ASA 설명서를 참조하십시오.
- ASA FirePOWER 디바이스는 SSL 검사를 지원하지 않습니다.
- 방어 센터 웹 인터페이스를 사용하여 ASA FirePOWER 인터페이스를 사용할 수 없습니다.
- 방어 센터를 사용하여 ASA FirePOWER 프로세스를 종료하거나 다시 시작하거나 다른 방식으로 관리할 수 없습니다.
- 방어 센터를 사용하여 ASA FirePOWER 디바이스에서 백업을 만들거나 여기로 백업을 복원할 수 없습니다.
- VLAN 태그 조건을 사용하여 트래픽과 일치시키기 위한 액세스 제어 규칙을 작성할 수 없습니다.

ASA FirePOWER 디바이스에는 FireSIGHT 웹 인터페이스가 없습니다. 하지만, ASA 플랫폼에 고유한 소프트웨어와 CLI(Command Line Interface)가 있습니다. 이러한 ASA별 툴을 사용하여 시스템을 설치하고 다른 플랫폼별 관리 작업을 수행할 수 있습니다. 자세한 내용은 ASA FirePOWER 모듈 설명서를 참조하십시오.

ASA 5506-X 디바이스는 독립 실행형 디바이스 또는 관리되는 디바이스로 관리할 수 있습니다. 독립 실행형 ASA FirePOWER 모듈은 ASDM으로 관리하고, 관리되는 ASA FirePOWER 디바이스는 방어 센터로 관리합니다. ASA FirePOWER 모듈이 방어 센터에 등록된 경우에는 ASDM으로 관리할 수 없습니다.

ASA FirePOWER 디바이스를 수정하면서 다중 컨텍스트 모드에서 단일 컨텍스트 모드로(또는 그 반대로) 전환하면 디바이스의 모든 인터페이스 이름이 변경됩니다. 업데이트된 ASA FirePOWER 인터페이스 이름을 사용하려면 모든 FireSIGHT 시스템 보안 영역, 상관관계 규칙 및 관련 컨피그레이션을 **반드시** 다시 구성해야 합니다.

참고 ASA FirePOWER 디바이스를 SPAN 포트 모드에서 구축한 경우 방어 센터에는 ASA 인터페이스가 표시되지 않습니다.

관리되는 디바이스 모델에서 지원되는 기능 요약

버전 5.4.1 실행 시 FireSIGHT 시스템 디바이스의 처리량과 기능은 모델 및 라이센스에 따라 달라집니다.

방어 센터 및 Series 3 디바이스 모두 브랜딩 전환 과정 중에 있습니다. 방어 센터를 FireSIGHT Management Center라고도 하며, Series 3 디바이스를 FirePOWER 디바이스라고도 합니다. 방어 센터의 제품 식별 번호는 DC보다는 FS로 시작될 수 있습니다. 마찬가지로, Series 3의 제품 식별 번호는 3D보다는 FP로 시작될 수 있습니다. 다른 모델 번호는 변경되지 않습니다. 예를 들어 DC4000 및 FS4000은 동일한 방어 센터를 가리킵니다.

어떤 버전 5.4.1 방어 센터를 사용하든 버전 5.4.1 디바이스를 관리할 수 있지만, DC500(그리고 그보다 덜한 범위의 DC750)은 FireSIGHT 시스템 기능의 일부만 지원합니다. 자세한 내용은 1-7페이지의 방어 센터 모델에서 지원되는 기능 요약을/를 참조하십시오.

다음 표에서는 시스템의 주요 액세스 제어 및 네트워크 관리 기능과 함께 이를 지원하는 관리되는 디바이스 및 사용자가 활성화해야 할 라이센스를 보여줍니다. 이러한 기능에 대한 간단한 설명은 1-11페이지의 FireSIGHT 시스템 구성 요소을/를 참조하십시오.

표 1-1 디바이스 모델별 지원되는 액세스 제어 기능

기능	Series 2 디바이스	Series 3 디바이스	ASA FirePOWER 디바이스	가상 디바이스	X-Series 디바이스	라이센스
액세스 제어: 기본적 네트워크 제어	예	예	VLAN 제어 없음	예	예	모두
액세스 제어: 리터럴 URL	아니요	예	예	예	예	모두
액세스 제어: SSL 검사	아니요	예	아니요	아니요	아니요	모두
네트워크 검사: 호스트, 사용자, 애플리케이션	예	예	예	예	예	FireSIGHT
액세스 제어: 위치 기반 필터링	아니요	예	예	예	아니요	FireSIGHT
보안 인텔리전스 필터링	아니요	예	예	예	예	보호
IPS(침입 감지 및 방지)	예	예	예	예	예	보호
파일 제어: 파일 유형별	예	예	예	예	예	보호
파일 제어: 아카이브 파일 검사	아니요	예	예	예	예	보호
AMP(Advanced Malware Protection)	아니요	예	예	예	아니요	악성코드
액세스 제어: 애플리케이션 제어	아니요	예	예	예	아니요	제어

표 1-1 디바이스 모델별 지원되는 액세스 제어 기능(계속)

기능	Series 2 디바이스	Series 3 디바이스	ASA FirePOWER 디바이스	가상 디바이스	X-Series 디바이스	라이센스
액세스 제어: 사용자 제어	아니요	예	예	예	아니요	제어
액세스 제어: 카테고리 및 평판별 URL 필터링	아니요	예	예	예	예	URL 필터링

표 1-2 디바이스 모델별 지원되는 관리 기능 및 네트워크 관리 기능

기능	Series 2 디바이스	Series 3 디바이스	ASA FirePOWER 디바이스	가상 디바이스	X-Series 디바이스	라이센스
트래픽 채널	아니요	예	아니요	아니요	아니요	모두
복수 관리 인터페이스	아니요	예	아니요	아니요	아니요	모두
링크 집계	아니요	예	아니요	아니요	아니요	모두
FireSIGHT 시스템 웹 인터페이스	제한적	제한적	아니요	아니요	아니요	모두
제한적 CLI(Command Line Interface)	아니요	예	예	예	아니요	모두
외부 인증	예	예	아니요	아니요	아니요	모두
eStreamer 클라이언트에 연결	예	예	예	아니요	아니요	모두
자동 애플리케이션 바이패스	예	예	아니요	예	아니요	모두
탭 모드	3D9900	예	아니요	아니요	아니요	모두
빠른 경로 규칙	3D9900	8000 Series	아니요	아니요	아니요	모두
엄격한 TCP 적용	아니요	예	아니요	아니요	아니요	보호
인라인 집합에 대한 우회 모드	예	NetMod/SFP 의존	아니요	아니요	아니요	보호
악성코드 스토리지 팩	아니요	예	아니요	아니요	아니요	악성코드
스위칭, 라우팅, 스위치드 및 라우티드 집계 인터페이스	아니요	예	아니요	아니요	아니요	제어
NAT 정책	아니요	예	아니요	아니요	아니요	제어
디바이스 스태킹	3D9900	3D8140 82xx 제품군 83xx 제품군	아니요	아니요	아니요	모두
디바이스 클러스터링	아니요	예	아니요	아니요	X-Series 기반	제어(X-Series 제외)
클러스터링 스택	아니요	3D8140 82xx 제품군 83xx 제품군	아니요	아니요	아니요	제어
VPN	아니요	예	아니요	아니요	아니요	VPN

방어 센터 소개

방어 센터에서는 FireSIGHT 시스템 구축을 위해 중앙 집중식 관리 콘솔 및 데이터베이스 저장소를 제공합니다. 방어 센터에서는 감염 지표를 이용하여 침입, 파일, 악성코드, 검색, 연결, 성능 데이터를 집계하고 상관 관계를 분석하며 이벤트가 특정 호스트와 태깅 호스트에 미치는 영향을 평가합니다. 따라서 디바이스가 디바이스 상호 관계에 대해 보고하는 정보를 모니터링할 수 있으며 네트워크에서 일어나는 전반적인 활동을 평가하고 제어할 수 있습니다. 방어 센터는 또한 디바이스에서 스위칭, NAT, VPN 등의 네트워크 관리 기능을 제어합니다.

방어 센터의 핵심 기능은 다음과 같습니다.

- 디바이스, 라이센스, 정책 관리
- 테이블, 그래프, 차트 형식으로 표시되는 이벤트 및 상황별 정보
- 상태 및 성능 모니터링
- 외부 알림 및 경고
- 상관 관계 분석, 감염 지표, 위협 요소 제거 기능으로 실시간 위협 대응
- 사용자 지정, 템플릿 기반 보고
- 고가용성(이중화) 기능으로 운영 연속성 보장

Series 2 및 Series 3 방어 센터는 Cisco에서 사용할 수 있는 폴트 톨러런트(fault-tolerant)의 특별히 구축된 물리적 네트워크 어플라이언스입니다. VMware vSphere Hypervisor 또는 vCloud Director 환경을 사용하여 64비트 가상 방어 센터를 ESXi 호스트로서 구축할 수 있습니다. 모든 방어 센터는 모든 유형의 디바이스(물리적, 가상, Cisco ASA with FirePOWER Services 및 Cisco NGIPS for Blue Coat X-Series)를 관리할 수 있습니다.

방어 센터에는 다양한 디바이스 관리, 이벤트 스토리지, 호스트 모니터링, 사용자 모니터링 기능이 있습니다. 리소스 및 아키텍처 제한 사항 때문에 DC500(그리고 그보다 덜한 범위의 DC750)은 FireSIGHT 시스템 기능의 일부만 지원합니다.

방어 센터 및 Series 3 디바이스 모두 브랜딩 전환 과정 중에 있습니다. 방어 센터를 FireSIGHT Management Center라고도 하며, Series 3 디바이스를 FirePOWER 디바이스라고도 합니다. 방어 센터의 제품 식별 번호는 DC보다는 FS로 시작될 수 있습니다. 마찬가지로, Series 3의 제품 식별 번호는 3D보다는 FP로 시작될 수 있습니다. 다른 모델 번호는 변경되지 않습니다. 예를 들어 DC4000 및 FS4000은 동일한 방어 센터를 가리킵니다.

참고 Cisco에서는 더 이상 새로운 Series 2 방어 센터를 출고하지 않지만, 버전 5.4.1로 업데이트하거나 이미지로 다시 설치할 수 있습니다. 이미지로 다시 설치할 경우 어플라이언스의 거의 **모든** 컨피그레이션과 이벤트 데이터가 손실됩니다. 자세한 내용은 *FireSIGHT 시스템 설치 가이드*을/를 참조하십시오.

방어 센터 모델에서 지원되는 기능 요약

버전 5.4.1을 실행할 경우 모든 방어 센터의 기능은 유사하지만 용량과 속도에서 중요한 차이가 있습니다. 방어 센터 모델은 관리할 수 있는 디바이스의 수, 저장할 수 있는 이벤트의 수, 그리고 모니터링할 수 있는 호스트와 사용자의 수가 다릅니다. 자세한 내용은 다음 링크를 참고하십시오.

- 4-1페이지의 디바이스 관리
- 63-15페이지의 데이터베이스 이벤트 제한 구성
- 65-8페이지의 FireSIGHT 호스트 및 사용자 라이센스 제한 이해

어떤 버전 5.4.1 방어 센터를 사용하든 버전 5.4.1 디바이스를 관리할 수 있지만, DC500(그리고 그보다 덜한 범위의 DC750)은 FireSIGHT 시스템 기능의 일부만 지원합니다. 또한 **디바이스**의 라이센스와 모델에 따라 많은 시스템 기능이 제한됩니다. 1-5페이지의 관리되는 디바이스 모델에서 지원되는 기능 요약을/를 참조하십시오.

DC2000 및 DC4000은 Cisco의 UCS(Unified Computing System) 플랫폼을 FireSIGHT 시스템 시스템에 도입합니다. DC2000 및 DC4000은 UCS Manager나 CIMC(Cisco Integrated Management Controller) 같은 BMC(베이스보드 관리 컨트롤러)에서 툴을 사용하는 Cisco 기능을 지원하지 않습니다. 다음 표에서는 시스템의 주요 액세스 제어 및 네트워크 관리 기능과 함께 이를 지원하는 방어 센터 및 사용자가 활성화해야 할 라이센스를 보여줍니다. 이러한 기능에 대한 간단한 설명은 1-11페이지의 FireSIGHT 시스템 구성 요소을/를 참조하십시오.

표 1-3 방어 센터 모델에서 지원되는 액세스 제어 기능

기능	Series 2 방어 센터	Series 3 방어 센터	가상 방어 센터	라이센스
간단한 네트워크 기반 액세스 제어를 수행하는 디바이스 관리	예	예	예	모두
리터럴(수동으로 입력된) URL에 의해 URL 제어를 수행하는 디바이스 관리	예	예	예	모두
SSL 검사를 수행하는 디바이스 관리	예	예	예	모두
관리되는 디바이스가 보고하는 검색 데이터(호스트, 애플리케이션, 사용자) 수집 및 조직의 네트워크 맵 구축	예	예	예	FireSIGHT
지오로케이션(국가 및 대륙) 데이터로 검색을 개선하고, 지오로케이션 기반 액세스 제어를 수행하는 디바이스 관리	DC1000, DC3000	예	예	FireSIGHT
보안 인텔리전스 필터링(블랙리스트에 추가)을 실행하는 디바이스 관리	DC1000, DC3000	예	예	보호
IPS(침입 감지 및 방지) 구축 관리	예	예	예	보호
파일 유형별로 간단한 파일 제어를 수행하는 디바이스 관리	예	예	예	보호
아카이브 파일 검사를 수행하는 디바이스 관리	DC1000, DC3000	예	예	보호
애플리케이션 제어를 실행하는 디바이스 관리	예	예	예	제어
사용자 제어를 실행하는 디바이스 관리	DC1000, DC3000	예	예	제어
카테고리 및 평판별 URL 필터링을 수행하는 디바이스 관리	DC1000, DC3000	예	예	URL 필터링
AMP(advanced malware protection) 구축 관리 및 악성코드 스토리지 팩 설치	DC1000, DC3000	예	예	악성코드
FireAMP 구축에서 엔드포인트 기반 악성코드(FireAMP) 이벤트 수신	예	예	예	FireAMP 구독
eStreamer, 호스트 입력 또는 데이터베이스 클라이언트에 연결	예	예	예	모두

표 1-4 방어 센터 모델별 지원되는 네트워크 관리 및 이중화 기능

기능	Series 2 방어 센터	Series 3 방어 센터	가상 방어 센터	라이센스
트래픽 채널을 이용하여 내부 및 외부 트래픽 구분 및 관리	아니요	예	예	모두
복수 관리 인터페이스를 사용하여 다른 네트워크에서 트래픽 격리 및 관리	아니요	예	예	모두
방어 센터 이중화(고가용성) 설정	DC1000, DC3000	DC1500, DC2000, DC3500, DC4000	아니요	모두
디바이스 기반 이중화 및 리소스 공유 관리(스택, 클러스터 및 클러스터링된 스택)	예	예	예	제어
하드웨어에 의존하는 네트워크 관리 기능으로 디바이스 관리: 빠른 경로 규칙, 엄격한 TCP 적용, 우회 모드, 탭 모드, 스위칭 및 라우팅, NAT, VPN	예	예	예	기능에 따라 다름

방어 센터 및 버전 5.4.1에서 제공하는 디바이스

다음 표에는 방어 센터 및 Cisco가 버전 5.4.1의 FireSIGHT 시스템으로 제공하는 관리되는 디바이스가 나열되어 있습니다.

표 1-5 버전 5.4.1 FireSIGHT 시스템 방어 센터 및 디바이스

모델/제품군	시리즈	유형
70xx 제품군: • 3D7010/7020/7030/7050	Series 3 FirePOWER(7000 Series)	디바이스
71xx 제품군: • 3D7110/7120 • 3D7115/7125 • AMP7150	Series 3 FirePOWER(7000 Series)	디바이스
81xx 제품군: • 3D8120/8130/8140 • AMP8150	Series 3 FirePOWER(8000 Series)	디바이스
82xx 제품군: • 3D8250 • 3D8260/8270/8290	Series 3 FirePOWER(8000 Series)	디바이스
83xx 제품군: • 3D8350 • 3D8360/8370/8390	Series 3 FirePOWER(8000 Series)	디바이스
64비트 가상 디바이스	해당 없음	디바이스
Cisco NGIPS for Blue Coat X-Series	해당 없음	디바이스

표 1-5 버전 5.4.1 FireSIGHT 시스템 방어 센터 및 디바이스(계속)

모델/제품군	시리즈	유형
ASA FirePOWER: • ASA5585-X-SSP-10 • ASA5585-X-SSP-20 • ASA5585-X-SSP-40 • ASA5585-X-SSP-60	해당 없음	디바이스
ASA FirePOWER: • ASA5506-X • ASA5512-X • ASA5515-X • ASA5525-X • ASA5545-X • ASA5555-X	해당 없음	디바이스
Series 3 방어 센터: • DC750/1500/3500 • DC2000/4000	Series 3	방어 센터
64비트 가상 방어 센터	해당 없음	방어 센터

방어 센터 및 Series 3 디바이스 모두 브랜딩 전환 과정 중에 있습니다. 방어 센터를 FireSIGHT Management Center라고도 하며, Series 3 디바이스를 FirePOWER 디바이스라고도 합니다. 방어 센터의 제품 식별 번호는 DC보다는 FS로 시작될 수 있습니다. 마찬가지로, Series 3의 제품 식별 번호는 3D보다는 FP로 시작될 수 있습니다. 다른 모델 번호는 변경되지 않습니다. 예를 들어 DC4000 및 FS4000은 동일한 방어 센터를 가리킵니다.

Cisco에서는 더 이상 새로운 Series 2 어플라이언스를 출고하지 않지만, 시스템의 이전 버전을 실행하는 Series 2 디바이스와 방어 센터를 버전 5.4.1로 업데이트하거나 이미지로 다시 설치할 수 있습니다. 이미지로 다시 설치할 경우 어플라이언스의 거의 **모든** 컨피그레이션과 이벤트 데이터가 손실됩니다. 자세한 내용은 *FireSIGHT 시스템 설치 가이드*을/를 참조하십시오.

팁 버전 4.10.3 구축에서 버전 5.2 구축으로 특정 컨피그레이션 및 이벤트 데이터를 마이그레이션한 다음 버전 5.4.1로 업데이트할 수 있습니다. 자세한 내용은 버전 5.2에 대한 *FireSIGHT 시스템 마이그레이션 가이드*을/를 참조하십시오.

FireSIGHT 시스템 구성 요소

다음 항목에서는 FireSIGHT 시스템이 조직의 보안, 허용되는 사용 정책, 트래픽 관리 전략에 기여하는 몇 가지 주요 기능에 대해 설명합니다.

- 1-11페이지의 이중화 및 리소스 공유
- 1-12페이지의 네트워크 트래픽 관리
- 1-13페이지의 FireSIGHT
- 1-13페이지의 액세스 제어
- 1-13페이지의 SSL 검사
- 1-14페이지의 침입 감지 및 방지
- 1-14페이지의 AMP 및 파일 제어
- 1-15페이지의 애플리케이션 프로그래밍 인터페이스

팁 대부분의 FireSIGHT 시스템 기능은 어플라이언스 모델, 라이센스, 사용자 역할에 따라 달라집니다. 이 문서에는 각 기능에 필요한 FireSIGHT 시스템 라이센스와 디바이스, 그리고 각 절차를 완료하는 데 필요한 권한이 있는 사용자 역할에 대한 정보가 포함되어 있습니다. 자세한 내용은 1-17페이지의 설명서 표기 규칙을/를 참조하십시오.

이중화 및 리소스 공유

FireSIGHT 시스템의 이중화 및 리소스 공유 기능을 이용하면 운영 연속성을 보장하고 복수 물리적 디바이스의 처리 리소스를 결합할 수 있습니다.

방어 센터 고가용성

운영의 연속성을 보장하려면 방어 센터 *고가용성* 기능을 사용하여 디바이스 관리를 위한 이중 DC1000, DC1500, DC2000, DC3000, DC3500 또는 DC4000 방어 센터를 지정할 수 있습니다. 이벤트 데이터는 관리되는 디바이스에서 두 방어 센터로 스트리밍되며 특정 컨피그레이션 요소가 두 방어 센터에서 유지됩니다. 한 방어 센터가 실패하면 다른 방어 센터를 사용하여 중단 없이 네트워크를 모니터링할 수 있습니다.

디바이스 스태킹

*디바이스 스태킹*을 이용하면 스택 컨피그레이션에서 물리적 디바이스 2~4개를 연결하여 네트워크 세그먼트에서 검사하는 트래픽의 양을 늘릴 수 있습니다. 스태킹된 컨피그레이션을 구축하면 각 스태킹된 디바이스의 리소스를 공유된 단일 컨피그레이션으로 결합합니다.

디바이스 클러스터링

*디바이스 클러스터링*을 이용하면 2개 이상의 Series 3 디바이스 또는 스택 사이에서 네트워킹 기능 및 컨피그레이션 데이터의 이중화를 구현할 수 있습니다. 둘 이상의 피어 디바이스나 스택을 클러스터링하면 정책 적용, 시스템 업데이트 및 등록을 위한 논리적 단일 시스템이 생성됩니다. 디바이스 클러스터링을 구현하면 시스템을 수동으로 또는 자동으로 장애 조치할 수 있습니다.

대부분의 경우, SFRP를 사용하여 디바이스 클러스터링 없이 레이어 3 이중화를 구현할 수 있습니다. SFRP를 사용하면 특정 IP 주소에 대해 디바이스가 이중 게이트웨이 역할을 하도록 지정할 수 있습니다. 네트워크 이중화를 구현하면, 네트워크의 다른 호스트에 대한 연결을 보장하기 위해 둘 이상의 디바이스나 스택에서 동일한 네트워크 연결을 제공하도록 구성할 수 있습니다.

Cisco NGIPS for Blue Coat X-Series를 이용한 로드 밸런싱

X-Series 플랫폼의 다중 멤버 VAP 그룹에서 Cisco NGIPS for Blue Coat X-Series를 개별 VAP로 구축하여 X-Series 플랫폼의 로드 밸런싱 및 이중화 이점을 활용할 수 있습니다(Cisco 물리적 디바이스 클러스터링과 비교). 그런 다음 방어 센터를 사용하여 이러한 VAP 그룹을 관리할 수 있습니다. 자세한 내용은 *Cisco NGIPS for Blue Coat X-Series Installation and Configuration Guide*를 참조하십시오.

네트워크 트래픽 관리

FireSIGHT 시스템의 네트워크 트래픽 관리 기능을 사용하면 관리되는 디바이스를 조직의 네트워크 인프라 중 일부처럼 작동할 수 있습니다. 스위치드, 라우티드 또는 하이브리드(스위치드와 라우티드) 환경에서 작동하고, NAT(network address translation)를 수행하며, 안전한 VPN(virtual private network) 터널을 구축하도록 Series 3 디바이스를 구성할 수 있습니다.

스위칭

둘 이상의 네트워크 세그먼트 간에 패킷 스위칭을 제공하도록 레이어 2 구축에서 FireSIGHT 시스템을 구성할 수 있습니다. 레이어 2 구축에서, 관리되는 디바이스에 스위치드 인터페이스 및 가상 스위치를 구성하여 독립형 브로드캐스트 도메인으로 운영할 수 있습니다. 가상 스위치에서는 호스트의 MAC 주소를 사용하여 패킷을 보낼 위치를 결정합니다. 또한 여러 물리적 인터페이스를 네트워크의 두 엔드포인트 간 패킷 스위칭을 제공하는 단일 논리적 링크로 그룹화할 수 있습니다. 엔드포인트는 FirePOWER 관리되는 디바이스, 또는 서드파티 액세스 스위치에 연결된 FirePOWER 관리되는 디바이스일 수 있습니다.

라우팅

둘 이상의 네트워크 세그먼트 간에 트래픽을 라우팅하도록 레이어 3 구축에서 FireSIGHT 시스템을 구성할 수 있습니다. 레이어 3 구축에서, 관리되는 디바이스에 라우티드 인터페이스 및 가상 라우터를 구성하여 트래픽을 수신 및 전달할 수 있습니다. 시스템은 목적지 IP 주소에 따라 패킷 전달 결정을 내려 패킷을 라우팅합니다. 라우터는 전달 기준에 따라 송신 인터페이스에서 대상을 확인하며, 액세스 제어 규칙은 적용할 보안 정책을 지정합니다.

가상 라우터를 구성할 때 고정 경로를 정의할 수 있습니다. 또한 RIP(Routing Information Protocol) 및 OSPF(Open Shortest Path First) 동적 라우팅 프로토콜을 구성할 수 있습니다. 고정 경로와 RIP 또는 고정 경로와 OSPF의 조합도 구성 가능합니다. 구성하는 각 가상 라우터에 대해 DHCP 릴레이를 설정할 수 있습니다.

Cisco 어플라이언스 컨피그레이션에서 가상 스위치와 가상 라우터를 모두 사용하는 경우, 둘 사이의 트래픽을 연결하기 위해 관련 하이브리드 인터페이스를 구성할 수 있습니다. 이러한 유틸리티는 유형 및 적절한 응답(경로, 스위치 등)을 결정하기 위해 트래픽을 분석합니다. 또한 여러 물리적 인터페이스를 네트워크의 두 엔드포인트 간 트래픽을 라우팅하는 단일 논리적 링크로 그룹화할 수 있습니다. 엔드포인트는 FirePOWER 관리되는 디바이스, 또는 서드파티 라우터에 연결된 FirePOWER 관리되는 디바이스일 수 있습니다.

NAT

레이어 3 구축에서는 NAT(network address translation)를 구성할 수 있습니다. 내부 서버를 외부 네트워크에 노출하거나, 내부 호스트 또는 서버가 외부 애플리케이션에 연결되도록 허용할 수 있습니다. 또한 IP 주소 블록을 사용하거나 IP 주소 및 포트 변환의 제한된 블록을 사용하여 외부 네트워크로부터 사설 네트워크 주소를 숨기도록 NAT를 구성할 수도 있습니다.

VPN

VPN(virtual private network)은 인터넷과 같은 공개 소스나 기타 네트워크를 통해 엔드포인트 간에 보안 터널을 설정하는 네트워크 연결입니다. Series 3 디바이스의 가상 라우터 간에 안전한 VPN 터널을 구축하도록 FireSIGHT 시스템을 구성할 수 있습니다.

FireSIGHT

FireSIGHT™ 는 네트워크에 대한 완전한 가시성을 제공하기 위해 호스트, 운영 체제, 애플리케이션, 사용자, 파일, 네트워크 위치 정보, 취약성에 대한 정보를 수집하는 Cisco 검색 및 인식 기술입니다.

방어 센터의 웹 인터페이스를 사용하면 시스템에서 수집한 데이터를 보고 분석할 수 있습니다. 또한 액세스를 제어하고 침입 규칙 상태를 수정할 때도 이 데이터를 사용할 수 있습니다. 또한 호스트에 대한 상관 관계 이벤트 데이터를 기준으로 네트워크의 호스트에 대한 감염 지표를 생성 및 추적할 수 있습니다.

액세스 제어

*액세스 제어*는 네트워크를 통해 이동할 수 있는 트래픽을 지정, 검사, 로깅할 수 있는 정책 기반 기능입니다. *액세스 제어 정책*에 따라 시스템이 네트워크의 트래픽을 처리하는 방식이 결정됩니다.

가장 간단한 액세스 제어 정책은 *기본 작업*을 사용하여 모든 트래픽을 처리하도록 대상 디바이스에 지시합니다. 이러한 기본 작업을 설정하여 추가 검사 없이 모든 트래픽을 차단하거나, 침입 및 검색 데이터에 대한 트래픽을 검사할 수 있습니다.

좀 더 복잡한 액세스 제어 정책은 보안 인텔리전스 데이터를 기반으로 트래픽을 블랙리스트에 추가하고, *액세스 제어 규칙*을 사용하여 네트워크 트래픽 로깅 및 처리를 세부적으로 제어하는 것입니다. 이러한 규칙은 간단하거나 복잡한 방식으로 여러 기준을 사용하여 트래픽을 매칭하고 검사합니다. 보안 영역, 네트워크 또는 지오로케이션, VLAN, 포트, 애플리케이션, 요청된 URL 및 사용자별로 트래픽을 제어할 수 있습니다. 고급 액세스 제어 옵션에는 해독, 전처리 및 성능이 포함됩니다.

각 액세스 제어 규칙에는 일치하는 트래픽의 모니터링, 신뢰, 차단 또는 허용 여부를 결정하는 *작업*이 있습니다. 허용하는 경우, 트래픽이 자산에 도달하거나 네트워크에서 빠져나가기 전에 시스템에서 먼저 침입 또는 파일 정책으로 트래픽을 검사하여 익스플로잇, 악성코드 또는 금지된 파일을 차단하도록 지정할 수 있습니다.

SSL 검사

*SSL 검사*는 해독 없이 암호화된 트래픽을 처리하거나, 추가 액세스 제어 검사를 위해 암호화된 트래픽을 해독할 수 있는 정책 기반 기능입니다. 트래픽의 해독 또는 추가 분석 없이 신뢰할 수 없는 암호화된 트래픽의 소스를 차단하도록 선택할 수 있습니다. 또는 암호화된 트래픽을 해독하지 않고 대신 액세스 제어로 검사하도록 선택할 수도 있습니다.

암호화된 트래픽을 더 자세히 살펴보려면, 공개 키 인증서 및 시스템에 업로드한 페어링된 개인 키를 사용하여 네트워크를 이동하는 암호화된 트래픽을 해독한 다음, 해독된 트래픽을 마치 암호화되지 않았던 것처럼 액세스 제어로 검사할 수 있습니다. 시스템은 해독된 트래픽 사후 분석을 차단하지 않는 경우, 목적지 호스트로 전달하기 전 트래픽을 다시 암호화합니다. 시스템은 암호화된 연결에 대해 작업할 때 이에 대한 세부사항을 로깅할 수 있습니다.

침입 감지 및 방지

침입 탐지와 방지는 트래픽이 목적지로 들어가기 전 시스템의 최후의 방어선입니다. *침입 정책*은 액세스 제어 정책에 의해 호출되는 침입 탐지 및 방지 컨피그레이션의 정의된 집합입니다. 침입 정책은 *침입 규칙* 및 기타 설정을 사용하여 트래픽에서 보안 위반을 검사하고, 인라인 구축 시 악성 트래픽을 차단 또는 변경할 수 있습니다.

Cisco에서는 FireSIGHT 시스템을 통해 몇 가지 침입 정책을 제공합니다. 시스템 제공 정책을 사용하면 Cisco VRT(Vulnerability Research Team)의 경험을 활용할 수 있습니다. 이러한 정책에 대해 VRT는 침입 및 프리프로세서 규칙 상태(enabled 또는 disabled)를 설정하며, 기타 고급 설정에 대한 초기 컨피그레이션을 제공합니다. 규칙을 활성화하면 시스템은 규칙과 일치하는 트래픽에 대해 침입 이벤트를 생성(선택적으로 차단)합니다.

시스템 제공 정책이 조직의 보안 요구를 충분히 충족하지 못하는 경우, 사용자 지정 정책을 사용하면 환경에서 시스템 성능을 높일 수 있으며 네트워크에서 발생하는 악성 트래픽과 정책 위반을 집중적으로 관찰할 수 있습니다. 사용자 지정 정책을 생성 및 조정함으로써, 시스템이 네트워크의 트래픽에서 침입을 처리하고 검사하는 방법을 매우 세밀하게 구성할 수 있습니다.

AMP 및 파일 제어

악성코드의 효과를 식별 및 감소할 수 있도록 FireSIGHT 시스템의 파일 제어, 네트워크 파일 전파 흔적 분석(File trajectory) 및 AMP 구성 요소는 네트워크 트래픽의 파일(악성코드 파일 및 아카이브 파일 내 중첩 파일 포함) 전송을 감지, 추적, 캡처, 분석하고, 선택적으로 차단할 수 있습니다.

파일 제어

*파일 제어*에서는 관리되는 디바이스가 사용자가 특정 애플리케이션 프로토콜에서 특정 유형의 파일을 업로드(전송) 또는 다운로드(수신)하는 행동을 감지하고 차단할 수 있습니다. 파일 제어를 전반적 액세스 제어 컨피그레이션의 일부로 구성하고, 액세스 제어 규칙과 연결된 파일 정책이 규칙 조건을 충족하는 네트워크 트래픽을 검사합니다.

네트워크 기반 AMP

네트워크 기반 *AMP*는 시스템에서 네트워크 트래픽을 검사하여 여러 유형의 파일에서 악성코드를 찾아냅니다. 어플라이언스는 감지된 파일을 하드 드라이브 또는 악성코드 스토리지 팩(일부 모델)에 저장하여 추가 분석을 수행할 수 있습니다.

감지된 파일의 저장 여부와 상관없이, 파일을 종합 보안 인텔리전스 클라우드에 제출하고 파일의 SHA-256 해시값을 이용하여 알려진 속성을 간단히 조회할 수 있습니다. 또한 파일을 위협 스코어를 생성하는 *동적 분석*으로 제출할 수도 있습니다. 이 상황인식 정보를 바탕으로 시스템을 구성하여 특정 파일을 차단 또는 허용할 수 있습니다.

악성코드 차단을 전반적 액세스 제어 컨피그레이션의 일부로 구성하면 액세스 제어 규칙과 연결된 파일 정책이 규칙 조건을 충족하는 네트워크 트래픽을 검사합니다.

FireAMP 통합

FireAMP는 첨단 악성코드 침투, APT(Advanced Persistent Threat), 표적 공격을 발견, 이해 및 차단하는 Cisco의 엔터프라이즈급 고급 악성코드 분석 및 보호 솔루션입니다.

조직이 FireAMP에 가입된 경우 개별 사용자는 컴퓨터와 모바일 디바이스(*엔드포인트*라고도 함)에 *FireAMP Connector*를 설치할 수 있습니다. 이와 같이 가벼운 에이전트는 Cisco 클라우드와 통신하며, Cisco 클라우드는 방어 센터와 통신합니다.

조직의 보안 정책이 기존 클라우드 서버 연결의 사용을 허용하지 않는 경우 Cisco의 프라이빗 온프레미스 클라우드 솔루션인 FireAMP Private Cloud를 구입하여 구성할 수 있습니다. 이 솔루션은 퍼블릭 Cisco 클라우드의 압축된 로컬 버전 역할을 하는 가상 머신입니다.

방어 센터를 구성하여 클라우드에 연결한 다음에는 방어 센터 웹 인터페이스를 사용하여 조직의 엔드포인트에서 검사, 감지, 격리의 결과로 생성된 엔드포인트 기반 악성코드 이벤트를 확인할 수 있습니다. 방어 센터에서는 또한 FireAMP 데이터를 사용하여 호스트의 감염 지표를 생성 및 추적하고 네트워크 파일 전파 흔적 분석을 표시합니다.

FireAMP 포털(http://amp.sourcefire.com/)을 사용하여 FireAMP 구축을 구성합니다. 이 포털을 통해 악성코드를 빠르게 식별 및 격리할 수 있습니다. 악성코드의 침입을 식별하고 전파 흔적을 추적하며 이로 인한 영향을 이해하고 성공적 복구 방법을 배울 수 있습니다. 또한 FireAMP를 사용하여 사용자 정의 보호를 만들고 그룹 정책을 기준으로 특정 애플리케이션의 실행을 차단하며 사용자 정의 화이트리스트를 작성할 수 있습니다.

네트워크 파일 전파 흔적 분석

네트워크 파일 전파 흔적 분석 기능은 네트워크에서 파일의 전송 경로를 추적합니다. 시스템은 SHA-256 해시값을 사용하여 파일을 추적하므로 파일을 추적하려면 시스템이 다음을 수행해야 합니다.

- 파일의 SHA-256 해시값을 계산하고 이 값을 사용하여 악성코드 클라우드 조회 수행
- 방어 센터를 조직의 FireAMP 구독과 통합하여 엔드포인트 기반 위협을 수신하고 해당 파일에 대한 데이터 격리

각 파일에는 관련 전파 흔적 맵이 있으며, 여기에는 시간의 추이에 따른 파일의 전송 상태를 시각적으로 보여주는 자료 및 파일에 대한 추가 정보가 포함됩니다.

애플리케이션 프로그래밍 인터페이스

API를 사용하여 시스템과 상호 작용하는 몇 가지 방법이 있습니다. 자세히 알아보려면 다음 지원 사이트 중 한 곳에서 추가 설명서를 다운로드할 수 있습니다.

- **Sourcefire:** (https://support.sourcefire.com/)
- **Cisco:** (http://www.cisco.com/cisco/web/support/index.html)

eStreamer

eStreamer(Event Streamer)에서는 Cisco 어플라이언스에서 맞춤 개발된 클라이언트 애플리케이션으로 여러 종류의 이벤트 데이터를 스트리밍할 수 있습니다. 클라이언트 애플리케이션을 만든 다음 eStreamer 서버(방어 센터 또는 관리되는 물리적 디바이스)에 연결하고 eStreamer 서비스를 시작하고 데이터 교환을 시작합니다.

eStreamer 통합은 사용자 정의 프로그래밍이 필요하지만 어플라이언스에서 특정 데이터를 요청할 수 있습니다. 예를 들어, 네트워크 관리 애플리케이션 중 하나 안에서 네트워크 호스트 데이터를 표시할 경우 방어 센터에서 호스트 중요도 또는 취약성 데이터를 검색하고 이 정보를 디스플레이에 추가할 수 있습니다.

외부 데이터베이스 액세스

데이터베이스 액세스 기능을 사용하면 JDBC SSL 연결을 지원하는 타사 클라이언트를 사용하여 방어 센터의 여러 데이터베이스 테이블을 쿼리할 수 있습니다.

Crystal Reports, Actuate BIRT 또는 JasperSoft iReport와 같은 업계 표준 보고 툴을 사용하여 쿼리를 설계 및 제출할 수 잇습니다. 또는 자체 사용자 정의 애플리케이션을 구성하여 Cisco 데이터를 쿼리할 수 있습니다. 예를 들어, 서블렛을 구축하여 침입 및 검색 이벤트 데이터를 정기적으로 보고하거나 알림 대시보드를 새로 고칠 수 있습니다.

호스트 입력

호스트 입력 기능은 스크립트 또는 명령행 파일을 사용하여 타사 소스에서 데이터를 가져오는 방법으로 네트워크 맵의 정보를 보강할 수 있습니다.

웹 인터페이스는 또한 몇 가지 호스트 입력 기능을 제공합니다. 운영 체제 또는 애플리케이션 프로토콜을 수정하거나 취약성을 식별, 검증, 무효화하고 클라이언트 및 서버 포트를 포함한 다양한 네트워크 맵에서 다양한 항목을 삭제할 수 있습니다.

교정

시스템에는 네트워크 조건이 관련 상관관계 정책 또는 규정 준수 화이트리스트를 위반할 경우 방어 센터에서 자동으로 시작하는 *교정*을 생성할 수 있는 API가 포함되어 있습니다. 이 프로그램은 문제를 즉시 해결할 수 없을 때 공격을 자동으로 완화할 뿐만 아니라 시스템이 조직의 보안 정책을 준수함을 보장할 수 있습니다. 리미디에이션을 만드는 것 이외에도, 방어 센터에는 여러 개의 사전 정의된 위협 요소 제거 모듈이 기본 제거됩니다.

문서 참고 자료

FireSIGHT 시스템 문서 집합에는 온라인 도움말과 PDF 파일이 포함됩니다. 웹 인터페이스에서 다음과 같은 방식으로 온라인 도움말에 도달할 수 있습니다.

- 각 페이지에서 상황별 도움말 링크 클릭
- **Help > Online** 선택

온라인 도움말에는 시스템 관리, 정책 관리, 이벤트 분석 등 방어 센터 또는 디바이스의 웹 인터페이스를 사용하여 완료할 수 있는 작업에 대한 정보가 포함되어 있습니다.

다음 지원 사이트 중 한 곳에서 PDF 문서의 최신 버전에 액세스할 수 있습니다.

- **Sourcefire:** (https://support.sourcefire.com/)
- **Cisco:** (http://www.cisco.com/cisco/web/support/index.html)

이곳에서 이용할 수 있는 문서

- *FireSIGHT 시스템 User Guide* - 온라인 도움말과 같은 내용을 인쇄하기 쉬운 형식으로 제공합니다.
- *FireSIGHT 시스템 Installation Guide* - Cisco 어플라이언스 설치에 대한 정보는 물론 하드웨어 사양과 보안 정보도 제공합니다.
- *FireSIGHT 시스템 Virtual Installation Guide* - 가상 디바이스 및 가상 방어 센터의 설치, 관리, 문제 해결에 대한 정보를 제공합니다.
- *Cisco NGIPS for Blue Coat X-Series Installation and Configuration Guide* - Cisco NGIPS for Blue Coat X-Series 의 설치, 관리 및 문제 해결에 대한 정보를 제공합니다.
- 각종 API 가이드 및 보충 자료

설명서 표기 규칙

이 문서에는 각 기능에 필요한 FireSIGHT 시스템 라이센스와 어플라이언스 모델, 그리고 각 절차를 완료하는 데 필요한 권한이 있는 사용자 역할에 대한 정보가 포함되어 있습니다. 자세한 내용은 다음 절을 참조하십시오.

- 1-17페이지의 라이센스 표기 규칙
- 1-18페이지의 지원되는 디바이스 및 방어 센터 표기 규칙
- 1-18페이지의 액세스 표기 규칙

라이센스 표기 규칙

절 시작 부분의 라이센스 문은 해당 절에 설명된 기능을 사용하려면 라이센스가 필요함을 나타냅니다.

FireSIGHT

FireSIGHT 라이센스는 구매한 방어 센터에 포함되어 있으며 호스트, 애플리케이션, 사용자 검색을 수행하는 데 필요합니다. 방어 센터의 FireSIGHT 라이센스에 따라, 방어 센터를 사용하여 모니터링할 수 있는 개별 호스트 및 사용자의 수, 관리되는 디바이스, 사용자 제어를 수행하는 데 사용할 수 있는 사용자 수가 결정됩니다.

보호

보호 라이센스에서는 관리되는 디바이스가 침입 감지 및 방지, 파일 제어, 보안 인텔리전스 필터링을 수행할 수 있습니다.

제어

제어 라이센스에서는 관리되는 디바이스가 사용자 및 애플리케이션 제어를 수행할 수 있습니다. 또한 디바이스가 스위칭 및 라우팅(DHCP 릴레이 포함), NAT를 수행하고 디바이스와 스택을 클러스터링할 수 있습니다. 제어 라이센스에는 보호 라이센스가 필요합니다.

URL 필터링

URL 필터링 라이센스에서는 관리되는 디바이스가 정기적으로 업데이트되는 클라우드 기반 카테고리 및 평판 데이터를 사용하고 모니터링되는 호스트에서 요청한 URL을 기준으로 네트워크를 이동할 수 있는 트래픽을 결정합니다. URL 필터링 라이센스에는 보호 라이센스가 필요합니다.

악성코드

악성코드 라이센스에서는 관리되는 디바이스가 네트워크 기반 AMP를 수행할 수 있습니다. 즉, 네트워크를 통해 전송되는 파일에서 악성코드를 탐지, 캡처 및 차단하고 동적 분석을 위해 그러한 파일을 제출할 수 있습니다. 또한 네트워크에서 전송된 파일을 추적하는 전파 흔적 분석을 볼 수 있습니다. 악성코드 라이센스에는 보호 라이센스가 필요합니다.

VPN

VPN 라이센스에서는 Cisco 관리되는 디바이스의 가상 라우터 간에 안전한 VPN 터널을 구축할 수 있습니다. VPN 라이센스에는 보호 및 제어 라이센스가 필요합니다.

라이센스된 기능은 종종 누적되므로 이 문서에서는 각 기능에서 가장 필요한 라이센스만 제공합니다. 예를 들어 기능에 FireSIGHT, 보호 및 제어 라이센스가 필요한 경우 제어만 나열됩니다.

라이센스 문의 "or" 문은 해당 절에서 설명하는 기능을 사용하려면 특정 라이센스가 필요하지만, 추가 라이센스는 기능을 추가할 수 있음을 나타냅니다. 예를 들어, 파일 정책 내에서 일부 파일 규칙 작업에는 보호 라이센스가 필요하지만 다른 작업에는 악성코드 라이센스가 필요합니다. 따라서 파일 규칙에 대한 문서의 라이센스 문에는 "보호 or 악성코드"가 나열됩니다.

아키텍처 및 리소스 제한으로 인해, 모든 라이센스를 관리되는 모든 디바이스에 적용할 수는 없습니다. 일반적으로 디바이스가 지원하지 않는 기능의 라이센스를 취득할 수 없습니다. 1-5페이지의 관리되는 디바이스 모델에서 지원되는 기능 요약을/를 참조하십시오. 자세한 내용은 65-1페이지의 라이센싱 이해을/를 참조하십시오.

지원되는 디바이스 및 방어 센터 표기 규칙

절 시작 부분의 지원되는 디바이스 문은 지정된 디바이스 시리즈, 제품군 또는 모델에서만 기능이 지원됨을 나타냅니다. 예를 들어 스태킹은 Series 3 디바이스에서만 지원됩니다. 절에 지원되는 디바이스 문이 없으면 해당 기능이 모든 디바이스에서 지원되거나 해당 절이 관리되는 디바이스에 적용되지 않는 것입니다.

이 릴리스에서 지원되는 플랫폼에 대한 자세한 내용은 1-7페이지의 방어 센터 소개을/를 참조하십시오.

액세스 표기 규칙

이 문서 각 절차 시작 부분의 액세스 문은 절차 수행에 필요한 사전 정의된 사용자 역할을 나타냅니다. 슬래시로 구분한 역할은 나열된 역할 중 하나로 절차를 수행할 수 있음을 나타냅니다. 다음 표에는 액세스 문에 나타나는 일반적인 용어가 정의되어 있습니다.

표 1-6 액세스 표기 규칙

액세스 용어	표시 내용
Access Admin	사용자에게 Access Control Admin 역할이 필요함
관리자	사용자에게 Administrator 역할이 필요함
모두	사용자 역할이 무엇이든 상관없음
Any/Admin	사용자 역할이 무엇이든 상관없지만, Administrator 역할은 무제한의 액세스 권한을 가짐(예: 비공개로 저장된 사용자 데이터를 볼 수 있음)
Any Security Analyst	사용자에게 Security Analyst 또는 Security Analyst(Read Only) 역할이 필요함
데이터베이스	사용자에게 External Database 역할이 필요함
Discovery Admin	사용자에게 Discovery Admin 역할이 필요함
Intrusion Admin	사용자에게 Intrusion Admin 역할이 필요함
Maint	사용자에게 Maintenance User 역할이 필요함
네트워크 관리자	사용자에게 Network Admin 역할이 필요함
보안 분석가	사용자에게 Security Analyst 역할이 필요함
Security Approver	사용자에게 Security Approver 역할이 필요함

사용자 지정 역할이 있는 사용자는 사전 정의 역할의 사용자와 다른 권한 집합을 가질 수 있습니다. 절차에 대한 액세스 요구 사항을 나타내는 데 사전 정의 역할이 사용된 경우, 유사한 권한의 사용자 지정 역할도 액세스 권한을 갖게 됩니다. 사용자 지정 역할이 있는 일부 사용자에게는 컨피그레이션 페이지에 도달하는 데 약간 다른 메뉴 경로가 표시될 수 있습니다. 예를 들어 침입 정책 권한만 있는 사용자 지정 역할을 가지고 있는 사용자는 액세스 제어 정책을 통한 표준 경로가 아니라 침입 정책을 통해 네트워크 분석 정책에 액세스할 수 있습니다. 사용자 지정 사용자 역할에 대한 자세한 내용은 61-51페이지의 사용자 지정 사용자 역할 관리을/를 참조하십시오.

IP 주소 표기 규칙

FireSIGHT 시스템의 많은 곳에서 주소 블록을 정의하기 위해 IPv4 CIDR(Classless Inter-Domain Routing) 표기법 및 유사한 IPv6 접두사 길이 표기법을 사용할 수 있습니다.

CIDR 표기법에서는 IP 주소와 비트 마스크를 함께 사용하여 지정된 주소 블록에서 IP 주소를 정의합니다. 예를 들어 다음 표에서 CIDR 표기법에는 사설 IPv4 주소 공간이 나열되어 있습니다.

표 1-7 CIDR 표기법 구문 예

CIDR 블록	CIDR 블록의 IP 주소	서브넷 마스크	IP 주소 수
10.0.0.0/8	10.0.0.0 - 10.255.255.255	255.0.0.0	16,777,216
172.16.0.0/12	172.16.0.0 - 172.31.255.255	255.240.0.0	1,048,576
192.168.0.0/16	192.168.0.0 - 192.168.255.255	255.255.0.0	65,536

마찬가지로, IPv6에서는 IP 주소와 접두사 길이를 함께 사용하여 지정된 블록에서 IP 주소를 정의합니다. 예를 들어 2001:db8::/32는 2001:db8:: 네트워크에서 접두사 길이 32비트(즉, 2001:db8::~2001:db8:ffff:ffff:ffff:ffff:ffff:ffff)의 IPv6 주소를 지정합니다.

IP 주소 블록을 지정하기 위해 CIDR 또는 접두사 길이 표기를 사용할 경우 FireSIGHT 시스템은 마스크 또는 접두사 길이로 지정된 네트워크 IP 주소 **부분만** 사용합니다. 예를 들어 10.1.2.3/8을 지정하면 FireSIGHT 시스템은 10.0.0.0/8을 사용합니다.

다시 말해, Cisco에서는 CIDR 또는 접두사 길이 표기법을 사용할 때 비트 경계에서 네트워크 IP 주소를 사용하는 표준 방법을 권장합니다. FireSIGHT 시스템에서는 이 방법을 요구하지 않습니다.

FireSIGHT 시스템에 로그인

이 장에서는 어플라이언스 기반 웹 인터페이스 및 CLI(명령줄 인터페이스)를 사용하여 FireSIGHT 시스템에 로그인하고 로그아웃하기 위해 필요한 단계에 대해 자세히 설명합니다. 또한 LDAP 또는 RADIUS 자격 증명을 사용하는 외부 인증 사용자 계정도 구성할 수 있습니다.

웹 인터페이스에 로그인한 후 포인터를 특정 영역 위로 이동하면 *컨텍스트 메뉴* 기능에서 추가 정보 및 유용한 탐색 링크를 제공합니다.

자세한 내용은 다음 절을 참조하십시오.

어플라이언스에 로그인

라이센스: 모두

FireSIGHT 시스템 방어 센터에는 관리 및 분석 작업을 수행하는 데 사용할 수 있는 웹 인터페이스가 있습니다. 관리되는 물리적 디바이스에는 또한 초기 설정과 기본 분석 및 컨피그레이션 작업을 수행하기 위해 사용할 수 있는 웹 인터페이스도 있습니다. 브라우저 요구 사항에 대한 자세한 내용은 FireSIGHT 시스템의 현재 버전에 대한 릴리스 정보를 참조하십시오.

관리되는 가상 디바이스에는 웹 인터페이스가 없습니다. 이러한 디바이스(그리고 Series 3 디바이스)에 대해 FireSIGHT 시스템은 인터랙티브 CLI를 제공하는데, 디바이스의 관리하는 방어 센터를 사용하여 완료할 수 없는 작업을 이 CLI로 수행할 수 있습니다.

Cisco NGIPS for Blue Coat X-Series에도 웹 인터페이스가 없습니다. 그러나 X-Series 플랫폼에 고유한 CLI가 있습니다. 이 CLI를 사용하여 시스템을 설치하고 다른 플랫폼별 관리 작업을 수행할 수 있습니다. X-Series 플랫폼 CLI에 로그인하는 방법을 비롯한 자세한 내용은 *Cisco NGIPS for Blue Coat X-Series Installation and Configuration Guide*를 참조하십시오.

ASA FirePOWER 디바이스에는 ASA 디바이스를 구성하기 위한 고유한 관리 애플리케이션(ASDM 및 CSM)과 CLI가 있습니다. 또한 FireSIGHT 시스템은 인터랙티브 CLI를 제공하는데, 디바이스의 관리하는 방어 센터를 사용하여 완료할 수 없는 작업을 이 CLI로 수행할 수 있습니다. ASA별 툴을 사용하여 시스템을 설치하고 다른 플랫폼별 관리 작업을 수행할 수 있습니다. 자세한 내용은 ASA 설명서를 참조하십시오.

참고 FirePOWER 어플라이언스는 사용자 계정을 기반으로 사용자 활동을 감사하므로, 사용자들이 올바른 계정으로 시스템에 로그인하도록 해야 합니다.

어플라이언스의 웹 인터페이스, CLI 또는 셸에 액세스하려면 사용자 이름과 비밀번호를 제공해야 합니다. 어플라이언스에 로그인하면, 액세스 가능한 기능은 사용자 계정에 허용되는 권한에 의해 제어됩니다. 자세한 내용은 61-43페이지의 사용자 계정 관리을/를 참조하십시오.

선택적으로, 조직에서 인증에 CAC(Common Access Cards)를 사용하는 경우 CAC 자격 증명을 사용하여 어플라이언스의 웹 인터페이스에 대한 액세스를 얻을 수 있습니다. CAC 인증 및 권한 부여에 대한 자세한 내용은 61-9페이지의 CAC를 사용하는 LDAP 인증 이해을/를 참조하십시오.

주의 잘못된 자격 증명을 여러 번 제공하면 셸 액세스 계정이 잠길 수 있습니다. 올바른 자격 증명을 제공하는데 로그인이 거부되면 로그인을 반복해서 시도하기보다는 시스템 관리자에게 문의하십시오.

웹 세션 중 어플라이언스 홈 페이지를 처음 방문하면 해당 어플라이언스의 마지막 로그인 세션에 대한 정보를 볼 수 있습니다. 마지막 로그인에 대한 다음 정보를 볼 수 있습니다.

- 로그인한 요일, 월, 날짜 및 연도
- 24시간 표기법의 어플라이언스 로컬 로그인 시간
- 어플라이언스에 액세스하기 위해 마지막으로 사용한 호스트 및 도메인 이름

세션 시간 초과에서 제외되도록 달리 구성하지 않는 한, 기본적으로 1시간 동안 활동이 없으면 세션에서 자동으로 로그아웃됩니다. Administrator 역할이 있는 사용자는 시스템 정책에서 세션 시간 초과 간격을 변경할 수 있습니다. 자세한 내용은 61-47페이지의 사용자 로그인 설정 관리 및 63-29페이지의 사용자 인터페이스 설정 구성을/를 참조하십시오.

상당한 시간이 걸리는 프로세스의 경우 웹 브라우저에 스크립트가 응답하지 않는다는 메시지가 표시될 수 있습니다. 이러한 경우 완료될 때까지 스크립트가 계속 진행되도록 해야 합니다.

참고 어플라이언스에 시스템을 새로 설치하는 경우 초기 설치 프로세스를 완료하려면 관리(admin) 사용자 계정으로 로그인해야 합니다. 자세한 내용은 *FireSIGHT 시스템 Installation Guide*를 참조하십시오. 61-44페이지의 새 사용자 계정 추가에 설명된 대로 다른 사용자 계정을 생성한 후에는 모든 사용자가 웹 인터페이스에 로그인하는 데 새로 생성된 계정을 사용해야 합니다.

팁 네트워크의 사용자가 CAC 자격 증명을 사용하여 CAC Login 페이지에 로그인하기 전에 CAC 인증 및 권한 부여를 **반드시** 구성해야 합니다. 자세한 내용은 61-9페이지의 CAC를 사용하는 LDAP 인증 이해을/를 참조하십시오.

웹 인터페이스를 통해 어플라이언스에 로그인하려면

액세스: 모두

1단계 브라우저 주소 창에 `https://hostname/`을 입력합니다. 여기서 *hostname*은 어플라이언스의 호스트 이름에 해당합니다.

로그인 페이지가 나타납니다.

2단계 **Username** 및 **Password** 필드에 사용자 이름과 비밀번호를 입력합니다. 사용자 이름은 대/소문자를 구분합니다.

조직에서 로그인 시 SecurID® 토큰을 사용하는 경우 토큰을 SecurID PIN에 추가하고 이를 로그인 시 비밀번호로 사용하십시오. 예를 들어 PIN이 `1111`이고 SecurID 토큰이 `222222`이면 `1111222222`를 입력합니다. FireSIGHT 시스템에 로그인하기 전에 SecurID PIN을 먼저 생성해야 합니다.

3단계 **Login**을 클릭합니다.

기본 시작 페이지가 나타납니다. 사용자 계정에 대해 사용자 지정 홈 페이지를 선택한 경우 해당 페이지가 대신 표시됩니다. 자세한 내용은 71-2페이지의 홈 페이지 지정을/를 참조하십시오.

팁 웹 인터페이스에 액세스할 수 없는 경우 관리자에게 연락하여 계정 권한을 수정해달라고 하거나, Administrator 권한의 사용자로 로그인하여 계정에 대한 권한을 수정하십시오. 자세한 내용은 61-54페이지의 사용자 권한 및 옵션 수정을/를 참조하십시오.

페이지 상단에 나열되는 메뉴 및 메뉴 옵션은 사용자 계정에 대한 권한을 기반으로 합니다. 그러나 기본 홈 페이지에 대한 링크에는 사용자 계정 권한 전반을 포괄하는 옵션이 포함되어 있습니다. 자신의 계정에 허용된 권한과 다른 권한을 필요로 하는 링크를 클릭하면 다음 경고 메시지가 표시됩니다.

```
You are attempting to view an unauthorized page. This activity has been logged.
```

사용 가능한 메뉴에서 다른 옵션을 선택하거나 브라우저 창에서 **Back**을 클릭하여 이전 페이지로 돌아갈 수 있습니다.

CAC 자격 증명을 사용하여 웹 인터페이스를 통해 어플라이언스에 로그인하려면

액세스: 모두

1단계 조직에서 안내하는 대로 CAC를 삽입합니다.

2단계 브라우저 주소 창에 `https://`*`hostname`*`/`을 입력합니다. 여기서 *hostname*은 어플라이언스의 호스트 이름에 해당합니다.

3단계 프롬프트가 나타나면 1단계에서 삽입한 CAC의 PIN을 입력합니다.

PIN이 승인됩니다.

4단계 프롬프트가 나타나면 드롭다운 목록에서 알맞은 인증서를 선택합니다.

브라우저에서 사용자의 선택 사항을 수용하면 CAC Login 페이지가 나타납니다.

5단계 CAC 자격 증명으로 인증을 받으려면 **Continue**를 클릭합니다.

사용자 이름과 비밀번호를 사용하여 인증을 받으려면 **Username** 및 **Password** 필드에 입력합니다. 사용자 이름은 대/소문자를 구분합니다.

기본 시작 페이지가 나타납니다. 사용자 계정에 대해 사용자 지정 홈 페이지를 선택한 경우 해당 페이지가 대신 표시됩니다. 자세한 내용은 71-2페이지의 홈 페이지 지정을/를 참조하십시오.

팁 웹 인터페이스에 액세스할 수 없는 경우 관리자에게 연락하여 계정 권한을 수정해달라고 하거나, Administrator 권한의 사용자로 로그인하여 계정에 대한 권한을 수정하십시오. 자세한 내용은 61-54페이지의 사용자 권한 및 옵션 수정을/를 참조하십시오.

페이지 상단에 나열되는 메뉴 및 메뉴 옵션은 사용자 계정에 대한 권한을 기반으로 합니다. 그러나 기본 홈 페이지에 대한 링크에는 사용자 계정 권한 전반을 포괄하는 옵션이 포함되어 있습니다. 자신의 계정에 허용된 권한과 다른 권한을 필요로 하는 링크를 클릭하면 다음 경고 메시지가 표시됩니다.

```
You are attempting to view an unauthorized page. This activity has been logged.
```

사용 가능한 메뉴에서 다른 옵션을 선택하거나 브라우저 창에서 **Back**을 클릭하여 이전 페이지로 돌아갈 수 있습니다.

참고 활성 브라우징 세션 중에는 CAC를 제거하지 **마십시오**. 세션 중에 CAC를 제거하거나 대체할 경우 웹 브라우저는 세션을 종료하며 웹 인터페이스에서 로그아웃됩니다.

명령줄을 통해 Series 3, 가상 또는 ASA FirePOWER 디바이스에 로그인하려면

액세스: CLI 기본 컨피그레이션

1단계 Series 3 및 가상 디바이스의 경우 *hostname*에서 어플라이언스에 대한 SSH 연결을 엽니다. 여기서 *hostname*은 어플라이언스의 호스트 이름에 해당합니다. ASA FirePOWER 디바이스의 경우 관리 주소에서 ASA FirePOWER 모듈에 대한 SSH 연결을 엽니다.

`login as:` 명령 프롬프트가 나타납니다.

2단계 사용자 이름을 입력하고 Enter를 누릅니다.

`Password:` 프롬프트가 나타납니다.

3단계 비밀번호를 입력하고 Enter를 누릅니다.

조직에서 로그인 시 SecurID® 토큰을 사용하는 경우 토큰을 SecurID PIN에 추가하고 이를 로그인 시 비밀번호로 사용하십시오. 예를 들어 PIN이 `1111`이고 SecurID 토큰이 `222222`이면 `1111222222`를 입력합니다. FireSIGHT 시스템에 로그인하기 전에 SecurID PIN을 먼저 생성해야 합니다.

로그인 배너가 나타나고 그 뒤에 `>` 프롬프트가 나타납니다.

사용자는 자신의 명령줄 액세스 레벨에서 허용되는 명령을 사용할 수 있습니다. 사용 가능한 CLI 명령에 대한 자세한 내용은 D-1페이지의 명령줄 참조을/를 참조하십시오.

어플라이언스에서 로그아웃

라이센스: 모두

웹 인터페이스를 더 이상 활발하게 사용하지 않는 경우 Cisco에서는 로그아웃할 것을 권장합니다. 잠시 웹 브라우저에서 떨어져 있는 경우에도 마찬가지입니다. 로그아웃하면 웹 세션이 종료되며, 내 자격 증명으로 타인이 어플라이언스를 사용할 수 없습니다.

세션 시간 초과에서 제외되도록 달리 구성하지 않는 한, 기본적으로 1시간 동안 활동이 없으면 세션에서 자동으로 로그아웃됩니다. Administrator 역할이 있는 사용자는 시스템 정책에서 세션 시간 초과 간격을 변경할 수 있습니다. 자세한 내용은 61-47페이지의 사용자 로그인 설정 관리 및 63-29 페이지의 사용자 인터페이스 설정 구성을/를 참조하십시오.

어플라이언스에서 로그아웃하려면

액세스: 모두

1단계 툴바에서 **Logout**을 클릭합니다.

컨텍스트 메뉴 사용

라이센스: 기능에 따라 다름

사용자 편의를 위해, 웹 인터페이스의 특정 페이지는 FireSIGHT 시스템의 다른 기능에 액세스하기 위한 바로 가기로 사용할 수 있는 팝업 컨텍스트 메뉴를 지원합니다. 메뉴의 내용은 액세스하는 *핫스팟*(페이지 및 특정 데이터)에 따라 달라집니다.

예를 들어 이벤트 보기, 침입 이벤트 패킷 보기, 대시보드, Context Explorer의 *IP 주소 핫스팟*은 추가 옵션을 제공합니다. 사용 가능한 whois 및 호스트 프로필 정보를 포함하여 해당 주소와 관련된 호스트에 대해 자세히 알아보려면 핫스팟을 마우스 오른쪽 버튼으로 클릭하여 IP 주소 컨텍스트 메뉴를 사용합니다. 보안 인텔리전스 필터링을 지원하지 않는 DC500 방어 센터를 제외하고, 보안 인텔리전스 전역 화이트리스트 또는 블랙리스트에 개별 IP 주소를 추가할 수도 있습니다.

또 다른 예로, 이벤트 보기 및 대시보드의 *SHA-256 값 핫스팟*을 사용하면 파일의 SHA-256 해시 값을 정상 목록 또는 사용자 지정 탐지 목록에 추가하거나, 복사하기 위한 전체 해시 값을 볼 수 있습니다. 이 기능 역시 DC500 방어 센터에서는 지원되지 않습니다.

다음 목록에서는 웹 인터페이스의 여러 페이지에 있는 컨텍스트 메뉴에서 사용할 수 있는 많은 옵션에 대해 설명합니다. Cisco 컨텍스트 메뉴가 지원되지 않는 페이지나 위치에는 브라우저의 일반 컨텍스트 메뉴가 나타납니다.

액세스 제어, SSL 및 NAT 정책 편집기

액세스 제어, SSL 및 NAT 정책 편집기에는 각 규칙에 대한 핫스팟이 포함되어 있습니다. 컨텍스트 메뉴를 사용하면 규칙 잘라내기, 복사, 붙여넣기, 규칙 상태 설정, 규칙 수정 등 새 규칙 및 카테고리를 삽입할 수 있습니다.

침입 규칙 편집기

침입 규칙 편집기에는 각 침입 규칙에 대한 핫스팟이 포함되어 있습니다. 컨텍스트 메뉴를 사용하면 규칙을 수정하고, 규칙 상태를 설정하고(규칙 비활성화 포함), 임계값 지정 및 억제 옵션을 구성하고, 규칙 설명서를 볼 수 있습니다.

이벤트 뷰어

이벤트 페이지(드릴다운 페이지 및 테이블 보기)에는 각 이벤트, IP 주소, 탐지된 특정 파일의 SHA-256 해시 값에 대한 핫스팟이 포함되어 있습니다. 대부분의 이벤트 유형에서 컨텍스트 메뉴를 사용하면 Context Explorer에서 관련 정보를 보거나, 새 창에서 이벤트 정보로 드릴다운할 수 있습니다. 이벤트 필드에 포함된 텍스트가 너무 길어 이벤트 보기에 모두 표시할 수 없는 경우(예: 파일의 SHA-256 해시 값, 취약성 설명, URL), 컨텍스트 메뉴를 사용하면 전체 텍스트를 볼 수 있습니다.

캡처된 파일, 파일 이벤트 및 악성코드 이벤트의 경우 컨텍스트 메뉴를 사용하면 정상 목록 또는 사용자 지정 탐지 목록에 파일을 추가하거나 제거하고, 파일 복사본을 다운로드하고, 아카이브 파일 내 중첩된 파일을 보고, 중첩된 파일에 대한 부모 아카이브 파일을 다운로드하거나, 동적 분석을 위해 종합 보안 인텔리전스 클라우드에 파일을 제출할 수 있습니다.

침입 이벤트의 경우 컨텍스트 메뉴를 사용하면 침입 규칙 편집기나 침입 정책의 경우와 유사한 작업을 수행할 수 있습니다. 즉, 트리거링 규칙을 수정하고, 규칙 상태를 설정하고(규칙 비활성화 포함), 임계값 지정 및 억제 옵션을 구성하고, 규칙 설명서를 볼 수 있습니다.

패킷 보기

침입 이벤트 패킷 보기에는 IP 주소 핫스팟이 포함되어 있습니다. 패킷 보기는 오른쪽 클릭 메뉴 대신 왼쪽 클릭 컨텍스트 메뉴를 사용합니다.

대시보드

많은 대시보드 위젯에 Context Explorer에서 관련 정보를 볼 수 있는 핫스팟이 포함되어 있습니다. 대시보드 위젯에는 또한 IP 주소 및 SHA-256 값 핫스팟도 포함할 수 있습니다.

Context Explorer

Context Explorer에는 차트, 테이블 및 그래프에 핫스팟이 포함되어 있습니다. Context Explorer에서 허용하는 것보다 더 자세히 그래프 또는 목록의 데이터를 검사하려면 관련 데이터의 테이블 보기로 드릴다운할 수 있습니다. 관련 호스트, 사용자, 애플리케이션, 파일 및 침입 규칙 정보도 볼 수 있습니다.

Context Explorer는 왼쪽 클릭 컨텍스트 메뉴를 사용하며, 여기에는 Context Explorer의 고유한 필터링 및 기타 옵션도 포함됩니다. 자세한 내용은 56-39페이지의 Context Explorer 데이터에 대해 드릴다운을/를 참조하십시오.

컨텍스트 메뉴에 액세스하려면

액세스: 모두

1단계 웹 인터페이스의 핫스팟 활성 페이지에서 핫스팟 위로 포인터를 이동합니다.

Context Explorer를 제외하고, `Right-click for menu` 메시지가 나타납니다.

2단계 컨텍스트 메뉴를 호출합니다.

- Context Explorer 또는 패킷 보기에서 포인팅 디바이스를 마우스 왼쪽 버튼으로 클릭합니다.
- 핫스팟이 활성화된 다른 모든 페이지에서는 포인팅 디바이스를 마우스 오른쪽 버튼으로 클릭합니다.

핫스팟에 적합한 옵션과 함께 팝업 컨텍스트 메뉴가 나타납니다.

3단계 옵션의 이름을 마우스 왼쪽 버튼으로 클릭하여 옵션 중 하나를 선택합니다.

액세스 제어 정책 편집기 또는 NAT 정책 편집기를 사용 중인 경우 규칙이 수정됩니다. 그렇지 않은 경우 선택한 옵션을 기반으로 새 브라우저 창이 나타납니다.

3장 재사용 가능 객체 관리

유연성 및 웹 인터페이스 사용 편이성을 높이기 위해 FireSIGHT 시스템에서는 명명된 *객체*의 생성을 허용합니다. 객체는 이름과 값이 연결된 재사용 가능 컨피그레이션으로서, 값을 사용하고자 할 때 대신 명명된 객체를 사용할 수 있습니다.

다음과 같은 유형의 객체를 생성할 수 있습니다.

- IP 주소 및 네트워크, 포트/프로토콜 쌍, VLAN 태그, 보안 영역, 원래/목적지 국가(지오로케이션)를 나타내는 네트워크 기반 객체
- 보안 인텔리전스 피드와 목록, 카테고리와 평판을 기반으로 하는 애플리케이션 필터, 파일 목록 등을 나타내는 평판 기반 객체
- URL 카테고리와 같이 평판을 기반으로 하지 않는 객체
- 침입 정책과 관련된 변수를 포함하는 침입 정책 변수 집합
- 암호 그룹, 공개 키 인증서 및 페이링된 개인 키, 인증서 DN 등 암호화된 트래픽 처리에 도움이 되는 객체

액세스 제어 정책, 네트워크 분석 정책, 침입 정책과 규칙, 네트워크 검색 규칙, 이벤트 검색, 보고서, 대시보드 등 시스템 웹 인터페이스의 여러 곳에서 이러한 객체를 사용할 수 있습니다.

객체를 그룹화하면 단일 컨피그레이션으로 여러 객체를 참조할 수 있습니다. 네트워크, 포트, VLAN 태그, URL 및 PKI(public key infrastructure) 객체를 그룹화할 수 있습니다.

참고 대부분의 경우 정책에 사용된 객체를 수정하면 정책을 다시 적용해야 변경 사항이 반영됩니다. 보안 영역을 수정하는 경우에도 해당 디바이스 컨피그레이션을 다시 적용해야 합니다.

자세한 내용은 다음 절을 참조하십시오.

객체 관리자 사용

라이센스: 모두

객체 관리자(**Objects > Object Management**)를 사용하여 애플리케이션 필터, 변수 집합, 보안 영역을 비롯한 객체를 생성 및 관리할 수 있습니다. 네트워크, 포트, VLAN 태그, URL 및 PKI 객체를 그룹화할 수 있습니다. 또한 객체 및 객체 그룹의 목록을 정렬, 필터링 및 탐색할 수 있습니다.

자세한 내용은 다음 링크를 참고하십시오.

객체 그룹화

라이센스: 모두

네트워크, 포트, VLAN 태그, URL 및 PKI 객체를 그룹화할 수 있습니다. 웹 인터페이스에서 객체와 객체 그룹을 상호 교환하여 사용할 수 있습니다. 예를 들어, 포트 객체를 사용할 수 있는 경우 포트 객체 그룹을 사용할 수도 있습니다. 동일한 유형의 객체 및 객체 그룹은 동일한 이름을 가질 수 있습니다.

팁 암호 그룹을 그룹화하려면 암호 그룹 목록을 구성하십시오. 자세한 내용은 3-40페이지의 암호 그룹 목록 작업을/를 참조하십시오.

정책에 사용되는 객체 그룹을 수정하는 경우(예: 액세스 제어 정책에 사용되는 네트워크 객체 그룹), 변경 사항을 반영하려면 정책을 다시 적용해야 합니다.

그룹을 삭제하는 경우 그룹 내 객체가 삭제되는 것이 아니라 서로의 관계가 해제되는 것입니다. 사용 중인 그룹은 삭제할 수 없습니다. 예를 들어, 저장된 액세스 제어 정책의 VLAN 조건에서 사용 중인 VLAN 태그 그룹은 삭제할 수 없습니다.

재사용 가능 객체를 그룹화하려면

액세스: Admin/Access Admin/Network Admin

1단계 **Objects > Object Management**를 선택합니다.

Object Management 페이지가 나타납니다.

2단계 다음 옵션을 이용할 수 있습니다.

- 그룹화하려는 **Network**, **Port**, **VLAN Tag**, **URL** 또는 **Distinguished Name** 객체 유형 아래에서 **Object Groups**를 선택합니다.
- **PKI** 아래에서, 그룹화하려는 PKI 객체 유형에 대해 **Internal CA Groups**, **Trusted CA Groups**, **Internal Cert Groups**, 또는 **External Cert Groups**를 선택합니다.

그룹화하는 객체 유형의 페이지가 나타납니다.

3단계 그룹화하려는 객체에 해당하는 **Add** 버튼을 클릭합니다.

그룹을 생성할 수 있는 팝업 창이 나타납니다.

4단계 그룹의 **Name**을 입력합니다. 파이프(|) 또는 중괄호({})를 제외한 인쇄 가능한 표준 ASCII 문자를 사용할 수 있습니다.

5단계 하나 이상의 객체를 선택하고 **Add**를 클릭합니다.

- Shift 및 Ctrl 키를 사용하여 여러 객체를 선택하거나, 마우스 오른쪽 버튼을 클릭하고 **Select All**을 선택합니다.
- 포함할 기존 객체를 검색하려면 필터 필드( )를 사용합니다. 이 필드는 입력 시 업데이트되어 일치하는 항목을 표시합니다. 검색 문자열을 지우려면 검색 필드 위의 다시 로드 아이콘( )을 클릭하거나, 검색 필드의 지우기 아이콘( )을 클릭합니다.
- 요구에 맞는 기존 객체가 없는 경우 추가 아이콘( )을 클릭하여 즉석에서 객체를 생성합니다.

6단계 **Save**를 클릭합니다.

그룹이 생성됩니다.

객체 찾아보기, 분류 및 필터링

라이센스: 모두

객체 관리자에서는 페이지당 20개의 객체 또는 그룹이 표시됩니다. 객체 또는 그룹 유형이 20개가 넘는 경우 추가 페이지를 보려면 페이지 하단의 탐색 링크를 사용하십시오. 특정 페이지로 이동할 수도 있고 새로 고침 아이콘( )을 클릭하여 보기를 새로 고칠 수도 있습니다.

기본적으로 페이지에는 객체 및 그룹이 이름별 알파벳순으로 나열됩니다. 그러나 표시된 보기에서 열을 기준으로 객체 또는 그룹의 각 유형을 정렬할 수 있습니다. 열 머리글 옆의 위쪽(▲) 또는 아래쪽(▼) 화살표는 해당 열이 그 방향으로 정렬됨을 나타냅니다. 페이지의 객체를 이름별로 필터링할 수도 있습니다. 일부 객체 유형의 경우 동일한 필터가 이름 또는 값에 대해 매칭합니다.

객체 또는 그룹을 정렬하려면

액세스: Admin/Access Admin/Network Admin

1단계 열 머리글을 클릭합니다. 반대 방향으로 정렬하려면 머리글을 다시 클릭합니다.

객체 또는 그룹을 필터링하려면

액세스: Admin/Access Admin/Network Admin

1단계 **Filter** 필드에 필터 기준을 입력합니다.

입력하여 일치하는 항목이 표시됨에 따라 페이지가 업데이트됩니다. 다음 메타 문자를 사용할 수 있습니다.

- 별표[*]는 0번 이상 나타나는 문자를 매칭합니다.
- 캐럿(^)은 문자열의 시작 부분에 있는 내용을 매칭합니다.
- 달러 기호($)는 문자열의 끝 부분에 있는 내용을 매칭합니다.

네트워크 객체 작업

라이센스: 모두

네트워크 객체는 개별적으로 또는 주소 블록으로 지정할 수 있는 하나 이상의 IP 주소를 나타냅니다. 액세스 제어 정책, 네트워크 변수, 침입 규칙, 네트워크 검색 규칙, 이벤트 검색, 보고서 등 시스템 웹 인터페이스의 여러 곳에서 네트워크 객체 및 그룹(3-2페이지의 객체 그룹화 참조)을 사용할 수 있습니다.

사용 중인 네트워크 객체는 삭제할 수 없습니다. 또한 액세스 제어, 네트워크 검색 또는 침입 정책에 사용된 네트워크 객체를 수정한 후 변경 사항을 반영하려면 정책을 다시 적용해야 합니다.

네트워크 객체를 생성하려면

액세스: Admin/Access Admin/Network Admin

1단계 **Objects > Object Management**를 선택합니다.

Object Management 페이지가 나타납니다.

2단계 **Network** 아래에서 **Individual Objects**를 선택합니다.

3단계 **Add Network**를 클릭합니다.

Network Objects 팝업 창이 나타납니다.

4단계 네트워크 객체의 **Name**을 입력합니다. 파이프(|) 또는 중괄호({})를 제외한 인쇄 가능한 표준 ASCII 문자를 사용할 수 있습니다.

5단계 네트워크 객체에 추가하고자 하는 각 IP 주소 또는 주소 블록에 대해 값을 입력하고 **Add**를 클릭합니다.

6단계 **Save**를 클릭합니다.

네트워크 객체가 추가됩니다.

보안 인텔리전스 목록 및 피드 작업

라이센스: 보호

지원되는 디바이스: Series 2를 제외한 모두

지원되는 Defense Center: DC500을 제외한 모두

액세스 제어 정책에 따라 보안 인텔리전스 기능을 사용하면 소스 또는 대상 IP 주소를 기준으로 지정된 트래픽이 네트워크를 이동하도록 설정할 수 있습니다. 이 기능은 트래픽을 분석하기 전에 특정 IP 주소 사이에서 이동하는 트래픽을 블랙리스트에 추가(거부)하려는 경우 특히 유용합니다. 이와 마찬가지로, IP 주소를 화이트리스트에 추가하면 시스템에서 액세스 제어를 사용하여 연결을 처리하도록 할 수 있습니다.

특정 IP 주소를 블랙리스트에 추가해야 할지 확실치 않으면 "모니터링 전용" 설정을 사용할 수 있습니다. 그러면 시스템에서는 액세스 제어를 사용하여 연결을 처리하는 것은 물론 연결의 일치 내용을 블랙리스트에 로깅할 수 있습니다.

모든 액세스 제어 정책에는 *전역 화이트리스트* 및 *전역 블랙리스트*가 기본적으로 포함되며 모든 영역에 적용됩니다. 또한 각 액세스 제어 정책 내에서 네트워크 개체와 그룹, 보안 인텔리전스 리스트 및 피드를 조합하여 별도의 화이트리스트 및 블랙리스트를 생성할 수 있으며, 이러한 모든 항목은 보안 영역으로 제한할 수 있습니다.

참고 기본적으로 다른 모든 보호 기능이 있더라도 Series 2 디바이스는 보안 인텔리전스 필터링을 수행할 수 없습니다.

피드 및 목록 비교

보안 인텔리전스 *피드*는 방어 센터가 사용자가 구성한 간격으로 HTTP 또는 HTTPS 서버에서 다운로드하는 IP 주소의 동적 컬렉션입니다. 피드는 정기적으로 업데이트되므로 시스템에서는 최신 정보를 사용하여 네트워크 트래픽을 필터링할 수 있습니다. 블랙리스트 작성을 돕기 위해 Cisco에서는 *인텔리전스 피드*(*Sourcefire 인텔리전스 피드*라고도 함)를 제공합니다. 인텔리전스 피드는 Cisco VRT에서 부정적인 평판을 받은 IP 주소를 나타냅니다.

방어 센터는 업데이트된 피드 정보를 다운로드할 때 관리되는 디바이스를 자동으로 업데이트합니다. 피드 업데이트가 구축 전체에서 반영되는 데 몇 분 정도 걸릴 수 있지만, 피드를 생성하거나 수정한 후 또는 예약된 피드 업데이트 후 액세스 제어 정책을 다시 적용할 필요는 없습니다.

참고 방어 센터가 인터넷에서 피드를 다운로드하는 시기를 엄격하게 제어하려면 해당 피드의 자동 업데이트를 비활성화할 수 있습니다. 그러나 Cisco에서는 자동 업데이트를 허용할 것을 권장합니다. 온디맨드 업데이트를 수동으로 수행할 수 있지만, 시스템이 정기적으로 피드를 다운로드하도록 허용하면 최신 관련 데이터를 얻을 수 있습니다.

피드와는 대조적인 보안 인텔리전스 *목록*은 방어 센터에 수동으로 업로드하는 IP 주소의 간단한 정적 목록입니다. 피드 및 전역 화이트리스트와 블랙리스트를 늘리고 세부적으로 조정하려면 사용자 지정 목록을 사용할 수 있습니다. 사용자 지정 목록을 수정하는 경우(또한 네트워크 객체를 수정하고 전역 화이트리스트나 블랙리스트에서 IP 주소를 제거하는 경우) 변경 사항을 반영하려면 액세스 제어 정책을 적용해야 합니다.

피드 데이터 서식 및 손상

피드와 목록 소스는 500MB를 넘지 않는 간단한 텍스트 파일이어야 하며, 한 줄에 하나의 IP 주소 또는 주소 블록이 있어야 합니다. 명령줄은 # 문자로 시작해야 합니다. 목록 소스 파일은 `.txt` 확장자를 사용해야 합니다.

방어 센터가 손상된 피드 또는 인식할 수 없는 IP 주소가 포함된 피드를 다운로드하면 시스템은 이전 피드 데이터를 계속 사용합니다(첫 번째 다운로드가 아닌 경우). 그러나 시스템이 피드에서 IP 주소를 하나라도 인식할 수 있으면 방어 센터는 관리되는 디바이스를 인식 가능한 주소로 업데이트합니다.

기본 상태 정책에는 보안 인텔리전스 모듈이 포함되며, 여기서는 방어 센터가 피드를 업데이트할 수 없거나 피드가 손상되었거나 피드에 인식할 수 없는 IP 주소가 없는 경우 등 보안 인텔리전스 필터링과 관련된 몇몇 상황에서 알림을 제공합니다.

인터넷 액세스 및 고가용성

인텔리전스 피드를 다운로드하는 데에는 포트 443/HTTPS가 사용되고, 사용자 지정 또는 서드파티 피드를 다운로드하는 데에는 443/HTTP 또는 80/HTTP가 사용됩니다. 피드를 업데이트하려면 방어 센터에서 적절한 포트(인바운드와 아웃바운드)를 열어야 합니다. 방어 센터는 피드 사이트에 직접 액세스할 수 없는 경우 프록시 서버를 사용할 수 있습니다(64-8페이지의 관리 인터페이스 구성 참조).

참고 방어 센터는 사용자 지정 피드를 다운로드할 때 SSL 인증서 인증을 수행하지 **않으며**, 인증서 번들 또는 자체 서명 인증서를 사용한 원격 피드 인증을 지원하지도 않습니다.

보안 인텔리전스 객체는 고가용성 구축에서 방어 센터 간에 동기화되지만, 기본 방어 센터 다운로드 피드만 업데이트됩니다. 기본 방어 센터가 실패하는 경우 보조 방어 센터가 피드 사이트에 액세스하도록 해야 하며, 자체 웹 인터페이스를 사용하여 보조 방어 센터를 Active로 승격해야 합니다. 자세한 내용은 4-15페이지의 고가용성 상태 모니터링 및 변경을/를 참조하십시오.

피드 및 목록 관리

객체 관리자의 Security Intelligence 페이지를 사용하여 보안 인텔리전스 목록과 피드(보안 인텔리전스 객체로 총칭)를 생성 및 관리합니다. 네트워크 객체와 그룹의 생성 및 관리에 대한 자세한 내용은 3-4페이지의 네트워크 객체 작업을/를 참조하십시오.

저장된 또는 적용된 액세스 제어 정책에서 현재 사용되고 있는 사용자 지정 목록 또는 피드는 삭제할 수 없습니다. 또한 개별 IP 주소를 제거할 수는 있지만 전역 목록은 삭제할 수 없습니다. 마찬가지로, 인텔리전스 피드를 삭제할 수는 없지만 수정을 통해 업데이트 빈도를 변경하거나 비활성화할 수는 있습니다.

보안 인텔리전스 객체 빠른 참조

다음 표에서는 보안 인텔리전스 필터링을 수행하기 위해 사용할 수 있는 객체에 대한 빠른 참조를 제공합니다.

표 3-1 보안 인텔리전스 객체 기능

기능	전역 화이트리스트 또는 블랙리스트	인텔리전스 피드	사용자 지정 피드	사용자 지정 목록	네트워크 개체
사용 방법	기본적으로 액세스 제어 정책에서	액세스 제어 정책에서 화이트리스트 또는 블랙리스트 객체로서			
보안 영역의 제한을 받는지 여부	아니요	예	예	예	예
삭제 가능 여부	아니요	아니요	저장된 또는 적용된 액세스 제어 정책에서 현재 사용되고 있지 않은 경우, 예		
객체 관리자 수정 기능	IP 주소만 삭제(컨텍스트 메뉴를 사용하여 IP 주소 추가)	업데이트 빈도 비활성화 또는 변경	전체 수정	수정된 목록 업로드만	전체 수정
수정 시 액세스 제어 정책 다시 적용 여부	삭제 시 예(IP 주소 추가 시에는 다시 적용 필요 없음)	아니요	아니요	예	예

보안 인텔리전스 목록 및 피드의 생성, 관리 및 사용에 대한 자세한 내용은 다음을 참조하십시오.

- 3-7페이지의 전역 화이트리스트 및 블랙리스트 작업
- 3-8페이지의 인텔리전스 피드 작업
- 3-9페이지의 사용자 지정 보안 인텔리전스 피드 작업
- 3-10페이지의 보안 인텔리전스 피드 수동 업데이트
- 3-10페이지의 사용자 지정 보안 인텔리전스 목록 작업
- 13-1페이지의 보안 인텔리전스 IP 주소 평판 블랙리스트에 추가

전역 화이트리스트 및 블랙리스트 작업

라이센스: 보호

지원되는 디바이스: Series 2를 제외한 모두

지원되는 Defense Center: DC500을 제외한 모두

분석 과정 중에 이벤트 보기의 IP 주소 컨텍스트 메뉴, Context Explorer 또는 대시보드를 사용하여 보안 인텔리전스 *전역 블랙리스트*를 작성할 수 있습니다. 익스플로잇 시도와 결합된 침입 이벤트에서 라우팅 가능한 IP 주소 집합이 발견되면 해당 IP 주소를 즉시 블랙리스트에 추가할 수 있습니다. 또한 유사한 방식으로 *전역 화이트리스트*를 작성할 수 있습니다.

모든 액세스 제어 정책에는 시스템의 전역 화이트리스트 및 블랙리스트가 기본적으로 포함되며 모든 영역에 적용됩니다. 정책 단위로 이러한 전역 목록을 사용하지 않도록 선택할 수 있습니다.

전역 목록에 IP 주소를 추가하면 방어 센터는 관리되는 디바이스를 자동으로 업데이트합니다. 구축 전체에서 변경 사항이 반영되려면 몇 분 정도 소요되지만, 전역 목록에 IP 주소를 추가한 후에는 액세스 제어 정책을 다시 적용할 필요가 없습니다. 반대로, 전역 화이트리스트나 블랙리스트에서 IP 주소를 삭제한 후에는 액세스 제어 정책을 다시 적용해야 변경 사항이 반영됩니다.

`/0` 넷마스크의 네트워크 객체를 화이트리스트나 블랙리스트에 추가할 수는 있지만, 해당 객체에서 `/0` 넷마스크를 사용하는 주소 블록은 무시되며 그러한 주소 기반으로는 화이트리스트 및 블랙리스트 필터링이 발생하지 않습니다. 보안 인텔리전스에서 `/0` 넷마스크가 있는 주소 블록 역시 무시됩니다. 정책의 대상인 모든 트래픽을 모니터링하거나 차단하려면 각각 **Monitor** 또는 **Block** 규칙 작업의 액세스 제어 규칙을 사용하고, **Source Networks** 및 **Destination Networks**에 보안 인텔리전스 필터링 대신 **any**를 사용하십시오.

전역 화이트리스트 또는 블랙리스트에 IP 주소를 추가하면 액세스 제어에 영향을 미치게 되므로 다음 중 하나가 필요합니다.

- 관리자 액세스 권한
- 기본 역할의 조합: Network Admin 또는 Access Admin 더하기 Security Analyst 및 Security Approver
- Modify Access Control Policy 및 Apply Access Control Policy 권한이 모두 있는 사용자 지정 역할. 12-4페이지의 사용자 지정 사용자 역할로 구축 관리을/를 참조하십시오.

컨텍스트 메뉴를 사용하여 전역 화이트리스트 또는 블랙리스트에 IP 주소를 추가하려면

액세스: Admin/Custom

1단계 이벤트 보기, 패킷 보기, Context Explorer 또는 대시보드에서 IP 주소 핫스팟 위로 포인터를 이동합니다.

팁 이벤트 보기 또는 대시보드에서 왼쪽의 호스트 아이콘( )이 아니라 IP 주소 위로 포인터를 이동하십시오.

2단계 컨텍스트 메뉴를 호출합니다.

- 이벤트 보기 또는 대시보드에서 마우스 오른쪽 버튼을 클릭합니다.
- Context Explorer 또는 패킷 보기에서 마우스 왼쪽 버튼을 클릭합니다.

3단계 컨텍스트 메뉴에서 **Whitelist Now** 또는 **Blacklist Now**를 선택합니다.

컨텍스트 메뉴의 다른 옵션에 대한 자세한 내용은 2-5페이지의 컨텍스트 메뉴 사용을/를 참조하십시오.

4단계 IP 주소를 화이트리스트 또는 블랙리스트에 추가할 것임을 확인합니다.

관리되는 디바이스에 추가한 항목과 방어 센터가 통신하면, 변경 사항에 따라 트래픽 필터링이 시작됩니다.

전역 화이트리스트 또는 블랙리스트에서 IP 주소를 제거하려면

액세스: Admin/Network Admin

1단계 객체 관리자의 Security Intelligence 페이지에서 전역 화이트리스트 또는 블랙리스트 옆에 있는 수정 아이콘( )을 클릭합니다.

Global Whitelist or Global Blacklist 팝업 창이 나타납니다.

2단계 목록에서 제거할 IP 주소 옆에 있는 삭제 아이콘( )을 클릭합니다.

여러 IP 주소를 동시에 삭제하려면 Shift 및 Ctrl 키로 선택하고 마우스 오른쪽 버튼을 클릭한 다음 **Delete**를 선택합니다.

3단계 **Save**를 클릭합니다.

변경 사항이 저장되지만 이를 반영하려면 액세스 제어 정책을 적용해야 합니다.

인텔리전스 피드 작업

라이센스: 보호

지원되는 디바이스: Series 2를 제외한 모두

지원되는 Defense Center: DC500을 제외한 모두

블랙리스트 작성을 돕기 위해 Cisco에서는 *인텔리전스 피드*(*Sourcefire 인텔리전스 피드*라고도 함)를 제공합니다. 인텔리전스 피드는 VRT에서 부정적인 평판을 받은 IP 주소를 정기적으로 업데이트한 몇몇 목록으로 구성됩니다. 인텔리전스 피드의 각 목록은 특정 카테고리, 즉 오픈 릴레이, 알려진 공격, bogon(bogus IP 주소) 등을 나타냅니다. 액세스 제어 정책에서는 특정 카테고리 또는 모든 카테고리를 블랙리스트에 추가할 수 있습니다.

인텔리전스 피드는 정기적으로 업데이트되므로 시스템에서는 최신 정보를 사용하여 네트워크 트래픽을 필터링할 수 있습니다. 악성코드, 스팸, 봇넷, 피싱 등 보안 위협을 나타내는 악의적인 IP 주소는 사용자가 새 정책을 업데이트하여 적용하는 속도보다 더 빠르게 나타났다 사라질 수 있습니다.

인텔리전스 피드를 삭제할 수는 없지만 수정을 통해 업데이트 빈도를 변경할 수는 있습니다. 기본적으로 피드는 2시간에 한 번씩 업데이트됩니다.

인텔리전스 피드의 업데이트 빈도를 수정하려면

액세스: Admin/Network Admin

1단계 객체 관리자의 Security Intelligence 페이지에서 Sourcefire Intelligence Feed 옆에 있는 수정 아이콘( )을 클릭합니다.

Sourcefire Security Intelligence 팝업 창이 나타납니다.

2단계 **Update Frequency**를 수정합니다.

2시간에서 일주일까지 여러 간격 중에서 선택할 수 있습니다. 피드 업데이트를 비활성화할 수도 있습니다.

3단계 **Save**를 클릭합니다.

변경 내용이 저장되었습니다.

사용자 지정 보안 인텔리전스 피드 작업

라이센스: 보호

지원되는 디바이스: Series 2를 제외한 모두

지원되는 Defense Center: DC500을 제외한 모두

사용자 지정 또는 서드파티 보안 인텔리전스 피드를 사용하면 정기적으로 업데이트되는, 평판이 좋은 인터넷의 다른 화이트리스트 및 블랙리스트로 인텔리전스 피드를 보강할 수 있습니다. 내부 피드를 설정할 수도 있습니다. 이는 하나의 소스 목록을 사용하여 구축에서 여러 방어 센터를 업데이트하려는 경우 유용합니다.

피드를 구성할 때 URL을 사용하여 위치를 지정합니다. URL은 Punycode로 인코딩할 수 없습니다. 기본적으로 방어 센터는 구성된 간격으로 전체 피드 소스를 다운로드한 다음 관리되는 디바이스를 자동으로 업데이트합니다.

선택적으로, 시스템이 업데이트된 피드의 다운로드 여부를 결정하는 데 md5 체크섬을 사용하도록 구성할 수 있습니다. 방어 센터에서 마지막으로 피드를 다운로드한 이후 체크섬이 변경되지 않은 경우에는 해당 피드를 다시 다운로드할 필요가 없습니다. 내부 피드, 특히 규모가 큰 피드에는 md5 체크섬을 사용할 수 있습니다. md5 체크섬은 간단한 텍스트 파일에 해당 체크섬만 포함하여 저장해야 합니다. 코멘트는 지원되지 않습니다.

보안 인텔리전스 피드를 구성하려면

액세스: Admin/Intrusion Admin

1단계 객체 관리자의 Security Intelligence 페이지에서 **Add Security Intelligence**를 클릭합니다.

Security Intelligence 팝업 창이 나타납니다.

2단계 피드의 **Name**을 입력합니다. 파이프(|) 또는 중괄호({})를 제외한 인쇄 가능한 표준 ASCII 문자를 사용할 수 있습니다.

3단계 **Type** 드롭다운 목록에서 **Feed**를 구성할 것임을 지정합니다.

새 옵션으로 팝업 창이 업데이트됩니다.

4단계 **Feed URL**을 지정하고, 선택적으로 **MD5 URL**을 지정합니다.

5단계 **Update Frequency**를 선택합니다.

2시간에서 일주일까지 여러 간격 중에서 선택할 수 있습니다. 피드 업데이트를 비활성화할 수도 있습니다.

6단계 **Save**를 클릭합니다.

보안 인텔리전스 피드 객체가 생성됩니다. 피드 업데이트를 비활성화하지 않은 경우 방어 센터는 피드의 다운로드 및 확인을 시도합니다. 이제 액세스 제어 정책에서 피드 객체를 사용할 수 있습니다.

보안 인텔리전스 피드 수동 업데이트

라이센스: 보호

지원되는 디바이스: Series 2를 제외한 모두

지원되는 Defense Center: DC500을 제외한 모두

보안 인텔리전스 피드를 수동으로 업데이트하면 인텔리전스 피드를 비롯한 모든 피드가 업데이트됩니다.

모든 보안 인텔리전스 피드를 업데이트하려면

액세스: Admin/Access Admin/Network Admin

1단계 객체 관리자의 Security Intelligence 페이지에서 **Update Feeds**를 클릭합니다.

2단계 모든 피드를 업데이트할 것임을 확인합니다.

확인 대화 상자가 나타나서, 업데이트가 반영되려면 몇 분 정도 걸릴 수 있음을 알립니다.

3단계 **OK**를 클릭합니다.

방어 센터는 피드 업데이트를 다운로드 및 확인한 후 변경 사항을 관리되는 디바이스로 전달합니다. 그러면 업데이트된 피드를 사용하여 트래픽 필터링이 시작됩니다.

사용자 지정 보안 인텔리전스 목록 작업

라이센스: 보호

지원되는 디바이스: Series 2를 제외한 모두

지원되는 Defense Center: DC500을 제외한 모두

보안 인텔리전스 목록은 방어 센터에 수동으로 업로드하는 IP 주소 및 주소 블록의 간단한 정적 목록입니다. 방어 센터의 단일 관리되는 디바이스에 대해 전역 목록 중 하나 또는 피드를 보강하고 세부적으로 조정하려는 경우에는 사용자 지정 목록이 유용합니다.

주소 블록에 대한 넷마스크는 `0~32` 또는 `0~128`(각각 IPv4 및 IPv6) 범위의 정수일 수 있습니다.

예를 들어, 평판이 좋은 피드가 중요한 리소스에 대한 액세스를 부적절하게 차단하지만 조직에서 전체적으로 유용한 경우, 액세스 제어 정책의 블랙리스트에서 보안 인텔리전스 피드 객체를 제거하는 것보다는 부적절하게 분류된 IP 주소만 포함하는 사용자 지정 화이트리스트를 생성할 수 있습니다.

보안 인텔리전스 목록을 수정하려면 소스 파일을 변경하고 새 복사본을 업로드해야 합니다. 자세한 내용은 3-11페이지의 보안 인텔리전스 목록 업데이트을/를 참조하십시오.

방어 센터에 새 보안 인텔리전스 목록을 업로드하려면

액세스: Admin/Access Admin/Network Admin

1단계 객체 관리자의 Security Intelligence 페이지에서 **Add Security Intelligence**를 클릭합니다.

Security Intelligence 팝업 창이 나타납니다.

2단계 목록의 **Name**을 입력합니다. 파이프(|) 또는 중괄호({})를 제외한 인쇄 가능한 표준 ASCII 문자를 사용할 수 있습니다.

3단계 **Type** 드롭다운 목록에서 **List**를 업로드할 것임을 지정합니다.

새 옵션으로 팝업 창이 업데이트됩니다.

4단계 **Browse**를 클릭하여 목록 `.txt` 파일을 찾은 다음 Upload를 클릭합니다.

목록이 업로드됩니다. 시스템이 목록에서 찾은 IP 주소 및 주소 블록의 총수가 팝업 창에 표시됩니다. 이 수가 예상한 것과 다르면 파일의 형식을 확인하고 다시 시도하십시오.

5단계 **Save**를 클릭합니다.

보안 인텔리전스 목록 객체가 저장됩니다. 이제 액세스 제어 정책에서 이 객체를 사용할 수 있습니다.

보안 인텔리전스 목록 업데이트

라이센스: 보호

지원되는 디바이스: Series 2를 제외한 모두

지원되는 Defense Center: DC500을 제외한 모두

보안 인텔리전스 목록을 수정하려면 소스 파일을 변경하고 새 복사본을 업로드해야 합니다. 방어 센터 웹 인터페이스를 사용하여 파일 내용을 수정할 수 없습니다. 소스 파일에 액세스할 수 없는 경우 방어 센터에서 복사본을 다운로드할 수 있습니다.

보안 인텔리전스 목록을 수정하려면

액세스: Admin/Access Admin/Network Admin

1단계 객체 관리자의 Security Intelligence 페이지에서 업데이트할 목록 옆에 있는 수정 아이콘( )을 클릭합니다.

Security Intelligence 팝업 창이 나타납니다.

2단계 수정할 목록의 복사본이 필요한 경우 **Download**를 클릭한 다음, 브라우저의 지침에 따라 목록을 텍스트 파일로 저장합니다.

3단계 필요한 대로 목록을 수정합니다.

4단계 Security Intelligence 팝업 창에서 **Browse**를 클릭하여 수정된 목록을 찾은 다음 **Upload**를 클릭합니다.

목록이 업로드됩니다.

5단계 **Save**를 클릭합니다.

변경 내용이 저장되었습니다. 목록이 활성 액세스 제어 정책에서 사용되고 있는 경우 변경 사항을 반영하려면 정책을 적용해야 합니다.

포트 객체 작업

라이센스: 모두

포트 객체는 약간 다른 방법으로 서로 다른 프로토콜을 나타냅니다.

- TCP 및 UDP의 경우 포트 객체는 전송 레이어 프로토콜을 나타냅니다. 프로토콜 번호는 괄호 안에 표시되고 선택적인 관련 포트 또는 포트 범위가 추가로 표시됩니다. 예: `TCP(6)/22`.
- ICMP 및 ICMPv6(IPv6-ICMP)의 경우 포트 객체는 인터넷 레이어 프로토콜과 선택적인 유형 및 코드를 나타냅니다. 예: `ICMP(1):3:3`.
- 포트 객체는 또한 포트를 사용하지 않는 다른 프로토콜을 나타낼 수도 있습니다.

Cisco에서는 잘 알려진 포트에 대한 기본 포트 객체를 제공합니다. 이러한 객체를 수정 또는 삭제할 수도 있지만 Cisco에서는 대신 사용자 지정 포트 객체를 생성할 것을 권장합니다.

액세스 제어 정책, 네트워크 검색 규칙, 포트 변수, 이벤트 검색 등 시스템 웹 인터페이스의 여러 곳에서 포트 객체 및 그룹(3-2페이지의 객체 그룹화 참조)을 사용할 수 있습니다. 예를 들어, 조직에서 특정 포트 범위를 사용하는 사용자 지정 클라이언트를 사용하며 시스템에서 잘못된 이벤트를 과도하게 생성하는 경우, 이러한 포트의 모니터링을 제외하도록 네트워크 검색 정책을 구성할 수 있습니다.

사용 중인 포트 객체는 삭제할 수 없습니다. 또한 액세스 제어나 네트워크 검색 정책에 사용된 포트 객체를 수정한 후 변경 사항을 반영하려면 정책을 다시 적용해야 합니다.

액세스 제어 규칙의 소스 포트 조건에 대해서는 TCP 또는 UDP 이외의 프로토콜을 추가할 수 없습니다. 또한 규칙에서 소스 및 목적지 포트 조건을 모두 설정하는 경우 전송 프로토콜을 혼합할 수 없습니다.

소스 포트 조건에서 포트 객체 그룹에 지원되지 않는 프로토콜을 추가하는 경우, 정책 적용 시 해당 프로토콜이 사용되는 규칙이 관리되는 디바이스에 적용되지 않습니다. 또한 TCP와 UDP 포트를 모두 포함하는 포트 객체를 생성한 다음 이를 규칙에서 소스 포트 조건으로 추가하는 경우 목적지 포트를 추가할 수 없으며, 그 반대의 경우도 마찬가지입니다.

포트 객체를 생성하려면

액세스: Admin/Access Admin/Network Admin

1단계 **Objects > Object Management**를 선택합니다.

Object Management 페이지가 나타납니다.

2단계 **Port** 아래에서 **Individual Objects**를 선택합니다.

3단계 **Add Port**를 클릭합니다.

Port Objects 팝업 창이 나타납니다.

4단계 포트 객체의 **Name**을 입력합니다. 파이프(|) 또는 중괄호({})를 제외한 인쇄 가능한 표준 ASCII 문자를 사용할 수 있습니다.

5단계 **Protocol**을 선택합니다.

TCP, **UDP**, **IP**, **ICMP** 또는 **IPv6-ICMP**를 신속하게 선택할 수 있으며, **Other** 드롭다운 목록에서 다른 프로토콜을 선택하거나 모든 프로토콜(**All**)을 선택할 수도 있습니다.

6단계 선택적으로, **Port** 또는 포트 범위를 사용하여 TCP 또는 UDP 포트 객체를 제한합니다.

1~65535 범위에서 임의의 포트를 지정할 수도 있고, 모든 포트를 매칭하려면 `any`를 지정할 수 있습니다. 포트의 범위를 지정하려면 하이픈을 사용합니다.

7단계 선택적으로, **Type** 및 관련 **Code**(해당되는 경우)를 사용하여 ICMP 또는 IPV6-ICMP 포트 객체를 제한합니다.

ICMP 또는 IPv6-ICMP 객체를 생성할 때 유형 및 코드(해당되는 경우)를 지정할 수 있습니다. ICMP 유형 및 코드에 대한 자세한 내용은 다음을 참조하십시오.

- http://www.iana.org/assignments/icmp-parameters/icmp-parameters.xml
- http://www.iana.org/assignments/icmpv6-parameters/icmpv6-parameters.xml

임의의 유형을 매칭하려면 유형을 any로 설정하고, 지정된 유형에 대한 임의의 코드를 매칭하려면 코드를 any로 설정할 수 있습니다.

8단계 선택적으로, **Other**를 선택하고 드롭다운 목록에서 프로토콜을 선택합니다. **All** 프로토콜을 선택하는 경우 **Port** 필드에 포트 번호를 입력합니다.

9단계 **Save**를 클릭합니다.

포트 객체가 추가됩니다.

VLAN 태그 객체 작업

라이센스: 모두

구성하는 각 VLAN 태그 객체는 VLAN 태그 또는 태그 범위를 나타냅니다. 액세스 제어 정책과 이벤트 검색 등 시스템 웹 인터페이스의 여러 곳에서 VLAN 태그 객체 및 그룹(3-2페이지의 객체 그룹화 참조)을 사용할 수 있습니다. 예를 들어 특정 VLAN에만 적용되는 액세스 제어 규칙을 작성할 수 있습니다.

사용 중인 VLAN 태그 객체는 삭제할 수 없습니다. 또한 액세스 제어 정책에 사용된 VLAN 태그 객체를 수정한 후 변경 사항을 반영하려면 정책을 다시 적용해야 합니다.

VLAN 태그 객체를 추가하려면

액세스: Admin/Access Admin/Network Admin

1단계 **Objects > Object Management**를 선택합니다.

Object Management 페이지가 나타납니다.

2단계 **VLAN Tag** 아래에서 **Individual Objects**를 선택합니다.

3단계 **Add VLAN Tag**를 클릭합니다.

VLAN Tag 팝업 창이 나타납니다.

4단계 VLAN 태그의 **Name**을 입력합니다. 파이프(|) 또는 중괄호({})를 제외한 인쇄 가능한 표준 ASCII 문자를 사용할 수 있습니다.

5단계 **VLAN Tag** 필드에 VLAN 태그에 대한 값을 입력합니다.

VLAN 태그는 1~4094 범위에서 지정할 수 있습니다. VLAN 태그의 범위를 지정하려면 하이픈을 사용합니다.

6단계 **Save**를 클릭합니다.

VLAN 태그 객체가 추가됩니다.

URL 객체 작업

라이센스: 모두

지원되는 디바이스: Series 2를 제외한 모두

지원되는 Defense Center: DC500을 제외한 모두

구성하는 각 URL 객체는 단일 URL 또는 IP 주소를 나타냅니다. 액세스 제어 정책과 이벤트 검색 등 시스템 웹 인터페이스의 여러 곳에서 URL 객체 및 그룹(3-2페이지의 객체 그룹화 참조)을 사용할 수 있습니다. 예를 들어 특정 웹사이트를 차단하는 액세스 제어 규칙을 작성할 수 있습니다.

URL 객체를 작성할 때, 특히 암호화된 트래픽을 해독하거나 차단할 SSL 검사를 구성하지 않는 경우 다음에 유의해야 합니다.

- URL 객체를 사용하여 액세스 제어 규칙에서 HTTPS 트래픽을 매칭하려는 경우, 트래픽 암호화에 사용되는 공개 키 인증서에서 주체 CN을 사용하여 객체를 생성합니다. 또한 주체 CN에 포함된 하위 도메인은 무시되므로 하위 도메인 정보를 포함하지 마십시오. 이를테면 www.example.com 대신 example.com을 사용하십시오.
- URL 조건과 함께 액세스 제어 규칙을 사용하여 웹 트래픽을 매칭할 경우 시스템은 암호화 프로토콜(HTTP 대 HTTPS)을 무시합니다. 다시 말해, 특정 웹사이트를 차단하는 경우 규칙을 세분화하는 애플리케이션 조건을 사용하지 않는 한 해당 웹사이트에 대한 HTTP 및 HTTPS 트래픽이 모두 차단됩니다. URL 객체를 생성할 때에는 객체 생성 시 프로토콜을 지정할 필요가 없습니다. 이를테면 `http://example.com/` 대신 `example.com`을 사용하십시오.

자세한 내용은 19-1페이지의 트래픽 해독 이해 및 16-8페이지의 URL 차단을/를 참조하십시오.

사용 중인 URL 객체는 삭제할 수 없습니다. 또한 액세스 제어 정책에 사용된 URL 객체를 수정한 후 변경 사항을 반영하려면 정책을 다시 적용해야 합니다.

URL 객체를 추가하려면

액세스: Admin/Access Admin/Network Admin

1단계 **Objects > Object Management**를 선택합니다.

Object Management 페이지가 나타납니다.

2단계 **URL** 아래에서 **Individual Objects**를 선택합니다.

3단계 **Add URL**을 클릭합니다.

URL Objects 팝업 창이 나타납니다.

4단계 URL 객체의 **Name**을 입력합니다. 파이프(|) 또는 중괄호({})를 제외한 인쇄 가능한 표준 ASCII 문자를 사용할 수 있습니다.

5단계 URL 객체의 **URL** 또는 IP 주소를 입력합니다. 이 필드에는 와일드카드(*)를 사용할 수 **없습니다**.

6단계 **Save**를 클릭합니다.

URL 객체가 추가됩니다.

애플리케이션 필터 작업

라이센스: FireSIGHT

지원되는 디바이스: Series 2를 제외한 모두

FireSIGHT 시스템은 IP 트래픽을 분석할 때 네트워크에서 자주 사용되는 애플리케이션을 확인하려고 시도합니다. 애플리케이션 인식은 애플리케이션 기반 액세스 제어를 수행하기 위한 중요한 요소입니다. 시스템에서는 많은 애플리케이션에 대한 탐지기를 제공하며 Cisco에서는 시스템 및 VDB(취약성 데이터베이스) 업데이트를 통해 자주 추가 탐지기를 업데이트합니다. 시스템 탐지 기능을 향상하기 위해 자신의 애플리케이션 프로토콜 탐지기를 생성할 수도 있습니다.

애플리케이션 필터는 애플리케이션의 위험, 비즈니스 연관성, 유형, 카테고리 및 태그와 관련된 기준에 따라 애플리케이션을 그룹화합니다. 45-11 페이지의 표 45-2을/를 참조하십시오. 애플리케이션 프로토콜 탐지기를 생성할 때에도 그러한 기준을 사용하여 애플리케이션을 구성해야 합니다. 애플리케이션 필터를 사용하면 애플리케이션을 개별적으로 검색 및 추가할 필요가 없으므로 액세스 제어 규칙에 대한 애플리케이션 조건을 빠르게 생성할 수 있습니다. 16-4페이지의 애플리케이션 필터로 트래픽 매칭을/를 참조하십시오.

애플리케이션 필터 사용에 따른 또 다른 이점은 새 애플리케이션을 수정 또는 추가할 때 필터를 사용하는 액세스 제어 규칙을 업데이트할 필요가 없다는 것입니다. 예를 들어, 모든 소셜 네트워킹 애플리케이션을 차단하도록 액세스 제어 정책을 구성하고 VDB 업데이트에 새로운 소셜 네트워킹 애플리케이션 탐지기를 포함하는 경우 VDB를 업데이트하면 정책이 업데이트됩니다. 시스템이 새 애플리케이션을 차단하도록 하려면 먼저 정책을 다시 적용해야 하지만, 애플리케이션을 차단하는 액세스 제어 규칙을 업데이트할 필요는 없습니다.

Cisco 제공 애플리케이션 필터가 필요에 맞게 애플리케이션을 그룹화하지 않는 경우 자신의 고유한 필터를 생성할 수 있습니다. 사용자 정의 필터는 Cisco 제공 필터를 그룹화 및 결합할 수 있습니다. 예를 들어 위험이 매우 높고 비즈니스 연관성이 낮은 애플리케이션을 모두 차단하는 필터를 생성할 수 있습니다. 개별 애플리케이션을 수동으로 지정하여 필터를 생성할 수도 있습니다. 그러나 그러한 필터는 시스템 소프트웨어 또는 VDB를 업데이트할 때 자동으로 업데이트되지 **않습니다**.

Cisco 제공 애플리케이션 필터와 마찬가지로 사용자 정의 애플리케이션 필터도 액세스 제어 규칙에서 사용할 수 있습니다. 다음과 같은 추가적인 방법으로 사용자 정의 필터를 사용할 수도 있습니다.

- 이벤트 뷰어를 사용하여 애플리케이션 검색: 60-5페이지의 검색에서 객체 및 애플리케이션 필터 사용 참조
- 보고서 템플릿에서 테이블 보기 제한: 57-17페이지의 보고서 템플릿 섹션에서 검색 작업 참조
- Custom Analysis 대시보드 위젯에서 애플리케이션 통계 필터링: 55-15페이지의 Custom Analysis 위젯 구성 참조

객체 관리자를 사용하여(**Objects > Object Management**) 애플리케이션 필터를 생성하고 관리할 수 있습니다. 액세스 제어 규칙에 애플리케이션 조건을 추가하는 동안 애플리케이션 필터를 즉석에서 생성할 수도 있습니다.

Application Filters 목록에는 고유한 필터를 작성하기 위해 선택할 수 있는 Cisco 제공 애플리케이션 필터가 포함되어 있습니다. 검색 문자열을 사용하여 나타나는 필터를 제한할 수 있습니다. 이는 카테고리 및 태그에 특히 유용합니다.

Available Applications 목록은 사용자가 선택하는 필터에 개별 애플리케이션을 포함합니다. 여기서도 검색 문자열을 사용하여 나타나는 필터를 제한할 수 있습니다.

동일한 필터 유형의 여러 필터는 OR 연산자로 연결됩니다. 중위험 필터에 애플리케이션 100개가 포함되고 고위험 필터에 애플리케이션 50개가 포함된 시나리오를 가정해보겠습니다. 두 필터를 모두 선택하면 150개의 사용 가능한 애플리케이션이 표시될 수 있습니다.

서로 다른 유형의 필터는 AND 연산자로 연결됩니다. 예를 들어 중위험/고위험 필터와 중간/높음 비즈니스 연관성 필터를 선택하면, 중위험이나 고위험 및 중간 비즈니스 연관성이나 높은 비즈니스 연관성의 애플리케이션이 표시됩니다.

팁 관련 애플리케이션에 대한 자세한 내용은 정보 아이콘( )을 클릭하십시오. 추가 정보를 표시하려면 나타나는 팝업에서 원하는 인터넷 검색 링크를 클릭하십시오.

필터에 추가할 애플리케이션을 결정했으면 개별적으로 추가할 수도 있고, 애플리케이션 필터를 선택한 경우 **All apps matching the filter**를 선택할 수도 있습니다. Selected Applications and Filters 목록의 총 항목 수가 50을 넘지 않는 한 여러 필터와 애플리케이션을 원하는 조합으로 추가할 수 있습니다.

애플리케이션 필터를 생성하면 객체 관리자의 Application Filters 페이지에 나열됩니다. 이 페이지에는 각 필터를 구성하는 총 조건 수가 표시됩니다.

나타나는 애플리케이션 필터를 정렬 및 필터링하는 방법에 대한 자세한 내용은 3-2페이지의 객체 관리자 사용을/를 참조하십시오. 사용 중인 애플리케이션 필터는 삭제할 수 없습니다. 또한 액세스 제어 정책에 사용된 애플리케이션 필터를 수정한 후 변경 사항을 반영하려면 정책을 다시 적용해야 합니다.

애플리케이션 필터를 생성하려면

액세스: Admin/Access Admin/Network Admin

1단계 **Objects > Object Management**를 선택합니다.

Object Management 페이지가 나타납니다.

2단계 **Application Filters**를 클릭합니다.

Application Filters 섹션이 나타납니다.

3단계 **Add Application Filter**를 클릭합니다.

Application Filter 팝업 창이 나타납니다.

4단계 필터의 **Name**을 지정합니다. 파이프(|) 또는 중괄호({})를 제외한 인쇄 가능한 표준 ASCII 문자를 사용할 수 있습니다.

5단계 선택적으로, 필터에 추가할 애플리케이션 목록의 범위를 좁히려면 **Application Filters** 목록에서 Cisco 제공 필터를 사용합니다.

- 목록을 확장 및 축소하려면 각 필터 옆에 있는 화살표를 클릭합니다.
- 필터 유형을 마우스 오른쪽 버튼으로 클릭하고 **Check All** 또는 **Uncheck All**을 클릭합니다. 목록에는 유형별로 선택한 필터 수가 표시됩니다.
- 나타나는 필터 범위를 좁히려면 **Search by name** 필드에 검색 문자열을 입력합니다. 이는 카테고리 및 태그에 특히 유용합니다. 검색을 지우려면 지우기 아이콘( )을 클릭합니다.
- 필터 목록을 새로 고치고 선택한 필터를 지우려면 다시 로드 아이콘( )을 클릭합니다.
- 모든 필터 및 검색 필드를 지우려면 **Clear All Filters**를 클릭합니다.

선택한 필터와 일치하는 애플리케이션이 Available Applications 목록에 나타납니다. 목록에는 한 번에 100개의 애플리케이션이 표시됩니다.

6단계 필터에 추가할 애플리케이션을 **Available Applications** 목록에서 선택합니다.

- 이전 단계에서 지정한 제약 조건과 일치하는 모든 애플리케이션을 추가하려면 **All apps matching the filter**를 선택합니다.
- 나타나는 개별 애플리케이션의 범위를 좁히려면 **Search by name** 필드에 검색 문자열을 입력합니다. 검색을 지우려면 지우기 아이콘( )을 클릭합니다.
- 사용 가능한 개별 애플리케이션 목록을 탐색하려면 목록 아래쪽에 있는 페이지 아이콘을 사용합니다.

- 여러 개별 애플리케이션을 선택하려면 Shift 및 Ctrl 키를 사용합니다. 현재 표시된 개별 애플리케이션을 모두 선택하려면 마우스 오른쪽 버튼을 클릭하고 **Select All**을 선택합니다.
- 애플리케이션 목록을 새로 고치고 선택한 애플리케이션을 지우려면 다시 로드 아이콘( )을 클릭합니다.

개별 애플리케이션과 **All apps matching the filter**를 동시에 선택할 수는 없습니다.

7단계 선택한 애플리케이션을 필터에 추가합니다. 클릭하고 끌거나, **Add to Rule**을 클릭할 수 있습니다.

다음의 조합이 결과로 나타납니다.

- 선택한 Application Filters
- 선택한 개별 Available Applications 또는 **All apps matching the filter**

필터에 최대 50개의 애플리케이션 및 필터를 추가할 수 있습니다. 선택한 애플리케이션에서 애플리케이션 또는 필터를 삭제하려면 해당 삭제 아이콘( )을 클릭합니다. 또한 하나 이상의 애플리케이션 및 필터를 선택하거나 **Select All**을 오른쪽 클릭한 다음, **Delete Selected**를 오른쪽 클릭할 수도 있습니다.

8단계 **Save**를 클릭합니다.

애플리케이션 필터가 저장됩니다.

변수 집합 작업

라이센스: 보호

변수는 소스 및 목적지 IP 주소와 포트를 식별하기 위해 침입 규칙에서 일반적으로 사용되는 값을 나타냅니다. 또한 규칙 억제, 적응형 프로필 및 동적 규칙 상태에서 IP 주소를 나타내기 위해 침입 정책에서 변수를 사용할 수 있습니다.

팁 침입 규칙에 사용된 네트워크 변수로 정의한 호스트와 상관없이 프리프로세서 규칙은 이벤트를 트리거할 수 있습니다.

변수를 관리하고 사용자 지정하고 그룹화하는 데 변수 집합을 사용합니다. Cisco에서 제공하는 기본 변수 집합을 사용할 수도 있고 사용자 지정 집합을 생성할 수도 있습니다. 어떤 집합에서든 사전 정의된 기본 변수는 물론 사용자 정의 변수도 수정할 수 있습니다.

FireSIGHT 시스템에서 제공하는 대부분의 공유 객체 규칙 및 표준 텍스트 규칙에서는 이러한 사전 정의된 기본 변수를 사용하여 네트워크 및 포트 번호를 정의합니다. 예를 들어 규칙의 대다수는 `$HOME_NET` 변수를 사용하여 보호되는 네트워크를 지정하고, `$EXTERNAL_NET` 변수를 사용하여 보호되지 않는(외부) 네트워크를 지정합니다. 또한 특수한 규칙은 종종 다른 사전 정의된 변수를 사용합니다. 예를 들어 웹 서버에 대해 익스플로잇을 탐지하는 규칙은 `$HTTP_SERVERS` 및 `$HTTP_PORTS` 변수를 사용합니다.

변수가 네트워크 환경을 좀 더 정확히 반영하는 경우 규칙이 더욱 효과적입니다. 3-18페이지의 사전 정의된 기본 변수 최적화에 설명된 대로 최소한 기본 집합의 기본 변수를 수정해야 합니다. `$HOME_NET` 같은 변수가 네트워크를 정확히 정의하는지 확인하고 `$HTTP_SERVERS`가 네트워크의 모든 웹 서버를 포함하는지 확인하면, 처리가 최적화되고 모든 관련 시스템에서 의심스러운 활동이 모니터링됩니다.

변수를 사용하려면 변수 집합을 액세스 제어 규칙 또는 액세스 제어 정책의 기본 작업과 관련된 침입 정책으로 설정합니다. 기본적으로 기본 변수 집합은 액세스 제어 정책에서 사용되는 모든 침입 정책에 연결됩니다.

자세한 내용은 다음 절을 참조하십시오.

사전 정의된 기본 변수 최적화

라이센스: 보호

기본적으로 FireSIGHT 시스템은 사전 정의된 기본 변수로 구성된 단일 기본 변수 집합을 제공합니다. Cisco VRT(Vulnerability Research Team)는 규칙 업데이트를 사용하여 새로운/업데이트된 침입 정책 및 기타 침입 정책 요소(기본 변수 포함)를 제공합니다. 자세한 내용은 66-14페이지의 규칙 업데이트 및 로컬 규칙 파일 가져오기을/를 참조하십시오.

Cisco에서 제공하는 많은 침입 규칙은 사전 정의된 기본 변수를 사용하므로 이러한 변수에 대한 적절한 값을 설정해야 합니다. 네트워크의 트래픽을 식별하기 위해 변수 집합을 사용하는 방법에 따라 특정 변수 집합 또는 모든 변수 집합에서 이러한 기본 변수의 값을 수정할 수 있습니다. 자세한 내용은 3-25페이지의 변수 추가 및 수정을/를 참조하십시오.

주의 액세스 제어 또는 침입 정책을 가져오면 가져온 기본 변수가 기본 변수 집합의 기본 변수를 덮어쓰게 됩니다. 가져온 기본 변수 집합에 없는 사용자 지정 변수가 기존 기본 변수 집합에 포함되어 있으면, 고유한 변수가 유지됩니다. 자세한 내용은 A-5페이지의 컨피그레이션 가져오기을/를 참조하십시오.

다음 표에서는 Cisco에서 제공하는 변수에 대해 설명하고 일반적으로 어떤 변수를 수정하는지를 나타냅니다. 변수를 네트워크에 맞게 맞춤화하는 방법에 대해 도움이 필요하면 Professional Services 또는 고객 지원에 문의하십시오.

표 3-2 Cisco에서 제공하는 변수

변수 이름	설명	수정 여부
$AIM_SERVERS	알려진 AIM(AOL Instant Messenger) 서버를 정의하며, 채팅 기반 규칙 및 AIM 익스플로잇을 찾는 규칙에 사용됩니다.	필요하지 않음.
$DNS_SERVERS	DNS(Domain Name Service) 서버를 정의합니다. 특히 DNS 서버에 영향을 주는 규칙을 생성하는 경우 $DNS_SERVERS 변수를 목적지 또는 소스 IP 주소로 사용할 수 있습니다.	현재 규칙 집합에 필요하지 않음.
$EXTERNAL_NET	FireSIGHT 시스템에서 보호되지 않은 네트워크로 판단하는 네트워크를 정의하며, 외부 네트워크를 정의하는 많은 규칙에 사용됩니다.	예. $HOME_NET를 적절히 정의해야 하며 $HOME_NET를 $EXTERNAL_NET의 값에서 제외해야 함.
$FILE_DATA_PORTS	네트워크 스트림에서 파일을 탐지하는 침입 규칙에 사용되는 암호화되지 않은 포트를 정의합니다.	필요하지 않음.

표 3-2 Cisco에서 제공하는 변수(계속)

변수 이름	설명	수정 여부
$FTP_PORTS	네트워크에서 FTP 서버의 포트를 정의하며 FTP 서버 익스플로잇 규칙에 사용됩니다.	FTP 서버가 기본 포트 이외의 포트를 사용하는 경우, 예(웹 인터페이스에서 기본 포트를 볼 수 있음).
$GTP_PORTS	패킷 디코더가 GTP(GPRS[General Packet Radio Service] Tunneling Protocol) PDU 내부에 페이로드를 추출하는 데이터 채널 포트를 정의합니다.	필요하지 않음.
$HOME_NET	관련된 침입 정책을 모니터링하는 네트워크를 정의하며, 내부 네트워크를 정의하는 많은 규칙에 사용됩니다.	내부 네트워크에 대한 IP 주소를 포함하려는 경우, 예.
$HTTP_PORTS	네트워크에서 웹 서버의 포트를 정의하며 웹 서버 익스플로잇 규칙에 사용됩니다.	웹 서버가 기본 포트 이외의 포트를 사용하는 경우, 예(웹 인터페이스에서 기본 포트를 볼 수 있음).
$HTTP_SERVERS	네트워크에서 웹 서버를 정의합니다. 웹 서버 익스플로잇 규칙에 사용됩니다.	HTTP 서버를 운영하는 경우, 예.
$ORACLE_PORTS	네트워크에서 Oracle 데이터베이스 서버 포트를 정의하며, Oracle 데이터베이스에서 공격을 스캔하는 규칙에 사용됩니다.	Oracle 서버를 운영하는 경우, 예.
$SHELLCODE_PORTS	시스템이 셸 코드 익스플로잇을 스캔할 포트를 정의하며, 셸 코드를 사용하는 익스플로잇을 탐지하는 규칙에 사용됩니다.	필요하지 않음.
$SIP_PORTS	네트워크에서 SIP의 포트를 정의하며 SIP 서버 익스플로잇 규칙에 사용됩니다.	필요하지 않음.
$SIP_SERVERS	네트워크에서 SIP 서버를 정의하며, SIP 대상 익스플로잇을 해결하는 규칙에 사용됩니다.	예. SIP 서버를 실행하는 경우 $HOME_NET를 적절히 정의해야 하며 $HOME_NET를 $SIP_SERVERS의 값에 포함해야 함.
$SMTP_SERVERS	네트워크에서 SMTP 서버를 정의하며, 메일 서버 대상의 익스플로잇을 해결하는 규칙에 사용됩니다.	SMTP 서버를 운영하는 경우, 예.
$SNMP_SERVERS	네트워크에서 SNMP 서버를 정의하며, SNMP 서버에 대한 공격을 스캔하는 규칙에 사용됩니다.	SNMP 서버를 운영하는 경우, 예.
$SNORT_BPF	FireSIGHT 시스템 소프트웨어 릴리스 버전 5.3.0 이전(후에 버전 5.3.0 이상으로 업그레이드)의 시스템에 존재한 경우에만 나타나는 레거시 고급 변수를 식별합니다. 3-32페이지의 고급 변수 이해을/를 참조하십시오.	아니요. 이 변수는 보거나 삭제할 수만 있고 수정하거나 삭제 후 복구할 수 없음.
$SQL_SERVERS	네트워크에서 데이터베이스 서버를 정의하며, 데이터베이스 대상 익스플로잇을 해결하는 규칙에 사용됩니다.	SQL 서버를 운영하는 경우, 예.
$SSH_PORTS	네트워크에서 SSH 서버의 포트를 정의하며 SSH 서버 익스플로잇 규칙에 사용됩니다.	SSH 서버가 기본 포트 이외의 포트를 사용하는 경우, 예(웹 인터페이스에서 기본 포트를 볼 수 있음).

표 3-2 Cisco에서 제공하는 변수(계속)

변수 이름	설명	수정 여부
$SSH_SERVERS	네트워크에서 SSH 서버를 정의하며, SSH 대상 익스플로잇을 해결하는 규칙에 사용됩니다.	예. SSH 서버를 실행하는 경우 $HOME_NET를 적절히 정의해야 하며 $HOME_NET를 $SSH_SERVERS의 값에 포함해야 함.
$TELNET_SERVERS	네트워크에서 알려진 텔넷 서버를 정의하며, 텔넷 서버 대상 익스플로잇을 해결하는 규칙에 사용됩니다.	텔넷 서버를 운영하는 경우, 예.
$USER_CONF	웹 인터페이스를 통해 사용할 수 없는 하나 이상의 기능을 구성할 수 있는 일반 툴을 제공합니다. 3-32페이지의 고급 변수 이해을/를 참조하십시오. ⚠ **주의** $USER_CONF 컨피그레이션이 충돌하거나 중복되면 시스템이 중단됩니다. 3-32페이지의 고급 변수 이해을/를 참조하십시오.	아니요. 기능 설명의 지침 또는 고객 지원의 안내 필요.

변수 집합 이해

라이센스: 보호

임의의 집합에 변수를 추가하면 모든 집합에 추가됩니다. 즉, 각 변수 집합은 현재 시스템에 구성된 모든 변수의 모음입니다. 임의의 변수 집합 내에서 사용자 정의 변수를 추가하고 변수의 값을 사용자 지정할 수 있습니다.

초기에 FireSIGHT 시스템은 사전 정의된 기본값으로 구성된 단일 기본 변수 집합을 제공합니다. 기본 집합의 각 변수는 초기에 기본값으로 설정됩니다. 사전 정의된 변수에는 이것이 VRT로 설정되고 규칙 업데이트에서 제공되는 값입니다.

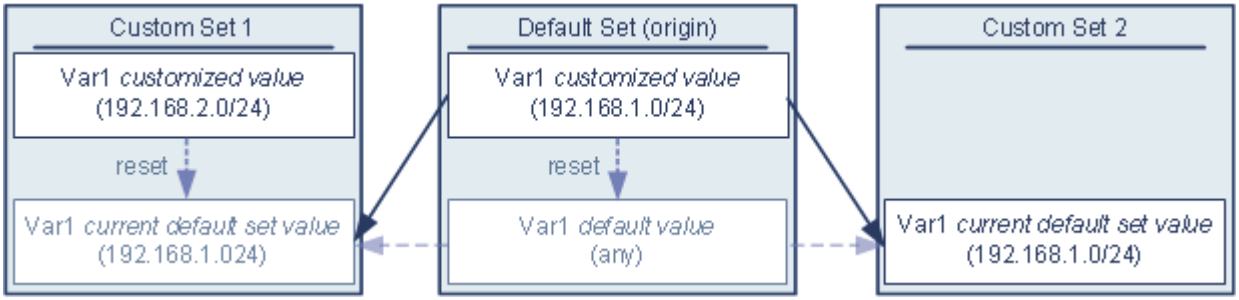
사전 정의된 기본 변수를 기본값으로 구성된 상태로 둘 수도 있지만 Cisco에서는 3-18페이지의 사전 정의된 기본 변수 최적화에 설명된 대로 사전 정의된 변수의 하위 집합을 수정할 것을 권장합니다.

기본 집합에서만 변수로 작업할 수 있지만, 하나 이상의 사용자 지정 집합을 추가하여 서로 다른 집합에서 서로 다른 변수 값을 구성하고, 심지어 새 변수를 추가함으로써 가장 큰 이점을 누릴 수 있습니다.

여러 집합을 사용 중인 경우 기본 집합에 있는 변수의 *현재 값*이 다른 모든 집합에 있는 변수의 *기본값*을 결정한다는 사실을 기억해야 합니다.

예: 사용자 정의 변수를 기본 집합에 추가

다음 다이어그램은 사용자 정의 변수 Var1을 값 192.168.1.0/24의 기본 집합에 추가할 경우의 집합 상호 작용을 설명합니다.



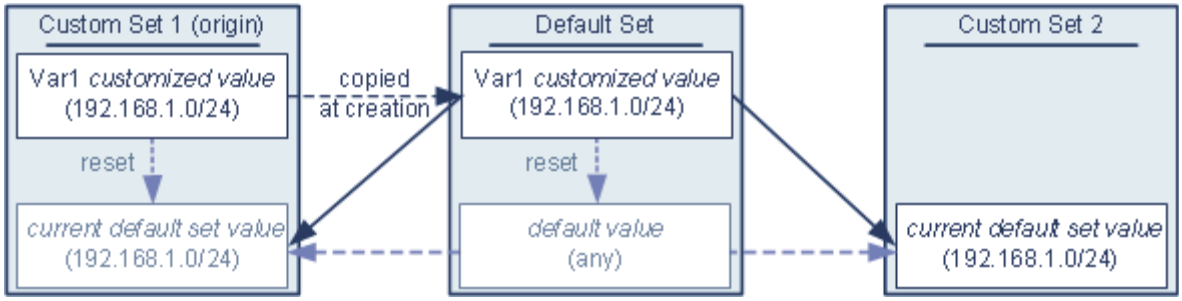
선택적으로, 어떤 집합에서든 Var1의 값을 사용자 지정할 수 있습니다. Var1이 사용자 지정된 Custom Set 2에서는 값이 192.168.1.0/24입니다. Custom Set 1에서는 Var1의 사용자 지정된 값 192.168.2.0/24가 기본값을 재정의합니다. 기본 집합의 사용자 정의 변수를 재설정하면 모든 집합에서 해당 기본값이 any로 재설정됩니다.

이 예에서는 다음 사항에 유의해야 합니다. Custom Set 2에서 Var1을 업데이트하지 않은 상태로 기본 집합에서 Var1을 추가로 사용자 지정하거나 재설정하면 Custom Set 2에서 Var1의 현재 기본값이 업데이트되어, 변수 집합에 연결된 침입 정책이 영향을 받게 됩니다.

이 예에는 표시되지 않았지만 집합 간 상호 작용은 사용자 정의 변수와 기본 변수에 대해 동일합니다. 단, 기본 집합에서 기본 변수를 재설정하면 현재 규칙 업데이트에서 Cisco에 의해 구성된 값으로 재설정됩니다.

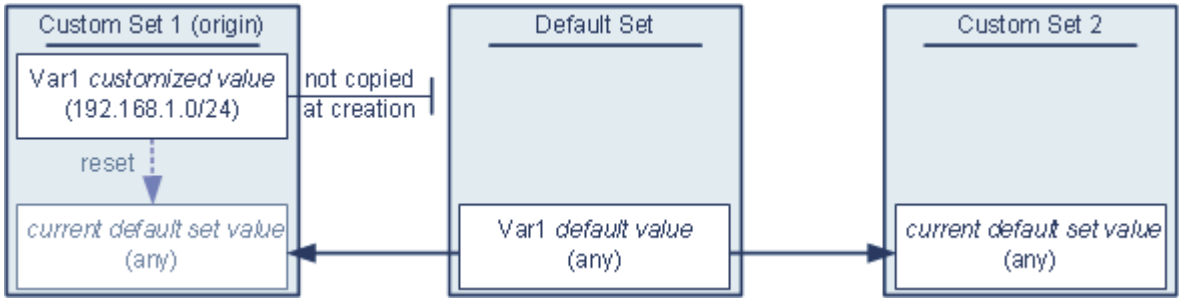
예: 사용자 정의 변수를 사용자 지정 집합에 추가

다음의 두 가지 예는 사용자 정의 변수를 사용자 지정 집합에 추가할 때의 변수 집합 상호 작용에 대해 설명합니다. 새 변수를 저장할 때, 구성된 값을 다른 집합에 대한 기본값으로 사용할지를 묻는 메시지가 표시됩니다. 다음 예에서는 구성된 값을 **사용하기로** 선택합니다.



Custom Set 1에서 온 Var1의 출처를 제외하고, 이 예는 기본 집합에 Var1을 추가한 위의 예와 동일합니다. Var1에 대한 사용자 지정된 값 192.168.1.0/24를 Custom Set 1에 추가하면 기본값 any의 사용자 지정된 값으로서 기본 집합에 값이 복사됩니다. 따라서 기본 집합에 Var1을 추가한 것처럼 Var1 값 및 상호 작용은 동일합니다. 이전의 예와 마찬가지로, 기본 집합에서 Var1을 추가로 사용자 지정하거나 재설정하면 Custom Set 2에서 Var1의 현재 기본값이 업데이트되어, 변수 집합에 연결된 침입 정책이 영향을 받게 됩니다.

다음 예에서는 이전 예처럼 값 192.168.1.0/24의 Var1을 Custom Set 1에 추가하되, Var1의 구성된 값을 다른 집합의 기본값으로 **사용하지 않기로** 선택합니다.



이렇게 하면 Var1이 기본값 any로 모든 집합에 추가됩니다. Var1을 추가한 후에는 어떤 집합에서든 값을 사용자 지정할 수 있습니다. 이 방식의 이점은 다음과 같습니다. 기본 집합에서 초기에 Var1을 사용자 지정하지 않음으로써 기본 집합의 값을 사용자 지정하는 위험, 그에 따라 집합(예: Var1을 사용자 지정하지 않은 Custom Set 2)에서 현재 값을 실수로 변경하는 위험을 줄일 수 있습니다.

변수 집합 관리

라이센스: 보호

Object Manager 페이지(**Objects > Object Management**)에서 **Variable Sets**를 선택하면 객체 관리자에 기본 변수 집합 및 사용자가 생성한 사용자 지정 집합이 나열됩니다.

새로 설치된 시스템에서 기본 변수 집합은 Cisco에서 사전 정의한 기본 변수로만 구성됩니다.

각 변수 집합에는 Cisco에서 제공한 기본 변수 및 사용자가 임의의 변수 집합에서 추가한 모든 사용자 지정 변수가 포함됩니다. 기본 집합은 수정할 수 있지만 이름을 변경하거나 삭제할 수는 없습니다.

주의 액세스 제어 또는 침입 정책을 가져오면 가져온 기본 변수가 기본 변수 집합의 기본 변수를 덮어쓰게 됩니다. 가져온 기본 변수 집합에 없는 사용자 지정 변수가 기존 기본 변수 집합에 포함되어 있으면, 고유한 변수가 유지됩니다. 자세한 내용은 A-5페이지의 컨피그레이션 가져오기을/를 참조하십시오.

다음 표에는 변수 집합을 관리하기 위해 수행할 수 있는 작업이 요약되어 있습니다.

표 3-3 변수 집합 관리 작업

목적	가능한 작업
변수 집합 표시	**Objects > Object Management**와 **Variable Set**를 차례로 선택.
이름으로 변수 집합 필터링	이름 입력을 시작합니다. 입력하는 동안 페이지가 새로 고쳐지면서 일치하는 이름이 표시됩니다.
이름 필터링 지우기	필터 필드에서 지우기 아이콘(✖)을 클릭합니다.

표 3-3 변수 집합 관리 작업(계속)

목적	가능한 작업
사용자 지정 변수 집합 추가	**Add Variable Set**를 클릭합니다. 사용자 편의를 위해, 새 변수 집합에는 모든 현재 정의된 기본 변수 및 사용자 지정된 변수가 포함됩니다. **참고** 변수 집합 이름에는 파이프(|) 또는 중괄호({})를 제외한 인쇄 가능한 표준 ASCII 문자를 사용할 수 있습니다.
변수 집합 수정	수정하려는 변수 집합 옆에 있는 수정 아이콘( )을 클릭합니다. **팁** 변수 집합의 행 내에서 오른쪽 클릭 후 **Edit**를 선택해도 됩니다.
사용자 지정 변수 집합 삭제	변수 집합 옆에 있는 삭제 아이콘( )을 클릭한 다음 **Yes**를 클릭합니다. 기본 변수 집합은 삭제할 수 없습니다. 삭제하는 변수 집합에 생성된 변수는 다른 집합에서는 삭제되거나 달리 영향을 받지 않습니다. **팁** 변수 집합의 행 내에서 오른쪽 클릭 후 **Delete**를 선택하고 **Yes**를 클릭해도 됩니다. 여러 집합을 선택하려면 Ctrl 키와 Shift 키를 사용합니다.

변수 집합을 구성한 후 이를 침입 정책에 연결할 수 있습니다.

변수 집합을 생성 또는 수정하려면

액세스: Admin/Access Admin/Network Admin

1단계 **Objects > Object Management**를 선택합니다.

Object Management 페이지가 나타납니다.

2단계 **Variable Set**를 선택합니다.

3단계 변수 집합을 추가하거나 기존 집합을 수정하려면

- 변수 집합을 추가하려면 **Add Variable Set**를 클릭합니다.
- 변수 집합을 수정하려면 변수 집합 옆에 있는 수정 아이콘( )을 클릭합니다.

New or Edit Variable Set 페이지가 나타납니다. 변수 집합 이름에는 파이프(|) 또는 중괄호({})를 제외한 인쇄 가능한 표준 ASCII 문자를 사용할 수 있습니다. 변수 집합 내에서 변수를 추가 및 수정하는 방법에 대한 자세한 내용은 3-25페이지의 변수 추가 및 수정을/를 참조하십시오.

변수 관리

라이센스: 보호

변수 집합 내 New or Edit Variables 페이지에서 변수를 관리합니다. 모든 변수 집합에 대한 변수 페이지는 변수를 Customized Variables and Default Variables 페이지 영역으로 분리합니다.

*기본 변수*는 Cisco에서 제공하는 변수입니다. 기본 변수의 값을 사용자 지정할 수 있습니다. 기본 변수는 이름을 변경하거나 삭제할 수 없으며, 기본값을 변경할 수도 없습니다.

*사용자 지정된 변수*는 다음 중 하나입니다.

- 사용자 지정된 기본 변수

  기본 변수에 대한 값을 수정하면 해당 변수는 Default Variables 영역에서 Customized Variables 영역으로 이동합니다. 기본 집합의 변수 값은 사용자 지정 집합에 있는 변수의 기본값을 결정하므로, 기본 집합의 기본 변수를 사용자 지정하면 다른 모든 집합에서 변수의 기본값이 수정됩니다.

- 사용자 정의 변수

  자신의 고유한 변수는 추가 및 삭제할 수 있고, 다른 변수 집합 내에서 해당 값을 사용자 지정할 수 있으며, 사용자 지정된 변수를 기본값으로 재설정할 수 있습니다. 사용자 정의 변수를 재설정하면 Customized Variables 영역에 남아 있게 됩니다.

다음 표에는 변수를 생성 또는 수정하기 위해 수행할 수 있는 작업이 요약되어 있습니다.

표 3-4 변수 관리 작업

목적	가능한 작업
변수 페이지 표시	변수 집합 페이지에서 **Add Variable Set**를 클릭하여 새 변수 집합을 생성하거나, 수정할 변수 집합 옆에 있는 수정 아이콘( )을 클릭합니다.
변수 집합의 이름 지정 및 선택적으로 설명 추가	**Name** 및 **Description** 필드에 공백과 특수 문자를 포함한 영숫자 문자열을 입력합니다. **참고** 변수 집합 이름에는 파이프(|) 또는 중괄호({})를 제외한 인쇄 가능한 표준 ASCII 문자를 사용할 수 있습니다.
변수에 대한 전체 값 표시	변수 옆에 있는 **Value** 열에서 값 위로 포인터를 이동합니다. **참고** 변수 값에는 최대 8192자를 포함할 수 있습니다. 그러나 이 제한은 변수의 확장된 값의 크기에 적용됩니다. 하나 이상의 변수를 사용하여 다른 변수를 정의하는 경우 모든 변수 값의 총 문자 및 공백 수는 8192자를 넘을 수 없습니다.
변수 추가	**Add**를 클릭합니다. 자세한 내용은 3-25페이지의 변수 추가 및 수정을/를 참조하십시오.
변수 수정	수정하려는 변수 옆에 있는 수정 아이콘( )을 클릭합니다. 자세한 내용은 3-25페이지의 변수 추가 및 수정을/를 참조하십시오.
수정된 변수를 기본값으로 재설정	수정된 변수 옆에 있는 재설정 아이콘( )을 클릭합니다. 공유 재설정 아이콘은 현재 값이 이미 기본값임을 나타냅니다. **팁** 기본값을 표시하려면 활성 재설정 아이콘 위로 포인터를 이동하십시오.
사용자 정의 사용자 지정 변수 삭제	변수 집합 옆에 있는 삭제 아이콘( )을 클릭합니다. 변수를 추가한 후 변수 집합을 저장한 경우 **Yes**를 클릭하여 변수를 삭제할 것임을 확인합니다. 기본 변수는 삭제할 수 없으며, 침입 규칙이나 다른 변수에서 사용되고 있는 사용자 정의 변수도 삭제할 수 없습니다.
변수 집합에 변경 사항 저장	변수 집합이 액세스 제어 정책에서 사용되고 있는 경우 변경 사항의 저장을 확인하려면 **Save**와 **Yes**를 차례로 클릭합니다. 기본 집합의 현재 값이 다른 모든 집합의 기본값을 결정하므로, 기본 집합에서 변수를 수정하거나 재설정하면 기본값을 사용자 지정하지 않은 다른 집합의 현재 값이 변경됩니다.

변수 집합에서 변수를 보려면

액세스: Admin/Access Admin/Network Admin

1단계 **Objects > Object Management**를 선택합니다.

Object Management 페이지가 나타납니다.

2단계 **Variable Set**를 선택합니다.

3단계 변수 집합을 추가하거나 기존 집합을 수정하려면

- 변수 집합을 추가하려면 **Add Variable Set**를 클릭합니다.
- 변수 집합을 수정하려면 변수 집합 옆에 있는 수정 아이콘( )을 클릭합니다.

New or Edit Variable Set 페이지가 나타납니다. 변수 집합 이름에는 파이프(|) 또는 중괄호({})를 제외한 인쇄 가능한 표준 ASCII 문자를 사용할 수 있습니다.

4단계 변수를 추가하거나 기존 변수를 수정합니다.

- 변수를 추가하려면 **Add**를 클릭합니다.
- 변수를 수정하려면 변수 옆에 있는 수정 아이콘( )을 클릭합니다.

New or Edit Variable 페이지가 나타납니다.

변수 집합 내에서 변수를 추가 및 수정하는 방법에 대한 자세한 내용은 3-25페이지의 변수 추가 및 수정을/를 참조하십시오.

변수 추가 및 수정

라이센스: 보호

사용자 지정 집합의 변수는 수정할 수 있습니다.

사용자 지정 표준 텍스트 규칙을 생성한 경우, 트래픽을 더 잘 반영하기 위해 또는 규칙 생성 프로세스를 간소화하기 위해 고유한 사용자 정의 변수를 추가할 수 있습니다. 예를 들어 DMZ에서만 트래픽을 검사하기 위한 규칙을 생성하는 경우 `$DMZ`라는 이름의 변수를 생성하여, 해당 값을 노출되는 서버 IP 주소에 나열할 수 있습니다. 그러면 이 영역에 대해 작성되는 모든 규칙에서 `$DMZ` 변수를 사용할 수 있습니다.

한 변수 집합에 변수를 추가하면 모든 변수 집합에 추가됩니다. 아래에서 설명한 한 가지를 제외하면, 변수는 기본값으로 다른 집합에 추가되며 다른 집합에서 사용자 지정할 수 있습니다.

사용자 지정 집합에서 변수를 추가하는 경우, 구성된 값을 기본 집합의 사용자 지정된 값으로 사용할지 여부를 선택해야 합니다.

- 구성된 값을 **사용하는** 경우(예: 192.168.0.0/16), 구성된 값을 사용자 지정된 값으로 사용하여(기본값 `any`) 기본 집합에 변수가 추가됩니다. 기본 집합의 현재 값이 다른 집합의 기본값을 결정하므로, 다른 사용자 지정 집합의 초기 기본값은 구성된 값입니다(이 예의 경우 192.168.0.0/16).
- 구성된 값을 **사용하지 않는** 경우 기본값 `any`만을 사용하여 변수가 기본 집합에 추가되므로, 다른 사용자 지정 집합의 초기 기본값은 `any`가 됩니다.

자세한 내용은 3-20페이지의 변수 집합 이해을/를 참조하십시오.

New Variable 페이지에서 변수 집합 내에 변수를 추가하고 Edit Variable 페이지에서 기존 변수를 수정합니다. 두 페이지의 사용 방법은 동일하지만, 기존 변수를 수정할 때는 변수 이름이나 유형을 변경할 수 없습니다.

각 페이지는 기본적으로 세 개의 창으로 구성됩니다.

- 기존 네트워크나 포트 변수, 객체, 네트워크 객체 그룹을 비롯한 사용 가능한 항목
- 변수 정의에 포함할 네트워크 또는 포트
- 변수 정의에서 제외할 네트워크 또는 포트

두 가지 변수 유형을 생성하거나 수정할 수 있습니다.

- *네트워크* 변수는 네트워크 트래픽에서 호스트의 IP 주소를 지정합니다. 3-29페이지의 네트워크 변수 작업을/를 참조하십시오.
- *포트* 변수는 네트워크 트래픽에서 TCP 또는 UDP 포트를 지정합니다(어느 한 유형에 대한 any 값 포함). 3-30페이지의 포트 변수 작업을/를 참조하십시오.

네트워크 또는 포트 변수 유형을 추가할지 여부를 지정하면 페이지가 새로 고쳐지고 사용 가능한 항목이 나열됩니다. 목록 위의 검색 필드를 사용하면 목록을 제한할 수 있으며, 목록은 입력 시 업데이트됩니다.

사용 가능한 항목을 선택한 다음 포함하거나 제외할 항목의 목록으로 끌어올 수 있습니다. 항목을 선택하고 **Include** 또는 **Exclude** 버튼을 클릭할 수도 있습니다. 여러 항목을 선택하려면 Ctrl 키와 Shift 키를 사용합니다. 포함된 항목 또는 제외된 항목의 목록 아래에 있는 컨피그레이션 필드를 사용하여 네트워크 변수에 대한 리터럴 IP 주소와 주소 블록, 그리고 포트 변수에 대한 포트와 포트 범위를 지정할 수 있습니다.

포함하거나 제외할 항목 목록은 리터럴 문자열과 기존 변수, 객체, 네트워크 객체 그룹(네트워크 변수의 경우)의 조합으로 구성할 수 있습니다.

다음 표에는 변수를 생성 또는 수정하기 위해 수행할 수 있는 작업이 요약되어 있습니다.

표 3-5 변수 수정 작업

목적	가능한 작업
변수 페이지 표시	변수 집합 페이지에서 **Add**를 클릭하여 새 변수를 추가하거나, 기존 변수 옆에 있는 수정 아이콘( )을 클릭합니다.
변수 이름 지정	고유한 대/소문자 구분 영숫자 문자열을 **Name** 필드에 입력합니다. 특수 문자 중에는 밑줄 문자(_)만 포함할 수 있습니다. 변수 이름은 대/소문자를 구분합니다. 예를 들어 `var`과 `Var`은 각각 고유합니다.
네트워크 또는 포트 변수 지정	**Type** 드롭다운 목록에서 **Network** 또는 **Port**를 선택합니다. 네트워크 및 포트 변수를 사용하고 구성하는 방법에 대한 자세한 내용은 3-29페이지의 네트워크 변수 작업 및 3-30페이지의 포트 변수 작업을/를 참조하십시오.
사용 가능한 네트워크의 목록에서 선택할 수 있도록 개별 네트워크 객체 추가	**Type** 드롭다운 목록에서 **Network**를 추가한 다음 추가 아이콘( )을 클릭합니다. 객체 관리자를 사용하여 네트워크 객체를 추가하는 방법에 대한 자세한 내용은 3-4페이지의 네트워크 객체 작업을/를 참조하십시오.
사용 가능한 포트의 목록에서 선택할 수 있도록 개별 포트 객체 추가	**Type** 드롭다운 목록에서 **Port**를 추가한 다음 추가 아이콘( )을 클릭합니다. 모든 포트 유형을 추가할 수 있지만 TCP 및 UDP 포트(어느 한 유형에 대한 any 값 포함)만이 유효한 변수 값이며, 사용 가능한 포트의 목록에는 이러한 값 유형을 사용하는 변수만 표시됩니다. 객체 관리자를 사용하여 포트 객체를 추가하는 방법에 대한 자세한 내용은 3-12페이지의 포트 객체 작업을/를 참조하십시오.
사용 가능한 포트 또는 네트워크 항목을 이름별로 검색	사용 가능한 항목의 목록 위에 있는 검색 필드에 이름을 입력하기 시작하면 페이지가 새로 고쳐지고 일치하는 이름이 표시됩니다.
이름 검색 지우기	Search 필드 위의 다시 로드 아이콘( )을 클릭하거나, 검색 필드의 지우기 아이콘( )을 클릭합니다.

표 3-5 변수 수정 작업(계속)

목적	가능한 작업
사용 가능한 항목 구분	변수 아이콘( ), 네트워크 객체 아이콘( ), 포트 아이콘( ), 객체 그룹 아이콘( ) 옆에서 항목을 찾습니다. 네트워크 그룹만 사용할 수 있습니다(포트 그룹은 사용 불가).
변수 정의에 포함하거나 제외할 객체 선택	사용 가능한 네트워크 또는 포트 목록에서 객체를 클릭합니다. 여러 객체를 선택하려면 Ctrl 및 Shift 키를 사용합니다.
포함된/제외된 네트워크 또는 포트의 목록에 선택한 항목 추가	선택한 항목을 끌어서 놓습니다. **Include** 또는 **Exclude**를 클릭해도 됩니다. 사용 가능한 항목의 목록에서 네트워크/포트 변수 및 객체를 추가할 수 있습니다. 네트워크 객체 그룹을 추가할 수도 있습니다.
포함하거나 제외할 네트워크 또는 포트의 목록에 리터럴 네트워크 또는 포트 추가	리터럴 **Network** 또는 **Port** 필드의 프롬프트를 클릭하여 제거하고, 네트워크 변수에 대해 리터럴 IP 주소나 주소 블록 또는 포트 변수에 대해 리터럴 포트나 포트 범위를 입력한 다음 **Add**를 클릭합니다. 도메인 이름 또는 목록은 입력할 수 없습니다. 여러 항목을 추가하려면 각각을 개별적으로 추가하십시오.
값 any로 변수 추가	변수의 이름을 지정하고 변수 유형을 선택한 다음 값을 구성하지 않은 채 **Save**를 클릭합니다. **참고** 변수 이름은 고유한 대/소문자 구분 영숫자 문자열이어야 하며, 특수 문자 중에는 밑줄 문자(_)만 포함할 수 있습니다.
포함된/제외된 목록에서 변수 또는 객체 삭제	변수 옆에 있는 삭제 아이콘( )을 클릭합니다.
새 변수 또는 수정된 변수 저장	**Save**를 클릭합니다. 사용자 지정 집합에서 변수를 추가하려면 **Yes**를 클릭하고, 기본값 any를 사용하려면 **No**를 클릭합니다.

자세한 내용은 다음 절을 참조하십시오.

- 3-29페이지의 네트워크 변수 작업
- 3-30페이지의 포트 변수 작업

변수를 추가 또는 수정하려면

액세스: Admin/Access Admin/Network Admin

1단계 **Objects > Object Management**를 선택합니다.

Object Management 페이지가 나타납니다.

2단계 **Variable Set**를 선택합니다.

3단계 변수 집합을 추가하거나 기존 집합을 수정하려면

- 변수 집합을 추가하려면 **Add Variable Set**를 클릭합니다.
- 기존 변수 집합을 수정하려면 변수 집합 옆에 있는 수정 아이콘( )을 클릭합니다.

New or Edit Variable Set 페이지가 나타납니다. 변수 집합 이름에는 파이프(|) 또는 중괄호({})를 제외한 인쇄 가능한 표준 ASCII 문자를 사용할 수 있습니다.

4단계 새 변수를 추가하거나 기존 변수를 수정합니다.

- 새 변수를 추가하려면 **Add**를 클릭합니다.
- 기존 변수를 수정하려면 변수 옆에 있는 수정 아이콘( )을 클릭합니다.

New or Edit Variable 페이지가 나타납니다.

팁 변수 페이지에서 오른쪽 클릭 컨텍스트 메뉴를 사용하여 항목을 선택하거나 삭제할 수 있습니다. 2-5페이지의 컨텍스트 메뉴 사용을/를 참조하십시오.

5단계 새 변수를 추가하려면

- 고유한 변수 **Name**을 입력합니다.

  영숫자 문자 및 밑줄 문자(_)를 사용할 수 있습니다.
- **Type** 드롭다운 목록에서 **Network** 또는 **Port** 변수를 선택합니다.

6단계 선택적으로, 사용 가능한 네트워크 또는 포트의 목록에서 포함된/제외된 항목의 목록으로 항목을 이동합니다.

하나 이상의 항목을 선택한 다음 끌어서 놓거나, **Include** 또는 **Exclude**를 클릭할 수 있습니다. 여러 항목을 선택하려면 Ctrl 키와 Shift 키를 사용합니다.

팁 네트워크나 포트 변수에 대한 포함된/제외된 목록의 주소 또는 포트가 중복되는 경우 제외된 주소 또는 포트가 우선 적용됩니다.

7단계 선택적으로, 단일 리터럴 값을 입력한 다음 **Add**를 클릭합니다.

네트워크 변수의 경우 단일 IP 주소 또는 주소 블록을 입력할 수 있습니다. 포트 변수의 경우 단일 포트를 추가하거나, 상한값과 하한값을 하이픈(-)으로 구분하여 포트 범위를 추가할 수 있습니다.

여러 리터럴 값을 입력하려면 이 단계를 필요한 만큼 반복합니다.

8단계 **Save**를 클릭하여 변수를 저장합니다. 사용자 지정 집합에서 새 변수를 추가하는 경우 다음 옵션을 이용할 수 있습니다.

- 구성된 값을 기본 집합의 사용자 지정된 값으로 사용하는 변수를 추가하여 다른 사용자 지정 집합의 기본값이 되도록 하려면 **Yes**를 클릭합니다.
- 기본 집합과 다른 사용자 지정 집합에서 변수를 any의 기본값으로 추가하려면 **No**를 클릭합니다.

9단계 변경이 완료되면 **Save**를 클릭하여 변수 집합을 저장한 다음 **Yes**를 클릭합니다.

변경 사항이 저장되며, 변수 집합이 연결된 액세스 제어 정책이 out-of-date 상태로 표시됩니다. 변경 사항을 반영하려면 변수 집합이 침입 정책에 연결된 액세스 제어 정책을 적용해야 합니다. 12-15 페이지의 액세스 제어 정책 적용을/를 참조하십시오.

네트워크 변수 작업

라이센스: 보호

네트워크 변수는 침입 정책과 침입 정책 규칙 억제에서 활성화한 침입 규칙, 동적 규칙 상태, 적응형 프로필에서 사용할 수 있는 IP 주소를 나타냅니다. 네트워크 변수는 침입 정책과 침입 규칙에만 사용할 수 있는 반면 네트워크 객체와 그룹은 액세스 제어 정책, 네트워크 변수, 침입 규칙, 네트워크 검색 규칙, 이벤트 검색, 보고서 등 시스템 웹 인터페이스의 여러 곳에서 IP 주소를 나타내기 위해 사용할 수 있다는 점에서 네트워크 변수가 네트워크 객체 및 네트워크 객체 그룹과 다릅니다. 자세한 내용은 3-4페이지의 네트워크 객체 작업을/를 참조하십시오.

네트워크에 있는 호스트의 IP 주소를 지정하기 위해 다음 컨피그레이션에서 네트워크 변수를 사용할 수 있습니다.

- 침입 규칙

  침입 규칙 **Source IPs** 및 **Destination IPs** 헤더 필드에서는 특정 IP 주소에서 오거나 그 주소로 이동하는 패킷으로 패킷 검사를 제한할 수 있습니다. 36-5페이지의 침입 규칙에서 IP 주소 지정을/를 참조하십시오.

- 억제

  소스 또는 목적지 침입 규칙 억제의 **Network** 필드에서는 특정 IP 주소 또는 IP 주소 범위가 침입 규칙이나 프리프로세서를 트리거할 때 침입 이벤트 알림을 억제할 수 있습니다. 32-26페이지의 침입 정책당 억제 구성을/를 참조하십시오.

- 동적 규칙 상태

  소스 또는 목적지 동적 규칙 상태의 **Network** 필드에서는 지정된 기간에 침입 규칙 또는 프리프로세서 규칙에 대한 일치가 너무 많이 발생하는 경우를 탐지합니다. 32-29페이지의 동적 규칙 상태 추가을/를 참조하십시오.

- 적응형 프로필

  적응형 프로필 **Networks** 필드에서는 패시브 구축에서 패킷 프래그먼트 및 TCP 스트림의 리어셈블리를 개선하려는 네트워크 맵의 호스트를 식별합니다. 30-1페이지의 수동 구축 시 전처리 튜닝을/를 참조하십시오.

이 절에서 설명하는 필드에서 변수를 사용하는 경우, 침입 정책에 연결한 변수 집합이 침입 정책을 사용하는 액세스 제어 정책에 의해 처리되는 네트워크 트래픽의 변수 값을 결정합니다.

다음 네트워크 컨피그레이션의 조합을 변수에 추가할 수 있습니다.

- 사용 가능한 네트워크 목록에서 선택하는 네트워크 변수, 네트워크 객체, 네트워크 객체 그룹의 임의의 조합

  객체 관리자를 사용하여 개별 및 그룹 네트워크 객체를 생성하는 방법에 대한 자세한 내용은 3-4페이지의 네트워크 객체 작업을/를 참조하십시오.

- New Variable or Edit Variable 페이지에서 추가한 다음 자신의 변수 및 기타 기존의/앞으로의 변수에 추가할 수 있는 개별 네트워크 객체

- 리터럴 단일 IP 주소 또는 주소 블록

  여러 리터럴 IP 주소 및 주소 블록을 개별적으로 추가하여 나열할 수 있습니다. IPv4 및 IPv6 주소와 주소 블록을 따로 또는 조합하여 나열할 수 있습니다. IPv6 주소를 지정할 때 RFC 4291에 정의된 주소 표기 규칙을 사용할 수 있습니다.

추가하는 변수에서 포함된 네트워크에 대한 기본값은 `any`인데, 이는 IPv4 또는 IPv6 주소를 나타냅니다. 제외된 네트워크의 기본값은 `none`인데, 이는 네트워크가 없음을 나타냅니다. 포함된 네트워크 목록에 있는 임의의 IPv6 주소 또는 제외 목록에 IPv6 주소 없음을 나타내기 위해 리터럴 값에 주소 `::`을 지정할 수도 있습니다.

네트워크를 제외된 목록에 추가하면 지정된 주소 및 주소 블록이 부정됩니다. 즉, 제외된 IP 주소 또는 주소 블록 외에 임의의 IP 주소를 매칭할 수 있습니다.

예를 들어 리터럴 주소 `!192.168.1.1`을 제외하면 192.168.1.1 이외의 IP 주소가 지정되고, `2001:db8:ca2e::fa4c`를 제외하면 2001:db8:ca2e::fa4c 이외의 IP 주소가 지정됩니다.

리터럴 또는 사용 가능한 네트워크를 사용하여 네트워크의 임의의 조합을 제외할 수 있습니다. 예를 들어 리터럴 값 `192.168.1.1`과 `192.168.1.5`를 제외하면 192.168.1.1 또는 192.168.1.5 외의 IP 주소가 *포함*됩니다. 즉, 시스템은 이를 "192.168.1.1이 **아니고** 192.168.1.5**도 아닌** 주소"로 해석합니다. 즉, 대괄호 안에 나열된 주소 이외의 IP 주소를 매칭합니다.

네트워크 변수를 추가 또는 수정할 경우 다음 사항에 유의하십시오.

- 제외될 경우 주소 없음을 나타낼 수 있는 값 `any`는 논리적으로 제외할 수 없습니다. 예를 들면 제외된 네트워크의 목록에 값 `any`의 변수를 추가할 수 없습니다.
- 네트워크 변수는 지정된 침입 규칙 및 침입 정책 기능에 대해 트래픽을 식별합니다. 침입 규칙에 사용된 네트워크 변수로 정의한 호스트와 상관없이 프리프로세서 규칙은 이벤트를 트리거할 수 있습니다.
- 제외된 값은 포함된 값의 하위 집합으로 해석해야 합니다. 예를 들면 주소 블록 192.168.5.0/24를 포함하면서 192.168.6.0/24를 제외할 수는 없습니다. 포함된 값의 범위를 벗어나는 값을 제외하면 오류 메시지가 나타나서 변수 위반을 경고하며 변수 집합을 저장할 수 없게 됩니다.

네트워크 변수의 추가 및 수정에 대한 자세한 내용은 3-25페이지의 변수 추가 및 수정을/를 참조하십시오.

포트 변수 작업

라이센스: 보호

포트 변수는 침입 정책에서 활성화하는 침입 규칙의 **Source Port** 및 **Destination Port** 헤더 필드에서 사용할 수 있는 TCP 및 UDP 포트를 나타냅니다. 포트 변수는 침입 규칙에서만 사용할 수 있다는 점에서 포트 객체 및 포트 객체 그룹과 다릅니다. TCP 및 UDP 외의 프로토콜에 대한 포트 객체를 생성할 수 있으며 포트 변수, 액세스 제어 정책, 네트워크 검색 규칙, 이벤트 검색을 비롯한 웹 인터페이스의 여러 곳에서 포트 객체를 사용할 수 있습니다. 자세한 내용은 3-12페이지의 포트 객체 작업을/를 참조하십시오.

특정 TCP 또는 UDP 포트에서 오거나 그 포트로 이동하는 패킷으로 패킷 검사를 제한하려면 **Source Port** 및 **Destination Port** 헤더 필드의 침입 규칙에서 포트 변수를 사용할 수 있습니다.

이러한 필드에서 변수를 사용하면, 액세스 제어 규칙 또는 정책과 관련이 있는 침입 정책에 연결된 변수 집합이 액세스 제어 정책을 적용하는 네트워크 트래픽에서 이러한 변수의 값을 결정합니다.

다음 포트 컨피그레이션의 조합을 변수에 추가할 수 있습니다.

- 사용 가능한 포트의 목록에서 선택하는 포트 변수 및 포트 객체의 조합

  사용 가능한 포트의 목록은 포트 객체 그룹을 표시하지 않으며, 이들을 변수에 추가할 수 없습니다. 객체 관리자를 사용하여 포트 객체를 생성하는 방법에 대한 자세한 내용은 3-12페이지의 포트 객체 작업을/를 참조하십시오.

- New Variable or Edit Variable 페이지에서 추가한 다음 자신의 변수 및 기타 기존의/앞으로의 변수에 추가할 수 있는 개별 포트 객체

  TCP 및 UDP 포트(어느 한 유형에 대한 `any` 값 포함)만이 유효한 변수 값입니다. New or Edit Variables 페이지를 사용하여 유효한 변수 값이 아닌 유효한 포트 객체를 추가하는 경우, 객체는 시스템에 추가되지만 사용 가능한 객체 목록에 표시되지 않습니다. 객체 관리자를 사용하여 변수에서 사용되는 포트 객체를 수정하는 경우, 해당 값만을 유효한 변수 값으로 변경할 수 있습니다.

- 단일 리터럴 포트 값 및 포트 범위

  포트 범위는 대시(-)로 구분해야 합니다. 이전 버전과의 호환성을 위해 콜론(:)으로 표시되는 포트 범위는 지원되지만, 새로 생성하는 포트 변수에서는 콜론을 사용할 수 없습니다.

  임의의 조합으로 각각을 개별적으로 추가하여 여러 리터럴 포트 값 및 범위를 나열할 수 있습니다.

포트 변수를 추가 또는 수정할 경우 다음 사항에 유의하십시오.

- 추가하는 변수에서 포함된 포트에 대한 기본값은 any인데, 이는 포트 또는 포트 범위를 나타냅니다. 제외된 포트의 기본값은 none인데, 이는 포트가 없음을 나타냅니다.

팁 값 any의 변수를 생성하려면 특정 값을 추가하지 않은 채 변수의 이름을 지정하고 저장하십시오.

- 제외될 경우 포트 없음을 나타낼 수 있는 값 any는 논리적으로 제외할 수 없습니다. 예를 들어 제외된 포트의 목록에 값 any의 변수를 추가하면 변수 집합을 저장할 수 없습니다.
- 포트를 제외된 목록에 추가하면 지정된 포트 및 포트 범위가 부정됩니다. 즉, 제외된 포트 또는 포트 범위 외에 임의의 포트를 매칭할 수 있습니다.
- 제외된 값은 포함된 값의 하위 집합으로 해석해야 합니다. 예를 들어 포트 범위 10~50을 포함하면서 포트 60을 제외할 수는 없습니다. 포함된 값의 범위를 벗어나는 값을 제외하면 오류 메시지가 나타나서 변수 위반을 경고하며 변수 집합을 저장할 수 없게 됩니다.

포트 변수의 추가 및 수정에 대한 자세한 내용은 3-25페이지의 변수 추가 및 수정을/를 참조하십시오.

변수 재설정

라이센스: 보호

변수 집합 New or Edit Variables 페이지에서 변수를 기본값으로 재설정할 수 있습니다. 다음 표에는 변수 재설정의 기본 원리가 요약되어 있습니다.

표 3-6 변수 재설정 값

재설정할 변수 유형	집합 유형	다음으로 재설정
default	default	규칙 업데이트 값
사용자 정의	default	any
기본값 또는 사용자 정의	custom	현재 기본 집합 값(수정됨 또는 수정되지 않음)

사용자 지정 집합에서 변수를 재설정하면 기본 집합의 해당 변수에 대한 현재 값으로 재설정됩니다.

반대로, 기본 집합에서 변수 값을 재설정 또는 수정하면 모든 사용자 지정 집합에서 해당 변수의 기본값이 항상 업데이트됩니다. 재설정 아이콘이 변수를 재설정할 수 없음을 나타내는 회색으로 표시되면 이는 해당 집합에서 변수에 사용자 지정된 값이 없음을 의미합니다. 사용자 지정 집합의 변수에 대해 값을 사용자 지정하지 않으면, 기본 집합에서 변수를 변경할 경우 변수 집합에 연결한 침입 정책에 사용되는 값이 업데이트됩니다.

참고 기본 집합의 변수를 수정할 때, 특히 사용자 지정 집합에서 변수 값을 사용자 지정하지 않은 경우에는 이러한 변경이 연결된 사용자 지정 집합의 변수를 사용하는 침입 정책에 어떤 영향을 미치는지 평가하는 것이 좋습니다.

재설정 값을 보려면 변수 집합의 재설정 아이콘( ) 위로 포인터를 이동할 수 있습니다. 사용자 지정된 값과 재설정 값이 동일하면 다음 중 하나를 나타내는 것입니다.

- 값 any로 변수를 추가한 사용자 지정 또는 기본 집합에 있는 것임
- 명시적인 값으로 변수를 추가했으며 구성된 값을 기본값으로 사용하도록 선택한 사용자 지정 집합에 있는 것임

변수 집합을 침입 정책에 연결

라이센스: 보호

기본적으로 FireSIGHT 시스템은 기본 변수 집합을 액세스 제어 정책에서 사용되는 모든 침입 정책에 연결합니다. 침입 정책을 사용하는 액세스 제어 정책을 적용하면 침입 정책에서 활성화한 침입 규칙이 연결된 변수 집합의 변수 값을 사용합니다.

액세스 제어 정책의 침입 정책에 사용되는 사용자 지정 변수 집합을 수정하면 시스템은 Access Control Policy 페이지에서 해당 정책의 상태를 out-of-date로 표시합니다. 변수 집합에서 변경 사항을 구현하려면 액세스 제어 정책을 다시 적용해야 합니다. 기본 집합을 수정하면 시스템은 침입 정책을 사용하는 모든 액세스 제어 정책의 상태를 out-of-date로 표시합니다. 변경 사항을 구현하려면 모든 액세스 제어 정책을 다시 적용해야 합니다.

자세한 내용은 다음 절을 참조하십시오.

- 기본 집합 외의 변수 집합을 액세스 제어 규칙에 연결하려면 18-7페이지의 액세스 제어 규칙을 구성하여 침입 방지 수행의 절차를 참조하십시오.
- 기본 집합 외의 변수 집합을 액세스 제어 정책의 기본 작업에 연결하려면 12-6페이지의 네트워크 트래픽의 기본 처리 및 검사 설정을/를 참조하십시오.
- 변수 집합을 침입 정책에 연결하는 정책을 비롯한 액세스 제어 정책을 적용하려면 12-15페이지의 액세스 제어 정책 적용을/를 참조하십시오.

고급 변수 이해

라이센스: 보호

고급 변수를 사용하면 웹 인터페이스를 통해 구성할 수 없는 기능을 구성할 수 있습니다. FireSIGHT 시스템에서는 현재 고급 변수를 2개만 제공하지만, USER_CONF 고급 변수만 수정할 수 있습니다.

USER_CONF

USER_CONF는 웹 인터페이스를 통해 사용할 수 없는 하나 이상의 기능을 구성할 수 있는 일반 툴을 제공합니다.

주의 기능 설명에 나와 있거나 지원 팀에서 안내한 경우가 아니면 침입 정책 기능을 구성하는 데 USER_CONF 고급 변수를 사용하지 **마십시오**. 컨피그레이션이 충돌하거나 중복되면 시스템이 중단됩니다.

USER_CONF를 수정할 때 한 줄에 최대 4096자를 입력할 수 있습니다. 텍스트는 자동으로 줄 바꿈됩니다. 변수의 최대 문자 길이 8192자 또는 디스크 공간 등 물리적 제한에 도달할 때까지 원하는 만큼의 유효한 지침 또는 줄을 포함할 수 있습니다. 명령 지시문에서 완전한 인수 뒤에 백슬래시(\) 줄 계속 문자를 사용하십시오.

USER_CONF를 재설정하면 빈 상태가 됩니다.

SNORT_BPF

SNORT_BPF는 FireSIGHT 시스템 소프트웨어 릴리스 버전 5.3.0 이전(후에 버전 5.3.0 이상으로 업그레이드)의 시스템에서 구성된 경우에만 나타나는 레거시 고급 변수입니다. 이 변수는 보거나 삭제할 수만 있습니다. 수정하거나 삭제 후 복구할 수 없음.

이 변수를 사용하면 트래픽이 시스템에 도달하기 전 BPF(Berkeley Packet Filter)를 적용하여 트래픽을 필터링할 수 있습니다. SNORT_BPF에서 제공한 필터링을 적용하는 데 이제 이 변수 대신 액세스 제어 규칙을 사용할 수 있습니다. 이 변수는 시스템 업그레이드 전에 존재하던 컨피그레이션에만 나타납니다.

파일 목록 작업

라이센스: 악성코드

지원되는 디바이스: Series 2 또는 X-Series를 제외한 모두

지원되는 Defense Center: DC500을 제외한 모두

네트워크 기반 AMP(advanced malware protection)를 사용 중인데 종합 보안 인텔리전스 클라우드에서 파일의 성향을 잘못 식별하는 경우, 앞으로 파일을 더 잘 탐지하려면 SHA-256 해시 값을 사용하여 파일을 *파일 목록*에 추가할 수 있습니다. 파일 목록 유형에 따라 다음을 수행할 수 있습니다.

- 클라우드가 정상 성향을 할당한 것처럼 파일을 취급하려면 *정상 목록*에 파일을 추가합니다.
- 클라우드가 악성코드 성향을 할당한 것처럼 파일을 취급하려면 *사용자 지정 탐지 목록*에 파일을 추가합니다.

이러한 파일에 대한 차단 동작을 수동으로 지정하므로 클라우드에서 파일을 악성코드로 식별하더라도 시스템은 악성코드 클라우드 조회를 수행하지 않습니다. 파일 정책에서 규칙을 **Malware Cloud Lookup** 또는 **Block Malware** 작업으로 구성해야 하며, 파일의 SHA 값을 계산하도록 일치하는 파일 형식을 구성해야 합니다. 자세한 내용은 37-17페이지의 파일 규칙 작업을/를 참조하십시오.

시스템의 정상 목록 및 사용자 지정 탐지 목록은 기본적으로 모든 파일 정책에 포함됩니다. 정책 단위로 둘 중 하나 또는 두 목록을 모두 사용하지 않도록 선택할 수 있습니다.

주의 실제로 악성코드인 파일은 이 목록에 포함하지 **마십시오**. 클라우드가 파일에 Malware 성향을 할당했더라도 또는 파일을 사용자 지정 탐지 목록에 추가했더라도 시스템에서는 해당 파일을 차단하지 않습니다.

각 파일 목록에는 최대 10000개의 고유한 SHA-256 값을 포함할 수 있습니다. 파일 목록에 파일을 추가하려면 다음과 같이 할 수 있습니다.

- 이벤트 뷰어 컨텍스트 메뉴를 사용하여 SHA-256 값을 추가합니다.
- 시스템이 파일의 SHA-256 값을 계산하고 추가하도록 파일을 업로드합니다.
- 파일의 SHA-256 값을 직접 입력합니다.
- 여러 SHA-256 값이 포함된 CSV(쉼표로 구분된 값) 소스 파일을 생성하여 업로드합니다. 중복되지 않은 모든 SHA-256 값이 파일 목록에 추가됩니다.

파일을 파일 목록에 추가하거나 파일 목록에서 SHA-256 값을 수정 또는 삭제할 때 변경 사항을 반영하려면 목록을 사용하는 파일 정책이 포함된 모든 액세스 제어 정책을 다시 적용해야 합니다.

파일을 파일 목록에 추가하면 액세스 제어에 영향을 미치므로, 파일 목록의 모든 부분을 관리할 수 있는 다음 권한 중 하나가 필요합니다.

- 관리자 액세스 권한
- Network Admin 또는 Access Admin 액세스 권한(파일 목록 수정), Security Approver 액세스 권한(액세스 제어 정책 다시 적용), Security Analyst 또는 Security Analyst(RO) 액세스 권한(이벤트 보기에서 SHA-256 값을 사용하여 파일 추가)의 조합
- Modify Access Control Policy 및 Object Manager(파일 목록 수정), Apply Access Control Policy(액세스 제어 정책 다시 적용), Modify File Events(이벤트 보기에서 SHA-256 값을 사용하여 파일 추가) 권한이 있는 사용자 지정 역할. 12-4페이지의 사용자 지정 사용자 역할로 구축 관리을/를 참조

파일 목록 사용에 대한 자세한 내용은 다음 항목을 참조하십시오.

- 2-5페이지의 컨텍스트 메뉴 사용
- 3-34페이지의 파일 목록에 여러 SHA-256 값 업로드
- 3-35페이지의 개별 파일을 파일 목록에 업로드
- 3-36페이지의 SHA-256 값을 파일 목록에 추가
- 3-37페이지의 파일 목록의 파일 수정
- 3-37페이지의 파일 목록에서 소스 파일 다운로드

파일 목록에 여러 SHA-256 값 업로드

라이센스: 악성코드

지원되는 디바이스: Series 2 또는 X-Series를 제외한 모두

지원되는 Defense Center: DC500을 제외한 모두

SHA-256 값과 설명의 목록을 포함하는 CSV 소스 파일을 업로드하여 파일 목록에 여러 SHA-256 값을 추가할 수 있습니다. 방어 센터는 내용을 검증하고 파일 목록을 유효한 SHA-256 값으로 채웁니다.

소스 파일은 .csv 파일 이름 확장명이 있는 단순한 텍스트 파일이어야 합니다. 헤더는 파운드 기호(#)로 시작해야 합니다. 파운드 기호로 시작된 헤더는 코멘트로 취급되어 업로드되지 않습니다. 각 항목은 단일 SHA-256 값과 그 뒤에 최대 256자의 영숫자 또는 특수 문자로 구성된 설명을 포함해야 하며, LF 또는 CR+LF 새 줄 문자로 끝나야 합니다. 항목의 다른 추가 정보는 무시됩니다.

다음에 유의하십시오.

- 파일 목록에서 소스 파일을 삭제하면 모든 관련된 SHA-256 해시도 제거됩니다.
- 성공적인 소스 파일 업로드 결과 파일 목록에 10000개가 넘는 서로 다른 SHA-256 값이 포함되는 경우 파일 목록에 여러 파일을 업로드할 수 없습니다.
- 업로드 시 256자가 넘는 설명은 처음 256자에서 잘립니다. 설명에 쉼표가 있으면 이스케이프 문자(\,)를 사용해야 합니다. 설명을 포함하지 않으면 소스 파일 이름이 대신 사용됩니다.
- 파일 목록에 SHA-256 값이 포함되어 있고 사용자가 이 값이 포함된 소스 파일을 업로드하면, 새로 업로드된 값이 기존의 SHA-256 값을 수정하지 않습니다. SHA-256 값과 관련된 캡처된 파일, 파일 이벤트 또는 악성코드 이벤트를 볼 때, 개별 SHA-256 값에서 위협 이름 또는 설명이 파생됩니다.
- 소스 파일의 유효하지 않은 SHA-256 값은 업로드되지 않습니다.
- 여러 업로드된 소스 파일에 동일한 SHA-256 값의 항목이 포함되어 있으면 가장 최근 값이 사용됩니다.

- 소스 파일에 동일한 SHA-256 값의 여러 항목이 포함되어 있으면 마지막 항목이 사용됩니다.
- 객체 관리자 내에서 직접 소스 파일을 수정할 수는 없습니다. 변경하려면 먼저 소스 파일을 직접 수정하고, 시스템에서 복사본을 삭제하고, 수정된 소스 파일을 업로드해야 합니다. 자세한 내용은 3-37페이지의 파일 목록에서 소스 파일 다운로드을/를 참조하십시오.

소스 파일을 파일 목록에 업로드하려면

액세스: Admin/Any Security Analyst

1단계 **Objects > Object Management**를 선택합니다.

Object Management 페이지가 나타납니다.

2단계 **File List**를 클릭합니다.

File List 섹션이 나타납니다.

3단계 소스 파일에서 값을 추가하려는 파일 목록 옆의 수정 아이콘()을 클릭합니다.

File List 팝업 창이 나타납니다.

4단계 **Add by** 필드에서 `List of SHAs`를 선택합니다.

팝업 창이 업데이트되어 새 필드가 표시됩니다.

5단계 선택적으로, **Description** 필드에 소스 파일에 대한 설명을 입력합니다.

설명을 입력하지 않으면 시스템에서 파일 이름을 사용합니다.

6단계 **Browse**를 클릭하여 소스 파일을 찾은 다음 **Upload and Add List**를 클릭하여 목록에 추가합니다.

소스 파일이 파일 목록에 추가됩니다. SHA-256 열에는 파일에 포함된 SHA-256 값의 개수가 나열됩니다.

7단계 **Save**를 클릭합니다.

8단계 파일 목록을 사용하는 파일 정책으로 모든 액세스 제어 정책을 다시 적용합니다.

정책이 적용되면 시스템은 파일 목록의 파일에 대해 더 이상 악성코드 클라우드 조회를 수행하지 않습니다.

개별 파일을 파일 목록에 업로드

라이센스: 악성코드

지원되는 디바이스: Series 2 또는 X-Series를 제외한 모두

지원되는 Defense Center: DC500을 제외한 모두

파일 목록에 복사하려는 파일의 복사본이 있는 경우 분석을 위해 파일을 방어 센터에 업로드할 수 있습니다. 시스템은 파일의 SHA-256 값을 계산하고 파일을 목록에 추가합니다. 시스템은 SHA-256 계산에서 파일 크기에 제한을 적용하지 않습니다.

방어 센터에서 해당 SHA-256 값을 계산하도록 하여 파일을 추가하려면

액세스: Admin/Network Admin

1단계 객체 관리자의 File List 페이지에서 파일을 추가하려는 정상 목록 또는 사용자 지정 탐지 목록 옆에 있는 수정 아이콘()을 클릭합니다.

File List 팝업 창이 나타납니다.

2단계 **Add by** 필드에서 **Calculate SHA**를 선택합니다.

팝업 창이 업데이트되어 새 필드가 표시됩니다.

3단계 선택적으로, **Description** 필드에 파일에 대한 설명을 입력합니다.

설명을 입력하지 않으면 업로드 시 설명에 파일 이름이 사용됩니다.

4단계 **Browse**를 클릭하여 소스 파일을 찾은 다음 **Calculate and Add SHA**를 클릭하여 목록에 추가합니다.

파일이 파일 목록에 추가됩니다.

5단계 **Save**를 클릭합니다.

6단계 파일 목록을 사용하는 파일 정책으로 모든 액세스 제어 정책을 다시 적용합니다.

정책이 적용되면 시스템은 파일 목록의 파일에 대해 더 이상 악성코드 클라우드 조회를 수행하지 않습니다.

SHA-256 값을 파일 목록에 추가

라이센스: 악성코드

지원되는 디바이스: Series 2 또는 X-Series를 제외한 모두

지원되는 Defense Center: DC500을 제외한 모두

파일 목록에 추가하기 위해 파일의 SHA-256 값을 제출할 수 있습니다. 중복된 SHA-256 값은 추가할 수 없습니다.

팁 파일의 전체 SHA-256 값을 보고 복사하려면 이벤트 보기에서 파일 또는 악성코드를 마우스 오른쪽 버튼으로 클릭하고 컨텍스트 메뉴에서 **Show Full Text**를 선택합니다.

파일의 SHA-256 값을 수동으로 입력하여 파일을 추가하려면

액세스: Admin/Network Admin

1단계 객체 관리자의 File List 페이지에서 파일을 추가하려는 정상 목록 또는 사용자 지정 탐지 목록 옆에 있는 수정 아이콘( )을 클릭합니다.

File List 팝업 창이 나타납니다.

2단계 **Add by** 필드에서 `Enter SHA Value`를 선택합니다.

팝업 창이 업데이트되어 새 필드가 표시됩니다.

3단계 **Description** 필드에 소스 파일에 대한 설명을 입력합니다.

4단계 파일의 전체 **SHA-256** 값을 입력하거나 붙여넣습니다. 시스템은 부분 값 매칭을 지원하지 않습니다.

5단계 **Add**를 클릭하여 파일을 추가합니다.

파일이 파일 목록에 추가됩니다.

6단계 **Save**를 클릭합니다.

7단계 파일 목록을 사용하는 파일 정책으로 모든 액세스 제어 정책을 다시 적용합니다.

정책이 적용되면 시스템은 파일 목록의 파일에 대해 더 이상 악성코드 클라우드 조회를 수행하지 않습니다.

파일 목록의 파일 수정

라이센스: 악성코드

지원되는 디바이스: Series 2 또는 X-Series를 제외한 모두

지원되는 Defense Center: DC500을 제외한 모두

파일 목록에서 개별 SHA-256 값을 수정 또는 삭제할 수 있습니다. 객체 관리자 내에서 직접 소스 파일을 수정할 수는 없습니다. 변경하려면 먼저 소스 파일을 직접 수정하고, 시스템에서 복사본을 삭제하고, 수정된 소스 파일을 업로드해야 합니다. 자세한 내용은 3-37페이지의 파일 목록에서 소스 파일 다운로드을/를 참조하십시오. 파일 목록에서 파일을 수정하려면

액세스: Admin/Network Admin

1단계 객체 관리자의 File List 페이지에서 파일을 수정하려는 정상 목록 또는 사용자 지정 탐지 목록 옆에 있는 수정 아이콘( )을 클릭합니다.

File List 팝업 창이 나타납니다.

2단계 수정하려는 SHA-256 값 옆에 있는 수정 아이콘( )을 클릭합니다.

Edit SHA-256 팝업 창이 나타납니다.

팁 목록에서 파일을 삭제할 수도 있습니다. 삭제하려는 파일 옆에 있는 삭제 아이콘( )을 클릭합니다.

3단계 **SHA-256** 값 또는 **Description**을 업데이트합니다.

4단계 **Save**를 클릭합니다.

File List 팝업 창이 나타납니다. 시스템이 목록에서 파일 항목을 업데이트합니다.

5단계 **Save**를 클릭합니다.

6단계 파일 목록을 사용하는 파일 정책으로 모든 액세스 제어 정책을 다시 적용합니다.

정책이 적용되면 시스템은 파일 목록의 파일에 대해 더 이상 악성코드 클라우드 조회를 수행하지 않습니다.

파일 목록에서 소스 파일 다운로드

라이센스: 악성코드

지원되는 디바이스: Series 2 또는 X-Series를 제외한 모두

지원되는 Defense Center: DC500을 제외한 모두

파일 목록에서 기존 소스 파일 항목을 보거나 다운로드하거나 삭제할 수 있습니다. 일단 업로드한 소스 파일은 수정할 수 없습니다. 파일 목록에서 소스 파일을 먼저 삭제한 후 업데이트된 파일을 업로드해야 합니다. 소스 파일 업로드에 대한 자세한 내용은 3-34페이지의 파일 목록에 여러 SHA-256 값 업로드을/를 참조하십시오.

소스 파일과 관련된 항목의 수는 서로 다른 SHA-256 값의 수를 참조합니다. 파일 목록에서 소스 파일을 삭제하면 소스 파일의 유효한 항목 수만큼 파일 목록에 포함된 총 SHA-256 항목 수가 줄어듭니다.

소스 파일을 다운로드하려면

액세스: Admin/Network Admin

1단계 객체 관리자의 File List 페이지에서 소스 파일을 다운로드하려는 정상 목록 또는 사용자 지정 탐지 목록 옆에 있는 수정 아이콘( )을 클릭합니다.

File List 팝업 창이 나타납니다.

2단계 다운로드하려는 소스 파일 옆에 있는 보기 아이콘( )을 클릭합니다.

View SHA-256's in list 팝업 창이 나타납니다.

3단계 **Download SHA List**를 클릭하고 화면의 지침에 따라 소스 파일을 저장합니다.

4단계 **Close**를 클릭합니다.

File List 팝업 창이 나타납니다.

보안 영역 작업

라이센스: 모두

*보안 영역*은 다양한 정책과 컨피그레이션에서 트래픽 플로우를 관리 및 분류하기 위해 사용할 수 있는 인라인, 패시브, 스위치드, 라우티드 또는 ASA 인터페이스의 그룹입니다. 단일 영역의 인터페이스를 여러 디바이스에서 사용할 수 있으며, 여러 영역을 단일 디바이스에서 구성할 수도 있습니다. 이 기능을 이용하면 다양한 정책을 적용할 수 있는 세그먼트로 네트워크를 나눌 수 있습니다. 한 보안 영역에 트래픽을 매칭하기 위해 적어도 하나의 인터페이스를 할당해야 하며, 각 인터페이스는 한 영역에만 속할 수 있습니다.

인터페이스 그룹화를 위해 보안 영역을 사용하는 것 외에도 액세스 제어 정책, 네트워크 검색 규칙, 이벤트 검색 등 시스템 웹 인터페이스의 여러 곳에서 영역을 사용할 수 있습니다. 예를 들어 특정 소스 또는 목적지 영역에만 적용되는 액세스 제어 규칙을 작성하거나, 특정 영역으로 오가는 트래픽으로 네트워크 검색을 제한할 수 있습니다.

보안 영역 객체를 업데이트하면 시스템은 객체의 새 개정을 저장합니다. 그 결과, 인터페이스에 보안 영역 객체의 서로 다른 여러 개정이 있는 관리되는 디바이스가 동일한 보안 영역에 있는 경우, 이중 연결처럼 보이는 내용이 로깅될 수 있습니다. 이중 연결 보고가 발견되면 객체의 동일한 개정을 사용하도록 모든 관리되는 디바이스를 업데이트할 수 있습니다. 객체 관리자에서 보안 영역을 수정하고, 모든 관리되는 디바이스를 제거하고, 객체를 저장하고, 관리되는 디바이스를 다시 추가하고, 객체를 다시 저장합니다. 그런 다음 영향받는 모든 디바이스 정책을 다시 적용합니다. 디바이스 정책 적용에 대한 자세한 내용은 4-25페이지의 디바이스에 변경 사항 적용을/를 참조하십시오.

보안 영역은 다음과 같은 방법으로 생성합니다.

- 초기 컨피그레이션 중에 디바이스에 대해 선택한 탐지 모드에 따라, 시스템이 디바이스 등록 시 보안 영역을 생성합니다. 예를 들어 시스템이 패시브 구축에서는 Passive 영역을 생성하는 반면, 인라인 구축에서는 External 및 Internal 영역을 생성합니다.
- 관리되는 디바이스에서 인터페이스를 구성하는 동안 즉석에서 보안 영역을 생성할 수 있습니다.
- 객체 관리자를 사용하여 보안 영역을 생성할 수 있습니다(**Objects > Object Management**).

객체 관리자의 Security Zones 페이지에는 관리되는 디바이스에 구성된 영역이 나열됩니다. 페이지의 각 영역에는 인터페이스 유형이 표시되며, 어떤 디바이스의 어떤 인터페이스가 각 영역에 속해 있는지 알아보려면 각 영역을 확장할 수 있습니다.

참고 한 보안 영역의 모든 인터페이스는 동일한 유형이어야 합니다. 즉, 모두가 인라인, 패시브, 스위치드, 라우티드 또는 ASA여야 합니다. 또한 보안 영역을 생성한 후에는 그곳에 포함된 인터페이스의 유형을 변경할 수 없습니다.

ASA 보안 컨텍스트를 수정하여 단일 컨텍스트 모드에서 멀티 컨텍스트 모드로 또는 그 반대로 전환하면, 보안 영역 컨피그레이션에서 모든 인터페이스가 제거됩니다.

사용 중인 보안 영역은 삭제할 수 없습니다. 영역에서 인터페이스를 추가 또는 제거한 후에는 인터페이스가 상주한 디바이스에 디바이스 컨피그레이션을 다시 적용해야 합니다. 해당 영역을 사용하는 액세스 제어 및 네트워크 검색 정책도 다시 적용해야 합니다.

보안 영역을 추가하려면

액세스: Admin/Access Admin/Network Admin

1단계 **Objects > Object Management**를 선택합니다.

Object Management 페이지가 나타납니다.

2단계 **Security Zones**를 선택합니다.

3단계 **Add Security Zone**을 클릭합니다.

Security Zones 팝업 창이 나타납니다.

4단계 영역의 **Name**을 입력합니다. 중괄호({}), 파이프(|), 세미콜론(;), 파운드 기호(#)를 제외한 모든 인쇄 가능한 표준 ASCII 문자를 사용할 수 있습니다.

5단계 영역의 인터페이스 **Type**을 선택합니다.

보안 영역을 생성한 후에는 유형을 변경할 수 없습니다.

6단계 영역에 추가할 인터페이스를 포함하는 디바이스를 **Device > Interfaces** 드롭다운 목록에서 선택합니다.

7단계 인터페이스를 하나 이상 선택합니다.

여러 객체를 선택하려면 Shift 및 Ctrl 키를 사용합니다. 관리되는 디바이스에서 아직 인터페이스를 구성하지 않은 경우 빈 영역을 생성하고 나중에 인터페이스를 추가할 수 있습니다. 이 경우 10단계 단계로 건너뜁니다.

8단계 **Add**를 클릭합니다.

선택한 인터페이스가 디바이스별로 그룹화되어 영역에 추가됩니다.

9단계 다른 디바이스의 인터페이스를 영역에 추가하려면 6~8단계를 반복합니다.

10단계 **Save**를 클릭합니다.

보안 영역이 추가됩니다.

암호 그룹 목록 작업

라이센스: 모두

지원되는 디바이스: Series 3

암호 그룹 목록은 여러 암호 그룹으로 구성된 객체입니다. 사전 정의된 각 암호 그룹 값은 SSL 또는 TLS 암호화 세션을 협상하는 데 사용되는 암호 그룹을 나타냅니다. 클라이언트와 서버가 해당 암호 그룹을 사용하여 SSL 세션을 협상했는지 여부를 기반으로 암호화된 트래픽을 제어하기 위해 SSL 규칙의 암호 그룹 및 암호 그룹 목록을 사용할 수 있습니다. SSL 규칙에 암호 그룹 목록을 추가하면 목록의 암호 그룹 중 하나와 협상한 SSL 세션이 규칙을 매칭합니다.

참고 암호 그룹 목록과 동일한 장소의 웹 인터페이스에서 암호 그룹을 사용할 수는 있지만 암호 그룹을 추가, 수정 또는 삭제할 수는 없습니다.

사용 중인 암호 그룹 목록은 삭제할 수 없습니다. 또한 SSL 정책에 사용된 암호 그룹 목록을 수정한 후 변경 사항을 반영하려면 관련 액세스 제어 정책을 다시 적용해야 합니다.

암호 그룹 목록을 생성하려면

액세스: Admin/Access Admin/Network Admin

1단계 **Objects > Object Management**를 선택합니다.

Object Management 페이지가 나타납니다.

2단계 **Cipher Suite List**를 선택합니다.

3단계 **Add Cipher Suites**를 클릭합니다.

Cipher Suite List 팝업 창이 나타납니다.

4단계 암호 그룹 목록의 **Name**을 입력합니다. 파이프(|) 또는 중괄호({})를 제외한 인쇄 가능한 표준 ASCII 문자를 사용할 수 있습니다.

5단계 하나 이상의 암호 그룹을 선택하고 **Add**를 클릭합니다.

- Shift 및 Ctrl 키를 사용하여 여러 암호 그룹을 선택하거나, 마우스 오른쪽 버튼을 클릭하고 **Select All**을 선택합니다.
- 포함할 기존 암호 그룹을 검색하려면 필터 필드( )를 사용합니다. 이 필드는 입력 시 업데이트되어 일치하는 항목을 표시합니다. 검색 문자열을 지우려면 검색 필드 위의 다시 로드 아이콘( )을 클릭하거나, 검색 필드의 지우기 아이콘( )을 클릭합니다.

6단계 **Save**를 클릭합니다.

암호 그룹 목록이 생성됩니다.

DN 객체 작업

라이센스: 모두

지원되는 디바이스: Series 3

각 DN 객체는 공개 키 인증서의 주체 또는 발행자에 대해 나열된 DN을 나타냅니다. 클라이언트와 서버가 주체 또는 발행자로서 DN과 함께 서버 인증서를 사용하여 SSL 세션을 협상했는지 여부를 기반으로 암호화된 트래픽을 제어하기 위해 SSL 규칙에서 DN 객체 및 그룹(3-2페이지의 객체 그룹화 참조)을 사용할 수 있습니다.

DN 객체는 CN 특성(**CN**)을 포함할 수 있습니다. "CN=" 없이 CN을 추가하면 객체를 저장하기 전에 시스템이 "CN="을 앞에 추가합니다.

다음 표에 나열된 각 특성 중 하나와 함께 쉼표로 구분하여 DN을 추가할 수 있습니다.

표 3-7 DN 특성

특성	설명	허용 값
C	국가 코드	영문자 2개
CN	공용 이름	최대 64자의 영숫자, 백슬래시(****), 하이픈(**-**), 따옴표(**'**), 별표(*****) 문자 또는 공백
O	조직	
OU	조직 단위	

특성에서 하나 이상의 별표(*****)를 와일드카드로 정의할 수 있습니다. CN 특성에서 도메인 이름 레이블당 하나 이상의 별표를 정의할 수 있습니다. 와일드카드로 여러 레이블을 정의할 수도 있지만 와일드카드는 해당 레이블 내에서만 매칭합니다. 다음 표의 예을/를 참조하십시오.

표 3-8 CN 특성 와일드카드 예

특성	일치	다음과 일치하지 않음
CN=”*ample.com”	example.com	mail.example.com example.text.com ampleexam.com
CN=”exam*.com”	example.com	mail.example.com example.text.com ampleexam.com
CN=”*xamp*.com”	example.com	mail.example.com example.text.com ampleexam.com
CN=”*.example.com”	mail.example.com	example.com example.text.com ampleexam.com

표 3-8 CN 특성 와일드카드 예(계속)

특성	일치	다음과 일치하지 않음
CN=”*.com”	example.com ampleexam.com	mail.example.com example.text.com
CN=”*.*.com”	mail.example.com example.text.com	example.com ampleexam.com

사용 중인 DN 객체는 삭제할 수 없습니다. 또한 SSL 정책에 사용된 DN 객체를 수정한 후 변경 사항을 반영하려면 관련 액세스 제어 정책을 다시 적용해야 합니다.

DN 객체를 추가하려면

액세스: Admin/Access Admin/Network Admin

1단계 **Objects > Object Management**를 선택합니다.

Object Management 페이지가 나타납니다.

2단계 **Distinguished Name** 아래에서 **Individual Objects**를 선택합니다.

3단계 **Add Distinguished Name**을 클릭합니다.

Distinguished Name 팝업 창이 나타납니다.

4단계 DN 객체의 **Name**을 입력합니다. 파이프(|) 또는 중괄호({})를 제외한 인쇄 가능한 표준 ASCII 문자를 사용할 수 있습니다.

5단계 DN 또는 CN의 값을 **DN** 필드에 입력합니다. 다음 옵션을 이용할 수 있습니다.

- DN을 추가하면 3-41 페이지의 표 3-7에 나열된 각 특성 중 하나를 쉼표로 구분하여 포함할 수 있습니다.
- CN을 추가하는 경우 여러 레이블과 와일드카드를 포함할 수 있습니다.

6단계 **Save**를 클릭합니다.

DN 객체가 추가됩니다.

PKI 객체 작업

라이센스: 모두

지원되는 디바이스: Series 3

PKI 객체는 SSL 검사 구축을 지원하는 데 필요한 공개 키 인증서 및 페어링된 개인 키를 나타냅니다. 내부 및 신뢰받는 CA 객체는 CA(인증 기관) 인증서로 구성되며, 내부 CA 객체는 인증서와 페어링된 개인 키도 포함합니다. 내부 및 외부 인증서 객체는 서버 인증서로 구성되며, 내부 인증서 객체는 인증서와 페어링된 개인 키도 포함합니다. SSL 규칙에서 이러한 객체를 사용하여 다음을 암호 해독할 수 있습니다.

- 발신 트래픽 - 내부 CA 객체로 서버 인증서를 다시 서명하여
- 수신 트래픽 - 내부 인증서 객체에서 알려진 개인 키를 사용하여

또한 SSL 규칙을 생성하고 다음으로 암호화된 트래픽을 매칭할 수 있습니다.

- 외부 인증서 객체의 인증서
- 신뢰받는 CA 객체에서 또는 CA의 신뢰 체인 내에서 CA에 의해 서명된 인증서

인증서와 키 정보를 수동으로 입력하거나, 해당 정보를 포함하는 파일을 업로드하거나, 경우에 따라 새 CA 인증서와 개인 키를 생성할 수 있습니다.

객체 관리자에서 PKI 객체의 목록을 볼 때 인증서의 Subject DN이 객체 값으로서 표시됩니다. 전체 인증서 Subject DN을 보려면 값 위로 포인터를 이동하십시오. 다른 인증서 세부사항을 보려면 PKI 객체를 수정하십시오.

참고 방어 센터 및 관리되는 디바이스는 저장 전에 무작위로 생성된 키를 이용하여 내부 CA 객체 및 내부 인증서 객체에 저장된 모든 개인 키를 암호화합니다. 비밀번호로 보호된 개인 키를 업로드하면 어플라이언스는 사용자 제공 비밀번호를 사용하여 키를 해독한 다음, 저장 전에 무작위로 생성된 키를 사용하여 다시 암호화합니다.

자세한 내용은 다음 절을 참조하십시오.

- 3-43페이지의 내부 인증 기관 객체 작업
- 3-48페이지의 신뢰받는 인증 기관 객체 작업
- 3-50페이지의 외부 인증 기관 객체 작업
- 3-51페이지의 내부 인증서 객체 작업

내부 인증 기관 객체 작업

라이센스: 모두

지원되는 디바이스: Series 3

사용자가 구성하는 각 내부 CA(인증 기관) 객체는 조직에서 제어하는 CA의 CA 공개 키 인증서를 나타냅니다. 객체는 객체 이름, CA 인증서 및 페어링된 개인 키로 구성됩니다. 내부 CA로 서버 인증서를 다시 서명하여 암호화된 발신 트래픽을 해독하려면 SSL 규칙의 내부 CA 객체 및 그룹(3-2페이지의 객체 그룹화 참조)을 사용할 수 있습니다.

참고 **Decrypt - Resign** SSL 규칙에서 내부 CA 객체를 참조하고 규칙이 암호화된 세션과 일치하는 경우, 사용자의 브라우저에 SSL 핸드셰이크를 협상하는 동안 인증서가 신뢰되지 않는다는 경고 메시지가 표시될 수 있습니다. 이 문제를 피하려면 내부 CA 객체 인증서를 신뢰받는 루트 인증서의 클라이언트 또는 도메인 목록에 추가하십시오.

다음과 같은 방법으로 내부 CA 객체를 생성할 수 있습니다.

- 기존의 RSA 기반 또는 EC(Elliptic Curve) 기반 CA 인증서와 개인 키 가져오기
- 새로운 자체 서명 RSA 기반 CA 인증서 및 개인 키 생성
- 서명되지 않은 RSA 기반 CA 인증서 및 개인 키 생성. 내부 CA 객체를 사용하려면 우선 인증서 서명을 위해 CSR(certificate signing request)을 다른 CA에 제출해야함

서명된 인증서를 포함하는 내부 CA 객체를 생성한 후에 CA 인증서 및 개인 키를 다운로드할 수 있습니다. 시스템은 다운로드된 인증서와 개인 키를 사용자 제공 비밀번호로 암호화합니다.

시스템에서 생성했든 사용자가 생성했든, 내부 CA 객체 이름을 수정할 수 있지만 다른 객체 속성은 수정할 수 없습니다.

사용 중인 내부 CA 객체는 삭제할 수 없습니다. 또한 SSL 정책에서 사용되는 내부 CA 객체를 수정하면 관련된 액세스 제어 정책은 out-of-date 상태가 됩니다. 변경 사항을 반영하려면 액세스 제어 정책을 다시 적용해야 합니다.

자세한 내용은 다음 절을 참조하십시오.

- 3-44페이지의 CA 인증서 및 개인 키 가져오기
- 3-45페이지의 새로운 CA 인증서 및 개인 키 생성
- 3-46페이지의 새로운 서명된 인증서 가져오기 및 업로드
- 3-47페이지의 CA 인증서 및 개인 키 다운로드

CA 인증서 및 개인 키 가져오기

라이센스: 모두

지원되는 디바이스: Series 3

X.509 v3 CA 인증서 및 개인 키를 가져와서 내부 CA 객체를 구성할 수 있습니다. 다음의 지원되는 형식 중 하나로 인코딩된 파일을 업로드할 수 있습니다.

- DER(Distinguished Encoding Rules)
- PEM(Privacy-enhanced Electronic Mail)

개인 키 파일이 비밀번호로 보호된 경우 해독 비밀번호를 제공할 수 있습니다. 인증서와 키가 PEM 형식으로 인코딩된 경우 정보를 복사하여 붙여넣을 수도 있습니다.

적절한 인증서 또는 키 정보를 포함하며 상호 페어링된 파일만 업로드할 수 있습니다. 시스템은 객체를 저장하기 전에 페어링을 검증합니다.

참고 **Decrypt - Resign** 작업으로 규칙을 구성할 경우 이 규칙은 구성된 규칙 조건과 더불어 참조된 내부 CA 인증서의 인증 알고리즘 유형을 기반으로 트래픽을 매칭합니다. 예를 들어 EC(Elliptic Curve) 기반 알고리즘으로 암호화된 발신 트래픽을 해독하려면 EC 기반 CA 인증서를 업로드해야 합니다. 자세한 내용은 21-10페이지의 Decrypt Actions: Decrypting Traffic for Further Inspection을/를 참조하십시오.

내부 CA 인증서 및 개인 키를 가져오려면

액세스: Admin/Access Admin/Network Admin

1단계 **Objects > Object Management**를 선택합니다.

Object Management 페이지가 나타납니다.

2단계 **PKI** 아래에서 **Internal CAs**를 선택합니다.

3단계 **Import CA**를 클릭합니다.

Import Internal Certificate Authority 팝업 창이 나타납니다.

4단계 내부 CA 객체의 **Name**을 입력합니다. 파이프(|) 또는 중괄호({})를 제외한 인쇄 가능한 표준 ASCII 문자를 사용할 수 있습니다.

5단계 **Certificate Data** 필드 위에서 **Browse**를 클릭하여 DER 또는 PEM으로 인코딩된 X.509 v3 CA 인증서 파일을 업로드합니다.

6단계 **Key** 필드 위에서 **Browse**를 클릭하여 DER 또는 PEM으로 인코딩된 페어링된 개인 키 파일을 업로드합니다.

7단계 업로드된 파일이 비밀번호로 보호된 경우 **Encrypted, and the password is:** 확인란을 선택하고 비밀번호를 입력합니다.

8단계 **Save**를 클릭합니다.

내부 CA 객체가 추가됩니다.

새로운 CA 인증서 및 개인 키 생성

라이센스: 모두

지원되는 디바이스: Series 3

자체 서명 RSA 기반 CA 인증서 및 개인 키를 생성하려면 식별 정보를 제공하여 내부 CA 객체를 구성할 수 있습니다. 다음 표에서는 인증서 생성을 위해 제공하는 식별 정보에 대해 설명합니다.

표 3-9 생성된 내부 CA 특성

필드	허용 값	필수
국가 이름(2자 코드)	영문자 2개	예
시/도	최대 64자의 영숫자, 백슬래시(/), 하이픈(-), 따옴표("), 별표(*), 마침표(.) 또는 공백 문자	아니요
지역 또는 구/군/시		
조직		
조직 단위		
공용 이름		

생성된 CA 인증서는 10년간 유효합니다. Valid From 날짜는 생성 이전의 주입니다.

자체 서명 CA 인증서를 생성하려면

액세스: Admin/Access Admin/Network Admin

1단계 **Objects > Object Management**를 선택합니다.

Object Management 페이지가 나타납니다.

2단계 **PKI** 아래에서 **Internal CAs**를 선택합니다.

3단계 **Generate CA**를 클릭합니다.

Generate Internal Certificate Authority 팝업 창이 나타납니다.

4단계 내부 CA 객체의 **Name**을 입력합니다. 파이프(|) 또는 중괄호({})를 제외한 인쇄 가능한 표준 ASCII 문자를 사용할 수 있습니다.

5단계 3-45 페이지의 표 3-9에 설명된 대로 식별 특성을 입력합니다.

6단계 **Generate self-signed CA**를 클릭합니다.

내부 CA 객체가 추가됩니다.

새로운 서명된 인증서 가져오기 및 업로드

라이센스: 모두

지원되는 디바이스: Series 3

CA에서 서명된 인증서를 가져와서 내부 CA 객체를 구성할 수 있습니다. 여기에는 두 단계가 관련됩니다.

- 내부 CA 객체를 구성하기 위한 식별 정보를 제공합니다. 그러면 서명되지 않은 인증서와 페어링된 개인 키, 그리고 사용자가 지정한 CA에 대한 CSR(certificate signing request)이 생성됩니다.
- CA가 서명된 인증서를 발행하면 이를 내부 CA 객체에 업로드하여 서명되지 않은 인증서를 교체합니다.

SSL 규칙에서 내부 CA 객체만 참조할 수 있습니다(해당 객체에 서명된 인증서가 포함된 경우).

서명되지 않은 CA 인증서 및 CSR을 생성하려면

액세스: Admin/Access Admin/Network Admin

1단계 **Objects > Object Management**를 선택합니다.

Object Management 페이지가 나타납니다.

2단계 **PKI** 아래에서 **Internal CAs**를 선택합니다.

3단계 **Generate CA**를 클릭합니다.

Generate Internal Certificate Authority 팝업 창이 나타납니다.

4단계 내부 CA 객체의 **Name**을 입력합니다. 파이프(|) 또는 중괄호({})를 제외한 인쇄 가능한 표준 ASCII 문자를 사용할 수 있습니다.

5단계 3-45 페이지의 표 3-9에 설명된 대로 식별 특성을 입력합니다.

6단계 **Generate CSR**을 클릭합니다.

Generate Internal Certificate Authority 팝업 창이 나타납니다.

7단계 CA에 제출할 CSR을 복사합니다.

8단계 **OK**를 클릭합니다.

CA 객체가 생성됩니다. 이 객체를 사용하려면 먼저 CA에서 발행한 서명된 인증서를 업로드해야 합니다.

CSR에 응답하여 발행된 서명된 인증서를 업로드하려면

액세스: Admin/Access Admin/Network Admin

1단계 **Objects > Object Management**를 선택합니다.

Object Management 페이지가 나타납니다.

2단계 **PKI** 아래에서 **Internal CAs**를 선택합니다.

3단계 CSR을 기다리는 서명되지 않은 인증서가 포함된 CA 객체 옆에 있는 수정 아이콘( )을 클릭합니다.

Edit Internal Certificate Authority 팝업 창이 나타납니다.

4단계 **Install Certificate**를 클릭합니다.

Install Internal Certificate Authority 팝업 창이 나타납니다.

5단계 **Certificate Data** 필드 위에서 **Browse**를 클릭하여 DER 또는 PEM으로 인코딩된 X.509 v3 CA 인증서 파일을 업로드합니다.

6단계 업로드된 파일이 비밀번호로 보호된 경우 **Encrypted, and the password is:** 확인란을 선택하고 비밀번호를 입력합니다.

7단계 **Save**를 클릭합니다.

CA 객체는 서명된 인증서를 포함하며 SSL 규칙에서 참조될 수 있습니다.

CA 인증서 및 개인 키 다운로드

라이센스: 모두

지원되는 디바이스: Series 3

내부 CA 객체의 인증서 및 키 정보를 포함하는 파일을 다운로드하여 CA 인증서 및 페어링된 개인 키를 백업하거나 전송할 수 있습니다.

주의 다운로드한 키 정보는 항상 안전한 장소에 저장하십시오.

시스템은 내부 CA 객체에 저장된 개인 키를 무작위로 생성된 키로 암호화한 후 디스크에 저장합니다. 내부 CA 객체에서 인증서와 개인 키를 다운로드하면 시스템은 인증서 및 개인 키 정보를 포함하는 파일을 생성하기 전에 먼저 해당 정보를 해독합니다. 그런 다음 시스템이 다운로드한 파일을 암호화하는 데 사용할 비밀번호를 제공해야 합니다.

주의 시스템 백업 과정에서 다운로드된 개인 키는 해독된 후 암호화되지 않은 백업 파일에 저장됩니다. 자세한 내용은 70-2페이지의 백업 파일 생성을/를 참조하십시오.

내부 CA 인증서 및 개인 키를 다운로드하려면

액세스: Admin/Access Admin/Network Admin

1단계 **Objects > Object Management**를 선택합니다.

Object Management 페이지가 나타납니다.

2단계 **PKI** 아래에서 **Internal CAs**를 선택합니다.

3단계 인증서 및 개인 키를 다운로드할 내부 CA 객체 옆에 있는 수정 아이콘( )을 클릭합니다.

Edit Internal Certificate Authority 팝업 창이 나타납니다.

4단계 **Download**를 클릭합니다.

Encrypt Download File 팝업 창이 나타납니다.

5단계 **Password** 및 **Confirm Password** 필드에 암호화 비밀번호를 입력합니다.

6단계 **OK**를 클릭합니다.

파일을 저장하라는 프롬프트가 표시됩니다.

신뢰받는 인증 기관 객체 작업

라이센스: 모두

지원되는 디바이스: Series 3

사용자가 구성하는 각 신뢰받는 CA(인증 기관) 객체는 조직 외부의 신뢰받는 CA에 속한 CA 공개 키 인증서를 나타냅니다. 객체는 객체 이름 및 CA 공개 키 인증서로 구성됩니다. 신뢰받는 CA 또는 신뢰 체인에 있는 임의의 CA에서 서명한 인증서로 암호화된 트래픽을 제어하려면 SSL 정책의 외부 CA 객체 및 그룹(3-2페이지의 객체 그룹화 참조)을 사용할 수 있습니다.

신뢰받는 CA 객체를 생성한 후에는 이름을 수정하고 CRL(certificate revocation lists)을 추가할 수 있지만 다른 객체 속성은 수정할 수 없습니다. 객체에 추가할 수 있는 CRL의 수에는 제한이 없습니다. 객체에 업로드한 CRL을 수정하려면 객체를 삭제하고 다시 생성해야 합니다.

사용 중인 신뢰받는 CA 객체는 삭제할 수 없습니다. 또한 SSL 정책에서 사용되는 신뢰받는 CA 객체를 수정하면 관련된 액세스 제어 정책은 out-of-date 상태가 됩니다. 변경 사항을 반영하려면 액세스 제어 정책을 다시 적용해야 합니다.

자세한 내용은 다음 절을 참조하십시오.

- 3-48페이지의 신뢰받는 CA 객체 추가
- 3-49페이지의 신뢰받는 CA 객체에 CRL 추가

신뢰받는 CA 객체 추가

라이센스: 모두

지원되는 디바이스: Series 3

X.509 v3 CA 인증서를 업로드하여 외부 CA 객체를 구성할 수 있습니다. 다음의 지원되는 형식 중 하나로 인코딩된 파일을 업로드할 수 있습니다.

- DER(Distinguished Encoding Rules)
- PEM(Privacy-enhanced Electronic Mail)

파일이 비밀번호로 보호된 경우 해독 비밀번호를 제공해야 합니다. 인증서가 PEM 형식으로 인코딩된 경우 정보를 복사하여 붙여넣을 수도 있습니다.

파일에 적절한 인증서 정보가 포함된 경우에만 CA 인증서를 업로드할 수 있습니다. 시스템은 객체를 저장하기 전에 인증서를 검증합니다.

신뢰받는 CA 인증서를 가져오려면

액세스: Admin/Access Admin/Network Admin

1단계 **Objects > Object Management**를 선택합니다.

Object Management 페이지가 나타납니다.

2단계 **PKI** 아래에서 **Trusted CAs**를 선택합니다.

3단계 **Add Trusted CAs**를 클릭합니다.

Import Trusted Certificate Authority 팝업 창이 나타납니다.

4단계 신뢰받는 CA 객체의 **Name**을 입력합니다. 파이프(|) 또는 중괄호({})를 제외한 인쇄 가능한 표준 ASCII 문자를 사용할 수 있습니다.

5단계 **Certificate Data** 필드 위에서 **Browse**를 클릭하여 DER 또는 PEM으로 인코딩된 X.509 v3 CA 인증서 파일을 업로드합니다.

6단계 파일이 비밀번호로 보호된 경우 **Encrypted, and the password is:** 확인란을 선택하고 비밀번호를 입력합니다.

7단계 **OK**를 클릭합니다.

신뢰받는 CA 객체가 추가됩니다.

신뢰받는 CA 객체에 CRL 추가

라이센스: 모두

지원되는 디바이스: Series 3

CRL을 신뢰받는 CA 객체에 업로드할 수 있습니다. SSL 정책에서 해당 신뢰받는 CA 객체를 참조하는 경우, 세션 암호화 인증서를 발행한 CA가 그 이후 인증서를 폐기했는지 여부에 따라 암호화된 트래픽을 제어할 수 있습니다. 다음의 지원되는 형식 중 하나로 인코딩된 파일을 업로드할 수 있습니다.

- DER(Distinguished Encoding Rules)
- PEM(Privacy-enhanced Electronic Mail)

CRL을 추가한 후에는 폐기된 인증서의 목록을 볼 수 있습니다. 객체에 업로드한 CRL을 수정하려면 객체를 삭제하고 다시 생성해야 합니다.

적절한 CRL을 포함하는 파일만 업로드할 수 있습니다. 신뢰받는 CA 객체에 추가할 수 있는 CRL의 수에는 제한이 없습니다. 그러나 CRL을 업로드할 때마다 또 다른 CRL을 추가하기 전에 객체를 저장해야 합니다.

CRL을 업로드하려면

액세스: Admin/Access Admin/Network Admin

1단계 **Objects > Object Management**를 선택합니다.

Object Management 페이지가 나타납니다.

2단계 **PKI** 아래에서 **Trusted CAs**를 선택합니다.

3단계 신뢰받는 CA 객체 옆에 있는 수정 아이콘( )을 클릭합니다.

Edit Trusted Certificate Authority 팝업 창이 나타납니다.

4단계 DER 또는 PEM으로 인코딩된 CRL 파일을 업로드하려면 **Add CRL**을 클릭합니다.

5단계 **OK**를 클릭합니다.

변경 내용이 저장되었습니다.

외부 인증 기관 객체 작업

라이센스: 모두

지원되는 디바이스: Series 3

사용자가 구성하는 각 외부 인증서 객체는 조직에 속하지 않은 서버 공개 키 인증서를 나타냅니다. 객체는 객체 이름 및 인증서로 구성됩니다. 서버 인증서로 암호화된 트래픽을 제어하려면 SSL 규칙에서 외부 인증서 객체 및 그룹(3-2페이지의 객체 그룹화 참조)을 사용할 수 있습니다. 예를 들어 사용자는 신뢰하는 자체 서명 서버 인증서를 업로드할 수 있지만 신뢰받는 CA 인증서로 확인할 수는 없습니다.

X.509 v3 서버 인증서를 업로드하여 외부 인증서 객체를 구성할 수 있습니다. 다음의 지원되는 형식 중 하나로 파일을 업로드할 수 있습니다.

- DER(Distinguished Encoding Rules)
- PEM(Privacy-enhanced Electronic Mail)

적절한 서버 인증서 정보가 포함된 파일만 업로드할 수 있습니다. 시스템은 객체를 저장하기 전에 파일을 검증합니다. 인증서가 PEM 형식으로 인코딩된 경우 정보를 복사하여 붙여넣을 수도 있습니다.

외부 인증서 객체를 생성한 후에는 이름을 수정할 수 있지만 다른 객체 속성은 수정할 수 없습니다.

사용 중인 외부 인증서 객체는 삭제할 수 없습니다. 또한 SSL 정책에서 사용되는 외부 인증서 객체를 수정하면 관련된 액세스 제어 정책은 out-of-date 상태가 됩니다. 변경 사항을 반영하려면 액세스 제어 정책을 다시 적용해야 합니다.

외부 인증서 객체를 추가하려면

액세스: Admin/Access Admin/Network Admin

1단계 **Objects > Object Management**를 선택합니다.

Object Management 페이지가 나타납니다.

2단계 **PKI** 아래에서 **External Certs**를 선택합니다.

3단계 **Add External Cert**를 클릭합니다.

Add Known External Certificate 팝업 창이 나타납니다.

4단계 외부 인증서 객체의 **Name**을 입력합니다. 파이프(|) 또는 중괄호({})를 제외한 인쇄 가능한 표준 ASCII 문자를 사용할 수 있습니다.

5단계 **Certificate Data** 필드 위에서 **Browse**를 클릭하여 DER 또는 PEM으로 인코딩된 X.509 v3 서버 인증서 파일을 업로드합니다.

6단계 **Save**를 클릭합니다.

내부 CA 객체가 추가됩니다.

내부 인증서 객체 작업

라이센스: 모두

지원되는 디바이스: Series 3

사용자가 구성하는 각 내부 인증서 객체는 조직에 속한 서버 공개 키 인증서를 나타냅니다. 객체는 객체 이름, 공개 키 인증서 및 페어링된 개인 키로 구성됩니다. 알려진 개인 키를 사용하여 조직의 서버 중 하나로 들어오는 트래픽을 해독하려면 SSL 규칙에서 내부 인증서 객체 및 그룹(3-2페이지의 객체 그룹화 참조)을 사용할 수 있습니다.

X.509 v3 RSA 기반 또는 EC 기반 서버 인증서 및 페어링된 개인 키를 업로드하여 내부 인증서 객체를 구성할 수 있습니다. 다음의 지원되는 형식 중 하나로 파일을 업로드할 수 있습니다.

- DER(Distinguished Encoding Rules)
- PEM(Privacy-enhanced Electronic Mail)

파일이 비밀번호로 보호된 경우 해독 비밀번호를 제공해야 합니다. 인증서와 키가 PEM 형식으로 인코딩된 경우 정보를 복사하여 붙여넣을 수도 있습니다.

적절한 인증서 또는 키 정보를 포함하며 상호 페어링된 파일만 업로드할 수 있습니다. 시스템은 객체를 저장하기 전에 페어링을 검증합니다.

내부 인증서 객체를 생성한 후에는 이름을 수정할 수 있지만 다른 객체 속성은 수정할 수 없습니다.

사용 중인 내부 인증서 객체는 삭제할 수 없습니다. 또한 SSL 정책에서 사용되는 내부 인증서 객체를 수정하면 관련된 액세스 제어 정책은 out-of-date 상태가 됩니다. 변경 사항을 반영하려면 액세스 제어 정책을 다시 적용해야 합니다.

내부 인증서 객체를 추가하려면

액세스: Admin/Access Admin/Network Admin

1단계 **Objects > Object Management**를 선택합니다.

Object Management 페이지가 나타납니다.

2단계 **PKI** 아래에서 **Internal Certs**를 선택합니다.

3단계 **Add Internal Cert**를 클릭합니다.

Add Known Internal Certificate 팝업 창이 나타납니다.

4단계 내부 인증서 객체의 **Name**을 입력합니다. 파이프(|) 또는 중괄호({})를 제외한 인쇄 가능한 표준 ASCII 문자를 사용할 수 있습니다.

5단계 **Certificate Data** 필드 위에서 **Browse**를 클릭하여 DER 또는 PEM으로 인코딩된 X.509 v3 서버 인증서 파일을 업로드합니다.

6단계 **Key** 필드 위에서 **Browse**를 클릭하여 DER 또는 PEM으로 인코딩된 페어링된 개인 키 파일을 업로드합니다.

7단계 업로드된 개인 키 파일이 비밀번호로 보호된 경우 **Encrypted, and the password is:** 확인란을 선택하고 비밀번호를 입력합니다.

8단계 **Save**를 클릭합니다.

내부 인증서 객체가 추가됩니다.

지오로케이션 객체 작업

라이센스: FireSIGHT

지원되는 디바이스: Series 3, 가상, ASA FirePOWER

지원되는 Defense Center: DC500을 제외한 모두

사용자가 구성하는 각 지오로케이션 객체는 시스템이 모니터링되는 네트워크에서 트래픽의 소스 또는 목적지로 식별한 하나 이상의 국가 또는 대륙을 나타냅니다. 액세스 제어 정책, SSL 정책, 이벤트 검색 등 시스템 웹 인터페이스의 여러 곳에서 지오로케이션 객체 및 그룹을 사용할 수 있습니다. 예를 들어 특정 국가에서 오가는 트래픽을 차단하는 액세스 제어 규칙을 작성할 수 있습니다. 지리적 위치로 트래픽을 필터링하는 방법에 대한 자세한 내용은 15-3페이지의 네트워크 또는 지리적 위치로 트래픽 제어을/를 참조하십시오. 지리적 위치로 암호화된 트래픽을 필터링하는 방법에 대한 자세한 내용은 22-4페이지의 암호화된 트래픽을 네트워크 또는 지리적 위치로 제어을/를 참조하십시오.

네트워크 트래픽 필터링에 최신 정보를 사용하려면 Cisco에서는 GeoDB(지오로케이션 데이터베이스)를 정기적으로 업데이트할 것을 적극 권장합니다. GeoDB 업데이트 다운로드 및 설치에 대한 자세한 내용은 66-27페이지의 지오로케이션 데이터베이스 업데이트을/를 참조하십시오.

사용 중인 지오로케이션 객체는 삭제할 수 없습니다. 또한 액세스 제어 정책 또는 SSL 정책에 사용된 지오로케이션 객체를 수정한 후 변경 사항을 반영하려면 액세스 제어 정책을 다시 적용해야 합니다.

지오로케이션 객체를 추가하려면

액세스: Admin/Access Admin/Network Admin

1단계 **Objects > Object Management**를 선택합니다.

Object Management 페이지가 나타납니다.

2단계 **Geolocation**을 선택합니다.

Geolocation Objects 페이지가 나타납니다.

3단계 **Add Geolocation**을 클릭합니다.

Geolocation Object 팝업 창이 나타납니다.

4단계 지오로케이션 객체의 **Name**을 입력합니다. 파이프(|) 또는 중괄호({})를 제외한 인쇄 가능한 표준 ASCII 문자를 사용할 수 있습니다.

5단계 지오로케이션 객체에 포함할 국가와 대륙에 대한 확인란을 선택합니다.

대륙을 선택하면 해당 대륙의 모든 국가가 선택되며, GeoDB가 업데이트하는 국가는 향후 해당 대륙 아래에 추가될 수 있습니다. 대륙 아래에서 한 국가의 선택을 취소하면 해당 대륙의 선택이 취소됩니다. 국가와 대륙의 조합을 선택할 수 있습니다.

6단계 **Save**를 클릭합니다.

지오로케이션 객체가 추가됩니다.

디바이스 관리

방어 센터는 FireSIGHT 시스템의 주요 구성 요소입니다. FireSIGHT 시스템를 포함한 전체 디바이스 범위를 관리하고 네트워크에서 탐지하는 위협을 집계, 분석 및 처리하려면 방어 센터를 사용할 수 있습니다.

방어 센터를 사용하여 디바이스를 관리하면 다음을 수행할 수 있습니다.

- 단일 위치에서 모든 디바이스에 대한 정책을 구성하므로 컨피그레이션을 좀 더 쉽게 변경할 수 있습니다.
- 디바이스에 각종 소프트웨어 업데이트를 설치할 수 있습니다.
- 관리되는 디바이스에 상태 정책을 푸시하고 방어 센터에서 상태를 모니터링할 수 있습니다.

방어 센터는 침입 이벤트, 네트워크 검색 정보 및 디바이스 성능 데이터를 집계하고 상호 연결하므로 사용자는 디바이스가 상호 관계에 대해 보고하는 정보를 모니터링하고 네트워크에서 발생하는 전반적인 활동을 평가할 수 있습니다.

자세한 내용은 다음 절을 참조하십시오.

- 4-2페이지의 관리 개념 — 방어 센터로 디바이스를 관리하는 것과 관련된 몇 가지 기능과 제한 사항에 대해 설명합니다.
- 4-3페이지의 관리 인터페이스 이해 — 트래픽 채널과 여러 관리 인터페이스를 사용하여 성능을 높이거나 서로 다른 네트워크의 디바이스 간 트래픽을 격리하는 방법에 대해 설명합니다.
- 4-7페이지의 NAT 환경에서 작업 — Network Address Translation 환경에서 디바이스의 관리를 설정하는 원리에 대해 설명합니다.
- 4-9페이지의 고가용성 구성 — 운영 연속성이 보장되도록 두 방어 센터를 고가용성 쌍으로 설정하는 방법에 대해 설명합니다.
- 4-19페이지의 디바이스 작업 — 디바이스와 방어 센터 간 연결을 설정 및 비활성화하는 방법에 대해 설명합니다. 또한 관리되는 디바이스를 추가 및 삭제하고 상태를 변경하는 방법에 대해서도 설명합니다.
- 4-27페이지의 디바이스 그룹 관리 — 디바이스 그룹을 생성하는 방법 및 그룹에서 디바이스를 추가 및 제거하는 방법에 대해 설명합니다.
- 4-29페이지의 디바이스 클러스터링 — 두 관리되는 디바이스 간에 고가용성을 설정 및 관리하는 방법에 대해 설명합니다.
- 4-49페이지의 디바이스 컨피그레이션 수정 — 수정할 수 있는 디바이스 특성 및 이러한 특성을 수정하는 방법에 대해 설명합니다.
- 4-43페이지의 스태킹된 디바이스 관리 — 관리되는 디바이스의 스택을 생성하는 방법 및 스택에서 디바이스를 제거하는 방법에 대해 설명합니다.
- 4-60페이지의 센싱 인터페이스 구성 — 관리되는 디바이스에서 인터페이스를 구성하는 방법에 대해 설명합니다.

관리 개념

방어 센터를 사용하면 디바이스 동작의 거의 모든 부분을 관리할 수 있습니다. 고가용성 쌍의 일부로 두 번째 방어 센터를 사용할 수는 있지만 하나의 디바이스를 관리하는 데에는 하나의 방어 센터만 필요합니다. 다음 절에서는 FireSIGHT 시스템 구축을 계획할 때 알아야 할 몇 가지 개념에 대해 설명합니다.

방어 센터로 관리할 수 있는 것

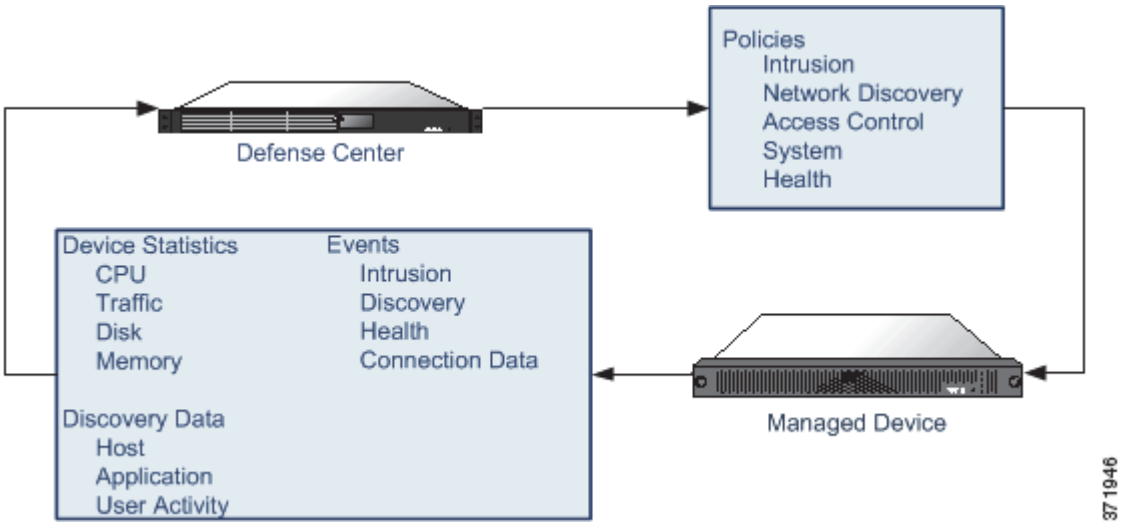
방어 센터를 다음과 같은 디바이스를 관리하기 위한 FireSIGHT 시스템 구축의 중앙 관리 지점으로 사용할 수 있습니다.

- FirePOWER 관리되는 디바이스
- Cisco ASA with FirePOWER Services 디바이스
- 가상 디바이스 같은 소프트웨어 기반 디바이스 및 Cisco NGIPS for Blue Coat X-Series

참고 Cisco에서는 DC500 모델 방어 센터를 사용할 경우 디바이스(소프트웨어 기반 디바이스 포함)를 최대 3개까지만 관리할 것을 권장합니다. DC500 데이터베이스 제한 사항에 대한 자세한 내용은 데이터베이스 이벤트 제한 수 표를 참조하십시오.

디바이스를 관리할 때에는 방어 센터와 디바이스 간에 안전한 SSL 암호화 TCP 터널을 통해 정보가 전송됩니다.

다음 그림에서는 방어 센터 및 해당 관리되는 디바이스 간에 무엇이 전송되는지를 보여줍니다. 어플라이언스 간에 전송되는 이벤트와 정책의 유형은 디바이스 유형을 기반으로 합니다.



정책과 이벤트 너머의 작업

라이센스: 모두

디바이스에 정책을 적용하고 디바이스에서 이벤트를 수신하는 것 외에도 방어 센터에서는 다른 디바이스 관련 작업을 수행할 수 있습니다.

디바이스 백업

관리되는 가상 디바이스, Cisco NGIPS for Blue Coat X-Series 또는 Cisco ASA with FirePOWER Services에 대해서는 백업 파일을 생성하거나 복원할 수 **없습니다**.

디바이스 자체에서 관리되는 물리적 디바이스의 백업을 수행할 경우 디바이스 컨피그레이션**만** 백업됩니다. 컨피그레이션 데이터 및 선택적으로 통합된 파일을 백업하려면 관리하는 방어 센터를 사용하여 디바이스의 백업을 수행할 수 있습니다.

이벤트 데이터를 백업하려면 관리하는 방어 센터의 백업을 수행하십시오. 자세한 내용은 70-2페이지의 백업 파일 생성을/를 참조하십시오.

디바이스 업데이트

때때로 Cisco에서는 다음을 포함하여 FireSIGHT 시스템에 대한 업데이트를 출시합니다.

- 침입 이벤트 업데이트(새로운 침입 규칙과 업데이트된 침입 규칙이 포함될 수 있음)
- 취약성 데이터베이스 업데이트
- 지오로케이션 업데이트
- 소프트웨어 패치 및 업데이트

관리하는 디바이스에 업데이트를 설치하려면 방어 센터를 사용할 수 있습니다.

이중 방어 센터 사용

라이센스: 모두

지원되는 Defense Center: DC1000, DC1500, DC2000, DC3000, DC3500, DC4000

두 개의 방어 센터를 고가용성 쌍으로 설정할 수 있습니다. 이렇게 하면 방어 센터 중 하나가 실패할 경우 이중 기능이 보장됩니다. 두 방어 센터 간에는 정책, 사용자 계정 등이 공유됩니다. 이벤트는 자동으로 두 방어 센터에 전송됩니다. 자세한 내용은 4-9페이지의 고가용성 구성을/를 참조하십시오.

관리 인터페이스 이해

관리 인터페이스는 방어 센터 및 모든 관리 대상 디바이스 간 통신 수단을 제공합니다. 구축에 성공하려면 어플라이언스 간 트래픽 제어를 잘 유지하는 것이 가장 중요합니다.

Series 3 어플라이언스 및 가상 방어 센터에서 방어 센터, 디바이스 또는 둘 모두의 관리 인터페이스를 활성화하여 어플라이언스 간 트래픽을 두 개의 별도 트래픽 채널로 정렬하도록 기본 컨피그레이션을 변경할 수 있습니다. *관리 트래픽 채널*은 모든 내부 트래픽(예: 어플라이언스 및 시스템의 관리와 관련된 디바이스 간 트래픽)을 전달하고, *이벤트 트래픽 채널*은 모든 이벤트 트래픽(예: 웹 이벤트)을 전달합니다. 트래픽을 두 채널로 나누면 어플라이언스 간 두 연결 지점이 생성되어 처리량이 많아지고 그에 따라 성능이 개선됩니다. 또한 각각 고유한 IP 주소(IPv4 또는 IPv6)와 호스트 이름이 있는 *여러 관리 인터페이스*를 활성화하면 트래픽 채널을 분리하여 관리하면서 더 많은 처리량을 제공할 수 있습니다.

여러 관리 인터페이스가 있는 경우 하나의 방어 센터만 사용하여 다른 네트워크에서 트래픽을 격리하고 관리할 수도 있습니다. 관리 인터페이스를 사용하여 고정 경로를 목적지 네트워크에 추가하며, 한 네트워크의 트래픽이 다른 네트워크의 트래픽과 격리되도록 디바이스를 각각 개별 관리 인터페이스에 등록합니다. 동일한 인터페이스에서 두 트래픽 채널을 전송할 수도 있고, 추가 관리 인터페이스가 충분히 있는 경우 네트워크 트래픽을 격리하고 각 관리 인터페이스에서 하나의 트래픽 채널만 전달하도록 구성할 수도 있습니다.

관리 인터페이스는 종종 어플라이언스의 뒷면에 있습니다. 자세한 내용은 *FireSIGHT 시스템 Installation Guide*의 Identifying the Management Interfaces 절을 참조하십시오. 관리 인터페이스에 대한 자세한 내용은 다음 절을 참조하십시오.

- 4-4페이지의 단일 관리 인터페이스 사용
- 4-5페이지의 여러 관리 인터페이스 사용
- 4-5페이지의 트래픽 채널 사용
- 4-7페이지의 네트워크 경로 사용

단일 관리 인터페이스 사용

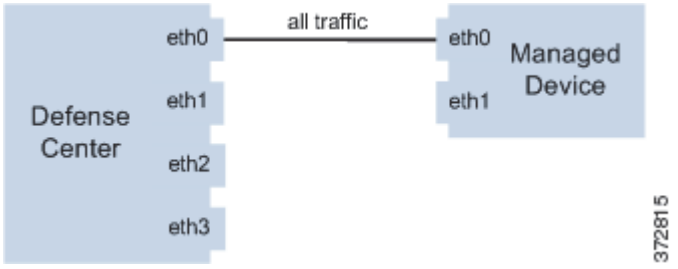
라이센스: 모두

지원되는 디바이스: 모두

지원되는 Defense Center: 모두

디바이스를 방어 센터에 등록하면 방어 센터의 관리 인터페이스와 디바이스의 관리 인터페이스 간 모든 트래픽을 전달하는 단일 통신 채널이 설정됩니다.

다음 그림에서는 기본 단일 통신 채널을 보여줍니다. 한 인터페이스는 관리 및 이벤트 트래픽을 모두 포함하는 한 통신 채널을 전달합니다.



여러 관리 인터페이스 사용

라이센스: 모두

지원되는 디바이스: Series 3

지원되는 Defense Center: Series 3, 가상

각 트래픽 채널을 서로 다른 관리 인터페이스로 전송하여 트래픽 처리량을 늘리려면 각각 고유한 IP 주소(IPv4 또는 IPv6)와 선택적으로 호스트 이름이 있는 여러 관리 인터페이스를 활성화 및 구성할 수 있습니다. 더 가벼운 관리 트래픽 로드를 전달하려면 더 작은 인터페이스를 구성하고, 더 무거운 관리 트래픽 로드를 전달하려면 더 큰 인터페이스를 구성합니다. 디바이스를 별도의 관리 인터페이스에 등록하고 동일한 인터페이스에 대해 두 트래픽 채널을 구성할 수도 있고, 방어 센터에 의해 관리되는 모든 디바이스의 이벤트 트래픽 채널을 전달하는 전용 관리 인터페이스를 사용할 수도 있습니다.

방어 센터의 특정 관리 인터페이스에서 다른 네트워크의 디바이스로 이동하는 경로를 생성할 수도 있습니다. 다른 네트워크의 디바이스를 비기본 관리 인터페이스에 등록하면 해당 디바이스의 트래픽은 기본(`eth0`) 관리 인터페이스에 등록된 디바이스의 트래픽과 격리됩니다. 자세한 내용은 4-7페이지의 네트워크 경로 사용을/를 참조하십시오.

다음을 제외하고, 비기본 관리 인터페이스에는 기본 관리 인터페이스와 동일한 기능(예: 방어 센터 간 고가용성 이용)이 대부분 포함되어 있습니다.

- 기본(`eth0`) 관리 인터페이스에서만 DHCP를 구성할 수 있습니다. 추가(`eth1` 등) 인터페이스에는 고유한 정적 IP 주소와 호스트 이름이 필요합니다.
- 기본이 아닌 관리 인터페이스를 사용하여 방어 센터 및 관리되는 디바이스를 연결하는 경우 해당 어플라이언스가 NAT 디바이스로 분리되어 있으면 두 트래픽 채널을 모두 구성하여 동일한 관리 인터페이스를 사용해야 합니다.
- 기본 관리 인터페이스에서만 Lights-Out 관리를 사용할 수 있습니다.
- 70xx 제품군에서는 트래픽을 두 개의 채널로 구분하고 해당 채널이 트래픽을 방어 센터에 있는 한 개 이상의 관리 인터페이스로 전송하도록 구성할 수 있습니다. 하지만, 70xx 제품군에는 하나의 관리 인터페이스만 포함되어 있기 때문에 디바이스가 하나의 관리 인터페이스에 있는 방어 센터에서 전송된 트래픽만 수신합니다.

트래픽 채널 사용

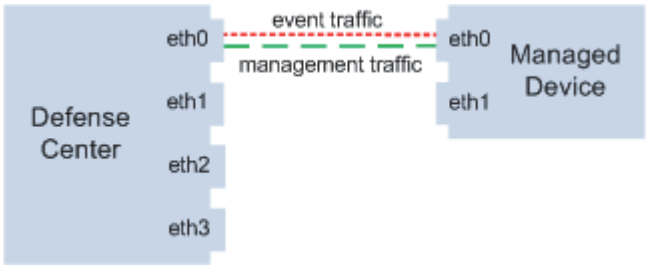
라이센스: 모두

지원되는 디바이스: Series 3

지원되는 Defense Center: Series 3, 가상

하나의 관리 인터페이스에서 두 개의 트래픽 채널을 사용하는 경우 방어 센터와 관리되는 디바이스 간에 두 개의 연결을 생성합니다. 동일한 인터페이스에서 각각 한 채널은 관리 트래픽을 전송하고 다른 채널을 이벤트 트래픽을 전송합니다.

다음 예는 동일한 인터페이스에 두 개의 별도 트래픽 채널이 있는 통신 채널을 보여줍니다.



여러 관리 인터페이스를 사용하는 경우 두 관리 인터페이스로 트래픽 채널을 나누고, 두 인터페이스의 용량을 추가하여 트래픽 플로우를 높임으로써 성능을 개선할 수 있습니다. 한 인터페이스는 관리 트래픽 채널을 전달하고 다른 인터페이스는 이벤트 트래픽 채널을 전달합니다. 둘 중 하나가 실패하면 모든 트래픽이 활성 인터페이스로 다시 라우팅되어 연결이 유지됩니다.

다음 그림에서는 두 개의 관리 인터페이스에서 운영되는 관리 트래픽 채널 및 이벤트 트래픽 채널을 보여줍니다.

여러 디바이스의 이벤트 트래픽만 전달하는 전용 관리 인터페이스를 사용할 수 있습니다. 이 컨피그레이션에서 각 디바이스는 관리 트래픽 채널을 전달하는 서로 다른 관리 인터페이스에 등록되어 있으며, 방어 센터의 한 관리 인터페이스는 모든 디바이스의 모든 이벤트 트래픽 채널을 전달합니다. 한 인터페이스가 실패하면 트래픽이 활성 인터페이스로 다시 라우팅되어 연결이 유지됩니다. 모든 디바이스에 대한 이벤트 트래픽이 동일한 인터페이스에서 전달되므로 네트워크 간 트래픽이 격리되지 않습니다.

다음 그림에서는 이벤트 트래픽 채널에 대해 동일한 전용 인터페이스를 공유하는 서로 다른 관리 채널 트래픽 인터페이스를 사용하는 두 개의 디바이스를 보여줍니다.

하나의 관리 인터페이스에서 두 개의 트래픽 채널을 사용하는 경우 방어 센터와 관리되는 디바이스 간에 두 개의 연결을 생성합니다. 동일한 인터페이스에서 각각 한 채널은 관리 트래픽을 전송하고 다른 채널을 이벤트 트래픽을 전송합니다. 여러 관리 인터페이스를 사용하는 경우 두 관리 인터페이스로 트래픽 채널을 나누고, 두 인터페이스의 용량을 추가하여 트래픽 플로우를 높임으로써 성능을 더욱 개선할 수 있습니다. 한 인터페이스는 관리 트래픽 채널을 전달하고 다른 인터페이스는 이벤트 트래픽 채널을 전달합니다. 둘 중 하나가 실패하면 모든 트래픽이 활성 인터페이스로 다시 라우팅되어 연결이 유지됩니다.

또한 여러 디바이스의 이벤트 트래픽만 전달하는 전용 관리 인터페이스를 사용할 수 있습니다. 이 컨피그레이션에서 각 디바이스는 관리 트래픽 채널을 전달하는 서로 다른 관리 인터페이스에 등록되어 있으며, 방어 센터의 한 관리 인터페이스는 모든 디바이스의 모든 이벤트 트래픽 채널을 전달합니다. 한 인터페이스가 실패하면 트래픽이 활성 인터페이스로 다시 라우팅되어 연결이 유지됩니다. 모든 디바이스에 대한 이벤트 트래픽이 동일한 인터페이스에서 전달되므로 네트워크 간 트래픽이 격리되지 않습니다.

네트워크 경로 사용

라이센스: 모두

지원되는 디바이스: Series 3

지원되는 Defense Center: Series 3, 가상

방어 센터의 특정 관리 인터페이스에서 다른 네트워크로 이동하는 경로를 생성할 수 있습니다. 네트워크의 디바이스를 방어 센터의 지정된 관리 인터페이스에 등록하면 방어 센터 및 다른 네트워크의 디바이스 간에 격리된 연결이 제공됩니다. 두 트래픽 채널이 동일한 관리 인터페이스를 사용하도록 구성하면 해당 디바이스의 트래픽을 다른 네트워크의 디바이스 트래픽과 격리할 수 있습니다. 라우팅된 인터페이스는 방어 센터의 다른 모든 인터페이스와 격리되므로, 라우팅된 관리 인터페이스가 실패하면 연결이 손실됩니다.

팁 Cisco에서는 기본(`eth0`) 관리 인터페이스가 아닌 다른 관리 인터페이스를 사용하여 방어 센터 및 해당 디바이스를 등록할 때 고정 IP 주소를 사용할 것을 권장합니다. DHCP는 기본 관리 인터페이스에서만 지원됩니다.

방어 센터를 설치한 후 웹 인터페이스를 사용하여 복수 관리 인터페이스를 구성합니다. 자세한 내용은 *FireSIGHT 시스템 사용 설명서*의 Configuring Appliance Settings을/를 참조하십시오.

다음 그림에서는 모든 트래픽에 대해 별도의 관리 인터페이스를 사용하여 네트워크 트래픽을 격리하는 두 디바이스를 보여줍니다. 각 디바이스에 대해 별도의 관리 및 이벤트 트래픽 채널 인터페이스를 구성하려면 관리 인터페이스를 더 추가할 수 있습니다.

NAT 환경에서 작업

라이센스: 모두

NAT(Network Address Translation)는 트래픽이 라우터를 통과할 때 소스 또는 목적지 IP 주소를 재할당하는 작업에 관여하는 라우터를 통해 네트워크 트래픽을 보내고 받는 방법입니다. NAT를 사용하는 일반적인 애플리케이션은 사설 네트워크의 여러 호스트가 단일 공용 IP 주소를 사용하여 공용 네트워크에 액세스하도록 합니다.

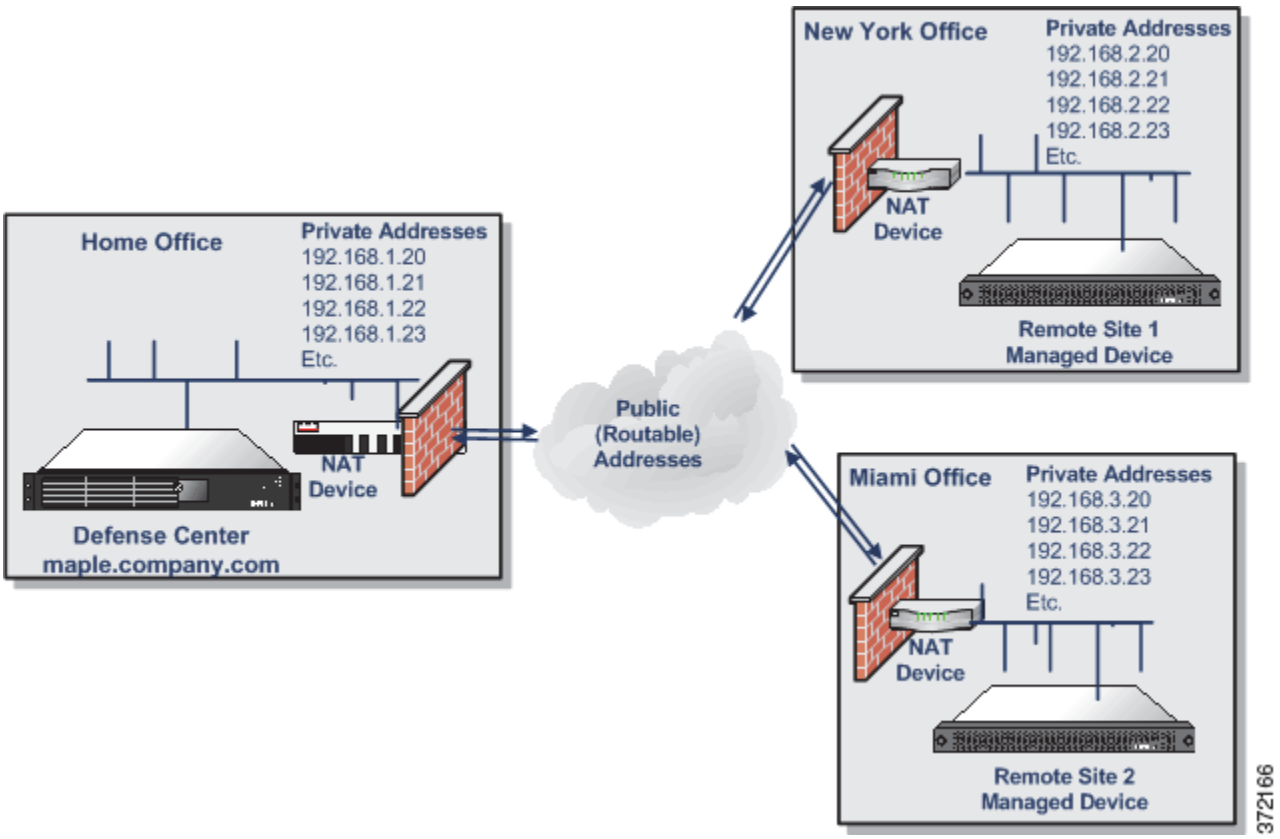
방어 센터에 디바이스를 추가하면 어플라이언스 간 통신이 설정됩니다. 통신을 설정해야 하는 정보는 환경에서 NAT를 사용하는지 여부에 따라 달라집니다.

- NAT가 없는 환경에서는 두 어플라이언스의 등록 키와 IP 주소 또는 정규화된 도메인 이름이 필요합니다.
- NAT가 있는 환경에서는 등록 키 및 고유한 NAT ID가 필요합니다.

참고 NAT ID는 방어 센터에 디바이스를 등록하는 데 사용되는 모든 NAT ID 가운데에서 **반드시** 고유해야 합니다.

비기본 관리 인터페이스를 사용하여 방어 센터와 관리되는 디바이스를 연결하고 그러한 어플라이언스를 NAT 디바이스로 구분하는 경우, 두 트래픽 채널이 동일한 관리 인터페이스를 사용하도록 구성해야 합니다.

다음 다이어그램에서는 NAT 환경에서 두 디바이스를 관리하는 방어 센터를 보여줍니다. 등록 키는 고유할 필요가 없으므로 두 디바이스를 추가할 때 동일한 등록 키를 사용할 수 있습니다. 그러나 방어 센터에 디바이스를 추가할 때는 **고유한** NAT ID를 사용해야 합니다.



고가용성 구성

라이센스: 모두

지원되는 Defense Center: DC1000, DC1500, DC2000, DC3000, DC3500, DC4000

운영의 연속성을 보장하려면 고가용성 기능을 사용하여 디바이스 관리를 위한 이중 방어 센터를 지정할 수 있습니다. 이벤트 데이터는 관리되는 디바이스에서 두 방어 센터로 스트리밍되며 특정 컨피그레이션 요소가 두 방어 센터에서 유지됩니다. 한 방어 센터가 실패하면 다른 방어 센터를 사용하여 중단 없이 네트워크를 모니터링할 수 있습니다.

주의 시스템은 일부 기능을 기본 방어 센터로 제한하므로 해당 어플라이언스가 실패하면 보조 방어 센터를 Active로 승격해야 합니다. 4-15페이지의 고가용성 상태 모니터링 및 변경을/를 참조하십시오.

고가용성 설정에 대한 자세한 내용은 다음 절을 참조하십시오.

- 4-9페이지의 고가용성 사용 — 고가용성을 구현할 때 공유하는 컨피그레이션 및 공유하지 않는 컨피그레이션을 나열합니다.
- 4-13페이지의 고가용성 구현을 위한 지침 — 고가용성을 구현하고자 할 때 따라야 할 지침의 개요를 안내합니다.
- 4-14페이지의 고가용성 설정 — 기본 및 보조 방어 센터를 지정하는 방법에 대해 설명합니다.
- 4-15페이지의 고가용성 상태 모니터링 및 변경 — 연결된 방어 센터의 상태를 확인하는 방법 및 기본 방어 센터가 실패할 때 방어 센터의 역할을 변경하는 방법에 대해 설명합니다.
- 4-17페이지의 고가용성 비활성화 및 디바이스 등록 취소 — 연결된 방어 센터 간에 영구적으로 연결을 제거하는 방법에 대해 설명합니다.
- 4-18페이지의 쌍을 이룬 방어 센터 간에 통신 일시 중지 — 연결된 방어 센터 간에 통신을 일시 중지하는 방법에 대해 설명합니다.
- 4-18페이지의 쌍을 이룬 방어 센터 간에 통신 다시 시작 — 연결된 방어 센터 간에 통신을 다시 시작하는 방법에 대해 설명합니다.

고가용성 사용

라이센스: 모두

지원되는 Defense Center: DC1000, DC1500, DC2000, DC3000, DC3500, DC4000

DC1500, DC2000, DC3500 및 DC4000은 고가용성 컨피그레이션을 지원하고, DC750 및 가상 방어 센터는 지원하지 않습니다. Cisco에서는 고가용성 쌍의 두 방어 센터를 동일한 모델로 사용할 것을 **적극** 권장합니다. 서로 다른 방어 센터 모델 간에는 고가용성 설정을 시도하지 **마십시오**.

고가용성 모드의 방어 센터는 *기본* 및 *보조*로 지정되므로 둘 중 한 방어 센터에 대해 정책이나 기타 변경 사항을 적용할 수 있습니다. 그러나 Cisco에서는 기본 방어 센터**에서만** 컨피그레이션을 변경하고 보조 방어 센터는 백업으로 유지할 것을 권장합니다.

방어 센터는 컨피그레이션 변경 사항을 주기적으로 상호 업데이트하며, 한 방어 센터에 대한 변경 사항은 10분 내에 다른 방어 센터에 적용됩니다. 각 방어 센터에는 5분의 동기화 주기가 있지만 주기 자체에는 최대 5분의 동기화 간격이 있을 수 있으므로, 두 번의 5분 주기 내에 변경 사항이 나타납니다. 이 10분 동안에는 두 방어 센터에서 컨피그레이션이 다르게 나타날 수 있습니다.

예를 들어 기본 방어 센터에서 정책을 생성하고 역시 보조 방어 센터에 의해 관리되는 디바이스에 적용하는 경우, 해당 디바이스는 방어 센터가 서로 연결하기 전에 보조 방어 센터에 연결할 수 있습니다. 이 디바이스에는 보조 방어 센터에서 인식할 수 없는 정책이 적용되어 있으므로, 두 방어 센터가 동기화될 때까지 보조 방어 센터는 새 정책을 "unknown"으로 표시하게 됩니다.

또한 방어 센터 동기화 사이에 동일한 기간 내에 충돌하는 정책 또는 기타 변경 사항을 두 방어 센터에 적용하면, 방어 센터의 기본 및 보조 지정과 상관없이 마지막으로 변경한 내용이 적용됩니다.

고가용성 쌍을 설정하기 전에 다음 전제 조건에 유의하십시오.

- 두 방어 센터에 모두 `admin`이라는 이름의 사용자 계정과 Administrator 권한이 있는지 확인합니다. 두 계정의 비밀번호는 동일해야 합니다.
- `admin` 계정 외에는 두 방어 센터에 동일한 사용자 이름의 사용자 계정이 없어야 합니다. 고가용성을 설정하기 전에 중복된 사용자 계정 중 하나를 제거하거나 이름을 변경하십시오.

고가용성 쌍으로 구성된 방어 센터는 신뢰할 수 있는 동일한 관리 네트워크에 있어야 할 필요가 없으며, 동일한 지오로케이션 위치에 있어야 할 필요도 없습니다.

운영 연속성을 보장하려면 고가용성 페어의 두 방어 센터에 인터넷 액세스가 있어야 합니다. E-1페이지의 인터넷 액세스 요구 사항을/를 참조하십시오. 특정 기능의 경우 기본 방어 센터에서 인터넷에 접속한 다음 동기화 프로세스 중 보조 방어 센터와 정보를 공유합니다. 기본 방어 센터에 장애가 발생할 경우 4-15페이지의 고가용성 상태 모니터링 및 변경에 설명된 대로 보조 방어 센터를 활성으로 승격합니다.

고가용성 쌍의 멤버 간에 어떤 컨피그레이션을 공유하거나 공유하지 않을지에 대한 자세한 내용은 다음을 참조하십시오.

- 4-10페이지의 공유 컨피그레이션
- 4-11페이지의 상태 및 시스템 정책
- 4-12페이지의 상관관계 응답
- 4-12페이지의 라이센스
- 4-12페이지의 URL 필터링 및 보안 인텔리전스
- 4-13페이지의 클라우드 연결 및 악성코드 정보
- 4-13페이지의 사용자 에이전트

공유 컨피그레이션

라이센스: 모두

지원되는 Defense Center: DC1000, DC1500, DC2000, DC3000, DC3500, DC4000

고가용성 쌍의 방어 센터에서는 다음 정보를 공유합니다.

- 사용자 계정 특성, 인증 컨피그레이션 및 사용자 지정 사용자 역할
- 사용자 계정 및 사용자 인식에 대한 인증 개체, 액세스 제어 규칙의 사용자 상태에서 사용 가능한 사용자 및 그룹
- 사용자 지정 대시보드
- 사용자 지정 워크플로 및 테이블
- 디바이스 속성(예: 디바이스의 호스트 이름, 디바이스에서 생성한 이벤트가 저장되는 위치, 디바이스가 상주하는 그룹)
- 액세스 제어, SSL, 네트워크 분석, 침입, 파일 및 네트워크 검색 정책
- 로컬 침입 규칙

- 사용자 지정 침입 규칙 분류
- 네트워크 검색 정책
- 사용자 정의 애플리케이션 프로토콜 탐지기 및 탐지되는 애플리케이션
- 활성화된 사용자 지정 핑거프린트
- 호스트 특성
- 네트워크 검색 사용자 피드백(예: 참고 사항 및 호스트 중요도, 네트워크 맵에서 호스트/애플리케이션/네트워크 삭제, 취약성 비활성화 또는 수정)
- 상관관계 정책 및 규칙, 규정 준수 화이트리스트, 트래픽 프로필
- 조정 스냅샷 및 보고 설정 변경
- 침입 규칙, GeoDB(지오로케이션 데이터베이스), VDB(취약성 데이터베이스) 업데이트
- 위 컨피그레이션과 관련된 재사용 가능한 객체(변수 집합 포함)

상태 및 시스템 정책

라이센스: 모두

지원되는 Defense Center: DC1000, DC1500, DC2000, DC3000, DC3500, DC4000

고가용성 쌍에서는 방어 센터 및 관리되는 디바이스에 대한 상태 및 시스템 정책이 공유됩니다. 충분한 시간을 가지고 상태 정책, 모듈, 블랙리스트에 대한 정보가 새로 활성화된 방어 센터에서 동기화되는지를 확인해야 합니다.

참고 시스템 정책은 고가용성 쌍의 방어 센터에서 공유되지만 자동으로 적용되지는 않습니다. 두 방어 센터에서 동일한 시스템 정책을 사용하려면 동기화 이후 정책을 적용하십시오.

고가용성 쌍의 방어 센터에서는 다음의 시스템 및 상태 정책 정보를 공유합니다.

- 시스템 정책
- 시스템 정책 컨피그레이션(어떤 정책이 어디에 적용되는지)
- 상태 정책
- 상태 모니터링 컨피그레이션(어떤 정책이 어디에 적용되는지)
- 어떤 어플라이언스가 상태 모니터링에서 블랙리스트에 추가되는지
- 어떤 어플라이언스가 블랙리스트에 추가된 개별 상태 모니터링 정책을 가지고 있는지

상관관계 응답

라이센스: 모두

지원되는 Defense Center: DC1000, DC1500, DC2000, DC3000, DC3500, DC4000

상관관계 정책, 규칙 및 응답은 방어 센터 간에 공유되지만, 상관관계 규칙과 응답 간의 *연결*은 방어 센터 간에 공유되지 않습니다. 이는 상관관계 정책 위반이 발생할 경우 중복 응답이 실행되지 않도록 하기 위한 것입니다.

교정을 이용하여 상관관계 정책을 연결할 수 있으려면 먼저 사용자 지정 교정 모듈을 업로드 및 설치하고 보조 방어 센터에서 교정 인스턴스를 구성해야 합니다. 기본 방어 센터가 실패하면 보조 방어 센터에서 상관관계 정책을 적절한 응답 및 교정과 신속하게 연결해야 하는 것은 물론, 운영 연속성을 유지하기 위해 보조 방어 센터의 웹 인터페이스를 사용하여 자체 상태를 Active로 승격해야 합니다. 자세한 내용은 4-15페이지의 고가용성 상태 모니터링 및 변경을/를 참조하십시오. 상관관계 응답에 대한 자세한 내용은 51-45페이지의 상관관계 정책 생성 및 54-1페이지의 교정 생성을/를 참조하십시오.

실패 후 기본 방어 센터를 복원할 때, 보조 방어 센터에서 규칙 또는 화이트리스트와 해당 응답 및 교정 간에 연결을 생성한 경우 응답 및 교정이 기본 방어 센터에서만 생성되도록 연결을 제거해야 합니다.

라이센스

라이센스: 모두

지원되는 Defense Center: DC1000, DC1500, DC2000, DC3000, DC3500, DC4000

고가용성 쌍의 방어 센터에서는 라이센스를 공유하지 **않습니다**. 쌍의 각 멤버에 동등한 라이센스를 추가해야 합니다. 자세한 내용은 65-1페이지의 라이센싱 이해을/를 참조하십시오.

URL 필터링 및 보안 인텔리전스

라이센스: URL 필터링 또는 보호

지원되는 디바이스: Series 3, 가상, X-Series, ASA FirePOWER

지원되는 Defense Center: DC1000, DC1500, DC2000, DC3000, DC3500, DC4000

URL 필터링과 보안 인텔리전스의 컨피그레이션 및 정보는 고가용성 구축에서 방어 센터 간에 동기화됩니다. 그러나 기본 방어 센터만 URL 카테고리 및 평판 데이터 그리고 보안 인텔리전스 피드에 대한 업데이트를 다운로드합니다.

기본 방어 센터가 실패하면, 보조 방어 센터가 URL 필터링 클라우드 및 모든 구성된 피드 사이트에 액세스할 수 있는지 확인하는 것은 물론 보조 방어 센터의 웹 인터페이스를 사용하여 자체 상태를 Active로 승격해야 합니다. 자세한 내용은 4-15페이지의 고가용성 상태 모니터링 및 변경을/를 참조하십시오.

클라우드 연결 및 악성코드 정보

라이센스: 모두 또는 악성코드

지원되는 디바이스: Series 2 또는 X-Series를 제외한 모두

지원되는 Defense Center: DC1000, DC1500, DC2000, DC3000, DC3500, DC4000

이들은 파일 정책 및 관련 컨피그레이션을 공유하지만 고가용성 쌍의 방어 센터는 종합 보안 인텔리전스 클라우드 연결과 악성코드 성향을 공유하지 않습니다. 운영 연속성을 보장하고, 탐지된 파일의 악성코드 속성을 두 방어 센터에서 동일하게 유지하려면 기본 및 보조 방어 센터에 클라우드에 대한 액세스 권한이 모두 있어야 합니다. 자세한 내용은 37-2페이지의 악성코드 차단 및 파일 제어 이해을/를 참조하십시오.

사용자 에이전트

라이센스: FireSIGHT

지원되는 Defense Center: DC1000, DC1500, DC2000, DC3000, DC3500, DC4000

User Agents는 동시에 최대 다섯 개의 방어 센터에 연결할 수 있습니다. 에이전트를 기본 방어 센터에 연결해야 합니다. 기본 방어 센터가 실패하면 에이전트가 보조 방어 센터와 통신할 수 있도록 해야 합니다. 자세한 내용은 17-9페이지의 User Agents를 사용하여 Active Directory 로그인 보고을/를 참조하십시오.

고가용성 구현을 위한 지침

라이센스: 모두

지원되는 Defense Center: DC1000, DC1500, DC2000, DC3000, DC3500, DC4000

고가용성을 활용하려면 다음 절의 지침을 따라야 합니다.

기본 및 보조 방어 센터 요구 사항

한 방어 센터는 기본 방어 센터로, 다른 것은 보조로 지정해야 합니다. 어플라이언스가 Active에서 Inactive로(그리고 그 반대로) 전환될 때 원래 기본 및 보조 지정은 그대로 유지됩니다.

기본 및 보조 지정과 상관없이, 고가용성을 설정하기 전에 두 방어 센터를 정책, 규칙, 관리되는 디바이스 등으로 구성할 수 있습니다.

혼동을 피하려면 보조 방어 센터를 원래 상태에서 시작하십시오. 즉, 정책을 생성하거나 수정하지 않고, 새 규칙을 생성하지 않고, 전에 다른 디바이스를 관리하지 않은 상태를 말합니다. 보조 방어 센터를 원래 상태로 만들려면 공장 기본 설정으로 복원하십시오. 이렇게 하면 방어 센터에서 이벤트 및 컨피그레이션 데이터가 삭제됩니다. 자세한 내용은 *FireSIGHT 시스템 설치 가이드*을/를 참조하십시오.

버전 요구 사항

두 방어 센터에서 동일한 소프트웨어 및 규칙 업데이트 버전을 실행해야 합니다. 또한 이 소프트웨어 버전은 관리되는 디바이스의 소프트웨어 버전과 같거나 더 새 버전이어야 합니다.

통신 요구 사항

기본적으로, 쌍을 이룬 방어 센터는 통신에 포트 8305/tcp를 사용합니다. 4-22페이지의 관리 포트 변경에 설명된 대로 포트를 변경할 수 있습니다.

두 방어 센터는 동일한 네트워크 세그먼트에 있어야 할 필요가 없지만, 각 방어 센터는 상호 간에 그리고 공유하는 디바이스와 통신할 수 있어야 합니다. 즉, 기본 방어 센터는 보조 방어 센터의 자체 관리 인터페이스에 있는 IP 주소에서 보조 방어 센터에 연결할 수 있어야 하고, 그 반대도 가능해야 합니다. 또한 방어 센터는 관리하는 디바이스에 연결할 수 있어야 하고, 디바이스는 방어 센터에 연결할 수 있어야 합니다.

고가용성 설정

라이센스: 모두

지원되는 Defense Center: DC1000, DC1500, DC2000, DC3000, DC3500, DC4000

고가용성을 사용하려면 한 방어 센터는 기본으로, 동일한 모델의 다른 방어 센터는 보조로 지정해야 합니다. 두 어플라이언스 간 원격 관리 통신을 수정하는 방법에 대한 자세한 내용은 4-22페이지의 원격 관리 수정을/를 참조하십시오.

주의 Cisco에서는 기본 방어 센터**에서만** 컨피그레이션을 변경하고 보조 방어 센터는 백업으로 유지할 것을 권장합니다.

고가용성을 구성하기 전에, 연결할 방어 센터 사이에 시간 설정을 동기화해야 합니다. 시간 설정에 대한 자세한 내용은 63-26페이지의 시간 동기화을/를 참조하십시오.

정책 및 정책에 포함된 사용자 지정 표준 텍스트 규칙의 수에 따라, 모든 규칙과 정책이 두 방어 센터에 나타나기까지 최대 10분이 걸릴 수 있습니다. 두 방어 센터 간 링크 상태를 확인하려면 High Availability 페이지를 볼 수 있습니다. 프로세스가 언제 완료되는지 알아보려면 Task Status를 모니터링할 수도 있습니다. 4-15페이지의 고가용성 상태 모니터링 및 변경을/를 참조하십시오.

고가용성 쌍의 방어 센터 중 하나에 이미지를 다시 적용해야 하는 경우 먼저 고가용성 링크를 비활성화하십시오. 방어 센터에 이미지를 다시 적용한 후 고가용성 쌍을 다시 설정하면 기존의 방어 센터에서 새로 추가한 방어 센터로 데이터가 동기화됩니다. 어플라이언스 실패 등의 이유로 방어 센터에 이미지를 다시 적용할 수 없는 경우 고객 지원에 문의하십시오.

두 방어 센터에 대한 고가용성을 설정하려면

액세스: 관리자

1단계 보조 방어 센터로 지정하려는 방어 센터에 로그인합니다.

2단계 **System > Local > Registration**을 선택합니다.

Registration 페이지가 나타납니다.

3단계 **High Availability**를 클릭합니다.

High Availability 페이지가 나타납니다.

4단계 **Secondary 방어 센터** 옵션을 클릭합니다.

Secondary 방어 센터 Setup 페이지가 나타납니다.

5단계 기본 방어 센터의 호스트 이름 또는 IP 주소를 **Primary DC Host** 텍스트 상자에 입력합니다.

주의 네트워크에서 DHCP를 사용하여 IP 주소를 할당하는 경우 IP 주소보다는 호스트 이름을 사용하십시오.

관리 호스트에 라우팅 가능한 주소가 없는 경우 **Primary DC Host** 필드를 비워둘 수 있습니다. 이 경우 **Registration Key** 및 **Unique NAT ID** 필드를 모두 사용하십시오.

6단계 1회용 등록 키를 **Registration Key** 텍스트 상자에 입력합니다.

7단계 선택적으로, 기본 방어 센터를 식별하는 데 사용할 고유한 영숫자 등록 ID를 **Unique NAT ID** 필드에 입력합니다. 자세한 내용은 4-7페이지의 NAT 환경에서 작업을/를 참조하십시오.

8단계 **Register**를 클릭합니다.

성공 메시지가 나타나고, Peer Manager 페이지가 나타나 보조 방어 센터의 현재 상태를 보여줍니다.

9단계 Admin 액세스 권한이 있는 계정을 사용하여, 기본으로 지정할 방어 센터에 로그인합니다.

10단계 **System > Local > Registration**을 선택합니다.

Registration 페이지가 나타납니다.

11단계 **High Availability**를 클릭합니다.

High Availability 페이지가 나타납니다.

12단계 **Primary 방어 센터** 옵션을 클릭합니다.

Primary 방어 센터 Setup 페이지가 나타납니다.

13단계 보조 방어 센터의 호스트 이름 또는 IP 주소를 **Secondary DC Host** 텍스트 상자에 입력합니다.

주의 네트워크에서 DHCP를 사용하여 IP 주소를 할당하는 경우 IP 주소보다는 호스트 이름을 사용하십시오.

14단계 6단계에서 사용한 것과 동일한 1회용 등록 키를 **Registration Key** 텍스트 상자에 입력합니다.

15단계 보조 방어 센터에서 고유한 NAT ID를 사용한 경우, 7단계에서 사용한 것과 동일한 등록 ID를 **Unique NAT ID** 텍스트 상자에 입력합니다.

16단계 **Register**를 클릭합니다.

성공 메시지가 나타나고, Peer Manager 페이지가 나타나 기본 방어 센터의 현재 상태를 보여줍니다.

고가용성 상태 모니터링 및 변경

라이센스: 모두

지원되는 Defense Center: DC1000, DC1500, DC2000, DC3000, DC3500, DC4000

기본 및 보조 Defense Center를 식별한 후, 고가용성 쌍의 한 어플라이언스에서 다음과 같이 로컬 Defense Center 및 해당 피어에 대한 정보를 볼 수 있습니다.

- 피어 IP 주소 또는 호스트 이름
- 피어 제품 모델
- 피어 소프트웨어 버전

- 피어 운영 체제
- 고가용성 쌍의 멤버를 마지막으로 동기화한 이후의 기간
- 로컬 어플라이언스의 역할 및 상태(Active & Primary, Inactive & Primary, Inactive & Secondary 또는 Active & Secondary)

또한 기본 방어 센터가 실패하는 경우 방어 센터의 역할을 변경하기 위해 High Availability 페이지를 사용할 수도 있습니다. 시스템은 다음 기능을 기본 방어 센터로 제한하므로 해당 어플라이언스가 실패하면 보조 방어 센터를 Active로 승격해야 합니다.

- URL 카테고리 및 평판 데이터에 대한 업데이트. 자세한 내용은 4-12페이지의 URL 필터링 및 보안 인텔리전스 참조.
- 보안 인텔리전스 피드에 대한 업데이트. 자세한 내용은 4-12페이지의 URL 필터링 및 보안 인텔리전스 참조.
- 상관관계 규칙 및 응답 간 연결. 자세한 내용은 4-12페이지의 상관관계 응답 참조.

고가용성 상태를 확인하려면

액세스: 관리자

1단계 고가용성을 사용하여 연결한 방어 센터 중 하나에 로그인합니다.

2단계 **System > Local > Registration**을 선택합니다.

Registration 페이지가 나타납니다.

3단계 **High Availability**를 클릭합니다.

High Availability 페이지가 나타납니다.

4단계 **High Availability Status**에서 고가용성 쌍의 방어 센터에 대한 다음과 같은 정보를 볼 수 있습니다.

- 피어 IP 주소 또는 호스트 이름
- 피어 제품 모델
- 피어 소프트웨어 버전
- 피어 운영 체제
- 고가용성 쌍의 멤버를 마지막으로 동기화한 이후의 기간
- 로컬 어플라이언스의 역할 및 상태(Active & Primary, Inactive & Primary, Inactive & Secondary 또는 Active & Secondary)
- 두 Defense Center 간 역할을 전환하기 위한 옵션

5단계 공유 기능에 영향을 주는 작업 후 10분 내에 두 방어 센터가 자동으로 동기화됩니다(각 방어 센터에 5분씩). 예를 들어 한 방어 센터에서 새 정책을 생성하면 5분 내에 다른 방어 센터와 자동으로 공유됩니다. 그러나 정책을 즉시 동기화하려면 **Synchronize**를 클릭합니다.

참고 고가용성 쌍에 구성된 방어 센터에서 디바이스를 삭제하고 다시 추가하려는 경우 Cisco에서는 디바이스를 다시 추가하기 전에 최소 5분 정도 기다릴 것을 권장합니다. 이 정도면 고가용성 쌍이 먼저 다시 동기화될 수 있는 시간입니다. 5분을 기다리지 않는 경우, 두 방어 센터에 디바이스를 추가하는 데 두 번 이상의 동기화 주기가 걸릴 수 있습니다.

6단계 Active에서 Inactive로 또는 Inactive에서 Active로 로컬 역할을 변경하려면 **Switch Roles**를 클릭합니다.

그러면 Primary 또는 Secondary 지정은 변경되지 않은 채 두 피어 간 역할이 전환됩니다.

7단계 툴바에서 **Peer Manager**를 클릭합니다.

Peer Manager 페이지가 나타납니다.

다음 정보를 볼 수 있습니다.

- 고가용성 쌍에서 다른 방어 센터의 IP 주소
- 통신 링크의 상태(registered 또는 unregistered)
- 고가용성 쌍의 상태(enabled 또는 disabled)

두 어플라이언스 간 원격 관리 통신을 수정하는 방법에 대한 자세한 내용은 4-22페이지의 원격 관리 수정을/를 참조하십시오.

고가용성 비활성화 및 디바이스 등록 취소

라이센스: 모두

지원되는 Defense Center: DC1000, DC1500, DC2000, DC3000, DC3500, DC4000

고가용성 쌍에서 방어 센터 중 하나를 제거하려면 먼저 둘 사이의 고가용성 링크를 비활성화해야 합니다.

고가용성 쌍을 비활성화하려면

액세스: 관리자

1단계 고가용성 쌍의 방어 센터 중 하나에 로그인합니다.

2단계 **System > Local > Registration**을 선택합니다.

Registration 페이지가 나타납니다.

3단계 **High Availability**를 클릭합니다.

High Availability 페이지가 나타납니다.

4단계 **Handle Registered Devices** 드롭다운 목록에서 다음 옵션 중 하나를 선택합니다.

- 이 페이지에 액세스하는 방어 센터에서 모든 관리되는 디바이스를 제어하려면 **Unregister devices on the other peer**를 선택합니다.
- 다른 방어 센터에서 모든 관리되는 디바이스를 제어하려면 **Unregister devices on this peer**를 선택합니다.
- 디바이스 관리를 완전히 중지하려면 **Unregister devices on both peers**를 선택합니다.

5단계 **Break High Availability**를 클릭합니다.

Do you really want to Break High Availability? 프롬프트에서 **OK**를 클릭하면 고가용성이 비활성화되고, 선택 사항에 따라 방어 센터에서 관리되는 디바이스가 삭제됩니다.

4-14페이지의 고가용성 설정에 설명된 대로 다른 방어 센터로 고가용성을 활성화할 수 있습니다.

쌍을 이룬 방어 센터 간에 통신 일시 중지

라이센스: 모두

지원되는 Defense Center: DC1000, DC1500, DC2000, DC3000, DC3500, DC4000

일시적으로 고가용성을 비활성화하려면 방어 센터 간 통신 채널을 비활성화할 수 있습니다.

고가용성 쌍에 대한 통신 채널을 비활성화하려면

액세스: 관리자

1단계 **Peer Manager**를 클릭합니다.

Peer Manager 페이지가 나타납니다.

2단계 두 방어 센터 간 통신 채널을 비활성화하려면 슬라이더를 클릭합니다.

두 어플라이언스 간 원격 관리 통신을 수정하는 방법에 대한 자세한 내용은 4-22페이지의 원격 관리 수정을/를 참조하십시오.

쌍을 이룬 방어 센터 간에 통신 다시 시작

라이센스: 모두

지원되는 Defense Center: DC1000, DC1500, DC2000, DC3000, DC3500, DC4000

일시적으로 고가용성을 비활성화한 경우 방어 센터 간 통신 채널을 활성화하여 고가용성을 다시 시작할 수 있습니다.

고가용성 쌍에 대한 통신 채널을 활성화하려면

액세스: 관리자

1단계 **Peer Manager**를 클릭합니다.

Peer Manager 페이지가 나타납니다.

2단계 두 방어 센터 간 통신 채널을 활성화하려면 슬라이더를 클릭합니다.

두 어플라이언스 간 원격 관리 통신을 수정하는 방법에 대한 자세한 내용은 4-22페이지의 원격 관리 수정을/를 참조하십시오.

디바이스 작업

라이센스: 모두

방어 센터를 사용하면 FireSIGHT 시스템의 일부인 전체 디바이스 범위를 관리할 수 있습니다. 디바이스를 관리할 때에는 방어 센터와 디바이스 간에 양방향 SSL 암호화 통신 채널을 설정합니다. 방어 센터는 이 채널을 사용하여 네트워크 트래픽을 분석하고 관리하고자 하는 방법에 대한 정보를 디바이스로 전송합니다.

디바이스는 트래픽을 평가할 때 이벤트를 생성하고 동일한 채널을 사용하여 방어 센터로 전송합니다.

디바이스 관리에 대한 자세한 내용은 다음 절을 참조하십시오.

- 4-19페이지의 Device Management 페이지 이해
- 4-20페이지의 원격 관리 구성
- 4-23페이지의 방어 센터에 디바이스 추가
- 4-20페이지의 원격 관리 구성
- 4-27페이지의 디바이스 그룹 관리
- 4-29페이지의 디바이스 클러스터링
- 4-49페이지의 디바이스 컨피그레이션 수정
- 4-60페이지의 센싱 인터페이스 구성

Device Management 페이지 이해

라이센스: 모두

Device Management 페이지에서는 등록된 디바이스, 디바이스 클러스터 및 디바이스 그룹을 관리하는 데 사용할 수 있는 다양한 정보와 옵션을 제공합니다. 현재 방어 센터에 등록된 모든 디바이스의 목록이 페이지에 표시됩니다.

필요에 따라 어플라이언스 목록을 정렬하려면 **sort-by** 드롭다운 목록을 사용할 수 있습니다. 디바이스는 선택한 카테고리별로 그룹화되어 어플라이언스 목록에 나타납니다. 다음을 기준으로 정렬할 수 있습니다.

- 그룹(디바이스 그룹). 자세한 내용은 4-27페이지의 디바이스 그룹 관리 참조.
- 유형(디바이스에 적용된 라이센스의 유형). 자세한 내용은 65-1페이지의 FireSIGHT 시스템 라이센싱 참조.
- 모델(방어 센터에 의해 관리되는 디바이스의 모델)
- 상태 정책. 자세한 내용은 68-1페이지의 상태 모니터링 사용 참조.
- 시스템 정책. 자세한 내용은 63-1페이지의 시스템 정책 관리 참조.
- 액세스 제어 정책. 자세한 내용은 12-10페이지의 액세스 제어 정책 관리 참조.

디바이스 그룹의 경우, 그룹에 있는 디바이스의 목록을 확장 및 축소할 수 있습니다. 목록은 기본적으로 축소되어 나타납니다.

어플라이언스 목록에 대한 자세한 내용은 다음 표를 참조하십시오.

표 4-1 어플라이언스 목록 필드

필드	설명
이름	각 디바이스의 호스트 이름, IP 주소, 디바이스 모델 및 소프트웨어 버전의 목록. 어플라이언스의 왼쪽에 있는 상태 아이콘은 현재 상태를 나타냅니다.
라이센스 유형	관리되는 디바이스에서 활성화된 라이센스.
상태 정책	디바이스에 대해 현재 적용된 상태 정책. 정책의 읽기 전용 버전을 보려면 상태 정책의 이름을 클릭할 수 있습니다. 기존 상태 정책 수정에 대한 자세한 내용은 68-30페이지의 상태 정책 수정을/를 참조하십시오.
시스템 정책	디바이스에 대해 현재 적용된 시스템 정책. 정책의 읽기 전용 버전을 보려면 시스템 정책의 이름을 클릭할 수 있습니다. 자세한 내용은 63-1페이지의 시스템 정책 관리을/를 참조하십시오.
액세스 제어 정책	현재 적용된 액세스 제어 정책에 대한 링크. 12-10페이지의 액세스 제어 정책 관리을/를 참조하십시오.

자세한 내용은 다음 절을 참조하십시오.

- 4-20페이지의 원격 관리 구성
- 4-23페이지의 방어 센터에 디바이스 추가
- 4-27페이지의 디바이스 그룹 관리
- 4-29페이지의 디바이스 클러스터링
- 4-43페이지의 스태킹된 디바이스 관리

원격 관리 구성

라이센스: 모두

한 FireSIGHT 시스템 어플라이언스를 다른 어플라이언스로 관리하려면 두 어플라이언스 사이에 양방향 SSL 암호화 통신 채널을 설정해야 합니다. 어플라이언스에서는 채널을 사용하여 컨피그레이션 및 이벤트 정보를 공유합니다. 고가용성 피어도 채널을 사용하며, 기본 포트는 8305/tcp입니다.

관리될 어플라이언스, 즉 방어 센터로 관리할 디바이스에서 원격 관리를 구성해야 합니다. 원격 관리를 구성했으면, 관리하는 어플라이언스의 웹 인터페이스를 사용하여 관리되는 어플라이언스를 구축에 추가할 수 있습니다.

이 절의 절차에서는 물리적 FirePOWER 어플라이언스에서 원격 관리를 구성하는 방법에 대해 설명합니다.

두 어플라이언스 간 통신을 활성화하려면 어플라이언스가 서로를 인식할 방법을 제공해야 합니다. 통신을 허용할 때 FireSIGHT 시스템에서 사용하는 세 가지 기준이 있습니다.

- 통신을 설정하려는 어플라이언스의 호스트 이름 또는 IP 주소

  NAT 환경에서는 다른 어플라이언스에 라우팅 가능한 주소가 없어도, 원격 관리를 구성할 때 또는 관리되는 어플라이언스를 추가할 때 호스트 이름이나 IP 주소를 제공해야 합니다.
- 연결을 식별하는, 자체 생성되는 최대 37자 길이의 영숫자 등록 키
- NAT 환경에서 FireSIGHT 시스템이 통신을 설정하도록 지원할 수 있는 선택적인 고유한 영숫자 NAT ID

NAT ID는 관리되는 어플라이언스를 등록하는 데 사용되는 모든 NAT ID 가운데에서 **반드시** 고유해야 합니다. 자세한 내용은 4-7페이지의 NAT 환경에서 작업을/를 참조하십시오.

관리되는 디바이스를 방어 센터에 등록할 때 디바이스에 적용할 액세스 제어 정책을 선택할 수 있습니다. 그러나 디바이스가 정책과 호환되지 않으면 정책 적용이 실패합니다. 이러한 비호환성은 라이센스 불일치, 모델 제약 조건, 수동 대 인라인 문제 및 기타 컨피그레이션 오류 등 다양한 이유로 발생할 수 있습니다. 초기 액세스 제어 정책 적용이 실패하면 초기 네트워크 검색 정책 적용도 실패합니다. 실패의 원인이 되는 문제를 해결한 후에는 액세스 제어 정책과 네트워크 검색 정책을 디바이스에 직접 적용해야 합니다. 액세스 제어 정책 적용 실패를 일으킬 수 있는 문제에 대한 자세한 내용은 12-21페이지의 액세스 제어 정책 및 규칙 문제 해결을/를 참조하십시오.

로컬 어플라이언스의 원격 관리를 구성하려면

액세스: 관리자

1단계 관리하려는 디바이스의 웹 인터페이스에서 **System > Local > Registration**을 선택합니다.

Remote Management 페이지가 나타납니다.

주의 Cisco에서는 관리 포트의 값을 변경하지 않을 것을 **적극** 권장합니다. 관리 포트를 변경하는 경우 구축에서 서로 통신해야 하는 모든 어플라이언스에 대해서도 변경해야 합니다. 자세한 내용은 4-22페이지의 관리 포트 변경을/를 참조하십시오.

2단계 **Add Manager**를 클릭합니다.

Add Remote Management 페이지가 나타납니다.

3단계 이 어플라이언스를 관리하기 위해 사용할 어플라이언스의 IP 주소 또는 호스트 이름을 **Management Host** 필드에 입력합니다.

호스트 이름은 정규화된 도메인 이름이거나, 유효한 IP 주소에 대한 로컬 DNS를 통해 확인되는 이름입니다.

NAT 환경에서는 관리되는 어플라이언스를 추가할 때 지정하려는 경우, 여기에서 IP 주소나 호스트 이름을 지정할 필요가 없습니다. 이 경우 FireSIGHT 시스템은 관리되는 어플라이언스의 웹 인터페이스에서 원격 관리자를 식별하기 위해 나중에 제공할 NAT ID를 사용합니다.

주의 네트워크에서 DHCP를 사용하여 IP 주소를 할당하는 경우 IP 주소보다는 호스트 이름을 사용하십시오.

4단계 어플라이언스 간 통신을 설정하는 데 사용할 등록 키를 **Registration Key** 필드에 입력합니다.

5단계 NAT 환경의 경우, 어플라이언스 간 통신을 설정하는 데 사용할 **고유한** 영숫자 NAT ID를 **Unique NAT ID** 필드에 입력합니다.

6단계 **Save**를 클릭합니다.

어플라이언스가 상호 통신 가능함을 확인하면 Pending Registration 상태가 나타납니다.

7단계 관리하는 어플라이언스의 웹 인터페이스를 사용하여 이 어플라이언스를 구축에 추가합니다.

자세한 내용은 4-23페이지의 방어 센터에 디바이스 추가을/를 참조하십시오.

참고 디바이스의 원격 관리를 활성화할 경우 NAT를 사용하는 일부 고가용성 구축에서는 보조 방어 센터도 관리자로서 추가해야 할 수 있습니다. 자세한 내용은 고객 지원에 문의하십시오.

원격 관리 수정

라이센스: 모두

관리하는 어플라이언스의 호스트 이름 또는 IP 주소를 수정하려면 다음 절차를 사용하십시오. FireSIGHT 시스템의 컨텍스트 내에서만 사용되는 이름인 관리하는 어플라이언스의 표시 이름도 변경할 수 있습니다. 호스트 이름을 어플라이언스의 표시 이름으로 사용할 수도 있지만 다른 표시 이름을 입력해도 호스트 이름이 변경되지 않습니다.

방어 센터보다 주요 버전이 둘 이상 낮은 소프트웨어를 실행하는 디바이스는 추가할 수 없습니다. 예를 들어 방어 센터에서 버전 5.4.0을 실행 중인 경우 5.3.x 이상을 실행하는 디바이스는 추가할 수 있지만 5.2.x를 실행하는 디바이스는 추가할 수 없습니다.

팁 관리되는 디바이스의 관리를 활성화 또는 비활성화하려면 슬라이더를 클릭할 수 있습니다. 관리를 비활성화하면 Defense Center와 디바이스 간 연결이 차단되지만, Defense Center에서 디바이스가 삭제되지는 **않습니다**. 디바이스를 더 이상 관리하지 않으려면 4-27페이지의 디바이스 삭제을/를 참조하십시오.

원격 관리를 수정하려면

액세스: 관리자

1단계 디바이스의 웹 인터페이스에서 **System > Local > Registration**을 선택합니다.

Remote Management 페이지가 나타납니다.

2단계 원격 관리 설정을 수정하려는 관리자 옆에 있는 수정 아이콘( )을 클릭합니다.

Edit Remote Management 페이지가 나타납니다.

3단계 관리하는 어플라이언스의 표시 이름을 **Name** 필드에서 변경합니다.

4단계 관리하는 어플라이언스의 IP 주소 또는 호스트 이름을 **Host** 필드에서 변경합니다.

호스트 이름은 정규화된 도메인 이름이거나, 유효한 IP 주소에 대한 로컬 DNS를 통해 확인되는 이름입니다.

5단계 **Save**를 클릭합니다.

변경 내용이 저장되었습니다.

관리 포트 변경

라이센스: 모두

FireSIGHT 시스템 어플라이언스는 기본적으로 포트 8305를 사용하는 양방향 SSL 암호화 통신 채널을 사용하여 통신합니다.

Cisco에서는 기본 설정을 유지할 것을 **적극** 권장하지만, 관리 포트가 네트워크의 다른 통신과 충돌하면 다른 포트를 선택할 수 있습니다. 일반적으로 관리 포트에 대한 변경은 FireSIGHT 시스템의 설치 중에 수행됩니다.

주의 관리 포트를 변경하는 경우 구축에서 서로 통신해야 하는 모든 어플라이언스에 대해 변경해야 합니다.

관리 포트를 변경하려면

액세스: 관리자

1단계 디바이스의 웹 인터페이스에서 **System > Local > Configuration**을 선택합니다.

Information 페이지가 나타납니다.

2단계 **Network**를 클릭합니다.

Network Settings 페이지가 나타납니다.

3단계 사용할 포트 번호를 **Remote Management Port** 필드에 입력합니다.

4단계 **Save**를 클릭합니다.

관리 포트가 변경됩니다.

5단계 이 어플라이언스와 통신해야 할 구축의 모든 어플라이언스에 대해 이 절차를 반복합니다.

방어 센터에 디바이스 추가

라이센스: 모두

디바이스를 관리할 때에는 방어 센터와 디바이스 간에 양방향 SSL 암호화 통신 채널을 설정합니다. 방어 센터는 이 채널을 사용하여 네트워크 트래픽을 분석하고자 하는 방법에 대한 정보를 디바이스로 전송합니다. 디바이스는 트래픽을 평가할 때 이벤트를 생성하고 동일한 채널을 사용하여 방어 센터로 전송합니다. 이 채널의 구성에 대한 자세한 내용은 4-20페이지의 원격 관리 구성을/를 참조하십시오.

방어 센터보다 주요 버전이 둘 이상 낮은 소프트웨어를 실행하는 디바이스는 추가할 수 없습니다. 예를 들어 방어 센터에서 버전 5.4를 실행 중인 경우 버전 5.3.x 이상을 실행하는 디바이스는 추가할 수 있지만 버전 5.2.x를 실행하는 디바이스는 추가할 수 없습니다.

방어 센터로 디바이스를 관리하기 전에 해당 디바이스에서 네트워크 설정이 정확히 구성되어 있는지 확인해야 합니다. 일반적으로 이 작업은 설치 과정 중에 완료됩니다. 자세한 내용은 64-8페이지의 관리 인터페이스 구성을/를 참조하십시오.

방어 센터 및 IPv4를 사용하는 디바이스를 등록했으며 IPv6으로 전환하려는 경우, 해당 디바이스를 삭제하고 다시 등록해야 합니다.

관리되는 디바이스를 방어 센터에 등록할 때 디바이스에 적용할 액세스 제어 정책을 선택할 수 있습니다. 그러나 디바이스가 정책과 호환되지 않으면 정책 적용이 실패합니다. 이러한 비호환성은 라이센스 불일치, 모델 제약 조건, 수동 대 인라인 문제 및 기타 컨피그레이션 오류 등 다양한 이유로 발생할 수 있습니다. 초기 액세스 제어 정책 적용이 실패하면 초기 네트워크 검색 정책 적용도 실패합니다. 실패의 원인이 되는 문제를 해결한 후에는 액세스 제어 정책과 네트워크 검색 정책을 디바이스에 직접 적용해야 합니다. 액세스 제어 정책 적용 실패를 일으킬 수 있는 문제에 대한 자세한 내용은 12-21페이지의 액세스 제어 정책 및 규칙 문제 해결을/를 참조하십시오.

디바이스 클러스터 또는 디바이스 스택을 등록할 때 라이센스를 선택할 수 있지만 이러한 라이센스는 디바이스 등록 시 적용할 수 없습니다. 이렇게 하면 클러스터 또는 스택이 올바른 라이센스를 실행하게 되어, 라이센스 불일치 때문에 강등된 상태로 전환되는 것을 방지할 수 있습니다. 등록 후에는 Device Management 페이지의 일반 속성(클러스터) 또는 스택 속성(스택)에서 라이센스를 평가할 수 있습니다. 자세한 내용은 4-32페이지의 디바이스 클러스터 설정 또는 4-45페이지의 디바이스 스택 설정을/를 참조하십시오.

Series 2 디바이스를 등록할 때 라이센스를 선택할 수 있지만, 선택하는 라이센스는 디바이스 등록 시 적용되지 않습니다. Series 2 디바이스는 보안 인텔리전스 필터링을 제외한 보호 기능을 자동으로 사용할 수 있습니다. 이러한 기능을 비활성화할 수 없으며, Series 2 디바이스에 다른 라이센스를 적용할 수도 없습니다.

팁 디바이스의 세부 컨피그레이션을 수정하려면 디바이스 옆에 있는 수정 아이콘( )을 클릭하십시오. 자세한 내용은 4-49페이지의 디바이스 컨피그레이션 수정 및 4-60페이지의 센싱 인터페이스 구성을/를 참조하십시오.

방어 센터에 디바이스를 추가하려면

액세스: Admin/Network Admin

1단계 방어 센터에 의해 관리되도록 디바이스를 구성합니다.

FirePOWER 디바이스의 경우 4-20페이지의 원격 관리 구성의 절차를 사용합니다. 디바이스가 방어 센터와의 통신을 확인하면 Pending Registration 상태가 나타납니다.

가상 디바이스, Cisco NGIPS for Blue Coat X-Series 및 ASA FirePOWER 디바이스의 경우 CLI(명령줄 인터페이스)를 사용하여 원격 관리를 구성합니다.

참고 NAT(network address translation)가 사용되는 일부 고가용성 구축의 경우 보조 방어 센터를 관리자로 추가해야 할 수 있습니다. 자세한 내용은 고객 지원에 문의하십시오.

2단계 방어 센터에 대한 웹 인터페이스에서 **Devices > Device Management**를 선택합니다.

Device Management(디바이스 관리) 페이지가 나타납니다.

3단계 **Add** 드롭다운 메뉴에서 **Add Device**를 클릭합니다.

Add Device 팝업 창이 나타납니다.

4단계 추가할 디바이스의 IP 주소 또는 호스트 이름을 **Host** 필드에 입력합니다.

디바이스의 호스트 이름은 정규화된 도메인 이름이거나, 유효한 IP 주소에 대한 로컬 DNS를 통해 확인되는 이름입니다.

NAT 환경에서는, 방어 센터로 관리할 디바이스를 구성할 때 방어 센터의 IP 주소 또는 호스트 이름을 이미 지정한 경우 디바이스의 IP 주소 또는 호스트 이름을 지정하지 않아도 될 수 있습니다. 자세한 내용은 4-7페이지의 NAT 환경에서 작업을/를 참조하십시오.

주의 네트워크에서 DHCP를 사용하여 IP 주소를 할당하는 경우 IP 주소보다는 호스트 이름을 사용하십시오.

5단계 방어 센터로 관리할 디바이스를 구성할 때 사용한 것과 동일한 등록 키를 **Registration Key** 필드에 입력합니다.

6단계 선택적으로 **Group** 드롭다운 목록에서 그룹을 선택하여 디바이스를 디바이스 그룹에 추가합니다.

디바이스 그룹에 대한 자세한 내용은 4-27페이지의 디바이스 그룹 관리을/를 참조하십시오.

7단계 **Access Control Policy** 드롭다운 목록에서 디바이스에 적용할 초기 정책을 선택합니다.

- **Default Access Control** 정책은 네트워크에 들어오는 모든 트래픽을 차단합니다.
- **Default Intrusion Prevention** 정책은 Balanced Security and Connectivity 침입 정책을 통과한 모든 트래픽을 허용합니다.

- **Default Network Discovery** 정책은 네트워크 검색만으로 검사되는 모든 트래픽을 허용합니다.
- 기존의 사용자 정의 액세스 제어 정책을 선택할 수 있습니다.

자세한 내용은 12-10페이지의 액세스 제어 정책 관리을/를 참조하십시오.

8단계 디바이스에 적용할 라이센스를 선택합니다. 다음 사항에 유의하십시오.

- 제어, 악성코드 및 URL 필터링 라이센스에는 보호 라이센스가 필요합니다.
- 가상 디바이스, Cisco NGIPS for Blue Coat X-Series 또는 ASA FirePOWER 디바이스에서는 VPN 라이센스를 활성화할 수 없습니다.
- Cisco NGIPS for Blue Coat X-Series에서는 Control 라이센스를 활성화할 수 없습니다.
- 가상 디바이스 또는 ASA FirePOWER 디바이스에서 제어 라이센스를 활성화할 수 있지만 이러한 디바이스는 빠른 경로 규칙, 스위칭, 라우팅, 스태킹 또는 클러스터링을 지원하지 **않습니다**.
- 클러스터링된 디바이스에 대한 라이센스 설정을 변경할 수 없습니다.
- 스태킹된 디바이스의 경우 어플라이언스 편집기의 Stack 페이지에서 스택에 대한 라이센스를 활성화 또는 비활성화합니다.
- Series 2 디바이스를 등록할 때, 선택하는 라이센스는 디바이스 등록 시 적용되지 않습니다. Series 2 디바이스는 보안 인텔리전스 필터링을 제외한 보호 기능을 자동으로 사용할 수 있습니다. 이러한 기능을 비활성화할 수 없으며, Series 2 디바이스에 다른 라이센스를 적용할 수도 없습니다.

자세한 내용은 65-1페이지의 FireSIGHT 시스템 라이센싱을/를 참조하십시오.

9단계 방어 센터에서 관리할 디바이스를 구성할 때 디바이스를 식별하기 위해 NAT ID를 사용한 경우, **Advanced** 섹션을 확장하고 **Unique NAT ID** 필드에 동일한 NAT ID를 입력합니다.

10단계 디바이스가 방어 센터로 패킷을 전송하도록 허용하려면 **Transfer Packets** 확인란을 선택합니다.

이 옵션은 기본적으로 활성화되어 있습니다. 이 옵션을 비활성화하면 방어 센터에 대한 패킷 전송이 완전히 차단됩니다.

11단계 **Register**를 클릭합니다.

디바이스가 방어 센터에 추가됩니다. 방어 센터가 디바이스의 하트비트를 확인하고 통신을 설정하는 데 최대 2분이 소요될 수 있습니다.

디바이스에 변경 사항 적용

라이센스: 모두

디바이스, 디바이스 클러스터 또는 디바이스 스택의 컨피그레이션을 변경한 후, 시스템 전체에 반영하려면 변경 사항을 반드시 적용해야 합니다. 디바이스에 적용되지 않은 변경 사항이 있어야 합니다. 그렇지 않으면 이 옵션이 비활성 상태로 표시됩니다.

인터페이스를 수정하고 디바이스 정책을 다시 적용하면 Snort는 디바이스의 모든 인터페이스 인스턴스(수정한 것만이 아니라)에 대해 다시 시작됩니다.

팁 Device Management 페이지 또는 어플라이언스 편집기의 **Interfaces** 탭에서 디바이스 변경 사항을 적용할 수 있습니다.

디바이스에 변경 사항을 적용하려면

액세스: Admin/Network Admin

1단계 **Devices > Device Management**를 선택합니다.

Device Management(디바이스 관리) 페이지가 나타납니다.

2단계 변경 사항을 적용하려는 디바이스 옆에 있는 수정 아이콘()을 클릭합니다.

3단계 프롬프트가 나타나면 **Apply**를 클릭합니다.

디바이스 변경 사항이 적용됩니다.

팁 선택적으로, Apply Device Changes 대화 상자에서 **View Changes**를 클릭합니다. Device Management Revision Comparison Report 페이지가 새 브라우저 창에 나타납니다. 자세한 내용은 4-26페이지의 디바이스 관리 개정 비교 보고서 사용을/를 참조하십시오.

4단계 **OK**를 클릭합니다.

Device Management 페이지로 돌아갑니다.

디바이스 관리 개정 비교 보고서 사용

라이센스: 모두

디바이스 관리 비교 보고서에서는 어플라이언스에 대해 수정한 내용을 적용 전에 볼 수 있습니다. 이 보고서는 현재 어플라이언스 컨피그레이션과 제안된 어플라이언스 컨피그레이션의 모든 차이점을 표시합니다. 따라서 잠재적 컨피그레이션 오류가 있으면 찾아낼 수 있습니다.

적용 전에 어플라이언스 변경 사항을 비교하려면

액세스: Admin/Network Admin

1단계 **Devices > Device Management**를 선택합니다.

Device Management(디바이스 관리) 페이지가 나타납니다.

2단계 변경 사항을 적용하려는 어플라이언스 옆에 있는 수정 아이콘()을 클릭합니다.

Apply Device Changes 팝업 창이 나타납니다. 어플라이언스에 적용되지 않은 변경 사항이 있어야 합니다. 그렇지 않으면 적용 아이콘이 비활성 상태로 표시됩니다.

3단계 **View Changes**를 클릭합니다.

Device Management Revision Comparison Report 페이지가 새 창에 나타납니다.

4단계 현재 어플라이언스 컨피그레이션과 제안된 어플라이언스 컨피그레이션 사이의 차이점을 스크롤하여 살펴보려면 **Previous** 및 **Next**를 클릭합니다.

5단계 선택적으로, 보고서의 PDF 버전을 생성하려면 **Comparison Report**를 클릭합니다.

디바이스 삭제

라이센스: 모두

디바이스를 더 이상 관리하지 않으려면 방어 센터에서 삭제할 수 있습니다. 디바이스 서버를 삭제하면 방어 센터와 디바이스 간 모든 통신이 단절됩니다. 나중에 디바이스를 다시 관리하려면 방어 센터에 다시 추가해야 합니다.

참고 고가용성 쌍에 구성된 방어 센터에서 디바이스를 삭제하고 다시 추가하려는 경우 Cisco에서는 디바이스를 다시 추가하기 전에 최소 5분 정도 기다릴 것을 권장합니다. 이 정도 기다리면 고가용성 쌍이 다시 동기화되어 두 방어 센터에서 모두 삭제를 인식할 수 있습니다. 5분을 기다리지 않는 경우, 두 방어 센터에 디바이스를 추가하는 데 두 번 이상의 동기화 주기가 걸릴 수 있습니다.

방어 센터에서 디바이스를 삭제하려면

액세스: Admin/Network Admin

1단계 **Devices > Device Management**를 선택합니다.

Device Management(디바이스 관리) 페이지가 나타납니다.

2단계 삭제하려는 디바이스 옆에 있는 삭제 아이콘( )을 클릭합니다.

확인 메시지가 표시되면 디바이스를 삭제할 것임을 확인합니다. 디바이스와 방어 센터 간 통신이 중단되고 Device Management(디바이스 관리) 페이지에서 디바이스가 삭제됩니다. 디바이스가 NTP를 통해 방어 센터에서 시간을 수신하도록 하는 시스템 정책이 있는 경우 해당 디바이스는 현지 시간 관리로 돌아갑니다.

디바이스 그룹 관리

라이센스: 모두

방어 센터에서는 정책을 손쉽게 적용하고 여러 디바이스에 업데이트를 설치하도록 디바이스를 그룹화할 수 있습니다. 그룹에 있는 디바이스의 목록을 확장 및 축소할 수 있습니다. 목록은 기본적으로 축소되어 나타납니다.

자세한 내용은 다음 절을 참조하십시오.

- 4-28페이지의 디바이스 그룹 추가
- 4-28페이지의 디바이스 그룹 수정
- 4-29페이지의 디바이스 그룹 삭제

디바이스 그룹 추가

라이센스: 모두

다음 절차에서는 정책을 손쉽게 적용하고 여러 디바이스에 업데이트를 설치할 수 있도록 디바이스 그룹을 추가하는 방법에 대해 설명합니다.

스택이나 클러스터의 기본 디바이스를 그룹에 추가하면 두 디바이스 모두 그룹에 추가됩니다. 디바이스의 스택 또는 클러스터를 해제하면 두 디바이스 모두 해당 그룹에 남아 있게 됩니다.

디바이스 그룹을 생성하고 여기에 디바이스를 추가하려면

액세스: Admin/Network Admin

1단계 **Devices > Device Management**를 선택합니다.

Device Management(디바이스 관리) 페이지가 나타납니다.

2단계 **Add** 드롭다운 메뉴에서 **Add Group**을 클릭합니다.

Add Group 팝업 창이 나타납니다.

3단계 **Name** 필드에 그룹의 이름을 입력합니다.

4단계 **Available Devices**에서 디바이스 그룹에 추가할 어플라이언스를 하나 이상 선택합니다. 여러 어플라이언스를 선택하려면 Ctrl 또는 Shift 키를 누른 채 클릭합니다.

5단계 디바이스 그룹에 선택한 어플라이언스를 포함하려면 **Add**를 클릭합니다.

6단계 **OK**를 클릭합니다.

디바이스 그룹이 추가됩니다.

디바이스 그룹 수정

라이센스: 모두

디바이스 그룹에 상주하는 디바이스의 설정을 변경할 수 있습니다. 어플라이언스를 새 그룹에 추가하려면 먼저 현재 그룹에서 제거해야 합니다.

어플라이언스를 새 그룹으로 이동할 경우 그룹에 전에 적용되었던 정책은 변경되지 않습니다. 디바이스의 정책을 변경하려면 디바이스 또는 디바이스 그룹에 새 정책을 적용해야 합니다.

스택이나 클러스터의 기본 디바이스를 그룹에 추가하면 두 디바이스 모두 그룹에 추가됩니다. 디바이스의 스택 또는 클러스터를 해제하면 두 디바이스 모두 해당 그룹에 남아 있게 됩니다.

디바이스 그룹을 수정하려면

액세스: Admin/Network Admin

1단계 **Devices > Device Management**를 선택합니다.

Device Management(디바이스 관리) 페이지가 나타납니다.

2단계 수정하려는 디바이스 그룹 옆에 있는 수정 아이콘( )을 클릭합니다.

Edit Group 팝업 창이 나타납니다.

3단계 선택적으로, **Name** 필드에 그룹의 새 이름을 입력합니다.

4단계 **Available Devices**에서 디바이스 그룹에 추가할 어플라이언스를 하나 이상 선택합니다. 여러 어플라이언스를 선택하려면 Ctrl 또는 Shift 키를 누른 채 클릭합니다.

5단계 디바이스 그룹에 선택한 어플라이언스를 포함하려면 **Add**를 클릭합니다.

6단계 디바이스 그룹에서 선택한 어플라이언스를 제거하려면 삭제 아이콘( )을 클릭합니다.

7단계 **OK**를 클릭합니다.

디바이스 그룹에 대한 변경 사항이 저장됩니다.

디바이스 그룹 삭제

라이센스: 모두

디바이스가 포함된 디바이스 그룹을 삭제하면 해당 디바이스는 Device Management 페이지의 Ungrouped 카테고리로 이동하며, 방어 센터에서 삭제되지 않습니다.

디바이스 그룹을 삭제하려면

액세스: Admin/Network Admin

1단계 **Devices > Device Management**를 선택합니다.

Device Management(디바이스 관리) 페이지가 나타납니다.

2단계 삭제하려는 디바이스 그룹 옆에 있는 삭제 아이콘( )을 클릭합니다.

3단계 확인 메시지가 표시되면 디바이스 그룹을 삭제할 것임을 확인합니다.

디바이스 그룹이 삭제됩니다.

디바이스 클러스터링

라이센스: 제어

지원되는 디바이스: Series 3

디바이스 클러스터링(디바이스 고가용성이라고도 함)을 이용하면 두 피어 디바이스 또는 두 피어 디바이스 스택 간에 네트워킹 기능 및 컨피그레이션 데이터의 이중화를 설정할 수 있습니다. 디바이스 스태킹에 대한 자세한 내용은 4-43페이지의 스태킹된 디바이스 관리을/를 참조하십시오.

컨피그레이션 이중화는 두 피어 디바이스 또는 두 피어 디바이스 스택을 정책 적용, 시스템 업데이트 및 등록을 위한 논리적인 단일 시스템으로 클러스터링함으로써 구현됩니다. 시스템은 자동으로 다른 컨피그레이션 데이터를 동기화합니다.

클러스터링 요구 사항

디바이스 클러스터를 구성할 수 있으려면 두 디바이스 또는 디바이스 스택의 기본 멤버가 동일한 모델이어야 하며 동일한 구리 또는 파이버 인터페이스를 가지고 있어야 합니다. 또한 두 디바이스 또는 디바이스 스택에서 동일한 소프트웨어를 실행해야 하며 동일한 라이센스를 가지고 있어야 합니다. 디바이스 스택의 하드웨어 컨피그레이션도 동일해야 합니다(설치된 악성코드 스토리지 팩 제외). 예를 들어 3D8290은 3D8290과 클러스터링할 수 있습니다. 악성코드 스토리지 팩은 스택에서 둘 중 하나 또는 둘 모두에 설치되어 있어도 되고, 둘 모두에 설치되지 않아도 됩니다. 디바이스가 NAT 정책의 대상이면 두 피어에 모두 동일한 NAT 정책이 적용되어야 합니다. 디바이스를 클러스터링한 후에는 개별 클러스터링된 디바이스에 대한 라이센스 옵션을 변경할 수 없지만, 전체 클러스터에 대한 라이센스는 변경할 수 있습니다. 자세한 내용은 4-32페이지의 디바이스 클러스터 설정을/를 참조하십시오.

주의 Cisco에서 제공하지 않은 하드 드라이브를 디바이스에 설치하려고 하지 마십시오. 지원되지 않는 하드 드라이브를 설치하면 디바이스가 손상될 수 있습니다. 악성코드 스토리지 팩 키트는 Cisco **전용**으로만, 그리고 8000 Series 디바이스 **전용**으로만 사용할 수 있습니다. 악성코드 스토리지 팩과 관련하여 도움이 필요하면 고객 지원에 문의하십시오. 자세한 내용은 FireSIGHT 시스템 *Malware Storage Pack Guide*를 참조하십시오.

클러스터링 장애 조치 및 유지 관리 모드

디바이스 클러스터링을 구현하면 시스템을 수동으로 또는 자동으로 장애 조치할 수 있습니다. 클러스터링된 디바이스 또는 스택 중 하나를 유지 관리 모드로 전환하면 장애 조치가 수동으로 트리거됩니다. 유지 관리 모드에 대한 자세한 내용은 4-37페이지의 클러스터링된 디바이스를 유지 관리 모드로 전환을/를 참조하십시오.

활성 디바이스 또는 스택의 상태가 손상된 후, 시스템 업데이트 중 또는 Administrator 권한의 사용자가 디바이스를 종료한 후에는 자동 장애 조치가 발생합니다. 활성 디바이스 또는 디바이스 스택에 NMSB 장애, NFE 장애, 하드웨어 장애, 펌웨어 장애, 중요한 프로세스 장애, 디스크 부족, 스태킹된 두 디바이스 간 연결 장애가 발생한 후에도 자동 장애 조치가 발생합니다. 백업 디바이스 또는 스택의 상태가 유사하게 손상되는 경우, 시스템은 장애 조치를 수행하는 대신 강등된 상태로 전환합니다. 디바이스 또는 디바이스 스택 중 하나가 유지 관리 모드에 있는 경우에도 시스템은 장애 조치를 수행하지 않습니다. 활성 스택에서 스태킹 케이블의 연결을 끊으면 해당 스택이 유지 관리 모드로 전환됩니다. 활성 스택에서 보조 디바이스를 종료하면 해당 스택이 유지 관리 모드로 전환됩니다.

참고 활성 클러스터 멤버가 유지 관리 모드로 들어가고 활성 역할이 다른 클러스터 멤버로 장애 조치되면, 원래 활성 클러스터 멤버가 정상적인 운영 상태로 복원되더라도 활성 역할이 자동으로 돌아오지 않습니다.

정책 및 업데이트 적용

정책을 적용할 경우 개별 디바이스 또는 스택이 아니라 디바이스 클러스터에 적용합니다. 정책이 실패하면 시스템은 디바이스나 스택에 정책을 적용하지 않습니다. 클러스터에 네트워크 트래픽을 처리하는 피어가 항상 하나만 있도록 정책은 먼저 활성 디바이스 또는 스택에 적용되고 그다음 백업에 적용됩니다.

클러스터링된 디바이스는 개별 디바이스 또는 스택으로서가 아니라 단일 엔티티로서 업데이트를 수신합니다. 업데이트가 시작되면 시스템은 먼저 백업 디바이스 또는 스택에 업데이트를 적용합니다. 그러면 이러한 디바이스 또는 스택은 필요한 프로세스가 다시 시작되고 디바이스가 다시 트래픽 처리를 시작할 때까지 유지 관리 모드로 전환됩니다. 그런 다음 시스템은 활성 디바이스 또는 스택에 업데이트를 적용하며, 동일한 프로세스가 이어집니다.

디바이스를 클러스터링하지 않고 이중화 구현

대부분의 경우, Cisco Redundancy Protocol(SFRP)을 사용하여 디바이스 클러스터링 없이 레이어 3 이중화를 구현할 수 있습니다. SFRP를 사용하면 특정 IP 주소에 대해 디바이스가 이중 게이트웨이 역할을 하도록 지정할 수 있습니다. 네트워크 이중화를 구현하면, 네트워크의 다른 호스트에 대한 연결을 보장하기 위해 두 디바이스나 스택에서 동일한 네트워크 연결을 제공하도록 구성할 수 있습니다. SFRP에 대한 자세한 내용은 7-7페이지의 SFRP 구성을/를 참조하십시오.

FireSIGHT 시스템 구축(수동, 인라인, 라우티드 또는 스위치드)에 따라 디바이스 고가용성의 구성 방법을 결정합니다. 동시에 여러 역할에서 시스템을 구축할 수도 있습니다. 네 가지 구축 유형 중 패시브 구축에서만 클러스터 디바이스 또는 스택이 이중화를 제공하도록 요구합니다. 나머지 구축 유형의 경우 디바이스 클러스터와 함께 또는 없이 네트워크 이중화를 설정할 수 있습니다. 다음 절에서는 구축 유형별로 간단하게 고가용성의 개요를 제공합니다.

패시브 구축 이중화

패시브 인터페이스는 일반적으로 중앙 스위치의 탭 포트에 연결되며, 이에 따라 스위치 전체에 흐르는 모든 트래픽을 분석할 수 있습니다. 여러 디바이스가 동일한 탭 피드에 연결되면 시스템은 각 디바이스에서 이벤트를 생성합니다. 클러스터링된 디바이스는 활성 또는 백업으로 작동하며, 시스템은 장애가 발생하더라도 트래픽을 분석하는 한편 이중 이벤트를 방지할 수 있습니다.

인라인 구축 이중화

인라인 집합은 통과하는 패킷의 라우팅을 제어하지 못하므로 구축에서 항상 활성 상태여야 합니다. 따라서 이중화는 트래픽을 올바르게 라우팅하기 위해 외부 시스템에 의존합니다. 디바이스 클러스터를 사용하거나 사용하지 않고 이중 인라인 집합을 구성할 수 있습니다.

이중 인라인 집합을 구축하려면, 순환 라우팅을 방지하는 한편 트래픽이 인라인 집합 중 하나만 통과하도록 네트워크 토폴로지를 구성해야 합니다. 인라인 집합 중 하나가 실패하면 주변 네트워크 인프라는 게이트웨이 주소에 대한 연결 손실을 탐지하고, 이중 설정을 통해 트래픽을 전송하도록 경로를 조정합니다.

라우티드 구축 이중화

IP 네트워크의 호스트는 잘 알려진 게이트웨이 주소를 사용하여 트래픽을 다른 네트워크로 전송해야 합니다. 라우티드 구축에서 이중화를 설정하려면, 라우티드 인터페이스가 게이트웨이 주소를 공유하여 특정 시점에 한 인터페이스만 해당 주소를 처리하도록 해야 합니다. 이렇게 하려면 가상 라우터에서 동일한 수의 IP 주소를 유지 관리해야 합니다. 한 인터페이스가 주소를 광고합니다. 이 인터페이스가 다운되면 백업 인터페이스가 주소의 광고를 시작합니다.

클러스터링되지 않은 디바이스에서는 게이트웨이 IP 주소가 여러 라우티드 인터페이스 간에 공유되도록 구성함으로써 SFRP를 사용하여 이중화를 설정합니다. 디바이스 클러스터를 사용하거나 사용하지 않고 SFRP를 구성할 수 있습니다. OSPF 또는 RIP와 같은 동적 라우팅을 사용하여 이중화를 설정할 수도 있습니다.

스위치드 구축 이중화

스위치드 구축에서는 STP(Spanning Tree Protocol)를 사용하여 이중화를 설정합니다. STP는 연결된 네트워크의 토폴로지를 관리하는 프로토콜로서, 백업 링크를 구성하지 않고도 이중 링크에서 스위치드 인터페이스에 대해 자동 백업을 제공하도록 특별히 설계되었습니다. 스위치드 구축의 디바이스는 STP를 사용하여 이중 인터페이스 간 트래픽을 관리합니다. 동일한 브로드캐스트 네트워크에 연결된 두 디바이스는 STP에 의해 계산된 토폴로지를 기반으로 트래픽을 수신합니다. STP 활성화에 대한 자세한 내용은 6-7페이지의 고급 가상 스위치 설정 컨피그레이션을/를 참조하십시오.

참고 Cisco에서는 디바이스 클러스터에 구축할 가상 스위치를 구성할 때는 STP를 활성화할 것을 권장합니다.

클러스터링 디바이스 및 스택에 대한 자세한 내용은 다음 절을 참조하십시오.

- 4-32페이지의 디바이스 클러스터 설정
- 4-34페이지의 디바이스 클러스터 수정
- 4-34페이지의 클러스터에서 개별 디바이스 구성
- 4-35페이지의 클러스터에서 개별 디바이스 스택 구성
- 4-36페이지의 클러스터링된 디바이스에서 인터페이스 구성
- 4-36페이지의 클러스터에서 활성 피어 전환
- 4-37페이지의 클러스터링된 디바이스를 유지 관리 모드로 전환
- 4-37페이지의 클러스터링된 스택에서 디바이스 교체
- 4-38페이지의 클러스터링된 상태 공유 설정
- 4-40페이지의 클러스터링된 상태 공유 문제 해결
- 4-43페이지의 클러스터링된 디바이스 분리
- 7-7페이지의 SFRP 구성
- 4-63페이지의 HA 링크 인터페이스 구성

디바이스 클러스터 설정

라이센스: 제어

지원되는 디바이스: Series 3

디바이스 클러스터를 설정하기 전에 다음 전제 조건을 충족해야 합니다.

- 스택의 각 디바이스 또는 각 기본 디바이스에서 인터페이스를 구성합니다.
- 클러스터에 포함하는 각 디바이스 또는 디바이스 스택 기본 멤버는 동일한 모델이어야 하며 동일한 구리 또는 파이버 인터페이스를 가지고 있어야 합니다.
- 두 디바이스 또는 디바이스 스택은 정상적인 상태여야 하고, 동일한 소프트웨어를 실행해야 하며, 동일한 라이센스를 보유해야 합니다. 자세한 내용은 68-41페이지의 상태 모니터 사용을/를 참조하십시오. 특히 디바이스에는 유지 관리 모드로 들어가서 장애 조치의 트리거를 유발하는 하드웨어 장애가 있어서는 안 됩니다.
- 클러스터의 디바이스와 스택에서는 불일치가 허용되지 않습니다. 하드웨어 컨피그레이션이 동일한 단일 디바이스 또는 디바이스 스택을 클러스터링해야 합니다(악성코드 스토리지 팩은 제외). 예를 들어 3D8290은 3D8290과 클러스터링할 수 있습니다. 악성코드 스토리지 팩은 스택에서 둘 중 하나 또는 둘 모두에 설치되어 있어도 되고, 둘 모두에 설치되지 않아도 됩니다. 악성코드 스토리지 팩에 대한 자세한 내용은 *FireSIGHT 시스템 Malware Storage Pack Guide*를 참조하십시오.

주의 Cisco에서 제공하지 않은 하드 드라이브를 디바이스에 설치하려고 하지 마십시오. 지원되지 않는 하드 드라이브를 설치하면 디바이스가 손상될 수 있습니다. 악성코드 스토리지 팩 키트는 Cisco **전용**으로만, 그리고 8000 Series 디바이스 **전용**으로만 사용할 수 있습니다. 악성코드 스토리지 팩과 관련하여 도움이 필요하면 고객 지원에 문의하십시오. 자세한 내용은 FireSIGHT 시스템 *Malware Storage Pack Guide*를 참조하십시오.

- 디바이스가 NAT 정책의 대상이면 두 피어에 모두 동일한 NAT 정책이 적용되어야 합니다.

디바이스 클러스터를 설정할 때 디바이스나 스택 중 하나는 활성으로, 다른 하나는 백업으로 지정합니다. 시스템은 클러스터링된 디바이스에 병합된 컨피그레이션을 적용합니다. 충돌이 있는 경우 활성으로 지정한 디바이스 또는 스택의 컨피그레이션이 적용됩니다.

디바이스를 클러스터링한 후에는 개별 클러스터링된 디바이스에 대한 라이센스 옵션을 변경할 수 없지만, 전체 클러스터에 대한 라이센스는 변경할 수 있습니다. 자세한 내용은 4-34페이지의 디바이스 클러스터 수정을/를 참조하십시오. 스위치드 또는 라우티드 인터페이스에서 설정해야 할 인터페이스 특성이 있는 경우 시스템은 클러스터를 구현하되 보류 상태로 설정합니다. 필요한 특성이 구성되면 시스템은 디바이스 클러스터를 완료하고 정상 상태로 설정합니다.

클러스터링된 쌍이 설정되면 시스템은 Device Management 페이지에서 피어 디바이스 또는 스택을 단일 디바이스로 취급합니다. 디바이스 클러스터는 어플라이언스 목록에 클러스터 아이콘( )을 표시합니다. 컨피그레이션에 대한 변경 사항은 클러스터링된 디바이스 간에 동기화됩니다. Device Management 페이지에는 클러스터의 어떤 디바이스 또는 스택이 활성 상태인지, 수동 또는 자동 장애 조치 후 어떤 것이 변경되는지가 표시됩니다. 수동 장애 조치에 대한 자세한 내용은 4-37페이지의 클러스터링된 디바이스를 유지 관리 모드로 전환을/를 참조하십시오.

방어 센터에서 디바이스 클러스터의 등록을 제거하면 두 디바이스 또는 스택에서 모두 등록이 제거됩니다. 개별 관리되는 디바이스에서 하듯 방어 센터에서 디바이스 클러스터를 제거합니다. 자세한 내용은 4-27페이지의 디바이스 삭제을/를 참조하십시오.

그런 다음 다른 방어 센터에서 클러스터를 등록할 수 있습니다. 클러스터링된 단일 디바이스를 등록하려면 클러스터의 활성 디바이스에 원격 관리를 추가한 다음 해당 디바이스를 방어 센터에 추가합니다. 그러면 전체 클러스터가 추가됩니다. 클러스터링된 스택 디바이스를 등록하려면 스택의 기본 디바이스에 원격 관리를 추가한 다음 해당 디바이스를 방어 센터에 추가합니다. 그러면 전체 클러스터가 추가됩니다. 자세한 내용은 4-23페이지의 방어 센터에 디바이스 추가을/를 참조하십시오.

디바이스 클러스터를 설정했으면 4-63페이지의 HA 링크 인터페이스 구성에 설명된 대로 고가용성 링크 인터페이스를 구성할 수 있습니다.

디바이스 또는 디바이스 스택을 클러스터링하려면

액세스: Admin/Network Admin

1단계 **Devices > Device Management**를 선택합니다.

Device Management(디바이스 관리) 페이지가 나타납니다.

2단계 **Add** 드롭다운 메뉴에서 **Add Cluster**를 클릭합니다.

Add Cluster 팝업 창이 나타납니다.

3단계 **Name** 필드에 클러스터의 이름을 입력합니다.

영숫자 문자 및 특수 문자를 사용할 수 있지만 +, (,), {, }, #, &, \, <, >, ?, ‘, “ 문자는 유효하지 않으므로 사용할 수 없습니다.

4단계 클러스터에 대한 **Active** 디바이스 또는 스택을 선택합니다.

5단계 클러스터에 대한 **Backup** 디바이스 또는 스택을 선택합니다.

6단계 **Cluster**를 클릭합니다.

디바이스 클러스터가 추가됩니다. 이 프로세스는 시스템 데이터를 동기화하는 데 몇 분 정도 걸립니다.

디바이스 클러스터 수정

라이센스: 제어

지원되는 디바이스: Series 3

디바이스 클러스터를 설정한 후 디바이스 컨피그레이션을 변경하면 대부분 전체 클러스터의 컨피그레이션도 변경됩니다.

General 섹션의 상태 아이콘 위로 포인터를 이동하면 클러스터의 상태를 볼 수 있습니다. 또한 어떤 디바이스 또는 스택이 클러스터에서 활성 피어 및 백업 피어인지 볼 수 있습니다.

자세한 내용은 다음 절을 참조하십시오.

- 4-50페이지의 일반 디바이스 설정 수정
- 4-51페이지의 디바이스 라이센스 활성화 및 비활성화
- 4-38페이지의 클러스터링된 상태 공유 설정
- 4-55페이지의 고급 디바이스 설정 수정

디바이스 클러스터를 수정하려면

액세스: Admin/Network Admin

1단계 **Devices > Device Management**를 선택합니다.

Device Management(디바이스 관리) 페이지가 나타납니다.

2단계 컨피그레이션을 수정하려는 디바이스 클러스터 옆에 있는 수정 아이콘( )을 클릭합니다.

Cluster 페이지가 나타납니다.

3단계 Cluster 페이지의 섹션을 사용하여 마치 단일 디바이스 컨피그레이션에 대해 하듯 클러스터링된 컨피그레이션을 변경합니다.

클러스터에서 개별 디바이스 구성

라이센스: 제어

지원되는 디바이스: Series 3

디바이스 클러스터를 설정한 후에도 여전히 클러스터 내에서 각 디바이스의 일부 특성을 구성할 수 있습니다. 단일 디바이스에 대해 하듯 클러스터링된 디바이스를 변경할 수 있습니다.

자세한 내용은 다음 절을 참조하십시오.

- 4-50페이지의 일반 디바이스 설정 수정
- 4-52페이지의 디바이스 시스템 설정 수정
- 4-53페이지의 디바이스의 상태 보기
- 4-53페이지의 디바이스 관리 설정 수정

클러스터의 개별 디바이스를 구성하려면

액세스: Admin/Network Admin

1단계 **Devices > Device Management**를 선택합니다.

Device Management(디바이스 관리) 페이지가 나타납니다.

2단계 컨피그레이션을 수정하려는 디바이스 클러스터 옆에 있는 수정 아이콘( )을 클릭합니다.

Cluster 페이지가 나타납니다.

3단계 **Devices**를 클릭합니다.

Devices 페이지가 나타납니다.

4단계 **Selected Device** 드롭다운 목록에서 수정할 디바이스를 선택합니다.

5단계 Devices 페이지의 섹션을 사용하여 마치 단일 디바이스에 대해 하듯 클러스터링된 개별 디바이스를 변경합니다.

클러스터에서 개별 디바이스 스택 구성

라이센스: 제어

지원되는 디바이스: Series 3

스태킹된 디바이스의 쌍을 클러스터링한 후에는 수정 가능한 스택 특성이 제한됩니다. 클러스터링된 스택에서는 스택의 이름을 수정할 수 있습니다. 또한 4-36페이지의 클러스터링된 디바이스에서 인터페이스 구성에 설명된 대로 네트워크 컨피그레이션을 수정할 수 있습니다.

클러스터에서 스택의 이름을 수정하려면

액세스: Admin/Network Admin

1단계 **Devices > Device Management**를 선택합니다.

Device Management(디바이스 관리) 페이지가 나타납니다.

2단계 컨피그레이션을 수정하려는 디바이스 클러스터 옆에 있는 수정 아이콘( )을 클릭합니다.

Cluster 페이지가 나타납니다.

3단계 **Stacks**를 클릭합니다.

Stacks 페이지가 나타납니다.

Selected Device 드롭다운 목록에서 수정할 스택을 선택합니다.

4단계 General 섹션 옆에 있는 수정 아이콘( )을 클릭합니다.

General 팝업 창이 나타납니다.

5단계 **Name** 필드에 스택에 대한 새로운 할당 이름을 입력합니다.

영숫자 문자 및 특수 문자를 사용할 수 있지만 +, (,), {, }, #, &, \, <, >, ?, ‘, “ 문자는 유효하지 않으므로 사용할 수 없습니다.

6단계 **Save**를 클릭합니다.

새 이름이 저장됩니다. 스택 컨피그레이션을 적용해야 변경 사항이 적용됩니다. 자세한 내용은 4-25페이지의 디바이스에 변경 사항 적용을/를 참조하십시오.

클러스터링된 디바이스에서 인터페이스 구성

라이센스: 제어

지원되는 디바이스: Series 3

클러스터의 개별 디바이스에서 인터페이스를 구성할 수 있습니다. 그러나 클러스터의 피어 디바이스에서도 그에 상응하는 인터페이스를 구성해야 합니다. 클러스터링된 스택의 경우 스택의 기본 디바이스에서 동일한 인터페이스를 구성합니다. 가상 라우터를 구성하는 경우 라우터를 구성할 스택을 선택할 수 있습니다. 자세한 내용은 7-9페이지의 가상 라우터 구성을/를 참조하십시오.

클러스터링된 디바이스의 Interfaces 페이지에는 개별 디바이스에 찾을 수 있는 하드웨어 및 인터페이스 보기가 포함됩니다. 자세한 내용은 4-60페이지의 센싱 인터페이스 구성을/를 참조하십시오.

클러스터링된 디바이스에서 인터페이스를 구성하려면

액세스: Admin/Network Admin

1단계 **Devices > Device Management**를 선택합니다.

Device Management 페이지가 나타납니다.

2단계 인터페이스를 구성할 디바이스 클러스터 옆에 있는 수정 아이콘( )을 클릭합니다.

Cluster 페이지가 나타납니다.

3단계 **Interfaces**를 클릭합니다.

Interfaces 페이지가 나타납니다.

4단계 **Selected Device** 드롭다운 목록에서 수정할 디바이스를 선택합니다.

5단계 개별 디바이스에서 하듯 인터페이스를 구성합니다. 자세한 내용은 4-60페이지의 센싱 인터페이스 구성을/를 참조하십시오.

클러스터에서 활성 피어 전환

라이센스: 제어

지원되는 디바이스: Series 3

디바이스 클러스터를 설정한 후 활성 및 백업 피어 디바이스 또는 스택을 수동으로 전환할 수 있습니다.

클러스터에서 활성 피어를 전환하려면

액세스: Admin/Network Admin

1단계 **Devices > Device Management**를 선택합니다.

Device Management 페이지가 나타납니다.

2단계 활성 피어를 변경할 디바이스 클러스터 옆에 있는 활성 피어 전환 아이콘( )을 클릭합니다.

Switch Active Peer 팝업 창이 나타납니다.

3단계 백업 디바이스를 클러스터의 활성 디바이스로 즉시 전환하려면 **Yes**를 클릭합니다. 취소하고 Device Management 페이지로 돌아가려면 **No**를 클릭합니다.

클러스터링된 디바이스를 유지 관리 모드로 전환

라이센스: 제어

지원되는 디바이스: Series 3

클러스터를 설정한 후 클러스터링된 디바이스 또는 스택 중 하나를 디바이스에서 유지 관리를 수행하기 위한 유지 관리 모드로 전환함으로써 수동으로 장애 조치를 트리거할 수 있습니다. 유지 관리 모드에서는 관리 인터페이스를 제외한 모든 인터페이스가 관리상 다운됩니다. 유지 관리가 완료되면 정상 운영이 시작되도록 디바이스를 다시 활성화할 수 있습니다.

참고 클러스터의 두 멤버를 동시에 유지 관리 모드로 전환해서는 안 됩니다. 그렇게 하면 클러스터에서 트래픽을 검사하지 못합니다.

클러스터링된 디바이스를 유지 관리 모드로 전환하려면

액세스: Admin/Network Admin

1단계 **Devices > Device Management**를 선택합니다.

Device Management 페이지가 나타납니다.

2단계 유지 관리 모드로 전환하려는 클러스터링된 디바이스 옆에 있는 유지 관리 모드 전환 아이콘( )을 클릭합니다.

Confirm Maintenance Mode 팝업 창이 나타납니다.

3단계 유지 관리 모드를 확인하려면 **Yes**를 클릭하고 취소하려면 **No**를 클릭합니다.

4단계 유지 관리 모드에서 나오려면 유지 관리 모드 전환 아이콘( )을 다시 클릭합니다.

클러스터링된 스택에서 디바이스 교체

라이센스: 제어

지원되는 디바이스: Series 3

클러스터 멤버인 스택을 유지 관리 모드로 전환했으면 스택의 보조 디바이스를 다른 디바이스로 교체할 수 있습니다. 현재 스태킹되거나 클러스터링되지 않은 디바이스만 선택할 수 있습니다. 새 디바이스는 디바이스 스택을 설정하기 위한 동일한 지침을 따라야 합니다. 4-45페이지의 디바이스 스택 설정을/를 참조하십시오.

클러스터링된 스택에서 디바이스를 교체하려면

액세스: Admin/Network Admin

1단계 **Devices > Device Management**를 선택합니다.

Device Management 페이지가 나타납니다.

2단계 유지 관리 모드로 전환하려는 스택 멤버 옆에 있는 유지 관리 모드 전환 아이콘( )을 클릭합니다.

Confirm Maintenance Mode 팝업 창이 나타납니다.

3단계 유지 관리 모드를 확인하려면 **Yes**를 클릭하고 취소하려면 **No**를 클릭합니다.

4단계 디바이스 교체 아이콘( )을 클릭합니다.

Replace Device 팝업 창이 나타납니다.

5단계 드롭다운 목록에서 **Replacement Device**를 선택합니다.

6단계 디바이스를 교체하려면 **Replace**를 클릭하고, 현재 디바이스를 유지하고 Device Management 페이지로 돌아가려면 **Cancel**을 클릭합니다.

7단계 유지 관리 모드에서 즉시 나오려면 유지 관리 모드 전환 아이콘( )을 다시 클릭합니다.

디바이스 컨피그레이션을 다시 적용할 필요가 없습니다.

클러스터링된 상태 공유 설정

라이센스: 제어

지원되는 디바이스: Series 3

클러스터링된 상태를 공유하면 클러스터링된 디바이스 또는 클러스터링된 스택의 상태를 필요한 만큼 동기화하여, 둘 중 한 디바이스 또는 스택이 실패하면 다른 피어가 중단 없이 트래픽 플로우를 처리하도록 할 수 있습니다. 상태를 공유하지 않으면 다음 기능이 제대로 장애 조치되지 않을 수 있습니다.

- Strict TCP enforcement
- Unidirectional access control rules
- Blocking persistence

그러나 상태 공유를 활성화하면 시스템 성능이 저하됩니다.

클러스터링된 상태 공유를 구성하려면 먼저 클러스터의 두 디바이스 또는 기본 스택 디바이스에서 HA 링크 인터페이스를 구성 및 활성화해야 합니다. 3D8250 디바이스에는 10G HA 링크가 필요한 반면, 다른 모델에는 1G HA 링크가 필요합니다. 자세한 내용은 4-63페이지의 HA 링크 인터페이스 구성을/를 참조하십시오.

참고 클러스터링된 디바이스가 장애 조치되면 시스템은 활성 디바이스에서 기존의 모든 SSL 암호화 세션을 종료합니다. 클러스터링된 상태 공유를 설정하더라도 백업 디바이스에서 이러한 세션을 재협상해야 합니다. SSL 세션을 설정한 서버에서 세션 재사용을 지원하며 백업 디바이스에 SSL 세션 ID가 없다면 세션을 재협상할 수 없습니다. 자세한 내용은 4-29페이지의 디바이스 클러스터링을/를 참조하십시오.

Strict TCP Enforcement

도메인에 대한 엄격한 TCP 적용을 활성화하면 시스템은 TCP 세션에서 순서가 뒤바뀐 모든 패킷을 삭제합니다. 예를 들어 시스템은 설정되지 않은 연결에서 수신한 비 SYN 패킷을 삭제합니다. 상태 공유를 사용할 경우 클러스터의 디바이스는 장애 조치 이후 연결을 재설정하지 않고도(엄격한 TCP 적용이 활성화된 경우에도) TCP 세션이 지속되도록 허용합니다. 인라인 집합, 가상 라우터 및 가상 스위치에서 엄격한 TCP 적용을 활성화할 수 있습니다.

Unidirectional Access Control Rules

단방향 액세스 제어 규칙을 구성한 경우, 네트워크 트래픽은 장애 조치 후 시스템이 연결 미드스트림을 재평가할 때 의도한 것과 다른 액세스 제어 규칙을 매칭할 수 있습니다. 예를 들어 다음의 두 가지 액세스 제어 규칙이 포함된 정책이 있다고 가정해보겠습니다.

```
Rule 1: Allow from 192.168.1.0/24 to 192.168.2.0/24
Rule 2: Block all
```

상태 공유를 사용하지 않는 경우, 192.168.1.1에서 192.168.2.1로의 허용된 연결이 장애 조치 후 여전히 활성 상태이며 다음 패킷이 응답 패킷으로 표시되는 경우 시스템은 연결을 거부합니다. 상태 공유를 사용하는 경우 미드스트림 픽업이 기존 연결을 매칭하며 계속 허용됩니다.

Blocking Persistence

액세스 제어 규칙 또는 기타 요인을 기반으로 첫 번째 패킷에서 많은 연결이 차단되지만, 연결을 차단해야 한다고 결정하기 전 시스템이 일부 패킷의 통과를 허용하는 경우가 있습니다. 상태 공유를 사용하는 경우 시스템은 피어 디바이스 또는 스택의 연결도 즉시 차단합니다.

클러스터링된 상태 공유를 설정하면 다음 옵션을 구성할 수 있습니다.

Enabled

상태 공유를 활성화하려면 확인란을 클릭합니다. 상태 공유를 비활성화하려면 확인란의 선택을 취소합니다.

Minimum Flow Lifetime

시스템이 동기화 메시지를 전송하기 전 세션의 최소 시간(밀리초)을 지정합니다. 0~65535의 정수를 사용할 수 있습니다. 시스템은 최소 플로우 수명 주기를 충족하지 않는 세션을 동기화하지 않으며, 연결에 대한 패킷을 수신하는 경우에만 동기화합니다.

Minimum Sync. Interval

세션에 대한 업데이트 메시지 간 최소 시간(밀리초)을 지정합니다. 0~65535의 정수를 사용할 수 있습니다. 최소 동기화 간격을 지정하면, 연결이 최소 수명 주기에 도달한 후 지정된 연결에 대한 동기화 메시지가 구성된 값보다 자주 전송되지 않습니다.

Maximum HTTP URL Length

시스템이 클러스터링된 디바이스 간에 동기화하는 URL의 최대 문자 수를 지정합니다. 0~225의 정수를 사용할 수 있습니다.

참고 구축에서 값을 변경할 합당한 이유가 없는 한 Cisco에서는 기본값 사용을 권장합니다. 값을 내리면 클러스터링된 피어의 준비 상태가 개선되는 반면, 값을 올리면 성능이 개선됩니다.

클러스터링된 상태 공유를 설정하려면

액세스: Admin/Network Admin

1단계 클러스터의 각 디바이스에 대해 HA 링크 인터페이스를 구성합니다.

자세한 내용은 4-63페이지의 HA 링크 인터페이스 구성을/를 참조하십시오.

2단계 **Devices > Device Management**를 선택합니다.

Device Management 페이지가 나타납니다.

3단계 수정하려는 디바이스 클러스터 옆에 있는 수정 아이콘( )을 클릭합니다.

Cluster 페이지가 나타납니다.

4단계 **State Sharing** 섹션 옆에 있는 수정 아이콘( )을 클릭합니다.

State Sharing 팝업 창이 나타납니다.

5단계 이 절에서 앞서 설명한 것처럼 상태 공유를 구성합니다.

6단계 **OK**를 클릭합니다.

변경 내용이 저장되었습니다. 디바이스 컨피그레이션을 적용해야 변경 사항이 적용됩니다. 자세한 내용은 4-25페이지의 디바이스에 변경 사항 적용을/를 참조하십시오.

클러스터링된 상태 공유 문제 해결

라이센스: 제어

지원되는 디바이스: Series 3

상태 공유를 활성화한 후 Cluster 페이지의 State Sharing 섹션에서 컨피그레이션에 대한 다음 정보를 볼 수 있습니다.

- 사용 중인 HA 링크 인터페이스 및 현재 링크 상태
- 문제 해결을 위한 자세한 동기화 통계

상태 공유 통계는 주로 주고받은 클러스터링된 동기화 트래픽의 여러 부분에 대한 카운터이며, 기타 몇 가지 오류 카운터도 포함됩니다. 또한 클러스터의 각 디바이스에 대한 최신 시스템 로그도 볼 수 있습니다.

각 디바이스에 대해 볼 수 있는 통계 및 그러한 통계를 사용하여 클러스터링된 상태 공유 컨피그레이션의 문제를 해결하는 방법에 대한 자세한 내용은 다음 절을 참조하십시오.

Messages Received(Unicast)

Messages Received는 클러스터링된 피어에서 수신한 클러스터 동기화 메시지의 수입니다.

이 값은 피어에서 전송한 메시지의 수에 근접해야 합니다. 활성 사용 중에는 값이 일치하지 않을 수 있지만 근접해야 합니다. 트래픽이 중지되면 값이 안정화되며 수신 메시지가 전송 메시지와 일치하게 됩니다.

문제를 해결하려면 수신 메시지와 전송 메시지를 모두 보고, 증가 속도를 비교하고, 값이 근접한지 확인해야 합니다. 각 피어의 전송 값은 반대 피어의 수신 값과 거의 같은 속도로 증가해야 합니다.

수신 메시지가 증가하지 않거나 피어에서 전송한 메시지보다 느린 속도로 증가하는 경우 고객 지원에 문의하십시오.

Packets Received

시스템은 오버헤드를 줄이기 위해 여러 메시지를 단일 패킷으로 일괄 처리합니다. Packets Received 카운터에는 이러한 데이터 패킷의 총수는 물론 디바이스에서 수신한 다른 제어 패킷도 표시됩니다.

이 값은 피어 디바이스에서 전송한 패킷의 수에 근접해야 합니다. 활성 사용 중에는 값이 일치하지 않을 수 있지만 근접해야 합니다. 수신한 메시지 수는 피어에서 전송한 메시지 수에 근접해야 하고 같은 속도로 증가해야 하므로, 수신한 패킷 수도 이와 같아야 합니다.

문제를 해결하려면 수신 패킷과 전송 메시지를 모두 보고, 증가 속도를 비교하고, 값이 같은 속도로 증가하는지 확인해야 합니다. 클러스터링된 피어의 전송 값이 증가하면 디바이스의 수신 값도 같은 속도로 증가해야 합니다.

수신 패킷이 증가하지 않거나 피어에서 전송한 메시지보다 느린 속도로 증가하는 경우 고객 지원에 문의하십시오.

Total Bytes Received

Total Bytes Received는 피어에서 수신한 패킷을 구성하는 바이트의 수입니다.

이 값은 다른 피어에서 수신한 바이트 수에 근접해야 합니다. 활성 사용 중에는 값이 일치하지 않을 수 있지만 근접해야 합니다.

문제를 해결하려면 총 수신 바이트와 전송 메시지를 모두 보고, 증가 속도를 비교하고, 값이 같은 속도로 증가하는지 확인해야 합니다. 클러스터링된 피어의 전송 값이 증가하면 디바이스의 수신 값도 같은 속도로 증가해야 합니다.

수신 바이트가 증가하지 않거나 피어에서 전송한 메시지보다 느린 속도로 증가하는 경우 고객 지원에 문의하십시오.

Protocol Bytes Received

Protocol Bytes Received는 수신한 프로토콜 오버헤드의 바이트 수입니다. 여기에는 세션 상태 동기화 메시지의 페이로드를 제외한 모든 것이 포함되어 있습니다.

이 값은 피어에서 전송한 바이트의 수에 근접해야 합니다. 활성 사용 중에는 값이 일치하지 않을 수 있지만 근접해야 합니다.

문제를 해결하려면 수신한 총 바이트를 보고, 프로토콜 데이터와 비교해서 실제 상태 데이터가 얼마나 공유되고 있는지 확인해야 합니다. 프로토콜 데이터가 전송되는 데이터의 상당 부분을 차지하는 경우 최소 동기화 간격을 조정할 수 있습니다.

수신한 프로토콜 바이트가 수신한 총 바이트와 비슷한 속도로 증가하는 경우 고객 지원에 문의하십시오. 수신한 프로토콜 바이트는 수신한 총 바이트의 극히 일부만 차지해야 합니다.

Messages Sent

Messages Sent는 클러스터링된 피어로 전송한 클러스터 동기화 메시지의 수입니다.

이 데이터는 수신한 메시지의 수와 비교해보면 유용합니다. 활성 사용 중에는 값이 일치하지 않을 수 있지만 근접해야 합니다.

문제를 해결하려면 수신 메시지와 전송 메시지를 모두 보고, 증가 속도를 비교하고, 값이 근접한지 확인해야 합니다.

전송한 메시지가 수신한 총 바이트와 비슷한 속도로 증가하는 경우 고객 지원에 문의하십시오.

Bytes Sent

Bytes Sent는 피어로 전송된 클러스터 동기화 메시지를 구성하는 전송된 총 바이트 수입니다.

이 데이터는 수신한 메시지의 수와 비교해보면 유용합니다. 활성 사용 중에는 값이 일치하지 않을 수 있지만 근접해야 합니다. 피어에서 수신한 바이트 수는 이 값에 근접해야 하지만 더 커서는 안 됩니다.

수신한 총 바이트가 전송한 바이트와 같은 속도로 증가하지 않는 경우 고객 지원에 문의하십시오.

Tx Errors

Tx Errors는 시스템이 클러스터링된 피어로 전송할 메시지를 위한 공간을 할당하려고 할 때 발생하는 메모리 할당 실패 수입니다.

이 값은 두 피어에서 모두 항상 0이어야 합니다. 이 값이 0이 아니거나 지속적으로 늘어나는 경우 메모리를 할당할 수 없는 오류가 발생했음을 나타내므로 고객 지원에 문의하십시오.

Tx Overruns

Tx Overruns는 시스템이 메시지를 전송 대기열에 추가하려고 시도하고 실패한 횟수입니다.

이 값은 두 피어에서 모두 항상 0이어야 합니다. 이 값이 0이 아니거나 지속적으로 늘어나면 이는 시스템이 HA 링크 전체에서 충분히 빠르게 전송할 수 없을 정도로 많은 데이터를 공유하고 있음을 나타내는 것입니다.

HA 링크 MTU가 기본값(까지 9918 또는 9922)보다 낮게 설정된 경우 이 값을 올려야 합니다. HA 링크 전체에서 공유하는 데이터의 양을 줄여 이 값의 증가를 막으려면 최소 플로우 수명 주기 및 최소 동기화 간격 설정을 변경할 수 있습니다.

이 값이 지속되거나 계속 늘어나는 경우 고객 지원에 문의하십시오.

Recent Logs

시스템 로그에는 가장 최근에 클러스터링된 동기화 메시지가 표시됩니다. 로그에 ERROR 또는 WARN 메시지가 표시되어서는 안 되며, 연결된 동일한 소켓의 수 등 피어 간에 비교 가능해야 합니다.

그러나 경우에 따라 반대되는 데이터가 표시될 수 있습니다. 예를 들면, 한 피어가 다른 피어에서 연결을 수신한 것으로 보고하면서 다른 IP 주소를 참조하는 경우입니다. 로그는 클러스터링된 상태 공유 연결의 포괄적인 보기 및 연결 내 오류를 제공합니다.

로그에 ERROR 또는 WARN 메시지가 표시되거나, 순수하게 정보용이 아닌 것 같은 메시지가 표시되는 경우 고객 지원에 문의하십시오.

클러스터링된 상태 공유 통계를 보려면

액세스: Admin/Network Admin

1단계 **Devices > Device Management**를 선택합니다.

Device Management 페이지가 나타납니다.

2단계 수정하려는 디바이스 클러스터 옆에 있는 수정 아이콘( )을 클릭합니다.

디바이스 클러스터에 대한 Cluster 페이지가 나타납니다.

3단계 **State Sharing** 섹션에서 통계 보기 아이콘( )을 클릭합니다.

State Sharing Statistics 팝업 창이 나타납니다.

4단계 선택적으로, 클러스터가 디바이스 스택으로 구성된 경우 보려는 **Device**를 선택합니다.

5단계 선택적으로, 통계를 업데이트하려면 **Refresh**를 클릭합니다.

6단계 선택적으로, 각 클러스터링된 디바이스에 대한 최신 데이터 로그를 보려면 **View**를 클릭합니다.

클러스터링된 디바이스 분리

라이센스: 제어

지원되는 디바이스: Series 3

디바이스 클러스터링을 중단하면 활성 디바이스 또는 스택의 구축 기능은 온전히 유지됩니다. 백업 디바이스 또는 스택은 인터페이스 컨피그레이션이 손실되고 활성 디바이스 또는 스택으로 장애 조치됩니다. 단, 해당 인터페이스 컨피그레이션을 활성 상태로 유지하도록 선택하면 백업 디바이스 또는 스택은 정상 운영이 다시 시작됩니다. 클러스터를 중단하면 항상 백업 디바이스에서 패시브 인터페이스의 컨피그레이션이 제거됩니다. 유지 관리 모드의 디바이스는 클러스터 중단 시 정상 운영이 다시 시작됩니다.

클러스터링된 디바이스를 분리하려면

액세스: Admin/Network Admin

1단계 **Devices > Device Management**를 선택합니다.

Device Management 페이지가 나타납니다.

2단계 중단하려는 디바이스 클러스터 옆에 있는 클러스터 중단 아이콘( )을 클릭합니다.

Confirm Break 팝업 창이 나타납니다.

3단계 선택적으로, 백업 디바이스 또는 스택에서 인터페이스 컨피그레이션을 제거하려면 확인란을 선택합니다. 이렇게 하면 관리 인터페이스를 제외한 모든 인터페이스가 관리상 다운됩니다.

4단계 **Yes**를 클릭합니다.

디바이스 클러스터가 분리됩니다.

스태킹된 디바이스 관리

라이센스: 모두

지원되는 디바이스: 3D8140, 3D8200 제품군, 3D8300 제품군, 3D9900

스태킹된 컨피그레이션에서 디바이스를 사용하여 네트워크 세그먼트에서 검사하는 트래픽의 양을 늘릴 수 있습니다. 각 스태킹된 컨피그레이션의 경우 스택의 모든 디바이스에서 하드웨어가 동일해야 합니다. 그러나 스택에 3D9900이 포함되어 있지 않으면 일부 또는 모든 디바이스에 악성코드 스토리지 팩을 설치할 수 있으며, 아무 곳에도 설치하지 않을 수도 있습니다. 또한 디바이스는 다음의 스태킹된 컨피그레이션을 기반으로 동일한 디바이스 제품군에 속해야 합니다.

Series 2 및 81xx 제품군:

- 3D8140 2개
- 3D9900 2개

82xx 제품군:

- 최대 4개의 3D8250
- 3D8260(기본 디바이스 1개 및 보조 디바이스 1개)
- 3D8270(40G 용량의 기본 디바이스 1개 및 보조 디바이스 2개)
- 3D8290(40G 용량의 기본 디바이스 1개 및 보조 디바이스 3개)

83xx 제품군:

- 최대 4개의 3D8350
- 3D8360(40G 용량의 기본 디바이스 1개 및 보조 디바이스 1개)
- 3D8370(40G 용량의 기본 디바이스 1개 및 보조 디바이스 2개)
- 3D8390(40G 용량의 기본 디바이스 1개 및 보조 디바이스 3개)

스태킹된 컨피그레이션에 대한 자세한 내용은 *FireSIGHT 시스템 Installation Guide*를 참조하십시오. 악성코드 스토리지 팩에 대한 자세한 내용은 *FireSIGHT 시스템 Malware Storage Pack Guide*를 참조하십시오.

주의 Cisco에서 제공하지 않은 하드 드라이브를 디바이스에 설치하려고 하지 마십시오. 지원되지 않는 하드 드라이브를 설치하면 디바이스가 손상될 수 있습니다. 악성코드 스토리지 팩 키트는 Cisco **전용**으로만, 그리고 8000 Series 디바이스 **전용**으로만 사용할 수 있습니다. 악성코드 스토리지 팩과 관련하여 도움이 필요하면 고객 지원에 문의하십시오. 자세한 내용은 FireSIGHT 시스템 *Malware Storage Pack Guide*를 참조하십시오.

스태킹된 컨피그레이션을 구축하면 각 스태킹된 디바이스의 리소스를 공유된 단일 컨피그레이션으로 결합합니다.

한 디바이스를 *기본* 디바이스로 지정하고, 여기서 전체 스택에 대한 인터페이스를 구성합니다. 다른 디바이스는 *보조*로 지정합니다. 보조 디바이스는 현재 트래픽을 감지하지 않아야 하며 어떤 인터페이스에서도 링크가 없어야 합니다.

단일 디바이스를 구성할 때와 동일한 방식으로 분석하려는 네트워크 세그먼트에 기본 디바이스를 연결합니다. 자세한 내용은 4-60페이지의 센싱 인터페이스 구성을/를 참조하십시오. *FireSIGHT 시스템 Installation Guide*에 나와 있는 지침에 따라 스태킹된 디바이스 케이블링을 사용하여 보조 디바이스를 기본 디바이스에 연결합니다.

스태킹된 컨피그레이션의 모든 디바이스는 하드웨어가 동일해야 하고, 동일한 소프트웨어 버전을 실행해야 하며, 동일한 라이센스가 있어야 합니다. 디바이스가 NAT 정책의 대상이면 기본 및 보조 디바이스에 모두 동일한 NAT 정책이 적용되어야 합니다. 자세한 내용은 11-7페이지의 NAT 정책 관리을/를 참조하십시오. 방어 센터에서 전체 스택에 업데이트를 적용해야 합니다. 스택의 디바이스 중 하나 이상에서 업데이트가 실패하면 스택은 혼합 버전 상태로 들어갑니다. 혼합 버전 상태의 스택에는 정책이나 업데이트를 적용할 수 없습니다. 이 상황을 해결하려면 스택을 중단하고, 개별 디바이스에서 서로 다른 버전을 제거하고, 개별 디바이스를 업데이트하고, 스태킹된 컨피그레이션을 다시 설정할 수 있습니다. 디바이스를 스태킹한 후에는 전체 스택에 대해서만 동시에 라이센스를 변경할 수 있습니다.

스태킹된 컨피그레이션을 설정한 후에는 모든 디바이스가 단일 공유 컨피그레이션처럼 작동합니다. 기본 디바이스가 실패하면 보조 디바이스로 트래픽이 전달되지 않습니다. 보조 디바이스에서 스태킹 하트비트가 실패했음을 알리는 상태 알림이 생성됩니다. 자세한 내용은 68-1페이지의 상태 모니터링 사용을/를 참조하십시오.

스택의 두 번째 디바이스가 실패하면, 구성 가능한 우회가 활성화된 인라인 집합이 기본 디바이스에서 우회 모드로 전환됩니다. 다른 모든 컨피그레이션에 대해 시스템은 계속해서 실패한 보조 디바이스로 트래픽을 로드 밸런싱합니다. 어떤 경우든 링크 손실을 알리는 상태 알림이 생성됩니다.

몇 가지를 제외하면 디바이스 스택을 구축의 단일 디바이스처럼 사용할 수 있습니다. 클러스터링된 디바이스가 있는 경우 디바이스 클러스터 또는 클러스터링된 쌍의 디바이스를 스태킹할 수 없습니다. 자세한 내용은 4-29페이지의 디바이스 클러스터링을/를 참조하십시오. 디바이스 스택에서는 NAT를 구성할 수 없습니다.

참고 스태킹된 디바이스에서 외부 클라이언트 애플리케이션으로 이벤트 데이터를 스트리밍하는 데 eStreamer를 사용하는 경우 각 디바이스의 데이터를 수집하고 각 디바이스를 똑같이 구성해야 합니다. eStreamer 설정은 스태킹된 디바이스 간에 자동으로 동기화되지 않습니다.

자세한 내용은 다음 절을 참조하십시오.

- 4-45페이지의 디바이스 스택 설정
- 4-47페이지의 디바이스 스택 수정
- 4-47페이지의 스택에서 개별 디바이스 구성
- 4-49페이지의 스태킹된 디바이스 분리

디바이스 스택 설정

라이센스: 모두

지원되는 디바이스: 3D8140, 3D8200 제품군, 3D8300 제품군, 3D9900

파이버 기반 3D9900 2개, 3D8140 디바이스 2개, 3D8250 최대 4개, 3D8260 1개, 3D8270 1개, 3D8290 1개, 3D8350 최대 4개, 3D8360 1개, 3D8270 1개 또는 3D8390 1개를 스태킹하고 단일 공유 컨피그레이션에서 결합된 리소스를 사용함으로써 네트워크 세그먼트에서 검사되는 트래픽의 양을 늘릴 수 있습니다. 시작하기 전에 다음을 수행해야 합니다.

- 어떤 유닛을 기본 디바이스로 할 것인지 결정
- 기본/보조 관계를 지정하기 전에 유닛을 올바르게 케이블링
  케이블링에 대한 자세한 내용은 *FireSIGHT 시스템 Installation Guide*를 참조하십시오.

참고 클러스터링된 디바이스가 있는 경우 디바이스 클러스터 또는 클러스터링된 쌍의 디바이스를 스태킹할 수 없습니다. 그러나 디바이스 스택은 클러스터링할 수 있습니다. 자세한 내용은 4-29페이지의 디바이스 클러스터링을/를 참조하십시오.

디바이스 스택이 설정되면 시스템은 Device Management 페이지에서 디바이스를 단일 디바이스로 취급합니다. 디바이스 스택은 어플라이언스 목록에 스택 아이콘( )을 표시합니다.

방어 센터에서 디바이스 스택의 등록을 제거하면 두 디바이스에서 모두 등록이 제거됩니다. 단일 관리되는 디바이스에서 하듯 방어 센터에서 스태킹된 디바이스를 삭제한 다음, 다른 방어 센터에 스택을 등록할 수 있습니다. 새 방어 센터에서 스태킹된 디바이스 중 하나만 등록하면 전체 스택이 나타납니다. 자세한 내용은 4-27페이지의 디바이스 삭제 및 4-23페이지의 방어 센터에 디바이스 추가을/를 참조하십시오.

디바이스 스택을 설정했으면, 스택을 중단한 후 다시 설정하지 않는 한 기본 디바이스와 보조 디바이스를 변경할 수 없습니다. 그러나 다음은 가능합니다.

- 3D8250 2~3개, 3D8260 1개 또는 3D8270 1개의 기존 스택에 스택당 최대 4개의 3D8250을 보조 디바이스로 추가할 수 있습니다.
- 3D8350 2~3개, 3D8360 1개 또는 3D8370 1개의 기존 스택에 스택당 최대 4개의 3D8350을 보조 디바이스로 추가할 수 있습니다.

추가 디바이스의 경우, 스택의 기본 디바이스에는 케이블된 추가 디바이스에 대한 스태킹 NetMod가 필요합니다. 예를 들어 기본에만 단일 스태킹 NetMod가 있는 3D8260이 있는 경우 이 스택에 또 다른 보조 디바이스를 추가할 수 없습니다. 스태킹된 디바이스 컨피그레이션을 처음 설정한 것과 같은 방식으로 기존 스택에 보조 디바이스를 추가합니다.

스태킹된 디바이스 컨피그레이션을 설정하려면

액세스: Admin/Network Admin

1단계 **Devices > Device Management**를 선택합니다.

Device Management 페이지가 나타납니다.

2단계 **Add** 드롭다운 메뉴에서 **Add Stack**을 클릭합니다.

Add Stack 팝업 창이 나타납니다.

3단계 기본 운영을 위해 케이블링한 디바이스를 **Primary** 드롭다운 목록에서 선택합니다.

참고 기본 디바이스로 케이블링되지 않은 디바이스를 수정하는 경우 이후의 단계를 수행할 수 없습니다.

4단계 **Name** 필드에 스택의 이름을 입력합니다. 영숫자 문자 및 특수 문자를 사용할 수 있지만 +, (,), {, }, #, &, \, <, >, ?, ‘, “ 문자는 유효하지 않으므로 사용할 수 없습니다.

5단계 스태킹할 디바이스를 선택하려면 **Add**를 클릭합니다.

Add Secondary Connection 팝업 창이 나타납니다. 다음 그림에서는 3D8140의 기본 디바이스 전면 보기를 보여줍니다.

6단계 **Slot on Primary Device** 드롭다운 목록에서 기본 디바이스를 보조 디바이스에 연결하는 스태킹 네트워크 모듈을 선택합니다.

7단계 **Secondary Device** 드롭다운 목록에서 보조 운영용으로 케이블링한 디바이스를 선택합니다.

참고 스택의 모든 디바이스는 하드웨어 모델이 동일해야 합니다(예: 3D9900과 3D9900, 3D8140과 3D8140 등). 82xx 제품군 및 83xx 제품군에서 최대 4개의 디바이스를 스태킹할 수 있습니다(기본 디바이스 1개 및 보조 디바이스 3개).

8단계 **Slot on Secondary Device** 드롭다운 목록에서 보조 디바이스를 기본 디바이스에 연결하는 스태킹 네트워크 모듈을 선택합니다.

9단계 **Add**를 클릭합니다.

보조 디바이스가 포함된 상태로 Add Stack 창이 다시 나타납니다.

10단계 선택적으로, 3D8250, 3D8260, 3D8270의 기존 스택, 3D8350, 3D8360 또는 3D8370의 기존 스택에 보조 디바이스를 추가하려면 5~8단계를 반복합니다.

11단계 **Stack**을 클릭합니다.

디바이스 스택이 설정되거나 추가 보조 디바이스가 추가됩니다. 이 프로세스는 시스템 데이터를 동기화하는 데 몇 분 정도 걸립니다.

디바이스 스택 수정

라이센스: 모두

지원되는 디바이스: 3D8140, 3D8200 제품군, 3D8300 제품군, 3D9900

디바이스 스택을 설정한 후 디바이스 컨피그레이션을 변경하면 대부분 전체 스택의 컨피그레이션도 변경됩니다. 어플라이언스 편집기의 Stack 페이지에서, 단일 디바이스의 Device 페이지에서 하듯 스택 컨피그레이션을 변경할 수 있습니다.

스택의 표시 이름을 변경하고, 라이센스를 활성화 및 비활성화하고, 시스템 및 상태 정책을 보고, 자동 애플리케이션 우회를 구성하고, 빠른 경로 규칙을 설정할 수 있습니다.

자세한 내용은 다음 절을 참조하십시오.

- 4-50페이지의 일반 디바이스 설정 수정
- 4-51페이지의 디바이스 라이센스 활성화 및 비활성화
- 4-55페이지의 고급 디바이스 설정 수정

스태킹된 컨피그레이션을 수정하려면

액세스: Admin/Network Admin

1단계 **Devices > Device Management**를 선택합니다.

Device Management 페이지가 나타납니다.

2단계 컨피그레이션을 수정하려는 스태킹된 디바이스 옆에 있는 수정 아이콘( )을 클릭합니다.

해당 디바이스의 Stack 페이지가 나타납니다.

3단계 Stack 페이지의 섹션을 사용하여 마치 단일 디바이스 컨피그레이션에 대해 하듯 스태킹된 컨피그레이션을 변경합니다.

스택에서 개별 디바이스 구성

라이센스: 모두

지원되는 디바이스: 3D8140, 3D8200 제품군, 3D8300 제품군, 3D9900

디바이스 스택을 설정한 후에도 여전히 스택 내에서 한 디바이스에 대해서만 일부 특성을 구성할 수 있습니다. 어플라이언스 편집기의 Devices 페이지에서, 단일 디바이스의 Device 페이지에서 하듯 스택에 구성된 디바이스를 변경할 수 있습니다.

디바이스의 표시 이름을 변경하고, 시스템 설정을 보고, 디바이스를 종료하거나 다시 시작하고, 상태 정보를 보고, 디바이스 관리 설정을 수정할 수 있습니다.

자세한 내용은 다음 절을 참조하십시오.

- 4-50페이지의 일반 디바이스 설정 수정
- 4-52페이지의 디바이스 시스템 설정 수정
- 4-53페이지의 디바이스의 상태 보기
- 4-53페이지의 디바이스 관리 설정 수정

스택의 개별 디바이스를 구성하려면

액세스: Admin/Network Admin

1단계 **Devices > Device Management**를 선택합니다.

Device Management 페이지가 나타납니다.

2단계 컨피그레이션을 수정하려는 스태킹된 디바이스 옆에 있는 수정 아이콘( )을 클릭합니다.

해당 디바이스의 Stack 페이지가 나타납니다.

3단계 **Devices**를 클릭합니다.

Devices 페이지가 나타납니다.

4단계 **Selected Device** 드롭다운 목록에서 수정할 디바이스를 선택합니다.

5단계 Devices 페이지의 섹션을 사용하여 마치 단일 디바이스에 대해 하듯 스태킹된 개별 디바이스를 변경합니다.

스태킹된 디바이스에서 인터페이스 구성

라이센스: 모두

지원되는 디바이스: 3D8140, 3D8200 제품군, 3D8300 제품군, 3D9900

관리 인터페이스를 제외하고, 스택의 기본 디바이스의 Interfaces 페이지에서 스태킹된 디바이스 인터페이스를 구성합니다. 스택에서 아무 디바이스나 선택하여 관리 인터페이스를 구성할 수 있습니다. 자세한 내용은 64-8페이지의 관리 인터페이스 구성을/를 참조하십시오.

Series 3 스태킹된 디바이스의 Interfaces 페이지에는 개별 디바이스에서 찾을 수 있는 하드웨어 및 인터페이스 보기가 포함됩니다. 3D9900의 인터페이스 페이지에는 이러한 보기가 포함되어 있지 않습니다. 자세한 내용은 4-60페이지의 센싱 인터페이스 구성을/를 참조하십시오.

스태킹된 디바이스에서 인터페이스를 구성하려면

액세스: Admin/Network Admin

1단계 **Devices > Device Management**를 선택합니다.

Device Management 페이지가 나타납니다.

2단계 인터페이스를 구성할 스태킹된 디바이스 옆에 있는 수정 아이콘( )을 클릭합니다.

해당 디바이스의 Stack 페이지가 나타납니다.

3단계 **Interfaces**를 클릭합니다.

Interfaces 페이지가 나타납니다.

4단계 **Selected Device** 드롭다운 목록에서 수정할 디바이스를 선택합니다.

5단계 개별 디바이스에서 하듯 인터페이스를 구성합니다. 자세한 내용은 4-60페이지의 센싱 인터페이스 구성을/를 참조하십시오.

스태킹된 디바이스 분리

라이센스: 모두

지원되는 디바이스: 3D8140, 3D8200 제품군, 3D8300 제품군, 3D9900

디바이스에 스태킹된 컨피그레이션을 더 이상 사용할 필요가 없으면 스택을 중단하고 디바이스를 분리할 수 있습니다.

스태킹된 디바이스를 분리하려면

액세스: Admin/Network Admin

1단계 **Devices > Device Management**를 선택합니다.

Device Management 페이지가 나타납니다.

2단계 중단하려는 디바이스 스택 옆에 있는 스택 중단 아이콘( )을 클릭합니다.

Confirm Break 팝업 창이 나타납니다.

팁 스택을 중단하지 않은 채 셋 이상의 3D8250 디바이스로 구성된 스택에서 보조 디바이스를 제거하려면 스택에서 제거 아이콘( )을 클릭합니다. 보조 디바이스를 제거하면, 시스템이 추가 디바이스 없이 운영하도록 스택을 재구성하는 동안 트래픽 검사, 트래픽 플로우 또는 링크 상태가 잠시 중단됩니다.

3단계 **Yes**를 클릭합니다.

디바이스 스택이 분리됩니다.

디바이스 컨피그레이션 수정

라이센스: 모두

어플라이언스 편집기의 Device 페이지에는 자세한 디바이스 컨피그레이션 및 정보가 표시됩니다. 여기에서는 또한 라이센스 활성화 및 비활성화, 디바이스 종료 및 다시 시작, 관리 수정, 빠른 경로 규칙 설정 등 디바이스 컨피그레이션의 일부를 변경할 수 있습니다.

자세한 내용은 다음 절을 참조하십시오.

- 4-50페이지의 일반 디바이스 설정 수정
- 4-51페이지의 디바이스 라이센스 활성화 및 비활성화
- 4-52페이지의 디바이스 시스템 설정 수정
- 4-53페이지의 디바이스의 상태 보기
- 4-53페이지의 디바이스 관리 설정 수정
- 4-54페이지의 고급 디바이스 설정 이해

일반 디바이스 설정 수정

라이센스: 모두

Device 탭의 General 섹션에는 사용자가 변경할 수 있는 다음과 같은 관리되는 디바이스 설정이 표시됩니다.

Name

관리되는 디바이스에 할당된 이름

Transfer Packets

이벤트와 함께 저장하도록 패킷 데이터를 방어 센터로 전송할지 여부를 나타냅니다.

일반 디바이스 설정을 수정하려면

액세스: Admin/Network Admin

1단계 **Devices > Device Management**를 선택합니다.

Device Management 페이지가 나타납니다.

2단계 할당된 이름을 수정할 디바이스 옆에 있는 수정 아이콘( )을 클릭합니다.

해당 디바이스의 Interfaces 페이지가 나타납니다.

3단계 **Device**를 클릭합니다.

Device 페이지가 나타납니다.

팁 스태킹된 디바이스의 경우 어플라이언스 편집기의 Stack 페이지에서 스택에 대해 할당된 디바이스 이름을 수정합니다. 어플라이언스 편집기의 Devices 페이지에서 개별 디바이스에 대해 할당된 디바이스 이름을 수정할 수 있습니다.

4단계 **General** 섹션 옆에 있는 수정 아이콘( )을 클릭합니다.

General 팝업 창이 나타납니다.

5단계 **Name** 필드에 디바이스에 대한 새로운 할당 이름을 입력합니다. 영숫자 문자 및 특수 문자를 사용할 수 있지만 +, (,), {, }, #, &, \, <, >, ?, ‘, “ 문자는 유효하지 않으므로 사용할 수 없습니다.

6단계 패킷 데이터를 이벤트와 함께 방어 센터에 저장하려면 **Transfer Packets** 확인란을 선택합니다. 관리되는 디바이스가 이벤트와 함께 패킷 데이터를 전송하지 않도록 하려면 이 확인란의 선택을 취소합니다.

7단계 **Save**를 클릭합니다.

변경 내용이 저장됩니다. 디바이스 컨피그레이션을 적용해야 변경 사항이 적용됩니다. 자세한 내용은 4-25페이지의 디바이스에 변경 사항 적용을/를 참조하십시오.

디바이스 라이센스 활성화 및 비활성화

라이센스: 모두

지원되는 디바이스: Series 3, 가상, X-Series, ASA FirePOWER

방어 센터에 사용 가능한 라이센스가 있으면 디바이스에서 라이센스를 활성화할 수 있습니다. 다음 사항에 유의하십시오.

- 제어, 악성코드 및 URL 필터링 라이센스에는 보호 라이센스가 필요합니다.
- 가상 디바이스, Cisco NGIPS for Blue Coat X-Series 또는 ASA FirePOWER 디바이스에서는 VPN 라이센스를 활성화할 수 없습니다.
- 가상 디바이스, Cisco NGIPS for Blue Coat X-Series 또는 ASA FirePOWER 디바이스에서 제어 라이센스를 활성화할 수 있지만 이러한 디바이스는 빠른 경로 규칙, 스위칭, 라우팅, 스태킹 또는 클러스터링을 지원하지 **않습니다**. Cisco NGIPS for Blue Coat X-Series는 또한 애플리케이션 또는 사용자 제어도 지원하지 않습니다.
- 클러스터링된 디바이스에 대한 라이센스 설정을 변경할 수 없습니다.
- Series 2 디바이스에는 자동으로 보호 기능이 있으므로(보안 인텔리전스 필터링 제외), 이러한 기능을 비활성화할 수 없으며 다른 라이센스를 Series 2 디바이스에 적용할 수도 없습니다.

자세한 내용은 65-1페이지의 FireSIGHT 시스템 라이센싱을/를 참조하십시오.

디바이스 라이센스를 활성화 또는 비활성화하려면

액세스: Admin/Network Admin

1단계 **Devices > Device Management**를 선택합니다.

Device Management 페이지가 나타납니다.

2단계 라이센스를 활성화 또는 비활성화하려는 디바이스 옆에 있는 수정 아이콘( )을 클릭합니다.

해당 디바이스의 **Interfaces** 탭이 나타납니다.

3단계 **Device**를 클릭합니다.

Devices 탭이 나타납니다.

팁 스태킹된 디바이스의 경우 어플라이언스 편집기의 Stack 페이지에서 스택에 대한 라이센스를 활성화 또는 비활성화합니다.

4단계 **License** 섹션 옆에 있는 수정 아이콘( )을 클릭합니다.

License 팝업 창이 나타납니다.

5단계 다음 옵션을 이용할 수 있습니다.

- 라이센스를 활성화하려면 라이센스 이름 옆에 있는 확인란을 선택합니다.
- 라이센스를 비활성화하려면 라이센스 이름 옆에 있는 확인란을 선택 취소합니다.

6단계 **Save**를 클릭합니다.

변경 내용이 저장됩니다. 디바이스 컨피그레이션을 적용해야 변경 사항이 적용됩니다. 자세한 내용은 4-25페이지의 디바이스에 변경 사항 적용을/를 참조하십시오.

디바이스 시스템 설정 수정

라이센스: 모두

다음 표에 설명된 것처럼, **Device** 탭의 System 섹션에는 시스템 정보의 읽기 전용 테이블이 표시됩니다.

표 4-2 System 섹션 테이블 필드

필드	설명
Model	관리되는 디바이스의 모델 이름 및 번호
Serial	관리되는 디바이스의 섀시의 일련 번호
Time	디바이스의 현재 시스템 시간
Version	관리되는 디바이스에 현재 설치된 소프트웨어의 버전
Policy	관리되는 디바이스에 현재 적용된 시스템 정책에 대한 링크

디바이스를 종료하거나 다시 시작할 수도 있습니다.

참고 X-Series 또는 ASA FirePOWER 디바이스는 FireSIGHT 시스템 사용자 인터페이스로 종료하거나 다시 시작할 수 없습니다. 각 디바이스를 종료하는 방법에 대한 자세한 내용은 *Cisco NGIPS for Blue Coat X-Series Installation Guide* 또는 ASA 설명서를 참조하십시오.

관리되는 디바이스를 종료하고 다시 시작하려면

액세스: Admin/Network Admin

1단계 **Devices > Device Management**를 선택합니다.

Device Management 페이지가 나타납니다.

2단계 시작할 디바이스 옆에 있는 수정 아이콘( )을 클릭합니다.

해당 디바이스의 **Interfaces** 탭이 나타납니다.

3단계 **Device**를 클릭합니다.

Devices 탭이 나타납니다.

팁 스태킹된 디바이스의 경우 어플라이언스 편집기의 Devices 페이지에서 개별 디바이스를 종료하거나 다시 시작합니다.

4단계 디바이스를 종료하려면 디바이스 종료 아이콘( )을 클릭합니다.

5단계 확인 메시지가 표시되면 디바이스를 종료할 것임을 확인합니다.

Device Management 페이지로 돌아갑니다.

6단계 디바이스를 다시 시작하려면 디바이스 다시 시작 아이콘( )을 클릭합니다.

7단계 확인 메시지가 표시되면 디바이스를 다시 시작할 것임을 확인합니다.

디바이스가 다시 시작됩니다.

디바이스 컨피그레이션을 적용해야 변경 사항이 적용됩니다. 자세한 내용은 4-25페이지의 디바이스에 변경 사항 적용을/를 참조하십시오.

디바이스의 상태 보기

라이센스: 모두

Device 탭의 Health 섹션에는 상태 관련 정보가 표시됩니다. 관리되는 디바이스의 현재 상태를 표시하는 아이콘을 볼 수 있습니다. 아이콘을 클릭하여 해당 디바이스의 Health Monitor 페이지로 이동할 수도 있습니다. 자세한 내용은 68-41페이지의 상태 모니터 상태 해석을/를 참조하십시오.

현재 적용된 상태 정책의 읽기 전용 버전을 보려면 **Policy** 링크를 클릭할 수 있습니다. 자세한 내용은 68-30페이지의 상태 정책 수정을/를 참조하십시오.

또한 **Blacklist** 링크를 클릭하여 Health Blacklist 페이지로 이동할 수 있으며, 여기에서 상태 블랙리스트 모듈을 활성화 및 비활성화할 수 있습니다. 자세한 내용은 68-37페이지의 상태 정책 모듈을 블랙리스트에 추가을/를 참조하십시오.

디바이스 관리 설정 수정

라이센스: 모두

Device 탭의 Management 섹션에는 아래에 나열된 원격 관리 정보가 표시됩니다.

호스트

디바이스의 현재 관리 호스트 이름 또는 IP 주소. 이 설정을 사용하여 관리 호스트 이름을 지정하고 가상 IP 주소를 다시 생성할 수 있습니다.

참고 경우에 따라 디바이스의 호스트 이름 또는 IP 주소를 다른 방법(예: 디바이스의 LCD 패널 또는 CLI 사용)으로 수정하는 경우, 아래의 절차를 사용하여 관리하는 방어 센터의 호스트 이름 또는 IP 주소를 수동으로 업데이트해야 할 수 있습니다.

상태

방어 센터와 관리되는 디바이스 간 통신 채널의 상태를 지정합니다.

팁 관리되는 디바이스의 관리를 활성화 또는 비활성화하려면 슬라이더를 클릭할 수 있습니다. 관리를 비활성화하면 Defense Center와 디바이스 간 연결이 차단되지만, Defense Center에서 디바이스가 삭제되지는 **않습니다**. 디바이스를 더 이상 관리하지 않으려면 4-27페이지의 디바이스 삭제을/를 참조하십시오.

디바이스 관리 옵션을 수정하려면

액세스: Admin/Network Admin

1단계 **Devices > Device Management**를 선택합니다.

Device Management 페이지가 나타납니다.

2단계 관리 옵션을 수정할 디바이스 옆에 있는 수정 아이콘( )을 클릭합니다.

해당 디바이스의 **Interfaces** 탭이 나타납니다.

3단계 **Device**를 클릭합니다.

Devices 탭이 나타납니다.

팁 스태킹된 디바이스의 경우 어플라이언스 편집기의 Devices 페이지에서 개별 디바이스의 관리 옵션을 수정합니다.

4단계 **Management** 섹션 옆에 있는 수정 아이콘( )을 클릭합니다.

Management 팝업 창이 나타납니다.

5단계 관리 호스트의 이름 또는 IP 주소를 **Host** 필드에 입력합니다.

6단계 **Save**를 클릭합니다.

변경 내용이 저장되었습니다. 디바이스 컨피그레이션을 적용해야 변경 사항이 적용됩니다. 자세한 내용은 4-25페이지의 디바이스에 변경 사항 적용을/를 참조하십시오.

고급 디바이스 설정 이해

라이센스: 모두

지원되는 디바이스: 기능에 따라 다름

다음 표에 설명된 것처럼, **Device** 탭의 Advanced 섹션에는 고급 컨피그레이션 설정의 테이블이 표시됩니다.

표 4-3 Advanced 섹션 테이블 필드

필드	설명	지원되는 장치
Application Bypass	디바이스에서 Automatic Application Bypass의 상태	Series 2, Series 3, 가상
Bypass Threshold	Automatic Application Bypass 임계값(밀리초 단위)	Series 2, Series 3, 가상
Inspect Local Router Traffic	디바이스가 라우티드 인터페이스에서 수신된, 스스로를 향하는 트래픽(예: ICMP, DHCP 및 OSPF 트래픽)을 검사할지 여부	Series 3
Fast-Path Rules	디바이스에서 생성된 빠른 경로 규칙의 수	8000 Series, 3D9900

이러한 설정을 수정하려면 Advanced 섹션을 사용할 수 있습니다. 자세한 내용은 다음 절을 참조하십시오.

- 4-55페이지의 자동 애플리케이션 바이패스
- 4-55페이지의 고급 디바이스 설정 수정
- 4-56페이지의 빠른 경로 규칙 구성

자동 애플리케이션 바이패스

라이센스: 모두

AAB(Automatic Application Bypass) 기능은 인터페이스를 통과하는 패킷 처리에 허용되는 시간을 제한하며, 시간이 초과되는 경우 패킷이 탐지를 우회하도록 허용합니다. 이 기능은 모든 구축에서 작동하지만, 인라인 구축에서 가장 효과적입니다.

패킷 처리 지연과 패킷 레이턴시에 대한 네트워크 허용 범위의 균형을 맞추십시오. Snort 내 오작동 또는 디바이스 컨피그레이션 오류 때문에 트래픽 처리 시간이 지정된 임계값을 초과하면 AAB는 실패 10분 내에 Snort가 다시 시작되도록 하며, 과도한 처리 시간의 원인을 조사하기 위해 분석할 수 있는 문제 해결 데이터를 생성합니다.

버전 5.4.1 이상에서 AAB 옵션의 기본 동작은 다음과 같이 디바이스에 따라 다릅니다.

- Series 3: 끄기
- Series 2 및 가상: 켜기
- ASA FirePOWER: 지원되지 않음
- X-Series: 지원되지 않음

5.3 이전 버전에서 업그레이드하는 경우 기존 설정이 유지됩니다. 옵션이 선택된 경우 우회 임계값을 변경할 수 있습니다. 기본 설정은 3000ms(밀리초)입니다. 유효한 범위는 250~60,000ms입니다.

일반적으로 레이턴시 임계값이 초과된 후 빠른 경로 패킷에 대한 침입 정책에서 Rule Latency Thresholding을 사용합니다. Rule Latency Thresholding은 엔진을 종료하지 않으며 문제 해결 데이터를 생성하지도 않습니다. 자세한 내용은 18-12페이지의 패킷 및 침입 규칙 레이턴시 임계값 구성을/를 참조하십시오.

참고 AAB는 단일 패킷을 처리하는 데 시간이 너무 많이 사용되는 경우에만 활성화됩니다. AAB가 활성화되면 시스템은 모든 Snort 프로세스를 종료합니다.

탐지가 우회되면 디바이스는 상태 모니터링 알림을 생성합니다. 상태 모니터링 알림에 대한 자세한 내용은 68-41페이지의 상태 모니터 사용을/를 참조하십시오.

Automatic Application Bypass 활성화 및 우회 임계값 설정에 대한 자세한 내용은 4-55페이지의 고급 디바이스 설정 수정을/를 참조하십시오.

고급 디바이스 설정 수정

라이센스: 모두

지원되는 디바이스: 기능에 따라 다름

Automatic Application Bypass 및 Inspect Local Router Traffic 설정을 수정하려면 **Devices** 탭의 Advanced 섹션을 사용할 수 있습니다. 또한 4-56페이지의 빠른 경로 규칙 구성에 설명된 대로 빠른 경로 규칙을 구성할 수 있습니다.

다음에 유의하십시오.

- 빠른 경로 규칙은 8000 Series 및 3D9900 디바이스에서만 구성할 수 있습니다.
- **Inspect Local Router Traffic**은 Series 3 디바이스에서만 구성할 수 있습니다.

고급 디바이스 설정을 수정하려면

액세스: Admin/Network Admin

1단계 **Devices > Device Management**를 선택합니다.

Device Management 페이지가 나타납니다.

2단계 고급 디바이스 설정을 수정하려는 디바이스 옆에 있는 수정 아이콘( )을 클릭합니다.

해당 디바이스의 **Interfaces** 탭이 나타납니다.

3단계 **Device**를 클릭합니다.

Devices 탭이 나타납니다.

팁 스태킹된 디바이스의 경우 어플라이언스 편집기의 Stack 페이지에서 스택에 대한 고급 디바이스 설정을 수정합니다.

4단계 **Advanced** 섹션 옆에 있는 수정 아이콘( )을 클릭합니다.

Advanced 팝업 창이 나타납니다.

5단계 선택적으로, 네트워크가 레이턴시에 민감한 경우 **Automatic Application Bypass**를 선택합니다. Automatic Application Bypass는 인라인 구축에서 가장 유용합니다. 자세한 내용은 4-55페이지의 자동 애플리케이션 바이패스을/를 참조하십시오.

6단계 Automatic Application Bypass 옵션을 선택한 경우 ms(밀리초) 단위로 **Bypass Threshold**를 입력할 수 있습니다. 기본 설정은 3000ms이고 유효 범위는 250~60,000ms입니다.

7단계 선택적으로, 라우터로 구축 시 예외 트래픽을 검사하려면 **Inspect Local Router Traffic** 확인란을 선택합니다.

8단계 선택적으로, 빠른 경로 규칙을 구성합니다. 자세한 내용은 4-56페이지의 빠른 경로 규칙 구성을/를 참조하십시오.

9단계 **Save**를 클릭합니다.

변경 내용이 저장되었습니다. 디바이스 컨피그레이션을 적용해야 변경 사항이 적용됩니다. 자세한 내용은 4-25페이지의 디바이스에 변경 사항 적용을/를 참조하십시오.

빠른 경로 규칙 구성

라이센스: 모두

지원되는 디바이스: 8000 Series, 3D9900

추가 검사 없이 디바이스를 직접 통과하도록 트래픽을 전송하려면 빠른 경로 규칙을 생성할 수 있습니다. 빠른 경로 규칙은 분석할 필요가 없는 트래픽이 디바이스를 우회하도록 전환합니다. 빠른 경로 규칙은 트래픽을 빠른 경로(인터페이스 외부)로 전송하거나 심층 분석을 위해 계속해서 디바이스로 이동하도록 허용합니다. 트래픽을 위한 올바른 경로를 결정하는 속도가 이 기능의 장점입니다. 빠른 경로 규칙은 하드웨어 수준에서 작동하므로 패킷에 대한 제한된 정보만 결정합니다.

자세한 내용은 다음 절을 참조하십시오.

- 4-57페이지의 IPv4 빠른 경로 규칙 추가
- 4-58페이지의 IPv6 빠른 경로 규칙 추가
- 4-60페이지의 Fast-Path 규칙 삭제

IPv4 빠른 경로 규칙 추가

라이센스: 모두

지원되는 디바이스: 8000 Series, 3D9900

빠른 경로 규칙은 트래픽을 빠른 경로(인터페이스 외부)로 전송하거나 심층 분석을 위해 디바이스로 전송합니다. 빠른 경로로 전환하고 검사하지 않을 IPv4 트래픽을 선택하려면 다음 기준을 사용할 수 있습니다.

- initiator 또는 responder IP 주소나 CIDR 블록
- 프로토콜
- TCP 또는 UDP 프로토콜의 경우 initiator 또는 responder 포트
- VLAN ID
- 양방향 옵션

가장 바깥쪽 ID가 빠른 경로 규칙에 사용됩니다.

팁 기존의 빠른 경로 규칙을 수정하려면 규칙 옆에 있는 수정 아이콘()을 클릭합니다.

IPv4 빠른 경로 규칙을 작성 또는 수정하려면

액세스: Admin/Network Admin

1단계 **Devices > Device Management**를 선택합니다.

Device Management 페이지가 나타납니다.

2단계 빠른 경로 규칙을 추가하려는 디바이스 옆에 있는 수정 아이콘()을 클릭합니다.

해당 디바이스의 **Interfaces** 탭이 나타납니다.

3단계 **Device**를 클릭합니다.

Devices 탭이 나타납니다.

4단계 **Advanced** 섹션 옆에 있는 수정 아이콘()을 클릭합니다.

Advanced 팝업 창이 나타납니다.

5단계 빠른 경로 규칙을 추가하려면 **New IPv4 Rule**을 클릭합니다.

New IPv4 Rule 팝업 창이 나타납니다.

6단계 **Domain** 드롭다운 목록에서 인라인 집합 또는 수동 보안 영역을 선택합니다. 자세한 내용은 5-1페이지의 IPS 디바이스 설정을/를 참조하십시오.

7단계 추가 분석을 위해 패킷을 우회해야 하는 initiator 또는 responder의 IP 주소를 지정하려면 **Initiator** 및 **Responder** 필드에서 CIDR 표기법을 사용합니다.

규칙은 지정된 initiator에서 오는 패킷 또는 지정된 responder로 가는 패킷을 매칭합니다. FireSIGHT 시스템에서 CIDR 표기법을 사용하는 방법에 대한 자세한 내용은 1-19페이지의 IP 주소 표기 규칙을/를 참조하십시오.

8단계 선택적으로, **Protocol** 드롭다운 목록에서 규칙을 적용할 프로토콜을 선택합니다. 목록의 모든 프로토콜에서 오는 트래픽을 매칭하려면 **All**을 선택합니다.

9단계 선택적으로, 8단계에서 TCP 또는 UDP 프로토콜을 선택한 경우 포트를 지정하려면 **Initiator Port** 및 **Responder Port** 필드에 initiator 및 responder 포트를 입력합니다.

팁 각 규칙에서 쉼표로 구분된 포트 번호 목록을 입력할 수 있습니다. IPv4 빠른 경로 규칙에는 포트 범위를 사용할 수 없습니다. 빈 포트 값은 **Any**로 취급됩니다.

Bidirectional 옵션도 선택하는 경우 필터 기준이 해당 initiator 포트에서 해당 responder 포트로 이동하는 패킷으로 좁혀집니다.

10단계 선택적으로, **VLAN** 필드에 VLAN ID를 입력합니다.

규칙은 해당 VLAN에 대한 트래픽만 매칭합니다. 빈 VLAN 값은 **Any**로 취급됩니다.

11단계 선택적으로, 지정된 initiator와 responder IP 주소 간에 이동하는 모든 트래픽을 필터링하려면 **Bidirectional** 옵션을 선택합니다. 지정된 initiator IP 주소에서 지정된 responder IP 주소로 이동하는 트래픽만 필터링하려면 이 옵션을 선택하지 않습니다.

12단계 **Save**를 클릭합니다.

Advanced 팝업 창의 Fast-Path Rules 아래에 규칙이 추가됩니다. 규칙이 추가되더라도 규칙을 저장하려면 **Save**를 다시 클릭해야 합니다. 디바이스 컨피그레이션을 적용해야 변경 사항이 적용됩니다. 자세한 내용은 4-25페이지의 디바이스에 변경 사항 적용을/를 참조하십시오.

IPv6 빠른 경로 규칙 추가

라이센스: 모두

지원되는 디바이스: Series 3, 3D9900

빠른 경로 규칙은 트래픽을 빠른 경로(인터페이스 외부)로 전송하거나 심층 분석을 위해 디바이스로 전송합니다. 빠른 경로로 전환하고 검사하지 않을 IPv6 트래픽을 선택하려면 다음 기준을 사용할 수 있습니다.

- initiator 또는 responder IP 주소나 주소 블록
- 프로토콜
- TCP 또는 UDP 프로토콜의 경우 initiator 또는 responder 포트
- VLAN ID
- 양방향 옵션

가장 바깥쪽 VLAN ID가 빠른 경로 규칙에 사용됩니다.

팁 기존의 빠른 경로 규칙을 수정하려면 규칙 옆에 있는 수정 아이콘()을 클릭합니다.

IPv6 빠른 경로 규칙을 추가하려면

액세스: Admin/Network Admin

1단계 **Devices > Device Management**를 선택합니다.

Device Management 페이지가 나타납니다.

2단계 빠른 경로 규칙을 추가하려는 디바이스 옆에 있는 수정 아이콘()을 클릭합니다.

해당 디바이스의 **Interfaces** 탭이 나타납니다.

3단계 **Device**를 클릭합니다.

Devices 탭이 나타납니다.

4단계 **Advanced** 섹션 옆에 있는 수정 아이콘을 클릭합니다.

Advanced 팝업 창이 나타납니다.

5단계 빠른 경로 규칙을 추가하려면 **New IPv6 Rule**을 클릭합니다.

New IPv6 Rule 팝업 창이 나타납니다. Initiator 및 responder 필드는 고정되어 있으며, 임의의 initiator 또는 responder에서 오는 IPv6 패킷에 필터가 적용됨을 나타냅니다.

6단계 **Domain** 드롭다운 목록에서 인라인 집합 또는 수동 보안 영역을 선택합니다. 자세한 내용은 5-1페이지의 IPS 디바이스 설정을/를 참조하십시오.

7단계 추가 분석을 위해 패킷을 우회해야 하는 initiator 또는 responder의 IP 주소에 대해 **Initiator** 및 **Responder** 필드에 주소 블록을 지정하려면 IP 주소를 입력하거나 IPv6 접두사 길이 표기법을 사용합니다.

규칙은 지정된 initiator에서 오는 패킷 또는 지정된 responder로 가는 패킷을 매칭합니다. FireSIGHT 시스템에서 IPv6 접두사 길이 표기법을 사용하는 방법에 대한 자세한 내용은 1-19페이지의 IP 주소 표기 규칙을/를 참조하십시오.

8단계 선택적으로, **Protocol** 드롭다운 목록에서 규칙을 적용할 프로토콜을 선택합니다. 목록의 모든 프로토콜에서 오는 트래픽을 매칭하려면 **All**을 선택합니다.

빠른 경로 규칙은 선택한 프로토콜의 패킷만 매칭합니다.

9단계 선택적으로, 7단계에서 TCP 또는 UDP 프로토콜을 선택한 경우 포트를 지정하려면 **Initiator Port** 및 **Responder Port** 필드에 initiator 및 responder 포트를 입력합니다.

팁 각 규칙에서 쉼표로 구분된 포트 번호 목록을 입력할 수 있습니다. IPv6 빠른 경로 규칙에는 포트 범위를 사용할 수 없습니다. 빈 포트 값은 **Any**로 취급됩니다.

10단계 선택적으로, **VLAN** 필드에 VLAN ID를 입력합니다.

규칙은 해당 VLAN에 대한 트래픽만 매칭합니다. 빈 VLAN 값은 **Any**로 취급됩니다.

11단계 선택적으로, 지정된 initiator와 responder 포트 간에 이동하는 모든 트래픽을 필터링하려면 **Bidirectional**을 선택합니다. 규칙이 해당 initiator 포트에서 오는 패킷 또는 해당 responder 포트로 가는 패킷만 매칭하도록 지정하려면 이 옵션을 선택하지 않습니다.

12단계 **Save**를 클릭합니다.

Advanced 팝업 창의 Fast-Path Rules 아래에 규칙이 추가됩니다.

13단계 Advanced 팝업 창에서 **Save**를 클릭합니다.

규칙이 저장됩니다. 디바이스 컨피그레이션을 적용해야 변경 사항이 적용됩니다. 자세한 내용은 4-25페이지의 디바이스에 변경 사항 적용을/를 참조하십시오.

Fast-Path 규칙 삭제

라이센스: 모두

지원되는 디바이스: 8000 Series, 3D9900

다음 절차에서는 IPv4 또는 IPv6 빠른 경로 규칙을 삭제하는 방법에 대해 설명합니다.

빠른 경로 규칙을 삭제하려면

액세스: Admin/Network Admin

1단계 **Devices > Device Management**를 선택합니다.

Device Management 페이지가 나타납니다.

2단계 빠른 경로 규칙을 삭제하려는 디바이스 옆에 있는 수정 아이콘( )을 클릭합니다.

해당 디바이스의 **Interfaces** 탭이 나타납니다.

3단계 **Device**를 클릭합니다.

Devices 탭이 나타납니다.

4단계 **Advanced** 섹션 옆에 있는 수정 아이콘( )을 클릭합니다.

Advanced 팝업 창이 나타납니다.

5단계 삭제하려는 빠른 경로 규칙 옆에 있는 삭제 아이콘( )을 클릭합니다.

6단계 확인 메시지가 표시되면 규칙을 삭제할 것임을 확인합니다.

Advanced 팝업 창에서 규칙이 제거됩니다.

7단계 **Save**를 클릭합니다.

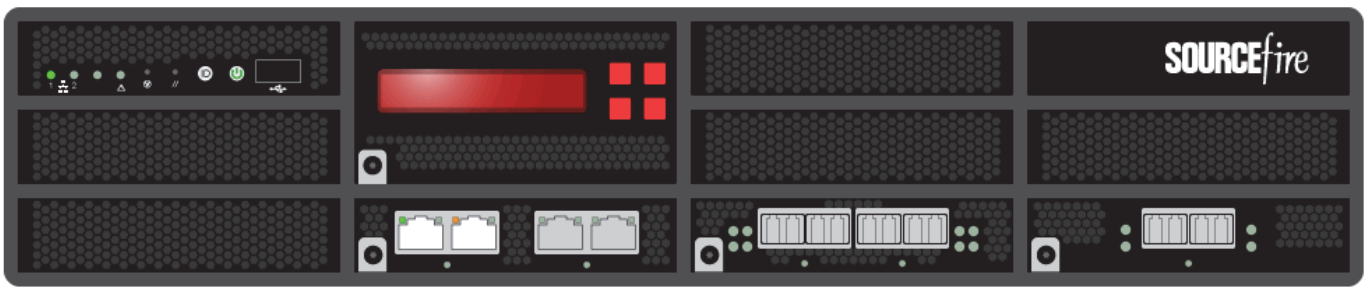
변경 내용이 저장되었습니다. 디바이스 컨피그레이션을 적용해야 변경 사항이 적용됩니다. 자세한 내용은 4-25페이지의 디바이스에 변경 사항 적용을/를 참조하십시오.

센싱 인터페이스 구성

라이센스: 모두

FireSIGHT 시스템 구축에 따라 어플라이언스 편집기의 Interfaces 페이지에서 관리되는 디바이스의 센싱 인터페이스를 구성할 수 있습니다.

Interfaces 페이지의 상단에는 관리되는 Series 3 디바이스의 물리적 하드웨어가 표시됩니다. Series 2, 가상 디바이스, Cisco NGIPS for Blue Coat X-Series 및 ASA FirePOWER 디바이스에는 물리적 하드웨어 보기가 없습니다. 다음 그림에서는 3D8250의 하드웨어 보기를 보여줍니다.



다음 표에서는 물리적 하드웨어 보기를 사용하는 방법에 대해 설명합니다.

표 4-4 하드웨어 보기 사용

목적	가능한 작업
네트워크 모듈의 유형, 부품 번호 및 일련 번호 보기	네트워크 모듈의 하단 왼쪽 구석에 있는 어두운 원 위로 커서를 이동합니다.
인터페이스 테이블 보기에서 인터페이스 선택	인터페이스를 클릭합니다.
인터페이스 편집기 열기	인터페이스를 두 번 클릭합니다.
인터페이스의 이름, 인터페이스의 유형, 인터페이스에 링크가 있는지 여부, 인터페이스의 속도 설정, 인터페이스가 현재 우회 모드에 있는지 여부 등을 보기	커서를 인터페이스 위로 이동합니다.
오류 또는 경고에 대한 세부사항 보기	네트워크 모듈에서 영향을 받는 포트 위로 커서를 이동합니다.

Series 3 하드웨어 보기 아래에 있는 인터페이스 테이블 보기에는 디바이스에서 사용할 수 있는 모든 인터페이스가 나열됩니다. 테이블에는 구성된 모든 인터페이스를 보기 위해 사용할 수 있는 확장 가능한 탐색 트리가 포함되어 있습니다. 하위 구성 요소를 숨기거나 보려면 인터페이스 옆에 있는 화살표 아이콘을 클릭하여 인터페이스를 확장하거나 축소할 수 있습니다. 인터페이스 테이블 보기에서는 또한 다음 표에 설명된 대로 각 인터페이스에 대한 요약된 정보를 제공합니다.
8000 Series 디바이스에만 MAC Address 및 IP Address 열이 표시됩니다. 자세한 내용은 다음 표를 참조하십시오.

표 4-5 인터페이스 테이블 보기 필드

필드	설명
Name	각 인터페이스 유형은 해당 유형 및 링크 상태(해당되는 경우)를 나타내는 고유한 아이콘으로 표시됩니다. 이름 또는 아이콘 위로 포인터를 이동하면 툴팁에서 인터페이스 유형, 속도 및 이중 모드(해당하는 경우)를 볼 수 있습니다. 인터페이스 아이콘에 대해서는 4-62 페이지의 표 4-6에 설명되어 있습니다. 아이콘은 인터페이스의 현재 링크 상태(다음의 세 가지 중 하나)를 나타내기 위해 배지 표기 규칙을 사용합니다. • 오류() • 장애() • 사용할 수 없음() 논리적 인터페이스의 링크 상태는 상위 물리적 인터페이스와 동일합니다. Cisco NGIPS for Blue Coat X-Series 및 ASA FirePOWER 디바이스는 링크 상태를 표시하지 않습니다. 비활성화된 인터페이스는 반투명 아이콘으로 표시됩니다. 아이콘 오른쪽에 나타나는 인터페이스 이름은 자동으로 생성됩니다. 단, 사용자가 정의하는 하이브리드 및 ASA FirePOWER 인터페이스는 예외입니다. ASA FirePOWER 인터페이스에 대해 시스템은 활성화되고 명명되고 링크가 있는 인터페이스만 표시합니다. 물리적 인터페이스는 물리적 인터페이스의 이름을 표시합니다. 논리적 인터페이스는 물리적 인터페이스의 이름 및 할당된 VLAN 태그를 표시합니다. 여러 보안 컨텍스트가 있는 경우 ASA FirePOWER 인터페이스는 보안 컨텍스트의 이름 및 인터페이스의 이름을 표시합니다. 보안 컨텍스트가 하나뿐이면 시스템은 인터페이스의 이름만 표시합니다.

표 4-5 인터페이스 테이블 보기 필드(계속)

필드	설명
Security Zone	인터페이스가 할당된 보안 영역. 보안 영역을 추가 또는 수정하려면 수정 아이콘()을 클릭합니다.
Used by	인터페이스가 할당된 인라인 집합, 가상 스위치 또는 가상 라우터. ASA FirePOWER 디바이스는 Used by 열을 표시하지 않습니다.
MAC Address	스위치드 및 라우티드 기능에 대해 활성화되었을 때 인터페이스에 대해 표시되는 MAC 주소. 가상 디바이스의 경우, 디바이스에 구성된 네트워크 어댑터를 Interfaces 페이지에 나타나는 인터페이스에 매칭할 수 있도록 MAC 주소가 표시됩니다. Cisco NGIPS for Blue Coat X-Series 및 ASA FirePOWER 디바이스는 MAC 주소를 표시하지 않습니다.
IP Addresses	인터페이스에 할당된 IP 주소. 활성 여부를 확인하려면 IP 주소 위로 포인터를 이동합니다. 비활성 IP 주소는 회색으로 표시됩니다. ASA FirePOWER 디바이스는 IP 주소를 표시하지 않습니다.

표 4-6 인터페이스 아이콘 유형 및 설명

아이콘	인터페이스 유형	참조 섹션
	물리적(Physical) — 구성되지 않은 물리적 인터페이스.	—
	수동(Passive) — 패시브 구축에서 트래픽을 분석하도록 구성된 센싱 인터페이스.	5-2페이지의 패시브 인터페이스 구성
	인라인(Inline) — 인라인 구축에서 트래픽을 처리하도록 구성된 센싱 인터페이스.	5-3페이지의 인라인 인터페이스 구성
	스위치드(Switched) — Layer 2 구축에서 트래픽을 전환하도록 구성된 인터페이스.	6-2페이지의 스위치드 인터페이스 컨피그레이션
	라우티드(Routed) — Layer 3 구축에서 트래픽을 라우팅하도록 구성된 인터페이스.	7-1페이지의 라우티드 인터페이스 구성
	HA — 디바이스 간 이중 통신 채널 역할을 하도록 디바이스의 클러스터링된 쌍의 각 멤버에 대해 구성된 인터페이스. 고가용성 링크 인터페이스라고도 함.	4-63페이지의 HA 링크 인터페이스 구성
	집계(Aggregate) — 단일 논리적 링크로서 구성된 여러 물리적 인터페이스.	8-1페이지의 집계 인터페이스 설정
	집계 스위치드(Aggregate Switched) — Layer 2 구축에서 단일 논리적 링크로서 구성된 여러 물리적 인터페이스.	8-5페이지의 스위치드 인터페이스 추가
	집계 라우티드(Aggregate Routed) — Layer 3 구축에서 단일 논리적 링크로서 구성된 여러 물리적 인터페이스.	8-7페이지의 집계 라우티드 인터페이스 추가

표 4-6 인터페이스 아이콘 유형 및 설명(계속)

아이콘	인터페이스 유형	참조 섹션
	하이브리드(Hybrid) — 가상 라우터와 가상 스위치 간 트래픽을 연결하도록 구성된 논리적 인터페이스.	9-1페이지의 논리적 하이브리드 인터페이스 추가
	ASA FirePOWER — ASA FirePOWER 모듈이 설치된 ASA 디바이스에 구성된 인터페이스.	4-65페이지의 Cisco ASA with FirePOWER Services 인터페이스 관리

FirePOWER 관리되는 디바이스에는 총 1024개의 인터페이스만 구성할 수 있습니다.

참고 ASA FirePOWER 디바이스를 SPAN 포트 모드에서 구축한 경우 방어 센터에는 ASA 인터페이스가 표시되지 않습니다.

디바이스에서 인터페이스를 구성할 수 있는 여러 방법에 대한 자세한 내용은 다음 절을 참조하십시오.

- 4-63페이지의 HA 링크 인터페이스 구성
- 4-64페이지의 센싱 인터페이스 MTU 구성
- 4-65페이지의 Cisco ASA with FirePOWER Services 인터페이스 관리
- 4-66페이지의 인터페이스 비활성화
- 4-66페이지의 이중 연결 로깅 방지
- 5-1페이지의 IPS 디바이스 설정
- 6-1페이지의 가상 스위치 설정
- 7-1페이지의 가상 라우터 설정
- 8-1페이지의 집계 인터페이스 설정
- 9-1페이지의 하이브리드 인터페이스 설정

HA 링크 인터페이스 구성

라이센스: 모두

지원되는 디바이스: Series 3

디바이스 클러스터를 설정했으면 HA(고가용성) 링크 인터페이스처럼 물리적 인터페이스를 구성할 수 있습니다. 이 링크는 클러스터링된 디바이스 간 상태 정보 공유를 위한 이중 통신 채널 역할을 합니다. 한 디바이스에서 HA 링크 인터페이스를 구성하면 두 번째 디바이스에서도 인터페이스가 자동으로 구성됩니다. 동일한 브로드캐스트 도메인에서는 두 HA 링크를 모두 구성해야 합니다. 자세한 내용은 4-29페이지의 디바이스 클러스터링을/를 참조하십시오.

동적 NAT는 동적 할당 IP 주소 및 포트에 의존하여 다른 IP 주소 및 포트에 매핑합니다. HA 링크가 없으면 이러한 매핑은 장애 조치 시 손실되어, 클러스터의 현재 활성 디바이스를 통해 라우팅될 때 변환된 모든 연결이 실패하게 됩니다.

주의 MTU(최대 전송 단위)를 변경하면 디바이스의 트래픽이 중단됩니다. MTU 설정 가능 범위는 FireSIGHT 시스템 디바이스 모델 및 인터페이스 유형에 따라 달라질 수 있습니다. 자세한 내용은 4-64페이지의 센싱 인터페이스 MTU 구성을/를 참조하십시오.

HA 링크 인터페이스를 구성하려면

액세스: Admin/Network Admin

1단계 **Devices > Device Management**를 선택합니다.

Device Management 페이지가 나타납니다.

2단계 HA 링크 인터페이스를 구성하려는 클러스터링된 디바이스 옆에 있는 수정 아이콘( )을 클릭합니다.

해당 디바이스의 **Interfaces** 탭이 나타납니다.

3단계 HA 링크 인터페이스로 구성하려는 인터페이스 옆에 있는 수정 아이콘( )을 클릭합니다.

Edit Interface 팝업 창이 나타납니다.

4단계 **HA Link**를 클릭하여 HA 링크 옵션을 표시합니다.

5단계 HA 링크 인터페이스에서 링크를 제공하도록 하려면 **Enabled** 확인란을 선택합니다.

확인란의 선택을 취소할 경우 인터페이스는 비활성화되고 관리상 다운됩니다.

6단계 **Mode** 드롭다운 목록에서 링크 모드를 지정하는 옵션을 선택하거나 **Autonegotiation**을 선택하여 인터페이스에서 속도 및 양방향 설정 자동 협상이 구성되도록 지정합니다.

7단계 **MDI/MDIX** 드롭다운 목록에서 옵션을 선택하여 인터페이스가 MDI(medium dependent interface), MDIX(medium dependent interface crossover) 또는 Auto-MDIX를 위해 구성되었는지 여부를 지정합니다.

일반적으로 MDI/MDIX는 **Auto-MDIX**로 설정됩니다. 그러면 MDI와 MDIX 간 스위칭을 자동으로 처리하여 링크를 확보합니다.

8단계 **MTU** 필드에 MTU를 입력합니다. 이는 허용되는 최대 크기 패킷을 나타냅니다.

MTU 설정 가능 범위는 FireSIGHT 시스템 디바이스 모델 및 인터페이스 유형에 따라 달라질 수 있습니다. 자세한 내용은 4-64페이지의 센싱 인터페이스 MTU 구성을/를 참조하십시오.

9단계 **Save**를 클릭합니다.

변경 내용이 저장되었습니다. 디바이스 컨피그레이션을 적용해야 변경 사항이 적용됩니다. 자세한 내용은 4-25페이지의 디바이스에 변경 사항 적용을/를 참조하십시오.

센싱 인터페이스 MTU 구성

라이센스: 모두

인터페이스 또는 인라인 집합에서 MTU(최대 전송 단위)를 변경하면 다음 기능이 영향을 받을 수 있습니다.

- 애플리케이션 인식 및 제어, URL 필터링, 침입 탐지 및 방지, 연결 로깅을 비롯한 트래픽 검사
- 스위칭, 라우팅 및 관련 기능을 비롯한 트래픽 플로우
- 링크 상태

네트워크 트래픽 중단 방법 및 기간은 인터페이스 유형 및 디바이스가 구성되고 구축된 방법에 따라 다릅니다.

Cisco NGIPS for Blue Coat X-Series의 경우 Cisco NGIPS for Blue Coat X-Series CLI를 사용하여 인터페이스 MTU를 구성합니다. 자세한 내용은 Cisco NGIPS for Blue Coat X-Series *Installation Guide*를 참조하십시오.

참고 시스템은 구성된 MTU 값에서 자동으로 18바이트를 잘라내므로 1298 아래의 값은 최소 IPv6 MTU 설정인 1280을 준수하지 못하며 594 아래의 값은 최소 IPv4 MTU 설정인 576을 준수하지 못합니다. 예를 들면 시스템은 구성된 값 576을 자동으로 558로 자릅니다.

다음 표에는 관리되는 디바이스에 대한 MTU 컨피그레이션 범위가 나열되어 있습니다.

표 4-7 디바이스별 MTU 범위

모델 디바이스	MTU 범위
Series 2(3D6500, 3D9900 제외)	576-1518(모든 인터페이스, 인라인 집합)
3D6500, 3D9900, 가상	576-9018(모든 인터페이스, 인라인 집합)
Series 3	576-9234(관리 인터페이스) 576-10172(인라인 집합) 576-9922(기타 모두)

Cisco ASA with FirePOWER Services 인터페이스 관리

라이센스: 보호

지원되는 디바이스: ASA FirePOWER

ASA FirePOWER 인터페이스를 수정할 경우 FireSIGHT 방어 센터에서 인터페이스의 보안 영역만 구성할 수 있습니다. 자세한 내용은 3-38페이지의 보안 영역 작업을/를 참조하십시오.

ASA 관련 소프트웨어 및 CLI를 사용하면 ASA FirePOWER 인터페이스를 완전히 구성할 수 있습니다. ASA FirePOWER 디바이스를 수정하면서 다중 컨텍스트 모드에서 단일 컨텍스트 모드로(또는 그 반대로) 전환하면 디바이스의 모든 인터페이스 이름이 변경됩니다. 업데이트된 ASA FirePOWER 인터페이스 이름을 사용하려면 모든 FireSIGHT 시스템 보안 영역, 상관관계 규칙 및 관련 컨피그레이션을 반드시 다시 구성해야 합니다. ASA FirePOWER 인터페이스 컨피그레이션에 대한 자세한 내용은 ASA 설명서를 참조하십시오.

참고 ASA FirePOWER 인터페이스의 유형을 변경할 수 없으며, FireSIGHT 방어 센터에서 인터페이스를 비활성화할 수도 없습니다.

ASA FirePOWER 인터페이스를 수정하려면

액세스: Admin/Network Admin

1단계 **Devices > Device Management**를 선택합니다.

Device Management 페이지가 나타납니다.

2단계 인터페이스를 수정할 디바이스 옆에 있는 수정 아이콘( )을 클릭합니다.

해당 디바이스의 **Interfaces** 탭이 나타납니다.

3단계 수정하려는 인터페이스 옆에 있는 수정 아이콘( )을 클릭합니다.

Edit Interface 팝업 창이 나타납니다.

4단계 **Security Zone** 드롭다운 목록에서 기존 보안 영역을 선택하거나 **New**를 선택하여 새 보안 영역을 추가합니다.

5단계 **Save**를 클릭합니다.

보안 영역이 구성됩니다. 디바이스 컨피그레이션을 적용해야 변경 사항이 적용됩니다. 자세한 내용은 4-25페이지의 디바이스에 변경 사항 적용을/를 참조하십시오.

인터페이스 비활성화

라이센스: 모두

인터페이스 유형을 **None**으로 설정하여 인터페이스를 비활성화할 수 있습니다. 비활성화된 인터페이스는 인터페이스 목록에서 회색으로 표시됩니다.

참고 ASA FirePOWER 인터페이스의 유형을 변경할 수 없으며, FireSIGHT 방어 센터에서 인터페이스를 비활성화할 수도 없습니다.

인터페이스를 비활성화하려면

액세스: Admin/Network Admin

1단계 **Devices > Device Management**를 선택합니다.

Device Management 페이지가 나타납니다.

2단계 인터페이스를 비활성화할 디바이스 옆에 있는 수정 아이콘( )을 클릭합니다.

해당 디바이스의 **Interfaces** 탭이 나타납니다.

3단계 비활성화할 인터페이스 옆에 있는 수정 아이콘( )을 클릭합니다.

Edit Interface 팝업 창이 나타납니다.

4단계 **None**을 클릭합니다.

5단계 **Save**를 클릭합니다.

변경 내용이 저장되었습니다. 디바이스 컨피그레이션을 적용해야 변경 사항이 적용됩니다. 자세한 내용은 4-25페이지의 디바이스에 변경 사항 적용을/를 참조하십시오.

이중 연결 로깅 방지

라이센스: 모두

보안 영역 객체를 업데이트하면 시스템은 객체의 새 개정을 저장합니다. 그 결과, 인터페이스에 보안 영역 객체의 서로 다른 여러 개정이 구성되어 있는 관리되는 디바이스가 동일한 보안 영역에 있는 경우, 이중 연결처럼 보이는 내용이 로깅될 수 있습니다.

이중 연결 보고가 발견되면 객체의 동일한 개정을 사용하도록 모든 관리되는 디바이스를 업데이트할 수 있습니다.

디바이스 전체에서 보안 영역 객체 개정을 동기화하려면

액세스: Admin/Network Admin

1단계 **Devices > Device Management**를 선택합니다.

Device Management 페이지가 나타납니다.

주의 동기화하려는 모든 디바이스에서 인터페이스에 대한 영역 설정을 수정하기 전에는 관리되는 디바이스 변경 사항을 디바이스에 다시 적용해서는 안 됩니다.

2단계 보안 영역 선택을 업데이트하려는 디바이스 옆에 있는 수정 아이콘( )을 클릭합니다.

해당 디바이스의 **Interfaces** 탭이 나타납니다.

3단계 이중 연결 이벤트를 로깅하는 각 인터페이스에 대해 **Security Zone**을 다른 영역으로 변경하고, **Save**를 클릭하고, 원하는 영역으로 다시 변경하고, **Save**를 다시 클릭합니다.

4단계 이중 이벤트를 로깅하는 각 디바이스에 대해 2단계와 3단계를 반복합니다.

5단계 모든 디바이스의 모든 인터페이스를 수정했으면 모든 관리되는 디바이스에 디바이스 변경 사항을 동시에 적용합니다.

IPS 디바이스 설정

패시브 또는 인라인 IPS 구축에서 디바이스를 구성할 수 있습니다. 패시브 구축에서는 네트워크 트래픽 플로우의 대역 밖에 시스템이 구축됩니다. 인라인 구축에서는 두 포트를 바인딩하여 네트워크 세그먼트에 투명하게 시스템을 구성합니다.

다음 섹션에서는 FireSIGHT 시스템의 패시브 및 인라인 구축을 위해 디바이스를 구성하는 방법에 대해 설명합니다.

패시브 IPS 구축 이해

라이센스: 보호

패시브 IPS 구축에서 FireSIGHT 시스템은 스위치 SPAN 또는 미러 포트를 사용하여 네트워크에서 이동하는 트래픽을 모니터링합니다. SPAN 또는 미러 포트를 사용하면 스위치의 다른 포트에서 트래픽을 복사할 수 있습니다. 이 기능을 사용하면 네트워크 트래픽의 플로우에 있지 않더라도 네트워크 내에서 가시성이 제공됩니다. 수동 구축으로 구성하는 경우 시스템이 트래픽 차단 또는 형성과 같은 특정 작업을 할 수 없습니다. 수동 인터페이스는 모든 트래픽을 조건 없이 수신하며 이러한 인터페이스에서 수신된 트래픽은 재전송되지 않습니다.

참고 아웃바운드 트래픽은 플로우 제어 패킷을 포함합니다. 따라서 어플라이언스의 패시브 인터페이스는 아웃바운드 트래픽을 표시할 수 있으며 컨피그레이션에 따라 이벤트를 생성할 수 있는데, 이는 자연스러운 동작입니다.

패시브 인터페이스 구성

라이센스: 보호

관리되는 디바이스에 수동 인터페이스와 같은 물리적 포트를 하나 이상 구성할 수 있습니다.

인터페이스를 수정하고 디바이스 정책을 다시 적용하면 Snort는 디바이스의 모든 인터페이스 인스턴스(수정한 것만이 아니라)에 대해 다시 시작됩니다.

Cisco 패키지를 설치할 때에는 Cisco NGIPS for Blue Coat X-Series 인터페이스를 패시브 또는 인라인으로 구성합니다. FireSIGHT 시스템 웹 인터페이스를 사용하여 Cisco NGIPS for Blue Coat X-Series 인터페이스를 다시 구성할 수 없습니다. 자세한 내용은 5-11페이지의 Cisco NGIPS for Blue Coat X-Series 인터페이스 구성을/를 참조하십시오.

주의 MTU(최대 전송 단위)를 변경하면 디바이스의 트래픽이 중단됩니다. MTU 설정 가능 범위는 FireSIGHT 시스템 디바이스 모델 및 인터페이스 유형에 따라 달라질 수 있습니다. 자세한 내용은 4-64페이지의 센싱 인터페이스 MTU 구성을/를 참조하십시오.

패시브 인터페이스를 구성하려면

액세스: Admin/Network Admin

1단계 **Devices > Device Management**를 선택합니다.

Device Management 페이지가 나타납니다.

2단계 패시브 인터페이스를 구성하려는 디바이스 옆의 수정 아이콘( )을 클릭합니다.

Interfaces 탭이 나타납니다.

3단계 패시브 인터페이스로 구성하려는 인터페이스 옆에 있는 수정 아이콘( )을 클릭합니다.

Edit Interface 팝업 창이 나타납니다.

4단계 **Passive**를 클릭하여 패시브 인터페이스 옵션을 표시합니다.

5단계 원한다면 **Security Zone** 드롭다운 목록에서 기존 보안 영역을 선택하거나 **New**를 선택하여 새 보안 영역을 추가합니다.

6단계 패시브 인터페이스에서 트래픽을 모니터링할 수 있게 하려면 **Enabled** 확인란을 선택합니다.

이 확인란의 선택을 취소하면 인터페이스가 비활성화되어 사용자가 보안 목적으로 액세스할 수 없게 됩니다.

7단계 **Mode** 드롭다운 목록에서 링크 모드를 지정하는 옵션을 선택하거나 **Autonegotiation**을 선택하여 인터페이스에서 속도 및 양방향 설정 자동 협상이 구성되도록 지정합니다. Mode 설정은 구리 인터페이스에 대해서만 가능합니다.

참고 8000 Series 어플라이언스의 인터페이스는 반이중 옵션을 지원하지 않습니다.

8단계 **MDI/MDIX** 드롭다운 목록에서 옵션을 선택하여 인터페이스가 MDI(medium dependent interface), MDIX(medium dependent interface crossover) 또는 Auto-MDIX를 위해 구성되었는지 여부를 지정합니다. MDI/MDIX 설정은 구리 인터페이스에 대해서만 가능합니다.

기본적으로 MDI/MDIX는 **Auto-MDIX**로 설정됩니다. 그러면 MDI와 MDIX 간 스위칭을 자동으로 처리하여 링크를 확보합니다.

9단계 **MTU** 필드에 MTU를 입력합니다. 이는 허용되는 최대 크기 패킷을 나타냅니다.

MTU 설정 가능 범위는 FireSIGHT 시스템 디바이스 모델 및 인터페이스 유형에 따라 달라질 수 있습니다. 자세한 내용은 4-64페이지의 센싱 인터페이스 MTU 구성을/를 참조하십시오.

10단계 **Save**를 클릭합니다.

패시브 인터페이스가 구성됩니다. 디바이스 컨피그레이션을 적용해야 변경 사항이 적용됩니다. 자세한 내용은 4-25페이지의 디바이스에 변경 사항 적용을/를 참조하십시오.

인라인 IPS 구축 이해

라이센스: 보호

인라인 IPS 구축에서는 두 포트를 바인딩하여 네트워크 세그먼트에 투명하게 FireSIGHT 시스템을 구성합니다. 그러면 인접한 네트워크 디바이스의 컨피그레이션 없이 네트워크 환경에 시스템을 설치할 수 있습니다. 인라인 인터페이스는 모든 트래픽을 조건 없이 수신하지만 이러한 인터페이스에서 수신한 모든 트래픽은 명시적으로 삭제되지 않는 한 인라인 집합으로부터 다시 전송됩니다.

인라인 인터페이스 구성

라이센스: 보호

관리되는 디바이스에 인라인 인터페이스와 같은 물리적 포트를 하나 이상 구성할 수 있습니다. 인라인 인터페이스가 인라인 구축의 트래픽을 처리할 수 있기 전에 인라인 인터페이스 페어를 인라인 세트로 할당해야 합니다.

인터페이스를 수정하고 디바이스 정책을 다시 적용하면 Snort는 디바이스의 모든 인터페이스 인스턴스(수정한 것만이 아니라)에 대해 다시 시작됩니다. 또한 인라인 쌍의 인터페이스를 다른 속도로 설정하거나 인터페이스가 서로 다른 속도로 협상하는 경우 경고가 표시됩니다.

Cisco 패키지를 설치할 때에는 Cisco NGIPS for Blue Coat X-Series 인터페이스를 패시브 또는 인라인으로 구성합니다. FireSIGHT 시스템 웹 인터페이스를 사용하여 Cisco NGIPS for Blue Coat X-Series 인터페이스를 다시 구성할 수 없습니다. 자세한 내용은 5-11페이지의 Cisco NGIPS for Blue Coat X-Series 인터페이스 구성을/를 참조하십시오.

참고 인터페이스를 인라인 인터페이스로 구성할 경우 해당 NetMod의 인접 포트도 인라인 인터페이스가 되어 페어를 완성합니다.

가상 디바이스에서 인라인 인터페이스를 구성하려면 인접 인터페이스를 사용하여 인라인 쌍을 생성해야 합니다.

인라인 인터페이스를 구성하려면

액세스: Admin/Network Admin

1단계 **Devices > Device Management**를 선택합니다.

Device Management 페이지가 나타납니다.

2단계 인라인 인터페이스를 구성하려는 디바이스 옆에 있는 수정 아이콘( )을 클릭합니다.

Interfaces 탭이 나타납니다.

3단계 인라인 인터페이스로 구성하려는 인터페이스 옆에 있는 수정 아이콘( )을 클릭합니다.

Edit Interface 팝업 창이 나타납니다.

4단계 **Inline**을 클릭하여 인라인 인터페이스 옵션을 표시합니다.

5단계 원한다면 **Security Zone** 드롭다운 목록에서 기존 보안 영역을 선택하거나 **New**를 선택하여 새 보안 영역을 추가합니다.

6단계 **Inline Set** 드롭다운 목록에서 기존 인라인 집합을 선택하거나 **New**를 선택하여 새 인라인 집합을 추가합니다.

새 인라인 집합을 추가할 경우 인라인 인터페이스를 설정한 다음에 Device Management 페이지(**Devices > Device Management > Inline Sets**)에서 이를 구성해야 합니다. 자세한 내용은 5-6페이지의 인라인 집합 추가을/를 참조하십시오.

7단계 인라인 인터페이스에서 트래픽을 처리할 수 있게 하려면 **Enabled** 확인란을 선택합니다.

이 확인란의 선택을 취소하면 인터페이스가 비활성화되어 사용자가 보안 목적으로 액세스할 수 없게 됩니다.

8단계 **Mode** 드롭다운 목록에서 링크 모드를 지정하는 옵션을 선택하거나 **Autonegotiation**을 선택하여 인터페이스에서 속도 및 양방향 설정 자동 협상이 구성되도록 지정합니다. Mode 설정은 구리 인터페이스에 대해서만 가능합니다.

참고 8000 Series 어플라이언스의 인터페이스는 반이중 옵션을 지원하지 않습니다.

9단계 **MDI/MDIX** 드롭다운 목록에서 옵션을 선택하여 인터페이스가 MDI(medium dependent interface), MDIX(medium dependent interface crossover) 또는 Auto-MDIX를 위해 구성되었는지 여부를 지정합니다. MDI/MDIX 설정은 구리 인터페이스에 대해서만 가능합니다.

기본적으로 MDI/MDIX는 **Auto-MDIX**로 설정됩니다. 그러면 MDI와 MDIX 간 스위칭을 자동으로 처리하여 링크를 확보합니다.

10단계 **Save**를 클릭합니다.

인라인 인터페이스가 구성됩니다. 디바이스 컨피그레이션을 적용해야 변경 사항이 적용됩니다. 자세한 내용은 4-25페이지의 디바이스에 변경 사항 적용을/를 참조하십시오.

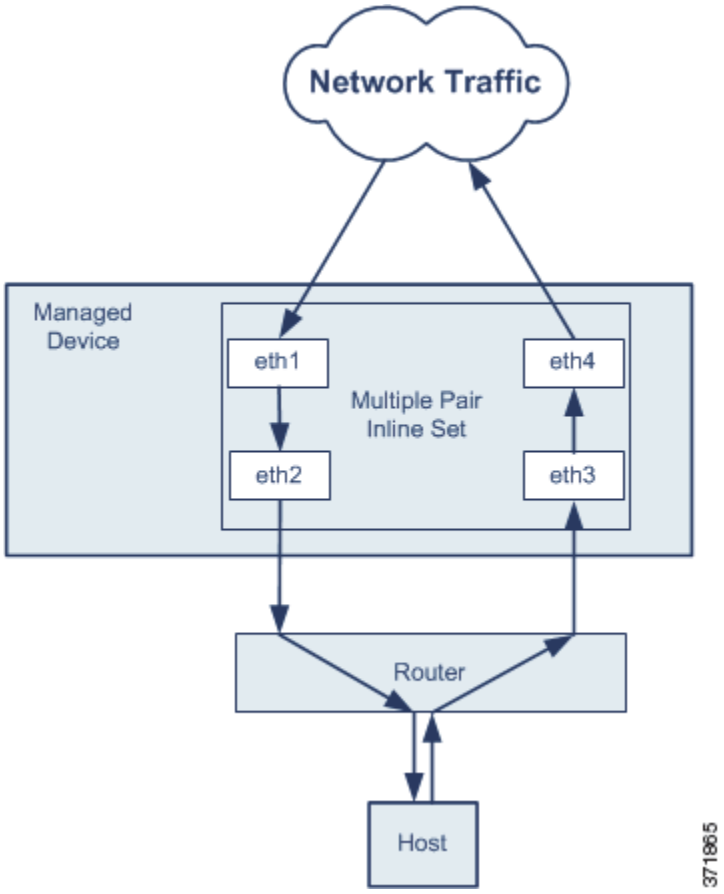
인라인 집합 구성

라이센스: 보호

인라인 구축에서 인라인 인터페이스를 사용하려면 인라인 집합을 구성하고 여기에 인라인 인터페이스 쌍을 할당해야 합니다. 인라인 집합은 디바이스에 있는 하나 이상의 인라인 인터페이스 쌍을 그룹화한 것입니다. 한 인라인 인터페이스 쌍은 동시에 한 인라인 집합에만 속할 수 있습니다.

디바이스 트래픽이 인바운드인지 아웃바운드인지에 따라 서로 다른 인라인 인터페이스 쌍을 통해 네트워크의 호스트와 외부 호스트 간 트래픽을 라우팅하도록 관리되는 디바이스에서 인터페이스를 구성할 수 있습니다. 이것이 *비동기 라우팅* 컨피그레이션입니다. 비동기 라우팅을 구축하지만 인라인 집합에 인터페이스 쌍을 하나만 포함하려는 경우, 트래픽이 절반만 표시될 수 있으므로 디바이스에서 네트워크 트래픽을 올바르게 분석하지 못할 수 있습니다. 동일한 인터페이스 집합에 여러 인라인 인터페이스 쌍을 추가하면 시스템은 동일한 트래픽 플로우의 일부로서 인바운드 및 아웃바운드 트래픽을 식별할 수 있습니다. 동일한 보안 영역에 인터페이스 쌍을 포함하여 이를 구현할 수도 있습니다.

시스템이 비동기 라우팅 컨피그레이션을 통과하는 트래픽에서 연결 이벤트를 생성하면, 해당 이벤트는 동일한 인터페이스 쌍에서 인그레스 및 이그레스 인터페이스를 식별할 수 있습니다. 예를 들어 다음 다이어그램의 컨피그레이션은 인그레스 인터페이스로 **eth3**을 식별하고, 이그레스 인터페이스로 **eth2**를 식별하는 연결 이벤트를 생성할 수 있습니다. 이 컨피그레이션에서는 이러한 동작이 예상됩니다.



참고 단일 인라인 인터페이스 집합에 여러 인터페이스 쌍을 할당하여 이중 트래픽의 문제가 발생하는 경우 시스템이 패킷을 고유하게 식별하도록 다시 구성해야 합니다. 예를 들면 인라인 쌍을 별도의 인라인 집합에 다시 할당하거나 보안 영역을 수정할 수 있습니다.

인라인 집합이 있는 디바이스의 경우 디바이스를 다시 시작하면 소프트웨어 브리지가 패킷을 전송하도록 자동으로 다시 설정됩니다. 디바이스가 다시 시작 중이면 소프트웨어 브리지가 어디서도 실행되지 않습니다. 인라인 집합에서 우회 모드를 활성화하면 디바이스가 다시 시작되는 동안 하드웨어 우회로 들어갑니다. 이 경우 디바이스와의 링크 재협상 때문에, 시스템이 종료되었다가 다시 시작되면서 몇 초 분량의 패킷이 손실될 수 있습니다. 그러나 시스템은 Snort가 다시 시작되는 동안 트래픽을 전달합니다.

주의 기존 인라인 집합을 변경하면 디바이스에서 트래픽이 중단될 수 있습니다. MTU(최대 전송 단위)를 변경하면 디바이스에서 트래픽이 중단되고, 일부 패킷이 검사 및 삭제 없이 전송됩니다. MTU 설정 가능 범위는 FireSIGHT 시스템 디바이스 모델 및 인터페이스 유형에 따라 달라질 수 있습니다. 자세한 내용은 4-64페이지의 센싱 인터페이스 MTU 구성을/를 참조하십시오.

자세한 내용은 다음 절을 참조하십시오.

인라인 집합 보기

라이센스: 보호

Device Management 페이지의 **Inline Sets** 탭은 디바이스에 구성한 모든 인라인 집합의 목록을 표시합니다. 가상 디바이스 또는 Cisco NGIPS for Blue Coat X-Series에서 인라인 집합이 우회 모드로 들어가도록 구성할 수 없습니다. 인라인 집합 테이블 보기 필드 표에 각 집합에 대한 요약 정보가 포함되어 있습니다.

표 5-1 인라인 집합 테이블 보기 필드

필드	설명
Name	인라인 집합의 이름
Interface Pairs	인라인 집합에 할당된 모든 인라인 인터페이스 쌍의 목록. Interfaces 탭에서 쌍의 두 인터페이스 중 하나를 비활성화하면 쌍을 사용할 수 없음
Bypass	인라인 집합의 구성된 우회 모드

인라인 집합 추가

라이센스: 보호

Device Management 페이지의 **Inline Sets** 탭에서 인라인 집합을 추가하거나, 인라인 인터페이스를 구성할 때 인라인 집합을 추가할 수 있습니다.

인라인 인터페이스 쌍은 인라인 집합**에만** 할당할 수 있습니다. 관리되는 디바이스에서 인라인 인터페이스를 구성하기 전에 인라인 집합을 생성하려는 경우 빈 인라인 집합을 만들고 나중에 여기에 인터페이스를 추가할 수 있습니다.

인라인 집합을 추가하려면

액세스: Admin/Network Admin

1단계 **Devices > Device Management**를 선택합니다.

Device Management 페이지가 나타납니다.

2단계 인라인 집합을 추가하려는 디바이스 옆의 수정 아이콘( )을 클릭합니다.

Interfaces 탭이 나타납니다.

3단계 **Inline Sets**를 클릭합니다.

Inline Sets 탭이 나타납니다.

4단계 **Add Inline Set**를 클릭합니다.

Add Inline Set 팝업 창이 나타납니다.

5단계 **Name** 필드에 인라인 집합의 이름을 입력합니다. 영숫자와 공백을 사용할 수 있습니다.

6단계 인라인 집합에 추가하기 위해 인라인 인터페이스 쌍을 선택하기 위한 두 가지 옵션이 있습니다.

- **Interfaces** 옆에서 하나 이상의 인라인 인터페이스 쌍을 선택한 다음 선택 항목 추가 아이콘()을 클릭합니다. 여러 인라인 인터페이스 쌍을 선택하려면 Ctrl 또는 Shift를 사용합니다.
- 인라인 집합에 모든 인터페이스 쌍을 추가하려면 모두 추가 아이콘()을 클릭합니다.

팁 인라인 집합에서 인라인 인터페이스를 제거하려면 하나 이상의 인라인 인터페이스 쌍을 선택하고 선택 항목 제거 아이콘()을 클릭합니다. 인라인 집합에서 모든 인터페이스 쌍을 제거하려면 모두 제거 아이콘()을 클릭합니다. **Interfaces** 탭에서 쌍의 두 인터페이스 중 하나를 비활성화하면 쌍 자체도 제거됩니다.

7단계 **MTU** 필드에 MTU를 입력합니다. 이는 허용되는 최대 크기 패킷을 나타냅니다.

MTU 설정 가능 범위는 FireSIGHT 시스템 디바이스 모델 및 인터페이스 유형에 따라 달라질 수 있습니다. 자세한 내용은 4-64페이지의 센싱 인터페이스 MTU 구성을/를 참조하십시오.

8단계 선택적으로, 트래픽이 탐지를 우회하여 디바이스로 계속 이동하도록 지정하려면 **Failsafe**를 선택합니다. 관리되는 디바이스는 내부 트래픽 버퍼를 모니터링하고 버퍼가 꽉 차면 탐지를 우회합니다.

Series 3 및 3D9900 디바이스만 이 옵션을 지원합니다.

9단계 인터페이스가 실패할 때 인라인 인터페이스의 릴레이가 반응하는 방법을 구성하려면 우회 모드를 선택합니다.

- 트래픽이 인터페이스를 계속 통과하도록 허용하려면 **Bypass**를 선택합니다.
- 트래픽을 차단하려면 **Non-Bypass**를 선택합니다.

참고 우회 모드에서 어플라이언스를 재부팅하면 패킷이 약간 손실될 수 있습니다. 클러스터링된 디바이스의 인라인 집합, 가상 디바이스나 Cisco NGIPS for Blue Coat X-Series의 인라인 집합, 8000 Series 디바이스의 비-우회 NetMods, 3D7115 또는 3D7125 디바이스의 SFP 모듈에 대해서는 우회 모드를 구성할 수 없습니다.

10단계 **OK**를 클릭합니다.

인라인 집합이 추가됩니다. 디바이스 컨피그레이션을 적용해야 변경 사항이 적용됩니다. 자세한 내용은 4-25페이지의 디바이스에 변경 사항 적용을/를 참조하십시오.

팁 인라인 집합에 대해 고급 설정(예: 탭 모드, 링크 상태 전파 및 투명 인라인 모드)을 구성하려면 5-8페이지의 고급 인라인 집합 옵션 구성을/를 참조하십시오.

고급 인라인 집합 옵션 구성

라이센스: 보호

지원되는 디바이스: 기능에 따라 다름

인라인 집합을 구성할 때 고려해야 할 몇 가지 옵션이 있습니다. 각 옵션에 대한 자세한 내용은 다음 절을 참조하십시오.

탭 모드

지원되는 디바이스: Series 3, 3D9900

탭 모드는 3D9900 및 Series 3 디바이스에서 인라인 또는 fail-open 포함 인라인 인터페이스 집합을 생성할 때 이용할 수 있습니다.

탭 모드에서는 디바이스가 인라인으로 구축되지만, 패킷 플로우가 디바이스를 통과하는 대신 각 패킷의 복사본이 디바이스로 전송되며 네트워크 트래픽 플로우가 방해받지 않습니다. 패킷 자체가 아니라 패킷의 복사본으로 작업하므로 삭제하도록 설정한 규칙 및 교체 키워드를 사용하는 규칙은 패킷 스트림에 영향을 주지 않습니다. 그러나 이런 유형의 규칙이 트리거되면 침입 이벤트가 생성되며, 인라인 구축이었다면 트리거링 패킷이 삭제되었을 것임이 침입 이벤트의 테이블 보기에 나타납니다.

인라인으로 구축된 디바이스에서 탭 모드를 사용하는 데에는 몇 가지 이점이 있습니다. 예를 들면, 디바이스가 인라인 상태인 것처럼 디바이스와 네트워크 간에 케이블링을 설정할 수 있으며 디바이스가 생성하는 침입 이벤트의 종류를 분석할 수 있습니다. 결과를 기반으로 침입 정책을 수정할 수 있으며, 효율성 저하 없이 네트워크를 가장 잘 보호하는 삭제 규칙을 추가할 수 있습니다. 디바이스를 인라인으로 구축할 준비가 되면, 디바이스와 네트워크 간 케이블링을 다시 구성하지 않고도 탭 모드를 비활성화하고 의심스러운 트래픽의 삭제를 시작할 수 있습니다.

동일한 인라인 집합에서 이 옵션 및 Strict TCP Enforcement를 활성화할 수 없습니다.

링크 상태 전파

지원되는 디바이스: Series 2 ,Series 3

링크 상태 전파는 인라인 집합의 두 쌍이 상태를 추적하도록 우회 모드에서 구성되는 인라인 집합의 기능입니다. 링크 상태 전파는 구리 및 파이버 구성 가능 우회 인터페이스에서 모두 사용할 수 있습니다.

링크 상태 전파는 인라인 집합의 인터페이스 중 하나가 다운될 때 인라인 인터페이스 쌍에서 두 번째 인터페이스를 자동으로 불러옵니다. 장애가 발생한 인터페이스가 복원되면 두 번째 인터페이스도 자동으로 활성화됩니다. 다시 말해, 한 인터페이스의 링크 상태가 변경되면 어플라이언스가 이를 감지하고 다른 인터페이스의 링크 상태를 이와 일치하도록 업데이트합니다. 어플라이언스가 링크 상태 변경 사항을 전파하려면 최대 4초가 걸립니다.

참고 링크 상태 전파가 트리거되면 Series 2 디바이스(3D9900의 디바이스 제외)에 fail-open으로 구성된 파이버 인라인 집합이 하드웨어 우회 모드를 활성화합니다. 이 경우 관련된 인터페이스 카드는 우회에서 자동으로 나오지 않으므로 반드시 수동으로 가져와야 합니다. 인라인 집합 및 하드웨어 우회의 파이버 인터페이스에 대한 자세한 내용은 5-10페이지의 Fail Open으로 구성된 파이버 인라인 집합에서 우회 모드 제거을/를 참조하십시오.

링크 상태 전파는 라우터가 장애 상태의 네트워크 디바이스 주위로 트래픽을 자동으로 다시 라우팅하도록 구성된 탄력적인 네트워크 환경에서 특히 유용합니다.

클러스터링된 디바이스에 구성된 인라인 집합에 대해서는 링크 상태 전파를 비활성화할 수 없습니다.

가상 디바이스, Cisco NGIPS for Blue Coat X-Series 및 Cisco ASA with FirePOWER Services는 링크 상태 전파를 지원하지 않습니다.

Transparent Inline Mode

Transparent Inline Mode 옵션을 선택하면 디바이스는 "bump in the wire" 역할을 수행할 수 있습니다. 즉, 디바이스는 소스 및 목적지와 상관없이 발견하는 모든 네트워크 트래픽을 전달합니다. Series 3 또는 3D9900 디바이스에서는 이 옵션을 비활성화할 수 없습니다.

Strict TCP Enforcement

지원되는 디바이스: Series 3

TCP 보안을 극대화하기 위해 엄격한 적용을 활성화할 수 있습니다. 그러면 3-way 핸드셰이크가 완료되지 않은 연결을 차단합니다. 엄격한 적용은 다음 항목도 차단합니다.

- 3-way 핸드셰이크가 완료되지 않은 연결의 비 SYN TCP 패킷
- TCP 연결의 responder가 SYN-ACK를 보내기 전에 initiator가 보낸 비 SYN/RST 패킷
- TCP 연결에서 SYN 이후에 그러나 세션이 설정되기 전에 responder가 보낸 비 SYN-ACK/RST 패킷
- 설정된 TCP 연결에서 initiator 또는 responder가 보낸 SYN 패킷

Series 2, 가상 디바이스 및 Cisco NGIPS for Blue Coat X-Series는 이 옵션을 지원하지 않습니다. 또한 동일한 인라인 집합에서 이 옵션 및 탭 모드를 활성화할 수 없습니다.

고급 인라인 집합 옵션을 구성하려면

액세스: Admin/Network Admin

1단계 **Devices > Device Management**를 선택합니다.

Device Management 페이지가 나타납니다.

2단계 인라인 집합을 수정하려는 디바이스 옆에 있는 수정 아이콘( )을 클릭합니다.

Interfaces 탭이 나타납니다.

3단계 **Inline Sets**를 클릭합니다.

Inline Sets 탭이 나타납니다.

4단계 수정하려는 인라인 집합 옆에 있는 수정 아이콘( )을 클릭합니다.

Edit Inline Set 팝업 창이 나타납니다.

5단계 **Advanced**를 클릭합니다.

Advanced 탭이 나타납니다.

6단계 선택적으로, Series 3 및 3D9900 디바이스의 인라인 인터페이스에서 탭 모드를 활성화하려면 **Tap Mode**를 선택합니다.

가상 디바이스, Cisco NGIPS for Blue Coat X-Series 및 Series 2 디바이스(3D9900 제외)는 이 옵션을 지원하지 않습니다. 또한 동일한 인라인 집합에서 Tap Mode 및 Strict TCP Enforcement를 활성화할 수 없습니다.

7단계 선택적으로, Series 2 또는 Series 3 디바이스에서 **Propagate Link State**를 선택합니다. 이 옵션은 네트워크의 라우터가 다운된 네트워크 디바이스 주위로 트래픽을 다시 라우팅할 수 있는 경우 특히 유용합니다.

클러스터링된 디바이스에 구성된 인라인 집합에 대해서는 링크 상태 전파를 비활성화할 수 없습니다.

가상 디바이스 및 Cisco NGIPS for Blue Coat X-Series는 이 옵션을 지원하지 않습니다.

8단계 선택적으로, **Strict TCP Enforcement**를 선택하여 Series 3 디바이스에서 엄격한 TCP 적용을 활성화합니다.

Series 2, 가상 디바이스 및 Cisco NGIPS for Blue Coat X-Series는 이 옵션을 지원하지 않습니다. 또한 동일한 인라인 집합에서 Strict TCP Enforcement 및 Tap Mode를 활성화할 수 없습니다.

9단계 선택적으로, **Transparent Inline Mode**를 선택합니다.

Series 3 또는 3D9900 디바이스에서는 이 옵션을 비활성화할 수 없습니다.

10단계 **OK**를 클릭합니다.

변경 내용이 저장되었습니다. 디바이스 컨피그레이션을 적용해야 변경 사항이 적용됩니다. 자세한 내용은 4-25페이지의 디바이스에 변경 사항 적용을/를 참조하십시오.

Fail Open으로 구성된 파이버 인라인 집합에서 우회 모드 제거

라이센스: 보호

지원되는 디바이스: Series 2(3D9900 제외)

파이버 인라인 집합이 fail open으로 구성된 Series 2 디바이스에서 링크 상태 전파가 활성화되고 디바이스가 우회 모드로 들어가는 경우, 모든 네트워크 트래픽은 분석 없이 인라인 집합을 통과합니다. 링크가 복원되면 fail open으로 구성된 대부분의 파이버 인라인 집합은 우회 모드에서 자동으로 돌아오지 않습니다. 인라인 집합이 우회 모드에서 빠져나오도록 하는 명령줄 툴을 사용할 수 있습니다.

이 툴은 파이버 인라인 인터페이스가 fail open으로 구성된 인라인 집합에서 작동합니다. 구리 인라인 인터페이스가 fail open으로 설정된 인라인 집합에서는 이 툴을 사용할 필요가 없습니다.

참고 디바이스에서 fail open으로 구성된 인라인 집합에 문제가 있는 경우 고객 지원에 문의하십시오.

디바이스에서 fail open으로 구성된 파이버 인라인 집합이 우회 모드에서 빠져나오도록 하려면

액세스: Admin/Network Admin

1단계 디바이스에서 터미널 창을 열고 관리자 사용자로서 로그인합니다.

2단계 명령줄에서 다음을 입력합니다.

```
sudo /var/sf/bin/unbypass_cards.sh
```

비밀번호를 입력하라는 메시지가 표시됩니다.

3단계 인터페이스가 우회 모드에서 빠져나오면 디바이스가 트래픽을 분석 중이라는 메시지가 syslog에 표시됩니다. 예를 들면 다음과 같습니다.

```
Fiber pair has been reset by un_bypass
```

인라인 집합 삭제

라이센스: 보호

인라인 집합을 삭제할 때 그 집합에 지정되었던 모든 인라인 인터페이스는 다른 집합에 포함될 수 있게 됩니다. 인터페이스가 삭제되지 않습니다.

인라인 집합을 삭제하려면

액세스: Admin/Network Admin

1단계 **Devices > Device Management**를 선택합니다.

Device Management 페이지가 나타납니다.

2단계 인라인 집합을 삭제하려는 디바이스 옆의 수정 아이콘( )을 클릭합니다.

Interfaces 탭이 나타납니다.

3단계 **Inline Sets**를 클릭합니다.

Inline Sets 탭이 나타납니다.

4단계 삭제하려는 인라인 집합 옆에 있는 삭제 아이콘( )을 클릭합니다.

5단계 확인 메시지가 표시되면 인라인 집합을 삭제할 것임을 확인합니다.

인라인 집합이 삭제됩니다. 디바이스 컨피그레이션을 적용해야 변경 사항이 적용됩니다. 자세한 내용은 4-25페이지의 디바이스에 변경 사항 적용을/를 참조하십시오.

Cisco NGIPS for Blue Coat X-Series 인터페이스 구성

라이센스: 보호

지원되는 디바이스: X-Series

Cisco NGIPS for Blue Coat X-Series 패키지를 구축할 때 또는 패키지가 설치된 후에 패시브 또는 인라인 인터페이스를 생성합니다. Cisco NGIPS for Blue Coat X-Series를 방어 센터에 추가하면 이러한 인터페이스는 이미 구성되어 있습니다. Cisco NGIPS for Blue Coat X-Series는 고급 컨피그레이션 옵션을 지원하지 않습니다.

FireSIGHT 시스템 웹 인터페이스를 사용하여 Cisco NGIPS for Blue Coat X-Series 인터페이스를 다시 구성할 수 없습니다. 다시 구성하려면 먼저 방어 센터에서 현재 인터페이스를 삭제한 다음 새 인터페이스를 생성하십시오. 인터페이스의 생성 및 삭제에 대한 자세한 내용은 *Cisco NGIPS for Blue Coat X-Series Installation Guide*를 참조하십시오.

Cisco NGIPS for Blue Coat X-Series에서 인터페이스를 구성하려면

액세스: Admin/Network Admin

1단계 **Devices > Device Management**를 선택합니다.

Device Management 페이지가 나타납니다.

2단계 구성하려는 디바이스 옆에 있는 수정 아이콘( )을 클릭합니다.

Interfaces 탭이 나타납니다. 모든 Cisco NGIPS for Blue Coat X-Series 인터페이스에 대해 Link는 항상 활성( )으로 표시됩니다.

3단계 구성하려는 인터페이스 옆에 있는 수정 아이콘()을 클릭합니다.

4단계 **Security Zone** 드롭다운 목록에서 기존 보안 영역을 선택하거나 **New**를 선택하여 새 보안 영역을 추가합니다.

5단계 선택적으로, 인라인 인터페이스의 경우 **Inline Set** 드롭다운 목록에서 기존 인라인 집합을 선택하거나 **New**를 선택하여 새 인라인 집합을 추가합니다.

새 인라인 집합을 추가할 경우 인라인 인터페이스를 설정한 다음에 Device Management 페이지(**Devices > Device Management > Inline Sets**)에서 이를 구성해야 합니다. 자세한 내용은 5-6페이지의 인라인 집합 추가을/를 참조하십시오.

6단계 **Save**를 클릭합니다.

인터페이스가 구성됩니다. 메뉴 모음 오른쪽 상단에서 **Apply Changes**를 클릭하여 디바이스 컨피그레이션을 적용할 때까지 변경 사항이 반영되지 않습니다.

6장

가상 스위치 설정

레이어 2 구축에서 관리 대상 디바이스를 구성하여 둘 이상의 네트워크 간에 패킷 스위칭을 수행하게 할 수 있습니다. 레이어 2 구축의 경우 관리 대상 디바이스의 가상 스위치가 독립형 브로드캐스트 도메인이 되도록 구성하여 네트워크를 논리적 세그먼트로 분할할 수 있습니다. 가상 스위치는 호스트의 MAC(Media Access Control) 주소를 사용하여 패킷을 보낼 대상을 결정합니다.

가상 스위치를 구성할 경우 이 스위치는 처음에 스위치에서 사용 가능한 모든 포트를 통해 패킷을 브로드캐스트합니다. 시간이 경과함에 따라 이 스위치는 태그가 지정된 반환 트래픽을 사용하여 각 포트에 연결된 네트워크에 상주하는 호스트를 알아냅니다.

가상 스위치에는 트래픽을 처리할 수 있도록 두 개 이상의 스위치드 인터페이스가 포함되어야 합니다. 각 가상 스위치에서 트래픽은 스위치드 인터페이스로 구성된 포트의 집합으로 제한됩니다. 예를 들어 4개의 스위치드 인터페이스로 가상 스위치를 구성할 경우 한 브로드캐스트용 포트를 거쳐 전송된 패킷은 오로지 스위치의 나머지 3개 포트로부터 전송된 것이어야 합니다.

물리적 스위치드 인터페이스를 구성할 때 이를 가상 스위치에 지정해야 합니다. 필요하다면 물리적 포트에 추가 논리적 스위치드 인터페이스를 정의할 수도 있습니다. Series 3이 관리하는 디바이스에서 여러 물리적 인터페이스를 단일 논리적 스위치드 인터페이스로 그룹화할 수 있으며, 이를 LAG(link aggregation group)라고 합니다. 이 단일 종합 논리적 링크는 두 엔드포인트 간에 더 우수한 대역폭, 이중화, 로드 밸런싱을 제공합니다.

주의 어떤 이유로 레이어 2 구축에 실패할 경우 디바이스는 더 이상 트래픽을 전달하지 않습니다.

레이어 2 구축을 구성하는 것에 대한 자세한 내용은 다음 절을 참조하십시오.

- 6-2페이지의 스위치드 인터페이스 컨피그레이션
- 6-5페이지의 가상 스위치 구성
- 8-2페이지의 LAG 구성

스위치드 인터페이스 컨피그레이션

라이센스: 제어

지원되는 디바이스: Series 3

스위치드 인터페이스가 물리적 또는 논리적 컨피그레이션을 갖도록 설정할 수 있습니다. 태그가 지정되지 않은 VLAN 트래픽을 처리하기 위해 물리적 스위치드 인터페이스를 구성할 수 있습니다. 또한 지정된 VLAN 태그가 포함된 트래픽을 처리하기 위해 논리적 스위치드 인터페이스를 만들 수 있습니다.

레이어 2 구축에서 대기 중인 스위치드 인터페이스가 없는 외부 물리적 인터페이스에 수신된 트래픽은 모두 삭제됩니다. VLAN 태그가 없는 패킷이 수신되고 해당 포트에 대한 물리적 스위치드 인터페이스를 구성하지 않은 경우에는 패킷이 삭제됩니다. VLAN 태그가 있는 패킷이 수신되었지만 논리적 스위치드 인터페이스를 구성하지 않은 경우에도 패킷이 삭제됩니다.

스위치드 인터페이스에서 VLAN 태그와 함께 수신된 트래픽은 규칙 평가 또는 전달 결정에 앞서 인그레스에서 가장 바깥쪽의 VLAN 태그를 스트리핑하는 방법으로 처리합니다. VLAN 태그 지정 논리적 스위치드 인터페이스를 통해 디바이스에서 전송되는 패킷은 이그레스에서 해당 VLAN 태그로 캡슐화됩니다.

상위 물리적 인터페이스를 인라인 또는 패시브로 변경할 경우 해당 논리적 인터페이스가 모두 삭제됩니다.

자세한 내용은 다음 절을 참조하십시오.

- 6-2페이지의 물리적 스위치드 인터페이스 컨피그레이션
- 6-3페이지의 논리적 스위치드 인터페이스 추가
- 6-5페이지의 논리적 스위치드 인터페이스 삭제

물리적 스위치드 인터페이스 컨피그레이션

라이센스: 제어

지원되는 디바이스: Series 3

관리 대상 디바이스에서 하나 이상의 물리적 포트를 스위치드 인터페이스로 구성할 수 있습니다. 가상 라우터에서 트래픽을 처리하려면 먼저 여기에 물리적 스위치드 인터페이스를 지정해야 합니다.

주의 MTU(maximum transmission unit)를 변경하면 디바이스의 트래픽이 중단되고 패킷이 삭제됩니다. MTU 설정 가능 범위는 FireSIGHT 시스템 디바이스 모델 및 인터페이스 유형에 따라 달라질 수 있습니다. 자세한 내용은 4-64페이지의 센싱 인터페이스 MTU 구성를 참조하십시오.

물리적 스위치드 인터페이스를 구성하려면

액세스: Admin/Network Admin

1단계 **Devices > Device Management**를 선택합니다.

Device Management 페이지가 나타납니다.

2단계 스위치드 인터페이스를 구성하려는 디바이스 옆의 수정 아이콘()을 클릭합니다.

Interfaces 탭이 나타납니다.

3단계 스위치드 인터페이스로 구성하려는 인터페이스 옆에서 수정 아이콘( )을 클릭합니다.

Edit Interface 팝업 창이 나타납니다.

4단계 **Switched**를 클릭하여 스위치드 인터페이스 옵션을 표시합니다.

5단계 원한다면 **Security Zone** 드롭다운 목록에서 기존 보안 영역을 선택하거나 **New**를 선택하여 새 보안 영역을 추가합니다.

6단계 원한다면 **Virtual Switch** 드롭다운 목록에서 기존 가상 스위치를 선택하거나 **New**를 선택하여 새 가상 라우터를 추가합니다.

새 가상 스위치를 추가할 경우 스위치드 인터페이스를 설정한 다음에 Device Management 페이지의 Virtual Switches 탭(**Devices > Device Management > Virtual Switches**)에서 이를 구성해야 합니다. 6-6페이지의 가상 스위치 추가를 참조하십시오.

7단계 스위치드 인터페이스에서 트래픽을 처리할 수 있게 하려면 **Enabled** 확인란을 선택합니다.

이 확인란의 선택을 취소하면 인터페이스가 비활성화되어 사용자가 보안 목적으로 액세스할 수 없게 됩니다.

8단계 **Mode** 드롭다운 목록에서 링크 모드를 지정하는 옵션을 선택하거나 **Autonegotiation**을 선택하여 인터페이스에서 속도 및 양방향 설정 자동 협상이 구성되도록 지정합니다. 모드 설정은 카퍼 인터페이스에 대해서만 가능합니다.

참고 8000 Series 어플라이언스의 인터페이스는 반이중 옵션을 지원하지 않습니다.

9단계 **MDI/MDIX** 드롭다운 목록에서 옵션을 선택하여 인터페이스가 MDI(medium dependent interface), MDIX(medium dependent interface crossover) 또는 Auto-MDIX를 위해 구성되었는지 여부를 지정합니다. MDI/MDIX 설정은 카퍼 인터페이스에 대해서만 가능합니다.

기본적으로 MDI/MDIX는 Auto-MDIX로 설정됩니다. 그러면 MDI와 MDIX 간 스위칭을 자동으로 처리하여 링크를 확보합니다.

10단계 **MTU** 필드에 MTU를 입력합니다. 이는 허용되는 최대 크기 패킷을 나타냅니다.

MTU 설정 가능 범위는 FireSIGHT 시스템 디바이스 모델 및 인터페이스 유형에 따라 달라질 수 있습니다. 자세한 내용은 4-64페이지의 센싱 인터페이스 MTU 구성를 참조하십시오.

11단계 **Save**를 클릭합니다.

물리적 스위치드 인터페이스가 구성되었습니다. 디바이스 컨피그레이션을 적용해야 변경 사항이 적용됩니다. 자세한 내용은 4-25페이지의 디바이스에 변경 사항 적용를 참조하십시오.

논리적 스위치드 인터페이스 추가

라이센스: 제어

지원되는 디바이스: Series 3

각 물리적 스위치드 인터페이스에 대해 여러 논리적 스위치드 인터페이스를 추가할 수 있습니다. 물리적 인터페이스에서 VLAN 태그와 함께 수신된 트래픽을 처리하려면 각 논리적 인터페이스를 해당 태그와 연결해야 합니다. 트래픽을 처리하려면 가상 스위치에 논리적 스위치드 인터페이스를 지정해야 합니다.

주의 MTU를 변경하면 디바이스의 스위치드 트래픽이 중단되고 패킷이 삭제됩니다.

기존 논리적 스위치드 인터페이스를 수정하려면 인터페이스 옆의 수정 아이콘()을 클릭합니다.

논리적 스위치드 인터페이스를 추가하려면

액세스: Admin/Network Admin

1단계 **Devices > Device Management**를 선택합니다.

Device Management 페이지가 나타납니다.

2단계 스위치드 인터페이스를 추가하려는 디바이스 옆의 수정 아이콘()을 클릭합니다.

Interfaces 탭이 나타납니다.

3단계 **Add Interface**를 클릭합니다.

Add Interface 팝업 창이 나타납니다.

4단계 **Switched**를 클릭하여 스위치드 인터페이스 옵션을 표시합니다.

5단계 **Interface** 드롭다운 목록에서 VLAN 태그가 지정된 트래픽을 수신할 물리적 인터페이스를 선택합니다.

6단계 **VLAN Tag** 필드에 이 인터페이스의 인바운드 및 아웃바운드 트래픽에 지정된 태그 값을 입력합니다. 이 값은 1과 4094 사이의 임의의 정수일 수 있습니다.

7단계 원한다면 **Security Zone** 드롭다운 목록에서 기존 보안 영역을 선택하거나 **New**를 선택하여 새 보안 영역을 추가합니다.

8단계 원한다면 Virtual Switch 드롭다운 목록에서 기존 가상 스위치를 선택하거나 **New**를 선택하여 새 가상 라우터를 추가합니다.

새 가상 스위치를 추가할 경우 스위치드 인터페이스를 설정한 다음에 Device Management 페이지(**Devices > Device Management > Virtual Switches**)에서 이를 구성해야 합니다. 6-6페이지의 가상 스위치 추가를 참조하십시오.

9단계 스위치드 인터페이스에서 트래픽을 처리할 수 있게 하려면 **Enabled** 확인란을 선택합니다.

확인란의 선택을 취소할 경우 인터페이스는 비활성화되고 관리상 다운됩니다. 물리적 인터페이스를 비활성화할 경우 그와 연결된 모든 논리적 인터페이스도 비활성화됩니다.

10단계 **MTU** 필드에 MTU를 입력합니다. 이는 허용되는 최대 크기 패킷을 나타냅니다.

MTU 설정 가능 범위는 FireSIGHT 시스템 디바이스 모델 및 인터페이스 유형에 따라 달라질 수 있습니다. 자세한 내용은 4-64페이지의 센싱 인터페이스 MTU 구성를 참조하십시오.

11단계 **Save**를 클릭합니다.

논리적 스위치드 인터페이스가 추가됩니다. 디바이스 컨피그레이션을 적용해야 변경 사항이 적용됩니다. 자세한 내용은 4-25페이지의 디바이스에 변경 사항 적용를 참조하십시오.

참고 물리적 인터페이스가 비활성화되면 그 물리적 인터페이스에 연결된 논리적 인터페이스도 비활성화됩니다.

논리적 스위치드 인터페이스 삭제

라이센스: 제어

지원되는 디바이스: Series 3

논리적 스위치드 인터페이스를 삭제하면 이 인터페이스가 상주하는 물리적 인터페이스뿐 아니라 연결된 가상 스위치 및 보안 영역에서도 제거됩니다.

스위치드 인터페이스를 삭제하려면

액세스: Admin/Network Admin

1단계 **Devices > Device Management**를 선택합니다.

Device Management 페이지가 나타납니다.

2단계 삭제할 스위치드 인터페이스가 있는 관리 대상 디바이스를 선택하고 그 디바이스의 수정 아이콘( )을 클릭합니다.

해당 디바이스의 Interfaces 탭이 나타납니다.

3단계 삭제할 논리적 스위치드 인터페이스 옆의 삭제 아이콘( )을 클릭합니다.

4단계 확인 메시지가 표시되면 인터페이스를 삭제할 것임을 확인합니다.

인터페이스가 삭제되었습니다. 디바이스 컨피그레이션을 적용해야 변경 사항이 적용됩니다. 자세한 내용은 4-25페이지의 디바이스에 변경 사항 적용를 참조하십시오.

가상 스위치 구성

라이센스: 제어

지원되는 디바이스: Series 3

레이어 2 구축에서 스위치드 인터페이스를 사용하려면 가상 스위치를 구성하고 여기에 스위치드 인터페이스를 지정해야 합니다. 가상 스위치는 네트워크를 지나는 인바운드 및 아웃바운드 트래픽을 처리하는 스위치드 인터페이스의 그룹입니다.

가상 스위치를 구성하는 것에 대한 자세한 내용은 다음 절을 참조하십시오.

- 6-6페이지의 가상 스위치 보기
- 6-6페이지의 가상 스위치 추가
- 6-7페이지의 고급 가상 스위치 설정 컨피그레이션
- 6-9페이지의 가상 스위치 삭제

가상 스위치 보기

라이센스: 제어

지원되는 디바이스: Series 3

Device Management 페이지의 Virtual Switches 탭은 디바이스에 구성한 모든 가상 스위치의 목록을 표시합니다. 여기에는 다음 표에 설명된 것과 같은 각 스위치에 대한 요약 정보가 포함됩니다.

표 6-1 가상 스위치 표 보기 필드

필드	설명
Name	가상 스위치의 이름
Interfaces	가상 스위치에 지정된 모든 스위치드 인터페이스. Interfaces 탭에서 비활성화한 인터페이스는 사용할 수 없습니다.
Hybrid Interface	선택 사항으로 구성되는 하이브리드 인터페이스로서 가상 스위치를 가상 라우터에 연결합니다.
Unicast Packets	가상 스위치에 대한 유니캐스트 패킷 통계로서 다음 항목을 포함합니다. • 수신된 유니캐스트 패킷 • 전달된 유니캐스트 패킷(호스트에 의해 삭제된 것 제외) • 의도치 않게 삭제된 유니캐스트 패킷
Broadcast Packets	가상 스위치에 대한 브로드캐스트 패킷 통계로서 다음 항목을 포함합니다. • 수신된 브로드캐스트 패킷 • 전달된 브로드캐스트 패킷 • 의도치 않게 삭제된 브로드캐스트 패킷

가상 스위치 추가

라이센스: 제어

지원되는 디바이스: Series 3

Device Management 페이지의 Virtual Switches 탭에서 가상 스위치를 추가할 수 있습니다. 스위치드 인터페이스를 구성할 때도 스위치를 추가할 수 있습니다.

가상 스위치에 스위치드 인터페이스만 지정할 수 있습니다. 관리 대상 디바이스에 스위치드 인터페이스를 구성하기 전에 가상 스위치를 생성하려는 경우 빈 가상 스위치를 만들고 나중에 여기에 인터페이스를 추가할 수 있습니다.

팁 기존 가상 스위치를 수정하려면 스위치 옆의 수정 아이콘()을 클릭합니다.

기존 가상 스위치에 대한 변경은 디바이스의 트래픽을 중단시킬 수 있습니다.

가상 스위치를 추가하려면

액세스: Admin/Network Admin

1단계 **Devices > Device Management**를 선택합니다.

Device Management 페이지가 나타납니다.

2단계 가상 스위치를 추가하려는 디바이스 옆의 수정 아이콘( )을 클릭합니다.

Interfaces 탭이 나타납니다.

3단계 **Virtual Switches**를 클릭합니다.

Virtual Switches 탭이 나타납니다.

4단계 **Add Virtual Switch**를 클릭합니다.

Add Virtual Switch 팝업 창이 나타납니다.

5단계 **Name** 필드에 가상 스위치의 이름을 입력합니다. 영숫자와 공백을 사용할 수 있습니다.

6단계 **Available**에서 가상 스위치에 추가할 스위치드 인터페이스를 하나 이상 선택합니다.

팁 Interfaces 탭에서 비활성화한 인터페이스는 사용할 수 없습니다. 인터페이스를 추가한 다음 비활성화하면 컨피그레이션에서 삭제됩니다.

7단계 **Add**를 클릭합니다.

8단계 **Hybrid Interface** 드롭다운 목록에서 가상 스위치를 가상 라우터에 연결하는 하이브리드 인터페이스를 선택할 수도 있습니다. 자세한 내용은 9-1페이지의 하이브리드 인터페이스 설정를 참조하십시오.

9단계 **Save**를 클릭합니다.

가상 스위치가 추가됩니다. 디바이스 컨피그레이션을 적용해야 변경 사항이 적용됩니다. 자세한 내용은 4-25페이지의 디바이스에 변경 사항 적용를 참조하십시오.

팁 스위치에 대해 고정 MAC 엔트리, 스패닝 트리와 같은 고급 설정을 구성하려면 6-7페이지의 고급 가상 스위치 설정 컨피그레이션를 참조하십시오.

고급 가상 스위치 설정 컨피그레이션

라이센스: 제어

지원되는 디바이스: Series 3

가상 스위치를 추가하거나 수정할 때 고정 MAC 엔트리를 추가하고 STP(Spanning Tree Protocol)를 활성화하고 BPDU(Bridge Protocol Data Unit)를 삭제하고 엄격한 TCP 적용을 활성화할 수 있습니다.

시간이 경과하면서 가상 스위치는 네트워크의 반환 트래픽에 태그를 지정하여 MAC 주소를 학습합니다. 수동으로 고정 MAC 엔트리를 추가할 수도 있습니다. 이는 MAC 주소가 특정 포트에 상주함을 지정합니다. 그 포트에서 트래픽을 수신하는지 여부와 무관하게 MAC 주소는 테이블에서 고정 상태를 유지합니다. 각 가상 스위치에 대해 하나 이상의 고정 MAC 주소를 지정할 수 있습니다.

STP는 네트워크 루프를 방지하는 데 사용하는 네트워크 프로토콜입니다. BPDU는 네트워크를 통해 교환되면서 네트워크 브리지에 대한 정보를 전달합니다. 네트워크에 이중 링크가 있을 경우 이 프로토콜에서는 BPDU를 사용하여 가장 빠른 네트워크 링크를 식별하고 선택합니다. 네트워크 링크가 실패할 경우 스패닝 트리는 기존 대체 링크에 장애 조치됩니다.

개별화된 라우터와 비슷하게 가상 스위치가 VLAN 간에 트래픽을 라우팅할 경우 BPDU는 다양한 논리적 스위치드 인터페이스를 통해 그러나 동일한 물리적 스위치드 인터페이스에서 디바이스에 들어오고 나갑니다. 그로 인해 STP는 디바이스를 이중 네트워크 루프로 식별하며, 이는 특정 레이어 2 구축에서 문제를 일으킬 수 있습니다. 이를 방지하기 위해 도메인 레벨에서 가상 스위치를 구성하여 트래픽을 모니터링할 때 디바이스에서 BPDU를 삭제하게 할 수 있습니다.

참고 Cisco에서는 디바이스 클러스터에 구축할 가상 스위치를 구성할 때는 STP를 활성화할 것을 권장합니다.

TCP 보안을 극대화하기 위해 엄격한 적용을 활성화할 수 있습니다. 그러면 3-way 핸드셰이크가 완료되지 않은 연결을 차단합니다. 엄격한 적용은 다음 항목도 차단합니다.

- 3-way 핸드셰이크가 완료되지 않은 연결의 비 SYN TCP 패킷
- TCP 연결의 responder가 SYN-ACK를 보내기 전에 initiator가 보낸 비 SYN/RST 패킷
- TCP 연결에서 SYN 이후에 그러나 세션이 설정되기 전에 responder가 보낸 비 SYN-ACK/RST 패킷
- 설정된 TCP 연결에서 initiator 또는 responder가 보낸 SYN 패킷

가상 스위치를 논리적 하이브리드 인터페이스와 연결할 경우 스위치는 논리적 하이브리드 인터페이스에 연결된 가상 라우터와 동일한 엄격한 TCP 적용 설정을 사용합니다. 이 경우에는 스위치에서 엄격한 TCP 적용을 지정할 수 없습니다.

고급 가상 스위치 설정을 구성하려면

액세스: Admin/Network Admin

1단계 **Devices > Device Management**를 선택합니다.

Device Management 페이지가 나타납니다.

2단계 수정하려는 가상 스위치가 있는 디바이스 옆의 수정 아이콘( )을 클릭합니다.

Interfaces 탭이 나타납니다.

3단계 **Virtual Switches**를 클릭합니다.

Virtual Switches 탭이 나타납니다.

4단계 수정하려는 가상 스위치 옆에서 수정 아이콘( )을 클릭합니다.

Edit Virtual Switch 팝업 창이 나타납니다.

5단계 **Advanced**를 클릭합니다.

Advanced 탭이 나타납니다.

6단계 고정 MAC 항목을 추가하려면 **Add**를 클릭합니다.

Add Static MAC Address 팝업 창이 나타납니다.

7단계 **MAC Address** 필드에서 2자리 16진수의 그룹 6개가 콜론으로 구분되는 표준 형식(예: 01:23:45:67:89:AB)을 사용하여 주소를 입력합니다.

참고 브로드캐스트 주소(00:00:00:00:00:00, FF:FF:FF:FF:FF:FF)는 고정 MAC 주소로 추가할 수 없습니다.

8단계 **Interface** 드롭다운 목록에서 MAC 주소를 지정하려는 인터페이스를 선택합니다.

9단계 **Add**를 클릭합니다.

MAC 주소가 Static MAC Entries 테이블에 추가됩니다.

MAC 주소를 수정하려면 수정 아이콘( )을 클릭합니다. MAC 주소를 삭제하려면 삭제 아이콘( )을 클릭합니다.

10단계 원한다면 **Enable Spanning Tree Protocol**을 선택하여 STP를 활성화합니다. 가상 스위치가 여러 네트워크 인터페이스 간에 트래픽을 전환할 때만 **Enable Spanning Tree Protocol**을 선택합니다.

Drop BPDUs를 선택하려면 **Enable Spanning Tree Protocol**을 선택을 취소해야 합니다.

11단계 **Strict TCP Enforcement**를 선택하여 엄격한 TCP 적용을 활성화할 수도 있습니다.

가상 스위치를 논리적 하이브리드 인터페이스와 연결할 경우, 이 옵션은 나타나지 않으며 스위치는 논리적 하이브리드 인터페이스에 연결된 가상 라우터와 동일한 설정을 사용합니다.

12단계 **Drop BPDUs**를 선택하여 도메인 레벨에서 BPDU를 삭제할 수도 있습니다. 가상 스위치가 단일 물리적 인터페이스에서 VLAN 간에 트래픽을 라우팅하는 경우에만 **Drop BPDUs**를 선택합니다.

Enable Spanning Tree Protocol을 선택하려면 **Drop BPDUs**의 선택을 취소해야 합니다.

13단계 **Save**를 클릭합니다.

변경 내용이 저장되었습니다. 디바이스 컨피그레이션을 적용해야 변경 사항이 적용됩니다. 자세한 내용은 4-25페이지의 디바이스에 변경 사항 적용를 참조하십시오.

가상 스위치 삭제

라이센스: 제어

지원되는 디바이스: Series 3

가상 스위치를 삭제할 때 그 스위치에 지정되었던 모든 스위치드 인터페이스는 다른 스위치에 포함될 수 있게 됩니다.

가상 스위치를 삭제하려면

액세스: Admin/Network Admin

1단계 **Devices > Device Management**를 선택합니다.

Device Management 페이지가 나타납니다.

2단계 삭제할 가상 스위치가 있는 관리 대상 디바이스를 선택하고 그 디바이스의 수정 아이콘( )을 클릭합니다.

해당 디바이스의 Interfaces 탭이 나타납니다.

3단계 **Virtual Switches**를 클릭합니다.

Virtual Switches 탭이 나타납니다.

4단계 삭제하려는 가상 스위치 옆에서 삭제 아이콘( )을 클릭합니다.

5단계 확인 메시지가 표시되면 가상 스위치를 삭제할 것임을 확인합니다.

가상 스위치가 삭제됩니다. 디바이스 컨피그레이션을 적용해야 변경 사항이 적용됩니다. 자세한 내용은 4-25페이지의 디바이스에 변경 사항 적용를 참조하십시오.

7장

가상 라우터 설정

레이어 3 구축에서 관리되는 디바이스를 구성하여 둘 이상의 인터페이스 간에 트래픽을 라우팅하게 할 수 있습니다. 트래픽을 라우팅하려면 IP 주소를 각 인터페이스로 할당하고 인터페이스를 가상 라우터에 할당해야 합니다. Series 3가 관리하는 디바이스에서 여러 물리적 인터페이스를 단일 논리적 라우티드 인터페이스로 그룹화할 수 있으며, 이를 LAG(link aggregation group)라고 합니다. 이 단일 종합 논리적 링크는 두 엔드포인트 간에 더 우수한 대역폭, 이중화, 로드 밸런싱을 제공합니다.

목적지 주소에 따라 패킷 전달 결정을 내려 패킷을 라우팅하도록 시스템을 구성할 수 있습니다. 라우티드 인터페이스로 구성된 인터페이스는 레이어 3 트래픽을 수신 및 전달합니다. 라우터는 전달 기준에 따라 발신 인터페이스에서 목적지를 확인하며 액세스 제어 규칙은 적용할 보안 정책을 지정합니다.

레이어 3 구축에서 고정 경로를 정의할 수 있습니다. 또한 RIP(Routing Information Protocol) 및 OSPF(Open Shortest Path First) 동적 라우팅 프로토콜을 구성할 수 있습니다. 고정 경로와 RIP 또는 고정 경로와 OSPF의 조합도 구성 가능합니다.

주의 어떤 이유로 레이어 3 구축에 실패할 경우 디바이스는 더 이상 트래픽을 전달하지 않습니다.

레이어 3 구축 구성에 대한 자세한 내용은 다음 절을 참조하십시오.

- 7-1페이지의 라우티드 인터페이스 구성
- 7-9페이지의 가상 라우터 구성
- 8-2페이지의 LAG 구성

라우티드 인터페이스 구성

라이센스: 제어

지원되는 디바이스: Series 3

물리적 또는 논리적 컨피그레이션으로 라우티드 인터페이스를 설정할 수 있습니다. 태그가 지정되지 않은 VLAN 트래픽을 처리하기 위해 물리적 라우티드 인터페이스를 구성할 수 있습니다. 또한 지정된 VLAN 태그가 포함된 트래픽을 처리하기 위해 논리적 라우티드 인터페이스를 만들 수 있습니다.

레이어 3 구축에서는 대기 중인 라우티드 인터페이스가 없는 외부 물리적 인터페이스에 수신된 트래픽은 모두 삭제됩니다. VLAN 태그가 없는 패킷이 수신되고 해당 포트에 대한 물리적 라우티드 인터페이스가 구성되지 않은 경우 패킷이 삭제됩니다. VLAN 태그가 있는 패킷이 수신되었지만 논리적 라우티드 인터페이스가 구성되지 않은 경우에도 패킷이 삭제됩니다.

스위치드 인터페이스에서 VLAN 태그와 함께 수신된 트래픽은 규칙 평가 또는 전달 결정에 앞서 인그레스에서 가장 바깥쪽의 VLAN 태그를 스트리핑하는 방법으로 처리됩니다. VLAN 태그 지정 논리적 라우티드 인터페이스를 통해 디바이스에서 전송되는 패킷은 이그레스에서 해당 VLAN 태그로 캡슐화됩니다. 스트리핑 프로세스가 끝난 후 VLAN 태그와 함께 수신된 모든 트래픽이 삭제됩니다.

상위 물리적 인터페이스를 인라인 또는 패시브로 변경할 경우 해당 논리적 인터페이스가 모두 삭제됩니다.

자세한 내용은 다음 절을 참조하십시오.

- 7-2페이지의 물리적 라우티드 인터페이스 구성
- 7-4페이지의 논리적 라우티드 인터페이스 추가
- 7-7페이지의 논리적 라우티드 인터페이스 삭제
- 7-7페이지의 SFRP 구성

물리적 라우티드 인터페이스 구성

라이센스: 제어

지원되는 디바이스: Series 3

관리 대상 디바이스에서 하나 이상의 물리적 포트를 라우티드 인터페이스로 구성할 수 있습니다. 가상 라우터에서 트래픽을 라우팅하려면 먼저 여기에 물리적 라우티드 인터페이스를 지정해야 합니다.

라우티드 인터페이스에 고정 ARP(Address Resolution Protocol) 항목을 추가할 수 있습니다. 외부 호스트가 로컬 네트워크에서 트래픽을 보낼 목적지 IP 주소의 MAC 주소를 알아야 할 경우 ARP 요청을 보냅니다. 고정 ARP 항목을 구성하면 가상 라우터는 IP 주소 및 해당 MAC 주소와 함께 응답합니다.

라우티드 인터페이스에 대해 **ICMP Enable Responses** 옵션을 비활성화하더라도 모든 시나리오에서 ICMP 응답이 차단되지는 않습니다. 목적지 IP가 라우티드 인터페이스의 IP이고 프로토콜이 ICMP일 때 패킷을 삭제하도록 액세스 제어 정책에 규칙을 추가할 수 있습니다. 15-1페이지의 네트워크 기반 규칙으로 트래픽 제어를 참조하십시오.

관리 대상 디바이스에서 **Inspect Local Router Traffic** 옵션을 활성화한 경우 호스트에 도달하기 전에 패킷을 삭제하므로 어떤 응답도 차단됩니다. 로컬 라우터 트래픽의 검사에 대한 자세한 내용은 4-54페이지의 고급 디바이스 설정 이해를 참조하십시오.

주의 MTU(최대 전송 단위)를 변경하면 디바이스의 트래픽이 중단되고 패킷이 삭제됩니다. MTU 설정 가능 범위는 FireSIGHT 시스템 디바이스 모델 및 인터페이스 유형에 따라 달라질 수 있습니다. 자세한 내용은 4-64페이지의 센싱 인터페이스 MTU 구성를 참조하십시오.

물리적 라우티드 인터페이스를 구성하려면

액세스: Admin/Network Admin

1단계 **Devices > Device Management**를 선택합니다.

Device Management 페이지가 나타납니다.

2단계 라우티드 인터페이스를 구성하려는 디바이스 옆의 수정 아이콘()을 클릭합니다.

해당 디바이스의 Interfaces 탭이 나타납니다.

3단계 라우티드 인터페이스로 구성하려는 인터페이스 옆의 수정 아이콘( )을 클릭합니다.

Edit Interface 팝업 창이 나타납니다.

4단계 라우티드 인터페이스 옵션을 표시하려면 **Routed**를 클릭합니다.

5단계 원한다면 **Security Zone** 드롭다운 목록에서 기존 보안 영역을 선택하거나 **New**를 선택하여 새 보안 영역을 추가합니다.

6단계 원한다면 **Virtual Router** 드롭다운 목록에서 기존 가상 라우터를 선택하거나 **New**를 선택하여 새 가상 라우터를 추가합니다.

새 가상 라우터를 추가할 경우 라우티드 인터페이스를 설정한 다음에 Device Management 페이지의 Virtual Routeres 탭(**Devices > Device Management > Virtual Routers**)에서 이를 구성해야 합니다. 7-9페이지의 가상 라우터 추가를 참조하십시오.

7단계 라우티드 인터페이스에서 트래픽을 처리할 수 있게 하려면 **Enabled** 확인란을 선택합니다.

이 확인란의 선택을 취소하면 인터페이스가 비활성화되어 사용자가 보안 목적으로 액세스할 수 없게 됩니다.

8단계 **Mode** 드롭다운 목록에서 링크 모드를 지정하는 옵션을 선택하거나 **Autonegotiation**을 선택하여 인터페이스에서 속도 및 양방향 설정 자동 협상이 구성되도록 지정합니다. 모드 설정은 카퍼 인터페이스에 대해서만 가능합니다.

참고 8000 Series 어플라이언스의 인터페이스는 반이중 옵션을 지원하지 않습니다.

9단계 **MDI/MDIX** 드롭다운 목록에서 옵션을 선택하여 인터페이스가 MDI(medium dependent interface), MDIX(medium dependent interface crossover) 또는 Auto-MDIX를 위해 구성되었는지 여부를 지정합니다. MDI/MDIX 설정은 카퍼 인터페이스에 대해서만 가능합니다.

일반적으로 MDI/MDIX는 Auto-MDIX로 설정됩니다. 그러면 MDI와 MDIX 간 스위칭을 자동으로 처리하여 링크를 확보합니다.

10단계 **MTU** 필드에 MTU를 입력합니다. 이는 허용되는 최대 크기 패킷을 나타냅니다. MTU는 레이어 3 MTU가 아니라 레이어 2 MTU/MRU입니다.

MTU 설정 가능 범위는 FireSIGHT 시스템 디바이스 모델 및 인터페이스 유형에 따라 달라질 수 있습니다. 자세한 내용은 4-64페이지의 센싱 인터페이스 MTU 구성를 참조하십시오.

11단계 인터페이스에서 ping, traceroute와 같은 ICMP 트래픽에 응답하는 것을 허용하려면 **ICMP** 옆의 **Enable Responses** 확인란을 선택합니다.

12단계 인터페이스에서 라우터 광고를 브로드캐스트하는 것을 허용하려면 **IPv6 NDP** 옆의 **Enable Router Advertisement** 확인란을 선택합니다.

13단계 IP 주소를 추가하려면 **Add**를 클릭합니다.

Add IP Address 팝업 창이 나타납니다.

14단계 **Address** 필드에 라우티드 인터페이스의 IP 주소와 서브넷 마스크를 CIDR 표기법으로 입력합니다. 다음에 유의하십시오.

- 네트워크 및 브로드캐스트 주소 또는 고정 MAC 주소 00:00:00:00:00:00 및 FF:FF:FF:FF:FF:FF를 추가할 수 없습니다.
- 서브넷 마스크와 상관없이 가상 라우터에 있는 인터페이스에 동일한 IP 주소를 추가할 수 없습니다.

15단계 IPv6 주소를 사용하는 경우, **IPv6** 필드 옆의 **Address Autoconfiguration** 확인란을 선택하여 인터페이스의 IP 주소를 자동으로 설정할 수도 있습니다.

16단계 **Type**으로는 Normal 또는 SFRP 중 하나를 선택합니다.

SFRP 옵션의 경우 7-7페이지의 SFRP 구성에서 자세한 내용을 참조하십시오.

17단계 **OK**를 클릭합니다.

IP 주소가 추가되었습니다.

IP 주소를 수정하려면 수정 아이콘( )을 클릭합니다. IP 주소를 삭제하려면 삭제 아이콘( )을 클릭합니다.

참고 클러스터링된 디바이스의 라우티드 인터페이스에 IP 주소를 추가할 때 클러스터 피어의 라우티드 인터페이스에 해당 IP 주소를 추가해야 합니다.

18단계 고정 ARP 항목을 추가하려면 **Add**를 클릭합니다.

Add Static ARP Entry 팝업 창이 나타납니다.

19단계 **IP Address** 필드에 고정 ARP 항목의 IP 주소를 입력합니다.

20단계 **MAC Address** 필드에 IP 주소와 연결할 MAC 주소를 입력합니다. 2자리 16진수의 그룹 6개가 콜론으로 구분되는 표준 형식(예: 01:23:45:67:89:AB)을 사용하여 주소를 입력합니다.

21단계 **OK**를 클릭합니다.

고정 ARP 항목이 추가되었습니다.

팁 고정 ARP 항목을 수정하려면 수정 아이콘( )을 클릭합니다. 고정 ARP 항목을 삭제하려면 삭제 아이콘( )을 클릭합니다.

22단계 **Save**를 클릭합니다.

물리적 라우티드 인터페이스가 구성되었습니다. 디바이스 컨피그레이션을 적용해야 변경 사항이 적용됩니다. 4-25페이지의 디바이스에 변경 사항 적용를 참조하십시오.

논리적 라우티드 인터페이스 추가

라이센스: 제어

지원되는 디바이스: Series 3

각 물리적 라우티드 인터페이스에 대해 여러 논리적 라우티드 인터페이스를 추가할 수 있습니다. 물리적 인터페이스에서 VLAN 태그와 함께 수신된 트래픽을 처리하려면 각 논리적 인터페이스를 해당 태그와 연결해야 합니다. 트래픽을 라우팅하려면 가상 라우터에 논리적 라우티드 인터페이스를 지정해야 합니다.

라우티드 인터페이스에 대해 **ICMP Enable Responses** 옵션을 비활성화하더라도 모든 시나리오에서 ICMP 응답이 차단되지는 않습니다. 목적지 IP가 라우티드 인터페이스의 IP이고 프로토콜이 ICMP일 때 패킷을 삭제하도록 액세스 제어 정책에 규칙을 추가할 수 있습니다. 15-1페이지의 네트워크 기반 규칙으로 트래픽 제어를 참조하십시오.

관리 대상 디바이스에서 **Inspect Local Router Traffic** 옵션을 활성화한 경우 호스트에 도달하기 전에 패킷을 삭제하므로 어떤 응답도 차단됩니다. 로컬 라우터 트래픽의 검사에 대한 자세한 내용은 4-54페이지의 고급 디바이스 설정 이해를 참조하십시오.

주의 MTU(maximum transmission unit)를 변경하면 디바이스의 트래픽이 중단되고 패킷이 삭제됩니다. MTU 설정 가능 범위는 FireSIGHT 시스템 디바이스 모델 및 인터페이스 유형에 따라 달라질 수 있습니다. 자세한 내용은 4-64페이지의 센싱 인터페이스 MTU 구성를 참조하십시오.

기존 라우티드 인터페이스를 수정하려면 인터페이스 옆의 수정 아이콘( )을 클릭합니다.

논리 라우티드 인터페이스를 추가하려면

액세스: Admin/Network Admin

1단계 **Devices > Device Management**를 선택합니다.

Device Management 페이지가 나타납니다.

2단계 라우티드 인터페이스를 추가하려는 디바이스 옆의 수정 아이콘( )을 클릭합니다.

해당 디바이스의 Interfaces 탭이 나타납니다.

3단계 **Add Interface**를 클릭합니다.

Add Interface 팝업 창이 나타납니다.

4단계 라우티드 인터페이스 옵션을 표시하려면 **Routed**를 클릭합니다.

5단계 **Interface** 드롭다운 목록에서 논리적 인터페이스를 추가할 물리적 인터페이스를 선택합니다.

6단계 **VLAN Tag** 필드에 이 인터페이스의 인바운드 및 아웃바운드 트래픽에 지정된 태그 값을 입력합니다. 이 값으로는 1과 4094 사이의 임의의 정수를 사용할 수 있습니다.

7단계 원한다면 **Security Zone** 드롭다운 목록에서 기존 보안 영역을 선택하거나 **New**를 선택하여 새 보안 영역을 추가합니다.

8단계 원한다면 **Virtual Router** 드롭다운 목록에서 기존 가상 라우터를 선택하거나 **New**를 선택하여 새 가상 라우터를 추가합니다.

새 가상 라우터를 추가할 경우 라우티드 인터페이스 설정을 마친 다음에 Device Management 페이지(**Devices > Device Management > Virtual Routers**)에서 이를 구성해야 합니다. 7-9페이지의 가상 라우터 추가를 참조하십시오.

9단계 라우티드 인터페이스에서 트래픽을 처리할 수 있게 하려면 **Enabled** 확인란을 선택합니다.

확인란의 선택을 취소할 경우 인터페이스는 비활성화되고 관리상 다운됩니다. 물리적 인터페이스를 비활성화할 경우 그와 연결된 모든 논리적 인터페이스도 비활성화됩니다.

10단계 **MTU** 필드에 MTU를 입력합니다. 이는 허용되는 최대 크기 패킷을 나타냅니다. MTU는 레이어 3 MTU가 아니라 레이어 2 MTU/MRU입니다.

MTU 설정 가능 범위는 FireSIGHT 시스템 디바이스 모델 및 인터페이스 유형에 따라 달라질 수 있습니다. 자세한 내용은 4-64페이지의 센싱 인터페이스 MTU 구성를 참조하십시오.

11단계 업데이트 또는 오류 정보를 다른 라우터, 중간 디바이스 또는 호스트에 전달하려면 **ICMP** 옆의 **Enable Responses** 확인란을 선택합니다.

12단계 인터페이스에서 라우터 광고를 브로드캐스트하는 것을 허용하려면 **IPv6 NDP** 옆의 **Enable Router Advertisement** 확인란을 선택합니다.

13단계 IP 주소를 추가하려면 **Add**를 클릭합니다.

Add IP Address 팝업 창이 나타납니다.

14단계 **Address** 필드에 IP 주소를 CIDR 표기법으로 입력합니다. 다음에 유의하십시오.

- 네트워크 및 브로드캐스트 주소 또는 고정 MAC 주소 00:00:00:00:00:00 및 FF:FF:FF:FF:FF:FF를 추가할 수 없습니다.
- 가상 라우터에 있는 인터페이스에, 서브넷 마스크와 무관하게, 동일한 IP 주소를 추가할 수 없습니다.

15단계 IPv6 주소를 사용하는 경우, **IPv6** 필드 옆의 **Address Autoconfiguration** 확인란을 선택하여 인터페이스의 IP 주소를 자동으로 설정할 수도 있습니다.

16단계 **Type**으로는 Normal 또는 SFRP 중 하나를 선택합니다.

SFRP 옵션의 경우 7-7페이지의 SFRP 구성에서 자세한 내용을 참조하십시오.

17단계 **OK**를 클릭합니다.

IP 주소가 추가되었습니다.

IP 주소를 수정하려면 수정 아이콘( )을 클릭합니다. IP 주소를 삭제하려면 삭제 아이콘( )을 클릭합니다.

참고 클러스터링된 디바이스의 라우티드 인터페이스에 IP 주소를 추가할 때 클러스터 피어의 라우티드 인터페이스에 해당 IP 주소를 추가해야 합니다.

18단계 고정 ARP 항목을 추가하려면 **Add**를 클릭합니다.

Add Static ARP Entry 팝업 창이 나타납니다.

19단계 **IP Address** 필드에 고정 ARP 항목의 IP 주소를 입력합니다.

20단계 **MAC Address** 필드에 IP 주소와 연결할 MAC 주소를 입력합니다. 2자리 16진수의 그룹 6개가 콜론으로 구분되는 표준 형식(예: 01:23:45:67:89:AB)을 사용하여 주소를 입력합니다.

21단계 **OK**를 클릭합니다.

고정 ARP 항목이 추가되었습니다.

팁 고정 ARP 항목을 수정하려면 수정 아이콘( )을 클릭합니다. 고정 ARP 항목을 삭제하려면 삭제 아이콘( )을 클릭합니다.

22단계 **Save**를 클릭합니다.

논리적 라우티드 인터페이스가 추가됩니다. 디바이스 컨피그레이션을 적용해야 변경 사항이 적용됩니다. 4-25페이지의 디바이스에 변경 사항 적용를 참조하십시오.

참고 물리적 인터페이스가 비활성화되면 그 물리적 인터페이스에 연결된 논리적 인터페이스도 비활성화됩니다.

논리적 라우티드 인터페이스 삭제

라이센스: 제어

지원되는 디바이스: Series 3

논리적 라우티드 인터페이스를 삭제하면 그 인터페이스가 상주하는 물리적 인터페이스뿐 아니라 지정된 가상 라우터 및 보안 영역에서도 제거됩니다.

라우티드 인터페이스를 삭제하려면

액세스: Admin/Network Admin

1단계 **Devices > Device Management**를 선택합니다.

Device Management 페이지가 나타납니다.

2단계 라우티드 인터페이스를 삭제하려는 디바이스 옆의 수정 아이콘( )을 클릭합니다.

해당 디바이스의 Interfaces 탭이 나타납니다.

3단계 삭제할 논리적 라우티드 인터페이스 옆의 삭제 아이콘( )을 클릭합니다.

4단계 확인 메시지가 표시되면 인터페이스를 삭제할 것임을 확인합니다.

인터페이스가 삭제되었습니다. 디바이스 컨피그레이션을 적용해야 변경 사항이 적용됩니다. 4-25페이지의 디바이스에 변경 사항 적용를 참조하십시오.

SFRP 구성

라이센스: 제어

지원되는 디바이스: Series 3

디바이스 클러스터 또는 개별 디바이스에서 고가용성을 위한 네트워크 이중화를 구현하기 위해 Cisco Redundancy Protocol(SFRP)을 구성할 수 있습니다. SFRP는 IPv4 및 IPv6 주소 모두에 게이트웨이 이중화를 제공합니다. 라우티드 인터페이스와 하이브리드 인터페이스에서 SFRP를 구성할 수 있습니다.

인터페이스가 개별 디바이스에서 구성되는 경우 동일한 브로드캐스트 도메인에 있어야 합니다. 인터페이스 중 하나 이상을 마스터로, 같은 수를 백업으로 지정해야 합니다. IP 주소당 마스터 1개와 백업 1개만 지원됩니다. 네트워크 연결이 끊길 경우 자동으로 백업이 마스터가 되어 연결을 유지합니다.

SFRP에 대해 설정하는 옵션이 SFRP 인터페이스 그룹의 모든 인터페이스에서 동일해야 합니다. 하나의 그룹에 속한 여러 IP 주소는 동일한 마스터/백업 상태여야 합니다. 따라서 IP 주소를 추가하거나 수정할 때 그 주소에 대해 설정한 상태가 그룹의 모든 주소에 전파됩니다. 보안을 위해 그룹의 인터페이스끼리 공유되는 **Group ID** 및 **Shared Secret**의 값을 입력해야 합니다.

가상 라우터에서 SFRP IP 주소를 활성화하려면 비 SFRP IP 주소도 하나 이상 구성해야 합니다.

클러스터링된 디바이스의 경우 공유 암호를 지정하며, 시스템에서는 SFRP IP 컨피그레이션과 함께 클러스터 피어에 복사합니다. 공유 암호는 피어 데이터를 인증합니다.

클러스터링 디바이스에 대한 자세한 내용은 4-29페이지의 디바이스 클러스터링를 참조하십시오.

SFRP를 구성하려면

액세스: Admin/Network Admin

1단계 **Devices > Device Management**를 선택합니다.

Device Management 페이지가 나타납니다.

2단계 SFRP를 구성하려는 디바이스 옆의 수정 아이콘( )을 클릭합니다.

해당 디바이스의 Interfaces 탭이 나타납니다.

3단계 SFRP를 구성하려는 인터페이스 옆의 수정 아이콘( )을 클릭합니다.

Edit Interface 팝업 창이 나타납니다.

4단계 SFRP를 구성하려는 인터페이스 유형을 선택합니다.

- 라우티드 인터페이스 옵션을 표시하려면 **Routed**를 클릭합니다.
- 하이브리드 인터페이스 옵션을 표시하려면 **Hybrid**를 클릭합니다.

5단계 IP 주소를 추가하거나 수정하면서 SFRP를 구성할 수 있습니다.

- IP 주소를 추가하려면 **Add**를 클릭합니다.
- IP 주소를 수정하려면 수정 아이콘( )을 클릭합니다.

Add IP Address 또는 Edit IP Address 팝업 창이 나타납니다.

6단계 **Type**에서 **SFRP**를 선택하여 SFRP 옵션을 표시합니다.

7단계 **Group ID** 필드에 SFRP에 대해 구성된 마스터 또는 백업 인터페이스 그룹을 지정하는 값을 입력합니다.

8단계 **Priority**에서는 **Master** 또는 **Backup**을 선택하여 선호하는 인터페이스를 지정합니다.

- 개별 디바이스에 대해 인터페이스 하나를 한 디바이스의 마스터로, 다른 하나는 2번째 디바이스의 백업으로 설정해야 합니다.
- 디바이스 클러스터의 경우 한 인터페이스를 마스터로 설정하면 다른 하나는 자동으로 백업이 됩니다.

9단계 **Shared Secret** 필드에 공유 암호를 입력합니다.

디바이스 클러스터의 그룹에 대해 Shared Secret 필드가 자동으로 채워집니다.

10단계 **Adv. Interval (seconds)** 필드에 레이어 3 트래픽의 경로 광고 간격을 입력합니다.

11단계 **OK**를 클릭합니다.

IP 주소가 추가되거나 수정됩니다.

12단계 **Save**를 클릭합니다.

변경 내용이 저장되었습니다. 디바이스 컨피그레이션을 적용해야 변경 사항이 적용됩니다. 4-25페이지의 디바이스에 변경 사항 적용를 참조하십시오.

가상 라우터 구성

라이센스: 제어

지원되는 디바이스: Series 3

레이어 3 구축에서 라우티드 인터페이스를 사용하려면 가상 라우터를 구성하고 여기에 라우티드 인터페이스를 지정해야 합니다. 가상 라우터는 레이어 3 트래픽을 라우팅하는 라우티드 인터페이스의 그룹입니다.

가상 라우터를 구성하는 것에 대한 자세한 내용은 다음 절을 참조하십시오.

가상 라우터 보기

라이센스: 제어

지원되는 디바이스: Series 3

Device Management 페이지의 Virtual Routers 탭**(Devices > Device Management > Virtual Routers)**에는 디바이스에서 구성한 모든 가상 라우터의 목록이 표시됩니다. 여기에는 다음 표에 설명된 것과 같은 각 라우터에 대한 요약 정보가 포함됩니다.

표 7-1 가상 라우터 표 보기 필드

필드	설명
Name	가상 라우터의 이름
Interfaces	가상 라우터에 지정된 모든 라우티드 인터페이스의 목록. Interfaces 탭에서 인터페이스를 비활성화하면 인터페이스가 제거됩니다.
Protocols	가상 라우터에서 현재 사용 중인 프로토콜이며, 다음 중 하나입니다. • Static • Static, RIP • Static, OSPF

가상 라우터 추가

라이센스: 제어

지원되는 디바이스: Series 3

Device Management 페이지의 Virtual Routers 탭에서 가상 라우터를 추가할 수 있습니다. 라우티드 인터페이스를 구성할 때도 라우터를 추가할 수 있습니다.

가상 라우터에 라우티드 인터페이스와 하이브리드 인터페이스만 지정할 수 있습니다. 관리 대상 디바이스에 인터페이스를 구성하기 전에 가상 라우터를 생성하려는 경우 빈 가상 라우터를 만들고 나중에 여기에 인터페이스를 추가할 수 있습니다.

TCP 보안을 극대화하기 위해 엄격한 적용을 활성화할 수 있습니다. 그러면 3-way 핸드셰이크가 완료되지 않은 연결을 차단합니다. 엄격한 적용은 다음 항목도 차단합니다.

- 3-way 핸드셰이크가 완료되지 않은 연결의 비 SYN TCP 패킷
- TCP 연결의 responder가 SYN-ACK를 보내기 전에 initiator가 보낸 비 SYN/RST 패킷
- TCP 연결에서 SYN 이후에, 그러나 세션이 설정되기 전에 responder가 보낸 비 SYN-ACK/RST 패킷
- 설정된 TCP 연결에서 initiator 또는 responder가 보낸 SYN 패킷

레이어 3 인터페이스의 컨피그레이션을 비 레이어 3 인터페이스로 변경하거나 가상 라우터에서 레이어 3 인터페이스를 제거할 경우 라우터는 무효 상태가 될 수 있습니다. 예를 들어 DHCPv6에서 사용되는 경우 업스트림 및 다운스트림의 불일치를 유발할 수 있습니다. 기존 가상 라우터에 대한 변경은 디바이스의 트래픽을 중단시킬 수 있습니다.

팁 기존 가상 라우터를 수정하려면 라우터 옆의 수정 아이콘( )을 클릭합니다.

일반 옵션 이외의 여러 다양한 방법으로 가상 라우터를 구성할 수 있습니다. 이 컨피그레이션에 대한 자세한 내용은 다음 절을 참조하십시오.

- 7-11페이지의 DHCP 릴레이 설정
- 7-13페이지의 고정 경로 설정
- 7-15페이지의 동적 라우팅 설정
- 7-15페이지의 RIP 컨피그레이션 설정
- 7-20페이지의 OSPF 컨피그레이션 설정
- 7-28페이지의 가상 라우터 필터 설정
- 7-30페이지의 가상 라우터 인증 프로필 추가

가상 라우터를 추가하려면

액세스: Admin/Network Admin

1단계 **Devices > Device Management**를 선택합니다.

Device Management 페이지가 나타납니다.

2단계 가상 라우터를 추가하려는 디바이스 옆의 수정 아이콘( )을 클릭합니다.

해당 디바이스의 Interfaces 탭이 나타납니다.

3단계 **Virtual Routers**를 클릭합니다.

Virtual Routers 탭이 나타납니다.

팁 디바이스가 클러스터링 스택 구축에 포함된 경우 **Selected Device** 드롭다운 목록에서 수정할 스택을 선택합니다.

4단계 **Add Virtual Router**를 클릭합니다.

Add Virtual Router 팝업 창이 나타납니다.

5단계 **Name** 필드에 가상 라우터의 이름을 입력합니다. 영숫자와 공백을 사용할 수 있습니다.

6단계 가상 라우터에서 IPv6 고정 라우팅, OSPFv3, RIPng을 활성화하려면 **IPv6 Support** 확인란을 선택합니다. 이러한 기능을 비활성화하려면 확인란의 선택을 취소합니다.

7단계 엄격한 TCP 적용을 활성화하지 않으려면 **Strict TCP Enforcement**의 선택을 취소할 수 있습니다.

이 옵션은 기본적으로 활성화되어 있습니다.

8단계 **Interfaces**에서 **Available** 목록에는 가상 라우터에 지정할 수 있는 디바이스의 모든 활성 레이어 3 인터페이스(라우티드 및 하이브리드)가 있습니다. 가상 라우터에 지정할 인터페이스를 하나 이상 선택하고 **Add**를 클릭합니다.

팁 가상 라우터에서 라우티드 또는 하이브리드 인터페이스를 제거하려면 삭제 아이콘( )을 클릭합니다. Interfaces 탭에서 구성된 인터페이스를 비활성화해도 제거됩니다.

9단계 **Save**를 클릭합니다.

가상 라우터가 추가됩니다. 디바이스 컨피그레이션을 적용해야 변경 사항이 적용됩니다. 4-25페이지의 디바이스에 변경 사항 적용를 참조하십시오.

DHCP 릴레이 설정

라이센스: 제어

지원되는 디바이스: Series 3

DHCP는 인터넷 호스트에 컨피그레이션 파라미터를 제공합니다. 아직 IP 주소를 획득하지 않은 DHCP 클라이언트는 브로드캐스트 도메인 바깥의 DHCP 서버와 직접 통신할 수 없습니다. DHCP 클라이언트와 DHCP 서버의 통신을 허용하기 위해 클라이언트가 서버와 동일한 브로드캐스트 도메인에 있지 않은 경우를 처리하도록 DHCP 릴레이 인스턴스를 구성할 수 있습니다.

구성하는 각 가상 라우터에 대해 DHCP 릴레이를 설정할 수 있습니다. 기본적으로 이 기능은 비활성화됩니다. DHCPv4 릴레이 또는 DHCPv6 릴레이 중 하나를 활성화할 수 있습니다.

자세한 내용은 다음 절을 참조하십시오.

- 7-11페이지의 DHCPv4 릴레이 설정
- 7-12페이지의 DHCPv6 릴레이 설정

DHCPv4 릴레이 설정

라이센스: 제어

지원되는 디바이스: Series 3

다음 절차에서는 가상 라우터에서 DHCPv4 릴레이를 설정하는 방법에 대해 설명합니다.

DHCPv4 릴레이를 설정하려면

액세스: Admin/Network Admin

1단계 **Devices > Device Management**를 선택합니다.

Device Management 페이지가 나타납니다.

2단계 DHCP 릴레이를 설정하려는 디바이스 옆의 수정 아이콘( )을 클릭합니다.

해당 디바이스의 Interfaces 탭이 나타납니다.

3단계 **Virtual Routers**를 클릭합니다.

Virtual Routers 탭이 나타납니다.

4단계 DHCP 릴레이를 설정하려는 가상 라우터 옆의 수정 아이콘( )을 클릭합니다.

Edit Virtual Router 팝업 창이 나타납니다.

5단계 DHCPv4에 대한 DHCP 릴레이를 설정하려면 **DHCPv4** 확인란을 선택합니다.

6단계 **Servers** 필드에 서버 IP 주소를 입력합니다.

7단계 **Add**를 클릭합니다.

IP 주소가 **Servers** 필드에 추가됩니다. 최대 4개의 DHCP 서버를 추가할 수 있습니다.

팁 DHCP 서버를 삭제하려면 서버 IP 주소 옆의 삭제 아이콘( )을 클릭합니다.

8단계 **Max Hops** 필드에 1과 255 사이의 값으로 최대 홉 수를 입력합니다.

9단계 **Save**를 클릭합니다.

변경 내용이 저장되었습니다. 디바이스 컨피그레이션을 적용해야 변경 사항이 적용됩니다. 4-25페이지의 디바이스에 변경 사항 적용를 참조하십시오.

DHCPv6 릴레이 설정

라이센스: 제어

지원되는 디바이스: Series 3

다음 절차에서는 가상 라우터에서 DHCPv6 릴레이를 설정하는 방법에 대해 설명합니다.

참고 동일한 디바이스에서 실행되는 둘 이상의 가상 라우터를 통해 DHCPv6 릴레이 체인을 실행할 수 없습니다.

DHCPv6 릴레이를 설정하려면

액세스: Admin/Network Admin

1단계 **Devices > Device Management**를 선택합니다.

Device Management 페이지가 나타납니다.

2단계 DHCP 릴레이를 설정하려는 디바이스 옆의 수정 아이콘( )을 클릭합니다.

해당 디바이스의 Interfaces 탭이 나타납니다.

3단계 **Virtual Routers**를 클릭합니다.

Virtual Routers 탭이 나타납니다.

4단계 DHCP 릴레이를 설정하려는 가상 라우터 옆의 수정 아이콘( )을 클릭합니다.

Edit Virtual Router 팝업 창이 나타납니다.

5단계 DHCPv6에 대한 DHCP 릴레이를 설정하려면 **DHCPv6** 확인란을 선택합니다.

6단계 **Interfaces** 필드에서 가상 라우터에 지정된 하나 이상의 인터페이스 옆 확인란을 선택합니다.

팁 DHCPv6 릴레이를 위해 구성된 상태의 인터페이스는 Interfaces 탭에서 비활성화할 수 없습니다. 먼저 DHCPv6 릴레이 인터페이스 확인란의 선택을 취소하고 컨피그레이션을 저장해야 합니다.

7단계 선택된 인터페이스 옆의 드롭다운 아이콘을 클릭하고 인터페이스가 **Upstream**, **Downstream** 또는 **Both** 로 DHCP 요청을 릴레이할지 선택합니다.

하나 이상의 다운스트림 인터페이스와 업스트림 인터페이스를 포함해야 합니다. 둘 다 선택하면 인터페이스가 다운스트림과 업스트림 모두 해당됩니다.

8단계 **Max Hops** 필드에 최대 홉 수를 1과 255 사이의 값으로 입력합니다.

9단계 **Save**를 클릭합니다.

변경 내용이 저장되었습니다. 디바이스 컨피그레이션을 적용해야 변경 사항이 적용됩니다. 4-25페이지의 디바이스에 변경 사항 적용를 참조하십시오.

고정 경로 설정

라이센스: 제어

지원되는 디바이스: Series 3

고정 라우팅에서는 라우터를 지나는 트래픽의 IP 주소에 대한 규칙을 작성할 수 있습니다. 이는 가상 라우터의 경로를 선택하는 가장 간단한 방법입니다. 네트워크의 현재 토폴로지와 관련하여 다른 라우터와 통신하지 않기 때문입니다.

자세한 내용은 다음 절을 참조하십시오.

- 7-13페이지의 고정 경로 표 보기 이해
- 7-14페이지의 고정 경로 추가

고정 경로 표 보기 이해

라이센스: 제어

지원되는 디바이스: Series 3

Virtual Router 편집기의 Static Routes 탭에는 가상 라우터에서 구성한 모든 고정 경로의 목록이 표시됩니다. 여기에는 다음 표에 설명된 것과 같은 각 경로에 대한 요약 정보가 포함됩니다.

표 7-2 고정 경로 표 보기 필드

필드	설명
Enabled	이 경로가 현재 활성화되었는지 아니면 비활성화되었는지 지정합니다.
Name	고정 경로의 이름
Destination	트래픽이 라우팅되는 목적지 네트워크

표 7-2 고정 경로 표 보기 필드(계속)

필드	설명
Type	이 경로에 대해 수행된 작업을 지정하며, 이는 다음 중 하나입니다. • IP — 인접 라우터의 주소에 패킷을 전달하도록 지정합니다. • Interface — 직접 연결된 네트워크의 호스트로 트래픽을 라우팅하는 인터페이스에 패킷을 전달하도록 지정합니다. • Discard — 패킷을 삭제하거나 도달 불가로 반환하거나 관리상 금지의 이유로 반환하도록 지정합니다.
Gateway	IP를 고정 경로 유형으로 선택한 경우는 대상 IP 주소이고, Interface를 고정 경로 유형으로 선택한 경우는 인터페이스입니다.
Preference	경로 선택 사항을 결정합니다. 동일한 목적지에 여러 경로가 있을 경우 우선 순위가 더 높은 경로를 선택합니다.

고정 경로 추가

라이센스: 제어

지원되는 디바이스: Series 3

다음 절차에서는 고정 경로를 추가하는 방법에 대해 설명합니다.

고정 경로를 수정하려면 수정 아이콘( )을 클릭합니다. 고정 경로를 삭제하려면 삭제 아이콘( )을 클릭합니다.

고정 경로를 추가하려면

액세스: Admin/Network Admin

1단계 **Devices > Device Management**를 선택합니다.

Device Management 페이지가 나타납니다.

2단계 고정 경로를 추가하려는 디바이스 옆의 수정 아이콘( )을 클릭합니다.

해당 디바이스의 Interfaces 탭이 나타납니다.

3단계 **Virtual Routers**를 클릭합니다.

Virtual Routers 탭이 나타납니다.

4단계 고정 경로를 추가하려는 가상 라우터 옆의 수정 아이콘( )을 클릭합니다.

Edit Virtual Router 팝업 창이 나타납니다.

5단계 **Static**을 클릭하여 고정 경로 옵션을 표시합니다.

6단계 **Add Static Route**를 클릭합니다.

Add Static Route 팝업 창이 나타납니다.

7단계 **Route Name** 필드에 고정 경로의 이름을 입력합니다. 영숫자와 공백을 사용할 수 있습니다.

8단계 **Enabled**에서는 확인란을 선택하여 경로가 현재 활성화되었음을 나타냅니다.

9단계 **Preference** 필드에는 경로 선택을 결정하기 위해 1과 65535 사이의 숫자 값을 입력합니다.

동일한 목적지에 여러 경로가 있을 경우 우선 순위가 더 높은 경로를 선택합니다.

10단계 **Type** 드롭다운 목록에서 구성하고 있는 고정 경로의 유형을 선택합니다.

11단계 **Destination** 필드에 트래픽을 라우팅할 목적지 네트워크의 IP 주소를 입력합니다.

12단계 **Gateway** 필드에서는 2가지 옵션이 있습니다.

- **IP**를 고정 경로 유형으로 선택한 경우 IP 주소를 입력합니다.
- **Interface**를 고정 경로 유형으로 선택한 경우 드롭다운 목록에서 활성화된 인터페이스를 선택합니다.

팁 Interfaces 탭에서 비활성화한 인터페이스는 사용할 수 없습니다. 추가한 인터페이스를 비활성화하면 그 인터페이스는 컨피그레이션에서 제거됩니다.

13단계 **OK**를 클릭합니다.

고정 경로가 추가되었습니다.

14단계 **Save**를 클릭합니다.

변경 내용이 저장되었습니다. 디바이스 컨피그레이션을 적용해야 변경 사항이 적용됩니다. 4-25페이지의 디바이스에 변경 사항 적용를 참조하십시오.

동적 라우팅 설정

라이센스: 제어

지원되는 디바이스: Series 3

동적, 즉 적응형 라우팅은 네트워크 조건의 변경에 대응하여 라우팅 프로토콜을 통해 경로를 변경합니다. 이러한 적응으로 최대한 많은 경로가 유효한 상태로 유지될 수 있습니다. 즉 변경에 대응하여 연결 가능한 목적지를 갖게 됩니다. 그러면 네트워크는 다른 경로 선택이 가능한 한 노드 손실, 노드 간 연결 끊김과 같은 피해를 "최소화하는 라우팅"이 가능해집니다. 어떤 라우터를 동적 라우팅 없이 구성하거나 RIP(Routing Information Protocol) 또는 OSPF(Open Shortest Path First) 라우팅 프로토콜을 구성할 수 있습니다.

자세한 내용은 다음 절을 참조하십시오.

- 7-15페이지의 RIP 컨피그레이션 설정
- 7-20페이지의 OSPF 컨피그레이션 설정

RIP 컨피그레이션 설정

라이센스: 제어

지원되는 디바이스: Series 3

RIP는 소규모 IP 네트워크를 위해 설계된 동적 라우팅 프로토콜로서 홉 수에 따라 경로를 결정합니다. 최상의 경로는 가장 적은 수의 홉을 사용합니다. RIP에 허용되는 최대 홉의 수는 15입니다. 이러한 홉 제한에 의해 RIP에서 지원할 수 있는 네트워크 크기도 제한됩니다.

RIP를 구성하는 것에 대한 자세한 내용은 다음 절을 참조하십시오.

- 7-16페이지의 RIP 컨피그레이션에 대한 인터페이스 추가
- 7-17페이지의 RIP 컨피그레이션의 인증 설정 구성
- 7-17페이지의 RIP 컨피그레이션의 고급 설정 구성
- 7-18페이지의 RIP 컨피그레이션에 대한 가져오기 필터 추가
- 7-19페이지의 RIP 컨피그레이션에 대한 내보내기 필터 추가

RIP 컨피그레이션에 대한 인터페이스 추가

라이센스: 제어

지원되는 디바이스: Series 3

RIP를 구성할 때 RIP를 구성하려는 가상 라우터에 이미 포함된 인터페이스 중에서 선택해야 합니다. 비활성화된 인터페이스는 사용할 수 없습니다.

RIP 인터페이스를 수정하려면 수정 아이콘( )을 클릭합니다. RIP 인터페이스를 삭제하려면 삭제 아이콘( )을 클릭합니다.

RIP 컨피그레이션에 대한 인터페이스를 추가하려면

액세스: Admin/Network Admin

1단계 **Devices > Device Management**를 선택합니다.

Device Management 페이지가 나타납니다.

2단계 RIP 인터페이스를 추가하려는 디바이스 옆의 수정 아이콘( )을 클릭합니다.

해당 디바이스의 Interfaces 탭이 나타납니다.

3단계 **Virtual Routers**를 클릭합니다.

Virtual Routers 탭이 나타납니다.

4단계 RIP 인터페이스를 추가하려는 가상 라우터 옆의 수정 아이콘( )을 클릭합니다.

Edit Virtual Router 팝업 창이 나타납니다.

5단계 **Dynamic Routing**을 클릭하여 동적 라우팅 옵션을 표시합니다.

6단계 **RIP**를 클릭하여 RIP 옵션을 표시합니다.

7단계 **Interfaces**에서 추가 아이콘( )을 클릭합니다.

Add an Interface 팝업 창이 나타납니다.

8단계 **Name** 드롭다운 목록에서 RIP를 구성하려는 인터페이스를 선택합니다.

팁 Interfaces 탭에서 비활성화한 인터페이스는 사용할 수 없습니다. 추가한 인터페이스를 비활성화하면 그 인터페이스는 컨피그레이션에서 제거됩니다.

9단계 **Metric** 필드에 인터페이스의 메트릭을 입력합니다. 여러 RIP 인스턴스의 경로가 사용 가능하고 모두 우선 순위가 동일할 경우 메트릭이 가장 낮은 경로가 우선 경로가 됩니다.

10단계 **Mode** 드롭다운 목록에서 다음 옵션 중 하나를 선택합니다.

- **Multicast** — 기본 모드로서 RIP가 지정된 주소에서 모든 인접 라우터에 전체 라우팅 테이블을 멀티캐스팅합니다.
- **Broadcast** — 멀티캐스트 모드가 가능하더라도 RIP에서 브로드캐스트(예: RIPv1)를 사용해야 합니다.
- **Quiet** — RIP에서 이 인터페이스에 어떤 정기 메시지도 보내지 않습니다.
- **No Listen** — RIP가 이 인터페이스에 전송하지만 수신하지는 않습니다.

11단계 **Save**를 클릭합니다.

변경 내용이 저장되었습니다. 디바이스 컨피그레이션을 적용해야 변경 사항이 적용됩니다. 4-25페이지의 디바이스에 변경 사항 적용를 참조하십시오.

RIP 컨피그레이션의 인증 설정 구성

라이센스: 제어

지원되는 디바이스: Series 3

RIP 인증에서는 가상 라우터에 구성한 인증 프로필 중 하나를 사용합니다. 인증 프로필을 구성하는 것에 대한 자세한 내용은 7-30페이지의 가상 라우터 인증 프로필 추가를 참조하십시오.

RIP 컨피그레이션의 인증 설정을 구성하려면

액세스: Admin/Network Admin

1단계 **Devices > Device Management**를 선택합니다.

Device Management 페이지가 나타납니다.

2단계 RIP 인증 프로필을 추가하려는 디바이스 옆의 수정 아이콘( )을 클릭합니다.

해당 디바이스의 Interfaces 탭이 나타납니다.

3단계 **Virtual Routers**를 클릭합니다.

Virtual Routers 탭이 나타납니다.

4단계 RIP 인증 프로필을 추가하려는 가상 라우터 옆의 수정 아이콘( )을 클릭합니다.

Edit Virtual Router 팝업 창이 나타납니다.

5단계 **Dynamic Routing**을 클릭하여 동적 라우팅 옵션을 표시합니다.

6단계 **RIP**를 클릭하여 RIP 옵션을 표시합니다.

7단계 **Authentication**에서 Profile 드롭다운 목록을 사용하여 기존 가상 라우터 인증 프로필을 선택하거나 **None**을 선택합니다.

8단계 **Save**를 클릭합니다.

변경 내용이 저장되었습니다. 디바이스 컨피그레이션을 적용해야 변경 사항이 적용됩니다. 4-25페이지의 디바이스에 변경 사항 적용를 참조하십시오.

RIP 컨피그레이션의 고급 설정 구성

라이센스: 제어

지원되는 디바이스: Series 3

프로토콜의 동작에 영향을 주는 다양한 시간 초과 값 및 기타 기능과 관련된 여러 고급 RIP 설정을 구성할 수 있습니다.

주의 고급 RIP 설정 중 하나라도 잘못된 값으로 변경하면 라우터가 다른 RIP 라우터와 통신하지 못할 수 있습니다.

RIP 컨피그레이션의 고급 설정을 구성하려면

액세스: Admin/Network Admin

1단계 **Devices > Device Management**를 선택합니다.

Device Management 페이지가 나타납니다.

2단계 RIP 고급 설정을 수정하려는 디바이스 옆의 수정 아이콘( )을 클릭합니다.

해당 디바이스의 Interfaces 탭이 나타납니다.

3단계 **Virtual Routers**를 클릭합니다.

Virtual Routers 탭이 나타납니다.

4단계 RIP 고급 설정을 수정하고자 하는 가상 라우터 옆의 수정 아이콘( )을 클릭합니다.

Edit Virtual Router 팝업 창이 나타납니다.

5단계 **Dynamic Routing**을 클릭하여 동적 라우팅 옵션을 표시합니다.

6단계 **RIP**를 클릭하여 RIP 옵션을 표시합니다.

7단계 **Preference** 필드에 라우팅 프로토콜의 우선 순위에 대한 숫자 값(높을수록 좋음)을 입력합니다. 고정 경로보다는 RIP를 통해 학습한 경로를 선호합니다.

8단계 **Period** 필드에 정기 업데이트의 간격(초)을 입력합니다. 숫자가 작을수록 더 빨리 통합되지만 네트워크 부하가 증가합니다.

9단계 **Timeout Time** 필드에 숫자 값을 입력하여 얼마의 시간(초)이 지나면 경로 도달 불가로 간주할 것인지 지정합니다.

10단계 **Garbage Time** 필드에 숫자 값을 입력하여 얼마의 시간(초)이 지나면 경로를 폐기할 것인지 지정합니다.

11단계 **Infinity** 필드에 숫자 값을 입력하여 통합 계산의 무한 거리에 대한 값을 지정합니다. 값이 클수록 프로토콜의 통합이 느려집니다.

12단계 **Honor** 드롭다운 목록에서 다음 옵션 중 하나를 선택하여 라우팅 테이블 폐기 요청을 수락하는 경우를 지정합니다.

- **Always** — 요청을 항상 받아들입니다.
- **Neighbor** — 직접 연결된 네트워크의 호스트가 보낸 요청만 받아들입니다.
- **Never** — 요청을 절대 받아들이지 않습니다.

13단계 **Save**를 클릭합니다.

변경 내용이 저장되었습니다. 디바이스 컨피그레이션을 적용해야 변경 사항이 적용됩니다. 4-25페이지의 디바이스에 변경 사항 적용를 참조하십시오.

RIP 컨피그레이션에 대한 가져오기 필터 추가

라이센스: 제어

지원되는 디바이스: Series 3

RIP에서 경로 테이블로 어떤 경로가 허용되거나 거부되는지 지정하기 위해 가져오기 필터를 추가할 수 있습니다. 가져오기 필터는 테이블에 나타난 순서대로 적용됩니다.

가져오기 필터를 추가할 때 가상 라우터에 구성한 필터 중 하나를 사용합니다. 필터를 구성하는 것에 대한 자세한 내용은 7-28페이지의 가상 라우터 필터 설정를 참조하십시오.

팁 RIP 가져오기 필터를 수정하려면 수정 아이콘( )을 클릭합니다. RIP 가져오기 필터를 삭제하려면 삭제 아이콘( )을 클릭합니다.

RIP 컨피그레이션에 대한 가져오기 필터를 추가하려면

액세스: Admin/Network Admin

1단계 **Devices > Device Management**를 선택합니다.

Device Management 페이지가 나타납니다.

2단계 RIP 가상 라우터 필터를 추가하려는 디바이스 옆의 수정 아이콘( )을 클릭합니다.

해당 디바이스의 Interfaces 탭이 나타납니다.

3단계 **Virtual Routers**를 클릭합니다.

Virtual Routers 탭이 나타납니다.

4단계 RIP 가상 라우터 필터를 추가하려는 가상 라우터 옆의 수정 아이콘( )을 클릭합니다.

Edit Virtual Router 팝업 창이 나타납니다.

5단계 **Dynamic Routing**을 클릭하여 동적 라우팅 옵션을 표시합니다.

6단계 **RIP**를 클릭하여 RIP 옵션을 표시합니다.

7단계 **Import Filters**에서 추가 아이콘( )을 클릭합니다.

Add an Import Filter 팝업 창이 나타납니다.

8단계 **Name** 드롭다운 목록에서 가져오기 필터로 추가할 필터를 선택합니다.

9단계 **Action** 옆의 **Accept** 또는 **Reject**를 선택합니다.

10단계 **OK**를 클릭합니다.

가져오기 필터가 추가되었습니다.

팁 가져오기 필터의 순서를 변경하려면 필요에 따라 위로 이동(▲) 및 아래로 이동(▼) 아이콘을 클릭합니다. 목록의 위 또는 아래로 필터를 드래그할 수도 있습니다.

11단계 **Save**를 클릭합니다.

변경 내용이 저장되었습니다. 디바이스 컨피그레이션을 적용해야 변경 사항이 적용됩니다. 4-25페이지의 디바이스에 변경 사항 적용를 참조하십시오.

RIP 컨피그레이션에 대한 내보내기 필터 추가

라이센스: 제어

지원되는 디바이스: Series 3

경로 테이블에서 RIP로 허용되거나 거부되는 경로를 정의하기 위해 내보내기 필터를 추가할 수 있습니다. 내보내기 필터는 테이블에 나타난 순서대로 적용됩니다.

내보내기 필터를 추가할 때 가상 라우터에 구성한 필터 중 하나를 사용합니다. 필터를 구성하는 것에 대한 자세한 내용은 7-28페이지의 가상 라우터 필터 설정를 참조하십시오.

RIP 컨피그레이션에 대한 내보내기 필터를 추가하려면

액세스: Admin/Network Admin

1단계 **Devices > Device Management**를 선택합니다.

Device Management 페이지가 나타납니다.

2단계 RIP 가상 라우터 필터를 추가하려는 디바이스 옆의 수정 아이콘( )을 클릭합니다.

해당 디바이스의 Interfaces 탭이 나타납니다.

3단계 **Virtual Routers**를 클릭합니다.

Virtual Routers 탭이 나타납니다.

4단계 RIP 가상 라우터 필터를 추가하려는 가상 라우터 옆의 수정 아이콘( )을 클릭합니다.

Edit Virtual Router 팝업 창이 나타납니다.

5단계 **Dynamic Routing**을 클릭하여 동적 라우팅 옵션을 표시합니다.

6단계 **RIP**를 클릭하여 RIP 옵션을 표시합니다.

7단계 **Export Filters**에서 추가 아이콘( )을 클릭합니다.

Add an Export Filter 팝업 창이 나타납니다.

8단계 **Name** 드롭다운 목록에서 내보내기 필터로 추가할 필터를 선택합니다.

9단계 **Action** 옆의 **Accept** 또는 **Reject**를 선택합니다.

10단계 **OK**를 클릭합니다.

내보내기 필터가 추가되었습니다.

팁 내보내기 필터의 순서를 변경하려면 필요에 따라 위로 이동( ) 및 아래로 이동( ) 아이콘을 클릭합니다. 목록의 위 또는 아래로 필터를 드래그할 수도 있습니다.

11단계 **Save**를 클릭합니다.

변경 내용이 저장되었습니다. 디바이스 컨피그레이션을 적용해야 변경 사항이 적용됩니다. 4-25페이지의 디바이스에 변경 사항 적용를 참조하십시오.

OSPF 컨피그레이션 설정

라이센스: 제어

지원되는 디바이스: Series 3

OSPF(Open Shortest Path First)는 적응형 라우팅 프로토콜로서 다른 라우터에서 정보를 얻고 링크 상태 광고를 통해 다른 라우터에 경로를 광고하면서 동적으로 경로를 정의합니다. 라우터가 자신과 목적지의 연결 링크에 대한 정보를 유지하면서 라우팅 결정을 내립니다. OSPF는 각 라우티드 인터페이스에 비용을 할당하고 비용이 가장 적은 것을 최상의 경로로 간주합니다.

자세한 내용은 다음 절을 참조하십시오.

- 7-21페이지의 OSPF 라우팅 영역 설정
- 7-26페이지의 OSPF 컨피그레이션에 대한 가져오기 필터 추가
- 7-27페이지의 OSPF 컨피그레이션에 대한 내보내기 필터 추가

OSPF 라우팅 영역 설정

라이센스: 제어

지원되는 디바이스: Series 3

관리를 간소화하고 트래픽 및 리소스 사용을 최적화하기 위해 OSPF 네트워크를 라우팅 영역으로 구성 또는 분할할 수 있습니다. 영역은 32비트 숫자로 식별되는데 간단하게 10진수로 나타내거나 대개는 옥텟 기반 점 구분 10진 표기법으로 나타냅니다.

일반적으로 영역 제로, 즉 0.0.0.0은 OSPF 네트워크의 코어 또는 백본 영역을 나타냅니다. 다른 영역을 식별하도록 선택할 수도 있습니다. 대개 관리자는 어떤 영역의 기본 라우터 IP 주소를 그 영역의 식별자로 선택합니다. 영역이 추가될 때마다 백본 OSPF 영역과 직접 또는 가상 연결이 설정되어야 합니다. 그러한 연결은 ABR(area border router)이라고 하는 인터커넥팅 라우터에서 관리합니다. ABR은 서비스하는 영역별 링크 상태 데이터베이스와 네트워크의 모든 영역에 대한 요약 경로를 관리합니다.

OSPF 영역 설정에 대한 자세한 내용은 다음 절을 참조하십시오.

- 7-21페이지의 OSPF 영역 추가
- 7-22페이지의 OSPF 영역 인터페이스 추가
- 7-25페이지의 OSPF 영역 Vlink 추가

OSPF 영역 추가

라이센스: 제어

지원되는 디바이스: Series 3

다음 절차에서는 OSPF 영역을 추가하고 일반 설정을 구성하는 방법에 대해 설명합니다.

OSPF 영역을 추가하려면

액세스: Admin/Network Admin

1단계 **Devices > Device Management**를 선택합니다.

Device Management 페이지가 나타납니다.

2단계 OSPF 일반 옵션을 수정하려는 디바이스 옆의 수정 아이콘( )을 클릭합니다.

해당 디바이스의 Interfaces 탭이 나타납니다.

3단계 **Virtual Routers**를 클릭합니다.

Virtual Routers 탭이 나타납니다.

4단계 OSPF 일반 옵션을 수정하고자 하는 가상 라우터 옆의 수정 아이콘( )을 클릭합니다.

Edit Virtual Router 팝업 창이 나타납니다.

5단계 **Dynamic Routing**을 클릭하여 동적 라우팅 옵션을 표시합니다.

6단계 **OSPF**를 클릭하여 OSPF 옵션을 표시합니다.

7단계 **Areas**에서 추가 아이콘( )을 클릭합니다.

Add OSPF Area 팝업 창이 나타납니다.

8단계 **Area Id** 필드에 영역에 대한 숫자 값을 입력합니다. 이 값은 정수 또는 IPv4 주소일 수 있습니다.

9단계 원한다면 **Stubnet** 확인란을 선택하여 이 영역이 자율 시스템 외부의 라우터 광고를 받지 않고 영역 내로부터의 라우팅은 전적으로 기본 경로를 기반으로 하도록 지정할 수 있습니다. 확인란의 선택을 취소하면 이 영역은 백본 영역이 되며 그렇지 않으면 비 스텁 영역이 됩니다.

Default cost 필드와 Stubnet 필드가 나타납니다.

10단계 **Default cost** 필드에는 영역의 기본 경로에 대한 비용을 입력합니다.

11단계 **Stubnets**에서 추가 아이콘( )을 클릭합니다.

12단계 **IP Address** 필드에 IP 주소를 CIDR 표기법으로 입력합니다.

13단계 **Hidden** 확인란을 선택하여 스텁넷을 숨기도록 지정합니다. 숨긴 스텁넷은 다른 영역에 전파되지 않습니다.

14단계 **Summary** 확인란을 선택하여 이 스텁넷의 서브네트워크인 기본 스텁넷을 억제하도록 지정합니다.

15단계 **Stub cost** 필드에 이 스텁 네트워크에 대한 라우팅의 비용을 정의하는 값을 입력합니다.

16단계 **OK**를 클릭합니다.

스텁넷이 추가되었습니다.

팁 스텁넷을 수정하려면 수정 아이콘( )을 클릭합니다. 스텁넷을 삭제하려면 삭제 아이콘( )을 클릭합니다.

17단계 원한다면 **Networks**에서 추가 아이콘( )을 클릭합니다.

18단계 **IP Address** 필드에 네트워크의 IP 주소를 CIDR 표기법으로 입력합니다.

19단계 **Hidden** 확인란을 선택하여 네트워크를 숨기도록 지정합니다. 숨긴 네트워크는 다른 영역에 전파되지 않습니다.

20단계 **OK**를 클릭합니다.

네트워크가 추가되었습니다.

팁 네트워크를 수정하려면 수정 아이콘( )을 클릭합니다. 네트워크를 삭제하려면 삭제 아이콘( )을 클릭합니다.

21단계 **Save**를 클릭합니다.

변경 내용이 저장되었습니다. 디바이스 컨피그레이션을 적용해야 변경 사항이 적용됩니다. 4-25페이지의 디바이스에 변경 사항 적용를 참조하십시오.

OSPF 영역 인터페이스 추가

라이센스: 제어

지원되는 디바이스: Series 3

OSPF 가상 라우터에 지정된 인터페이스의 일부를 구성할 수 있습니다. 다음 목록에서는 각 인터페이스에 지정할 수 있는 옵션에 대해 설명합니다.

Interfaces

OSPF를 구성하려는 인터페이스를 선택합니다. Interfaces 탭에서 비활성화한 인터페이스는 사용할 수 없습니다.

Type

OSPF 인터페이스의 유형을 다음 중에서 선택합니다.

- Broadcast — 브로드캐스트 네트워크에서 플러딩 및 hello 메시지가 모든 네이버를 위한 단일 패킷인 멀티캐스트를 사용하여 전송됩니다. 이 옵션은 링크 상태 데이터베이스를 동기화하고 네트워크 링크 상태 광고를 시작할 라우터를 지정합니다. 이 네트워크 유형은 물리적으로 NBMP(non-broadcast multiple-access)인 네트워크와 번호가 지정되지 않은 네트워크에서 알맞은 IP 접두사 없이 사용할 수 없습니다.
- PtP(Point-to-Point) — 포인트 투 포인트 네트워크는 단지 2개의 라우터를 함께 연결합니다. 어떤 선택도 수행되지 않고 네트워크 링크 상태 광고도 시작되지 않으므로 더 간단하고 빠르게 설정할 수 있습니다. 이 네트워크 유형은 물리적으로 PtP인 인터페이스뿐 아니라 PtP 링크로 쓰이는 브로드캐스트 네트워크에도 유용합니다. 이 네트워크 유형은 물리적으로 NBMP인 네트워크에서 사용할 수 없습니다.
- Non-Broadcast — NBMP 네트워크에서는 멀티캐스트 기능이 없으므로 패킷이 각 네이버에 개별적으로 전송됩니다. 이 옵션은 브로드캐스트 네트워크와 비슷하게 라우터를 지정하는데, 이는 링크 상태 광고를 전파하는 데 중심적 역할을 합니다. 이 네트워크 유형은 번호가 지정되지 않은 네트워크에서 사용할 수 없습니다.
- Autodetect — 시스템에서 지정된 인터페이스에 따라 알맞은 유형을 결정합니다.

Cost

인터페이스의 출력 비용을 지정합니다.

Stub

인터페이스에서 OSPF 트래픽을 수신하고 자신의 트래픽을 전송할지 여부를 지정합니다.

Priority

지정된 라우터 선택 시 사용되는 우선 순위의 값을 숫자로 입력합니다. 각 다중 액세스 네트워크에 라우터와 백업 라우터가 지정됩니다. 이 라우터는 플러딩 프로세스에서 특별한 기능을 수행합니다. 우선 순위가 높으면 여기서 우선적으로 선택됩니다. 라우터를 우선 순위 0으로 구성할 수 없습니다.

Nonbroadcast

Hello 패킷이 미정의 네이버에 전송되는지 여부를 지정합니다. 이 스위치는 NBMA 네트워크에서 무시됩니다.

Authentication

이 인터페이스에서 사용하는 OSPF 인증 프로필을 가상 라우터에서 구성한 인증 프로필 중 하나로 선택하거나 **None**을 선택합니다. 인증 프로필을 구성하는 것에 대한 자세한 내용은 7-30페이지의 가상 라우터 인증 프로필 추가를 참조하십시오.

Hello Interval

Hello 메시지를 보내는 간격(초)을 입력합니다.

Poll

NBMA 네트워크의 일부 네이버에 대해 hello 메시지를 보내는 간격(초)을 입력합니다.

Retrans Interval

미승인 업데이트의 재전송 간격(초)을 입력합니다.

Retrans Delay

인터페이스를 통해 링크 상태 업데이트 패킷을 전송하는 데 걸리는 예상 시간(초)을 입력합니다.

Wait Time

라우터에서 선택 시작 후 인접성 생성까지 기다리는 시간(초)을 입력합니다.

Dead Interval

라우터에서 어떤 네이버의 메시지가 수신되지 않을 경우 그 네이버가 다운된 것으로 결정할 때까지 기다리는 시간(초)을 입력합니다. 이 값이 정의된 경우 Dead Count에서 계산된 값을 재정의합니다.

Dead Count

여기에 입력하는 숫자 값에 hello 간격을 곱하면 라우터가 어떤 네이버의 메시지가 수신되지 않을 경우 그 네이버가 다운된 것으로 결정할 때까지 기다리는 시간(초)이 됩니다.

OSPF 영역 인터페이스를 수정하려면 수정 아이콘( )을 클릭합니다. OSPF 영역 인터페이스를 삭제하려면 삭제 아이콘( )을 클릭합니다. Interfaces 탭에서 구성된 인터페이스를 비활성화해도 삭제됩니다.

참고 한 OSPF 영역에서 사용할 인터페이스를 하나만 선택할 수 있습니다.

OSPF 영역 인터페이스를 추가하려면

액세스: Admin/Network Admin

1단계 **Devices > Device Management**를 선택합니다.

Device Management 페이지가 나타납니다.

2단계 OSPF 인터페이스를 추가하려는 디바이스 옆의 수정 아이콘( )을 클릭합니다.

해당 디바이스의 Interfaces 탭이 나타납니다.

3단계 **Virtual Routers**를 클릭합니다.

Virtual Routers 탭이 나타납니다.

4단계 OSPF 인터페이스를 추가하려는 가상 라우터 옆의 수정 아이콘( )을 클릭합니다.

Edit Virtual Router 팝업 창이 나타납니다.

5단계 **Dynamic Routing**을 클릭하여 동적 라우팅 옵션을 표시합니다.

6단계 **OSPF**를 클릭하여 OSPF 옵션을 표시합니다.

7단계 **Areas**에서 추가 아이콘( )을 클릭합니다.

Add OSPF Area 팝업 창이 나타납니다.

8단계 **Interfaces**를 클릭합니다.

Interfaces 탭이 나타납니다.

9단계 추가 아이콘( )을 클릭합니다.

Add OSPF Area Interface 팝업 창이 나타납니다.

10단계 7-22페이지의 OSPF 영역 인터페이스 추가에 설명된 작업 중 하나를 수행합니다.

11단계 원한다면 **Neighbors**에서 추가 아이콘( )을 클릭합니다.

12단계 **IP address** 필드에는 비 브로드캐스트 네트워크에서 이 인터페이스로부터 hello 메시지를 수신하는 네이버의 IP 주소를 입력합니다.

13단계 **Eligible** 확인란을 선택하여 네이버가 메시지를 수신할 자격이 있음을 나타냅니다.

14단계 **OK**를 클릭합니다.

네이버가 추가되었습니다.

팁 네이버를 수정하려면 수정 아이콘( )을 클릭합니다. 네이버를 삭제하려면 삭제 아이콘( )을 클릭합니다.

15단계 **OK**를 클릭합니다.

OSPF 영역 인터페이스가 추가되었습니다.

16단계 **Save**를 클릭합니다.

OSPF 영역이 저장되었습니다.

17단계 **Save**를 클릭합니다.

변경 내용이 저장되었습니다. 디바이스 컨피그레이션을 적용해야 변경 사항이 적용됩니다. 4-25페이지의 디바이스에 변경 사항 적용를 참조하십시오.

OSPF 영역 Vlink 추가

라이센스: 제어

지원되는 디바이스: Series 3

OSPF 자율 시스템의 모든 영역이 물리적으로 백본 영역에 연결되어야 합니다. 이러한 물리적 연결이 불가능한 어떤 경우에는 vlink를 사용하여 비 백본 영역을 통해 백본에 연결할 수 있습니다. Vlink는 분할된 백본의 두 부분을 비 백본 영역을 통해 연결하는 데에도 사용할 수 있습니다.

Vlink를 추가하려면 먼저 둘 이상의 OSPF 영역을 추가해야 합니다.

OSPF 영역 vlink를 추가하려면

액세스: Admin/Network Admin

1단계 **Devices > Device Management**를 선택합니다.

Device Management 페이지가 나타납니다.

2단계 OSPF vlink를 추가하려는 디바이스 옆의 수정 아이콘( )을 클릭합니다.

해당 디바이스의 Interfaces 탭이 나타납니다.

3단계 **Virtual Routers**를 클릭합니다.

Virtual Routers 탭이 나타납니다.

4단계 OSPF 인터페이스를 추가하려는 가상 라우터 옆의 수정 아이콘( )을 클릭합니다.

Edit Virtual Router 팝업 창이 나타납니다.

5단계 **Dynamic Routing**을 클릭하여 동적 라우팅 옵션을 표시합니다.

6단계 **OSPF**를 클릭하여 OSPF 옵션을 표시합니다.

7단계 **Areas**에서 추가 아이콘( )을 클릭합니다.

Add OSPF Area 팝업 창이 나타납니다.

8단계 **Vlinks**를 클릭합니다.

Vlinks 탭이 나타납니다.

9단계 추가 아이콘( )을 클릭합니다.

Add OSPF Area Vlink 팝업 창이 나타납니다.

10단계 **Router ID** 필드에 라우터의 IP 주소를 입력합니다.

11단계 **Authentication** 드롭다운 목록에서 vlink가 사용할 인증 프로필을 선택합니다.

12단계 **Hello Interval** 필드에 hello 메시지를 보내는 간격(초)을 입력합니다.

13단계 **Retrans Interval** 필드에 미승인 업데이트를 재전송하는 간격(초)을 입력합니다.

14단계 **Wait Time** 필드에 라우터에서 선택 시작 후 인접성 생성까지 기다리는 시간(초)을 입력합니다.

15단계 **Dead Interval** 필드에 라우터에서 어떤 네이버의 메시지가 수신되지 않을 경우 그 네이버가 다운된 것으로 결정할 때까지 기다리는 시간(초)을 입력합니다. 이 값이 정의된 경우 Dead Count에서 계산된 값을 무시합니다.

16단계 **Dead Count** 필드에 입력하는 숫자 값에 hello 간격을 곱하면 라우터가 어떤 네이버의 메시지가 수신되지 않을 경우 그 네이버가 다운된 것으로 결정할 때까지 기다리는 시간(초)이 됩니다.

17단계 **OK**를 클릭합니다.

OSPF 영역 vlink가 추가되었습니다.

18단계 **Save**를 클릭합니다.

OSPF 영역이 저장되었습니다.

19단계 **Save**를 클릭합니다.

변경 내용이 저장되었습니다. 디바이스 컨피그레이션을 적용해야 변경 사항이 적용됩니다. 4-25페이지의 디바이스에 변경 사항 적용를 참조하십시오.

OSPF 컨피그레이션에 대한 가져오기 필터 추가

라이센스: 제어

지원되는 디바이스: Series 3

OSPF에서 경로 테이블로 허용되거나 거부되는 경로를 정의하기 위해 가져오기 필터를 추가할 수 있습니다. 가져오기 필터는 테이블에 나타난 순서대로 적용됩니다.

가져오기 필터를 추가할 때 가상 라우터에 구성한 필터 중 하나를 사용합니다. 필터를 구성하는 것에 대한 자세한 내용은 7-28페이지의 가상 라우터 필터 설정를 참조하십시오.

OSPF 컨피그레이션에 대한 가져오기 필터를 추가하려면

액세스: Admin/Network Admin

1단계 **Devices > Device Management**를 선택합니다.

Device Management 페이지가 나타납니다.

2단계 OSPF 가상 라우터 필터를 추가하려는 디바이스 옆의 수정 아이콘( )을 클릭합니다.

해당 디바이스의 Interfaces 탭이 나타납니다.

3단계 **Virtual Routers**를 클릭합니다.

Virtual Routers 탭이 나타납니다.

4단계 OSPF 가상 라우터 필터를 추가하려는 가상 라우터 옆의 수정 아이콘()을 클릭합니다.

Edit Virtual Router 팝업 창이 나타납니다.

5단계 **Dynamic Routing**을 클릭하여 동적 라우팅 옵션을 표시합니다.

6단계 **OSPF**를 클릭하여 OSPF 옵션을 표시합니다.

7단계 **Import Filters**에서 추가 아이콘()을 클릭합니다.

Add Import Filter 팝업 창이 나타납니다.

8단계 **Name** 드롭다운 목록에서 가져오기 필터로 추가할 필터를 선택합니다.

9단계 **Action** 옆의 **Accept** 또는 **Reject**를 선택합니다.

10단계 **OK**를 클릭합니다.

가져오기 필터가 추가되었습니다.

팁 가져오기 필터의 순서를 변경하려면 필요에 따라 위로 이동( ) 및 아래로 이동( ) 아이콘을 클릭합니다. 목록의 위 또는 아래로 필터를 드래그할 수도 있습니다.

11단계 **Save**를 클릭합니다.

변경 내용이 저장되었습니다. 디바이스 컨피그레이션을 적용해야 변경 사항이 적용됩니다. 4-25페이지의 디바이스에 변경 사항 적용를 참조하십시오.

OSPF 컨피그레이션에 대한 내보내기 필터 추가

라이센스: 제어

지원되는 디바이스: Series 3

경로 테이블에서 OSPF로 허용되거나 거부되는 경로를 정의하기 위해 내보내기 필터를 추가할 수 있습니다. 내보내기 필터는 테이블에 나타난 순서대로 적용됩니다.

내보내기 필터를 추가할 때 가상 라우터에 구성한 필터 중 하나를 사용합니다. 필터를 구성하는 것에 대한 자세한 내용은 7-28페이지의 가상 라우터 필터 설정를 참조하십시오.

OSPF 컨피그레이션에 대한 내보내기 필터를 추가하려면

액세스: Admin/Network Admin

1단계 **Devices > Device Management**를 선택합니다.

Device Management 페이지가 나타납니다.

2단계 OSPF 가상 라우터 필터를 추가하려는 디바이스 옆의 수정 아이콘()을 클릭합니다.

해당 디바이스의 Interfaces 탭이 나타납니다.

3단계 **Virtual Routers**를 클릭합니다.

Virtual Routers 탭이 나타납니다.

4단계 OSPF 가상 라우터 필터를 추가하려는 가상 라우터 옆의 수정 아이콘()을 클릭합니다.

Edit Virtual Router 팝업 창이 나타납니다.

5단계 **Dynamic Routing**을 클릭하여 동적 라우팅 옵션을 표시합니다.

6단계 **OSPF**를 클릭하여 OSPF 옵션을 표시합니다.

7단계 **Export Filters**에서 추가 아이콘( )을 클릭합니다.

Add an Export Filter 팝업 창이 나타납니다.

8단계 **Name** 드롭다운 목록에서 내보내기 필터로 추가할 필터를 선택합니다.

9단계 **Action** 옆의 **Accept** 또는 **Reject**를 선택합니다.

10단계 **OK**를 클릭합니다.

내보내기 필터가 추가되었습니다.

팁 내보내기 필터의 순서를 변경하려면 필요에 따라 위로 이동( ) 및 아래로 이동( ) 아이콘을 클릭합니다. 목록의 위 또는 아래로 필터를 드래그할 수도 있습니다.

11단계 **Save**를 클릭합니다.

변경 내용이 저장되었습니다. 디바이스 컨피그레이션을 적용해야 변경 사항이 적용됩니다. 4-25페이지의 디바이스에 변경 사항 적용를 참조하십시오.

가상 라우터 필터 설정

라이센스: 제어

지원되는 디바이스: Series 3

필터는 가상 라우터의 경로 테이블에 경로를 가져오고 동적 프로토콜에 경로를 내보낼 때 경로를 매칭하는 방법을 제공합니다. 필터의 목록을 생성하고 관리할 수 있습니다. 각 필터는 고정 경로나 동적 프로토콜로부터 받은 경로를 찾기 위한 기준을 정의합니다.

팁 가상 라우터 필터를 수정하려면 수정 아이콘( )을 클릭합니다. 가상 라우터 필터를 삭제하려면 삭제 아이콘( )을 클릭합니다.

Virtual Router 편집기의 Filter 탭에서는 가상 라우터에 대해 구성한 모든 필터를 표 목록으로 표시합니다. 여기에는 다음 표에 설명된 것과 같은 각 필터에 대한 요약 정보가 포함됩니다.

표 7-3 가상 라우터 필터 표 보기 필드

필드	설명
Name	필터의 이름
Protocol	경로가 시작하는 프로토콜: • Static — 로컬 고정 경로에서 시작합니다. • RIP — 동적 RIP 컨피그레이션에서 시작합니다. • OSPF — 동적 OSPF 컨피그레이션에서 시작합니다.
From Router	이 필터가 라우터에서 매칭을 시도할 라우터 IP 주소. 고정 및 RIP 필터에 대해 이 값을 입력해야 합니다.
Next Hop	이 경로를 사용하는 패킷이 전달되는 다음 홉. 고정 및 RIP 필터에 대해 이 값을 입력해야 합니다.

표 7-3 가상 라우터 필터 표 보기 필드(계속)

필드	설명
Destination Type	패킷이 전송되는 목적지의 유형: • Router • Device • Discard
Destination Network	이 필터가 경로에서 매칭을 시도할 네트워크
OSPF Path Type	OSPF 프로토콜에만 적용됩니다. 경로 유형은 다음 중 하나일 수 있습니다. • Ext-1 • Ext-2 • Inter Area • Intra Area
OSPF Router ID	OSPF 프로토콜에만 적용됩니다. 해당 라우터/네트워크를 광고하는 라우터의 라우터 ID

가상 라우터 필터를 추가하려면

액세스: Admin/Network Admin

1단계 **Devices > Device Management**를 선택합니다.

Device Management 페이지가 나타납니다.

2단계 가상 라우터 필터를 추가하려는 디바이스 옆의 수정 아이콘( )을 클릭합니다.

해당 디바이스의 Interfaces 탭이 나타납니다.

3단계 **Virtual Routers**를 클릭합니다.

Virtual Routers 탭이 나타납니다.

4단계 가상 라우터 필터를 추가하려는 가상 라우터 옆의 수정 아이콘( )을 클릭합니다.

Edit Virtual Router 팝업 창이 나타납니다.

5단계 **Filter**를 클릭하여 Filter 옵션을 표시합니다.

6단계 **Add Filter**를 클릭합니다.

Create Filter 팝업 창이 나타납니다.

7단계 **Name** 필드에 필터의 이름을 입력합니다. 영숫자만 사용할 수 있습니다.

8단계 **Protocol**에서 **All**을 선택하거나 필터에 적용되는 프로토콜을 선택합니다.

9단계 Protocol에 All, Static 또는 RIP를 선택한 경우 **From Router**에 이 필터가 경로에서 매칭을 시도할 라우터 IP 주소를 입력합니다.

IPv4 주소에 대해 /32 CIDR 블록을, IPv6 주소에 대해서는 /128 접두부 길이도 입력할 수 있습니다. 그 밖의 모든 주소 블록은 이 필드에 적합하지 않습니다.

10단계 **Add**를 클릭합니다.

From Router 필드가 채워집니다.

11단계 Protocol에 All, Static 또는 RIP를 선택한 경우 **Next Hop**에 이 필터가 경로에서 매칭을 시도할 게이트웨이의 IP 주소를 입력합니다.

IPv4 주소에 대해 /32 CIDR 블록을, IPv6 주소에 대해서는 /128 접두사 길이도 입력할 수 있습니다. 그 밖의 모든 주소 블록은 이 필드에 적합하지 않습니다.

12단계 **Add**를 클릭합니다.

Next Hop 필드가 채워집니다.

13단계 **Destination Type**에서 필터에 적용될 옵션을 선택합니다.

14단계 **Destination Network**에 이 필터가 경로에서 매칭을 시도할 네트워크의 IP 주소를 입력합니다.

15단계 **Add**를 클릭합니다.

Destination Network 필드가 채워집니다.

16단계 Protocol에 All 또는 OSPF를 선택한 경우 **Path Type**에서 필터에 적용될 옵션을 선택합니다.

하나 이상의 경로 유형을 선택해야 합니다.

17단계 Protocol에 OSPF를 선택한 경우 **Router ID**에서 해당 경로/네트워크를 광고하는 라우터의 ID가 될 IP 주소를 입력합니다.

18단계 **Add**를 클릭합니다.

Router ID 필드가 채워집니다.

19단계 **OK**를 클릭합니다.

필터가 추가되었습니다.

20단계 **Save**를 클릭합니다.

변경 내용이 저장되었습니다. 디바이스 컨피그레이션을 적용해야 변경 사항이 적용됩니다. 4-25페이지의 디바이스에 변경 사항 적용를 참조하십시오.

가상 라우터 인증 프로필 추가

라이센스: 제어

지원되는 디바이스: Series 3

RIP 및 OSPF 컨피그레이션에서 사용할 인증 프로필을 설정할 수 있습니다. 단순 비밀번호를 구성하거나 공유 암호 키를 지정할 수 있습니다. 단순 비밀번호에서는 모든 패킷이 8바이트의 비밀번호를 전달할 수 있습니다. 이 비밀번호가 없는 수신 패킷은 무시됩니다. 암호 키를 지정하면 유효성 검사가 가능합니다. 비밀번호에서 생성된 16바이트 길이의 다이제스트가 모든 패킷에 추가됩니다.

OSPF에서는 각 영역에서 서로 다른 인증 방법을 사용할 수 있습니다. 따라서 여러 영역에서 공유할 수 있는 인증 프로필을 생성합니다. OSPFv3에 대한 인증은 추가할 수 없습니다.

팁 인증 프로필을 수정하려면 수정 아이콘( )을 클릭합니다. 인증 프로필을 삭제하려면 삭제 아이콘( )을 클릭합니다.

가상 라우터 인증 프로필을 추가하려면

액세스: Admin/Network Admin

1단계 **Devices > Device Management**를 선택합니다.

Device Management 페이지가 나타납니다.

2단계 가상 라우터 인증 프로필을 추가하려는 디바이스 옆의 수정 아이콘( )을 클릭합니다.

해당 디바이스의 Interfaces 탭이 나타납니다.

3단계 **Virtual Routers**를 클릭합니다.

Virtual Routers 탭이 나타납니다.

4단계 가상 라우터 인증 프로필을 추가하려는 가상 라우터 옆의 수정 아이콘( )을 클릭합니다.

Edit Virtual Router 팝업 창이 나타납니다.

5단계 **Authentication Profile**을 클릭합니다.

Authentication Profile 탭이 나타납니다.

6단계 **Add Authentication Profile**을 클릭합니다.

Add Authentication Profile 팝업 창이 나타납니다.

7단계 **Authentication Profile Name** 필드에 인증 프로필의 이름을 입력합니다.

8단계 **Authentication Type** 드롭다운 목록에서 **simple** 또는 **cryptographic**을 선택합니다.

9단계 **Password** 필드에 보안 비밀번호를 입력합니다.

10단계 **Confirm Password** 필드에 비밀번호를 다시 입력하여 확인합니다.

11단계 **OK**를 클릭합니다.

인증 프로필이 추가됩니다.

12단계 **Save**를 클릭합니다.

변경 내용이 저장되었습니다. 디바이스 컨피그레이션을 적용해야 변경 사항이 적용됩니다. 4-25페이지의 디바이스에 변경 사항 적용를 참조하십시오.

가상 라우터 통계 보기

라이센스: 제어

지원되는 디바이스: Series 3

각 가상 라우터에 대한 런타임 통계를 볼 수 있습니다. 이 통계에서는 유니캐스트 패킷과 삭제된 패킷을 보여주며 IPv4 주소와 IPv6 주소에 대한 별도의 라우팅 테이블을 표시합니다.

가상 라우터 통계를 보려면

액세스: Admin/Network Admin

1단계 **Devices > Device Management**를 선택합니다.

Device Management 페이지가 나타납니다.

2단계 가상 라우터 통계를 표시할 디바이스 옆의 수정 아이콘( )을 클릭합니다.

해당 디바이스의 Interfaces 탭이 나타납니다.

3단계 **Virtual Routers**를 클릭합니다.

Virtual Routers 탭이 나타납니다.

4단계 라우터 통계를 표시할 가상 라우터 옆의 수정 아이콘( )을 클릭합니다.

Statistics 팝업 창이 나타납니다.

5단계 **OK**를 클릭하여 창을 닫습니다.

가상 라우터 삭제

라이센스: 제어

지원되는 디바이스: Series 3

가상 라우터를 삭제할 때 그 라우터에 지정되었던 모든 라우티드 인터페이스는 다른 라우터에 포함될 수 있게 됩니다.

가상 라우터를 삭제하려면

액세스: Admin/Network Admin

1단계 **Devices > Device Management**를 선택합니다.

Device Management 페이지가 나타납니다.

2단계 가상 라우터를 삭제하려는 디바이스 옆의 수정 아이콘( )을 클릭합니다.

해당 디바이스의 Interfaces 탭이 나타납니다.

3단계 **Virtual Routers**를 클릭합니다.

Virtual Routers 탭이 나타납니다.

4단계 삭제할 가상 라우터 옆의 삭제 아이콘( )을 클릭합니다.

5단계 확인 메시지가 표시되면 가상 라우터를 삭제할 것임을 확인합니다.

가상 라우터가 삭제됩니다. 디바이스 컨피그레이션을 적용해야 변경 사항이 적용됩니다. 4-25페이지의 디바이스에 변경 사항 적용를 참조하십시오.

집계 인터페이스 설정

네트워크 간에 전환되는 패킷을 제공하는 레이어 2 구축 또는 인터페이스 간에 트래픽을 라우팅하는 레이어 3 구축으로 구성된 Series 3 관리되는 디바이스에서 단일 논리적 링크로 여러 물리적 이더넷 인터페이스를 그룹화할 수 있습니다. 이 단일 집계 논리적 링크는 두 엔드포인트 간에 더 우수한 대역폭, 이중화, 로드 밸런싱을 제공합니다.

스위치드 또는 라우티드 LAG(link aggregation group)를 생성하여 링크를 집계할 수 있습니다. 집계 그룹을 생성하면 집계 인터페이스라는 논리적 인터페이스가 생성됩니다. 상위 레이어 엔티티에는 LAG가 단일 논리적 링크처럼 보이고 데이터 트래픽은 집계 인터페이스를 통해 전송됩니다. 집계 링크는 여러 링크의 대역폭을 함께 추가함으로써 증가된 대역폭을 제공합니다. 또한 사용 가능한 모든 링크에서 트래픽을 로드 밸런싱하여 이중성을 제공합니다. 한 링크가 실패하면 시스템은 나머지 모든 링크에서 자동으로 트래픽을 로드 밸런싱합니다.

LAG의 엔드포인트는 위의 그림에 보이는 것처럼 두 개의 FirePOWER 관리되는 디바이스이거나, 서드파티 액세스 스위치 또는 라우터에 연결된 FirePOWER 관리되는 디바이스일 수 있습니다. 두 디바이스는 일치해야 할 필요는 없지만, 물리적 컨피그레이션이 동일해야 하며 IEEE 802.ad 링크 집계 표준을 지원해야 합니다. LAG에 대한 일반적인 구축은 두 개의 관리되는 디바이스 간 액세스 링크를 집계하거나, 관리되는 디바이스와 액세스 스위치 또는 라우터 간 포인트-투-포인트 연결을 생성합니다.

가상 관리되는 디바이스, Cisco ASA with FirePOWER Services 디바이스 또는 Cisco NGIPS for Blue Coat X-Series 디바이스에서는 집계 인터페이스를 구성할 수 없습니다.

집계 인터페이스 설정에 대한 자세한 내용은 8-2페이지의 LAG 구성을/를 참조하십시오.

LAG 구성

라이센스: 제어

지원되는 디바이스: Series 3

집계 인터페이스에는 두 가지 유형, 즉 스위치드(레이어 2 집계 인터페이스)와 라우티드(레이어 3 집계 인터페이스)가 있습니다. LAG(link aggregation group)를 사용하여 링크 집계를 구현합니다. 집계 스위치드 또는 라우티드 인터페이스를 생성한 다음 물리적 인터페이스 집합을 링크와 연결하여 LAG를 구성합니다. 모든 물리적 인터페이스는 속도와 미디어가 동일해야 합니다.

집계 링크는 동적으로 또는 정적으로 생성합니다. 동적 링크 집계는 IEEE 802.ad 링크 집계 표준의 구성 요소인 LACP(Link Aggregation Control Protocol)를 사용하는 반면 고정 링크 집계는 그렇지 않습니다. LACP를 활성화하면 LAG의 끝에 있는 각 디바이스는 링크 및 시스템 정보를 교환하여 어떤 링크가 집계에서 적극적으로 사용될지를 파악할 수 있습니다. 정적 LAG 컨피그레이션에서는 링크 집계를 수동으로 유지 관리하고 로드 밸런싱 및 링크 선택 정책을 적용해야 합니다.

스위치드 또는 라우티드 집계 인터페이스를 생성하면 동일한 유형의 LAG가 생성되고 자동으로 번호가 매겨집니다. 예를 들어 첫 번째 LAG(스위치드 또는 라우티드)를 생성하면 관리되는 디바이스의 Interfaces 탭에 있는 **lag0** 레이블로 집계 인터페이스를 식별할 수 있습니다. 물리적 및 논리적 인터페이스를 이 LAG와 연결하면 계층적 트리 메뉴의 주 LAG 아래에 중첩되어 나타납니다. 스위치드 LAG는 스위치드 물리적 인터페이스만 포함할 수 있고 라우티드 LAG는 라우티드 물리적 인터페이스만 포함할 수 있습니다.

LAG를 구성할 때 다음 요구 사항을 고려하십시오.

- FireSIGHT 시스템은 최대 14개의 LAG를 지원하고 0~13 범위의 각 LAG 인터페이스에 고유한 ID를 할당합니다. LAG ID는 구성할 수 없습니다.
- 링크의 양쪽에 LAG를 구성해야 하며, 링크 양쪽의 인터페이스에서 속도를 동일하게 설정해야 합니다.
- LAG당 물리적 인터페이스를 최소 2개에서 최대 8개까지 연결해야 합니다. 하나의 물리적 인터페이스는 둘 이상의 LAG에 속할 수 없습니다.
- LAG의 물리적 인터페이스는 다른 운영 모드에서 인라인 또는 패시브로 사용할 수 없으며, 태그가 지정된 트래픽에 대한 또 다른 논리적 인터페이스의 일부로 사용할 수 없습니다.
- LAG의 물리적 인터페이스는 여러 NetMod에 걸쳐 있을 수 있지만, 여러 센서에 걸쳐 있을 수는 없습니다(즉, 모든 물리적 인터페이스는 동일한 디바이스에 상주해야 함).
- LAG에는 스태킹 NetMod를 포함할 수 없습니다.

참고 링크 집계는 디바이스 클러스터에서 지원되지 않습니다.

자세한 내용은 다음 절을 참조하십시오.

- 8-3페이지의 로드 밸런싱 알고리즘 지정
- 8-3페이지의 링크 선택 정책 지정
- 8-4페이지의 LACP 구성
- 8-5페이지의 스위치드 인터페이스 추가
- 8-7페이지의 집계 라우티드 인터페이스 추가
- 8-11페이지의 논리적 집계 인터페이스 추가
- 8-12페이지의 집계 인터페이스 통계 보기
- 8-13페이지의 집계 인터페이스 삭제

로드 밸런싱 알고리즘 지정

라이센스: 제어

지원되는 디바이스: Series 3

LAG 번들의 멤버 링크에 트래픽을 분산하는 방법을 결정하는 이그레스 로드 밸런싱 알고리즘을 LAG에 할당합니다. 로드 밸런싱 알고리즘은 레이어 2 MAC 주소, 레이어 3 IP 주소, 레이어 4 포트 번호(TCP/UDP 트래픽) 등 각종 패킷 필드의 값을 기반으로 해싱을 결정합니다. 선택하는 로드 밸런싱 알고리즘은 모든 LAG 번들 멤버 링크에 적용됩니다.

LAG를 구성할 때 다음 옵션 중에서 구축 시나리오를 지원하는 로드 밸런싱 알고리즘을 선택하십시오.

- 대상 IP
- 대상 MAC
- 대상 포트
- 소스 IP
- 소스 MAC
- 소스 포트
- 소스 및 대상 IP
- 소스 및 대상 MAC
- 소스 및 대상 포트

참고 LAG 양쪽 끝에서 로드 밸런싱 알고리즘을 동일하게 구성해야 합니다. 상위 레이어 알고리즘은 필요에 따라 하위 레이어 알고리즘으로 후퇴합니다(예: 레이어 4 알고리즘이 ICMP 트래픽용 레이어 3으로 후퇴).

링크 선택 정책 지정

라이센스: 제어

지원되는 디바이스: Series 3

링크 집계를 사용하려면 양쪽 엔드포인트에서 각 링크의 속도와 미디어가 동일해야 합니다. 링크 속성은 동적으로 변경될 수 있으므로 시스템이 링크 선택 프로세스를 관리하는 방법을 결정하는 데 링크 선택 정책이 도움이 됩니다. 최고 포트 카운트를 최대화하는 링크 선택 정책은 링크 이중성을 지원하는 반면, 총 대역폭을 최대화하는 링크 선택 정책은 전체적인 링크 속도를 지원합니다. 안정적인 링크 선택 정책은 링크 상태의 과도한 변경을 최소화하려고 시도합니다.

참고 LAG 양쪽 끝에서 링크 선택 정책을 동일하게 구성해야 합니다.

LAG를 구성할 때 다음 옵션에서 구축 시나리오를 지원하는 링크 선택 정책을 선택합니다.

- Highest Port Count — 추가 이중성을 제공하는 가장 높은 총 활성 포트 카운트에 대해 이 옵션을 선택합니다.
- Highest Total Bandwidth — 집계된 링크에 대해 가장 높은 총 대역폭을 제공하려면 이 옵션을 제공합니다.

- Stable — 주요 관심사가 링크 안정성인 경우 이 옵션을 선택합니다. LAG를 구성하면, 포트 카운트나 대역폭 추가에 대해서보다는 절대적으로 필요한 경우(예: 링크 실패)에만 활성 링크가 변경됩니다.
- LACP Priority — LAG에서 어떤 링크가 활성 상태인지 파악하는 데 LACP를 사용하려면 이 옵션을 선택합니다. 구축 목표를 정의하지 않은 경우 또는 LAG 다른 쪽 끝의 디바이스가 비 -FirePOWER 디바이스인 경우 이 설정이 적합합니다.

  LACP가 활성화되면 LACP 우선순위 기반의 링크 선택 정책은 LACP의 두 속성(시스템 우선순위 및 링크 우선순위)을 사용합니다. 자세한 내용은 다음과 같습니다.

  - LACP 시스템 우선순위. LACP를 실행하는 각 파트너 디바이스에서 어떤 것이 링크 집계에서 상위인지 결정하기 위해 이 값을 구성합니다. 값이 낮을수록 시스템의 우선순위가 더 높습니다. 동적 링크 집계에서 LACP 시스템 우선순위가 더 높은 시스템이 먼저 자신의 쪽에서 멤버 링크의 선택한 상태를 설정한 다음, 우선순위가 더 낮은 시스템이 그에 따라 해당 멤버 링크를 설정합니다. 0~65535를 지정할 수 있습니다. 값을 지정하지 않으면 기본 우선순위 32768이 사용됩니다.
  - LACP 링크 우선순위. 집계 그룹에 속한 각 링크에서 이 값을 구성합니다. 링크 우선순위는 LAG에서 활성 및 대기 링크를 결정합니다. 값이 낮을수록 링크의 우선순위가 더 높습니다. 활성 링크가 다운되면 다운된 링크를 교체하기 위해 최고 우선순위의 대기 링크가 선택됩니다. 그러나 동일한 LACP 링크 우선순위가 둘 이상인 경우 가장 낮은 물리적 포트 번호의 링크가 대기 링크로 선택됩니다. 0~65535를 지정할 수 있습니다. 값을 지정하지 않으면 기본 우선순위 32768이 사용됩니다.

LACP는 동적 링크 집계를 지원하는 링크 선택 방법을 자동화하는 주요 부분입니다. 자세한 내용은 8-4페이지의 LACP 구성을/를 참조하십시오.

LACP 구성

라이센스: 제어

지원되는 디바이스: Series 3

IEEE 802.3ad의 구성 요소인 LACP(Link Aggregation Control Protocol)는 LAG 번들을 생성 및 유지하기 위해 시스템과 포트 정보를 교환하는 방법입니다. LACP를 활성화하면 LAG의 끝에 있는 각 디바이스는 LACP를 사용하여 어떤 링크가 집계에서 적극적으로 사용될지를 파악할 수 있습니다. LACP는 링크 간 LACP 패킷(또는 제어 메시지)을 교환하여 가용성과 이중성을 제공합니다. LACP는 링크의 기능을 동적으로 학습하여 다른 링크를 알립니다. LACP는 정확하게 일치하는 링크를 식별하면 링크를 LAG에 그룹화합니다. 한 링크가 실패하면 나머지 링크에서 트래픽이 계속 진행됩니다. 링크가 작동하려면 LACP를 LAG의 양쪽 끝에서 활성화해야 합니다.

LACP를 활성화할 때, 파트너 디바이스 간 LACP 패킷이 교환되는 방법을 결정하는 전송 모드를 LAG의 각 끝에 대해 선택해야 합니다. LACP 모드의 두 가지 옵션이 있습니다.

- Active — 디바이스가 LACP 패킷을 전송하여 원격 링크와 협상을 시작하는 Active 협상 상태로 전환하려면 이 모드를 선택합니다.
- Passive — 디바이스가 수신하는 LACP 패킷에 응답하지만 LACP 협상을 시작하지 못하는 Passive 협상 상태로 전환하려면 이 모드를 선택합니다.

참고 두 가지 모드에서 모두 LACP는 포트 속도와 같은 기준을 기반으로 링크 번들을 형성할 수 있는지 여부를 확인하기 위해 링크 간에 협상할 수 있습니다. 그러나 본질적으로 LAG의 양쪽 끝을 수신 대기 모드로 전환하는 passive-passive 컨피그레이션은 피해야 합니다.

LACP에는 디바이스 간에 LACP 패킷을 전송하는 방법을 정의하는 타이머가 있습니다. LACP는 다음 속도로 패킷을 교환합니다.

- Slow — 30초
- Fast — 1초

이 옵션이 적용된 디바이스는 LAG의 다른 쪽에 있는 파트너 디바이스에서 이 빈도로 LACP 패킷을 수신할 것으로 예상됩니다.

참고 디바이스 스택의 일부인 관리되는 디바이스에 LAG가 구성된 경우 기본 디바이스만이 파트너 시스템과의 LACP 통신에 참여합니다. 모든 보조 디바이스는 LACP 메시지를 기본 디바이스로 전달합니다. 기본 디바이스는 모든 동적 LAG 수정 사항을 보조 디바이스에 릴레이합니다.

스위치드 인터페이스 추가

라이센스: 제어

지원되는 디바이스: Series 3

관리되는 디바이스에서 2개 물리적 포트와 8개 물리적 포트 간에 결합하여 스위치드 LAG 인터페이스를 생성할 수 있습니다. 가상 스위치에서 트래픽을 처리하려면 먼저 스위치드 LAG 인터페이스를 할당해야 합니다. 관리되는 디바이스는 최대 14개의 LAG 인터페이스를 지원할 수 있습니다.

주의 MTU(최대 전송 단위)를 변경하면 디바이스의 트래픽이 중단되고 패킷이 삭제됩니다. MTU 설정 가능 범위는 FireSIGHT 시스템 디바이스 모델 및 인터페이스 유형에 따라 달라질 수 있습니다. 자세한 내용은 4-64페이지의 센싱 인터페이스 MTU 구성을/를 참조하십시오.

기존 스위치드 LAG 인터페이스를 수정하려면 인터페이스 옆의 수정 아이콘( )을 클릭합니다.

스위치드 LAG 인터페이스를 구성하려면

액세스: Admin/Network Admin

1단계 **Devices > Device Management**를 선택합니다.

Device Management 페이지가 나타납니다.

2단계 스위치드 LAG 인터페이스를 구성하려는 디바이스 옆의 수정 아이콘( )을 클릭합니다.

Interfaces 탭이 나타납니다.

3단계 **Add** 드롭다운 메뉴에서 **Add Aggregate Interface**를 클릭합니다.

4단계 **Switched**를 클릭하여 스위치드 LAG 인터페이스 옵션을 표시합니다.

5단계 원한다면 **Security Zone** 드롭다운 목록에서 기존 보안 영역을 선택하거나 **New**를 선택하여 새 보안 영역을 추가합니다.

6단계 **Virtual Switch** 드롭다운 목록에서 기존 가상 스위치를 선택하거나 **New**를 선택하여 새 가상 라우터를 추가해야 합니다.

참고 새 가상 스위치를 추가할 경우 스위치드 인터페이스를 설정한 다음에 Device Management 페이지의 Virtual Switches 탭(**Devices > Device Management > Virtual Switches**)에서 이를 구성해야 합니다. 6-6페이지의 가상 스위치 추가을/를 참조하십시오.

7단계 스위치드 LAG 인터페이스에서 트래픽을 처리할 수 있게 하려면 **Enabled** 확인란을 선택합니다.

이 확인란의 선택을 취소하면 인터페이스가 비활성화되어 사용자가 보안 목적으로 액세스할 수 없게 됩니다.

8단계 **Mode** 드롭다운 목록에서 링크 모드를 지정하는 옵션을 선택하거나 **Autonegotiation**을 선택하여 인터페이스에서 속도 및 양방향 설정 자동 협상이 구성되도록 지정합니다. Mode 설정은 구리 인터페이스에 대해서만 가능합니다.

참고 8000 Series 어플라이언스의 인터페이스는 반이중 옵션을 지원하지 않습니다. 링크가 속도를 자동 협상하면 동일한 속도 설정을 기반으로 LAG에 대해 모든 활성 링크가 선택됩니다.

9단계 **MDI/MDIX** 드롭다운 목록에서 옵션을 선택하여 인터페이스가 MDI(medium dependent interface), MDIX(medium dependent interface crossover) 또는 Auto-MDIX를 위해 구성되었는지 여부를 지정합니다. MDI/MDIX 설정은 구리 인터페이스에 대해서만 가능합니다.

기본적으로 MDI/MDIX는 Auto-MDIX로 설정됩니다. 그러면 MDI와 MDIX 간 스위칭을 자동으로 처리하여 링크를 확보합니다.

10단계 **MTU** 필드에 MTU를 입력합니다. 이는 허용되는 최대 크기 패킷을 나타냅니다.

MTU 설정 가능 범위는 FireSIGHT 시스템 디바이스 모델 및 인터페이스 유형에 따라 달라질 수 있습니다. 자세한 내용은 4-64페이지의 센싱 인터페이스 MTU 구성을/를 참조하십시오.

11단계 LAG 번들에 추가하기 위해 물리적 인터페이스를 선택하기 위한 두 가지 옵션이 **Link Aggregation** 아래에 있습니다.

- **Available Interfaces** 옆에서 하나 이상의 인터페이스를 선택한 다음 선택 항목 추가 아이콘( )을 클릭합니다. 여러 물리적 인터페이스를 선택하려면 **Ctrl** 또는 **Shift**를 사용합니다.
- LAG 번들에 모든 인터페이스 쌍을 추가하려면 모두 추가 아이콘( )을 클릭합니다.

팁 LAG 번들에서 물리적 인터페이스를 제거하려면 하나 이상의 물리적 인터페이스를 선택하고 선택 항목 제거 아이콘( )을 클릭합니다. LAG 번들에서 모든 물리적 인터페이스를 제거하려면 모두 제거 아이콘( )을 클릭합니다. Interfaces 탭에서 LAG 인터페이스를 삭제해도 인터페이스가 제거됩니다.

12단계 **Load-Balancing Algorithm** 드롭다운 목록에서 구축 시나리오를 지원하는 옵션을 선택합니다. 자세한 내용은 8-3페이지의 로드 밸런싱 알고리즘 지정을/를 참조하십시오.

13단계 **Link Selection Policy** 드롭다운 목록에서 구축 시나리오를 지원하는 옵션 Highest Port Count(이중화), Highest Total Bandwidth(속도), Stable(유지 관리 링크 상태의 과도하지 않은 변경) 또는 LACP Priority(자동 링크 집계)를 선택합니다.

LACP Priority를 선택하는 경우 **System Priority**에 대한 값을 할당해야 합니다. 그런 다음 **Configure Interface Priority** 링크를 클릭하여 LAG의 각 인터페이스에 대해 우선순위 값을 할당해야 합니다. 0~65535를 지정할 수 있습니다. 값을 지정하지 않으면 기본 우선순위 32768이 사용됩니다. 자세한 내용은 8-3페이지의 링크 선택 정책 지정을/를 참조하십시오.

참고 FireSIGHT 시스템 디바이스와 서드파티 네트워크 디바이스 간 집계 인터페이스를 구성하는 경우에는 **LACP Priority**를 선택하십시오.

14단계 **Tunnel Level** 드롭다운 목록에서 구축 시나리오를 지원하는 옵션, **Inner** 또는 **Outer**를 선택합니다.

레이어 3 로드 밸런싱이 구성된 경우 터널 레벨은 IPv4 트래픽에만 적용됩니다. Outer 터널은 레이어 2 및 IPv6 트래픽에 항상 사용됩니다. **Tunnel Level**이 명시적으로 설정되지 않은 경우 기본값은 **Outer**입니다.

15단계 스위치드 LAG 인터페이스가 Link Aggregation Control Protocol을 사용하여 트래픽을 처리하도록 하려면 **LACP** 아래에서 **Enabled** 확인란을 선택합니다. 자세한 내용은 8-4페이지의 LACP 구성을/를 참조하십시오.

확인란을 지우면 LAG 인터페이스는 고정 컨피그레이션이 되고 FireSIGHT 시스템은 집계에 대해 선택된 모든 물리적 인터페이스를 사용합니다.

16단계 파트너 디바이스에서 LACP 제어 메시지를 수신하는 빈도를 결정하는 값을 설정하려면 **Rate** 라디오 버튼을 선택합니다.

- 30초마다 패킷을 수신하려면 **Slow**를 선택합니다.
- 1초마다 패킷을 수신하려면 **Fast**를 선택합니다.

17단계 디바이스의 수신 대기 모드를 설정하려면 **Mode** 라디오 버튼을 선택합니다.

- LACP 패킷을 파트너 디바이스로 전송하여 원격 링크와의 협상을 시작하려면 **Active**를 선택합니다.
- 수신한 LACP 패킷에 응답하려면 **Passive**를 선택합니다.

18단계 **Save**를 클릭합니다.

스위치드 LAG 인터페이스가 구성됩니다. 디바이스 컨피그레이션을 적용해야 변경 사항이 적용됩니다. 자세한 내용은 4-25페이지의 디바이스에 변경 사항 적용을/를 참조하십시오.

집계 라우티드 인터페이스 추가

라이센스: 제어

지원되는 디바이스: Series 3

관리되는 디바이스에서 2개 물리적 포트와 8개 물리적 포트 간에 결합하여 라우티드 LAG 인터페이스를 생성할 수 있습니다. 가상 라우터에서 트래픽을 라우팅하려면 먼저 여기에 라우티드 LAG 인터페이스를 할당해야 합니다. 관리되는 디바이스는 최대 14개의 LAG 인터페이스를 지원할 수 있습니다.

라우티드 LAG 인터페이스에 고정 ARP(Address Resolution Protocol) 항목을 추가할 수 있습니다. 외부 호스트가 로컬 네트워크에서 트래픽을 보낼 목적지 IP 주소의 MAC 주소를 알아야 할 경우 ARP 요청을 보냅니다. 고정 ARP 항목을 구성하면 가상 라우터는 IP 주소 및 해당 MAC 주소와 함께 응답합니다.

라우티드 LAG 인터페이스에 대해 **ICMP Enable Responses** 옵션을 비활성화하더라도 모든 시나리오에서 ICMP 응답이 차단되지는 않습니다. 목적지 IP가 라우티드 인터페이스의 IP이고 프로토콜이 ICMP일 때 패킷을 삭제하도록 액세스 제어 정책에 규칙을 추가할 수 있습니다. 15-1페이지의 네트워크 기반 규칙으로 트래픽 제어을/를 참조하십시오.

관리되는 디바이스에서 **Inspect Local Router Traffic** 옵션을 활성화한 경우 호스트에 도달하기 전에 패킷을 삭제하므로 어떤 응답도 차단됩니다. 로컬 라우터 트래픽의 검사에 대한 자세한 내용은 4-54페이지의 고급 디바이스 설정 이해을/를 참조하십시오.

주의 MTU(최대 전송 단위)를 변경하면 디바이스의 트래픽이 중단되고 패킷이 삭제됩니다. MTU 설정 가능 범위는 FireSIGHT 시스템 디바이스 모델 및 인터페이스 유형에 따라 달라질 수 있습니다. 자세한 내용은 4-64페이지의 센싱 인터페이스 MTU 구성을/를 참조하십시오.

기존 라우티드 LAG 인터페이스를 수정하려면 인터페이스 옆의 수정 아이콘( )을 클릭합니다.

라우티드 LAG 인터페이스를 구성하려면

액세스: Admin/Network Admin

1단계 **Devices > Device Management**를 선택합니다.

Device Management 페이지가 나타납니다.

2단계 라우티드 LAG 인터페이스를 구성하려는 디바이스 옆의 수정 아이콘( )을 클릭합니다.

해당 디바이스의 Interfaces 탭이 나타납니다.

3단계 **Add** 드롭다운 메뉴에서 **Add Aggregate Interface**를 클릭합니다.

4단계 라우티드 LAG 인터페이스 옵션을 표시하려면 **Routed**를 클릭합니다.

5단계 원한다면 **Security Zone** 드롭다운 목록에서 기존 보안 영역을 선택하거나 **New**를 선택하여 새 보안 영역을 추가합니다.

6단계 **Virtual Router** 드롭다운 목록에서 기존 가상 라우터를 선택하거나 **New**를 선택하여 새 가상 라우터를 추가해야 합니다.

참고 새 가상 라우터를 추가할 경우 라우티드 인터페이스를 설정한 다음에 Device Management 페이지의 Virtual Routeres 탭(**Devices > Device Management > Virtual Routers**)에서 이를 구성해야 합니다. 7-9페이지의 가상 라우터 추가을/를 참조하십시오.

7단계 라우티드 LAG 인터페이스에서 트래픽을 처리할 수 있게 하려면 **Enabled** 확인란을 선택합니다.

이 확인란의 선택을 취소하면 인터페이스가 비활성화되어 사용자가 보안 목적으로 액세스할 수 없게 됩니다.

8단계 **Mode** 드롭다운 목록에서 링크 모드를 지정하는 옵션을 선택하거나 **Autonegotiation**을 선택하여 LAG 인터페이스에서 속도 및 양방향 설정 자동 협상이 구성되도록 지정합니다. Mode 설정은 구리 인터페이스에 대해서만 가능합니다.

참고 8000 Series 어플라이언스의 인터페이스는 반이중 옵션을 지원하지 않습니다. 링크가 속도를 자동 협상하면 동일한 속도 설정을 기반으로 LAG에 대해 모든 활성 링크가 선택됩니다.

9단계 **MDI/MDIX** 드롭다운 목록에서 옵션을 선택하여 LAG 인터페이스가 MDI(medium dependent interface), MDIX(medium dependent interface crossover) 또는 Auto-MDIX를 위해 구성되었는지 여부를 지정합니다. MDI/MDIX 설정은 구리 인터페이스에 대해서만 가능합니다.

일반적으로 MDI/MDIX는 Auto-MDIX로 설정됩니다. 그러면 MDI와 MDIX 간 스위칭을 자동으로 처리하여 링크를 확보합니다.

10단계 **MTU** 필드에 MTU를 입력합니다. 이는 허용되는 최대 크기 패킷을 나타냅니다. MTU는 레이어 3 MTU가 아니라 레이어 2 MTU/MRU입니다.

MTU 설정 가능 범위는 FireSIGHT 시스템 디바이스 모델 및 인터페이스 유형에 따라 달라질 수 있습니다. 자세한 내용은 4-64페이지의 센싱 인터페이스 MTU 구성을/를 참조하십시오.

11단계 LAG 인터페이스에서 ping, traceroute와 같은 ICMP 트래픽에 응답하는 것을 허용하려면 **ICMP** 옆에서 **Enable Responses** 확인란을 선택합니다.

12단계 LAG 인터페이스에서 라우터 광고를 브로드캐스트하는 것을 허용하려면 **IPv6 NDP** 옆에서 **Enable Router Advertisement** 확인란을 선택합니다.

13단계 IP 주소를 추가하려면 **Add**를 클릭합니다.

Add IP Address 팝업 창이 나타납니다.

14단계 **Address** 필드에 라우티드 LAG 인터페이스의 IP 주소와 서브넷 마스크를 CIDR 표기법으로 입력합니다. 다음에 유의하십시오.

- 네트워크 및 브로드캐스트 주소 또는 고정 MAC 주소 00:00:00:00:00:00 및 FF:FF:FF:FF:FF:FF를 추가할 수 없습니다.
- 가상 라우터에 있는 인터페이스에, 서브넷 마스크와 무관하게, 동일한 IP 주소를 추가할 수 없습니다.

15단계 IPv6 주소를 사용하는 경우, **IPv6** 필드 옆에서 **Address Autoconfiguration** 확인란을 선택하여 LAG 인터페이스의 IP 주소를 자동으로 설정할 수도 있습니다.

16단계 **Type**에서는 Normal 또는 SFRP 중 하나를 선택합니다.

SFRP 옵션의 경우 7-7페이지의 SFRP 구성에서 자세한 내용을/를 참조하십시오.

17단계 **OK**를 클릭합니다.

IP 주소가 추가되었습니다.

IP 주소를 수정하려면 수정 아이콘( )을 클릭합니다. IP 주소를 삭제하려면 삭제 아이콘( )을 클릭합니다.

참고 클러스터링된 디바이스의 라우티드 인터페이스에 IP 주소를 추가할 때 클러스터 피어의 라우티드 인터페이스에 해당 IP 주소를 추가해야 합니다.

18단계 고정 ARP 항목을 추가하려면 **Add**를 클릭합니다.

Add Static ARP Entry 팝업 창이 나타납니다.

19단계 **IP Address** 필드에 고정 ARP 항목의 IP 주소를 입력합니다.

20단계 **MAC Address** 필드에 IP 주소와 연결할 MAC 주소를 입력합니다. 2자리 16진수의 그룹 6개가 콜론으로 구분되는 표준 형식(예: 01:23:45:67:89:AB)을 사용하여 주소를 입력합니다.

21단계 **OK**를 클릭합니다.

고정 ARP 항목이 추가되었습니다.

팁 고정 ARP 항목을 수정하려면 수정 아이콘( )을 클릭합니다. 고정 ARP 항목을 삭제하려면 삭제 아이콘( )을 클릭합니다.

22단계 LAG 번들에 추가하기 위해 물리적 인터페이스를 선택하기 위한 두 가지 옵션이 **Link Aggregation** 아래에 있습니다.

- **Available Interfaces** 옆에서 하나 이상의 인터페이스를 선택한 다음 선택 항목 추가 아이콘( )을 클릭합니다. 여러 물리적 인터페이스를 선택하려면 **Ctrl** 또는 **Shift**를 사용합니다.
- LAG 번들에 모든 인터페이스 쌍을 추가하려면 모두 추가 아이콘( )을 클릭합니다.

팁 LAG 번들에서 물리적 인터페이스를 제거하려면 하나 이상의 물리적 인터페이스를 선택하고 선택 항목 제거 아이콘( )을 클릭합니다. LAG 번들에서 모든 물리적 인터페이스를 제거하려면 모두 제거 아이콘( )을 클릭합니다. Interfaces 탭에서 LAG 인터페이스를 삭제해도 인터페이스가 제거됩니다.

23단계 **Load-Balancing Algorithm** 드롭다운 목록에서 구축 시나리오를 지원하는 옵션을 선택합니다. 자세한 내용은 8-3페이지의 로드 밸런싱 알고리즘 지정을/를 참조하십시오.

24단계 **Link Selection Policy** 드롭다운 목록에서 구축 시나리오를 지원하는 옵션 Highest Port Count(이중화), Highest Total Bandwidth(속도), Stable(유지 관리 링크 상태의 과도하지 않은 변경) 또는 LACP Priority(자동 링크 집계)를 선택합니다.

LACP Priority를 선택하는 경우 **System Priority**에 대한 값을 할당해야 합니다. 그런 다음 **Configure Interface Priority** 링크를 클릭하여 LAG의 각 인터페이스에 대해 우선순위 값을 할당해야 합니다. 0~65535를 지정할 수 있습니다. 값을 지정하지 않으면 기본 우선순위 32768이 사용됩니다. 자세한 내용은 8-3페이지의 링크 선택 정책 지정을/를 참조하십시오.

참고 FireSIGHT 시스템 디바이스와 서드파티 네트워크 디바이스 간 집계 인터페이스를 구성하는 경우에는 **LACP Priority**를 선택하십시오.

25단계 **Tunnel Level** 드롭다운 목록에서 구축 시나리오를 지원하는 옵션, **Inner** 또는 **Outer**를 선택합니다.

레이어 3 로드 밸런싱이 구성된 경우 터널 레벨은 IPv4 트래픽에만 적용됩니다. Outer 터널은 레이어 2 및 IPv6 트래픽에 항상 사용됩니다. **Tunnel Level**이 명시적으로 설정되지 않은 경우 기본값은 **Outer**입니다.

26단계 스위치드 LAG 인터페이스가 Link Aggregation Control Protocol을 사용하여 트래픽을 처리하도록 하려면 **LACP** 아래에서 **Enabled** 확인란을 선택합니다. 자세한 내용은 8-4페이지의 LACP 구성을/를 참조하십시오.

확인란을 지우면 LAG 인터페이스는 고정 컨피그레이션이 되고 FireSIGHT 시스템은 집계에 대한 모든 물리적 인터페이스를 사용합니다.

27단계 파트너 디바이스에서 LACP 제어 메시지를 수신하는 빈도를 결정하는 값을 설정하려면 **Rate** 라디오 버튼을 선택합니다.

- 30초마다 패킷을 수신하려면 **Slow**를 선택합니다.
- 1초마다 패킷을 수신하려면 **Fast**를 선택합니다.

28단계 디바이스의 수신 대기 모드를 설정하려면 **Mode** 라디오 버튼을 선택합니다.

- LACP 패킷을 파트너 디바이스로 전송하여 원격 링크와의 협상을 시작하려면 **Active**를 선택합니다.
- 수신한 LACP 패킷에 응답하려면 **Passive**를 선택합니다.

29단계 **Save**를 클릭합니다.

라우티드 LAG 인터페이스가 구성됩니다. 디바이스 컨피그레이션을 적용해야 변경 사항이 적용됩니다. 4-25페이지의 디바이스에 변경 사항 적용을/를 참조하십시오.

논리적 집계 인터페이스 추가

라이센스: 제어

지원되는 디바이스: Series 3

각 스위치드 또는 라우티드 집계 인터페이스에 대해 여러 논리적 인터페이스를 추가할 수 있습니다. VLAN 태그가 포함된 LAG 인터페이스에서 수신한 트래픽을 처리하려면 각 논리적 LAG 인터페이스를 해당 VLAN 태그와 연결해야 합니다. 물리적 스위치드 또는 라우티드 인터페이스에서 추가하는 것처럼 논리적 인터페이스를 스위치드 또는 라우티드 집계 인터페이스에 추가합니다.

참고 LAG 인터페이스를 생성할 때 기본적으로 "태그가 지정되지 않은" 논리적 인터페이스도 생성됩니다. 이 인터페이스는 **lag*n.0*** 레이블로 식별되며, 여기서 ***n***은 0~13의 정수입니다. 작동하려면 각 LAG에 이 논리적 인터페이스가 적어도 하나는 필요합니다. 추가 논리적 인터페이스를 LAG와 연결하여 VLAN 태그 트래픽을 처리할 수 있습니다. 각 추가 논리적 인터페이스에 고유한 VLAN 태그가 필요합니다. FireSIGHT 시스템은 1~4094 범위의 VLAN 태그를 지원합니다.

또한 논리적 라우티드 인터페이스에서 SFRP를 구성할 수 있습니다. 자세한 내용은 7-7페이지의 SFRP 구성을/를 참조하십시오.

논리적 라우티드 인터페이스에 대해 **ICMP Enable Responses** 옵션을 비활성화하더라도 모든 시나리오에서 ICMP 응답이 차단되지는 않습니다. 목적지 IP가 라우티드 인터페이스의 IP이고 프로토콜이 ICMP일 때 패킷을 삭제하도록 액세스 제어 정책에 규칙을 추가할 수 있습니다. 15-1페이지의 네트워크 기반 규칙으로 트래픽 제어을/를 참조하십시오.

관리되는 디바이스에서 **Inspect Local Router Traffic** 옵션을 활성화한 경우 호스트에 도달하기 전에 패킷을 삭제하므로 어떤 응답도 차단됩니다. 로컬 라우터 트래픽의 검사에 대한 자세한 내용은 4-54페이지의 고급 디바이스 설정 이해을/를 참조하십시오.

주의 MTU(최대 전송 단위)를 변경하면 디바이스의 라우티드 또는 스위치드 트래픽이 중단되고 패킷이 삭제됩니다. MTU 설정 가능 범위는 FireSIGHT 시스템 디바이스 모델 및 인터페이스 유형에 따라 달라질 수 있습니다. 자세한 내용은 4-64페이지의 센싱 인터페이스 MTU 구성을/를 참조하십시오.

기존 논리적 LAG 인터페이스를 수정하려면 인터페이스 옆의 수정 아이콘( )을 클릭합니다.

논리적 LAG 인터페이스를 추가하려면

액세스: Admin/Network Admin

1단계 **Devices > Device Management**를 선택합니다.

Device Management 페이지가 나타납니다.

2단계 논리적 LAG 인터페이스를 추가하려는 디바이스 옆의 수정 아이콘( )을 클릭합니다.

Interfaces 탭이 나타납니다.

3단계 **Add** 드롭다운 메뉴에서 **Add Logical Interface**를 클릭합니다.

Add Interface 팝업 창이 나타납니다.

4단계 스위치드 인터페이스 옵션을 표시하려면 **Switched**를 클릭하고, 라우티드 인터페이스 옵션을 표시하려면 **Routed**를 클릭합니다.

LAG에 대한 논리적 인터페이스를 생성할 경우 **Interface** 드롭다운 목록에서 사용 가능한 LAG를 선택합니다. 집계 인터페이스는 **lag*n*** 레이블로 식별되며, 여기서 ***n***은 0~13의 정수입니다.

스위치드 인터페이스에 논리적 인터페이스를 추가하는 방법에 대한 자세한 내용은 6-3페이지의 논리적 스위치드 인터페이스 추가을/를 참조하십시오.

라우티드 인터페이스에 논리적 인터페이스를 추가하는 방법에 대한 자세한 내용은 7-4페이지의 논리적 라우티드 인터페이스 추가을/를 참조하십시오.

참고 집계 인터페이스가 비활성화되면 그 집계 인터페이스에 연결된 논리적 인터페이스도 비활성화됩니다.

집계 인터페이스 통계 보기

라이센스: 제어

지원되는 디바이스: Series 3

각 집계 인터페이스에 대한 프로토콜과 트래픽 통계를 볼 수 있습니다. 통계에는 LACP 키와 파트너 정보, 수신된 패킷, 패킷 송신기, 삭제된 패킷 등의 LACP 프로토콜 정보가 표시됩니다. 포트 단위로 트래픽과 링크 정보를 표시하기 위해 멤버 인터페이스에 대해 통계가 더 세분화됩니다.

집계 인터페이스 정보는 사전 정의된 대시보드 위젯을 통해 대시보드에도 표시됩니다. Current Interface Status 위젯은 활성화되었든 사용되고 있지 않든, 어플라이언스에 있는 모든 인터페이스의 상태를 표시합니다. Interface Traffic 위젯은 대시보드 시간 범위 중에 어플라이언스의 인터페이스에서 트래픽의 수신(Rx) 및 송신(Tx) 속도를 보여줍니다. 55-7페이지의 사전 정의된 위젯 이해을/를 참조하십시오.

집계 인터페이스 통계를 보려면

액세스: Admin/Network Admin

1단계 **Devices > Device Management**를 선택합니다.

Device Management 페이지가 나타납니다.

2단계 논리적 집계 인터페이스 통계를 표시할 디바이스 옆에 있는 수정 아이콘( )을 클릭합니다.

해당 디바이스의 Interfaces 탭이 나타납니다.

3단계 통계를 표시할 인터페이스 옆에 있는 수정 아이콘( )을 클릭합니다.

Statistics 팝업 창이 나타납니다.

4단계 **OK**를 클릭하여 창을 닫습니다.

집계 인터페이스 삭제

라이센스: 제어

지원되는 디바이스: Series 3

다음 절차에서는 집계 인터페이스를 삭제하는 방법에 대해 설명합니다.

집계 인터페이스를 삭제하려면

액세스: Admin/Network Admin

1단계 **Devices > Device Management**를 선택합니다.

Device Management 페이지가 나타납니다.

2단계 집계 인터페이스를 삭제하려는 디바이스 옆의 수정 아이콘()을 클릭합니다.

해당 디바이스의 Interfaces 탭이 나타납니다.

3단계 삭제하려는 집계 인터페이스 옆에 있는 삭제 아이콘()을 클릭합니다.

집계 인터페이스는 **lag*n*** 레이블로 식별할 수 있으며, 여기서 ***n***은 0~13의 정수입니다.

4단계 확인 메시지가 표시되면 집계 인터페이스를 삭제할 것임을 확인합니다.

인터페이스가 삭제되었습니다. 디바이스 컨피그레이션을 적용해야 변경 사항이 적용됩니다. 4-25 페이지의 디바이스에 변경 사항 적용을/를 참조하십시오.

9장 하이브리드 인터페이스 설정

관리되는 디바이스에 논리적 하이브리드 인터페이스를 구성하여 FireSIGHT 시스템에서 가상 라우터와 가상 스위치 사이의 트래픽을 연결하도록 지정할 수 있습니다. 가상 스위치의 인터페이스에 수신된 IP 트래픽의 주소가 연결된 하이브리드 논리적 인터페이스의 MAC 주소로 지정된 경우, 레이어 3 트래픽으로 처리되고 대상 IP 주소에 따라 트래픽을 라우팅하거나 다른 방식으로 응답합니다. 시스템이 다른 트래픽을 수신할 경우 레이어 2 트래픽으로 처리하고 적절히 스위칭합니다. 가상의 관리되는 디바이스 또는 Cisco NGIPS for Blue Coat X-Series에서는 논리적 하이브리드 인터페이스를 구성할 수 없습니다.

하이브리드 인터페이스 설정에 대한 자세한 내용은 9-1페이지의 논리적 하이브리드 인터페이스 추가을/를 참조하십시오.

논리적 하이브리드 인터페이스 추가

라이센스: 제어

지원되는 디바이스: Series 3

레이어 2와 레이어 3 간에 트래픽을 연결하려면 논리적 하이브리드 인터페이스를 가상 라우터 및 가상 스위치와 연결해야 합니다. 단일 하이브리드 인터페이스는 하나의 가상 스위치에만 연결할 수 있습니다. 그러나 여러 하이브리드 인터페이스를 하나의 가상 라우터에 연결할 수 있습니다.

또한 논리적 하이브리드 인터페이스에서 SFRP를 구성할 수 있습니다. 자세한 내용은 7-7페이지의 SFRP 구성을/를 참조하십시오.

하이브리드 인터페이스에 대해 **ICMP Enable Responses** 옵션을 비활성화하더라도 모든 시나리오에서 ICMP 응답이 차단되지는 않습니다. 목적지 IP가 하이브리드 인터페이스의 IP이고 프로토콜이 ICMP일 때 패킷을 삭제하도록 액세스 제어 정책에 규칙을 추가할 수 있습니다. 15-1페이지의 네트워크 기반 규칙으로 트래픽 제어을/를 참조하십시오.

관리되는 디바이스에서 **Inspect Local Router Traffic** 옵션을 활성화한 경우 호스트에 도달하기 전에 패킷을 삭제하므로 어떤 응답도 차단됩니다. 로컬 라우터 트래픽의 검사에 대한 자세한 내용은 4-54페이지의 고급 디바이스 설정 이해을/를 참조하십시오.

주의 MTU(최대 전송 단위)를 변경하면 디바이스의 라우티드 또는 스위치드 트래픽이 중단되고 패킷이 삭제됩니다. MTU 설정 가능 범위는 FireSIGHT 시스템 디바이스 모델 및 인터페이스 유형에 따라 달라질 수 있습니다. 자세한 내용은 4-64페이지의 센싱 인터페이스 MTU 구성을/를 참조하십시오.

기존 하이브리드 인터페이스를 수정하려면 인터페이스 옆의 수정 아이콘( )을 클릭합니다.

논리적 하이브리드 인터페이스를 추가하려면

액세스: Admin/Network Admin

1단계 **Devices > Device Management**를 선택합니다.

Device Management 페이지가 나타납니다.

2단계 하이브리드 인터페이스를 추가하려는 디바이스 옆의 수정 아이콘( )을 클릭합니다.

Interfaces 탭이 나타납니다.

3단계 **Add** 드롭다운 메뉴에서 **Add Logical Interface**를 클릭합니다.

Add Interface 팝업 창이 나타납니다.

4단계 하이브리드 인터페이스 옵션을 표시하려면 **Hybrid**를 클릭합니다.

5단계 **Name** 필드에 인터페이스의 이름을 입력합니다. 영숫자와 공백을 사용할 수 있습니다.

6단계 **Virtual Router** 드롭다운 목록에서 기존 가상 라우터를 선택하거나, **None**을 선택하거나, **New**를 선택하여 새 가상 라우터를 추가합니다.

새 가상 라우터를 추가할 경우 하이브리드 인터페이스 설정을 마친 다음에 Device Management 페이지(**Devices > Device Management > Virtual Routers**)에서 이를 구성해야 합니다. 7-9페이지의 가상 라우터 추가을/를 참조하십시오.

7단계 **Virtual Switch** 드롭다운 목록에서 기존 가상 스위치를 선택하거나, **None**을 선택하거나, **New**를 선택하여 새 가상 스위치를 추가합니다.

새 가상 스위치를 추가할 경우 하이브리드 인터페이스 설정을 마친 다음에 Device Management 페이지(**Devices > Device Management > Virtual Switches**)에서 이를 구성해야 합니다. 6-6페이지의 가상 스위치 추가을/를 참조하십시오.

8단계 하이브리드 인터페이스에서 트래픽을 처리할 수 있게 하려면 **Enabled** 확인란을 선택합니다.

확인란의 선택을 취소할 경우 인터페이스는 비활성화되고 관리상 다운됩니다.

9단계 **MTU** 필드에 MTU를 입력합니다. 이는 허용되는 최대 크기 패킷을 나타냅니다.

MTU 설정 가능 범위는 FireSIGHT 시스템 디바이스 모델 및 인터페이스 유형에 따라 달라질 수 있습니다. 자세한 내용은 4-64페이지의 센싱 인터페이스 MTU 구성을/를 참조하십시오.

10단계 인터페이스에서 ping, traceroute와 같은 ICMP 트래픽에 응답하는 것을 허용하려면 **ICMP** 옆에서 **Enable Responses** 확인란을 선택합니다.

11단계 인터페이스에서 라우터 광고를 브로드캐스트하는 것을 허용하려면 **IPv6 NDP** 옆에서 **Enable Router Advertisement** 확인란을 선택합니다.

IPv6 주소를 추가한 경우에만 이 옵션을 선택할 수 있습니다.

12단계 IP 주소를 추가하려면 **Add**를 클릭합니다.

Add IP Address 팝업 창이 나타납니다.

13단계 **Address** 필드에 IP 주소와 서브넷 마스크를 입력합니다. 다음에 유의하십시오.

- 네트워크 및 브로드캐스트 주소 또는 고정 MAC 주소 00:00:00:00:00:00 및 FF:FF:FF:FF:FF:FF를 추가할 수 없습니다.
- 가상 라우터에 있는 인터페이스에, 서브넷 마스크와 무관하게, 동일한 IP 주소를 추가할 수 없습니다.

14단계 선택적으로, IPv6 주소가 있는 경우 **IPv6** 필드 옆에서 **Address Autoconfiguration** 확인란을 선택하여 인터페이스의 IP 주소를 자동으로 설정할 수도 있습니다.

15단계 **Type**에서는 Normal 또는 SFRP 중 하나를 선택합니다.

SFRP 옵션의 경우 7-7페이지의 SFRP 구성에서 자세한 내용을/를 참조하십시오.

16단계 **OK**를 클릭합니다.

IP 주소가 추가되었습니다.

팁 IP 주소를 수정하려면 수정 아이콘( )을 클릭합니다. IP 주소를 삭제하려면 삭제 아이콘( )을 클릭합니다.

17단계 **Save**를 클릭합니다.

논리적 하이브리드 인터페이스가 추가됩니다. 디바이스 컨피그레이션을 적용해야 변경 사항이 적용됩니다. 4-25페이지의 디바이스에 변경 사항 적용을/를 참조하십시오.

논리적 하이브리드 인터페이스 삭제

라이센스: 제어

지원되는 디바이스: Series 3

다음 절차에서는 논리적 하이브리드 인터페이스를 삭제하는 방법에 대해 설명합니다.

하이브리드 인터페이스를 삭제하려면

액세스: Admin/Network Admin

1단계 **Devices > Device Management**를 선택합니다.

Device Management 페이지가 나타납니다.

2단계 논리적 하이브리드 인터페이스를 삭제하려는 디바이스 옆의 수정 아이콘( )을 클릭합니다.

해당 디바이스의 Interfaces 탭이 나타납니다.

3단계 삭제하려는 논리적 하이브리드 인터페이스 옆에 있는 삭제 아이콘( )을 클릭합니다.

4단계 확인 메시지가 표시되면 인터페이스를 삭제할 것임을 확인합니다.

인터페이스가 삭제되었습니다. 디바이스 컨피그레이션을 적용해야 변경 사항이 적용됩니다. 4-25페이지의 디바이스에 변경 사항 적용을/를 참조하십시오.

10장 게이트웨이 VPN 사용

VPN(virtual private network)은 인터넷과 같은 공개 소스나 기타 네트워크를 통해 엔드포인트 간에 보안 터널을 설정하는 네트워크 연결입니다. FireSIGHT 시스템에서 Cisco이 관리하는 디바이스와 . 이 시스템에서는 IPSec(Internet Protocol Security) 프로토콜을 사용하여 터널을 생성합니다.

Cisco가 관리하는 디바이스만 Cisco VPN 구축에서 엔드포인트로 사용될 수 있습니다. 서드파티 엔드포인트는 지원되지 않습니다.

VPN 연결이 설정되면 로컬 게이트웨이의 뒤에 있는 호스트는 보안 VPN 터널을 통해 원격 게이트의 뒤에 있는 호스트와 연결할 수 있습니다. 연결은 두 게이트웨이의 IP 주소와 호스트 이름, 그 뒤에 있는 서브넷, 두 게이트웨이의 상호 인증에 사용되는 공유 암호로 구성됩니다.

VPN 엔드포인트는 IKE(Internet Key Exchange) 버전 1 또는 버전 2 프로토콜로 상호 인증하여 터널에 대한 보안 연결을 만듭니다. 터널에 들어오는 데이터를 인증하는 데 IPSec AH(authentication header) 프로토콜 또는 IPSec ESP(encapsulating security payload) 프로토콜 중 하나를 사용합니다. ESP 프로토콜은 AH와 동일한 기능을 제공할 뿐 아니라 데이터를 암호화합니다.

구축에 액세스 제어 정책이 있을 경우 액세스 제어를 통과해야 VPN 트래픽을 보낼 수 있습니다. 또한 터널이 다운된 상태에서는 공개 소스에 터널 트래픽을 보내지 않습니다.

VPN 구축을 구성하고 적용하려면 각 타겟 관리 대상 디바이스에서 VPN 라이센스가 활성화되어야 합니다. 또한 VPN 기능은 Series 3 디바이스에서만 사용할 수 있습니다.

VPN 구축의 생성 및 관리에 대한 자세한 내용은 다음 절을 참조하십시오.

- 10-1페이지의 IPSec 이해
- 10-2페이지의 VPN 구축 이해
- 10-5페이지의 VPN 구축 관리

IPSec 이해

IPSec 프로토콜 모음은 VPN 터널 전반의 IP 패킷이 ESP 또는 AH 보안 프로토콜에서 해싱, 암호화, 캡슐화되는 방식을 정의합니다. FireSIGHT 시스템에서는 SA(Security Association)의 해시 알고리즘 및 암호화 키를 사용하는데, 이는 IKE 프로토콜에 의해 두 게이트웨이 사이에서 설정됩니다.

SA는 두 디바이스 간에 공유 보안 특성을 설정하고 VPN 엔드포인트의 보안 통신 지원을 가능하게 합니다. SA를 통해 두 VPN 엔드포인트 간의 VPN 터널을 보호하는 방식에 대한 매개 변수를 처리할 수 있습니다.

IPSec 연결 협상의 초기 단계에서 ISAKMP(Internet Security Association and Key Management Protocol)를 사용하여 엔드포인트와 인증된 키 교환 간에 VPN을 설정합니다. IKE 프로토콜은 ISAKMP 내에 상주합니다. IKE 프로토콜에 대한 자세한 내용은 10-2페이지의 IKE 이해을/를 참조하십시오.

AH 보안 프로토콜은 패킷 헤더와 데이터를 보호하지만 이를 암호화할 수는 없습니다. ESP는 패킷에 대한 암호화와 보호를 수행하지만, 가장 바깥쪽 IP 헤더를 보호할 수 없습니다. 대개는 이 보호가 필요하지 않으며, 대부분의 VPN 구축에서는 암호화 기능 때문에 AH보다 ESP를 더 자주 사용합니다. VPN은 터널 모드에서만 작동하므로 ESP 프로토콜에서 레이어 3 이상의 전체 패킷을 암호화하고 인증합니다. 터널 모드의 ESP는 후자의 암호화 기능을 제공할 뿐 아니라 데이터를 암호화합니다.

IKE 이해

FireSIGHT 시스템에서는 수동으로 두 게이트웨이를 상호 인증하고 터널에 대해 SA를 협상하는 데 IKE 프로토콜을 사용합니다. 이 프로세스는 2단계로 구성됩니다.

IKE 1단계에서는 Diffie-Hellman 키 교환을 통해 향후 IKE 통신의 암호화를 위한 사전 공유 키를 생성하는 방법으로 보안 인증 통신 채널을 설정합니다. 이러한 협상을 통해 양방향 ISAKMP SA가 생성됩니다. 사전 공유 키를 사용한 인증을 지원합니다. 1단계는 기본 모드에서 작동하는데, 협상 중에 모든 데이터의 보호를 모색하면서 피어의 ID도 보호합니다.

IKE 2단계에서는 IKE 피어가 1단계에서 설정된 보안 채널을 통해 IPSec을 대신하여 SA를 협상합니다. 이 협상에서는 적어도 2개의 단방향 SA, 즉 인바운드 1개와 아웃바운드 1개가 생성됩니다.

VPN 구축 이해

VPN 구축은 VPN에 포함된 엔드포인트와 네트워크 및 이들의 상호 연결 방식을 지정합니다. VPN 구축을 구성한 다음에는 관리 대상 디바이스 또는 또 다른 방어 센터가 관리하는 디바이스에 적용할 수 있습니다.

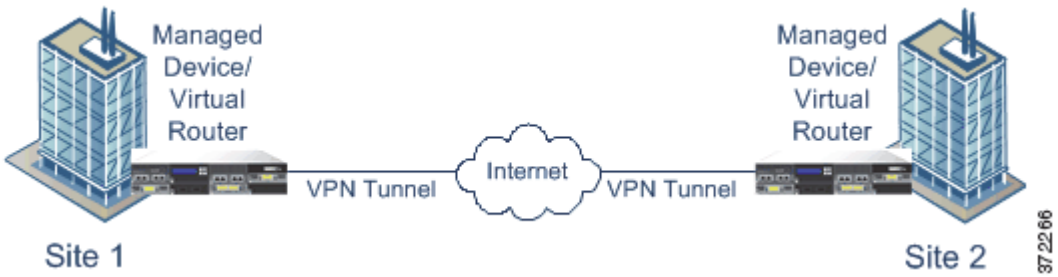
포인트-투-포인트(point-to-point), 스타(star), 메시(mesh)의 3가지 VPN 구축 유형을 지원합니다. 이 VPN 구축에 대한 자세한 내용은 다음 절을 참조하십시오.

- 10-2페이지의 포인트-투-포인트 VPN 구축 이해
- 10-3페이지의 스타 VPN 구축 이해
- 10-4페이지의 메시 VPN 구축 이해

포인트-투-포인트 VPN 구축 이해

포인트-투-포인트 VPN 구축에서는 2개의 엔드포인트가 서로 직접 통신합니다. 두 엔드포인트를 피어 디바이스로 구성하며, 둘 중 하나가 보안 연결을 시작할 수 있습니다. 이 컨피그레이션의 각 디바이스는 VPN을 지원하는 관리 대상 디바이스여야 합니다.

다음 다이어그램은 일반적인 포인트-투-포인트 VPN 구축을 보여줍니다.



자세한 내용은 10-6페이지의 PTP VPN 구축 컨피그레이션을/를 참조하십시오.

스타 VPN 구축 이해

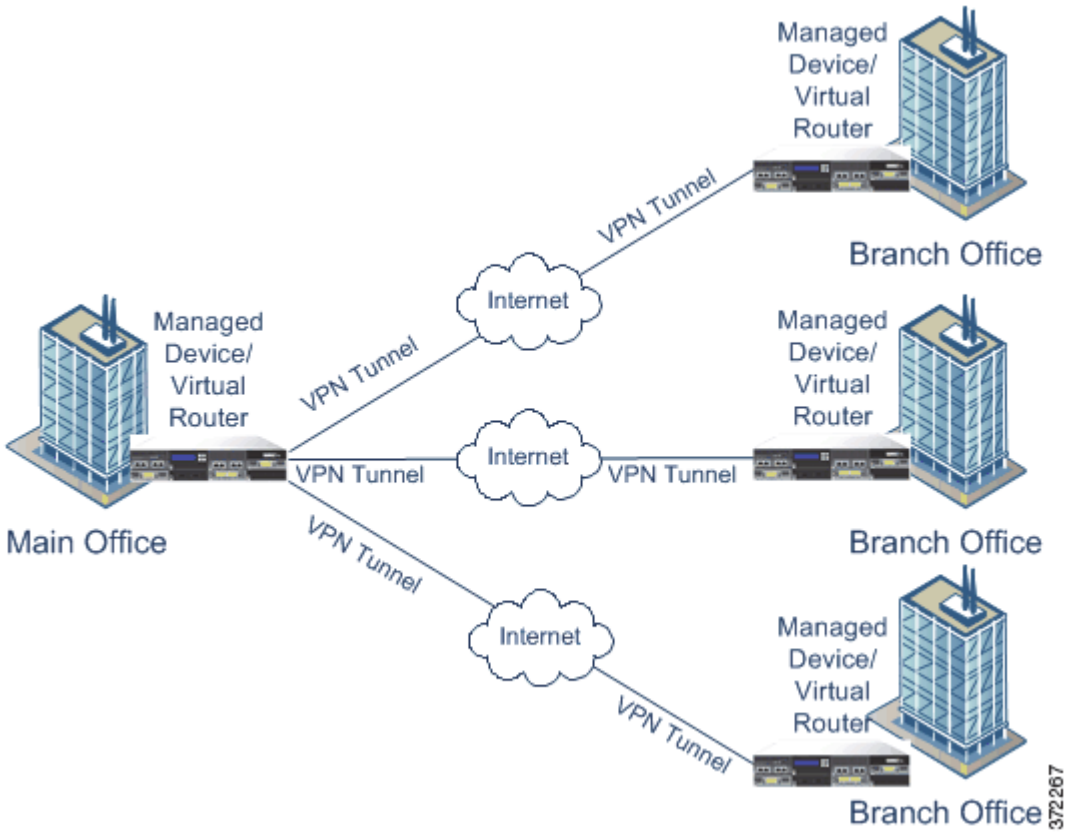
스타 VPN 구축에서는 중앙 엔드포인트(허브 노드)가 여러 원격 엔드포인트(리프 노드)와의 보안 연결을 설정합니다. 허브 노드와 개별 리프 노드 간 연결 각각은 별도의 VPN 터널입니다. 리프 노드의 뒤에 있는 호스트는 허브 노드를 통해 서로 통신할 수 있습니다.

스타 구축은 주로 인터넷이나 기타 서드파티 네트워크를 통한 보안 연결을 사용하여 조직의 본사 및 지사 위치와 연결하는 VPN을 나타냅니다. 스타 VPN 구축에서는 모든 직원이 조직의 네트워크에 대해 통제된 액세스 권한을 갖습니다.

일반적인 스타 구축에서는 허브 노드가 본사에 위치합니다. 리프 노드는 지사에 있으며 대부분의 트래픽을 시작합니다. 각 노드는 VPN을 지원하는 관리 대상 디바이스여야 합니다.

스타 구축은 IKE 버전 2만 지원합니다.

다음 다이어그램에서는 일반적인 스타 VPN 구축을 보여줍니다.

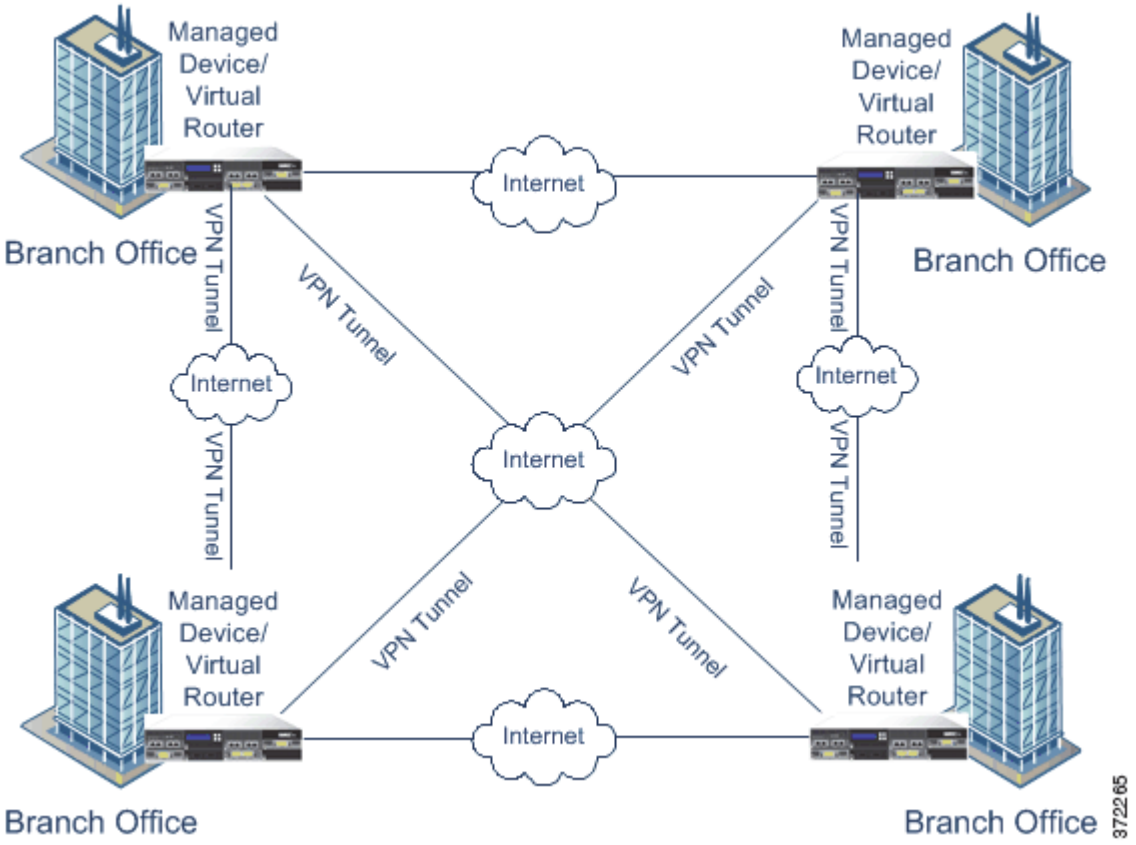


자세한 내용은 10-8페이지의 스타 VPN 구축 구성을/를 참조하십시오.

메시 VPN 구축 이해

메시 VPN 구축에서는 모든 엔드포인트가 개별 VPN 터널을 통해 나머지 모든 엔드포인트와 통신할 수 있습니다. 메시 구축은 이중화를 제공하므로 한 엔드포인트에 장애가 발생하더라도 나머지 엔드포인트는 계속 서로 통신할 수 있습니다. 이러한 유형의 구축은 대개 분산된 지사의 위치를 연결하는 VPN에 사용됩니다. 이러한 구성으로 구축하는 VPN을 지원하는 관리 대상 디바이스의 수는 필요한 이중화 레벨에 따라 달라집니다. 각 엔드포인트는 VPN을 사용하는 관리 대상 디바이스여야 합니다.

다음 다이어그램에서는 일반적인 메시 VPN 구축을 보여줍니다.



자세한 내용은 10-10페이지의 메시 VPN 구축 구성을/를 참조하십시오.

VPN 구축 관리

라이센스: VPN

지원되는 디바이스: Series 3

VPN 페이지(**Devices > VPN**)에서 모든 현재 VPN 구축을 이름별로 확인하고 그 구축에 포함된 엔드포인트도 볼 수 있습니다. 이 페이지의 옵션으로 VPN 구축의 상태를 보고 새 구축을 생성하며 구축을 적용하고 수정 또는 삭제할 수 있습니다.

주의 방어 센터에 디바이스를 등록할 때 기본 액세스 제어 정책을 선택할 경우 기본 액세스 제어 규칙이 모든 트래픽을 차단합니다. 이 디바이스에 VPN 구축을 구성하면 구축은 실패합니다.

방어 센터에 디바이스를 등록할 때 적용된 VPN 구축이 등록 과정에서 방어 센터와 동기화됩니다.

다음 표에서는 VPN 페이지에서 구축을 관리하기 위해 수행할 수 있는 작업에 대해 설명합니다.

표 10-1 VPN 구축 관리 작업

목적	가능한 작업
새 VPN 구축 생성	**Add**를 클릭합니다. 자세한 내용은 10-5페이지의 VPN 구축 구성을/를 참조하십시오.
기존 VPN 구축의 설정 수정	수정 아이콘( )을 클릭합니다. 자세한 내용은 10-5페이지의 VPN 구축 구성을/를 참조하십시오.
기존 VPN 구축의 상태 보기	상태 아이콘을 클릭합니다. 자세한 내용은 10-14페이지의 VPN 구축 상태 보기을/를 참조하십시오.
구축의 대상인 모든 디바이스에 VPN 구축 적용	적용 아이콘( )을 클릭합니다. 자세한 내용은 10-14페이지의 VPN 구축 적용을/를 참조하십시오.
VPN 구축 삭제	삭제 아이콘( )을 클릭한 다음 **Yes**를 클릭하고, 구축을 삭제하지 않으려면 **No**를 클릭합니다.

VPN 구축 구성

라이센스: VPN

지원되는 디바이스: Series 3

새 VPN 구축을 생성할 때 최소한 고유한 이름을 부여하고 구축 유형을 지정하며 사전 공유 키를 지정해야 합니다. 각각 VPN 터널의 그룹을 포함하는 3가지 구축 유형 중에서 선택할 수 있습니다.

- PTP(Point-to-point) 구축에서는 두 엔드포인트 간에 VPN 터널을 설정합니다.
- 스타 구축에서는 VPN 터널 그룹을 설정하여 허브 엔드포인트를 리프 엔드포인트 그룹에 연결합니다.
- 메시 구축에서는 엔드포인트 집합에서 VPN 터널 그룹의 설정합니다.

Cisco가 관리하는 디바이스만 Cisco VPN 구축에서 엔드포인트로 사용될 수 있습니다. 서드파티 엔드포인트는 지원되지 않습니다.

VPN 인증을 위해 사전 공유 키를 정의해야 합니다. 구축에서 생성하는 모든 VPN 연결에 사용할 기본 키를 지정할 수 있습니다. PTP 구축의 경우 각 엔드포인트 쌍에 대해 사전 공유 키를 지정할 수 있습니다.

각 VPN 구축 유형의 생성에 대한 자세한 내용은 다음 절을 참조하십시오.

- 10-6페이지의 PTP VPN 구축 컨피그레이션
- 10-8페이지의 스타 VPN 구축 구성
- 10-10페이지의 메시 VPN 구축 구성

PTP VPN 구축 컨피그레이션

라이센스: VPN

지원되는 디바이스: Series 3

PTP VPN 구축을 구성할 때 엔드포인트 쌍의 그룹을 정의한 다음 각 쌍의 두 노드 간에 VPN을 생성합니다. 자세한 내용은 10-2페이지의 포인트-투-포인트 VPN 구축 이해을/를 참조하십시오.

다음 목록에서는 구축에서 지정할 수 있는 옵션에 대해 설명합니다.

Name

구축의 고유한 이름을 지정합니다.

Type

PTP를 클릭하여 포인트-투-포인트 구축을 구성하고 있음을 확인합니다.

Pre-shared Key

인증을 위해 고유한 사전 공유 키를 정의합니다. 각 엔드포인트 쌍에 대해 사전 공유 키를 지정하지 않는 한 구축의 모든 VPN에 이 키를 사용합니다.

Device

디바이스 스택 또는 클러스터를 포함하여 관리 대상 디바이스를 구축의 엔드포인트로 선택할 수 있습니다. Cisco가 관리하는 디바이스이지만 현재 사용 중인 방어 센터의 관리를 받지 않는 경우 **Other**를 선택하고 엔드포인트의 IP 주소를 지정합니다.

Virtual Router

관리 대상 디바이스를 엔드포인트로 선택한 경우 선택된 디바이스에 현재 적용된 가상 라우터를 선택합니다. 둘 이상의 엔드포인트에 대해 동일한 가상 라우터를 선택할 수 없습니다.

Interface

관리 대상 디바이스를 엔드포인트로 선택한 경우 선택된 가상 라우터에 지정된 라우티드 인터페이스를 선택합니다.

IP Address

- 관리 대상 디바이스를 엔드포인트로 선택한 경우 선택된 라우티드 인터페이스에 지정된 IP 주소를 선택합니다.
- 관리 대상 디바이스가 디바이스 클러스터일 경우 SFRP IP 주소의 목록에서만 선택할 수 있습니다.
- 관리 대상이지만 방어 센터의 관리를 받지 **않는** 디바이스를 선택한 경우 그 엔드포인트의 IP 주소를 지정합니다.

Protected Networks

구축에서 암호화된 네트워크를 지정합니다. 각 네트워크에 대해 CIDR 영역과 함께 서브넷을 입력합니다. IKE 버전 1은 단일 보안 네트워크만 지원합니다.

VPN 엔드포인트가 동일한 IP 주소를 가질 수 없으며 VPN 엔드포인트 쌍의 보안 네트워크는 중복될 수 없습니다. 어떤 엔드포인트의 보안 네트워크 목록에 IPv4 또는 IPv6 엔트리가 하나 이상 포함될 경우 나머지 엔드포인트의 보안 네트워크는 동일한 유형(즉 IPv4 또는 IPv6)의 엔트리를 하나 이상 가져야 합니다. 그렇지 않으면 나머지 엔드포인트의 IP 주소가 동일한 유형이고 또한 보안 네트워크의 엔트리와 중복되지 않아야 합니다. IPv4에는 /32 CIDR 주소 영역을, IPv6에는 /128 CIDR 주소 영역을 사용합니다. 두 검사 모두 실패할 경우 엔드포인트 쌍은 잘못된 것입니다.

Internal IP

엔드포인트가 네트워크 주소 변환 기능을 갖춘 방화벽의 뒤에 상주할 경우 확인란을 선택합니다.

Public IP

Internal IP를 선택한 경우 방화벽의 공용 IP 주소를 지정합니다. 엔드포인트가 responder일 경우 이 값을 지정해야 합니다.

Public IKE Port

Internal IP를 선택한 경우 1에서 65535까지의 단일 숫자를 내부 엔드포인트에 포트 전달되는 방화벽의 UDP 포트로 지정합니다. 엔드포인트가 responder이고 전달되는 방화벽의 포트가 500 또는 4500이 아닐 경우 이 값을 지정해야 합니다.

Use Deployment Key

구축에 대해 정의된 사전 공유 키를 사용하려면 확인란을 선택합니다. 이 엔드포인트 쌍의 VPN 인증을 위한 사전 공유 키를 지정하려면 확인란을 선택 취소합니다.

Pre-shared Key

Use Deployment Key 확인란을 선택 취소한 경우 이 필드에 사전 공유 키를 지정합니다.

팁 기존 PTP 구축을 수정하려면 구축 옆의 수정 아이콘( )을 클릭합니다. 초기에 구축을 저장한 후 구축 유형을 수정할 수 없습니다. 두 명의 사용자가 동일한 구축을 동시에 수정해서는 **안됩니다**. 하지만 웹 인터페이스에서는 동시 수정이 가능합니다.

PTP VPN 구축을 구성하려면

액세스: Admin/Network Admin

1단계 **Devices > VPN**을 선택합니다.

VPN 페이지가 나타납니다.

2단계 **Add**를 클릭합니다.

Create New VPN Deployment 팝업 창이 나타납니다.

3단계 구축의 고유한 **Name**을 지정합니다.

공백과 특수 문자를 포함하여 인쇄 가능한 모든 문자를 사용할 수 있습니다.

4단계 **PTP**가 **Type**으로 선택되어야 합니다.

5단계 구축에 고유한 **Pre-shared Key**를 지정합니다.

6단계 **Node Pairs** 옆의 추가 아이콘( )을 클릭합니다.

Add New Endpoint Pair 팝업 창이 나타납니다.

7단계 이 절에서 앞서 설명한 것처럼 VPN 구축을 구성합니다.

8단계 **Node A** 아래의 **Protected Networks** 옆에 있는 추가 아이콘( )을 클릭합니다.

Add Network 팝업 창이 나타납니다.

9단계 보안 네트워크에 대한 CIDR 영역을 입력합니다.

10단계 **OK**를 클릭합니다.

보안 네트워크가 추가되었습니다.

11단계 **노드 B**에 대해 8단계부터 10단계까지 반복합니다.

12단계 **Save**를 클릭합니다.

엔드포인트 쌍이 구축에 추가되었고 Create New VPN Deployment 팝업 창이 다시 나타납니다.

13단계 **Save**를 클릭하여 구축 컨피그레이션을 마치면 VPN 페이지가 다시 나타납니다.

구축을 적용해야 효력을 갖습니다. 10-14페이지의 VPN 구축 적용을/를 참조하십시오.

스타 VPN 구축 구성

라이센스: VPN

지원되는 디바이스: Series 3

스타 VPN 구축을 구성할 때 단일 허브 노드 엔드포인트와 리프 노드 엔드포인트 그룹을 정의합니다. 구축을 구성하려면 허드 노드 엔드포인트와 하나 이상의 리프 노드 엔드포인트를 정의해야 합니다. 자세한 내용은 10-3페이지의 스타 VPN 구축 이해을/를 참조하십시오.

다음 목록에서는 구축에서 지정할 수 있는 옵션에 대해 설명합니다.

Name

구축의 고유한 이름을 지정합니다.

Type

Star를 클릭하여 스타 구축을 구성하고 있음을 확인합니다.

Pre-shared Key

인증을 위해 고유한 사전 공유 키를 정의합니다.

Device

디바이스 스택 또는 클러스터를 포함하여 관리 대상 디바이스를 구축의 엔드포인트로 선택할 수 있습니다. Cisco가 관리하는 디바이스이지만 현재 사용 중인 방어 센터의 관리를 받지 않는 경우 **Other**를 선택하고 엔드포인트의 IP 주소를 지정합니다.

Virtual Router

관리 대상 디바이스를 엔드포인트로 선택한 경우 선택된 디바이스에 현재 적용된 가상 라우터를 선택합니다. 둘 이상의 엔드포인트에 대해 동일한 가상 라우터를 선택할 수 없습니다.

Interface

관리 대상 디바이스를 엔드포인트로 선택한 경우 선택된 가상 라우터에 지정된 라우티드 인터페이스를 선택합니다.

IP Address

- 관리 대상 디바이스를 엔드포인트로 선택한 경우 선택된 라우티드 인터페이스에 지정된 IP 주소를 선택합니다.
- 관리 대상 디바이스가 디바이스 클러스터일 경우 SFRP IP 주소의 목록에서만 선택할 수 있습니다.
- 관리 대상이지만 방어 센터의 관리를 받지 **않는** 디바이스를 선택한 경우 그 엔드포인트의 IP 주소를 지정합니다.

Protected Networks

구축에서 암호화된 네트워크를 지정합니다. 각 네트워크에 대해 CIDR 영역과 함께 서브넷을 입력합니다.

VPN 엔드포인트가 동일한 IP 주소를 가질 수 없으며 VPN 엔드포인트 쌍의 보안 네트워크는 중복될 수 없습니다. 어떤 엔드포인트의 보안 네트워크 목록에 IPv4 또는 IPv6 엔트리가 하나 이상 포함될 경우 나머지 엔드포인트의 보안 네트워크는 동일한 유형(즉 IPv4 또는 IPv6)의 엔트리를 하나 이상 가져야 합니다. 그렇지 않으면 나머지 엔드포인트의 IP 주소가 동일한 유형이어야 하고 또한 보안 네트워크의 엔트리와 중복되지 않아야 합니다. IPv4에는 /32 CIDR 주소 영역을, IPv6에는 /128 CIDR 주소 영역을 사용합니다. 두 검사 모두 실패할 경우 엔드포인트 쌍은 잘못된 것입니다.

Internal IP

엔드포인트가 네트워크 주소 변환 기능을 갖춘 방화벽 뒤에 상주할 경우 확인란을 선택합니다.

Public IP

Internal IP를 선택한 경우 방화벽의 공용 IP 주소를 지정합니다. 엔드포인트가 reponder일 경우 이 값을 지정해야 합니다.

Public IKE Port

Internal IP를 선택한 경우, 1에서 65535까지의 단일 숫자를 내부 엔드포인트로 포트 전달되는 방화벽의 UDP 포트로 지정합니다. 엔드포인트가 responder이고 전달되는 방화벽의 포트가 500 또는 4500이 아닐 경우 이 값을 지정해야 합니다.

팁 기존 스타 구축을 수정하려면 구축 옆의 수정 아이콘( )을 클릭합니다. 초기에 구축을 저장한 후 구축 유형을 수정할 수 없습니다. 구축 유형을 변경하려면 구축을 삭제하고 새로 생성해야 합니다. 두 명의 사용자가 동일한 구축을 동시에 수정해서는 **안됩니다**. 하지만 웹 인터페이스에서는 동시 수정이 가능합니다.

스타 구축을 구성하려면

액세스: Admin/Network Admin

1단계 **Devices > VPN**을 선택합니다.

VPN 페이지가 나타납니다.

2단계 **Add**를 클릭합니다.

Create New VPN Deployment 팝업 창이 나타납니다.

3단계 구축의 고유한 **Name**을 지정합니다.

공백과 특수 문자를 포함하여 인쇄 가능한 모든 문자를 사용할 수 있습니다.

4단계 **Star**를 클릭하여 **Type**을 지정합니다.

5단계 구축에 고유한 **Pre-shared Key**를 지정합니다.

6단계 **Hub Node** 옆의 추가 아이콘( )을 클릭합니다.

Add Hub Node 팝업 창이 나타납니다.

7단계 이 절에서 앞서 설명한 것처럼 VPN 구축을 구성합니다.

8단계 **Protected Networks** 옆의 추가 아이콘( )을 클릭합니다.

Add Network 팝업 창이 나타납니다.

9단계 보안 네트워크의 IP 주소를 입력합니다.

10단계 **OK**를 클릭합니다.

보안 네트워크가 추가되었습니다.

11단계 **Save**를 클릭합니다.

허브 노드가 구축에 추가되었고 Create New VPN Deployment 팝업 창이 다시 나타납니다.

12단계 **Leaf Nodes** 옆의 추가 아이콘( )을 클릭합니다.

Add Leaf Node 팝업 창이 나타납니다.

13단계 7단계부터 10단계까지 반복하여 리프 노드를 완성합니다. 이는 허브 노드와 동일한 옵션을 제공합니다.

14단계 **Save**를 클릭합니다.

리프 노드가 구축에 추가되고 Create New VPN Deployment 팝업 창이 다시 나타납니다.

15단계 **Save**를 클릭하여 구축 컨피그레이션을 마치면 VPN 페이지가 다시 나타납니다.

구축을 적용해야 효력을 갖습니다. 10-14페이지의 VPN 구축 적용을/를 참조하십시오.

메시 VPN 구축 구성

라이센스: VPN

지원되는 디바이스: Series 3

메시 VPN 구축을 구성할 때 지정된 엔드포인트 집합에 대해 임의의 두 지점을 연결하도록 VPN 그룹을 정의합니다. 자세한 내용은 10-4페이지의 메시 VPN 구축 이해을/를 참조하십시오.

다음 목록에서는 구축에서 지정할 수 있는 옵션에 대해 설명합니다.

Name

구축의 고유한 이름을 지정합니다.

Type

Mesh를 클릭하여 메시 구축 구성을 지정합니다.

Pre-shared Key

인증을 위해 고유한 사전 공유 키를 정의합니다.

Device

디바이스 스택 또는 클러스터를 포함하여 관리 대상 디바이스를 구축의 엔드포인트로 선택할 수 있습니다. Cisco가 관리하는 디바이스이지만 현재 사용 중인 방어 센터의 관리를 받지 않는 경우 **Other**를 선택하고 엔드포인트의 IP 주소를 지정합니다.

Virtual Router

관리 대상 디바이스를 엔드포인트로 선택한 경우 선택된 디바이스에 현재 적용된 가상 라우터를 선택합니다. 둘 이상의 엔드포인트에 대해 동일한 가상 라우터를 선택할 수 없습니다.

Interface

관리 대상 디바이스를 엔드포인트로 선택한 경우 선택된 가상 라우터에 지정된 라우티드 인터페이스를 선택합니다.

IP Address

- 관리 대상 디바이스를 엔드포인트로 선택한 경우 선택된 라우티드 인터페이스에 지정된 IP 주소를 선택합니다.
- 관리 대상 디바이스가 디바이스 클러스터일 경우 SFRP IP 주소의 목록에서만 선택할 수 있습니다.
- 관리 대상이지만 방어 센터의 관리를 받지 **않는** 디바이스를 선택한 경우, 해당 엔드포인트의 IP 주소를 지정합니다.

Protected Networks

구축에서 암호화된 네트워크를 지정합니다. 각 네트워크에 대해 CIDR 영역과 함께 서브넷을 입력합니다. IKE 버전 1은 단일 보안 네트워크만 지원합니다.

VPN 엔드포인트가 동일한 IP 주소를 가질 수 없으며 VPN 엔드포인트 쌍의 보안 네트워크는 중복될 수 없습니다. 어떤 엔드포인트의 보안 네트워크 목록에 IPv4 또는 IPv6 엔트리가 하나 이상 포함될 경우 나머지 엔드포인트의 보안 네트워크는 동일한 유형(즉 IPv4 또는 IPv6)의 엔트리를 하나 이상 가져야 합니다. 그렇지 않으면 나머지 엔드포인트의 IP 주소가 동일한 유형이고 또한 보안 네트워크의 엔트리와 중복되지 않아야 합니다. IPv4에는 /32 CIDR 주소 영역을, IPv6에는 /128 CIDR 주소 영역을 사용합니다. 두 검사 모두 실패할 경우 엔드포인트 쌍은 잘못된 것입니다.

Internal IP

엔드포인트가 네트워크 주소 변환 기능을 갖춘 방화벽의 뒤에 상주할 경우 확인란을 선택합니다.

Public IP

Internal IP를 선택한 경우 방화벽의 공용 IP 주소를 지정합니다. 엔드포인트가 responder일 경우 이 값을 지정해야 합니다.

Public IKE Port

Internal IP를 선택한 경우 1에서 65535까지의 단일 숫자를 내부 엔드포인트에 포트 전달되는 방화벽의 UDP 포트로 지정합니다. 엔드포인트가 responder이고 전달되는 방화벽의 포트가 500 또는 4500이 아닐 경우 이 값을 지정해야 합니다.

팁 기존 메시 구축을 수정하려면 구축 옆의 수정 아이콘( )을 클릭합니다. 초기에 구축을 저장한 후 구축 유형을 수정할 수 없습니다. 구축 유형을 변경하려면 구축을 삭제하고 새로 생성해야 합니다. 두 명의 사용자가 동일한 구축을 동시에 수정해서는 **안됩니다**. 하지만 웹 인터페이스에서는 동시 수정이 가능합니다.

메시 VPN 구축을 구성하려면

액세스: Admin/Network Admin

1단계 **Devices > VPN**을 선택합니다.

VPN 페이지가 나타납니다.

2단계 **Add**를 클릭합니다.

Create New VPN Deployment 팝업 창이 나타납니다.

3단계 구축의 고유한 **Name**을 지정합니다.

공백과 특수 문자를 포함하여 인쇄 가능한 모든 문자를 사용할 수 있습니다.

4단계 **Mesh**를 클릭하여 **Type**을 지정합니다.

5단계 구축에 고유한 **Pre-shared Key**를 지정합니다.

6단계 **Nodes** 옆의 추가 아이콘( )을 클릭합니다.

Add Endpoint 팝업 창이 나타납니다.

7단계 이 절에서 앞서 설명한 것처럼 VPN 구축을 구성합니다.

8단계 **Protected Networks** 옆의 추가 아이콘( )을 클릭합니다.

Add Network 팝업 창이 나타납니다.

9단계 보안 네트워크에 대한 CIDR 영역을 입력합니다.

10단계 **OK**를 클릭합니다.

보안 네트워크가 추가되었습니다.

11단계 **Save**를 클릭합니다.

엔드포인트가 구축에 추가되었고 Create New VPN Deployment 팝업 창이 다시 나타납니다.

12단계 6단계부터 11단계까지 반복하여 엔드포인트를 추가합니다.

13단계 **Save**를 클릭하여 구축을 완성하면 VPN 페이지가 다시 나타납니다.

구축을 적용해야 효력을 갖습니다. 10-14페이지의 VPN 구축 적용을/를 참조하십시오.

고급 VPN 구축 설정 구성

라이센스: VPN

지원되는 디바이스: Series 3

VPN 구축은 여러 공통 설정을 포함하며, 이는 구축 내의 VPN끼리 공유할 수 있습니다. 각 VPN에서 기본 설정을 사용할 수 있으며, 기본 설정을 재정의할 수도 있습니다. 고급 설정은 일반적으로 거의 또는 전혀 수정할 필요가 없으며 모든 구축에 공통적으로 적용하지는 않습니다.

다음 목록에서는 구축에서 지정할 수 있는 고급 옵션에 대해 설명합니다.

Other Algorithm Allowed

Algorithm 목록에는 없지만 가 제안한 알고리즘에 대한 자동 협상을 활성화하려면 이 확인란을 선택합니다.

Algorithm

구축의 데이터를 보호하기 위해 1단계 및 2단계 알고리즘 제안을 지정합니다. 두 단계 모두에 대해 **Cipher**, **Hash**, **DH**(Diffie-Hellman) 그룹 인증 메시지를 선택합니다.

IKE Life Time

최대 IKE SA 재협상 간격에 대해 숫자 값을 지정하고 시간 단위를 선택합니다. 최소 15분, 최대 30일로 지정할 수 있습니다.

IKE v2

시스템에서 IKE 버전 2를 사용하도록 지정하려면 이 확인란을 선택합니다. 이 버전은 스타 구축 및 여러 보안 네트워크를 지원합니다.

Life Time

최대 SA 재협상 간격에 대해 숫자 값을 지정하고 시간 단위를 선택합니다. 최소 5분, 최대 2시간으로 지정할 수 있습니다.

Life Packets

만료되기 전에 IPsec SA를 통해 전송될 수 있는 패킷 수를 지정합니다. 0에서 18446744073709551615까지의 어떤 정수도 사용할 수 있습니다.

Life Bytes

만료되기 전에 IPsec SA를 통해 전송될 수 있는 바이트 수를 지정합니다. 0에서 18446744073709551615까지의 어떤 정수도 사용할 수 있습니다.

AH

데이터를 보호하는 데 AH(authentication header) 보안 프로토콜을 사용하도록 지정하려면 이 확인란을 선택합니다. ESP(encryption service payload) 프로토콜을 사용하려면 이 확인란을 선택 취소합니다. 각 프로토콜을 언제 사용할 것인가에 대한 지침은 10-1페이지의 IPSec 이해를 참조하십시오.

고급 VPN 구축 설정을 구성하려면

액세스: Admin/Network Admin

1단계 **Devices > VPN**을 선택합니다.

VPN 페이지가 나타납니다.

2단계 **Add**를 클릭합니다.

Create New VPN Deployment 팝업 창이 나타납니다.

3단계 **Advanced** 탭을 클릭합니다.

4단계 이 절에서 앞서 설명한 것처럼 고급 설정을 구성합니다.

5단계 **Algorithms** 옆의 추가 아이콘( )을 클릭합니다.

Add IKE Algorithm Proposal 팝업 창이 나타납니다.

6단계 두 단계 모두에 대해 **Cipher**, **Hash**, **DH**(Diffie-Hellman) 그룹 인증 메시지를 선택합니다.

7단계 **OK**를 클릭합니다.

IKE 알고리즘 제안이 추가됩니다.

8단계 **Save**를 클릭합니다.

변경사항이 저장되었고 VPN 페이지가 나타납니다.

구축을 적용해야 효력을 갖습니다. 10-14페이지의 VPN 구축 적용을/를 참조하십시오.

VPN 구축 적용

라이센스: VPN

지원되는 디바이스: Series 3

VPN 구축을 구성하거나 변경한 다음 하나 이상의 디바이스에 구축을 적용해야 이 구축에 대해 지정한 설정이 구현됩니다.

VPN 구축을 적용하려면

액세스: Admin/Network Admin

1단계 **Devices > VPN**을 선택합니다.

VPN 페이지가 나타납니다.

2단계 적용할 VPN 구축 옆의 적용 아이콘()을 클릭합니다.

3단계 프롬프트가 나타나면 **Yes**를 클릭합니다.

VPN 구축이 적용되었습니다.

팁 Apply VPN deployment 대화 상자에서 **View Changes**를 클릭할 수도 있습니다. VPN Comparison View 페이지가 새 브라우저 창에 나타납니다. 자세한 내용은 10-17페이지의 VPN 구축 비교 보기 사용을/를 참조하십시오.

4단계 **OK**를 클릭합니다.

VPN 페이지로 돌아갑니다.

VPN 구축 상태 보기

라이센스: VPN

지원되는 디바이스: Series 3

VPN 구축을 구성한 다음 구성된 VPN 터널의 상태를 볼 수 있습니다. VPN 페이지는 적용된 각 VPN 구축의 상태 아이콘을 표시합니다.

- () 아이콘은 모든 VPN 엔드포인트가 실행 상태임을 나타냅니다.
- () 아이콘은 모든 VPN 엔드포인트가 다운 상태임을 나타냅니다.
- () 아이콘은 일부 엔드포인트가 실행 상태, 다른 엔드포인트는 다운 상태임을 나타냅니다.

상태 아이콘을 클릭하여 구축 상태 및 구축의 엔드포인트에 대한 기본 정보(예: 엔드포인트 이름, IP 주소)를 볼 수 있습니다. VPN 상태는 1분마다 또는 상태가 변경될 때(예: 엔드포인트가 다운되거나 시작할 때) 업데이트됩니다.

VPN 상태를 보려면

액세스: Admin/Network Admin

1단계 **Devices > VPN**을 선택합니다.

VPN 페이지가 나타납니다.

2단계 상태를 보려는 구축 옆의 VPN 상태 아이콘을 클릭합니다.

VPN Status 팝업 창이 나타납니다.

3단계 **OK**를 클릭하여 VPN 페이지로 돌아갑니다.

VPN 통계 및 로그 보기

라이센스: VPN

지원되는 디바이스: Series 3

VPN 구축을 구성한 다음 구성된 VPN 터널을 지나는 데이터에 대한 통계를 볼 수 있습니다. 또한 각 엔드포인트의 최신 VPN 시스템과 IKE 로그를 볼 수 있습니다.

다음 통계가 표시됩니다.

Endpoint

VPN 엔드포인트로 지정된 라우티드 인터페이스의 디바이스 경로 및 IP 주소

Status

VPN 연결이 실행 또는 다운 상태인지 여부

Protocol

암호화에 사용되는 프로토콜(ESP 또는 AH)

Packets Received

IPsec SA 협상 과정에서 VPN 터널이 수신하는 인터페이스당 패킷 수

Packets Forwarded

IPsec SA 협상 과정에서 VPN 터널이 전송하는 인터페이스당 패킷 수

Bytes Received

IPsec SA 협상 과정에서 VPN 터널이 수신하는 인터페이스당 바이트 수

Bytes Forwarded

IPsec SA 협상 과정에서 VPN 터널이 전송하는 인터페이스당 바이트 수

Time Created

VPN 연결이 생성된 날짜와 시간

Time Last Used

사용자가 마지막으로 VPN 연결을 시작한 시간

NAT Traversal

Yes가 표시될 경우 VPN 엔드포인트 중 하나 이상이 NAT 기능을 갖춘 디바이스 뒤에 상주합니다.

IKE State

IKE SA의 상태로서 connecting, established, deleting 또는 destroying입니다.

IKE Event

IKE SA 이벤트로서 reauthentication 또는 rekeying입니다.

IKE Event Time

다음 이벤트의 발생 시간(초)

IKE Algorithm

VPN 구축에서 사용하는 IKE 알고리즘

IPSec State

IPSec SA의 상태로서 installing, installed, updating, rekeying, deleting, destroying입니다.

IPSec Event

IPSec SA 이벤트에서 키를 재생성하는 시점에 대한 알림입니다.

IPSec Event Time

다음 이벤트가 일어날 때까지의 시간(초)

IPSec Algorithm

VPN 구축에서 사용하는 IPSec 알고리즘

VPN 통계를 보려면

액세스: Admin/Network Admin

1단계 **Devices > VPN**을 선택합니다.

VPN 페이지가 나타납니다.

2단계 VPN 통계를 보려는 구축 옆의 VPN 상태 아이콘을 클릭합니다.

VPN Status 팝업 창이 나타납니다.

3단계 통계 보기 아이콘()을 클릭합니다.

VPN Statistics 팝업 창이 나타납니다.

4단계 **Refresh**를 클릭하여 VPN 통계를 업데이트할 수도 있습니다.

5단계 **View Recent Log**를 클릭하여 엔드포인트별로 최신 데이터 로그를 볼 수도 있습니다.

클러스터링된 디바이스 및 스태킹된 디바이스의 로그를 보기 위해 액티브/기본 또는 백업/보조 디바이스 중 하나의 링크를 선택할 수 있습니다.

VPN 구축 비교 보기 사용

라이센스: VPN

지원되는 디바이스: Series 3

VPN 구축 비교 보기에서는 구축의 변경사항을 실제로 적용하기 전에 볼 수 있습니다. 이 보고서는 현재 구축과 제안된 구축의 모든 차이점을 표시합니다. 따라서 잠재적 컨피그레이션 오류가 있으면 찾아낼 수 있습니다.

비교 보기에서는 두 구축을 나란히 표시하며, 각 구축은 비교 보기의 좌우 제목 표시줄에 있는 이름으로 식별됩니다. 마지막 수정 시간 및 마지막 수정자가 구축 이름과 함께 표시됩니다.

두 구축의 차이점이 강조 표시됩니다.

- 파란색은 강조 표시된 설정이 두 구축에서 다름을 의미하며, 그 차이점이 빨간색 텍스트로 표시됩니다.
- 녹색은 강조 표시된 설정이 둘 중 한 구축에만 나타남을 의미합니다.

다음 표의 어떤 작업도 수행할 수 있습니다.

표 10-2 VPN 구축 비교 보기의 작업

목적	가능한 작업
개별 변경 사항 탐색	제목 표시줄 위의 **Previous** 또는 **Next**를 클릭합니다. 왼쪽과 오른쪽 사이의 중앙에 있는 이중 화살표 아이콘( )이 움직이고 **Difference** 번호가 조정되면서 어떤 차이점을 보고 있는지 나타냅니다.
구축 비교 보고서 생성	**Comparison Report**를 클릭합니다. 구축 비교 보고서에서는 두 정책의 차이점만 나열하는 PDF 문서를 생성합니다.

11 장

NAT 정책 사용

NAT(network address translation) 정책은 시스템이 NAT로 라우팅을 구현하는 방법을 결정합니다. 하나 이상의 NAT 정책을 구성할 수 있으며, 구성한 정책을 하나 이상의 관리되는 디바이스에 적용할 수 있습니다. 각 디바이스에는 현재 적용된 정책이 하나씩 포함될 수 있습니다.

시스템이 NAT를 처리하는 방법을 제어하려면 NAT 규칙을 정책에 추가합니다. 각 규칙에는 변환할 특정 트래픽을 식별하는 조건 집합이 포함됩니다. 다음과 같은 유형의 규칙을 생성할 수 있습니다.

- Static — 목적지 네트워크에 대한 일대일 변환 및 선택적으로 포트와 프로토콜을 제공합니다.
- Dynamic IP — 다대다 소스 네트워크를 변환하지만 포트와 프로토콜을 유지 관리합니다.
- Dynamic IP + Port — 다대일 또는 다대다 소스 네트워크 및 포트와 프로토콜을 변환합니다.

시스템은 동적 변환이 검사되기 전에 트래픽을 고정 변환에 매칭합니다. 그런 다음 시스템은 트래픽을 동적 NAT 규칙에 순서대로 매칭합니다. 처음 매칭된 규칙이 트래픽을 처리합니다. 자세한 내용은 11-5페이지의 NAT 정책에서 규칙 구성을/를 참조하십시오.

구축에 액세스 제어 정책이 있을 경우 액세스 제어를 통과해야 트래픽을 변환할 수 있습니다.

어플라이언스에서 NAT 정책을 적용하고 적용하려면 타겟 관리 대상 디바이스 각각에서 제어 라이센스가 활성화되어야 합니다. 추가로, 구성된 가상 라우터 또는 하이브리드 인터페이스와 함께 NAT 정책을 Series 3 디바이스에만 적용할 수 있습니다.

NAT 정책을 구성 및 구축한 후, 구축 관련 문제를 해결하려면 관리되는 디바이스 대상에 CLI(명령줄 인터페이스)를 사용할 수 있습니다. CLI는 세 가지 유형의 NAT 정보, 즉 컨피그레이션, 규칙 정의 및 활성 변환을 표시합니다. 자세한 내용은 D-1페이지의 명령줄 참조을/를 참조하십시오.

NAT 정책의 생성 및 관리에 대한 자세한 내용은 다음 절을 참조하십시오.

NAT 정책 계획 및 구현

라이센스: 모두

특정 네트워크 요구를 관리하려면 NAT 정책을 서로 다른 방법으로 구성할 수 있습니다. 이 절에서는 NAT 정책을 구축할 수 있는 몇 가지 방법에 대한 정보를 제공합니다.

주의 NAT 변환의 영향을 받는 모든 네트워크가 사설 네트워크인 경우 클러스터링된 컨피그레이션에서는 클러스터링된 디바이스에서 고정 NAT 규칙에 대한 개별 피어 인터페이스만 선택하십시오. 공용 네트워크와 사설 네트워크 간 트래픽에 영향을 미치는 고정 NAT 규칙에는 이 컨피그레이션을 사용하지 **마십시오**.

내부 서버를 외부 네트워크에 노출하도록 NAT를 구성할 수 있습니다. 이 컨피그레이션에서는 시스템이 네트워크 외부에서 내부 서버에 액세스할 수 있도록, 외부 IP 주소에서 내부 IP 주소로의 고정 변환을 정의합니다. 서버로 전송된 트래픽은 외부 IP 주소 또는 IP 주소와 포트를 대상으로 하며, 내부 IP 주소 또는 IP 주소와 포트로 변환됩니다. 서버에서 오는 반환 트래픽이 다시 외부 주소로 변환됩니다.

내부 호스트 또는 서버가 외부 애플리케이션에 연결되도록 NAT를 구성할 수 있습니다. 이 컨피그레이션에서는 내부 주소에서 외부 주소로의 고정 변환을 정의합니다. 이렇게 정의하면 내부 호스트나 서버는 내부 호스트나 서버에서 특정 IP 주소와 포트를 기대하는 외부 애플리케이션과의 연결을 시작할 수 있습니다. 따라서 시스템은 내부 호스트나 서버의 주소를 동적으로 할당할 수 없습니다.

IP 주소 불록을 사용하여 외부 네트워크로부터 사설 네트워크 주소를 숨기도록 NAT를 구성할 수 있습니다. 이 방식은 내부 네트워크 주소를 가리고 내부 네트워크 요구를 충족할만한 외부 IP 주소가 충분한 경우 유용합니다. 이 컨피그레이션에서는 발신 트래픽의 소스 IP 주소를 외부에서 대면하는 IP 주소에서 오는 미사용 IP 주소로 자동으로 변환하는 동적 변환을 생성합니다.

IP 주소의 제한된 불록과 포트 변환을 사용하여 외부 네트워크로부터 사설 네트워크 주소를 숨기도록 NAT를 구성할 수 있습니다. 이 방식은 내부 네트워크 주소를 가리되, 내부 네트워크 요구를 충족할만한 외부 IP 주소 수가 부족한 경우 유용합니다. 이 컨피그레이션에서는 발신 트래픽의 소스 IP 주소와 포트를 외부에서 대면하는 IP 주소에서 오는 미사용 IP 주소와 포트로 자동으로 변환하는 동적 변환을 생성합니다.

NAT 정책 구성

라이센스: 제어

지원되는 디바이스: Series 3

NAT 정책을 구성하려면 정책에 고유한 이름을 지정하고, 정책을 적용하려는 디바이스(또는 *대상*)를 식별해야 합니다. NAT 규칙을 추가, 수정, 삭제, 활성화 또는 비활성화할 수 있습니다. NAT 정책을 생성하거나 수정한 후 전체 또는 일부 대상 디바이스에 정책을 적용할 수 있습니다.

독립형 디바이스에서 하듯 NAT 정책을 디바이스 클러스터(클러스터링된 스택 포함)에 적용할 수 있습니다. 그러나 개별 클러스터링된 디바이스 또는 전체 클러스터의 인터페이스에 대해 고정 NAT 규칙을 정의하고 소스 영역에서 인터페이스를 사용할 수 있습니다. 동적 규칙의 경우 소스 또는 목적지 영역에 있는 전체 클러스터의 인터페이스만 사용할 수 있습니다.

주의 NAT 변환의 영향을 받는 모든 네트워크가 사설 네트워크인 경우 클러스터링된 컨피그레이션에서는 클러스터링된 디바이스에서 고정 NAT 규칙에 대한 개별 피어 인터페이스만 선택하십시오. 공용 네트워크와 사설 네트워크 간 트래픽에 영향을 미치는 고정 NAT 규칙에는 이 컨피그레이션을 사용하지 **마십시오**.

설정된 HA 링크 인터페이스 없이 디바이스 클러스터에서 동적 NAT를 구성하는 경우, 클러스터링된 두 디바이스는 동적 NAT 항목을 독립적으로 할당하며 시스템은 디바이스 간에 항목을 동기화할 수 없습니다. 자세한 내용은 4-63페이지의 HA 링크 인터페이스 구성을/를 참조하십시오.

독립형 디바이스에서 하듯 NAT 정책을 디바이스 스택에 적용할 수 있습니다. NAT 정책에 포함되었으며 스택의 멤버인 보조 디바이스의 인터페이스와 관련된 규칙이 있던 디바이스에서 디바이스 스택을 설정하는 경우, 보조 디바이스의 인터페이스는 NAT 정책에 그대로 유지됩니다. 이러한 인터페이스가 포함된 정책을 저장 및 적용할 수 있지만, 규칙이 변환을 제공하지는 않습니다. 자세한 내용은 4-43페이지의 스태킹된 디바이스 관리을/를 참조하십시오.

다음 표는 NAT 정책 Edit 페이지에서 수행할 수 있는 컨피그레이션 작업을 요약한 것입니다.

표 11-1 NAT 정책 컨피그레이션 작업

목적	가능한 작업
정책 이름 또는 설명 수정	**Name** 또는 **Description** 필드를 클릭하고 필요에 따라 임의의 문자를 삭제한 다음 새 이름 또는 설명을 입력합니다.
정책 대상 관리	11-4페이지의 NAT 정책 대상 관리에서 자세히 알아보십시오.
정책 변경 사항 저장	**Save**를 클릭합니다.
정책 저장 및 적용	**Save and Apply**를 클릭합니다. 자세한 내용은 11-14페이지의 NAT 정책 적용을/를 참조하십시오.
정책 변경 사항 취소	**Cancel**을 클릭한 다음 이미 변경한 경우에는 **OK**를 클릭합니다.
정책에 규칙 추가	**Add Rule**을 클릭합니다. 자세한 내용은 11-16페이지의 NAT 규칙 생성 및 수정을/를 참조하십시오. **팁** 기존 규칙을 마우스 오른쪽 버튼으로 클릭하고 **Insert new rule**을 선택할 수도 있습니다.
기존 규칙 수정	규칙 옆의 수정 아이콘( )을 클릭합니다. 자세한 내용은 11-16페이지의 NAT 규칙 생성 및 수정을/를 참조하십시오. **팁** 규칙을 마우스 오른쪽 버튼으로 클릭하고 **Edit**를 선택할 수도 있습니다.
규칙 삭제	규칙 옆의 삭제 아이콘( )을 클릭한 다음 **OK**를 클릭합니다. **팁** 하나 이상의 선택한 규칙을 삭제하려면 선택한 규칙의 행에서 빈 영역을 마우스 오른쪽 버튼으로 클릭하고 **Delete**를 선택한 다음 **OK**를 클릭할 수 있습니다.
기존 규칙 활성화 또는 비활성화	선택한 규칙을 마우스 오른쪽 버튼으로 클릭하고 **State**를 선택한 다음 **Disable** 또는 **Enable**을 선택합니다. 비활성화된 규칙은 회색으로 처리되며, 규칙 이름 아래에 `(disabled)`가 표시됩니다.
특정 규칙 속성에 대한 컨피그레이션 페이지 표시	규칙의 행, 조건의 열에서 이름, 값 또는 아이콘을 클릭합니다. 예를 들면 **Source Networks** 열의 이름이나 값을 클릭하여 선택한 규칙의 Source Network 페이지를 표시합니다. 자세한 내용은 11-24페이지의 NAT 규칙에서 서로 다른 조건 유형 작업을/를 참조하십시오.

NAT 정책 대상 관리

라이센스: 제어

지원되는 디바이스: Series 3

NAT 정책을 적용할 수 있으려면 먼저 정책을 적용하고자 하는 관리되는 디바이스(디바이스 스택, 클러스터, 그룹 등)를 식별해야 합니다. 정책을 생성하거나 수정하는 동안 정책의 대상이 될 관리되는 디바이스를 식별할 수 있습니다. 사용 가능한 디바이스, 스택 및 클러스터의 목록을 검색하고, 이들을 선택한 디바이스 목록에 추가할 수 있습니다. 또한 선택한 디바이스를 끌어서 놓거나, 두 목록 사이의 버튼을 사용하여 디바이스를 추가할 수 있습니다.

FireSIGHT 시스템의 서로 다른 버전을 실행하는(예: 디바이스 중 하나에 대한 업그레이드가 실패한 경우) 스태킹된 디바이스는 대상으로 설정할 수 없습니다. 자세한 내용은 4-43페이지의 스태킹된 디바이스 관리을/를 참조하십시오.

다음 표에는 대상 디바이스를 관리할 경우 수행할 수 있는 작업이 요약되어 있습니다.

표 11-2 대상 디바이스 관리 작업

목적	가능한 작업
사용 가능한 디바이스, 스택 및 클러스터의 목록 검색	Search 필드의 내부를 클릭한 다음 검색 문자열을 입력합니다. 입력하면 디바이스 목록이 업데이트되어 매칭되는 디바이스 이름이 표시됩니다.
사용 가능한 디바이스에 대한 검색 지우기	검색 필드에서 지우기 아이콘( )을 클릭합니다.
선택한 대상의 목록에 추가할 사용 가능한 디바이스, 스택 또는 클러스터 선택	디바이스 이름을 클릭합니다. 여러 디바이스를 선택하려면 Ctrl 및 Shift 키를 사용합니다. **팁** 사용 가능한 디바이스를 마우스 오른쪽 버튼으로 클릭하고 **Select All**을 클릭합니다.
선택한 디바이스, 스택 또는 클러스터 추가	**Add to Policy**를 클릭합니다. **팁** 선택한 디바이스의 목록으로 끌어서 놓을 수도 있습니다.
Selected Devices 목록에서 단일 디바이스, 스택 또는 클러스터 삭제	디바이스 옆에 있는 삭제 아이콘( )을 클릭합니다. **팁** 디바이스를 마우스 오른쪽 버튼으로 클릭하고 **Delete**를 선택할 수도 있습니다.
Selected Devices 목록에서 여러 디바이스 삭제	Ctrl 및 Shift 키를 사용하여 여러 디바이스를 선택하고, 마우스 오른쪽 버튼을 클릭하여 선택한 디바이스의 행을 강조 표시한 다음, **Delete Selected**를 클릭합니다.
컨피그레이션 저장	**Save**를 클릭합니다.
변경 사항을 저장하지 않은 채 컨피그레이션 취소	**Cancel**을 클릭합니다.

다음 절차에서는 대상 디바이스를 관리하기 위해 NAT 정책을 구성하는 방법에 대해 설명합니다. NAT 정책을 수정하는 전체 절차는 11-9페이지의 NAT 정책 수정을/를 참조하십시오.

NAT 정책에서 대상 디바이스를 관리하려면

액세스: Admin/Network Admin

1단계 **Devices > NAT**를 선택합니다.

NAT 페이지가 나타납니다.

2단계 구성하려는 NAT 정책 옆의 수정 아이콘( )을 클릭합니다.

NAT Policy Editor 페이지가 나타납니다.

3단계 **Targets** 탭을 클릭합니다.

Targets 페이지가 나타납니다.

4단계 선택적으로, Available Devices 목록 위의 **Search** 프롬프트를 클릭하고 이름을 입력합니다.

입력할 때 목록이 업데이트되면서 일치하는 디바이스를 표시합니다. 목록을 삭제하려면 지우기 아이콘( )을 클릭할 수 있습니다.

5단계 추가할 디바이스, 스택, 클러스터 또는 디바이스 그룹을 클릭합니다. 여러 디바이스를 선택하려면 Ctrl 및 Shift를 사용합니다.

팁 사용 가능한 디바이스를 마우스 오른쪽 버튼으로 클릭하고 **Select All**을 클릭합니다.

6단계 **Add to Policy**를 클릭합니다.

선택한 디바이스가 추가됩니다.

팁 디바이스를 추가하려면 끌어서 놓을 수도 있습니다.

7단계 선택적으로, 선택한 디바이스 목록에서 디바이스를 삭제하려면 삭제 아이콘( )을 클릭합니다. 또는 Ctrl 및 Shift 키를 사용하여 여러 디바이스를 선택하고 마우스 오른쪽 버튼을 클릭한 다음 **Delete Selected**를 선택합니다.

8단계 컨피그레이션을 저장하려면 **Save**를 클릭하고, 취소하려면 **Cancel**을 클릭합니다.

NAT 정책에서 규칙 구성

라이센스: 모두

NAT 정책의 Edit 페이지에는 고정 NAT 규칙 및 동적 NAT 규칙이 별도로 나열됩니다. 시스템은 고정 규칙을 알파벳 이름순으로 정렬하며, 사용자는 표시 순서를 변경할 수 없습니다. 동일한 매칭 값으로 고정 규칙을 생성할 수 없습니다. 시스템은 동적 변환을 검사하기 전에 고정 변환에서 일치를 검사합니다.

동적 규칙은 숫자 순서로 처리됩니다. 각 동적 규칙의 숫자 위치가 규칙 옆에 있는 페이지의 왼쪽에 나타납니다. 동적 규칙을 이동 또는 삽입하거나 규칙 순서를 변경할 수 있습니다. 예를 들어 동적 규칙 10을 동적 규칙 3 아래로 이동하면, 규칙 10은 규칙 4가 되고 이후의 모든 숫자는 그에 따라 증가합니다.

시스템은 정책 Edit 페이지에 있는 규칙의 숫자 순서대로 패킷을 동적 규칙과 비교하므로 동적 규칙의 위치는 중요합니다. 패킷이 동적 규칙의 모든 조건을 충족하면 시스템은 해당 규칙의 조건을 패킷에 적용하고, 해당 패킷에 대한 모든 후속 규칙을 무시합니다.

선택적으로, 동적 규칙을 추가 또는 수정할 때 동적 규칙의 숫자 위치를 지정할 수 있습니다. 또한 새 동적 규칙을 추가하기 전에 동적 규칙을 강조 표시하고, 강조 표시한 규칙 아래에 새 규칙을 삽입할 수 있습니다. 11-16페이지의 NAT 규칙 생성 및 수정을/를 참조하십시오.

규칙의 열에서 빈 공간을 클릭하여 하나 이상의 동적 규칙을 선택할 수 있습니다. 선택한 동적 규칙을 새 위치로 끌어서 놓을 수 있는데, 이 경우 이동한 규칙 및 모든 후속 규칙의 위치가 변경됩니다.

선택한 규칙을 잘라내거나 복사하여 기존 규칙의 위나 아래에 붙여넣을 수 있습니다. Static Translations 목록에는 고정 규칙만, Dynamic Translations 목록에는 동적 규칙만 붙여넣을 수 있습니다. 또한 선택한 규칙을 삭제하고 기존 규칙 목록의 새 위치에 새 규칙을 삽입할 수 있습니다.

참고 고정 규칙은 복사할 수 있지만 잘라낼 수는 없습니다.

선행 규칙에 의해 선점되기 때문에 매칭되지 않을 규칙을 식별하기 위한 설명 경고를 표시할 수 있습니다.

구축에 액세스 제어 정책이 있을 경우 액세스 제어를 통과해야 트래픽을 변환할 수 있습니다.

다음 표에는 규칙을 조직화하기 위해 수행할 수 있는 작업이 요약되어 있습니다.

표 11-3 NAT 규칙 조직화 작업

목적	가능한 작업
규칙 선택	규칙의 행에서 빈 영역을 클릭합니다. 여러 규칙을 선택하려면 Ctrl 또는 Shift 키를 사용합니다. 선택한 규칙이 강조 표시됩니다.
규칙 선택 지우기	페이지 오른쪽 하단에 있는 다시 로드 아이콘( )을 클릭합니다. 개별 규칙을 지우려면 Ctrl 키를 누른 상태로 규칙의 행에서 빈 영역을 클릭합니다.
선택한 규칙 잘라내기 또는 복사	선택한 규칙의 행에서 빈 영역을 마우스 오른쪽 버튼으로 클릭하고 **Cut** 또는 **Copy**를 선택합니다. **팁** 고정 규칙은 복사할 수 있지만 잘라낼 수는 없습니다.
잘라내거나 복사한 규칙을 규칙 목록에 붙여넣기	선택한 규칙을 붙여넣을 규칙의 행에서 빈 영역을 마우스 오른쪽 버튼으로 클릭하고 **Paste above** 또는 **Paste below**를 선택합니다. **팁** Static Translations 목록에는 고정 규칙만, Dynamic Translations 목록에는 동적 규칙만 붙여넣을 수 있습니다.
선택한 규칙 이동	새 위치 아래로 선택한 규칙을 끌어서 놓습니다. 새 위치는 끌어올 때 포인터 위에 파란색 가로선으로 표시됩니다.
규칙 삭제	규칙 옆의 삭제 아이콘( )을 클릭한 다음 **OK**를 클릭합니다. **팁** 선택한 규칙의 행에서 빈 영역을 마우스 오른쪽 버튼으로 클릭하고 **Delete**를 선택한 다음 **OK**를 클릭하여 하나 이상의 선택한 규칙을 삭제할 수도 있습니다.
경고 표시	**Show Warnings**를 클릭합니다. 11-7페이지의 NAT 규칙 경고 및 오류 작업을/를 참조하십시오.

NAT 규칙 경고 및 오류 작업

라이센스: 모두

어떤 NAT 규칙의 조건 때문에 후속 규칙이 트래픽과 매칭하지 못할 수 있습니다. 모든 유형의 규칙 조건은 후속 규칙을 선점할 수 있습니다.

또한 모든 구성된 조건이 동일한 경우, 규칙은 동일한 후속 규칙을 선점합니다. 조건 중 하나라도 다르면 후속 규칙이 선점되지 않습니다.

다음 표에는 경고를 표시하고 지우기 위해 수행할 수 있는 작업이 요약되어 있습니다.

표 11-4 선점된 규칙 경고 작업

목적	가능한 작업
경고 표시	**Show Warnings**를 클릭합니다. 선점된 각 규칙 옆에 있는 경고 아이콘( )과 함께 페이지가 업데이트됩니다.
규칙에 대한 경고 표시	규칙 옆에 있는 경고 아이콘( ) 위로 포인터를 이동합니다. 해당 규칙을 선점한 규칙을 알리는 메시지가 표시됩니다.
경고 지우기	**Hide Warnings**를 클릭합니다. 페이지가 새로 고쳐지고 경고가 사라집니다. **팁** 규칙의 추가 또는 수정, 다시 로드 아이콘( ) 클릭 등 페이지를 새로 고치는 작업을 수행해도 경고가 지워집니다.

적용 시 NAT 정책이 실패하는 규칙을 생성한 경우 규칙 옆에 오류 아이콘( )이 나타납니다. 고정 규칙에 충돌이 있거나 정책에 사용된 네트워크 객체를 수정하여 그로 인해 정책이 무효화되는 경우 오류가 발생합니다. 예를 들어 IPv6 주소만을 사용하도록 네트워크 객체를 변경하고, 해당 객체를 사용하는 규칙에 더 이상 유효한 네트워크가 없는 경우(하나 이상의 네트워크가 필요하지만) 오류가 발생합니다. 오류 아이콘이 자동으로 나타나며, **Show Warnings**를 클릭할 필요가 없습니다.

NAT 정책 관리

라이센스: 제어

지원되는 디바이스: Series 3

NAT 정책 페이지(**Devices > NAT**)에서 모든 현재 NAT 정책을 이름별로 확인하고 선택 사항인 설명과 다음 상태 정보도 볼 수 있습니다.

- 녹색 텍스트 — 정책이 대상 디바이스에서 최신 상태인 경우
- 빨간색 텍스트 — 정책이 대상 디바이스에서 최신 상태가 아닌 경우

이 페이지의 옵션을 통해 정책 비교, 새 정책 생성, 대상 디바이스에 정책 적용, 정책 복사, 각 정책에서 최근에 저장된 모든 설정을 나열하는 보고서 보기 및 정책 수정을 수행할 수 있습니다.

참고 관리되는 디바이스에 NAT 정책을 적용한 후에는 최신 상태가 아니더라도 정책을 삭제할 수 없습니다. 대신, 관리되는 디바이스에서 적용된 NAT 규칙을 제거하려면 규칙 없이 NAT 정책을 적용해야 합니다.

다음 표에서는 NAT 정책 페이지에서 정책 관리를 위해 수행할 수 있는 작업에 대해 설명합니다.

표 11-5 NAT 정책 관리 작업

목적	가능한 작업
새 NAT 정책 생성	**New Policy**를 클릭합니다. 자세한 내용은 11-8페이지의 NAT 정책 생성을/를 참조하십시오.
기존 NAT 정책의 설정 수정	수정 아이콘( )을 클릭합니다. 자세한 내용은 11-9페이지의 NAT 정책 수정을/를 참조하십시오.
정책의 대상인 모든 디바이스에 NAT 정책 적용	정책 적용 아이콘( )을 클릭합니다. 자세한 내용은 11-14페이지의 NAT 정책 적용을/를 참조하십시오.
NAT 정책 복사	복사 아이콘( )을 클릭합니다. 자세한 내용은 11-10페이지의 NAT 정책 복사을/를 참조하십시오.
NAT 정책의 현재 컨피그레이션 설정을 나열하는 PDF 보고서 보기	보고서 아이콘( )을 클릭합니다. 자세한 내용은 11-10페이지의 NAT 정책 보고서 보기을/를 참조하십시오.
NAT 정책 비교	**Compare Policies**를 클릭합니다. 자세한 내용은 11-11페이지의 두 NAT 정책 비교을/를 참조하십시오.
NAT 정책 삭제	삭제 아이콘( )을 클릭한 다음 **OK**를 클릭합니다. 또는 정책을 삭제하지 않으려면 **Cancel**을 클릭합니다. 계속할지 여부를 물을 때 다른 사용자가 정책을 변경했고 저장하지 않았으면 알려줍니다. **참고** 관리되는 디바이스에 NAT 정책을 적용한 후에는 디바이스에서 정책을 삭제할 수 없습니다. 대신, 관리되는 디바이스에서 적용된 NAT 규칙을 제거하려면 규칙 없이 NAT 정책을 적용해야 합니다. 또한 대상 디바이스에 마지막으로 적용한 정책은 최신 상태가 아니더라도 삭제할 수 없습니다. 정책을 완전히 삭제할 수 있으려면 해당 대상에 다른 정책을 적용해야 합니다.

NAT 정책 생성

라이센스: 제어

지원되는 디바이스: Series 3

새 NAT 정책을 생성할 때 최소한 고유한 이름을 지정해야 합니다. 정책 생성 시간에 정책 대상을 식별해야 할 필요는 없지만 정책을 적용하기 전에 이 단계를 수행해야 합니다. 11-4페이지의 NAT 정책 대상 관리을/를 참조하십시오. 규칙 없는 NAT 정책을 디바이스에 적용하는 경우 시스템은 해당 디바이스에서 모든 NAT 규칙을 제거합니다.

NAT 정책을 생성하려면

액세스: Admin/Network Admin

1단계 **Devices > NAT**를 선택합니다.

NAT 페이지가 나타납니다.

2단계 **New Policy**를 클릭합니다.

New NAT Policy 팝업 창이 나타납니다.

3단계 정책에 고유한 **Name**을 지정하고 선택 사항인 **Description**도 입력합니다.

공백과 특수 문자를 포함하여 인쇄 가능한 모든 문자를 사용할 수 있습니다.

4단계 정책을 적용할 **Available Devices**를 선택합니다.

Ctrl 및 Shift 키를 사용하여 여러 디바이스를 선택하거나, 마우스 오른쪽 버튼을 클릭하고 **Select All**을 선택합니다. 나타나는 디바이스의 범위를 좁히려면 **Search** 필드에 검색 문자열을 입력합니다. 검색을 지우려면 지우기 아이콘( )을 클릭합니다.

5단계 **Selected Devices**를 추가합니다. 클릭하고 끌거나, **Add to Policy**를 클릭할 수 있습니다.

6단계 **Save**를 클릭합니다.

NAT 정책 Edit 페이지가 나타납니다. 규칙 추가를 비롯하여 새 정책 구성에 대한 자세한 내용은 11-9페이지의 NAT 정책 수정을/를 참조하십시오. 정책을 반영하려면 적용해야 합니다. 11-14페이지의 NAT 정책 적용을/를 참조하십시오.

NAT 정책 수정

라이센스: 제어

지원되는 디바이스: Series 3

NAT 정책 Edit 페이지에서 정책을 구성할 수 있습니다. 자세한 내용은 11-2페이지의 NAT 정책 구성을/를 참조하십시오.

컨피그레이션을 변경할 때 메시지가 나타나 저장하지 않은 변경 사항이 있음을 알립니다. 변경 사항을 유지하려면 NAT 정책 Edit 페이지를 종료하기 전에 정책을 저장해야 합니다. 변경 사항을 저장하지 않고 정책 Edit 페이지를 종료하려고 할 경우 저장하지 않은 변경 사항이 있다는 주의 메시지가 나타납니다. 그러면 변경 사항을 취소하고 정책을 종료하거나 정책 Edit 페이지로 돌아갈 수 있습니다.

정책 Edit 페이지에서 60분간 아무런 활동이 없으면 세션의 개인 정보 보호를 위해 정책의 변경 사항이 취소되고 NAT 페이지로 돌아갑니다. 아무런 활동 없이 최초 30분이 지나면 메시지가 나타나고 이 메시지가 정기적으로 업데이트되면서 변경 사항이 취소될 때까지 남은 시간(분)을 알려줍니다. 페이지에서 어떤 활동이 일어나면 타이머가 재설정됩니다.

2개의 브라우저 창에서 동일한 정책을 수정하려고 하면, 새 창에서 수정을 시작하고 원래의 창에서 변경한 사항을 취소한 다음 새 창에서 수정을 계속할지 아니면 두 번째 창을 취소하고 정책 Edit 페이지로 돌아갈지 묻습니다.

여러 사용자가 동시에 동일한 정책을 수정할 경우 정책 Edit 페이지의 각 사용자에게 메시지가 나타나 정책을 변경하고 저장하지 않은 다른 사용자가 있음을 알려줍니다. 변경을 시도하는 사용자에게는 자신의 변경이 다른 사용자의 변경을 덮어쓸 것이라는 주의 메시지가 표시됩니다. 여러 사용자가 동일한 정책을 저장할 경우 마지막으로 저장된 변경 사항이 유지됩니다.

인터페이스 유형을 해당 인터페이스가 있는 디바이스를 대상으로 하는 NAT 정책과 함께 사용하기에 적절하지 않은 유형으로 변경하면, 정책에는 해당 인터페이스가 삭제된 것으로 표시됩니다. 정책에서 인터페이스를 자동으로 제거하려면 NAT 정책에서 **Save**를 클릭합니다.

NAT 정책을 수정하려면

액세스: Admin/Network Admin

1단계 **Devices > NAT**를 선택합니다.

NAT 페이지가 나타납니다.

2단계 구성하려는 NAT 정책 옆의 수정 아이콘( )을 클릭합니다.

NAT 정책 Edit 페이지가 나타납니다.

3단계 정책을 구성하려면 11-2페이지의 NAT 정책 구성에 설명된 작업을 수행할 수 있습니다.

4단계 컨피그레이션을 저장하거나 취소합니다. 다음 옵션을 이용할 수 있습니다.

- 변경 사항을 저장하고 계속 수정하려면 **Save**를 클릭합니다.
- 변경 사항을 저장하고 정책을 적용하려면 **Save and Apply**를 클릭합니다. 11-14페이지의 NAT 정책 적용을/를 참조하십시오.

  변경 사항을 반영하려면 정책을 적용해야 합니다.
- 변경 사항을 취소하려면 **Cancel**을 클릭하고 메시지가 표시되면 **OK**를 클릭합니다.

  변경 사항이 취소되고 NAT 페이지가 나타납니다.

NAT 정책 복사

라이센스: 제어

지원되는 디바이스: Series 3

NAT 정책을 복사하고 이름을 변경할 수 있습니다. 복사하는 정책에는 모든 정책 규칙 및 컨피그레이션이 포함됩니다.

NAT 정책을 복사하려면

액세스: Admin/Network Admin

1단계 **Devices > NAT**를 선택합니다.

NAT 페이지가 나타납니다.

2단계 구성하려는 NAT 정책 옆의 복사 아이콘( )을 클릭합니다.

Copy NAT Policy 팝업 창이 나타납니다.

3단계 고유한 정책 **Name**을 입력합니다.

공백과 특수 문자를 포함하여 인쇄 가능한 모든 문자를 사용할 수 있습니다.

4단계 **OK**를 클릭합니다.

복사본은 이름의 알파벳순으로 NAT 페이지에 나타납니다.

NAT 정책 보고서 보기

라이센스: 제어

지원되는 디바이스: Series 3

NAT 정책 보고서는 특정 시점의 정책 및 규칙 컨피그레이션에 대한 기록입니다. 감사의 목적으로 또는 현재 컨피그레이션을 검사하는 데 이 보고서를 사용할 수 있습니다.

팁 정책을 현재 적용된 정책과 비교하거나 다른 정책과 비교하는 NAT 비교 보고서도 생성할 수 있습니다. 자세한 내용은 11-11페이지의 두 NAT 정책 비교을/를 참조하십시오.

NAT 정책 보고서는 다음 표에 설명된 섹션으로 구성됩니다.

표 11-6 NAT 정책 보고서 섹션

섹션	설명
Title Page	정책 보고서의 이름, 정책이 마지막으로 수정된 날짜와 시간, 마지막으로 수정한 사용자의 이름을 나타냅니다.
Table of Contents	보고서의 내용에 대해 설명합니다.
Policy Information	정책의 이름과 설명, 마지막으로 정책을 수정한 사용자의 이름, 정책이 마지막으로 수정된 날짜와 시간을 제공합니다. 11-9페이지의 NAT 정책 수정을/를 참조하십시오.
Device Targets	정책으로 대상을 지정한 매니지드 디바이스가 나열됩니다. 11-4페이지의 NAT 정책 대상 관리을/를 참조하십시오.
Rules	정책에 있는 각 규칙에 대해 규칙 유형 및 조건을 제공합니다. 11-16페이지의 NAT 규칙 생성 및 수정을/를 참조하십시오.
Referenced Objects	정책에 사용되는 모든 개별 객체 및 그룹 객체의 이름과 컨피그레이션을 그 객체가 구성된 조건의 유형(Zones, Networks 및 Ports)별로 제공합니다.

NAT 정책 보고서를 보려면

액세스: Admin/Network Admin

1단계 **Devices > NAT**를 선택합니다.

NAT 페이지가 나타납니다.

2단계 보고서를 생성할 정책 옆의 보고서 아이콘( )을 클릭합니다. NAT 정책 보고서를 생성하기 전에 모든 변경 사항을 저장해야 합니다. 저장된 변경 사항만 보고서에 나타납니다.

시스템에서 보고서를 생성합니다. 브라우저 설정에 따라 보고서가 팝업 창에 나타날 수 있으며, 컴퓨터에 보고서를 저장하는 프롬프트가 표시될 수도 있습니다.

두 NAT 정책 비교

라이센스: 제어

지원되는 디바이스: Series 3

정책 변경 사항을 검토하려면 두 NAT 정책의 차이점을 확인할 수 있습니다. 두 정책을 비교하거나 현재 적용된 정책을 다른 정책과 비교할 수 있습니다. 선택적으로, 비교 후 두 정책의 차이를 기록하는 PDF 보고서를 생성할 수도 있습니다.

정책 비교에 사용할 수 있는 2가지 툴이 있습니다.

- 비교 보기에서는 두 정책의 차이점만 나란히 표시합니다. 각 정책의 이름이 비교 보기의 좌우 제목 표시줄에 나타납니다. 단, **Running Configuration**을 선택할 경우 빈 표시줄에 현재 활성 상태의 정책이 나타납니다.

  이를 사용하여 웹 인터페이스에서 그 차이점이 강조 표시된 상태에서 두 정책을 모두 보고 탐색할 수 있습니다.
- 비교 보고서는 두 정책의 차이점에 대해서만 기록을 생성하는데, 그 형식은 정책 보고서와 비슷하지만 PDF 형식입니다.

이를 사용하여 향후 점검을 위해 정책 비교를 저장, 복사, 인쇄, 공유할 수 있습니다.

정책 비교 툴을 이해하고 사용하는 방법에 대한 자세한 내용은 다음 절을 참조하십시오.

- 11-12페이지의 NAT 정책 비교 보기 사용
- 11-12페이지의 NAT 정책 비교 보고서 사용

NAT 정책 비교 보기 사용

라이센스: 제어

지원되는 디바이스: Series 3

비교 보기에서는 두 정책을 나란히 표시하며, 각 정책은 비교 보기의 좌우 제목 표시줄에 있는 이름으로 식별됩니다. 실행 중인 컨피그레이션이 아닌 두 정책을 비교할 경우 마지막 수정 시간 및 마지막으로 수정한 사용자가 정책 이름과 함께 표시됩니다.

두 정책 간의 차이점이 강조 표시됩니다.

- 파란색은 강조 표시된 설정이 두 정책에서 다름을 의미하며, 그 차이점이 빨간색 텍스트로 표시됩니다.
- 녹색은 강조 표시된 설정이 둘 중 한 정책에만 나타남을 의미합니다.

다음 표의 작업을 수행할 수 있습니다.

표 11-7 NAT 정책 비교 보기의 작업

목적	가능한 작업
개별 변경 사항 탐색	제목 표시줄 위의 **Previous** 또는 **Next**를 클릭합니다. 왼쪽과 오른쪽 사이의 중앙에 있는 이중 화살표 아이콘( )이 움직이고, 어떤 차이점을 보고 있는지 식별할 수 있도록 **Difference** 번호가 조정됩니다.
새 정책 비교 보기 생성	**New Comparison**을 클릭합니다. **Select Comparison** 창이 나타납니다. 자세한 내용은 11-12페이지의 NAT 정책 비교 보고서 사용을/를 참조하십시오.
정책 비교 보고서 생성	**Comparison Report**를 클릭합니다. 정책 비교 보고서에서는 두 정책의 차이점만 나열하는 PDF 문서를 생성합니다.

NAT 정책 비교 보고서 사용

라이센스: 제어

지원되는 디바이스: Series 3

NAT 정책 비교 보고서는 두 NAT 정책 또는 어떤 정책과 정액 비교 보기에 의해 식별되는 현재 적용된 정책의 모든 차이점에 대한 기록이며 PDF 형식으로 제공됩니다. 두 정책 컨피그레이션의 차이점을 더 자세히 살펴보고 조사 결과를 저장하여 배포하는 데 이 보고서를 사용할 수 있습니다.

액세스 권한이 있는 모든 NAT 정책에 대해 비교 보기에서 정책 비교 보고서를 생성할 수 있습니다. 정책 보고서를 생성하기 전에 모든 변경 사항을 저장해야 합니다. 저장된 변경 사항만 보고서에 나타납니다.

정책 비교 보고서의 형식은 정책 보고서와 동일합니다. 단, 정책 보고서는 정책의 모든 컨피그레이션을 포함하는 것과 달리 정책 비교 보고서는 두 정책에서 달라지는 컨피그레이션만 나열합니다. NAT 정책 비교 보고서는 NAT 정책 보고서 섹션 표에 설명된 섹션으로 구성됩니다.

두 NAT 정책을 비교하려면

액세스: Admin/Network Admin

1단계 **Devices > NAT**를 선택합니다.

NAT 페이지가 나타납니다.

2단계 **Compare Policies**를 클릭합니다.

Select Comparison 창이 나타납니다.

3단계 **Compare Against** 드롭다운 목록에서 원하는 비교 유형을 선택합니다.

- 두 개의 다른 정책을 비교하려면 **Other Policy**를 선택합니다.

  페이지가 새로 고쳐지고 Policy A 및 Policy B 드롭다운 목록이 나타납니다.
- 두 개의 서로 다른 개정을 비교하려면 **Other Revision**을 선택합니다.

  페이지가 새로 고쳐지고 Policy, Revision A 및 Revision B 드롭다운 목록이 나타납니다.
- 다른 정책과 현재 활성 정책을 비교하려면 **Running Configuration**을 선택합니다.

  페이지가 새로 고쳐지고 Target/Running Configuration A 및 Policy B 드롭다운 목록이 나타납니다.

4단계 선택한 비교 유형에 따라 다음을 선택할 수 있습니다.

- 두 개의 다른 정책을 비교할 경우 비교할 정책을 **Policy A** 및 **Policy B** 드롭다운 목록에서 각각 선택합니다.
- 두 개의 서로 다른 개정을 비교하는 경우 정책을 선택한 다음, **Revision A** 및 **Revision B** 드롭다운 목록에서 비교할 개정을 선택합니다.
- 실행 중인 컨피그레이션을 다른 정책과 비교할 경우 **Policy B** 드롭다운 목록에서 두 번째 정책을 선택합니다.

5단계 **OK**를 클릭하여 정책 비교 보기를 표시합니다.

비교 보기가 나타납니다.

6단계 선택적으로, **Comparison Report**를 클릭하여 NAT 정책 비교 보고서를 생성합니다.

NAT 정책 비교 보고서가 나타납니다. 브라우저 설정에 따라 보고서가 팝업 창에 나타날 수 있으며, 컴퓨터에 보고서를 저장하는 프롬프트가 표시될 수도 있습니다.

NAT 정책 적용

라이센스: 제어

지원되는 디바이스: Series 3

NAT 정책을 변경한 후, 디바이스에 의해 모니터링되는 네트워크에서 컨피그레이션 변경 사항을 구현하려면 하나 이상의 디바이스에 해당 정책을 적용해야 합니다. 정책을 적용하려면 해당 정책을 적용할 디바이스를 대상으로 지정해야 합니다. 11-4페이지의 NAT 정책 대상 관리을/를 참조하십시오.

NAT 정책을 적용할 때 다음 사항에 유의하십시오.

- 방어 센터에서 여러 NAT 정책을 구성 및 유지 관리할 수 있지만 한 번에 한 디바이스에 한 정책만 적용할 수 있습니다.
- 두 개의 서로 다른 NAT 정책을 서로 다른 디바이스에 적용할 수 있으며, 이러한 디바이스가 여러 정책의 대상인 경우에도 그러합니다.
- FireSIGHT 시스템의 서로 다른 버전을 실행하는(예: 디바이스 중 하나에 대한 업그레이드가 실패한 경우) 스태킹된 디바이스에는 NAT 정책을 적용할 수 없습니다. 자세한 내용은 4-43페이지의 스태킹된 디바이스 관리을/를 참조하십시오.
- 정책 적용이 아직 보류 중인 새 NAT 정책은 적용할 수 없습니다.
- NAT 정책의 인터페이스에 영향을 주는 디바이스 컨피그레이션을 적용하는 경우, 시스템은 인터페이스 변경 사항을 포함하여 디바이스에 NAT 정책을 다시 적용합니다. 그러나 DC에서 정책은 변경되지 않은 상태로 남아 있으며 인터페이스에 오류 아이콘( )이 표시됩니다.

참고 빈 NAT 정책을 적용하면 디바이스에서 모든 NAT 규칙이 제거됩니다.

자세한 내용은 다음 절을 참조하십시오.

- 11-14페이지의 완전한 NAT 정책 적용 — 빠른 적용 옵션을 사용하여 NAT 정책을 적용하는 방법에 대해 설명합니다.
- 11-15페이지의 선택한 정책 컨피그레이션 적용 — NAT 정책 내에서 컨피그레이션을 선택하고 적용하는 방법에 대해 설명합니다.

완전한 NAT 정책 적용

라이센스: 제어

지원되는 디바이스: Series 3

한 번에 하나의 NAT 정책을 적용할 수 있습니다. NAT 정책을 적용하면 관련된 규칙 컨피그레이션, 객체 및 정책 변경 사항도 정책 대상 디바이스에 적용됩니다. 팝업 창에서는 모든 변경 사항을 단일 빠른 적용 작업으로 적용할 수 있습니다.

완전한 NAT 정책의 빠른 적용을 수행하려면

액세스: Admin/Network Admin

1단계 **Devices > NAT**를 선택합니다.

NAT 페이지가 나타납니다.

2단계 적용할 정책 옆에 있는 적용 아이콘( )을 클릭합니다.

Apply NAT Rules 팝업 창이 나타납니다.

또는 정책 Edit 페이지에서 **Save and Apply**를 클릭할 수 있습니다. 11-9페이지의 NAT 정책 수정을/를 참조하십시오.

3단계 **Apply All**을 클릭합니다.

정책 적용 작업이 대기열에 추가됩니다. **OK**를 클릭하여 NAT 페이지로 돌아갑니다.

팁 Task Status 페이지(**System > Monitoring > Task Status**)에서 정책 적용 작업의 진행 상황을 모니터링할 수 있습니다.

선택한 정책 컨피그레이션 적용

라이센스: 제어

지원되는 디바이스: Series 3

NAT 정책 및 지정된 대상 디바이스에 변경 사항을 적용하려면 자세한 정책 적용 페이지를 사용할 수 있습니다. 자세한 페이지에는 정책 대상이 되는 각 디바이스가 나열되며 디바이스별 NAT 정책에 대한 열이 표시됩니다. 최신 상태가 아닌 각 대상 디바이스에 대한 NAT 정책에 변경 사항을 적용할지 여부를 지정할 수 있습니다.

선택한 NAT 정책 컨피그레이션을 적용하려면

액세스: Admin/Network Admin

1단계 **Devices > NAT**를 선택합니다.

NAT 페이지가 나타납니다.

2단계 적용할 정책 옆에 있는 적용 아이콘( )을 클릭합니다.

Apply NAT Rules 팝업 창이 나타납니다.

또는 정책 Edit 페이지에서 **Save and Apply**를 클릭할 수 있습니다. 11-9페이지의 NAT 정책 수정을/를 참조하십시오.

3단계 **Details**를 클릭합니다.

자세한 Apply NAT Rules 팝업 창이 나타납니다.

팁 정책의 **Status** 열에서 오래된 메시지를 클릭하여 NAT 페이지(**Devices > NAT**)에서 팝업 창을 열 수도 있습니다.

4단계 대상 디바이스에 NAT 정책을 적용할지 여부를 지정하려면 디바이스 이름 옆에 있는 **NAT policy** 확인란을 선택하거나 선택 취소합니다.

5단계 **Apply Selected Configurations**를 클릭합니다.

정책 적용 작업이 대기열에 추가됩니다. **OK**를 클릭하여 NAT 페이지로 돌아갑니다.

팁 Task Status 페이지(**System > Monitoring > Task Status**)에서 정책 적용 작업의 진행 상황을 모니터링할 수 있습니다.

NAT 규칙 생성 및 수정

라이센스: 제어

지원되는 디바이스: Series 3

NAT 규칙은 단순히 컨피그레이션 및 조건의 집합으로 다음을 수행합니다.

- 네트워크 트래픽 정규화
- 해당 자격과 일치하는 트래픽의 변환 방법 지정

기존 NAT 정책 내에서 NAT 규칙을 생성 및 수정합니다. 각 규칙은 하나의 정책에 속합니다.

규칙을 추가 또는 수정하기 위한 웹 인터페이스는 유사합니다. 페이지 상단에서 규칙 이름, 상태, 유형 및 위치(동적인 경우)를 지정합니다. 페이지 왼쪽에 있는 탭을 사용하여 조건을 작성합니다. 각 조건 유형에 자체 탭이 있습니다.

다음 목록에는 NAT 규칙의 구성 가능한 구성 요소가 요약되어 있습니다.

Name

각 규칙에 고유한 이름을 지정합니다. 고정 NAT 규칙에는 최대 22자를 사용합니다. 동적 NAT 규칙에는 최대 30자를 사용합니다. 콜론(:)을 제외한 특수 문자 및 공백을 포함하여 인쇄 가능한 문자를 사용할 수 있습니다.

Rule State

기본적으로 규칙은 활성화되어 있습니다. 규칙을 비활성화하면 시스템은 네트워크 트래픽의 변환 평가에 규칙을 사용하지 않습니다. NAT 정책에서 규칙의 목록을 볼 때 비활성화된 규칙은 회색으로 표시됩니다. 단, 이 규칙은 수정 가능합니다.

Type

규칙 유형은 규칙의 조건과 일치하는 트래픽을 처리하는 방법을 결정합니다. NAT 규칙을 생성 및 수정하면 구성 가능한 구성 요소는 규칙 유형에 따라 변경됩니다.

규칙 유형 및 규칙 유형이 변환과 트래픽 플로우에 미치는 영향에 대한 자세한 내용은 11-17페이지의 NAT 규칙 유형 이해을/를 참조하십시오.

Position (Dynamic Rules Only)

NAT 정책의 동적 규칙은 1부터 시작하여 번호가 지정됩니다. 시스템은 오름차순 규칙 번호에 따라 하향식 순서로 트래픽이 NAT 규칙과 일치하는지를 확인합니다.

정책에 규칙을 추가할 때 규칙 번호를 참조점으로 사용하여 특정 규칙의 **위** 또는 **아래**에 위치를 지정합니다. 기존 규칙을 수정할 때에도 유사한 방식으로 규칙을 이동(**Move**)할 수 있습니다. 자세한 내용은 11-5페이지의 NAT 정책에서 규칙 구성을/를 참조하십시오.

Conditions

규칙 조건은 변환하려는 특정 트래픽을 식별합니다. 조건은 보안 영역, 네트워크, 전송 프로토콜 포트 등 여러 특성의 조합으로 트래픽을 매칭할 수 있습니다.

조건 추가에 대한 자세한 내용은 11-19페이지의 NAT 규칙 조건 및 조건 원리 이해 및 11-24페이지의 NAT 규칙에서 서로 다른 조건 유형 작업을/를 참조하십시오.

NAT 규칙을 생성 또는 수정하려면

액세스: Admin/Network Admin

1단계 **Devices > NAT**를 선택합니다.

NAT 페이지가 나타납니다.

2단계 규칙을 추가하려는 NAT 정책 옆의 수정 아이콘( )을 클릭합니다.

NAT 정책 Edit 페이지가 나타납니다.

3단계 새 규칙을 추가하거나 기존 규칙을 수정합니다.

- 새 규칙을 추가하려면 **Add Rule**을 클릭합니다.
- 기존 규칙을 수정하려면 수정하려는 규칙 옆에 있는 수정 아이콘( )을 클릭합니다.

Add Rule 또는 Editing Rule 페이지가 나타납니다.

팁 오른쪽 클릭 컨텍스트 메뉴를 사용하여 많은 규칙 생성 및 관리 작업을 수행할 수 있습니다. 2-5페이지의 컨텍스트 메뉴 사용을/를 참조하십시오. 규칙을 끌어서 놓아 순서를 변경할 수도 있습니다.

4단계 이 절에서 앞서 설명한 것처럼 규칙 구성 요소를 구성합니다. 기본값을 제외하고 다음과 같이 구성할 수 있습니다.

- 고유한 규칙 **Name**을 제공해야 합니다.
- 규칙의 **Enabled** 여부를 지정합니다.
- 규칙 **Type**을 선택합니다.
- 규칙 위치를 지정합니다(동적 규칙의 경우에만).
- 규칙의 조건을 구성합니다.

  고정 규칙에는 원래 목적지 네트워크를 포함해야 합니다.

  동적 규칙에는 변환된 소스 네트워크를 포함해야 합니다.

5단계 **Add** 또는 **Save**를 클릭합니다.

변경 내용이 저장되었습니다. 변경 사항을 적용하려면 NAT 정책을 적용해야 합니다. 11-14페이지의 NAT 정책 적용을/를 참조하십시오.

NAT 규칙 유형 이해

라이센스: 모두

모든 NAT 규칙에는 다음을 수행하는 관련 유형이 있습니다.

- 네트워크 트래픽 정규화
- 해당 자격과 일치하는 트래픽의 변환 방법 지정

다음 목록에는 NAT 규칙 유형이 요약되어 있습니다.

Static

Static 규칙은 목적지 네트워크에 대한 일대일 변환 및 선택적으로 포트와 프로토콜을 제공합니다. 고정 변환을 구성할 때 소스 영역, 목적지 네트워크 및 목적지 포트를 구성할 수 있습니다. 목적지 영역 또는 소스 네트워크는 구성할 수 없습니다.

원래 목적지 네트워크를 **반드시** 지정해야 합니다. 목적지 네트워크의 경우 단일 IP 주소를 포함하는 네트워크 객체 및 그룹만 선택할 수 있습니다. 또는 단일 IP 주소를 나타내는 리터럴 IP 주소를 입력할 수 있습니다. 단일 원래 목적지 네트워크 및 단일 변환된 목적지 네트워크만 지정할 수 있습니다.

선택적으로, 단일 원래 목적지 포트 및 단일 변환된 목적지 포트만 지정할 수 있습니다. 원래 목적지 포트를 지정하기 전에 원래 목적지 네트워크를 지정해야 합니다. 또한 원래 목적지 포트를 지정하지 않는 한 변환된 목적지 포트도 지정할 수 없으며, 변환된 값은 원래 값의 프로토콜과 일치해야 합니다.

주의 클러스터링된 디바이스의 고정 NAT 규칙에 대해서는, NAT 변환의 영향을 받는 모든 네트워크가 사설 네트워크인 경우에만 개별 피어 인터페이스를 선택하십시오. 공용 네트워크와 사설 네트워크 간 트래픽에 영향을 미치는 고정 NAT 규칙에는 이 컨피그레이션을 사용하지 **마십시오**.

Dynamic IP Only

Dynamic IP Only 규칙은 다대다 소스 네트워크를 변환하지만 포트와 프로토콜을 유지 관리합니다. Dynamic IP Only 변환을 구성할 때에는 영역, 소스 네트워크, 원래 목적지 네트워크 및 원래 목적지 포트를 구성할 수 있습니다. 변환된 목적지 네트워크 또는 변환된 목적지 포트를 구성할 수 없습니다.

하나 이상의 변환된 소스 네트워크를 **반드시** 지정해야 합니다. 변환된 소스 네트워크 값의 수가 원래 소스 네트워크의 수보다 적으면, 해당 규칙에 대해 모든 원래 주소가 매칭되기 전에 변환된 주소가 부족해질 수 있음을 알리는 경고가 표시됩니다.

동일한 패킷과 일치하는 조건이 포함된 여러 규칙이 있는 경우 낮은 우선순위 규칙은 Dead 상태가 됩니다. 즉, 이러한 규칙은 트리거할 수 없습니다. 시스템은 또한 Dead 규칙에 대한 경고를 표시합니다. 어떤 규칙이 Dead 규칙을 대신하는지 확인하려면 툴팁을 볼 수 있습니다.

참고 Dead 규칙이 포함된 정책을 저장 및 적용할 수 있지만, 이러한 규칙은 변환을 제공할 수 없습니다.

경우에 따라, 좀 더 범위가 넓은 제한된 범위의 선행 규칙으로 규칙을 생성할 수 있습니다. 예를 들면 다음과 같습니다.

```
Rule 1: Match on address A and port A/Translate to address B
Rule 2: Match on address A/Translate to Address C
```

이 예에서 Rule 1은 Rule 2와도 일치하는 일부 패킷을 매칭합니다. 따라서 Rule 2는 완전히 Dead 상태가 될 수 없습니다.

선택적으로, 원래 목적지 포트만 지정할 수 있습니다. 변환된 목적지 포트는 지정할 수 없습니다.

Dynamic IP + Port

Dynamic IP + Port 규칙은 다대일 또는 다대다 소스 네트워크 및 포트와 프로토콜을 변환합니다. Dynamic IP + Port 변환을 구성할 때에는 영역, 소스 네트워크, 원래 목적지 네트워크 및 원래 목적지 포트를 구성할 수 있습니다. 변환된 목적지 네트워크 또는 변환된 목적지 포트를 구성할 수 없습니다.

하나 이상의 변환된 소스 네트워크를 **반드시** 지정해야 합니다. 동일한 패킷과 일치하는 조건이 포함된 여러 규칙이 있는 경우 낮은 우선순위 규칙은 Dead 상태가 됩니다. 즉, 이러한 규칙은 트리거할 수 없습니다. 시스템은 또한 Dead 규칙에 대한 경고를 표시합니다. 어떤 규칙이 Dead 규칙을 대신하는지 확인하려면 툴팁을 볼 수 있습니다.

참고 Dead 규칙이 포함된 정책을 저장 및 적용할 수 있지만, 이러한 규칙은 변환을 제공할 수 없습니다.

선택적으로, 원래 목적지 포트만 지정할 수 있습니다. 변환된 목적지 포트는 지정할 수 없습니다.

참고 사용자는 동적 IP 및 포트 규칙을 생성하고 시스템은 포트를 사용하지 않는 트래픽을 전달하는 경우, 해당 트래픽에 대해 변환이 발생하지 않습니다. 예를 들어, ICMP는 포트를 사용하지 않으므로 소스 네트워크와 일치하는 IP 주소에서 수행하는 ping(ICMP)은 매핑되지 않습니다.

다음 표에는 지정된 NAT 규칙 유형을 기반으로 구성할 수 있는 NAT 규칙 조건 유형이 요약되어 있습니다.

표 11-8 NAT 규칙 유형별 사용 가능한 NAT 규칙 조건 유형

상태	정적	동적(IP Only 또는 IP + Port)
Source Zones	옵션	옵션
Destination Zones	허용되지 않음	옵션
Original Source Networks	허용되지 않음	옵션
Translated Source Networks	허용되지 않음	**필수**
Original Destination Networks	**필수**	옵션
Translated Destination Networks	선택, 단일 주소 전용	허용되지 않음
Original Destination Ports	선택, 단일 포트 전용, 원래 목적지 네트워크를 정의한 경우에만 허용됨	옵션
Translated Destination Ports	선택, 단일 포트 전용, 원래 목적지 포트를 정의한 경우에만 허용됨	허용되지 않음

NAT 규칙 조건 및 조건 원리 이해

라이센스: 모두

규칙과 일치하는 트래픽 유형을 식별하려면 조건을 NAT 규칙에 추가할 수 있습니다. 각 조건 유형에 대해, 사용 가능한 조건 목록에서 규칙에 추가할 조건을 선택합니다. 해당되는 경우 조건 필터를 사용하면 사용 가능한 조건을 제한할 수 있습니다. 사용 가능한 선택된 조건 목록은 단일 조건 길이만큼 짧을 수도 있고 여러 페이지 길이일 수도 있습니다. 사용 가능한 조건을 검색하고, 입력 시 업데이트되는 목록에서 입력된 이름이나 값과 일치하는 조건만 표시할 수 있습니다.

조건 유형에 따라, 사용 가능한 조건 목록은 Cisco에서 직접 제공하는 조건의 조합으로 구성될 수도 있고 객체 관리자(**Objects > Object Management**)에서 생성된 객체, 개별 조건 페이지에서 직접 생성된 객체 및 리터럴 조건을 비롯한 기타 FireSIGHT 시스템 기능으로 구성될 수도 있습니다.

규칙 조건 지정에 대한 자세한 내용은 다음 절을 참조하십시오.

- 11-20페이지의 NAT 규칙 조건 이해 — 서로 다른 규칙 조건의 유형을 정의합니다.
- 11-20페이지의 NAT 규칙에 조건 추가 — 규칙 조건을 선택하고 추가하는 데 사용되는 컨트롤에 대해 설명합니다.
- 11-22페이지의 NAT 규칙 조건 목록 검색 — 사용 가능한 조건을 검색하고, 입력 시 업데이트되는 목록에서 입력된 이름이나 값과 일치하는 조건만 표시하는 방법에 대해 설명합니다.
- 11-23페이지의 NAT 규칙에 리터럴 조건 추가 — 리터럴 조건을 규칙에 추가하는 방법에 대해 설명합니다.
- 11-23페이지의 NAT 규칙 조건에서 객체 사용 — 관련 조건 유형에 대한 컨피그레이션 페이지에서 시스템에 개별 객체를 추가하는 방법에 대해 설명합니다.

NAT 규칙 조건 이해

라이센스: 모두

다음 표에 설명된 조건을 충족하는 트래픽을 매칭하도록 NAT 규칙을 설정할 수 있습니다.

표 11-9 NAT 규칙 조건 유형

상태	설명	지원되는 방어 센터	지원되는 장치
영역	NAT 정책을 적용할 수 있는 하나 이상의 라우팅된 인터페이스의 컨피그레이션. 영역은 소스 및 목적지 인터페이스에서 트래픽 분류를 위한 메커니즘을 제공하며, 사용자는 소스 및 목적지 영역 조건을 규칙에 추가할 수 있습니다. 객체 관리자를 사용하여 영역을 생성하는 방법에 대한 자세한 내용은 3-38페이지의 보안 영역 작업을/를 참조하십시오.	모두	Series 3
네트워크	명시적으로 지정되거나 네트워크 객체 및 그룹을 사용하여 지정된 개별 IP 주소, CIDR 블록, 접두사 길이의 조합(3-4페이지의 네트워크 객체 작업 참조). 소스 및 목적지 네트워크 조건을 NAT 규칙에 추가할 수 있습니다.	모두	Series 3
대상 포트	전송 프로토콜을 기반으로 생성하는 개별 및 그룹 포트 객체를 비롯한 전송 프로토콜 포트. 객체 관리자를 사용하여 개별 및 그룹 전송 프로토콜 객체를 생성하는 방법에 대한 자세한 내용은 3-12페이지의 포트 객체 작업을/를 참조하십시오.	모두	Series 3

NAT 규칙에 조건 추가

라이센스: 모두

NAT 규칙에 조건을 추가하는 것은 기본적으로 각 조건 유형에 대해 동일합니다. 왼쪽에 있는 사용 가능한 조건의 목록에서 선택하고, 선택한 조건을 오른쪽에 있는 하나 또는 두 개의 선택한 조건 목록에 추가합니다.

모든 조건 유형에 대해, 클릭하고 강조 표시하여 하나 이상의 사용 가능한 개별 조건을 선택합니다. 두 목록 유형 사이의 버튼을 클릭하여 선택한 사용 가능한 조건을 선택한 조건 목록에 추가할 수도 있고, 선택한 사용 가능한 조건을 선택한 조건 목록으로 끌어서 놓을 수도 있습니다.

각 유형의 최대 50개의 조건을 선택한 조건 목록에 추가할 수 있습니다. 예를 들면, 어플라이언스의 상한에 도달할 때까지 최대 50개의 소스 영역 조건, 최대 50개의 목적지 영역 조건, 최대 50개의 소스 네트워크 조건 등을 추가할 수 있습니다.

다음 표에서는 조건을 선택하여 규칙에 추가하기 위해 수행할 수 있는 작업에 대해 설명합니다.

표 11-10 NAT 규칙에 조건 추가

목적	가능한 작업
사용 가능한 조건을 선택하여 선택한 조건 목록에 추가	사용 가능한 조건을 클릭합니다. 여러 조건을 선택하려면 Ctrl 및 Shift 키를 사용합니다.
나열된 모든 사용 가능한 조건 선택	사용 가능한 조건에 대한 행을 마우스 오른쪽 버튼으로 클릭하고 **Select All**을 클릭합니다.
사용 가능한 조건 또는 필터 목록 검색	**Search** 필드의 내부를 클릭한 다음 검색 문자열을 입력합니다. 자세한 내용은 11-22페이지의 NAT 규칙 조건 목록 검색을/를 참조하십시오.
사용 가능한 조건이나 필터 검색 시 검색 지우기	Search 필드 위의 다시 로드 아이콘( )을 클릭하거나, 검색 필드의 지우기 아이콘( )을 클릭합니다.
사용 가능한 조건 목록에서 선택한 영역 조건을 선택한 소스 또는 목적지 조건 목록에 추가	**Add to Source** 또는 **Add to Destination**을 클릭합니다. 자세한 내용은 11-24페이지의 NAT 규칙에 영역 조건 추가을/를 참조하십시오.
사용 가능한 조건 목록에서 선택한 네트워크 및 포트 조건을 선택한 원래 또는 변환된 조건 목록에 추가	**Add to Original** 또는 **Add to Translated**를 클릭합니다. 자세한 내용은 11-26페이지의 소스 네트워크 조건을 동적 NAT 규칙에 추가, 11-27페이지의 목적지 네트워크 조건을 NAT 규칙에 추가 또는 11-29페이지의 NAT 규칙에 포트 조건 추가을/를 참조하십시오.
선택한 사용 가능한 조건을 선택한 조건 목록으로 끌어서 놓기	선택한 조건을 클릭한 다음 선택한 조건 목록으로 끌어서 놓습니다.
리터럴 필드를 사용하여 리터럴 조건을 선택한 조건 목록에 추가	클릭하여 리터럴 필드에서 프롬프트를 제거하고, 리터럴 조건을 입력하고, **Add**를 클릭합니다. 네트워크 조건은 리터럴 조건을 추가하기 위한 필드를 제공합니다.
드롭다운 목록을 사용하여 리터럴 조건을 선택한 조건 목록에 추가	드롭다운 목록에서 조건을 선택하고 **Add**를 클릭합니다. 포트 조건은 리터럴 조건을 추가하기 위한 드롭다운 목록을 제공합니다. 자세한 내용은 11-29페이지의 NAT 규칙에 포트 조건 추가을/를 참조하십시오.
사용 가능한 조건 목록에서 선택할 수 있도록 개별 객체 또는 조건 필터 추가	추가 아이콘( )을 클릭합니다. 객체 관리자를 사용하여 객체를 추가하는 방법에 대한 자세한 내용은 3-1페이지의 재사용 가능 객체 관리을/를 참조하십시오.
선택한 조건 목록에서 단일 조건 삭제	조건 옆에 있는 삭제 아이콘( )을 클릭합니다.
선택한 조건 목록에서 조건 하나 삭제	마우스 오른쪽 버튼을 클릭하여 선택한 조건에 대한 행을 강조 표시하고 **Delete**를 클릭합니다.
선택한 조건 목록에서 조건 여러 개 삭제	Shift 및 Ctrl 키를 사용하여 여러 조건을 선택하거나 마우스 오른쪽 버튼을 클릭하여 **Select All**을 선택합니다. 그런 다음 선택한 조건의 행을 강조 표시하고 **Delete Selected**를 클릭합니다.

관련 조건 페이지 및 정책 Edit 페이지에서는 포인터를 개별 객체 위로 이동하여 객체의 내용을 표시하고, 그룹 객체 위로 이동하여 그룹에 있는 개별 객체의 수를 표시할 수 있습니다.

다음의 기본 절차는 새 규칙에 조건을 추가하는 방법에 대해 설명합니다. 규칙 추가 및 수정에 대한 전체 지침은 11-16페이지의 NAT 규칙 생성 및 수정을/를 참조하십시오.

선택한 조건 목록에 사용 가능한 조건을 추가하려면

액세스: Admin/Network Admin

1단계 **Devices > NAT**를 선택합니다.

NAT 페이지가 나타납니다.

2단계 수정하려는 NAT 정책 옆의 수정 아이콘( )을 클릭합니다.

정책 Edit 페이지가 나타납니다.

3단계 **Add Rule**을 클릭합니다.

Add Rule 페이지가 나타납니다.

4단계 규칙에 추가할 조건의 유형에 대한 탭을 클릭합니다.

선택한 조건 유형에 대한 조건 페이지가 나타납니다.

5단계 NAT 규칙에 조건 추가 표에 있는 사용 가능한 작업을 수행합니다.

6단계 **Add**를 클릭하여 컨피그레이션을 저장합니다.

규칙이 추가되고 정책 Edit 페이지가 나타납니다.

NAT 규칙 조건 목록 검색

라이센스: 모두

목록에 표시되는 항목 수를 제한하려면 사용 가능한 NAT 규칙 조건 목록을 필터링할 수 있습니다. 입력하여 일치하는 항목이 표시됨에 따라 목록이 업데이트됩니다.

선택적으로, 객체 이름 및 객체에 대해 구성된 값을 검색할 수 있습니다. 예를 들어 `Texas Office`라는 개별 네트워크 객체가 `192.168.3.0/24` 값으로 구성되어 있고 `US Offices`라는 그룹 객체에 포함된 경우 전체 또는 부분 검색 문자열(예: `Tex`)을 입력하거나 값(예: `3`)을 입력하여 두 객체를 모두 표시할 수 있습니다.

다음의 기본 절차는 새 규칙에서 목록을 필터링하는 방법에 대해 설명합니다. 규칙 추가 및 수정에 대한 전체 지침은 11-16페이지의 NAT 규칙 생성 및 수정을/를 참조하십시오.

사용 가능한 조건 목록을 검색하려면

액세스: Admin/Network Admin

1단계 **Devices > NAT**를 선택합니다.

NAT 페이지가 나타납니다.

2단계 수정하려는 NAT 정책 옆의 수정 아이콘( )을 클릭합니다.

정책 Edit 페이지가 나타납니다.

3단계 **Add Rule**을 클릭합니다.

Add Rule 페이지가 나타납니다.

4단계 목록을 검색하려면 검색 필드 내부를 클릭하여 프롬프트를 지운 다음 검색 문자열을 입력합니다.

입력하는 동안 목록이 업데이트되어 일치하는 항목이 표시되고, 검색 필드에 목록 지우기 아이콘( )이 나타납니다. 목록이 업데이트되며, 검색 문자열과 일치하는 항목이 없으면 항목이 나열되지 않습니다.

5단계 선택적으로, 검색 문자열을 지우려면 **Search** 필드 위의 다시 로드 아이콘( )을 클릭하거나, **Search** 필드의 지우기 아이콘( )을 클릭합니다.

전체 목록이 나타납니다.

6단계 **Add**를 클릭하여 컨피그레이션을 저장합니다.

규칙이 추가되고 정책 Edit 페이지가 나타납니다.

NAT 규칙에 리터럴 조건 추가

라이센스: 모두

다음 조건 유형에 대한 원래 조건 및 변환된 조건의 목록에 리터럴 값을 추가할 수 있습니다.

- 네트워크
- 포트

네트워크 조건의 경우, 원래 조건 또는 변환된 조건의 목록 아래에 있는 컨피그레이션 필드에 리터럴 값을 입력합니다.

포트 조건의 경우 드롭다운 목록에서 프로토콜을 선택합니다. 프로토콜이 `All`인 경우 및 선택적으로 프로토콜이 `TCP` 또는 `UDP`인 경우 컨피그레이션 필드에 포트 번호를 입력합니다.

각 관련 조건 페이지는 리터럴 값을 추가하기 위해 필요한 컨트롤을 제공합니다. 컨피그레이션 필드에 입력하는 값은 유효하지 않은 경우 또는 유효한 것으로 인식될 때까지 빨간색 텍스트로 나타납니다. 입력한 값이 유효한 것으로 인식되면 파란색 텍스트로 나타납니다. 유효한 값이 인식되면 회색으로 표시된 **Add** 버튼이 활성화됩니다. 추가한 리터럴 값이 선택한 조건 목록에 즉시 나타납니다.

각 리터럴 값 유형 추가에 대한 특정 세부사항은 다음 절을 참조하십시오.

- 11-26페이지의 소스 네트워크 조건을 동적 NAT 규칙에 추가
- 11-27페이지의 목적지 네트워크 조건을 NAT 규칙에 추가
- 11-29페이지의 NAT 규칙에 포트 조건 추가

NAT 규칙 조건에서 객체 사용

라이센스: 모두

객체 관리자(**Objects > Object Management**)에서 생성하는 객체는 사용 가능한 NAT 규칙 조건의 목록에서 즉시 선택할 수 있습니다. 자세한 내용은 3-1페이지의 재사용 가능 객체 관리을/를 참조하십시오.

NAT 정책에서 즉시 객체를 생성할 수도 있습니다. 관련 조건 페이지에 대한 컨트롤은 객체 관리자에서 사용하는 것과 동일한 컨피그레이션 컨트롤에 대한 액세스를 제공합니다.

즉석에서 생성하는 개별 객체는 사용 가능한 객체의 목록에 즉시 나타납니다. 이러한 객체를 현재 규칙과 기타 기존의/앞으로의 규칙에 추가할 수 있습니다. 관련 조건 페이지 및 정책 Edit 페이지에서는 포인터를 개별 객체 위로 이동하여 객체의 내용을 표시하고, 그룹 객체 위로 이동하여 그룹에 있는 개별 객체의 수를 표시할 수 있습니다.

NAT 규칙에서 서로 다른 조건 유형 작업

라이센스: 모두

트래픽을 하나 이상의 규칙 조건과 매칭할 수 있습니다. 자세한 내용은 다음 절을 참조하십시오.

- 11-24페이지의 NAT 규칙에 영역 조건 추가 — 객체 관리자를 사용하여 생성하는 보안 영역으로 트래픽을 매칭하는 방법에 대해 설명합니다.
- 11-26페이지의 소스 네트워크 조건을 동적 NAT 규칙에 추가 및 11-27페이지의 목적지 네트워크 조건을 NAT 규칙에 추가 — IP 주소 또는 주소 블록으로 트래픽을 매칭하는 방법에 대해 설명합니다.
- 11-29페이지의 NAT 규칙에 포트 조건 추가 — 지정된 전송 프로토콜 포트로 트래픽을 매칭하는 방법에 대해 설명합니다.

NAT 규칙에 영역 조건 추가

라이센스: 모두

시스템의 보안 영역은 관리되는 디바이스의 인터페이스로 구성됩니다. NAT 규칙에 추가하는 영역은 규칙의 대상을 라우팅된 인터페이스 또는 하이브리드 인터페이스가 있는 네트워크의 디바이스로 지정합니다. 라우팅된 인터페이스 또는 하이브리드 인터페이스가 있는 보안 영역만 NAT 규칙의 조건으로 추가할 수 있습니다. 객체 관리자를 사용하여 보안 영역을 생성하는 방법에 대한 자세한 내용은 3-38페이지의 보안 영역 작업을/를 참조하십시오.

현재 가상 라우터에 할당된 영역 또는 독립형 인터페이스를 NAT 규칙에 추가할 수 있습니다. 적용되지 않은 디바이스 컨피그레이션의 디바이스가 있는 경우 Zones 페이지의 사용 가능한 영역 목록 상단에 경고 아이콘( )이 표시되어, 적용된 영역 및 인터페이스만 표시된다고 알려줍니다. 인터페이스를 숨기거나 보려면 영역 옆에 있는 화살표 아이콘( )을 클릭하여 영역을 확장하거나 축소할 수 있습니다.

인터페이스가 클러스터링된 디바이스에 있는 경우 사용 가능한 영역 목록에 해당 인터페이스에서 나온 추가 브랜치가 표시되며, 클러스터의 다른 인터페이스는 클러스터의 활성 디바이스에 있는 기본 인터페이스의 하위 인터페이스로 표시됩니다. 인터페이스를 숨기거나 보려면 화살표 아이콘( )을 클릭하여 클러스터링된 디바이스 인터페이스를 확장하거나 축소할 수 있습니다.

참고 비활성화된 인터페이스가 있는 정책을 저장 및 적용할 수 있지만, 인터페이스가 활성화될 때까지 이러한 규칙은 변환을 제공할 수 없습니다.

오른쪽에 있는 두 개의 목록은 NAT 규칙으로 매칭하기 위해 사용되는 소스 및 목적지 영역입니다. 규칙에 이미 구성된 값이 있는 경우 규칙을 수정하면 이러한 목록에 기존 값이 표시됩니다. 소스 영역 목록이 비어 있으면 규칙은 모든 영역 또는 인터페이스에서 *오는* 트래픽을 매칭합니다. 목적지 영역 목록이 비어 있으면 규칙은 모든 영역 또는 인터페이스로 *가는* 트래픽을 매칭합니다.

시스템은 대상 디바이스에서 트리거되지 않는 영역 조합이 포함된 규칙에 대해 경고를 표시합니다.

참고 이러한 영역 조합이 포함된 정책을 저장 및 적용할 수 있지만, 규칙이 변환을 제공하지는 않습니다.

영역의 항목을 선택하여 또는 독립형 인터페이스를 선택하여 개별 인터페이스를 추가할 수 있습니다. 인터페이스가 할당된 영역이 아직 소스 영역 또는 목적지 영역 목록에 추가되지 않은 경우에만 영역의 인터페이스를 추가할 수 있습니다. 개별적으로 선택된 이러한 인터페이스는 제거하거나 다른 영역에 추가하더라도 영역에 대한 변경 사항의 영향을 받지 않습니다. 인터페이스가 클러스터의 기본 멤버이고 동적 규칙을 구성 중인 경우, 소스 영역 또는 목적지 영역 목록에 기본 인터페이스만 추가할 수 있습니다. 고정 규칙의 경우 개별 클러스터 멤버 인터페이스를 소스 영역 목록에 추가할 수 있습니다. 하위 인터페이스가 추가되지 않은 경우에만 목록에 기본 클러스터 인터페이스를 추가할 수 있으며, 기본 인터페이스가 추가되지 않은 경우에만 개별 클러스터 인터페이스를 추가할 수 있습니다.

영역을 추가하는 경우 규칙은 해당 영역과 관련된 모든 인터페이스를 사용합니다. 영역에서 인터페이스를 추가하거나 제거하면, 인터페이스가 상주하는 디바이스에 디바이스 컨피그레이션이 다시 적용될 때까지 규칙은 영역의 업데이트된 버전을 사용하지 않습니다.

참고 고정 NAT 규칙에서는 소스 영역만 추가할 수 있습니다. 동적 NAT 규칙에서는 소스 영역과 목적지 영역을 모두 추가할 수 있습니다.

다음 절차에서는 NAT 규칙을 추가 또는 수정하는 동안 소스 및 목적지 영역 조건을 추가하는 방법에 대해 설명합니다. 자세한 내용은 11-19페이지의 NAT 규칙 조건 및 조건 원리 이해을/를 참조하십시오.

영역 조건을 NAT 규칙에 추가하려면

액세스: Admin/Network Admin

1단계 규칙 Edit 페이지에서 **Zones** 탭을 선택합니다.

Zones 페이지가 나타납니다.

2단계 선택적으로, **Available Zones** 목록 위에 있는 **Search by name** 프롬프트를 클릭한 다음 이름이나 값을 입력합니다.

입력할 때 목록이 업데이트되면서 일치하는 조건을 표시합니다. 자세한 내용은 11-22페이지의 NAT 규칙 조건 목록 검색을/를 참조하십시오.

3단계 **Available Zones** 목록에서 영역 또는 인터페이스를 클릭합니다. Shift 및 Ctrl 키를 사용하여 여러 조건을 선택하거나 마우스 오른쪽 버튼을 클릭하고 **Select All**을 클릭합니다.

선택한 조건이 강조 표시됩니다.

4단계 다음 옵션을 이용할 수 있습니다.

- 소스 영역 기준으로 트래픽을 매칭하려면 **Add to Source**를 클릭합니다.
- 목적지 영역 기준으로 트래픽을 매칭하려면 **Add to Destination**을 클릭합니다.

선택적으로, 선택한 조건을 **Source Zones** 또는 **Destination Zones** 목록으로 끌어서 놓을 수 있습니다.

선택한 조건이 추가됩니다. 비활성화된 인터페이스를 NAT 규칙에 추가할 수 있지만, 규칙이 변환을 제공하지는 않습니다.

참고 소스 영역은 고정 NAT 규칙에만 추가할 수 있습니다.

5단계 규칙을 저장하거나 계속 수정합니다.

변경 사항을 적용하려면 NAT 정책을 적용해야 합니다. 11-14페이지의 NAT 정책 적용을/를 참조하십시오.

소스 네트워크 조건을 동적 NAT 규칙에 추가

라이센스: 모두

패킷에 대한 소스 IP 주소의 매칭 값 및 변환 값을 구성합니다. 원래 소스 네트워크가 구성되지 않은 경우 소스 IP 주소는 동적 NAT 규칙을 매칭합니다. 고정 NAT 규칙에 대한 소스 네트워크를 구성할 수 없습니다. 패킷이 NAT 규칙과 일치하는 경우 시스템은 변환된 소스 네트워크의 값을 사용하여 소스 IP 주소에 대한 새 값을 할당합니다. 동적 규칙의 경우, 변환된 소스 네트워크를 하나 이상의 값으로 구성해야 합니다.

주의 네트워크 객체 또는 객체 그룹이 NAT 규칙에 의해 사용되고 있는데 객체 또는 그룹을 변경하거나 삭제한 경우, 규칙이 무효화될 수 있습니다.

다음과 같은 종류의 소스 네트워크 조건을 동적 NAT 규칙에 추가할 수 있습니다.

- 객체 관리자를 사용하여 생성한 개별 및 그룹 네트워크 객체

  객체 관리자를 사용하여 개별 및 그룹 네트워크 객체를 생성하는 방법에 대한 자세한 내용은 3-4페이지의 네트워크 객체 작업을/를 참조하십시오.

- Source Network 조건 페이지에서 추가한 다음 자신의 규칙과 기타 기존의/앞으로의 규칙에 추가할 수 있는 개별 네트워크 객체

  자세한 내용은 11-23페이지의 NAT 규칙 조건에서 객체 사용을/를 참조하십시오.

- 리터럴 단일 IP 주소, 범위 또는 주소 블록

  자세한 내용은 11-23페이지의 NAT 규칙에 리터럴 조건 추가을/를 참조하십시오.

다음 절차에서는 동적 NAT 규칙을 추가 또는 수정하는 동안 소스 네트워크 조건을 추가하는 방법에 대해 설명합니다. 자세한 내용은 11-19페이지의 NAT 규칙 조건 및 조건 원리 이해을/를 참조하십시오.

네트워크 조건을 동적 NAT 규칙에 추가하려면

액세스: Admin/Network Admin

1단계 규칙 Edit 페이지에서 **Source Networks** 탭을 선택합니다.

Source Network 페이지가 나타납니다.

2단계 선택적으로, **Available Networks** 목록 위에 있는 **Search by name or value** 프롬프트를 클릭한 다음 이름이나 값을 입력합니다.

입력할 때 목록이 업데이트되면서 일치하는 조건을 표시합니다. 자세한 내용은 11-22페이지의 NAT 규칙 조건 목록 검색을/를 참조하십시오.

3단계 **Available Networks** 목록에서 조건을 클릭합니다. Shift 및 Ctrl 키를 사용하여 여러 조건을 선택하거나 마우스 오른쪽 버튼을 클릭하고 **Select All**을 클릭합니다.

선택한 조건이 강조 표시됩니다.

4단계 다음 옵션을 이용할 수 있습니다.

- 원래 소스 네트워크 기준으로 트래픽을 매칭하려면 **Add to Original**을 클릭합니다.
- 변환된 소스 네트워크와 일치하는 트래픽의 변환 값을 지정하려면 **Add to Translated**를 클릭합니다.

선택적으로, 선택한 조건을 **Original Source Network** 또는 **Translated Source Network** 목록으로 끌어서 놓을 수 있습니다.

선택한 조건이 추가됩니다.

5단계 선택적으로, 개별 네트워크 객체를 추가하려면 **Available Networks** 목록 위에 있는 추가 아이콘( )을 클릭합니다.

각 네트워크 객체에 여러 IP 주소, CIDR 블록 및 접두사 길이를 추가할 수 있습니다.

그런 다음 선택적으로, 추가한 객체를 선택할 수 있습니다. 자세한 내용은 3-4페이지의 네트워크 객체 작업 및 11-23페이지의 NAT 규칙 조건에서 객체 사용을/를 참조하십시오.

6단계 선택적으로, **Original Source Network** 또는 **Translated Source Network** 목록 아래의 **Enter an IP address** 프롬프트를 클릭한 다음 IP 주소, 범위 또는 주소 블록을 입력하고 **Add**를 클릭합니다.

하한 IP 주소-상한 IP 주소 형식으로 범위를 추가합니다. 예: `179.13.1.1-179.13.1.10`.

목록이 업데이트되어 항목이 표시됩니다. 자세한 내용은 11-23페이지의 NAT 규칙에 리터럴 조건 추가을/를 참조하십시오.

7단계 규칙을 저장하거나 계속 수정합니다.

참고 적용된 정책에서 사용하는 동적 규칙에서 네트워크 조건을 업데이트하면 시스템은 기존의 변환된 주소 풀을 사용하는 네트워크 세션을 삭제합니다.

변경 사항을 적용하려면 NAT 정책을 적용해야 합니다. 11-14페이지의 NAT 정책 적용을/를 참조하십시오.

목적지 네트워크 조건을 NAT 규칙에 추가

라이센스: 모두

패킷에 대한 목적지 IP 주소의 매칭 값 및 변환 값을 구성합니다. 동적 NAT 규칙에 대한 변환된 목적지 네트워크를 구성할 수 없습니다.

고정 NAT 규칙은 일대일 변환이므로 **Available Networks** 목록에는 단일 IP 주소만 포함하는 네트워크 객체 및 그룹만 포함됩니다. 고정 변환의 경우, 단일 객체 또는 리터럴 값만 **Original Destination Network** 또는 **Translated Destination Network** 목록 모두에 추가할 수 있습니다.

주의 네트워크 객체 또는 객체 그룹이 NAT 규칙에 의해 사용되고 있는데 객체 또는 그룹을 변경하거나 삭제한 경우, 규칙이 무효화될 수 있습니다.

다음과 같은 종류의 목적지 네트워크 조건을 NAT 규칙에 추가할 수 있습니다.

- 객체 관리자를 사용하여 생성한 개별 및 그룹 네트워크 객체

  객체 관리자를 사용하여 개별 및 그룹 네트워크 객체를 생성하는 방법에 대한 자세한 내용은 3-4페이지의 네트워크 객체 작업을/를 참조하십시오.

- Destination Network 조건 페이지에서 추가한 다음 자신의 규칙과 기타 기존의/앞으로의 규칙에 추가할 수 있는 개별 네트워크 객체

  자세한 내용은 11-23페이지의 NAT 규칙 조건에서 객체 사용을/를 참조하십시오.

- 리터럴 단일 IP 주소, 범위 또는 주소 블록

  고정 NAT 규칙의 경우 목록에 아직 값이 없는 경우에 한해 서브넷 마스크 `/32`의 CIDR만 추가할 수 있습니다.

  자세한 내용은 11-23페이지의 NAT 규칙에 리터럴 조건 추가을/를 참조하십시오.

다음 절차에서는 NAT 규칙을 추가 또는 수정하는 동안 목적지 네트워크 조건을 추가하는 방법에 대해 설명합니다. 자세한 내용은 11-19페이지의 NAT 규칙 조건 및 조건 원리 이해을/를 참조하십시오.

목적지 네트워크 조건을 NAT 규칙에 추가하려면

액세스: Admin/Network Admin

1단계 규칙 Edit 페이지에서 **Destination Network** 탭을 선택합니다.

Destination Network 페이지가 나타납니다.

2단계 선택적으로, **Available Networks** 목록 위에 있는 **Search by name or value** 프롬프트를 클릭한 다음 이름이나 값을 입력합니다.

입력할 때 목록이 업데이트되면서 일치하는 조건을 표시합니다. 자세한 내용은 11-22페이지의 NAT 규칙 조건 목록 검색을/를 참조하십시오.

3단계 **Available Networks** 목록에서 조건을 클릭합니다. Shift 및 Ctrl 키를 사용하여 여러 조건을 선택하거나 마우스 오른쪽 버튼을 클릭하고 **Select All**을 클릭합니다.

선택한 조건이 강조 표시됩니다.

4단계 다음 옵션을 이용할 수 있습니다.

- 원래 목적지 네트워크 기준으로 트래픽을 매칭하려면 **Add to Original**을 클릭합니다.
- 변환된 목적지 네트워크와 일치하는 트래픽의 변환 값을 지정하려면 **Add to Translated**를 클릭합니다.

선택적으로, 선택한 조건을 **Original Destination Network** 또는 **Translated Destination Network** 목록으로 끌어서 놓을 수 있습니다.

선택한 조건이 추가됩니다.

5단계 선택적으로, 개별 네트워크 객체를 추가하려면 **Available Networks** 목록 위에 있는 추가 아이콘( )을 클릭합니다.

동적 규칙의 경우, 각 네트워크 객체에 여러 IP 주소, CIDR 블록 및 접두사 길이를 추가할 수 있습니다. 고정 규칙의 경우 단일 IP 주소만 추가할 수 있습니다. 그런 다음 선택적으로, 추가한 객체를 선택할 수 있습니다. 자세한 내용은 3-4페이지의 네트워크 객체 작업 및 11-23페이지의 NAT 규칙 조건에서 객체 사용을/를 참조하십시오.

6단계 선택적으로, **Original Destination Network** 또는 **Translated Destination Network** 목록 아래의 **Enter an IP address** 프롬프트를 클릭한 다음 IP 주소 또는 주소 블록을 입력하고 **Add**를 클릭합니다.

목록이 업데이트되어 항목이 표시됩니다. 자세한 내용은 11-23페이지의 NAT 규칙에 리터럴 조건 추가을/를 참조하십시오.

7단계 규칙을 저장하거나 계속 수정합니다.

참고 적용된 정책에서 사용하는 동적 규칙에서 네트워크 조건을 업데이트하면 시스템은 기존의 변환된 주소 풀을 사용하는 네트워크 세션을 삭제합니다.

변경 사항을 적용하려면 NAT 정책을 적용해야 합니다. 11-14페이지의 NAT 정책 적용을/를 참조하십시오.

NAT 규칙에 포트 조건 추가

라이센스: 모두

원래/변환된 목적지 포트 및 변환용 전송 프로토콜을 기반으로 네트워크 트래픽을 매칭하려면 포트 조건을 규칙에 추가할 수 있습니다. 원래 포트가 구성되지 않은 경우 목적지 포트가 규칙을 매칭합니다. 패킷이 NAT 규칙과 일치하며 변환된 목적지 포트가 구성된 경우 시스템은 포트를 해당 값으로 변환합니다. 동적 규칙의 경우 원래 목적지 포트만 지정할 수 있습니다. 고정 규칙의 경우 변환된 목적지 포트를 정의할 수 있지만, 원래 목적지 포트 객체 또는 리터럴 값과 동일한 프로토콜의 객체만 사용해야 합니다.

시스템은 고정 규칙의 경우 원래 목적지 포트 목록에서, 동적 규칙의 경우 여러 값에서 포트 객체 또는 리터럴 포트의 값을 기준으로 목적지 포트를 매칭합니다.

고정 NAT 규칙은 일대일 변환이므로 **Available Ports** 목록에는 단일 포트만 포함하는 포트 객체 및 그룹만 포함됩니다. 고정 변환의 경우, 단일 객체 또는 리터럴 값만 **Original Port** 또는 **Translated Port** 목록 모두에 추가할 수 있습니다.

동적 규칙의 경우 포트 범위를 추가할 수 있습니다. 예를 들어 원래 목적지 포트를 지정할 때 리터럴 값으로 `1000-1100`을 추가할 수 있습니다.

주의 포트 객체 또는 객체 그룹이 NAT 규칙에 의해 사용되고 있는데 객체 또는 그룹을 변경하거나 삭제한 경우, 규칙이 무효화될 수 있습니다.

다음과 같은 종류의 포트 조건을 NAT 규칙에 추가할 수 있습니다.

- 객체 관리자를 사용하여 생성한 개별 및 그룹 포트 객체

  객체 관리자를 사용하여 개별 및 그룹 포트 객체를 생성하는 방법에 대한 자세한 내용은 3-12 페이지의 포트 객체 작업을/를 참조하십시오.

- Destination Ports 조건 페이지에서 추가한 다음 자신의 규칙과 기타 기존의/앞으로의 규칙에 추가할 수 있는 개별 포트 객체

  자세한 내용은 11-23페이지의 NAT 규칙 조건에서 객체 사용을/를 참조하십시오.

- TCP, UDP 또는 All(TCP 및 UDP) 전송 프로토콜 및 포트로 구성된 리터럴 포트 값

  자세한 내용은 11-23페이지의 NAT 규칙에 리터럴 조건 추가을/를 참조하십시오.

다음 절차에서는 NAT 규칙을 추가 또는 수정하는 동안 포트 조건을 추가하는 방법에 대해 설명합니다. 자세한 내용은 11-19페이지의 NAT 규칙 조건 및 조건 원리 이해을/를 참조하십시오.

목적지 포트 조건을 NAT 규칙에 추가하려면

액세스: Admin/Network Admin

1단계 규칙 Edit 페이지에서 **Destination Port** 탭을 선택합니다.

Destination Port 페이지가 나타납니다.

2단계 선택적으로, **Available Port** 목록 위에 있는 **Search by name or value** 프롬프트를 클릭한 다음 이름이나 값을 입력합니다.

입력할 때 목록이 업데이트되면서 일치하는 조건을 표시합니다. 자세한 내용은 11-22페이지의 NAT 규칙 조건 목록 검색을/를 참조하십시오.

3단계 **Available Port** 목록에서 조건을 클릭합니다. Shift 및 Ctrl 키를 사용하여 여러 조건을 선택하거나 마우스 오른쪽 버튼을 클릭하고 모든 조건을 선택합니다. 최대 50개의 조건을 추가할 수 있습니다.

선택한 조건이 강조 표시됩니다.

4단계 다음 옵션을 이용할 수 있습니다.

- 선택한 포트를 Original Ports 목록에 추가하려면 **Add to Original**을 클릭합니다.
- 선택한 포트를 Translated Ports 목록에 추가하려면 **Add to Translated**를 클릭합니다.
- 사용 가능한 포트를 목록으로 끌어서 놓습니다.

5단계 선택적으로, 개별 포트 객체를 생성하여 추가하려면 **Available Ports** 목록 위에 있는 추가 아이콘( )을 클릭합니다.

추가하는 각 포트 객체에서 단일 포트 또는 포트 범위를 식별할 수 있습니다. 그런 다음 규칙에 대한 조건으로 추가한 객체를 선택할 수 있습니다. 자세한 내용은 11-23페이지의 NAT 규칙 조건에서 객체 사용을/를 참조하십시오.

고정 규칙의 경우 단일 포트가 있는 포트 객체만 사용할 수 있습니다.

6단계 선택적으로, 리터럴 포트를 추가하려면 **Original Port** 또는 **Translated Port** 목록 아래에 있는 **Protocol** 드롭다운 목록에서 항목을 선택합니다.

포트를 입력한 다음 **Add**를 클릭합니다. 0~65535 범위의 포트 번호를 지정할 수 있습니다. 동적 규칙의 경우 단일 포트 또는 범위를 지정할 수 있습니다.

목록이 업데이트되어 선택 항목이 표시됩니다. 자세한 내용은 11-23페이지의 NAT 규칙에 리터럴 조건 추가을/를 참조하십시오.

선택한 조건이 추가됩니다

7단계 규칙을 저장하거나 계속 수정합니다.

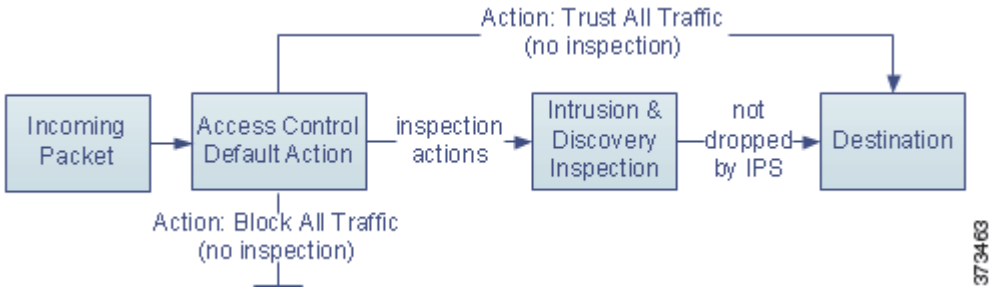
변경 사항을 적용하려면 NAT 정책을 적용해야 합니다. 11-14페이지의 NAT 정책 적용을/를 참조하십시오.

12장

액세스 제어 정책 시작

*액세스 제어 정책*은 시스템이 네트워크의 비 fast-path 트래픽을 처리하는 방식을 결정합니다. 하나 이상의 액세스 제어 정책을 구성한 다음, 하나 이상의 매니지드 디바이스에 이를 적용할 수 있습니다. 각 디바이스에는 현재 적용된 정책이 하나씩 포함될 수 있습니다.

가장 간단한 액세스 제어 정책은 *기본 작업*을 사용하여 모든 트래픽을 처리하도록 대상 디바이스에 지시합니다. 이러한 기본 작업을 설정하여 추가 검사 없이 모든 트래픽을 차단하거나, 침입 및 검색 데이터에 대한 트래픽을 검사할 수 있습니다.



인라인으로 구축된 디바이스만 트래픽의 흐름에 영향을 미칠 수 있습니다. 트래픽을 차단하거나 변경하도록 구성된 액세스 제어 정책을 수동으로 구축된 디바이스에 적용할 경우 예기치 않은 결과가 발생할 수 있습니다. 경우에 따라, 인라인 컨피그레이션을 수동으로 구축된 디바이스에 적용하지 못할 수 있습니다.

이 장에서는 간단한 액세스 제어 정책을 생성하고 적용하는 방법에 대해 설명합니다. 또한 이 장에는 액세스 제어 정책을 관리하는 방법인 수정, 업데이트, 비교 등에 대한 기본적인 정보가 포함되어 있습니다. 자세한 내용은 다음 링크를 참고하십시오.

좀 더 복잡한 액세스 제어 정책은 보안 인텔리전스 데이터를 기반으로 트래픽을 블랙리스트에 추가하고, *액세스 제어 규칙*을 사용하여 네트워크 트래픽 로깅 및 처리를 세부적으로 제어하는 것입니다. 이러한 규칙은 간단하거나 복잡할 수 있으며 여러 조건을 사용하여 트래픽을 매칭하고 검사합니다. 고급 액세스 제어 정책 옵션은 해독, 전처리, 성능 및 기타 일반적인 기본 설정을 제어합니다.

기본적인 액세스 제어 정책을 생성한 후, 이를 해당 구축 환경에 맞추는 방법에 대한 자세한 내용은 다음 장을 참조하십시오.

- 13-1페이지의 보안 인텔리전스 IP 주소 평판 블랙리스트에 추가에서는 최신 평판 인텔리전스를 바탕으로 연결을 블랙리스트(차단)에 즉시 추가하는 방법을 설명합니다.
- 19-1페이지의 트래픽 해독 이해에서는 SSL 정책을 사용하여 검사 없이 암호화된 트래픽을 차단하거나, 선택에 따라 해당 트래픽을 해독한 후 액세스 제어 규칙으로 전달하는 방법에 대해 설명합니다.
- 23-1페이지의 네트워크 분석 및 침입 정책 이해에서는 시스템의 침입 탐지 및 방지 기능의 일부인 네트워크 분석 및 침입 정책으로 패킷을 전처리하고 검사하는 방법을 설명합니다.
- 14-1페이지의 액세스 제어 규칙을 사용하여 트래픽 플로우 조정에서는 액세스 제어 규칙이 어떤 방식을 통해 여러 매니지드 디바이스 전반의 네트워크 트래픽을 처리하는 세부적인 방법을 제공하는지 설명합니다.
- 18-1페이지의 침입 정책 및 파일 정책을 사용하여 트래픽 제어에서는 침입 및 파일 정책이 침입, 금지된 파일, 악성코드를 탐지하고 선택에 따라 이를 차단하여 트래픽이 원하는 대상에 도달할 수 있게 되기 전에 최종 방어선을 제공하는 방법을 설명합니다.

액세스 제어 라이센스 및 역할 요구 사항

방어 센터의 라이센스에 상관없이 액세스 제어 정책을 생성할 수 있지만, 대다수의 기능은 정책을 적용하기 전에 알맞은 라이센스를 활성화해야 합니다. 또한 일부 기능은 특정 모델에서만 사용할 수 있습니다.

이와 더불어, 사용 가능한 액세스 제어 관련 기능 및 작업은 사용자 역할에 따라 달라집니다. 시스템에는 다양한 관리자 및 분석가를 위해 설계된 사전 정의된 사용자 역할이 포함되며, 특수 액세스 권한을 가진 사용자 지정 사용자 역할을 만들 수 있습니다.

자세한 내용은 다음 링크를 참고하십시오.

- 12-2페이지의 액세스 제어를 위한 라이센스 및 모델 요구 사항
- 12-4페이지의 사용자 지정 사용자 역할로 구축 관리

액세스 제어를 위한 라이센스 및 모델 요구 사항

방어 센터의 라이센스에 상관없이 액세스 제어 정책을 생성할 수 있지만, 액세스 제어의 특정 부분으로 인해 정책을 적용하기 전에 대상 디바이스에서 특정 라이센스 기능을 활성화해야 합니다. 또한 일부 기능은 특정 모델에서만 사용할 수 있습니다.

경고 아이콘 및 확인 대화 상자는 구축 시 지원되지 않는 기능을 지정합니다. 자세한 내용을 보려면 경고 아이콘에 마우스 포인터를 올리고 12-21페이지의 액세스 제어 정책 및 규칙 문제 해결을/를 참조하십시오.

다음 표에는 액세스 제어 정책을 적용하기 위한 라이센스 및 어플라이언스 모델이 설명되어 있습니다. Series 2 디바이스에는 대부분의 보호 기능이 자동으로 포함되므로 해당 디바이스에서는 보호을 명시적으로 활성화하지 않아도 됩니다.

표 12-1 액세스 제어에 대한 라이센스 및 모델 요구 사항

액세스 제어 정책 적용을 위해 수행할 작업	라이센스	지원되는 방어 센터	지원되는 장치
영역, 네트워크, VLAN 또는 포트 기반 액세스 제어 수행 리터럴 URL 및 URL 객체를 사용하여 URL 필터링 수행	모든	모든	다음을 제외한 모두 • Series 2 디바이스는 URL 필터링을 수행할 수 없음 • ASA FirePOWER 디바이스는 VLAN 필터링을 수행할 수 없음
SSL 검사 수행, 12-3 페이지의 표 12-2 참조	모든	모두, DC500은 네트워크, 애플리케이션, SSL 관련 제어에 국한되므로 제외	Series 3
위치 데이터(소스 또는 대상 국가/대륙)를 사용하여 액세스 제어 수행	FireSIGHT	DC500을 제외한 모두	Series 3 가상 ASA FirePOWER
침입 탐지 및 방지, 파일 제어 또는 보안 인텔리전스 필터링 수행	보호	모든	모두, Series 2 디바이스는 보안 인텔리전스 필터링을 수행할 수 없으므로 제외
지능형 악성코드 차단(즉, 네트워크 기반 악성코드 탐지 및 차단) 수행	악성코드	DC500을 제외한 모두	Series 2 또는 X-Series를 제외한 모두
사용자 또는 애플리케이션 제어 수행	제어	모두, DC500은 사용자 제어를 수행할 수 없으므로 제외	Series 2 또는 X-Series를 제외한 모두
카테고리 및 평판 데이터를 사용하여 URL 필터링 수행	URL 필터링	DC500을 제외한 모두	Series 2를 제외한 모든 디바이스

다음 표에는 SSL 정책을 호출하여 SSL 검사를 수행하는 액세스 제어 정책을 적용해야 하는 라이센스가 설명되어 있습니다.

표 12-2 SSL 검사를 위한 라이센스 및 모델 요구 사항

SSL 정책 적용을 위해 수행할 작업	라이센스	지원되는 방어 센터	지원되는 장치
영역, 네트워크, VLAN, 포트 또는 SSL 관련 기준을 기반으로 암호화된 트래픽 처리	모든	모든	Series 3
지오로케이션 데이터를 사용하여 암호화된 트래픽 처리	FireSIGHT	DC500을 제외한 모든 방어 센터	Series 3
애플리케이션 또는 사용자 기준을 사용하여 암호화된 트래픽 처리	제어	모두, DC500은 사용자 제어를 수행할 수 없으므로 제외	Series 3
URL 카테고리 및 평판 데이터를 사용하여 암호화된 트래픽 필터링	URL 필터링	DC500을 제외한 모두	Series 3

사용자 지정 사용자 역할로 구축 관리

라이센스: 기능에 따라 다름

61-51페이지의 사용자 지정 사용자 역할 관리에 설명된 대로, 특수 액세스 권한을 가진 사용자 지정 사용자 역할을 만들 수 있습니다. 사용자 지정 사용자 역할은 어떠한 메뉴 기반 및 시스템 권한도 가질 수 있으며 원래 역할을 그대로 유지하거나 사전 정의된 사용자 역할을 기반으로 하여 변경할 수 있습니다. 액세스 제어 관련 기능을 위한 사용자 지정 역할은 사용자가 액세스 제어, 침입, 파일 정책을 보고, 수정하고, 적용할 수 있는지 여부를 결정할 뿐만 아니라 관리자 규칙 또는 루트 규칙 카테고리에서 규칙을 삽입하거나 수정할 수 있는지 여부를 결정합니다.

다음 표에는 FireSIGHT 시스템 사용자가 액세스 제어 기능과 어떻게 상호 작용하는지 볼 수 있는 다섯 가지 사용자 지정 역할의 예시가 나와 있습니다. 이 표에는 각 사용자 지정 역할에 필요한 권한 목록이 사용자 지정 사용자 역할을 만들 때 표시되는 순서대로 나열되어 있습니다.

표 12-3 액세스 제어 사용자 지정 역할 예

사용자 지정 역할 권한	액세스 제어 및 SSL 편집기	침입 및 네트워크 분석 편집기	파일 정책 편집기	정책 적용자(모두)	침입 정책 적용자
액세스 제어	예	아니요	아니요	예	예
ACL(Access Control List)	예	아니요	아니요	예	예
액세스 제어 정책 수정	예	아니요	아니요	아니요	아니요
침입 정책 적용	아니요	아니요	아니요	예	예
액세스 제어 정책 적용	아니요	아니요	아니요	예	아니요
침입(네트워크 분석 권한도 부여)	아니요	예	아니요	아니요	아니요
침입 정책	아니요	예	아니요	아니요	아니요
침입 정책 수정	아니요	예	아니요	아니요	아니요
파일 정책	아니요	아니요	예	아니요	아니요
파일 정책 수정	아니요	아니요	예	아니요	아니요
SSL	예	아니요	아니요	아니요	아니요
SSL 정책 수정	예	아니요	아니요	아니요	아니요
SSL 정책 적용	아니요	아니요	아니요	예	아니요

FireSIGHT 시스템 사용자 계정 역할이 Intrusion Policy 또는 Modify Intrusion Policy로 제한된 경우 네트워크 정책과 침입 정책을 생성 및 수정할 수 있습니다.

시스템에서는 사용자가 전체 액세스 제어 정책을 적용할 수 있는지, 침입 정책만 적용할 수 있는지, 또는 두 가지 모두 적용 불가능한지에 따라 웹 인터페이스를 다르게 렌더링합니다. 예를 들어, 위 표의 침입 정책 적용자는 액세스 제어 정책을 보고 침입 정책을 적용할 수 있으나 두 정책을 수정할 수는 없습니다. 또한 액세스 제어 정책을 적용하거나, 파일 또는 SSL 정책을 보는 것도 할 수 없습니다. 이 경우 웹 인터페이스는 다음과 같습니다.

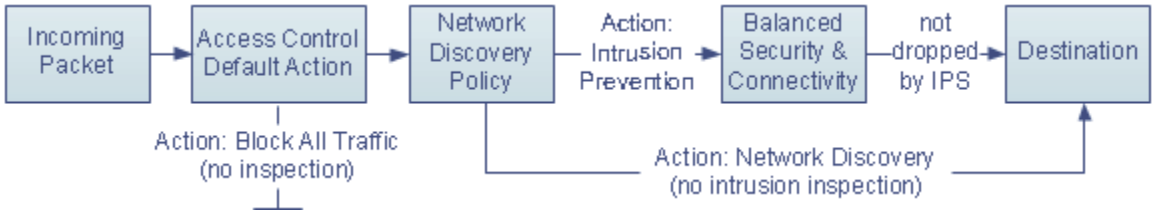
- 수정 아이콘( )이 Access Control Policy 페이지에 표시되지 않습니다.
- 삭제 아이콘( )이 Access Control Policy 페이지에 표시되지 않습니다.
- 빠른 적용 팝업 창에서는 침입 정책만 적용합니다.
- 세부적인 적용 팝업 창에서 액세스 제어 정책 확인란이 비활성화됩니다.

기본 액세스 제어 정책 생성

라이센스: 모든

새 액세스 제어 정책을 생성할 경우 고유한 이름을 부여하고 기본 작업을 지정해야 합니다. 이때 기본 작업은 정책의 대상 디바이스가 모든 비 fast-path 트래픽을 어떤 방식으로 처리할지 결정하며, 나중에 트래픽 흐름에 영향을 미치는 다른 컨피그레이션을 추가할 수 있습니다. 생성 시 정책 대상을 식별할 필요는 없지만 정책을 적용하기 전에 이 단계를 수행해야 합니다.

새 정책을 생성할 경우, 다음 다이어그램에 표시된 것처럼 추가 검사 없이 모든 트래픽을 차단하거나, 침입 및 검색 데이터에 대한 트래픽을 검사하도록 기본 작업을 설정할 수 있습니다.



팁 액세스 제어 정책을 처음 생성할 경우에는 트래픽을 신뢰하는 것을 기본 작업으로 선택할 수 없습니다. 기본적으로 모든 트래픽을 신뢰하려면 정책을 생성한 후 기본 작업을 변경합니다.

Access Control Policy 페이지(**Policies > Access Control**)를 사용하여 정책을 새로 생성하고 기존 액세스 제어 정책을 관리할 수 있습니다. 디바이스를 방어 센터에 등록했는지, 그리고 어떤 방식으로 등록했는지에 따라 두 가지 사전 정의된 액세스 제어 정책 중 하나가 표시되며 디바이스에 미리 적용될 수 있습니다.

- Default Access Control 정책은 추가 검사 없이 모든 트래픽을 차단합니다.
- Default Intrusion Prevention 정책은 모든 트래픽을 허용하지만, Balanced Security and Connectivity Intrusion 정책 및 기본 침입 변수 집합으로 검사를 수행합니다.

이러한 액세스 제어 정책을 사용하고 수정할 수 있습니다. 이러한 기본 정책은 로깅이 활성화되어 있지 않습니다.

액세스 제어 정책을 생성하려면

액세스: Admin/Access Admin/Network Admin

1단계 **Policies > Access Control**을 선택합니다.

Access Control Policy 페이지가 나타납니다.

팁 이 방어 센터에서 기존 정책을 복사하거나 다른 방어 센터에서 정책을 가져올 수도 있습니다. 정책을 복사려면 복사 아이콘( )을 클릭합니다. 정책을 가져오려면 A-1페이지의 컨피그레이션 가져오기 및 내보내기을/를 참조하십시오.

2단계 **New Policy**를 클릭합니다.

New Access Control Policy 팝업 창이 표시됩니다.

3단계 정책에 고유한 **Name**을 지정하고 선택 사항인 **Description**도 입력합니다.

공백과 특수 문자를 비롯한 모든 인쇄 가능 문자를 사용할 수 있으나, 파운드 기호(#), 세미 콜론(;), 중괄호({})는 제외합니다. 이름에는 공백이 아닌 문자를 최소 1개 이상 포함해야 합니다.

4단계 최초 **Default Action**을 지정합니다.

- **Block all traffic**을 선택하면 **Access Control: Block All Traffic** 기본 작업이 포함된 정책이 생성됩니다.
- **Intrusion Prevention**을 선택하면 **Intrusion Prevention: Balanced Security and Connectivity** 기본 작업이 포함된 정책이 생성됩니다.
- **Network Discovery**를 선택하면 **Network Discovery Only** 기본 작업이 포함된 정책이 생성됩니다.

최초 기본 작업을 선택하는 방법 및 나중에 이를 변경하는 방법에 대한 지침을 보려면 12-6페이지의 네트워크 트래픽의 기본 처리 및 검사 설정을/를 참조하십시오.

5단계 정책을 적용할 **Available Devices**를 선택합니다.

Ctrl 및 Shift 키를 사용하여 여러 디바이스를 선택하거나, 마우스 오른쪽 버튼을 클릭하고 **Select All**을 선택합니다. 나타나는 디바이스의 범위를 좁히려면 **Search** 필드에 검색 문자열을 입력합니다. 대상 디바이스 추가를 건너뛸 경우, 나중에 이를 추가하는 방법을 보려면 12-9페이지의 액세스 제어 정책에 대한 대상 디바이스 설정을/를 참조하십시오.

6단계 **Add to Policy**를 클릭하여 선택한 디바이스를 추가합니다.

선택한 객체를 끌어서 놓을 수도 있습니다.

7단계 **Save**를 클릭합니다.

액세스 제어 정책 편집기가 나타납니다. 새 정책 구성에 대한 자세한 내용은 12-11페이지의 액세스 제어 정책 수정을/를 참조하십시오. 정책을 반영하려면 적용해야 합니다. 12-15페이지의 액세스 제어 정책 적용을/를 참조하십시오.

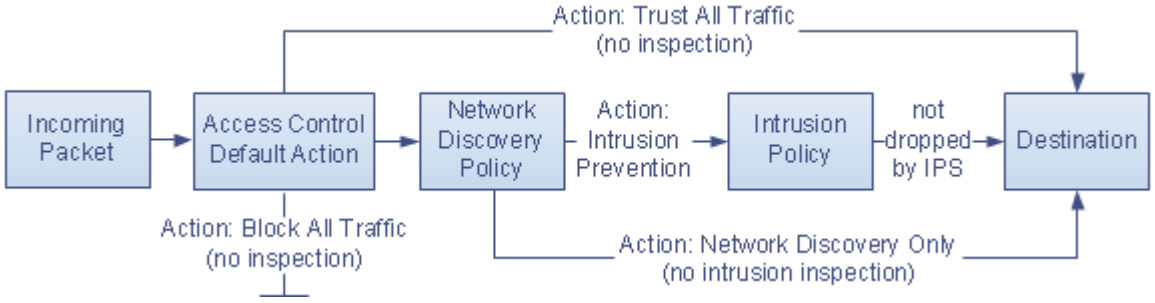
네트워크 트래픽의 기본 처리 및 검사 설정

라이센스: 모든

액세스 제어 정책을 생성할 경우, 기본 작업을 선택해야 합니다. 액세스 제어 정책의 기본 작업은 시스템에서 다음과 같은 트래픽을 처리하는 방식을 결정합니다.

- 보안 인텔리전스에서 블랙리스트에 추가하지 않은 트래픽
- SSL 검사에서 차단되지 않은 트래픽(암호화된 트래픽만 해당)
- 정책의 규칙과 매칭되지 않는 트래픽(트래픽과 매칭되고 로깅(처리 또는 검사는 수행하지 않음)되는 Monitor 규칙은 제외)

따라서 액세스 제어 규칙 또는 보안 인텔리전스 컨피그레이션을 포함하지 않고, 암호화된 트래픽을 처리하는 SSL 정책을 호출하지 않는 액세스 제어 정책을 적용할 경우, 기본 작업에서는 네트워크의 *모든* 트래픽을 어떻게 처리할지 결정합니다. 추가 검사 없이 모든 트래픽을 차단하거나 신뢰할 수 있으며, 침입 및 검색 데이터에 대한 트래픽을 검사할 수 있습니다. 선택 가능한 방법은 아래 다이어그램에 나와 있습니다.

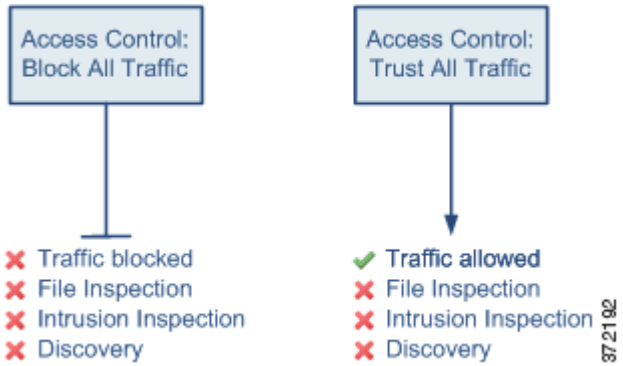


다음 표에는 다양한 기본 작업에서 트래픽을 처리하는 방법, 그리고 각 기본 작업을 통해 처리된 트래픽에 수행할 수 있는 검사 종류가 나열되어 있습니다. 기본 작업을 통해 처리된 트래픽에는 파일 또는 악성코드 검사를 수행할 수 **없습니다**. 자세한 내용은 18-1페이지의 침입 정책 및 파일 정책을 사용하여 트래픽 제어을/를 참조하십시오.

표 12-4 액세스 제어 정책 기본 작업

기본 작업	트래픽에 미치는 영향	검사 종류 및 정책
Access Control: Block All Traffic	추가 검사 없이 차단	없음
Access Control: Trust All Traffic	신뢰(추가 검사 없이 최종 대상까지 도달하도록 허용)	없음
Intrusion Prevention	허용 — 사용자가 지정한 침입 정책에 의해 통과된 경우에 한함(보호 필요)	침입 — 지정된 침입 정책 및 관련 변수 집합 사용 검색 — 네트워크 검색 정책 사용
Network Discovery Only	허용	검색만 수행 — 네트워크 검색 정책 사용

아래 다이어그램에는 **Block All Traffic** 및 **Trust All Traffic** 기본 작업이 나와 있습니다.



아래 다이어그램에는 **Intrusion Prevention** 및 **Network Discovery Only** 기본 작업이 나와 있습니다.

팁 **Network Discovery Only**의 목적은 검색 전용 구축 작업의 성능을 향상하는 것입니다. 침입 탐지 및 방지만 사용하려는 경우 다른 컨피그레이션으로 검색을 비활성화할 수 있습니다. 준수해야 할 기타 지침을 비롯하여 자세한 내용을 보려면 12-19페이지의 IPS 또는 검색 전용 성능 고려 사항을/를 참조하십시오.

액세스 제어 정책을 처음 생성할 경우, 기본 작업을 통해 처리되는 로깅 연결은 기본적으로 비활성화되어 있습니다. 침입 검사를 수행하는 기본 작업을 선택할 경우, 시스템에서는 기본 침입 변수 집합을 사용자가 선택하는 침입 정책과 자동으로 연결합니다. 정책을 생성한 후에는 이러한 옵션은 물론 기본 작업 자체도 변경할 수 있습니다.

액세스 제어 정책의 기본 작업 및 관련 옵션을 변경하려면

액세스: Admin/Access Admin/Network Admin

1단계 **Policies > Access Control**을 선택합니다.

Access Control Policy 페이지가 나타납니다.

2단계 구성할 액세스 제어 정책 옆에 있는 수정 아이콘( )을 클릭합니다.

액세스 제어 정책 편집기가 나타납니다.

3단계 **Default Action**을 선택합니다.

- 모든 트래픽을 차단하려면 **Access Control: Block All Traffic**을 선택합니다.
- 모든 트래픽을 신뢰하려면 **Access Control: Trust All Traffic**을 선택합니다.
- 모든 트래픽을 허용하고 네트워크 검색으로 이를 검사하려면 **Network Discovery Only**를 선택합니다.
- 네트워크 검색 및 침입 정책을 모두 사용하여 모든 트래픽을 검사하려면 **Intrusion Prevention**이라는 레이블로 시작하는 모든 침입 정책을 선택합니다. 침입 정책은 트래픽을 차단할 수 있습니다.

주의 Cisco 담당자의 지침이 없는 한 `Experimental Policy 1`을 사용하지 **마십시오**. Cisco에서는 테스트 목적으로 이 정책을 사용합니다.

4단계 **Intrusion Prevention** 기본 작업을 선택한 경우, 변수 아이콘( )을 클릭하여 선택한 침입 정책과 연결된 변수 집합을 변경합니다.

표시되는 팝업 창에서 새 변수 집합을 선택하고 **OK**를 클릭합니다. 수정 아이콘( )을 클릭하여 새 창에서 선택한 변수 집합을 수정할 수도 있습니다. 변수 집합을 변경하지 않으면 기본 집합이 사용됩니다. 자세한 내용은 3-17페이지의 변수 집합 작업을/를 참조하십시오.

5단계 로깅 아이콘( )을 클릭하여 기본 작업을 통해 처리된 연결의 로깅 옵션을 변경합니다.

기본 작업에 따라 시작, 끝에 또는 시작과 끝 모든 경우에 매칭 연결을 로깅할 수 있습니다. 연결을 방어 센터 데이터베이스, 외부 시스템 로그(syslog) 또는 SNMP 트랩 서버에 로깅할 수 있습니다. 자세한 내용은 38-17페이지의 액세스 제어 기본 작업에 의해 처리되는 연결 로깅을/를 참조하십시오.

액세스 제어 정책에 대한 대상 디바이스 설정

라이센스: 모든

액세스 제어 정책을 적용하려면 우선 정책을 적용할 매니지드 디바이스를 식별해야 합니다. 정책을 생성하는 동안 해당 정책으로 대상을 지정할 디바이스를 식별하거나, 나중에 이를 추가할 수 있습니다.

다음 표에는 대상 디바이스를 관리할 경우 수행할 수 있는 작업이 요약되어 있습니다.

표 12-5 대상 디바이스 관리 작업

목적	가능한 작업
사용 가능한 디바이스 목록 검색	Search 필드의 내부를 클릭한 다음 검색 문자열을 입력합니다. 입력하면 디바이스 목록이 업데이트되어 매칭되는 디바이스 이름이 표시됩니다.
사용 가능한 디바이스에 대한 검색 지우기	검색 필드에서 지우기 아이콘( )을 클릭합니다.
사용 가능한 디바이스를 선택하여 선택한 대상 목록에 추가합니다.	디바이스 이름을 클릭합니다. 여러 디바이스를 선택하려면 Ctrl 및 Shift 키를 사용합니다. 사용 가능한 디바이스를 마우스 오른쪽 버튼으로 클릭하고 **Select All**을 클릭합니다.
선택한 디바이스 추가	**Add to Policy**를 클릭하거나 선택한 디바이스 목록으로 끌어서 놓습니다.
Selected Devices 목록에서 하나의 디바이스 삭제	디바이스 옆의 삭제 아이콘( )을 클릭하거나, 마우스 오른쪽 버튼으로 해당 디바이스를 클릭하고 **Delete**를 선택합니다.
Selected Devices 목록에서 여러 디바이스 삭제	Ctrl 및 Shift 키를 사용하여 여러 디바이스를 선택하고, 마우스 오른쪽 버튼을 클릭하여 선택한 디바이스의 행을 강조 표시한 다음, **Delete Selected**를 클릭합니다.

다른 버전의 시스템을 실행 중인 스태킹된 디바이스는 대상으로 지정할 수 없습니다(예: 디바이스 중 하나의 업그레이드가 실패할 경우). 디바이스 스택은 대상으로 지정할 수 있으나, 스택 내의 개별 디바이스는 지정할 수 없습니다. 자세한 내용은 4-43페이지의 스태킹된 디바이스 관리을/를 참조하십시오.

액세스 제어 정책에서 대상 디바이스를 관리하려면

액세스: Admin/Access Admin/Network Admin

1단계 **Policies > Access Control**을 선택합니다.

Access Control Policy 페이지가 나타납니다.

2단계 구성할 액세스 제어 정책 옆에 있는 수정 아이콘()을 클릭합니다.

액세스 제어 정책 편집기가 나타납니다.

3단계 디바이스 대상 링크를 클릭한 다음 **Manage Targets**를 클릭합니다.

Manage Device Targets 팝업 창이 표시됩니다.

4단계 대상 목록을 작성합니다.

12-9 페이지의 표 12-5에 요약된 작업을 사용합니다.

5단계 **OK**를 클릭합니다.

컨피그레이션이 정책이 추가되고 액세스 제어 정책 편집기가 표시됩니다.

액세스 제어 정책 관리

라이센스: 모든

Access Control Policy 페이지(**Policies > Access Control**)에서 적절한 경우 다음 정보와 함께 현재 사용자 지정 액세스 제어 정책을 볼 수 있습니다.

- 각 액세스 제어 정책을 사용하여 트래픽을 검사하는 디바이스의 수(정책이 일부 대상에만 적용되었는지 또는 해당 정책으로 현재 대상화되지 않은 디바이스에 정책이 적용되었는지에 대한 정보도 포함)
- 각 정책의 기한이 지난 대상 디바이스의 수(각 정책을 현재 수정 중인 사용자(있는 경우)에 대한 정보도 포함)

사용자가 생성하는 사용자 지정 정책 외에도, 시스템에서는 Default Access Control, Default Intrusion Prevention, Default Network Discovery라는 세 가지 사용자 지정 정책을 제공할 수 있습니다. 시스템은 초기 컨피그레이션 과정에서 선택한 디바이스의 탐지 모드에 따라, 처음 디바이스를 등록할 때 이러한 정책을 생성합니다. 이러한 시스템 제공 사용자 지정 정책을 수정 및 사용할 수 있습니다. 디바이스의 탐지 모드는 나중에 변경할 수 있는 설정이 아니며 시스템이 디바이스의 초기 컨피그레이션을 맞춤 설정하는 데 도움이 되도록 설정 과정에서 선택하는 옵션에 불과합니다.

Access Control Policy 페이지에서는 다음 표에 나와 있는 작업을 수행할 수 있습니다.

표 12-6 액세스 제어 정책 관리 작업

목적	가능한 작업	참조
새 액세스 제어 정책 생성	**New Policy**를 클릭합니다.	12-5페이지의 기본 액세스 제어 정책 생성
기존 액세스 제어 정책 수정	수정 아이콘()을 클릭합니다.	12-11페이지의 액세스 제어 정책 수정
매니지드 디바이스에 대한 액세스 제어 정책 다시 적용	적용 아이콘()을 클릭합니다.	12-15페이지의 액세스 제어 정책 적용

표 12-6 액세스 제어 정책 관리 작업(계속)

목적	가능한 작업	참조
액세스 제어 정책을 내보내기하여 다른 방어 센터에서 가져오기	내보내기 아이콘( )을 클릭합니다.	A-2페이지의 컨피그레이션 내보내기
액세스 제어 정책의 현재 컨피그레이션 설정이 나열된 PDF 보고서 보기	보고서 아이콘( )을 클릭합니다.	12-25페이지의 현재 액세스 제어 설정에 대한 보고서 생성
액세스 제어 정책 비교	**Compare Policies**를 클릭합니다.	12-26페이지의 액세스 제어 정책 비교
액세스 제어 정책 삭제	삭제 아이콘( )을 클릭한 다음 정책을 삭제할 것임을 확인합니다. 적용된 액세스 제어 정책 또는 현재 적용 중인 액세스 제어 정책은 삭제할 수 없습니다.	

액세스 제어 정책 수정

라이센스: 모든

새 액세스 제어 정책을 처음 생성할 경우, Rules 탭에 중점을 둔 액세스 제어 정책 편집기가 표시됩니다. 다음 그래픽에는 새로 생성된 정책이 나와 있습니다. 새 정책에는 규칙이나 다른 컨피그레이션이 아직 없으므로, 기본 작업이 *모든* 트래픽을 처리합니다. 이 경우, 기본 작업은 암호화되지 않은 트래픽이 최종 대상에 도달하는 것을 허용하기 전에 시스템에서 제공한 Balanced Security and Connectivity Intrusion 정책을 사용하여 해당 트래픽을 검사합니다. 기본적으로, 시스템은 암호화된 페이로드에 대해서는 파일 및 침입 검사를 사용하지 않습니다.

액세스 제어 정책 편집기를 사용하여 규칙을 추가 및 구성하고, 정책을 사용할 디바이스를 지정하는 등의 작업을 수행할 수 있습니다. 다음 목록에서는 변경할 수 있는 정책 컨피그레이션에 대한 정보를 제공합니다.

Name and Description

정책의 이름 및 설명을 변경하려면 해당 필드를 클릭하고 새 이름 또는 설명을 입력합니다.

Targets

액세스 제어 정책을 적용하려면 우선 Targets 탭을 사용하여 정책을 적용할 디바이스 그룹을 비롯한 매니지드 디바이스를 확인합니다. 자세한 내용은 12-9페이지의 액세스 제어 정책에 대한 대상 디바이스 설정을/를 참조하십시오.

Security Intelligence

보안 인텔리전스는 악의적인 인터넷 콘텐츠를 차단하는 1차적인 방어선입니다. 이 기능을 사용하면 최신 평판 인텔리전스를 기준으로 연결을 블랙리스트에 즉시 추가(차단)할 수 있습니다. 중요한 리소스에 지속적으로 액세스할 수 있도록 보장하려면 사용자 지정 화이트리스트로 블랙리스트를 재정의할 수 있습니다. 이러한 트래픽 필터링은 다른 정책 기반 검사, 분석 또는 트래픽 처리(규칙 및 기본 작업 포함)가 발생하기 **전에** 이루어집니다. 자세한 내용은 13-1페이지의 보안 인텔리전스 IP 주소 평판 블랙리스트에 추가을/를 참조하십시오.

Rules

규칙은 네트워크 트래픽 처리를 위한 세부적인 방법을 제공합니다. 액세스 제어 정책의 규칙은 번호가 1부터 시작합니다. 시스템은 오름차순 규칙 번호에 따라 하향식 순서로 트래픽이 액세스 제어 규칙과 일치하는지를 확인합니다.

대부분의 경우, 시스템은 *모든* 규칙의 조건이 트래픽과 매칭되는 *첫 번째* 액세스 제어 규칙에 따라 네트워크 트래픽을 처리합니다. 이러한 조건에는 보안 영역, 네트워크 또는 지리적 위치, VLAN, 포트, 애플리케이션, 요청 URL 또는 사용자가 포함됩니다. 조건은 단순하거나 복잡할 수 있으며, 조건의 사용은 특정 라이센스 및 어플라이언스 모델에 따라 달라지는 경우가 많습니다.

Rules 탭을 사용하여 규칙을 추가, 분류, 활성화, 비활성화, 필터링하고 관리할 수 있습니다. 자세한 내용은 14-1페이지의 액세스 제어 규칙을 사용하여 트래픽 플로우 조정을/를 참조하십시오.

Default Action

기본 작업은 시스템이 보안 인텔리전스에 의해 블랙리스트에 추가되지 않고, 액세스 제어 규칙과 매칭되지 않는 트래픽을 어떻게 처리할지 결정합니다. 기본 작업을 사용하면 추가 검사 없이 모든 트래픽을 차단하거나 신뢰할 수 있으며, 침입 및 검색 데이터에 대한 트래픽을 검사할 수 있습니다. 또한 사용자 지정 변수 집합을 만든 경우 이를 선택할 수 있으며, 기본 작업에 의해 처리되는 연결의 로깅을 활성화하거나 비활성화할 수 있습니다.

자세한 내용은 12-6페이지의 네트워크 트래픽의 기본 처리 및 검사 설정 및 38-15페이지의 액세스 제어 처리 기반 연결 로깅을/를 참조하십시오.

HTTP Responses

시스템이 사용자의 웹 사이트 요청을 차단할 경우 브라우저에서 사용자에게 표시되는 내용을 지정할 수 있습니다. 시스템에서 제공하는 일반적인 응답 페이지를 표시하거나, 사용자 지정 HTML을 입력합니다. 또한 사용자에게 경고 메시지를 안내하는 것은 물론, 버튼을 클릭하여 페이지를 계속 진행하거나 새로고침으로써 원래 요청한 사이트를 로드할 수 있는 페이지를 표시할 수도 있습니다. 자세한 내용은 16-17페이지의 차단된 URL에 대한 사용자 지정 웹 페이지 표시을/를 참조하십시오.

Advanced Access Control Options

고급 액세스 제어 정책 설정은 일반적으로 수정이 거의 필요하지 않습니다. 기본 설정은 대부분의 구축에 적합합니다. 수정할 수 있는 고급 설정은 다음과 같습니다.

- 사용자가 요청한 각 URL에 대한 방어 센터 데이터베이스에 저장하는 문자 수(38-18페이지의 연결에서 탐지된 URL 로깅 참조)
- 사용자가 최초 차단을 우회한 이후에 관리자가 웹 사이트를 다시 차단하기 전까지 소요되는 시간(16-16페이지의 차단된 웹 사이트에 대한 사용자 우회 시간 초과 설정 참조)
- SSL(Secure Socket Layer) 또는 TLS(Transport Layer Security)로 암호화된 애플리케이션 레이어 프로토콜 트래픽을 모니터링, 해독, 차단하거나 허용하는 SSL 정책(20-9페이지의 액세스 제어를 사용하여 해독 설정 적용 참조)
- 정책을 적용하는 동안 트래픽 검사 허용 또는 보안 연결을 위해 트래픽 검사 비활성화(12-15페이지의 액세스 제어 정책 적용 참조)
- 네트워크, 영역, VLAN에 대한 많은 전처리 옵션을 맞춤화하고 기본 침입 검사 동작을 설정할 수 있는 네트워크 분석 및 침입 정책 설정(25-1페이지의 트래픽 전처리 맞춤화 참조)
- 액세스 제어 정책을 적용하는 모든 네트워크, 영역, VLAN에 전역으로 적용되는 고급 전송 및 네트워크 프리프로세서 설정(29-2페이지의 고급 Transport/Network 설정 구성 참조)
- 네트워크의 호스트 운영 체제를 기준으로 수동 구축에서 패킷 프래그먼트 및 TCP 스트림의 재결합을 향상하는 적응형 프로필(30-1페이지의 수동 구축 시 전처리 튜닝 참조)
- 침입 검사, 파일 제어, 파일 스토리지, 동적 분석, 지능형 악성코드 차단을 위한 성능 옵션(18-8페이지의 침입 방지 성능 조정 및 18-20페이지의 파일 및 악성코드 검사 성능과 저장 조정 참조)

액세스 제어 정책을 수정할 경우, 저장되지 않은 변경 사항이 있음을 알리는 메시지가 표시됩니다. 변경 사항을 유지하려면 정책 편집기를 종료하기 전에 정책을 저장해야 합니다. 변경 사항을 저장하기 전에 정책 편집기를 종료하려고 할 경우, 저장되지 않은 변경 사항이 있다는 경고가 표시됩니다. 이 경우 변경 사항을 취소하고 정책을 종료하거나, 정책 편집기로 돌아갈 수 있습니다.

세션의 개인 정보를 보호하기 위해, 정책 편집기에서 60분 동안 아무런 작업을 수행하지 않으면 정책의 변경 사항이 취소되며 Access Control Policy 페이지로 되돌아갑니다. 작업이 없는 상태로 30분이 경과하면 변경 사항이 취소되기 전까지 몇 분이 남았는지 알려 주는 메시지가 표시되며 이는 주기적으로 업데이트됩니다. 페이지에서 작업을 수행하면 이러한 타이머가 사라집니다.

두 개의 브라우저 창에서 동일한 정책을 편집하려고 할 경우, 새 창에서 편집을 다시 시작할지, 원래 창의 변경 사항을 취소하고 새 창에서 편집을 계속할지, 또는 두 번째 창을 취소하고 정책 편집기로 돌아갈지 묻는 메시지가 표시됩니다.

여러 사용자가 동일한 정책을 동시에 편집할 경우, 저장되지 않은 변경 사항이 있는 다른 사용자를 확인하는 메시지가 각 정책 편집기에 표시됩니다. 사용자가 변경 사항을 저장하려고 할 경우 해당 변경 사항이 다른 사용자의 변경 사항을 덮어쓰게 된다는 경고가 표시됩니다. 여러 사용자가 동일한 정책을 저장하면 최종 저장된 변경 사항이 유지됩니다.

액세스 제어 정책을 수정하려면

액세스: Admin/Access Admin/Network Admin

1단계 **Policies > Access Control**을 선택합니다.

Access Control Policy 페이지가 나타납니다.

2단계 구성할 액세스 제어 정책 옆에 있는 수정 아이콘()을 클릭합니다.

액세스 제어 정책 편집기가 나타납니다.

3단계 정책을 수정합니다. 위에 요약된 작업 중 하나를 수행합니다.

4단계 컨피그레이션을 저장하거나 취소합니다.

- 변경 사항을 저장하고 계속 수정하려면 **Save**를 클릭합니다.
- 변경 사항을 저장하고 정책을 적용하려면 **Save and Apply**를 클릭합니다. 12-15페이지의 액세스 제어 정책 적용을/를 참조하십시오.
- 변경 사항을 취소하려면 **Cancel**을 클릭하고 메시지가 표시되면 **OK**를 클릭합니다.

기한이 지난 정책 경고 이해

라이센스: 모든

Access Control Policy 페이지(**Policies > Access Control**)에서 기한이 지난 정책은 빨간색 상태 텍스트로 표시되며, 이는 정책 업데이트가 필요한 대상 디바이스의 수가 얼마인지 나타냅니다.

거의 모든 경우, 액세스 제어 정책을 변경할 때마다 해당 정책을 다시 적용해야 변경 사항이 구현됩니다. 액세스 제어 정책이 다른 정책을 호출하거나 다른 컨피그레이션에 의존할 경우, 이러한 항목을 변경할 경우 액세스 제어 정책을 다시 적용해야 합니다(또는 침입 정책 변경 사항의 경우에는 침입 정책만 다시 적용할 수 있음).

정책을 다시 적용해야 하는 컨피그레이션 변경 사항은 다음과 같습니다.

- 액세스 제어 정책 자체를 수정하는 경우: 액세스 제어 규칙, 기본 작업, 정책 대상, 보안 인텔리전스 필터링, NAP 규칙을 포함한 고급 옵션 등의 모든 변경 사항
- 액세스 제어 정책으로 호출되는 정책을 변경하는 경우: SSL 정책, 네트워크 분석 정책, 침입 정책, 파일 정책
- 액세스 제어 정책에서 사용된 재사용 가능한 객체나 컨피그레이션 또는 해당 정책으로 호출되는 정책을 변경한 경우: 네트워크, 포트, VLAN 태그, URL, 위치 객체, 보안 인텔리전스 목록 및 피드, 애플리케이션 필터 또는 탐지기, 침입 정책 변수 집합, 파일 목록, 해독 관련 객체, 보안 영역 등
- 시스템 소프트웨어, 침입 규칙, 취약성 데이터베이스(VDB)를 업데이트하는 경우

웹 인터페이스의 여러 위치에서 이러한 컨피그레이션의 일부를 변경할 수 있습니다. 예를 들어, 객체 관리자(**Objects > Object Management**)를 사용하여 보안 영역을 수정할 수 있으나, 디바이스의 컨피그레이션(**Devices > Device Management**)에서 인터페이스 유형을 수정하는 경우에도 영역을 변경할 수 있으며 정책을 다시 적용해야 합니다.

다음과 같은 업데이트의 경우 정책을 다시 적용할 필요가 **없습니다**.

- 보안 인텔리전스 피드에 대한 자동 업데이트 및 컨텍스트 메뉴를 사용하여 보안 인텔리전스 블랙리스트 또는 화이트리스트에 추가
- URL 필터링 데이터에 대한 자동 업데이트
- 예약된 위치 데이터베이스(GeoDB) 업데이트

액세스 제어 또는 침입 정책의 기한이 지난 이유를 확인하려면 비교 뷰어를 사용합니다.

액세스 제어 정책의 기한이 지난 이유를 확인하려면

액세스: Admin/Security Approver

1단계 **Policies > Access Control**을 선택합니다.

Access Control Policy 페이지가 나타납니다. 기한이 지난 정책은 빨간색 상태 텍스트로 표시되며, 이는 정책 업데이트가 필요한 대상 디바이스의 수가 얼마인지 나타냅니다.

2단계 기한이 지난 정책의 정책 상태를 클릭합니다.

자세한 Apply Access Control Policy 팝업 창이 표시됩니다.

3단계 관심이 있는 변경된 구성 요소 옆에 있는 **Out-of-date**를 클릭합니다.

정책 비교 보고서가 새 창에 표시됩니다. 자세한 내용은 12-26페이지의 액세스 제어 정책 비교 및 31-10페이지의 두 가지 침입 정책 또는 개정 비교을/를 참조하십시오.

4단계 선택에 따라 정책을 다시 적용합니다.

다음 섹션 액세스 제어 정책 적용을 참조합니다.

액세스 제어 정책 적용

라이센스: 모든

액세스 제어 정책을 변경한 후, 디바이스에서 모니터링하는 네트워크에 변경 사항을 구현하려면 하나 이상의 대상 디바이스에 정책을 적용해야 합니다. 액세스 제어 정책과 관련 침입 정책을 얼마든지 조합하여 적용할 수 있으나, 액세스 제어 정책을 적용하면 모든 관련 SSL, 네트워크 분석, 파일 정책이 자동으로 적용됩니다. 이러한 정책은 개별적으로 적용할 수 없습니다.

주의 고급 탭에서 **Inspect Traffic During Policy Apply** 옵션을 선택한 상태로 둘 경우, 정책을 적용하는 동안 연결을 잠깐 중단하여 검사되지 않은 트래픽의 통과를 허용하지 않습니다. 트래픽 검사보다 연결이 더 중요하다고 판단될 경우, **Inspect Traffic During Policy Apply** 옵션의 선택을 취소하면 검사되지 않은 트래픽을 연결 중단 없이 허용할 수 있습니다. 3D7010, 3D7020, 3D7030 매니지드 디바이스에서 액세스 제어 정책을 적용할 경우 5분 정도 소요될 수 있습니다. 불편을 최소화하려면 창을 변경하는 동안 액세스 제어 정책을 적용하거나 **Inspect Traffic During Policy Apply** 옵션을 선택한 상태로 둡니다.

트래픽 중단은 Snort® 프로세스가 다시 시작될 때 발생합니다. 이러한 예로는 방어 센터 업그레이드 후 Snort의 새 버전을 매니지드 디바이스에 푸시하는 액세스 제어 정책을 적용할 경우, 공유 객체 규칙을 포함한 규칙을 가져온 후 정책을 처음 적용할 경우, 그리고 간혹 VDB 업데이트를 설치한 경우 등을 들 수 있습니다. 고급 탭에서 **Inspect Traffic During Policy Apply**를 선택한 경우, 시스템은 정책을 적용하는 동안 트래픽을 계속 검사합니다.

팁 인라인으로 구축된 Cisco NGIPS for Blue Coat X-Series를 사용 중이고 로드 밸런싱 및 이중화를 위해 다중 VAP 그룹을 구성할 경우, 디바이스가 다시 시작되고 복구되기 전까지 로드 밸런싱된 목록에서 영향을 받은 VAP를 제거하면 처리가 일시 중지되는 것을 방지할 수 있습니다.

인라인으로 구축된 디바이스만 트래픽의 흐름에 영향을 미칠 수 있습니다. 트래픽을 차단하거나 변경하도록 구성된 액세스 제어 정책을 수동으로 구축된 디바이스에 적용할 경우 예기치 않은 결과가 발생할 수 있습니다. 예를 들어, 차단된 연결은 수동 구축에서 실제로 차단되지 않으므로 시스템에서는 각 차단된 연결에 대해 여러 개의 beginning-of-connection 이벤트를 보고할 수 있습니다.

경우에 따라 시스템에서는 탭 모드의 인라인 디바이스를 비롯하여 수동으로 구축된 디바이스에 인라인 컨피그레이션을 적용하지 못하도록 할 수 있습니다. 이를테면 수동 구축을 수행할 경우 암호화된 트래픽을 차단하거나, 해독된 트래픽을 다시 로그인하도록 구성된 SSL 정책을 참조하는 액세스 제어 정책을 적용할 수 있습니다. 또한 수동 구축은 단명 Diffie-Hellman(DHE) 또는 타원 곡선 Diffie-Hellman(ECDHE) 암호 그룹으로 암호화된 트래픽의 해독을 지원하지 않습니다.

액세스 제어 정책을 적용할 경우 다음과 같은 추가적인 주의 사항을 숙지하십시오.

- 일부 기능을 사용하려면 특정 라이센스, 시스템의 최소 버전 또는 특정 디바이스 모델이 필요합니다. 매니지드 디바이스에서 실행 중인 시스템의 버전에 대한 자세한 내용은 12-2페이지의 액세스 제어를 위한 라이센스 및 모델 요구 사항 및 릴리스 정보를 참조하십시오. 최근 적용된 디바이스 컨피그레이션을 통해 활성화된 라이센스가 액세스 제어 정책에 필요한 경우, 시스템에서는 디바이스 컨피그레이션의 적용이 완료될 때까지 액세스 제어 정책 적용을 대기열에 둡니다.
- 다른 버전의 시스템을 실행 중인 스택 디바이스에는 액세스 제어 정책을 적용할 수 없습니다(예: 디바이스 중 하나에서 업그레이드가 실패한 경우).
- 액세스 제어 정책을 적용할 경우, 시스템에서는 모든 규칙을 함께 평가하며, 대상 디바이스가 네트워크 트래픽을 평가하는 데 사용하는 확장된 조건 집합을 생성합니다. 대상 디바이스에서 지원되는 최대 액세스 제어 규칙 또는 침입 정책의 수를 초과했다는 경고 메시지가 팝업 창에 표시될 수 있습니다. 이러한 최대값은 여러 요인(예: 물리적 메모리)의 개수 및 디바이스의 프로세서 개수에 따라 달라집니다. . 컴퓨팅 리소스가 적은 디바이스의 경우, 제한된 메모리로 인해 전체 액세스 제어 정책에 걸쳐 침입 정책을 3개만 선택해야 할 수 있습니다. 자세한 내용은 12-22페이지의 규칙 간소화로 성능 향상을/를 참조하십시오.
- 애플리케이션 제어를 수행할 경우, 액세스 제어 또는 SSL 규칙의 조건으로 사용된 각 애플리케이션에 최소 하나 이상의 탐지기를 활성화해야 합니다. 애플리케이션에 탐지기가 활성화되지 않은 경우, 시스템은 시스템에서 제공된 모든 탐지기를 해당 애플리케이션에 자동으로 활성화합니다. 시스템은 가장 최근에 수정된 사용자 정의 탐지기를 애플리케이션에 활성화합니다.
- 침입 규칙 업데이트를 가져올 경우, 가져오기가 완료된 후 액세스 제어 및 침입 정책을 자동으로 다시 적용할 수 있습니다. 이렇게 하면 대부분의 최신 침입 규칙 및 고급 설정은 물론, 프리프로세서 규칙 및 프리프로세서 설정을 사용할 수 있습니다. 이는 특히 규칙 업데이트를 사용하여 시스템에서 제공된 기본 정책을 수정할 경우 유용합니다. 규칙 업데이트는 액세스 제어 정책의 고급 전처리 및 성능 옵션에 대한 기본 값을 수정할 수도 있습니다. 자세한 내용은 66-14페이지의 규칙 업데이트 및 로컬 규칙 파일 가져오기을/를 참조하십시오.

자세한 내용은 다음 절을 참조하십시오.

- 12-16페이지의 완전한 정책 적용에서는 액세스 제어 정책과 함께 모든 관련 SSL, 네트워크 분석, 침입, 파일 정책을 적용할 수 있는 빠른 적용 옵션을 사용하는 방법에 대해 설명합니다.
- 12-17페이지의 선택한 정책 컨피그레이션 적용에서는 개별 침입 정책을 비롯하여 특정 액세스 제어 정책 컨피그레이션을 적용하는 방법에 대해 설명합니다.

완전한 정책 적용

라이센스: 모든

지원되는 디바이스:

대상 디바이스에 언제든지 액세스 제어 정책을 적용할 수 있습니다. 액세스 제어 정책을 적용하면 현재 실행 중인 정책과 다른 모든 관련 정책도 적용됩니다.

- SSL 정책
- 네트워크 분석 정책
- 침입 정책
- 파일 정책

팝업 창에서 한 번의 빠른 적용 작업으로 모든 정책을 함께 적용할 수 있습니다. 빠른 적용 옵션을 사용할 경우 변경되지 않은 정책은 적용되지 않습니다.

빠른 적용 팝업 창에 있는 적용 버튼의 레이블은 사용자가 액세스 제어 정책, 침입 정책 또는 두 가지를 모두 적용할 수 있는 권한이 있는지 여부에 따라 달라질 수 있습니다(12-4페이지의 사용자 지정 사용자 역할로 구축 관리 참조).

완전한 액세스 제어 정책을 빠르게 적용하려면

액세스: Admin/Security Approver

1단계 **Policies > Access Control**을 선택합니다.

Access Control Policy 페이지가 나타납니다.

2단계 적용할 정책 옆에 있는 적용 아이콘( )을 클릭합니다.

Apply Access Control Policy 팝업 창이 표시됩니다.

또는 정책을 수정하는 동안 **Save and Apply**를 클릭할 수 있습니다(12-11페이지의 액세스 제어 정책 수정 참조).

3단계 **Apply All**을 클릭합니다.

Inspect Traffic During Policy Apply 옵션은 기본적으로 선택되어 있으며 정책을 적용하는 동안 트래픽 검사가 허용됩니다. 트래픽 검사보다 연결이 더 중요하다고 판단될 경우, 고급 탭에서 이 옵션의 선택을 취소합니다.

정책 적용 작업이 대기열에 추가됩니다. **OK**를 클릭하여 Access Control Policy 페이지로 돌아갑니다. Task Status 페이지(**System > Monitoring > Task Status**)에서 정책 적용 작업의 진행 상황을 모니터링할 수 있습니다.

선택한 정책 컨피그레이션 적용

라이센스: 모든

세부적인 정책 적용 페이지를 사용하여 액세스 제어 정책 및 모든 관련 침입 정책에 대한 변경 사항을 적용할 수 있습니다. 세부 페이지에는 정책에 의해 대상으로 지정된 각 디바이스가 나열되며, 디바이스를 기준으로 한 액세스 제어 정책의 열, 디바이스를 기준으로 한 관련 침입 정책의 열을 제공합니다. 각 대상 디바이스에서 액세스 제어 정책 및 관련 침입 정책의 변경 사항을 개별적으로 적용할지 또는 함께 적용할지, 아니면 두 정책의 변경 사항을 모두 적용할지 여부를 지정할 수 있습니다.

다음 상황에 해당되는 경우, 액세스 제어 정책 및 관련 침입 정책을 모두 적용해야 합니다.

- 액세스 제어 정책이 디바이스에 처음 적용된 경우
- 침입 정책이 액세스 제어 정책에 새로 추가된 경우

두 경우 모두, 액세스 제어 정책과 침입 정책의 상태가 연결됩니다. 즉, 두 가지를 모두 적용하거나 적용하지 말아야 합니다.

적용하는 침입 정책에 상관없이, 액세스 제어 정책을 적용하면 디바이스에 의해 대상으로 지정된 디바이스에서 현재 실행 중인 것과 다른 모든 관련 SSL, 네트워크 분석, 파일 정책이 자동으로 적용됩니다. 이러한 정책은 개별적으로 적용할 수 없습니다.

Access Control Policy 열

Access Control Policy 열에서는 액세스 제어 정책을 적용할지 여부를 나타내는 확인란을 제공합니다.

팁 정책이 아직 작업 대기열에 있는 동안(즉, 적용 작업이 아직 완료되지 않은 동안) 정책을 다시 적용할 수 있으나, 이에 따른 특별한 이점은 없습니다.

상태 메시지는 정책이 현재 최신 상태인지 또는 기한이 지났는지 여부를 나타냅니다. 정책의 기한이 지난 경우, 새 브라우저 창에서 해당 정책과 현재 실행 중인 정책을 간편하게 비교하여 표시할 수 있습니다. 이러한 비교 내용에는 액세스 제어 정책과 관련된 침입 정책의 차이점은 포함되지 않습니다.

Intrusion Policies 열

Intrusion Policies 열에서는 액세스 제어 정책과 관련된 침입 정책을 디바이스에 적용할지 여부를 나타내는 하나 이상의 확인란을 제공합니다. 하나의 회색 확인란은 모든 관련 침입 정책이 현재 실행 중인 정책과 동일함을 나타내며, 이 경우 해당 확인란은 선택이 취소되고 선택할 수 없습니다. 변경되지 않은 침입 정책은 적용할 수 없습니다. 변경된 침입 정책만 나열되며, 개별적으로 선택할 수 있습니다. 동일한 침입 정책이 정책의 여러 규칙과 연관된 경우, 각 디바이스에는 침입 정책이 한 번만 나열됩니다.

침입 정책의 확인란을 선택하면 해당 확인란은 회색으로 바뀌며, 위에서 설명했듯이 다음 상황 중 하나에 해당하게 되면 액세스 제어 정책 및 침입 정책을 함께 적용해야 할 경우 변경할 수 없습니다.

- 액세스 제어 정책이 디바이스에 처음 적용된 경우
- 침입 정책이 액세스 제어 정책에 새로 추가된 경우

상태 메시지는 침입 정책이 현재 최신 상태인지 기한이 지났는지 여부를 나타냅니다. 나열된 디바이스에서 현재 실행 중인 침입 정책과 동일하지 않을 경우 침입 정책의 기한이 지난 것입니다. 디바이스의 동일한 침입 정책은 최신 상태입니다. 정책의 기한이 지난 경우, 새 브라우저 창에서 해당 정책과 현재 실행 중인 정책을 간편하게 비교하여 표시할 수 있습니다.

선택한 액세스 제어 정책 컨피그레이션을 적용하려면

액세스: Admin/Security Approver

1단계 **Policies > Access Control**을 선택합니다.

Access Control Policy 페이지가 나타납니다.

2단계 적용할 정책 옆에 있는 적용 아이콘( )을 클릭합니다.

Apply Access Control Policy 팝업 창이 표시됩니다.

또는 정책을 수정하는 동안 **Save and Apply**를 클릭할 수 있습니다(12-11페이지의 액세스 제어 정책 수정 참조).

3단계 **Details**를 클릭합니다.

자세한 Apply Access Control Policy 팝업 창이 표시됩니다. 정책에 대한 **Status** 열에서 기한이 지난 메시지를 클릭하여 Access Control Policy 페이지(**Policies > Access Control**)에서 팝업 창을 열 수도 있습니다.

4단계 디바이스 이름 옆의 액세스 제어 정책 확인란을 선택하거나 선택을 취소하여 액세스 제어 정책을 대상 디바이스에 적용할지 여부를 지정합니다.

5단계 디바이스 이름 옆의 침입 정책 확인란을 선택하거나 선택을 취소하여 침입 정책을 대상 디바이스에 적용할지 여부를 지정합니다.

6단계 **Apply Selected Configurations**를 클릭합니다.

정책 적용 작업이 대기열에 추가됩니다. **OK**를 클릭하여 Access Control Policy 페이지로 돌아갑니다.

디바이스에서 지원되는 최대 침입 정책 수를 초과했다는 경고 메시지가 팝업 창에 표시될 수 있습니다. 액세스 제어 정책을 다시 평가하고 침입 정책을 통합해야 합니다. 관련 침입 정책(기본 작업 포함) 수가 최대값의 범위에 들어가기 전까지는 액세스 제어 정책을 적용할 수 없습니다.

Inspect Traffic During Policy Apply 옵션은 기본적으로 선택되어 있으며 정책을 적용하는 동안 트래픽 검사가 허용됩니다. 트래픽 검사보다 연결이 더 중요하다고 판단될 경우, 고급 탭에서 이 옵션의 선택을 취소합니다.

Task Status 페이지(**System > Monitoring > Task Status**)에서 정책 적용 작업의 진행 상황을 모니터링할 수 있습니다.

IPS 또는 검색 전용 성능 고려 사항

라이센스: FireSIGHT 또는 보호

FireSIGHT 라이센스는 방어 센터에 포함되어 있으며 호스트, 애플리케이션, 사용자 검색을 수행할 수 있도록 합니다. 검색 데이터를 사용하면 네트워크의 완전한 최신 프로필을 생성할 수 있습니다. 보호 라이센스가 매니지드 디바이스에 적용된 경우, 시스템은 침입 탐지 및 방지 시스템(IPS)으로서의 역할을 수행할 수 있습니다. 침입 및 익스플로잇에 대한 네트워크 트래픽을 분석할 수 있으며, 선택에 따라 문제의 패킷을 폐기할 수도 있습니다.

검색 및 IPS를 결합하면 네트워크 작업에 대한 컨텍스트가 제공되며 다음과 같은 다양한 기능을 활용할 수 있습니다.

- 영향 플래그 및 보안 침해 지표 — 특정 익스플로잇, 공격 또는 악성코드에 취약한 호스트가 무엇인지 나타냄
- 적응형 프로필 및 FireSIGHT 권장 사항 — 대상 호스트에 따라 트래픽을 다른 방식으로 검사할 수 있음
- 상관관계 — 영향을 받은 호스트에 따라 침입(및 기타 이벤트)에 다른 방식으로 대응할 수 있음

그러나 IPS 수행 또는 검색 수행에만 관심이 있는 조직의 경우, 다음 섹션에 설명된 것처럼 몇 가지 컨피그레이션으로 시스템의 성능을 최적화할 수 있습니다.

- 12-19페이지의 Network Discovery-Only 구축 최적화
- 12-20페이지의 검색 없이 침입 탐지 및 방지 수행

Network Discovery-Only 구축 최적화

라이센스: FireSIGHT

검색 기능을 사용하면 네트워크 트래픽을 모니터링하고 네트워크에 있는 호스트(네트워크 디바이스 포함)의 개수와 유형뿐만 아니라 이러한 호스트의 운영 체제, 액티브 애플리케이션, 개방된 포트를 확인할 수 있습니다. 매니지드 디바이스 및 사용자 에이전트를 구성하여 네트워크의 사용자 작업을 모니터링할 수도 있습니다. 검색 데이터를 사용하여 트래픽 프로파일링을 수행하고, 네트워크 규정준수를 평가하고, 정책 위반에 대응할 수 있습니다.

기본 구축(검색 및 단순한 네트워크 기반 액세스 제어만 수행)의 경우, 액세스 제어 정책을 구성할 경우 몇 가지 중요한 지침에 따라 디바이스의 성능을 향상할 수 있습니다.

참고 단순히 모든 트래픽을 허용하는 경우에도 액세스 제어 정책을 적용해야 합니다. 네트워크 검색 정책은 액세스 제어 정책이 통과를 허용하는 트래픽에 **한해서만** 검사할 수 있습니다.

우선 해당 액세스 제어 정책에 복잡한 처리 과정이 필요하지 않으며, 단순한 네트워크 기반 조건을 사용하여 네트워크 트래픽을 처리할 수 있는지 확인합니다. 그리고 다음 지침을 **모두** 구현해야 합니다. 이러한 옵션 중 하나라도 컨피그레이션 오류가 발생할 경우 성능 이점이 사라집니다.

- 보안 인텔리전스 기능을 사용하지 **마십시오**. 정책의 보안 인텔리전스 컨피그레이션에서 입력된 전역 블랙리스트 또는 화이트리스트를 제거합니다.
- 액세스 제어 규칙에 Monitor 또는 Interactive Block 작업을 포함하지 **마십시오**. Allow, Trust, Block 규칙만 사용합니다. 허용된 트래픽은 검색을 통해서만 검사할 수 있으며, 신뢰 및 차단된 트래픽은 검사할 수 없습니다.
- 디바이스에 라이센스가 올바르게 제공된 경우에도 액세스 제어 규칙에 애플리케이션, 사용자, URL 또는 위치 기반 네트워크 상태를 포함하지 **마십시오**. 단순한 네트워크 기반 조건(영역, IP 주소, VLAN 태그, 포트)만 사용합니다.
- 디바이스에 라이센스가 올바르게 제공된 경우에도 파일, 악성코드 또는 침입 검사를 수행하는 액세스 제어 규칙을 포함하지 **마십시오**. 즉, 파일 정책 또는 침입 정책을 액세스 제어 규칙과 연결하지 마십시오.
- 액세스 제어 정책의 기본 침입 정책이 **No Rules Active**로 설정되어 있는지 확인합니다(25-1페이지의 액세스 제어에 대한 기본 침입 정책 설정 참조).
- **Network Discovery Only**를 정책의 기본 작업으로 선택합니다. 침입 검사를 수행하는 정책의 기본 작업을 선택하지 **마십시오**.

위치 기반 액세스 제어를 제외하고, 위에 설명된 옵션은 최소한 하나 이상의 보호 라이센스가 있어야 합니다. FireSIGHT 라이센스만 있는 경우, 이러한 기능을 사용하여 액세스 제어 정책을 적용할 수 없습니다.

액세스 제어 정책을 구성 및 적용한 후에는 네트워크 검색 정책을 구성 및 적용할 수 있습니다. 이러한 정책을 통해 검색 데이터뿐만 아니라 세그먼트, 포트, 영역에서 호스트, 애플리케이션, 사용자가 검색되었는지 여부를 시스템에서 검사하는 네트워크 세그먼트, 포트, 영역을 지정합니다.

검색 없이 침입 탐지 및 방지 수행

라이센스: 보호

침입 탐지 및 방지 기능을 사용하면 침입 및 익스플로잇에 대한 네트워크 트래픽을 분석할 수 있으며, 선택에 따라 문제의 패킷을 폐기할 수도 있습니다. 침입 검사를 수행하려고 하지만 검색 데이터를 활용할 필요는 없는 경우, 검색을 비활성화하여 디바이스의 성능을 향상할 수 있습니다.

참고 애플리케이션, 사용자 또는 URL 제어를 수행할 경우 성능 이점을 위해 검색을 비활성화할 수 **없습니다**. 시스템에 검색 데이터가 저장되지 않도록 할 수 있으나, 이러한 기능을 구현하려면 검색 데이터를 **반드시** 수집하고 검사해야 합니다.

검색을 비활성화하려면 다음 지침을 **모두** 구현하십시오. 컨피그레이션 오류가 발생할 경우 성능 이점이 사라집니다.

- 디바이스에 라이센스가 올바르게 제공된 경우에도 액세스 제어 정책에 애플리케이션, 사용자, URL 또는 위치 기반 네트워크 상태와 관련한 규칙을 포함하지 **마십시오**. 단순한 네트워크 기반 조건(영역, IP 주소, VLAN 태그, 포트)만 사용합니다.

- 네트워크 검색 정책에서 모든 규칙을 삭제합니다.

액세스 제어 정책을 적용한 다음 네트워크 검색 정책을 적용하면, 대상 디바이스에서 새로운 검색이 중단됩니다. 시스템에서는 네트워크 검색 정책에 지정된 시간 제한 기간에 따라 네트워크 맵의 정보를 단계적으로 삭제합니다. 또는 모든 검색 데이터를 즉시 제거할 수 있습니다(B-1페이지의 데이터베이스에서 검색 데이터 삭제 참조).

액세스 제어 정책 및 규칙 문제 해결

라이센스: 모든

액세스 제어 정책을 올바르게 구성하는 작업 중에서도 특히 액세스 제어 규칙을 생성하고 순서를 지정하는 것은 복잡한 작업입니다. 그러나 이는 효과적인 구축을 구성하는 데 필수적인 작업입니다. 정책을 신중하게 계획하지 않을 경우, 한 규칙이 다른 규칙을 선점하거나 잘못된 컨피그레이션이 포함될 수 있습니다. 규칙 및 기타 정책 설정에는 모두 추가 라이센스가 필요합니다.

시스템이 예상한 대로 트래픽을 처리하도록 보장하기 위해, 액세스 제어 정책 인터페이스에는 강력한 피드백 시스템이 포함되어 있습니다. 액세스 제어 정책 및 규칙 편집기의 아이콘에는 액세스 제어 오류 아이콘 표에 설명된 것처럼 경고 및 오류가 표시됩니다. 마우스 포인터를 아이콘에 올리면 경고, 오류 또는 정보 텍스트를 읽을 수 있습니다.

팁 액세스 제어 정책 편집기에서 **Show Warnings**를 클릭하여 정책에 대한 모든 경고가 나열된 팝업 창을 표시합니다.

또한 트래픽 분석 및 흐름에 영향을 미칠 수 있는 문제가 적용될 경우 경고 메시지가 표시됩니다.

표 12-7 액세스 제어 오류 아이콘

아이콘	설명	세부 사항
	오류	규칙 또는 컨피그레이션에 오류가 있을 경우, 영향을 받은 규칙을 비활성화한 경우에도 해당 문제를 수정하기 전까지는 정책을 적용할 수 없습니다.
	경고	규칙 또는 기타 경고를 표시하는 액세스 제어 정책을 적용할 수 있습니다. 그러나 경고와 함께 표시되는 컨피그레이션 오류는 아무런 영향을 미치지 않습니다. 예를 들어, 선점된 규칙 또는 컨피그레이션 오류(빈 객체 그룹, 애플리케이션과 매칭되지 않는 애플리케이션 필터를 사용하는 조건, 클라우드 커뮤니케이션을 활성화하지 않은 URL 조건 구성 등)로 인해 트래픽을 매칭할 수 없는 규칙이 포함된 정책을 적용할 수 있습니다. 이러한 규칙은 트래픽을 평가할 수 없습니다. 경고가 포함된 규칙을 비활성화하면 경고 아이콘이 사라집니다. 기본 문제를 수정하지 않은 채 규칙을 활성화하면 경고 아이콘이 다시 나타납니다. 또 다른 예로는 특정 라이센스 또는 디바이스 모델이 필요한 다수의 기능을 들 수 있습니다. 액세스 제어 정책은 적격한 대상 디바이스에만 올바르게 적용됩니다.
	정보	정보 아이콘은 트래픽의 흐름에 영향을 미칠 수 있는 컨피그레이션에 대한 유용한 정보를 제공합니다. 이러한 문제로 인해 정책을 적용하지 못할 수 있습니다. 예를 들어, 애플리케이션 제어 또는 URL 필터링을 수행할 경우 해당 연결의 애플리케이션 또는 웹 트래픽을 식별할 때까지 시스템에서는 일부 액세스 제어 규칙에 어긋나는 처음 몇 가지 연결 패킷의 매칭을 건너뛸 수 있습니다. 이를 통해 연결을 설정하여 애플리케이션 및 HTTP 요청을 식별할 수 있습니다. 자세한 내용은 16-7페이지의 애플리케이션 제어의 제한 사항 및 16-14페이지의 URL 탐지 및 차단의 제한 사항을/를 참조하십시오.

액세스 제어 정책 및 규칙을 올바르게 구성하면 네트워크 트래픽을 처리하는 데 필요한 리소스를 줄일 수도 있습니다. 복잡한 규칙이 생성되면 여러 가지 다른 침입 정책이 호출되며 규칙의 순서가 잘못 지정되어 모든 성능에 영향을 미칠 수 있습니다.

자세한 내용은 다음 링크를 참고하십시오.

- 12-2페이지의 액세스 제어 라이센스 및 역할 요구 사항
- 12-22페이지의 규칙 간소화로 성능 향상
- 12-23페이지의 규칙 선점 및 잘못된 컨피그레이션 경고 이해
- 12-24페이지의 성능 향상 및 선점 방지를 위한 규칙 순서 지정

규칙 간소화로 성능 향상

복잡한 액세스 제어 정책 및 규칙은 상당한 자원을 소모할 수 있습니다. 액세스 제어 정책을 적용할 경우, 시스템에서는 모든 규칙을 함께 평가하며, 대상 디바이스가 네트워크 트래픽을 평가하는 데 사용하는 확장된 조건 집합을 생성합니다. 대상 디바이스에서 지원되는 최대 액세스 제어 규칙 또는 침입 정책의 수를 초과했다는 경고 메시지가 팝업 창에 표시될 수 있습니다. 이러한 최대값은 여러 요인(예: 물리적 메모리)의 개수 및 디바이스의 프로세서 개수에 따라 달라집니다.

액세스 제어 규칙 간소화

다음 지침은 액세스 제어 규칙을 간소화하고 성능을 향상하는 데 도움이 될 수 있습니다.

- 규칙을 구성할 경우, 조건에서 개별 요소를 가급적 최소한으로 사용합니다. 예를 들어, 네트워크 조건의 경우 개별 IP 주소 대신 IP 주소 블록을 사용합니다. 포트 조건의 경우에는 포트 범위를 사용합니다. 애플리케이션 필터와 URL 카테고리 및 평판을 사용하여 애플리케이션 제어 및 URL 필터링을 수행하고, LDAP 사용자 그룹을 사용하여 사용자 제어를 수행합니다.

  여러 요소를 객체로 통합한 다음 액세스 제어 규칙 조건에서 사용할 경우 성능이 향상되지 않습니다. 예를 들어, 50개의 개별 IP 주소가 포함된 네트워크 객체를 사용할 경우 조건에 IP 주소를 개별적으로 포함하는 방법과 비교했을 때 성능적인 측면이 아니라 조직적인 측면에서만 이점이 제공됩니다.
- 가능한 경우 항상 보안 영역으로 규칙을 제한하십시오. 디바이스의 인터페이스가 영역 제한 규칙의 영역 중 하나에 속하지 않을 경우, 이 규칙은 해당 디바이스의 성능에 영향을 미치지 않습니다.
- 규칙을 초과 구성하지 마십시오. 처리하려는 트래픽을 하나의 조건만으로도 충분히 매칭할 수 있는 경우, 두 가지 조건을 사용하지 마십시오.

침입 정책 및 변수 집합 확산 방지

액세스 제어 정책의 트래픽을 검사하는 데 사용할 수 있는 고유한 침입 정책의 개수는 디바이스의 리소스 및 정책의 복잡성에 따라 달라집니다. 하나의 침입 정책을 각 Allow 및 Interactive Block 규칙과 연결하고, 기본 작업과 연결할 수 있습니다. 모든 고유한 침입 정책 및 변수 집합의 **쌍**은 하나의 정책으로 계산됩니다.

디바이스에서 지원되는 침입 정책 수를 초과할 경우, 액세스 제어 정책을 다시 평가합니다. 침입 정책 또는 변수 집합을 통합하여 단일한 침입 정책 변수 집합 쌍을 여러 개의 액세스 제어 규칙과 연결할 수 있습니다.

사용자가 선택하는 정책의 수와 액세스 제어 정책의 각 다음 위치에서 이러한 정책이 사용하는 변수 집합의 수를 확인합니다. **액세스 제어 규칙 이전에 사용된 침입 정책은** 고급 액세스 제어 정책 설정, 액세스 제어 정책에 대한 기본 작업, 정책의 액세스 제어 규칙에 대한 검사 설정에서 결정된 옵션입니다.

규칙 선점 및 잘못된 컨피그레이션 경고 이해

라이센스: 모든

액세스 제어 규칙(및 고급 구축의 네트워크 분석 규칙)의 올바른 구성 및 순서 지정은 효과적인 구축을 구성하는 데 필수적인 작업입니다. 액세스 제어 정책 내의 액세스 제어 규칙은 다른 규칙을 선점하거나 잘못된 컨피그레이션을 포함할 수 있습니다. 이와 마찬가지로, 액세스 제어 정책의 고급 설정을 사용하여 구성하는 네트워크 분석 규칙에도 동일한 문제가 있을 수 있습니다. 시스템에서는 경고 및 오류 아이콘을 사용하여 이러한 문제를 표시합니다.

규칙 선점 경고 이해

액세스 제어 규칙의 조건은 매칭하는 트래픽의 후속 규칙을 선점할 수 있습니다. 예를 들면 다음과 같습니다.

```
Rule 1: allow Admin users
Rule 2: block Admin users
```

첫 번째 규칙이 이미 트래픽을 허용했으므로 위의 두 번째 규칙은 트래픽을 차단하지 않습니다.

모든 유형의 규칙 조건은 후속 규칙을 선점할 수 있습니다. 예를 들어, 다음 첫 번째 규칙의 VLAN 범위에는 두 번째 규칙의 VLAN이 포함되므로 첫 번째 규칙이 두 번째 규칙을 선점합니다.

```
Rule 1: allow VLAN 22-33
Rule 2: block VLAN 27
```

다음 예시의 경우 구성된 VLAN이 없으므로, 규칙 1은 모든 VLAN과 매칭됩니다. 따라서 규칙 1은 VLAN 2 매칭을 시도하는 규칙 2를 선점합니다.

```
Rule 1: allow Source Network 10.4.0.0/16
Rule 2: allow Source Network 10.4.0.0/16, VLAN 2
```

또한 모든 구성된 조건이 동일한 경우, 규칙은 동일한 후속 규칙을 선점합니다. 예를 들면 다음과 같습니다.

```
Rule 1: allow VLAN 1 URL www.example.com
Rule 2: allow VLAN 1 URL www.example.com
```

조건이 하나라도 다른 경우 후속 규칙을 선점할 수 없습니다. 예를 들면 다음과 같습니다.

```
Rule 1: allow VLAN 1 URL www.example.com
Rule 2: allow VLAN 2 URL www.example.com
```

잘못된 컨피그레이션 경고 이해

액세스 제어 정책의 기준이 되는 외부 설정은 변경될 수 있으므로, 올바른 액세스 제어 정책 설정이 잘못될 수 있습니다. 다음 사례를 고려하십시오.

- URL 필터링을 수행하는 규칙은 URL 필터링 라이센스가 없는 디바이스를 대상으로 지정할 때까지 올바르지 않을 수 있습니다. 이 경우, 규칙 옆에 오류 아이콘이 표시되며 해당 규칙을 수정 또는 삭제하고, 정책의 대상을 다시 지정하거나 올바른 라이센스를 활성화할 때까지 해당 디바이스에는 정책을 적용할 수 없습니다.
- 포트 그룹을 규칙의 소스 포트에 추가한 다음 ICMP 포트를 포함하도록 해당 포트 그룹을 변경할 경우, 규칙이 잘못된 것으로 바뀌며 규칙 옆에 경고 아이콘이 표시됩니다. 정책을 계속 적용할 수는 있으나, 규칙은 네트워크 트래픽에 아무런 영향을 미치지 못합니다.
- 사용자를 규칙에 추가한 다음 해당 사용자를 제외하도록 LDAP 사용자 인식 설정을 변경할 경우, 이 사용자는 더 이상 액세스 제어 사용자가 아니므로 규칙은 아무런 영향을 미치지 못합니다.

성능 향상 및 선점 방지를 위한 규칙 순서 지정

라이센스: 모든

액세스 제어 정책의 규칙은 번호가 1부터 시작합니다. 시스템은 오름차순 규칙 번호에 따라 하향식 순서로 트래픽이 규칙과 일치하는지를 확인합니다. 모니터링 규칙을 제외하고, 트래픽의 일치 여부를 확인하는 첫 번째 규칙은 해당 트래픽을 처리하는 규칙입니다.

액세스 제어 규칙 순서를 적절히 지정하면 네트워크 트래픽 처리에 필요한 리소스가 감소하고 규칙 선점이 방지됩니다. 생성하는 규칙이 모든 조직과 구축에서 고유하더라도, 요구를 충족하면서도 성능을 최적화할 수 있는 규칙의 순서를 지정할 경우 따라야 할 몇 가지 일반 지침이 있습니다.

중요도에 따라 최우선부터 최하위까지 규칙 순서 지정

우선 규칙의 순서를 조직의 요구 사항에 맞게 지정해야 합니다. 모든 트래픽을 적용해야 하는 우선순위 규칙은 정책의 위쪽에 배치합니다. 예를 들어, 침입에 대한 단일 사용자의 트래픽을 검사(Allow 규칙 사용)하는 반면 해당 부서의 다른 모든 사용자는 신뢰(Trust 규칙 사용)하려는 경우, 두 개의 액세스 제어 규칙을 이러한 순서로 배치합니다.

특정 항목부터 일반 항목까지 규칙 순서 지정

특정 규칙 즉, 처리하는 트래픽의 정의를 좁히는 규칙을 초기에 배치하여 성능을 향상할 수 있습니다. 광범위한 조건이 포함된 규칙은 다양한 종류의 많은 트래픽을 매칭할 수 있으며, 나중에 더욱 특정한 규칙을 선점할 수 있다는 점에서도 이는 중요합니다.

대부분의 소셜 네트워킹 사이트를 차단하되 특정 소셜 네트워킹 사이트에 대한 액세스는 허용하고자 하는 시나리오를 가정해 보십시오. 예를 들어, 그래픽 디자이너가 Creative Commons Flickr 및 deviantART 콘텐츠에는 액세스할 수 있지만 Facebook 또는 Google+ 같은 다른 사이트에는 액세스할 수 없도록 설정하고자 합니다. 규칙의 순서를 다음과 같이 지정해야 합니다.

```
Rule 1: Allow Flickr, deviantART for the "Design" LDAP user group
Rule 2: Block social networking
```

규칙을 반대로 설정할 경우

```
Rule 1: Block social networking
Rule 2: Allow Flickr, deviantART for the "Design" LDAP user group
```

첫 번째 규칙은 Flickr 및 deviantART를 포함한 모든 소셜 네트워킹 트래픽을 차단합니다. 트래픽이 두 번째 규칙과 매칭되지 않으므로, 디자이너는 사용해야 할 콘텐츠에 액세스할 수 없습니다.

나중에 트래픽을 검사하는 규칙 배치

검색, 침입, 파일, 악성코드 검사를 수행하려면 처리 리소스가 필요하므로, 트래픽을 검사하는 규칙(Allow, Interactive Block) 앞에 트래픽을 검사하지 않는 규칙(Trust, Block)을 배치하면 성능을 향상할 수 있습니다. 그 이유는 이렇게 하지 않을 경우 시스템에서 트래픽을 검사하게 될 수 있으나, Trust 및 Block 규칙이 이러한 트래픽을 전환하기 때문입니다. 다른 모든 요소가 동일한 경우 즉, 규칙 집합의 중요도가 더 높지 않고 선점이 문제되지 않을 경우, 해당 규칙을 다음 순서로 배치합니다.

- Monitor 규칙 — 매치되는 연결을 로깅하지만 트래픽에 다른 작업은 수행하지 않음
- Trust 및 Block 규칙 — 추가 검사 없이 트래픽 처리
- Allow 및 Interactive Block 규칙 — 트래픽을 추가 검사하지 않음
- Allow 및 Interactive Block 규칙 — 선택에 따라 악성코드, 침입 또는 두 가지 모두에 대한 트래픽 검사

현재 액세스 제어 설정에 대한 보고서 생성

라이센스: 모든

액세스 제어 정책 보고서는 특정 시점의 정책 레코드이자 규칙 컨피그레이션입니다. 감사의 목적으로 또는 현재 컨피그레이션을 검사하는 데 다음 정보를 포함하는 이 보고서를 사용할 수 있습니다.

표 12-8 액세스 제어 정책 보고서 섹션

섹션	설명
정책 정보	정책의 이름과 설명, 마지막으로 정책을 수정한 사용자의 이름, 정책이 마지막으로 수정된 날짜와 시간을 제공합니다.
디바이스 대상	정책으로 대상을 지정한 매니지드 디바이스가 나열됩니다.
HTTP 차단 응답 HTTP 인터랙티브 차단 응답	정책을 사용하여 웹 사이트를 차단한 경우 사용자에게 표시되는 페이지에 대한 세부 정보를 제공합니다.
보안 인텔리전스	정책의 보안 인텔리전스 화이트리스트 및 블랙리스트에 대한 세부 정보를 제공합니다.
기본 작업	기본 작업 및 관련 변수 집합이 나열됩니다.
규칙	정책의 각 액세스 제어 규칙이 나열되며, 해당 컨피그레이션에 대한 세부 정보를 제공합니다.
고급 설정	다음과 같은 정책의 고급 설정에 대한 자세한 정보를 제공합니다. • 액세스 제어 정책의 트래픽을 전처리하는 데 사용되는 네트워크 분석 정책 및 전역 전처리 옵션 • 패시브 구축에 대한 적응형 프로필 설정 • 파일, 악성코드, 침입 탐지를 위한 성능 설정 • 기타 정책 전반에 대한 설정
참조 객체	액세스 제어 정책에서 참조하는 재사용 가능한 객체에 대한 세부 정보를 제공하며, 여기에는 침입 정책 변수 집합 및 SSL 정책에서 사용되는 객체가 포함됩니다.

또한 특정 정책을 현재 적용된 정책 또는 다른 정책과 비교하는 액세스 제어 비교 보고서를 생성할 수도 있습니다. 자세한 내용은 12-26페이지의 액세스 제어 정책 비교을/를 참조하십시오.

액세스 제어 정책 보고서를 보려면

액세스: Admin/Access Admin/Network Admin

1단계 **Policies > Access Control**을 선택합니다.

Access Control Policy 페이지가 나타납니다.

2단계 보고서를 생성할 정책 옆의 보고서 아이콘( )을 클릭합니다. 액세스 제어 정책 보고서를 생성하기 전에 모든 변경 사항을 저장해야 합니다. 저장된 변경 사항만 보고서에 표시됩니다.

시스템에서 보고서를 생성합니다. 브라우저 설정에 따라 보고서가 팝업 창에 나타날 수 있으며, 컴퓨터에 보고서를 저장하는 프롬프트가 표시될 수도 있습니다.

액세스 제어 정책 비교

라이센스: 모든

조직의 표준 준수를 위해 정책 변경 사항을 검토하거나 시스템 성능을 최적화하기 위해, 두 액세스 제어 정책 간의 차이점을 검사할 수 있습니다. 두 정책을 비교하거나 현재 적용된 정책을 다른 정책과 비교할 수 있습니다. 선택적으로, 비교 후 두 정책의 차이를 기록하는 PDF 보고서를 생성할 수도 있습니다.

정책 비교에 사용할 수 있는 2가지 툴이 있습니다.

- 비교 보기에서는 두 정책의 차이점만 나란히 표시합니다. 각 정책의 이름이 비교 보기의 좌우 제목 표시줄에 나타납니다. 단, **Running Configuration**을 선택할 경우 빈 표시줄에 현재 활성 상태의 정책이 나타납니다.

  이를 사용하여 웹 인터페이스에서 그 차이점이 강조 표시된 상태에서 두 정책을 모두 보고 탐색할 수 있습니다.
- 비교 보고서는 두 정책의 차이점에 대해서만 기록을 생성하는데, 그 형식은 정책 보고서와 비슷하지만 PDF 형식입니다.

  이를 사용하여 향후 점검을 위해 정책 비교를 저장, 복사, 인쇄, 공유할 수 있습니다.

정책 비교 툴을 이해하고 사용하는 것에 대한 자세한 내용은 다음을 참조하십시오.

- 12-26페이지의 액세스 제어 정책 비교 보기 사용
- 12-27페이지의 액세스 제어 정책 비교 보고서 사용

액세스 제어 정책 비교 보기 사용

라이센스: 모든

비교 보기에서는 두 정책을 나란히 표시하며, 각 정책은 비교 보기의 좌우 제목 표시줄에 있는 이름으로 식별됩니다. 실행 중인 컨피그레이션이 아닌 두 정책을 비교할 경우 마지막 수정 시간 및 마지막으로 수정한 사용자가 정책 이름과 함께 표시됩니다.

두 정책 간의 차이점이 강조 표시됩니다.

- 파란색은 강조 표시된 설정이 두 정책에서 다름을 의미하며, 그 차이점이 빨간색 텍스트로 표시됩니다.
- 녹색은 강조 표시된 설정이 둘 중 한 정책에만 나타남을 의미합니다.

다음 표의 작업을 수행할 수 있습니다.

표 12-9 액세스 제어 정책 비교 보기 작업

목적	가능한 작업
개별 변경 사항 탐색	제목 표시줄 위의 **Previous** 또는 **Next**를 클릭합니다. 왼쪽과 오른쪽 사이의 중앙에 있는 이중 화살표 아이콘()이 움직이고, 어떤 차이점을 보고 있는지 식별할 수 있도록 **Difference** 번호가 조정됩니다.
새 정책 비교 보기 생성	**New Comparison**을 클릭합니다. **Select Comparison** 창이 나타납니다. 자세한 내용은 12-27페이지의 액세스 제어 정책 비교 보고서 사용을/를 참조하십시오.
정책 비교 보고서 생성	**Comparison Report**를 클릭합니다. 정책 비교 보고서에서는 두 정책의 차이점만 나열하는 PDF 문서를 생성합니다.

액세스 제어 정책 비교 보고서 사용

라이센스: 모든

액세스 제어 정책 비교 보고서는 정책 비교 보기를 통해 확인된 두 액세스 제어 정책 간의 모든 차이점, 또는 특정 정책과 현재 적용된 정책 간의 모든 차이점을 PDF 형식으로 제공하는 레코드입니다. 두 정책 컨피그레이션의 차이점을 더 자세히 살펴보고 조사 결과를 저장하여 배포하는 데 이 보고서를 사용할 수 있습니다.

액세스 권한이 있는 모든 정책에 대한 비교 보기에서 액세스 제어 정책 비교 보고서를 생성할 수 있습니다. 정책 보고서를 생성하기 전에 모든 변경 사항을 저장해야 합니다. 저장된 변경 사항만 보고서에 나타납니다.

정책 비교 보고서의 형식은 한 가지 점만 제외하면 정책 보고서와 동일합니다. 정책 보고서에는 정책의 모든 컨피그레이션이 포함되지만, 정책 비교 보고서에는 정책 간에 서로 다른 컨피그레이션만 나열됩니다. 액세스 제어 정책 비교 보고서에는 12-25 페이지의 표 12-8에 설명된 섹션이 포함됩니다.

팁 유사한 절차를 사용하여 SSL, 네트워크 분석, 침입, 파일, 시스템 또는 상태 정책을 비교할 수 있습니다.

두 액세스 제어 정책을 비교하려면

액세스: Admin/Access Admin/Network Admin

1단계 **Policies > Access Control**을 선택합니다.

Access Control Policy 페이지가 나타납니다.

2단계 **Compare Policies**를 클릭합니다.

Select Comparison 창이 나타납니다.

3단계 **Compare Against** 드롭다운 목록에서 원하는 비교 유형을 선택합니다.

- 두 개의 다른 정책을 비교하려면 **Other Policy**를 선택합니다.

  페이지가 새로 고쳐지고 Policy A 및 Policy B 드롭다운 목록이 나타납니다.
- 다른 정책과 현재 활성 정책을 비교하려면 **Running Configuration**을 선택합니다.

  페이지가 새로 고쳐지고 Target/Running Configuration A 및 Policy B 드롭다운 목록이 나타납니다.

4단계 선택한 비교 유형에 따라 다음을 선택할 수 있습니다.

- 두 개의 다른 정책을 비교할 경우 비교할 정책을 Policy A 및 Policy B 드롭다운 목록에서 각각 선택합니다.
- 실행 중인 컨피그레이션을 다른 정책과 비교할 경우 Policy B 드롭다운 목록에서 두 번째 정책을 선택합니다.

5단계 **OK**를 클릭하여 정책 비교 보기를 표시합니다.

비교 보기가 나타납니다.

6단계 선택에 따라, **Comparison Report**를 클릭하여 액세스 제어 정책 비교 보고서를 생성합니다.

액세스 제어 정책 비교 보고서가 표시됩니다. 브라우저 설정에 따라 보고서가 팝업 창에 나타날 수 있으며, 컴퓨터에 보고서를 저장하는 프롬프트가 표시될 수도 있습니다.

13장

보안 인텔리전스 IP 주소 평판 블랙리스트에 추가

악의적인 인터넷 콘텐츠에 대한 1차 방어선으로서, FireSIGHT 시스템에는 최신 평판 인텔리전스를 기반으로 연결을 즉시 블랙리스트에 추가하여(차단하여) 리소스 소모가 더 큰 심층 분석이 필요 없도록 하는 보안 인텔리전스 기능이 포함되어 있습니다.보호 라이센스가 필요한 보안 인텔리전스 필터링은 Series 2를 제외한 모든 관리되는 디바이스에서 지원됩니다.

보안 인텔리전스는 알려진 나쁜 평판이 있는 IP 주소와의 트래픽을 차단하는 방식으로 작동합니다. 이러한 트래픽 필터링은 다른 정책 기반 검사, 분석 또는 트래픽 처리 **전에** 발생합니다(그러나 빠른 경로 지정 등의 하드웨어 레벨 처리 이후 발생).

IP 주소별로 트래픽을 수동으로 제한하여 보안 인텔리전스 필터링과 유사하게 작동하는 액세스 제어 규칙을 생성할 수 있습니다. 그러나 액세스 제어 규칙은 범위가 더 넓고 구성하기가 더 복잡하며, 동적 피드를 사용하여 자동으로 업데이트할 수 없습니다.

보안 인텔리전스를 통해 블랙리스트에 추가된 트래픽은 즉시 차단되므로 침입, 악성코드, 익스플로잇 등은 물론 네트워크 검색에 대해서도 추가 검사가 이루어지지 않습니다. 선택적으로, 보안 인텔리전스 필터링에 "모니터링 전용" 설정을 사용할 수 있습니다(패시브 구축의 권장 사항). 이 경우 시스템은 블랙리스트에 추가된 연결을 분석하는 것은 물론, 일치 항목을 블랙리스트에 기록하고 연결 끝 보안 인텔리전스 이벤트를 생성합니다.

주의 Series 3 디바이스에 의해 처리되는 트래픽의 경우 시스템은 액세스 제어 정책의 보안 인텔리전스 블랙리스트 이전에 특정 신뢰 규칙을 처리하는데, 이 경우 블랙리스트 트래픽이 검사 없이 통과될 수 있습니다. 자세한 내용은 14-12페이지의 Series 3 디바이스를 이용한 트래픽 신뢰 또는 차단 제한 사항을/를 참조하십시오.

사용자 편의를 위해 Cisco에서는 *인텔리전스 피드*(*Sourcefire 인텔리전스 피드*라고도 함)를 제공합니다. 인텔리전스 피드는 VRT에서 부정적인 평판을 받은 IP 주소를 정기적으로 업데이트한 몇몇 모음으로 구성되며 오픈 릴레이, 알려진 공격자, 가짜 IP 주소(bogon) 등을 추적합니다. 조직의 고유한 요구에 맞게 이 기능을 맞춤화할 수 있습니다. 예를 들면 다음과 같습니다.

- **서드파티 피드** — 인텔리전스 피드를 서드파티 평판 피드로 보충할 수 있습니다. 시스템에서는 Cisco 피드와 마찬가지로 자동으로 이를 업데이트할 수 있습니다.
- **사용자 지정 블랙리스트** — 사용자는 각자의 요구에 맞게 여러 방법으로 특정 IP 주소를 블랙리스트에 추가할 수 있습니다.
- **보안 영역별로 블랙리스트에 추가 적용** — 예를 들어 스팸 블랙리스트 추가는 이메일 트래픽을 처리하는 영역으로 제한하는 등 성능 향상을 위해 적용 대상을 지정할 수 있습니다.
- **블랙리스트 추가 대신 모니터링** — 구현 이전의 패시브 구축 및 피드 테스트에 특히 유용합니다. 위반 세션을 차단하는 대신 모니터링만 하여 연결 끝 이벤트를 생성할 수 있습니다.

- **오탐을 없애기 위해 화이트리스트에 추가** — 블랙리스트 범위가 너무 넓은 경우 또는 중요한 리소스 등 허용하려는 트래픽을 잘못 차단하는 경우 사용자 지정 화이트리스트로 블랙리스트를 재정의할 수 있습니다.

보안 인텔리전스 필터링을 수행하는 액세스 제어 정책을 구성하는 방법 및 이 필터링이 생성하는 이벤트 데이터를 보는 방법에 대한 자세한 내용은 다음 절을 참조하십시오.

- 13-2페이지의 보안 인텔리전스 전략 선택
- 13-3페이지의 보안 인텔리전스 화이트리스트 및 블랙리스트 작성
- 38-10페이지의 보안 인텔리전스(블랙리스팅) 결정 로깅
- 39-1페이지의 연결 및 보안 인텔리전스 데이터 작업

보안 인텔리전스 전략 선택

라이센스: 보호

지원되는 디바이스: Series 2를 제외한 모두

지원되는 Defense Center: DC500을 제외한 모두

블랙리스트를 생성하는 가장 쉬운 방법은 오픈 릴레이로 알려진 IP 주소, 알려진 공격자, 가짜 IP 주소(bogon) 등을 추적하는 인텔리전스 피드를 사용하는 것입니다. 인텔리전스 피드는 정기적으로 업데이트되므로 이 피드를 사용하면 시스템에서 최신 정보를 사용하여 네트워크 트래픽을 필터링할 수 있습니다. 악성코드, 스팸, 봇넷, 피싱 등 보안 위협을 나타내는 악의적인 IP 주소는 사용자가 새 정책을 업데이트하여 적용하는 속도보다 더 빠르게 나타났다 사라질 수 있습니다.

인텔리전스 피드를 강화하려면 사용자 지정 또는 서드파티 IP 주소와 피드를 사용하여 보안 인텔리전스 필터링을 수행할 수 있습니다.

- *목록*은 방어 센터에 업로드하는 IP 주소의 고정 목록입니다.
- *피드*는 방어 센터가 인터넷에서 정기적으로 다운로드하는 IP 주소의 동적 목록입니다. 인텔리전스 피드는 특수한 종류의 피드입니다.

고가용성과 인터넷 액세스 요건을 비롯하여 보안 인텔리전스 목록과 피드에 대한 자세한 내용은 3-4페이지의 보안 인텔리전스 목록 및 피드 작업을/를 참조하십시오.

보안 인텔리전스 전역 블랙리스트 사용

분석 과정 중에 이벤트 보기, Context Explorer 또는 대시보드에서 IP 주소를 선택하여 *전역 블랙리스트*를 작성할 수 있습니다. 익스플로잇 시도와 결합된 침입 이벤트에서 라우팅 가능한 IP 주소 집합이 발견되면 해당 IP 주소를 즉시 블랙리스트에 추가할 수 있습니다. 방어 센터에서는 이 전역 블랙리스트(및 연결된 *전역 화이트리스트*)를 사용하여 모든 액세스 제어 정책에서 보안 인텔리전스 필터링을 수행합니다. 이러한 전역 목록 관리에 대한 자세한 내용은 3-7페이지의 전역 화이트리스트 및 블랙리스트 작업을/를 참조하십시오.

참고 전역 블랙리스트(또는 전역 화이트리스트, 아래 참조)에 대해 피드를 업데이트 및 추가하면 구축 전체에서 변경 사항이 자동으로 구현되지만, 보안 인텔리전스 객체에 대한 변경 사항의 경우 액세스 제어 정책을 다시 적용해야 합니다. 자세한 내용은 3-6 페이지의 표 3-1을/를 참조하십시오.

네트워크 객체 사용

끝으로, 블랙리스트를 구성하는 간단한 방법은 IP 주소, IP 주소 블록, 또는 IP 주소 모음을 나타내는 *네트워크 객체 또는 네트워크 객체 그룹*을 사용하는 것입니다. 네트워크 객체 생성 및 수정에 대한 자세한 내용은 3-4페이지의 네트워크 객체 작업을/를 참조하십시오.

보안 인텔리전스 화이트리스트 사용

각 액세스 제어 정책에는 블랙리스트 외에도 관련된 화이트리스트가 있습니다. 화이트리스트 역시 보안 인텔리전스 객체로 채울 수 있습니다. 정책의 화이트리스트는 블랙리스트를 재정의합니다. 즉, 시스템은 액세스 제어 규칙을 사용하여 화이트리스트에 있는 소스 및 목적지 IP 주소로 트래픽을 평가합니다(IP 주소가 블랙리스트에도 있더라도). 일반적으로, 블랙리스트가 여전히 유용하지만 범위가 너무 넓고 검사하려는 트래픽을 정확하게 차단하지 못하는 경우 화이트리스트를 사용합니다.

예를 들어, 평판이 좋은 피드가 중요한 리소스에 대한 액세스를 부적절하게 차단하지만 조직에서 전체적으로 유용한 경우, 블랙리스트에서 전체 피드를 제거하는 것보다는 부적절하게 분류된 IP 주소만 화이트리스트에 추가할 수 있습니다.

보안 영역 보안 인텔리전스 필터링 적용

세분화를 더하려면 연결에서 소스 또는 목적지 IP 주소가 특정 보안 영역에 상주하는지 여부를 기반으로 보안 인텔리전스 필터링을 적용할 수 있습니다.

위의 화이트리스트 예를 확장하려면, 부적절하게 분류된 IP 주소를 화이트리스트에 추가한 다음 해당 IP 주소에 액세스해야 하는 조직의 사용자들이 사용하는 보안 영역을 통해 화이트리스트 객체를 제한할 수 있습니다. 그렇게 하면 비즈니스 요구가 있는 사용자만 화이트리스트에 추가된 IP 주소에 액세스할 수 있습니다. 또 다른 예로, 이메일 서버 보안 영역에서 트래픽을 블랙리스트에 추가하기 위해 서드파티 스팸 피드를 사용할 수 있습니다.

연결을 블랙리스트에 추가하는 대신 모니터링 이용

특정 IP 주소 또는 주소 집합을 블랙리스트에 추가해야 할지 확실치 않으면 "모니터링 전용" 설정을 사용할 수 있습니다. 그러면 시스템에서는 일치하는 연결을 액세스 제어 규칙으로 전달하는 것은 물론, 일치 내용을 블랙리스트에 기록하고 연결 끝 보안 인텔리전스 이벤트를 생성할 수 있습니다. 전역 블랙리스트는 모니터링 전용으로 설정할 수 없습니다. 자세한 내용은 다음을 참조하십시오.

서드파티 피드를 사용한 차단을 구현하기 전에 해당 피드를 테스트할 시나리오를 생각해보십시오. 모니터링 전용 피드를 설정하면, 시스템에서 더 심층적으로 분석했다면 차단되었을 연결이 허용되지만, 사용자가 평가할 수 있도록 그러한 각 연결의 레코드가 기록됩니다.

패시브 구축에서 성능을 최적화할 수 있도록 Cisco에서는 항상 모니터링 전용 설정을 사용할 것을 권장합니다. 관리되는 디바이스가 수동으로 구축된 경우 트래픽 플로우에 영향을 미칠 수 없습니다. 시스템이 트래픽을 차단하도록 구성하는 방식에는 이점이 없습니다. 또한 차단된 연결은 패시브 구축에서 실제로 차단되지 않으므로, 시스템은 각각의 차단된 연결에 대해 여러 개의 연결 시작 이벤트를 보고할 수 있습니다.

보안 인텔리전스 화이트리스트 및 블랙리스트 작성

라이센스: 보호

지원되는 디바이스: Series 2를 제외한 모두

지원되는 Defense Center: DC500을 제외한 모두

화이트리스트 및 블랙리스트를 작성하려면 네트워크 객체와 그룹은 물론, 보안 인텔리전스 피드와 목록도 결합하여 해당 목록을 채울 수 있으며, 이 모두를 보안 영역으로 제한할 수 있습니다.

기본적으로 액세스 제어 정책에서는 방어 센터의 전역 화이트리스트 및 블랙리스트를 사용하며, 이는 모든 영역에 적용됩니다. 컨텍스트 메뉴를 사용하여 개별 IP 주소를 빠르게 추가할 수 있는 조직 내 분석가들이 이러한 목록을 채웁니다. 정책 단위로 이러한 전역 목록을 사용하지 않도록 선택할 수 있습니다.

참고 채워진 전역 화이트리스트 또는 블랙리스트를 사용하는 액세스 제어 정책은 Series 2 디바이스(또는 보호에 대해 사용이 허가되지 않은 다른 디바이스)에 적용할 수 없습니다. 두 전역 목록 중 하나에 IP 주소를 추가한 경우, 정책을 적용하기 전에 정책의 보안 인텔리전스 컨피그레이션에서 비어 있지 않은 목록을 **반드시** 제거해야 합니다. 자세한 내용은 3-7페이지의 전역 화이트리스트 및 블랙리스트 작업을/를 참조하십시오.

화이트리스트 및 블랙리스트를 작성한 후에는 블랙리스트에 추가된 연결을 기록할 수 있습니다. 피드와 목록을 비롯한 개별 블랙리스트 객체를 모니터링 전용으로 설정할 수도 있습니다. 이렇게 하면 시스템에서는 액세스 제어를 사용하여 블랙리스트 IP 주소와 관련된 연결을 처리하는 것은 물론, 연결에서 일치하는 항목을 블랙리스트에 기록할 수도 있습니다.

화이트리스트, 블랙리스트 및 로깅 옵션을 구성하려면 액세스 제어 정책에서 Security Intelligence 탭을 사용합니다. 해당 페이지에는 화이트리스트나 블랙리스트에서 사용할 수 있는 Available Objects는 물론, 화이트리스트나 블랙리스트에 추가되는 객체를 제한하기 위해 사용할 수 있는 Available Zones도 나열됩니다. 각 객체 또는 영역 유형은 서로 다른 아이콘으로 구분됩니다. Cisco 아이콘(Cisco)으로 표시된 객체는 인텔리전스 피드의 서로 다른 영역을 나타냅니다.Cisco

블랙리스트에서, 차단하도록 설정된 객체는 차단 아이콘( )으로 표시되는 반면 모니터링 전용 객체는 모니터링 아이콘( )으로 표시됩니다. 화이트리스트는 블랙리스트를 재정의하므로 동일한 객체를 두 목록에 추가하면 블랙리스트의 객체는 취소선으로 표시됩니다.

화이트리스트 및 블랙리스트에 총 255개의 객체를 추가할 수 있습니다. 즉, 화이트리스트의 객체 수와 블랙리스트의 객체 수의 합은 255를 초과할 수 없습니다.

/0 넷마스크의 네트워크 객체를 화이트리스트나 블랙리스트에 추가할 수는 있지만, 해당 객체에서 /0 넷마스크를 사용하는 주소 블록은 무시되며 그러한 주소 기반으로는 화이트리스트 및 블랙리스트 필터링이 발생하지 않습니다. 보안 인텔리전스에서 /0 넷마스크가 있는 주소 블록 역시 무시됩니다. 정책의 대상인 모든 트래픽을 모니터링하거나 차단하려면 각각 **Monitor** 또는 **Block** 규칙 작업의 액세스 제어 규칙을 사용하고, **Source Networks** 및 **Destination Networks**에 보안 인텔리전스 필터링 대신 **any**를 사용하십시오.

액세스 제어 정책에 대해 보안 인텔리전스 화이트리스트 및 블랙리스트를 작성하려면

액세스: Admin/Access Admin/Network Admin

1단계 **Policies > Access Control**을 선택합니다.

Access Control Policy 페이지가 나타납니다.

2단계 구성할 액세스 제어 정책 옆에 있는 수정 아이콘( )을 클릭합니다.

액세스 제어 정책 편집기가 나타납니다.

3단계 **Security Intelligence** 탭을 선택합니다.

액세스 제어 정책에 대한 Security Intelligence 설정이 나타납니다.

4단계 선택적으로, 블랙리스트 연결을 기록하려면 로깅 아이콘( )을 클릭합니다.

블랙리스트 객체를 모니터링 전용으로 설정하려면 먼저 로깅을 활성화해야 합니다. 자세한 내용은 38-10페이지의 보안 인텔리전스(블랙리스팅) 결정 로깅을/를 참조하십시오.

5단계 하나 이상의 **Available Objects**를 선택하여 화이트리스트 및 블랙리스트 작성을 시작합니다.

Shift 및 Ctrl 키를 사용하여 여러 객체를 선택하거나, 마우스 오른쪽 버튼을 클릭하고 **Select All**을 선택합니다.

팁 포함할 기존 객체를 검색할 수도 있고, 조직의 요구에 맞는 기존 객체가 없는 경우 즉석에서 객체를 생성할 수도 있습니다. 자세한 내용은 13-5페이지의 화이트리스트 또는 블랙리스트에 추가할 객체 검색 및 13-6페이지의 화이트리스트 또는 블랙리스트에 추가할 객체 생성을/를 참조하십시오.

6단계 객체 선택을 영역별로 제한하려는 경우 **Available Zone**을 선택합니다.

기본적으로 객체는 제한되지 않습니다. 즉, 영역의 기본값은 Any입니다. **Any** 이외의 값을 사용하면 하나의 영역으로만 제한할 수 있습니다. 여러 영역에서 하나의 객체에 대해서만 보안 인텔리전스 필터링을 적용하려면 각 영역에 대해 화이트리스트 또는 블랙리스트에 객체를 별도로 추가해야 합니다. 또한 전역 화이트리스트 또는 블랙리스트는 영역별로 제한할 수 없습니다.

7단계 **Add to Whitelist** 또는 **Add to Blacklist**를 클릭합니다.

선택한 객체를 두 목록 중 하나로 끌어다 놓을 수도 있습니다.

선택한 객체가 화이트리스트 또는 블랙리스트에 추가됩니다.

팁 목록에서 객체를 제거하려면 삭제 아이콘( )을 클릭합니다. Shift 및 Ctrl 키를 사용하여 여러 객체를 선택하거나, 마우스 오른쪽 버튼을 클릭하고 **Select All**을 선택한 다음 마우스 오른쪽 버튼을 클릭하고 **Delete Selected**를 선택합니다. 전역 목록을 삭제하는 경우 선택 사항을 확인해야 합니다. 화이트리스트 또는 블랙리스트에서 객체를 제거해도 방어 센터에서 객체가 삭제되지는 않습니다.

8단계 화이트리스트 또는 블랙리스트에 객체를 모두 추가할 때까지 5~7단계를 반복합니다.

9단계 선택적으로, **Blacklist** 아래에서 마우스 오른쪽 버튼으로 객체를 선택한 다음 **Monitor-only (do not block)**를 선택하여 블랙리스트 객체를 모니터링 전용으로 설정합니다.

패시브 구축의 경우 Cisco에서는 모든 블랙리스트 객체를 모니터링 전용으로 설정할 것을 권장합니다. 그러나 전역 블랙리스트는 모니터링 전용으로 설정할 수 없습니다.

10단계 **Save**를 클릭합니다.

변경 사항을 적용하려면 액세스 제어 정책을 적용해야 합니다. 12-15페이지의 액세스 제어 정책 적용을/를 참조하십시오.

화이트리스트 또는 블랙리스트에 추가할 객체 검색

라이센스: 보호

지원되는 디바이스: Series 2를 제외한 모두

지원되는 Defense Center: DC500을 제외한 모두

여러 네트워크 객체, 그룹, 피드 및 목록이 있는 경우 블랙리스트 또는 화이트리스트에 추가할 객체의 범위를 좁히려면 검색 기능을 사용할 수 있습니다.

화이트리스트 또는 블랙리스트에 추가할 객체를 검색하려면

액세스: Admin/Access Admin/Network Admin

1단계 **Search by name or value** 필드에 쿼리를 입력합니다.

입력하여 일치하는 항목이 표시됨에 따라 Available Objects 목록이 업데이트됩니다. 검색 문자열을 지우려면 검색 필드 위의 다시 로드 아이콘( )을 클릭하거나, 검색 필드의 지우기 아이콘( )을 클릭합니다.

네트워크 객체 이름 및 그러한 객체에 대해 구성된 값을 검색할 수 있습니다. 예를 들어 `Texas Office`라는 개별 네트워크 객체가 `192.168.3.0/24` 값으로 구성되어 있고 `US Offices`라는 그룹 객체에 포함된 경우 전체 또는 부분 검색 문자열(예: `Tex`)을 입력하거나 값(예: `3`)을 입력하여 두 객체를 모두 표시할 수 있습니다.

화이트리스트 또는 블랙리스트에 추가할 객체 생성

라이센스: 보호

지원되는 디바이스: Series 2를 제외한 모두

지원되는 Defense Center: DC500을 제외한 모두

액세스 제어 정책을 수정하는 동안 화이트리스트 및 블랙리스트에 사용할 객체(네트워크 객체 또는 보안 인텔리전스 목록이나 피드)를 즉석에서 생성할 수 있습니다. 네트워크 객체를 그룹화하거나 네트워크 객체 그룹을 생성하려면 객체 관리자를 사용해야 합니다.

화이트리스트 또는 블랙리스트에 추가할 객체를 생성하려면

액세스: Admin/Access Admin/Network Admin

1단계 추가 아이콘( )을 클릭한 다음 생성할 객체 유형을 선택합니다.

- 보안 인텔리전스 목록 또는 피드를 생성하려면 **Add IP List**를 선택합니다. 3-4페이지의 보안 인텔리전스 목록 및 피드 작업을/를 참조하십시오.
- 네트워크 객체를 추가하려면 **Add Network Object**를 선택합니다. 3-4페이지의 네트워크 객체 작업을/를 참조하십시오.

14장

액세스 제어 규칙을 사용하여 트래픽 플로우 조정

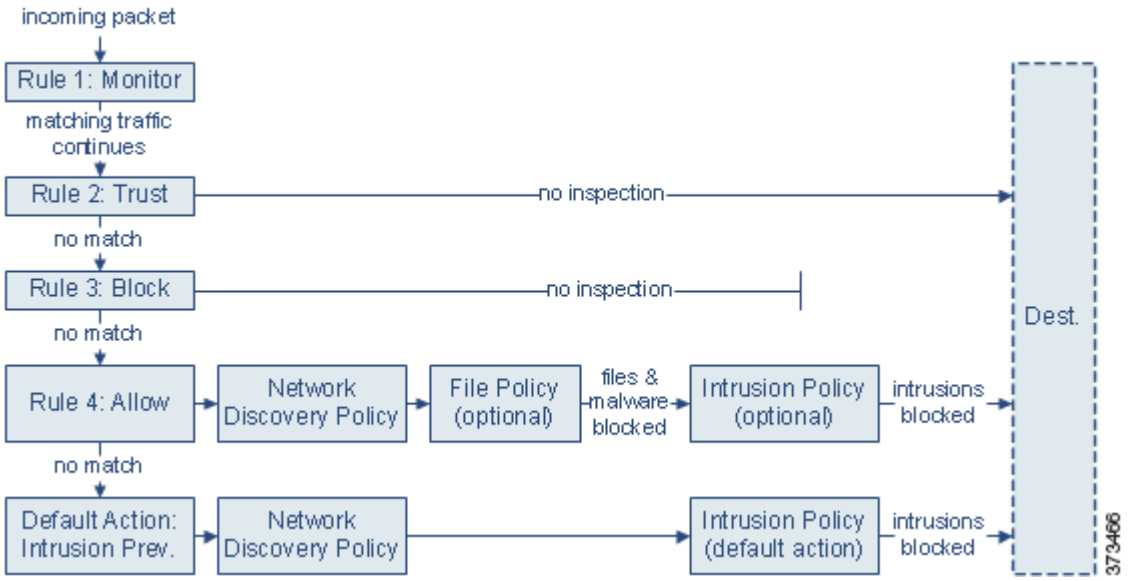
액세스 제어 정책 내에서 *액세스 제어 규칙*은 여러 관리되는 디바이스 간에 세분화된 네트워크 트래픽 처리 방법을 제공합니다.

참고 하드웨어 기반 빠른 경로 규칙, 보안 인텔리전스 기반 트래픽 필터링, 일부 디코딩과 전처리는 네트워크 트래픽이 액세스 제어 규칙에 의해 평가되기 **전에** 발생합니다. 액세스 제어 규칙에 의해 평가되기 전에 암호화된 트래픽을 차단 또는 암호 해독하도록 *SSL 검사* 기능을 구성할 수도 있습니다.

시스템에서는 사용자가 지정한 순서에 따라 트래픽을 액세스 제어 규칙에 대해 매칭합니다. 대부분의 경우, 시스템은 *모든* 규칙의 조건이 트래픽과 매칭되는 *첫 번째* 액세스 제어 규칙에 따라 네트워크 트래픽을 처리합니다. 조건은 간단할 수도 있고 복잡할 수도 있습니다. 보안 영역, 네트워크 또는 지오로케이션, VLAN, 포트, 애플리케이션, 요청된 URL 및 사용자별로 트래픽을 제어할 수 있습니다.

각 규칙에는 일치하는 트래픽의 모니터링, 신뢰, 차단 또는 허용 여부를 결정하는 *작업*이 있습니다. 허용하는 경우, 트래픽이 자산에 도달하거나 네트워크에서 빠져나가기 전에 시스템에서 먼저 침입 또는 파일 정책으로 트래픽을 검사하여 익스플로잇, 악성코드 또는 금지된 파일을 차단하도록 지정할 수 있습니다. 그러나 시스템에서는 트래픽을 신뢰 또는 차단한 후에는 추가 검사를 수행하지 **않습니다**.

다음 시나리오에는 인라인 침입 방지 구축에서 액세스 제어 규칙으로 트래픽을 평가할 수 있는 몇 가지 방법이 요약되어 있습니다.



이 시나리오에서 트래픽은 다음과 같이 평가됩니다.

- **규칙 1: 모니터링** — 트래픽을 첫 번째로 평가합니다. 모니터링 규칙은 네트워크 트래픽을 추적 및 로깅하지만 트래픽 플로우에 영향을 미치지 않습니다. 시스템은 허용 또는 거부 여부를 결정하기 위해 계속해서 트래픽이 추가 규칙과 일치하는지 확인합니다.
- **규칙 2: 신뢰** — 트래픽을 두 번째로 평가합니다. 일치하는 트래픽은 추가 검사 없이 목적지로 전달될 수 있습니다. 일치하지 않는 트래픽은 다음 규칙으로 계속 진행됩니다.
- **규칙 3: 차단** — 트래픽을 세 번째로 평가합니다. 일치하는 트래픽은 추가 검사 없이 차단됩니다. 일치하지 않는 트래픽은 마지막 규칙으로 계속 진행됩니다.
- **규칙 4: 허용** — 마지막 규칙입니다. 이 규칙에서, 일치하는 트래픽은 허용되지만 해당 트래픽 내 금지된 파일, 악성코드, 침입 및 익스플로잇은 탐지 및 차단됩니다. 나머지 금지되지 않은 비악성 트래픽은 목적지로 전달됩니다. 파일 검사나 침입 검사 중 하나만 수행하거나 둘 다 수행하지 않는 추가 허용 규칙을 사용할 수도 있습니다.
- **기본 작업** — 위의 규칙과 일치하지 않는 모든 트래픽을 처리합니다. 이 시나리오에서 기본 작업은 비악성 트래픽의 통과를 허용하기 전에 침입 방지를 수행하는 것입니다. 다른 구축에서는 추가 검사 없이 모든 트래픽을 신뢰 또는 차단하는 기본 작업을 사용할 수도 있습니다. (기본 작업에 의해 처리되는 트래픽에 대해서는 파일 또는 악성코드 검사를 수행할 수 없습니다.)

액세스 제어 규칙 또는 기본 작업을 통해 허용되는 트래픽은 자동으로 네트워크 검색 정책에 의한 호스트, 애플리케이션 및 사용자 데이터의 검사 대상이 됩니다. 검색을 강화 또는 비활성화할 수는 있지만 명시적으로 활성화하지는 마십시오. 그러나 트래픽을 허용한다고 해서 자동으로 검색 데이터 수집이 보장되는 것은 아닙니다. 시스템은 네트워크 검색 정책에 의해 명시적으로 모니터링되는 IP 주소와 관련된 연결에 대해서만 검색을 수행합니다. 추가로, 암호화된 세션에 대해서는 애플리케이션 검색이 제한됩니다. 자세한 내용은 45-1페이지의 네트워크 검색 소개을/를 참조하십시오.

SSL 검사 컨피그레이션에서 통과를 허용하는 경우 또는 SSL 검사를 구성하지 않은 경우, 액세스 제어 규칙이 암호화된 트래픽을 처리합니다. 그러나 일부 액세스 제어 규칙 조건에는 암호화되지 않은 트래픽이 필요하므로, 암호화된 트래픽과 일치하는 규칙이 더 적을 수 있습니다. 또한 기본적으로 시스템은 암호화된 페이로드의 침입 및 파일 검사를 비활성화합니다. 이는 암호화 연결이 침입 및 파일 검사가 구성된 액세스 제어 규칙과 일치하는 경우 오탐을 줄이고 성능을 높이는 데 도움이 됩니다. 자세한 내용은 19-1페이지의 트래픽 해독 이해 및 27-70페이지의 SSL 프리프로세서 사용을/를 참조하십시오.

액세스 제어 규칙에 대한 자세한 내용은 다음을 참조하십시오.

- 14-3페이지의 액세스 제어 규칙 생성 및 수정
- 14-13페이지의 정책의 액세스 제어 규칙 관리
- 12-21페이지의 액세스 제어 정책 및 규칙 문제 해결

액세스 제어 규칙 생성 및 수정

라이센스: 모두

액세스 제어 정책 내에서 액세스 제어 규칙은 여러 관리되는 디바이스 간에 세분화된 네트워크 트래픽 처리 방법을 제공합니다. 각 액세스 제어 규칙에는 고유한 이름 외에도 다음과 같은 기본 구성 요소가 있습니다.

주

기본적으로 규칙은 활성화되어 있습니다. 규칙을 비활성화하면 시스템은 네트워크 트래픽 평가에 규칙을 사용하지 않으며, 해당 규칙에 대해 경고 및 오류 생성을 중지합니다.

위치

액세스 제어 정책의 규칙은 번호가 1부터 시작합니다. 시스템은 오름차순 규칙 번호에 따라 하향식 순서로 트래픽이 규칙과 일치하는지를 확인합니다. 모니터링 규칙을 제외하고, 트래픽의 일치 여부를 확인하는 첫 번째 규칙은 해당 트래픽을 처리하는 규칙입니다.

상태

조건은 규칙이 처리하는 특정 트래픽을 지정합니다. 조건은 보안 영역, 네트워크 또는 지오로케이션, VLAN, 포트, 애플리케이션, 요청된 URL 또는 사용자 기준으로 트래픽의 일치 여부를 확인할 수 있습니다. 조건은 간단할 수도 있고 복잡할 수도 있습니다. 조건의 사용은 종종 대상 디바이스 라이센스 및 모델에 따라 다릅니다.

작업

규칙의 작업은 시스템이 일치하는 트래픽을 처리하는 방법을 결정합니다. 추가 검사와 함께 또는 추가 검사 없이, 일치하는 트래픽을 모니터링, 신뢰, 차단 또는 허용할 수 있습니다. 시스템은 신뢰받는 트래픽 또는 차단된 트래픽에 대해 검사를 수행하지 **않습니다**.

인스팩션

액세스 제어 규칙에 대한 검사 옵션은, 사용자가 허용할 수도 있는 악성 트래픽을 시스템이 검사 및 차단하는 방법을 제어합니다. 규칙으로 트래픽을 허용하는 경우 트래픽이 자산에 도달하거나 네트워크에서 빠져나가기 전에, 시스템에서 먼저 침입 또는 파일 정책으로 트래픽을 검사하여 익스플로잇, 악성코드 또는 금지된 파일을 차단하도록 지정할 수 있습니다.

로깅

규칙의 로깅 설정은, 처리하는 트래픽에 대해 시스템에서 유지하는 레코드를 관리합니다. 규칙과 일치하는 트래픽의 레코드를 유지할 수 있습니다. 일반적으로 연결의 시작 또는 끝에, 아니면 시작과 끝 모두에 세션을 로깅할 수 있습니다. 시스템 로그(syslog)나 SNMP 트랩 서버는 물론 방어 센터 데이터베이스에 대한 연결도 로깅할 수 있습니다.

코멘트

액세스 제어 규칙에 대한 변경 사항을 저장할 때마다 코멘트를 추가할 수 있습니다.

액세스 제어 규칙을 추가 및 수정하려면 액세스 제어 규칙 편집기를 사용하십시오. 액세스 제어 정책 편집기의 Rules 탭에서 규칙 편집기에 액세스할 수 있습니다. 규칙 편집기에서 다음을 수행할 수 있습니다.

- 편집기의 상단에서 규칙의 이름, 상태, 위치 및 작업과 같은 기본 속성을 구성합니다.
- 편집기의 하단 왼쪽에 있는 탭을 사용하여 조건을 추가합니다.
- 편집기의 하단 오른쪽에 있는 탭을 사용하여 검사 및 로깅 옵션을 구성하고, 규칙에 코멘트를 추가합니다. 편의를 위해, 사용자가 어떤 탭에 있든 편집기에는 규칙의 검사 및 로깅 옵션이 나열됩니다.

참고 액세스 제어 규칙을 제대로 만들고 순서를 지정하는 것은 복잡한 작업이지만, 효과적인 구축을 작성하기 위해 반드시 필요합니다. 정책을 신중하게 계획하지 않으면 규칙이 다른 규칙을 선점하거나, 추가 라이센스를 요구하거나, 잘못된 컨피그레이션을 포함할 수 있습니다. 시스템이 트래픽을 예상대로 처리하도록 보장하기 위해, 액세스 제어 정책 인터페이스에는 규칙에 대한 강력한 경고 및 오류 피드백 시스템이 있습니다. 자세한 내용은 12-21페이지의 액세스 제어 정책 및 규칙 문제 해결을/를 참조하십시오.

액세스 제어 규칙을 만들거나 수정하려면

액세스: Admin/Access Admin/Network Admin

1단계 **Policies > Access Control**을 선택합니다.

Access Control Policy 페이지가 나타납니다.

2단계 규칙을 추가할 액세스 제어 정책 옆에 있는 수정 아이콘( )을 클릭합니다.

정책 페이지가 나타나고 Rules 탭이 활성화됩니다.

3단계 다음 옵션을 이용할 수 있습니다.

- 새 규칙을 추가하려면 **Add Rule**을 클릭합니다.
- 기존 규칙을 수정하려면 수정하려는 규칙 옆에 있는 수정 아이콘( )을 클릭합니다.

액세스 제어 규칙 편집기가 나타납니다.

4단계 규칙의 **Name**을 입력합니다.

각 규칙에는 고유한 이름이 있어야 합니다. 콜론(:)을 제외한 특수 문자 및 공백을 포함하여 최대 30개의 인쇄 가능한 문자를 사용할 수 있습니다.

5단계 위에 요약된 대로 규칙 구성 요소를 구성합니다. 기본값을 제외하고 다음과 같이 구성할 수 있습니다.

- 규칙의 **Enabled** 여부를 지정합니다.
- 규칙 위치를 지정합니다. 14-5페이지의 규칙의 평가 순서 지정을/를 참조하십시오.
- 규칙 **Action**을 선택합니다. 14-8페이지의 규칙 작업을 사용하여 트래픽 처리 및 검사 확인을/를 참조하십시오.

- 규칙의 조건을 구성합니다. 14-6페이지의 조건을 사용하여 규칙이 처리할 트래픽 지정을/를 참조하십시오.
- 허용 및 인터랙티브 차단 규칙에 대해서는 규칙의 **Inspection** 옵션을 구성합니다. 18-1페이지의 침입 정책 및 파일 정책을 사용하여 트래픽 제어을/를 참조하십시오.
- **Logging** 옵션을 지정합니다. 38-1페이지의 네트워크 트래픽의 연결 로깅을/를 참조하십시오.
- **Comments**를 추가합니다. 14-13페이지의 규칙에 코멘트 추가을/를 참조하십시오.

6단계 **Save**를 클릭하여 규칙을 저장합니다.

규칙이 저장됩니다. 규칙을 삭제하려면 삭제 아이콘( )을 클릭할 수 있습니다. 변경 사항을 적용하려면 액세스 제어 정책을 적용해야 합니다. 12-15페이지의 액세스 제어 정책 적용을/를 참조하십시오.

규칙의 평가 순서 지정

라이센스: 모두

액세스 제어 규칙을 처음 만들 때에는 규칙 편집기의 **Insert** 드롭다운 목록을 사용하여 위치를 지정합니다. 액세스 제어 정책의 규칙은 번호가 1부터 시작합니다. 시스템은 오름차순 규칙 번호에 따라 하향식 순서로 트래픽이 액세스 제어 규칙과 일치하는지를 확인합니다.

대부분의 경우, 시스템은 *모든* 규칙의 조건이 트래픽과 매칭되는 *첫 번째* 액세스 제어 규칙에 따라 네트워크 트래픽을 처리합니다. 트래픽을 로깅하지만 트래픽 플로우에는 영향을 주지 않는 모니터링 규칙의 경우를 제외하고, 트래픽이 규칙과 일치한 이후 시스템은 더 낮은 우선순위의 추가 규칙에 대해 해당 트래픽을 계속해서 평가하지 **않습니다**.

팁 액세스 제어 규칙 순서를 적절히 지정하면 네트워크 트래픽 처리에 필요한 리소스가 감소하고 규칙 선점이 방지됩니다. 생성하는 규칙이 모든 조직과 구축에서 고유하더라도, 요구를 충족하면서도 성능을 최적화할 수 있는 규칙의 순서를 지정할 경우 따라야 할 몇 가지 일반 지침이 있습니다. 자세한 내용은 12-24페이지의 성능 향상 및 선점 방지를 위한 규칙 순서 지정을/를 참조하십시오.

번호로 규칙의 순서를 지정하는 것 외에도 카테고리로 규칙을 그룹화할 수 있습니다. 기본적으로 시스템에서는 관리자, 표준 및 루트의 세 카테고리를 제공합니다. 사용자 지정 카테고리를 추가할 수 있지만, Cisco에서 제공하는 카테고리의 경우 삭제하거나 순서를 변경할 수는 없습니다. 기존 규칙의 위치나 카테고리를 변경하는 방법에 대한 자세한 내용은 14-16페이지의 규칙의 위치 또는 카테고리 변경을/를 참조하십시오.

규칙을 수정 또는 생성하는 동안 카테고리에 추가하려면

액세스: Admin/Access Admin/Network Admin

1단계 액세스 제어 규칙 편집기의 **Insert** 드롭다운 목록에서 **Into Category**를 선택한 다음 사용할 카테고리를 선택합니다.

규칙을 저장하면 해당 카테고리의 맨 끝에 배치됩니다.

규칙을 수정 또는 생성하는 동안 번호순으로 배치하려면

액세스: Admin/Access Admin/Network Admin

1단계 액세스 제어 규칙 편집기의 **Insert** 드롭다운 목록에서 **above rule** 또는 **below rule**을 선택한 다음 적절한 규칙 번호를 입력합니다.

규칙을 저장하면 지정한 위치에 배치됩니다.

조건을 사용하여 규칙이 처리할 트래픽 지정

라이센스: 기능에 따라 다름

지원되는 디바이스: 기능에 따라 다름

지원되는 Defense Center: 기능에 따라 다름

액세스 제어 규칙의 조건은 규칙이 처리하는 트래픽 유형을 식별합니다. 조건은 간단할 수도 있고 복잡할 수도 있습니다. 보안 영역, 네트워크 또는 지오로케이션, VLAN, 포트, 애플리케이션, 요청된 URL 및 사용자별로 트래픽을 제어할 수 있습니다.

액세스 제어 규칙에 조건을 추가할 경우에는 다음을 염두에 두십시오.

- 규칙당 여러 조건을 구성할 수 있습니다. 규칙을 트래픽에 적용할 수 있으려면 트래픽이 규칙의 **모든** 조건과 일치해야 합니다. 예를 들면, 특정 호스트에 대해 URL 필터링(URL 조건)을 수행하려면 단일 규칙을 사용할 수 있습니다.
- 규칙의 각 조건에 대해 최대 50개의 기준을 추가할 수 있습니다. **임의의** 조건 기준과 일치하는 트래픽은 조건을 충족합니다. 예를 들면 단일 규칙을 사용하여 최대 50의 사용자 및 그룹에 대해 사용자 제어를 수행할 수 있습니다.

최대 50개의 소스 및 최대 50개의 목적지 기준을 사용하여 소스 및 목적지별로 영역과 네트워크 조건을 제한할 수 있습니다. 영역 또는 네트워크 조건에 소스와 목적지 기준을 모두 추가하면, 일치하는 트래픽은 지정된 소스 영역/네트워크 중 하나에서 와야 하고 **또한** 목적지 영역/네트워크 중 하나를 통해 나가야 합니다. 다시 말하면 시스템은 동일한 유형의 여러 조건 기준을 OR 연산자로 연결하고, 여러 조건 유형을 AND 연산자로 연결합니다. 예를 들어 규칙 조건이 다음과 같은 경우:

```
Source Networks: 10.0.0.0/8, 192.168.0.0/16
Application Category: peer to peer
```

규칙은 사설 IPv4 네트워크 중 하나에서 호스트의 피어 투 피어 애플리케이션 트래픽과 일치해야 하며, 패킷은 둘 중 하나 **또는(OR)** 다른 소스 네트워크에서 와야 하고 **그리고(AND)** 피어 투 피어 애플리케이션 트래픽을 나타내야 합니다. 다음 연결은 둘 다 규칙을 트리거합니다.

```
10.42.0.105 to anywhere, using LimeWire
192.168.42.105 to anywhere, using Kazaa
```

규칙에 대해 특별한 조건을 구성하지 않으면 시스템에서는 해당 기준을 기반으로 트래픽의 일치를 확인하지 않습니다. 예를 들어, 네트워크 조건만 있고 애플리케이션 조건은 없는 규칙은 세션에서 사용되는 애플리케이션과 상관없이 소스 또는 목적지를 기준으로 트래픽을 평가합니다.

참고 액세스 제어 정책을 적용하면 시스템은 모든 규칙을 평가하고 대상 디바이스가 네트워크 트래픽을 평가하기 위해 사용하는 확장 기준 집합을 생성합니다. 복잡한 액세스 제어 정책 및 규칙은 상당한 자원을 소모할 수 있습니다. 성능 향상을 위한 액세스 제어 규칙 간소화 방법 및 기타 방법에 대해 알아보려면 12-21페이지의 액세스 제어 정책 및 규칙 문제 해결을/를 참조하십시오.

액세스 제어 규칙을 추가 또는 수정할 때에는 규칙 편집기의 하단 왼쪽에 있는 탭을 사용하여 규칙 조건을 추가 및 수정하십시오. 다음 표에는 추가할 수 있는 조건 유형이 요약되어 있습니다.

표 14-1 액세스 제어 규칙 조건 유형

조건	트래픽 일치 확인	세부 사항
영역	특정 보안 영역에서 인터페이스를 통해 디바이스로 들어가거나 디바이스에서 나옴	보안 영역은 구축 및 보안 정책에 따라 하나 이상의 인터페이스를 논리적으로 그룹화한 것입니다. 한 영역의 인터페이스는 여러 디바이스에 걸쳐 있을 수 있습니다. 영역 조건을 작성하려면 15-2페이지의 보안 영역을 통한 트래픽 제어을/를 참조하십시오.
네트워크	소스 또는 목적지 IP 주소, 국가 또는 대륙별	IP 주소 또는 주소 블록을 명시적으로 지정할 수 있습니다. 지오로케이션 기능을 사용해도 소스 또는 목적지 국가나 대륙을 기반으로 트래픽을 제어할 수 있습니다. 네트워크 조건을 작성하려면 15-3페이지의 네트워크 또는 지리적 위치로 트래픽 제어을/를 참조하십시오.
VLAN Tags	VLAN별로 태그됨	시스템에서는 가장 안쪽의 VLAN 태그를 사용하여 VLAN을 기준으로 패킷을 확인합니다. VLAN 조건을 작성하려면 15-5페이지의 VLAN 트래픽 제어을/를 참조하십시오.
포트	소스 또는 목적지 포트별	TCP 및 UDP의 경우 전송 레이어 프로토콜을 기반으로 트래픽을 제어할 수 있습니다. ICMP 및 ICMPv6(IPv6-ICMP)의 경우 인터넷 레이어 프로토콜과 선택적인 유형 및 코드를 기반으로 트래픽을 제어할 수 있습니다. 포트 조건을 사용하면, 포트를 사용하지 않는 다른 프로토콜을 사용하여 트래픽을 제어할 수도 있습니다. 포트 조건을 작성하려면 15-7페이지의 포트 및 ICMP 코드로 트래픽 제어을/를 참조하십시오.
애플리케이션	세션에서 탐지되는 애플리케이션별	개별 애플리케이션에 대한 액세스를 제어하거나, 기본 특성인 유형, 위험, 비즈니스 연관성, 카테고리 및 태그 에 따라 액세스를 필터링할 수 있습니다.애플리케이션 조건을 작성하려면 16-2페이지의 애플리케이션 트래픽 제어을/를 참조하십시오.
URL	세션에서 요청된 URL별	네트워크의 사용자가 개별적으로 또는 URL의 일반 분류 및 위험 레벨을 기반으로 액세스할 수 있는 웹사이트를 제한할 수 있습니다. URL 조건을 작성하려면 16-8페이지의 URL 차단을/를 참조하십시오.
사용자	세션에 개입된 사용자별	모니터링되는 세션에 개입된 호스트에 로그인한 LDAP 사용자를 기반으로 트래픽을 제어할 수 있습니다. Microsoft Active Directory 서버에서 검색된 개별 사용자 또는 그룹을 기반으로 트래픽을 제어할 수 있습니다. 사용자 조건을 작성하려면 17-1페이지의 사용자 기반으로 트래픽 제어을/를 참조하십시오.

어떤 라이센스로든 액세스 제어 규칙을 생성할 수 있지만, 특정 규칙 조건에서는 정책을 적용하려면 우선 액세스 제어 정책의 대상 디바이스에서 특정 라이센스 기능을 활성화해야 합니다. 자세한 내용은 12-2페이지의 액세스 제어를 위한 라이센스 및 모델 요구 사항을/를 참조하십시오.

규칙 작업을 사용하여 트래픽 처리 및 검사 확인

라이센스: 모두

모든 액세스 제어 규칙에는 일치하는 트래픽을 위해 다음을 확인하는 *작업*이 있습니다.

- 처리 — 무엇보다도, 규칙 작업은 규칙 조건과 일치하는 트래픽을 시스템이 모니터링, 신뢰, 차단 또는 허용할지 여부를 관리합니다.
- 검사 — 특정 규칙 작업에서는(해당 라이센스가 있는 경우) 통과를 허용하기 전에 일치하는 트래픽을 추가로 검사할 수 있습니다.
- 로깅 — 규칙 작업은 일치하는 트래픽에 대한 세부사항을 로깅할 수 있는 시기와 방법을 결정합니다.

액세스 제어 정책의 *기본 작업*은 비 모니터링 액세스 제어 규칙의 조건을 충족하지 않는 트래픽을 처리합니다. 12-6페이지의 네트워크 트래픽의 기본 처리 및 검사 설정을/를 참조하십시오.

인라인으로 구축된 디바이스만 트래픽을 차단 또는 수정할 수 있습니다. 패시브 방식으로 또는 탭 모드에서 구축한 디바이스는 트래픽 플로우를 분석 및 로깅할 수는 있지만, 트래픽 플로우에 영향을 주지는 않습니다. 규칙 작업 및 규칙 작업이 트래픽 처리, 검사 및 로깅에 미치는 영향에 대해 자세히 알아보려면 다음 절을 참조하십시오.

- 14-8페이지의 모니터링 작업: 작업 연기 및 로깅 보장
- 14-9페이지의 신뢰 작업: 검사 없이 트래픽 전달
- 14-9페이지의 작업 차단: 검사 없이 트래픽 차단
- 14-10페이지의 Interactive Blocking 작업: 사용자가 웹사이트 차단을 우회하도록 허용
- 14-11페이지의 Allow 작업: 트래픽 허용 및 검사
- 14-12페이지의 Series 3 디바이스를 이용한 트래픽 신뢰 또는 차단 제한 사항
- 18-1페이지의 침입 정책 및 파일 정책을 사용하여 트래픽 제어
- 38-15페이지의 액세스 제어 처리 기반 연결 로깅

모니터링 작업: 작업 연기 및 로깅 보장

라이센스: 모두

모니터링 작업은 트래픽 플로우에 영향을 미치지 않습니다. 일치하는 트래픽은 즉시 허용 또는 거부되지 않습니다. 대신 허용 또는 거부를 결정할 수 있도록, 트래픽이 추가 규칙과 일치하는지 확인합니다. 일치하는 첫 번째 비 모니터링 규칙은 트래픽 플로우 및 추가 검사를 결정합니다. 추가로 일치하는 규칙이 없으면 시스템은 기본 작업을 사용합니다.

모니터링 규칙의 기본 목적은 네트워크 트래픽을 추적하는 것이므로, 시스템은 모니터링된 트래픽의 연결 끝 이벤트를 자동으로 로깅합니다. 즉, 트래픽과 일치하는 다른 규칙이 없고 기본 작업에서 로깅을 활성화하지 않은 경우에도 연결이 로깅됩니다. 자세한 내용은 38-6페이지의 모니터링되는 연결에 대한 로깅 이해을/를 참조하십시오.

참고 로컬에서 바인딩된 트래픽이 레이어 3 구축에서 모니터링 규칙과 일치하면, 해당 트래픽은 검사를 우회할 수 있습니다. 트래픽의 검사를 보장하려면 트래픽을 라우팅하는 관리되는 디바이스의 고급 디바이스 설정에서 **Inspect Local Router Traffic**을 활성화하십시오. 자세한 내용은 4-54페이지의 고급 디바이스 설정 이해을/를 참조하십시오.

신뢰 작업: 검사 없이 트래픽 전달

라이센스: 모두

신뢰 작업은 어떤 종류의 추가 검사도 없이 트래픽 통과를 허용합니다.

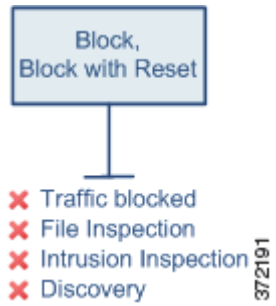
연결의 시작과 끝에서 모두 신뢰할 수 있는 네트워크 트래픽을 로깅할 수 있습니다. 시스템은 연결을 탐지한 디바이스의 모델에 따라 다르게, 신뢰 규칙에 의해 처리되는 TCP 연결을 로깅합니다. 자세한 내용은 38-7페이지의 신뢰하는 연결에 대한 로깅 이해을/를 참조하십시오.

주의 Series 3 디바이스에 의해 처리되는 트래픽의 경우 시스템은 액세스 제어 정책의 보안 인텔리전스 블랙리스트 이전에 특정 신뢰 규칙을 처리하는데, 이 경우 블랙리스트 트래픽이 검사 없이 통과될 수 있습니다. 자세한 내용은 14-12페이지의 Series 3 디바이스를 이용한 트래픽 신뢰 또는 차단 제한 사항을/를 참조하십시오.

작업 차단: 검사 없이 트래픽 차단

라이센스: 모두

Block 및 **Block with reset** 작업은 어떤 종류의 추가 검사도 없이 트래픽을 거부합니다. Block with reset 규칙은 연결도 재설정합니다.



암호화되지 않은 또는 HTTP 트래픽의 경우 시스템이 웹 요청을 차단하면, 사용자는 연결이 거부되었음을 설명하는 사용자 지정 페이지로 기본 브라우저 또는 서버 페이지를 재정의할 수 있습니다. 시스템에서는 이러한 사용자 지정 페이지를 *HTTP 응답 페이지*라고 합니다. 16-17페이지의 차단된 URL에 대한 사용자 지정 웹 페이지 표시을/를 참조하십시오.

암호 해독된/암호화된(HTTPS) 트래픽의 경우 인터랙티브 차단 규칙은 상호 작용 없이 일치하는 연결을 차단하며, 시스템은 응답 페이지를 표시하지 **않습니다**.

시스템은 Series 3 디바이스에 의해 처리되는 일부 성공적으로 차단된 트래픽에 대해 구성된 응답 페이지를 표시하지 않습니다. 대신, 금지된 URL을 요청하는 사용자는 연결이 재설정되거나 시간 초과됩니다. 자세한 내용은 14-12페이지의 Series 3 디바이스를 이용한 트래픽 신뢰 또는 차단 제한 사항을/를 참조하십시오.

연결의 시작에서만 차단된 네트워크 트래픽을 로깅할 수 있습니다. 인라인으로 구축된 디바이스만 트래픽을 차단할 수 있습니다. 차단된 연결은 패시브 구축에서 실제로 차단되지 않으므로, 시스템은 각각의 차단된 연결에 대해 여러 개의 연결 시작 이벤트를 보고할 수 있습니다. 자세한 내용은 38-7페이지의 차단된 연결 및 인터랙티브 차단된 연결에 대한 로깅 이해을/를 참조하십시오.

주의 DoS(서비스 거부) 공격 중에 차단된 TCP 연결을 로깅하는 경우 시스템 성능에 영향을 미칠 수 있으며, 데이터베이스가 유사한 다수의 이벤트로 가득 찰 수 있습니다. 차단 규칙에 대한 로깅을 활성화하기 전에, 인터넷에 접하는 인터페이스 또는 DoS 공격에 취약한 다른 인터페이스에서 트래픽을 모니터링할지 여부를 고려하십시오.

Interactive Blocking 작업: 사용자가 웹사이트 차단을 우회하도록 허용

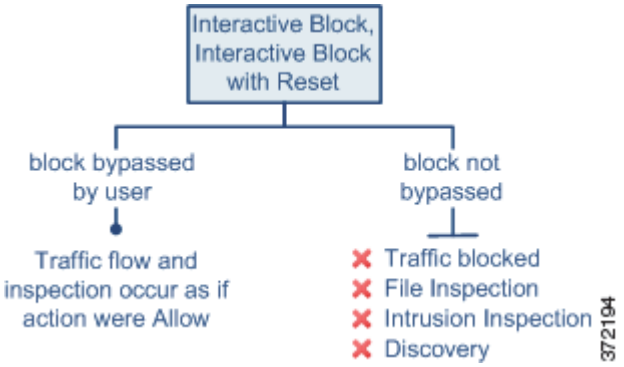
라이센스: 모두

암호화되지 않은 또는 HTTP 트래픽의 경우, **Interactive Block** 및 **Interactive Block with reset** 작업은 사용자에게 *HTTP response page*라는 사용자 지정 경고 페이지를 클릭하여 웹사이트 차단을 우회할 수 있는 기회를 제공합니다. Interactive Block with reset 규칙은 연결도 재설정합니다.

참고 암호 해독된/암호화된(HTTPS) 트래픽의 경우 인터랙티브 차단 규칙은 상호 작용 없이 일치하는 연결을 차단하며, 시스템은 응답 페이지를 표시하지 **않습니다**. 트래픽을 암호 해독하도록 SSL 검사 기능을 구성하는 방법에 대한 자세한 내용은 19-1페이지의 트래픽 해독 이해을/를 참조하십시오.

인터랙티브 방식으로 차단된 모든 트래픽에서 시스템의 처리, 검사 및 로깅은 사용자가 차단을 우회하는지 여부에 따라 달라집니다.

- 사용자가 차단을 우회하지 않으면(또는 우회할 수 없으면) 규칙은 차단 규칙을 모방합니다. 일치하는 트래픽이 추가 검사 없이 거부되며 사용자는 연결의 시작 부분만 로깅할 수 있습니다. 이러한 연결 시작 이벤트는 `Interactive Block` 또는 `Interactive Block with Reset` 작업을 사용합니다.
- 사용자가 차단을 우회하면 규칙은 허용 규칙을 모방합니다. 따라서 인터랙티브 차단 규칙 중 한 유형을 파일 및 침입 정책과 연결하여, 사용자가 허용한 이 트래픽을 검사할 수 있습니다. 시스템은 네트워크 검색을 사용하여 검사할 수도 있으며, 사용자는 연결의 시작 및 끝 이벤트를 모두 로깅할 수 있습니다. 이러한 연결 이벤트는 `Allow` 작업을 사용합니다.



Allow 작업: 트래픽 허용 및 검사

라이센스: 모두

Allow 작업은 일치하는 트래픽의 통과를 허용합니다. 트래픽을 허용할 경우, 암호화되지 않은 또는 암호 해독된 네트워크 트래픽을 추가로 조사하거나 차단하기 위해 연결된 침입 또는 파일 정책(또는 둘 모두)을 사용할 수 있습니다.

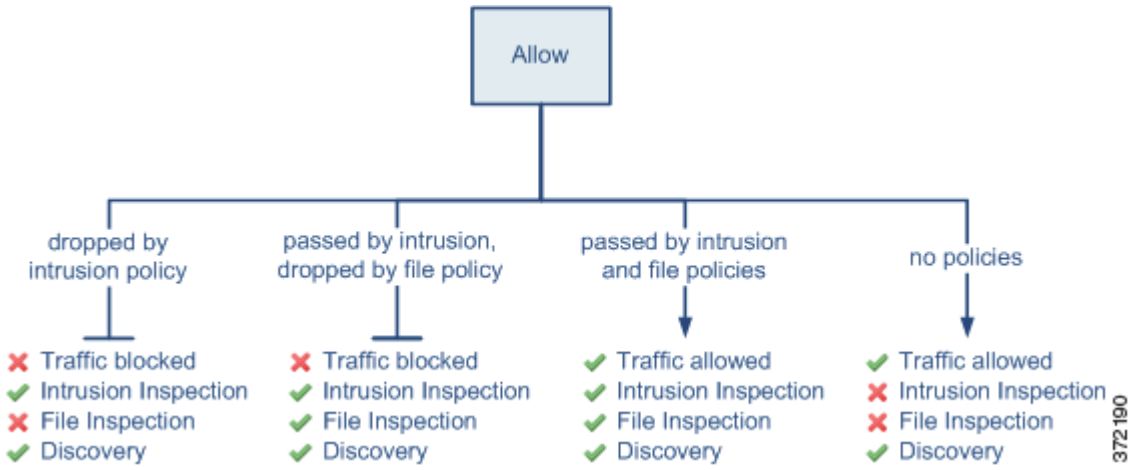
- 보호 라이센스가 있으면 침입 정책을 사용하여 침입 탐지 및 방지 컨피그레이션에 따라 네트워크 트래픽을 분석할 수 있으며, 선택적으로 위반 패킷을 삭제할 수 있습니다.
- 또한 보호 라이센스가 있으면 파일 정책을 사용하여 파일 제어를 수행할 수 있습니다. 파일 제어를 수행하면, 사용자가 특정 애플리케이션 프로토콜에서 특정 유형의 파일을 업로드(전송) 또는 다운로드(수신)하는 행동을 탐지하고 차단할 수 있습니다.
- 악성코드 라이센스가 있으면 역시 파일 정책을 사용하여 네트워크 기반 AMP(advanced malware protection)를 수행할 수 있습니다. 네트워크 기반 AMP는 파일에서 악성코드를 검색할 수 있으며, 선택적으로 탐지된 악성코드를 차단할 수 있습니다.

침입 또는 파일 정책을 액세스 제어 규칙과 연결하는 방법에 대한 자세한 내용은 18-1페이지의 침입 정책 및 파일 정책을 사용하여 트래픽 제어을/를 참조하십시오.

아래의 다이어그램은 허용 규칙의 조건을 충족하는 트래픽에 대해 수행되는 검사 유형을 설명합니다(또는 사용자 우회 인터랙티브 차단 규칙은 14-10페이지의 Interactive Blocking 작업: 사용자가 웹사이트 차단을 우회하도록 허용 참조). 파일 검사는 침입 검사 전에 발생합니다. 차단된 파일에 대해서는 침입 관련 익스플로잇을 검사하지 않습니다.

간소화를 위해 다이어그램에서는 침입과 파일 정책이 모두 액세스 제어 규칙과 연결된(또는 둘 다 연결되지 않은) 상황에 대한 트래픽 플로우를 표시합니다. 그러나 하나가 없더라도 다른 하나를 구성할 수 있습니다. 파일 정책이 없으면 트래픽 플로우는 침입 정책에 의해 결정되고, 침입 정책이 없으면 트래픽 플로우는 파일 정책에 의해 결정됩니다.

침입 또는 파일 정책에 의해 트래픽이 검사되든 삭제되든 상관없이, 시스템은 네트워크 검색을 사용하여 트래픽을 검사할 수 있습니다. 그러나 트래픽을 허용한다고 해서 자동으로 검색 검사가 보장되는 것은 아닙니다. 시스템은 네트워크 검색 정책에 의해 명시적으로 모니터링되는 IP 주소와 관련된 연결에 대해서만 검색을 수행합니다. 추가로, 암호화된 세션에 대해서는 애플리케이션 검색이 제한됩니다. 자세한 내용은 45-1페이지의 네트워크 검색 소개을/를 참조하십시오.



연결의 시작과 끝에서 모두 허용되는 네트워크 트래픽을 로깅할 수 있습니다.

Series 3 디바이스를 이용한 트래픽 신뢰 또는 차단 제한 사항

라이센스: 모두

지원되는 디바이스: Series 3

액세스 제어 정책을 Series 3 디바이스에 적용하면 시스템에서는 특정 기준을 충족하는 액세스 제어 규칙을 *프로모션*할 수 있습니다. 프로모션된 규칙은 Series 3 디바이스에서 특수 하드웨어를 활용하여, DPI(Deep Packet Inspection)가 필요하지 않은 트래픽을 전환 또는 차단합니다. 트래픽을 위한 올바른 경로를 결정하는 속도가 이 기능의 장점입니다.

이 평가는 하드웨어 레벨에서 시간이 소요되므로, 시스템은 규칙을 프로모션하여 연결을 신속하게 처리하는 데 제한된 정보만 사용할 수 있습니다. Series 3 디바이스는 다음 기준을 모두 충족하는 규칙을 프로모션합니다.

- **Trust**, **Block** 또는 **Block with reset** 작업이 있는 규칙
- 간단한 네트워크 기반 **조건만** 사용하는 규칙: 보안 영역, IP 주소, VLAN 태그 및 포트
- DPI(Deep Packet Inspection)를 수행하는, 즉 애플리케이션, URL, 사용자 또는 지오로케이션 기반 조건이 있는 다른 **모든** 액세스 제어 규칙 위에 있는 규칙(작업과 무관)
- 또한 **모든** 모니터링 규칙 위에 있는 규칙

따라서 성능 개선을 위해 프로모션된 규칙은 대부분 간단한 신뢰 또는 차단 규칙으로서, 액세스 제어 정책의 상단 근처에 있거나(번호가 낮은 규칙) 간단한 네트워크 기반 규칙만 사용하는 정책에 있습니다. 그러나 규칙 프로모션에서 실현된 성능 이점은 예기치 않은 동작을 일으킬 수 있습니다.

보안 인텔리전스 선점

시스템은 액세스 제어 정책의 보안 인텔리전스 블랙리스트 이전에 프로모션된 규칙을 처리합니다. 즉, 프로모션된 신뢰 규칙은 블랙리스트에 있는 트래픽이 Series 3 디바이스를 검사 없이 통과하도록 허용할 수 있습니다. 보안 인텔리전스에 대한 자세한 내용은 13-1페이지의 보안 인텔리전스 IP 주소 평판 블랙리스트에 추가을/를 참조하십시오.

HTTP 응답 페이지 표시 방지

프로모션된 차단 규칙에 의해 웹 트래픽이 차단되면, 시스템은 트래픽을 성공적으로 차단하더라도 구성된 HTTP 응답 페이지를 사용자에게 표시할 수 없습니다. 대신, 금지된 URL을 요청하는 사용자는 연결이 재설정되거나 시간 초과됩니다. 응답 페이지를 구성하는 방법에 대한 자세한 내용은 16-17페이지의 차단된 URL에 대한 사용자 지정 웹 페이지 표시을/를 참조하십시오.

IPv6 트래픽 처리

시스템은 IPv4 및 IPv6 트래픽을 모두 검사할 수 있습니다. IPv6 검사에는 4in6, 6in4, 6to4 및 6in6 터널링 체계가 포함되며, UDP 헤더가 포트 3544를 지정하는 경우 Teredo 터널링도 포함됩니다. IP 주소 조건과 함께 액세스 제어 규칙을 사용하여 트래픽을 평가하면, 대부분의 경우 Series 3 디바이스는 사용자가 지정한 IP 주소를 가장 안쪽 패킷 헤더에 있는 IP 주소와 확인합니다.

그러나 프로모션된 규칙은 트래픽의 터널링 여부와 상관없이, 그리고 IPv6 헤더가 어디에 있는지(가장 안쪽이든 가장 바깥쪽이든)와 상관없이, **가장 바깥쪽** 헤더에 있는 IP 주소를 사용하여 IPv6 트래픽을 평가합니다. 다시 말하면, 프로모션된 규칙이 터널링된 트래픽을 평가할 때 4in4 트래픽은 액세스 제어 규칙 기준의 일치 여부를 확인하는 데 가장 안쪽 헤더만 사용합니다.

예를 들어 IPv4 네트워크를 통해 전송되는 6in4 터널링된 트래픽을 검사하기 위해 Series 3 디바이스를 사용하는 시나리오를 가정해보겠습니다. 특정 IPv6 주소와 주고받는 트래픽을 차단하는 간단한 네트워크 기반 액세스 제어 규칙을 생성합니다. 시스템이 액세스 제어 정책에 있는 위치를 기준으로 규칙을 프로모션하면 해당 규칙은 아무런 영향도 미치지 않습니다. 시스템은 터널링된 패킷의 가장 바깥쪽 IPv4 헤더를 IPv6 규칙 조건에 대해 확인하는데, 이는 트리거될 수 없기 때문입니다. 시스템은 후속 액세스 제어 규칙 또는 정책의 기본 작업을 사용하여 규칙이 존재하지 않는 것처럼 트래픽을 처리합니다.

규칙에 코멘트 추가

라이센스: 모두

액세스 제어 규칙을 생성 또는 수정할 때 코멘트를 추가할 수 있습니다. 예를 들면 다른 사용자에게 도움이 되도록 전체적인 컨피그레이션을 요약하거나, 규칙을 변경한 시기 및 변경 이유를 적을 수 있습니다. 각 코멘트를 추가한 사용자 및 코멘트 추가 날짜와 함께 규칙에 대한 모든 코멘트의 목록을 표시할 수 있습니다.

팁 액세스 제어 규칙을 저장할 때 FireSIGHT 시스템 사용자에게 코멘트를 입력하도록 프롬프트를 표시하는 방법은 63-8페이지의 액세스 제어 정책 환경 설정 구성을/를 참조하십시오.

규칙을 저장하면, 마지막 저장 이후 생성된 모든 코멘트는 읽기 전용이 됩니다.

규칙에 코멘트를 추가하려면

액세스: Admin/Access Admin/Network Admin

1단계 액세스 제어 규칙 편집기에서 **Comments** 탭을 선택합니다.

Comments 페이지가 나타납니다.

2단계 **New Comment**를 클릭합니다.

New Comment 팝업 창이 나타납니다.

3단계 코멘트를 입력하고 **OK**를 클릭합니다.

코멘트가 저장됩니다. 규칙을 저장할 때까지 이 코멘트를 수정 또는 삭제할 수 있습니다.

4단계 규칙을 저장하거나 계속 수정합니다.

정책의 액세스 제어 규칙 관리

라이센스: 모두

다음 그래프에 나오는 액세스 제어 정책 편집기의 Rules 탭에서는 정책 내 액세스 제어 규칙을 추가, 수정, 검색, 이동, 활성화, 비활성화, 삭제 및 관리할 수 있습니다.

정책 편집기에는 각 규칙의 이름, 조건의 요약, 규칙 작업이 표시되며 규칙의 검사 및 로깅 옵션을 알리는 아이콘도 표시됩니다. 다른 아이콘은 다음 표에 설명된 대로 코멘트, 경고, 오류 및 기타 중요한 정보를 나타냅니다. 비활성화된 규칙은 회색으로 처리되며, 규칙 이름 아래에 (disabled)가 표시됩니다.

표 14-2 액세스 제어 정책 편집기 이해

아이콘	설명	가능한 작업
	침입 검사	규칙에 대한 검사 옵션을 수정하려면 활성(노란색) 검사 아이콘을 클릭합니다. 18-1페이지의 침입 정책 및 파일 정책을 사용하여 트래픽 제어을/를 참조하십시오. 아이콘이 비활성 상태이면(흰색) 규칙에 대해 해당 유형의 정책이 선택되지 않습니다.
	파일 및 악성 코드 검사	
	로깅	규칙에 대한 로깅 옵션을 수정하려면 활성(파란색) 로깅 아이콘을 클릭합니다. 38-15페이지의 액세스 제어 처리 기반 연결 로깅을/를 참조하십시오. 아이콘이 비활성 상태이면(흰색) 규칙에 대해 연결 로깅이 활성화되지 않습니다.
	참고	규칙에 코멘트를 추가하려면 코멘트 열에서 숫자를 클릭합니다. 14-13페이지의 규칙에 코멘트 추가을/를 참조하십시오. 숫자는 규칙에 이미 포함되어 있는 코멘트 수를 나타냅니다.
	경고	경고, 오류 또는 정보 텍스트를 읽으려면 포인터를 아이콘으로 가져갑니다. 12-21페이지의 액세스 제어 정책 및 규칙 문제 해결을/를 참조하십시오.
	오류	
	정보	

액세스 제어 규칙 관리에 대한 자세한 내용은 다음을 참조하십시오.

- 14-3페이지의 액세스 제어 규칙 생성 및 수정
- 14-14페이지의 액세스 제어 규칙 검색
- 14-15페이지의 영향받는 디바이스별 규칙 표시
- 14-16페이지의 규칙 활성화 및 비활성화
- 14-16페이지의 규칙의 위치 또는 카테고리 변경

액세스 제어 규칙 검색

라이센스: 모두

공백 및 인쇄 가능한 특수 문자를 비롯한 영숫자 문자열을 사용하여 액세스 제어 규칙 목록에서 일치하는 값을 검색할 수 있습니다. 규칙 이름과 규칙에 추가한 규칙 조건을 검사하게 됩니다. 규칙 조건의 경우, 각 조건 유형(영역, 네트워크, 애플리케이션 등)에 대해 추가할 수 있는 이름 또는 값의 일치 여부를 확인합니다. 여기에는 개별 객체 이름 또는 값, 그룹 객체 이름, 그룹 내 개별 객체 이름 또는 값, 리터럴 값 등이 포함됩니다.

전체 또는 부분 검색 문자열을 사용할 수 있습니다. 일치하는 값의 열이 일치하는 각 규칙에 대해 강조 표시됩니다. 예를 들어 100Bao 문자열의 전체 또는 일부를 검색하면, 100Bao 애플리케이션을 추가한 각 규칙에 대해 최소한 Applications 열이 강조 표시됩니다. 100Bao라는 이름의 규칙도 있다면 Name 및 Applications 열이 강조 표시됩니다.

각각의 이전 또는 다음의 일치하는 규칙으로 이동할 수 있습니다. 상태 메시지에는 현재의 일치 및 총 일치 수가 표시됩니다.

다중 페이지 규칙 목록의 어떤 페이지에서나 일치가 발생할 수 있습니다. 첫 번째 일치가 첫 번째 페이지에 없으면, 첫 번째 일치가 발생하는 페이지가 표시됩니다. 마지막 일치에 있을 때 다음 일치를 선택하면 첫 번째 일치로 이동하며, 첫 번째 일치에 있을 때 이전 일치를 선택하면 마지막 일치로 이동합니다.

규칙을 검색하려면

액세스: Admin/Access Admin/Network Admin

1단계 검색하려는 정책의 액세스 제어 정책 편집기에서 **Search Rules** 프롬프트를 클릭하고, 검색 문자열을 입력하고, Enter 키를 누릅니다. Tab 키를 사용하거나 빈 페이지 영역을 클릭하여 검색을 시작할 수도 있습니다.

일치하는 값이 있는 규칙의 열이 강조 표시되고, 표시된(첫 번째) 일치에 대해서는 다른 강조 표시가 사용됩니다.

2단계 관심이 있는 첫 번째 규칙을 찾습니다.

- 규칙 간에 이동하려면 다음 검색(▼) 또는 이전 검색(▲) 아이콘을 클릭합니다.
- 페이지를 새로 고치고 검색 문자열 및 강조 표시를 지우려면 지우기 아이콘(✖)을 클릭합니다.

영향받는 디바이스별 규칙 표시

라이센스: 모두

하나 이상의 지정된 디바이스에 대해 트래픽을 관리하는 규칙만 표시하려면 액세스 제어 정책에 나열된 액세스 제어 규칙을 필터링할 수 있습니다.

디바이스에 영향을 미치는 규칙을 확인하기 위해 시스템에서는 액세스 제어 규칙의 영역 조건을 사용합니다. 보안 영역은 인터페이스를 논리적으로 그룹화한 것이므로, 영역 조건에 인터페이스가 포함되어 있으면 해당 인터페이스가 있는 트래픽을 처리하는 디바이스는 해당 규칙의 영향을 받습니다. 영역 조건이 없는 규칙은 모든 영역, 따라서 모든 디바이스에 적용됩니다.

새 규칙을 추가하거나 기존 규칙을 수정 및 저장하면 필터가 지워집니다.

디바이스 또는 디바이스 그룹별로 규칙을 필터링하려면

액세스: Admin/Access Admin/Network Admin

1단계 필터링하려는 정책의 액세스 제어 정책 편집기에서 규칙 목록 위에 있는 **Filter by Device**를 클릭합니다.

Filter by Device 팝업 창이 나타납니다. 정책에 디바이스 또는 디바이스 그룹을 추가한 경우 대상 디바이스 및 디바이스 그룹의 목록이 나타납니다.

2단계 해당 디바이스 또는 그룹에 적용되는 규칙만 표시하려면 하나 이상의 확인란을 선택합니다. 또는, 재설정하고 모든 규칙을 표시하려면 **All** 확인란을 선택합니다.

3단계 **OK**를 클릭합니다.

선택한 디바이스 및 디바이스 그룹에 대한 규칙을 표시하고 선택하지 않은 디바이스 및 디바이스 그룹에 대한 규칙을 숨기도록 페이지가 업데이트됩니다.

규칙 활성화 및 비활성화

라이센스: 모두

액세스 제어 규칙을 생성하면 기본적으로 활성화됩니다. 규칙을 비활성화하면 시스템은 네트워크 트래픽 평가에 규칙을 사용하지 않으며, 해당 규칙에 대해 경고 및 오류 생성을 중지합니다. 액세스 제어 정책에서 규칙 목록을 볼 경우 비활성화된 규칙은 회색으로 표시됩니다(그래도 수정은 가능함). 규칙 편집기를 사용하여 액세스 제어 규칙을 활성화 또는 비활성화할 수도 있습니다. 14-3페이지의 액세스 제어 규칙 생성 및 수정을/를 참조하십시오.

액세스 제어 규칙의 상태를 변경하려면

액세스: Admin/Access Admin/Network Admin

1단계 활성화 또는 비활성화하려는 규칙이 포함된 정책의 액세스 제어 정책 편집기에서 규칙을 마우스 오른쪽 버튼으로 클릭하고 규칙 상태를 선택합니다.

- 비활성화된 규칙을 활성화하려면 **State > Enable**을 선택합니다.
- 활성 규칙을 비활성화하려면 **State > Disable**을 선택합니다.

2단계 **Save**를 클릭하여 정책을 저장합니다.

변경 사항을 적용하려면 액세스 제어 정책을 적용해야 합니다. 12-15페이지의 액세스 제어 정책 적용을/를 참조하십시오.

규칙의 위치 또는 카테고리 변경

라이센스: 모두

액세스 제어 규칙의 체계화에 도움이 되도록 모든 액세스 제어 정책에는 시스템에서 제공하는 규칙 카테고리, 즉 관리자 규칙, 표준 규칙 및 루트 규칙이 있습니다. 이러한 카테고리는 이동 또는 삭제하거나 이름을 변경할 수 없지만, 사용자 지정 카테고리를 만들 수는 있습니다.

기본적으로 액세스 제어 정책의 수정을 허용하는 사전 정의된 사용자 역할을 사용하면 규칙 카테고리 내에서 그리고 규칙 카테고리 간에 액세스 제어 규칙을 이동 및 수정할 수 있습니다. 그러나 사용자의 규칙 이동 및 수정을 제한하는 사용자 지정 역할을 만들 수 있습니다.

자세한 내용은 다음 링크를 참고하십시오.

- 14-16페이지의 규칙 이동
- 14-17페이지의 새 규칙 카테고리 추가

규칙 이동

라이센스: 모두

액세스 제어 규칙 순서를 적절히 지정하면 네트워크 트래픽 처리에 필요한 리소스가 감소하고 규칙 선점이 방지됩니다. 기본적으로 액세스 제어 정책의 수정을 허용하는 사전 정의된 사용자 역할을 사용하면 규칙 카테고리 내에서 그리고 규칙 카테고리 간에 액세스 제어 규칙을 이동할 수 있습니다. 그러나 시스템에서 제공하는 카테고리에서 사용자의 규칙 이동을 제한하는 사용자 지정 역할을 만들 수 있습니다.

다음 절차에서는 액세스 제어 정책 편집기를 사용하여 동시에 하나 이상의 규칙을 이동하는 방법에 대해 설명합니다. 규칙 편집기를 사용하여 개별 액세스 제어 규칙을 이동할 수도 있습니다. 14-3페이지의 액세스 제어 규칙 생성 및 수정을/를 참조하십시오.

규칙을 이동하려면

액세스: Admin/Access Admin/Network Admin

1단계 이동하려는 규칙이 포함된 정책의 액세스 제어 정책 편집기에서 각 규칙의 빈 영역을 클릭하여 규칙을 선택합니다. 여러 규칙을 선택하려면 Ctrl 키와 Shift 키를 사용합니다.

선택한 규칙이 강조 표시됩니다.

2단계 규칙을 이동합니다. 잘라내어 붙여넣거나 끌어다 놓을 수 있습니다.

규칙을 새 위치로 잘라내어 붙여넣으려면 선택한 규칙을 마우스 오른쪽 버튼으로 클릭하고 **Cut**을 선택합니다. 그런 다음 잘라낸 규칙을 붙여넣을 위치의 옆에서 규칙의 빈 영역을 마우스 오른쪽 버튼으로 클릭하고 **Paste above** 또는 **Paste below**를 선택합니다. 두 개의 서로 다른 액세스 제어 정책 간에는 액세스 제어 규칙을 복사하여 붙여넣을 수 없습니다.

3단계 **Save**를 클릭하여 정책을 저장합니다.

변경 사항을 적용하려면 액세스 제어 정책을 적용해야 합니다. 12-15페이지의 액세스 제어 정책 적용을/를 참조하십시오.

새 규칙 카테고리 추가

라이센스: 모두

액세스 제어 규칙의 체계화에 도움이 되도록 모든 액세스 제어 정책에는 시스템에서 제공하는 규칙 카테고리, 즉 관리자 규칙, 표준 규칙 및 루트 규칙이 있습니다. 이러한 카테고리는 이동 또는 삭제하거나 이름을 변경할 수 없지만, 표준 규칙과 루트 규칙 간에 사용자 지정 카테고리를 만들 수는 있습니다.

사용자 지정 카테고리를 추가하면 추가 정책을 생성하지 않고도 규칙을 더 세부적으로 구성할 수 있습니다. 추가한 카테고리를 삭제하거나 이름을 변경할 수 있습니다. 이러한 카테고리는 이동할 수 없지만, 카테고리 내외 및 카테고리 내에서 규칙을 이동할 수는 있습니다.

시스템에서 제공하는 카테고리에서 사용자의 규칙 이동 및 수정을 제한하는 사용자 역할을 만들 수 있지만, 액세스 제어 정책을 수정할 수 있는 사용자는 누구나 사용자 지정 카테고리에 규칙을 추가할 수 있으며 해당 카테고리에서 제한 없이 규칙을 수정할 수 있습니다.

새 카테고리를 추가하려면

액세스: Admin/Access Admin/Network Admin

1단계 규칙 카테고리를 추가하려는 정책의 액세스 제어 정책 편집기에서 Add Category를 클릭합니다.

팁 정책에 이미 규칙이 포함되어 있으면, 추가하기 전에 기존 규칙에 대한 행의 빈 영역을 클릭하여 새 카테고리의 위치를 설정할 수 있습니다. 기존 규칙을 마우스 오른쪽 버튼으로 클릭하고 **Insert new category**를 선택할 수도 있습니다.

Add Category 팝업 창이 나타납니다.

2단계 고유한 카테고리 **Name**을 입력합니다.

공백 및 인쇄 가능한 특수 문자를 포함하여 최대 30자의 영숫자 이름을 입력할 수 있습니다.

3단계 다음 옵션을 이용할 수 있습니다.

- 새 카테고리를 기존 카테고리 바로 위에 두려면 첫 번째 **Insert** 드롭다운 목록에서 **above Category**를 선택하고, 두 번째 드롭다운 목록에서 규칙을 바로 위에 배치할 카테고리를 선택합니다.
- 새 카테고리 규칙을 기존 규칙 바로 아래에 두려면 드롭다운 목록에서 **below rule**을 선택하고 기존 규칙 번호를 입력합니다. 이 옵션은 정책에 규칙이 하나 이상 있는 경우에만 유효합니다.
- 규칙을 기존 규칙 위에 두려면 드롭다운 목록에서 **above rule**을 선택하고 기존 규칙 번호를 입력합니다. 이 옵션은 정책에 규칙이 하나 이상 있는 경우에만 유효합니다.

4단계 **OK**를 클릭합니다.

카테고리가 추가됩니다. 사용자 지정 이름을 수정하려면 해당 카테고리 옆에 있는 수정 아이콘( )을 클릭하고, 카테고리를 삭제하려면 삭제 아이콘( )을 클릭할 수 있습니다. 삭제하는 카테고리의 규칙은 위 카테고리에 추가됩니다.

5단계 **Save**를 클릭하여 정책을 저장합니다.

15장 네트워크 기반 규칙으로 트래픽 제어

*액세스 제어 정책*의 *액세스 제어 규칙*으로 네트워크 트래픽의 로깅 및 처리를 정밀하게 제어할 수 있습니다. 네트워크 기반 조건에서는 다음 기준 중 하나를 사용하여 어떤 트래픽의 네트워크 통과 가능 여부를 관리할 수 있습니다.

- 소스 및 목적지 보안 영역
- 소스 및 목적지 IP 주소 또는 지리적 위치
- 패킷의 가장 안쪽에 있는 VLAN 태그
- 소스 및 목적지 포트 — 전송 계층 프로토콜 및 ICMP 코드 옵션도 포함

네트워크 기반 조건끼리 또는 다른 조건 유형과 조합하여 액세스 제어 규칙을 생성할 수 있습니다. 이러한 액세스 제어 규칙은 단순할 수도 있고, 아니면 여러 조건으로 트래픽을 매칭하고 검사하는 복잡한 형태를 띨 수도 있습니다. 액세스 제어 규칙에 대한 자세한 내용은 14-1페이지의 액세스 제어 규칙을 사용하여 트래픽 플로우 조정을/를 참조하십시오.

참고 하드웨어 기반 빠른 경로 규칙, 보안 인텔리전스 기반 트래픽 필터링, 일부 디코딩 및 재처리는 액세스 제어 규칙에서 네트워크 트래픽을 평가하기 **전에** 이루어집니다. 또한 액세스 제어 규칙에서 트래픽을 평가하기 전에 암호화 트래픽을 차단하거나 해독하도록 *SSL 검사* 기능을 구성할 수도 있습니다.

어떤 FireSIGHT 시스템 어플라이언스 및 라이센스에서도 대부분의 네트워크 기반 액세스 제어를 수행할 수 있지만, 지오로케이션 기반 액세스 제어에는 FireSIGHT 라이센스가 필요하며 다수의 Series 2 어플라이언스와 Cisco NGIPS for Blue Coat X-Series에서는 지원되지 않습니다. 또한 ASA FirePOWER 디바이스는 VLAN을 통한 액세스 제어를 지원하지 않습니다.

표 15-1 네트워크 기반 액세스 제어 규칙의 라이센스 및 모델 요구 사항

요구 사항	VLAN 태그	지오로케이션 제어	기타 네트워크 기반 제어
라이센스	모두	FireSIGHT	모두
디바이스	ASA FirePOWER를 제외하고 모두	Series 3 가상 ASA FirePOWER	모두
방어 센터	모두	DC500을 제외하고 모두	모두

네트워크 기반 액세스 제어 규칙 작성에 대한 자세한 내용은 다음을 참조하십시오.

보안 영역을 통한 트래픽 제어

라이센스: 모두

액세스 제어 규칙의 영역 조건에서는 소스 및 목적지 보안 영역으로 트래픽을 제어할 수 있습니다. *보안 영역*이란 하나 이상의 인터페이스를 그룹화한 것이며, 이 인터페이스는 여러 디바이스에 걸쳐 위치할 수도 있습니다. 디바이스의 초기 설정에서 선택하는 옵션인 *탐지 모드*는 디바이스 인터페이스의 초기 컨피그레이션 및 이 인터페이스가 보안 영역에 속하는지 여부를 결정합니다.

단순한 예로, 디바이스에 **Inline** 탐지 모드를 등록할 때 방어 센터에서는 Internal과 External의 2가지 영역을 생성하며 디바이스의 첫 번째 인터페이스 쌍을 이 영역에 지정합니다. 내부 영역의 네트워크에 연결되는 호스트는 보호되는 자산을 나타냅니다.

이 시나리오를 확장하자면 동일하게 구성된 (동일한 방어 센터에서 관리하는) 추가 디바이스를 구축하여 여러 다른 위치에 있는 유사한 리소스를 보호할 수 있습니다. 첫 번째 디바이스처럼 이 디바이스 각각은 내부 보안 영역의 자산을 보호합니다.

팁 모든 내부 (또는 외부) 인터페이스를 하나의 영역으로 그룹화할 필요는 없습니다. 구축 및 보안 정책에 알맞은 그룹화를 선택합니다. 영역 생성에 대한 자세한 내용은 3-38페이지의 보안 영역 작업을/를 참조하십시오.

이 구축에서는 호스트에 인터넷에 대한 무제한 액세스를 허용하더라도 수신 트래픽에서 침입 및 악성코드 검사를 수행하여 보호하도록 결정할 수 있습니다.

액세스 제어를 통해 이를 실현하려면 영역 조건이 있는 액세스 제어 규칙을 구성합니다. 여기서 **Destination Zone**은 **Internal**로 설정됩니다. 이 단순한 액세스 제어 규칙은 내부 영역에 속한 임의의 인터페이스로부터 디바이스를 떠나는 트래픽을 매칭합니다.

매칭하는 트래픽에 대해 침입 및 악성코드 검사를 수행하려면 **Allow** 규칙 작업을 선택한 다음 이 규칙을 침입 및 파일 정책과 연결합니다. 자세한 내용은 14-8페이지의 규칙 작업을 사용하여 트래픽 처리 및 검사 확인및 18-1페이지의 침입 정책 및 파일 정책을 사용하여 트래픽 제어을/를 참조하십시오.

더 복잡한 규칙을 작성하려는 경우 단일 영역 조건에서 각 **Source Zones** 및 **Destination Zones**에 최대 50개 영역을 추가할 수 있습니다.

- 이 영역에 속한 인터페이스로부터 디바이스를 *떠나는* 트래픽을 매칭하려면 **Destination Zones**에 영역을 추가합니다.

  패시브 구축된 디바이스는 트래픽을 전송하지 않으므로 **Destination Zone** 조건에서 패시브 인터페이스로 구성된 영역을 사용할 수 없습니다.
- 이 영역에 속한 인터페이스로부터 디바이스에 *들어오는* 트래픽을 매칭하려면 **Source Zones**에 영역을 추가합니다.
- 어떤 규칙에 소스 영역과 목적지 영역 조건을 모두 추가할 경우, 매칭하는 트래픽은 지정된 소스 영역 중 하나에서 시작하고 **또한** 목적지 영역 중 하나를 이그레스해야 합니다.

어떤 영역의 모든 인터페이스가 동일한 유형(모두 인라인, 패시브, 스위치드 또는 라우티드)이어야 하므로 어떤 액세스 제어 규칙의 영역 조건에 사용된 모든 영역도 동일한 유형이어야 합니다. 즉 하나의 규칙에서 매칭하는 트래픽의 소스나 목적지가 서로 다른 유형의 영역이 되도록 작성할 수 없습니다.

영역 조건을 작성할 때 잘못된 컨피그레이션에는 경고 아이콘이 표시됩니다. 자세한 내용은 아이콘 위에 포인터를 놓으면 볼 수 있습니다. 12-21페이지의 액세스 제어 정책 및 규칙 문제 해결도 참조하십시오.

영역으로 트래픽을 제어하려면

액세스: Admin/Access Admin/Network Admin

1단계 영역을 기준으로 트래픽을 제어할 디바이스에 대한 액세스 제어 정책에서 새 액세스 제어 규칙을 생성하거나 기존 규칙을 수정합니다.

자세한 내용은 14-3페이지의 액세스 제어 규칙 생성 및 수정을/를 참조하십시오.

2단계 규칙 편집기에서 Zones 탭을 선택합니다.

Zones 탭이 나타납니다.

3단계 **Available Zones**에서 추가할 영역을 찾아 선택합니다.

추가할 영역을 검색하려면 **Available Zones** 목록 위에서 **Search by name** 프롬프트를 클릭한 다음 영역 이름을 입력합니다. 입력할 때 목록이 업데이트되면서 매칭하는 영역을 표시합니다.

영역을 클릭하여 선택합니다. 여러 영역을 선택하려면 Shift 키와 Ctrl 키를 사용합니다. 또는 마우스 오른쪽 버튼을 클릭하고 **Select All**을 선택합니다.

4단계 **Add to Source** 또는 **Add to Destination**을 클릭하여 선택된 영역을 알맞은 목록에 추가합니다.

선택된 영역을 끌어서 놓을 수도 있습니다.

5단계 규칙을 저장하거나 계속 수정합니다.

변경 사항이 적용되려면 액세스 제어 정책을 적용해야 합니다. 12-15페이지의 액세스 제어 정책 적용을/를 참조하십시오.

네트워크 또는 지리적 위치로 트래픽 제어

라이센스: 기능에 따라

지원되는 디바이스: 기능에 따라

지원되는 Defense Center: 기능에 따라

액세스 제어 규칙의 네트워크 조건에서는 소스 및 목적지 IP 주소로 트래픽을 제어할 수 있습니다. 다음 중 하나를 수행할 수 있습니다.

- 제어하려는 트래픽에 대해 소스 및 목적지 IP 주소를 명시적으로 지정합니다.
- IP 주소를 지리적 위치와 연결하는 지오로케이션 기능을 사용하여 소스 또는 목적지 국가나 대륙을 기반으로 트래픽을 제어합니다.

네트워크 기반 액세스 제어 규칙 조건을 작성할 때 수동으로 IP 주소 및 지리적 위치를 지정할 수 있습니다. 또는 네트워크 및 지오로케이션 *객체*를 사용하여 네트워크 조건을 구성할 수 있습니다. 이 객체는 재사용 가능하며 어떤 이름을 하나 이상의 IP 주소, 주소 영역, 국가, 대륙 등과 연결합니다.

팁

네트워크 또는 지오로케이션 객체를 생성한 다음 이를 사용하여 액세스 제어 규칙을 작성할 뿐 아니라 시스템 웹 인터페이스의 다른 여러 곳에서 IP 주소를 나타낼 수 있습니다. 객체 관리자를 사용하여 이러한 객체를 생성할 수 있습니다. 액세스 제어 규칙을 구성하는 중에 즉석에서 네트워크 객체를 생성할 수도 있습니다. 자세한 내용은 3-1페이지의 재사용 가능 객체 관리을/를 참조하십시오.

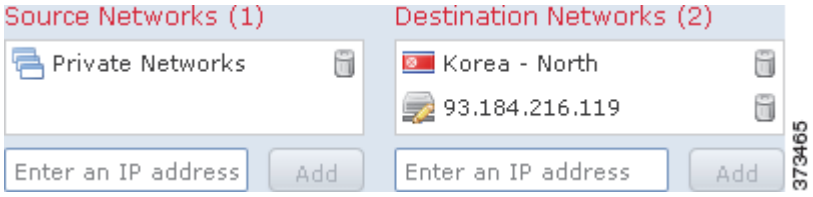
지리적 위치를 기준으로 트래픽 제어 규칙을 작성하려는 경우 최신 지오로케이션 데이터를 사용하여 트래픽을 필터링할 수 있도록 Cisco에서는 방어 센터에서 정기적으로 GeoDB(지오로케이션 데이터베이스)를 업데이트할 것을 **강력하게** 권장합니다. 66-27페이지의 지오로케이션 데이터베이스 업데이트을/를 참조하십시오.

또한 어떤 FireSIGHT 시스템 어플라이언스 및 라이센스에서도 단순한 IP 주소 기반 액세스 제어를 수행할 수 있지만, 지오로케이션 기반 액세스 제어에는 FireSIGHT 라이센스가 필요하며 다수의 Series 2 어플라이언스와 Cisco NGIPS for Blue Coat X-Series에서는 지원되지 않습니다.

표 15-2 네트워크 조건의 라이센스 및 모델 요구 사항

요구 사항	지오로케이션 제어	IP 주소 제어
라이센스	FireSIGHT	모두
디바이스	Series 3, 가상, ASA FirePOWER	모두
방어 센터	DC500을 제외하고 모두	모두

다음 그림에서 보여주는 액세스 제어 규칙의 네트워크 조건은 내부 네트워크에서 시작하고 북한 또는 93.184.216.119(example.com)의 리소스에 액세스하려는 연결을 차단합니다.



이 예에서는 Private Networks라는 네트워크 객체 그룹(표시되지 않았지만 IPv4 및 IPv6 Private Networks 네트워크 객체로 구성됨)이 내부 네트워크를 나타냅니다. 또한 이 예에서는 example.com IP 주소를 수동으로 지정하고 시스템에서 제공한 North Korea 지오로케이션 객체를 사용하여 북한의 IP 주소를 나타냅니다.

하나의 네트워크 조건에서 각 **Source Networks** 및 **Destination Networks**에 최대 50개의 항목을 추가할 수 있으며, 네트워크 컨피그레이션과 지오로케이션 기반 컨피그레이션을 혼합할 수도 있습니다.

- 어떤 IP 주소 또는 지리적 위치에서 *오는* 트래픽을 매칭하려면 **Source Networks**를 구성합니다.
- 어떤 IP 주소 또는 지리적 위치로 *가는* 트래픽을 매칭하려면 **Destination Networks**를 구성합니다.

소스 및 목적지 네트워크 조건을 모두 규칙에 추가할 경우 매칭하는 트래픽은 지정된 IP 주소 중 하나에서 시작하고 **또한** 목적지 IP 주소 중 하나로 가는 것이어야 합니다.

네트워크 조건을 작성할 때 잘못된 컨피그레이션에는 경고 아이콘이 표시됩니다. 자세한 내용은 아이콘 위에 포인터를 놓으면 볼 수 있습니다. 12-21페이지의 액세스 제어 정책 및 규칙 문제 해결도 참조하십시오.

네트워크 또는 지리적 위치로 트래픽을 제어하려면

액세스: Admin/Access Admin/Network Admin

1단계 네트워크를 기준으로 트래픽을 제어할 디바이스에 대한 액세스 제어 정책에서 새 액세스 제어 규칙을 생성하거나 기존 규칙을 수정합니다.

자세한 내용은 14-3페이지의 액세스 제어 규칙 생성 및 수정을/를 참조하십시오.

2단계 규칙 편집기에서 Networks 탭을 선택합니다.

Networks 탭이 나타납니다.

3단계 다음과 같이 추가할 네트워크를 **Available Networks**에서 찾아 선택합니다.

- Networks 탭을 클릭하여 추가할 네트워크 객체 및 그룹을 표시합니다. Geolocation 탭을 클릭하여 지오로케이션 객체를 표시합니다.
- 즉석에서 네트워크 객체를 추가하려면(그런 다음 조건에 추가할 수 있음) **Available Networks** 목록 위에서 추가 아이콘( )을 클릭합니다. 3-4페이지의 네트워크 객체 작업을/를 참조하십시오.
- 추가할 네트워크 또는 지오로케이션 객체를 검색하려면 해당 탭을 선택하고 **Available Networks** 목록 위의 **Search by name or value** 프롬프트를 선택한 다음 객체 이름 또는 객체의 구성 요소 중 하나의 값을 입력합니다. 입력할 때 목록이 업데이트되면서 매칭하는 객체를 표시합니다.

객체를 클릭하여 선택합니다. 여러 객체를 선택하려면 Shift 키와 Ctrl 키를 사용합니다. 또는 마우스 오른쪽 버튼을 클릭하여 **Select All**을 선택합니다.

4단계 **Add to Source** 또는 **Add to Destination**을 클릭하여 선택된 객체를 알맞은 목록에 추가합니다.

선택된 객체를 끌어서 놓을 수도 있습니다.

5단계 수동으로 지정하려는 소스 또는 목적지 IP 주소나 주소 영역을 추가합니다.

Source Networks 또는 **Destination Networks** 목록 아래의 **Enter an IP address** 프롬프트를 클릭한 다음 IP 주소 또는 주소 영역을 입력하고 **Add**를 클릭합니다.

6단계 규칙을 저장하거나 계속 수정합니다.

변경 사항이 적용되려면 액세스 제어 정책을 적용해야 합니다. 12-15페이지의 액세스 제어 정책 적용을/를 참조하십시오.

VLAN 트래픽 제어

라이센스: 모두

지원되는 디바이스: ASA FirePOWER를 제외하고 모두

액세스 제어 규칙의 VLAN 조건으로 VLAN 태그 지정 트래픽을 제어할 수 있습니다. 가장 안쪽의 VLAN 태그를 사용하여 VLAN을 기준으로 패킷을 식별합니다.

VLAN 기반 액세스 제어 규칙 조건을 작성할 때 VLAN 태그를 수동으로 지정할 수 있습니다. 또는 VLAN 태그 *객체*를 사용하여 VLAN 조건을 구성할 수 있습니다. 이 객체는 재사용 가능하며 어떤 이름을 하나 이상의 VLAN 태그와 연결합니다.

팁 VLAN 태그 객체를 생성한 다음 이를 사용하여 액세스 제어 규칙을 작성할 뿐 아니라 시스템 웹 인터페이스의 다른 여러 곳에서 VLAN 태그를 나타낼 수 있습니다. 객체 관리자를 사용하여 또는 액세스 제어 규칙을 구성할 때 즉석에서 VLAN 태그 객체를 생성할 수 있습니다. 자세한 내용은 3-13페이지의 VLAN 태그 객체 작업을/를 참조하십시오.

다음 그림에서 보여주는 액세스 제어 규칙의 VLAN 태그 조건은 일반에게 공개되는 VLAN(VLAN 태그 객체 그룹으로 표시됨)뿐 아니라 수동으로 추가된 VLAN 42의 트래픽을 매칭합니다.

하나의 VLAN 태그 조건에서 **Selected VLAN Tags**에 최대 50개의 항목을 추가할 수 있습니다. VLAN 태그 조건을 작성할 때 잘못된 컨피그레이션에는 경고 아이콘이 표시됩니다. 자세한 내용은 아이콘 위에 포인터를 놓으면 볼 수 있습니다. 12-21페이지의 액세스 제어 정책 및 규칙 문제 해결도 참조하십시오.

VLAN 태그로 트래픽을 제어하려면

액세스: Admin/Access Admin/Network Admin

1단계 VLAN 태그를 기준으로 트래픽을 제어할 디바이스에 대한 액세스 제어 정책에서 새 액세스 제어 규칙을 생성하거나 기존 규칙을 수정합니다.

자세한 내용은 14-3페이지의 액세스 제어 규칙 생성 및 수정을/를 참조하십시오.

2단계 규칙 편집기에서 VLAN Tags 탭을 선택합니다.

VLAN Tags 탭이 나타납니다.

3단계 다음과 같이 추가할 VLAN을 **Available VLAN Tags**에서 찾아 선택합니다.

- 즉석에서 VLAN 태그 객체를 추가하려면(그런 다음 조건에 추가할 수 있음) Available VLAN Tags 목록 위에서 추가 아이콘( )을 클릭합니다. 3-13페이지의 VLAN 태그 객체 작업을/를 참조하십시오.
- 추가할 VLAN 태그 객체 및 그룹을 검색하려면 **Available VLAN Tags** 목록 위에서 **Search by name or value** 프롬프트를 클릭한 다음 객체의 이름 또는 객체에 있는 VLAN 태그의 값을 입력합니다. 입력할 때 목록이 업데이트되면서 매칭하는 객체를 표시합니다.

객체를 클릭하여 선택합니다. 여러 객체를 선택하려면 Shift 키와 Ctrl 키를 사용합니다. 또는 마우스 오른쪽 버튼을 클릭하고 **Select All**을 선택합니다.

4단계 **Add to Rule**을 클릭하거나 선택된 객체를 **Selected VLAN Tags** 목록으로 추가합니다.

선택된 객체를 끌어서 놓을 수도 있습니다.

5단계 수동으로 지정할 VLAN 태그가 있으면 추가합니다.

Selected VLAN Tags 목록 아래의 **Enter a VLAN Tag** 프롬프트를 클릭합니다. 그런 다음 VLAN 태그 또는 범위를 입력하고 **Add**를 클릭합니다. VLAN 태그는 1에서 4094 사이의 숫자 중 하나로 지정할 수 있습니다. VLAN 태그의 범위를 지정하려면 하이픈을 사용합니다.

6단계 규칙을 저장하거나 계속 수정합니다.

변경 사항이 적용되려면 액세스 제어 정책을 적용해야 합니다. 12-15페이지의 액세스 제어 정책 적용을/를 참조하십시오.

포트 및 ICMP 코드로 트래픽 제어

라이센스: 모두

액세스 제어 규칙의 네트워크 조건에서는 소스 및 목적지 포트를 기준으로 트래픽을 제어할 수 있습니다. 여기서 "포트"는 다음 중 하나를 의미합니다.

- TCP 및 UDP에서는 전송 계층 프로토콜을 기반으로 트래픽을 제어할 수 있습니다. 괄호로 묶은 프로토콜 번호와 선택 사항인 해당 포트 또는 포트 범위를 사용하여 이 컨피그레이션을 나타냅니다. 예를 들면 TCP(6)/22입니다.
- ICMP 및 ICMPv6(IPv6-ICMP)는 인터넷 계층 프로토콜과 선택 사항인 유형 및 코드를 기반으로 트래픽을 제어할 수 있습니다. 예를 들면 ICMP(1):3:3입니다.
- 포트를 사용하지 않는 다른 프로토콜에서 트래픽을 제어할 수 있습니다.

포트 기반 액세스 제어 규칙 조건을 작성할 때 포트를 수동으로 지정할 수 있습니다. 또는 포트 *객체*를 사용하여 포트 조건을 구성할 수 있습니다. 이 객체는 재사용 가능하며 어떤 이름을 하나 이상의 포트와 연결합니다.

팁 포트 태그 객체를 생성한 다음 이를 사용하여 액세스 제어 규칙을 작성할 뿐 아니라 시스템 웹 인터페이스의 다른 여러 곳에서 포트를 나타낼 수 있습니다. 객체 관리자를 사용하여 또는 액세스 제어 규칙을 구성할 때 즉석에서 포트 객체를 생성할 수 있습니다. 자세한 내용은 3-12페이지의 포트 객체 작업을/를 참조하십시오.

하나의 네트워크 조건에서 각 **Selected Source Ports** 및 **Selected Destination Ports** 목록에 최대 50개의 항목을 추가할 수 있습니다.

- 어떤 포트에서 *오는* 트래픽을 매칭하려면 **Selected Source Ports**를 구성합니다.

  소스 포트만 조건에 추가할 경우 다양한 전송 프로토콜을 사용하는 포트를 추가할 수 있습니다. 예를 들어 하나의 액세스 제어 규칙에서 DNS over TCP 및 DNS over UDP를 소스 포트 조건으로 추가할 수 있습니다.

- 어떤 포트로 *가는* 트래픽을 매칭하려면 **Selected Destination Ports**를 구성합니다.

  목적지 포트만 조건에 추가할 경우 다양한 전송 프로토콜을 사용하는 포트를 추가할 수 있습니다.

- 특정 **Selected Source Ports**에서 시작하고 *또한* 특정 **Selected Destination Ports**로 가는 트래픽을 매칭하려면 둘 다 구성합니다.

  소스 포트와 목적지 포트를 모두 조건에 추가할 경우 단일 전송 프로토콜(TCP 또는 UDP)을 공유하는 포트만 추가할 수 있습니다. 예를 들어 DNS over TCP를 소스 포트로 추가할 경우 Yahoo Messenger Voice Chat(TCP)을 목적지 포트로 추가할 수 있지만 Yahoo Messenger Voice Chat(UDP)은 추가할 수 없습니다.

포트 조건을 작성할 때 다음 사항에 유의하십시오.

- 유형이 0으로 설정된 목적지 ICMP 포트 또는 유형이 129로 설정된 목적지 ICMPv6 포트를 추가할 경우 액세스 제어 규칙은 요청되지 않은 에코 회신만 매칭합니다. ICMP 에코 요청에 대한 응답으로 보내진 ICMP 에코 회신은 무시됩니다. 어떤 ICMP 에코에서 규칙을 매칭하려면 ICMP 유형 8 또는 ICMPv6 유형 128을 사용하십시오.
- GRE(47)프로토콜을 목적지 포트 조건으로 사용할 경우 다른 네트워크 기반 조건, 즉 영역, 네트워크, VLAN 태그 조건만 액세스 제어 규칙에 추가할 수 있습니다. 평판 또는 사용자 기반 조건을 추가할 경우 그 규칙을 저장할 수 없습니다.

포트 조건을 작성할 때 잘못된 컨피그레이션에는 경고 아이콘이 표시됩니다. 이를테면 사용 중인 포트 객체를 객체 관리자에서 수정하여 이 객체 그룹을 사용하는 규칙을 유효하지 않게 할 수 있습니다. 자세한 내용은 아이콘 위에 포인터를 놓으면 볼 수 있습니다. 12-21페이지의 액세스 제어 정책 및 규칙 문제 해결도 참조하십시오.

포트로 트래픽을 제어하려면

액세스: Admin/Access Admin/Network Admin

1단계 포트를 기준으로 트래픽을 제어할 디바이스에 대한 액세스 제어 정책에서 새 액세스 제어 규칙을 생성하거나 기존 규칙을 수정합니다.

자세한 내용은 14-3페이지의 액세스 제어 규칙 생성 및 수정을/를 참조하십시오.

2단계 규칙 편집기에서 Ports 탭을 선택합니다.

Ports 탭이 나타납니다.

3단계 다음과 같이 추가할 포트를 **Available Ports**에서 찾아 선택합니다.

- 즉석에서 포트 객체를 추가하려면(그런 다음 조건에 추가할 수 있음) Available Ports 목록 위에서 추가 아이콘( )을 클릭합니다. 3-12페이지의 포트 객체 작업을/를 참조하십시오.
- 추가할 포트 객체 및 그룹을 검색하려면 **Available Ports** 목록 위에서 **Search by name or value** 프롬프트를 클릭한 다음 객체의 이름 또는 객체에 있는 포트의 값을 입력합니다. 입력할 때 목록이 업데이트되면서 매칭하는 객체를 표시합니다. 예를 들어 80이라고 입력하면 방어 센터에서는 Cisco에서 제공한 HTTP 포트 객체를 표시합니다.

  객체를 클릭하여 선택합니다. 여러 객체를 선택하려면 Shift 키와 Ctrl 키를 사용합니다. 또는 마우스 오른쪽 버튼을 클릭하고 **Select All**을 선택합니다.

4단계 **Add to Source** 또는 **Add to Destination**을 클릭하여 선택된 객체를 알맞은 목록에 추가합니다.

선택된 객체를 끌어서 놓을 수도 있습니다.

5단계 수동으로 지정하려는 소스 또는 목적지 포트를 추가합니다.

- 소스 포트의 경우 **Selected Source Ports** 목록 아래의 **Protocol** 드롭다운 목록에서 **TCP** 또는 **UDP** 중 하나를 선택합니다. 그런 다음 **Port**의 값을 입력합니다. 0에서 65535까지의 값으로 단일 포트를 지정할 수 있습니다.
- **Selected Destination Ports** 목록 아래의 **Protocol** 드롭다운 목록에서 프로토콜(모든 프로토콜이면 **All**)을 선택합니다. 목록에 없는 지정되지 않은 프로토콜의 번호도 입력할 수 있습니다.

  ICMP 또는 **IPv6-ICMP**를 선택할 경우 팝업 창이 나타나며, 여기에서 유형과 관련 코드를 선택할 수 있습니다. ICMP 유형 및 코드에 대한 자세한 내용은 http://www.iana.org/assignments/icmp-parameters/icmp-parameters.xml 및 http://www.iana.org/assignments/icmpv6-parameters/icmpv6-parameters.xml을 참조하십시오.

  어떤 프로토콜을 지정하지 않으려는 경우 또는 선택 사항으로 TCP 또는 UDP를 지정한 경우 **Port**의 값을 입력합니다. 0에서 65535까지의 값으로 단일 포트를 지정할 수 있습니다.

Add를 클릭합니다. 방어 센터에서는 잘못된 컨피그레이션을 생성하는 규칙 조건에 포트를 추가하지 않습니다.

6단계 규칙을 저장하거나 계속 수정합니다.

변경 사항이 적용되려면 액세스 제어 정책을 적용해야 합니다. 12-15페이지의 액세스 제어 정책 적용을/를 참조하십시오.

16장

평판 기반 규칙으로 트래픽 제어

*액세스 제어 정책*의 *액세스 제어 규칙*으로 네트워크 트래픽의 로깅 및 처리를 정밀하게 제어할 수 있습니다. 액세스 제어 규칙의 평판 기반 조건에서 네트워크 트래픽의 컨텍스트를 지정하고 필요에 따라 제한하는 식으로 어떤 트래픽이 네트워크를 통과할 수 있는가를 관리합니다. 액세스 제어 규칙은 다음 유형의 평판 기반 제어를 수행합니다.

- 애플리케이션 조건에서는 *애플리케이션 제어*를 수행할 수 있습니다. 이는 개별 애플리케이션뿐 아니라 애플리케이션의 기본 특성, 즉 유형, 위험, 비즈니스 연관성, 범주, 태그를 기반으로 애플리케이션 트래픽을 제어합니다.
- URL 조건에서는 *URL 필터링*을 수행할 수 있습니다. 즉 개별 웹 사이트뿐 아니라 웹 사이트의 시스템 지정 범주 및 평판을 기반으로 웹 트래픽을 제어합니다.

평판 기반 조건끼리 또는 다른 조건 유형과 조합하여 액세스 제어 규칙을 생성할 수 있습니다. 이러한 액세스 제어 규칙은 단순할 수도, 아니면 여러 조건으로 트래픽을 매칭하고 검사하는 복잡한 형태를 띨 수도 있습니다. 액세스 제어 규칙에 대한 자세한 내용은 14-1페이지의 액세스 제어 규칙을 사용하여 트래픽 플로우 조정을/를 참조하십시오.

참고 하드웨어 기반 빠른 경로 규칙, 보안 인텔리전스 기반 트래픽 필터링, 일부 디코딩 및 재처리는 액세스 제어 규칙에서 네트워크 트래픽을 평가하기 **전에** 이루어집니다. 또한 액세스 제어 규칙에서 트래픽을 평가하기 전에 암호화 트래픽을 차단하거나 해독하도록 *SSL 검사* 기능을 구성할 수도 있습니다.

평판 기반 액세스 제어를 수행하려면 다음 라이센스, 디바이스, 방어 센터가 필요합니다.

표 16-1 평판 기반 액세스 제어 규칙의 라이센스 및 모델 요구 사항

요구 사항	애플리케이션 제어	URL 필터링(범주 및 평판)	URL 필터링(수동)
라이센스	제어	URL 필터링	모두
디바이스	Series 2 또는 X-Series를 제외하고 모두	Series 2를 제외하고 모두	Series 2를 제외하고 모두
방어 센터	모두	DC500을 제외하고 모두	모두

액세스 제어 규칙에 평판 기반 조건을 추가하는 것에 대한 자세한 내용은 다음을 참조하십시오.

- 16-2페이지의 애플리케이션 트래픽 제어
- 16-8페이지의 URL 차단

FireSIGHT 시스템에서는 다른 유형의 평판 기반 제어를 수행할 수 있지만, 이러한 제어는 액세스 제어 규칙으로 구성하지 않습니다. 자세한 내용은 다음 링크를 참조하십시오.

- 13-1페이지의 보안 인텔리전스 IP 주소 평판 블랙리스트에 추가에서는 연결의 출처 또는 목적지의 평판을 1차 방어선으로 삼아 트래픽을 제한하는 방법에 대해 설명합니다.
- 18-8페이지의 침입 방지 성능 조정에서는 악성코드 및 기타 금지된 파일 유형을 탐지, 추적, 저장, 분석하고 차단하는 방법에 대해 설명합니다.

애플리케이션 트래픽 제어

라이센스: 제어

지원되는 디바이스: Series 2 또는 X-Series를 제외하고 모두

FireSIGHT 시스템에서 IP 트래픽을 분석할 때 네트워크에서 자주 사용되는 애플리케이션을 식별하여 분류할 수 있습니다. 이 검색 기반 *애플리케이션 인식* 기능이 네트워크에서 애플리케이션 트래픽을 제어하는 데 활용될 수 있습니다.

애플리케이션 제어 이해

액세스 제어 규칙의 애플리케이션 조건을 통해 이러한 *애플리케이션 제어*를 수행할 수 있습니다. 단일 액세스 제어 규칙 내에서 트래픽을 제어할 애플리케이션을 몇 가지 방법으로 지정할 수 있습니다.

- 사용자 지정 애플리케이션을 비롯한 개별 애플리케이션을 선택할 수 있습니다.
- 시스템에서 제공한 *애플리케이션 필터*를 사용할 수 있습니다. 이는 이름이 지정된 애플리케이션 모음으로서 애플리케이션의 기본 특성, 즉 유형, 위험, 비즈니스 연관성, 범주, 태그에 따라 구성됩니다.
- 원하는 대로 (사용자 지정 애플리케이션을 비롯한) 애플리케이션을 그룹화하는 사용자 지정 애플리케이션 필터를 생성하고 사용할 수 있습니다.

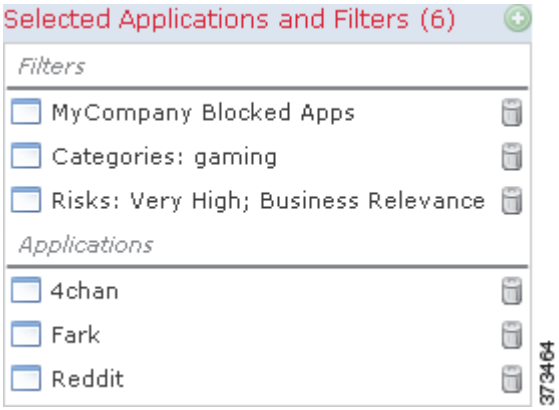
애플리케이션 필터를 사용하여 액세스 제어 규칙을 위한 애플리케이션 조건을 신속하게 생성할 수 있습니다. 이를 통해 정책 생성 및 관리를 간소화할 뿐 아니라 예상대로 웹 트래픽 제어가 이루어지고 있음을 보장할 수 있습니다. 예를 들어 위험도가 높고 비즈니스 연관성이 낮은 모든 애플리케이션을 식별하여 차단하는 액세스 제어 규칙을 생성할 수 있습니다. 사용자가 이 애플리케이션 중 하나를 사용하려 하면 세션이 차단됩니다.

또한 Cisco에서는 시스템 및 VDB(vulnerability database) 업데이트를 통해 자주 탐지기를 업데이트하고 추가합니다. 직접 탐지기를 생성하고 여기서 탐지하는 애플리케이션에 특성(위험, 연관성 등)을 부여할 수도 있습니다. 애플리케이션 특성을 기반으로 한 필터를 통해 최신 탐지기를 사용한 애플리케이션 트래픽 모니터링을 보장할 수 있습니다.

애플리케이션 조건 작성

트래픽이 애플리케이션 조건이 있는 액세스 제어 규칙과 매칭하려면 **Selected Applications and Filters** 목록에 추가된 필터 또는 애플리케이션 중 하나와 매칭해야 합니다.

다음 그림은 MyCompany의 사용자 지정 애플리케이션 그룹, 위험도가 높고 비즈니스 연관성이 낮은 모든 애플리케이션, 게임 애플리케이션, 일부 개별적으로 선택된 애플리케이션을 차단하는 액세스 제어 규칙을 위한 애플리케이션 조건을 보여줍니다.



하나의 애플리케이션 조건에서 최대 50개 항목을 **Selected Applications and Filters** 목록에 추가할 수 있습니다. 다음 각각이 하나의 항목으로 간주됩니다.

- **Application Filters** 목록에 있는 개별적 또는 사용자 지정 조합 형태의 하나 이상의 필터. 이 항목은 특성을 기준으로 그룹화된 애플리케이션 모음입니다.
- **Available Applications** 목록에 애플리케이션 검색을 저장하여 생성하는 필터. 이 항목은 하위 문자열 매칭에 의해 그룹화된 애플리케이션 모음입니다.
- **Available Applications** 목록의 개별 애플리케이션

웹 인터페이스에서 조건에 추가된 필터는 개별적으로 추가된 애플리케이션의 위에 따로 나열됩니다.

액세스 제어 정책을 적용할 때 애플리케이션 조건이 있는 각 규칙에 대해 매칭할 고유 애플리케이션의 목록이 생성됩니다. 따라서 중복되는 필터 및 개별적으로 지정된 애플리케이션을 사용하여 완전한 범위를 보장할 수 있습니다.

참고 암호화 트래픽의 경우 **SSL Protocol** 태그가 지정된 애플리케이션만 사용하여 트래픽을 식별하고 필터링할 수 있습니다. 이 태그가 없는 애플리케이션은 암호화되지 않은 트래픽 또는 해독된 트래픽에서만 탐지할 수 있습니다. 또한 **decrypted traffic** 태그는 암호화 트래픽 또는 암호화되지 않은 트래픽이 아닌 해독된 트래픽에서만 탐지할 수 있는 애플리케이션에 지정됩니다. 액세스 제어 규칙과 매칭하기 전에 암호화 트래픽을 해독하거나 차단하는 SSL 검사 기능을 사용하는 것에 대한 자세한 내용은 19-1페이지의 트래픽 해독 이해을/를 참조하십시오.

자세한 내용은 다음 절을 참조하십시오.

- 16-4페이지의 애플리케이션 필터로 트래픽 매칭
- 16-5페이지의 개별 애플리케이션의 트래픽 매칭
- 16-6페이지의 액세스 제어 규칙에 애플리케이션 조건 추가
- 16-7페이지의 애플리케이션 제어의 제한 사항

애플리케이션 필터로 트래픽 매칭

라이센스: 제어

지원되는 디바이스: 지원되는 디바이스: Series 2 또는 X-Series를 제외하고 모두

액세스 제어 규칙에서 애플리케이션 조건을 작성할 때 **Application Filters** 목록을 사용하여 애플리케이션 모음을 생성하는데, 이는 트래픽을 매칭할 애플리케이션을 특성에 따라 그룹화한 것입니다.

사용자의 편의를 위해 45-11 페이지의 표 45-2에 설명된 기준에 따라 탐지된 애플리케이션 각각에 특성을 부여합니다. 이 기준을 필터로 사용하거나 사용자 지정 필터 조합을 생성하여 애플리케이션 제어를 수행할 수 있습니다.

액세스 제어 규칙 내에서 애플리케이션을 필터링하는 메커니즘은 객체 관리자를 사용하여 재사용 가능한 사용자 지정 애플리케이션 필터를 생성하는 메커니즘과 동일합니다. 3-15페이지의 애플리케이션 필터 작업을/를 참조하십시오. 또한 생성하는 여러 필터를 액세스 제어 규칙에 새로운 재사용 가능 필터로 즉시 저장할 수도 있습니다. 사용자 생성 필터는 중첩 불가하므로 다른 사용자 생성 필터를 포함하는 필터를 저장할 수 없습니다.

필터를 조합하는 방법 이해

필터를 하나씩 또는 조합하여 선택할 때 **Available Applications** 목록이 업데이트되어 기준에 부합하는 애플리케이션만 표시됩니다. 시스템에서 제공하는 필터를 조합하여 선택할 수 있지만, 사용자 지정 필터는 선택할 수 없습니다.

동일한 필터 유형의 여러 필터는 OR 연산자로 연결됩니다. 예를 들어 Risks 유형에 속하는 Medium 및 High 필터를 선택하면 다음과 같은 필터가 만들어집니다.

```
Risk: Medium OR High
```

Medium 필터에 110개 애플리케이션이, High 필터에 82개 애플리케이션이 있을 경우 총 192개 애플리케이션이 **Available Applications** 목록에 표시됩니다.

서로 다른 유형의 필터는 AND 연산자로 연결합니다. 예를 들어 Risks 유형의 Medium 및 High 필터, Business Relevance 유형의 Medium 및 High 필터를 선택하면 다음과 같은 필터가 만들어집니다.

```
Risk: Medium OR High
AND
Business Relevance: Medium OR High
```

여기서는 Medium 또는 High Risk 유형과 Medium 또는 High Business Relevance 유형에 모두 해당되는 애플리케이션만 표시합니다.

필터 찾기 및 선택

필터를 선택하려면 필터 유형 옆의 화살표를 클릭하여 확장한 다음 애플리케이션을 표시하거나 숨길 각 필터 옆의 확인란을 선택하거나 선택 취소합니다. 시스템 제공 필터 유형(**Risks**, **Business Relevance**, **Types**, **Categories**, **Tags**)을 마우스 오른쪽 버튼으로 클릭한 다음 **Check All** 또는 **Uncheck All**을 선택할 수도 있습니다.

필터를 검색하려면 **Available Filters** 목록 위의 **Search by name** 프롬프트를 클릭하고 이름을 입력합니다. 입력할 때 목록이 업데이트되면서 매칭하는 필터를 표시합니다.

필터 선택을 완료했으면 **Available Applications** 목록을 사용하여 규칙에 필터를 추가합니다. 16-5페이지의 개별 애플리케이션의 트래픽 매칭을/를 참조하십시오.

개별 애플리케이션의 트래픽 매칭

라이센스: 제어

지원되는 디바이스: 지원되는 디바이스: Series 2 또는 X-Series를 제외하고 모두

액세스 제어 규칙에서 애플리케이션 조건을 작성할 때 **Available Applications** 목록을 사용하여 트래픽을 매칭할 애플리케이션을 선택합니다.

애플리케이션 목록 탐색

조건 작성을 처음 시작할 때는 목록이 제한되지 않은 상태이므로 시스템에서 탐지하는 모든 애플리케이션을 한 번에 100개씩 표시합니다.

- 페이지별로 애플리케이션을 보려면 목록 아래의 화살표를 클릭합니다.
- 애플리케이션의 특성에 대한 요약 정보 및 연결 가능한 인터넷 검색 링크를 포함한 팝업 창을 표시하려면 애플리케이션 옆의 정보 아이콘( )을 클릭합니다.

매칭할 애플리케이션 찾기

매칭할 애플리케이션을 효과적으로 찾기 위해 다음과 같이 **Available Applications** 목록을 제한할 수 있습니다.

- 애플리케이션을 검색하려면 목록 위의 **Search by name** 프롬프트를 클릭하고 이름을 입력합니다. 입력할 때 목록이 업데이트되면서 매칭하는 애플리케이션을 표시합니다.
- 필터를 적용하여 애플리케이션을 제한하려면 **Application Filters** 목록을 사용합니다(16-4페이지의 애플리케이션 필터로 트래픽 매칭 참조). 필터를 적용할 때 **Available Applications** 목록이 업데이트됩니다. 사용자의 편의를 위해 잠금 취소 아이콘( )을 사용하여 암호화 트래픽이나 암호화되지 않은 트래픽이 아닌 해독된 트래픽에서만 식별할 수 있는 애플리케이션을 표시합니다.

제한이 적용되면 **All apps matching the filter** 옵션이 **Available Applications** 목록의 맨 위에 나타납니다. 이 옵션으로 제한 목록의 모든 애플리케이션을 **Selected Applications and Filters** 목록에 한꺼번에 추가할 수 있습니다.

참고 Application Filters 목록에서 하나 이상의 필터를 선택하고 **Available Applications** 목록도 검색할 경우 선택 내용과 검색 필터링된 **Available Applications** 목록이 AND 연산자로 조합됩니다. 즉 **All apps matching the filter** 조건은 현재 **Available Applications** 목록에 표시된 모든 개별 조건과 **Available Applications** 목록 위에 입력된 검색 문자열을 포함합니다.

조건에서 매칭할 단일 애플리케이션 선택

매칭할 애플리케이션을 찾은 다음 클릭하여 선택합니다. 여러 애플리케이션을 선택하려면 Shift 및 Ctrl 키를 사용하거나 마우스 오른쪽 버튼을 클릭하고 **Select All**을 선택하여 현재 제한된 보기의 모든 애플리케이션을 선택합니다.

단일 애플리케이션 조건에서 최대 50개의 애플리케이션을 개별적으로 선택하여 매칭할 수 있습니다. 50개보다 많이 추가하려면 여러 액세스 제어 규칙을 생성하거나 필터를 사용하여 애플리케이션을 그룹화해야 합니다.

어떤 조건의 필터와 매칭하는 모든 애플리케이션 선택

검색 또는 **Application Filters** 목록의 필터 사용을 통해 제한되면 **All apps matching the filter** 옵션이 **Available Applications** 목록의 맨 위에 나타납니다.

이 옵션으로 제한된 **Available Applications** 목록의 전체 애플리케이션을 **Selected Applications and Filters** 목록에 한꺼번에 추가할 수 있습니다. 애플리케이션을 개별적으로 추가하는 것과 달리 이렇게 애플리케이션 모음을 추가하면 최대 50개 항목의 한도에서 1개의 항목으로 간주됩니다. 그 모음에 포함된 애플리케이션 수는 무관합니다.

이렇게 애플리케이션 조건을 작성할 때 **Selected Applications and Filters** 목록에 추가되는 필터의 이름은 필터에 나타난 필터 유형에 유형별로 최대 3개 필터의 이름이 연결된 것입니다. 동일한 유형의 필터가 4개 이상이면 줄임표(...)가 붙습니다. 예를 들어 다음 필터 이름은 Risks 유형의 2개 필터와 Business Relevance 유형의 4개 필터를 포함합니다.

```
Risks: Medium, High Business Relevance: Low, Medium, High,...
```

All apps matching the filter로 추가한 필터에 나타나지 않는 필터 유형은 추가하는 필터의 이름에 포함되지 않습니다. **Selected Applications and Filters** 목록에서 필터 위에 포인터를 둘 때 표시되는 지침 텍스트는 이 필터 유형이 *any*로 설정되었음을 알립니다. 즉 이 필터 유형이 필터를 제한하지 않으므로 이에 대해 어떤 값도 허용됩니다.

All apps matching the filter의 여러 인스턴스를 하나의 애플리케이션 조건에 추가할 수 있습니다. 그러면 각 인스턴스가 **Selected Applications and Filters** 목록에서 각각의 항목으로 간주됩니다. 예를 들어 위험도가 높은 모든 애플리케이션을 하나의 항목으로 추가하고 선택을 취소한 다음 비즈니스 연관성이 낮은 모든 애플리케이션을 또 다른 항목으로 추가할 수 있습니다. 이 애플리케이션 조건은 위험도 높음 또는 비즈니스 연관성 낮음에 해당하는 애플리케이션과 매칭합니다.

액세스 제어 규칙에 애플리케이션 조건 추가

라이센스: 제어

지원되는 디바이스: 지원되는 디바이스: Series 2 또는 X-Series를 제외하고 모두

트래픽이 애플리케이션 조건이 있는 액세스 제어 규칙과 매칭하려면 **Selected Applications and Filters** 목록에 추가된 필터 또는 애플리케이션 중 하나와 매칭해야 합니다.

조건당 최대 50개 항목을 추가할 수 있으며, 조건에 추가된 필터는 개별적으로 추가된 애플리케이션의 위에 따로 나열됩니다. 애플리케이션 조건을 작성할 때 잘못된 컨피그레이션에는 경고 아이콘이 표시됩니다. 자세한 내용은 아이콘 위에 포인터를 놓으면 볼 수 있습니다. 12-21페이지의 액세스 제어 정책 및 규칙 문제 해결도 참조하십시오.

애플리케이션 트래픽을 제어하려면

액세스: Admin/Access Admin/Network Admin

1단계 애플리케이션을 기준으로 트래픽을 제어할 디바이스에 대한 액세스 제어 정책에서 새 액세스 제어 규칙을 생성하거나 기존 규칙을 수정합니다.

자세한 내용은 14-3페이지의 액세스 제어 규칙 생성 및 수정을/를 참조하십시오.

2단계 규칙 편집기에서 Applications 탭을 선택합니다.

Applications 탭이 나타납니다.

3단계 필터를 사용하여 **Available Applications** 목록에 표시되는 애플리케이션의 목록을 제한할 수도 있습니다.

Application Filters 목록에서 하나 이상의 필터를 선택합니다. 자세한 내용은 16-4페이지의 애플리케이션 필터로 트래픽 매칭을/를 참조하십시오.

4단계 **Available Applications** 목록에서 추가할 애플리케이션을 찾아 선택합니다.

개별 애플리케이션을 검색하여 선택하거나 목록이 제한된 경우 **Selected Applications and Filters**을 선택할 수 있습니다. 잠금 취소 아이콘( )은 암호화되었거나 암호화되지 않은 트래픽이 아닌 해독된 트래픽에서만 식별할 수 있는 애플리케이션을 나타냅니다. 자세한 내용은 16-5페이지의 개별 애플리케이션의 트래픽 매칭을/를 참조하십시오.

5단계 **Add to Rule**을 클릭하여 선택된 애플리케이션을 **Selected Applications and Filters** 목록에 추가합니다.

선택된 애플리케이션과 필터를 끌어서 놓을 수도 있습니다. 필터는 *Filters*라는 제목 아래, 애플리케이션은 *Applications*라는 제목 아래에 나타납니다.

팁 이 애플리케이션 조건에 다른 필터를 추가하기 전에 **Clear All Filters**를 클릭하여 기존 선택을 취소합니다.

6단계 **Selected Applications and Filters** 목록 위의 추가 아이콘( )을 클릭하여 현재 목록에 있는 모든 개별 애플리케이션과 필터로 구성된 사용자 지정 필터를 저장할 수도 있습니다.

객체 관리자를 사용하여 즉석에서 생성된 이 필터를 관리합니다. 3-15페이지의 애플리케이션 필터 작업을/를 참조하십시오. 사용자 생성 필터는 중첩이 불가능하므로 다른 사용자 생성 필터를 포함하는 필터를 저장할 수 없습니다.

7단계 규칙을 저장하거나 계속 수정합니다.

변경 사항이 적용되려면 액세스 제어 정책을 적용해야 합니다. 12-15페이지의 액세스 제어 정책 적용을/를 참조하십시오.

애플리케이션 제어의 제한 사항

라이센스: 제어

지원되는 디바이스: 지원되는 디바이스: Series 2 또는 X-Series를 제외하고 모두

애플리케이션 제어를 수행할 때 다음 사항에 유의하십시오.

애플리케이션 식별의 속도

애플리케이션 제어를 수행하려면 다음 조건이 충족되어야 합니다.

- 클라이언트와 서버 간에 모니터링되는 연결이 설정되었습니다.
- 세션에서 애플리케이션이 식별되었습니다.

이 식별은 3개 ~ 5개 패킷 내에서 또는 트래픽이 암호화된 경우에는 SSL 핸드셰이크의 서버 인증서 교환 후에 이루어져야 합니다. 이 첫 패킷 중 하나가 애플리케이션 조건이 포함된 액세스 제어 규칙의 다른 모든 조건과 매칭하지만 식별이 완료되지 않을 경우 액세스 제어 정책은 패킷의 통과를 허용합니다. 이러한 동작으로 연결이 설정되어 애플리케이션이 식별될 수 있습니다. 사용자의 편의를 위해 해당 규칙은 정보 아이콘( )으로 표시됩니다.

허용된 패킷은 액세스 제어 정책의 *기본* 침입 정책(*기본 작업* 침입 정책 또는 almost-matched 규칙의 침입 정책이 아님)에 의해 검사를 받습니다. 자세한 내용은 25-1페이지의 액세스 제어에 대한 기본 침입 정책 설정을/를 참조하십시오.

식별이 완료되면 애플리케이션 조건과 매칭하는 나머지 세션 트래픽에 액세스 제어 규칙 작업 및 모든 관련 침입 및 파일 정책이 적용됩니다.

암호화 트래픽 처리

SMTPS, POPS, FTPS, TelnetS, IMAPS와 같이 StartTLS 암호화 대상인 암호화되지 않은 애플리케이션 트래픽을 식별하여 필터링할 수 있습니다. 또한 TLS 클라이언트 hello 메시지의 Server Name 표시 또는 서버 인증서 주체 DN 값을 기반으로 특정 암호화 애플리케이션을 식별할 수 있습니다.

이러한 애플리케이션은 **SSL Protocol** 태그가 지정됩니다. 이 태그가 없는 애플리케이션은 암호화되지 않은 트래픽 또는 해독된 트래픽에서만 탐지할 수 있습니다. 액세스 제어 규칙과 매칭하기 전에 암호화 트래픽을 해독하거나 차단하는 SSL 검사 기능을 사용하는 것에 대한 자세한 내용은 19-1페이지의 트래픽 해독 이해을/를 참조하십시오.

페이로드 없는 애플리케이션 트래픽 패킷 처리

연결에 애플리케이션이 식별되는 페이로드가 없는 패킷에는 기본 정책 작업이 적용됩니다.

참조된 트래픽 처리

웹 서버에서 참조하는 트래픽(예: 광고 트래픽)에 적용될 규칙을 생성하려면 참조하는 애플리케이션이 아닌 참조되는 애플리케이션에 대한 조건을 추가합니다. 자세한 내용은 45-15페이지의 특별 고려 사항: 참조된 웹 애플리케이션을/를 참조하십시오.

애플리케이션 탐지기 자동 활성화

정책의 각 애플리케이션 규칙 조건에 대해 하나 이상의 탐지기가 활성화되어야 합니다(46-27페이지의 탐지기 활성화 및 비활성화 참조). 어떤 애플리케이션에 대해 활성화된 탐지기가 없을 경우 자동으로 모든 시스템 제공 탐지기가 해당 애플리케이션에 대해 활성화됩니다. 시스템 제공 탐지기가 하나도 없을 경우 가장 최근에 수정된 사용자 정의 탐지기를 이 애플리케이션에 대해 활성화합니다.

다중 프로토콜을 사용하는 애플리케이션 트래픽 제어(Skype)

여러 유형의 Skype 애플리케이션 트래픽을 탐지할 수 있습니다. Skype 트래픽을 제어할 애플리케이션 조건을 작성할 때 개별 애플리케이션을 선택하기보다는 **Application Filters** 목록에서 **Skype** 태그를 선택합니다. 그러면 모든 Skype 트래픽을 탐지하여 동일하게 제어할 수 있습니다. 자세한 내용은 16-4페이지의 애플리케이션 필터로 트래픽 매칭을/를 참조하십시오.

URL 차단

라이센스: 기능에 따라

지원되는 디바이스: Series 2를 제외하고 모두

지원되는 Defense Center: 기능에 따라

액세스 제어 규칙의 URL 조건으로 네트워크 사용자의 액세스가 가능한 웹 사이트를 제한할 수 있습니다. 이 기능을 *URL 필터링*이라고 합니다. 액세스 제어를 통해 차단하거나 허용할 URL을 지정하는 2가지 방법이 있습니다.

- 어떤 라이센스에서도 개별 URL 또는 URL 그룹을 수동으로 지정하여 웹 트래픽에 대한 정밀한 사용자 지정 제어를 수행할 수 있습니다.
- URL 필터링 라이센스에서는 URL의 일반 분류 또는 *범주*, 위험 레벨 혹은 *평판*을 기반으로 웹 사이트에 대한 액세스를 제어할 수도 있습니다. 이러한 범주 및 평판 데이터는 연결 로그, 침입 이벤트, 애플리케이션 세부사항에 표시됩니다.

참고 이벤트에서 URL 범주 및 평판 정보를 확인하려면 URL 조건이 있는 액세스 제어 규칙을 하나 이상 생성해야 합니다.

웹 사이트를 차단할 때 사용자의 브라우저에서 기본 동작을 허용하거나 일반 시스템 제공 페이지 또는 사용자 지정 페이지를 표시할 수 있습니다. 사용자가 경고 페이지를 클릭하여 웹 사이트 차단을 우회하게 할 수도 있습니다.

암호화 웹 트래픽 처리

암호화 트래픽을 해독하는 SSL 검사(19-1페이지의 트래픽 해독 이해 참조)를 구성할 경우 액세스 제어 규칙은 해독된 트래픽을 암호화되지 않은 것처럼 평가합니다. 그러나 SSL 검사 컨피그레이션에서 암호화 연결이 해독되지 않고 통과하는 것을 허용하거나 SSL 검사를 구성하지 않을 경우 액세스 제어 규칙은 암호화 트래픽을 평가합니다.

URL 조건이 있는 액세스 제어 규칙으로 웹 트래픽을 평가할 때 트래픽 암호화에 쓰이는 공개 키 인증서의 주체 CN(common name)을 기반으로 HTTPS 트래픽을 매칭합니다. 또한 주체 CN에 포함된 하위 도메인은 무시하므로 수동으로 HTTPS URL을 필터링할 때 하위 도메인 정보를 포함하지 마십시오. 이를테면 `www.example.com` 대신 `example.com`을 사용하십시오.

또한 암호화 프로토콜(HTTP 대 HTTPS)을 무시합니다. 이는 수동 및 평판 기반 URL 조건 모두에 해당됩니다. 즉 액세스 제어 규칙은 다음 웹 사이트에 대한 트래픽을 동일하게 처리합니다.

- http://example.com/
- https://example.com/

HTTP 또는 HTTPS 트래픽만 매칭하는 액세스 제어 규칙을 구성하려면 규칙에 애플리케이션 조건을 추가합니다. 예를 들어 각각 애플리케이션 및 URL 조건을 갖춘 2개의 액세스 제어 규칙을 작성하여 어떤 사이트에 대한 HTTPS 액세스를 허용하되 HTTP 액세스는 허용하지 않을 수 있습니다.

첫 번째 규칙은 웹 사이트에 대한 HTTPS 트래픽을 허용합니다.

```
Action: Allow
Application: HTTPS
URL: example.com
```

두 번째 규칙은 동일한 웹 사이트에 대한 HTTP 액세스를 차단합니다.

```
Action: Block
Application: HTTP
URL: example.com
```

참고 기본적으로 세션 암호화 시도를 탐지하는 즉시 암호화 페이로드에 대한 침입 및 파일 검사를 비활성화합니다. 그러면 암호화 연결이 침입 및 파일 검사가 구성된 액세스 제어 규칙과 매칭할 때 오탐지를 줄이고 성능을 향상할 수 있습니다. 자세한 내용은 27-70페이지의 SSL 프리프로세서 사용을/를 참조하십시오.

Series 2가 아닌 어플라이언스에서 어떤 라이센스로도 URL을 수동 차단할 수 있지만, 범주 및 평판 기반 URL 필터링에는 URL 필터링 라이센스가 필요하며 DC500에서는 지원되지 않습니다.

표 16-2 URL 필터링을 위한 라이센스 및 모델 요구 사항

요구 사항	범주 및 평판 기반	수동
라이센스	URL 필터링	모두
디바이스	Series 2를 제외하고 모두	Series 2를 제외하고 모두
방어 센터	DC500을 제외하고 모두	모두

자세한 내용은 다음 링크를 참조하십시오.

- 16-10페이지의 평판 기반 URL 차단 수행
- 16-12페이지의 수동 URL 차단 수행
- 16-14페이지의 URL 탐지 및 차단의 제한 사항
- 16-15페이지의 사용자의 URL 차단 우회 허용
- 16-17페이지의 차단된 URL에 대한 사용자 지정 웹 페이지 표시

평판 기반 URL 차단 수행

라이센스: URL 필터링

지원되는 디바이스: Series 2를 제외하고 모두

지원되는 Defense Center: DC500을 제외하고 모두

URL 필터링 라이센스에서는 요청된 URL의 범주 및 평판을 기반으로 웹 사이트에 대한 사용자의 액세스를 제어할 수 있습니다. FireSIGHT 시스템에서는 Cisco 클라우드에서 이 범주 및 평판 정보를 얻습니다.

- URL *범주*는 URL의 일반적인 분류 중 하나입니다. 예를 들어 ebay.com은 **Auctions** 범주에, monster.com은 **Job Search** 범주에 속합니다. URL은 둘 이상의 범주에 속할 수 있습니다.
- URL *평판*은 이 URL이 조직의 보안 정책에 부합하지 않을 목적으로 사용될 가능성을 나타냅니다. URL의 위험은 **High Risk**(레벨 1)부터 **Well Known**(레벨 5)까지 다양합니다.

참고 범주 및 평판 기반 URL 조건이 있는 액세스 제어 규칙이 적용되려면 먼저 Cisco 클라우드와의 통신을 활성화해야 합니다. 그러면 방어 센터에서 URL 데이터를 검색할 수 있습니다. 자세한 내용은 64-27페이지의 클라우드 통신 활성화을/를 참조하십시오.

평판 기반 URL 차단의 장점

URL 범주 및 평판을 사용하면 액세스 제어 규칙을 위한 URL 조건을 신속하게 생성할 수 있습니다. 예를 들어 **Abused Drugs** 범주의 모든 **High Risk** URL을 식별하고 차단하는 액세스 제어 규칙을 생성할 수 있습니다. 사용자가 이 범주 및 평판 조합의 URL로 이동하려 하면 세션이 차단됩니다.

또한 Cisco 클라우드의 범주 및 평판 데이터를 사용하므로 정책 생성 및 관리가 간소화됩니다. 시스템에서 정상적으로 웹 트래픽을 제어하고 있음을 보장합니다. 또한 클라우드에서 새로운 URL 및 기존 URL의 새로운 범주와 리스크가 지속적으로 업데이트되므로, 요청된 URL이 최신 정보를 토대로 필터링되고 있음을 확신할 수 있습니다. 악성코드, 스팸, 봇넷, 피싱과 같은 보안 위협을 나타내는 악성 사이트가 새 정책을 업데이트하고 적용하는 것보다 빠른 속도로 등장했다가 사라지기도 합니다.

몇 가지 예를 들면 다음과 같습니다.

- 어떤 규칙이 모든 게임 사이트를 차단할 경우 새로운 도메인이 등록되어 **Gaming**으로 분류되면 이 사이트를 자동으로 차단할 수 있습니다.
- 어떤 규칙이 모든 악성코드 사이트를 차단할 경우 어떤 블로그가 악성코드에 감염되면 클라우드에서 해당 URL을 **Blog**에서 **Malware**로 재분류하고 시스템에서 이 사이트를 차단할 수 있습니다.
- 어떤 규칙이 위험도가 높은 소셜 네트워킹 사이트를 차단할 경우 누군가가 악성 페이로드 링크가 포함된 링크를 자신의 프로필 페이지에 게시하면 클라우드는 그 페이지의 평판을 **Benign sites**에서 **High Risk**로 변경하여 시스템이 이를 차단하게 할 수 있습니다.

클라우드에서 어떤 URL의 범주나 평판을 알지 못할 경우 또는 방어 센터에서 클라우드에 연결할 수 없을 경우 URL은 범주 또는 평판 기반 URL 조건이 있는 액세스 제어 규칙을 트리거하지 **않습니다**. 수동으로 URL에 범주나 평판을 지정할 수 없습니다.

URL 조건 작성

다음 그림은 모든 악성코드 사이트, 모든 고위험도 사이트, 모든 비 양성 소셜 네트워킹 사이트를 차단하는 액세스 제어 규칙의 URL 조건을 보여줍니다. 또한 URL 객체로 나타나는 example.com이라는 단일 사이트도 차단합니다.

Selected URLs에 최대 50개 항목을 추가하여 단일 URL 조건에서 매칭할 수 있습니다. 선택 사항으로 평판에 따라 정규화된 각 URL 범주는 하나의 항목으로 간주됩니다. URL 조건에 리터럴 URL과 URL 객체를 사용할 수도 있으나 이러한 항목을 평판으로 정규화할 수는 없습니다. 자세한 내용은 16-12페이지의 수동 URL 차단 수행을/를 참조하십시오.

다음 표에서는 위에서 소개한 조건을 작성하는 방법을 요약하여 보여줍니다. 리터럴 URL 또는 URL 객체는 평판으로 정규화할 수 없습니다.

표 16-3 예: URL 조건 작성

차단할 대상	선택할 범주 또는 URL 객체	평판
평판과 상관없이 악성 코드 사이트	Malware Sites	모두
위험도가 높은(레벨 1) 모든 URL	모두	1 — High Risk
위험도가 양성(benign)보다 높은(레벨 1부터 3까지) 소셜 네트워킹 사이트	Social Network	3 — Benign sites with security risks
example.com	example.com이라는 이름의 URL 객체	없음

URL 조건을 작성할 때 잘못된 컨피그레이션에는 경고 아이콘이 표시됩니다. 자세한 내용은 아이콘 위에 포인터를 놓으면 볼 수 있습니다. 12-21페이지의 액세스 제어 정책 및 규칙 문제 해결도 참조하십시오.

범주 및 평판 데이터를 사용하여 요청된 URL의 트래픽을 제어하려면

액세스: Admin/Access Admin/Network Admin

1단계 URL을 기준으로 트래픽을 제어할 디바이스에 대한 액세스 제어 정책에서 새 액세스 제어 규칙을 생성하거나 기존 규칙을 수정합니다.

자세한 내용은 14-3페이지의 액세스 제어 규칙 생성 및 수정을/를 참조하십시오.

2단계 규칙 편집기에서 URLs 탭을 선택합니다.

URLs 탭이 나타납니다.

3단계 **Categories and URLs** 목록에서 추가할 URL의 범주를 찾아 선택합니다. 범주와 상관없이 웹 트래픽과 매칭하려면 **Any** 범주를 선택합니다.

추가할 범주를 검색하려면 **Categories and URLs** 목록 위에서 **Search by name or value** 프롬프트를 클릭하고 범주 이름을 입력합니다. 입력할 때 목록이 업데이트되면서 매칭하는 범주를 표시합니다.

범주를 클릭하여 선택합니다. 여러 범주를 선택하려면 Shift 키와 Ctrl 키를 사용합니다.

팁 마우스 오른쪽 버튼을 클릭하고 **Select All** 범주를 선택할 수 있지만, 이렇게 모든 범주를 추가하면 액세스 제어 규칙의 최대 50개 항목 한도를 초과합니다. 그 대신 **Any**를 사용합니다.

4단계 **Reputations** 목록에서 평판 레벨을 클릭하여 범주 선택을 정규화할 수도 있습니다. 평판 레벨을 지정하지 않으면 모든 레벨을 의미하는 **Any**가 기본적으로 선택됩니다.

하나의 평판 레벨만 선택할 수 있습니다. 평판 레벨을 선택할 때 액세스 제어 규칙은 그 목적에 따라 다르게 작동합니다.

- 규칙이 웹 액세스를 차단하거나 모니터링할 경우(규칙 작업이 **Block**, **Block with reset**, **Interactive Block**, **Interactive Block with reset** 또는 **Monitor**) 평판 레벨을 선택하면 그 레벨보다 심각한 평판도 모두 선택됩니다. 예를 들어 **Suspicious sites**(레벨 2)를 차단하거나 모니터링하도록 규칙을 구성하면 **High risk**(레벨 1) 사이트도 자동으로 차단되거나 모니터링됩니다.
- 규칙에서 신뢰 또는 추가 검사로 웹 액세스를 허용할 경우(규칙 작업이 **Allow** 또는 **Trust**) 평판 레벨을 선택하면 그 레벨보다 덜 심각한 평판도 모두 선택됩니다. 예를 들어 **Benign sites**(레벨 4)를 허용하도록 규칙을 구성하면 **Well known**(레벨 5) 사이트도 자동으로 허용됩니다.

어떤 규칙에 대해 규칙 작업을 변경할 경우 위 설명과 같이 URL 조건의 평판 레벨이 자동으로 변경됩니다.

5단계 **Add to Rule**을 클릭하거나 선택된 항목을 끌어서 놓아 **Selected URLs** 목록에 추가합니다.

6단계 규칙을 저장하거나 계속 수정합니다.

변경 사항이 적용되려면 액세스 제어 정책을 적용해야 합니다. 12-15페이지의 액세스 제어 정책 적용을/를 참조하십시오.

수동 URL 차단 수행

라이센스: 모두

지원되는 디바이스: Series 2를 제외하고 모두

범주 및 평판으로 URL 필터링을 보완하거나 선택적으로 재정의하기 위해 개별 URL 또는 URL 그룹을 수동으로 지정하여 웹 트래픽을 제어할 수 있습니다. 그러면 허용된 웹 트래픽과 차단된 웹 트래픽에 대한 정밀한 사용자 지정 제어가 가능해집니다. 또한 특별한 라이센스 없이 이러한 유형의 URL 필터링을 수행할 수 있습니다.

액세스 제어 규칙에서 허용하거나 차단할 URL을 수동으로 지정하기 위해 단일 리터럴 URL에 입력할 수 있습니다. 또는 재사용 가능한 URL 객체를 사용하여 URL 조건을 구성하고 URL 또는 IP 주소에 이름을 연결할 수 있습니다.

팁 URL 객체를 생성한 다음 이를 사용하여 액세스 제어 규칙을 작성할 뿐 아니라 시스템 웹 인터페이스의 다른 여러 곳에서 URL을 나타낼 수 있습니다. 객체 관리자를 사용하여 이러한 객체를 생성할 수 있습니다. 액세스 제어 규칙을 구성하는 중에 즉석에서 URL 객체를 생성할 수도 있습니다. 자세한 내용은 3-14페이지의 URL 객체 작업을/를 참조하십시오.

URL 조건에서 URL 수동 지정

수동 입력을 통해 허용되거나 차단되는 웹 트래픽을 정확하게 제어할 수 있지만 수동으로 지정된 URL은 평판으로 정규화할 수 없습니다. 또한 규칙이 뜻밖의 결과를 초래하지 않는지 확인해야 합니다. 네트워크 트래픽이 URL 조건과 매칭하는지 확인하기 위해 단순 하위 문자열 매칭을 수행합니다. URL 객체 또는 수동으로 입력한 URL의 값이 모니터링되는 호스트에서 요청한 URL의 일부와 매칭할 경우 액세스 제어 규칙의 URL 조건을 충족합니다.

따라서 URL 객체를 비롯한 URL 조건에서 수동으로 URL을 지정할 때 다른 트래픽이 영향을 받지 않을지 신중하게 고려하십시오. 예를 들어 example.com에 대한 모든 트래픽을 허용할 경우 사용자는 다음과 같은 URL로 이동할 수 있습니다.

- http://example.com/
- http://example.com/newexample
- http://www.example.com/

또 다른 예로 ign.com(게임 사이트)을 명시적으로 차단하려 합니다. 그러나 하위 문자열 매칭에서는 *ign.com*을 차단하면 원래 의도와 다르게 veris*ign.com*도 차단됩니다.

암호화 웹 트래픽 수동 차단

SSL 검사 컨피그레이션에서 암호화 트래픽의 통과를 허용할 경우 또는 SSL 검사가 구성되지 않은 경우 액세스 제어 규칙은 암호화 트래픽을 처리합니다. 19-1페이지의 트래픽 해독 이해을/를 참조하십시오. 액세스 제어 규칙의 URL 조건:

- 웹 트래픽의 암호화 프로토콜(HTTP 대 HTTPS)을 무시합니다.

  예를 들어 액세스 제어 규칙은 http://example.com/에 대한 트래픽을 https://example.com/에 대한 트래픽과 동일하게 처리합니다. HTTP 또는 HTTPS 트래픽만 매칭하는 액세스 제어 규칙을 구성하려면 규칙에 애플리케이션 조건을 추가합니다. 자세한 내용은 16-8페이지의 URL 차단을/를 참조하십시오.

- 트래픽 암호화에 쓰이는 공개 키 인증서의 주체 CN을 기반으로 HTTPS 트래픽을 매칭하고, 주체 CN에 포함된 하위 도메인은 무시합니다.

  수동으로 HTTPS 트래픽을 필터링할 때 하위 도메인 정보를 포함하지 않습니다.

URL 조건을 작성할 때 잘못된 컨피그레이션에는 경고 아이콘이 표시됩니다. 자세한 내용은 아이콘 위에 포인터를 놓으면 볼 수 있습니다. 12-21페이지의 액세스 제어 정책 및 규칙 문제 해결도 참조하십시오.

허용하거나 차단할 URL을 수동으로 지정하여 웹 트래픽을 제어하려면

액세스: Admin/Access Admin/Network Admin

1단계 URL을 기준으로 트래픽을 제어할 디바이스에 대한 액세스 제어 정책에서 새 액세스 제어 규칙을 생성하거나 기존 규칙을 수정합니다.

자세한 내용은 14-3페이지의 액세스 제어 규칙 생성 및 수정을/를 참조하십시오.

2단계 규칙 편집기에서 URLs 탭을 선택합니다.

URLs 탭이 나타납니다.

3단계 **Categories and URLs** 목록에서 추가할 URL 객체 및 그룹을 찾아 선택합니다.

- 즉석에서 URL 객체를 추가하려면(그런 다음 조건에 추가할 수 있음) **Categories and URLs** 목록 위에서 추가 아이콘( )을 클릭합니다. 3-14페이지의 URL 객체 작업을/를 참조하십시오.
- 추가할 URL 객체 및 그룹을 검색하려면 **Categories and URLs** 목록 위에서 **Search by name or value** 프롬프트를 클릭한 다음 객체의 이름 또는 객체에 있는 URL이나 IP 주소의 값을 입력합니다. 입력할 때 목록이 업데이트되면서 매칭하는 객체를 표시합니다.

객체를 클릭하여 선택합니다. 여러 객체를 선택하려면 Shift 키와 Ctrl 키를 사용합니다. 마우스 오른쪽 버튼을 클릭하고 **Select All** URL 객체를 선택할 수 있지만, 이렇게 모든 URL을 추가하면 액세스 제어 규칙의 최대 50개 항목 한도를 초과합니다.

4단계 **Add to Rule**을 클릭하거나 선택된 항목을 **Selected URLs** 목록으로 추가합니다.

선택된 항목을 끌어서 놓을 수도 있습니다.

5단계 수동으로 지정할 리터럴 URL이 있으면 추가합니다. 이 필드에는 와일드카드(*)를 사용할 수 **없습니다**.

Selected URLs 목록 위의 **Enter URL** 프롬프트를 클릭합니다. 그런 다음 URL 또는 IP 주소를 입력하고 **Add**를 클릭합니다.

6단계 규칙을 저장하거나 계속 수정합니다.

변경 사항이 적용되려면 액세스 제어 정책을 적용해야 합니다. 12-15페이지의 액세스 제어 정책 적용을/를 참조하십시오.

URL 탐지 및 차단의 제한 사항

라이센스: 모두

지원되는 디바이스: Series 2를 제외하고 모두

URL 탐지 및 차단을 수행할 때 다음 사항에 유의하십시오.

URL 식별의 속도

URL을 필터링하려면 다음 조건이 충족되어야 합니다.

- 클라이언트와 서버 간에 모니터링되는 연결이 설정되었습니다.
- 세션에서 HTTP 또는 HTTPS 애플리케이션을 식별합니다.
- 요청된 URL을 식별합니다. 암호화 세션의 경우 클라이언트 hello 메시지 또는 서버 인증서에서 식별합니다.

이 식별은 3개 ~ 5개 패킷 내에서 또는 트래픽이 암호화된 경우에는 SSL 핸드셰이크의 서버 인증서 교환 후에 이루어져야 합니다. 이 첫 패킷 중 하나가 URL 조건이 포함된 액세스 제어 규칙의 다른 모든 조건과 매칭하지만 식별이 완료되지 않을 경우 액세스 제어 정책은 패킷의 통과를 허용합니다. 이러한 동작으로 연결이 설정되어 URL이 식별될 수 있습니다. 사용자의 편의를 위해 해당 규칙은 정보 아이콘( )으로 표시됩니다.

허용된 패킷은 액세스 제어 정책의 *기본* 침입 정책(*기본 작업* 침입 정책 또는 almost-matched 규칙의 침입 정책이 아님)에 의해 검사를 받습니다. 자세한 내용은 25-1페이지의 액세스 제어에 대한 기본 침입 정책 설정을/를 참조하십시오.

식별이 완료되면 URL 조건과 매칭하는 나머지 세션 트래픽에 액세스 제어 규칙 작업 및 모든 관련 침입 및 파일 정책이 적용됩니다.

암호화 웹 트래픽 처리

URL 조건이 있는 액세스 제어 규칙으로 암호화 웹 트래픽을 평가할 경우

- 암호화 프로토콜을 무시합니다. 액세스 제어 규칙은 URL 조건을 포함하지만 프로토콜을 지정하는 애플리케이션 조건이 없을 경우 HTTPS와 HTTP 트래픽 모두 매칭합니다.
- 트래픽 암호화에 쓰이는 공개 키 인증서의 주체 CN을 기반으로 HTTPS 트래픽을 매칭하고, 주체 CN에 포함된 하위 도메인은 무시합니다.
- HTTP 응답 페이지를 구성했더라도 표시하지 않습니다.

HTTP 응답 페이지

다음 조건과 함께 웹 트래픽이 차단되면 HTTP 응답 페이지는 나타나지 않습니다.

- 세션이 암호화되었거나 암호화된 적이 있습니다.
- 승격된 액세스 제어 규칙으로 인해 Series 3 디바이스에서 차단되었습니다.
- 위에서 설명한 것처럼, 연결이 설정되고 몇 개 패킷만큼 플로우가 허용될 때까지는 연결에서 요청된 URL을 식별하지 않습니다.

자세한 내용은 16-17페이지의 차단된 URL에 대한 사용자 지정 웹 페이지 표시을/를 참조하십시오.

URL의 검색 쿼리 파라미터

URL 조건을 매칭하는 데 URL의 검색 쿼리 파라미터를 사용하지 않습니다. 예를 들어 모든 쇼핑 트래픽을 차단하는 경우가 있습니다. 그러면 amazon.com을 찾는 웹 검색은 차단되지 않지만 amazon.com으로 이동하는 것은 차단됩니다.

사용자의 URL 차단 우회 허용

라이센스: 모두

지원되는 디바이스: Series 2를 제외하고 모두

액세스 제어 규칙을 사용하여 어떤 사용자의 HTTP 웹 요청을 차단할 때 그 규칙의 작업을 **Interactive Block** 또는 **Interactive Block with reset**으로 설정하면 사용자가 경고 *HTTP 응답 페이지*를 클릭하여 차단을 우회하는 것이 가능해집니다. 일반 시스템 제공 응답 페이지를 표시하거나 사용자 지정 HTML을 입력할 수 있습니다.

기본적으로 후속 방문 시 경고 페이지를 표시하지 않고 10분(600초) 동안 차단 우회를 허용할 수 있습니다. 이 기간을 1년만큼 길게 설정할 수 있으며, 또는 사용자가 항상 차단을 우회하게 할 수도 있습니다.

사용자가 차단을 우회하지 않을 경우 매칭하는 트래픽은 추가 검사 없이 거부됩니다. 또한 연결을 초기화할 수도 있습니다. 이와 달리 사용자가 차단을 우회하면 그 트래픽이 허용됩니다. 이 트래픽을 허용하면 계속 암호화되지 않은 페이로드를 대상으로 침입, 악성코드, 금지 파일, 검색 데이터에 대한 조사를 수행할 수 있습니다. 사용자가 차단을 우회한 후 새로 고침을 수행해야 로드되지 않았던 페이지 요소가 로드되는 경우도 있습니다.

인터랙티브 HTTP 응답 페이지는 차단 규칙에 대해 구성하는 응답 페이지와 별개로 구성합니다. 예를 들어 세션이 차단된 사용자에게 인터랙션 없이 시스템 제공 페이지를 표시할 수 있지만, 사용자 지정 페이지를 표시하여 사용자가 클릭한 다음 계속하게 할 수 있습니다. 자세한 내용은 16-17페이지의 차단된 URL에 대한 사용자 지정 웹 페이지 표시을/를 참조하십시오.

다음 상황에서는 응답 페이지가 나타나지 **않으며** 트래픽은 인터랙션 없이 차단됩니다. 세션이 인터랙티브 차단(Interactive Block) 규칙과 매칭하는 경우에도 그렇습니다.

- 세션이 암호화된 적이 있거나 현재 암호화된 경우. 여기에는 시스템에서 해독한 세션도 포함됩니다.
- 연결이 설정되었고 요청된 URL와 애플리케이션 세부사항의 조사가 가능한 패킷 수만큼 플로우가 허용된 후. 12-21페이지의 액세스 제어 정책 및 규칙 문제 해결을/를 참조하십시오.

팁 액세스 제어 정책의 모든 규칙에 대해 인터랙티브 차단을 신속하게 비활성화하려면 시스템 제공 페이지나 사용자 지정 페이지를 표시하지 않습니다. 그러면 인터랙티브 차단 규칙과 매칭하는 모든 연결을 인터랙션 없이 차단하게 됩니다.

사용자가 웹 사이트 차단을 우회할 수 있게 하려면

액세스: Admin/Access Admin/Network Admin

1단계 URL 조건으로 웹 트래픽과 매칭하는 액세스 제어 규칙을 생성합니다.

16-10페이지의 평판 기반 URL 차단 수행 및 16-12페이지의 수동 URL 차단 수행을/를 참조하십시오.

2단계 액세스 제어 규칙의 작업이 **Interactive Block** 또는 **Interactive Block with reset**이어야 합니다.

14-8페이지의 규칙 작업을 사용하여 트래픽 처리 및 검사 확인을/를 참조하십시오.

3단계 사용자가 차단을 우회할 것으로 가정하고 규칙에 대한 검사 및 로깅 옵션을 그에 알맞게 선택합니다. 허용 규칙의 경우

- 인터랙티브 차단 규칙의 어떤 유형도 파일 및 침입 정책과 연결할 수 있습니다. 또한 검색을 사용하여 이 사용자 허용 트래픽을 조사할 수 있습니다. 자세한 내용은 18-1페이지의 침입 정책 및 파일 정책을 사용하여 트래픽 제어을/를 참조하십시오.
- 인터랙티브 차단 트래픽에 대한 로깅 옵션은 허용된 트래픽의 로깅 옵션과 동일합니다. 단, 사용자가 인터랙티브 차단을 우회하지 않을 경우 연결 시작 이벤트만 로깅할 수 있습니다.

  초기에 사용자에게 경고 메시지가 표시될 때 인터랙티브 차단 또는 인터랙티브 차단 후 초기화 작업과 관련하여 로깅된 연결 시작 이벤트를 모두 표시합니다. 사용자가 차단을 우회할 경우 그 세션에 대해 로깅되는 추가 연결 이벤트의 작업은 허용(Allow)이 됩니다. 자세한 내용은 38-15페이지의 액세스 제어 처리 기반 연결 로깅을/를 참조하십시오.

4단계 사용자가 차단을 우회한 후 경고 페이지가 다시 표시될 때까지의 시간을 설정할 수도 있습니다.

16-16페이지의 차단된 웹 사이트에 대한 사용자 우회 시간 초과 설정을/를 참조하십시오.

5단계 사용자의 차단 우회를 허용하기 위해 표시할 사용자 지정 페이지를 생성하고 사용할 수도 있습니다.

16-17페이지의 차단된 URL에 대한 사용자 지정 웹 페이지 표시을/를 참조하십시오.

차단된 웹 사이트에 대한 사용자 우회 시간 초과 설정

라이센스: 모두

기본적으로 후속 방문 시 경고 페이지를 표시하지 않고 10분(600초) 동안 인터랙티브 차단 우회를 허용할 수 있습니다. 이 기간을 최대 1년까지 설정할 수 있으며, 0으로 설정하여 사용자가 항상 차단을 우회하게 할 수도 있습니다. 이 제한은 정책의 모든 인터랙티브 차단 규칙에 적용됩니다. 규칙별로 제한을 설정할 수 없습니다.

사용자 우회 만료 기한을 사용자 지정하려면

액세스: Admin/Access Admin/Network Admin

1단계 **Policies > Access Control**을 선택합니다.

Access Control Policy 페이지가 나타납니다.

2단계 구성하려는 액세스 제어 정책 옆의 수정 아이콘()을 클릭합니다.

액세스 제어 정책 편집기가 나타납니다.

3단계 **Advanced** 탭을 선택합니다.

액세스 제어 정책에 대한 고급 설정이 나타납니다.

4단계 General Settings 옆의 수정 아이콘()을 클릭합니다.

General Settings 팝업 창이 나타납니다.

5단계 **Allow an Interactive Block to bypass blocking for (seconds)** 필드에 사용자 우회가 만료될 때까지 경과할 시간(초)을 입력합니다.

0초에서 3,153만 6,000초(1년)까지 어떤 값도 지정할 수 있습니다. 0으로 지정하면 사용자는 매번 차단을 우회해야 합니다.

6단계 **OK**를 클릭합니다.

액세스 제어 정책에 대한 고급 설정이 나타납니다.

7단계 **Save**를 클릭합니다.

변경 사항이 적용되려면 액세스 제어 정책을 적용해야 합니다. 자세한 내용은 12-15페이지의 액세스 제어 정책 적용을/를 참조하십시오.

차단된 URL에 대한 사용자 지정 웹 페이지 표시

라이센스: 모두

지원되는 디바이스: Series 2를 제외하고 모두

사용자의 HTTP 웹 요청을 차단할 때 사용자의 브라우저에 표시되는 내용은 액세스 제어 규칙의 작업으로 세션을 차단하는 방식에 따라 달라집니다. 다음과 같이 선택해야 합니다.

- **Block** 또는 **Block with reset**을 선택하여 연결을 거부합니다. 차단된 세션의 시간이 초과되며 차단 후 초기화(Block with reset) 연결이 초기화됩니다. 그러나 두 가지 차단 작업 모두 연결이 거부되었음을 설명하는 사용자 지정 페이지로 기본 브라우저 또는 서버 페이지를 재정의할 수 있습니다. 이 사용자 지정 페이지를 *HTTP 응답 페이지*라고 합니다.
- **Interactive Block** 또는 **Interactive Block with reset**을 선택하여 사용자에게 경고하는 *인터랙티브 HTTP 응답 페이지*를 표시합니다. 또한 사용자는 버튼을 클릭하여 페이지를 계속하거나 새로 고쳐 원래 요청했던 사이트를 로드할 수 있습니다. 사용자가 응답 페이지를 우회한 후 새로 고침을 수행해야 로드되지 않았던 페이지 요소가 로드되는 경우도 있습니다.

일반 시스템 제공 응답 페이지를 표시하거나 사용자 지정 HTML을 입력할 수 있습니다. 사용자 지정 텍스트를 입력할 때 카운터가 나타나 현재까지 입력한 글자 수를 보여줍니다.

각 액세스 제어 정책에서 구성하는 인터랙티브 HTTP 응답 페이지는 인터랙션 없이 트래픽을 차단하는 데, 즉 차단 규칙에 쓰이는 응답 페이지와 별개입니다. 예를 들어 세션이 차단된 사용자에게 인터랙션 없이 시스템 제공 페이지를 표시할 수 있지만, 사용자 지정 페이지를 표시하여 사용자가 클릭한 다음 계속하게 할 수 있습니다.

사용자에게 HTTP 응답 페이지를 안정적으로 표시하는 데에는 네트워크 컨피그레이션, 트래픽 로드, 페이지의 크기가 영향을 줍니다. 사용자 지정 응답 페이지를 작성할 경우 페이지가 작을수록 성공적으로 표시될 가능성이 높음을 기억하십시오.

다음 조건과 함께 웹 트래픽이 차단되면 응답 페이지는 나타나지 않습니다.

- 보안 인텔리전스 블랙리스트에 의해 차단되었습니다.
- 그리고 세션이 원래 암호화되었습니다. 여기에는 SSL 검사 기능에 의해 차단된 암호화 연결뿐 아니라 차단 또는 인터랙티브 차단 액세스 제어 규칙과 매칭하는 해독된 트래픽과 암호화 트래픽도 포함됩니다.
- 승격된 액세스 제어 규칙으로 인해 Series 3 디바이스에서 차단되었습니다. 14-12페이지의 Series 3 디바이스를 이용한 트래픽 신뢰 또는 차단 제한 사항을/를 참조하십시오.
- 연결이 설정되었고 요청된 URL와 애플리케이션 세부사항의 조사가 가능한 패킷 수만큼 플로우가 허용된 후. 12-21페이지의 액세스 제어 정책 및 규칙 문제 해결을/를 참조하십시오.

HTTP 응답 페이지를 구성하려면

액세스: Admin/Access Admin/Network Admin

1단계 웹 트래픽을 모니터링하는 디바이스를 대상으로 한 액세스 제어 정책을 수정합니다.

자세한 내용은 12-11페이지의 액세스 제어 정책 수정을/를 참조하십시오.

2단계 HTTP Responses 탭을 선택합니다.

액세스 제어 정책에 대한 HTTP 응답 페이지 설정이 나타납니다.

3단계 **Block Response Page** 및 **Interactive Block Response Page**의 드롭다운 목록에서 응답을 선택합니다. 각 페이지에 대해 다음 옵션이 있습니다.

- 일반 응답을 사용하려면 **System-provided**를 선택합니다. 보기 아이콘( )을 클릭하여 이 페이지의 HTML 코드를 볼 수 있습니다.
- 사용자 지정 응답을 생성하려면 **Custom**을 선택합니다.

  팝업 창이 나타납니다. 시스템 제공 코드가 미리 입력되어 있으며, 이는 대체하거나 수정할 수 있습니다. 완료했으면 변경사항을 저장합니다. 수정 아이콘( )을 클릭하여 사용자 지정 페이지를 수정할 수 있습니다.
- HTTP 응답 페이지를 표시하지 않으려면 **None**을 선택합니다. 인터랙티브 차단 세션에 대해 이 옵션을 선택하면 사용자는 클릭하여 계속할 수 없습니다. 인터랙션 없이 세션이 차단됩니다.

4단계 **Save**를 클릭합니다.

변경 사항이 적용되려면 액세스 제어 정책을 적용해야 합니다. 자세한 내용은 12-15페이지의 액세스 제어 정책 적용을/를 참조하십시오.

17장 사용자 기반으로 트래픽 제어

*액세스 제어 정책*내 *액세스 제어 규칙*은 네트워크 트래픽 로깅 및 처리를 세부적으로 제어합니다. 액세스 제어 규칙의 사용자 조건을 사용하면 *사용자 제어*를 수행하여, 호스트에 로그인한 LDAP 사용자를 기반으로 트래픽을 제한함으로써 어떤 트래픽이 네트워크를 통과할 수 있는지를 제어할 수 있습니다.

사용자 제어는 *액세스 제어 대상 사용자*를 IP 주소와 연결함으로써 작동합니다. 구축된 에이전트는 지정된 사용자가 호스트에 로그인하고 로그아웃할 경우 해당 사용자를 모니터링하거나, 기타 사유에 따라 Active Directory 자격 증명을 인증합니다. 예를 들어, 조직에서는 중앙 집중식 인증을 위해 Active Directory에 기반한 서비스나 애플리케이션을 사용할 수 있습니다.

액세스 제어 규칙과 사용자 조건이 일치하는지 확인해야 하는 트래픽의 경우, 모니터링되는 세션에서 소스 또는 대상 호스트의 IP 주소를 로그인한 액세스 제어 대상 사용자와 연결해야 합니다. 개별 사용자 또는 그러한 사용자가 속한 그룹을 기반으로 트래픽을 제어할 수 있습니다.

사용자 조건을 상호 결합하거나 다른 유형의 조건과 결합하여 액세스 제어 규칙을 생성할 수 있습니다. 이러한 액세스 제어 규칙은 간단할 수도 있고 복잡할 수도 있으며, 여러 조건을 사용하여 트래픽을 검사하고 일치 여부를 확인할 수 있습니다. 액세스 제어 규칙에 대한 자세한 내용은 14-1페이지의 액세스 제어 규칙을 사용하여 트래픽 플로우 조정을/를 참조하십시오.

참고 하드웨어 기반 빠른 경로 규칙, 보안 인텔리전스 기반 트래픽 필터링, 일부 디코딩과 전처리는 네트워크 트래픽이 액세스 제어 규칙에 의해 평가되기 **전에** 발생합니다. 액세스 제어 규칙에 의해 평가되기 전에 암호화된 트래픽을 차단 또는 암호 해독하도록 *SSL 검사* 기능을 구성할 수도 있습니다.

제어 라이센스가 필요한 사용자 제어는 LDAP 사용자 및 그룹(액세스 제어 대상 사용자)에 대해서만 지원되며, Microsoft Active Directory 서버를 모니터링하는 User Agent에서 보고하는 로그인 및 로그오프 레코드를 사용합니다.

그러나 FireSIGHT 라이센스만 있어도 사용자 제어의 기본인 *사용자 인식*을 이용할 수 있습니다. 사용자 인식을 이용하면 에이전트에서 보고한 사용자 활동은 물론 *비 액세스 제어 대상 사용자*의 추가 활동도 볼 수 있습니다. 이를 통해 시스템은, 허용되는 네트워크 트래픽에서 관리되는 디바이스가 언제 검색 데이터를 검토하는지를 탐지할 수 있습니다. 시스템은 AIM, IMAP, LDAP, Oracle, POP3, SIP, FTP, HTTP, MDNS 등 다양한 프로토콜에서 로그인 시도를 식별할 수 있습니다.

시스템에서 보고한 사용자 활동에 컨텍스트를 추가하려면 구축에서 LDAP 서버를 쿼리하여, 액세스 제어 대상 사용자는 물론 비 액세스 제어 대상 사용자(사용자 검색에 의해 탐지되는 POP3 및 IMAP 사용자, 사용자 검색 또는 User Agent에 의해 활동이 탐지되는 LDAP 사용자)에 대해서도 메타데이터를 검색할 수 있습니다.

사용자 인식 기능을 이용하면 모든 구축 유형에서 "무엇" 뒤에 "누가" 있는지를 확인할 수 있습니다. 예를 들면 다음을 확인할 수 있습니다.

- 호스트 중요도가 높은 서버에 무단 액세스를 시도하는 사용자
- 대역폭을 너무 많이 사용하는 사용자
- 중요한 운영 체제 업데이트를 적용하지 않은 사용자
- 회사 IT 정책을 위반하며 인스턴트 메시징 소프트웨어나 피어 투 피어 파일 공유 애플리케이션을 사용하는 사용자
- 영향 레벨이 Vulnerable(level 1: red)인 침입 이벤트의 대상이 된 호스트를 소유한 사용자(보호 필요)
- 내부 공격 또는 포트 스캔을 시작한 사용자(보호 필요)

이러한 정보로 무장하면 표적 접근 방식을 통해 위험을 완화하고 다른 곳의 중단을 방지하기 위한 조치를 취할 수 있습니다. 사용자 제어를 통해 LDAP 사용자 및 사용자 활동을 차단할 수 있습니다. 사용자 인식 및 제어 기능을 함께 사용하면 감사 제어 효과를 크게 높이고 규정 준수를 강화할 수 있습니다. 자세한 내용은 45-3페이지의 사용자 데이터 수집 이해을/를 참조하십시오.

다음 표에는 사용자 인식 및 제어의 요건이 나열되어 있습니다. User Agents에 대한 자세한 최신 정보는 *User Agent Configuration Guide*를 참조하십시오.

표 17-1 사용자 인식 및 제어 요건

요건	사용자 인식	사용자 제어
라이센스	FireSIGHT	제어
디바이스	모두	Series 2 또는 X-Series를 제외한 모두
방어 센터	모두	DC500을 제외한 모든 방어 센터
사용자 에이전트	모니터링할 방어 센터 및 Microsoft Active Directory 서버와의 TCP/IP 액세스와 함께 다음 중 하나를 실행 중인 Windows 컴퓨터에 User Agent 버전 2.2 설치: • Windows Vista, Windows 7 또는 Windows 8 • Windows Server 2003, 2008 또는 2012 Microsoft .NET Framework 버전 4.0 Client Profile 및 Microsoft SQL CE(SQL Server Compact) 버전 3.5도 설치해야 합니다.	
사용자 메타데이터 검색을 위한 LDAP 서버	방어 센터에서의 TCP/IP 액세스와 함께 다음 중 하나: • Windows Server 2003 및 Windows Server 2008의 Microsoft Active Directory(사용자 제어에 필요) • Windows Server 2003 및 Windows Server 2008의 Oracle Directory Server Enterprise Edition 7.0(사용자 인식만) • Linux의 OpenLDAP(사용자 인식만) 이러한 서버는 실시간 모니터링을 지원하지 않는 Windows Server 2003을 제외하고, User Agents 및 정기 예약 폴링에 의한 실시간 모니터링을 지원합니다.	

자세한 내용은 다음 링크를 참고하십시오.

- 17-3페이지의 액세스 제어 규칙에 사용자 조건 추가
- 17-4페이지의 액세스 제어 대상 사용자 및 LDAP 사용자 메타데이터 검색
- 17-9페이지의 User Agents를 사용하여 Active Directory 로그인 보고

액세스 제어 규칙에 사용자 조건 추가

라이센스: 제어

지원되는 디바이스: Series 2 또는 X-Series를 제외한 모두

지원되는 Defense Center: DC500을 제외한 모든 방어 센터

FireSIGHT 시스템의 사용자 제어 기능은 액세스 제어 대상 사용자를 호스트 IP 주소와 연결함으로써 작동합니다. 구축된 User Agents는 Microsoft Active Directory 자격 증명으로 인증받는 지정된 사용자를 모니터링합니다. 액세스 제어 규칙과 사용자 조건이 일치하는지 확인해야 하는 트래픽의 경우, 모니터링되는 세션에서 소스 또는 대상 호스트의 IP 주소를 로그인한 액세스 제어 대상 사용자와 연결해야 합니다.

사용자 제어를 수행하려면 먼저 다음을 수행해야 합니다.

- 방어 센터와 Microsoft Active Directory 서버 간 연결을 구성합니다. 17-4페이지의 액세스 제어 대상 사용자 및 LDAP 사용자 메타데이터 검색을/를 참조하십시오.
- Active Directory 서버에 대한 TCP/IP 액세스와 함께 Microsoft Windows에 User Agent를 설치합니다. 17-9페이지의 User Agents를 사용하여 Active Directory 로그인 보고을/를 참조하십시오.

주의 모니터링할 대규모 사용자 그룹을 구성하는 경우 또는 매우 많은 수의 사용자를 네트워크의 호스트에 매핑하는 경우, 메모리 제한 때문에 시스템에서는 그룹을 기반으로 사용자 매핑을 삭제할 수 있습니다. 그 결과, 사용자 그룹 기반의 액세스 제어 규칙이 예상대로 작동하지 않을 수 있습니다.

단일 사용자 조건에서 최대 50명의 사용자 및 그룹을 **Selected Users**에 추가할 수 있습니다. 사용자 그룹의 조건은 하위 그룹의 멤버를 비롯한 그룹 멤버가 주고받는 트래픽을 확인합니다(제외된 하위 그룹에서 개별적으로 제외된 사용자 및 멤버 제외).

참고 그룹 기준을 사용하여 사용자 제어를 수행하려면 우선 시스템이 해당 그룹에 속한 사용자 한 명 이상의 활동을 탐지해야 합니다. 이 초기 연결은 일치하는 액세스 제어 그룹에 의해 처리되는 것이 **아니라**, 일치하는 다음 규칙 또는 액세스 제어 정책 기본 작업에 의해 처리됩니다.

사용자 조건을 작성하는 동안 경고 아이콘은 잘못된 컨피그레이션을 나타냅니다. 자세한 내용을 보려면 마우스 포인터를 아이콘 위에 올리고 12-21페이지의 액세스 제어 정책 및 규칙 문제 해결을/를 참조하십시오.

사용자 트래픽을 제어하려면

액세스: Admin/Access Admin/Network Admin

1단계 LDAP 사용자 또는 그룹별로 트래픽을 제어할 디바이스를 대상으로 하는 액세스 제어 정책에서 새 액세스 제어 규칙을 생성하거나 기존 규칙을 수정합니다.

자세한 지침은 14-3페이지의 액세스 제어 규칙 생성 및 수정을/를 참조하십시오.

2단계 규칙 편집기에서 Users 탭을 선택합니다.

Users 탭이 나타납니다.

3단계 **Available Users** 목록에서 추가할 사용자 및 그룹을 찾아 선택합니다.

사용자와 그룹은 서로 다른 아이콘으로 표시됩니다. 추가할 사용자와 그룹을 검색하려면 **Available Users** 목록 위에서 **Search by name or value** 프롬프트를 클릭하고 사용자 또는 그룹의 이름을 입력합니다. 입력하여 일치하는 항목이 표시됨에 따라 목록이 업데이트됩니다.

항목을 선택하려면 클릭합니다. 여러 항목을 선택하려면 Shift 및 Ctrl 키를 사용하거나, 마우스 오른쪽 버튼을 클릭하고 **Select All**을 선택합니다.

4단계 선택한 사용자와 그룹을 **Selected Users** 목록에 추가하려면 **Add to Rule**을 클릭합니다.

선택한 사용자와 그룹을 끌어다 놓을 수도 있습니다.

5단계 규칙을 저장하거나 계속 수정합니다.

변경 사항을 적용하려면 액세스 제어 정책을 적용해야 합니다. 12-15페이지의 액세스 제어 정책 적용을/를 참조하십시오.

액세스 제어 대상 사용자 및 LDAP 사용자 메타데이터 검색

라이센스: FireSIGHT 또는 제어

지원되는 디바이스: 기능에 따라 다름

지원되는 Defense Center: 기능에 따라 다름

사용자 제어를 수행(즉, 사용자 조건으로 액세스 제어 규칙 작성)하기 전에 방어 센터 및 조직의 Microsoft Active Directory 서버 중 하나 이상 사이에 연결을 구성해야 합니다. 방어 센터에서는 액세스 제어 대상 사용자(User Agents로 활동을 모니터링할 사용자와 그룹 및 트래픽을 제한할 때 기준으로 사용할 수 있는 사용자와 그룹)의 메타데이터를 업데이트하기 위해 규칙적으로 그리고 자동으로 LDAP 서버에 쿼리합니다. 방어 센터에서는 또한 User Agent에서 활동을 이미 보고한 비 액세스 제어 대상 사용자의 메타데이터도 검색합니다. 또는 주문형 쿼리를 수행할 수 있습니다.

사용자 제어를 수행하지 않는 경우 추가 유형의 LDAP 서버에서 사용자 인식 데이터(POP3 및 IMAP 사용자와 연결된 메타데이터는 물론, User Agent보다는 사용자 검색에 의해 활동이 탐지되는 LDAP 사용자와 연결된 메타데이터)를 쿼리할 수 있습니다. 시스템은 POP3 및 IMAP 로그인에서 이메일 주소를 사용하여 Active Directory, OpenLDAP 또는 Oracle Directory Server Enterprise Edition 서버의 LDAP 사용자를 연계합니다. 이 경우 방어 센터는 마지막 쿼리 이후 시스템에서 활동을 탐지한 사용자에 대한 새로운 메타데이터와 업데이트된 메타데이터를 얻기 위해 LDAP 서버에 규칙적으로 쿼리합니다.

자세한 내용은 다음 링크를 참고하십시오.

- 17-4페이지의 사용자 인식 및 제어를 위해 LDAP 서버에 연결
- 17-8페이지의 사용자 제어 매개변수 온디맨드 업데이트
- 17-9페이지의 LDAP 서버와의 통신 일시 중지

사용자 인식 및 제어를 위해 LDAP 서버에 연결

라이센스: FireSIGHT 또는 제어

지원되는 디바이스: 기능에 따라 다름

지원되는 Defense Center: 기능에 따라 다름

방어 센터 및 조직의 LDAP 서버 간 연결을 통해 다음을 수행할 수 있습니다.

- User Agents로 활동을 모니터링하고자 하며 액세스 제어 규칙으로 트래픽을 제한할 때 기준으로 사용할 수 있는 액세스 제어 대상 사용자 및 그룹을 지정할 수 있습니다.
- 서버에서 액세스 제어 대상 사용자 및 비 액세스 제어 대상 사용자(사용자 검색에 의해 탐지되는 POP3 및 IMAP 사용자, 그리고 사용자 검색 또는 User Agent에 의해 활동이 탐지되는 LDAP 사용자)에 대한 메타데이터를 쿼리할 수 있습니다.

이러한 연결 또는 *사용자 인식 객체*는 LDAP 서버에 대한 연결 설정 및 인증 필터 설정을 지정합니다. 이들은 FireSIGHT 시스템의 웹 인터페이스에 대한 외부 인증을 관리하기 위해 구성하는 인증 객체와 유사합니다. 61-5페이지의 인증 객체 관리을/를 참조하십시오.

사용자 제어를 수행하려면 Microsoft Active Directory LDAP 서버에 **반드시** 연결해야 합니다. LDAP 사용자 메타데이터만 검색하려는 경우 시스템에서는 다른 LDAP 서버 유형에 대한 연결을 지원합니다. 17-2 페이지의 표 17-1을/를 참조하십시오.

시스템에서는 사용자 활동을 탐지하면 해당 사용자의 레코드를 방어 센터 사용자 데이터베이스(사용자 ID 데이터베이스라고도 함)에 추가할 수 있습니다. 마지막 쿼리 이후 활동이 탐지된 새 사용자 및 업데이트된 사용자의 메타데이터를 얻기 위해 방어 센터에서는 규칙적으로 LDAP 서버에 쿼리합니다. 사용자가 이미 데이터베이스에 있는 경우, 지난 12시간 동안 업데이트되지 않았으면 메타데이터를 업데이트합니다. 시스템에서 새 사용자 로그인을 탐지한 후 방어 센터에서 사용자 메타데이터를 업데이트하는 데 몇 분 정도 걸릴 수 있습니다.

시스템에서는 LDAP 서버의 사용자를 연계하기 위해 POP3 및 IMAP 로그인의 이메일 주소를 사용합니다. 예를 들어, 관리되는 디바이스가 LDAP 사용자와 동일한 이메일 주소의 사용자에 대해 POP3 로그인을 탐지하면 시스템은 LDAP 사용자의 메타데이터를 해당 사용자와 연결합니다.

참고 시스템에서 탐지한 사용자를 LDAP 서버에서 제거해도 방어 센터에서는 해당 사용자를 자체 사용자 데이터베이스에서 제거하지 **않습니다**. 따라서 해당 사용자를 수동으로 삭제해야 합니다. 그러나 방어 센터에서 액세스 제어 대상 사용자의 목록을 다음에 업데이트할 때 LDAP 변경 사항이 액세스 제어 규칙에 **반영됩니다**.

다음 표에는 모니터링되는 사용자와 연결할 수 있는 LDAP 메타데이터가 나열되어 있습니다. 사용자 메타데이터를 LDAP 서버에서 성공적으로 검색하려면 서버에서는 표에 나열된 LDAP 필드 이름을 **반드시** 사용해야 합니다. LDAP 서버에서 필드 이름을 변경하면 방어 센터에서는 자체 데이터베이스를 해당 필드의 정보로 채우지 못합니다.

표 17-2 LDAP 필드를 Cisco 필드에 매핑

메타데이터	방어 센터	Active Directory	Oracle Directory Server	OpenLDAP
LDAP 사용자 이름	아이디	samaccountname	cn UID	cn UID
first name	이름	givenname	givenname	givenname
last name	성	sn	sn	sn
email address	이메일	mail userprincipalname(mail에 값이 없는 경우)	mail	mail
department	부서	department distinguishedname(department에 값이 없는 경우)	department	ou
telephone number	전화	telephonenumber	해당 없음	telephonenumber

LDAP 서버가 올바르게 구성되어 있으며 연결 가능한지 확인할 수 있도록, 그리고 LDAP 연결을 생성할 때 제공해야 할 정보를 얻을 수 있도록 LDAP 관리자와 긴밀하게 협력하십시오.

서버 유형, IP 주소 및 포트

서버 유형, IP 주소 또는 호스트 이름, 그리고 주(선택적으로 백업) LDAP 서버에 대한 포트를 지정해야 합니다. 사용자 제어를 수행하려면 **반드시** Microsoft Active Directory 서버를 사용해야 합니다.

LDAP 전용 매개변수

인증 서버에서 사용자 정보를 찾기 위해 LDAP 서버를 검색할 때 방어 센터에 해당 검색의 시작 지점이 필요합니다. 기본 고유 이름, 즉 *기본 DN*을 제공하여 *네임스페이스* 또는 디렉토리 트리를 지정할 수 있습니다. 일반적으로 기본 DN에는 회사 도메인 및 운영 단위를 나타내는 기본 구조가 있습니다. 예를 들어, Example 회사의 Security 조직에는 기본 DN `ou=security,dc=example,dc=com`이 있을 수 있습니다. 주 서버를 식별한 후에는 서버에서 사용 가능한 기본 DN 목록을 자동으로 검색하고 적절한 기본 DN을 선택할 수 있습니다.

검색할 사용자 정보에 대한 적절한 권한과 함께 사용자에 대한 자격 증명을 제공해야 합니다. 사용자에 대해 지정하는 고유 이름은 디렉토리 서버용 디렉토리 정보 트리에서 고유해야 합니다.

LDAP 연결을 위한 암호화 방법을 지정할 수도 있습니다. 인증서를 사용하여 인증하는 경우 인증서의 LDAP 서버 이름이 방어 센터 웹 인터페이스에서 지정한 호스트 이름과 **반드시** 일치해야 합니다. 예를 들어 LDAP 연결 구성 시 `10.10.10.250`을 사용했지만 인증서에는 `computer1.example.com`으로 되어 있으면 연결이 실패합니다.

끝으로, 무응답 LDAP 서버를 백업 연결로 롤오버하기까지 대기해야 할 시간 초과 기간을 지정해야 합니다.

사용자 및 그룹 액세스 제어 매개변수

사용자 제어를 수행하려면 액세스 제어 규칙에서 기준으로 사용하려는 그룹을 지정하십시오.

그룹을 포함하면 하위 그룹의 멤버를 포함하여 해당 그룹의 모든 멤버가 자동으로 포함됩니다. 그러나 액세스 제어 규칙에서 하위 그룹을 사용하려면 하위 그룹을 명시적으로 포함해야 합니다. 그룹 및 개별 사용자를 제외할 수도 있습니다. 그룹을 제외하면, 사용자들이 포함된 그룹의 멤버인 경우에도, 해당 그룹의 모든 멤버가 제외됩니다.

액세스 제어에 사용할 수 있는 최대 사용자 수는 FireSIGHT 라이센스에 따라 다릅니다. 포함할 사용자 및 그룹을 선택할 경우 총 사용자 수가 FireSIGHT 사용자 라이센스 미만인지 확인하십시오. 액세스 제어 매개변수가 너무 광범위하면, 방어 센터에서는 최대한 많은 사용자의 정보를 가져오며 검색에 실패한 사용자 수를 작업 대기열에 보고합니다.

참고 포함할 그룹을 지정하지 않으면 시스템은 제공된 LDAP 매개변수와 일치하는 모든 그룹에서 사용자 데이터를 검색합니다. 성능상의 이유로, Cisco에서는 액세스 제어에 사용할 사용자를 대표하는 그룹만을 명시적으로 포함할 것을 권장합니다. 사용자 또는 도메인 사용자 그룹은 포함할 수 **없습니다**.

액세스 제어에 사용할 새 사용자를 가져오기 위해 방어 센터에서 LDAP 서버에 쿼리할 빈도를 지정해야 합니다.

LDAP 연결을 생성한 후, 삭제 아이콘( )을 클릭하고 확인하여 연결을 삭제할 수 있습니다. LDAP 연결을 수정하려면 수정 아이콘( )을 클릭합니다. 연결이 활성화되면, 방어 센터에서 다음에 LDAP 서버에 쿼리할 때 저장된 변경 사항이 적용됩니다.

사용자 인식 또는 사용자 제어를 위해 LDAP 연결을 생성하려면

액세스: Admin/Discovery Admin

1단계 **Policies > Users**를 선택합니다.

Users Policy 페이지가 나타납니다.

2단계 **Add LDAP Connection**을 클릭합니다.

Create User Awareness Authentication Object 페이지가 나타납니다.

3단계 객체의 **Name** 및 **Description**을 입력합니다.

4단계 LDAP **Server Type**을 선택합니다.

사용자 제어를 수행하려면 Microsoft Active Directory LDAP 서버를 **반드시** 사용해야 합니다.

참고 User Agents는 $ 문자로 끝나는 Active Directory 사용자 이름을 방어 센터로 전송할 수 없습니다. 해당 사용자를 모니터링하려면 마지막 $ 문자를 제거해야 합니다.

5단계 주(선택적으로 백업) LDAP 서버에 대한 **IP Address** 또는 **Host Name**을 지정합니다.

6단계 LDAP 서버에서 인증 트래픽을 위해 사용할 **Port**를 지정합니다.

7단계 액세스할 LDAP 디렉토리의 **Base DN**을 지정합니다.

예를 들어 Example 회사의 Security 조직에서 이름을 인증하려면 `ou=security,dc=example,dc=com`을 입력합니다.

팁 사용 가능한 모든 도메인의 목록을 가져오려면 **Fetch DNs**를 클릭하고 드롭다운 목록에서 해당 기본 고유 이름을 선택합니다.

8단계 LDAP 디렉토리에 대한 액세스를 검증하는 데 사용할 고유한 **User Name** 및 **Password**를 지정합니다. 비밀번호를 확인합니다.

예를 들어, 사용자 객체가 `uid` 특성을 가지고 있고 Example 회사 Security 부서의 관리자에 대한 객체의 `uid` 값이 `NetworkAdmin`인 OpenLDAP 서버에 연결하는 경우 `uid=NetworkAdmin,ou=security,dc=example,dc=com`을 입력합니다.

9단계 **Encryption** 방법을 선택합니다. 암호화를 사용 중인 경우 **SSL Certificate**를 추가할 수 있습니다.

인증서의 호스트 이름은 5단계에서 지정한 LDAP 서버의 호스트 이름과 **반드시** 일치해야 합니다.

10단계 무응답 주 LDAP 서버를 백업 연결로 롤오버하기까지 대기해야 할 **Timeout** 기간을 지정합니다.

11단계 선택적으로, 객체에 대한 사용자 인식 설정을 지정하기 전에 **Test**를 클릭하여 연결을 테스트합니다.

12단계 4단계에서 선택한 LDAP 서버 유형에 따라 두 가지 옵션이 있습니다.

- Active Directory 서버에 연결하는 경우, 액세스 제어에 사용할 사용자를 지정하기 위해 **User/Group Access Control Parameters**를 활성화할 수 있습니다. 다음 단계로 계속 진행합니다.
- 다른 종류의 서버에 연결하거나 사용자 제어를 수행하지 않으려는 경우 17단계로 건너뜁니다.

13단계 제공한 LDAP 매개변수를 사용하여 사용 가능한 그룹 목록을 채우려면 **Fetch Groups**를 클릭합니다.

14단계 오른쪽 및 왼쪽 화살표 버튼으로 그룹을 포함하고 제외하여 액세스 제어에서 사용할 사용자를 지정합니다.

그룹을 포함하면 하위 그룹의 멤버를 포함하여 해당 그룹의 모든 멤버가 자동으로 포함됩니다. 그러나 액세스 제어 규칙에서 하위 그룹을 사용하려면 하위 그룹을 명시적으로 포함해야 합니다. 그룹을 제외하면, 사용자들이 포함된 그룹의 멤버인 경우에도, 해당 그룹의 모든 멤버가 제외됩니다.

15단계 특별한 **User Exclusions**를 지정합니다.

사용자를 제외하면 해당 사용자를 조건으로 사용하여 액세스 제어 규칙을 작성할 수 없습니다. 사용자가 여러 명인 경우 쉼표로 구분하십시오. 이 필드에서는 와일드카드 문자로 별표(*)를 사용할 수도 있습니다.

16단계 새 사용자 및 그룹 정보를 얻기 위해 LDAP 서버에 쿼리할 빈도를 지정합니다.

기본적으로 방어 센터에서는 하루에 한 번 자정에 서버에 쿼리합니다.

- 쿼리할 시간을 지정하려면 **Start At** 드롭다운 목록을 사용합니다. **0**은 자정, **1**은 1:00 AM 등을 나타냅니다.
- 서버에 쿼리할 빈도를 지정하려면(시간 단위) **Update Interval** 드롭다운 목록을 사용합니다.

17단계 **Save**를 클릭합니다.

사용자 및 그룹 액세스 제어 매개변수를 추가 또는 변경한 경우 변경 사항의 구현 여부를 확인해야 합니다. 객체가 저장되고 Users Policy 페이지가 다시 나타납니다.

18단계 방금 생성한 연결 옆에 있는 슬라이더를 클릭하여 연결을 활성화합니다.

연결을 활성화하려고 하며 연결에 사용자 및 그룹 액세스 제어 매개변수가 있는 경우, 사용자 및 그룹 정보를 가져오기 위해 LDAP 서버에 즉시 쿼리할지 여부를 선택합니다. LDAP 서버에 즉시 쿼리하지 않으면 예정된 시간에 쿼리가 발생합니다. 작업 대기열에서 쿼리 진행 상황을 모니터링할 수 있습니다(**System > Monitoring > Task Status**).

사용자 제어 매개변수 온디맨드 업데이트

라이센스: 제어

지원되는 디바이스: Series 2 또는 X-Series를 제외한 모두

지원되는 Defense Center: DC500을 제외한 모든 방어 센터

LDAP 연결에서 사용자 및 그룹 액세스 제어 매개변수를 변경하는 경우, 또는 LDAP 서버에서 사용자 또는 그룹을 변경하고 사용자 제어를 위해 변경 사항을 즉시 적용하려는 경우, 방어 센터가 Active Directory 서버에서 온디맨드 사용자 데이터 검색을 수행하도록 강제로 지정할 수 있습니다.

방어 센터가 서버에서 검색할 수 있는 최대 사용자 수는 FireSIGHT 라이센스에 따라 다릅니다. LDAP 연결의 액세스 제어 매개변수가 너무 광범위하면, 방어 센터에서는 최대한 많은 사용자의 정보를 가져오며 검색에 실패한 사용자 수를 작업 대기열에 보고합니다.

온디맨드 사용자 데이터 검색을 수행하려면

액세스: Admin/Discovery Admin

1단계 **Policies > Users**를 선택합니다.

Users Policy 페이지가 나타납니다.

2단계 LDAP 서버에 쿼리하는 데 사용할 LDAP 연결 옆에서 다운로드 아이콘( )을 클릭합니다.

쿼리가 시작됩니다. 작업 대기열에서 진행 상황을 모니터링할 수 있습니다(**System > Monitoring > Task Status**).

LDAP 서버와의 통신 일시 중지

라이센스: FireSIGHT 또는 제어

지원되는 디바이스: 기능에 따라 다름

지원되는 Defense Center: 기능에 따라 다름

LDAP 연결이 활성화된 경우에만 방어 센터에서 LDAP 서버에 쿼리할 수 있습니다. 쿼리를 중지하려면 LDAP 연결을 삭제하기보다는 일시적으로 비활성화할 수 있습니다.

액세스 제어에 사용되는 LDAP 연결을 다시 활성화할 때, 방어 센터에서 서버에 업데이트된 사용자 및 그룹 정보를 즉시 쿼리하도록 강제로 지정할 수도 있고 첫 번째 예정된 쿼리가 발생할 때까지 기다릴 수도 있습니다.

LDAP 연결을 비활성화 또는 다시 활성화하려면

액세스: Admin/Discovery Admin

1단계 **Policies > Users**를 선택합니다.

Users Policy 페이지가 나타납니다.

2단계 방금 생성한 연결 옆에 있는 슬라이더를 클릭하여 연결을 일시 중지 또는 다시 활성화합니다.

연결을 다시 활성화하려고 하며 연결에 사용자 및 그룹 액세스 제어 매개변수가 있는 경우, 사용자 및 그룹 정보를 가져오기 위해 LDAP 서버에 즉시 쿼리할지 여부를 선택합니다. LDAP 서버에 즉시 쿼리하지 않으면 예정된 시간에 쿼리가 발생합니다. 작업 대기열에서 쿼리 진행 상황을 모니터링할 수 있습니다(**System > Monitoring > Task Status**).

User Agents를 사용하여 Active Directory 로그인 보고

라이센스: FireSIGHT

Microsoft Windows 컴퓨터에 구축된 User Agents는 Microsoft Active Directory 서버를 모니터링한 다음, 조직의 LDAP 사용자가 호스트에서 로그인 또는 로그아웃하거나 다른 이유로 Active Directory 자격 증명으로 인증을 받을 때 방어 센터에 알립니다. 예를 들어, 조직에서는 중앙 집중식 인증을 위해 Active Directory에 기반한 서비스나 애플리케이션을 사용할 수 있습니다.

에이전트에서 보고하는 이 정보는 조직에서 사용자 활동의 레코드로 사용되는 것은 물론, 사용자 제어의 기본 정보로도 사용됩니다. 액세스 제어 규칙과 사용자 조건이 일치하는지 확인해야 하는 트래픽의 경우, 모니터링되는 세션에서 소스 또는 대상 호스트의 IP 주소를 로그인한 액세스 제어 대상 사용자와 연결해야 합니다. 개별 사용자 또는 그러한 사용자가 속한 그룹을 기반으로 트래픽을 제어할 수 있습니다.

참고 사용자 제어를 수행하려면 User Agents를 **반드시** 설치 및 사용해야 합니다. 그러나 User Agents는 Active Directory 인증과 관련된 사용자 활동만 보고합니다. 사용자 인식을 사용하면 에이전트에서 보고하는 모든 사용자 활동은 물론, 허용되는 네트워크 트래픽에서 관리되는 디바이스에 의해 탐지되는 추가 활동도 볼 수 있습니다. 시스템은 디렉토리 기능을 사용하여 AIM, IMAP, LDAP, Oracle, POP3, SIP, FTP, HTTP, MDNS 등 다양한 프로토콜에서 로그인 시도를 식별할 수 있습니다. 자세한 내용은 45-3페이지의 사용자 데이터 수집 이해을/를 참조하십시오.

사용자 인식 또는 제어용 User Agents로 LDAP 사용자 인증 레코드를 검색할 경우, 먼저 에이전트에서의 연결을 허용하도록 각 방어 센터를 구성합니다. 고가용성 구축에서는 주 방어 센터 및 보조 방어 센터에서 모두 에이전트 통신을 활성화합니다. User Agents는 동시에 최대 다섯 개의 방어 센터에 연결할 수 있습니다. 방어 센터에서 User Agent 통신을 활성화한 후 Windows 컴퓨터에 에이전트를 설치할 수 있습니다. 17-2 페이지의 표 17-1을/를 참조하십시오.

끝으로, Microsoft Active Directory 서버에서 데이터를 검색하고 정보를 방어 센터에 보고하도록 User Agents를 구성합니다. 특정 사용자 이름 및 IP 주소를 보고에서 제외하고, 로컬 이벤트 로그 또는 Windows 애플리케이션 로그에 상태 메시지를 기록하도록 에이전트를 구성할 수도 있습니다. User Agent Status Monitor 상태 모듈은 방어 센터에 연결된 에이전트를 모니터링합니다. 68-28페이지의 User Agent Status 모니터링 구성을/를 참조하십시오.

User Agent에 연결하도록 방어 센터를 구성하려면

액세스: Admin/Discovery Admin

1단계 **Policies > Users**를 선택합니다.

Users Policy 페이지가 나타납니다.

2단계 **Add User Agent**를 클릭합니다.

Add User Agent 팝업 창이 나타납니다.

3단계 에이전트의 **Name**을 입력합니다.

4단계 에이전트를 설치할 컴퓨터의 **Hostname 또는 Address**를 입력합니다. IPv4 주소를 **반드시** 사용해야 합니다. IPv6 주소를 사용하여 User Agent에 연결하도록 방어 센터를 구성할 수는 없습니다.

5단계 **Add User Agent**를 클릭합니다.

방어 센터는 이제 지정한 컴퓨터에서 User Agent에 연결할 수 있습니다. 연결을 삭제하려면 삭제 아이콘( )을 클릭하고 확인합니다.

6단계 지정한 컴퓨터에 User Agent를 설치합니다. Microsoft Active Directory 서버에서 데이터를 검색하고 정보를 방어 센터에 보고하도록 User Agent를 구성합니다.

자세한 최신 정보는 *User Agent Configuration Guide*를 참조하십시오.

18장

침입 정책 및 파일 정책을 사용하여 트래픽 제어

침입 및 파일 정책은 FireSIGHT 시스템의 일부로서, 트래픽이 원하는 대상에 도달하도록 허용하기 전에 최종 방어선으로서의 역할을 함께 수행합니다.

- **침입 정책**은 시스템의 침입 방지 기능을 제어합니다(23-1페이지의 네트워크 분석 및 침입 정책 이해 참조).
- **파일 정책**은 시스템의 네트워크 기반 지능형 악성코드 차단(AMP) 기능을 제어합니다(37-9페이지의 파일 정책 이해 및 생성 참조).

하드웨어 기반의 fast-path, 보안 인텔리전스 기반의 트래픽 필터링(블랙리스트 추가), SSL 검사 기반의 결정, 트래픽 디코딩 및 전처리 작업은 침입, 금지된 파일, 악성코드에 대해 네트워크 트래픽 검사를 수행하기 **전에** 이루어집니다. 액세스 제어 규칙 및 액세스 제어 기본 작업은 어떤 트래픽이 침입 및 파일 정책으로 검사되는지 결정합니다.

침입 또는 파일 정책을 액세스 제어 정책과 연결할 경우, 액세스 제어 규칙의 조건과 매칭되는 트래픽이 통과되기 전에 침입 정책이나 파일 정책 또는 두 정책을 모두 사용하여 우선 트래픽을 검사하도록 할 수 있습니다.

참고 기본적으로, 시스템에서는 암호화된 페이로드의 침입 및 파일 검사를 비활성화합니다. 이는 암호화 연결이 침입 및 파일 검사가 구성된 액세스 제어 규칙과 일치하는 경우 오탐을 줄이고 성능을 높이는 데 도움이 됩니다. 자세한 내용은 19-1페이지의 트래픽 해독 이해 및 27-70페이지의 SSL 프리프로세서 사용을/를 참조하십시오.

침입 방지 및 AMP 기능의 경우 다음 표에 설명된 것처럼 액세스 제어 정책의 대상 디바이스에서 특정 라이센스 기능을 활성화해야 합니다.

표 18-1 침입 및 파일 검사를 위한 라이센스 및 모델 요구 사항

기능	설명	라이센스	지원되는 방어 센터	지원되는 장치
침입 방지	침입 및 익스플로잇을 탐지하고 선택적으로 차단	보호	모든	모든
파일 제어	파일 유형의 전송을 탐지하고 선택적으로 차단	보호	모든	모든
AMP(Advanced Malware Protection)	악성코드의 전송을 탐지, 저장, 추적 및 선택적으로 차단 악성코드 분석을 위해 캡처 파일을 Cisco 클라우드에 제출	악성코드	DC500을 제외한 모두	Series 2 또는 X-Series를 제외한 모두

조직이 FireAMP 서브스크립션을 보유한 경우, 방어 센터는 Cisco 클라우드에서 엔드포인트 기반의 악성코드 탐지 데이터를 전송받을 수도 있습니다. 방어 센터는 이러한 데이터를 시스템에서 생성된 네트워크 기반 파일 및 악성코드 데이터와 함께 제공합니다. FireAMP 데이터를 가져올 경우 FireAMP 서브스크립션 외에 라이센스가 필요하지 않습니다. 자세한 내용은 37-24페이지의 FireAMP를 위한 클라우드 연결 작업을/를 참조하십시오.

침입, 금지된 파일, 악성코드에 대해 트래픽을 검사하는 방법에 대한 자세한 내용은 다음을 참조하십시오.

- 18-2페이지의 침입 및 악성코드에 대해 허용된 트래픽 검사
- 18-8페이지의 침입 방지 성능 조정
- 18-20페이지의 파일 및 악성코드 검사 성능과 저장 조정

침입 및 악성코드에 대해 허용된 트래픽 검사

라이센스: 보호 또는 악성코드

지원되는 디바이스: 기능에 따라 다름

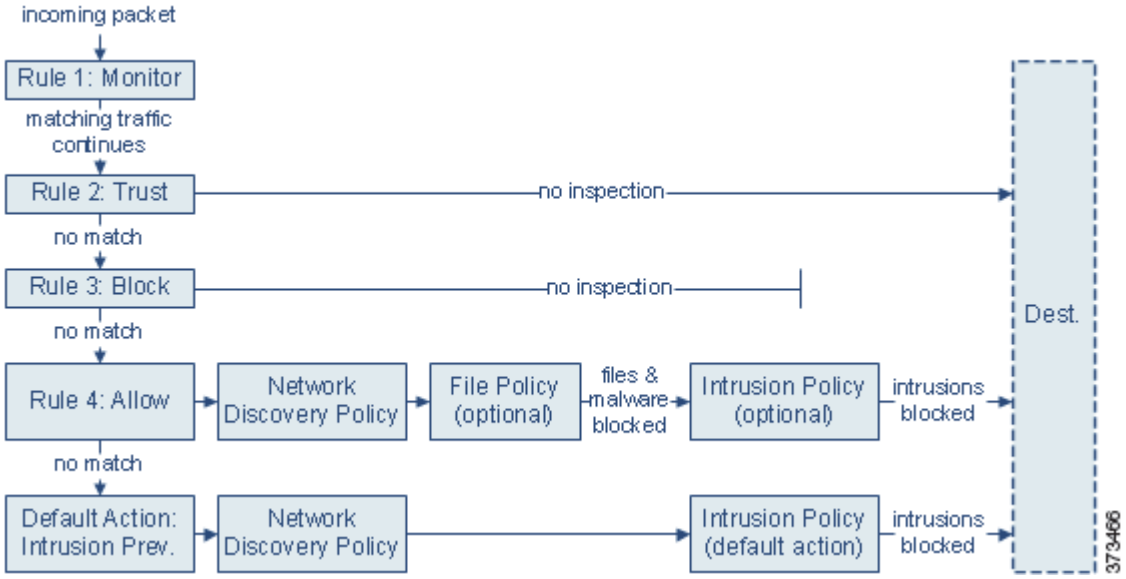
지원되는 Defense Center: 기능에 따라 다름

침입 및 파일 정책은 트래픽이 원하는 대상에 도달할 수 있게 되기 전에 최종 방어선으로서 시스템의 침입, 파일 제어, AMP 기능을 제어합니다. 하드웨어 기반의 fast-path 규칙, 보안 인텔리전스 기반의 트래픽 필터링, SSL 검사 결정(해독 포함), 디코딩 및 전처리, 액세스 제어 규칙 선택은 침입 및 파일 검사보다 **먼저** 수행됩니다.

액세스 제어 규칙은 여러 매니지드 디바이스 전반의 네트워크 트래픽을 처리할 수 있는 세부적인 방법을 제공합니다. 침입 또는 파일 정책을 액세스 제어 정책과 연결할 경우, 액세스 제어 규칙의 조건과 매칭되는 트래픽이 통과되기 전에 침입 정책이나 파일 정책 또는 두 정책을 모두 사용하여 우선 트래픽을 검사하도록 할 수 있습니다. 액세스 제어 규칙 조건은 간단하거나 복잡할 수 있으며 보안 영역, 네트워크 또는 지리적 위치, VLAN, 포트, 애플리케이션, 요청 URL, 사용자로 트래픽을 제어할 수 있습니다.

시스템에서는 사용자가 지정한 순서에 따라 트래픽을 액세스 제어 규칙에 대해 매칭합니다. 대부분의 경우, 시스템은 *모든* 규칙의 조건이 트래픽과 매칭되는 *첫 번째* 액세스 제어 규칙에 따라 네트워크 트래픽을 처리합니다. 액세스 제어 규칙의 *작업*은 시스템에서 매칭되는 트래픽을 처리하는 방식을 결정합니다. 매칭되는 트래픽을 모니터링, 신뢰, 차단, 허용(추가 검사 실행 또는 실행 안 함)할 수 있습니다(14-8페이지의 규칙 작업을 사용하여 트래픽 처리 및 검사 확인 참조).

다음 다이어그램에는 네 가지 다른 유형의 액세스 제어 규칙 및 기본 작업이 포함된 액세스 제어 정책으로 제어되는 인라인 침입 방지 및 AMP 구축 시 트래픽의 흐름이 나와 있습니다.



위 시나리오의 경우, 정책에 있는 처음 세 개의 액세스 제어 규칙(Monitor, Trust, Block)은 매칭되는 트래픽을 검사할 수 없습니다. Monitor 규칙은 네트워크 트래픽을 추적하고 로깅하지만 검사를 수행하지는 않으므로, 시스템에서는 트래픽을 추가 규칙과 매칭하여 해당 트래픽을 허용할지 거부할지 결정합니다. Trust 및 Block 규칙은 어떠한 종류의 추가 검사 없이 매칭되는 트래픽을 처리하지만, 매칭되지 않는 트래픽은 다음 액세스 제어 규칙을 계속 진행합니다.

정책의 네 번째이자 마지막 규칙인 Allow 규칙은 여러 가지 다른 정책을 호출하여 매칭되는 트래픽을 다음과 같은 순서로 검사하고 처리합니다.

- **검색: 네트워크 검색 정책 —** 우선 네트워크 검색 정책은 검색 데이터에 대해 트래픽을 검사합니다. 검색은 수동 분석이며 트래픽의 흐름에 영향을 미치지 않습니다. 검색을 명시적으로 활성화하지 않은 경우에도 이를 향상하거나 비활성화할 수 있습니다. 그러나 트래픽을 허용한다고 해서 검색 데이터 수집이 자동으로 보장되는 것은 아닙니다. 시스템에서는 네트워크 검색 정책에서 명시적으로 모니터링하는 IP 주소와 관련된 연결에 대해서만 검색을 수행합니다. 자세한 내용은 45-1페이지의 네트워크 검색 소개을/를 참조하십시오.
- **지능형 악성코드 차단 및 파일 제어: 파일 정책 —** 검색으로 트래픽이 검사되면, 시스템에서는 금지된 파일 및 악성코드에 대해 해당 트래픽을 검사할 수 있습니다. 네트워크 기반의 AMP는 다양한 종류의 파일(PDF, Microsoft Office 문서 등)에 존재하는 악성코드를 탐지하고 선택적으로 차단합니다. 조직에서 악성코드 파일의 전송뿐만 아니라 특정 유형의 모든 파일(해당 파일의 악성코드 포함 여부에 상관없이)을 차단하려는 경우, *파일 제어*를 사용하면 특정 파일 유형의 전송에 대해 네트워크 트래픽을 모니터링한 다음 해당 파일을 차단하거나 허용할 수 있습니다.
- **침입 방지: 침입 정책 —** 파일 검사 후, 시스템에서는 침입 및 익스플로잇에 대해 트래픽을 검사할 수 있습니다. 침입 정책은 패턴을 기반으로 공격에 대해 디코딩된 패킷을 검사하고, 악의적인 트래픽을 차단하거나 변경할 수 있습니다. 침입 정책은 네트워크 환경을 정확하게 반영하는 명명된 값을 사용할 수 있도록 지원하는 *변수 집합*과 쌍을 이룹니다.
- **대상 —** 트래픽이 위에 설명된 모든 확인 사항을 통과하여 원하는 대상에 도달합니다.

Interactive Block 규칙(다이어그램에 나와 있지 않음)에는 Allow 규칙과 동일한 검사 옵션이 있습니다. 이를 사용하면 사용자가 경고 페이지를 클릭하여 차단된 웹 페이지를 우회할 경우 악의적인 콘텐츠에 대해 트래픽을 검사할 수 있습니다. 자세한 내용은 14-10페이지의 Interactive Blocking 작

업: 사용자가 웹사이트 차단을 우회하도록 허용을/를 참조하십시오.

정책의 모든 비 Monitor 액세스 제어 규칙과 일치하지 않는 트래픽은 기본 작업에 의해 처리됩니다. 이 시나리오의 경우, 기본 작업은 침입 방지 작업이며 이 작업은 사용자가 지정한 침입 정책이 트래픽 통과를 허용할 경우 해당 트래픽은 원하는 최종 대상에 도달할 수 있도록 합니다. 다른 구축 작업의 경우, 추가 검사 없이 모든 트래픽을 신뢰하거나 차단하는 기본 작업이 있을 수 있습니다 (12-7 페이지의 표 12-4 참조). 시스템은 기본 작업에서 허용하는 트래픽은 검색 데이터 및 침입 여부를 검사할 수 있으나, 금지된 파일 또는 악성코드 여부는 검사할 수 없습니다. 파일 정책을 액세스 제어 기본 작업과 연결할 수 **없습니다**.

참고 액세스 제어 정책으로 연결을 분석할 경우, 시스템에서는 어떤 액세스 제어 규칙으로 트래픽을 처리할 것인지 결정하기 전에 해당 연결의 처음 몇 가지 패킷을 처리하여, **통과되도록 허용**해야 합니다. 그러나 이러한 패킷은 검사하지 않은 대상에는 도달할 수 없으며, 기본 침입 정책이라고 하는 침입 정책을 사용하여 이러한 패킷을 검사하고 침입 이벤트를 생성할 수 있습니다. 자세한 내용은 25-1페이지의 액세스 제어에 대한 기본 침입 정책 설정을/를 참조하십시오.

위의 시나리오에 대한 자세한 내용 및 파일과 침입 정책을 액세스 제어 규칙 및 액세스 제어 기본 작업과 연결하는 방법에 대한 지침을 보려면 다음을 참조하십시오.

- 18-4페이지의 파일 및 침입 검사 순서 이해
- 18-6페이지의 액세스 제어 규칙을 구성하여 AMP 또는 파일 제어 수행
- 18-7페이지의 액세스 제어 규칙을 구성하여 침입 방지 수행
- 12-6페이지의 네트워크 트래픽의 기본 처리 및 검사 설정

파일 및 침입 검사 순서 이해

라이센스: 보호 또는 악성코드

지원되는 디바이스: 기능에 따라 다름

지원되는 Defense Center: 기능에 따라 다름

18-2페이지의 침입 및 악성코드에 대해 허용된 트래픽 검사의 시나리오에는 파일 정책 및 침입 정책 모두와 연결된 Allow 규칙을 비롯하여 각 종류의 액세스 제어 규칙이 하나씩 나와 있습니다. 액세스 제어 정책에서 여러 개의 Allow 및 Interactive Block 규칙을 다양한 침입 및 파일 정책과 연결하여, 검사 프로필이 다양한 유형의 트래픽과 매칭되는지 알아볼 수 있습니다.

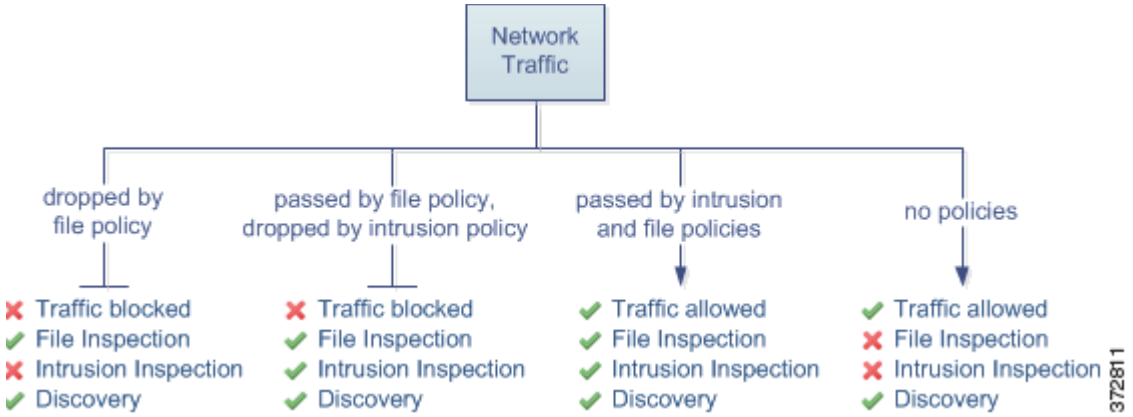
참고 Intrusion Prevention 또는 Network Discovery Only 기본 작업에서 허용되는 트래픽은 검색 데이터 및 침입 여부를 검사할 수 있으나, 금지된 파일 또는 악성코드 여부는 검사할 수 없습니다. 파일 정책을 액세스 제어 기본 작업과 연결할 수 **없습니다**.

동일한 규칙에서 파일 및 침입 검사를 모두 수행할 필요는 없습니다. Allow 또는 Interactive Block 규칙과 매칭되는 연결의 경우:

- 파일 정책이 없는 경우, 트래픽 흐름은 침입 정책에 의해 결정됨
- 침입 정책이 없는 경우, 트래픽 흐름은 파일 정책에 의해 결정됨
- 두 가지 정책이 모두 없는 경우, 허용되는 트래픽은 Network Discovery Only에 의해 검사됨

팁 시스템은 신뢰할 수 있는 트래픽에는 검사를 수행하지 않습니다. Trust 규칙처럼 Allow 규칙은 침입 또는 파일 정책 모두 트래픽을 통과하지 못하도록 구성하지만, Allow 규칙은 일치되는 트래픽에 검색을 수행할 수 있도록 합니다.

아래 다이어그램에는 Allow 또는 사용자 우회 Interactive Block 액세스 제어 규칙의 조건을 충족하는 트래픽에 수행할 수 있는 검사의 종류가 나와 있습니다. 간단한 설명을 위해, 다이어그램에는 침입 및 파일 정책 모두가 단일한 액세스 제어 규칙과 연결된 경우 또는 모두 연결되지 않은 경우의 트래픽 흐름이 표시되어 있습니다.



액세스 제어 규칙으로 처리되는 단일한 연결의 경우, 침입 검사 전에 파일 검사가 이루어집니다. 즉, 시스템에서는 파일 정책 또는 침입에 의해 차단된 파일은 검사하지 않습니다. 파일 검사 내에서 유형을 기준으로 한 간단한 차단은 악성코드 검사 및 차단보다 우선합니다.

예를 들어, 액세스 제어 규칙에 정의된 대로 특정 네트워크 트래픽을 일반적으로 허용하고자 하는 시나리오를 가정해보겠습니다. 그러나 일종의 예방 조치로서 실행 파일의 다운로드를 차단하고, 다운로드된 PDF의 악성코드 여부를 검사하고 검색된 모든 인스턴스를 차단하며, 트래픽에 침입 검사를 수행하고자 합니다.

프로비저닝으로 허용하고자 하는 트래픽의 특성과 매칭되는 규칙으로 액세스 제어 정책을 생성하고, 이를 침입 정책 및 파일 정책에 모두 연결합니다. 파일 정책은 모든 실행 파일의 다운로드를 차단하며, 검사를 수행하고 악성코드가 포함된 PDF를 차단합니다.

- 우선 시스템에서는 파일 정책에 지정된 것과 매칭되는 간단한 유형을 기준으로 모든 실행 파일의 다운로드를 차단합니다. 해당 파일은 즉시 차단되므로, 이러한 파일은 악성코드 클라우드 조회 또는 침입 검사 대상에서 제외됩니다.
- 그다음, 시스템에서는 네트워크의 호스트에 다운로드된 PDF에 악성코드 클라우드 조회를 수행합니다. 악성코드 파일 속성이 포함된 모든 PDF 파일은 차단되며, 침입 검사 대상에서 제외됩니다.
- 마지막으로, 시스템에서는 액세스 제어 규칙과 연결된 침입 정책을 사용하여 모든 나머지 트래픽을 검사하며 여기에는 파일 정책으로 차단되지 않은 파일이 포함됩니다.

참고 파일이 세션의 세션 패킷에서 탐지되고 차단될 때까지는 침입 검사 대상일 수 있습니다.

액세스 제어 규칙을 구성하여 AMP 또는 파일 제어 수행

라이센스: 보호 또는 악성코드

지원되는 디바이스: 기능에 따라 다름

지원되는 Defense Center: 기능에 따라 다름

액세스 제어 정책에는 파일 정책과 연결된 여러 액세스 제어 규칙이 포함될 수 있습니다. Allow 또는 Interactive Block 액세스 제어 규칙에 파일 검사를 구성할 수 있으며, 이는 트래픽이 최종 대상에 도달하기 전에 여러 파일 및 악성코드 검사 프로필을 네트워크에 있는 다양한 종류의 트래픽과 매칭할 수 있도록 허용합니다.

시스템에서 정책의 설정에 따라 금지된 파일(악성코드 포함)을 탐지할 경우, 이벤트를 방어 센터 데이터베이스에 자동으로 로깅합니다. 로그 파일 또는 악성코드 이벤트를 로깅하지 않으려는 경우, 액세스 제어 규칙마다 이러한 로깅을 비활성화할 수 있습니다. 파일 정책을 액세스 제어 규칙과 연결한 후에는 액세스 제어 규칙 편집기의 Logging 탭에서 **Log Files** 확인란의 선택을 취소합니다. 자세한 내용은 38-8페이지의 허용된 연결에 대한 파일 및 악성코드 이벤트 로깅 비활성화을/를 참조하십시오.

또한 시스템에서는 연결된 연결의 끝을 방어 센터 데이터베이스에 로깅하며, 이는 호출 액세스 제어 규칙의 로깅 컨피그레이션에 상관없이 이루어집니다(38-4페이지의 파일 및 악성코드 이벤트 관련 연결(자동) 참조).

파일 정책을 액세스 제어 규칙과 연결하려면

액세스: Admin/Access Admin/Network Admin

1단계 **Policies > Access Control**을 선택합니다.

Access Control Policy 페이지가 나타납니다.

2단계 액세스 제어 규칙을 사용하여 AMP 또는 파일 제어를 구성하려는 경우 액세스 제어 정책 옆의 수정 아이콘( )을 클릭합니다.

3단계 새 규칙을 생성하거나 기존 규칙을 수정하려면 14-3페이지의 액세스 제어 규칙 생성 및 수정을/를 참조하십시오.

액세스 제어 규칙 편집기가 나타납니다.

4단계 규칙 작업이 **Allow**, **Interactive Block** 또는 **Interactive Block with reset**으로 설정되었는지 확인합니다.

5단계 Inspection 탭을 선택합니다.

Inspection 탭이 나타납니다.

6단계 **File Policy**를 선택하여 액세스 제어 규칙과 매칭되는 트래픽을 검사하거나, **None**을 선택하여 매칭되는 트래픽에 대한 파일 검사를 비활성화합니다.

새 브라우저 탭에서 정책을 수정할 수 있도록 표시되는 수정 아이콘( )을 클릭할 수 있습니다 (37-16페이지의 파일 정책 생성 참조).

7단계 **Add**를 클릭하여 규칙을 저장합니다.

규칙이 저장됩니다. 변경 사항을 구현하려면 액세스 제어 정책을 저장하고 적용해야 합니다(12-15페이지의 액세스 제어 정책 적용 참조).

액세스 제어 규칙을 구성하여 침입 방지 수행

라이센스: 보호

액세스 제어 정책에는 침입 정책과 연결된 여러 액세스 제어 규칙이 포함될 수 있습니다. Allow 또는 Interactive Block 액세스 제어 규칙에 침입 검사를 구성할 수 있으며, 이는 트래픽이 최종 대상에 도달하기 전에 여러 침입 검사 프로필을 네트워크에 있는 다양한 종류의 트래픽과 매칭할 수 있도록 허용합니다.

시스템에서는 침입 정책을 사용하여 트래픽을 평가할 때마다, 연결된 *변수 집합*을 사용합니다. 한 집합의 변수는 소스 및 대상 IP 주소와 포트를 식별하기 위해 침입 규칙에서 일반적으로 사용되는 값을 나타냅니다. 또한 침입 정책의 변수를 사용하여 규칙 억제 및 동적 규칙 상태의 IP 주소를 나타낼 수도 있습니다.

팁 시스템에서 제공된 침입 정책을 사용하는 경우에도, Cisco에서는 네트워크 환경을 정확하게 반영하도록 시스템의 침입 변수를 구성할 것을 **적극** 권장합니다. 최소한 기본 집합의 기본 변수를 수정하십시오(3-18페이지의 사전 정의된 기본 변수 최적화 참조).

단일한 액세스 제어 정책에서 사용할 수 있는 고유한 침입 정책의 수는 대상 디바이스의 모델에 따라 다르며, 성능이 뛰어난 디바이스일수록 더 많은 양을 처리할 수 있습니다. 모든 고유한 침입 정책 및 변수 집합의 **쌍**은 하나의 정책으로 계산됩니다. 다른 침입 정책 변수 집합 쌍을 각 Allow 및 Interactive Block 규칙(기본 작업도 해당)과 연결할 수 있으나, 대상 디바이스가 구성에 따라 검사를 수행하는 데 필요한 리소스가 부족할 경우 액세스 제어 정책을 적용할 수 없습니다. 자세한 내용은 12-22페이지의 규칙 간소화로 성능 향상을/를 참조하십시오.

시스템에서 제공된 정책 및 사용자 지정 침입 정책 이해

Cisco에서는 FireSIGHT 시스템을 통해 몇 가지 침입 정책을 제공합니다. 시스템에서 제공된 침입 정책을 사용하여, Cisco VRT(Vulnerability Research Team)의 환경을 활용할 수 있습니다. 이러한 정책을 대상으로, VRT는 침입 정책 및 프리프로세서 규칙 상태를 설정할 뿐만 아니라 고급 설정의 초기 컨피그레이션을 제공합니다. 시스템에서 제공된 정책을 그대로 사용하거나, 이를 사용자 지정 정책의 기본으로 사용할 수 있습니다. 사용자 지정 정책을 만들면 해당 환경의 시스템 성능을 개선하고 악성 트래픽 및 네트워크에서 발생하는 정책 위반에 중점을 둔 보기를 제공할 수 있습니다.

생성하는 사용자 지정 정책 외에도 시스템에서는 두 가지 사용자 지정 정책인 Initial Inline Policy 및 Initial Passive Policy를 제공합니다. 이러한 두 가지 침입 정책에서는 Balanced Security and Connectivity Intrusion 정책을 기본으로 사용합니다. 두 정책의 유일한 차이점은 **Drop When Inline** 설정이며, 이 설정은 인라인 정책의 동작을 삭제하고 패시브 정책에서 이를 비활성화합니다. 자세한 내용은 23-7페이지의 시스템 제공 정책과 사용자 지정 정책 비교을/를 참조하십시오.

연결 및 침입 이벤트 로깅

액세스 제어 규칙에 의해 호출된 침입 정책이 침입을 탐지하고 침입 이벤트를 생성할 경우, 해당 이벤트는 방어 센터 데이터베이스에 저장됩니다. 또한 시스템에서는 침입이 발생한 연결의 끝을 방어 센터 데이터베이스에 자동으로 로깅하며, 이는 액세스 제어 규칙의 로깅 컨피그레이션에 상관없이 이루어집니다(38-3페이지의 침입 관련 연결(자동) 참조).

침입 정책을 액세스 제어 규칙과 연결하려면

액세스: Admin/Access Admin/Network Admin

1단계 **Policies > Access Control**을 선택합니다.

Access Control Policy 페이지가 나타납니다.

2단계 액세스 제어 규칙을 사용하여 침입 검사를 구성하려는 경우 액세스 제어 정책 옆의 수정 아이콘()을 클릭합니다.

3단계 새 규칙을 생성하거나 기존 규칙을 수정하려면 14-3페이지의 액세스 제어 규칙 생성 및 수정을/를 참조하십시오.

액세스 제어 규칙 편집기가 나타납니다.

4단계 규칙 작업이 **Allow**, **Interactive Block** 또는 **Interactive Block with reset**으로 설정되었는지 확인합니다.

5단계 Inspection 탭을 선택합니다.

Inspection 탭이 나타납니다.

6단계 시스템에서 제공된 또는 사용자 지정 **Intrusion Policy**를 선택하거나, **None**을 선택하여 액세스 제어 정책과 매칭되는 트래픽에 대한 침입 검사를 비활성화합니다.

사용자 지정 침입 정책을 선택할 경우, 새 브라우저 탭에서 정책을 수정할 수 있도록 표시되는 수정 아이콘()을 클릭할 수 있습니다(31-4페이지의 침입 정책 수정 참조).

주의 Cisco 담당자의 지침이 없는 한 `Experimental Policy 1`을 선택하지 **마십시오**. Cisco에서는 테스트 목적으로 이 정책을 사용합니다.

7단계 필요한 경우, 침입 정책과 연결된 **Variable Set**을 변경합니다.

새 브라우저 탭에서 변수 집합을 수정하도록 표시되는 수정 아이콘()을 클릭할 수 있습니다(3-17페이지의 변수 집합 작업 참조).

8단계 **Save**를 클릭하여 규칙을 저장합니다.

규칙이 저장됩니다. 변경 사항을 구현하려면 액세스 제어 정책을 저장하고 적용해야 합니다(12-15페이지의 액세스 제어 정책 적용 참조).

침입 방지 성능 조정

라이센스: 보호

Cisco에서는 시스템이 트래픽에 대한 침입 시도 여부를 분석할 경우 해당 시스템의 성능을 개선할 수 있는 몇 가지 기능을 제공합니다. 이러한 성능 설정은 액세스 제어 규칙마다 구성할 수 있으며, 해당 설정은 상위 액세스 제어 정책에 의해 호출된 모든 침입 정책에 적용됩니다.

자세한 내용은 다음 링크를 참고하십시오.

- 18-9페이지의 침입에 대한 패턴 매칭 제한에서는 이벤트 대기열에서 허용할 패킷의 수를 지정하는 방법과 대규모 스트림에서 다시 작성될 패킷의 검사를 활성화 또는 비활성화하는 방법에 대해 설명합니다.
- 18-10페이지의 침입 규칙에 대한 정규식 제한 재정의에서는 PCRE(Perl-compatible regular expressions: Perl 호환 정규식)에 대한 기본 매치 및 재귀 제한을 재정의하는 방법에 대해 설명합니다.

- 18-11페이지의 패킷당 생성된 침입 이벤트 제한에서는 규칙 처리 이벤트 대기열 설정을 구성하는 방법에 대해 설명합니다.
- 18-12페이지의 패킷 및 침입 규칙 레이턴시 임계값 구성에서는 디바이스 레이턴시를 적정한 수준으로 유지해야 하는 경우 패킷 및 규칙 레이턴시 임계값을 사용하여 보안의 균형을 맞추는 방법에 대해 설명합니다.
- 18-19페이지의 침입 성능 통계 로깅 구성에서는 매니지드 디바이스의 기본 성능 모니터링 및 보고 매개변수를 구성하는 방법에 대해 설명합니다.

침입에 대한 패턴 매칭 제한

라이센스: 보호

이벤트 대기열에서 허용할 패킷의 수를 지정할 수 있습니다. 또한 스트림을 재결합하기 전후에, 대규모 스트림에서 다시 작성될 패킷의 수를 활성화하거나 비활성화할 수 있습니다.

이벤트 대기열 설정을 구성하려면

액세스: Admin/Access Admin/Network Admin

1단계 **Policies > Access Control**을 선택합니다.

Access Control Policy 페이지가 나타납니다.

2단계 수정할 액세스 제어 정책 옆에 있는 수정 아이콘( )을 클릭합니다.

액세스 제어 정책 편집기가 나타납니다.

3단계 Advanced 탭을 선택합니다.

Access control policy advanced settings 페이지가 나타납니다.

4단계 **Performance Settings** 옆에 있는 수정 아이콘( )을 클릭한 다음, 표시되는 팝업 창에서 **Pattern Matching Limits** 탭을 선택합니다.

5단계 다음 옵션을 수정할 수 있습니다.

- **Maximum Pattern States to Analyze Per Packet** 필드에서 대기열에 대한 최대 이벤트 수의 값을 입력합니다.
- 스트림을 재결합하기 전후에 대규모 데이터 스트림에서 다시 작성될 패킷을 검사하려면, **Disable Content Checks on Traffic Subject to Future Reassembly**를 선택합니다. 재결합 전후에 검사를 수행할 경우 추가적인 처리 오버헤드가 증가하며 성능이 저하될 수 있습니다.
- 스트림을 재결합하기 전후에 대규모 데이터 스트림에서 다시 작성될 패킷의 검사를 비활성화하려면, **Disable Content Checks on Traffic Subject to Future Reassembly**의 선택을 취소합니다. 검사를 비활성화하면 스트림 삽입 검사를 위한 처리 오버헤드가 줄어들고 성능이 향상될 수 있습니다.

6단계 **OK**를 클릭합니다.

변경 사항을 구현하려면 액세스 제어 정책을 저장하고 적용해야 합니다(12-15페이지의 액세스 제어 정책 적용 참조).

침입 규칙에 대한 정규식 제한 재정의

라이센스: 보호

침입 규칙에 사용된 PCRE에 대한 기본 매치 및 억제 제한을 재정의하여 패킷 페이로드 콘텐츠를 검사할 수 있습니다. 침입 규칙에서 `pcre` 키워드 사용에 대한 자세한 내용은 36-35페이지의 PCRE를 사용하여 내용 검색을/를 참조하십시오. 기본 제한은 성능의 최소 수준을 보장합니다. 이러한 제한을 재정의하면 보안을 높일 수 있으나, 비효율적인 정규식에 대해 패킷 평가를 허용하므로 성능에도 큰 영향을 미칠 수 있습니다.

주의 생산성이 떨어지는 패턴이 미치는 영향에 대한 지식이 있는 숙련된 침입 규칙 작성자를 제외하고는 기본 PCRE 제한을 재정의하지 마십시오.

다음 표에는 기본 제한을 재정의하도록 구성할 수 있는 옵션이 설명되어 있습니다.

표 18-2 정규식 제한 옵션

옵션	설명
Match Limit State	**Match Limit**을 재정의할지 지정합니다. 다음 옵션을 이용할 수 있습니다. • **Default**를 선택하여 **Match Limit**에 구성된 값을 사용합니다. • **Unlimited**를 선택하여 무제한 시도 횟수를 허용합니다. • **Custom**을 선택하여 **Match Limit**의 제한값을 1 이상으로 지정하거나, 0으로 지정하여 PCRE 매치 평가를 완전히 비활성화합니다.
Match Limit	PCRE 정규식에 정의된 패턴과 매칭을 시도하는 횟수를 지정합니다.
Match Recursion Limit State	**Match Recursion Limit**을 재정의할지 지정합니다. 다음 옵션을 이용할 수 있습니다. • **Default**를 선택하여 **Match Recursion Limit**에 구성된 값을 사용합니다. • **Unlimited**를 선택하여 무제한 억제 횟수를 허용합니다. • **Custom**을 선택하여 **Match Recursion Limit**의 제한값을 1 이상으로 지정하거나, 0으로 지정하여 PCRE 억제를 완전히 비활성화합니다. **Match Recursion Limit**의 값이 유의미하려면 이는 **Match Limit**보다 작아야 합니다.
Match Recursion Limit	패킷 페이로드에 대해 PCRE 정규식을 평가할 경우 억제 횟수를 지정합니다.

PCRE 재정의를 구성하려면

액세스: Admin/Access Admin/Network Admin

1단계 **Policies > Access Control**을 선택합니다.

Access Control Policy 페이지가 나타납니다.

2단계 수정할 액세스 제어 정책 옆에 있는 수정 아이콘( )을 클릭합니다.

액세스 제어 정책 편집기가 나타납니다.

3단계 Advanced 탭을 선택합니다.

Access control policy advanced settings 페이지가 나타납니다.

4단계 **Performance Settings** 옆에 있는 수정 아이콘( )을 클릭한 다음, 표시되는 팝업 창에서 Regular Expression Limits 탭을 선택합니다.

5단계 정규식 제한 옵션 표의 옵션을 수정할 수 있습니다.

6단계 **OK**를 클릭합니다.

변경 사항을 구현하려면 액세스 제어 정책을 저장하고 적용해야 합니다(12-15페이지의 액세스 제어 정책 적용 참조).

패킷당 생성된 침입 이벤트 제한

라이센스: 보호

규칙 엔진이 규칙에 대해 트래픽을 평가할 경우, 규칙 엔진은 주어진 패킷 또는 패킷 스트림에 대해 생성된 이벤트를 이벤트 대기열에 배치한 다음, 해당 대기열의 상위 이벤트를 사용자 인터페이스에 보고합니다. 여러 이벤트가 생성된 경우 패킷 또는 패킷 스트림당 둘 이상의 이벤트를 로깅하는 규칙 엔진을 선택할 수 있습니다. 이러한 이벤트를 로깅하면 보고된 이벤트 이외의 정보를 수집할 수 있습니다. 이 옵션을 구성할 경우, 대기열에 배치할 수 있는 이벤트 수 및 로깅 수를 지정할 수 있으며, 대기열의 이벤트 순서를 결정할 조건을 선택할 수 있습니다.

다음 표에는 패킷 또는 스트림당 로깅되는 이벤트 수를 결정하도록 구성할 수 있는 옵션이 설명되어 있습니다.

표 18-3 침입 이벤트 로깅 제한 옵션

옵션	설명
Maximum Events Stored Per Packet	주어진 패킷 또는 패킷 스트림에 대해 저장할 최대 이벤트 수입니다.
Maximum Events Logged Per Packet	주어진 패킷 또는 패킷 스트림에 대해 로깅할 이벤트 수입니다. 이는 **Maximum Events Stored Per Packet** 값을 초과할 수 없습니다.
Prioritize Event Logging By	이벤트 대기열 내의 이벤트 순서 지정을 결정하는 데 사용되는 값입니다. 순서가 가장 높은 이벤트는 사용자 인터페이스를 통해 보고됩니다. 다음 중 선택할 수 있습니다. • `priority` — 이벤트 우선순위를 기준으로 대기열의 이벤트 순서를 지정합니다. • `content_length` — 식별된 콘텐츠 매치 중 가장 긴 항목을 기준으로 이벤트 순서를 지정합니다. 콘텐츠 길이로 이벤트 순서가 지정된 경우, 규칙 이벤트는 디코더 및 프리프로세서 이벤트보다 항상 우선합니다.

패킷 또는 스트림당 로깅되는 이벤트 수를 구성하려면

액세스: Admin/Access Admin/Network Admin

1단계 **Policies > Access Control**을 선택합니다.

Access Control Policy 페이지가 나타납니다.

2단계 수정할 액세스 제어 정책 옆에 있는 수정 아이콘( )을 클릭합니다.

액세스 제어 정책 편집기가 나타납니다.

3단계 Advanced 탭을 선택합니다.

Access control policy advanced settings 페이지가 나타납니다.

4단계 **Performance Settings** 옆에 있는 수정 아이콘( )을 클릭한 다음, 표시되는 팝업 창에서 **Intrusion Event Logging Limits** 탭을 선택합니다.

5단계 침입 이벤트 로깅 제한 옵션 표의 옵션을 수정할 수 있습니다.

6단계 **OK**를 클릭합니다.

변경 사항을 구현하려면 액세스 제어 정책을 저장하고 적용해야 합니다(12-15페이지의 액세스 제어 정책 적용 참조).

패킷 및 침입 규칙 레이턴시 임계값 구성

라이센스: 보호

디바이스 레이턴시를 적정한 수준으로 유지해야 하는 경우 패킷 및 규칙 레이턴시 임계값을 사용하여 보안의 균형을 맞출 수 있습니다. 자세한 내용은 다음 링크를 참고하십시오.

- 18-12페이지의 패킷 레이턴시 임계값 이해
- 18-14페이지의 패킷 레이턴시 임계값 구성
- 18-15페이지의 패킷 레이턴시 임계값을 비활성화하려면
- 18-17페이지의 규칙 레이턴시 임계값 구성

패킷 레이턴시 임계값 이해

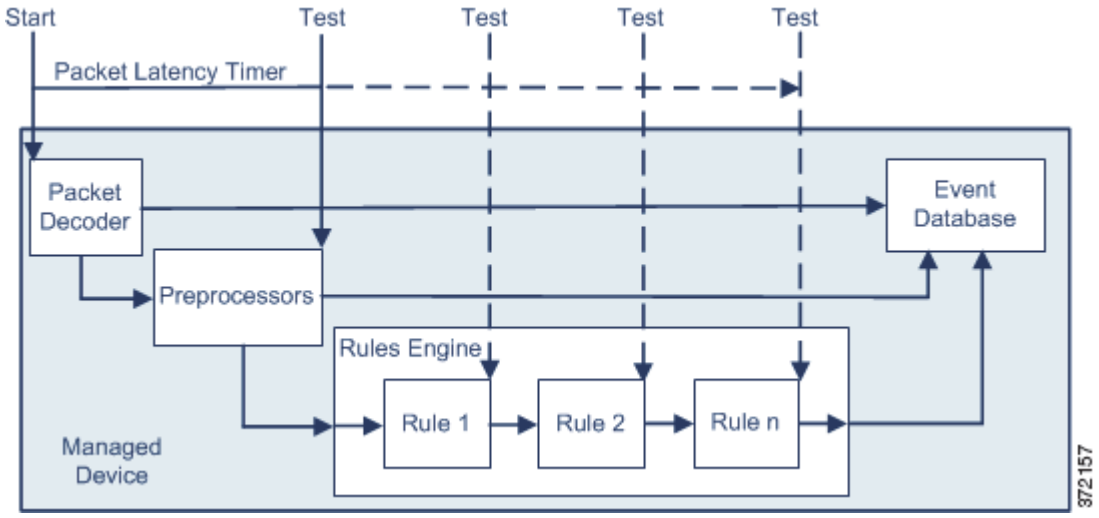
라이센스: 보호

레이턴시를 적정한 수준으로 유지해야 하는 경우 패킷 레이턴시 임계값을 사용하여 보안의 균형을 맞출 수 있습니다. 패킷 레이턴시 임계값은 해당 디코더, 프리프로세서, 규칙으로 패킷을 처리하는 데 걸린 총 경과 시간을 측정하고, 처리 시간이 구성 가능한 임계값을 초과할 경우 패킷의 검사를 중단합니다.

패킷 레이턴시 임계값은 처리 시간뿐만 아니라 소요된 시간까지 측정하여 패킷을 처리하는 규칙에 필요한 실제 시간을 더욱 정확하게 반영합니다. 그러나 레이턴시 임계값은 엄격한 타이밍을 시행하지 않는 소프트웨어 기반 레이턴시 구현입니다.

레이턴시 임계값에서 파생되는 성능 이점과 레이턴시 이점의 단점은 검사되지 않은 패킷에 공격이 포함될 수 있다는 것입니다. 그러나 패킷 레이턴시 임계값은 보안과 연결의 균형을 맞추는 데 사용할 수 있는 툴을 제공합니다.

디코더가 처리를 시작하면 각 패킷에 타이머가 시작됩니다. 타이밍은 패킷의 모든 처리가 종료되거나, 처리 시간이 타이밍 테스트 지점의 임계값을 초과할 때까지 계속됩니다.



위의 그림에 표시된 대로, 패킷 레이턴시 타이밍은 다음과 같은 테스트 지점에서 테스트됩니다.

- 모든 디코더 및 프리프로세서 처리가 완료된 이후 및 규칙 처리가 시작되기 이전
- 각 규칙에 따라 처리된 이후

처리 시간이 테스트 지점의 임계값을 초과할 경우, 패킷 검사가 중단됩니다.

팁 총 패킷 처리 시간에는 일상적인 TCP 스트림 또는 IP 프래그먼트 재결합 시간은 포함되지 않습니다.

패킷 레이턴시 임계값은 패킷을 처리하는 디코더, 프리프로세서 또는 규칙에 의해 트리거된 이벤트에 영향을 미치지 않습니다. 해당하는 모든 디코더, 프리프로세서, 규칙은 패킷이 완전히 처리될 때까지 또는 레이턴시 임계값이 초과되어 패킷 처리가 종료될 때까지 트리거되며 둘 중 더 먼저 일어난 상황이 우선합니다. 삭제 규칙이 인라인 구축의 침입을 탐지할 경우, 삭제 규칙은 이벤트를 트리거하며 해당 패킷이 삭제됩니다.

참고 패킷 레이턴시 임계값 위반으로 인해 패킷 처리가 중단된 후에는 규칙에 대해 패킷이 평가되지 않습니다. 이벤트를 트리거한 규칙은 해당 이벤트를 트리거할 수 없으며, 삭제 규칙은 패킷을 삭제할 수 없습니다.

삭제 규칙에 대한 자세한 내용은 32-20페이지의 규칙 상태 설정을/를 참조하십시오.

패킷 레이턴시 임계값을 사용하면 과도한 처리 시간이 요구되는 패킷 검사를 중단함으로써 패시브 및 인라인 구축 시 시스템 성능을 향상하고, 인라인 구축 시 레이턴시를 줄일 수 있습니다. 다음과 같은 경우 이러한 성능 이점을 누릴 수 있습니다.

- 패시브 및 인라인 구축에서 과도한 시간을 들여 여러 규칙별 패킷 검사를 순차적으로 수행하는 경우
- 인라인 구축에서 네트워크 성능이 저하된 경우(예: 누군가 대용량 파일을 다운로드하여 패킷 처리 속도가 느려짐)

패시브 구축에서 패킷의 처리를 중단한다고 해서 네트워크 성능 복구에 도움이 되는 것은 아닐 수 있습니다. 이 경우 처리 작업은 다음 패킷으로 넘어가기 때문입니다.

패킷 레이턴시 임계값 구성

라이센스: 보호

레이턴시 기반의 성능 설정은 시스템에서 제공되는 Balanced Security and Connectivity Intrusion 정책에 의해 기본적으로 활성화됩니다. 다음 표에는 패킷 레이턴시 임계값을 구성하도록 설정할 수 있는 옵션이 설명되어 있습니다.

표 18-4 패킷 레이턴시 임계값 옵션

옵션	설명
임계값(마이크로초)	패킷 검사가 중단되는 시간을 마이크로초 단위로 지정합니다. 권장 최소 임계값 설정은 최소 패킷 레이턴시 임계값 설정 표를 참조하십시오.

패킷 레이턴시 임계값이 초과하여 패킷 검사가 중단될 경우 규칙 134:3을 사용하여 이벤트를 생성할 수 있습니다. 자세한 내용은 41-9페이지의 침입 이벤트 보기 및 32-20페이지의 규칙 상태 설정을/를 참조하십시오.

CPU 속도, 데이터 속도, 패킷 크기, 프로토콜 유형 같은 다양한 요인이 시스템 성능 및 패킷 레이턴시의 측정에 영향을 미칩니다. 이러한 이유로 인해, Cisco에서는 사용자가 자체적인 계산을 통해 네트워크 환경에 맞춤화된 설정을 도출한 경우를 제외하고는 다음 표의 임계값 설정을 사용하는 것을 권장합니다.

표 18-5 최소 패킷 레이턴시 임계값 설정

데이터 속도	최소 임계값(마이크로초) 설정
1Gbps	100
100Mbps	250
5Mbps	1000

설정을 계산할 경우 다음을 확인해야 합니다.

- 초당 평균 패킷
- 패킷당 평균 마이크로초

네트워크의 패킷당 평균 마이크로초를 유효 안전 인수와 곱하여 패킷 검사를 불필요하게 중단하지 않도록 합니다.

예를 들어, 최소 패킷 레이턴시 임계값 설정 표의 권장 사항에 따르면 1기가비트 환경의 최소 패킷 레이턴시 임계값은 100마이크로초입니다. 이러한 최소 권장 사항은 초당 평균 250,000개의 패킷(마이크로초당 0.25패킷 또는 패킷당 4마이크로초)을 표시하는 테스트 데이터를 기반으로 합니다. 25개 인수를 곱한 결과 권장 최소 임계값이 100마이크로초로 계산되었습니다.

패킷 레이턴시 임계값을 구성하려면

액세스: Admin/Access Admin/Network Admin

1단계 **Policies > Access Control**을 선택합니다.

Access Control Policy 페이지가 나타납니다.

2단계 수정할 액세스 제어 정책 옆에 있는 수정 아이콘( )을 클릭합니다.

액세스 제어 정책 편집기가 나타납니다.

3단계 Advanced 탭을 선택합니다.

Access control policy advanced settings 페이지가 나타납니다.

4단계 **Latency-Based Performance Settings** 옆에 있는 수정 아이콘()을 클릭한 다음, 표시되는 팝업 창에서 Regular Expression Limits 탭을 선택합니다.

팁 기본적으로, 패킷 레이턴시 임계값은 활성화되어 있습니다. 레이턴시 임계값을 완전히 비활성화하려면 **Enable** 확인란의 선택을 취소합니다.

5단계 권장 최소 **Threshold** 설정은 최소 패킷 레이턴시 임계값 설정 표를 참조하십시오.

6단계 **OK**를 클릭합니다.

변경 사항을 구현하려면 액세스 제어 정책을 저장하고 적용해야 합니다(12-15페이지의 액세스 제어 정책 적용 참조).

패킷 레이턴시 임계값을 비활성화하려면

액세스: Admin/Access Admin/Network Admin

1단계 **Policies > Access Control**을 선택합니다.

Access Control Policy 페이지가 나타납니다.

2단계 수정할 액세스 제어 정책 옆에 있는 수정 아이콘()을 클릭합니다.

액세스 제어 정책 편집기가 나타납니다.

3단계 Advanced 탭을 선택합니다.

Access control policy advanced settings 페이지가 나타납니다.

4단계 **Latency-Based Performance Settings** 옆에 있는 수정 아이콘()을 클릭한 다음, 표시되는 팝업 창에서 Regular Expression Limits 탭을 선택합니다.

5단계 권장 최소 **Threshold** 설정은 최소 패킷 레이턴시 임계값 설정 표를 참조하십시오.

6단계 **OK**를 클릭합니다.

변경 사항을 구현하려면 액세스 제어 정책을 저장하고 적용해야 합니다(12-15페이지의 액세스 제어 정책 적용 참조).

규칙 레이턴시 임계값 이해

라이센스: 보호

레이턴시를 적정한 수준으로 유지해야 하는 경우 규칙 레이턴시 임계값을 사용하여 보안의 균형을 맞출 수 있습니다. 규칙 레이턴시 임계값은 각 규칙에서 개별 패킷을 처리하는 데 걸리는 시간을 측정하고, 처리 시간이 규칙 레이턴시 임계값(구성 가능한 연속 횟수)을 넘을 경우 위반 규칙 및 지정된 시간에 대한 관련 규칙 그룹을 동시에 중단하며, 일시 중단이 만료되면 해당 규칙을 복원합니다.

규칙 레이턴시 임계값은 처리 시간뿐만 아니라 소요된 시간까지 측정하여 패킷을 처리하는 규칙에 필요한 실제 시간을 더욱 정확하게 반영합니다. 그러나 레이턴시 임계값은 엄격한 타이밍을 시행하지 않는 소프트웨어 기반 레이턴시 구현입니다.

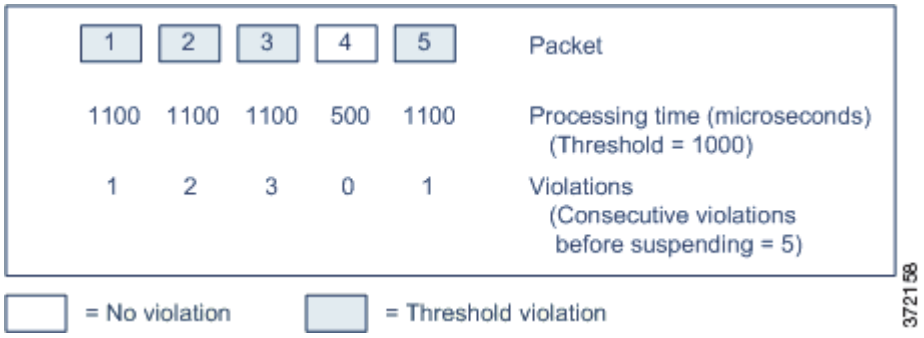
레이턴시 임계값에서 파생되는 성능 이점과 레이턴시 이점의 단점은 검사되지 않은 패킷에 공격이 포함될 수 있다는 것입니다. 그러나 규칙 레이턴시 임계값은 보안과 연결의 균형을 맞추는 데 사용할 수 있는 툴을 제공합니다.

타이머는 규칙 그룹에 의해 패킷이 처리될 때마다 처리 시간을 측정합니다. 규칙 처리 시간이 지정된 규칙 레이턴시 임계값을 초과할 경우, 시스템에서는 카운터를 늘립니다. 연속 임계값 위반이 지정된 횟수에 도달할 경우, 시스템에서는 다음과 같은 조치를 취합니다.

- 지정된 기간 동안 규칙 중단
- 규칙이 중단되었음을 나타내는 이벤트 트리거
- 중단 만료 시 규칙 다시 활성화
- 규칙이 다시 활성화되었음을 나타내는 이벤트 트리거

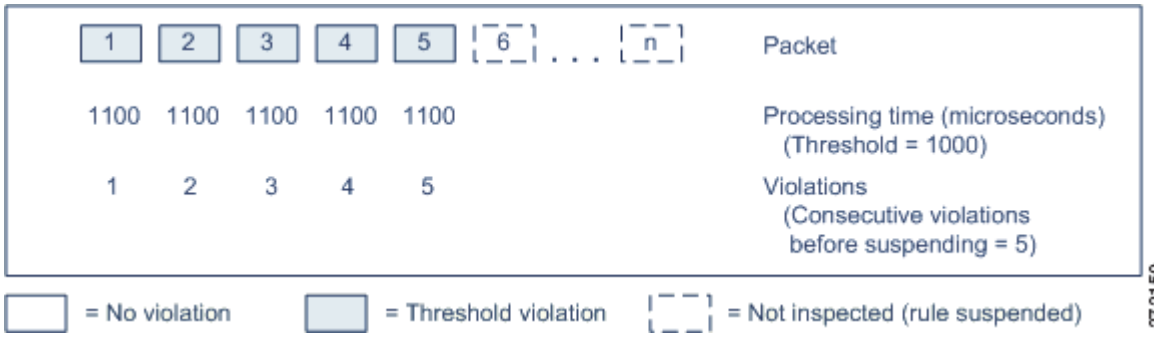
시스템은 규칙 그룹이 중단되거나 규칙 위반이 연속적이지 않은 경우, 카운터를 0으로 돌립니다. 규칙을 중단하기 전에 연속 위반을 일부 허용할 경우, 성능에 거의 영향을 미치지 않는 우발적인 규칙 위반은 무시하고, 그 대신 규칙 레이턴시 임계값을 반복적으로 초과하는 규칙이 미치는 중요한 영향을 중점적으로 살펴볼 수 있습니다.

다음 예에서는 규칙 중단을 유발하지 않는 다섯 번의 연속 규칙의 처리 시간이 나와 있습니다.



위의 예에서 처음 세 개의 각 패킷을 처리하는 데 필요한 시간은 규칙 레이턴시 임계값 1000마이크로초를 위반하며, 위반이 발생할 때마다 위반 카운터는 증가합니다. 네 번째 패킷의 처리 시간은 임계값을 위반하지 않으며, 위반 카운터는 0으로 재설정됩니다. 다섯 번째 패킷은 임계값을 위반하며 위반 카운터가 한 번 재설정됩니다.

다음 예에서는 규칙 중단을 유발하는 다섯 번의 연속 규칙의 처리 시간이 나와 있습니다.



두 번째 예에서, 다섯 개의 각 패킷을 처리하는 데 필요한 시간은 규칙 레이턴시 임계값 1000초를 위반합니다. 각 패킷의 규칙 처리 시간이 1100마이크로초이며 이는 지정된 다섯 번의 연속 위반에 대한 임계값인 1000마이크로초를 위반하므로, 규칙 그룹이 중단됩니다. 그림에 6부터 n까지의 패킷으로 표시된 모든 후속 패킷은 중단이 만료될 때까지 중단된 규칙에 대해 검사되지 않습니다. 규칙이 다시 활성화된 후 추가 패킷이 발생할 경우, 위반 카운터는 0부터 다시 시작됩니다.

규칙 레이턴시 임계값은 패킷을 처리하는 규칙에 의해 트리거된 침입 이벤트에 영향을 미치지 않습니다. 규칙은 규칙 처리 시간이 임계값을 초과하는지 여부에 상관없이, 패킷에서 탐지된 모든 침입에 대해 이벤트를 트리거합니다. 규칙에서 탐지한 침입이 인라인 구축의 삭제 규칙인 경우, 패킷이 삭제됩니다. 삭제 규칙이 규칙 중단을 유발하는 침입을 패킷에서 탐지할 경우 삭제 규칙은 침입 이벤트를 트리거하고, 패킷이 삭제되며, 해당 규칙 및 모든 관련 규칙이 중단됩니다. 삭제 규칙에 대한 자세한 내용은 32-20페이지의 규칙 상태 설정을/를 참조하십시오.

참고 패킷은 중단된 규칙에 대해 평가되지 않습니다. 이벤트를 트리거한 중단된 규칙은 해당 이벤트를 트리거할 수 없으며, 삭제 규칙은 패킷을 삭제할 수 없습니다.

규칙 레이턴시 임계값은 패시브 구축 및 인라인 구축에서 모두 시스템 성능을 향상할 수 있으며, 패킷 처리 시 대부분의 시간이 소요되는 규칙을 중단하여 인라인 구축의 레이턴시를 줄일 수 있습니다. 구성 가능한 시간이 만료될 때까지 패킷은 중단된 규칙에 대해 다시 평가되지 않으므로, 복구할 수 있는 오버로드된 디바이스 시간이 제공됩니다. 다음과 같은 경우 이러한 성능 이점을 누릴 수 있습니다.

- 급하게 작성된 대부분의 테스트되지 않은 규칙은 처리 시간이 매우 오래 걸림
- 네트워크 성능이 저하된 동안(예: 다른 사용자가 너무 큰 파일을 다운로드하는 경우)에는 패킷 검사 속도가 느려짐

규칙 레이턴시 임계값 구성

라이센스: 보호

규칙 레이턴시 임계값, 중단된 규칙에 대한 중단 시간, 규칙을 중단하기 전에 발생해야 하는 연속 임계값 위반의 횟수를 수정할 수 있습니다.

시간 규칙이 패킷을 처리하는 시간이 **Consecutive Threshold Violations Before Suspending Rule**에 의해 지정된 연속 시간 횟수의 **Threshold**를 초과할 경우, **Suspension Time**에 의해 지정된 시간의 규칙 레이턴시 임계값이 규칙을 중단합니다.

규칙이 중단된 경우 규칙 134:1을 사용하여 이벤트를 생성할 수 있으며, 중단된 규칙이 활성화된 경우 규칙 134:2를 사용하여 이벤트를 생성할 수 있습니다. 자세한 내용은 41-9페이지의 침입 이벤트 보기 및 32-20페이지의 규칙 상태 설정을/를 참조하십시오.

다음 표에는 규칙 레이턴시 임계값을 구성하도록 설정할 수 있는 옵션이 설명되어 있습니다.

표 18-6 규칙 레이턴시 임계값 옵션

옵션	설명
Threshold	패킷 검사 시 규칙이 초과해서는 안 되는 시간을 마이크로초 단위로 지정합니다. 권장 최소 임계값 설정은 최소 규칙 레이턴시 임계값 설정 표를 참조하십시오.
Consecutive Threshold Violations Before Suspending Rule	**Threshold**에 대해 지정된 시간보다 오래 소요될 수 있는 연속 시간 횟수를 지정하여 규칙이 중단되기 전에 패킷을 검사할 수 있도록 합니다.
Suspension Time	규칙 그룹을 몇 초 동안 중단할지 지정합니다.

CPU 속도, 데이터 속도, 패킷 크기, 프로토콜 유형 같은 다양한 요인이 시스템 성능의 측정에 영향을 미칩니다. 이러한 이유로 인해, Cisco에서는 사용자가 자체적인 계산을 통해 네트워크 환경에 맞춤화된 설정을 도출한 경우를 제외하고는 다음 표의 임계값 설정을 사용하는 것을 권장합니다.

표 18-7 최소 규칙 레이턴시 임계값 설정

데이터 속도	최소 임계값(마이크로초) 설정
1Gbps	500
100Mbps	1250
5Mbps	5000

설정을 계산할 경우 다음을 확인해야 합니다.

- 초당 평균 패킷
- 패킷당 평균 마이크로초

네트워크의 패킷당 평균 마이크로초를 유효 안전 인수와 곱하여 규칙을 불필요하게 중단하지 않도록 합니다.

규칙 레이턴시 임계값을 구성하려면

액세스: Admin/Access Admin/Network Admin

1단계 **Policies > Access Control**을 선택합니다.

Access Control Policy 페이지가 나타납니다.

2단계 수정할 액세스 제어 정책 옆에 있는 수정 아이콘( )을 클릭합니다.

액세스 제어 정책 편집기가 나타납니다.

3단계 Advanced 탭을 선택합니다.

Access control policy advanced settings 페이지가 나타납니다.

4단계 **Latency-Based Performance Settings** 옆에 있는 수정 아이콘( )을 클릭한 다음, 표시되는 팝업 창에서 Rule Handling 탭을 선택합니다.

5단계 규칙 레이턴시 임계값 옵션 표의 옵션을 구성할 수 있습니다.

권장 최소 **Threshold** 설정은 최소 규칙 레이턴시 임계값 설정 표를 참조하십시오.

6단계 **OK**를 클릭합니다.

변경 사항을 구현하려면 액세스 제어 정책을 저장하고 적용해야 합니다(12-15페이지의 액세스 제어 정책 적용 참조).

침입 성능 통계 로깅 구성

라이센스: 보호

디바이스를 모니터링하고 자체 성능을 보고하는 방법에 대한 기본 매개변수를 구성할 수 있습니다. 이렇게 하면 다음 옵션을 구성하여 시스템에서 디바이스의 성능 통계를 업데이트하는 간격을 지정할 수 있습니다.

샘플 시간(초) 및 최소 패킷 수

지정된 수치(초)가 성능 통계 업데이트 간격을 경과할 경우, 시스템에서는 지정된 패킷 수를 분석했는지 확인합니다. 분석한 경우, 시스템에서는 성능 통계를 업데이트합니다. 그렇지 않을 경우 시스템에서는 지정된 패킷 수가 분석될 때까지 기다립니다.

문제 해결 옵션: 로그 세션/프로토콜 배포

지원 팀에서는 문제 해결 통화 도중 프로토콜 배포, 패킷 길이, 포트 통계를 로깅해달라고 요청할 수 있습니다.

주의 이러한 문제 해결 옵션에 대한 설정 변경은 성능에 영향을 미치므로 지원 안내에 따라서만 수행해야 합니다.

문제 해결 옵션: 요약

문제 해결 통화 중에 지원 팀에서 Snort® 프로세스가 종료되고 다시 시작된 경우에만 성능 통계를 계산하도록 시스템을 구성하라고 요청할 수 있습니다. 이 옵션을 활성화하려면 **Log Session/Protocol Distribution** 문제 해결 옵션도 활성화해야 합니다.

주의 이러한 문제 해결 옵션에 대한 설정 변경은 성능에 영향을 미치므로 지원 안내에 따라서만 수행해야 합니다.

기본 성능 통계 매개변수를 구성하려면

액세스: Admin/Access Admin/Network Admin

1단계 **Policies > Access Control**을 선택합니다.

Access Control Policy 페이지가 나타납니다.

2단계 수정할 액세스 제어 정책 옆에 있는 수정 아이콘( )을 클릭합니다.

액세스 제어 정책 편집기가 나타납니다.

3단계 Advanced 탭을 선택합니다.

Access control policy advanced settings 페이지가 나타납니다.

4단계 **Performance Settings** 옆에 있는 수정 아이콘( )을 클릭한 다음, 표시되는 팝업 창에서 Performance Statistics 탭을 선택합니다.

5단계 **Sample time** 또는 **Minimum number of packets**를 위에 설명된 대로 수정합니다.

6단계 선택에 따라, 지원 팀에서 요청한 경우에 한하여 **Troubleshoot Options** 섹션을 확장하고 이러한 옵션을 수정할 수 있습니다.

7단계 **OK**를 클릭합니다.

변경 사항을 구현하려면 액세스 제어 정책을 저장하고 적용해야 합니다(12-15페이지의 액세스 제어 정책 적용 참조).

파일 및 악성코드 검사 성능과 저장 조정

라이센스: 보호 또는 악성코드

지원되는 디바이스: 기능에 따라 다름

지원되는 Defense Center: 기능에 따라 다름

파일 정책을 사용하여 파일 제어, 파일 저장, 동적 분석, 악성코드 탐지 또는 차단을 수행할 경우 다음 표에 나열된 옵션을 설정할 수 있습니다. 파일 크기를 늘리면 시스템의 성능에 영향을 미칠 수 있습니다.

표 18-8 고급 액세스 제어 파일 및 악성코드 탐지 옵션

필드	설명	기본값	범위	참고
Limit the number of bytes inspected when doing file type detection	파일 유형 탐지를 수행할 경우 검사되는 바이트 수를 지정합니다.	1460바이트 또는 TCP 패킷의 최대 세그먼트 크기	0 - 4294967295 (4GB)	제한을 없애려면 0으로 설정합니다. 대부분의 경우, 시스템에서는 첫 번째 패킷을 사용하여 일반적인 파일 유형을 식별할 수 있습니다.
Do not calculate SHA-256 hash values for files larger than (in bytes)	파일에 대해 종합 보안 인텔리전스 클라우드 조회를 수행하거나, 사용자 지정 탐지 목록에 추가된 파일을 차단하여 특정 크기보다 큰 파일이 시스템에 저장되지 않도록 합니다.	10485760(10MB)	0 - 4294967295 (4GB)	제한을 없애려면 0으로 설정합니다. 이 값은 **Maximum file size to store (bytes)** 및 **Maximum file size for dynamic analysis testing (bytes)**보다 크거나 같아야 합니다.
Allow file if cloud lookup for Block Malware takes longer than (seconds)	악성코드 클라우드 조회가 이루어지는 동안, **Block Malware** 규칙과 매칭되고 캐싱된 속성이 없는 파일의 마지막 바이트를 얼마 동안 보유할지 지정합니다. 시스템이 속성을 갖기 전에 이 시간이 경과될 경우, 파일이 통과됩니다. Dispositions of Unavailable are not cached.	2초	0 - 30초	이 옵션에서 허용되는 값은 최대 30초까지이며, Cisco에서는 연결 오류로 인해 트래픽이 차단되는 것을 방지하기 위해 기본값을 사용하는 것을 권장합니다. 지원 팀에 문의하지 않은 경우 이 옵션을 0으로 설정하지 **마십시오**.
Minimum file size to store (bytes)	파일 규칙을 사용하여 시스템에 저장할 수 있는 최소 파일 크기를 지정합니다.	6144(6KB)	0 - 10485760 (10MB)	파일 저장을 비활성화하려면 0으로 설정합니다. 이 필드는 **Maximum file size to store (bytes)** 및 **Do not calculate SHA-256 hash values for files larger than (in bytes)**보다 작거나 같아야 합니다.

표 18-8 고급 액세스 제어 파일 및 악성코드 탐지 옵션(계속)

필드	설명	기본값	범위	참고
Maximum file size to store (bytes)	파일 규칙을 사용하여 시스템에 저장할 수 있는 최대 파일 크기를 지정합니다.	1048576(1MB)	0 - 10485760 (10MB)	파일 저장을 비활성화하려면 0으로 설정합니다. 이 필드는 **Minimum file size to store (bytes)**보다 크거나 같아야 하고, **Do not calculate SHA-256 hash values for files larger than (in bytes)**보다 작거나 같아야 합니다.
Minimum file size for dynamic analysis testing (bytes)	동적 분석을 위해 시스템이 클라우드에 제출할 수 있는 최소 파일 크기를 지정합니다.	6144(6KB)	6144(6KB) - 2097152(2MB)	이 필드는 **Maximum file size for dynamic analysis testing (bytes)** 및 **Do not calculate SHA-256 hash values for files larger than (in bytes)** 보다 작거나 같아야 합니다. 시스템은 제출할 수 있는 최소 파일 크기에 대한 업데이트를 클라우드에서 확인합니다(하루에 한 번만 수행). 새로운 최소 크기가 현재 값보다 큰 경우, 현재 값이 새 최소값으로 업데이트되며 해당 정책은 기한이 지난 것으로 표시됩니다.
Maximum file size for dynamic analysis testing (bytes)	동적 분석을 위해 시스템이 클라우드에 제출할 수 있는 최대 파일 크기를 지정합니다.	1048576(1MB)	6144(6KB) -2097152(2MB)	이 필드는 **Minimum file size for dynamic analysis testing (bytes)**보다 크거나 같아야 하고, **Do not calculate SHA-256 hash values for files larger than (in bytes)**보다 작거나 같아야 합니다. 시스템은 제출할 수 있는 최대 파일 크기에 대한 업데이트를 클라우드에서 확인합니다(하루에 한 번만 수행). 새로운 최대 크기가 현재 값보다 큰 경우, 현재 값이 새 최대값으로 업데이트되며 해당 정책은 기한이 지난 것으로 표시됩니다.

악성코드 라이센스를 DC500에 사용할 수 없고 Series 2 디바이스 또는 Cisco NGIPS for Blue Coat X-Series에 대한 악성코드 라이센스도 활성화할 수 없으므로 이러한 어플라이언스를 사용하여 개별 파일을 캡처, 저장, 차단하거나, 동적 분석을 위해 파일을 제출하거나, 악성코드 클라우드 조회를 시행할 파일의 파일 전파 흔적 분석을 볼 수 없습니다.

파일 및 악성코드 검사 성능 및 저장을 구성하려면

액세스: Admin/Access Admin/Network Admin

1단계 **Policies > Access Control**을 선택합니다.

Access Control Policy 페이지가 나타납니다.

2단계 수정할 액세스 제어 정책 옆에 있는 수정 아이콘( )을 클릭합니다.

액세스 제어 정책 편집기가 나타납니다.

3단계 Advanced 탭을 선택합니다.

Access control policy advanced settings 페이지가 나타납니다.

4단계 **Files and Malware Settings** 옆의 수정 아이콘( )을 클릭합니다.

Files and Malware Settings 팝업 창이 표시됩니다.

5단계 고급 액세스 제어 파일 및 악성코드 탐지 옵션 표의 옵션을 설정할 수 있습니다.

6단계 **OK**를 클릭합니다.

변경 사항을 구현하려면 액세스 제어 정책을 저장하고 적용해야 합니다(12-15페이지의 액세스 제어 정책 적용 참조).

19장

트래픽 해독 이해

기본적으로 시스템은 SSL(Secure Socket Layer) 또는 TLS(Transport Layer Security) 프로토콜로 암호화된 트래픽을 검사할 수 없습니다. 액세스 제어의 일부로 *SSL 검사* 기능을 사용하면 암호화된 트래픽을 검사 없이 차단하거나, 암호화된 또는 해독된 트래픽을 액세스 제어로 검사할 수 있습니다. 시스템은 암호화된 세션을 다룰 때 트래픽에 대한 세부사항을 로깅합니다. 암호화된 트래픽의 검사 및 암호화된 세션 데이터의 분석을 결합하면 네트워크에서 암호화된 애플리케이션과 트래픽을 더 잘 인식하고 제어할 수 있습니다.

시스템은 TCP 연결을 통해 SSL 또는 TLS 핸드셰이크를 탐지하는 경우 탐지된 트래픽의 해독 가능 여부를 확인합니다. 확인할 수 없는 경우 구성된 작업을 적용합니다.

- 암호화된 트래픽을 차단하고 선택적으로 TCP 연결 재설정
- 암호화된 트래픽을 해독하지 않음

SSL 검사 컨피그레이션에서 통과를 허용하는 경우 또는 SSL 검사를 구성하지 않은 경우, 액세스 제어 규칙이 암호화된 트래픽을 처리합니다. 그러나 일부 액세스 제어 규칙 조건에는 암호화되지 않은 트래픽이 필요하므로, 암호화된 트래픽과 일치하는 규칙이 더 적을 수 있습니다. 또한 기본적으로 시스템은 암호화된 페이로드의 침입 및 파일 검사를 비활성화합니다. 이는 암호화 연결이 침입 및 파일 검사가 구성된 액세스 제어 규칙과 일치하는 경우 오탐을 줄이고 성능을 높이는 데 도움이 됩니다. 자세한 내용은 14-3페이지의 액세스 제어 규칙 생성 및 수정 및 27-70페이지의 SSL 프리프로세서 사용을/를 참조하십시오.

트래픽을 해독할 수 있는 경우 시스템은 추가 검사 없이 트래픽을 차단하거나, 해독되지 않은 트래픽을 액세스 제어로 평가하거나, 다음 방법 중 하나를 사용하여 트래픽을 해독합니다.

- 알려진 개인 키로 해독합니다. 외부 호스트가 네트워크의 서버로 SSL 핸드셰이크를 시작하면 시스템은 교환된 서버 인증서를 전에 어플라이언스에 업로드한 서버 인증서에 매칭합니다. 그런 다음 업로드된 개인 키를 사용하여 트래픽을 해독합니다.
- 서버 인증서를 다시 서명하여 해독합니다. 네트워크의 호스트가 외부 서버와의 SSL 핸드셰이크를 시작하면 시스템은 교환된 서버 인증서를 전에 업로드된 CA(인증 기관) 인증서로 다시 서명합니다. 그런 다음 업로드된 개인 키를 사용하여 트래픽을 해독합니다.

해독된 트래픽에는 원래 암호화되지 않은 트래픽과 동일한 트래픽 처리 및 분석(네트워크, 평판, 사용자 기반 액세스 제어, 침입 탐지와 방지, AMP, 검색 등)이 적용됩니다. 시스템은 해독된 트래픽 사후 분석을 차단하지 않는 경우, 목적지 호스트로 전달하기 전 트래픽을 다시 암호화합니다.

참고 트래픽 차단 및 발신 트래픽 해독 등 특정 SSL 검사 작업은 트래픽 플로우를 수정합니다. 인라인으로 구축한 디바이스는 이러한 작업을 수행할 수 있습니다. 패시브 방식으로 또는 탭 모드에서 구축한 디바이스는 트래픽 플로우에 영향을 미칠 수 없습니다. 그러나 이러한 디바이스는 여전히 수신 트래픽을 해독할 수 있습니다. 자세한 내용은 19-5페이지의 예: 패시브 구축에서 트래픽 해독을/를 참조하십시오.

자세한 내용은 다음 절을 참조하십시오.

- 19-2페이지의 SSL 검사 요구 사항
- 19-5페이지의 SSL 검사 어플라이언스 구축 분석

SSL 검사 요구 사항

라이센스: 기능에 따라 다름

지원되는 디바이스: Series 3

특정 어플라이언스 모델만 SSL 검사를 지원합니다. 컨피그레이션 설정 및 라이센스 외에 네트워크에 어플라이언스를 구축하는 방법은 암호화된 트래픽을 제어하고 해독하기 위해 수행할 수 있는 작업에 영향을 미칩니다.

SSL 검사를 구성하기 위해 사용할 수 있는 기능과 작업은 사용자 역할에 따라 다릅니다. 시스템에는 다양한 관리자 및 분석가를 위해 설계된 사전 정의된 사용자 역할이 포함되며, 특수 액세스 권한을 가진 사용자 지정 사용자 역할을 만들 수 있습니다.

SSL 검사를 수행하려면 공개 키 인증서 및 특정 기능을 위한 페어링된 개인 키가 필요합니다. 암호화 세션 특성을 기반으로 트래픽을 해독 및 제어하려면 인증서 및 페어링된 개인 키를 방어 센터에 업로드해야 합니다.

자세한 내용은 다음 절을 참조하십시오.

- 19-2페이지의 SSL 검사를 지원하는 어플라이언스 구축
- 19-3페이지의 SSL 검사에 필요한 라이센스 확인
- 19-3페이지의 사용자 지정 사용자 역할로 SSL 검사 구축 관리
- 19-4페이지의 SSL 규칙 구성을 위한 필수 정보 수집

SSL 검사를 지원하는 어플라이언스 구축

라이센스: 모두

지원되는 디바이스: Series 3

SSL 검사에는 Series 3 디바이스가 필요합니다.

인라인, 라우티드, 스위치드 또는 하이브리드 인터페이스로 구성 및 구축한 디바이스는 트래픽 플로우를 수정할 수 있습니다. 이러한 디바이스는 수신 및 발신 트래픽을 모니터링, 차단, 허용 및 해독할 수 있습니다.

패시브 또는 인라인(탭 모드) 인터페이스로 구성 및 구축한 디바이스는 트래픽 플로우에 영향을 미칠 수 없습니다. 이러한 디바이스는 수신 트래픽을 모니터링, 허용 및 해독할 수 있을 뿐입니다. 패시브 구축은 DHE(ephemeral Diffie-Hellman) 또는 ECDHE(elliptic curve Diffie-Hellman) 암호화 솔루션으로 암호화된 트래픽의 해독을 지원하지 않습니다.

조직에 어떤 구축 유형이 더 적합한지 알아보려면 매핑된 작업 목록, 기존의 네트워크 구축 및 전반적인 요구 사항을 검토하십시오. 자세한 내용은 19-5페이지의 SSL 검사 어플라이언스 구축 분석을/를 참조하십시오.

SSL 검사에 필요한 라이센스 확인

라이센스: 기능에 따라 다름

라이센스에 따라, 암호화된 트래픽을 처리하는 방법을 결정하기 위한 기준의 조합을 사용할 수 있습니다. 방어 센터에서는 라이센스와 상관없이 SSL 정책을 생성할 수 있지만, 정책을 적용하려면 먼저 SSL 검사의 일부 요소의 경우 대상 디바이스에서 특정 라이센스 기능을 활성화해야 합니다. 구축에서 지원되지 않는 기능을 나타내기 위해 방어 센터는 경고 아이콘(⚠) 및 확인 대화 상자를 사용합니다. 자세한 내용은 경고 아이콘 위에 포인터를 두면 확인할 수 있습니다.

액세스 제어 정책의 일부로서 관리되는 디바이스에 SSL 정책을 적용하게 되며, 액세스 제어 정책은 SSL 정책으로 해독된 트래픽을 검사합니다. 액세스 제어 라이센싱에 대한 자세한 내용은 12-2 페이지의 액세스 제어 라이센스 및 역할 요구 사항을/를 참조하십시오.

다음 표에서는 액세스 제어 정책의 일부로서 SSL 정책을 적용하기 위한 라이센스 권장 사항에 대해 설명합니다.

표 19-1 SSL 검사를 위한 라이센스 및 모델 요구 사항

SSL 정책 적용을 위해 수행할 작업	라이센스	지원되는 방어 센터	지원되는 장치
영역, 네트워크, VLAN, 포트 또는 SSL 관련 기준을 기반으로 암호화된 트래픽 처리	모두	모두	Series 3
지오로케이션 데이터를 사용하여 암호화된 트래픽 처리	FireSIGHT	DC500을 제외한 모든 방어 센터	Series 3
애플리케이션 또는 사용자 기준을 사용하여 암호화된 트래픽 처리	제어	모두, DC500은 사용자 제어를 수행할 수 없으므로 제외	Series 3
URL 카테고리 및 평판 데이터를 사용하여 암호화된 트래픽 필터링	URL 필터링	DC500을 제외한 모두	Series 3

사용자 지정 사용자 역할로 SSL 검사 구축 관리

라이센스: 모두

61-51페이지의 사용자 지정 사용자 역할 관리에 설명된 대로, 특수 액세스 권한을 가진 사용자 지정 사용자 역할을 만들 수 있습니다. 사용자 지정 사용자 역할은 어떠한 메뉴 기반 및 시스템 권한도 가질 수 있으며 원래 역할을 그대로 유지하거나 사전 정의된 사용자 역할을 기반으로 하여 변경할 수 있습니다. 다음 표에서는 SSL 검사를 구성 및 구축할 사용자 권한을 결정하는 역할 권한에 대해 설명합니다.

표 19-2 SSL 검사 관련 사용자 역할 권한

사용자 권한	설명
Object Manager	SSL 검사와 관련된 객체를 생성, 수정 및 삭제할 수 있습니다.
SSL	SSL 정책에 대한 보고서를 생성하고 SSL 정책 또는 정책 개정을 비교할 수 있습니다.
Modify SSL Policy	SSL 정책을 볼 수 있고 생성, 수정 및 삭제할 수 있으며 Administrator Rules 또는 Root Rules 카테고리에 속하지 않은 SSL 규칙을 생성, 수정 및 삭제할 수 있습니다.

표 19-2 SSL 검사 관련 사용자 역할 권한(계속)

사용자 권한	설명
Modify Administrator Rules	Administrator Rules 카테고리에서 SSL 규칙을 생성, 수정 및 삭제할 수 있습니다.
Modify Root Rules	Root Rules 카테고리에서 SSL 규칙을 생성, 수정 및 삭제할 수 있습니다.
Apply SSL Policy	관련된 액세스 제어 정책을 적용할 경우 SSL 정책을 적용할 수 있습니다.
ACL(Access Control List)	액세스 제어 정책의 목록을 볼 수 있습니다.
Modify Access Control Policy	SSL 정책을 액세스 제어 정책과 연결할 수 있습니다.
Apply Access Control Policies	SSL 정책과 관련된 액세스 제어 정책을 적용할 수 있습니다.

자세한 내용은 12-2페이지의 액세스 제어 라이센스 및 역할 요구 사항을/를 참조하십시오.

SSL 규칙 구성을 위한 필수 정보 수집

라이센스: 기능에 따라 다름

SSL 검사는 상당량의 PKI 정보 지원에 의존합니다. 구성할 수 있는 매칭 규칙 조건을 결정하려면 조직의 트래픽 패턴을 고려하십시오. 다음 표에 나열된 정보를 수집해야 합니다.

표 19-3 SSL 규칙 조건 전제 조건

매칭할 내용	수집할 항목
자체 서명 서버 인증서를 비롯한 탐지된 서버 인증서	서버 인증서
신뢰받는 서버 인증서	CA 인증서
탐지된 서버 인증서 subject 또는 issuer	서버 인증서 subject DN 또는 issuer DN

자세한 내용은 22-1페이지의 SSL 규칙을 사용하여 트래픽 해독 조정을/를 참조하십시오.

규칙을 매칭할 암호화된 트래픽에 대한 해독, 차단, 모니터링 여부를 결정하고, 이러한 결정 사항을 SSL 규칙 작업, 해독할 수 없는 트래픽 작업 및 SSL 정책 기본 작업에 매핑하십시오. 트래픽을 해독하려면 다음 표를 참조하십시오.

표 19-4 SSL 해독 전제 조건

해독할 내용	수집
제어하는 서버에 대한 수신 트래픽	서버의 인증서 파일 및 페어링된 개인 키 파일
외부 서버에 대한 발신 트래픽	CA 인증서 파일 및 페어링된 개인 키 파일 또한 CA 인증서 및 개인 키를 생성할 수 있습니다.

자세한 내용은 21-8페이지의 규칙 작업을 사용하여 암호화 트래픽 처리 및 조사 결정을/를 참조하십시오.

이 정보를 수집한 후에는 시스템에 업로드하고 재사용 가능한 객체를 구성하십시오. 자세한 내용은 3-1페이지의 재사용 가능 객체 관리을/를 참조하십시오.

SSL 검사 어플라이언스 구축 분석

라이센스: 기능에 따라 다름

지원되는 디바이스: Series 3

이 절에서는 Life Insurance Example, Inc. 생명보험사(LifeIns)가 프로세스 감사를 위해 암호화된 트래픽에서 SSL 검사를 사용하는 몇 가지 시나리오를 보여줍니다. LifeIns는 비즈니스 프로세스를 기반으로 다음을 구축할 계획입니다.

- Customer Service 부서를 위한 패시브 구축의 Series 3 관리되는 디바이스 하나
- Underwriting 부서를 위한 인라인 구축의 Series 3 관리되는 디바이스 하나
- 두 디바이스를 관리하기 위한 방어 센터 하나

Customer Service 비즈니스 프로세스

LifeIns는 고객을 위해 고객 대면 웹사이트를 생성했습니다. LifeIns는 웹사이트와 이메일을 통해 잠재 고객으로부터 보험 증권에 대한 암호화된 질문과 요청을 수신합니다. LifeIns의 Customer Service 부서는 24시간 내에 이를 처리하고 필요한 정보를 제공합니다. Customer Service는 수신 연락처 메트릭 수집을 확장하고자 합니다. LifeIns에는 Customer Service에 대해 설정된 내부 감사 검토가 있습니다.

LifeIns는 또한 온라인으로 암호화된 신청서를 수신합니다. Customer Service 부서는 사례 파일을 Underwriting 부서로 전송하기 전 24시간 내에 신청서를 처리합니다. Customer Service는 온라인 양식으로 전송된, 명백하게 잘못된 신청서를 필터링하며, 이 과정에 상당한 시간이 소요됩니다.

Underwriting 비즈니스 프로세스

LifeIns의 보험업자는 암호화된 의료 정보 요청을 Medical Repository Example, LLC 의료 데이터 저장소(MedRepo)에 온라인으로 제출합니다. MedRepo는 요청을 검토하고, 72시간 내에 암호화된 레코드를 LifeIns로 전송합니다. 그 후 보험업자는 신청서에 서명하고 보험 증권 및 요금 결정 사항을 제출합니다. Underwriting은 메트릭 수집을 확장하고자 합니다.

최근에 알 수 없는 소스에서 LifeIns에 스푸핑된 응답을 전송했습니다. LifeIns의 보험업자는 올바른 인터넷 사용에 대한 교육을 받았지만, LifeIns의 IT 부서는 의료 응답 양식을 전송하는 모든 암호화된 트래픽을 분석하고 모든 스푸핑 시도를 차단하고자 합니다.

LifeIns는 6개월 훈련 기간을 거쳐 하급 보험업자를 배치합니다. 최근에 이러한 보험업자가 암호화된 의료 규제 요청을 MedRepo의 고객 서비스 부서에 잘못 제출했습니다. MedRepo는 응답 과정에서 여러 불만 사항을 LifeIns에 제출했습니다. LifeIns는 신입 보험업자 교육 기간을 연장하고 MedRepo에 제출하는 보험업자 요청에 대해 감사를 수행할 계획입니다.

자세한 내용은 다음 절을 참조하십시오.

- 19-5페이지의 예: 패시브 구축에서 트래픽 해독
- 19-10페이지의 예: 인라인 구축에서 트래픽 해독

예: 패시브 구축에서 트래픽 해독

라이센스: 기능에 따라 다름

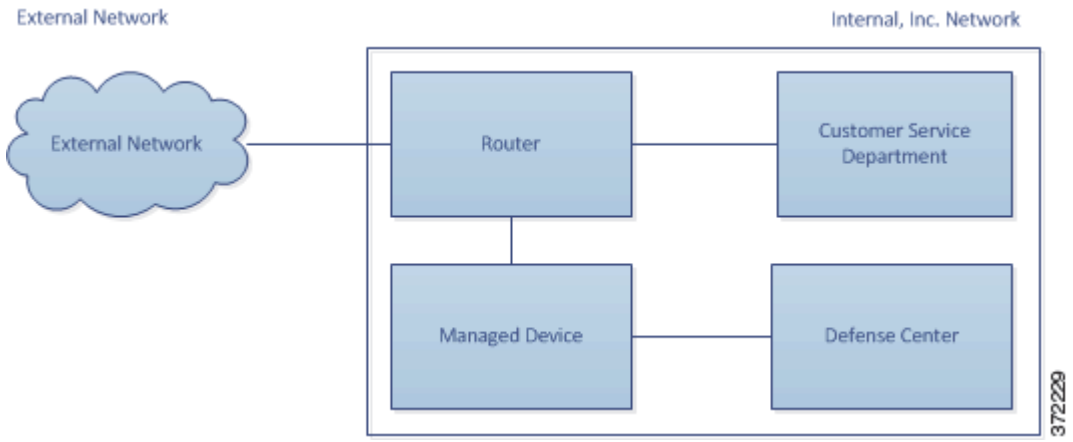
지원되는 디바이스: Series 3

LifeIns의 비즈니스 요구 사항에서는 Customer Service에 다음을 수행하도록 규정합니다.

- 모든 요청과 신청서를 24시간 내에 처리
- 수신 연락처 메트릭 수집 프로세스 개선
- 잘못된 수신 신청서 식별 및 폐기

Customer Service에서는 추가 감사 검토를 요구하지 않습니다.

LifeIns는 Customer Service 관리되는 디바이스를 패시브 방식으로 구축할 계획입니다. 다음 다이어그램은 LifeIns의 패시브 구축을 보여줍니다.



외부 네트워크에서 오는 트래픽은 LifeIns의 라우터로 이동합니다. 라우터는 트래픽을 Customer Service 부서로 라우팅하고, 검사를 위해 트래픽 복사본을 관리되는 디바이스에 미러링합니다.

관리하는 방어 센터에서 Access Control 및 SSL Editor 사용자 지정 역할을 보유한 사용자는 다음을 수행하도록 SSL 검사를 구성합니다.

- Customer Service 부서로 전송되는 모든 암호화된 트래픽 로깅
- 온라인 신청서를 사용하여 Customer Service로 전송되는 암호화된 트래픽 해독
- 온라인 요청 양식을 사용하여 전송되는 트래픽을 비롯하여 Customer Service로 전송되는 다른 모든 암호화된 트래픽은 해독하지 않음

사용자는 또한 해독된 신청서에서 위조된 신청 데이터를 검사하고 위조된 데이터 탐지 시 로깅하도록 액세스 제어를 구성할 수 있습니다.

다음 시나리오에서 사용자는 Customer Service에 온라인 양식을 제출합니다. 사용자의 브라우저는 서버와 TCP 연결을 설정하고 SSL 핸드셰이크를 시작합니다. 관리되는 디바이스는 이 트래픽의 복사본을 수신합니다. 클라이언트와 서버는 SSL 핸드셰이크를 완료하여 암호화된 세션을 설정합니다. 핸드셰이크 및 연결 세부사항을 기반으로, 시스템은 연결을 로깅하고 암호화된 트래픽의 복사본에 대해 조치를 취합니다.

자세한 내용은 다음을 참조하십시오.

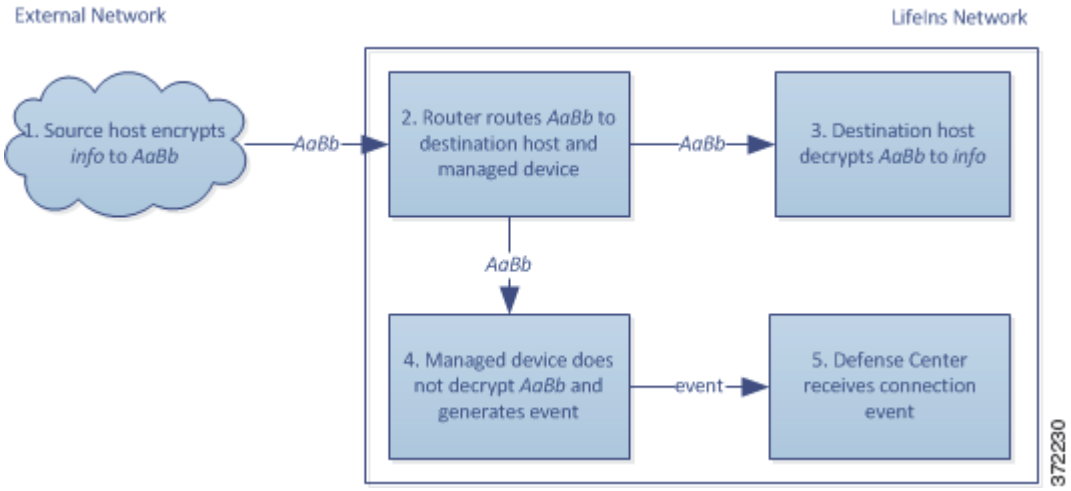
- 19-7페이지의 패시브 구축에서 암호화된 트래픽 모니터링
- 19-8페이지의 패시브 구축에서 암호화된 트래픽 해독 안 함
- 19-9페이지의 패시브 구축에서 개인 키로 암호화된 트래픽 검사

패시브 구축에서 암호화된 트래픽 모니터링

라이센스: 모두

지원되는 디바이스: Series 3

Customer Service로 전송된 모든 SSL 암호화 트래픽에 대해 시스템은 연결을 로깅합니다. 다음 다이어그램은 시스템 모니터링 암호화 트래픽을 보여줍니다.



다음 단계가 발생합니다.

1. 사용자가 일반 텍스트 요청을 제출합니다(`info`). 클라이언트가 이를 암호화하고(`AaBb`) 암호화된 트래픽을 Customer Service로 전송합니다.
2. LifeIns의 라우터가 암호화된 트래픽을 수신한 다음 Customer Service 부서 서버로 라우팅합니다. 또한 복사본을 관리되는 디바이스에 미러링합니다.
3. Customer Service 부서 서버는 암호화된 정보 요청을 수신하고(`AaBb`) 이를 일반 텍스트로 해독합니다(`info`).
4. 관리되는 디바이스는 트래픽을 해독하지 않습니다.

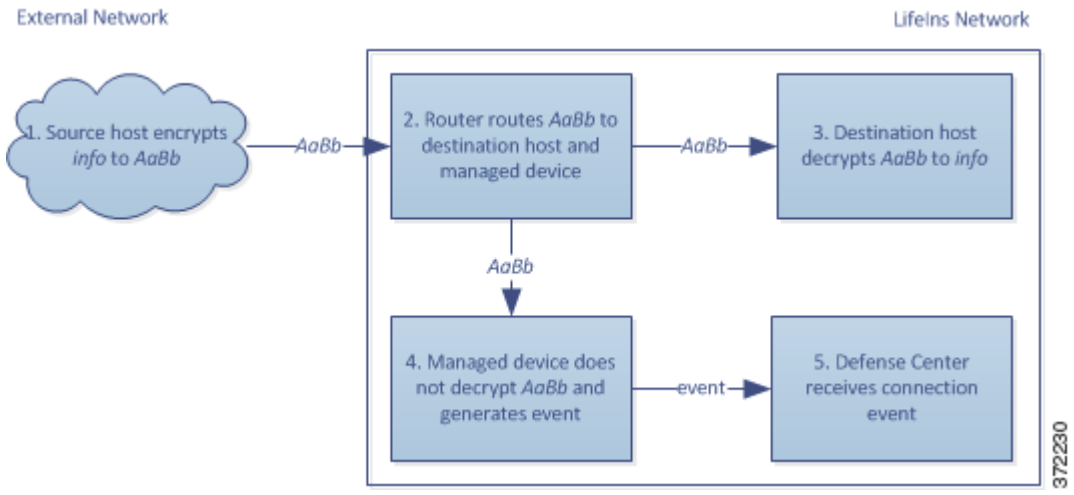
   액세스 제어 정책은 계속해서 암호화된 트래픽을 처리하고 허용합니다. 디바이스는 세션 종료 후 연결 이벤트를 생성합니다.
5. 방어 센터는 연결 이벤트를 수신합니다.

패시브 구축에서 암호화된 트래픽 해독 안 함

라이센스: 모두

지원되는 디바이스: Series 3

정책에 대한 요청을 포함하는 모든 SSL 암호화 트래픽의 경우, 시스템은 해독 없이 트래픽을 허용하고 연결을 로깅합니다. 다음 다이어그램은 추가 검사 없이 시스템에서 허용하는 암호화 트래픽을 보여줍니다.



다음 단계가 발생합니다.

1. 사용자가 일반 텍스트 요청을 제출합니다(`info`). 클라이언트가 이를 암호화하고(`AaBb`) 암호화된 트래픽을 Customer Service로 전송합니다.
2. LifeIns의 라우터가 암호화된 트래픽을 수신한 다음 Customer Service 부서 서버로 라우팅합니다. 또한 복사본을 관리되는 디바이스에 미러링합니다.
3. Customer Service 부서 서버는 암호화된 정보 요청을 수신하고(`AaBb`) 이를 일반 텍스트로 해독합니다(`info`).
4. 관리되는 디바이스는 트래픽을 해독하지 않습니다.

   액세스 제어 정책은 계속해서 암호화된 트래픽을 처리하고 허용합니다. 디바이스는 세션 종료 후 연결 이벤트를 생성합니다.
5. 방어 센터는 연결 이벤트를 수신합니다.

패시브 구축에서 개인 키로 암호화된 트래픽 검사

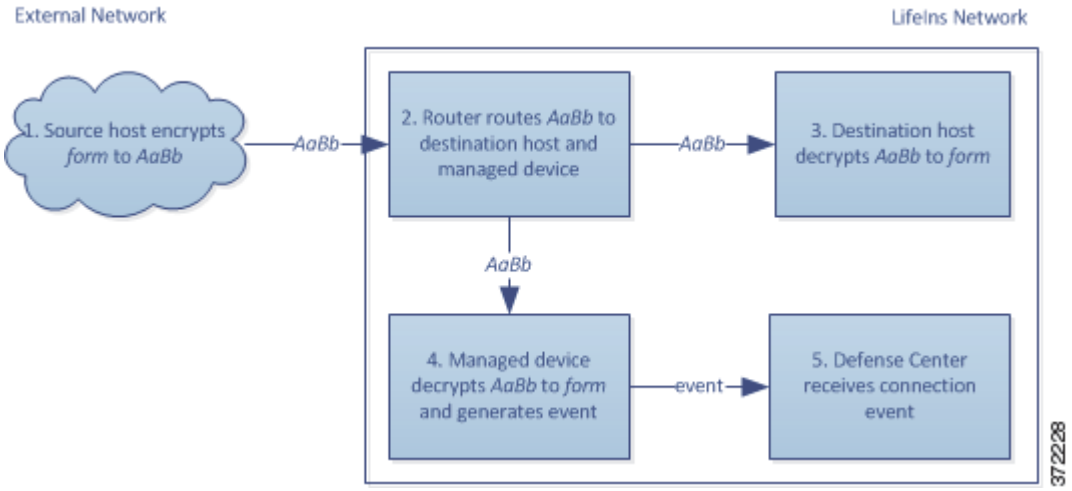
라이센스: 모두

지원되는 디바이스: Series 3

신청서 데이터를 포함하는 모든 SSL 암호화 트래픽의 경우, 시스템은 트래픽을 해독하고 연결을 로깅합니다.

참고 패시브 구축에서 트래픽이 DHE 또는 ECDHE 암호 그룹으로 암호화된 경우 알려진 개인 키로 해독할 수 없습니다.

합법적인 신청서 정보를 포함한 트래픽의 경우 시스템은 연결을 로깅합니다. 다음 다이어그램은 알려진 개인 키를 사용한 트래픽 해독을 보여줍니다.

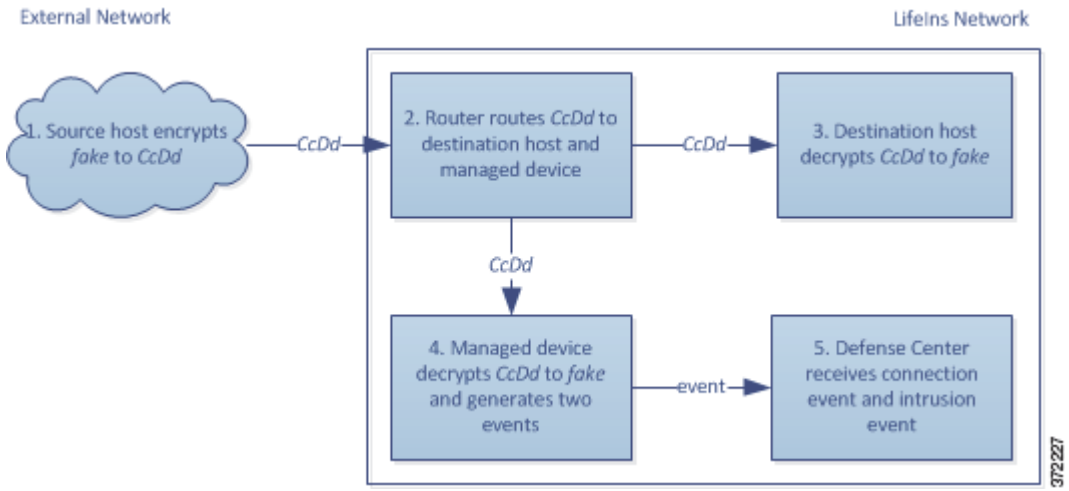


다음 단계가 발생합니다.

1. 사용자가 일반 텍스트 요청을 제출합니다(`form`). 클라이언트가 이를 암호화하고(`AaBb`) 암호화된 트래픽을 Customer Service로 전송합니다.
2. LifeIns의 라우터가 암호화된 트래픽을 수신한 다음 Customer Service 부서 서버로 라우팅합니다. 또한 복사본을 관리되는 디바이스에 미러링합니다.
3. Customer Service 부서 서버는 암호화된 정보 요청을 수신하고(`AaBb`) 이를 일반 텍스트로 해독합니다(`form`).
4. 관리되는 디바이스는 업로드된 알려진 개인 키로 얻은 세션 키를 사용하여, 암호화된 트래픽을 일반 텍스트로 해독합니다(`form`).

   액세스 제어 정책은 계속해서 해독된 트래픽을 처리하며 위조된 신청서 정보를 찾지 않습니다. 디바이스는 세션 종료 후 연결 이벤트를 생성합니다.
5. 방어 센터는 암호화된 트래픽과 해독된 트래픽에 대한 정보가 포함된 연결 이벤트를 수신합니다.

이와 반대로, 해독된 트래픽에 위조된 신청서 데이터가 포함된 경우 시스템은 연결 및 위조된 데이터를 로깅합니다. 다음 다이어그램은 알려진 개인 키를 사용하여 위조된 신청서 데이터가 포함된 수신 트래픽을 해독하는 시스템을 보여줍니다.



다음 단계가 발생합니다.

1. 사용자가 일반 텍스트 요청을 제출합니다(`fake`). 클라이언트가 이를 암호화하고(`CcDd`) 암호화된 트래픽을 Customer Service로 전송합니다.
2. LifeIns의 라우터가 암호화된 트래픽을 수신한 다음 Customer Service 부서 서버로 라우팅합니다. 또한 복사본을 관리되는 디바이스에 미러링합니다.
3. Customer Service 부서 서버는 암호화된 정보 요청을 수신하고(`CcDd`) 이를 일반 텍스트로 해독합니다(`fake`).
4. 관리되는 디바이스는 업로드된 알려진 개인 키로 얻은 세션 키를 사용하여, 암호화된 트래픽을 일반 텍스트로 해독합니다(`fake`).

   액세스 제어 정책은 계속해서 해독된 트래픽을 처리하며 위조된 신청서 정보를 찾습니다. 디바이스가 침입 이벤트를 생성합니다. 세션이 종료된 후 연결 이벤트가 생성됩니다.
5. 방어 센터는 암호화된 트래픽 및 해독된 트래픽에 대한 정보가 포함된 연결 이벤트, 그리고 위조된 신청서 데이터에 대한 침입 이벤트를 수신합니다.

예: 인라인 구축에서 트래픽 해독

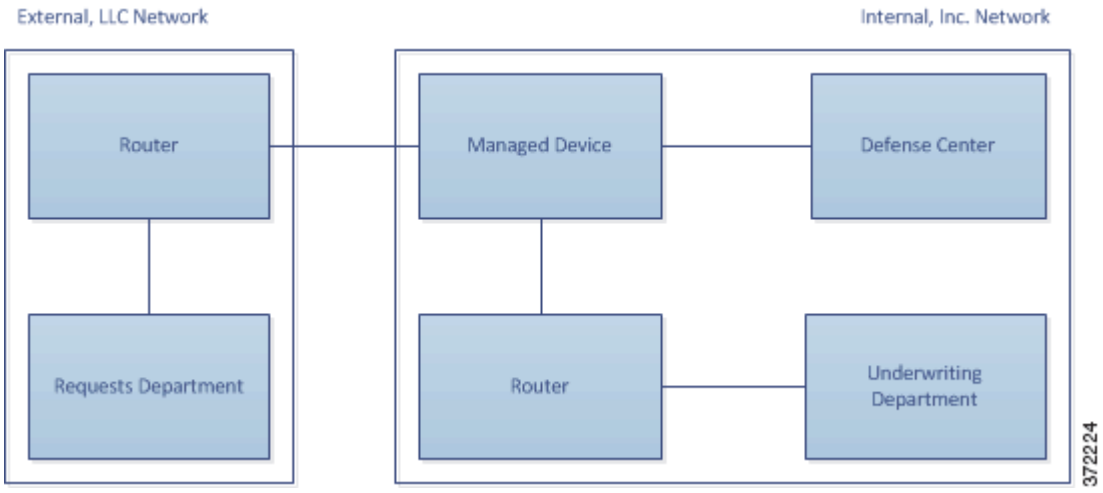
라이센스: 기능에 따라 다름

지원되는 디바이스: Series 3

LifeIns의 비즈니스 요구 사항에서는 Underwriting에서 다음을 수행하도록 규정합니다.

- 신입 및 하급 보험업자를 감사하여, MedRepo에 대한 정보 요청이 모든 해당 규정을 준수하는지 확인합니다.
- 보험 가입 메트릭 수집 프로세스 개선
- MedRepo에서 온 것처럼 보이는 모든 요청을 검토하고 모든 스푸핑 시도 삭제
- Underwriting 부서에서 MedRepo의 Customer Service 부서로 이동하는 모든 부적절한 규제 요청 삭제
- 상급 보험업자는 감사하지 않음

LifeIns는 Underwriting 부서를 위한 인라인 구축에 디바이스를 구축할 계획입니다. 다음 다이어그램은 LifeIns의 인라인 구축을 보여줍니다.



MedRepo의 네트워크에서 오는 트래픽은 MedRepo의 라우터로 이동합니다. 트래픽이 LifeIns의 네트워크로 라우팅됩니다. 관리되는 디바이스는 트래픽을 수신하고, 트래픽을 LifeIns의 라우터에 전달하고, 이벤트를 관리하는 방어 센터로 전송합니다. LifeIns의 라우터는 트래픽을 목적지 호스트로 라우팅합니다.

관리하는 방어 센터에서 Access Control 및 SSL Editor 사용자 지정 역할을 보유한 사용자는 다음을 수행하도록 SSL 검사를 구성합니다.

- Underwriting 부서로 전송되는 모든 암호화된 트래픽 로깅
- LifeIns의 Underwriting 부서에서 MedRepo의 Customer Service 부서로 잘못 전송된 모든 암호화된 트래픽 차단
- MedRepo에서 LifeIns의 Underwriting 부서, 그리고 LifeIns의 하급 보험업자가 MedRepo의 Requests 부서로 전송한 모든 암호화된 트래픽 해독
- 상급 보험업자가 전송한 암호화된 트래픽은 해독하지 않음

또한 사용자는 해독된 트래픽을 사용자 지정 침입 정책으로 검사하도록 액세스 제어를 구성하고 다음을 수행할 수 있습니다.

- 스푸핑 시도가 포함된 경우 해독된 트래픽을 차단하고 스푸핑 시도 로깅
- 규정을 준수하지 않는 정보가 포함된 해독된 트래픽을 차단하고 부적절한 정보 로깅
- 다른 모든 암호화된 트래픽 및 해독된 트래픽 허용

시스템은 해독된 트래픽을 목적지 호스트로 전송하기 전에 다시 암호화합니다.

다음 시나리오에서 사용자는 원격 서버에 온라인으로 정보를 제출합니다. 사용자의 브라우저는 서버와 TCP 연결을 설정하고 SSL 핸드셰이크를 시작합니다. 관리되는 디바이스는 이 트래픽을 수신합니다. 핸드셰이크와 연결 세부사항을 기반으로 시스템은 연결을 로깅하고 트래픽에 대해 조치를 취합니다. 시스템은 트래픽을 차단하는 경우 TCP 연결도 닫습니다. 그렇지 않은 경우, 클라이언트와 서버는 SSL 핸드셰이크를 완료하여 암호화된 세션을 설정합니다.

자세한 내용은 다음을 참조하십시오.

- 19-12페이지의 인라인 구축에서 암호화된 트래픽 모니터링
- 19-13페이지의 인라인 구축에서 특정 사용자의 암호화된 트래픽 허용
- 19-14페이지의 인라인 구축에서 암호화된 트래픽 차단

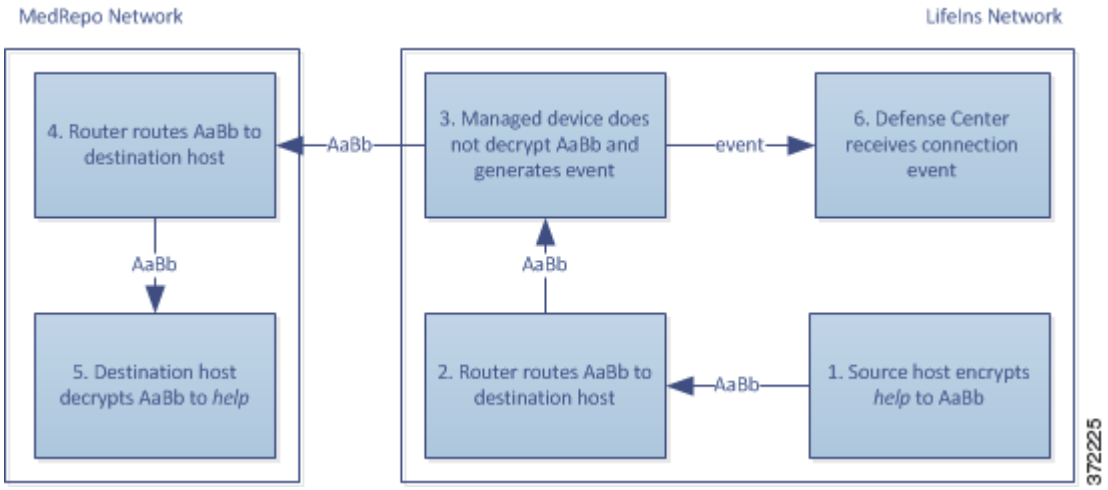
- 19-15페이지의 인라인 구축에서 개인 키로 암호화된 트래픽 검사
- 19-16페이지의 인라인 구축에서 다시 서명된 인증서로 특정 사용자의 암호화된 트래픽 검사

인라인 구축에서 암호화된 트래픽 모니터링

라이센스: 모두

지원되는 디바이스: Series 3

Underwriting 부서에서 주고받는 모든 SSL 암호화 트래픽에 대해 시스템은 연결을 로깅합니다. 다음 다이어그램은 시스템 모니터링 암호화 트래픽을 보여줍니다.



다음 단계가 발생합니다.

1. 사용자가 일반 텍스트 요청을 제출합니다(`help`). 클라이언트가 이를 암호화하고(`AaBb`) 암호화된 트래픽을 MedRepo의 Requests 부서 서버로 전송합니다.
2. LifeIns의 라우터가 암호화된 트래픽을 수신한 다음 Requests 부서 서버로 라우팅합니다.
3. 관리되는 디바이스는 트래픽을 해독하지 않습니다.

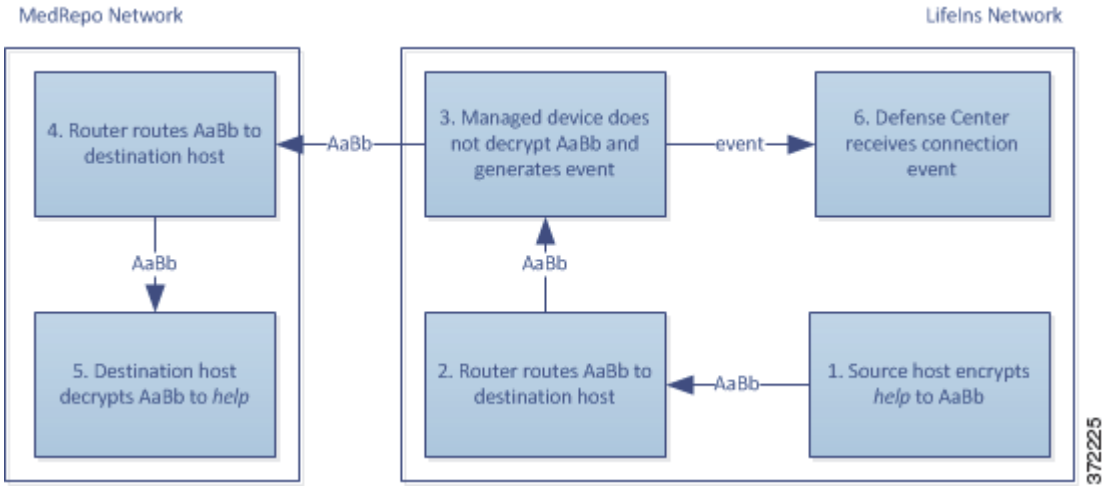
   액세스 제어 정책은 계속해서 암호화된 트래픽을 처리하고 허용한 다음, 세션이 종료된 후 연결 이벤트를 생성합니다.
4. 외부 라우터가 트래픽을 수신한 다음 Requests 부서 서버로 라우팅합니다.
5. Underwriting 부서 서버는 암호화된 정보 요청을 수신하고(`AaBb`) 이를 일반 텍스트로 해독합니다(`help`).
6. 방어 센터는 연결 이벤트를 수신합니다.

인라인 구축에서 특정 사용자의 암호화된 트래픽 허용

라이센스: 제어

지원되는 디바이스: Series 3

상급 보험업자로부터 시작된 모든 SSL 암호화 트래픽의 경우, 시스템은 해독 없이 트래픽을 허용하고 연결을 로깅합니다. 다음 다이어그램은 시스템 허용 암호화 트래픽을 보여줍니다.



다음 단계가 발생합니다.

1. 사용자가 일반 텍스트 요청을 제출합니다(`help`). 클라이언트가 이를 암호화하고(`AaBb`) 암호화된 트래픽을 MedRepo의 Requests 부서 서버로 전송합니다.
2. LifeIns의 라우터가 암호화된 트래픽을 수신한 다음 Requests 부서 서버로 라우팅합니다.
3. 관리되는 디바이스는 이 트래픽을 해독하지 않습니다.

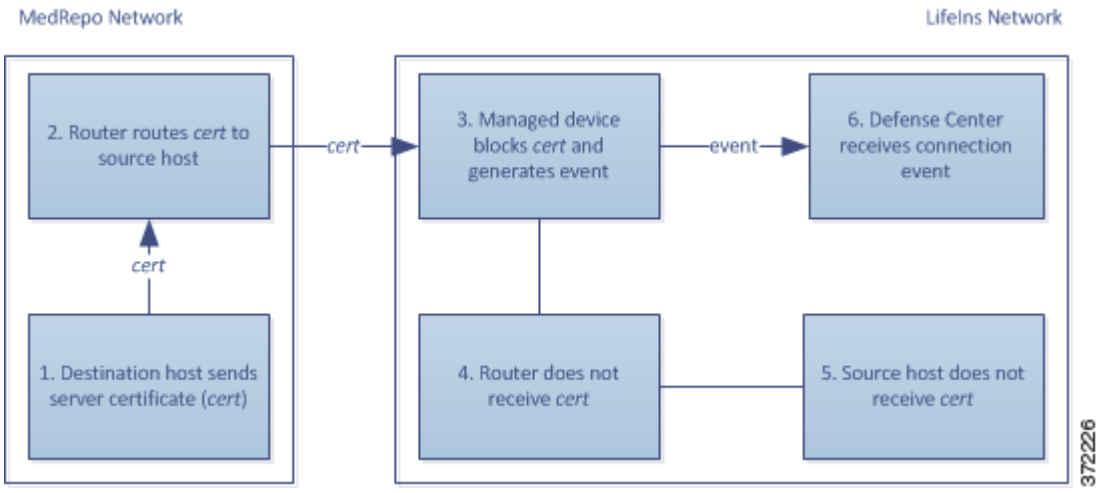
   액세스 제어 정책은 계속해서 암호화된 트래픽을 처리하고 허용한 다음, 세션이 종료된 후 연결 이벤트를 생성합니다.
4. 외부 라우터가 트래픽을 수신한 다음 Requests 부서 서버로 라우팅합니다.
5. Requests 부서 서버는 암호화된 정보 요청을 수신하고(`AaBb`) 이를 일반 텍스트로 해독합니다(`help`).
6. 방어 센터는 연결 이벤트를 수신합니다.

인라인 구축에서 암호화된 트래픽 차단

라이센스: 모두

지원되는 디바이스: Series 3

LifeIns의 Underwriting 부서에서 MedRepo의 Customer Service 부서로 부적절하게 전송된 모든 SMTPS 이메일 트래픽에 대해 시스템은 추가 검사 없이 SSL 핸드셰이크 중에 트래픽을 차단하고 연결을 로깅합니다. 다음 다이어그램은 시스템 차단 암호화 트래픽을 보여줍니다.



다음 단계가 발생합니다.

1. 클라이언트 브라우저에서 SSL 핸드셰이크 설정 요청을 받으면 Customer Service 부서 서버는 SSL 핸드셰이크의 다음 단계로서 LifeIns 보험업자에게 서버 인증서(`cert`)를 전송합니다.
2. MedRepo의 라우터는 인증서를 수신한 다음 LifeIns 보험업자에게 라우팅합니다.
3. 관리되는 디바이스는 추가 검사 없이 트래픽을 차단하고 TCP 연결을 종료하며, 연결 이벤트를 생성합니다.
4. 내부 라우터는 차단된 트래픽을 수신하지 않습니다.
5. 보험업자는 차단된 트래픽을 수신하지 않습니다.
6. 방어 센터는 연결 이벤트를 수신합니다.

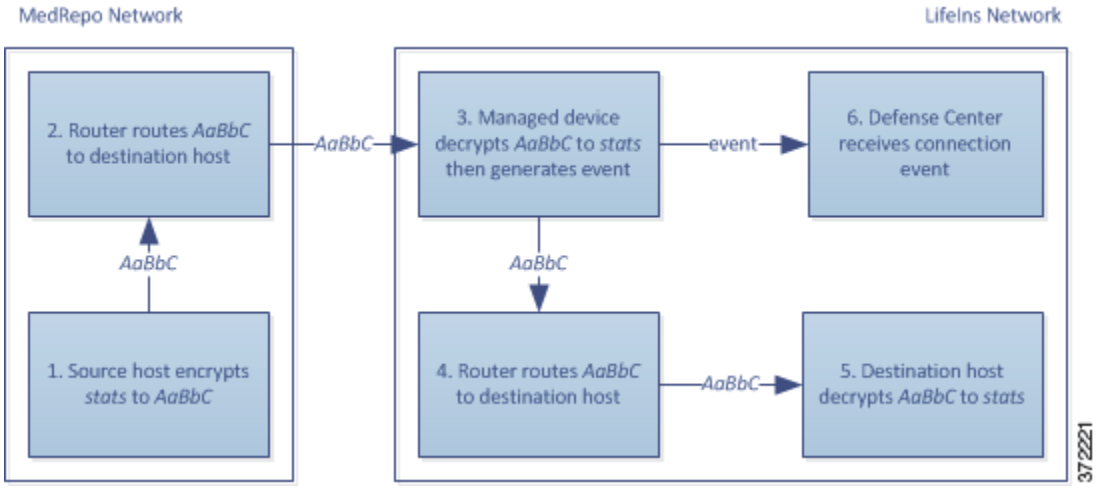
인라인 구축에서 개인 키로 암호화된 트래픽 검사

라이센스: 모두

지원되는 디바이스: Series 3

MedRepo에서 LifeIns의 Underwriting 부서로 전송되는 모든 SSL 암호화 트래픽에 대해 시스템은 업로드된 서버 개인 키를 사용하여 세션 키를 가져온 다음 트래픽을 해독하고 연결을 로깅합니다. 합법적인 트래픽은 Underwriting 부서로 전송되기 전에 허용되고 다시 암호화됩니다.

다음 다이어그램은 알려진 개인 키로 암호화된 트래픽을 해독한 다음, 액세스 제어를 사용하여 트래픽을 검사하고 해독된 트래픽을 허용하는 시스템을 보여줍니다.

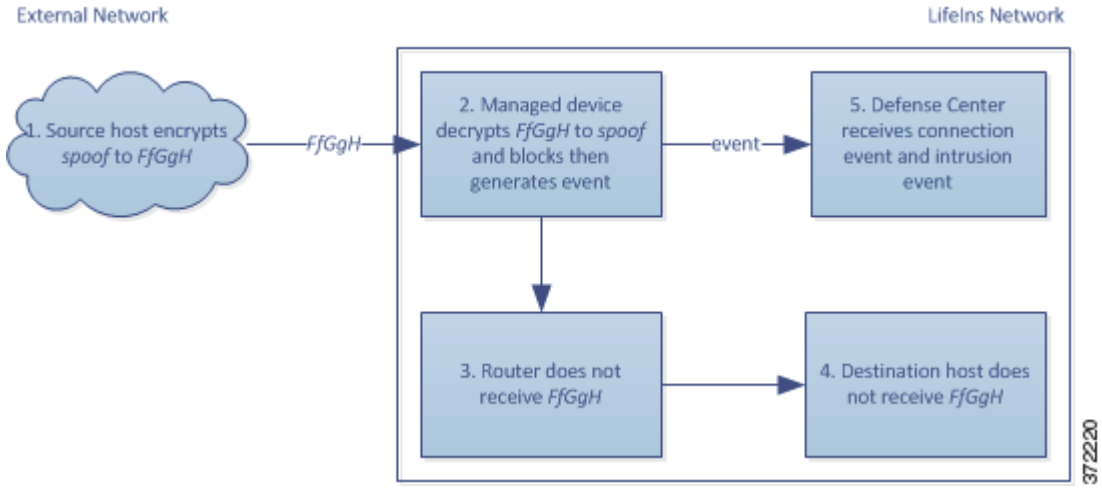


다음 단계가 발생합니다.

1. 사용자가 일반 텍스트 요청을 제출합니다(`stats`). 클라이언트가 이를 암호화하고(`AaBbC`) 암호화된 트래픽을 Underwriting 부서 서버로 전송합니다.
2. 외부 라우터가 트래픽을 수신한 다음 Underwriting 부서 서버로 라우팅합니다.
3. 관리되는 디바이스는 업로드된 알려진 개인 키로 얻은 세션 키를 사용하여 이 트래픽을 일반 텍스트로 해독합니다(`stats`).

   액세스 제어 정책은 사용자 지정 침입 정책을 이용해 계속해서 해독된 트래픽을 처리하며 스푸핑 시도를 찾지 않습니다. 디바이스는 암호화된 트래픽을 전달한 다음(`AaBbC`) 세션 종료 후 연결 이벤트를 생성합니다.
4. 내부 라우터가 트래픽을 수신한 다음 Underwriting 부서 서버로 라우팅합니다.
5. Underwriting 부서 서버는 암호화된 정보를 수신하고(`AaBbC`) 이를 일반 텍스트로 해독합니다(`stats`).
6. 방어 센터는 암호화된 트래픽과 해독된 트래픽에 대한 정보가 포함된 연결 이벤트를 수신합니다.

이와 반대로, 스푸핑 시도를 나타내는 해독된 트래픽은 삭제됩니다. 시스템은 연결 및 스푸핑 시도를 로깅합니다. 다음 다이어그램은 알려진 개인 키로 암호화된 트래픽을 해독한 다음, 액세스 제어 정책을 사용하여 트래픽을 검사하고 해독된 트래픽을 차단하는 시스템을 보여줍니다.



다음 단계가 발생합니다.

1. 사용자가 일반 텍스트 요청을 제출하고(`spoof`), MedRepo, LLC에서 시작된 것으로 보이는 트래픽을 변경합니다. 클라이언트가 이를 암호화하고(`FfGgH`) 암호화된 트래픽을 Underwriting 부서 서버로 전송합니다.
2. 관리되는 디바이스는 업로드된 알려진 개인 키로 얻은 세션 키를 사용하여 이 트래픽을 일반 텍스트로 해독합니다(`spoof`).

   액세스 제어 정책은 사용자 지정 침입 정책을 이용해 계속해서 해독된 트래픽을 처리하며 스푸핑 시도를 찾습니다. 디바이스는 트래픽을 차단한 다음 침입 이벤트를 생성하며, 세션 종료 후 연결 이벤트를 생성합니다.
3. 내부 라우터는 차단된 트래픽을 수신하지 않습니다.
4. Underwriting 부서 서버는 차단된 트래픽을 수신하지 않습니다.
5. 방어 센터는 암호화된 트래픽 및 해독된 트래픽에 대한 정보가 포함된 연결 이벤트, 그리고 스푸핑 시도에 대한 침입 이벤트를 수신합니다.

인라인 구축에서 다시 서명된 인증서로 특정 사용자의 암호화된 트래픽 검사

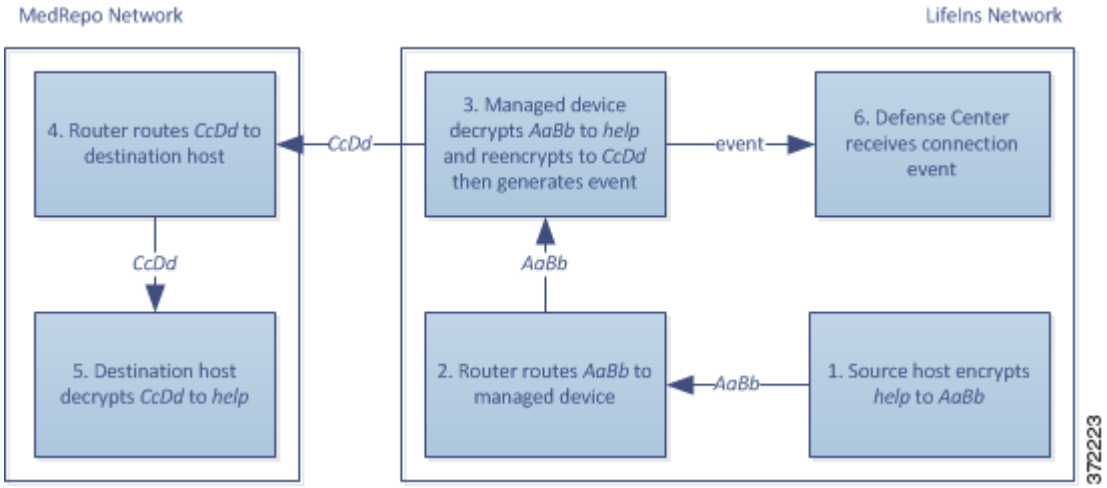
라이센스: 제어

지원되는 디바이스: Series 3

신입 및 하급 보험업자가 MedRepo의 Requests 부서로 전송하는 모든 SSL 암호화 트래픽에 대해 시스템은 다시 서명된 서버 인증서를 사용하여 세션 키를 얻은 다음 트래픽을 해독하고 연결을 로깅합니다. 합법적인 트래픽은 MedRepo로 전송되기 전에 허용되고 다시 암호화됩니다.

참고 다시 서명된 서버 인증서로 인라인 구축에서 트래픽을 해독할 때 디바이스는 중간자(man-in-the-middle) 역할을 합니다. 클라이언트와 관리되는 디바이스 간, 관리되는 디바이스와 서버 간에 각각 하나씩 2개의 SSL 세션을 생성합니다. 그 결과 각 세션에는 서로 다른 암호 세션 세부사항이 포함됩니다.

다음 다이어그램은 다시 서명된 서버 인증서 및 개인 키로 암호화된 트래픽을 해독한 다음, 액세스 제어를 사용하여 트래픽을 검사하고 해독된 트래픽을 허용하는 시스템을 보여줍니다.



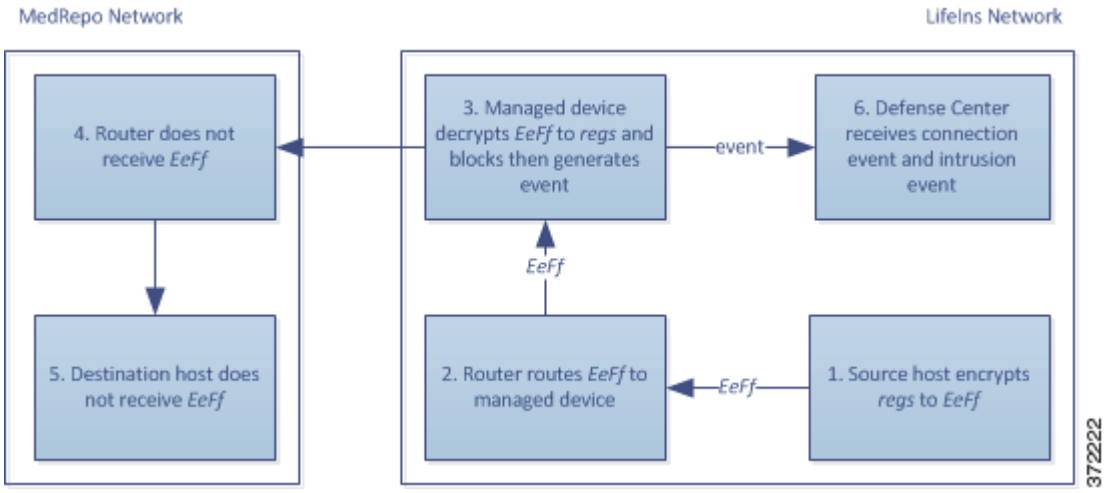
다음 단계가 발생합니다.

1. 사용자가 일반 텍스트 요청을 제출합니다(`help`). 클라이언트가 이를 암호화하고(`AaBb`) 암호화된 트래픽을 Requests 부서 서버로 전송합니다.
2. 내부 라우터가 트래픽을 수신한 다음 Requests 부서 서버로 라우팅합니다.
3. 관리되는 디바이스는 다시 서명된 서버 인증서 및 개인 키로 얻은 세션 키를 사용하여 이 트래픽을 일반 텍스트로 해독합니다(`stats`).

   액세스 제어 정책은 사용자 지정 침입 정책을 이용해 계속해서 해독된 트래픽을 처리하며 부적절한 요청을 찾지 않습니다. 디바이스는 트래픽을 다시 암호화하여(`CcDd`) 통과하도록 허용합니다. 세션 종료 후 연결 이벤트를 생성합니다.
4. 외부 라우터가 트래픽을 수신한 다음 Requests 부서 서버로 라우팅합니다.
5. Requests 부서 서버는 암호화된 정보를 수신하고(`CcDd`) 이를 일반 텍스트로 해독합니다(`help`).
6. 방어 센터는 암호화된 트래픽과 해독된 트래픽에 대한 정보가 포함된 연결 이벤트를 수신합니다.

참고 다시 서명된 서버 인증서로 트래픽을 암호화하면 클라이언트 브라우저에 신뢰되지 않은 인증서에 대한 경고가 표시됩니다. 이를 피하려면 CA 인증서를 조직의 도메인 루트 신뢰받는 인증서 저장소 또는 클라이언트 신뢰받는 인증서 저장소에 추가하십시오.

이와 반대로, 규정 요구 사항을 충족하지 못하는 정보를 포함하는 해독된 트래픽은 삭제됩니다. 시스템은 연결 및 비준수 정보를 로깅합니다. 다음 다이어그램은 다시 서명된 서버 인증서 및 개인 키로 암호화된 트래픽을 해독한 다음, 액세스 제어 정책을 사용하여 트래픽을 검사하고 해독된 트래픽을 차단하는 시스템을 보여줍니다.



다음 단계가 발생합니다.

1. 사용자가 규정 요구 사항을 준수하지 않는 일반 텍스트 요청을 제출합니다(`regs`). 클라이언트가 이를 암호화하고(`EeFf`) 암호화된 트래픽을 Requests 부서 서버로 전송합니다.
2. 내부 라우터가 트래픽을 수신한 다음 Requests 부서 서버로 라우팅합니다.
3. 관리되는 디바이스는 다시 서명된 서버 인증서 및 개인 키로 얻은 세션 키를 사용하여 이 트래픽을 일반 텍스트로 해독합니다(`regs`).

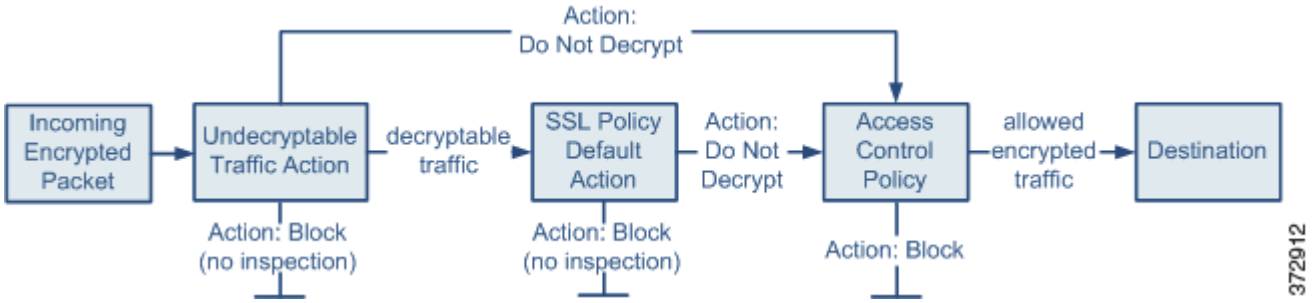
   액세스 제어 정책은 사용자 지정 침입 정책을 이용해 계속해서 해독된 트래픽을 처리하며 부적절한 요청을 찾습니다. 디바이스는 트래픽을 차단한 다음 침입 이벤트를 생성하며, 세션 종료 후 연결 이벤트를 생성합니다.
4. 외부 라우터는 차단된 트래픽을 수신하지 않습니다.
5. Requests 부서 서버는 차단된 트래픽을 수신하지 않습니다.
6. 방어 센터는 암호화된 트래픽 및 해독된 트래픽에 대한 정보가 포함된 연결 이벤트, 그리고 부적절한 요청에 대한 침입 이벤트를 수신합니다.

20장

SSL 정책 시작하기

*SSL 정책*에 따라 시스템에서 네트워크의 암호화 트래픽을 처리하는 방식이 결정됩니다. 하나 이상의 SSL 정책을 구성할 수 있습니다. SSL 정책을 액세스 제어 정책과 연결한 다음, 관리하는 디바이스에 액세스 제어 정책을 적용합니다. 디바이스에서 TCP 핸드셰이크를 탐지하면 먼저 액세스 제어 정책으로 트래픽을 처리하고 검사합니다. 그 이후에 TCP 연결을 통한 SSL 암호화 세션을 식별할 경우 SSL 정책이 넘겨받아 암호화 트래픽을 처리하고 해독합니다. Series 3 디바이스에 적용 중인 하나의 SSL 정책을 보유할 수 있습니다.

다음 다이어그램에서 보여주는 것처럼 가장 간단한 SSL 정책은 디바이스에 적용되어 단일 기본 작업을 통해 암호화 트래픽을 처리합니다. 추가 검사 없이 해독 가능 트래픽을 차단하거나 액세스 제어와 함께 아직 해독되지는 않았지만 해독 가능한 트래픽을 검사하도록 기본 작업을 설정할 수 있습니다. 그러면 시스템에서 암호화 트래픽을 허용하거나 차단할 수 있습니다. 디바이스에서 해독 불가 트래픽을 탐지할 경우 추가 검사 없이 차단하거나 해독하지 않고 액세스 제어로 검사합니다.



이 장에서는 과 간단한 SSL 정책을 생성하고 적용하는 방법에 대해 설명합니다. 또한 SSL 정책 관리(수정, 업데이트, 비교 등)에 대한 기본적인 정보도 제공합니다. 자세한 내용은 다음 링크를 참조하십시오.

- 20-2페이지의 기본 SSL 정책 생성
- 20-7페이지의 SSL 정책 수정
- 20-9페이지의 액세스 제어를 사용하여 해독 설정 적용
- 20-10페이지의 현재 트래픽 해독 설정에 대한 보고서 생성
- 20-11페이지의 SSL 정책 비교

더 복잡한 SSL 정책에서는 다양한 유형의 해독 불가 트래픽을 각기 다른 작업으로 처리하고, CA(인증 기관)에서 암호화 인증서를 발급하였는지 신뢰하는지에 따라 트래픽을 제어하고, 암호화 트래픽 로깅 및 처리를 정밀하게 제어하기 위해 SSL 규칙을 사용할 수 있습니다. 이러한 규칙은 다양한 기준에 따라 암호화 트래픽을 매칭하고 검사하기 때문에 간단할 수도 있고 복잡할 수도 있습니다. 기본 SSL 정책 생성 후, 해당 구축에 따른 맞춤화에 대한 자세한 내용은 다음 장을 참조하십시오.

- 3-1페이지의 재사용 가능 객체 관리에서는 암호화 트래픽을 더 효과적으로 제어하고 해독하기 위해 재사용 가능 PKI(public key infrastructure) 객체 및 기타 SSL 검사 관련 객체를 구성하는 방법에 대해 설명합니다.
- 38-1페이지의 네트워크 트래픽의 연결 로깅에서는 암호화 트래픽의 해독이 가능하든 아니든 로깅을 구성하는 방법에 대해 설명합니다.
- 20-9페이지의 액세스 제어를 사용하여 해독 설정 적용에서는 SSL 정책을 액세스 제어 정책과 연결하는 방법에 대해 설명합니다.
- 12-1페이지의 액세스 제어 정책 시작에서는 디바이스에 액세스 제어 정책을 적용하는 방법에 대해 설명합니다.
- 14-1페이지의 액세스 제어 규칙을 사용하여 트래픽 플로우 조정에서는 해독된 트래픽을 검사하기 위해 액세스 제어 규칙을 구성하는 방법에 대해 설명합니다.
- 21-1페이지의 SSL 규칙 시작하기에서는 암호화 트래픽을 처리하고 로깅하기 위해 SSL 규칙을 구성하는 방법에 대해 설명합니다.
- 22-1페이지의 SSL 규칙을 사용하여 트래픽 해독 조정에서는 특정 암호화 트래픽을 더 효과적으로 매칭하기 위한 SSL 규칙 조건을 구성하는 방법에 대해 설명합니다.

기본 SSL 정책 생성

라이센스: 모두

지원되는 디바이스: Series 3

새 SSL 정책을 생성할 때에는 최소한 고유한 이름과 정책 기본 작업을 지정해야 합니다. 새 정책에 대한 기본 작업을 선택할 때 다음 옵션을 선택할 수 있습니다.

- **Do not decrypt** Do not decrypt 기본 작업으로 정책을 생성합니다.
- **Block** Block 기본 작업으로 정책을 생성합니다.
- **Block with reset** Block with reset 기본 작업으로 정책을 생성합니다.

SSL 정책을 생성한 후에 기본 작업을 수정할 수 있습니다. 기본 작업 선택에 대한 지침은 20-4페이지의 암호화 트래픽에 대한 기본 처리 및 검사 설정을/를 참조하십시오.

새 SSL 정책에는 시스템에서 해독할 수 없는 트래픽에 대한 기본 작업도 포함되어 있습니다. 해독 불가한 트래픽에 대해 선택했던 기본 작업을 상속하거나 이를 차단하거나 트래픽을 해독하지 않고 액세스 제어로 검사합니다. SSL 정책을 생성한 후에 해독 불가 트래픽 작업을 수정할 수 있습니다. 해독 불가 트래픽 작업의 선택에 대한 지침은 20-5페이지의 해독 불가 트래픽에 대한 기본 처리 설정을/를 참조하십시오.

SSL 정책 페이지(**Policies > SSL**)에서 모든 현재 SSL 정책을 이름별로 확인하고 선택 사항인 설명도 볼 수 있습니다. 이 페이지의 옵션을 통해 정책 비교, 새 정책 생성, 정책 복사, 각 정책에서 최근 저장한 모든 설정을 보여주는 보고서 확인, 정책 수정 또는 정책 삭제를 수행할 수 있습니다.

팁 구축한 환경의 다른 방어 센터에 SSL 정책을 내보내고 그로부터 SSL 정책을 가져올 수 있습니다. 자세한 내용은 A-1페이지의 컨피그레이션 가져오기 및 내보내기을/를 참조하십시오.

다음 표에서는 SSL Policy 페이지에서 정책 관리를 위해 수행할 수 있는 작업에 대해 설명합니다.

표 20-1 SSL 정책 관리 작업

목적	가능한 작업
새 SSL 정책 생성	**New Policy**를 클릭합니다. 자세한 내용은 20-2페이지의 기본 SSL 정책 생성을/를 참조하십시오.
기존 SSL 정책의 설정 수정	수정 아이콘( )을 클릭합니다. 자세한 내용은 20-7페이지의 SSL 정책 수정을/를 참조하십시오.
SSL 정책 비교	**Compare Policies**를 클릭합니다. 자세한 내용은 20-11페이지의 SSL 정책 비교을/를 참조하십시오.
SSL 정책 복사	복사 아이콘( )을 클릭합니다. 복사된 정책의 수정에 대한 자세한 내용은 20-7페이지의 SSL 정책 수정을/를 참조하십시오.
SSL 정책의 현재 컨피그레이션 설정을 나열하는 PDF 보고서 보기	보고서 아이콘( )을 클릭합니다. 자세한 내용은 20-10페이지의 현재 트래픽 해독 설정에 대한 보고서 생성을/를 참조하십시오.
SSL 정책 삭제	삭제 아이콘( )을 클릭한 다음 **OK**를 클릭합니다. 계속할지 여부를 물을 때, 다른 사용자가 정책을 변경했으나 저장하지 않은 경우 또한 알려줍니다.

SSL 정책을 생성하려면

액세스: Admin/Access Admin/Network Admin

1단계 **Policies > SSL**을 선택합니다.

SSL Policy 페이지가 나타납니다.

2단계 **New Policy**를 클릭합니다.

New SSL Policy 팝업 창이 나타납니다.

3단계 정책에 고유한 **Name**을 지정하고 선택 사항인 **Description**도 입력합니다.

공백과 특수 문자를 포함하여 인쇄 가능한 모든 문자를 사용할 수 있습니다.

4단계 **Default Action**을 지정합니다.

SSL 정책을 생성한 다음 선택한 기본 작업을 수정할 수 있습니다. 자세한 내용은 20-4페이지의 암호화 트래픽에 대한 기본 처리 및 검사 설정을/를 참조하십시오.

5단계 **Save**를 클릭합니다.

SSL Policy Editor 페이지가 나타납니다. 자세한 내용은 20-7페이지의 SSL 정책 수정을/를 참조하십시오.

암호화 트래픽에 대한 기본 처리 및 검사 설정

라이센스: 모두

지원되는 디바이스: Series 3

SSL 정책에 대한 기본 작업은 시스템에서 정책의 비 모니터 규칙에 매칭하지 않는 해독 가능한 암호화 트래픽을 어떻게 처리할지 결정합니다. SSL 규칙이 없는 SSL 정책을 적용할 경우 네트워크의 모든 해독 가능 트래픽이 처리되는 방식이 기본 작업에 따라 결정됩니다. 시스템에서 해독 불가 암호화 트래픽을 처리하는 방식에 대한 자세한 내용은 20-5페이지의 해독 불가 트래픽에 대한 기본 처리 설정을/를 참조하십시오.

다음 표에서는 선택 가능한 기본 작업과 이 작업이 암호화 트래픽에 미치는 영향을 보여줍니다. 기본 작업에 의해 차단된 암호화 트래픽에 대해서는 어떠한 검사도 수행하지 않습니다.

:

표 20-2 SSL 정책 기본 작업

기본 작업	암호화 트래픽에 미치는 영향
차단	추가 검사 없이 SSL 세션 차단
차단 및 재설정	추가 검사 없이 SSL 세션 차단 및 TCP 연결 재설정
해독하지 않음	액세스 제어와 함께 암호화 트래픽 검사

SSL 정책을 처음 생성할 때 기본 작업에 의해 처리되는 로깅 연결은 기본적으로 비활성화됩니다. 정책을 생성한 다음 기본 작업 자체뿐 아니라 이것도 변경할 수 있습니다.

다음 절차에서는 SSL 정책을 수정하면서 그 기본 작업을 설정하는 방법에 대해 설명합니다. SSL 정책을 수정하는 전체 절차는 20-7페이지의 SSL 정책 수정을/를 참조하십시오.

SSL 정책에 대한 기본 작업을 설정하려면

액세스: Admin/Access Admin/Network Admin

1단계 **Policies > SSL**을 선택합니다.

SSL Policy 페이지가 나타납니다.

2단계 구성하려는 SSL 정책 옆의 수정 아이콘( )을 클릭합니다.

SSL 정책 편집기가 나타납니다.

3단계 **Default Action**을 선택합니다. 자세한 내용은 SSL 정책 기본 작업 표를 참조하십시오.

4단계 38-13페이지의 SSL 규칙으로 해독 가능 연결 로깅에 설명된 대로 기본 작업에 대한 로깅 옵션을 구성합니다.

5단계 **Save**를 클릭합니다.

SSL Policy Editor 페이지가 나타납니다. 자세한 내용은 20-7페이지의 SSL 정책 수정을/를 참조하십시오.

해독 불가 트래픽에 대한 기본 처리 설정

라이센스: 모두

지원되는 디바이스: Series 3

시스템에서 해독하거나 검사하지 못하는 암호화 트래픽의 특정 유형을 처리하도록 SSL 정책 레벨에서 해독 불가 트래픽 작업을 설정할 수 있습니다. 어떤 SSL 규칙도 포함하지 않는 SSL 정책을 적용할 경우, 네트워크의 모든 해독 불가 암호화 트래픽이 처리되는 방식은 해독 불가 트래픽 작업에 의해 결정됩니다.

해독 불가 트래픽의 유형에 따라 다음 작업을 선택할 수 있습니다.

- 연결 차단
- 연결을 차단한 다음 재설정
- 액세스 제어와 함께 암호화 트래픽 검사
- SSL 정책에서 기본 작업 상속

다음 표에서는 해독 불가 트래픽 유형에 대해 설명합니다.

표 20-3 해독 불가 트래픽 유형

유형	설명	기본 작업	가능한 작업
압축된 세션	SSL 세션에서 데이터 압축 방식을 적용합니다.	기본 작업 상속	해독하지 않음 차단 차단 및 재설정 기본 작업 상속
SSLv2 세션	세션이 SSL 버전 2로 암호화됩니다. 클라이언트 hello 메시지가 SSL 2.0이고 전송된 트래픽의 나머지가 SSL 3.0일 경우 트래픽은 해독 가능합니다.	기본 작업 상속	해독하지 않음 차단 차단 및 재설정 기본 작업 상속
알 수 없는 암호화 솔루션	시스템에서 암호화 솔루션을 인식하지 않습니다.	기본 작업 상속	해독하지 않음 차단 차단 및 재설정 기본 작업 상속
지원되지 않는 암호화 솔루션	시스템에서 탐지된 암호화 솔루션 기반의 해독을 지원하지 않습니다.	기본 작업 상속	해독하지 않음 차단 차단 및 재설정 기본 작업 상속
캐싱되지 않는 세션	SSL 세션에서 세션 재사용이 활성화되었고 클라이언트 및 서버가 세션 식별자로 세션을 재설정했으며 시스템에서 그 세션 식별자를 캐싱하지 않았습니다.	기본 작업 상속	해독하지 않음 차단 차단 및 재설정 기본 작업 상속

표 20-3 해독 불가 트래픽 유형(계속)

유형	설명	기본 작업	가능한 작업
핸드셰이크 오류	SSL 핸드셰이크 협상 중에 오류가 발생했습니다.	기본 작업 상속	해독하지 않음 차단 차단 및 재설정 기본 작업 상속
해독 오류	트래픽 해독 중에 오류가 발생했습니다.	차단	차단 차단 및 재설정

SSL 정책을 처음 생성할 때 기본 작업에 의해 처리되는 로깅 연결은 기본적으로 비활성화됩니다. 기본 작업에 대한 로깅 설정이 해독 불가 트래픽 처리에도 적용되므로 해독 불가 트래픽 작업에 의해 처리되는 로깅 연결은 기본적으로 비활성화됩니다. 기본 로깅을 구성하는 것에 대한 자세한 내용은 38-13페이지의 SSL 규칙으로 해독 가능 연결 로깅을/를 참조하십시오.

참고 클라이언트와 관리되는 디바이스의 사이에 HTTP 프록시가 위치하고 클라이언트와 서버가 CONNECT HTTP 메서드를 사용하여 터널링된 SSL 연결을 설정할 경우 시스템에서 트래픽을 해독할 수 없습니다. 시스템에서 이 트래픽을 처리하는 방법은 **핸드셰이크 오류** 해독 불가 작업에 의해 결정됩니다. 자세한 내용은 21-10페이지의 Decrypt Actions: Decrypting Traffic for Further Inspection을/를 참조하십시오.

해독 불가 트래픽에 대한 기본 처리를 설정하려면

액세스: Admin/Access Admin/Network Admin

1단계 **Policies > SSL**을 선택합니다.

SSL Policy 페이지가 나타납니다.

2단계 구성하려는 SSL 정책 옆의 수정 아이콘()을 클릭합니다.

SSL 정책 편집기가 나타납니다.

3단계 **Undecryptable Actions** 탭을 선택합니다.

Undecryptable Actions 탭이 나타납니다.

4단계 각 필드에서 해독 불가 트래픽 유형에 대해 수행할 작업을 선택하거나 SSL 정책의 기본 작업을 적용할지 여부를 선택합니다. 자세한 내용은 SSL 정책 기본 작업 표를 참조하십시오.

5단계 변경 사항을 저장하려면 **Save**를 클릭합니다.

변경 사항이 적용되려면 연결된 액세스 제어 목록을 적용해야 합니다. 12-15페이지의 액세스 제어 정책 적용을/를 참조하십시오.

SSL 정책 수정

라이센스: 모두

지원되는 디바이스: Series 3

SSL 정책 편집기에서 정책을 구성하고 SSL 규칙을 체계화할 수 있습니다. SSL 정책을 구성하려면 정책에 고유한 이름과 기본 작업을 지정해야 합니다. 다음 작업도 가능합니다.

- SSL 규칙 추가, 수정, 삭제, 활성화, 비활성화
- 신뢰받는 CA 인증서 추가
- 시스템에서 해독할 수 없는 암호화 트래픽의 처리 결정
- 기본 작업 및 해독 불가 트래픽 작업으로 처리되는 트래픽 로깅

SSL 정책을 생성하거나 수정한 다음 이를 액세스 제어 정책과 연결하고 나서 액세스 제어 정책을 적용할 수 있습니다. 사용자 지정 사용자 역할을 생성하여 정책을 구성, 체계화, 적용하는 권한을 사용자에 따라 각기 다르게 부여할 수도 있습니다.

다음 표는 SSL 정책 편집기에서 수행할 수 있는 컨피그레이션 작업을 요약한 것입니다.

표 20-4 SSL 정책 컨피그레이션 작업

목적	가능한 작업
정책 이름 또는 설명 수정	이름 또는 설명 필드를 클릭하고 필요에 따라 임의의 문자를 삭제한 다음 새 이름 또는 설명을 입력합니다.
기본 작업 설정	추가 정보는 20-4페이지의 암호화 트래픽에 대한 기본 처리 및 검사 설정 참조
해독 불가 트래픽에 대한 기본 처리 설정	추가 정보는 20-5페이지의 해독 불가 트래픽에 대한 기본 처리 설정 참조
기본 작업 및 해독 불가 트래픽 작업에 대한 연결 로깅	추가 정보는 38-13페이지의 SSL 규칙으로 해독 가능 연결 로깅 참조
신뢰받는 CA 인증서 추가	추가 정보는 22-23페이지의 외부 인증 기관 신뢰 참조
사용자에 따라 각기 다른 권한 부여	추가 정보는 19-3페이지의 사용자 지정 사용자 역할로 SSL 검사 구축 관리 참조
정책 변경 사항 저장	**Save**를 클릭합니다.
정책 변경 사항 취소	**Cancel**을 클릭한 다음 이미 변경한 경우에는 **OK**를 클릭합니다.
정책에 규칙 추가	**Add Rule**을 클릭합니다. 자세한 내용은 21-4페이지의 SSL 규칙 이해 및 생성참조 **팁** 어떤 규칙의 행에서 빈 영역을 마우스 오른쪽 버튼으로 클릭하고 **Insert new rule**을 선택할 수도 있습니다.
기존 규칙 수정	규칙 옆의 수정 아이콘( )을 클릭합니다. 자세한 내용은 21-4페이지의 SSL 규칙 이해 및 생성참조 **팁** 규칙을 마우스 오른쪽 버튼으로 클릭하고 **Edit**를 선택할 수도 있습니다.
규칙 삭제	규칙 옆의 삭제 아이콘( )을 클릭한 다음 **OK**를 클릭합니다. **팁** 선택한 규칙의 행에서 빈 영역을 마우스 오른쪽 버튼으로 클릭하고 **Delete**를 선택한 다음 **OK**를 클릭하여 하나 이상의 선택한 규칙을 삭제할 수도 있습니다.

표 20-4 SSL 정책 컨피그레이션 작업(계속)

목적	가능한 작업
기존 규칙 활성화 또는 비활성화	선택한 규칙을 마우스 오른쪽 버튼으로 클릭하고 **State**를 선택한 다음 **Disable** 또는 **Enable**을 선택합니다. 비활성화된 규칙은 회색으로 나타나고 규칙 이름 아래에 (비활성) 상태임이 표시됩니다.
특정 규칙 속성에 대한 컨피그레이션 페이지 표시	규칙의 행, 조건의 열에서 이름, 값 또는 아이콘을 클릭합니다. 이를테면 **Source Networks** 열의 이름이나 값을 클릭하여 선택한 규칙의 Networks 페이지를 표시합니다. 자세한 내용은 22-1페이지의 SSL 규칙을 사용하여 트래픽 해독 조정을/를 참조하십시오.

컨피그레이션을 변경할 때 메시지가 나타나 저장하지 않은 변경 사항이 있음을 알립니다. 변경 사항을 유지하려면 정책 편집기를 종료하기 전에 정책을 저장해야 합니다. 변경 사항을 저장하지 않고 정책 편집기를 종료하려고 할 경우 저장하지 않은 변경 사항이 있다는 주의 메시지가 나타납니다. 이 때, 변경 사항을 취소하고 정책을 종료하거나 정책 편집기로 돌아갈 수 있습니다.

정책 편집기에서 60분간 아무런 활동이 없으면 세션의 개인 정보 보호를 위해 정책의 변경 사항이 취소되고 SSL Policy 페이지로 돌아갑니다. 아무런 활동 없이 최초 30분이 지나면 메시지가 나타나고 이 메시지가 정기적으로 업데이트되면서 변경 사항이 취소될 때까지 남은 시간(분)을 알려줍니다. 해당 페이지에서 어떠한 활동이라도 일어나게 되면 타이머가 취소됩니다.

2개의 브라우저 창에서 동일한 정책을 수정하려고 하면, 새 창에서 수정을 시작하고 원래의 창에서 변경한 사항을 취소한 다음 새 창에서 수정을 계속할지 아니면 2번째 창을 취소하고 정책 편집기로 돌아갈지 묻습니다.

여러 사용자가 동시에 동일한 정책을 수정할 경우 정책 편집기에 메시지가 나타나 정책을 변경하고 저장하지 않은 다른 사용자를 보여줍니다. 변경을 시도하는 사용자에게는 자신의 변경이 다른 사용자의 변경을 덮어쓸 것이라는 주의 메시지가 표시됩니다. 여러 사용자가 동일한 정책을 저장할 경우 마지막으로 저장된 변경 사항이 유지됩니다.

SSL 정책을 수정하려면

액세스: Admin/Access Admin/Network Admin

1단계 **Policies > SSL**을 선택합니다.

SSL Policy 페이지가 나타납니다.

2단계 구성하려는 SSL 정책 옆의 수정 아이콘( )을 클릭합니다.

SSL 정책 편집기 페이지가 나타납니다.

3단계 다음과 같이 선택할 수 있습니다.

- 정책을 구성하기 위해 SSL 정책 컨피그레이션 작업 표에 요약된 작업을 수행할 수 있습니다.
- 정책에서 규칙을 체계화하기 위해 21-12페이지의 정책의 SSL 규칙 관리 표에 설명된 작업을 수행할 수 있습니다.

4단계 컨피그레이션을 저장하거나 취소합니다. 다음과 같이 선택할 수 있습니다.

- 변경 사항을 저장하고 계속 수정하려면 **Save**를 클릭합니다.
- 변경 사항을 취소하려면 **Cancel**을 클릭하고 메시지가 표시되면 **OK**를 클릭합니다.

  변경 사항이 취소되고 SSL Policy 페이지가 나타납니다.

액세스 제어를 사용하여 해독 설정 적용

라이센스: 모두

지원되는 디바이스: Series 3

SSL 정책을 변경한 다음에는 그 정책이 연결된 액세스 제어 정책을 적용해야 합니다. 자세한 내용은 12-15페이지의 액세스 제어 정책 적용을/를 참조하십시오.

SSL 정책을 적용할 때 다음 사항을 유념하십시오.

- 이미 적용되었거나 현재 적용되고 있는 SSL 정책을 삭제할 수 없습니다.
- 액세스 제어 정책을 적용하면 연결된 SSL 정책이 자동으로 적용됩니다. SSL 정책을 독립적으로 적용할 수는 없습니다.

참고 수동 구축에서는 시스템이 트래픽의 플로우에 영향을 줄 수 없습니다. 적용하려는 액세스 제어 정책이 암호화 트래픽을 차단하는 SSL 정책 또는 서버 인증서 재서명으로 트래픽을 해독하도록 구성된 SSL 정책을 참조할 경우 시스템에서 경고를 표시합니다. 또한 수동 구축에서는 DHE(ephemeral Diffie-Hellman) 또는 ECDHE(elliptic curve Diffie-Hellman) 암호화 솔루션으로 암호화된 트래픽의 해독을 지원하지 않습니다.

SSL 정책을 액세스 제어 정책과 연결하려면

액세스: Admin/Security Approver

1단계 **Policies > Access Control**을 선택합니다.

Access Control Policy 페이지가 나타납니다.

2단계 구성하려는 액세스 제어 정책 옆의 수정 아이콘()을 클릭합니다.

액세스 제어 정책 편집기가 나타납니다.

3단계 **Advanced** 탭을 선택합니다.

액세스 제어 정책에 대한 고급 설정이 나타납니다.

4단계 General Settings 옆의 수정 아이콘()을 클릭합니다.

General Settings 팝업 창이 나타납니다.

5단계 **SSL Policy to use for inspecting encrypted connections** 드롭다운에서 SSL 정책을 선택합니다.

6단계 **OK**를 클릭합니다.

액세스 제어 정책에 대한 고급 설정이 나타납니다.

7단계 변경 사항을 저장하려면 **Save**를 클릭합니다.

변경 사항이 적용되려면 액세스 제어 정책을 적용해야 합니다. 12-15페이지의 액세스 제어 정책 적용을/를 참조하십시오.

현재 트래픽 해독 설정에 대한 보고서 생성

라이센스: 모두

SSL 정책 보고서는 특정 시점의 정책 및 규칙 컨피그레이션에 대한 기록입니다. 감사의 목적으로 또는 현재 컨피그레이션을 검사하는 데 이 보고서를 사용할 수 있습니다.

팁 정책을 현재 적용된 정책과 또는 다른 정책과 비교하는 SSL 비교 보고서도 생성할 수 있습니다. 자세한 내용은 20-11페이지의 SSL 정책 비교을/를 참조하십시오.

SSL 정책 보고서는 다음 표에 설명된 섹션으로 구성됩니다.

표 20-5 SSL 정책 보고서 섹션

섹션	설명
Title Page	정책 보고서의 이름, 정책이 마지막으로 수정된 날짜와 시간, 수정한 사용자의 이름을 나타냅니다.
Table of Contents	보고서의 내용에 대해 설명합니다.
Policy Information	정책의 이름과 설명, 마지막으로 정책을 수정한 사용자의 이름, 정책이 마지막으로 수정된 날짜와 시간을 제공합니다.
Default Action	기본 작업을 제공합니다.
Default Logging	기본 연결 로깅 설정을 제공합니다.
Rules	정책에 있는 각 규칙에 대해 규칙 작업과 조건을 규칙 범주별로 제공합니다.
Trusted CA Certificates	탐지된 트래픽이 여기에 있는 CA 인증서 또는 신뢰 체인에 속한 다른 인증서를 통해 암호화된 경우 자동으로 신뢰됩니다.
Undecryptable Actions	탐지되었으나 해독 불가한 트래픽 유형에 대해 수행되는 작업을 제공합니다.
Referenced Objects	정책에 사용되는 모든 개별 객체 및 그룹 객체의 이름과 컨피그레이션을 그 객체가 구성된 조건의 유형(네트워크, VLAN 태그 등)별로 제공합니다.

SSL 정책 보고서를 보려면

액세스: Admin/Access Admin/Network Admin/Security Approver

1단계 **Policies > SSL**을 선택합니다.

SSL Policy 페이지가 나타납니다.

2단계 보고서를 생성할 정책 옆의 보고서 아이콘( )을 클릭합니다. SSL 정책 보고서를 생성하기 전에 모든 변경 사항을 저장해야 합니다. 저장된 변경 사항만 보고서에 나타납니다.

시스템에서 보고서를 생성합니다. 브라우저 설정에 따라 보고서가 팝업 창에 나타날 수 있으며, 컴퓨터에 보고서를 저장하는 프롬프트가 표시될 수도 있습니다.

SSL 정책 비교

라이센스: 모두

조직의 표준을 준수하거나 시스템 성능을 최적화하기 위해 정책 변경 사항을 검토할 경우 두 SSL 정책 간의 차이를 확인할 수 있습니다. 두 정책을 비교하거나 현재 적용된 정책을 다른 정책과 비교할 수 있습니다. 원한다면 비교 후 두 정책의 차이를 기록하는 PDF 보고서를 생성할 수도 있습니다.

정책 비교에 사용할 수 있는 2가지 툴이 있습니다.

- 비교 보기에서는 두 정책의 차이점만 나란히 표시합니다. 각 정책의 이름이 비교 보기의 좌우 제목 표시줄에 나타납니다. 단, **Running Configuration**을 선택할 경우 빈 표시줄에서 현재 활성 상태의 정책을 나타냅니다.

  이를 사용하여 웹 인터페이스에서 그 차이점이 강조 표시된 상태에서 두 정책을 모두 보고 탐색할 수 있습니다.
- 비교 보고서는 두 정책의 차이점에 대해서만 기록을 생성하는데, 그 형식은 정책 보고서와 비슷하긴 하나 PDF 포맷입니다.

  이를 사용하여 향후 점검을 위해 정책 비교를 저장, 복사, 인쇄, 공유할 수 있습니다.

정책 비교 툴을 이해하고 사용하는 것에 대한 자세한 내용은 다음을 참조하십시오.

- 20-11페이지의 SSL 정책 비교 보기 사용
- 20-12페이지의 SSL 정책 비교 보고서 사용

SSL 정책 비교 보기 사용

라이센스: 모두

비교 보기에서는 두 정책을 나란히 표시하며, 각 정책은 비교 보기의 좌우 제목 표시줄에 있는 이름으로 식별됩니다. 실행 중인 컨피그레이션이 아닌 두 정책을 비교할 경우 마지막 수정 시간 및 마지막으로 수정한 사용자가 정책 이름과 함께 표시됩니다. 두 정책의 차이점이 강조 표시됩니다.

- 파란색은 강조 표시된 설정이 두 정책에서 다름을 의미하며, 그 차이점이 빨간색 텍스트로 표시됩니다.
- 녹색은 강조 표시된 설정이 둘 중 한 정책에만 나타남을 의미합니다.

다음 표의 어떤 작업도 수행할 수 있습니다.

표 20-6 SSL 정책 비교 보기의 작업

목적	가능한 작업
개별 변경 사항 탐색	제목 표시줄 위의 **Previous** 또는 **Next**를 클릭합니다. 왼쪽과 오른쪽 사이의 중앙에 있는 이중 화살표 아이콘()이 움직이고 **Difference** 번호가 조정되면서 어떤 차이점을 보고 있는지 나타냅니다.
새 정책 비교 보기 생성	**New Comparison**을 클릭합니다. **Select Comparison** 창이 나타납니다. 자세한 내용은 20-12페이지의 SSL 정책 비교 보고서 사용을/를 참조하십시오.
정책 비교 보고서 생성	**Comparison Report**를 클릭합니다. 정책 비교 보고서에서는 두 정책의 차이점만 나열하는 PDF 문서를 생성합니다.

SSL 정책 비교 보고서 사용

라이센스: 모두

SSL 정책 비교 보고서는 두 SSL 정책 또는 어떤 정책과 정액 비교 보기에 의해 식별되는 현재 적용된 정책의 모든 차이점에 대한 기록이며 PDF 포맷으로 제공됩니다. 두 정책 컨피그레이션의 차이점을 더 자세히 살펴보고 조사 결과를 저장하여 배포하는 데 이 보고서를 사용할 수 있습니다.

액세스 권한이 있는 어떤 SSL 정책에 대해서도 비교 보기에서 정책 비교 보고서를 생성할 수 있습니다. 정책 보고서를 생성하기 전에 모든 변경 사항을 저장해야 합니다. 저장된 변경 사항만 보고서에 나타납니다.

정책 비교 보고서의 형식은 정책 보고서와 동일합니다. 단, 정책 보고서는 정책의 모든 컨피그레이션을 포함하는 것과 달리 정책 비교 보고서는 두 정책에서 달라지는 컨피그레이션만 나열합니다. SSL 정책 비교 보고서는 20-10페이지의 현재 트래픽 해독 설정에 대한 보고서 생성에 설명된 섹션으로 구성됩니다.

팁 액세스 제어, 네트워크 분석, 침입, 파일, 시스템 또는 상태 정책을 비교하는 절차도 비슷합니다.

두 SSL 정책을 비교하려면

액세스: Admin/Access Admin/Network Admin/Security Approver

1단계 **Policies > SSL**을 선택합니다.

SSL Policy가 나타납니다.

2단계 **Compare Policies**를 클릭합니다.

Select Comparison 창이 나타납니다.

3단계 **Compare Against** 드롭다운 목록에서 원하는 비교 유형을 선택합니다.

- 2개의 다른 정책을 비교하려면 **Other Policy**를 선택합니다.

  페이지가 새로 고쳐지고 Policy A 및 Policy B 드롭다운 목록이 나타납니다.
- 다른 정책과 현재 활성 정책을 비교하려면 **Running Configuration**을 선택합니다.

  페이지가 새로 고쳐지고 Target/Running Configuration A 및 Policy B 드롭다운 목록이 나타납니다.

4단계 선택한 비교 유형에 따라 다음을 선택할 수 있습니다.

- 2개의 다른 정책을 비교할 경우 비교할 정책을 Policy A 및 Policy B 드롭다운 목록에서 각각 선택합니다.
- 실행 중인 컨피그레이션을 다른 정책과 비교할 경우 Policy B 드롭다운 목록에서 2번째 정책을 선택합니다.

5단계 **OK**를 클릭하여 정책 비교 보기를 표시합니다.

비교 보기가 나타납니다.

6단계 원한다면 **Comparison Report**를 클릭하여 SSL 정책 비교 보고서를 생성합니다.

SSL 정책 비교 보고서가 나타납니다. 브라우저 설정에 따라 보고서가 팝업 창에 나타날 수 있으며, 컴퓨터에 보고서를 저장하는 프롬프트가 표시될 수도 있습니다.

21장

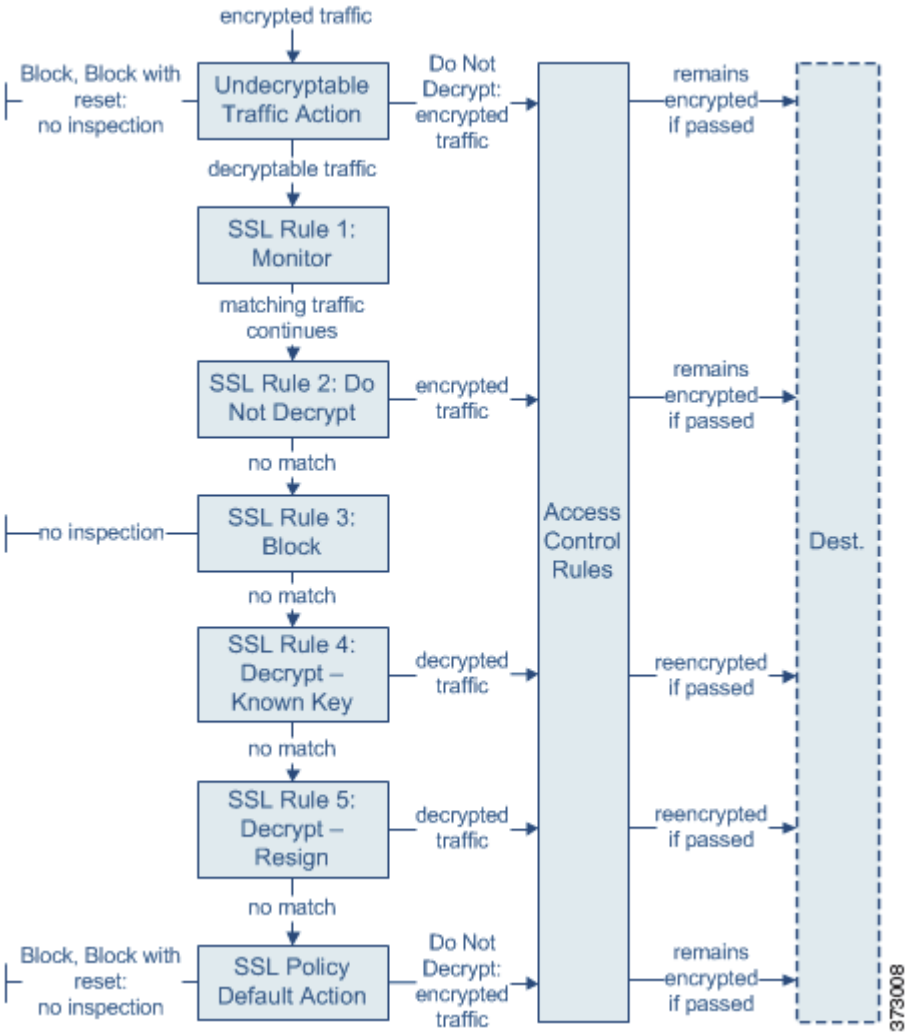
SSL 규칙 시작하기

SSL 정책에서 *SSL 규칙*은 관리되는 여러 디바이스의 전 범위에서 암호화 트래픽을 더 정밀하게 처리할 방법을 제공합니다. 이를테면 추가 검사 없이 트래픽을 차단하거나 트래픽을 해독하지 않고 액세스 제어로 검사하거나 액세스 제어 분석을 위해 트래픽을 해독할 수 있습니다.

사용자가 지정하는 순서대로 트래픽과 SSL 규칙을 매칭합니다. 대개는 이는 *모든* 규칙의 조건이 트래픽과 매칭하는 *제1* SSL 규칙에 따라 암호화 트래픽을 처리합니다. 조건은 단순할 수도 있고, 복잡할 수도 있습니다. 보안 영역, 네트워크 또는 지리적 위치, VLAN, 포트, 애플리케이션, 요청된 URL, 사용자, 인증서, 인증서 DN(distinguished name), 인증서 상태, 암호 그룹(cipher suite) 또는 암호화 프로토콜 버전을 기준으로 트래픽을 제어할 수 있습니다.

각 규칙에는 *작업*도 포함되는데, 이는 매칭하는 트래픽을 모니터링, 차단 또는 액세스 제어로 검사할지 여부를 결정합니다. 매칭하는 트래픽을 해독한 후에 이러한 작업을 수행하게 할 수도 있습니다. 암호화 트래픽을 차단한 경우 더 이상 검사하지 **않습니다**. 암호화된 트래픽과 해독 불가 트래픽은 액세스 제어로 검사합니다. 그러나 일부 액세스 제어 규칙 조건은 암호화되지 않은 트래픽을 요구하므로, 암호화 트래픽이 더 적은 수의 규칙과 매칭할 수도 있습니다. 또한 암호화 페이로드는 기본적으로 침입 및 파일 검사가 비활성화되어 있습니다.

다음 시나리오는 인라인 구축에서 SSL 규칙이 트래픽을 처리하는 방식을 요약한 것입니다.



이 시나리오에서는 다음과 같이 트래픽이 평가됩니다.

- **Undecryptable Traffic Action**은 암호화 트래픽을 먼저 평가합니다. 시스템에서 해독할 수 없는 트래픽의 경우 추가 검사 없이 차단하거나 액세스 제어 검사를 위해 전달합니다. 매칭하지 않는 암호화 트래픽은 다음 규칙으로 진행합니다.
- **SSL Rule 1: Monitor**가 그다음에 암호화 트래픽을 평가합니다. 모니터 규칙은 암호화 트래픽을 추적하고 로깅하지만 트래픽 플로우에 영향을 주지 않습니다. 계속해서 추가 규칙과 트래픽을 매칭하여 허용할지 아니면 거부할지 결정합니다.
- **SSL Rule 2: Do Not Decrypt**가 세 번째로 암호화 트래픽을 평가합니다. 매칭하는 트래픽은 해독되지 않습니다. 이 트래픽을 액세스 제어로 검사하지만, 파일 또는 침입 검사는 하지 않습니다. 매칭하지 않는 트래픽은 다음 규칙으로 진행합니다.
- **SSL Rule 3: Block**에서 네 번째로 암호화 트래픽을 평가합니다. 매칭하는 트래픽은 추가 검사 없이 차단됩니다. 매칭하지 않는 트래픽은 다음 규칙으로 진행합니다.

- **SSL Rule 4: Decrypt - Known Key**에서 다섯 번째로 암호화 트래픽을 평가합니다. 네트워크에 수신된 매칭 트래픽은 업로드된 개인 키를 사용하여 해독됩니다. 그런 다음 해독된 트래픽은 액세스 제어 규칙에 따라 평가됩니다. 액세스 제어 규칙은 해독된 트래픽과 암호화되지 않은 트래픽을 동일하게 처리합니다. 이 추가 검사의 결과에 따라 트래픽을 차단할 수 있습니다. 나머지 모든 트래픽은 다시 암호화된 후에 목적지로 갈 수 있습니다. 이 SSL 규칙과 매칭하지 않는 트래픽은 다음 규칙으로 진행합니다.
- **SSL Rule 5: Decrypt - Resign**이 최종 규칙입니다. 트래픽이 이 규칙과 매칭할 경우 시스템은 서버 인증서를 업로드된 CA 인증서로 다시 서명한 다음 중간자(man-in-the-middle) 역할을 하면서 트래픽을 해독합니다. 그런 다음 해독된 트래픽은 액세스 제어 규칙에 따라 평가됩니다. 액세스 제어 규칙은 해독된 트래픽과 암호화되지 않은 트래픽을 동일하게 처리합니다. 이 추가 검사의 결과에 따라 트래픽을 차단할 수 있습니다. 나머지 모든 트래픽은 다시 암호화된 후에 목적지로 갈 수 있습니다. 이 SSL 규칙과 매칭하지 않는 트래픽은 다음 규칙으로 진행합니다.
- **SSL Policy Default Action**은 어떤 SSL 규칙과도 매칭하지 않는 모든 트래픽을 처리합니다. 이 기본 작업은 암호화 트래픽을 추가 검사 없이 차단하거나 해독하지 않고 액세스 제어 검사를 위해 전달합니다.

자세한 내용은 다음 절을 참조하십시오.

- 21-3페이지의 지원 검사 정보 구성
- 21-4페이지의 SSL 규칙 이해 및 생성
- 21-12페이지의 정책의 SSL 규칙 관리

지원 검사 정보 구성

라이센스: 모두

암호화 세션 특성을 기반으로 암호화 트래픽을 제어하고 암호화 트래픽을 해독하려면 재사용 가능한 PKI(public key infrastructure) 객체를 생성해야 합니다. SSL 정책에 신뢰받는 CA(certificate authority) 인증서를 업로드하고 SSL 규칙 조건을 생성하는 시점에 이 정보를 추가하여 해당 객체를 생성할 수 있습니다. 그러나 이 객체를 미리 구성하면 잘못된 객체가 생성될 가능성이 줄어듭니다.

인증서 및 쌍 키를 사용하여 암호화 트래픽 해독

세션 암호화에 쓰이는 서버 인증서와 개인 키를 업로드하여 내부 인증서 객체를 구성할 경우 수신되는 암호화 트래픽을 해독할 수 있습니다. **Decrypt - Known Key** 작업의 규칙에서 객체를 참조하고 트래픽이 그 규칙과 매칭할 경우 업로드된 개인 키를 사용하여 세션을 해독합니다.

또한 CA 인증서와 개인 키를 업로드하여 내부 CA 객체를 구성할 경우 발신 트래픽을 해독할 수 있습니다. **Decrypt - Resign** 작업의 규칙에서 객체를 참조하고 트래픽이 그 규칙과 매칭할 경우 클라이언트 브라우저에 전달된 서버 인증서에 다시 서명하고 중간자로서 세션을 해독합니다.

자세한 내용은 다음을 참조하십시오.

- 3-51페이지의 내부 인증서 객체 작업
- 3-43페이지의 내부 인증 기관 객체 작업

암호화 세션 특성 기반의 트래픽 제어

세션 협상에 사용된 암호 그룹 또는 서버 인증서를 기반으로 암호화 트래픽을 제어할 수 있습니다. 다양한 재사용 가능 객체 중 하나를 구성하고 SSL 규칙 조건에서 그 객체를 참조하여 트래픽과 매칭할 수 있습니다. 다음 표에서는 구성할 수 있는 재사용 가능 객체의 여러 유형에 대해 설명합니다.

다음을 구성할 경우	다음 조건을 기반으로 암호화 트래픽 제어 가능
하나 이상의 암호 그룹을 포함한 암호 그룹 목록 구성	암호화 세션의 협상에 사용된 암호 그룹이 암호 그룹 목록에 있는 암호 그룹과 매칭합니다.
조직에서 신뢰하는 CA 인증서를 업로드하는 방법으로 신뢰받는 CA 객체 구성	다음 조건에서 신뢰받는 CA가 세션 암호화에 사용된 서버 인증서를 신뢰합니다. • CA가 직접 인증서를 발급한 경우 • CA가 중개 CA에 인증서를 발급했고, 이 중개 CA가 서버 인증서를 발급한 경우
서버 인증서를 업로드하는 방법으로 외부 인증서 객체 구성	세션 암호화에 사용된 서버 인증서가 업로드된 서버 인증서와 매칭합니다.
인증서 주체 또는 발급자 DN을 포함하는 DN 객체	세션 암호화에 사용된 인증서의 주체 또는 발급자 CN(common name), 국가, 조직 또는 조직 단위가 구성된 DN과 매칭합니다.

자세한 내용은 다음을 참조하십시오.

- 3-40페이지의 암호 그룹 목록 작업
- 3-48페이지의 신뢰받는 인증 기관 객체 작업
- 3-50페이지의 외부 인증 기관 객체 작업
- 3-41페이지의 DN 객체 작업

SSL 규칙 이해 및 생성

라이센스: 모두

지원되는 디바이스: Series 3

SSL 정책에서 SSL 규칙은 여러 관리 대상 디바이스의 전 범위에서 네트워크 트래픽을 처리하는 세부적인 방법을 제공합니다. 각 SSL 규칙은 고유한 이름과 함께 다음과 같은 기본 구성 요소를 갖습니다.

상태

기본적으로 규칙은 활성화되어 있습니다. 어떤 규칙을 비활성화할 경우 네트워크 트래픽 평가에 이를 사용하지 않으며 그 규칙에 대한 경고 및 오류는 더 이상 생성되지 않습니다.

위치

SSL 정책의 규칙은 1부터 시작하여 번호가 지정됩니다. 하향식, 규칙 번호 오름차순으로 트래픽을 규칙에 매칭합니다. 모니터 규칙을 제외하고 트래픽이 매칭하는 첫 번째 규칙은 그 트래픽을 처리하는 규칙입니다.

조건

규칙에서 처리하는 구체적인 트래픽을 지정합니다. 조건에서는 보안 영역, 네트워크 또는 지리적 위치, VLAN, 포트, 애플리케이션, 요청된 URL, 사용자, 인증서, 인증서 주체 또는 발급자, 인증서 상태, 암호 그룹 또는 암호화 프로토콜 버전을 기준으로 트래픽을 매칭할 수 있습니다. 조건은 단순하거나 복잡할 수 있습니다. 그 용도는 대상 디바이스 라이센스에 따라 달라질 수 있습니다.

작업

규칙의 작업은 매칭하는 트래픽을 처리하는 방식을 결정합니다. 매칭하는 트래픽을 모니터링, 신뢰, 차단하거나 해독할 수 있습니다. 해독된 트래픽은 추가 조사의 대상이 됩니다. 차단되었거나 신뢰받는 암호화 트래픽에 대해서는 검사를 수행하지 **않습니다**.

로깅

규칙의 로깅 설정은 처리되는 트래픽에 관한 지속적인 기록에 적용됩니다. 규칙과 매칭하는 트래픽에 대해 기록할 수 있습니다. SSL 정책의 설정에 따라 암호화 세션이 차단되거나 조사 없이 전달될 때 연결을 로깅할 수 있습니다. 또한 추후 어떻게 트래픽을 처리하거나 조사하든지 상관없이 액세스 제어 규칙에 따른 추가 평가를 위해 해독된 연결을 반드시 로깅하게 할 수도 있습니다. 방어 센터 데이터베이스뿐 아니라 시스템 로그(syslog) 또는 SNMP 트랩 서버에 연결을 로깅할 수 있습니다.

팁 올바르게 SSL 규칙을 생성하고 순서를 지정하는 것은 복잡한 일이지만, 효과적인 구축에 필수적입니다. 신중하게 정책을 계획하지 않으면 규칙이 다른 규칙보다 선점하거나 추가 라이센스를 필요로 하거나 잘못된 컨피그레이션을 포함하게 될 수 있습니다. 트래픽이 예상대로 처리되는지 확인할 수 있도록 SSL 정책 인터페이스는 규칙에 대한 강력한 경고 및 오류 피드백 시스템을 갖추고 있습니다. 자세한 내용은 21-16페이지의 SSL 규칙의 문제 해결을/를 참조하십시오.

SSL 규칙을 생성하거나 수정하려면

액세스: Admin/Access Admin/Network Admin

1단계 **Policies > SSL**을 선택합니다.

SSL Policy 페이지가 나타납니다.

2단계 규칙을 추가하려는 SSL 정책 옆의 수정 아이콘()을 클릭합니다.

SSL 정책 편집기가 나타나며 Rules 탭에 포커스가 있습니다.

3단계 다음 옵션을 이용할 수 있습니다.

- 새 규칙을 추가하려면 **Add Rule**을 클릭합니다.
- 기존 규칙을 수정하려면 수정하려는 규칙 옆의 수정 아이콘()을 클릭합니다.

SSL 규칙 편집기가 나타납니다.

4단계 규칙의 **Name**을 입력합니다.

각 규칙에는 고유한 이름이 있어야 합니다. 공백과 특수 문자(콜론(:) 제외)를 포함하여 최대 30자의 인쇄 가능 문자로 지정할 수 있습니다.

5단계 위에 요약된 규칙 구성 요소를 구성합니다. 다음을 구성하거나 기본값을 적용할 수 있습니다.

- 규칙이 **Enabled** 상태인지의 여부를 지정합니다.
- 규칙 위치를 지정합니다. 21-6페이지의 SSL 규칙의 평가 순서 지정을/를 참조하십시오.
- 규칙의 **Action**을 선택합니다. 21-8페이지의 규칙 작업을 사용하여 암호화 트래픽 처리 및 조사 결정을/를 참조하십시오.

- 규칙의 조건을 구성합니다. 21-7페이지의 규칙에서 처리하는 암호화 트래픽 지정에 조건 사용을/를 참조하십시오.
- **Logging** 옵션을 지정합니다. 38-13페이지의 SSL 규칙으로 해독 가능 연결 로깅을/를 참조하십시오.

6단계 규칙을 저장하려면 **Save**를 클릭합니다.

SSL 정책이 연결된 액세스 제어 정책을 적용해야 변경사항이 적용됩니다. 12-15페이지의 액세스 제어 정책 적용을/를 참조하십시오.

SSL 규칙의 평가 순서 지정

라이센스: 모두

지원되는 디바이스: Series 3

SSL 규칙을 처음 생성할 때 규칙 편집기에서 **Insert** 드롭다운 목록을 사용하여 그 위치를 지정합니다. SSL 정책의 SSL 규칙은 1부터 시작하여 번호가 지정됩니다. 하향식, 규칙 번호 오름차순으로 트래픽을 SSL 규칙에 매칭합니다.

대개는 이는 *모든* 규칙의 조건이 트래픽과 매칭하는 *제1* SSL 규칙에 따라 네트워크 트래픽을 처리합니다. (트래픽을 로깅하지만 트래픽 플로우에 영향을 주지 않는) 모니터 규칙의 경우를 제외하고, 트래픽이 어떤 규칙과 매칭한 후에는 **더 이상** 더 낮은 우선 순위의 추가 규칙에 매칭하여 트래픽을 평가하지 않습니다.

팁 SSL 규칙 순서가 올바르면 네트워크 트래픽 처리에 필요한 리소스가 줄어들면서 규칙 선점이 방지됩니다. 생성하는 규칙은 각 조직과 구축에서 고유하지만, 규칙의 순서를 정할 때 몇 가지 일반 지침을 따름으로써 요구 사항을 해결하면서 성능도 최적화할 수 있습니다. 자세한 내용은 21-19페이지의 성능 향상 및 선점 방지를 위한 SSL 규칙 순서 지정을/를 참조하십시오.

번호를 기준으로 규칙의 순서를 지정할 뿐 아니라 범주를 기준으로 규칙을 그룹화할 수 있습니다. 기본적으로 관리자(Administrator), 표준(Standard), 루트(Root)의 3가지 범주가 제공됩니다. 사용자 지정 범주를 추가할 수 있으나, 시스템에서 제공한 범주를 삭제하거나 그 순서를 변경할 수는 없습니다. 기존 규칙의 위치 또는 범주를 변경하는 것에 대한 자세한 내용은 21-14페이지의 SSL 규칙의 위치 또는 범주 변경을/를 참조하십시오.

규칙을 수정하거나 생성하는 동안 범주에 규칙을 추가하려면

액세스: Admin/Access Admin/Network Admin

1단계 SSL 규칙 편집기의 **Insert** 드롭다운 목록에서 **Into Category**를 선택한 다음 사용할 범주를 선택합니다.

규칙을 저장하면 해당 범주의 마지막에 위치합니다.

규칙을 수정하거나 생성하는 동안 번호를 기준으로 규칙의 위치를 지정하려면

액세스: Admin/Access Admin/Network Admin

1단계 SSL 규칙 편집기의 **Insert** 드롭다운 목록에서 **above rule** 또는 **below rule**을 선택하고 알맞은 규칙 번호를 입력합니다.

규칙을 저장하면 지정한 곳에 위치합니다.

규칙에서 처리하는 암호화 트래픽 지정에 조건 사용

라이센스: 기능에 따라

지원되는 디바이스: Series 3

SSL 규칙의 조건은 규칙에서 처리하는 암호화 트래픽의 유형을 식별합니다. 조건은 단순하거나 복잡할 수 있으며, 하나의 규칙에 둘 이상의 조건 유형을 지정할 수 있습니다. 트래픽이 규칙의 모든 조건을 충족해야 규칙이 트래픽에 적용됩니다.

어떤 규칙에 대해 조건을 구성하지 않을 경우 그 기준에 따른 트래픽 매칭은 이루어지지 않습니다. 예를 들어 인증서 조건이 있지만 버전 조건이 없는 규칙은 세션 SSL 또는 TLS 버전과 무관하게 세션 협상에 쓰인 서버 인증서를 기반으로 트래픽을 평가합니다.

SSL 규칙을 추가하거나 수정할 때 규칙 편집기의 왼쪽 아래에 있는 탭을 사용하여 규칙 조건을 추가하고 수정합니다. SSL 규칙에 추가할 수 있는 조건에 대해서는 다음 표에서 설명합니다.

표 21-1 SSL 규칙 조건 유형

조건	암호화 트래픽 매칭	세부 사항
Zones	특정 보안 영역에서 인터페이스를 통해 디바이스에 들어오거나 나가는 암호화 트래픽과 매칭	보안 영역은 구축 및 보안 정책에 따라 하나 이상의 인터페이스를 논리적으로 그룹화한 것입니다. 어떤 영역의 인터페이스가 여러 디바이스에 분산될 수도 있습니다. 영역 조건을 작성하려면 22-2페이지의 암호화된 트래픽을 네트워크 영역으로 제어을/를 참조하십시오.
Networks	그 소스 또는 목적지 IP 주소, 국가 또는 대륙을 기준으로 매칭	명시적으로 IP 주소를 지정할 수 있습니다. 이 지오로케이션 기능으로 소스 또는 목적지 국가나 대륙을 기반으로 트래픽을 제어하는 것도 가능합니다. 네트워크 조건을 작성하려면 22-4페이지의 암호화된 트래픽을 네트워크 또는 지리적 위치로 제어을/를 참조하십시오.
VLAN Tags	VLAN 태그가 지정된 암호화 트래픽과 매칭	가장 안쪽의 VLAN 태그를 사용하여 VLAN을 기준으로 패킷을 식별합니다. VLAN 연결을 작성하려면 22-5페이지의 암호화된 VLAN 트래픽 제어를 참조하십시오.
Ports	그 소스 또는 목적지 포트를 기준으로 매칭	TCP 포트를 기반으로 암호화 트래픽을 제어할 수 있습니다. 포트 조건을 작성하려면 22-7페이지의 암호화된 트래픽을 포트로 제어을/를 참조하십시오.
Users	세션에 참여한 사용자를 기준으로 매칭	모니터링되는 암호화 세션에 쓰인 호스트에 로그인한 LDAP 사용자를 기반으로 암호화 트래픽을 제어할 수 있습니다. Microsoft Active Directory Server에서 가져온 개별 사용자 또는 그룹을 기반으로 트래픽을 제어할 수 있습니다. 사용자 조건을 작성하려면 22-8페이지의 암호화된 트래픽을 사용자에 따라 제어을/를 참조하십시오.

표 21-1 SSL 규칙 조건 유형(계속)

조건	암호화 트래픽 매칭	세부 사항
Applications	세션에서 탐지된 애플리케이션을 기준으로 매칭	암호화 세션에서 개별 애플리케이션에 대한 액세스를 제어하거나 유형, 위험, 비즈니스 연관성, 범주와 같은 기본 특성에 따라 액세스를 필터링할 수 있습니다. 애플리케이션 조건을 작성하려면 22-10페이지의 암호화된 트래픽을 애플리케이션에 따라 제어을/를 참조하십시오.
Categories	인증서 주제 DN을 기반으로 하여 세션에서 요청된 URL을 기준으로 매칭	URL의 일반 분류 및 위험 레벨을 기반으로 네트워크 사용자가 액세스 가능한 웹 사이트를 제한할 수 있습니다. URL 조건을 작성하려면 22-15페이지의 암호화된 트래픽을 URL 카테고리 및 평판으로 제어을/를 참조하십시오.
Distinguished Names	암호화 세션의 협상에 쓰이는 서버 인증서의 주체 또는 발급자 DN을 기준으로 매칭	서버 인증서를 발급한 CA 또는 서버 인증서 소유자를 기반으로 암호화 트래픽을 제어할 수 있습니다. DN 조건을 작성하려면 22-19페이지의 암호화된 트래픽을 인증서 고유 이름으로 제어을/를 참조하십시오.
Certificates	암호화 세션의 협상에 쓰이는 서버 인증서를 기준으로 매칭	암호화 세션의 협상을 위해 사용자의 브라우저에 전달된 서버 인증서를 기반으로 암호화 트래픽을 제어할 수 있습니다. 인증서 조건을 작성하려면 22-23페이지의 암호화된 트래픽을 인증서 상태로 제어을/를 참조하십시오.
Certificate Status	암호화 세션의 협상에 쓰이는 서버 인증서의 속성을 기준으로 매칭	서버 인증서의 상태를 기반으로 암호화 트래픽을 제어할 수 있습니다. 인증서 상태 조건을 작성하려면 22-23페이지의 암호화된 트래픽을 인증서 상태로 제어을/를 참조하십시오.
Cipher Suites	암호화 세션의 협상에 쓰이는 암호 그룹을 기준으로 매칭	서버에서 암호화 세션의 협상을 위해 선택한 암호 그룹을 기반으로 암호화 트래픽을 제어할 수 있습니다. 암호 그룹 조건을 작성하려면 22-27페이지의 암호화된 트래픽을 암호 그룹으로 제어을/를 참조하십시오.
Versions	세션 암호화에 쓰이는 SSL 또는 TLS 버전을 기준으로 매칭	세션 암호화에 쓰이는 SSL 또는 TLS 버전을 기반으로 암호화 트래픽을 제어할 수 있습니다. 버전 조건을 작성하려면 22-28페이지의 트래픽을 암호화 프로토콜 버전으로 제어을/를 참조하십시오.

Series 3 디바이스에서 암호화 트래픽을 제어하고 검사할 수 있지만 탐지된 애플리케이션, URL 범주 또는 사용자를 통한 트래픽 제어에는 추가 라이센스가 필요합니다. 또한 지나치게 복잡한 규칙은 과도한 리소스를 사용할 수 있으며, 그로 인해 정책을 적용하지 못할 수도 있습니다. 자세한 내용은 21-16페이지의 SSL 규칙의 문제 해결을/를 참조하십시오.

규칙 작업을 사용하여 암호화 트래픽 처리 및 조사 결정

라이센스: 모두

지원되는 디바이스: Series 3

모든 SSL 규칙에는 매칭하는 암호화 트래픽에 대해 다음 사항을 결정하는 작업이 있습니다.

- 처리 — 무엇보다도 이 규칙 작업은 시스템에서 규칙의 조건과 매칭하는 암호화 트래픽을 모니터링, 신뢰, 차단 또는 해독할지 여부를 결정합니다.
- 로깅 — 이 규칙 작업은 매칭하는 암호화 트래픽의 세부사항을 로깅할 수 있는 시점과 그 방법을 결정합니다.

SSL 검사 컨피그레이션에서 해독된 트래픽을 처리, 검사, 로깅합니다.

- SSL 정책의 해독 불가 작업은 시스템에서 해독할 수 없는 트래픽을 처리합니다. 20-5페이지의 해독 불가 트래픽에 대한 기본 처리 설정을/를 참조하십시오.
- 정책의 기본 작업은 모니터 외 SSL 규칙의 조건을 충족하지 않는 트래픽을 처리합니다. 20-4페이지의 암호화 트래픽에 대한 기본 처리 및 검사 설정을/를 참조하십시오.

암호화 세션이 차단되거나 신뢰받을 때 연결 이벤트를 로깅할 수 있습니다. 또한 추후 어떻게 트래픽을 처리하거나 조사하든지 상관없이 액세스 제어 규칙에 따른 추가 평가를 위해 해독된 연결을 반드시 로깅하게 할 수도 있습니다. 암호화 세션의 연결 로그는 세션 암호화에 사용된 인증서와 같은 해독 세부 사항이 포함되어 있습니다. 그러나 연결 종료 이벤트만 로깅할 수 있습니다.

- 차단된 연결(Block, Block with reset)의 경우 즉시 세션을 종료하고 이벤트를 생성합니다.
- 신뢰하는 연결(Do not decrypt)의 경우 세션 종료 시 이벤트를 생성합니다.

규칙 작업 및 이 작업이 처리와 로깅에 미치는 영향에 대한 자세한 내용은 다음 절을 참조하십시오.

- 21-9페이지의 Monitor Action: Postponing Action and Ensuring Logging
- 21-9페이지의 Do Not Decrypt Action: Passing Encrypted Traffic Without Inspection
- 21-10페이지의 Blocking Actions: Blocking Encrypted Traffic Without Inspection
- 21-10페이지의 Decrypt Actions: Decrypting Traffic for Further Inspection
- 21-12페이지의 정책의 SSL 규칙 관리

Monitor Action: Postponing Action and Ensuring Logging

라이센스: 모두

지원되는 디바이스: Series 3

Monitor 작업은 암호화 트래픽 플로우에 영향을 주지 않습니다. 매칭하는 트래픽은 당장 허용되거나 거부되지 않습니다. 그 대신 추가 규칙이 있을 경우 그와 매칭하여 트래픽을 신뢰, 차단, 해독할지 여부를 결정합니다. 첫 번째로 매칭하는 비 모니터 규칙은 트래픽 플로우 및 추가 검사를 결정합니다. 다른 매칭 규칙이 없을 경우 기본 작업을 사용합니다.

모니터 규칙의 주 목적은 네트워크 트래픽을 추적하는 것이므로 모니터링되는 트래픽에 대해 연결 종료 이벤트를 자동으로 로깅합니다. 즉 나중에 연결을 처리하는 규칙 또는 기본 작업의 로깅 컨피그레이션과 무관하게 항상 연결의 종료를 방어 센터 데이터베이스에 로깅합니다. 따라서 어떤 패킷이 모니터 규칙과 매칭할 경우, 패킷이 다른 어떤 규칙과도 매칭하지 않고 기본 작업에서 로깅을 활성화하지 않았더라도 그 연결은 항상 로깅됩니다.

Do Not Decrypt Action: Passing Encrypted Traffic Without Inspection

라이센스: 모두

지원되는 디바이스: Series 3

Do not decrypt 작업은 액세스 제어 정책의 규칙 및 기본 작업을 통한 평가를 위해 암호화 트래픽을 전달합니다. 일부 액세스 제어 규칙 조건은 암호화되지 않은 트래픽을 요구하므로 이 트래픽이 더 적은 수의 규칙과 매칭할 수도 있습니다. 암호화 트래픽에 대해서는 침입 또는 파일 검사와 같은 심층 검사를 수행할 수 없습니다.

Blocking Actions: Blocking Encrypted Traffic Without Inspection

라이센스: 모두

지원되는 디바이스: Series 3

Block 및 **Block with reset** 작업은 액세스 제어 규칙 작업인 차단 및 차단 후 초기화와 유사합니다. 이 작업은 클라이언트 및 서버가 SSL 암호화 세션을 설정하고 암호화 트래픽을 전달하는 것을 막습니다. 차단 후 초기화 규칙은 연결도 초기화합니다.

차단된 암호화 트래픽에 대해서는 구성된 응답 페이지를 표시하지 않습니다. 그 대신 금지된 URL을 요청하는 사용자는 연결이 초기화되거나 시간 초과됩니다. 자세한 내용은 16-17페이지의 차단된 URL에 대한 사용자 지정 웹 페이지 표시을/를 참조하십시오.

팁 패시브 또는 인라인(탭 모드) 구축에서는 디바이스에서 직접 트래픽을 검사하지 않으므로 차단 또는 차단 후 초기화 작업을 사용할 수 없습니다. 차단 또는 차단 후 초기화 작업의 규칙을 생성할 경우 여기에 보안 영역 조건의 패시브 또는 인라인(탭 모드) 인터페이스가 포함된다면 정책 편집기는 해당 규칙의 옆에 경고 아이콘(⚠)을 표시합니다.

Decrypt Actions: Decrypting Traffic for Further Inspection

라이센스: 모두

지원되는 디바이스: Series 3

해독 - 확인된 키(**Decrypt - Known Key**) 및 해독 - 재서명(**Decrypt - Resign**) 작업은 암호화 트래픽을 해독합니다. 해독된 트래픽은 액세스 제어 검사를 받습니다. 액세스 제어 규칙은 해독된 트래픽과 암호화되지 않은 트래픽을 동일하게 처리합니다. 검색 데이터를 위해 조사하고 침입, 금지된 파일, 악성코드를 탐지하여 차단할 수 있습니다. 허용된 트래픽은 다시 암호화되어 목적지에 전달됩니다.

Decrypt - Known Key 작업을 구성할 때 하나 이상의 서버 인증서 및 쌍 개인 키를 이 작업과 연결할 수 있습니다. 트래픽이 규칙과 매칭할 경우 트래픽 암호화에 쓰이는 인증서가 해당 작업과 연결된 인증서와 매칭한다면 알맞은 개인 키를 사용하여 세션 암호화 및 해독 키를 얻습니다. 개인 키에 대한 액세스 권한이 있어야 하므로 이 작업은 조직에서 제어하는 서버에서 수신하는 트래픽의 해독에 가장 적합합니다.

또한 하나의 CA 인증서와 개인 키를 **Decrypt - Resign** 작업에 연결할 수 있습니다. 트래픽이 이 규칙과 매칭할 경우 시스템은 서버 인증서를 CA 인증서로 다시 서명한 다음 중간자(man-in-the-middle) 역할을 합니다. 클라이언트와 관리 대상 디바이스 간, 관리 대상 디바이스와 서버 간에 각각 하나씩 2개의 SSL 세션을 생성합니다. 각 세션은 암호화 세션 세부사항이 서로 다르며, 시스템에서 트래픽을 해독하고 다시 암호화하는 것을 허용합니다. 이 작업은 발신 트래픽에 더 적합합니다. 인증서의 개인 키를 자신이 제어하는 키로 대체하여 세션 키를 얻기 때문입니다.

서버 인증서를 다시 서명하면 인증서의 공개 키를 CA 인증서 공개 키로 대체하거나 전체 인증서를 대체하게 됩니다. 일반적으로 전체 서버 인증서를 대체할 경우 클라이언트 브라우저는 SSL 연결 설정 시 신뢰받는 CA가 인증서를 서명하지 않았다고 경고합니다. 그러나 클라이언트 브라우저가 정책에서 해당 CA를 신뢰할 경우 인증서가 신뢰받지 않았음을 경고하지 않습니다. 원래의 서버 인증서가 자체 서명된 경우 전체 인증서를 대체하고 재서명 CA를 신뢰하지만, 사용자의 브라우저는 인증서가 자체 서명되었음을 경고하지 않습니다. 그러한 경우 서버 인증서 공개 키만 대체하면 클라이언트 브라우저가 자체 서명된 인증서임을 경고합니다.

Decrypt - Resign 작업으로 규칙을 구성할 경우 이 규칙은 구성된 규칙 조건과 더불어 참조된 내부 CA 인증서의 서명 알고리즘 유형을 기반으로 트래픽을 매칭합니다. CA 인증서를 **Decrypt - Resign** 작업과 연결하므로, 서로 다른 서명 알고리즘으로 암호화된 여러 발신 트래픽 유형을 해독하는 SSL 규칙을 생성할 수 없습니다. 또한 규칙에 추가하는 외부 인증서 객체와 암호 그룹은 연결된 CA 인증서 암호화 알고리즘 유형과 매칭해야 합니다.

예를 들어 EC(elliptic curve) 알고리즘으로 암호화된 발신 트래픽은 작업에서 EC 기반 CA 인증서를 참조할 때만 **Decrypt - Resign** 규칙과 매칭합니다. 인증서 및 암호 그룹 규칙 조건을 생성하려면 EC 기반 외부 인증서와 암호 그룹을 규칙에 추가해야 합니다. 또한 RSA 기반 CA 인증서를 참조하는 **Decrypt - Resign** 규칙은 RSA 알고리즘으로 암호화된 발신 트래픽만 매칭합니다. EC 알고리즘으로 암호화된 발신 트래픽은 구성된 다른 모든 규칙 조건에 매칭하더라도 이 규칙과 매칭하지 않습니다.

다음에 유의하십시오.

- SSL 연결 설정에 사용된 암호 그룹이 DHE(Diffie-Hellman ephemeral) 또는 ECDHE(elliptic curve Diffie-Hellman ephemeral) 키 교환 알고리즘 중 하나를 적용할 경우 패시브 구축에 **Decrypt - Known Key** 작업을 사용할 수 없습니다. SSL 정책이 패시브 또는 인라인(탭 모드) 인터페이스 디바이스를 대상으로 하고 DHE 또는 ECDHE 암호 그룹을 포함하는 암호 그룹 조건의 **Decrypt - Known Key** 규칙이 있을 경우, 규칙 옆에 정보 아이콘( )이 표시됩니다. 패시브 또는 인라인(탭 모드) 인터페이스가 있는 SSL 규칙에 향후 영역 조건이 추가될 경우 경고 아이콘( )이 표시됩니다.
- 패시브 또는 인라인(탭 모드) 구축에서는 디바이스가 직접 트래픽을 검사하지 않으므로 **Decrypt - Resign** 작업을 사용할 수 없습니다. 보안 영역 내에 패시브 또는 인라인(탭 모드) 인터페이스가 있는 **Decrypt - Resign** 작업으로 규칙을 생성할 경우 정책 편집기는 규칙 옆에 경고 아이콘( )을 표시합니다. SSL 정책이 패시브 또는 인라인(탭 모드) 인터페이스가 있는 디바이스를 대상으로 하고 **Decrypt - Resign** 규칙을 포함할 경우 규칙 옆에 정보 아이콘( )이 표시됩니다. 패시브 또는 인라인(탭 모드) 인터페이스가 있는 SSL 규칙에 향후 영역 조건이 추가될 경우 경고 아이콘( )이 표시됩니다. Decrypt - Resign 규칙이 있는 SSL 정책을 패시브 또는 인라인(탭 모드) 인터페이스가 있는 디바이스에 적용할 경우 그 규칙과 매칭하는 모든 SSL 세션이 실패합니다.
- 클라이언트가 서버 인증서 재서명에 쓰이는 CA를 신뢰하지 않을 경우 신뢰할 수 없는 인증서임을 사용자에게 경고합니다. 이를 방지하려면 클라이언트가 신뢰하는 CA 저장소에 CA 인증서를 가져오십시오. 또는 조직에 개인 PKI가 있을 경우, 조직의 모든 클라이언트가 자동으로 신뢰하는 루트 CA에 의해 서명된 중간 CA 인증서를 발급한 다음 그 CA 인증서를 디바이스에 업로드할 수 있습니다.
- 익명 암호 그룹으로 암호화한 트래픽은 해독할 수 없습니다. **Cipher Suite** 조건에 익명 암호 그룹을 추가할 경우 **Decrypt - Resign**과 **Decrypt - Known Key** 작업 모두 사용할 수 없습니다.
- 클라이언트와 관리 대상 디바이스의 사이에 HTTP 프록시가 위치하고 클라이언트와 서버가 CONNECT HTTP 메서드를 사용하여 터널링된 SSL 연결을 설정할 경우 시스템에서 트래픽을 해독할 수 없습니다. 시스템에서 이 트래픽을 처리하는 방법은 **핸드셰이크 오류** 해독 불가 작업에 의해 결정됩니다. 자세한 내용은 20-5페이지의 해독 불가 트래픽에 대한 기본 처리 설정을/를 참조하십시오.
- **Decrypt - Known Key** 작업으로 SSL 규칙을 생성할 때 **Distinguished Name** 또는 **Certificate** 조건에서 매칭할 수 없습니다. 이 규칙이 트래픽과 매칭할 경우 인증서, 주체 DN, 발급자 DN이 규칙과 연결된 인증서와 이미 매칭한다고 전제합니다. 자세한 내용은 21-8페이지의 규칙 작업을 사용하여 암호화 트래픽 처리 및 조사 결정을/를 참조하십시오.
- 내부 CA 객체를 생성하고 CSR(certificate signing request) 생성을 선택할 경우, 서명된 인증서를 객체에 업로드해야 **Decrypt - Resign** 작업에 이 CA를 사용할 수 있습니다. 자세한 내용은 3-46페이지의 새로운 서명된 인증서 가져오기 및 업로드을/를 참조하십시오.

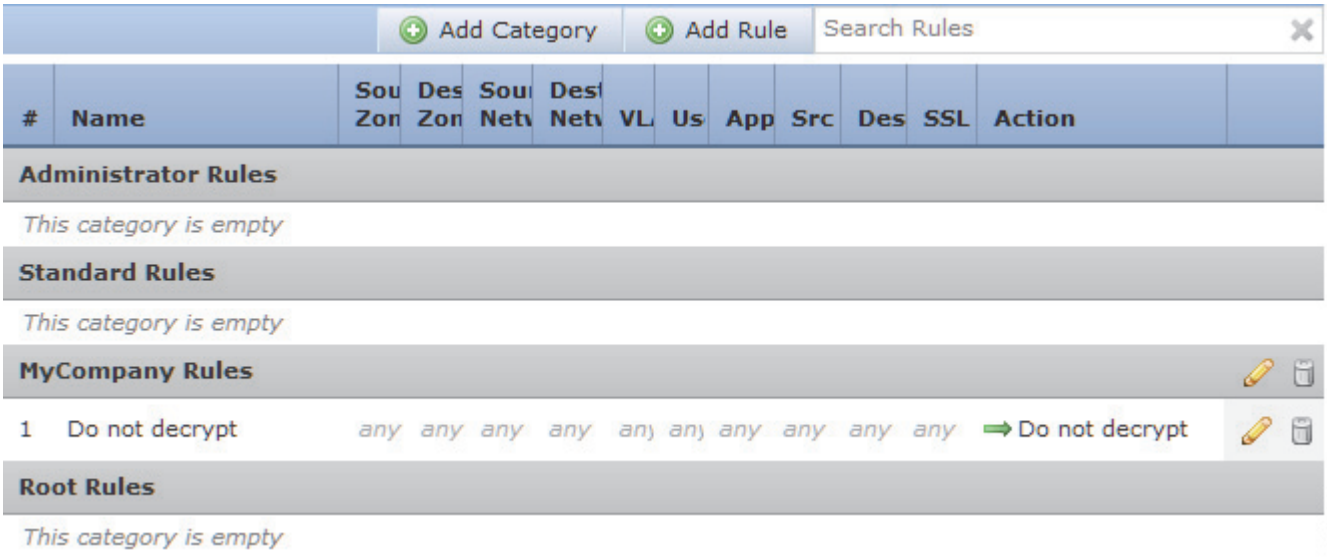
- **Decrypt - Resign** 작업으로 규칙을 구성한 경우 하나 이상의 외부 인증서 객체나 암호 그룹에서 서명 알고리즘 유형 불일치가 있다면 정책 편집기는 규칙 옆에 정보 아이콘( )을 표시합니다. 모든 외부 인증서 객체 또는 모든 암호 그룹에 대해 서명 알고리즘 유형을 잘못 매칭할 경우, 정책은 규칙 옆에 경고 아이콘( )을 표시하며 SSL 정책과 연결된 액세스 제어 정책을 적용할 수 없습니다. 자세한 내용은 22-21페이지의 암호화된 트래픽을 인증서로 제어및 22-27페이지의 암호화된 트래픽을 암호 그룹으로 제어을/를 참조하십시오.
- 해독된 트래픽이 **Interactive Block** 또는 **Interactive Block with reset** 작업의 액세스 제어 규칙과 매칭할 경우, 매칭 연결이 상호 작용 없이 차단되며 시스템에서 응답 페이지를 표시하지 **않았습니다**.
- 인라인 표준화 프리프로세서에서 **Normalize Excess Payload** 옵션을 활성화할 경우, 프리프로세서가 해독된 트래픽을 표준화할 때 어떤 패킷을 삭제하고 잘린 패킷으로 대체할 수 있습니다. 그로 인해 SSL 세션이 종료되지 않습니다. 트래픽이 허용될 경우 잘린 패킷이 SSL 세션의 일환으로 암호화됩니다. 이 옵션에 대한 자세한 내용은 29-7페이지의 인라인 트래픽 표준화을/를 참조하십시오.

정책의 SSL 규칙 관리

라이센스: 모두

지원되는 디바이스: Series 3

다음 그림에서 보여주는 SSL 정책 편집기의 Rules 탭에서는 정책 내의 SSL 규칙을 추가, 수정, 검색, 이동, 활성화, 비활성화, 삭제하고 그 밖의 방식으로 관리할 수 있습니다.



정책 편집기는 각 규칙에 대해 그 이름, 조건의 요약, 규칙 작업을 표시합니다. 아이콘은 경고, 오류, 기타 중요한 정보를 나타냅니다. 비활성화된 규칙은 회색으로 나타나고 규칙 이름 아래에 (비활성) 상태임이 표시됩니다. 아이콘에 대한 자세한 내용은 21-16페이지의 SSL 규칙의 문제 해결을/를 참조하십시오.

SSL 규칙 관리에 대한 자세한 내용은 다음을 참조하십시오.

- 21-13페이지의 SSL 규칙 검색
- 21-14페이지의 SSL 규칙 활성화 및 비활성화
- 21-14페이지의 SSL 규칙의 위치 또는 범주 변경

SSL 규칙 검색

라이센스: 모두

지원되는 디바이스: Series 3

공백, 인쇄 가능 특수 문자 등이 포함된 영숫자 문자열을 사용하여 SSL 규칙의 목록에서 매칭하는 값을 찾을 수 있습니다. 이 검색에서는 규칙 이름과 규칙에 추가된 모든 규칙 조건을 검사합니다. 규칙 조건의 경우 각 조건 유형(영역, 네트워크, 애플리케이션 등)에 대해 추가할 수 있는 어떤 이름이나 값도 매칭합니다. 여기에는 개별 객체 이름 또는 값, 그룹 객체 이름, 그룹에 속한 개별 객체 이름 또는 값, 리터럴 값 등이 포함됩니다.

전체 또는 부분 검색 문자열을 사용할 수 있습니다. 매칭하는 규칙 각각에서 매칭하는 값의 열이 하이라이트됩니다. 예를 들어 문자열 `100Bao`의 전체 또는 일부를 검색할 경우 100Bao 애플리케이션을 추가한 각 규칙의 Applications 열만큼은 하이라이트됩니다. `100Bao`라는 이름의 규칙도 있다면 Name 및 Applications 열 모두 하이라이트됩니다.

매칭하는 이전 규칙 또는 다음 규칙 각각으로 이동할 수 있습니다. 상태 메시지는 현재 매칭 항목 및 총 매칭 항목 수를 표시합니다.

다중 페이지 규칙 목록의 어떤 페이지에서도 매칭 항목이 나타날 수 있습니다. 첫 번째 매칭이 첫 페이지에 없을 경우 첫 번째 매칭이 일어나는 페이지가 표시됩니다. 마지막 매칭에서 다음 매칭을 선택하면 첫 번째 매칭으로 이동하고, 첫 번째 매칭에서 이전 매칭을 선택하면 마지막 매칭으로 이동합니다.

규칙을 검색하려면

액세스: Admin/Access Admin/Network Admin

1단계 검색하려는 정책의 SSL 정책 편집기에서 **Search Rules** 프롬프트를 클릭하고 검색 문자열을 입력한 다음 Enter를 누릅니다. Tab 키를 사용하거나 빈 페이지 영역을 클릭하여 검색을 시작할 수도 있습니다.

매칭하는 값이 있는 규칙의 열이 하이라이트되고, 해당 (첫 번째) 매칭은 색다르게 하이라이트됩니다.

2단계 관심 있는 규칙을 찾으십시오.

- 매칭하는 규칙 사이를 이동하려면 다음 매칭(▼) 또는 이전 매칭(▲) 아이콘을 클릭합니다.
- 페이지를 새로 고치고 검색 문자열 및 모든 하이라이트를 지우려면 지우기 아이콘(✖)을 클릭합니다.

SSL 규칙 활성화 및 비활성화

라이센스: 모두

지원되는 디바이스: Series 3

SSL 규칙을 생성하면 기본적으로 활성화됩니다. 어떤 규칙을 비활성화할 경우 네트워크 트래픽 평가에 이를 사용하지 않으며 그 규칙에 대한 경고 및 오류는 더 이상 생성되지 않습니다. SSL 정책에서 규칙의 목록을 볼 때 비활성화된 규칙은 회색으로 표시됩니다. 단, 이 규칙은 수정 가능합니다. 규칙 편집기를 사용하여 SSL 규칙을 활성화하거나 비활성화할 수도 있습니다. 21-4페이지의 SSL 규칙 이해 및 생성을/를 참조하십시오.

SSL 규칙의 상태를 변경하려면

액세스: Admin/Access Admin/Network Admin

1단계 활성화하거나 비활성화할 규칙이 있는 정책의 SSL 정책 편집기에서 마우스 오른쪽 버튼으로 규칙을 클릭하고 규칙 상태를 선택합니다.

- 비활성 규칙을 활성화하려면 **State > Enable**을 선택합니다.
- 활성 규칙을 비활성화하려면 **State > Disable**을 선택합니다.

2단계 정책을 저장하려면 **Save**를 클릭합니다.

SSL 정책이 연결된 액세스 제어 정책을 적용해야 변경사항이 적용됩니다. 12-15페이지의 액세스 제어 정책 적용을/를 참조하십시오.

SSL 규칙의 위치 또는 범주 변경

라이센스: 모두

지원되는 디바이스: Series 3

SSL 규칙의 체계화를 위해 모든 SSL 정책에는 시스템에서 제공한 3가지 규칙 범주가 있습니다. 관리자 규칙(Administrator Rules), 표준 규칙(Standard Rules), 루트 규칙(Root Rules)입니다. 이 범주는 이동, 삭제, 이름 변경이 불가하지만, 사용자 지정 범주를 생성할 수는 있습니다.

기본적으로 SSL 정책의 수정을 허용하는 사전 정의 사용자 역할은 규칙 범주 내에서 또는 다른 규칙 범주로 SSL 규칙을 이동하고 수정하는 것도 허용합니다. 그러나 사용자의 규칙 이동 및 수정을 제한하는 사용자 지정 역할을 생성할 수 있습니다.

자세한 내용은 다음 링크를 참조하십시오.

- 21-15페이지의 SSL 규칙 이동
- 21-15페이지의 새 SSL 규칙 범주 추가

SSL 규칙 이동

라이센스: 모두

지원되는 디바이스: Series 3

SSL 규칙 순서가 올바르면 네트워크 트래픽 처리에 필요한 리소스가 줄어들면서 규칙 선점이 방지됩니다. 기본적으로 SSL 정책의 수정을 허용하는 사전 정의 사용자 역할은 규칙 범주 내에서 또는 다른 규칙 범주로 SSL 규칙을 이동하는 것도 허용합니다. 그러나 사용자가 시스템 제공 범주에서 규칙 이동을 허용하지 않는 사용자 지정 역할을 생성할 수 있습니다.

다음 절차에서는 SSL 정책 편집기를 사용하여 하나 이상의 규칙을 한꺼번에 이동하는 방법을 설명합니다. 규칙 편집기를 사용하여 개별 SSL 규칙을 이동할 수도 있습니다. 21-4페이지의 SSL 규칙 이해 및 생성을/를 참조하십시오.

규칙을 이동하려면

액세스: Admin/Access Admin/Network Admin

1단계 이동하려는 규칙이 있는 정책의 SSL 정책 편집기에서 각 규칙의 빈 영역을 클릭하여 규칙을 선택합니다. Ctrl 및 Shift 키를 사용하여 여러 규칙을 선택할 수 있습니다.

선택한 규칙이 하이라이트됩니다.

2단계 규칙을 이동합니다. 잘라내어 붙여넣기 또는 끌어서 놓기가 가능합니다.

규칙을 잘라내어 새 위치에 붙여넣으려면 선택한 규칙을 마우스 오른쪽 버튼을 클릭하고 **Cut**을 선택합니다. 그런 다음 잘라낸 규칙을 붙여넣을 공간 옆에 있는 빈 영역에서 마우스 오른쪽 버튼을 클릭한 다음 **Paste above** 또는 **Paste below**를 선택합니다. SSL 규칙을 복사하여 다른 SSL 정책에 붙여넣을 수는 없습니다.

3단계 정책을 저장하려면 **Save**를 클릭합니다.

SSL 정책이 연결된 액세스 제어 정책을 적용해야 변경사항이 적용됩니다. 12-15페이지의 액세스 제어 정책 적용을/를 참조하십시오.

새 SSL 규칙 범주 추가

라이센스: 모두

지원되는 디바이스: Series 3

SSL 규칙의 체계화를 위해 모든 SSL 정책에는 시스템에서 제공한 3가지 규칙 범주가 있습니다. 관리자 규칙, 표준 규칙, 루트 규칙입니다. 이 범주는 이동, 삭제, 이름 변경이 불가하지만, 표준 규칙과 루트 규칙의 사이에 사용자 지정 범주를 생성할 수 있습니다.

사용자 지정 범주를 추가하면 정책을 추가로 생성하지 않고도 더 체계적으로 규칙을 관리할 수 있습니다. 사용자가 추가한 범주는 이름 변경 및 삭제가 가능합니다. 이 범주를 이동할 수는 없지만 여기로 규칙을 이동하거나 범주 내에서 이동하거나 범주 바깥으로 이동할 수는 있습니다.

사용자가 시스템 제공 범주에서 규칙을 이동하고 수정할 수 없게 하는 사용자 지정 역할을 생성할 수 있는데, 이는 해당 역할에 추가되는 사용자 권한을 기반으로 합니다. 자세한 내용은 61-56페이지의 사용자 계정 권한을/를 참조하십시오.

새 범주를 추가하려면

액세스: Admin/Access Admin/Network Admin

1단계 규칙 범주를 추가하려는 정책의 SSL 정책 편집기에서 **Add Category**를 클릭합니다.

팁 정책에 이미 규칙이 있을 경우 기존 규칙 행의 빈 영역을 클릭하여 새 범주의 위치를 설정한 다음 추가할 수 있습니다. 또한 기존 규칙을 마우스 오른쪽 버튼으로 클릭한 다음 **Insert new category**를 선택합니다.

Add Category 팝업 창이 나타납니다.

2단계 고유한 범주 **Name**을 입력합니다.

공백과 인쇄 가능한 특수 문자를 포함한 영숫자를 사용하여 최대 30자까지 입력할 수 있습니다.

3단계 다음과 같이 선택할 수 있습니다.

- 기존 범주의 바로 위에 새 범주를 배치하려면 첫 번째 **Insert** 드롭다운 목록에서 **above Category**를 선택하고 두 번째 드롭다운 목록에서는 규칙이 위치할 곳의 아래에 있는 범주를 선택합니다.
- 기존 규칙의 아래에 새 범주를 배치하려면 드롭다운 목록에서 **below rule**을 선택한 다음 기존 규칙 번호를 입력합니다. 이 옵션은 하나 이상의 규칙이 정책에 있는 경우에만 사용 가능합니다.
- 기존 규칙의 위에 규칙을 배치하려면 드롭다운 목록에서 **above rule**을 선택한 다음 기존 규칙 번호를 입력합니다. 이 옵션은 하나 이상의 규칙이 정책에 있는 경우에만 사용 가능합니다.

4단계 **OK**를 클릭합니다.

범주가 추가되었습니다. 사용자 지정 범주의 옆에 있는 수정 아이콘( )을 클릭하여 이름을 수정하거나 삭제 아이콘( )을 클릭하여 범주를 삭제할 수 있습니다. 삭제하는 범주의 규칙은 그 위에 있는 범주에 추가됩니다.

5단계 정책을 저장하려면 **Save**를 클릭합니다.

SSL 규칙의 문제 해결

라이센스: 모두

지원되는 디바이스: Series 3

올바르게 SSL 규칙을 생성하고 순서를 지정하는 것은 복잡한 일이지만, 효과적인 구축에 필수적입니다. 신중하게 정책을 계획하지 않으면 규칙이 다른 규칙보다 선점하거나 추가 라이센스를 필요로 하거나 잘못된 컨피그레이션을 포함하게 될 수 있습니다. 트래픽이 예상대로 처리되는지 확인할 수 있도록 SSL 정책 인터페이스는 규칙에 대한 강력한 경고 및 오류 피드백 시스템을 갖추고 있습니다.

다음 표에서 설명하는 것처럼 각 규칙에 대해 정책 편집기의 아이콘이 경고와 오류를 표시합니다. 아이콘 위에 포인터를 놓으면 경고, 오류 또는 정보 텍스트를 읽을 수 있습니다.

표 21-2 SSL 오류 아이콘

아이콘	설명	세부 사항
	경고	해당 사안에 따라 규칙 또는 기타 경고를 표시하는 SSL 정책의 적용이 가능할 수도 있습니다. 그러한 경우 잘못 구성된 설정은 아무런 영향을 주지 않습니다. 예를 들어 선점당한 규칙은 절대 트래픽을 평가하지 않습니다. 그러나 경고 아이콘이 라이센싱 오류 또는 모델 불일치를 표시할 경우 문제를 해결해야 정책을 적용할 수 있습니다. 경고가 표시된 규칙을 비활성화할 경우 경고 아이콘이 사라집니다. 근본적인 문제를 해결하지 않고 규칙을 활성화할 경우 다시 나타납니다.
	오류	어떤 규칙이나 기타 SSL 정책 컨피그레이션에 오류가 있을 경우 문제를 해결해야 정책을 적용할 수 있습니다.
	정보	정보 아이콘은 트래픽 플로우에 영향을 줄 수 있는 컨피그레이션에 대한 유익한 정보를 전달합니다. 이 사안은 사소한 것이며 정책 적용을 막지 않습니다.

SSL 규칙을 제대로 구성하면 네트워크 트래픽 처리에 필요한 리소스도 절약할 수 있습니다. 복잡한 규칙이 생성되고 규칙의 순서가 잘못되면 성능에 영향을 줄 수 있습니다.

자세한 내용은 다음 링크를 참조하십시오.

- 21-17페이지의 SSL 규칙 경고 및 오류 이해
- 21-18페이지의 규칙 선점 및 잘못된 컨피그레이션 경고 이해
- 21-19페이지의 성능 향상 및 선점 방지를 위한 SSL 규칙 순서 지정

SSL 규칙 경고 및 오류 이해

라이센스: 기능에 따라

지원되는 디바이스: Series 3

어떤 라이센스에서도 SSL 규칙을 생성할 수 있지만, 일부 규칙 조건과 검사 옵션은 대상 디바이스에 대한 특정 라이센스 기능을 활성화해야 사용 가능합니다. 라이센스 기능을 사용하는 정책을 라이센스가 없는 디바이스에 적용할 수 없습니다. 경고 아이콘과 확인 대화 상자를 통해 라이센스 없는 기능을 표시합니다. 자세한 내용은 경고 아이콘 위에 포인터를 두면 확인할 수 있습니다.

다음 표에서는 SSL 규칙을 사용하기 위해 갖춰야 할 라이센스에 대해 설명합니다.

표 21-3 SSL 규칙의 라이센스 요구 사항

사용할 규칙	라이센스	지원되는 방어 센터	지원되는 디바이스
영역, 네트워크, VLAN, 포트, 인증서, DN, 인증서 상태, 암호 그룹 또는 버전 조건	모두	모두	Series 3
지오로케이션 데이터를 사용하는 네트워크 조건	FireSIGHT	DC500을 제외하고 모두	Series 3
애플리케이션 또는 사용자 조건	제어	모두. 단, DC500은 사용자 제어를 수행할 수 없음	Series 3
URL 범주 및 평판 데이터를 사용하는 범주 조건	URL 필터링	DC500을 제외하고 모두	Series 3

규칙 선점 및 잘못된 컨피그레이션 경고 이해

라이센스: 모두

지원되는 디바이스: Series 3

효과적인 구축을 위해서는 SSL 규칙을 올바르게 구성하고 그 순서를 지정해야 합니다. SSL 정책 내에서 SSL 규칙이 다른 규칙보다 선점하거나 잘못된 컨피그레이션을 포함할 수 있습니다. 경고 및 오류 아이콘을 사용하여 이러한 사안을 표시합니다.

규칙 선점 경고 이해

어떤 SSL 규칙의 조건 때문에 후속 규칙이 트래픽과 매칭하지 않을 수 있습니다. 예를 들면 다음과 같습니다.

```
Rule 1: do not decrypt Administrators
Rule 2: block Administrators
```

첫 번째 규칙이 이미 트래픽을 허용했기 때문에 두 번째 규칙은 트래픽을 차단하지 못합니다.

어떤 유형의 규칙 조건도 후속 규칙보다 선점할 수 있습니다. 예를 들어 아래의 첫 번째 규칙에 있는 VLAN 범위는 두 번째 규칙의 VLAN을 포함하므로 첫 번째 규칙이 두 번째 규칙보다 선점한 것입니다.

```
Rule 1: do not decrypt VLAN 22-33
Rule 2: block VLAN 27
```

다음 예에서는 어떤 VLAN도 구성되지 않았기 때문에 Rule 1이 모든 VLAN과 매칭합니다. 따라서 Rule 1은 VLAN 2와의 매칭을 시도하는 Rule 2보다 선점합니다.

```
Rule 1: do not decrypt Source Network 10.4.0.2/16
Rule 2: do not decrypt Source Network 10.4.0.2/16, VLAN 2
```

또한 어떤 규칙은 동일한 후속 규칙, 즉 구성된 모든 조건이 동일한 규칙보다 선점합니다. 예를 들면 다음과 같습니다.

```
Rule 1: do not decrypt VLAN 1 URL www.example.com
Rule 2: do not decrypt VLAN 1 URL www.example.com
```

조건 중 하나라도 다르면 후속 규칙이 선점당하지 않습니다. 예를 들면 다음과 같습니다.

```
Rule 1: do not decrypt VLAN 1 URL www.example.com
Rule 2: do not decrypt VLAN 2 URL www.example.com
```

잘못된 컨피그레이션 경고 이해

SSL 정책에 적용되는 외부 설정이 달라질 수 있으므로, 유효했던 SSL 정책 설정이 무효화될 수도 있습니다. 예를 들면,

- URL 범주 조건을 포함한 규칙은 URL 필터링 라이센스가 없는 디바이스를 대상으로 하면 무효화될 수 있습니다. 그러면 규칙 옆에 오류 아이콘이 나타나며, 규칙을 수정 또는 삭제하거나 정책의 대상을 다시 지정하거나 알맞은 라이센스를 활성화해야 그 디바이스에 정책을 적용할 수 있습니다.
- Decrypt-Resign 규칙을 생성했다가 나중에 패시브 인터페이스가 있는 보안 영역을 영역 조건에 추가할 경우 그 규칙 옆에 경고 아이콘이 표시됩니다. 패시브 구축에서는 인증서 재서명으로 트래픽을 해독할 수 없으므로, 규칙에서 패시브 인터페이스를 제거하거나 규칙 작업을 변경하지 않는 한 규칙은 아무 효력이 없습니다.
- 어떤 규칙에 사용자를 추가한 다음 LDAP 사용자 인식 설정을 변경하여 그 사용자를 제외할 경우, 해당 사용자가 액세스 제어 사용자에서 제외되지 않는 한 규칙은 아무 효력이 없습니다.

성능 향상 및 선점 방지를 위한 SSL 규칙 순서 지정

라이센스: 모두

지원되는 디바이스: Series 3

SSL 정책의 규칙은 1부터 시작하여 번호가 지정됩니다. 하향식, 규칙 번호 오름차순으로 트래픽을 규칙에 매칭합니다. 모니터 규칙을 제외하고 트래픽이 매칭하는 첫 번째 규칙은 그 트래픽을 처리하는 규칙입니다.

SSL 규칙 순서가 올바르면 네트워크 트래픽 처리에 필요한 리소스가 줄어들면서 규칙 선점이 방지됩니다. 생성하는 규칙은 각 조직과 구축에서 고유하지만, 규칙의 순서를 정할 때 몇 가지 일반 지침을 따름으로써 요구 사항을 해결하면서 성능도 최적화할 수 있습니다.

중요도순 규칙 순서 지정

무엇보다도 조직의 필요에 맞게 규칙의 순서를 지정해야 합니다. 모든 트래픽에 적용해야 하는 우선적인 규칙은 정책의 맨 위 근처에 배치합니다. 예를 들어 어떤 단일 사용자의 발신 트래픽을 추가 분석을 위해 해독하지만(Decrypt-Resign 규칙 사용) 해당 부서의 다른 모든 사용자의 트래픽은 해독하지 않을 경우(Do not decrypt 규칙 사용) 두 SSL 규칙을 이 순서로 배치합니다.

구체적인 규칙부터 배치

구체적인 규칙, 즉 처리하는 트래픽을 한정하는 규칙을 앞에 배치하여 성능을 향상할 수 있습니다. 또한 광범위한 조건의 규칙이 다양한 트래픽 유형과 매칭할 수 있어 나중에 나오는 더 구체적인 규칙보다 선점할 가능성이 있다는 점에서 중요합니다.

예를 들어 신뢰받는 CA(Good CA)에서 악성 엔티티(Bad CA)에 CA 인증서를 잘못 발급했지만 아직 그 인증서를 폐기하지 않았습니다. 신뢰받지 않는 CA에서 발급한 인증서로 암호화된 트래픽을 차단하되 신뢰받는 CA의 신뢰 체인에 속한 트래픽은 허용하려 합니다. CA 인증서와 모든 중간 CA 인증서를 업로드하고 다음과 같이 규칙의 순서를 지정해야 합니다.

```
Rule 1: Block issuer CN=www.badca.com
Rule 2: Do not decrypt issuer CN=www.goodca.com
```

규칙의 순서가 바뀔 경우

```
Rule 1: Do not decrypt issuer CN=www.goodca.com
Rule 2: Block issuer CN=www.badca.com
```

첫 번째 규칙이 Good CA에서 신뢰한 모든 트래픽과 매칭하는데, 여기에는 Bad CA에서 신뢰한 트래픽도 포함됩니다. 어떤 트래픽도 두 번째 규칙과 매칭하지 않으므로 악성 트래픽이 차단되지 않고 허용될 수 있습니다.

트래픽을 해독하는 규칙을 나중에 배치

트래픽 해독에는 처리 리소스가 필요하므로 트래픽을 해독하지 않는 규칙(Do not decrypt, Block)을 해독하는 규칙(Decrypt-Known Key, Decrypt-Resign)보다 앞에 배치함으로써 성능을 향상할 수 있습니다. 이는 트래픽 해독에 상당한 리소스가 필요할 수 있기 때문입니다. 또한 차단(Block) 규칙은 다른 상황에서 해독했거나 검사했을 트래픽을 막을 수 있습니다. 다른 변수가 동일하다는 전제하에 중요도가 더 높은 규칙도 없고 규칙 선점도 일어나지 않는다면 다음 순서대로 규칙을 배치해 보십시오.

- 매칭하는 연결을 로깅하지만 트래픽에 다른 어떤 작업도 수행하지 않는 Monitor 규칙
- 추가 검사 없이 트래픽을 차단하는 Block 규칙
- 암호화 트래픽을 해독하지 않는 Do not decrypt 규칙
- 확인된 개인 키로 수신 트래픽을 해독하는 Decrypt-Known Key 규칙
- 서버 인증서를 재서명하여 발신 트래픽을 해독하는 Decrypt-Resign 규칙

성능 향상을 위한 SSL 검사 구성

라이센스: 모두

지원되는 디바이스: Series 3

복잡한 SSL 정책과 규칙 때문에 많은 리소스가 필요할 수 있습니다. SSL 정책을 적용할 때 모든 규칙을 한꺼번에 평가한 다음 확장 기준 모음을 생성하고, 대상 디바이스에서 이를 사용하여 네트워크 트래픽을 평가합니다. 대상 디바이스에서 지원하는 최대 SSL 규칙 수를 초과했다는 경고 팝업 창이 나타날 수 있습니다. 이 최대 한도는 디바이스의 물리적 메모리, 프로세서 수 등 여러 변수에 따라 달라집니다.

규칙 간소화

다음 지침에 따라 SSL 규칙을 간소화하고 성능을 향상할 수 있습니다.

- 규칙을 작성할 때 조건에 포함되는 개별 요소를 최소화하십시오. 예를 들어 네트워크 조건에서는 개별 IP 주소보다는 IP 주소 영역을 사용합니다. 포트 조건에서는 포트 범위를 사용합니다. 애플리케이션 필터, URL 범주 및 평판을 사용하여 애플리케이션 제어 및 URL 필터링을 수행하고, LDAP 사용자 그룹을 사용하여 사용자 제어를 수행합니다.

  여러 요소를 객체로 통합한 다음 SSL 규칙 조건에 이를 사용하더라도 성능이 향상되지 않습니다. 예를 들어 50개의 개별 IP 주소를 포함하는 네트워크 객체를 사용할 경우 이 IP 주소를 각각 조건에 포함하는 것에 비해 더 체계적인 관리가 가능하겠지만 성능이 향상되지는 않습니다.
- 가급적 보안 영역으로 규칙을 제한하십시오. 어떤 디바이스의 인터페이스가 영역 제한 규칙의 어떤 영역에도 속하지 않을 경우 이 규칙은 이 디바이스의 성능에 영향을 주지 않습니다.
- 규칙을 과다하게 구성하지 마십시오. 처리하려는 트래픽을 매칭하는 데 조건 하나로 충분하다면 2개를 사용하지 마십시오.

트래픽 해독 구성

트래픽 해독을 구성할 때 다음 지침을 기억하십시오.

- 트래픽 해독에는 처리 리소스가 필요하며 액세스 제어 검사를 수행해야 합니다. 광범위한 해독 규칙보다는 집중된 해독 규칙을 생성하여 해독할 트래픽의 양을 줄이십시오. 그러면 트래픽 해독에 필요한 처리 리소스도 절약됩니다. 트래픽을 해독한 후에 액세스 제어 규칙을 사용하여 허용하거나 차단하기보다는 가급적 트래픽을 차단하거나 암호화 트래픽 해독 안 함을 선택하십시오.
- 루트 발급자 CA를 기반으로 트래픽을 신뢰하는 인증서 상태 조건을 구성할 경우 루트 CA 인증서 및 루트 CA 신뢰 체인에 속한 모든 중간 CA 인증서를 SSL 정책에 업로드하십시오. 신뢰받는 CA 신뢰 체인의 모든 트래픽은 불필요하게 해독하지 않고 허용할 수 있습니다.

22장

SSL 규칙을 사용하여 트래픽 해독 조정

기본적인 SSL 규칙은 디바이스에서 검사된 모든 암호화된 트래픽에 자체적인 규칙 작업을 적용합니다. 암호화된 트래픽의 제어 및 해독을 개선하기 위해, 특정 유형의 트래픽을 처리하고 로깅하도록 규칙 조건을 구성할 수 있습니다. 각 SSL 규칙에는 0, 1 또는 추가적인 규칙 조건을 포함할 수 있습니다. 트래픽이 SSL 규칙의 모든 조건과 매칭될 경우 규칙은 해당 트래픽만 매칭합니다.

참고 트래픽이 규칙과 매칭될 경우, 디바이스는 구성 규칙 작업을 트래픽에 적용합니다. 트래픽 로깅이 구성되어 있는 경우 연결이 종료될 때 디바이스는 트래픽을 로깅합니다. 자세한 내용은 21-8페이지의 규칙 작업을 사용하여 암호화 트래픽 처리 및 조사 결정 및 38-12페이지의 암호화 연결 로깅을/를 참조하십시오.

각 규칙 조건을 사용하면 매칭하려는 트래픽의 속성을 하나 이상 지정할 수 있으며, 이러한 속성에는 다음에 대한 세부 정보가 포함됩니다.

- 트래픽의 흐름 - 트래픽이 이동할 때 통과하는 보안 영역, IP 주소 및 포트, 원본 또는 대상 국가, 원본 또는 대상 VLAN 포함
- 탐지된 IP 주소와 연결된 사용자
- 트래픽 페이로드 - 트래픽에서 탐지된 애플리케이션 포함
- 연결 암호화 - 연결을 암호화하는 데 사용되는 SSL/TLS 프로토콜 버전, 암호 그룹, 서버 인증서 포함
- 서버 인증서의 고유 이름에 지정된 URL의 카테고리 및 평판

자세한 내용은 다음 절을 참조하십시오.

- 38-13페이지의 SSL 규칙으로 해독 가능 연결 로깅
- 22-2페이지의 암호화된 트래픽을 네트워크 기반 조건으로 제어
- 22-9페이지의 암호화된 트래픽을 평판으로 제어
- 22-19페이지의 암호화 속성을 기준으로 트래픽 제어

암호화된 트래픽을 네트워크 기반 조건으로 제어

라이센스: 모든

지원되는 디바이스: Series 3

SSL 정책 내의 SSL *규칙*은 암호화된 트래픽 로깅 및 처리에 대한 세부적인 제어를 수행합니다. 네트워크 기반 조건을 활용하면 다음 조건 중 하나를 사용하여, 어떤 암호화된 트래픽이 네트워크를 통과할 수 있는지 관리가 가능합니다.

- 소스 및 대상 보안 영역
- 소스 및 대상 IP 주소 또는 지리적 위치
- 패킷의 가장 안쪽의 VLAN 태그
- 소스 및 대상 포트

네트워크 기반 조건을 서로 조합하고 다른 유형의 조건과 조합하여 SSL 규칙을 생성할 수 있습니다. 이러한 SSL 규칙은 간단하거나 복잡할 수 있으며, 여러 조건을 사용하여 트래픽을 매칭하고 검사합니다. SSL 규칙에 대한 자세한 내용은 21-1페이지의 SSL 규칙 시작하기을/를 참조하십시오.

자세한 내용은 다음 절을 참조하십시오.

- 22-2페이지의 암호화된 트래픽을 네트워크 영역으로 제어
- 22-4페이지의 암호화된 트래픽을 네트워크 또는 지리적 위치로 제어
- 22-5페이지의 암호화된 VLAN 트래픽 제어
- 22-7페이지의 암호화된 트래픽을 포트로 제어

암호화된 트래픽을 네트워크 영역으로 제어

라이센스: 모든

지원되는 디바이스: Series 3

SSL 규칙의 영역 조건을 사용하면 소스 및 대상 보안 영역에 따라 암호화된 트래픽을 제어할 수 있습니다.

*보안 영역*은 여러 디바이스 전반에 걸쳐 있을 수 있는 하나 이상의 인터페이스를 그룹화한 것입니다. 디바이스의 초기 설정 과정에서 선택하게 되는 *탐지 모드*라는 옵션은 시스템이 처음에 디바이스의 인터페이스를 구성하는 방법 및 이러한 인터페이스가 보안 영역에 속하는지 여부를 결정합니다.

간단한 예를 들자면, **Inline** 탐지 모드로 디바이스를 등록할 경우 방어 센터에서는 Internal 및 External이라는 두 개의 영역을 생성하며, 디바이스에 있는 인터페이스의 첫 번째 쌍을 해당 영역에 할당합니다. Internal 측의 네트워크에 연결된 호스트는 보호받는 자산을 나타냅니다.

이 시나리오를 확장하려는 경우, 동일하게 구성되고 동일한 방어 센터에서 관리되는 추가 디바이스를 구축하여 여러 다른 위치에 있는 유사한 리소스를 보호할 수 있습니다. 첫 번째 디바이스와 마찬가지로, 이러한 각 디바이스는 Internal 보안 영역의 자산을 보호합니다.

팁 내부(또는 외부) 인터페이스를 단일한 영역으로 그룹화할 필요가 없습니다. 해당하는 구축 및 보안 정책에 맞는 그룹화 방법을 선택합니다. 영역 생성에 대한 자세한 내용은 3-38페이지의 보안 영역 작업을/를 참조하십시오.

이 구축 시나리오의 경우, 호스트가 인터넷에 무제한으로 액세스하도록 결정할 수 있으나, 그럼에도 불구하고 수신되는 암호화된 트래픽을 해독 및 검사하여 이러한 호스트를 보호하고자 할 것입니다.

SSL 검사로 이를 구현하려면 **Destination Zone**이 **Internal**로 설정된 영역 조건이 포함된 SSL 규칙을 구성합니다. 이러한 간단한 SSL 규칙은 Internal 영역의 인터페이스를 통해 디바이스에서 나가는 트래픽을 매칭합니다.

더 복잡한 규칙을 만들려면, 단일한 영역 조건의 각 **Sources Zones** 및 **Destination Zones**에 최대 50개의 영역을 추가할 수 있습니다.

- 영역의 인터페이스를 통해 디바이스에서 *나가는* 암호화된 트래픽을 매칭하려면, 해당 영역을 **Destination Zones**에 추가합니다.

  수동으로 구축된 디바이스는 트래픽을 전송할 수 없으므로, **Destination Zone** 조건에서는 패시브 인터페이스로 구성된 영역을 사용할 수 없습니다.
- 영역의 인터페이스를 통해 디바이스로 *들어오는* 암호화된 트래픽을 매칭하려면, 해당 영역을 **Source Zones**에 추가합니다.

소스 및 대상 영역 조건을 규칙에 모두 추가할 경우, 매칭되는 트래픽은 지정된 소스 영역 중 하나에서 시작되고 대상 영역 중 하나를 통해 나가야 합니다.

영역의 모든 인터페이스가 동일한 유형(전체 인라인, 전체 패시브, 전체 스위칭, 전체 라우팅)이어야 하듯이, SSL 규칙의 영역 조건에 사용되는 모든 영역도 동일한 유형이어야 합니다. 즉, 서로 다른 유형의 영역으로 들어가거나 나가는 암호화된 트래픽과 매칭되는 단일한 규칙은 쓸 수 없습니다.

경고 아이콘은 인터페이스가 없는 영역 같은 잘못된 컨피그레이션을 나타냅니다. 자세한 내용을 보려면 마우스 포인터를 아이콘 위에 올려놓습니다.

암호화된 트래픽을 영역으로 제어하려면

액세스: Admin/Access Admin/Network Admin

1단계 영역별로 암호화된 트래픽을 제어하려는 SSL 정책에서 새로운 SSL 규칙을 생성하거나 기존 규칙을 수정합니다.

자세한 지침은 21-4페이지의 SSL 규칙 이해 및 생성을/를 참조하십시오.

2단계 SSL 규칙 편집기에서 Zones 탭을 선택합니다.

Zones 탭이 나타납니다.

3단계 **Available Zones**에서 추가할 영역을 찾아 선택합니다.

추가할 영역을 검색하려면 **Available Zones** 목록 위의 **Search by name** 프롬프트를 클릭한 다음 영역 이름을 입력합니다. 입력을 수행하면 목록이 업데이트되어 매칭되는 영역을 표시합니다.

선택할 영역을 클릭합니다. 여러 영역을 선택하려면 Shift +Ctrl 키를 사용하거나, 마우스 오른쪽 버튼을 클릭한 다음 **Select All**을 선택합니다.

4단계 **Add to Source** 또는 **Add to Destination**을 클릭하여 선택한 영역을 해당 목록에 추가합니다.

선택한 영역을 끌어서 놓을 수도 있습니다.

5단계 규칙을 저장하거나 계속 수정합니다.

변경 사항을 구현하려면 SSL 정책과 연결된 액세스 제어 정책을 적용해야 합니다(12-15페이지의 액세스 제어 정책 적용 참조).

암호화된 트래픽을 네트워크 또는 지리적 위치로 제어

라이센스: 모든

지원되는 디바이스: Series 3

SSL 규칙의 네트워크 조건을 사용하면 암호화된 트래픽을 소스 및 대상 IP 주소로 제어하고 해독할 수 있습니다. 다음 중 하나를 수행할 수 있습니다.

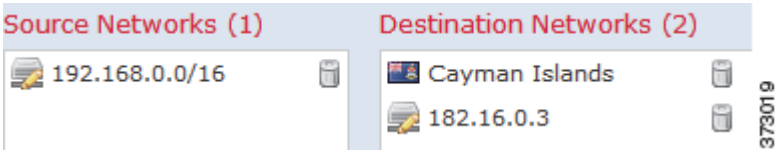
- 제어하려는 암호화된 트래픽의 소스 및 대상 IP 주소를 명시적으로 지정
- IP 주소를 지리적 위치와 연결하는 위치 기능을 사용하여, 암호화된 트래픽을 소스 또는 대상 국가/대륙으로 제어

네트워크 기반 SSL 규칙 조건을 만들 경우, IP 주소 및 지리적 위치를 수동으로 지정할 수 있습니다. 또는 재사용 가능한 네트워크 및 위치 *객체*로 네트워크 조건을 구성하고 하나 이상의 IP 주소, 주소 블록, 국가, 대륙 등과 연결할 수 있습니다.

팁 네트워크 또는 위치 객체를 생성한 후에는 이를 사용하여 SSL 규칙을 생성할 수 있을 뿐만 아니라, 시스템의 웹 인터페이스의 여러 다른 위치에 있는 IP 주소를 나타낼 수도 있습니다. 객체 관리자를 사용하여 이러한 객체를 생성할 수 있으며, SSL 규칙을 구성하는 동안 네트워크 객체를 즉시 생성할 수도 있습니다. 자세한 내용은 3-1페이지의 재사용 가능 객체 관리을/를 참조하십시오.

지리적 위치로 트래픽을 제어하는 규칙을 작성하려는 경우, 최신 위치 데이터를 사용하여 트래픽을 필터링해야 하므로 Cisco에서는 방어 센터의 위치 데이터베이스(GeoDB)를 정기적으로 업데이트하는 것을 **적극** 권장합니다(66-27페이지의 지오로케이션 데이터베이스 업데이트 참조).

다음 그래픽에는 내부 네트워크에서 시작한 암호화된 연결을 차단하는 SSL 규칙의 네트워크 조건, 그리고 182.16.0.3에 회사 서버를 보유한 Cayman Islands 또는 연안의 리소스에 액세스를 시도하는 예가 나와 있습니다.



이 예에서는 회사 서버의 IP 주소를 보유한 연안을 수동으로 지정하고, 시스템에서 제공된 Cayman Islands의 위치 객체를 사용하여 Cayman Islands의 IP 주소를 나타냅니다.

단일한 네트워크 조건의 각 **Source Networks** 및 **Destination Networks**에 최대 50개의 항목을 추가할 수 있으며, 네트워크와 위치 기반 컨피그레이션을 혼합할 수 있습니다.

- IP 주소 또는 지리적 위치에서 *나가는* 암호화된 트래픽을 매칭하려면, **Source Networks**를 구성합니다.
- IP 주소 또는 지리적 위치로 *들어오는* 암호화된 트래픽을 매칭하려면, **Destination Networks**를 구성합니다.

소스 및 대상 네트워크 조건을 규칙에 모두 추가할 경우, 매칭되는 암호화된 트래픽은 지정된 IP 주소 중 하나에서 시작되고 대상 IP 주소 중 하나로 향해야 합니다.

네트워크 조건을 만들 경우, 경고 아이콘은 잘못된 컨피그레이션을 나타냅니다. 자세한 내용을 보려면 마우스 포인터를 아이콘 위에 올려놓습니다.

네트워크 또는 지리적 위치를 기준으로 트래픽을 제어하려면

액세스: Admin/Access Admin/Network Admin

1단계 네트워크별로 암호화된 트래픽을 제어하려는 SSL 정책에서 새로운 SSL 규칙을 생성하거나 기존 규칙을 수정합니다.

자세한 지침은 21-4페이지의 SSL 규칙 이해 및 생성을/를 참조하십시오.

2단계 SSL 규칙 편집기에서 Networks 탭을 선택합니다.

Networks 탭이 나타납니다.

3단계 **Available Networks**에서 추가할 네트워크를 다음과 같이 찾아 선택합니다.

- Networks 탭을 클릭하여 추가할 네트워크 객체 및 그룹을 표시합니다. Geolocation 탭을 클릭하여 위치 객체를 표시합니다.
- 네트워크 객체를 즉시 추가한 다음 조건에 추가하려면, Available Networks 목록 위의 추가 아이콘( )을 클릭합니다(3-4페이지의 네트워크 객체 작업 참조).
- 추가할 네트워크 또는 위치 객체를 검색하려면, 해당 탭을 선택하여 **Available Networks** 목록 위의 **Search by name or value** 프롬프트를 클릭한 다음, 객체 이름 또는 객체 구성 요소 중 하나의 값을 입력합니다. 입력을 수행하면 목록이 업데이트되어 매칭되는 객체를 표시합니다.

객체를 선택하려면 클릭합니다. 여러 객체를 선택하려면 Shift +Ctrl 키를 사용하거나, 마우스 오른쪽 버튼을 클릭한 다음 **Select All**을 선택합니다.

4단계 **Add to Source** 또는 **Add to Destination**을 클릭하여 선택한 객체를 해당 목록에 추가합니다.

선택한 객체를 끌어서 놓을 수도 있습니다.

5단계 수동으로 지정하려는 소스/대상 IP 주소 또는 주소 블록을 추가합니다.

Source Networks 또는 **Destination Networks** 목록 아래의 **Enter an IP address** 프롬프트를 클릭한 다음, IP 주소 또는 주소 블록을 입력하고 **Add**를 클릭합니다.

6단계 규칙을 저장하거나 계속 수정합니다.

변경 사항을 구현하려면 SSL 정책과 연결된 액세스 제어 정책을 적용해야 합니다(12-15페이지의 액세스 제어 정책 적용 참조).

암호화된 VLAN 트래픽 제어

라이센스: 모든

지원되는 디바이스: Series 3

SSL 규칙의 VLAN 조건을 사용하면 VLAN 태그 처리된 트래픽을 제어할 수 있습니다. 시스템에서는 가장 안쪽의 VLAN 태그를 사용하여 VLAN을 기준으로 패킷을 확인합니다.

VLAN 기반의 SSL 규칙 조건을 만들 경우, VLAN 태그를 1~4094 범위까지 수동으로 지정할 수 있습니다. 또는 재사용 가능한 VLAN 태그 *객체*로 VLAN 조건을 구성하고, 이름을 하나 이상의 VLAN 태그와 연결할 수 있습니다.

팁 VLAN 태그 객체를 생성한 후에는 이를 사용하여 SSL 규칙을 만들 수 있을 뿐만 아니라, 시스템의 웹 인터페이스의 여러 다른 위치에 있는 VLAN 태그를 나타낼 수도 있습니다. 객체 관리자를 사용하여 VLAN 태그 객체를 생성하거나, 액세스 제어 규칙을 구성하는 동안 즉시 생성할 수 있습니다. 자세한 내용은 3-13페이지의 VLAN 태그 객체 작업을/를 참조하십시오.

다음 그래픽에는 공용 VLAN의 암호화된 트래픽과 매칭되는 SSL 규칙의 VLAN 태그 조건뿐만 아니라, 수동으로 추가된 VLAN 42가 나와 있습니다.

단일한 VLAN 태그 조건의 **Selected VLAN Tags**에 최대 50개의 항목을 추가할 수 있습니다. VLAN 태그 조건을 만들 경우, 경고 아이콘은 잘못된 컨피그레이션을 나타냅니다. 자세한 내용을 보려면 마우스 포인터를 아이콘 위에 올려놓습니다.

VLAN 태그로 트래픽을 제어하려면

액세스: Admin/Access Admin/Network Admin

1단계 VLAN 태그별로 암호화된 트래픽을 제어하려는 SSL 정책에서 새로운 SSL 규칙을 생성하거나 기존 규칙을 수정합니다.

자세한 지침은 21-4페이지의 SSL 규칙 이해 및 생성을/를 참조하십시오.

2단계 SSL 규칙 편집기에서 VLAN Tags 탭을 선택합니다.

VLAN Tags 탭이 나타납니다.

3단계 **Available VLAN Tags**에서 추가할 VLAN을 다음과 같이 찾아 선택합니다.

- VLAN 태그 객체를 즉시 추가한 다음 조건에 추가하려면, Available VLAN Tags 목록 위의 추가 아이콘( )을 클릭합니다(3-13페이지의 VLAN 태그 객체 작업 참조).
- 추가할 VLAN 태그 객체 및 그룹을 검색하려면, **Available VLAN Tags** 목록 위의 **Search by name or value** 프롬프트를 클릭한 다음 객체의 이름을 입력하거나, 객체의 VLAN 태그의 값을 입력합니다. 입력을 수행하면 목록이 업데이트되어 매칭되는 객체를 표시합니다.

객체를 선택하려면 클릭합니다. 여러 객체를 선택하려면 Shift +Ctrl 키를 사용하거나, 마우스 오른쪽 버튼을 클릭한 다음 **Select All**을 선택합니다.

4단계 **Add to Rule**을 클릭하거나 선택한 객체를 **Selected VLAN Tags** 목록에 추가합니다.

선택한 객체를 끌어서 놓을 수도 있습니다.

5단계 수동으로 지정할 VLAN 태그를 추가합니다.

Selected VLAN Tags 목록 아래의 **Enter a VLAN Tag** 프롬프트를 클릭한 다음, VLAN 태그 또는 범위를 입력하고 **Add**를 클릭합니다. 1~4094 범위의 VLAN 태그를 지정할 수 있으며, 하이픈을 사용하여 VLAN 태그의 범위를 지정합니다.

6단계 규칙을 저장하거나 계속 수정합니다.

변경 사항을 구현하려면 SSL 정책과 연결된 액세스 제어 정책을 적용해야 합니다(12-15페이지의 액세스 제어 정책 적용 참조).

암호화된 트래픽을 포트로 제어

라이센스: 모든

지원되는 디바이스: Series 3

SSL 규칙의 포트 조건을 사용하면 소스 및 TCP 대상 포트에 따라 암호화된 트래픽을 제어할 수 있습니다. 포트 기반 SSL 규칙 조건을 만들 경우, TCP 포트를 수동으로 지정할 수 있습니다. 또는 재사용 가능한 포트 *객체*로 포트 조건을 구성하고, 이름을 하나 이상의 포트 태그와 연결할 수 있습니다.

팁 포트 객체를 생성한 후에는 이를 사용하여 SSL 규칙을 만들 수 있을 뿐만 아니라, 시스템의 웹 인터페이스의 여러 다른 위치에 있는 포트를 나타낼 수도 있습니다. 객체 관리자를 사용하여 포트 객체를 생성하거나, 액세스 제어 규칙을 구성하는 동안 즉시 생성할 수 있습니다. 자세한 내용은 3-12페이지의 포트 객체 작업을/를 참조하십시오.

단일한 네트워크 조건의 각 **Selected Source Ports** 및 **Selected Destination Ports** 목록에 최대 50개의 항목을 추가할 수 있습니다.

- TCP 포트에서 *나가는* 암호화된 트래픽을 매칭하려면, **Selected Source Ports**를 구성합니다.
- TCP 포트로 *들어오는* 암호화된 트래픽을 매칭하려면, **Selected Destination Ports**를 구성합니다.
- TCP **Selected Source Ports**에서 시작되면서 TCP **Selected Destination Ports**로 향하는 암호화된 트래픽을 매칭하려면, 두 가지를 모두 구성합니다.

Selected Source Ports 및 **Selected Destination Ports** 목록만 TCP 포트와 구성할 수 있습니다. 비 TCP 포트가 포함된 포트 객체는 **Available Ports** 목록에서 회색으로 표시됩니다.

포트 조건을 만들 경우, 경고 아이콘은 잘못된 컨피그레이션을 나타냅니다. 예를 들어, 객체 관리자를 사용하여 현재 사용 중인 포트 객체를 수정하면 해당 객체 그룹을 사용하는 규칙은 유효하지 않게 됩니다. 자세한 내용을 보려면 마우스 포인터를 아이콘 위에 올려놓습니다.

포트로 트래픽을 제어하려면

액세스: Admin/Access Admin/Network Admin

1단계 TCP 포트별로 암호화된 트래픽을 제어하려는 SSL 정책에서 새로운 SSL 규칙을 생성하거나 기존 규칙을 수정합니다.

자세한 지침은 21-4페이지의 SSL 규칙 이해 및 생성을/를 참조하십시오.

2단계 SSL 규칙 편집기에서 Ports 탭을 선택합니다.

Ports 탭이 나타납니다.

3단계 **Available Ports**에서 추가할 TCP 포트를 다음과 같이 찾아 선택합니다.

- TCP 포트 객체를 즉시 추가한 다음 조건에 추가하려면, Available Ports 목록 위의 추가 아이콘 ( )을 클릭합니다(3-12페이지의 포트 객체 작업 참조).
- 추가할 TCP 기반 태그 객체 및 그룹을 검색하려면, **Available Ports** 목록 위의 **Search by name or value** 프롬프트를 클릭한 다음 객체의 이름을 입력하거나, 객체의 포트 값을 입력합니다. 입력을 수행하면 목록이 업데이트되어 매칭되는 객체를 표시합니다. 예를 들어, 443을 입력하면 방어 센터에는 시스템에서 제공된 HTTPS 포트 객체가 표시됩니다.

TCP 기반 포트 객체를 선택하려면 이를 클릭합니다. 여러 TCP 기반 포트 객체를 선택하려면 Shift +Ctrl 키를 사용하거나, 마우스 오른쪽 버튼을 클릭한 다음 **Select All**을 선택합니다. 객체에 비 TCP 기반 포트가 포함된 경우, 이를 포트 조건에 추가할 수 없습니다.

4단계 **Add to Source** 또는 **Add to Destination**을 클릭하여 선택한 객체를 해당 목록에 추가합니다.

선택한 객체를 끌어서 놓을 수도 있습니다.

5단계 **Selected Source Ports** 또는 **Selected Destination Ports** 목록 아래에 있는 **Port**로 들어가 소스 또는 대상 포트를 수동으로 지정합니다. 0~65535 사이의 값을 사용하여 단일 포트를 지정할 수 있습니다.

6단계 **Add**를 클릭합니다.

방어 센터는 컨피그레이션이 잘못될 수 있는 규칙 조건에 포트를 추가하지 않습니다.

7단계 규칙을 저장하거나 계속 수정합니다.

변경 사항을 구현하려면 SSL 정책과 연결된 액세스 제어 정책을 적용해야 합니다(12-15페이지의 액세스 제어 정책 적용 참조).

암호화된 트래픽을 사용자에 따라 제어

라이센스: 제어

지원되는 디바이스: Series 3

Microsoft Active Directory Server에서 검색된 사용자와 트래픽을 매칭하는 SSL 규칙을 구성할 수 있습니다. SSL 규칙의 사용자 조건을 사용하면 *사용자 제어*를 수행할 수 있습니다. 이렇게 하면 호스트에 로깅된 LDAP 사용자를 기준으로 트래픽을 제한하여 어떤 트래픽이 네트워크를 통과할 수 있는지 관리가 가능합니다.

사용자 제어는 *액세스 제어 사용자*와 IP 주소를 연결하여 구현됩니다. 구축된 에이전트는 지정된 사용자가 호스트에 로그인하고 로그아웃할 경우 해당 사용자를 모니터링하거나, 기타 사유에 따라 Active Directory 자격 증명을 인증합니다. 예를 들어, 조직에서는 중앙 집중식 인증을 위해 Active Directory에 기반한 서비스나 애플리케이션을 사용할 수 있습니다.

사용자 조건이 포함된 SSL 규칙을 매칭하려는 트래픽의 경우, 모니터링된 세션의 소스 또는 대상 호스트의 IP 주소를 로그인된 액세스 제어 사용자와 연결해야 합니다. 개별 사용자 또는 그러한 사용자가 속한 그룹을 기반으로 트래픽을 제어할 수 있습니다.

사용자 조건을 서로 조합하고 다른 유형의 조건과 조합하여 SSL 규칙을 생성할 수 있습니다. 이러한 SSL 규칙은 간단하거나 복잡할 수 있으며, 여러 조건을 사용하여 트래픽을 매칭하고 검사합니다. SSL 규칙에 대한 자세한 내용은 21-4페이지의 SSL 규칙 이해 및 생성을/를 참조하십시오.

사용자 제어를 사용하려면 제어 라이센스가 있어야 하며 이 기능은 Microsoft Active Directory를 모니터링하는 사용자 에이전트에 의해 보고되는 로그인 및 로그오프 레코드를 사용하는 LDAP 사용자 및 그룹(*액세스 제어 사용자*)에만 지원됩니다.

사용자 조건이 포함된 SSL 규칙을 작성하려면, 우선 방어 센터와 조직에 있는 하나 이상의 Microsoft Active Directory 서버 간에 연결을 구성해야 합니다. 이러한 컨피그레이션을 인증 객체라고 하며, 여기에는 서버의 연결 설정 및 인증 필터 설정이 포함됩니다. 또한 이 구성은 사용자 조건 내에서 사용할 수 있는 사용자를 지정합니다. 자세한 내용은 17-4페이지의 액세스 제어 대상 사용자 및 LDAP 사용자 메타데이터 검색을/를 참조하십시오.

이와 더불어, 사용자 에이전트를 설치해야 합니다. 에이전트는 사용자가 Active Directory 자격 증명을 인증할 경우 해당 사용자를 모니터링하며, 이러한 로그인 레코드를 방어 센터에 전송합니다. 이러한 레코드는 사용자와 IP 주소(사용자 조건이 포함된 SSL 규칙을 트리거할 수 있도록 하는 요소)를 연결합니다. 자세한 내용은 17-9페이지의 User Agents를 사용하여 Active Directory 로그인 보고을/를 참조하십시오.

암호화된 트래픽을 사용자로 제어하려면

액세스: Admin/Access Admin/Network Admin

1단계 사용자별로 암호화된 트래픽을 제어하려는 SSL 정책에서 새로운 SSL 규칙을 생성하거나 기존 규칙을 수정합니다.

자세한 지침은 21-4페이지의 SSL 규칙 이해 및 생성을/를 참조하십시오.

2단계 SSL 규칙 편집기에서 Users 탭을 선택합니다.

Users 탭이 나타납니다.

3단계 추가할 사용자를 검색하려면 **Available Users** 목록 위의 **Search by name or value** 프롬프트를 클릭한 다음 사용자 이름을 입력합니다. 입력을 수행하면 목록이 업데이트되어 매칭되는 사용자를 표시합니다.

사용자를 선택하려면 클릭합니다. 여러 사용자를 선택하려면 Shift +Ctrl 키를 사용하거나, 마우스 오른쪽 버튼을 클릭한 다음 **Select All**을 선택합니다.

4단계 **Add to Rule**을 클릭하거나 선택한 객체를 **Selected Users** 목록에 추가합니다.

선택한 사용자를 끌어서 놓을 수도 있습니다.

5단계 규칙을 저장하거나 계속 수정합니다.

변경 사항을 구현하려면 SSL 정책과 연결된 액세스 제어 정책을 적용해야 합니다(12-15페이지의 액세스 제어 정책 적용 참조).

암호화된 트래픽을 평판으로 제어

라이센스: 제어 또는 URL 필터링

지원되는 디바이스: Series 3

SSL 규칙의 평판 기반 조건을 사용하면 네트워크 트래픽의 상황을 분석하고 적절한 경우 이를 제한하여, 어떤 암호화된 트래픽이 네트워크를 통과할 수 있는지 관리가 가능합니다. SSL 규칙은 다음과 같은 유형의 평판 기반 제어를 관리합니다.

- 애플리케이션 조건을 사용하면 *애플리케이션 제어*를 수행할 수 있으며, 이는 개별 애플리케이션뿐만 아니라 애플리케이션의 기본 특성(유형, 위험, 비즈니스 관련성, 카테고리)를 기준으로 애플리케이션 트래픽을 제어합니다.
- URL 조건을 사용하면 웹 사이트의 할당된 카테고리 및 평판을 기준으로 웹 트래픽을 제어할 수 있습니다.

평판 기반 조건을 서로 조합하고 다른 유형의 조건과 조합하여 SSL 규칙을 생성할 수 있습니다. 이러한 SSL 규칙은 간단하거나 복잡할 수 있으며, 여러 조건을 사용하여 트래픽을 매칭하고 검사합니다.

평판 기반 SSL 검사를 사용하려면 다음과 같은 라이센스, 디바이스, 방어 센터가 있어야 합니다.

표 22-1 평판 기반 SSL 규칙의 라이센스 및 어플라이언스 요건

요건	애플리케이션 제어	URL 필터링(카테고리 및 평판)
라이센스	제어	URL 필터링
디바이스	Series 3	Series 3
방어 센터	Series 3, 가상	Series 3, 가상

자세한 내용은 다음 절을 참조하십시오.

- 22-10페이지의 암호화된 트래픽을 애플리케이션에 따라 제어
- 22-15페이지의 암호화된 트래픽을 URL 카테고리 및 평판으로 제어

암호화된 트래픽을 애플리케이션에 따라 제어

라이센스: 제어

지원되는 디바이스: Series 3

FireSIGHT 시스템은 암호화된 IP 트래픽을 분석할 경우, 암호화된 세션을 해독하기 전에 네트워크에서 일반적으로 사용된 암호화된 애플리케이션을 식별하고 분류할 수 있습니다. 이 시스템은 이러한 검색 기반의 *애플리케이션 인식* 기능을 사용하여 사용자가 네트워크의 암호화된 애플리케이션 트래픽을 제어할 수 있도록 합니다.

SSL 규칙의 애플리케이션 조건을 사용하면 이러한 *애플리케이션 제어*를 수행할 수 있습니다. 단일한 SSL 규칙에는 트래픽을 제어할 애플리케이션을 지정할 수 있는 몇 가지 방법이 있습니다.

- 사용자 지정 애플리케이션을 비롯하여 개별 애플리케이션을 선택할 수 있습니다.
- 시스템에서 제공된 *애플리케이션 필터*를 사용할 수 있으며 이는 애플리케이션의 기본 특성(유형, 위험, 비즈니스 관련성, 카테고리)에 따라 구성한 명명된 애플리케이션 집합입니다.
- 사용자 지정 애플리케이션 필터를 생성하고 사용할 수 있으며, 이는 선택하는 모든 방식을 통해 애플리케이션(사용자 지정 애플리케이션 포함)을 그룹화합니다.

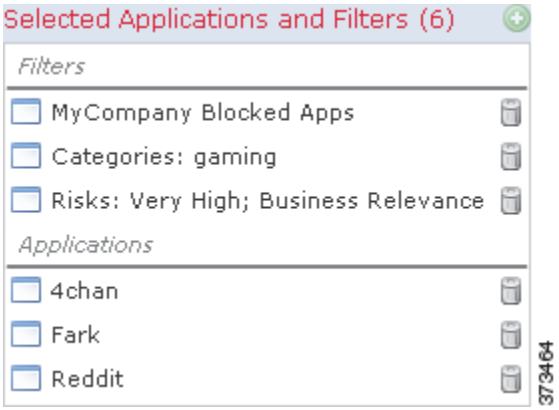
참고 액세스 제어 규칙을 사용하여 애플리케이션 트래픽을 필터링할 경우, 애플리케이션 태그를 기준으로 사용하여 필터링할 수 있습니다. 그러나 애플리케이션 태그를 사용하여 암호화된 트래픽을 필터링하는 것은 아무런 이점이 없으므로 이 방법은 사용할 수 없습니다. 시스템에 암호화된 트래픽에서 탐지할 수 있는 모든 애플리케이션은 태그된 **SSL Protocol**입니다. 이 태그가 없는 애플리케이션은 암호화되지 않거나 해독된 트래픽에서만 탐지될 수 있습니다.

애플리케이션 필터를 사용하면 SSL 규칙에 대한 애플리케이션 조건을 신속하게 생성할 수 있습니다. 이러한 필터는 정책 생성 및 관리를 간소화하며, 시스템에서 웹 트래픽을 예상대로 제어한다는 확신을 가질 수 있습니다. 예를 들어, 암호화된 트래픽에서 위험도가 높고 비즈니스 관련성이 낮은 모든 애플리케이션을 식별하고 해독하는 SSL 규칙을 생성할 수 있습니다. 사용자가 이러한 애플리케이션 중 하나를 사용하려고 시도할 경우, 액세스 제어를 통해 해당 세션이 해독 및 검사됩니다.

이와 더불어 Cisco에서는 VDB(System and Vulnerability Database: 취약점 데이터베이스)를 통해 추가 탐지기를 자주 업데이트하고 추가합니다. 또한 사용자는 자체 탐지기를 생성할 수 있으며, 이를 사용하여 탐지하는 애플리케이션에 특성(위험, 관련성 등)을 할당할 수 있습니다. 애플리케이션 특징을 기준으로 한 필터를 사용하면 시스템에서는 최신 탐지기를 사용하여 애플리케이션 트래픽을 모니터링할 수 있습니다.

애플리케이션 조건이 포함된 SSL 규칙을 매칭하려는 트래픽의 경우, 트래픽은 **Selected Applications and Filters** 목록에 추가된 필터 또는 애플리케이션 중 하나와 매칭되어야 합니다.

다음 그래픽에는 MyCompany의 사용자 지정 애플리케이션 그룹, 위험도가 높고 비즈니스 관련성이 낮은 모든 애플리케이션, 개별적으로 선택된 일부 애플리케이션을 해독하는 SSL 규칙에 대한 애플리케이션 조건이 나와 있습니다.



단일 애플리케이션 조건의 경우, **Selected Applications and Filters** 목록에 최대 50개의 항목을 추가할 수 있습니다. 다음 각 항목은 하나의 항목으로 간주됩니다.

- 개별적으로 조합하거나 맞춤형으로 조합한 **Application Filters** 목록의 하나 이상의 필터. 이 항목은 특성을 기준으로 그룹화된 애플리케이션 집합을 나타냅니다.
- **Available Applications** 목록의 애플리케이션 검색 결과를 저장하여 생성된 필터. 이 항목은 부분 문자열 매치를 기준으로 그룹화된 애플리케이션 집합을 나타냅니다.
- **Available Applications** 목록의 개별 애플리케이션.

웹 인터페이스의 경우, 조건에 추가된 필터는 위에 나열되며 개별적으로 추가된 애플리케이션과 따로 구분됩니다.

SSL 정책을 적용할 경우, 시스템에서는 애플리케이션 조건이 포함된 각 규칙에 대해 매칭할 수 있는 고유한 애플리케이션 목록을 생성합니다. 즉, 겹치는 필터 및 개별적으로 지정된 애플리케이션을 사용하여 완전한 범위를 포괄할 수 있습니다.

자세한 내용은 다음 절을 참조하십시오.

- 22-11페이지의 암호화된 트래픽을 애플리케이션 필터와 매칭
- 22-12페이지의 개별 애플리케이션에서 나가는 트래픽 일치
- 22-14페이지의 SSL 규칙에 애플리케이션 조건 추가
- 22-15페이지의 암호화된 애플리케이션 제어의 제한 사항

암호화된 트래픽을 애플리케이션 필터와 매칭

라이센스: 제어

지원되는 디바이스: Series 3

SSL 규칙에서 애플리케이션 조건을 만들 경우 **Application Filters** 목록을 사용하여, 특성을 기준으로 그룹화된 애플리케이션(트래픽을 매칭할 애플리케이션) 집합을 생성합니다.

사용자의 편의를 위해, 시스템에서는 45-10페이지의 애플리케이션 탐지 이해에 설명된 기준을 사용하여 탐지하는 각 애플리케이션의 특징을 분류합니다. 이러한 기준을 필터로 사용하거나 사용자 지정 필터 조합을 생성하여 애플리케이션 제어를 수행할 수 있습니다.

SSL 규칙의 필터링 애플리케이션 메커니즘은 객체 관리자를 사용하는 재사용 가능한 사용자 지정 애플리케이션 필터와 동일합니다(3-15페이지의 애플리케이션 필터 작업 참조). 액세스 제어 규칙에서 즉시 생성하는 많은 필터를 새로운 재사용 가능한 필터로 저장할 수도 있습니다. 사용자가 생성한 필터는 중첩할 수 없으므로, 다른 사용자가 생성한 필터가 포함된 필터를 저장할 수 없습니다.

필터를 조합하는 방법 이해

필터를 단독으로 또는 조합하여 선택할 경우, 해당 기준에 맞는 애플리케이션만 표시하도록 **Available Applications** 목록이 업데이트됩니다. 시스템에서 제공된 필터를 조합하여 선택할 수 있으나, 사용자 지정 필터는 그렇지 않습니다.

동일한 필터 유형의 여러 필터는 OR 연산자로 연결됩니다. 예를 들어, Risks 유형 아래에서 Medium 및 High 필터를 선택할 경우 결과 필터는 다음과 같습니다.

```
Risk: Medium OR High
```

Medium 필터에 110개의 애플리케이션이 포함되어 있고 High 필터에 82개의 애플리케이션이 포함된 경우, **Available Applications** 목록에는 총 192개의 애플리케이션이 표시됩니다.

서로 다른 유형의 필터는 AND 연산자로 연결됩니다. 예를 들어, Risks 유형 아래에서 Medium 및 High 필터를 선택하고, Business Relevance 유형 아래에서 Medium 및 High 필터를 선택한 경우 결과 필터는 다음과 같습니다.

```
Risk: Medium OR High
AND
Business Relevance: Medium OR High
```

이 경우, Medium 또는 High Risk 유형과 Medium 또는 High Business Relevance 유형이 모두 포함된 애플리케이션만 표시됩니다.

필터 찾기 및 선택

필터를 선택하려면 필터 옆의 활살표를 클릭하여 확장한 다음, 표시하거나 숨기려는 애플리케이션의 각 필터 옆에 있는 확인란을 선택하거나 선택을 취소합니다. 또한 Cisco에서 제공된 필터 유형(**Risks**, **Business Relevance**, **Types**, 또는 **Categories**)를 마우스 오른쪽 버튼으로 클릭하고 **Check All** 또는 **Uncheck All**을 선택할 수 있습니다.

필터를 검색하려면 **Available Filters** 목록 위의 **Search by name** 프롬프트를 클릭한 다음 이름을 입력합니다. 입력을 수행하면 목록이 업데이트되어 매칭되는 필터를 표시합니다.

필터 선택을 완료한 후에는 **Available Applications** 목록을 사용하여 해당 필터를 규칙에 추가합니다 (22-12페이지의 개별 애플리케이션에서 나가는 트래픽 일치 참조).

개별 애플리케이션에서 나가는 트래픽 일치

라이센스: 제어

지원되는 디바이스: Series 3

SSL 규칙에서 애플리케이션 조건을 만들 경우, **Available Applications** 목록을 사용하여 트래픽을 매칭할 애플리케이션을 선택할 수 있습니다.

애플리케이션 목록 탐색

조건 만들기를 처음 시작할 경우 목록은 제한되지 않은 상태이며, 시스템에서 탐지되는 모든 애플리케이션이 한 번에 100개씩 표시됩니다.

- 애플리케이션 페이지를 넘기려면 목록 아래의 화살표를 클릭합니다.
- 애플리케이션의 특성에 대한 요약 정보 및 사용 가능한 인터넷 검색 링크가 포함된 팝업 창을 표시하려면, 애플리케이션 옆의 정보 아이콘( )을 클릭합니다.

매칭할 애플리케이션 찾기

매칭할 애플리케이션을 찾으려면, 다음과 같은 방법으로 **Available Applications** 목록을 제한할 수 있습니다.

- 애플리케이션을 검색하려면 **Search by name** 프롬프트를 클릭한 다음 이름을 입력합니다. 입력을 수행하면 목록이 업데이트되어 매칭되는 애플리케이션을 표시합니다.
- 필터를 적용하여 애플리케이션을 제한하려면 **Application Filters** 목록을 사용합니다(22-11페이지의 암호화된 트래픽을 애플리케이션 필터와 매칭 참조). 필터를 적용하면 **Available Applications** 목록이 업데이트됩니다.

제한이 이루어지면 **Available Applications** 목록의 상단에 **All apps matching the filter** 옵션이 표시됩니다. 이 옵션을 사용하면 제한된 목록의 모든 애플리케이션을 **Selected Applications and Filters** 목록에 한 번에 추가할 수 있습니다.

참고 Application Filters 목록에서 하나 이상의 필터를 선택하고 **Available Applications** 목록에서 검색을 수행할 경우, 선택 항목 및 검색 필터링된 **Available Applications** 목록이 AND 연산을 사용하여 조합됩니다. 즉, **All apps matching the filter** 조건에는 **Available Applications** 목록에 현재 표시된 모든 개별 조건 및 **Available Applications** 목록의 위에 입력한 검색 문자열이 포함됩니다.

조건에서 매칭할 단일 애플리케이션 선택

매칭할 애플리케이션을 찾은 후에는 이를 클릭하여 선택합니다. 여러 사용자를 선택하려면 Shift +Ctrl 키를 사용하거나, 마우스 오른쪽 버튼을 클릭한 다음 **Select All**을 선택하여 현재 제한된 보기에서 모든 애플리케이션을 선택합니다.

단일한 애플리케이션 조건의 경우, 최대 50개의 애플리케이션을 개별적으로 선택하여 매칭할 수 있습니다. 50개 이상을 추가하려면 여러 SSL 규칙을 생성하거나 필터를 사용하여 애플리케이션을 그룹화해야 합니다.

조건에 대한 필터와 매칭되는 모든 애플리케이션 선택

Application Filters 목록에서 필터를 검색하거나 사용하여 제한이 이루어진 경우, **Available Applications** 목록의 상단에 **All apps matching the filter** 옵션이 표시됩니다.

이 옵션을 사용하면 **Available Applications** 목록에서 제한된 전체 애플리케이션 집합을 **Selected Applications and Filters** 목록에 한 번에 추가할 수 있습니다. 애플리케이션을 개별적으로 추가할 때와 달리, 이러한 애플리케이션 집합을 추가할 경우 구성되는 개별 애플리케이션의 수에 상관없이, 그리고 최대 50개까지라는 제한 없이 하나의 항목으로만 간주됩니다.

애플리케이션 조건을 이러한 방식으로 만들 경우, **Selected Applications and Filters** 목록에 추가하는 필터의 이름은 필터에 표시된 필터 유형과 각 유형의 세 가지 필터의 이름을 최대 세 개까지 더하여 연결됩니다. 유형이 동일한 세 개 이상의 필터 뒤에는 생략 부호(...)가 붙습니다. 예를 들어, 다음 필터 이름에는 Risks 유형 아래의 필터 2개, Business Relevance 아래의 필터 4개가 포함됩니다.

```
Risks: Medium, High Business Relevance: Low, Medium, High,...
```

All apps matching the filter와 함께 추가하는 필터에 표시되지 않는 필터 유형은 추가하는 필터의 이름에 포함되지 않습니다. **Selected Applications and Filters** 목록의 필터 이름 위에 마우스 포인터를 올릴 때 표시되는 설명 텍스트는 이러한 필터 유형이 *임의의* 값으로 설정되어 있음을 나타냅니다. 즉, 이러한 필터 유형은 필터를 제한하지 않으므로 모든 값을 필터에 사용할 수 있습니다.

All apps matching the filter의 여러 인스턴스를 애플리케이션에 추가할 수 있으며, 각 인스턴스는 **Selected Applications and Filters** 목록에서 하나의 개별 항목으로 계산됩니다. 예를 들어, 위험도가 높은 모든 애플리케이션을 하나의 항목으로 추가하고 선택 항목을 취소한 다음, 비즈니스 관련성이 낮은 모든 애플리케이션을 다른 항목으로 추가할 수 있습니다. 이러한 애플리케이션 조건은 위험도가 높거나 비즈니스 관련성이 낮은 애플리케이션과 매칭됩니다.

SSL 규칙에 애플리케이션 조건 추가

라이센스: 제어

지원되는 디바이스: Series 3

애플리케이션 조건이 포함된 SSL 규칙을 매칭하려는 암호화된 트래픽의 경우, 트래픽은 **Selected Applications and Filters** 목록에 추가된 필터 또는 애플리케이션 중 하나와 매칭되어야 합니다.

조건당 최대 50개의 항목을 추가할 수 있으며, 조건에 추가된 필터는 위에 나열되고 개별적으로 추가된 애플리케이션과 따로 구분됩니다. 애플리케이션 조건을 만들 경우, 경고 아이콘은 잘못된 컨피그레이션을 나타냅니다. 자세한 내용을 보려면 마우스 포인터를 아이콘 위에 올려놓습니다.

암호화된 애플리케이션 트래픽을 제어하려면

액세스: Admin/Access Admin/Network Admin

1단계 암호화된 트래픽을 애플리케이션으로 제어하려는 SSL 규칙에서, 새로운 SSL 규칙을 생성하거나 기존 규칙을 수정합니다.

자세한 지침은 21-4페이지의 SSL 규칙 이해 및 생성을/를 참조하십시오.

2단계 SSL 규칙 편집기에서 Applications 탭을 선택합니다.

Applications 탭이 나타납니다.

3단계 필요한 경우, 필터를 사용하여 **Available Applications** 목록에 표시되는 애플리케이션의 목록을 제한할 수 있습니다.

Application Filters 목록에서 하나 이상의 필터를 선택합니다. 자세한 내용은 22-11페이지의 암호화된 트래픽을 애플리케이션 필터와 매칭을/를 참조하십시오.

4단계 **Available Applications**에서 추가할 애플리케이션을 찾아 선택합니다.

개별 애플리케이션을 검색하고 선택하거나, 목록이 제한된 경우 **All apps matching the filter**를 사용할 수 있습니다. 자세한 내용은 22-12페이지의 개별 애플리케이션에서 나가는 트래픽 일치을/를 참조하십시오.

5단계 **Add to Rule**을 클릭하여 선택된 애플리케이션을 **Selected Applications and Filters** 목록에 추가합니다.

선택한 애플리케이션 및 필터를 끌어서 놓을 수도 있습니다. 필터는 맨 앞의 *Filters* 아래에 표시되며, 애플리케이션은 맨 앞의 *Applications* 아래에 표시됩니다.

팁 이 애플리케이션 조건에 다른 필터를 추가하려면, 우선 **Clear All Filters**를 클릭하여 기존 선택 사항을 취소합니다.

6단계 규칙을 저장하거나 계속 수정합니다.

변경 사항을 구현하려면 SSL 정책과 연결된 액세스 제어 정책을 적용해야 합니다(12-15페이지의 액세스 제어 정책 적용 참조).

암호화된 애플리케이션 제어의 제한 사항

라이센스: 제어

지원되는 디바이스: Series 3

애플리케이션 제어를 수행할 경우 다음 사항에 유의해야 합니다.

암호화된 애플리케이션 식별

시스템은 StartTLS를 사용하여 암호화되는 해독된 애플리케이션을 식별할 수 있습니다. 여기에는 SMTPS, POPS, FTPS, TelnetS, IMAPS 같은 애플리케이션이 포함됩니다. 또한 시스템은 TLS 클라이언트 hello 메시지의 Server Name Indication 또는 서버 인증서 주체 고유 이름 값을 기준으로 특정한 암호화된 애플리케이션을 식별할 수 있습니다.

애플리케이션 식별 속도

시스템은 다음이 구현되지 않으면 암호화 트래픽에 애플리케이션 제어를 수행할 수 없습니다.

- 클라이언트와 서버 간에 암호화 연결 설정
- 암호화 세션의 애플리케이션 식별

이러한 식별은 서버 인증서 교환 후에 이루어집니다. 핸드셰이크 중에 교환된 트래픽이 애플리케이션 조건을 포함하는 SSL 규칙의 모든 다른 조건과 매칭되지만 식별이 완료되지 않은 경우, SSL 정책을 사용하여 패킷을 통과하도록 할 수 있습니다. 이러한 동작을 통해 핸드셰이크가 완료되므로 애플리케이션을 식별할 수 있습니다. 사용자의 편의를 위해, 영향을 받은 규칙은 정보 아이콘 ( )으로 표시됩니다.

시스템에서 식별을 완료하면, 애플리케이션 조건과 매칭되는 나머지 세션 트래픽에 SSL 규칙 작업을 적용합니다.

애플리케이션 탐지기 자동 활성화

정책의 각 애플리케이션 규칙 조건에 최소 하나의 탐지기를 활성화해야 합니다(46-27페이지의 탐지기 활성화 및 비활성화 참조). 애플리케이션에 탐지기가 활성화되지 않은 경우, 시스템은 시스템에서 제공된 모든 탐지기를 해당 애플리케이션에 자동으로 활성화합니다. 시스템은 가장 최근에 수정된 사용자 정의 탐지기를 애플리케이션에 활성화합니다.

암호화된 트래픽을 URL 카테고리 및 평판으로 제어

라이센스: URL 필터링

지원되는 디바이스: Series 3

SSL 규칙의 URL 조건을 사용하면 네트워크의 사용자가 액세스할 수 있는 암호화된 웹 사이트 트래픽을 처리하고 해독할 수 있습니다. 시스템에서는 SSL 핸드셰이크 중에 전달된 정보를 기준으로 요청한 URL을 탐지합니다. URL 필터링 라이센스가 있을 경우, URL의 일반 분류 또는 *카테고리*, 위험 수준 또는 *평판*을 기준으로 웹 사이트에 대한 액세스를 제어할 수 있습니다.

참고 고유 이름 SSL 규칙 조건을 정의하여 특정 URL에 대한 트래픽을 처리하고 해독할 수 있습니다. 인증서의 주체 고유 이름의 공용 이름 속성에는 사이트의 URL이 포함됩니다. 자세한 내용은 22-19페이지의 암호화된 트래픽을 인증서 고유 이름으로 제어을/를 참조하십시오.

자세한 내용은 다음 링크를 참고하십시오.

- 22-16페이지의 평판 기반 URL 차단 수행
- 22-18페이지의 URL 탐지 및 차단의 제한 사항

평판 기반 URL 차단 수행

라이센스: URL 필터링

지원되는 디바이스: Series 3

URL 필터링 라이센스가 있을 경우, 요청한 URL의 카테고리 및 평판을 기준으로 웹 사이트에 대한 사용자의 액세스를 제어할 수 있습니다.

- URL *카테고리*는 URL의 일반 분류입니다. 예를 들어, ebay.com은 **Auctions** 카테고리에 속하고 monster.com은 **Job Search** 카테고리에 속합니다. URL은 여러 카테고리에 속할 수 있습니다.
- URL *평판*은 URL이 조직의 보안 정책에 반할 수 있는 목적으로 사용될 가능성이 어느 정도 되는지 나타냅니다. URL의 위험도 범위는 **High Risk**(수준 1)에서 **Well Known**(수준 5)까지 지정할 수 있습니다.

FireSIGHT 시스템가 Cisco 클라우드를 통해 얻는 URL 카테고리 및 평판을 사용하면 SSL 규칙에 대한 URL 조건을 신속하게 생성할 수 있습니다. 예를 들어, **Abused Drugs** 카테고리의 **High risk** URL을 식별하고 차단하는 SSL 규칙을 생성할 수 있습니다. 사용자가 암호화된 연결을 통해 해당 카테고리와 평판이 조합된 URL을 찾아보려고 시도할 경우, 세션이 차단됩니다.

참고 카테고리 및 평판 기반 URL 조건이 포함된 SSL 규칙을 적용하려면, 우선 Cisco 클라우드와의 통신을 **반드시** 활성화해야 합니다. 이렇게 하면 방어 센터가 URL 데이터를 검색할 수 있습니다. 자세한 내용은 64-27페이지의 클라우드 통신 활성화을/를 참조하십시오.

Cisco 클라우드의 카테고리 및 평판 데이터를 사용하면 정책 생성 및 관리가 간소화됩니다. 이를 통해 시스템에서 암호화된 웹 트래픽을 예상대로 제어한다는 확신을 가질 수 있습니다. 마지막으로, 클라우드는 새로운 URL, 새로운 카테고리 및 기존 URL의 위험도가 지속적으로 업데이트되므로 시스템에서 최신 정보를 사용하여 요청된 URL을 필터링하도록 보장할 수 있습니다. 악성코드, 스팸, 봇넷, 피싱 같은 보안 위협을 나타내는 악의적인 사이트는 사용자가 새로운 정책을 업데이트하고 적용하는 속도보다 빨리 나타나고 사라질 수 있습니다.

예를 들면 다음과 같습니다.

- 규칙에 의해 모든 게임 사이트가 차단된 경우, 새로운 도메인이 등록되고 **Gaming**으로 분류되면 시스템에서는 해당 사이트를 자동으로 차단할 수 있습니다.
- 규칙에 의해 모든 악성코드, 악성코드로 감염된 블로그 페이지가 차단된 경우, 클라우드는 URL의 카테고리를 **Blog**에서 **Malware**로 다시 분류하여 시스템이 해당 사이트를 차단할 수 있도록 합니다.
- 규칙에 의해 위험도가 높은 소셜 네트워킹 사이트를 차단되었고, 누군가가 악성 페이로드로 연결되는 링크가 포함된 프로필 페이지에 링크를 게시한 경우, 클라우드는 해당 페이지의 평판을 **Benign sites**에서 **High risk**로 변경하므로 시스템에서는 이러한 페이지를 차단할 수 있습니다.

클라우드가 URL의 카테고리 또는 평판을 모르거나, 방어 센터가 클라우드에 연결할 수 없는 경우 해당 URL은 카테고리 또는 평판 기반 URL 조건이 포함된 SSL 규칙을 트리거하지 **않습니다**. URL에 카테고리 또는 평판을 수동으로 할당할 수 없습니다.

다음 그래픽에는 모든 악성코드 사이트, 위험도가 높은 사이트, 악성 소셜 네트워킹 사이트를 차단하는 액세스 제어 규칙의 URL 조건이 나와 있습니다.

팁 트래픽을 해독한 다음 액세스 제어로 이를 차단할 경우, 사용자에게 경고 페이지를 클릭하여 차단을 우회할 수 있는 기회를 제공할 수 있습니다. 자세한 내용은 14-10페이지의 Interactive Blocking 작업: 사용자가 웹사이트 차단을 우회하도록 허용을/를 참조하십시오.

단일한 URL 조건과 매칭할 최대 50개의 **Selected Categories**를 추가할 수 있습니다. 선택에 따라 각 URL 카테고리는 평판을 기준으로 검증되며, 단일한 항목으로 간주됩니다.

다음 표에는 위에 표시된 조건을 만드는 방법이 요약되어 있습니다. 평판으로는 리터럴 URL 또는 URL 객체를 검증할 수 없습니다.

표 22-2 예: URL 조건 만들기

차단 대상	다음 Category 또는 URL Object 선택	평판
악성코드 사이트(평판과 상관없음)	악성코드 사이트	모든
위험도가 높은 모든 URL(수준 1)	모든	1 - High Risk
위험도가 Benign보다 높은 소셜 네트워킹 사이트(수준 1~3)	소셜 네트워크	3 - Benign sites with security risks

URL 조건을 만들 경우, 경고 아이콘은 잘못된 컨피그레이션을 나타냅니다. 자세한 내용을 보려면 마우스 포인터를 아이콘 위에 올리고 12-21페이지의 액세스 제어 정책 및 규칙 문제 해결을/를 참조하십시오.

카테고리 및 평판 데이터를 사용하여 요청된 URL에 따라 트래픽을 제어하려면

액세스: Admin/Access Admin/Network Admin

1단계 URL별로 암호화된 트래픽을 제어하려는 SSL 정책에서 새로운 SSL 규칙을 생성하거나 기존 규칙을 수정합니다.

자세한 지침은 21-4페이지의 SSL 규칙 이해 및 생성을/를 참조하십시오.

2단계 SSL 규칙 편집기에서 Categories 탭을 선택합니다.

Categories 탭이 나타납니다.

3단계 추가할 URL의 카테고리를 **Categories** 목록에서 찾아 선택합니다. 카테고리에 상관없이 암호화된 트래픽을 매칭하려면, **Any** 카테고리를 선택합니다.

추가할 카테고리를 검색하려면 **Categories** 목록 위의 **Search by name or value** 프롬프트를 클릭한 다음 카테고리 이름을 입력합니다. 입력을 수행하면 목록이 업데이트되어 매칭되는 카테고리를 표시합니다.

카테고리를 선택하려면 클릭합니다. 여러 카테고리를 선택하려면 Shift + Ctrl 키를 사용합니다.

팁 마우스 오른쪽 버튼을 클릭하여 **Select All** 카테고리를 선택할 수 있으나, 이 방법으로 모든 카테고리를 추가하면 SSL 규칙의 최대값인 50개 항목을 초과합니다. 이렇게 하는 대신 **Any**를 사용합니다.

4단계 선택에 따라, **Reputations** 목록에서 평판 수준을 클릭하여 카테고리 선택 사항을 검증할 수 있습니다. 평판 수준을 지정하지 않을 경우, 기본값이 **Any**로 설정되며 이는 모든 수준을 의미합니다.

평판 수준은 하나만 선택할 수 있습니다. 평판 수준을 선택하면, SSL 규칙은 해당 목적에 따라 다르게 동작합니다.

- 규칙에 의해 웹 액세스가 차단되거나 트래픽이 해독될 경우(작업 규칙은 **Block**, **Block with reset**, **Decrypt - Known Key**, **Decrypt - Resign**, 또는 **Monitor**) 평판 수준을 선택하면 해당 수준보다 심각도가 높은 모든 평판이 선택됩니다. 예를 들어, **Suspicious sites**(수준 2)를 차단하는 규칙을 구성할 경우 해당 규칙은 **High Risk**(수준 1) 사이트도 자동으로 차단합니다.
- 규칙이 웹 액세스, 액세스 제어에 대한 주체를 허용할 경우(작업 규칙은 **Do not decrypt**), 평판 수준을 선택하면 해당 수준보다 심각도가 낮은 모든 평판도 선택됩니다. 예를 들어, **Benign sites**(수준 4)를 허용하는 규칙을 구성할 경우, 해당 규칙은 **Well known**(수준 5) 사이트도 자동으로 허용합니다.

규칙의 규칙 작업을 변경할 경우, 시스템에서는 위에 언급한 사항에 따라 URL 조건의 평판 수준을 자동으로 변경합니다.

5단계 **Add to Rule**을 클릭하거나 선택한 항목을 **Selected Categories** 목록에 추가합니다.

선택한 항목을 끌어서 놓을 수도 있습니다.

6단계 규칙을 저장하거나 계속 수정합니다.

변경 사항을 구현하려면 SSL 정책과 연결된 액세스 제어 정책을 적용해야 합니다(12-15페이지의 액세스 제어 정책 적용 참조).

URL 탐지 및 차단의 제한 사항

라이센스: URL 필터링

지원되는 디바이스: Series 3

URL 탐지 및 차단을 수행할 경우 다음 사항에 유의해야 합니다.

URL 식별 속도

시스템에서는 다음이 구현되지 않으면 URL 카테고리를 분류할 수 없습니다.

- 클라이언트와 서버 간에 모니터링된 연결 설정
- 세션의 HTTPS 애플리케이션 식별
- 클라이언트 hello 메시지 또는 서버 인증서를 통해 요청된 URL 식별

이러한 식별은 서버 인증서 교환 후에 이루어집니다. 핸드셰이크 중에 교환된 트래픽이 URL 조건을 포함하는 SSL 규칙의 모든 다른 조건과 매칭되지만 식별이 완료되지 않은 경우, SSL 정책을 사용하여 패킷을 통과하도록 할 수 있습니다. 이러한 동작을 통해 연결을 설정하여 URL을 식별할 수 있습니다. 사용자의 편의를 위해, 영향을 받은 규칙은 정보 아이콘( )으로 표시됩니다.

시스템에서 식별을 완료하면, URL 조건과 매칭되는 나머지 세션 트래픽에 SSL 규칙 작업을 적용합니다.

URL의 검색 쿼리 매개변수

시스템에서는 URL의 검색 쿼리 매개변수를 사용하여 URL을 매칭하지 않습니다. 예를 들어, 모든 쇼핑 트래픽을 차단하는 시나리오를 가정해보십시오. 이 경우 웹 검색을 사용하여 amazon.com을 검색하는 작업은 차단되지 않지만, amazon.com을 탐색하는 것은 차단됩니다.

암호화 속성을 기준으로 트래픽 제어

라이센스: 모든

지원되는 디바이스: Series 3

암호화된 연결 특성을 기준으로, 암호화된 트래픽을 처리하고 해독하는 SSL 규칙을 생성할 수 있습니다. 세션을 암호화하고, 이에 따라 트래픽을 처리하는 데 사용되는 프로토콜 버전 또는 암호 그룹을 탐지할 수 있습니다. 또한 다음과 같은 인증서 특성을 기준으로 서버 인증서를 탐지하고 트래픽을 처리할 수 있습니다.

- 서버 인증서
- 인증서 발급자(CA 발급 인증서인지 또는 자체 서명 인증서인지 확인)
- 인증서 보유자
- 다양한 인증서 상태(예: 인증서가 유효한지 또는 CA 발급에 의해 취소된 것인지 확인)

규칙의 여러 암호 그룹, 인증서 발급자 또는 인증서 보유자를 탐지하려는 경우, 재사용 가능한 암호 그룹 및 고유 이름 객체를 생성하고 이를 규칙에 추가할 수 있습니다. 서버 인증서 및 특정 인증서 상태를 탐지하려면 해당 규칙에 대한 외부 인증서 및 외부 CA 객체를 생성해야 합니다.

자세한 내용은 다음 절을 참조하십시오.

- 22-19페이지의 암호화된 트래픽을 인증서 고유 이름으로 제어
- 22-21페이지의 암호화된 트래픽을 인증서로 제어
- 22-23페이지의 암호화된 트래픽을 인증서 상태로 제어
- 22-27페이지의 암호화된 트래픽을 암호 그룹으로 제어
- 22-28페이지의 트래픽을 암호화 프로토콜 버전으로 제어

암호화된 트래픽을 인증서 고유 이름으로 제어

라이센스: 모든

지원되는 디바이스: Series 3

SSL 규칙의 고유 이름 조건을 사용하면 서버 인증서를 발급한 CA 또는 인증서 보유자를 기준으로, 암호화된 트래픽을 처리하고 검사할 수 있습니다. 발급자 고유 이름에 따라, 사이트의 서버 인증서를 발급한 CA를 기준으로 트래픽을 처리할 수 있습니다.

규칙 조건을 구성할 경우 리터럴 값을 수동으로 지정하고, 고유 이름 객체를 참조하거나 여러 객체가 포함된 고유 이름 그룹을 참조할 수 있습니다.

참고 **Decrypt - Known Key** 작업도 선택할 경우 고유 이름 조건을 구성할 수 없습니다. 이 작업은 서버 인증서를 선택하여 트래픽을 해독해야 하므로, 인증서가 트래픽과 이미 매칭됩니다. 자세한 내용은 21-10페이지의 Decrypt Actions: Decrypting Traffic for Further Inspection을/를 참조하십시오.

단일한 인증서 상태 규칙 조건의 여러 주체 및 발급자 고유 이름을 대상으로 매칭할 수 있습니다. 규칙과 매칭하려면 하나의 공용 또는 고유 이름만 매칭해야 합니다.

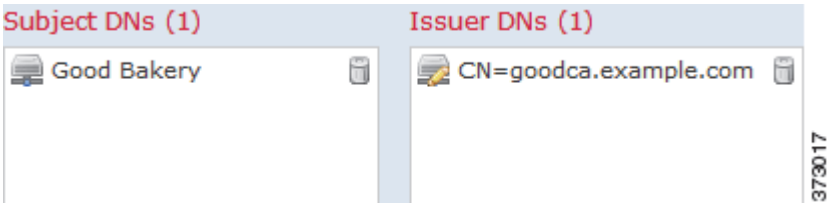
고유 이름을 수동으로 추가할 경우, 공용 이름 특성(**CN**)을 포함할 수 있습니다. CN=이 없는 공용 이름을 추가하면 객체를 저장하기 전에 CN=이 추가됩니다.

다음 표에 나열된 각 특성 중 하나와 함께 쉼표로 구분하여 DN을 추가할 수 있습니다.

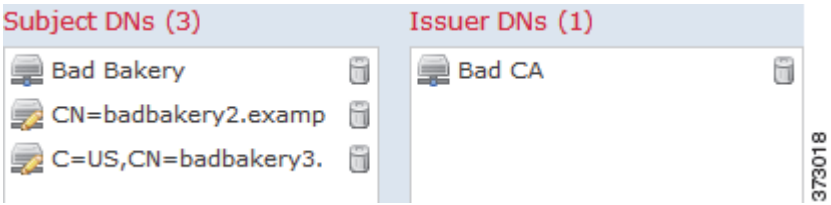
표 22-3 고유 이름 속성

특성	설명	허용 값
C	국가 코드	영문자 2개
CN	공용 이름	최대 64개의 영숫자, 백슬래시(\), 하이픈(-), 따옴표("), 별표(*), 마침표(.) 또는 공백 문자
O	조직	
OU	조직 단위	

다음 표에는 goodbakery.example.com에 발급되었거나 goodca.example.com에서 발급한 인증서를 검색하는 고유 이름 규칙이 나와 있습니다. 이러한 인증서로 암호화된 트래픽은 허용되며 액세스 제어 규칙의 대상이 됩니다.



다음 표에는 badbakery.example.com에 발급된 인증서 및 연결된 도메인, 또는 badca.example.com에서 발급한 인증서를 검색하는 고유 이름 규칙 조건이 나와 있습니다. 이러한 인증서로 암호화된 트래픽은 재서명된 인증서를 사용하여 해독됩니다.



단일한 DN 조건에서 최대 50개의 리터럴 값 및 고유 이름 객체를 **Subject DNs**에 추가하고, 50개의 리터럴 값 및 고유 이름 객체를 **Issuer DNs**에 추가할 수 있습니다.

시스템에서 제공된 DN 객체 그룹인 Sourcefire Undecryptable Sites에는 시스템이 해독할 수 없는 트래픽이 있는 웹 사이트가 포함됩니다. 이 그룹을 DN 조건에 추가하면, 이러한 웹 사이트에서 나가고 들어오는 트래픽을 차단하거나 해독하지 않도록 할 수 있으므로, 트래픽 해독을 시도하느라 시스템 리소스를 낭비하지 않아도 됩니다. 이 그룹의 개별 항목을 수정할 수 있습니다. 단, 이 그룹은 삭제할 수 없습니다. 시스템 업데이트로 인해 이 목록의 항목이 수정될 수 있으나, 사용자 변경 사항은 그대로 유지됩니다.

암호화된 트래픽을 인증서 주체 또는 발급자 고유 이름을 기준으로 검사하려면

액세스: Admin/Access Admin/Network Admin

1단계 인증서 주체 또는 발급자 고유 이름별로 암호화된 트래픽을 제어하려는 SSL 정책에서 새로운 SSL 규칙을 생성하거나 기존 규칙을 수정합니다.

자세한 지침은 21-4페이지의 SSL 규칙 이해 및 생성을/를 참조하십시오.

2단계 SSL 규칙 편집기에서 DN 탭을 선택합니다.

DN 탭이 나타납니다.

3단계 **Available DNs**에서 추가할 네트워크를 다음과 같이 찾아 선택합니다.

- 고유 이름 객체를 즉시 추가한 다음 조건에 추가하려면, **Available DNs** 목록 위의 추가 아이콘 ( )을 클릭합니다(3-41페이지의 DN 객체 작업 참조).
- 추가할 고유 이름 객체 및 그룹을 검색하려면, **Available DNs** 목록 위의 **Search by name or value** 프롬프트를 클릭한 다음 객체의 이름을 입력하거나, 객체의 값을 입력합니다. 입력을 수행하면 목록이 업데이트되어 매칭되는 객체를 표시합니다.

객체를 선택하려면 클릭합니다. 여러 객체를 선택하려면 Shift +Ctrl 키를 사용하거나, 마우스 오른쪽 버튼을 클릭한 다음 **Select All**을 선택합니다.

4단계 다음 옵션을 이용할 수 있습니다.

- **Add to Subject**를 클릭하여 선택한 객체를 **Subject DNs** 목록에 추가합니다.
- **Add to Issuer**를 클릭하여 선택한 객체를 **Issuer DNs** 목록에 추가합니다.

선택한 객체를 끌어서 놓을 수도 있습니다.

5단계 수동으로 지정할 리터럴 공용 이름 또는 고유 이름을 추가합니다.

Subject DNs 또는 **Issuer DNs** 목록 아래의 **Enter DN or CN** 프롬프트를 클릭한 다음, 공용 이름 또는 고유 이름을 입력하고 **Add**를 클릭합니다.

6단계 규칙을 추가하거나 계속 수정합니다.

변경 사항을 구현하려면 SSL 정책과 연결된 액세스 제어 정책을 적용해야 합니다(12-15페이지의 액세스 제어 정책 적용 참조).

암호화된 트래픽을 인증서로 제어

라이센스: 모든

지원되는 디바이스: Series 3

SSL 규칙의 인증서 조건을 사용하면 트래픽을 암호화하는 데 사용된 서버 인증서를 기준으로, 암호화된 트래픽을 처리하고 검사할 수 있습니다. 하나 이상의 인증서로 규칙을 구성할 수 있습니다. 인증서가 조건의 모든 인증서와 매칭될 경우, 트래픽은 규칙과 매칭됩니다.

인증서 기반 SSL 규칙 조건을 만들 경우, 서버 인증서를 업로드할 수 있습니다. 인증서를 재사용 가능한 외부 인증서 *객체*로 저장하고, 이름을 서버 인증서와 연결할 수 있습니다. 또는 기존 외부 인증서 객체 및 객체 그룹으로 인증서 조건을 구성할 수 있습니다.

다음과 같은 인증서 고유 이름 특성을 기준으로, 외부 인증서 객체 및 객체 그룹에 따라 규칙 조건의 **Available Certificates** 필드를 검색할 수 있습니다.

- 주체 또는 발급자 공용 이름(CN)
- 주체 또는 발급자 조직(O)
- 주제 또는 발급자 부서(OU)

단일한 인증거 규칙 조건의 여러 인증서와 매칭되도록 선택할 수 있습니다. 업로드된 인증서와 매칭되는 트래픽을 암호화하는 데 인증서가 사용된 경우, 암호화된 트래픽은 규칙과 매칭됩니다.

단일한 인증서 조건에서 최대 50개의 외부 인증서 객체 및 외부 인증서 객체 그룹을 **Selected Certificates**에 추가할 수 있습니다.

다음에 유의하십시오.

- **Decrypt - Known Key** 작업도 선택할 경우 인증서 조건을 구성할 수 없습니다. 이 작업은 서버 인증서를 선택하여 트래픽을 해독해야 하므로, 이렇게 할 경우 인증서가 트래픽과 이미 매칭됩니다. 자세한 내용은 21-10페이지의 Decrypt Actions: Decrypting Traffic for Further Inspection을/를 참조하십시오.
- 외부 인증서 객체가 포함된 인증서 조건을 구성할 경우, 암호 그룹 조건에 추가하는 모든 암호 그룹 또는 **Decrypt - Resign** 작업에 연결되는 내부 CA 객체는 외부 인증서의 시그니처 알고리즘 유형과 매칭되어야 합니다. 예를 들어, 규칙의 인증서 조건이 EC 기반 서버 인증서를 참조할 경우, 추가되는 모든 암호 그룹 또는 **Decrypt - Resign** 작업과 연결되는 CA 인증서도 EC 기반이어야 합니다. 이때 시그니처 알고리즘 유형이 매칭되지 않을 경우, 정책 편집기에서는 규칙 옆에 경고 아이콘이 표시됩니다. 자세한 내용은 22-27페이지의 암호화된 트래픽을 암호 그룹으로 제어 및 21-10페이지의 Decrypt Actions: Decrypting Traffic for Further Inspection을/를 참조하십시오.

암호화된 트래픽을 서버 인증서를 기준으로 검사하려면

액세스: Admin/Access Admin/Network Admin

1단계 서버 인증서를 기반으로 암호화된 트래픽을 제어하려는 SSL 정책에서 새로운 SSL 규칙을 생성하거나 기존 규칙을 수정합니다.

자세한 지침은 21-4페이지의 SSL 규칙 이해 및 생성을/를 참조하십시오.

2단계 SSL 규칙 편집기에서 Certificate 탭을 선택합니다.

Certificate 탭이 나타납니다.

3단계 **Available Certificates**에서 추가할 서버 인증서를 다음과 같이 찾아 선택합니다.

- 외부 인증서 객체를 즉시 추가한 다음 조건에 추가하려면, **Available Certificates** 목록 위의 추가 아이콂( )을 클릭합니다(3-50페이지의 외부 인증 기관 객체 작업 참조).
- 추가할 인증서 객체 및 그룹을 검색하려면, **Available Certificates** 목록 위의 **Search by name or value** 프롬프트를 클릭한 다음 객체의 이름을 입력하거나, 객체의 값을 입력합니다. 입력을 수행하면 목록이 업데이트되어 매칭되는 객체를 표시합니다.

객체를 선택하려면 클릭합니다. 여러 객체를 선택하려면 Shift +Ctrl 키를 사용하거나, 마우스 오른쪽 버튼을 클릭한 다음 **Select All**을 선택합니다.

4단계 **Add to Rule**을 클릭하여 선택한 객체를 **Subject Certificates** 목록에 추가합니다.

선택한 객체를 끌어서 놓을 수도 있습니다.

5단계 규칙을 추가하거나 계속 수정합니다.

변경 사항을 구현하려면 SSL 정책과 연결된 액세스 제어 정책을 적용해야 합니다(12-15페이지의 액세스 제어 정책 적용 참조).

암호화된 트래픽을 인증서 상태로 제어

라이센스: 모든

지원되는 디바이스: Series 3

SSL 규칙의 인증서 상태 조건을 사용하면 트래픽을 암호화하는 데 사용된 서버 인증서의 상태(예: 인증서의 유효성, 취소, 만료, 아직 유효하지 않음, 자체 서명 여부, 신뢰할 수 있는 CA의 서명 여부)를 기준으로 암호화된 트래픽을 처리하고 검사할 수 있습니다.

CA가 인증서를 발급하거나 취소했는지 확인하려면 루트 및 중간 CA 인증서와 관련 CRL을 객체로 업로드해야 합니다. 그런 다음 이러한 신뢰할 수 있는 CA 객체를 SSL 정책의 신뢰할 수 있는 CA 인증서 목록에 추가합니다.

구성하는 각 인증서 상태 SSL 규칙 조건을 위해, 지정된 상태가 있는 경우 또는 없는 경우에 대해 트래픽을 매칭할 수 있습니다. 하나의 규칙 조건에서 여러 개의 상태를 선택할 수 있습니다. 인증서가 선택한 상태와 매칭되는 경우, 규칙은 트래픽과 매칭됩니다.

자세한 내용은 다음 링크를 참고하십시오.

- 22-23페이지의 외부 인증 기관 신뢰
- 22-24페이지의 인증서 상태를 기준으로 트래픽 매칭

외부 인증 기관 신뢰

라이센스: 모든

지원되는 디바이스: Series 3

루트 및 중간 CA 인증서를 SSL 정책에 추가하여 CA를 신뢰할 수 있으며, 그런 다음 이러한 신뢰할 수 있는 CA를 활용하면 트래픽을 암호화하는 데 사용된 서버 인증서를 식별할 수 있습니다. 식별된 서버 인증서에는 신뢰할 수 있는 CA가 서명한 인증서가 포함됩니다.

신뢰할 수 있는 CA 인증서에 업로드된 CRL(Certificate Revocation List: 인증서 폐기 목록)이 포함되어 있는 경우, 신뢰할 수 있는 CA가 암호 인증서를 취소한 것인지 확인할 수도 있습니다. 자세한 내용은 3-49페이지의 신뢰받는 CA 객체에 CRL 추가을/를 참조하십시오.

신뢰할 수 있는 CA 인증서를 SSL 정책에 추가한 후에는, 다양한 인증서 상태 조건이 포함된 SSL 규칙을 구성하여 이 트래픽에 대해 매칭할 수 있습니다. 자세한 내용은 3-48페이지의 신뢰받는 인증 기관 객체 작업 및 22-23페이지의 암호화된 트래픽을 인증서 상태로 제어을/를 참조하십시오.

팁 루트 CA의 트러스트 체인 내의 모든 인증서를 신뢰할 수 있는 CA 인증서 목록에 업로드하며, 여기에는 루트 CA 인증서 및 모든 중간 CA 인증서가 포함됩니다. 이렇게 하지 않으면 중간 CA가 발급한 신뢰할 수 있는 인증서를 탐지하는 것이 더 어려워집니다.

SSL 정책을 생성할 경우, 시스템은 Trusted CA Certificates 탭을 기본 Trusted CA 객체 그룹인 Sourcefire Trusted Authorities로 채웁니다. 그룹의 개별 항목을 수정하고, 이 그룹을 SSL 정책에 포함할지 선택할 수 있습니다. 단, 이 그룹은 삭제할 수 없습니다. 시스템 업데이트로 인해 이 목록의 항목이 수정될 수 있으나, 사용자 변경 사항은 그대로 유지됩니다. 자세한 내용은 20-2페이지의 기본 SSL 정책 생성을/를 참조하십시오.

신뢰할 수 있는 CA를 정책에 추가하려면

액세스: Admin/Access Admin/Network Admin

1단계 **Policies > SSL**을 선택합니다.

SSL Policy 페이지가 나타납니다.

2단계 구성할 SSL 정책 옆의 수정 아이콘( )을 클릭합니다.

SSL 정책 편집기가 나타납니다.

3단계 **Trusted CA Certificates** 탭을 선택합니다.

Trusted CA Certificates 페이지가 나타납니다.

4단계 **Available Trusted CAs**에서 추가할 신뢰할 수 있는 CA를 다음과 같이 찾아 선택합니다.

- 신뢰할 수 있는 CA 객체를 즉시 추가한 다음 조건에 추가하려면, **Available Trusted CAs** 목록 위의 추가 아이콘( )을 클릭합니다(3-48페이지의 신뢰받는 인증 기관 객체 작업 참조).
- 추가할 신뢰할 수 있는 CA 객체 및 그룹을 검색하려면, **Available Trusted CAs** 목록 위의 **Search by name or value** 프롬프트를 클릭한 다음 객체의 이름을 입력하거나, 객체의 값을 입력합니다. 입력을 수행하면 목록이 업데이트되어 매칭되는 객체를 표시합니다.

객체를 선택하려면 클릭합니다. 여러 객체를 선택하려면 Shift +Ctrl 키를 사용하거나, 마우스 오른쪽 버튼을 클릭한 다음 **Select All**을 선택합니다.

5단계 **Add to Rule**을 클릭하거나 선택한 객체를 **Selected Trusted CAs** 목록에 추가합니다.

선택한 객체를 끌어서 놓을 수도 있습니다.

6단계 규칙을 추가하거나 계속 수정합니다.

변경 사항을 구현하려면 SSL 정책과 연결된 액세스 제어 정책을 적용해야 합니다(12-15페이지의 액세스 제어 정책 적용 참조).

인증서 상태를 기준으로 트래픽 매칭

라이센스: 모든

지원되는 디바이스: Series 3

인증서 상태 규칙 조건 컨피그레이션을 기준으로, 트래픽을 암호화하는 데 사용된 서버 인증서의 상태에 따라 암호화된 트래픽을 매칭할 수 있습니다. 다음이 가능합니다.

- 서버 인증서 상태 확인
- 인증서에 상태가 없는지 확인
- 인증서 상태가 있는지 없는지 확인하는 작업 건너뛰기

단일한 인증서 상태 규칙 조건에 여러 인증서 상태가 있는 경우 또는 없는 경우와 매칭하도록 선택할 수 있습니다. 인증서는 규칙과 매칭하는 조건 중 하나에만 매칭되어야 합니다.

다음 표에는 시스템에서 암호화하는 서버 인증서 상태를 기준으로, 암호화된 트래픽을 평가하는 방법이 설명되어 있습니다.

표 22-4 인증서 상태 규칙 조건 기준

상태 확인	상태가 **Yes**로 설정	상태가 **No**로 설정
Revoked	정책이 서버 인증서를 발급한 CA를 신뢰하며, 정책에 업로드된 CA 인증서에 서버 인증서를 취소하는 CRL이 포함되어 있습니다.	정책이 서버 인증서를 발급한 CA를 신뢰하며, 정책에 업로드된 CA 인증서에 해당 인증서를 취소하는 CRL이 포함되어 있지 않습니다.
Self-signed	탐지된 서버 인증서에 동일한 주체 및 발급자 고유 이름이 포함되어 있습니다.	탐지된 서버 인증서에 다른 주체 및 발급자 고유 이름이 포함되어 있습니다.
Valid	다음의 모든 사항이 유효합니다. • 정책이 인증서를 발급한 CA를 신뢰함 • 시그니처가 유효함 • 발급자가 유효함 • 정책의 신뢰할 수 있는 CA가 인증서를 취소하지 않음 • 현재 날짜가 인증서의 유효 시작일과 유효 만료일 사이에 해당함	다음 중 하나 이상이 유효하지 않습니다. • 정책이 인증서를 발급한 CA를 신뢰하지 않음 • 서명이 유효하지 않음 • 발급자가 유효하지 않음 • 정책의 신뢰할 수 있는 CA가 인증서를 취소함 • 현재 날짜가 인증서의 유효 시작일보다 이전임 • 현재 날짜가 인증서의 유효 만료일을 경과함
Invalid signature	인증서의 시그니처를 인증서의 내용과 올바르게 확인할 수 없습니다.	인증서의 시그니처를 인증서의 내용과 올바르게 확인할 수 있습니다.
Invalid issuer	발급자 CA 인증서가 정책의 신뢰할 수 있는 CA 인증서 목록에 저장되지 않습니다.	발급자 CA 인증서가 정책의 신뢰할 수 있는 CA 인증서 목록에 저장됩니다.
Expired	현재 날짜가 인증서의 유효 만료일을 경과했습니다.	현재 날짜가 유효 만료일 이전이거나 해당일입니다.
Not yet valid	현재 날짜가 인증서의 유효 시작일보다 이전입니다.	현재 날짜가 유효 시작일 이후이거나 해당일입니다.

다음과 같은 사례를 가정해보십시오. 조직에서는 Verified Authority 인증 기관을 신뢰합니다. 조직에서는 Spammer Authority 인증 기관을 신뢰하지 않습니다. 시스템 관리자가 Verified Authority 인증서 및 Verified Authority에서 발급한 중간 CA 인증서를 시스템에 업로드합니다. Verified Authority가 이전에 발급한 인증서를 취소했으므로, 시스템 관리자는 Verified Authority가 배포한 CRL을 업로드합니다.

다음 그래픽에는 유효한 인증서를 확인하는 인증서 상태 규칙 조건이 나와 있습니다. 이러한 인증서는 Verified Authority에서 발급하였으며, CRL에 포함되지 않고, 유효 시작일과 유효 만료일 사이의 기간이 아직 남아 있는 상태입니다. 이러한 인증서로 암호화된 트래픽은 컨피그레이션으로 인해, 액세스 제어를 통해 해독 및 검사되지 않습니다.

다음 그래픽에는 상태가 없는지 확인하는 인증서 상태 규칙 조건이 나와 있습니다. 이 경우 컨피그레이션으로 인해, 만료되지 않은 인증서로 암호화된 트래픽과 매칭을 수행하며 해당 트래픽을 모니터링합니다.

다음 그래픽에는 몇 가지 상태가 있는 경우 또는 없는 경우와 매칭하는 인증서 상태 규칙 조건이 나와 있습니다. 잘못된 사용자(자체 서명 사용자, 유효하지 않거나 만료된 사용자)가 발급한 인증서로 암호화된 수신 트래픽과 규칙이 매칭할 경우, 컨피그레이션으로 인해 Known Key로 트래픽을 해독합니다.

인증서는 여러 상태와 매칭될 수 있으나, 규칙은 트래픽에 대한 작업을 한 번만 수행합니다.

암호화된 트래픽을 서버 인증서 상태로 검사하려면

액세스: Admin/Access Admin/Network Admin

1단계 서버 인증서 상태를 기반으로 암호화된 트래픽을 제어하려는 SSL 정책에서 새로운 SSL 규칙을 생성하거나 기존 규칙을 수정합니다.

자세한 지침은 21-4페이지의 SSL 규칙 이해 및 생성을/를 참조하십시오.

2단계 SSL 규칙 편집기에서 Cert Status 탭을 선택합니다.

Cert Status 탭이 나타납니다.

3단계 각 인증서 상태에는 다음과 같은 옵션이 있습니다.

- **Yes**를 선택하여 인증서 상태가 있는 경우와 매칭합니다.
- **No**를 선택하여 인증서 상태가 없는 경우와 매칭합니다.
- **Do Not Match**를 선택하여 인증서 상태와 매칭하지 않습니다.

4단계 규칙을 추가하거나 계속 수정합니다.

변경 사항을 구현하려면 SSL 정책과 연결된 액세스 제어 정책을 적용해야 합니다(12-15페이지의 액세스 제어 정책 적용 참조).

암호화된 트래픽을 암호 그룹으로 제어

라이센스: 모든

지원되는 디바이스: Series 3

SSL 규칙의 암호 그룹 조건을 사용하면 암호화된 세션을 협상하는 데 사용된 암호 그룹을 기준으로, 암호화된 트래픽을 처리하고 검사할 수 있습니다. Cisco에서는 암호 그룹 규칙 조건에 추가할 수 있는 미리 정의된 암호 그룹을 제공합니다. 여러 암호 그룹이 포함된 암호 그룹 목록 객체를 추가할 수도 있습니다. 암호 그룹 목록에 대한 자세한 내용은 3-40페이지의 암호 그룹 목록 작업을/를 참조하십시오.

참고 새 암호 그룹을 추가할 수 없습니다. 또한 미리 정의된 암호 그룹을 수정하거나 삭제할 수 없습니다.

단일한 암호 그룹 조건의 **Selected Cipher Suites**에 최대 50개의 암호 그룹 및 암호 그룹 목록을 추가할 수 있습니다.

다음에 유의하십시오.

- 구축 환경에서 지원하지 않는 암호 그룹을 추가할 경우, SSL 정책과 연결된 액세스 제어 정책을 적용할 수 없습니다. 예를 들어, 패시브 구축은 단명 Diffie-Hellman(DHE) 또는 타원 곡선 Diffie-Hellman(ECDHE) 암호 그룹으로 트래픽의 해독을 지원하지 않습니다. 이러한 암호 그룹이 포함된 규칙을 생성할 경우 액세스 제어 정책을 적용할 수 없습니다.
- 암호 그룹이 포함된 암호 그룹 조건을 구성할 경우, 인증서 조건에 추가하는 외부 인증서 객체 또는 **Decrypt - Resign** 작업에 연결되는 내부 CA 객체는 암호 그룹의 시그니처 알고리즘 유형과 매칭되어야 합니다. 예를 들어, 규칙의 암호 그룹 조건이 EC 기반 암호 그룹을 참조할 경우, 추가되는 모든 서버 인증서 또는 **Decrypt - Resign** 작업과 연결되는 CA 인증서도 EC 기반이어야 합니다. 이때 시그니처 알고리즘 유형이 매칭되지 않을 경우, 정책 편집기에서는 규칙 옆에 경고 아이콘이 표시됩니다. 자세한 내용은 22-27페이지의 암호화된 트래픽을 암호 그룹으로 제어 및 21-10페이지의 Decrypt Actions: Decrypting Traffic for Further Inspection을/를 참조하십시오.
- 시스템에서는 익명 암호 그룹으로 암호화된 트래픽을 해독할 수 없습니다. 익명 암호 그룹을 **Cipher Suite** 조건에 추가할 경우, SSL 규칙에서 **Decrypt - Resign** 또는 **Decrypt - Known Key** 작업을 사용할 수 없습니다.

암호화된 트래픽을 암호 그룹으로 검사하려면

액세스: Admin/Access Admin/Network Admin

1단계 암호 그룹별로 암호화된 트래픽을 제어하려는 SSL 정책에서 새로운 SSL 규칙을 생성하거나 기존 규칙을 수정합니다.

자세한 지침은 21-4페이지의 SSL 규칙 이해 및 생성을/를 참조하십시오.

2단계 SSL 규칙 편집기에서 Cipher Suite 탭을 선택합니다.

Cipher Suite 탭이 나타납니다.

3단계 **Available Cipher Suites**에서 추가할 암호 그룹을 다음과 같이 찾아 선택합니다.

- 암호 그룹 목록을 즉시 추가한 다음 조건에 추가하려면, **Available Cipher Suites** 목록 위의 추가 아이콘( )을 클릭합니다(3-40페이지의 암호 그룹 목록 작업 참조).
- 추가할 암호 그룹 및 목록을 검색하려면, **Available Cipher Suites** 목록 위의 **Search by name or value** 프롬프트를 클릭한 다음 암호 그룹의 이름을 입력하거나 암호 그룹의 값을 입력합니다. 입력을 수행하면 목록이 업데이트되어 매칭되는 암호 그룹을 표시합니다.

암호 그룹을 선택하려면 클릭합니다. 여러 암호 그룹을 선택하려면 Shift +Ctrl 키를 사용하거나, 마우스 오른쪽 버튼을 클릭한 다음 **Select All**을 선택합니다.

4단계 **Add to Rule**을 클릭하여 선택한 암호 그룹을 **Selected Cipher Suites** 목록에 추가합니다.

선택한 암호 그룹을 끌어서 놓을 수도 있습니다.

5단계 규칙을 추가하거나 계속 수정합니다.

변경 사항을 구현하려면 SSL 정책과 연결된 액세스 제어 정책을 적용해야 합니다(12-15페이지의 액세스 제어 정책 적용 참조).

트래픽을 암호화 프로토콜 버전으로 제어

라이센스: 모든

지원되는 디바이스: Series 3

SSL 규칙의 세션 조건을 사용하면 트래픽을 암호화하는 데 사용된 SSL 또는 TLS 버전을 기준으로, 암호화된 트래픽을 검사할 수 있습니다. SSL 버전 3.0, 또는 TLS 버전 1.0, 1.1, 1.2로 암호화된 트래픽과 매칭되도록 선택할 수 있습니다. 기본적으로, 규칙을 생성할 때 모든 프로토콜 버전이 선택됩니다. 여러 버전을 선택할 경우, 선택한 버전과 매칭되는 암호화된 트래픽은 규칙과 매칭됩니다. 규칙 조건을 저장할 경우 하나 이상의 프로토콜 버전을 선택해야 합니다.

참고 SSL v2.0은 버전 규칙 조건에서 선택할 수 없습니다. 시스템에서는 SSL 버전 2.0으로 암호화된 트래픽의 해독을 지원하지 않습니다. 해독 불가능한 작업을 구성하여 추가 검사 없이 이 트래픽을 허용하거나 차단하도록 할 수 있습니다. 자세한 내용은 38-13페이지의 SSL 규칙으로 해독 가능 연결 로깅을/를 참조하십시오.

암호화된 트래픽을 SSL 또는 TLS 버전으로 검사하려면

액세스: Admin/Access Admin/Network Admin

1단계 암호화 프로토콜 버전별로 암호화된 트래픽을 제어하려는 SSL 정책에서 새로운 SSL 규칙을 생성하거나 기존 규칙을 수정합니다.

자세한 지침은 21-4페이지의 SSL 규칙 이해 및 생성을/를 참조하십시오.

2단계 SSL 규칙 편집기에서 Version 탭을 선택합니다.

Version 탭이 나타납니다.

3단계 **SSL v3.0**, **TLS v1.0**, **TLS v1.1**, **TLS v1.2** 중에서 매칭할 프로토콜 버전을 선택합니다.

4단계 규칙을 추가하거나 계속 수정합니다.

변경 사항을 구현하려면 SSL 정책과 연결된 액세스 제어 정책을 적용해야 합니다(12-15페이지의 액세스 제어 정책 적용 참조).

23장

네트워크 분석 및 침입 정책 이해

네트워크 분석 및 침입 정책은 FireSIGHT 시스템 침입 탐지 및 방지 기능의 일부로 함께 작동합니다. *침입 탐지*란 용어는 일반적으로 네트워크 트래픽에서 잠재적인 침입을 수동적으로 분석하고 보안 분석을 위한 공격 데이터를 저장하는 프로세스를 말합니다. *침입 방지*란 용어에는 침입 탐지의 개념이 포함되지만, 악성 트래픽이 네트워크를 통과할 때 이를 차단 또는 변경하는 기능이 추가됩니다.

침입 방지 구축에서 시스템이 패킷을 검토할 때:

- **네트워크 분석 정책**은 트래픽(특히 침입 시도의 신호일 수 있는 변칙적인 트래픽)이 추가로 평가될 수 있도록 *디코딩* 및 *전처리*되는 방법을 제어합니다.
- **침입 정책**은 패턴을 기반으로 디코딩된 공격용 패킷을 검토하기 위해 *침입 및 프리프로세서 규칙*(*침입 규칙*으로 총칭)을 사용합니다. 침입 정책은 네트워크 환경을 정확하게 반영하는 명명된 값을 사용할 수 있도록 지원하는 *변수 집합*과 쌍을 이룹니다.

네트워크 분석과 침입 정책 모두 상위 액세스 제어 정책에 의해 호출되지만 그 시점은 다릅니다. 시스템이 트래픽을 분석할 때, 침입 방지(추가 전처리 및 침입 규칙) 단계 전에 이와 별도로 네트워크 분석(디코딩 및 전처리) 단계가 발생합니다. 네트워크 분석 및 침입 정책은 폭넓고 심층적인 패킷 검사를 제공합니다. 이 둘을 함께 사용하면 호스트 및 호스트 데이터의 가용성, 무결성 및 신뢰성을 위협할 수 있는 네트워크 트래픽을 탐지하고 알리고 방지할 수 있습니다.

FireSIGHT 시스템에서는 상호 보완하고 함께 작동하는 비슷한 이름의 여러 네트워크 분석 및 침입 정책(예: Balanced Security and Connectivity)을 제공합니다. 시스템 제공 정책을 사용하면 Cisco VRT(Vulnerability Research Team)의 경험을 활용할 수 있습니다. 이러한 정책에 대해 VRT는 침입 및 프리프로세서 규칙 상태를 설정하며, 프리프로세서 및 기타 고급 설정에 대한 초기 컨피그레이션을 제공합니다.

사용자 지정 네트워크 분석 및 침입 정책을 생성할 수도 있습니다. 관리되는 디바이스의 성능을 향상하고 여기에서 생성되는 이벤트에 더욱 효과적으로 대응할 수 있도록 가장 중요한 방식으로 트래픽을 검사하기 위해 사용자 지정 정책의 설정을 조정할 수 있습니다.

웹 인터페이스에서 유사한 정책 편집기를 사용하여 네트워크 분석 및 침입 정책을 생성, 수정, 저장 및 관리합니다. 정책의 한 유형을 수정할 때 웹 인터페이스의 왼쪽에는 탐색 패널이 나타나며, 오른쪽에는 다양한 컨피그레이션 페이지가 표시됩니다.

이 장에서는 네트워크 분석 및 침입 정책에서 제어하는 컨피그레이션의 유형에 대해 간략하게 살펴보고, 트래픽을 검토하고 정책 위반 레코드를 생성하기 위해 정책이 함께 작동하는 방법에 대해 설명하고, 정책 편집기 탐색에 대한 기본적인 정보를 제공합니다. 또한 사용자 지정 정책과 시스템 제공 정책 사용의 이점과 제한 사항에 대해서도 설명합니다. 자세한 내용은 다음 절을 참조하십시오.

침입 구축을 사용자 지정하려면 다음을 참조하십시오.

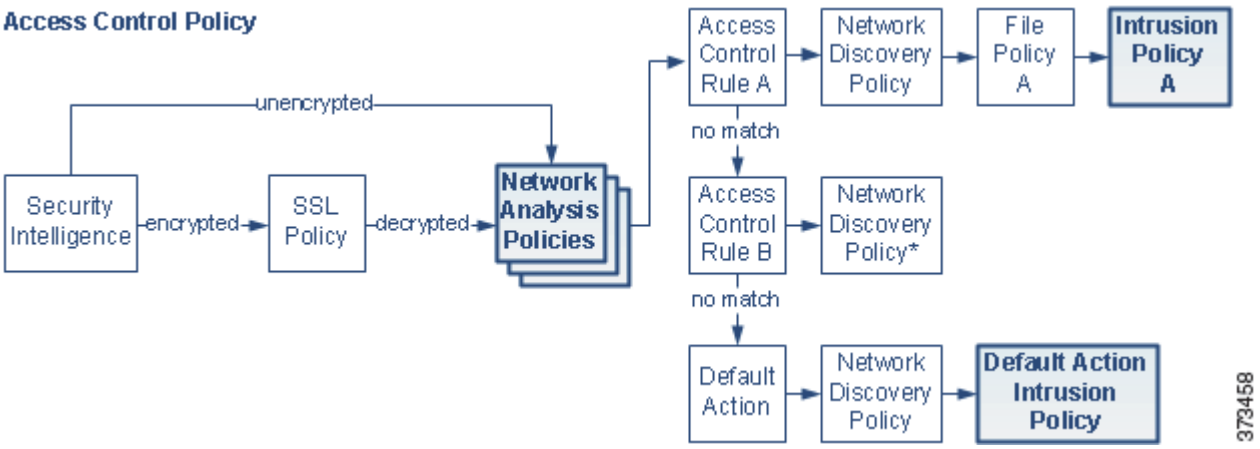
- 3-17페이지의 변수 집합 작업 - 네트워크 환경을 정확히 반영하기 위해 시스템의 침입 변수를 구성하는 방법에 대해 설명합니다. 사용자 지정 정책을 사용하지 않더라도 Cisco에서는 기본 변수 집합에서 기본 변수를 수정할 것을 **적극** 권장합니다. 고급 사용자는 하나 이상의 사용자 지정 침입 정책과 쌍을 이루도록 사용자 지정 변수 집합을 생성 및 사용할 수 있습니다.
- 31-1페이지의 침입 정책 시작하기 - 간단한 사용자 지정 침입 정책을 생성 및 수정하는 방법에 대해 설명합니다.
- 18-1페이지의 침입 정책 및 파일 정책을 사용하여 트래픽 제어 - 침입 정책과 상위 액세스 제어 정책을 연결함으로써 관심이 있는 트래픽만 검토하도록 침입 정책을 사용하여 시스템을 구성하는 방법에 대해 설명합니다. 또한 고급 침입 정책 성능 옵션을 구성하는 방법에 대해서도 설명합니다.
- 29-2페이지의 고급 Transport/Network 설정 구성 - 액세스 제어 정책의 대상 디바이스에서 처리되는 모든 트래픽에 전역적으로 적용되는 고급 전송 및 네트워크 프리프로세서 설정을 구성하는 방법에 대해 설명합니다. 이러한 고급 설정은 네트워크 분석 또는 침입 정책보다는 액세스 제어 정책에서 구성합니다.
- 26-1페이지의 네트워크 분석 정책 시작하기 - 간단한 사용자 지정 네트워크 분석 정책을 생성 및 수정하는 방법에 대해 설명합니다.
- 25-3페이지의 네트워크 분석 정책으로 전처리 맞춤화 - 기본 네트워크 분석 정책을 변경하는 방법에 대해 설명합니다. 이 절에서는 고급 사용자를 위해, 일치하는 트래픽을 전처리하도록 사용자 지정 네트워크 분석 정책을 할당함으로써 특정 보안 영역, 네트워크 및 VLAN에 대한 전처리를 맞춤화하는 방법에 대해서도 설명합니다.
- 24-1페이지의 네트워크 분석 또는 침입 정책에서 레이어 사용 - 좀 더 큰 조직이나 복잡한 구축에서 정책 *레이어*라는 구성 요소를 사용하여 여러 네트워크 분석 또는 침입 정책을 좀 더 효과적으로 관리하는 방법에 대해 설명합니다.

정책이 트래픽에서 침입을 검토하는 방법 이해

라이센스: 보호

시스템이 액세스 제어 구축의 일부로 트래픽을 분석할 때, 침입 방지(침입 규칙 및 고급 설정) 단계 이전에 이와 별도로 네트워크 분석(디코딩 및 전처리) 단계가 발생합니다.

다음 다이어그램에서는 인라인, 침입 방지 및 AMP(advanced malware protection) 구축에서 트래픽 분석의 순서를 간략하게 보여줍니다. 또한 액세스 제어 정책이 다른 정책을 호출하여 트래픽을 검토하는 방법 및 그러한 정책이 호출되는 순서를 보여줍니다. 네트워크 분석 및 침입 정책 선택 단계가 강조 표시되어 있습니다.



인라인 구축의 경우 시스템은 그림에 있는 프로세스의 거의 모든 단계에서 추가 검사 없이 트래픽을 차단할 수 있습니다. 보안 인텔리전스, SSL 정책, 네트워크 분석 정책, 파일 정책 및 침입 정책은 모두 트래픽을 삭제 또는 수정할 수 있습니다. 수동적으로 패킷을 검사하는 네트워크 검색 정책만으로는 트래픽의 플로우에 영향을 줄 수 없습니다.

마찬가지로 프로세스의 각 단계에서 패킷은 시스템이 이벤트를 생성하도록 할 수 있습니다. 침입 및 프리프로세서 이벤트(*침입 이벤트*로 총칭)는 패킷 또는 패킷의 내용에 보안 위험 있음을 나타내는 것입니다.

팁 SSL 검사 컨피그레이션이 통과를 허용하는 경우 또는 SSL 검사를 구성하지 않는 경우, 액세스 제어 규칙이 암호화된 트래픽을 처리하는 것이 이 다이어그램에는 반영되어 있지 않습니다. 기본적으로, 시스템에서는 암호화된 페이로드의 침입 및 파일 검사를 비활성화합니다. 이는 암호화 연결이 침입 및 파일 검사가 구성된 액세스 제어 규칙과 일치하는 경우 오탐을 줄이고 성능을 높이는 데 도움이 됩니다. 자세한 내용은 19-1페이지의 트래픽 해독 이해 및 27-70페이지의 SSL 프리프로세서 사용을/를 참조하십시오.

단일 연결의 경우 다이어그램에 보이는 것처럼, 시스템이 액세스 제어 규칙 이전에 네트워크 분석 정책을 선택하더라도 일부 전처리(특히 애플리케이션 레이어 전처리)는 액세스 제어 규칙 선택 이후 발생합니다. 이는 사용자 지정 네트워크 분석 정책에서 전처리를 구성하는 방법에 영향을 주지 **않습니다**.

자세한 내용은 다음 링크를 참고하십시오.

- 23-3페이지의 디코딩, 표준화 및 전처리: 네트워크 분석 정책
- 23-4페이지의 액세스 제어 규칙: 침입 정책 선택
- 23-5페이지의 침입 검사: 침입 정책, 규칙 및 변수 집합
- 23-6페이지의 침입 이벤트 생성

디코딩, 표준화 및 전처리: 네트워크 분석 정책

라이센스: 보호

프로토콜 차이가 패턴 매칭을 불가능하게 만들 수 있으므로 디코딩 및 전처리가 없으면 시스템은 트래픽에서 침입을 제대로 평가할 수 없습니다. 23-2페이지의 정책이 트래픽에서 침입을 검토하는 방법 이해의 다이어그램에서 볼 수 있듯이, 네트워크 분석 정책이 이러한 트래픽 처리 작업을 제어합니다.

- 보안 인텔리전스에 의해 트래픽이 필터링된 **후**
- 암호화된 트래픽이 선택적인 SSL 정책에 의해 해독된 **후**
- 트래픽을 파일 또는 침입 정책으로 검사할 수 있기 **전**

네트워크 분석 정책은 처리 단계에서 패킷을 제어합니다. 먼저 시스템은 처음 세 개의 TCP/IP 레이어를 통해 패킷을 디코딩한 다음, 계속해서 프로토콜 변칙을 표준화, 전처리 및 탐지합니다.

- 패킷 디코더는 패킷 헤더 및 페이로드를 프리프로세서(그리고 나중에 침입 규칙)에서 손쉽게 사용할 수 있는 형식으로 변환합니다. TCP/IP 스택의 각 레이어는 데이터 링크 레이어로 시작하여 계속해서 네트워크 및 전송 레이어를 통해 차례로 디코딩됩니다. 패킷 디코더는 또한 패킷 헤더에서 각종 비정상적인 동작을 탐지합니다. 자세한 내용은 29-17페이지의 패킷 디코딩 이해을/를 참조하십시오.
- 인라인 구축에서 인라인 표준화 프리프로세서는 공격자가 탐지를 회피할 가능성을 최소화하기 위해 트래픽의 형식을 변경(표준화)합니다. 다른 프리프로세서 및 침입 규칙에서 검토하도록 패킷을 준비하고, 시스템이 처리하는 패킷이 네트워크의 호스트에서 수신하는 패킷과 동일

한지 확인합니다. 자세한 내용은 29-7페이지의 인라인 트래픽 표준화을/를 참조하십시오.

팁 패시브 구축의 경우 Cisco는 네트워크 분석 레벨에서 인라인 표준화를 구성하는 대신 액세스 제어 정책 레벨에서 적응형 프로필을 구성할 것을 권장합니다. 자세한 내용은 30-1페이지의 수동 구축 시 전처리 튜닝을/를 참조하십시오.

- 다양한 네트워크 및 전송 레이어 프리프로세서는 IP 프래그먼트화를 악용하는 공격을 탐지하고, 체크섬을 검증하고, TCP 및 UDP 세션 전처리를 수행합니다. 29-1페이지의 전송 및 네트워크 레이어 전처리 구성을/를 참조하십시오.

  일부 고급 전송 및 네트워크 프리프로세서 설정은 액세스 제어 정책의 대상 디바이스에서 처리되는 모든 트래픽에 전역적으로 적용됩니다. 이러한 설정은 네트워크 분석 정책보다는 액세스 제어 정책에서 구성합니다. 29-2페이지의 고급 Transport/Network 설정 구성을/를 참조하십시오.

- 다양한 애플리케이션 레이어 프로토콜 디코더는 특정 패킷 데이터 유형을 침입 규칙 엔진이 분석할 수 있는 형식으로 표준화합니다. 애플리케이션 레이어 프로토콜 인코딩을 정규화함으로써 시스템에서는 데이터가 다르게 표현된 패킷에 동일한 콘텐츠 관련 침입 규칙을 효과적으로 적용하고 의미 있는 결과를 얻을 수 있습니다. 자세한 내용은 27-1페이지의 애플리케이션 레이어 프리프로세서 사용을/를 참조하십시오.

- Modbus 및 DNP3 SCADA 프리프로세서는 트래픽 변칙을 탐지하고 침입 규칙에 데이터를 제공합니다. SCADA(Supervisory Control and Data Acquisition) 프로토콜은 산업, 인프라 및 설비 공정(예: 제조, 생산, 물 처리, 전력 분배, 공항 및 배송 시스템 등)에서 데이터를 모니터링하고 제어하고 수집합니다. 자세한 내용은 28-1페이지의 SCADA 전처리 구성을/를 참조하십시오.

- 몇몇 프리프로세서에서는 Back Orifice, 포트스캔, SYN 플러드 및 기타 등급 기반 공격과 같은 특정 위협을 탐지할 수 있습니다. 34-1페이지의 특정 위협 탐지을/를 참조하십시오.

  침입 정책에서 ASCII 텍스트의 신용카드 번호 및 주민등록번호 같은 민감한 데이터를 탐지하는 민감한 데이터 프리프로세서를 구성할 수 있습니다. 34-18페이지의 민감한 데이터 탐지을/를 참조하십시오.

새로 생성된 액세스 제어 정책에서는 하나의 기본 네트워크 분석 정책이 동일한 상위 액세스 제어 정책에 의해 호출되는 *모든* 침입 정책의 *모든* 트래픽에 대한 전처리를 제어합니다. 초기에 시스템은 Balanced Security and Connectivity 네트워크 분석 정책을 기본값으로 사용하지만, 나중에 이를 시스템 제공 또는 사용자 지정 네트워크 분석 정책으로 변경할 수 있습니다. 좀 더 복잡한 구축에서 고급 사용자는 일치하는 트래픽을 전처리하도록 여러 사용자 지정 네트워크 분석 정책을 할당함으로써 특정 보안 영역, 네트워크 및 VLAN에 대한 트래픽 전처리 옵션을 맞춤화할 수 있습니다. 자세한 내용은 23-7페이지의 시스템 제공 정책과 사용자 지정 정책 비교을/를 참조하십시오.

액세스 제어 규칙: 침입 정책 선택

라이센스: 보호

초기 전처리 이후에는 액세스 제어 규칙(있는 경우)이 트래픽을 평가합니다. 대부분의 경우 패킷과 일치하는 첫 번째 액세스 제어 규칙이 트래픽을 처리하는 규칙입니다. 일치하는 트래픽을 모니터링, 신뢰, 차단 또는 허용할 수 있습니다.

액세스 제어 규칙에서 트래픽을 허용하는 경우 시스템은 트래픽에서 검색 데이터, 악성코드, 금지된 파일 및 침입을 순서대로 검사합니다. 액세스 제어 규칙과 일치하지 않는 트래픽은 검색 데이터와 침입을 검사할 수 있는 액세스 제어 정책의 기본 작업에 의해 처리됩니다.

참고 전처리하는 네트워크 분석 정책이 무엇이든 **상관없이** 모든 패킷은 구성된 액세스 제어 규칙(따라서 잠재적으로 침입 정책의 검사를 받을 수 있음)에 대해 하향식 순서로 매칭됩니다. 자세한 내용은 23-12페이지의 사용자 지정 정책의 제한 사항을/를 참조하십시오.

23-2페이지의 정책이 트래픽에서 침입을 검토하는 방법 이해의 다이어그램은 다음과 같이 인라인, 침입 방지 및 AMP 구축에서 디바이스를 통과하는 트래픽의 플로우를 보여줍니다.

- Access Control Rule A는 일치하는 트래픽의 진행을 허용합니다. 그런 다음 트래픽에 대해 네트워크 검색 정책이 검색 데이터를 검사하고, File Policy A가 금지된 파일 및 악성코드를 검사하고, Intrusion Policy A가 침입을 검사합니다.
- Access Control Rule B 역시 일치하는 트래픽의 진행을 허용합니다. 그러나 이 시나리오에서는 트래픽에서 침입(또는 파일이나 악성코드)을 검사하지 않으므로, 규칙과 관련된 침입 또는 파일 정책이 없습니다. 기본적으로 진행을 허용하는 트래픽은 네트워크 검색 정책의 검사를 받으며, 이것은 구성할 필요가 없습니다.
- 이 시나리오에서 액세스 제어 정책의 기본 작업은 일치하는 트래픽을 허용하는 것입니다. 그런 다음 트래픽은 네트워크 검색 정책, 그다음에는 침입 정책의 검사를 받습니다. 침입 정책을 액세스 제어 규칙 또는 기본 작업과 연결할 때 다른 침입 정책을 사용할 수 있습니다(그러나 반드시 그렇게 해야 할 필요는 없음).

시스템은 차단된 트래픽 또는 신뢰할 수 있는 트래픽은 검사하지 않으므로 다이어그램의 예에는 차단 또는 신뢰 규칙이 포함되어 있지 않습니다. 자세한 내용은 14-8페이지의 규칙 작업을 사용하여 트래픽 처리 및 검사 확인 및 12-6페이지의 네트워크 트래픽의 기본 처리 및 검사 설정을/를 참조하십시오.

침입 검사: 침입 정책, 규칙 및 변수 집합

라이센스: 보호

침입 방지는 트래픽이 목적지로 들어가기 전 시스템의 최후의 방어선으로 사용할 수 있습니다. 침입 정책은 시스템이 트래픽에서 보안 위반을 검사하고, 인라인 구축 시 악성 트래픽을 차단 또는 변경하는 방법을 제어합니다. 침입 정책의 주요 기능은 어떤 침입 및 프리프로세서 규칙을 활성화할지, 이러한 규칙을 어떻게 구성할지를 관리하는 것입니다.

침입 및 프리프로세서 규칙

침입 규칙은 네트워크에서 취약성을 악용하려는 시도를 탐지하는 키워드와 인수의 지정된 집합입니다. 시스템은 침입 규칙을 사용하여 네트워크 트래픽을 분석하여 규칙의 기준과 일치하는지를 검사합니다. 시스템은 패킷을 각 규칙에 지정된 조건과 비교하고, 패킷이 규칙에 지정된 모든 조건과 일치하면 규칙을 트리거합니다.

시스템에는 VRT로 생성한 다음과 같은 유형의 규칙이 포함됩니다.

- *공유 객체 침입 규칙* - 컴파일되지만 수정할 수는 없습니다(소스 및 목적지 포트와 IP 주소 같은 규칙 헤더 정보 제외).
- *표준 텍스트 침입 규칙* - 규칙의 새로운 사용자 지정 인스턴스로서 저장 및 수정할 수 있습니다.
- *프리프로세서 규칙* - 네트워크 분석 정책에서 프리프로세서 및 패킷 디코더 탐지 옵션과 연결된 규칙입니다. 프리프로세서 규칙은 복사 또는 수정할 수 없습니다. 대부분의 프리프로세서 규칙은 기본적으로 비활성화되어 있습니다. 프리프로세서를 사용하여 이벤트를 생성하고 인라인 구축에서 위반 패킷을 삭제하려면 반드시 활성화해야 합니다.

시스템이 침입 정책에 따라 패킷을 처리할 때, 먼저 rule optimizer는 전송 레이어, 애플리케이션 프로토콜, 보호되는 네트워크로 오가는 방향 등의 기준을 기반으로 모든 활성화된 규칙을 하위 집합으로 분류합니다. 그런 다음 침입 규칙 엔진은 각 패킷에 적용할 적절한 규칙 하위 집합을 선택합니다. 마지막으로, 트래픽이 규칙과 일치하는지를 확인하기 위해 다중 규칙 검색 엔진이 세 가지 유형의 검색을 수행합니다.

- 프로토콜 필드는 애플리케이션 프로토콜의 특정 필드에서 일치를 검색합니다.
- 일반 내용 검색은 패킷 페이로드에서 ASCII 또는 이진 바이트 일치를 찾습니다.
- 패킷 변칙 검색은 특정 내용을 포함하기보다는 잘 설정된 프로토콜을 위반하는 패킷 헤더 및 페이로드를 찾습니다.

사용자 지정 침입 정책에서 규칙을 활성화 및 비활성화하고, 자신의 고유한 표준 텍스트 규칙을 작성하고 추가하여 탐지를 조정할 수 있습니다. FireSIGHT 권장 사항을 사용하여, 네트워크에서 탐지되는 운영 체제, 서버 및 클라이언트 애플리케이션 프로토콜을 이러한 자산 보호를 위해 특별히 작성된 규칙과 연결할 수도 있습니다.

변수 집합

시스템에서는 침입 정책을 사용하여 트래픽을 평가할 때마다, 연결된 *변수 집합*을 사용합니다. 집합에 있는 대부분의 변수는 소스 및 목적지 IP 주소와 포트를 식별하기 위해 침입 규칙에서 일반적으로 사용되는 값을 나타냅니다. 또한 침입 정책의 변수를 사용하여 규칙 억제 및 동적 규칙 상태의 IP 주소를 나타낼 수도 있습니다.

시스템은 사전 정의된 기본 변수로 구성된 단일 기본 변수 집합을 제공합니다. 대부분의 시스템 제공 공유 객체 규칙 및 표준 텍스트 규칙에서는 이러한 사전 정의된 기본 변수를 사용하여 네트워크 및 포트 번호를 정의합니다. 예를 들어 규칙의 대다수는 `$HOME_NET` 변수를 사용하여 보호되는 네트워크를 지정하고, `$EXTERNAL_NET` 변수를 사용하여 보호되지 않는(외부) 네트워크를 지정합니다. 또한 특수한 규칙은 종종 다른 사전 정의된 변수를 사용합니다. 예를 들어 웹 서버에 대해 익스플로잇을 탐지하는 규칙은 `$HTTP_SERVERS` 및 `$HTTP_PORTS` 변수를 사용합니다.

팁 시스템 제공 침입 정책을 사용하더라도 Cisco에서는 기본 집합에서 주요 기본 변수를 수정할 것을 **적극** 권장합니다. 네트워크 환경을 정확히 반영하는 변수를 사용하면 처리가 최적화되고 시스템은 관련 시스템에서 의심스러운 활동을 모니터링할 수 있습니다. 고급 사용자는 하나 이상의 사용자 지정 침입 정책과 쌍을 이루도록 사용자 지정 변수 집합을 생성 및 사용할 수 있습니다. 자세한 내용은 3-18페이지의 사전 정의된 기본 변수 최적화을/를 참조하십시오.

침입 이벤트 생성

라이센스: 보호

시스템은 침입 가능성을 식별하면 *침입 또는 프리프로세서 이벤트*(*침입 이벤트*로 총칭)를 생성합니다. 관리되는 디바이스는 방어 센터에 이벤트를 전송합니다. 여기에서 집계된 데이터를 보고 네트워크 자산에 대한 공격을 더 잘 이해할 수 있습니다. 인라인 구축에서 관리되는 디바이스는 유해한 것으로 알려진 패킷을 삭제 또는 교체할 수도 있습니다.

데이터베이스의 각 침입 이벤트에는 이벤트 헤더가 있으며 이벤트 이름 및 분류에 대한 정보가 포함되어 있습니다. 그 밖에도 소스 및 목적지 IP 주소, 포트, 이벤트를 생성한 프로세스, 이벤트의 날짜와 시간, 공격 소스와 대상에 대한 컨텍스트 정보 등이 포함되어 있습니다. 패킷 기반 이벤트의 경우 시스템은 디코딩된 패킷 헤더의 복사본 및 이벤트를 트리거한 패킷에 대한 페이로드도 로깅합니다.

패킷 디코더, 프리프로세서 및 침입 규칙 엔진은 모두 시스템이 이벤트를 생성하도록 유도할 수 있습니다. 예를 들면 다음과 같습니다.

- 패킷 디코더(네트워크 분석 정책에서 구성됨)는 20바이트 미만의 IP 패킷(옵션 또는 페이로드가 없는 IP 데이터그램의 크기)을 수신하면 이를 변칙 트래픽으로 해석합니다. 나중에 패킷을 검토하는 침입 정책의 동반 디코더 규칙이 활성화되면 시스템은 프리프로세서 이벤트를 생성합니다.
- IP 디프래그먼트화 프리프로세서는 일련의 중첩 IP 프래그먼트를 발견하면 이를 공격 가능성으로 해석하며, 동반 프리프로세서 규칙이 활성화된 경우 시스템은 프리프로세서 이벤트를 생성합니다.
- 패킷에 의해 트리거될 때 침입 이벤트를 생성할 수 있도록 침입 규칙 엔진 내에서 대부분의 표준 텍스트 규칙 및 공유 객체 규칙이 작성됩니다.

데이터베이스에 침입 이벤트가 누적되면 잠재적인 공격의 분석을 시작할 수 있습니다. 시스템은 침입 이벤트를 검토하고, 이러한 이벤트가 네트워크 환경 및 보안 정책의 컨텍스트에서 중요한지를 평가하기 위해 필요한 툴을 제공합니다.

시스템 제공 정책과 사용자 지정 정책 비교

라이센스: 보호

새로운 액세스 제어 정책을 생성하는 것이 FireSIGHT 시스템을 사용하여 트래픽 플로우를 관리하는 첫 과정 중 하나입니다. 기본적으로 새로 생성된 액세스 제어 정책은 시스템 제공 네트워크 분석 및 침입 정책을 호출하여 트래픽을 검토합니다.

다음 다이어그램은 인라인, 침입 방지 구축에서 새로 생성된 액세스 제어 정책이 초기에 트래픽을 처리하는 방법을 보여줍니다. 전처리 및 침입 방지 단계가 강조 표시됩니다.

다음에 유의하십시오.

- 기본 네트워크 분석 정책은 액세스 제어 정책이 처리하는 *모든* 트래픽의 전처리를 제어합니다. 초기에는 시스템 제공 *Balanced Security and Connectivity 네트워크 분석 정책*이 기본값입니다.
- 액세스 제어 정책의 기본 작업은 시스템 제공 *Balanced Security and Connectivity 침입 정책*에 정의된 대로 모든 비악성 트래픽을 허용하는 것입니다. 기본 작업에서 트래픽 통과를 허용하므로, 침입 정책이 악성 트래픽을 검토하고 잠재적으로 차단하기 전에 검색 기능이 호스트, 애플리케이션 또는 사용자 데이터에서 트래픽을 검토할 수 있습니다.
- 정책은 기본 보안 인텔리전스 옵션(전역 화이트리스트 및 블랙리스트만)을 사용하고, SSL 정책 내에서 암호화된 트래픽을 해독하지 않으며, 액세스 제어 규칙을 사용하여 네트워크 트래픽의 특수 처리 및 검사를 수행하지 않습니다.

침입 방지 구축 조정을 위해 수행할 수 있는 간단한 단계는 다른 시스템 제공 네트워크 분석 및 침입 정책 집합을 기본값으로 사용하는 것입니다. Cisco는 FireSIGHT 시스템에서 이러한 정책의 여러 쌍을 제공합니다.

또는 사용자 지정 정책을 생성하고 사용하여 침입 방지 구축을 맞춤화할 수 있습니다. 그러한 정책에 구성된 프리프로세서 옵션, 침입 규칙 및 기타 고급 설정으로는 네트워크의 보안 요구를 해결할 수 없는 경우가 있을 수 있습니다. 네트워크 분석 및 침입 정책을 조정함으로써, 시스템이 네트워크의 트래픽에서 침입을 처리하고 검사하는 방법을 매우 세밀하게 구성할 수 있습니다.

자세한 내용은 다음 링크를 참고하십시오.

- 23-8페이지의 시스템 제공 정책 이해
- 23-9페이지의 사용자 지정 정책의 이점
- 23-12페이지의 사용자 지정 정책의 제한 사항

시스템 제공 정책 이해

라이센스: 보호

Cisco는 FireSIGHT 시스템에서 네트워크 분석 및 침입 정책의 여러 쌍을 제공합니다. 시스템 제공 네트워크 분석 및 침입 정책을 사용하면 Cisco VRT(Vulnerability Research Team)의 경험을 활용할 수 있습니다. 이러한 정책에 대해 VRT는 침입 및 프리프로세서 규칙 상태를 설정하며, 프리프로세서 및 기타 고급 설정에 대한 초기 컨피그레이션을 제공합니다. 시스템에서 제공된 정책을 그대로 사용하거나, 이를 사용자 지정 정책의 기본으로 사용할 수 있습니다.

팁 시스템 제공 네트워크 분석 및 침입 정책을 사용하더라도 네트워크 환경을 정확히 반영하도록 시스템의 침입 변수를 구성해야 합니다. 최소한 기본 집합에서 주요 기본 변수를 수정하십시오. 3-18페이지의 사전 정의된 기본 변수 최적화을/를 참조하십시오.

새로운 취약성이 알려지면 VRT에서 침입 규칙 업데이트를 릴리스합니다. 이러한 규칙 업데이트는 시스템 제공 네트워크 분석 또는 침입 정책을 수정할 수 있으며, 새로운/업데이트된 침입 규칙 및 프리프로세서 규칙, 기존 규칙에 대한 수정된 상태 및 수정된 기본 정책 설정을 제공할 수 있습니다. 규칙 업데이트는 또한 시스템 제공 정책에서 규칙을 삭제하고 새로운 규칙 카테고리를 제공하는 것은 물론 기본 변수 집합을 수정할 수도 있습니다.

규칙 업데이트가 구축에 영향을 미치는 경우, 웹 인터페이스는 영향받는 침입 및 네트워크 분석 정책은 물론 해당 상위 액세스 제어 정책에 대해서도 최신 상태가 아닌 것으로 표시합니다. 변경 사항을 반영하려면 업데이트된 정책을 다시 적용해야 합니다.

편의상, 단독으로 또는 영향받는 액세스 제어 정책의 조합으로 영향받는 침입 정책을 자동으로 다시 적용하도록 규칙 업데이트를 구성할 수 있습니다. 이렇게 하면 최근에 검색된 익스플로잇과 침입으로부터 보호할 수 있도록 구축을 손쉽게 자동으로 최신 상태로 유지할 수 있습니다.

최신 전처리 설정을 보장하려면 **반드시** 액세스 제어 정책을 다시 적용해야 합니다. 그러면 현재 실행 중인 것과 다른 모든 관련 SSL, 네트워크 분석 및 파일 정책이 다시 적용되며, 고급 전처리 및 성능 옵션에 대한 기본값도 업데이트될 수 있습니다. 자세한 내용은 66-14페이지의 규칙 업데이트 및 로컬 규칙 파일 가져오기을/를 참조하십시오.

Cisco는 FireSIGHT 시스템에서 다음 네트워크 분석 및 침입 정책을 제공합니다.

Balanced Security and Connectivity 네트워크 분석 및 침입 정책

이러한 정책은 속도와 탐지 모두를 위해 작성됩니다. 함께 사용하면 대부분의 조직 및 구축 유형에서 사용할 수 있는 훌륭한 출발점이 됩니다. 시스템은 대부분의 경우 Balanced Security and Connectivity 정책 및 설정을 기본값으로 사용합니다.

Connectivity Over Security 네트워크 분석 및 침입 정책

이러한 정책은 네트워크 인프라 보안보다 연결(모든 리소스에 도달할 수 있는 기능)이 더 중요한 조직을 위해 작성됩니다. 침입 정책은 Security over Connectivity 정책에서 활성화하는 것보다 훨씬 적은 수의 규칙을 활성화합니다. 트래픽을 차단하는 가장 중요한 규칙만 활성화됩니다.

Security Over Connectivity 네트워크 분석 및 침입 정책

이러한 정책은 사용자 편의성보다 네트워크 인프라 보안이 더 중요한 조직을 위해 작성됩니다. 침입 정책은 올바른 트래픽에 대해 알림을 전송하거나 삭제를 수행할 수 있는 다수의 네트워크 변칙 침입 규칙을 활성화합니다.

No Rules Active 침입 정책

No Rules Active 침입 정책에서는 모든 침입 규칙 및 고급 설정이 비활성화됩니다. 이 정책은 다른 시스템 제공 정책 중 하나에서 활성화된 규칙을 기반으로 하는 대신 자신의 고유한 침입 정책을 생성하려는 사용자에게 출발점을 제공합니다.

주의 Cisco는 테스트용으로 또 다른 정책인 `Experimental Policy 1`을 제공합니다. Cisco 담당자의 지침 없이는 이 정책을 사용하지 마십시오.

사용자 지정 정책의 이점

라이센스: 보호

시스템 제공 네트워크 분석 및 침입 정책에 구성된 프리프로세서 옵션, 침입 규칙 및 기타 고급 설정으로 조직의 보안 요구가 충분히 해결되지 않을 수도 있습니다.

사용자 지정 정책을 작성하면 환경에서 시스템의 성능을 개선하고, 네트워크에서 발생하는 악성 트래픽과 정책 위반을 집중적으로 관찰할 수 있습니다. 사용자 지정 정책을 생성 및 조정함으로써, 시스템이 네트워크의 트래픽에서 침입을 처리하고 검사하는 방법을 매우 세밀하게 구성할 수 있습니다.

모든 사용자 지정 정책에는 정책의 모든 컨피그레이션에 대한 기본 설정을 정의하는 기반 정책(기반 레이어라고도 함)이 있습니다. 레이어는 여러 네트워크 분석 또는 침입 정책을 효과적으로 관리하기 위해 사용할 수 있는 구성 요소입니다. 24-1페이지의 네트워크 분석 또는 침입 정책에서 레이어 사용을/를 참조하십시오.

대부분의 경우 시스템 제공 정책을 사용자 지정 정책의 기반으로 사용하지만, 다른 사용자 지정 정책을 사용할 수도 있습니다. 그러나 정책 체인에서 보면 모든 사용자 지정 정책의 궁극적인 기반은 시스템 제공 정책입니다. 규칙 업데이트는 시스템 제공 정책을 수정하므로, 규칙 업데이트를 가져오면 사용자 지정 정책을 기반으로 사용하는 경우에도 영향을 받을 수 있습니다. 규칙 업데이트가 구축에 영향을 미치는 경우 웹 인터페이스는 영향받는 정책을 최신 상태가 아닌 것으로 표시합니다. 자세한 내용은 24-4페이지의 규칙 업데이트가 시스템 제공 기반 정책을 수정하도록 허용을/를 참조하십시오.

생성하는 사용자 지정 정책 외에도 시스템에서는 두 가지 사용자 지정 침입 및 네트워크 정책인 Initial Inline Policy 및 Initial Passive Policy를 제공합니다. 이러한 정책은 적절한 Balanced Security and Connectivity 정책을 기반으로 사용합니다. 이 둘의 유일한 차이점은, 인라인 정책에서는 트래픽 차단 및 수정을 활성화하고 패시브 정책에서는 이를 비활성화하는 *삭제 동작*입니다. 이러한 시스템 제공 사용자 지정 정책을 수정 및 사용할 수 있습니다.

자세한 내용은 다음 링크를 참고하십시오.

- 23-10페이지의 사용자 지정 네트워크 분석 정책의 이점
- 23-11페이지의 사용자 지정 침입 정책의 이점

사용자 지정 네트워크 분석 정책의 이점

라이센스: 보호

기본적으로 하나의 네트워크 분석 정책이 액세스 제어 정책에서 다루는 모든 암호화되지 않은 트래픽을 전처리합니다. 즉, 나중에 패킷을 검토하는 침입 정책(및 그에 따른 침입 규칙 집합)과 상관없이 모든 패킷이 동일한 설정에 따라 디코딩 및 전처리되는 것입니다.

초기에는 시스템 제공 Balanced Security and Connectivity 네트워크 분석 정책이 기본값입니다. 전처리를 조정하는 간단한 방법은 사용자 지정 네트워크 분석 정책을 생성하여 기본값으로 사용하는 것입니다. 25-4페이지의 액세스 제어에 대한 기본 네트워크 분석 정책 설정을/를 참조하십시오.

사용 가능한 조정 옵션은 프리프로세서에 따라 다르지만, 프리프로세서 및 디코더를 조정할 수 있는 몇 가지 방법은 다음과 같습니다.

- 모니터링하는 트래픽에 적용되지 않는 프리프로세서는 비활성화할 수 있습니다. 예를 들어 HTTP Inspect 프리프로세서는 HTTP 트래픽을 표준화합니다. 네트워크에 Microsoft IIS(Internet Information Services)를 사용하는 웹 서버가 없는 것이 확실하면 IIS 관련 트래픽을 찾는 프리프로세서 옵션을 비활성화하여 시스템 처리 오버헤드를 줄일 수 있습니다.

참고 사용자 지정 네트워크 분석 정책에서 프리프로세서를 비활성화했지만 나중에 시스템이 활성화된 침입 또는 프리프로세서 규칙에 대해 패킷을 평가하기 위해 해당 프리프로세서를 사용해야 하는 경우, 프리프로세서가 네트워크 분석 정책 웹 인터페이스에서 비활성 상태로 유지되더라도 시스템은 프리프로세서를 자동으로 활성화하여 사용합니다.

- 특정 프리프로세서의 활동에 집중할 수 있도록 해당되는 경우 포트를 지정합니다. 예를 들어, DNS 서버 응답 및 암호화된 SSL 세션을 모니터링하기 위한 추가 포트 또는 텔넷, HTTP 및 RPC 트래픽을 디코딩하는 포트를 식별할 수 있습니다.

복잡한 구축 환경을 갖춘 고급 사용자를 위해, 여러 개의 네트워크 분석 정책을 생성할 수 있으며 각 정책은 트래픽을 각기 다른 방식으로 전처리하도록 맞춤화됩니다. 그런 다음 이러한 정책을 사용하도록 시스템을 구성하여 서로 다른 보안 영역, 네트워크 또는 VLAN을 사용하는 트래픽의 전처리를 제어할 수 있습니다 (ASA FirePOWER 디바이스는 VLAN을 통한 전처리를 제한할 수 없습니다.).

참고 사용자 지정 네트워크 분석 정책(특히 여러 네트워크 분석 정책)을 사용하여 전처리를 맞춤화하는 것은 고급 작업입니다. 전처리 및 침입 검사는 밀접하게 관련되어 있으므로, 단일 패킷을 검토하는 네트워크 분석 및 침입 정책이 상호 보완 관계가 되도록 **각별히** 유의해야 합니다. 자세한 내용은 23-12페이지의 사용자 지정 정책의 제한 사항을/를 참조하십시오.

사용자 지정 침입 정책의 이점

라이센스: 보호

초기에 침입 방지를 수행하도록 구성된 새로 생성된 액세스 제어 정책의 경우, 기본 작업은 모든 트래픽을 허용하지만 먼저 시스템 제공 Balanced Security and Connectivity 침입 정책으로 트래픽을 검사합니다. 액세스 제어 규칙을 추가하거나 기본 작업을 변경하지 않는 한 해당 침입 정책이 모든 트래픽을 검사합니다. 23-7페이지의 시스템 제공 정책과 사용자 지정 정책 비교의 다이어그램을/를 참조하십시오.

침입 방지 구축을 사용자 지정하려면 여러 침입 정책을 생성하고, 트래픽을 달리 검사하도록 각각을 맞춤화할 수 있습니다. 그런 다음 어떤 정책이 어떤 트래픽을 검사할지를 지정하는 규칙으로 액세스 제어 정책을 구성합니다. 액세스 제어 규칙은 보안 영역, 네트워크 또는 지오로케이션, VLAN, 포트, 애플리케이션, 요청된 URL, 사용자 등 여러 기준을 사용하여 간단하거나 복잡한 방식으로 트래픽을 매칭하고 검사할 수 있습니다. 23-2페이지의 정책이 트래픽에서 침입을 검토하는 방법 이해의 시나리오는 두 침입 정책 중 하나로 트래픽을 검사하는 구축을 보여줍니다.

침입 정책의 주요 기능은 다음과 같이 어떤 침입 및 프리프로세서 규칙을 활성화할지, 이러한 규칙을 어떻게 구성할지를 관리하는 것입니다.

- 각 침입 정책 내에서, 환경에 해당되는 모든 규칙이 활성화되었는지를 확인하고 환경에 해당되지 않는 규칙을 비활성화하여 성능을 개선해야 합니다. 인라인 구축에서는 어떤 규칙이 악의적인 패킷을 삭제 또는 수정할지를 지정할 수 있습니다. 자세한 내용은 32-20페이지의 규칙 상태 설정을/를 참조하십시오.
- FireSIGHT 권장 사항에서는 네트워크에서 탐지되는 운영 체제, 서버 및 클라이언트 애플리케이션 프로토콜을 이러한 자산 보호를 위해 특별히 작성된 규칙과 연결하도록 허용합니다. 33-1페이지의 네트워크 자산에 대한 침입 방지 맞춤화을/를 참조하십시오.
- 새 익스플로잇을 파악하고 보안 정책을 적용하기 위해 필요할 경우 기존 규칙을 수정하고 새 표준 텍스트 규칙을 작성할 수 있습니다. 36-1페이지의 침입 규칙 이해 및 작성을/를 참조하십시오.

침입 정책에 대해 수행할 수 있는 기타 사용자 지정 작업에는 다음이 포함됩니다.

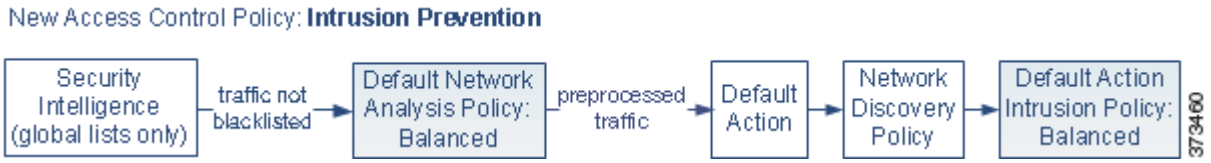
- 민감한 데이터 프리프로세서는 ASCII 텍스트의 신용카드 번호 및 주민등록번호 같은 민감한 데이터를 탐지합니다. 후면 구멍 공격, 몇몇 포트 스캔 유형, 과도한 트래픽으로 네트워크의 무력화를 시도하는 속도 기반 공격 등 특정 위협을 탐지하는 기타 프리프로세서는 네트워크 분석 정책에서 구성됩니다. 자세한 내용은 34-1페이지의 특정 위협 탐지을/를 참조하십시오.
- 전역 임계값을 지정하면, 침입 규칙과 일치하는 트래픽이 지정된 기간 내에 특정 주소나 주소 범위에서 발생하거나 그러한 주소나 주소 범위로 이동하는 횟수를 기반으로 시스템은 이벤트를 생성합니다. 이렇게 하면 이벤트 수가 너무 많아서 시스템이 혼란스러워지는 상황을 피할 수 있습니다. 자세한 내용은 35-1페이지의 전체적으로 침입 이벤트 로깅 제한을/를 참조하십시오.
- 개별 규칙 또는 전체 침입 정책에 대해 침입 이벤트 알림을 억제하고 임계값을 설정하는 것도 이벤트 수가 너무 많아서 시스템이 혼란스러워지는 상황을 피할 수 있는 방법입니다. 자세한 내용은 32-22페이지의 정책당 침입 이벤트 알림 필터링을/를 참조하십시오.
- 웹 인터페이스 내의 다양한 침입 이벤트 보기 외에도 syslog 장소에 로깅하는 기능을 활성화하거나 이벤트 데이터를 SNMP 트랩 서버로 전송할 수 있습니다. 정책 단위로 침입 이벤트 알림 제한을 지정하고, 외부 로깅 장소에 대한 침입 이벤트 알림을 설정하고, 침입 이벤트에 대한 외부 응답을 구성할 수 있습니다. 이러한 정책 단위 알림 컨피그레이션 외에도 각 규칙이나 규칙 그룹에 대해 침입 이벤트의 이메일 알림을 전역적으로 활성화 또는 비활성화할 수 있습니다. 어떤 침입 정책이 패킷을 처리하는지와 상관없이 이메일 알림 설정이 사용됩니다. 자세한 내용은 44-1페이지의 침입 규칙에 대한 외부 알림 구성을/를 참조하십시오.

사용자 지정 정책의 제한 사항

라이센스: 보호

전처리 및 침입 검사는 밀접하게 관련되어 있으므로, 컨피그레이션에서 단일 패킷을 검토하는 네트워크 분석 및 침입 정책이 상호 보완 관계가 되는 것을 허용하도록 **각별히** 유의해야 합니다.

기본적으로 시스템은 단일 액세스 제어 정책을 사용하여 관리되는 디바이스에서 다루는 모든 트래픽을 전처리하기 위해 하나의 네트워크 분석 정책을 사용합니다. 다음 다이어그램은 인라인, 침입 방지 구축에서 새로 생성된 액세스 제어 정책이 초기에 트래픽을 처리하는 방법을 보여줍니다. 전처리 및 침입 방지 단계가 강조 표시됩니다.



기본 네트워크 분석 정책이 액세스 제어 정책에서 다루는 *모든* 트래픽의 전처리를 어떻게 제어하는지 확인하십시오. 초기에는 시스템 제공 Balanced Security and Connectivity 네트워크 분석 정책이 기본값입니다.

전처리를 조정하는 간단한 방법은 23-10페이지의 사용자 지정 네트워크 분석 정책의 이점에 요약된 대로, 사용자 지정 네트워크 분석 정책을 생성하여 기본값으로 사용하는 것입니다. 그러나 사용자 지정 네트워크 분석 정책에서 프리프로세서를 비활성화했지만 나중에 시스템이 활성화된 침입 또는 프리프로세서 규칙에 대해 전처리된 패킷을 평가해야 하는 경우, 프리프로세서가 네트워크 분석 정책 웹 인터페이스에서 비활성 상태로 유지되더라도 시스템은 프리프로세서를 자동으로 활성화하여 사용합니다.

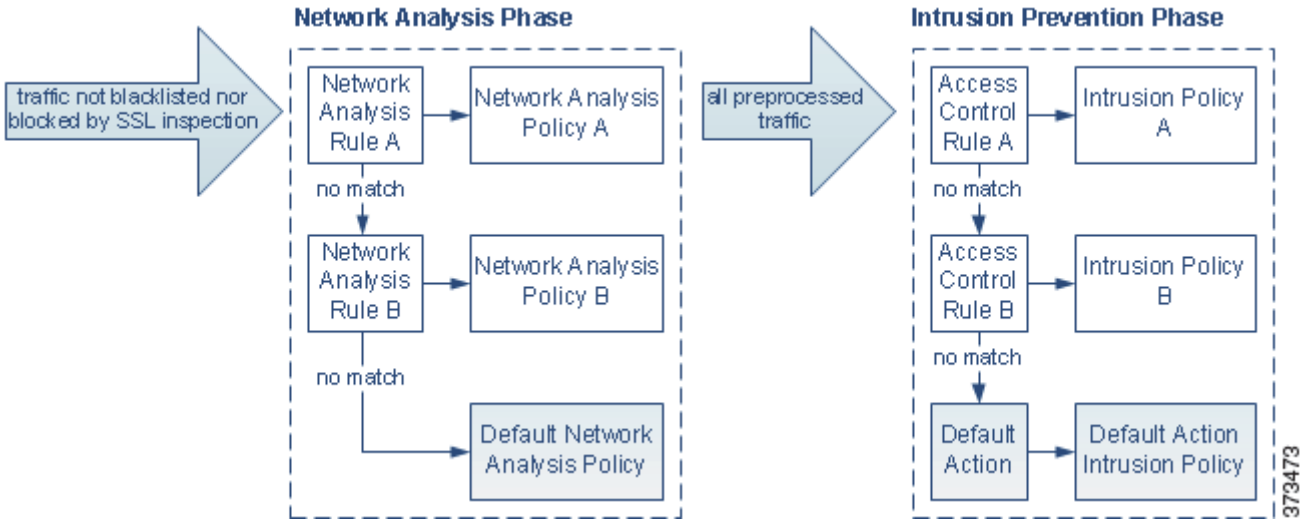
참고 프리프로세서 비활성화를 통해 성능 이점을 누리려면, 침입 정책 중에 해당 프리프로세서를 필요로 하는 규칙을 활성화한 것이 없는지를 **반드시** 확인해야 합니다.

여러 사용자 지정 네트워크 분석 정책을 사용하는 경우 추가 과제가 발생합니다. 복잡한 구축을 수행하는 고급 사용자의 경우 일치하는 트래픽을 전처리하도록 사용자 지정 네트워크 분석 정책을 할당함으로써 특정 보안 영역, 네트워크 및 VLAN에 대한 전처리를 맞춤화할 수 있습니다. (ASA FirePOWER 디바이스는 VLAN 단위로 전처리를 제한할 수 없습니다.) 이를 수행하려면 사용자 지정 *네트워크 분석 규칙*을 액세스 제어 정책에 추가합니다. 각 규칙에는 규칙과 일치하는 트래픽의 전처리를 제어하는 관련 네트워크 분석 정책이 있습니다.

팁 액세스 제어 정책에서 네트워크 분석 규칙을 고급 설정으로 구성할 수 있습니다. FireSIGHT 시스템의 다른 규칙 유형과는 달리, 네트워크 분석 규칙은 네트워크 분석 정책을 호출합니다(정책에 포함되기보다는).

시스템은 규칙 번호에 따라 하향식 순서로 패킷이 구성된 네트워크 분석 규칙과 일치하는지를 확인합니다. 네트워크 분석 규칙과 일치하지 않는 트래픽은 기본 네트워크 분석 정책으로 전처리됩니다. 이렇게 하면 트래픽을 매우 유연하게 전처리할 수 있지만, 어떤 네트워크 분석 정책이 전처리하는지와 **상관없이** 모든 패킷은 자체 프로세스에서 이후 액세스 제어 규칙과 매칭됩니다(따라서 잠재적으로 침입 정책의 검사를 받음). 다시 말해, 특별한 네트워크 분석 정책으로 패킷을 전처리하더라도 패킷이 특별한 침입 정책으로 검토될 것이라고 보장되지 **않습니다**. 특별한 패킷을 평가하려면 올바른 네트워크 분석 및 침입 정책을 호출하도록 **반드시** 액세스 제어 정책을 신중하게 구성해야 합니다.

다음 다이어그램은 침입 방지(규칙) 단계 이전에 이와 별도로 어떻게 네트워크 분석 정책(전처리) 선택 단계가 발생하는지를 집중적으로 자세히 보여줍니다. 간소화를 위해 검색 및 파일/악성코드 검사 단계는 생략되었습니다. 또한 기본 네트워크 분석 및 기본 작업 침입 정책이 강조 표시됩니다.



이 시나리오에서 액세스 제어 정책은 두 개의 네트워크 분석 규칙 및 기본 네트워크 분석 정책과 함께 구성됩니다.

- Network Analysis Rule A는 Network Analysis Policy A로 일치하는 트래픽을 전처리합니다. 나중에 Intrusion Policy A가 이 트래픽을 검사하도록 할 수 있습니다.
- Network Analysis Rule B는 Network Analysis Policy B로 일치하는 트래픽을 전처리합니다. 나중에 Intrusion Policy B가 이 트래픽을 검사하도록 할 수 있습니다.
- 모든 나머지 트래픽은 네트워크 분석 정책으로 전처리됩니다. 나중에 액세스 제어 정책의 기본 작업과 연결된 침입 정책이 이 트래픽을 검사하도록 할 수 있습니다.

시스템은 트래픽을 전처리한 후, 트래픽에서 침입을 검토할 수 있습니다. 이 다이어그램은 액세스 제어 규칙 및 기본 작업과 함께 액세스 제어 정책을 보여줍니다.

- Access Control Rule A는 일치하는 트래픽을 허용합니다. 그런 다음 Intrusion Policy A가 트래픽을 검사합니다.
- Access Control Rule B 역시 일치하는 트래픽을 허용합니다. 그런 다음 Intrusion Policy B가 트래픽을 검사합니다.
- 액세스 제어 정책의 기본 작업은 일치하는 트래픽을 허용하는 것입니다. 그런 다음 기본 작업의 침입 정책이 트래픽을 검사합니다.

각 패킷의 처리는 네트워크 분석 정책 및 침입 정책 쌍으로 제어되지만, 시스템에서 자동으로 쌍을 조정하지는 **않습니다**. 액세스 제어 정책을 잘못 구성하여 Network Analysis Rule A 및 Access Control Rule A가 동일한 트래픽을 처리하지 않는 시나리오를 가정해보겠습니다. 쌍을 이룬 정책이 특별한 보안 영역에서 트래픽의 처리를 제어하도록 하려고 했지만, 실수로 두 개의 규칙 조건에서 서로 다른 영역을 사용할 수 있습니다. 이렇게 하면 트래픽이 올바르지 않게 전처리될 수 있습니다. 이런 이유로, 네트워크 분석 규칙 및 사용자 지정 정책을 사용한 사용자 지정 전처리는 **고급** 작업입니다.

단일 연결의 경우, 시스템이 액세스 제어 규칙 이전에 네트워크 분석 정책을 선택하더라도 일부 전처리(특히 애플리케이션 레이어 전처리)는 액세스 제어 규칙 선택 이후 발생합니다. 이는 사용자 지정 네트워크 분석 정책에서 전처리를 구성하는 방법에 영향을 주지 **않습니다**.

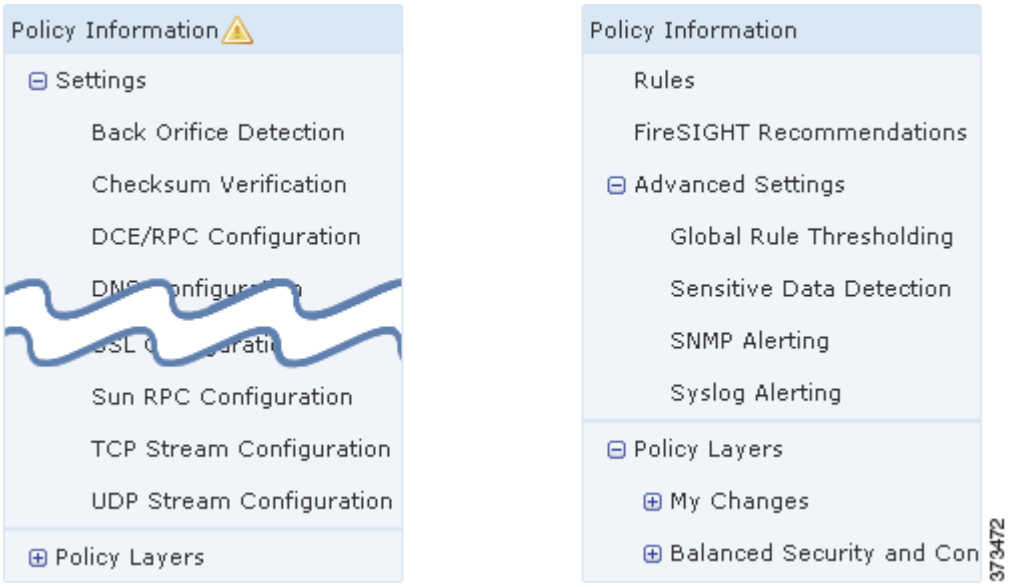
탐색 패널 사용

라이센스: 보호

네트워크 분석 및 침입 정책은 유사한 웹 인터페이스를 사용하여 컨피그레이션을 수정하고 해당 변경 사항을 저장합니다. 다음을 참조하십시오.

- 26-4페이지의 네트워크 분석 정책 수정
- 31-4페이지의 침입 정책 수정

탐색 패널은 정책 유형 중 하나를 수정할 때 웹 인터페이스의 왼쪽에 나타납니다. 다음 그림에서는 네트워크 분석 정책(왼쪽) 및 침입 정책(오른쪽)의 탐색 패널을 보여줍니다.



구분선은 정책 레이어와의 직접 상호 작용을 사용하여(아래) 또는 사용하지 않고(위) 구성할 수 있는 정책 설정에 대한 링크로 탐색 패널을 구분합니다. 설정 페이지로 이동하려면 탐색 패널의 이름을 클릭하십시오. 탐색 패널에서 항목의 어두운 음영은 현재 설정 페이지를 강조 표시합니다. 예를 들어 위의 그림에서는 탐색 패널의 오른쪽에 Policy Information 페이지가 표시될 수 있습니다.

Policy Information

Policy Information 페이지는 일반적으로 사용되는 설정에 대한 컨피그레이션 옵션을 제공합니다. 위의 네트워크 분석 정책 패널에 대한 그림에 보이는 것처럼, 정책에 저장되지 않은 변경 사항이 포함된 경우 탐색 패널의 **Policy Information** 옆에 정책 변경 아이콘(⚠)이 나타납니다. 변경 사항을 저장하면 아이콘이 사라집니다.

Rules(침입 정책 전용)

침입 정책의 Rules 페이지에서는 공유 객체 규칙, 표준 텍스트 규칙 및 프리프로세서 규칙을 위한 규칙 상태 및 기타 설정을 구성할 수 있습니다. 자세한 내용은 32-1페이지의 규칙을 사용하여 침입 정책 조정을/를 참조하십시오.

FireSIGHT Recommendations(침입 정책 전용)

침입 정책의 FireSIGHT Recommendations 페이지에서는 네트워크에서 탐지되는 운영 체제, 서버 및 클라이언트 애플리케이션 프로토콜을 이러한 자산 보호를 위해 특별히 작성된 침입 규칙과 연결하도록 허용합니다. 이렇게 하면 모니터링되는 네트워크의 특정 요구에 맞게 침입 정책을 맞춤

화할 수 있습니다. 자세한 내용은 33-1페이지의 네트워크 자산에 대한 침입 방지 맞춤화을/를 참조하십시오.

Settings(네트워크 분석 정책) 및 Advanced Settings(침입 정책)

네트워크 분석 정책의 Settings 페이지에서는 프리프로세서 및 액세스 프리프로세서 컨피그레이션 페이지를 활성화 또는 비활성화할 수 있습니다. **Settings** 링크를 확장하면 정책에서 활성화된 모든 프리프로세서의 개별 컨피그레이션 페이지에 대한 하위 링크가 표시됩니다. 자세한 내용은 26-6페이지의 네트워크 분석 정책에서 프리프로세서 구성을/를 참조하십시오.

침입 정책의 Advanced Settings 페이지에서는 고급 설정을 활성화 또는 비활성화할 수 있으며, 해당 고급 설정의 컨피그레이션 페이지에 액세스할 수 있습니다. **Advanced Settings** 링크를 확장하면 정책에서 활성화된 모든 고급 설정의 개별 컨피그레이션 페이지에 대한 하위 링크가 표시됩니다. 자세한 내용은 31-7페이지의 침입 정책에서 고급 설정 구성을/를 참조하십시오.

Policy Layers

Policy Layers 페이지에는 네트워크 분석 또는 침입 정책을 구성하는 레이어에 대한 요약이 표시됩니다. Policy Layers 링크를 확장하면 정책에 있는 레이어의 요약 페이지에 대한 하위 링크가 표시됩니다. 각 레이어 하위 링크를 확장하면 레이어에서 활성화된 모든 규칙, 프리프로세서 또는 고급 설정의 컨피그레이션 페이지에 대한 추가 하위 링크가 표시됩니다. 자세한 내용은 24-1페이지의 네트워크 분석 또는 침입 정책에서 레이어 사용을/를 참조하십시오.

충돌 해결 및 정책 변경 사항 커밋

라이센스: 보호

네트워크 분석 또는 침입 정책을 수정할 때, 정책에 저장되지 않은 변경 사항이 포함되었음을 나타내기 위해 탐색 패널의 **Policy Information** 옆에 정책 변경 아이콘(⚠)이 나타납니다. 시스템이 인식하기 전에 변경 사항을 저장(또는 *커밋*)해야 합니다.

참고 저장 후 변경 사항을 반영하려면 정책 분석 또는 침입 정책을 적용해야 합니다. 저장하지 않고 정책을 적용하는 경우 시스템에서는 가장 최근에 저장된 컨피그레이션을 사용합니다. 침입 정책을 독립적으로 다시 적용할 수는 있지만, 네트워크 분석 정책은 상위 액세스 제어 정책과 함께 적용됩니다.

충돌 수정 해결

Network Analysis Policy 페이지(**Policies > Access Control** 선택 후 **Network Analysis Policy** 클릭) 및 Intrusion Policy 페이지(**Policies > Intrusion Policy > Intrusion Policy**)에는 각 정책에 저장되지 않은 변경 사항이 있는지가 표시되며, 현재 정책을 수정하고 있는 사용자에 대한 정보도 표시됩니다. Cisco에서는 한 번에 한 사용자만 정책을 수정할 것을 권장합니다. 동시 수정을 수행하는 경우 다음과 같은 결과가 나타납니다.

- 자신이 네트워크 분석과 침입 정책을 수정할 때 동시에 다른 사용자도 동일한 정책을 수정하는데 다른 사용자가 정책에 변경 사항을 저장하는 경우, 다른 사용자의 변경 사항을 덮어쓰는 정책을 커밋할 때 경고가 표시됩니다.
- 여러 웹 인터페이스 인스턴스를 통해 동일한 사용자로서 동일한 네트워크 분석 또는 침입 정책을 수정하면서 한 인스턴스에 대한 변경 사항을 저장하는 경우, 다른 인스턴스에 대한 변경 사항은 저장할 수 없습니다.

컨피그레이션 의존성 해결

특별 분석을 수행하려는 경우 다수의 프리프로세서 및 침입 규칙에서는 트래픽을 특정 방법으로 디코딩 또는 전처리하도록 요구하거나, 트래픽에 대해 다른 종속성을 요구합니다. 네트워크 분석 또는 침입 정책을 저장하면 시스템은 다음과 같이 자동으로 필수 설정을 활성화하거나, 비활성화된 설정이 트래픽에 아무런 영향도 미치지 못함을 경고합니다.

- SNMP 규칙 알림을 추가했지만 SNMP 알림을 구성하지 않은 경우 침입 정책을 저장할 수 없습니다. SNMP 알림을 구성하거나 규칙 알림을 비활성화한 다음 다시 저장해야 합니다.
- 침입 정책에 활성화된 민감한 데이터 규칙이 포함되어 있지만 민감한 데이터 프리프로세서를 활성화하지 않은 경우, 침입 정책을 저장할 수 없습니다. 시스템이 프리프로세서를 활성화하고 정책을 저장하도록 허용하거나, 규칙을 비활성화하고 다시 저장해야 합니다.
- 네트워크 분석 정책에서 필수 프리프로세서를 비활성화하더라도 정책을 저장할 수는 있습니다. 그러나 프리프로세서가 웹 인터페이스에서 비활성화되었더라도, 시스템은 비활성화된 프리프로세서를 자동으로 현재 설정을 통해 사용합니다. 자세한 내용은 23-12페이지의 사용자 지정 정책의 제한 사항을/를 참조하십시오.
- 네트워크 분석 정책에서 인라인 모드를 비활성화하고 Inline Normalization 프리프로세서를 활성화하는 경우, 여전히 정책을 저장할 수 있습니다. 그러나 표준화 설정이 무시될 것임을 알리는 경고가 표시됩니다. 인라인 모드를 비활성화하는 경우 시스템은 프리프로세서가 트래픽을 수정 또는 차단하도록 허용하는 기타 설정(예: 체크섬 확인 및 등급 기반 공격 방지)도 무시하게 됩니다. 자세한 내용은 26-5페이지의 인라인 구축에서 프리프로세서가 트래픽에 영향을 미치도록 허용 및 29-7페이지의 인라인 트래픽 표준화을/를 참조하십시오.

정책 변경 사항 커밋, 취소 및 캐싱

네트워크 분석 또는 침입 정책을 수정하는 동안 변경 사항을 저장하지 않고 정책 편집기를 종료하면 시스템은 그러한 변경 사항을 캐시합니다. 사용자가 시스템에서 로그아웃하거나 시스템 충돌이 발생하더라도 변경 사항은 캐시됩니다. 사용자당 하나의 네트워크 분석 및 하나의 침입 정책에 대한 저장되지 않은 변경 사항이 시스템 캐시에 저장됩니다. 동일한 유형의 다른 정책을 수정하기 전에 변경 사항을 커밋하거나 취소해야 합니다. 변경 사항을 첫 번째 정책에 저장하지 않은 채 또 다른 정책을 수정하거나 침입 규칙 업데이트를 가져오면 캐시된 변경 사항이 취소됩니다.

네트워크 분석 또는 침입 정책 편집기의 Policy Information 페이지에서 정책 변경 사항을 커밋하거나 취소할 수 있습니다. 26-4페이지의 네트워크 분석 정책 수정 및 31-4페이지의 침입 정책 수정을/를 참조하십시오.

다음 표에는 네트워크 분석 또는 침입 정책에 대한 변경 사항을 저장하거나 취소하는 방법이 요약되어 있습니다.

표 23-1 네트워크 분석 또는 침입 정책에 대한 변경 사항 커밋

목적	Policy Information 페이지에서 수행
정책에 대한 변경 사항 저장	**Commit Changes**를 클릭합니다. 시스템 정책의 설정은 네트워크 분석 또는 침입 정책 변경 사항을 커밋할 때 이에 대한 코멘트를 추가하라는(필수 또는 선택) 프롬프트의 표시 여부를 제어합니다. 시스템 정책은 또한 변경 사항과 코멘트를 감사 로그에 기록할지 여부도 제어합니다. 자세한 내용은 63-19페이지의 네트워크 분석 정책 환경 설정 구성 및 63-20페이지의 침입 정책 환경 설정 구성을/를 참조하십시오.
저장되지 않은 모든 변경 사항 취소	변경 사항을 취소하고 Intrusion Policy 페이지로 돌아가려면 **Discard Changes**를 클릭하고 **OK**를 클릭합니다. 변경 사항을 취소하지 않으려면 **Cancel**을 클릭하여 Policy Information 페이지로 돌아갑니다.
정책을 종료하되 변경 사항 캐싱	메뉴를 선택하거나 다른 페이지에 대한 다른 경로를 선택합니다. 종료 시 프롬프트가 표시되면 **Leave page**를 클릭하고, 고급 편집기에 남아 있으려면 **Stay on page**를 클릭합니다.

24장

네트워크 분석 또는 침입 정책에서 레이어 사용

관리되는 디바이스가 많은 좀 더 큰 조직에는 여러 부서, 사업부 또는 경우에 따라 여러 회사의 고유한 요구를 지원하기 위한 다수의 침입 정책 및 네트워크 분석 정책이 있을 수 있습니다. 두 정책 유형의 컨피그레이션은 여러 정책을 효율적으로 관리하기 위해 사용할 수 있는 *레이어*라는 구성 요소에 포함됩니다.

침입 및 네트워크 분석 정책의 레이어는 기본적으로 동일한 방식으로 작동합니다. 의식적으로 레이어를 사용하지 않고도 두 정책 유형을 생성 및 수정할 수 있습니다. 정책 컨피그레이션을 수정할 수 있으며, 정책에 사용자 레이어를 추가하지 않은 경우 시스템은 변경 사항을 초기 이름이 *My Changes*인 구성 가능한 단일 레이어에 자동으로 포함합니다. 선택적으로, 최대 200개의 레이어를 추가할 수 있으며 여기에서 설정의 조합을 구성할 수 있습니다. 사용자 레이어를 복사, 병합, 이동 및 삭제할 수 있으며 가장 중요한 기능으로 개별 사용자 레이어를 동일한 유형의 다른 정책과 공유할 수 있습니다.

자세한 내용은 다음 절을 참조하십시오.

- 24-1페이지의 레이어 스택 이해 - 기본 정책을 이루는 사용자 구성 가능한 내장 레이어에 대해 설명합니다.
- 24-7페이지의 레이어 관리 - 정책에서 레이어를 사용하는 방법에 대해 설명합니다.

레이어 스택 이해

라이센스: 보호

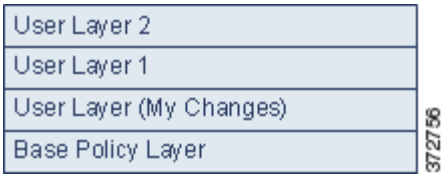
레이어를 추가하지 않은 네트워크 분석 또는 침입 정책에는 내장된 읽기 전용 기반 정책 레이어 및 초기 이름이 My Changes인 사용자 구성 가능한 단일 레이어가 포함되어 있습니다. 사용자 구성 가능한 레이어를 복사, 병합, 이동 또는 삭제할 수 있으며사용자 구성 가능한 모든 레이어를 동일한 유형의 다른 정책과 공유할 수 있습니다.

각 정책 레이어에는 네트워크 분석 정책의 모든 프리프로세서에 대한 또는 침입 정책의 모든 침입 규칙 및 고급 설정에 대한 완전한 컨피그레이션이 포함되어 있습니다. 최하위 기반 정책 레이어에는 정책 생성 시 선택한 기반 정책의 모든 설정이 포함되어 있습니다. 상위 레이어의 설정이 하위 레이어의 동일한 설정에 비해 우선권을 갖습니다. 레이어에 명시적으로 설정되지 않은 기능은 명시적으로 설정된 다음 최상위 레이어에서 설정을 *상속*합니다.

시스템은 레이어를 *병합*합니다. 즉, 네트워크 트래픽을 처리할 때 모든 설정의 누적된 효과만 적용합니다.

팁 기반 정책의 기본 설정만을 기반으로 침입 또는 네트워크 분석 정책을 생성할 수 있으며, 선택적으로 침입 정책의 경우 FireSIGHT 규칙 상태 권장 사항을 사용할 수 있습니다.

다음 그림에서는 레이어 스택의 예를 보여줍니다. 여기에는 기반 정책 레이어 및 초기 My Changes 레이어 외에 두 개의 사용자 구성 가능한 레이어인 *User Layer 1* 및 *User Layer 2*가 포함되어 있습니다. 이 그림에서, 추가하는 사용자 구성 가능한 각 레이어는 처음에 스택의 최상위 레이어에 배치됩니다. 따라서 그림의 User Layer 2는 스택에서 가장 마지막에 추가된 것이며 최상위 레이어입니다.



여러 레이어로 작업할 경우 다음 사항에 유의해야 합니다.

- 정책에서 최상위 레이어가 읽기 전용 레이어이거나 24-11페이지의 정책 간에 레이어 공유에 설명된 대로 공유 레이어인 경우, 사용자가 다음 중 하나를 수행하면 시스템은 사용자 구성 가능한 레이어를 침입 정책에서 최상위 레이어로 자동으로 추가합니다.
  - 침입 정책 Rules 페이지에서 규칙 작업(즉, 규칙 상태, 이벤트 필터링, 동적 상태 또는 알림) 수정. 자세한 내용은 32-1페이지의 규칙을 사용하여 침입 정책 조정을/를 참조
  - 프리프로세서, 침입 규칙 또는 고급 설정의 활성화, 비활성화 또는 수정

  시스템에서 추가한 레이어의 모든 설정은 상속됩니다. 단, 변경 사항이 새 레이어가 되는 경우는 예외입니다.
- 최상위 레이어가 공유 레이어이면 시스템은 사용자가 다음 작업 중 하나를 수행할 때 레이어를 추가합니다.
  - 최상위 레이어를 다른 정책과 공유
  - 공유 레이어를 정책에 추가
- 규칙 업데이트가 정책을 수정하도록 허용하는지와 상관없이, 규칙 업데이트의 변경 사항은 레이어에서 사용자가 수행한 변경 사항을 재정의하지 않습니다. 이는 규칙 업데이트의 변경 사항은 기반 정책에서 이루어지며, 이것이 기반 정책 레이어의 기본 설정을 결정하기 때문입니다. 사용자 변경 사항은 항상 최상위 레이어에서 이루어지므로, 규칙 업데이트가 기반 정책에 대해 수행하는 모든 변경 사항을 재정의합니다. 자세한 내용은 66-14페이지의 규칙 업데이트 및 로컬 규칙 파일 가져오기을/를 참조하십시오.

자세한 내용은 다음 절을 참조하십시오.

- 24-3페이지의 기반 레이어 이해
- 24-6페이지의 RecommendationsFireSIGHT 레이어 이해

기반 레이어 이해

라이센스: 보호

침입 또는 네트워크 분석 정책의 기반 레이어(기반 정책이라고도 함)는 정책의 모든 컨피그레이션에 대한 기본 설정을 정의하며 정책에서 최하위 레이어입니다. 새 정책을 생성할 때 새 레이어를 추가하지 않은 채 설정을 변경하면 변경 사항은 My Changes 레이어에 저장되며 기반 정책의 설정을 재정의합니다(그러나 변경하지는 않음).

자세한 내용은 다음 절을 참조하십시오.

- 24-3페이지의 시스템 제공 기반 정책 이해
- 24-3페이지의 사용자 지정 기반 정책 이해
- 24-4페이지의 기반 정책 변경
- 24-4페이지의 규칙 업데이트가 시스템 제공 기반 정책을 수정하도록 허용

시스템 제공 기반 정책 이해

라이센스: 보호

Cisco는 FireSIGHT 시스템에서 네트워크 분석 및 침입 정책의 여러 쌍을 제공합니다. 시스템 제공 네트워크 분석 및 침입 정책을 사용하면 Cisco VRT(Vulnerability Research Team)의 경험을 활용할 수 있습니다. 이러한 정책에 대해 VRT는 침입 및 프리프로세서 규칙 상태를 설정하며, 프리프로세서 및 기타 고급 설정에 대한 초기 컨피그레이션을 제공합니다. 이러한 시스템 제공 정책을 있는 그대로 사용할 수도 있고 사용자 지정 정책의 기반으로 사용할 수도 있습니다.

시스템 제공 정책을 기반으로 사용하는 경우 규칙 업데이트를 가져오면 기반 정책의 설정이 수정될 수 있습니다. 그러나 시스템 제공 기반 정책에 대해 이러한 변경이 자동으로 수행되지 않도록 사용자 지정 정책을 구성할 수 있습니다. 그러면 사용자는 규칙 업데이트 가져오기와는 별개의 일정에 따라 수동으로 시스템 제공 기반 정책을 업데이트할 수 있습니다. 어떤 경우든, 규칙 업데이트가 기반 정책에 대해 수행하는 변경 사항은 My Changes 또는 다른 레이어의 설정을 변경하거나 재정의하지 않습니다. 자세한 내용은 24-4페이지의 규칙 업데이트가 시스템 제공 기반 정책을 수정하도록 허용을/를 참조하십시오.

시스템 제공 침입 및 네트워크 분석 정책은 이름은 비슷하지만 컨피그레이션은 다릅니다. 예를 들어, Balanced Security and Connectivity 네트워크 분석 정책과 Balanced Security and Connectivity 침입 정책은 함께 작동하며 둘 다 침입 규칙 업데이트에서 업데이트할 수 있습니다. 자세한 내용은 23-8페이지의 시스템 제공 정책 이해을/를 참조하십시오.

사용자 지정 기반 정책 이해

라이센스: 보호

시스템 제공 정책을 네트워크 분석 또는 침입 정책의 기반 정책으로 사용하지 않으려는 경우 사용자 지정 정책을 기반으로 사용할 수 있습니다. 관리되는 디바이스의 성능을 향상하고 여기에서 생성되는 이벤트에 더욱 효과적으로 대응할 수 있도록 가장 중요한 방식으로 트래픽을 검사하기 위해 사용자 지정 정책의 설정을 조정할 수 있습니다.

최대 다섯 개의 사용자 지정 정책을 연결하여, 다섯 개 중 네 개는 전에 생성된 다른 네 개 중 하나를 기반 정책으로 사용하도록 할 수 있습니다. 다섯 번째는 시스템 제공 정책을 기반으로 사용해야 합니다.

다른 정책에 대한 기반으로 사용하는 사용자 지정 정책에 대한 변경 사항은 기반을 사용하는 정책의 기본 설정으로서 자동으로 사용됩니다. 또한 모든 정책은 정책 체인의 궁극적인 기반으로 시스템 제공 정책을 가지고 있으므로, 규칙 업데이트를 가져오면 사용자 지정 기반 정책을 사용하더라도 정책에 영향이 미칠 수 있습니다. 체인의 첫 번째 사용자 지정 정책(시스템 제공 정책을 기반으로 사용하는 정책)에서 규칙 업데이트가 기반 정책을 수정하도록 허용하면 정책이 영향을 받을 수 있습니다. 이 설정 변경에 대한 자세한 내용은 24-4페이지의 규칙 업데이트가 시스템 제공 기반 정책을 수정하도록 허용을/를 참조하십시오.

규칙 업데이트에 의한 것이든 기반 정책으로 사용하는 사용자 지정 정책을 수정하는 것이든, 수행 방법과 상관없이 기반 정책에 대한 변경 사항은 My Changes 또는 다른 레이어의 설정을 변경하거나 재정의하지 않습니다.

기반 정책 변경

라이센스: 보호

네트워크 분석 또는 침입 정책에 대해 다른 기반 정책을 선택할 수 있으며, 선택적으로 상위 레이어의 수정에 영향을 주지 않은 채 규칙 업데이트가 시스템 제공 기반 정책을 수정하도록 허용할 수 있습니다.

기반 정책을 변경하려면

액세스: Admin/Intrusion Admin

1단계 정책을 수정하는 동안 탐색 패널에서 **Policy Information**을 클릭합니다.

Policy Information 페이지가 나타납니다.

2단계 **Base Policy** 드롭다운 목록에서 기반 정책을 선택합니다.

3단계 선택적으로, 시스템 제공 기반 정책을 선택한 경우 침입 규칙 업데이트가 기반 정책을 자동으로 수정할 수 있는지 여부를 지정하려면 **Manage Base Policy**를 클릭합니다.

자세한 내용은 24-4페이지의 규칙 업데이트가 시스템 제공 기반 정책을 수정하도록 허용을/를 참조하십시오.

4단계 정책을 저장하거나, 계속 수정하거나, 변경 사항을 취소하거나, 기반 정책의 기본 컨피그레이션 설정으로 돌아가거나, 시스템 캐시에 변경 사항이 남아 있는 상태로 종료합니다. 자세한 내용은 23-15페이지의 충돌 해결 및 정책 변경 사항 커밋을/를 참조하십시오.

규칙 업데이트가 시스템 제공 기반 정책을 수정하도록 허용

라이센스: 보호

가져온 규칙 업데이트는 시스템 제공 정책에 수정된 네트워크 분석 프리프로세서 설정, 수정된 침입 정책 고급 설정, 새로운/업데이트된 침입 규칙, 기존 규칙의 수정된 상태 등을 제공합니다. 또한 규칙 업데이트는 규칙을 삭제하고 새로운 규칙 카테고리와 기본 변수를 제공할 수 있습니다. 자세한 내용은 66-14페이지의 규칙 업데이트 및 로컬 규칙 파일 가져오기을/를 참조하십시오.

규칙 업데이트는 항상 프리프로세서, 고급 설정 및 규칙에 대한 변경 사항으로 시스템 제공 정책을 수정합니다. 기본 변수 및 규칙 카테고리에 대한 변경 사항은 시스템 레벨에서 처리됩니다. 자세한 내용은 24-3페이지의 시스템 제공 기반 정책 이해을/를 참조하십시오.

시스템 제공 정책을 기반 정책으로 사용하는 경우 규칙 업데이트(이 경우 시스템 제공 정책의 복사본)가 기반 정책을 수정하도록 허용할 수 있습니다. 규칙 업데이트가 기반 정책을 업데이트하도록 허용하는 경우, 새 규칙 업데이트는 기반 정책으로 사용하는 시스템 제공 정책에 대해 변경하는 것과 동일한 변경을 기반 정책에서 수행합니다. 해당 설정을 수정하지 않은 경우 기반 정책의 설정이 현재 정책의 설정을 결정합니다. 그러나 규칙 업데이트는 현재 정책에서 수행하는 변경 사항을 재정의하지 않습니다.

규칙 업데이트가 기반 정책을 업데이트하도록 허용하지 않는 경우, 하나 이상의 규칙 업데이트를 가져온 후 기반 정책을 수동으로 업데이트할 수 있습니다.

침입 정책의 규칙 상태와 상관없이 또는 규칙 업데이트가 기반 침입 정책을 업데이트하도록 허용하는지 여부와 상관없이, 규칙 업데이트는 항상 VRT가 삭제하는 침입 규칙을 삭제합니다. 변경 사항을 네트워크 트래픽에 다시 적용할 때까지, 현재 적용된 침입 정책의 규칙은 다음과 같이 작동합니다.

- 비활성화된 규칙은 비활성 상태로 남아 있습니다.
- Generate Events로 설정된 규칙은 트리거될 때 계속해서 이벤트를 생성합니다.
- Drop and Generate Events로 설정된 규칙은 트리거될 때 계속해서 이벤트를 생성하고 위반 패킷을 삭제합니다.

다음 두 조건이 모두 충족되지 않으면 규칙 업데이트는 사용자 지정 기반 정책을 수정하지 않습니다.

- 규칙 업데이트가 상위 정책(사용자 지정 기반 정책이 시작된 정책)의 시스템 제공 기반 정책을 수정하도록 허용함
- 상위 기반 정책의 해당 설정을 재정의하는 변경 사항을 상위 정책에서 수행함

두 조건이 충족되면 상위 정책을 저장할 때 규칙 업데이트의 변경 사항이 하위 정책(즉, 사용자 지정 기반 정책을 사용하는 정책)으로 전달됩니다.

예를 들어 규칙 업데이트가 전에 비활성화된 침입 규칙을 활성화하며 상위 침입 정책에서 규칙의 상태를 수정하지 않은 경우, 상위 정책을 저장하면 수정된 규칙 상태가 기반 정책으로 전달됩니다.

마찬가지로, 규칙 업데이트가 기본 프리프로세서 설정을 수정하며 상위 네트워크 분석 정책에서 설정을 수정하지 않은 경우, 상위 정책을 저장하면 수정된 설정이 기반 정책으로 전달됩니다.

자세한 내용은 24-4페이지의 기반 정책 변경을/를 참조하십시오.

규칙 업데이트가 시스템 제공 기반 정책을 수정하도록 허용하려면

액세스: Admin/Intrusion Admin

1단계 시스템 제공 정책을 기반 정책으로 사용하는 정책을 수정하는 동안 탐색 패널에서 **Policy Information**을 클릭합니다.

Policy Information 페이지가 나타납니다.

2단계 **Manage Base Policy**를 클릭합니다.

Base Policy 요약 페이지가 나타납니다.

3단계 **Update when a new Rule Update is installed** 확인란을 선택하거나 선택 취소합니다.

확인란을 취소하고 정책을 저장한 다음 규칙 업데이트를 가져오면 Base Policy 요약 페이지에 **Update Now** 버튼이 나타나고, 페이지의 상태 메시지가 업데이트되어 정책이 최신 상태가 아님을 알립니다. 선택적으로, 가장 최근에 가져온 규칙 업데이트의 변경 사항으로 기반 정책을 업데이트하려면 **Update Now**를 클릭할 수 있습니다.

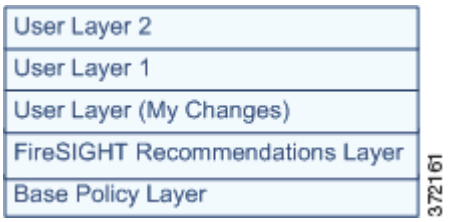
4단계 정책을 저장하거나, 계속 수정하거나, 변경 사항을 취소하거나, 기반 정책의 기본 컨피그레이션 설정으로 돌아가거나, 시스템 캐시에 변경 사항이 남아 있는 상태로 종료합니다. 자세한 내용은 23-15페이지의 충돌 해결 및 정책 변경 사항 커밋을/를 참조하십시오.

RecommendationsFireSIGHT 레이어 이해

라이센스: 보호

침입 정책에서 규칙 상태 권장 사항을 생성할 때 권장 사항을 기반으로 규칙 상태를 자동으로 수정할지 여부를 선택할 수 있습니다. 자세한 내용은 33-1페이지의 네트워크 자산에 대한 침입 방지 맞춤화을/를 참조하십시오.

다음 그림에서 알 수 있듯이, 권장 규칙 상태를 사용하면 읽기 전용의 내장 FireSIGHT Recommendations 레이어가 기반 레이어 바로 위에 추가됩니다.



이 레이어는 침입 정책에 대해 고유합니다.

나중에 권장 규칙 상태를 사용하지 않기로 선택하면 시스템은 FireSIGHT Recommendations 레이어를 제거합니다. 이 레이어는 수동으로 삭제할 수 없지만, 권장 규칙 상태의 사용 여부를 선택하여 추가 또는 제거할 수 있습니다.

FireSIGHT Recommendations 레이어를 추가하면 탐색 패널의 Policy Layers 아래에 FireSIGHT Recommendations 링크가 추가됩니다. 이 링크를 클릭하면 FireSIGHT Recommendations 레이어 페이지의 읽기 전용 보기가 나타납니다. 여기에서 Rules 페이지의 필터링된 권장 사항 보기에 읽기 전용 모드로 액세스할 수 있습니다. Rules 페이지에서 규칙으로 작업하는 방법에 대한 자세한 내용은 32-1페이지의 규칙을 사용하여 침입 정책 조정을/를 참조하십시오.

권장 규칙 상태를 사용하면 또한 탐색 패널의 FireSIGHT Recommendations 링크 아래에 Rules 하위 링크가 추가됩니다. Rules 하위 링크를 클릭하면 FireSIGHT Recommendations 레이어에서 Rules 페이지의 읽기 전용 표시에 액세스할 수 있습니다 이 보기에서 다음에 유의하십시오.

- 상태 열에 규칙 상태 아이콘이 없으면 해당 상태는 기반 정책에서 상속된 것입니다.
- 여기 또는 다른 Rules 페이지 보기의 FireSIGHT Recommendations 열에 규칙 상태 아이콘이 없으면 이 규칙에 대한 권장 사항이 없는 것입니다.

팁 규칙 상태가 권장되지 않으면 규칙의 오버헤드 등급이 권장 사항 생성 시 **Recommendation Threshold (By Rule Overhead)**에 대한 설정보다 높은 것입니다. 자세한 내용은 33-3페이지의 규칙 오버헤드 이해을/를 참조하십시오.

레이어 관리

라이센스: 보호

Policy Layers 페이지는 네트워크 분석 또는 침입 정책의 완전한 레이어 스택에 대한 단일 페이지 요약을 제공합니다. 이 페이지에서 공유 및 비공유 레이어를 추가하고, 레이어를 복사, 병합, 이동 및 삭제하고, 각 레이어의 요약 페이지에 액세스하고, 각 레이어 내에서 활성화, 비활성화 및 재정의된 컨피그레이션에 대한 컨피그레이션 페이지에 액세스할 수 있습니다.

각 레이어에 대해 다음 정보를 볼 수 있습니다.

- 레이어가 내장 레이어인지, 공유된 사용자 레이어인지, 공유되지 않은 사용자 레이어인지 여부
- 어떤 레이어에 가장 높은(효과적인) 프리프로세서 또는 고급 설정 컨피그레이션이 포함되어 있는지(기능 이름별)
- 침입 정책에서, 상태가 레이어에 설정되어 있고 각 규칙 상태에 대해 규칙 수가 설정된 침입 규칙의 수

각 레이어의 요약에 있는 기능 이름은 어떤 컨피그레이션이 레이어에서 활성화, 비활성화, 재정의 또는 상속되었는지를 다음과 같이 나타냅니다.

기능의 상태	기능의 이름
레이어에서 활성화됨	일반 텍스트로 작성됨
레이어에서 비활성화됨	취소선으로 표시됨
상위 레이어의 컨피그레이션에 의해 재정의됨	기울임꼴 텍스트로 작성됨
하위 레이어에서 상속됨	표시되지 않음

이 페이지는 또한 활성화된 모든 프리프로세서(네트워크 분석) 또는 고급 설정(침입), 침입 정책, 침입 규칙의 최종 효과에 대한 요약을 제공합니다.

다음 표에는 Policy Layers 페이지에서 사용할 수 있는 작업이 나열되어 있습니다.

표 24-1 네트워크 분석 및 침입 정책 레이어 컨피그레이션 작업

목적	가능한 작업
Policy Information 페이지 표시	**Policy Summary**를 클릭합니다. Policy Information 페이지에서 수행할 수 있는 작업에 대한 자세한 내용은 32-1페이지의 규칙을 사용하여 침입 정책 조정, 26-1페이지의 네트워크 분석 정책 시작하기 및 31-1페이지의 침입 정책 시작하기을/를 참조하십시오.
레이어의 요약 페이지 표시	레이어에 대한 행에서 레이어 이름을 클릭하거나, 사용자 레이어 옆에 있는 수정 아이콘( )을 클릭합니다. 공유 레이어에 대한 읽기 전용 요약 페이지에 액세스하려면 보기 아이콘( )을 클릭할 수도 있습니다. 레이어에 대한 요약 페이지에서 수행할 수 있는 작업에 대한 자세한 내용은 24-11페이지의 정책 간에 레이어 공유, 24-16페이지의 레이어에서 프리프로세서 및 고급 설정 구성 및 24-12페이지의 레이어에서 침입 규칙 구성을/를 참조하십시오.
레이어 레벨 프리프로세서 또는 고급 설정 컨피그레이션 페이지에 액세스	레이어에 대한 행에서 기능 이름 클릭 컨피그레이션 페이지는 기반 정책 및 공유 레이어에 있는 읽기 전용 페이지입니다. 자세한 내용은 24-16페이지의 레이어에서 프리프로세서 및 고급 설정 구성을/를 참조하십시오.

표 24-1 네트워크 분석 및 침입 정책 레이어 컨피그레이션 작업(계속)

목적	가능한 작업
규칙 상태 유형으로 필터링된 레이어 레벨 규칙 컨피그레이션 페이지에 액세스	레이어에 대한 요약에서 이벤트 삭제 및 생성(✖), 이벤트 생성(➡) 또는 비활성(➡)에 대한 아이콘을 클릭합니다. 선택한 규칙 상태에 대해 설정된 규칙이 레이어에 포함되지 않은 경우 규칙이 표시되지 않습니다.
레이어를 정책에 추가	24-8페이지의 레이어 추가을/를 참조하십시오.
다른 정책에서 공유 레이어 추가	24-11페이지의 정책 간에 레이어 공유을/를 참조하십시오.
레이어의 이름 또는 설명 변경	24-9페이지의 레이어의 이름 및 설명 변경을/를 참조하십시오.
레이어 이동, 복사 또는 삭제	24-9페이지의 레이어 이동, 복사 및 삭제을/를 참조하십시오.
레이어를 그 아래에 있는 다음 레이어로 병합	24-10페이지의 레이어 병합을/를 참조하십시오.

Policy Layers 페이지를 사용하려면

액세스: Admin/Intrusion Admin

1단계 정책을 수정하는 동안 탐색 패널에서 **Policy Layers**를 클릭합니다.

Policy Layers 요약 페이지가 나타납니다.

2단계 네트워크 분석 및 침입 정책 레이어 컨피그레이션 작업 표의 작업을 수행할 수 있습니다.

3단계 정책을 저장하거나, 계속 수정하거나, 변경 사항을 취소하거나, 기반 정책의 기본 컨피그레이션 설정으로 돌아가거나, 시스템 캐시에 변경 사항이 남아 있는 상태로 종료합니다. 자세한 내용은 23-15페이지의 충돌 해결 및 정책 변경 사항 커밋을/를 참조하십시오.

레이어 추가

라이센스: 보호

네트워크 분석 또는 침입 정책에 최대 200개의 레이어를 추가할 수 있습니다. 레이어를 추가하면 정책에서 최상위 레이어로 나타납니다. 초기 상태는 모든 기능에 대해 Inherit이며 침입 정책에 이벤트 필터링, 동적 상태 또는 알림 규칙 작업이 설정되어 있지 않습니다.

네트워크 분석 또는 침입 정책에 레이어를 추가하려면

액세스: Admin/Intrusion Admin

1단계 정책을 수정하는 동안 탐색 패널에서 **Policy Layers**를 클릭합니다.

Policy Layers 페이지가 나타납니다.

2단계 User Layers 옆에 있는 레이어 추가 아이콘(⊕)을 클릭합니다.

Add Layer 팝업 창이 나타납니다.

3단계 고유한 레이어 **Name**을 입력하고 **OK**를 클릭합니다.

새 레이어가 User Layers 아래의 맨 위 레이어로 나타납니다.

4단계 정책을 저장하거나, 계속 수정하거나, 변경 사항을 취소하거나, 기반 정책의 기본 컨피그레이션 설정으로 돌아가거나, 시스템 캐시에 변경 사항이 남아 있는 상태로 종료합니다. 자세한 내용은 23-15 페이지의 충돌 해결 및 정책 변경 사항 커밋을/를 참조하십시오.

레이어의 이름 및 설명 변경

라이센스: 보호

네트워크 분석 또는 침입 정책에서 사용자 구성 가능한 레이어의 이름을 변경할 수 있으며, 선택적으로 레이어를 수정할 때 표시되는 설명을 추가 또는 수정할 수 있습니다.

레이어의 이름을 변경하고 설명을 추가 또는 수정하려면

액세스: Admin/Intrusion Admin

1단계 정책을 수정하는 동안 탐색 패널에서 **Policy Layers**를 클릭합니다.

Policy Layers 페이지가 나타납니다.

2단계 수정하려는 사용자 레이어 옆에 있는 수정 아이콘( )을 클릭합니다.

레이어에 대한 요약 페이지가 나타납니다.

3단계 다음과 같은 작업을 수행할 수 있습니다.

- 레이어 **Name**을 수정합니다.
- 레이어 **Description**을 추가 또는 수정합니다.

4단계 정책을 저장하거나, 계속 수정하거나, 변경 사항을 취소하거나, 기반 정책의 기본 컨피그레이션 설정으로 돌아가거나, 시스템 캐시에 변경 사항이 남아 있는 상태로 종료합니다. 자세한 내용은 23-15 페이지의 충돌 해결 및 정책 변경 사항 커밋을/를 참조하십시오.

레이어 이동, 복사 및 삭제

라이센스: 보호

네트워크 분석 또는 침입 정책에서 사용자 레이어(초기 My Changes 레이어 포함)를 복사, 이동 또는 삭제할 수 있습니다. 다음 사항을 고려하십시오.

- 레이어를 복사하면 복사본이 최상위 레이어로 나타납니다.
- 공유 레이어를 복사하면 비공유 복사본이 생성되며, 선택적으로 이를 다른 정책과 공유할 수 있습니다.
- 공유 레이어는 삭제할 수 없습니다. 공유가 활성화되었지만 다른 정책과 공유되지 않은 레이어는 공유 레이어가 아닙니다.

레이어를 복사, 이동 또는 삭제하려면

액세스: Admin/Intrusion Admin

1단계 정책을 수정하는 동안 탐색 패널에서 **Policy Layers**를 클릭합니다.

Policy Layers 페이지가 나타납니다.

2단계 다음과 같은 작업을 수행할 수 있습니다.

- 레이어를 복사하려면 복사할 레이어에 대한 복사 아이콘()을 클릭합니다.

  페이지가 새로 고쳐지고 레이어의 복사본이 최상위 레이어로 나타납니다.

- User Layers 페이지 영역 내에서 레이어를 위나 아래로 이동하려면, 레이어 요약에서 열린 영역을 클릭하고 위치 화살표()가 이동하려는 레이어의 위나 아래에 있는 선을 가리킬 때까지 끕니다.

  화면이 새로 고쳐지고 레이어가 새 위치에 나타납니다.

- 레이어를 삭제하려면 삭제할 레이어에 대한 삭제 아이콘()을 클릭하고 **OK**를 클릭합니다.

  페이지가 새로 고쳐지고 레이어가 삭제됩니다.

3단계 정책을 저장하거나, 계속 수정하거나, 변경 사항을 취소하거나, 기반 정책의 기본 컨피그레이션 설정으로 돌아가거나, 시스템 캐시에 변경 사항이 남아 있는 상태로 종료합니다. 자세한 내용은 23-15 페이지의 충돌 해결 및 정책 변경 사항 커밋을/를 참조하십시오.

레이어 병합

라이센스: 보호

네트워크 분석 또는 침입 정책의 사용자 구성 가능한 레이어를 아래에 있는 다음 사용자 레이어와 병합할 수 있습니다. 병합된 레이어는 각 레이어의 고유한 설정을 모두 보유하며, 두 레이어 모두 동일한 프리프로세서에 대한 설정, 침입 규칙 또는 고급 설정을 포함한 경우 상위 레이어의 설정을 수용합니다. 병합된 레이어는 하위 레이어의 이름을 유지합니다.

다른 정책에 추가한 공유 레이어를 생성하는 정책에서, 공유 레이어 바로 위의 비공유 레이어는 공유 레이어와 병합할 수 있지만, 아래에 있는 비공유 레이어는 공유 레이어와 병합할 수 없습니다.

또 다른 정책에서 생성한 공유 레이어를 추가하는 정책에서는 공유 레이어를 바로 아래에 있는 비공유 레이어에 병합할 수 있으며 이 경우 그 결과 레이어는 더 이상 공유되지 않습니다. 비공유 레이어는 그 아래에 있는 공유 레이어에 병합할 수 없습니다.

사용자 레이어를 그 아래의 사용자 레이어와 병합하려면

액세스: Admin/Intrusion Admin

1단계 정책을 수정하는 동안 탐색 패널에서 **Policy Layers**를 클릭합니다.

Policy Layers 페이지가 나타납니다.

2단계 두 레이어 중 위의 레이어에 있는 병합 아이콘()을 클릭하고 **OK**를 클릭합니다.

페이지가 새로 고쳐지고 레이어가 그 아래에 있는 레이어와 병합됩니다.

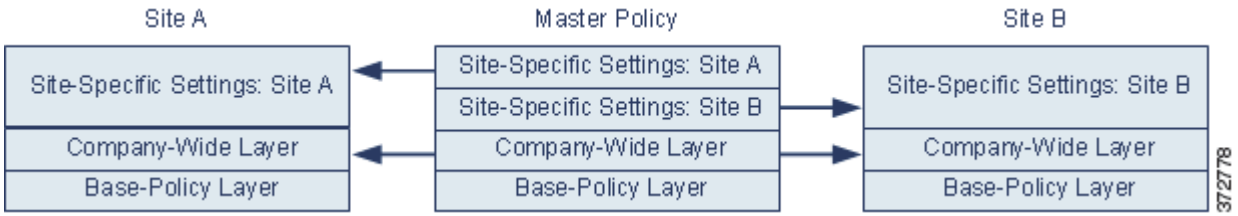
3단계 정책을 저장하거나, 계속 수정하거나, 변경 사항을 취소하거나, 기반 정책의 기본 컨피그레이션 설정으로 돌아가거나, 시스템 캐시에 변경 사항이 남아 있는 상태로 종료합니다. 자세한 내용은 23-15 페이지의 충돌 해결 및 정책 변경 사항 커밋을/를 참조하십시오.

정책 간에 레이어 공유

라이센스: 보호

사용자 공유 가능한 레이어를 동일한 유형(침입 또는 네트워크 분석)의 다른 정책과 공유할 수 있습니다. 공유 레이어 내에서 컨피그레이션을 수정하고 변경 사항을 커밋하면, 시스템은 공유 레이어를 사용하는 모든 정책을 업데이트하고 영향받는 모든 정책의 목록을 제공합니다. 레이어를 생성한 정책에 있는 공유 레이어 기능 컨피그레이션만 수정할 수 있습니다.

다음 그림은 사이트별 정책에 대한 소스로 사용되는 마스터 정책의 예입니다.



이 그림의 마스터 정책에는 Site A 및 Site B의 정책에 적용되는 설정과 함께 회사 전체의 레이어가 포함됩니다. 또한 각 정책에 대한 사이트별 레이어도 포함됩니다. 예를 들어 네트워크 분석 정책의 경우 Site A에는 모니터링되는 네트워크에 웹 서버가 없을 수 있으며 HTTP Inspect 프리프로세서의 보호 또는 처리 오버헤드가 필요하지 않을 수 있지만, 두 사이트에 모두 TCP 스트림 전처리가 필요할 수 있습니다. 두 사이트에서 공유하는 회사 전체의 레이어에서 TCP 스트림 처리를 활성화하고, Site A와 공유하는 사이트별 레이어에서 HTTP Inspect 프리프로세서를 비활성화하고, Site B와 공유하는 사이트별 레이어에서 HTTP Inspect 프리프로세서를 활성화할 수 있습니다. 사이트별 정책의 상위 레이어에서 컨피그레이션을 수정함으로써 필요 시 컨피그레이션 조정과 함께 각 사이트에 대한 정책을 더 세부적으로 조정할 수도 있습니다.

마스터 정책 예에서 합병된 최종 설정이 트래픽 모니터링에 유용할 것이라고 말할 수는 없지만, 사이트별 정책의 구성 및 업데이트에서 절약되는 시간을 고려하면 정책 레이어를 유용하게 응용하는 예라고 할 수 있습니다.

다른 많은 레이어 컨피그레이션도 가능합니다. 예를 들어 회사, 부서, 네트워크, 심지어 사용자 단위로도 정책 레이어를 정의할 수 있습니다. 침입 정책의 경우 한 레이어에는 고급 설정을 포함하고 다른 레이어에는 규칙 설정을 포함할 수도 있습니다.

팁 기반 정책이 공유하려는 레이어가 생성된 사용자 지정 정책인 경우에는 정책에 공유 레이어를 추가할 수 없습니다. 변경 사항을 저장하려고 시도하면 정책에 순환 종속성이 포함되어 있다는 오류 메시지가 표시됩니다. 자세한 내용은 24-3페이지의 사용자 지정 기반 정책 이해을/를 참조하십시오.

레이어를 다른 정책과 공유하려면 다음을 수행해야 합니다.

- 공유할 레이어의 레이어 요약 페이지에서 공유를 활성화합니다.
- 공유하려는 정책의 Policy Layers 페이지에서 공유 레이어를 추가합니다.

다른 정책에서 사용되고 있는 레이어에 대한 공유를 비활성화할 수 없습니다. 먼저 다른 정책에서 레이어를 삭제하거나 다른 정책을 삭제해야 합니다.

다른 정책과의 레이어 공유를 활성화 또는 비활성화하려면

액세스: Admin/Intrusion Admin

1단계 정책을 수정하는 동안 탐색 패널에서 **Policy Layers**를 클릭합니다.

Policy Layers 페이지가 나타납니다.

2단계 다른 정책과 공유하려는 레이어 옆에 있는 수정 아이콘( )을 클릭합니다.

레이어에 대한 요약 페이지가 나타납니다.

3단계 **Sharing** 확인란을 선택(활성화) 또는 선택 취소(비활성화)합니다.

4단계 정책을 저장하거나, 계속 수정하거나, 변경 사항을 취소하거나, 기반 정책의 기본 컨피그레이션 설정으로 돌아가거나, 시스템 캐시에 변경 사항이 남아 있는 상태로 종료합니다. 자세한 내용은 23-15 페이지의 충돌 해결 및 정책 변경 사항 커밋을/를 참조하십시오.

공유 레이어를 정책에 추가하려면

액세스: Admin/Intrusion Admin

1단계 정책을 수정하는 동안 탐색 패널에서 **Policy Layers**를 클릭합니다.

Policy Layers 페이지가 나타납니다.

2단계 User Layers 옆에 있는 공유 레이어 추가 아이콘( )을 클릭합니다.

Add Shared Layer 팝업 창이 나타납니다.

3단계 추가하려는 공유 레이어를 Add Shared Layer 드롭다운 목록에서 선택하고 **OK**를 클릭합니다.

Policy Layers 요약 페이지가 나타나고, 선택한 공유 레이어가 정책에서 최상위 레이어로 나타납니다.

다른 정책에 공유 레이어가 없으면 드롭다운 목록이 나타나지 않습니다. 팝업 창에서 **OK**를 클릭하거나, Policy Layers 요약 페이지로 돌아가려면 **Cancel**을 클릭합니다.

4단계 정책을 저장하거나, 계속 수정하거나, 변경 사항을 취소하거나, 기반 정책의 기본 컨피그레이션 설정으로 돌아가거나, 시스템 캐시에 변경 사항이 남아 있는 상태로 종료합니다. 자세한 내용은 23-15 페이지의 충돌 해결 및 정책 변경 사항 커밋을/를 참조하십시오.

레이어에서 침입 규칙 구성

라이센스: 보호

침입 정책에서 사용자 구성 가능한 레이어의 규칙에 대해 규칙 상태, 이벤트 필터링, 동적 상태, 알림, 규칙 코멘트를 설정할 수 있습니다. 변경할 수 있는 레이어에 액세스한 후 침입 정책 Rules 페이지에서 하듯 레이어에 대한 Rules 페이지에서 설정을 추가합니다. 32-1페이지의 규칙을 사용하여 침입 정책 조정을/를 참조하십시오.

레이어에 대한 Rules 페이지에서 개별 레이어 설정을 볼 수도 있고, Rules 페이지의 정책 보기에서 모든 설정의 최종 효과를 볼 수도 있습니다. Rules 페이지의 정책 보기에서 규칙 설정을 수정할 경우 정책에서 사용자 구성 가능한 최상위 레이어를 수정하게 됩니다. Rules 페이지의 레이어 드롭다운 목록을 사용하여 다른 레이어로 전환할 수 있습니다.

다음 표에서는 여러 레이어에서 동일한 설정 유형을 구성하는 효과에 대해 설명합니다.

표 24-2 레이어 규칙 설정

설정 가능 개수	설정 유형	목적
1	규칙 상태	하위 레이어의 규칙에 대해 설정된 규칙 상태를 재정의하고, 하위 레이어에서 구성된 해당 규칙에 대한 모든 임계값, 억제, 등급 기반 규칙 상태 및 알림을 무시합니다. 자세한 내용은 32-20페이지의 규칙 상태 설정을/를 참조하십시오. 규칙이 기반 정책 또는 하위 레이어에서 상태를 상속하도록 하려면 규칙 상태를 Inherit로 설정합니다. 침입 정책 Rules 페이지에서 작업할 때에는 규칙 상태를 Inherit로 설정할 수 없습니다. 규칙 상태 설정은 특정 레이어에 대한 Rules 페이지에서 볼 때 색으로 표시됩니다. 유효한 상태가 하위 레이어에 설정된 규칙은 노란색으로 강조 표시되고, 유효한 상태가 상위 레이어에 설정된 규칙은 빨간색으로 강조 표시되며, 유효한 상태가 현재 레이어에 설정된 규칙은 강조 표시되지 않습니다. 침입 정책 Rules 페이지는 모든 규칙 설정의 최종 효과에 대한 복합 보기이므로, 이 페이지에서는 규칙 상태가 색으로 표시되지 않습니다.
1	임계값 SNMP 알림	하위 레이어의 규칙에 대한 동일한 유형의 설정을 재정의합니다. 임계값을 설정하면 레이어의 규칙에 대한 기존 임계값을 덮어쓰게 됩니다. 자세한 내용은 32-22페이지의 이벤트 임계값 구성 및 32-33페이지의 SNMP 알림 추가을/를 참조하십시오.
하나 이상	억제 등급 기반 규칙 상태	선택한 각 규칙에 대해 동일한 유형의 설정을 규칙에 대해 규칙 상태가 설정된 첫 번째 레이어까지 아래로 누적 결합합니다. 규칙 상태가 설정된 레이어 아래의 설정은 무시됩니다. 자세한 내용은 32-26페이지의 침입 정책당 억제 구성 및 32-29페이지의 동적 규칙 상태 추가을/를 참조하십시오.
하나 이상	참고	규칙에 코멘트를 추가합니다. 코멘트는 정책이나 레이어별이 아니라 규칙별로 추가됩니다. 모든 레이어에서 규칙에 하나 이상의 코멘트를 추가할 수 있습니다. 자세한 내용은 32-9페이지의 규칙에 대한 규칙 코멘트 추가을/를 참조하십시오.

예를 들어 한 레이어에서는 규칙 상태를 Drop and Generate Events로 설정하고 상위 레이어에서는 Disabled로 설정하면, 침입 정책 Rules 페이지에는 규칙이 Disabled로 표시됩니다.

또 다른 예에서, 규칙에 대한 소스 기반 억제를 한 레이어에서 192.168.1.1로 설정하고 규칙에 대한 목적지 기반 억제를 다른 레이어에서 192.168.1.2로 설정하면, Rules 페이지에서는 누적 효과가 소스 주소 192.168.1.1 및 목적지 주소 192.168.1.2에 대한 이벤트를 억제하는 것으로 표시됩니다. 억제 및 등급 기반 규칙 상태 설정은 선택한 각 규칙에 대해 동일한 유형의 설정을 규칙에 대해 규칙 상태가 설정된 첫 번째 레이어까지 아래로 누적 결합합니다. 규칙 상태가 설정된 레이어 아래의 설정은 무시됩니다.

레이어에서 규칙을 수정하려면

액세스: Admin/Intrusion Admin

1단계 침입 정책을 수정하는 동안 탐색 패널에서 **Policy Layers**를 확장하고 수정하려는 정책 레이어를 확장합니다.

2단계 수정하려는 정책 레이어 바로 아래에 있는 **Rules**를 클릭합니다.

레이어에 대한 Rules 페이지가 나타납니다.

레이어 규칙 설정 표의 설정을 수정할 수 있습니다. 침입 규칙 구성에 대한 자세한 내용은 32-1페이지의 규칙을 사용하여 침입 정책 조정을/를 참조하십시오.

수정 가능한 레이어에서 개별 설정을 삭제하려면, 규칙 세부사항을 표시할 레이어에 대한 Rules 페이지에서 규칙 메시지를 두 번 클릭합니다. 삭제할 설정 옆에 있는 **Delete**를 클릭한 다음 **OK**를 두 번 클릭합니다.

3단계 정책을 저장하거나, 계속 수정하거나, 변경 사항을 취소하거나, 기반 정책의 기본 컨피그레이션 설정으로 돌아가거나, 시스템 캐시에 변경 사항이 남아 있는 상태로 종료합니다. 자세한 내용은 23-15 페이지의 충돌 해결 및 정책 변경 사항 커밋을/를 참조하십시오.

다중 레이어 규칙 설정 제거

라이센스: 보호

침입 정책 Rules 페이지에서 하나 이상의 규칙을 선택한 다음 침입 정책의 여러 레이어에서 특정 유형의 이벤트 필터, 동적 상태 또는 알림을 동시에 제거할 수 있습니다.

시스템은 모든 설정을 제거할 때까지 또는 규칙에 대해 규칙 상태가 설정된 레이어에 도달할 때까지, 설정된 각 레이어를 통해 아래로 설정 유형을 제거합니다. 규칙 상태가 설정된 레이어에 도달하면 해당 레이어에서 설정이 제거되고 설정 유형 제거가 중지됩니다.

공유 레이어 또는 기반 정책에서 설정 유형에 도달하거나 정책에서 최상위 레이어가 수정 가능한 상태인 경우, 시스템은 규칙에 대한 나머지 설정 및 규칙 상태를 수정 가능한 해당 레이어로 복사합니다. 또는 정책에서 최상위 레이어가 공유 레이어인 경우, 시스템은 공유 레이어 위에 새로운 수정 가능한 레이어를 생성하고 규칙에 대한 나머지 설정 및 규칙 상태를 수정 가능한 해당 레이어로 복사합니다.

참고 공유 레이어 또는 기반 정책에서 파생된 규칙 설정을 제거하면 하위 레이어 또는 기반 정책에서 온 이 규칙에 대한 변경 사항이 무시됩니다. 하위 레이어 또는 기반 정책에서 온 변경 사항이 무시되는 것을 중지하려면 맨 위의 레이어에 대한 요약 페이지에서 규칙 상태를 **Inherit**로 설정합니다. 자세한 내용은 32-20페이지의 규칙 상태 설정을/를 참조하십시오.

여러 레이어에서 규칙 설정을 제거하려면

액세스: Admin/Intrusion Admin

1단계 침입 정책을 수정하는 동안 탐색 패널에서 Policy Information 바로 아래에 있는 **Rules**를 클릭합니다.

팁 또한 모든 레이어의 Rules 페이지에 있는 레이어 드롭다운 목록에서 **Policy**를 선택하거나, Policy Information 페이지에서 **Manage Rules**를 선택할 수도 있습니다.

침입 정책 Rules 페이지가 나타납니다.

2단계 여러 설정을 제거할 하나 이상의 규칙을 선택합니다. 다음 옵션을 이용할 수 있습니다.

- 특정 규칙을 선택하려면 규칙 옆에 있는 확인란을 선택합니다.
- 현재 목록의 모든 규칙을 선택하려면 열 맨 위에 있는 확인란을 선택합니다.

규칙 찾기에 대한 자세한 내용은 32-10페이지의 침입 정책의 규칙 필터링 이해 및 32-18페이지의 침입 정책에서 규칙 필터 설정을/를 참조하십시오.

3단계 다음 옵션을 이용할 수 있습니다.

- 규칙에 대한 모든 임계값을 제거하려면 **Event Filtering > Remove Thresholds**를 선택합니다.
- 규칙에 대한 모든 억제를 제거하려면 **Event Filtering > Remove Suppressions**를 선택합니다.
- 규칙에 대한 모든 등급 기반 규칙 상태를 제거하려면 **Dynamic State > Remove Rate-Based Rule States**를 선택합니다.
- 규칙에 대한 모든 SNMP 알림 설정을 제거하려면 **Alerting > Remove SNMP Alerts**를 선택합니다.

확인 팝업 창이 나타납니다.

참고 공유 레이어 또는 기반 정책에서 파생된 규칙 설정을 제거하면 하위 레이어 또는 기반 정책에서 온 이 규칙에 대한 변경 사항이 무시됩니다. 하위 레이어 또는 기반 정책에서 온 변경 사항이 무시되는 것을 중지하려면 맨 위의 레이어에 대한 요약 페이지에서 규칙 상태를 **Inherit**로 설정합니다. 자세한 내용은 32-20페이지의 규칙 상태 설정을/를 참조하십시오.

4단계 **OK**를 클릭합니다.

시스템은 선택한 설정을 제거하고, 규칙에 대한 나머지 설정을 정책에서 수정 가능한 최상위 레이어로 복사합니다. 시스템이 나머지 설정을 복사하는 방법에 영향을 주는 조건은 이 절차의 소개 부분을/를 참조하십시오.

5단계 정책을 저장하거나, 계속 수정하거나, 변경 사항을 취소하거나, 기반 정책의 기본 컨피그레이션 설정으로 돌아가거나, 시스템 캐시에 변경 사항이 남아 있는 상태로 종료합니다. 자세한 내용은 23-15페이지의 충돌 해결 및 정책 변경 사항 커밋을/를 참조하십시오.

사용자 지정 기반 정책에서 규칙 변경 사항 수용

라이센스: 보호

레이어를 추가하지 않은 사용자 지정 네트워크 분석 또는 침입 정책이 기반 정책으로 다른 사용자 지정 정책을 사용할 때, 다음과 같은 경우 해당 규칙 상태를 상속할 규칙을 설정해야 합니다.

- 기반 정책의 규칙에 대해 설정된 이벤트 필터, 동적 상태 또는 SNMP 알림 설정을 삭제하는 경우
- 기반 정책으로 사용하는 다른 사용자 지정 정책에서 수행하는 후속 변경 사항을 규칙이 수용하도록 하려는 경우

다음 절차에서는 이를 수행하는 방법에 대해 설명합니다. 레이어를 추가한 정책에서 이러한 규칙에 대한 설정을 수용하려면 24-14페이지의 다중 레이어 규칙 설정 제거을/를 참조하십시오.

레이어를 추가하지 않은 정책에서 규칙 변경 사항을 수용하려면

액세스: Admin/Intrusion Admin

1단계 침입 정책을 수정하는 동안 탐색 패널에서 **Policy Layers** 링크를 확장한 다음 **My Changes** 링크를 확장합니다.

2단계 My Changes 바로 아래에 있는 **Rules** 링크를 클릭합니다.

My Changes 레이어에 대한 Rules 페이지가 나타납니다.

3단계 설정을 수용할 하나 이상의 규칙을 선택합니다. 다음 옵션을 이용할 수 있습니다.

- 특정 규칙을 선택하려면 규칙 옆에 있는 확인란을 선택합니다.
- 현재 목록의 모든 규칙을 선택하려면 열 맨 위에 있는 확인란을 선택합니다.

규칙 찾기에 대한 자세한 내용은 32-10페이지의 침입 정책의 규칙 필터링 이해 및 32-18페이지의 침입 정책에서 규칙 필터 설정을/를 참조하십시오.

4단계 **Rule State** 드롭다운 목록에서 **Inherit**를 선택합니다.

5단계 정책을 저장하거나, 계속 수정하거나, 변경 사항을 취소하거나, 기반 정책의 기본 컨피그레이션 설정으로 돌아가거나, 시스템 캐시에 변경 사항이 남아 있는 상태로 종료합니다. 자세한 내용은 23-15페이지의 충돌 해결 및 정책 변경 사항 커밋을/를 참조하십시오.

레이어에서 프리프로세서 및 고급 설정 구성

라이센스: 보호

네트워크 분석 정책에서 프리프로세서를 구성할 때와 침입 정책에서 고급 설정을 구성할 때 유사한 메커니즘을 사용합니다. 네트워크 분석 Settings 페이지에서 프리프로세서를 활성화 및 비활성화할 수 있으며 침입 정책 Advanced Settings 페이지에서 침입 정책 고급 설정을 활성화 및 비활성화할 수 있습니다. 이러한 페이지에는 또한 모든 관련 기능에 대한 유효한 상태가 요약되어 표시됩니다. 예를 들어 네트워크 분석 SSL 프리프로세서가 한 레이어에서 비활성화되고 상위 레이어에서 활성화된 경우 Settings 페이지에는 활성 상태로 표시됩니다. 이러한 페이지에 대한 변경 사항은 정책의 상위 레이어에 나타납니다.

또한 프리프로세서나 고급 설정을 활성화하거나 비활성화할 수 있으며, 사용자 구성 가능한 레이어에 대한 요약 페이지에서 해당 컨피그레이션 페이지에 액세스할 수 있습니다. 이 페이지에서 레이어 이름과 설명을 수정하고, 동일한 유형의 다른 정책과 레이어를 공유할지 여부를 구성할 수 있습니다. 자세한 내용은 24-11페이지의 정책 간에 레이어 공유을/를 참조하십시오. 탐색 패널의 **Policy Layers** 아래에서 레이어 이름을 선택하여 다른 레이어에 대한 요약 페이지로 전환할 수 있습니다.

프리프로세서 또는 고급 설정을 활성화하면 해당 기능의 컨피그레이션 페이지에 대한 하위 링크가 탐색 패널의 레이어 이름 아래에 나타나며, 레이어의 요약 페이지에서 기능 옆에 수정 아이콘()이 나타납니다. 레이어에서 기능을 비활성화하거나 Inherit로 설정하면 이러한 링크와 아이콘이 사라집니다.

프리프로세서 또는 고급 설정에 대해 상태(활성 또는 비활성)를 설정하면 하위 레이어에서 해당 기능에 대한 상태 및 컨피그레이션 설정이 재정의됩니다. 프리프로세서 또는 고급 설정이 기반 정책 또는 하위 레이어에서 상태와 컨피그레이션을 상속하도록 하려면 **Inherit**로 설정합니다. Settings 또는 Advanced Settings 페이지에서 작업할 때에는 Inherit를 선택할 수 없습니다.

각 레이어 요약 페이지에서 색으로 지정되어 있어서 유효한 컨피그레이션이 상위, 하위 또는 현재 레이어 중 어디에 있는지를 다음과 같이 알 수 있습니다.

- 빨간색 - 유효한 컨피그레이션이 상위 레이어에 있음
- 노란색 - 유효한 컨피그레이션이 하위 레이어에 있음
- 색 없음 - 유효한 컨피그레이션이 현재 레이어에 있음

Settings 및 Advanced Settings 페이지는 모든 관련 설정에 대한 복합 보기이므로 유효한 컨피그레이션의 위치를 표시하는 데 색이 사용되지 않습니다.

시스템은 기능이 활성화된 최상위 레이어의 컨피그레이션을 사용합니다. 컨피그레이션을 명시적으로 수정하지 않는 한 시스템은 기본 컨피그레이션을 사용합니다. 예를 들어 한 레이어에서 네트워크 분석 DCE/RPC 프리프로세서를 활성화 및 수정하고 상위 레이어에서 활성화하되 수정하지 않는 경우, 시스템은 상위 레이어의 기본 컨피그레이션을 사용합니다.

다음 표에서는 사용자 구성 가능한 레이어에 대한 요약 페이지에서 사용할 수 있는 작업에 대해 설명합니다.

표 24-3 레이어 요약 페이지 작업

목적	가능한 작업
레이어 이름 또는 설명 수정	**Name** 또는 **Description**에 대해 새 값을 입력합니다.
레이어를 다른 침입 정책과 공유	**Allow this layer to be used by other policies**를 선택합니다. 자세한 내용은 24-11페이지의 정책 간에 레이어 공유을/를 참조하십시오.
현재 레이어에서 프리프로세서/고급 설정을 활성화 또는 비활성화	기능 옆에 있는 **Enabled** 또는 **Disabled**를 클릭합니다. 활성화하면, 컨피그레이션 페이지에 대한 하위 링크가 탐색 패널의 레이어 이름 아래에 나타나고, 요약 페이지에서 기능 옆에 수정 아이콘()이 나타납니다. 비활성화하면 하위 링크 및 수정 아이콘이 제거됩니다.
현재 레이어 아래의 최상위 레이어에 있는 설정에서 프리프로세서/고급 설정 상태 및 컨피그레이션 상속	**Inherit**를 클릭합니다. 페이지가 새로 고쳐지고, 기능이 활성화된 경우 탐색 패널의 기능 하위 링크와 수정 아이콘이 더 이상 나타나지 않습니다.
활성화된 프리프로세서/고급 설정에 대한 컨피그레이션 페이지에 액세스	현재 컨피그레이션을 수정하려면 수정 아이콘() 또는 기능 하위 링크를 클릭합니다. Back Orifice 프리프로세서에는 사용자 구성 가능한 옵션이 없습니다.

사용자 레이어에서 프리프로세서/고급 설정을 수정하려면

액세스: Admin/Intrusion Admin

1단계 정책을 수정하는 동안 탐색 패널에서 **Policy Layers**를 확장한 다음 수정하려는 레이어의 이름을 클릭합니다.

레이어에 대한 요약 페이지가 나타납니다.

2단계 레이어 요약 페이지 작업 표의 작업을 수행할 수 있습니다.

3단계 정책을 저장하거나, 계속 수정하거나, 변경 사항을 취소하거나, 기반 정책의 기본 컨피그레이션 설정으로 돌아가거나, 시스템 캐시에 변경 사항이 남아 있는 상태로 종료합니다. 자세한 내용은 23-15페이지의 충돌 해결 및 정책 변경 사항 커밋을/를 참조하십시오.

25장 트래픽 전처리 맞춤화

액세스 제어 정책의 많은 고급 설정은 구성하는 데 특정한 전문 지식을 필요로 하는 침입 탐지 및 방지 컨피그레이션을 제어합니다. 고급 설정은 일반적으로 거의 또는 전혀 수정할 필요가 없으며 모든 구축에서 공통적으로 적용하지 않습니다.

이 장에서는 다음 기본 설정을 설정하는 방법에 대해 설명합니다.

- 25-1페이지의 액세스 제어에 대한 기본 침입 정책 설정에서는 시스템에서 트래픽을 검사하는 방법을 결정하기 전에 트래픽을 초기에 검사하는 데 사용되는 액세스 제어 정책의 기본 침입 정책을 변경하는 방법에 대해 설명합니다.
- 25-3페이지의 네트워크 분석 정책으로 전처리 맞춤화에서는 매칭되는 트래픽을 전처리하는 사용자 지정 네트워크 분석 정책을 할당하여 특정 보안 영역, 네트워크, VLAN에 대한 특정한 트래픽 전처리 옵션을 맞춤화하는 방법에 대해 설명합니다.

다른 장에서는 액세스 제어 정책에 대한 정책 전반의 전처리 및 성능 옵션을 설명합니다. 자세한 내용은 다음 링크를 참고하십시오.

- 29-2페이지의 고급 Transport/Network 설정 구성
- 30-1페이지의 수동 구축 시 전처리 튜닝
- 18-8페이지의 침입 방지 성능 조정
- 18-20페이지의 파일 및 악성코드 검사 성능과 저장 조정

액세스 제어에 대한 기본 침입 정책 설정

라이센스: 모든

각 액세스 제어 정책은 *기본 침입 정책*을 사용하여 시스템에서 트래픽을 검사하는 방법을 결정하기 전에 트래픽을 초기에 검사합니다. 이렇게 해야 하는 이유는 시스템에서 어떤 액세스 제어 규칙으로 트래픽을 처리할 수 있는지 결정하기 전에, 연결의 처음 몇 가지 패킷을 처리하여 **해당 패킷의 통과를 허용**해야 하는 경우가 있기 때문입니다. 그러나 이러한 패킷은 검사하지 않은 대상에 도달할 수 없으므로, 침입 정책(기본 침입 정책)을 사용하여 해당 패킷을 검사하고 침입 이벤트를 생성할 수 있습니다.

기본 침입 정책은 애플리케이션 제어 및 URL 필터링을 수행할 때 특히 유용합니다. 시스템은 클라이언트와 서버 간의 연결이 완전히 설정되기 전에는 애플리케이션 또는 필터 URL을 확인할 수 없기 때문입니다. 예를 들어, 어떤 패킷이 애플리케이션 또는 URL 조건이 포함된 액세스 제어 규칙의 다른 모든 조건과 매칭될 경우, 해당 패킷과 후속 패킷은 연결이 설정되고 애플리케이션 또는 URL 확인이 완료될 때까지 통과될 수 있으며 일반적으로 3~5개의 패킷이 허용됩니다.

시스템에서는 기본 침입 정책으로 이러한 허용된 패킷을 검사합니다. 해당 정책은 이벤트를 생성할 수 있으며, 인라인으로 배치된 경우 악성 트래픽을 차단할 수 있습니다. 시스템이 액세스 제어 규칙 또는 연결을 처리해야 하는 기본 작업을 확인하면, 연결의 나머지 패킷이 처리되고 그에 따라 검사됩니다.

액세스 제어 정책을 생성할 경우, 기본 침입 정책은 **처음** 선택한 기본 작업에 따라 달라집니다. 액세스 제어를 위한 최초 기본 침입 정책은 다음과 같습니다.

- Balanced Security and Connectivity(시스템에서 제공된 정책)는 **Intrusion Prevention** 기본 작업을 처음 선택한 액세스 제어 정책의 기본 침입 정책입니다.
- No Rules Active는 **Block all traffic** 또는 **Network Discovery** 기본 작업을 처음 선택한 액세스 제어 정책의 기본 침입 정책입니다. 이 옵션을 선택하면 위에 설명한 허용된 패킷에 대한 침입 검사가 비활성화되긴 하지만, 침입 데이터를 크게 중요시하지 않는 경우에는 성능을 향상할 수 있습니다.

참고 침입 검사를 수행하지 않을 경우(예: 보호에 대한 라이센스가 없는 검색 전용 구축의 경우), No Rules Active 정책을 기본 침입 정책으로 유지하십시오. 자세한 내용은 12-19페이지의 IPS 또는 검색 전용 성능 고려 사항을/를 참조하십시오.

액세스 제어 정책을 생성한 후 기본 작업을 변경할 경우, 기본 침입 정책은 자동으로 변경되지 **않습니다**. 이를 수동으로 변경하려면 액세스 제어 정책의 고급 옵션을 사용하십시오.

액세스 제어 정책의 기본 침입 정책을 변경하려면

액세스: Admin/Access Admin/Network Admin

1단계 기본 침입 정책을 변경할 액세스 제어 정책에서, **Advanced** 탭을 선택한 다음 Network Analysis and Intrusion Policies 섹션 옆의 수정 아이콘()을 클릭합니다.

Network and Analysis Policies 대화 상자가 나타납니다.

2단계 **Intrusion Policy used before Access Control rule is determined** 드롭다운 목록에서 기본 침입 정책을 선택합니다. 시스템에서 생성된 정책 또는 사용자가 생성한 정책을 선택할 수 있습니다.

사용자가 생성한 정책을 선택할 경우, 수정 아이콘()을 클릭하여 새 창에서 정책을 수정할 수 있습니다. 시스템에서 제공된 정책은 수정할 수 없습니다.

주의 Cisco 담당자의 지침이 없는 한 `Experimental Policy 1`을 사용하지 **마십시오**. Cisco에서는 테스트 목적으로 이 정책을 사용합니다.

3단계 **OK**를 클릭하여 변경 사항을 저장합니다.

변경 사항을 구현하려면 액세스 제어 정책을 적용해야 합니다.

네트워크 분석 정책으로 전처리 맞춤화

라이센스: 모든

지원되는 디바이스: 기능에 따라 다름

*네트워크 분석 정책*은 트래픽의 디코딩 및 전처리 방법을 제어하여 트래픽을 추가적으로 평가할 수 있도록 하며, 특히 침입 시도를 알리는 신호일 수 있는 비정상적인 트래픽이 그 대상입니다. 이러한 트래픽 전처리는 보안 인텔리전스의 블랙리스트 추가 및 트래픽 해독이 수행된 후에 발생하되, 침입 정책이 패킷을 세부적으로 검사하기 전에 이루어집니다. 기본적으로, 시스템에서 제공된 Balanced Security and Connectivity 네트워크 분석 정책은 액세스 제어 정책에 의해 처리되는 *모든* 트래픽에 적용됩니다.

팁 시스템에서 제공된 Balanced Security and Connectivity 네트워크 분석 정책 및 Balanced Security and Connectivity 침입 정책은 함께 사용되며 침입 규칙 업데이트 시 함께 업데이트할 수 있습니다. 그러나 네트워크 분석 정책은 주로 전처리 옵션을 제어하는 반면, 침입 정책은 주로 침입 규칙을 제어합니다.

전처리를 조정하는 간단한 방법은 사용자 지정 네트워크 분석 정책을 생성하여 기본값으로 사용하는 것입니다. 26-2페이지의 사용자 지정 네트워크 분석 정책 생성을/를 참조하십시오. 사용 가능한 조정 옵션은 프리프로세서에 따라 다릅니다.

복잡한 구축 환경을 갖춘 고급 사용자를 위해, 여러 개의 네트워크 분석 정책을 생성할 수 있으며 각 정책은 트래픽을 각기 다른 방식으로 전처리하도록 맞춤화됩니다. 그런 다음 이러한 정책을 사용하도록 시스템을 구성하여 서로 다른 보안 영역, 네트워크 또는 VLAN을 사용하는 트래픽의 전처리를 제어할 수 있습니다. (ASA FirePOWER 디바이스는 VLAN을 통한 전처리를 제한할 수 없습니다.)

이를 구현하려면 사용자 지정 *네트워크 분석 규칙*을 액세스 제어 정책에 추가합니다. 각 규칙에는 다음이 포함됩니다.

- 전처리할 특정 트래픽을 확인하는 규칙 조건 집합
- 모든 규칙의 조건을 충족하는 트래픽을 전처리하는 데 사용할 관련 네트워크 분석 정책

시스템에서 트래픽을 전처리할 경우, 규칙 번호에 따라 위에서부터 아래 순서로 패킷을 네트워크 분석 규칙과 매칭합니다. 네트워크 분석 규칙과 매칭되지 않는 트래픽은 기본 네트워크 분석 정책에 의해 전처리됩니다.

참고 프리프로세서를 비활성화하되 전처리된 패킷을 활성화된 침입 또는 프리프로세서 규칙에 따라 평가해야 할 경우, 네트워크 분석 정책 웹 인터페이스에서는 프리프로세서가 비활성화된 상태로 유지되지만 시스템은 프리프로세서를 자동으로 활성화하고 사용합니다. 전처리를 맞춤화하는 작업 중에서도 특히 여러 개의 사용자 지정 네트워크 분석 정책을 사용하는 것은 **고급** 작업입니다. 전처리와 침입 검사는 밀접하게 연관되어 있으므로, 네트워크 분석 및 침입 정책이 단일한 패킷을 검사하여 서로 보완하도록 허용할 경우 **반드시** 주의를 기울여야 합니다. 자세한 내용은 23-12페이지의 사용자 지정 정책의 제한 사항을/를 참조하십시오.

자세한 내용은 다음 절을 참조하십시오.

- 25-4페이지의 액세스 제어에 대한 기본 네트워크 분석 정책 설정
- 25-4페이지의 네트워크 분석 규칙을 사용하여 전처리할 트래픽 지정
- 25-9페이지의 네트워크 분석 규칙 관리

액세스 제어에 대한 기본 네트워크 분석 정책 설정

라이센스: 모든

기본적으로, 시스템에서 제공된 Balanced Security and Connectivity 네트워크 분석 정책은 액세스 제어 정책에 의해 처리되는 모든 트래픽에 적용됩니다. 네트워크 분석 규칙을 트래픽 전처리 옵션에 추가할 경우, 기본 네트워크 분석 정책은 해당 규칙에서 처리되지 않는 모든 트래픽을 전처리합니다.

액세스 제어 정책의 고급 설정을 사용하면 이러한 기본 정책을 변경할 수 있습니다.

액세스 제어 정책의 기본 네트워크 분석 정책을 변경하려면

액세스: Admin/Access Admin/Network Admin

1단계 기본 네트워크 분석 정책을 변경할 액세스 제어 정책에서, **Advanced** 탭을 선택한 다음 Network Analysis and Intrusion Policies 섹션 옆의 수정 아이콘()을 클릭합니다.

Network and Analysis Policies 대화 상자가 나타납니다.

2단계 **Default Network Analysis Policy** 드롭다운 목록에서 기본 네트워크 분석 정책을 선택합니다. 시스템에서 생성된 정책 또는 사용자가 생성한 정책을 선택할 수 있습니다.

사용자가 생성한 정책을 선택할 경우, 수정 아이콘()을 클릭하여 새 창에서 정책을 수정할 수 있습니다. 시스템에서 제공된 정책은 수정할 수 없습니다.

주의 Cisco 담당자의 지침이 없는 한 `Experimental Policy 1`을 사용하지 **마십시오**. Cisco에서는 테스트 목적으로 이 정책을 사용합니다.

3단계 **OK**를 클릭하여 변경 사항을 저장합니다.

변경 사항을 구현하려면 액세스 제어 정책을 적용해야 합니다.

네트워크 분석 규칙을 사용하여 전처리할 트래픽 지정

라이센스: 모든

지원되는 디바이스: 기능에 따라 다름

액세스 제어 정책의 고급 설정에서, 네트워크 분석 규칙을 사용하여 네트워크 트래픽에 대한 전처리 컨피그레이션을 맞춤화할 수 있습니다. 액세스 제어 규칙과 마찬가지로, 네트워크 분석 규칙도 1번을 시작으로 번호가 지정됩니다.

시스템에서 트래픽을 전처리할 경우, 오름차순 규칙 번호에 따라 위에서부터 아래 순서로 패킷을 네트워크 분석 규칙과 매칭하며, 모든 규칙의 조건이 매칭되는 첫 번째 규칙에 따라 트래픽을 전처리합니다. 규칙에 추가할 수 있는 조건은 아래 표에 설명되어 있습니다.

표 25-1 네트워크 분석 규칙 조건 유형

조건	트래픽 매칭	세부 사항
영역	특정 보안 영역에서 인터페이스를 통해 디바이스로 들어가거나 디바이스에서 나옴	보안 영역은 구축 및 보안 정책에 따라 하나 이상의 인터페이스를 논리적으로 그룹화한 것입니다. 한 영역의 인터페이스는 여러 디바이스에 걸쳐 있을 수 있습니다. 영역 조건을 작성하려면 25-6페이지의 영역당 트래픽 전처리을/를 참조하십시오.

표 25-1 네트워크 분석 규칙 조건 유형(계속)

조건	트래픽 매칭	세부 사항
네트워크	소스 또는 목적지 IP 주소, 국가 또는 대륙별	IP 주소를 명시적으로 지정할 수 있습니다. 네트워크 조건을 작성하려면 25-7페이지의 네트워크당 트래픽 전처리을/를 참조하십시오.
VLAN 태그	VLAN별로 태그됨	시스템에서는 가장 안쪽의 VLAN 태그를 사용하여 VLAN을 기준으로 패킷을 확인합니다. (ASA FirePOWER는 VLAN을 통한 전처리를 제한할 수 없습니다.) VLAN 조건을 작성하려면 25-8페이지의 VLAN당 트래픽 전처리을/를 참조하십시오.

규칙에 대해 특별한 조건을 구성하지 않으면 시스템에서는 해당 기준을 기반으로 트래픽의 일치를 확인하지 않습니다. 예를 들어, 네트워크 조건은 있지만 영역 조건이 없는 규칙의 경우 인그레스 또는 이그레스 인터페이스에 상관없이 소스 또는 대상 IP 주소에 따라 트래픽을 평가합니다. 네트워크 분석 규칙과 매칭되지 않는 트래픽은 기본 네트워크 분석 정책에 의해 전처리됩니다.

사용자 지정 네트워크 분석 규칙을 추가하려면

액세스: Admin/Access Admin/Network Admin

1단계 사용자 지정 전처리 컨피그레이션을 생성할 액세스 제어 정책에서, **Advanced** 탭을 선택한 다음 Intrusion and Network Analysis Policies 섹션 옆의 수정 아이콘( )을 클릭합니다.

Network and Analysis Policies 대화 상자가 나타납니다. 사용자 지정 네트워크 분석 규칙을 추가하지 않은 경우, 웹 인터페이스에서는 **No Custom Rules**가 있음을 나타내며 그렇지 않을 경우 구성된 개수가 표시됩니다.

팁 새 창에서 Network Analysis Policy 페이지를 표시하려면 **Network Analysis Policy List**를 클릭합니다. 이 페이지를 사용하여 사용자 지정 네트워크 분석 정책을 보고 수정합니다(26-3페이지의 네트워크 분석 정책 관리 참조).

2단계 **Network Analysis Rules** 옆에 있는 사용자 지정 규칙의 개수를 나타내는 설명을 클릭합니다.

사용자 지정 규칙이 있는 경우 대화 상자가 확장되어 표시됩니다.

3단계 **Add Rule**을 클릭합니다.

네트워크 분석 규칙 편집기가 나타납니다.

4단계 규칙의 조건을 작성합니다. 다음 조건을 사용하여 NAP 전처리를 제한할 수 있습니다.

- 25-6페이지의 영역당 트래픽 전처리
- 25-7페이지의 네트워크당 트래픽 전처리
- 25-8페이지의 VLAN당 트래픽 전처리

5단계 **Network Analysis** 탭을 클릭하고 **Network Analysis Policy** 드롭다운 목록에서 정책을 선택하여 네트워크 분석 정책과 규칙을 연결합니다.

시스템에서는 모든 규칙의 조건을 충족하는 트래픽을 전처리하기 위해 선택한 네트워크 분석 정책을 사용합니다. 사용자가 생성한 정책을 선택할 경우, 수정 아이콘( )을 클릭하여 새 창에서 정책을 수정할 수 있습니다. 시스템에서 제공된 정책은 수정할 수 없습니다.

주의 Cisco 담당자의 지침이 없는 한 `Experimental Policy 1`을 사용하지 **마십시오**. Cisco에서는 테스트 목적으로 이 정책을 사용합니다.

6단계 **Add**를 클릭합니다.

규칙은 다른 규칙 뒤에 추가됩니다. 규칙의 평가 순서를 변경하려면 25-9페이지의 네트워크 분석 규칙 관리을/를 참조하십시오.

영역당 트래픽 전처리

라이센스: 모든

네트워크 분석 규칙의 영역 조건을 사용하면 소스 및 대상 보안 영역으로 트래픽을 전처리할 수 있습니다. 보안 영역은 여러 디바이스 전반에 걸쳐 있을 수 있는 하나 이상의 인터페이스를 구축 및 보안 정책에 알맞은 방식으로 그룹화한 것입니다. 영역 생성에 대한 자세한 내용은 3-38페이지의 보안 영역 작업을/를 참조하십시오.

단일한 영역 조건의 각 **Source Zones** 및 **Destination Zones**에 최대 50개의 영역을 추가할 수 있습니다.

- 영역에 있는 인터페이스를 통해 디바이스에서 *나가는* 트래픽을 매칭하려면, 해당 영역을 **Destination Zones**에 추가합니다. 수동으로 구축된 디바이스는 트래픽을 전송할 수 없으므로, **Destination Zone** 조건에서는 패시브 인터페이스로 구성된 영역을 사용할 수 없습니다.
- 영역에 있는 인터페이스를 통해 디바이스로 *들어오는* 트래픽을 매칭하려면, 해당 영역을 **Source Zones**에 추가합니다.

소스 및 대상 영역 조건을 규칙에 모두 추가할 경우, 매칭되는 트래픽은 지정된 소스 영역 중 하나에서 시작되고 대상 영역 중 하나를 통해 나가야 합니다.

영역의 모든 인터페이스가 동일한 유형(전체 인라인, 전체 패시브, 전체 스위칭, 전체 라우팅)이어야 하듯이, 네트워크 분석 규칙의 영역 조건에 사용되는 모든 영역도 동일한 유형이어야 합니다. 즉, 서로 다른 유형의 영역으로 들어가거나 나가는 트래픽과 매칭되는 단일한 규칙은 쓸 수 없습니다.

경고 아이콘(⚠)은 인터페이스가 없는 영역 같은 잘못된 컨피그레이션을 나타냅니다. 자세한 내용을 보려면 마우스 포인터를 아이콘 위에 올려놓습니다.

영역으로 트래픽을 전처리하려면

액세스: Admin/Access Admin/Network Admin

1단계 영역으로 트래픽을 전처리하려는 액세스 제어 정책에서, 새로운 네트워크 분석 규칙을 생성하거나 기존 규칙을 수정합니다.

자세한 지침은 25-4페이지의 네트워크 분석 규칙을 사용하여 전처리할 트래픽 지정을/를 참조하십시오.

2단계 네트워크 분석 규칙 편집기에서 **Zones** 탭을 선택합니다.

Zones 탭이 나타납니다.

3단계 **Available Zones**에서 추가할 영역을 찾아 선택합니다.

추가할 영역을 검색하려면 **Available Zones** 목록 위의 **Search by name** 프롬프트를 클릭한 다음 영역 이름을 입력합니다. 입력을 수행하면 목록이 업데이트되어 매칭되는 영역을 표시합니다.

선택할 영역을 클릭합니다. 여러 영역을 선택하려면 **Shift** +**Ctrl** 키를 사용하거나, 마우스 오른쪽 버튼을 클릭한 다음 **Select All**을 선택합니다.

4단계 **Add to Source** 또는 **Add to Destination**을 클릭하여 선택한 영역을 해당 목록에 추가합니다.

선택한 영역을 끌어서 놓을 수도 있습니다.

5단계 규칙을 저장하거나 계속 수정합니다.

변경 사항을 적용하려면 액세스 제어 정책을 적용해야 합니다. 12-15페이지의 액세스 제어 정책 적용을/를 참조하십시오.

네트워크당 트래픽 전처리

라이센스: 모든

네트워크 분석 규칙의 네트워크 조건을 사용하면 소스 및 대상 IP 주소로 트래픽을 전처리할 수 있습니다. 전처리할 트래픽에 대한 소스 및 대상 IP 주소를 수동으로 지정하거나, 재사용 가능한 네트워크 객체로 네트워크 조건을 구성하고 이름을 하나 이상의 IP 주소 및 주소 블록과 연결할 수 있습니다.

팁 네트워크 객체를 생성한 후에는 이를 사용하여 네트워크 분석 규칙을 만들 수 있을 뿐만 아니라, 시스템의 웹 인터페이스의 여러 위치에 있는 IP 주소를 나타낼 수도 있습니다. 객체 관리자를 사용하여 이러한 객체를 생성할 수 있으며, 네트워크 분석 규칙을 구성하는 동안 네트워크 객체를 즉시 생성할 수도 있습니다. 자세한 내용은 3-4페이지의 네트워크 객체 작업을/를 참조하십시오.

단일한 네트워크 조건의 각 **Source Networks** 및 **Destination Networks**에 최대 50개의 항목을 추가할 수 있습니다.

- IP 주소에서 나가는 트래픽을 매칭하려면 **Source Networks**를 구성합니다.
- IP 주소로 들어오는 트래픽을 매칭하려면 **Destination Networks**를 구성합니다.

소스 및 대상 네트워크 조건을 규칙에 모두 추가할 경우, 매칭되는 트래픽은 지정된 IP 주소 중 하나에서 시작되고 대상 IP 주소 중 하나로 향해야 합니다.

네트워크 조건을 만들 경우, 경고 아이콘( )은 잘못된 컨피그레이션을 나타냅니다. 자세한 내용을 보려면 마우스 포인터를 아이콘 위에 올려놓습니다.

네트워크로 트래픽을 전처리하려면

액세스: Admin/Access Admin/Network Admin

1단계 네트워크로 트래픽을 전처리하려는 액세스 제어 정책에서, 새로운 네트워크 분석 규칙을 생성하거나 기존 규칙을 수정합니다.

자세한 지침은 25-4페이지의 네트워크 분석 규칙을 사용하여 전처리할 트래픽 지정을/를 참조하십시오.

2단계 네트워크 분석 규칙 편집기에서 **Networks** 탭을 선택합니다.

Networks 탭이 나타납니다.

3단계 **Available Networks**에서 추가할 네트워크를 다음과 같이 찾아 선택합니다.

- 네트워크 객체를 즉시 추가한 다음 조건에 추가하려면, **Available Networks** 목록 위의 추가 아이콘( )을 클릭합니다(3-4페이지의 네트워크 객체 작업 참조).
- 추가할 네트워크를 검색하려면 **Available Networks** 목록 위의 **Search by name or value** 프롬프트를 클릭한 다음 객체 이름 또는 객체의 구성 요소 중 하나의 값을 입력합니다. 입력을 수행하면 목록이 업데이트되어 매칭되는 객체를 표시합니다.

객체를 선택하려면 클릭합니다. 여러 객체를 선택하려면 Shift +Ctrl 키를 사용하거나, 마우스 오른쪽 버튼을 클릭한 다음 **Select All**을 선택합니다.

4단계 **Add to Source** 또는 **Add to Destination**을 클릭하여 선택한 객체를 해당 목록에 추가합니다.

선택한 객체를 끌어서 놓을 수도 있습니다.

5단계 수동으로 지정하려는 소스/대상 IP 주소 또는 주소 블록을 추가합니다.

Source Networks 또는 **Destination Networks** 목록 아래의 **Enter an IP address** 프롬프트를 클릭한 다음, IP 주소 또는 주소 블록을 입력하고 **Add**를 클릭합니다.

6단계 규칙을 저장하거나 계속 수정합니다.

변경 사항을 적용하려면 액세스 제어 정책을 적용해야 합니다. 12-15페이지의 액세스 제어 정책 적용을/를 참조하십시오.

VLAN당 트래픽 전처리

라이센스: 모든

지원되는 디바이스: ASA FirePOWER를 제외한 모두

네트워크 분석 규칙의 VLAN 조건을 사용하면 VLAN 태그 트래픽의 전처리 방식을 제어할 수 있습니다. 시스템에서는 가장 안쪽의 VLAN 태그를 사용하여 VLAN을 기준으로 패킷을 확인합니다. ASA FirePOWER 디바이스는 VLAN을 통한 전처리를 제한할 수 없습니다.

VLAN 기반 네트워크 분석 조건을 만들 경우, VLAN 태그를 수동으로 지정할 수 있습니다. 또는 재사용 가능한 VLAN 태그 객체로 VLAN 조건을 구성하고, 이름을 하나 이상의 VLAN 태그와 연결할 수 있습니다.

팁 VLAN 태그 객체를 생성한 후에는 이를 사용하여 네트워크 분석 규칙을 만들 수 있을 뿐만 아니라, 시스템의 웹 인터페이스의 여러 위치에 있는 VLAN 태그를 나타낼 수도 있습니다. 객체 관리자를 사용하여 VLAN 태그 객체를 생성하거나, 네트워크 분석 규칙을 구성하는 동안 즉시 생성할 수 있습니다. 자세한 내용은 3-13페이지의 VLAN 태그 객체 작업을/를 참조하십시오.

단일한 VLAN 태그 조건의 **Selected VLAN Tags**에 최대 50개의 항목을 추가할 수 있습니다. VLAN 태그 조건을 만들 경우, 경고 아이콘( )은 잘못된 컨피그레이션을 나타냅니다. 자세한 내용을 보려면 마우스 포인터를 아이콘 위에 올려놓습니다.

VLAN 태그로 트래픽을 전처리하려면

액세스: Admin/Access Admin/Network Admin

1단계 VLAN 태그로 트래픽을 전처리하려는 액세스 제어 정책에서, 새로운 네트워크 분석 규칙을 생성하거나 기존 규칙을 수정합니다.

자세한 지침은 25-4페이지의 네트워크 분석 규칙을 사용하여 전처리할 트래픽 지정을/를 참조하십시오.

2단계 네트워크 분석 규칙 편집기에서 **VLAN Tags** 탭을 선택합니다.

VLAN Tags 탭이 나타납니다.

3단계 **Available VLAN Tags**에서 추가할 VLAN을 다음과 같이 찾아 선택합니다.

- VLAN 태그 객체를 즉시 추가한 다음 조건에 추가하려면, Available VLAN Tags 목록 위의 추가 아이콘( )을 클릭합니다(3-13페이지의 VLAN 태그 객체 작업 참조).
- 추가할 VLAN 태그 객체 및 그룹을 검색하려면, **Available VLAN Tags** 목록 위의 **Search by name or value** 프롬프트를 클릭한 다음 객체의 이름을 입력하거나, 객체의 VLAN 태그의 값을 입력합니다. 입력을 수행하면 목록이 업데이트되어 매칭되는 객체를 표시합니다.
- 객체를 선택하려면 클릭합니다. 여러 객체를 선택하려면 Shift +Ctrl 키를 사용하거나, 마우스 오른쪽 버튼을 클릭한 다음 **Select All**을 선택합니다.

4단계 **Add to Rule**을 클릭하거나 선택한 객체를 끌어서 놓아 **Selected VLAN Tags** 목록에 추가합니다.

5단계 수동으로 지정할 VLAN 태그를 추가합니다.

Selected VLAN Tags 목록 아래의 **Enter a VLAN tag** 프롬프트를 클릭한 다음, VLAN 태그 또는 범위를 입력하고 **Add**를 클릭합니다. 1~4094 범위의 VLAN 태그를 지정할 수 있으며, 하이픈을 사용하여 VLAN 태그의 범위를 지정합니다.

6단계 규칙을 저장하거나 계속 수정합니다.

변경 사항을 구현하려면 액세스 제어 정책을 적용해야 합니다. 369페이지의 액세스 제어 정책 적용을/를 참조하십시오.

네트워크 분석 규칙 관리

라이센스: 모든

네트워크 분석 규칙은 해당 자격과 매칭되는 트래픽을 어떤 방식으로 전처리할지 지정하는 컨피그레이션 및 조건 집합입니다. 기존 액세스 제어 정책의 고급 옵션에서 네트워크 분석 규칙을 생성하고 수정합니다. 각 규칙은 하나의 정책에 속합니다.

사용자 지정 네트워크 분석 규칙을 수정하려면

액세스: Admin/Access Admin/Network Admin

1단계 사용자 지정 전처리 컨피그레이션을 변경할 액세스 제어 정책에서, **Advanced** 탭을 선택한 다음 Intrusion and Network Analysis Policies 섹션 옆의 수정 아이콘( )을 클릭합니다.

Network and Analysis Policies 대화 상자가 나타납니다. 사용자 지정 네트워크 분석 규칙을 추가하지 않은 경우, 웹 인터페이스에서는 **No Custom Rules**가 있음을 나타내며 그렇지 않을 경우 구성된 개수가 표시됩니다.

2단계 **Network Analysis Rules** 옆에 있는 사용자 지정 규칙의 개수를 나타내는 설명을 클릭합니다.

사용자 지정 규칙이 있는 경우 대화 상자가 확장되어 표시됩니다.

3단계 사용자 지정 규칙을 수정합니다. 다음 옵션을 이용할 수 있습니다.

- 규칙의 조건을 수정하거나 규칙에 의해 호출된 네트워크 분석 정책을 변경하려면, 규칙 옆의 수정 아이콘( )을 클릭합니다.
- 규칙의 평가 순서를 변경하려면 규칙을 클릭하고 올바른 위치로 끌어서 놓습니다. 여러 규칙을 선택하려면 Shift + Ctrl 키를 사용합니다.
- 규칙을 삭제하려면 규칙 옆의 삭제 아이콘( )을 클릭합니다.

팁 마우스 오른쪽 버튼으로 규칙을 클릭하면 새로운 네트워크 분석 규칙을 잘라내기, 복사, 붙여넣기, 수정, 추가할 수 있는 컨텍스트 메뉴가 표시됩니다.

4단계 **OK**를 클릭하여 변경 사항을 저장합니다.

변경 사항을 적용하려면 액세스 제어 정책을 적용해야 합니다. 12-15페이지의 액세스 제어 정책 적용을/를 참조하십시오.

26장 네트워크 분석 정책 시작하기

*네트워크 분석 정책*은 많은 트래픽 전처리 옵션을 관리하며, 액세스 제어 정책의 고급 설정에 의해 호출됩니다. 네트워크 분석 관련 전처리는 보안 인텔리전스 블랙리스트 추가 및 SSL 해독 후, 그리고 침입 또는 파일 검사 시작 전에 발생합니다.

기본적으로 시스템은 액세스 제어 정책에 의해 처리되는 모든 트래픽을 전처리하기 위해 *Balanced Security and Connectivity* 네트워크 분석 정책을 사용합니다. 그러나 이 전처리를 수행하려면 다른 기본 네트워크 분석 정책을 선택할 수 있습니다. 사용자 편의를 위해 시스템에서는 Cisco VRT(Vulnerability Research Team)에서 보안과 연결 간 균형을 위해 조정한, 수정할 수 없는 여러 네트워크 분석 정책 중에서 선택할 수 있는 기능을 제공합니다. 이 기본 정책을 사용자 지정 전처리 설정이 포함된 사용자 지정 네트워크 분석 정책으로 교체할 수도 있습니다.

팁 시스템 제공 침입 및 네트워크 분석 정책은 이름은 비슷하지만 컨피그레이션은 다릅니다. 예를 들어, Balanced Security and Connectivity 네트워크 분석 정책과 Balanced Security and Connectivity 침입 정책은 함께 작동하며 둘 다 침입 규칙 업데이트에서 업데이트할 수 있습니다. 그러나 네트워크 분석 정책은 주로 전처리 옵션을 제어하는 반면, 침입 정책은 주로 침입 규칙을 제어합니다. 23-1페이지의 네트워크 분석 및 침입 정책 이해에서는 네트워크 분석과 침입 정책이 트래픽 검토를 위해 함께 작동하는 방식의 개요는 물론 탐색 패널 사용, 충돌 해결, 변경 사항 커밋 등의 기본 사항에 대해서도 설명합니다.

여러 사용자 지정 네트워크 분석 정책을 생성하고 서로 다른 트래픽을 전처리하도록 할당하여 특정 보안 영역, 네트워크 및 VLAN에 대해 트래픽 전처리 옵션을 맞춤화할 수 있습니다. (ASA FirePOWER 디바이스는 VLAN을 통한 전처리를 제한할 수 없습니다.)

참고 전처리를 맞춤화하는 작업 중에서도 특히 여러 개의 사용자 지정 네트워크 분석 정책을 사용하는 것은 **고급** 작업입니다. 전처리 및 침입 검사는 밀접하게 관련되어 있으므로, 단일 패킷을 검토하는 네트워크 분석 및 침입 정책은 **반드시** 상호 보완 관계여야 합니다. 시스템에서 자동으로 정책을 조정하지는 **않습니다**. 자세한 내용은 23-12페이지의 사용자 지정 정책의 제한 사항을/를 참조하십시오.

이 장에서는 간단한 사용자 지정 네트워크 분석 정책을 생성하는 방법에 대해 설명합니다. 또한 네트워크 분석 정책 관리(수정, 비교 등)에 대한 기본적인 정보도 제공합니다. 자세한 내용은 다음 링크를 참고하십시오.

사용자 지정 네트워크 분석 정책 생성

라이센스: 보호

새 네트워크 분석 정책을 생성할 때에는 고유한 이름과 기반 정책을 지정하고 *인라인 모드*를 선택해야 합니다.

기반 정책은 네트워크 분석 정책의 기본 설정을 정의합니다. 새 정책에서 설정을 수정하면 기반 정책의 설정이 재정의됩니다(변경되지는 않음). 시스템 제공 정책 또는 사용자 지정 정책을 기반 정책으로 사용할 수 있습니다. 자세한 내용은 24-3페이지의 기반 레이어 이해을/를 참조하십시오.

네트워크 분석 정책의 인라인 모드에서는 공격자의 탐지 회피 가능성을 최소화하기 위해 프리프로세서가 트래픽을 수정(표준화) 및 삭제할 수 있습니다. 인라인 모드와 상관없이, 패시브 구축에서는 시스템이 트래픽 플로우에 영향을 줄 수 없습니다. 자세한 내용은 26-5페이지의 인라인 구축에서 프리프로세서가 트래픽에 영향을 미치도록 허용을/를 참조하십시오.

네트워크 분석 정책을 생성하려면

액세스: Admin/Intrusion Admin

1단계 **Policies > Access Control**을 선택하여 Access Control Policy 페이지를 표시한 다음 **Network Analysis Policy**를 클릭합니다.

Network Analysis Policy 페이지가 나타납니다.

FireSIGHT 시스템 사용자 계정 역할이 Intrusion Policy 또는 Modify Intrusion Policy로 제한된 경우 네트워크 정책과 침입 정책을 생성 및 수정할 수 있습니다. Network Analysis Policy 페이지에 액세스하려면 **Policies > Intrusion**을 선택하고 **Network Analysis Policy**를 클릭합니다. 자세한 내용은 61-51페이지의 사용자 지정 사용자 역할 관리을/를 참조하십시오.

2단계 **Create Policy**를 클릭합니다.

다른 정책에 저장하지 않은 변경 사항이 있는 경우 Network Analysis Policy 페이지로 돌아갈지 묻는 대화 상자가 나타나면 **Cancel**을 클릭합니다. 저장하지 않은 변경 사항을 다른 정책에 저장하는 방법에 대한 자세한 내용은 23-15페이지의 충돌 해결 및 정책 변경 사항 커밋을/를 참조하십시오.

Create Network Analysis Policy 팝업 창이 나타납니다.

3단계 정책에 고유한 **Name**을 지정하고 선택 사항인 **Description**도 입력합니다.

4단계 초기 **Base Policy**를 지정합니다.

시스템 제공 정책 또는 사용자 지정 정책을 기반 정책으로 사용할 수 있습니다.

주의 Cisco 담당자의 지침이 없는 한 `Experimental Policy 1`을 사용하지 **마십시오**. Cisco에서는 테스트 목적으로 이 정책을 사용합니다.

5단계 프리프로세서가 인라인 구축에서 트래픽에 영향을 미치도록 허용할지 여부를 지정합니다.

- 프리프로세서가 트래픽에 영향을 미치도록 허용하려면 **Inline Mode**를 활성화합니다.
- 프리프로세서가 트래픽에 영향을 미치지 못하도록 하려면 **Inline Mode**를 비활성화합니다.

6단계 정책을 생성합니다.

- 새 정책을 생성하고 Network Analysis Policy 페이지로 돌아가려면 **Create Policy**를 클릭합니다. 새 정책은 기반 정책과 설정이 동일합니다.
- 정책을 생성한 후 고급 네트워크 분석 정책 편집기에서 수정하기 위해 열려면 **Create and Edit Policy**를 클릭합니다. 26-4페이지의 네트워크 분석 정책 수정을/를 참조하십시오.

네트워크 분석 정책 관리

라이센스: 보호

Network Analysis Policy 페이지(**Policies > Access Control** 선택 후 **Network Analysis Policy** 클릭)에서 다음 정보와 함께 현재의 사용자 지정 네트워크 분석 정책을 볼 수 있습니다.

- 정책이 마지막으로 수정된 시간과 날짜(현지 시간) 및 수정한 사용자
- **Inline Mode** 설정의 활성화 여부(프리프로세서가 트래픽에 영향을 미치도록 허용)
- 트래픽 전처리를 위해 네트워크 분석 정책을 사용 중인 액세스 제어 정책 및 디바이스
- 정책에 저장되지 않은 변경 사항이 있는지, 현재 정책을 수정 중인 사용자(있는 경우)에 대한 정보가 있는지 여부

생성하는 사용자 지정 정책 외에도 시스템에서는 두 가지 사용자 지정 정책인 Initial Inline Policy 및 Initial Passive Policy를 제공합니다. 이 두 가지 네트워크 분석 정책은 Balanced Security and Connectivity 네트워크 분석 정책을 기반으로 사용합니다. 이 둘의 유일한 차이점은, 인라인 모드에서는 프리프로세서가 트래픽에 영향을 미치도록 허용하고 패시브 정책에서는 이를 비활성화한다는 점입니다. 이러한 시스템 제공 사용자 지정 정책을 수정 및 사용할 수 있습니다.

Network Analysis Policy 페이지의 옵션을 사용하면 다음 표의 작업을 수행할 수 있습니다.

표 26-1 네트워크 분석 정책 관리 작업

목적	가능한 작업	참조
새 네트워크 분석 정책 생성	**Create Policy**를 클릭합니다.	26-2페이지의 사용자 지정 네트워크 분석 정책 생성
기존의 네트워크 분석 정책 수정	수정 아이콘( )을 클릭합니다.	26-4페이지의 네트워크 분석 정책 수정
네트워크 분석 정책의 현재 컨피그레이션 설정을 나열하는 PDF 보고서 보기	보고서 아이콘( )을 클릭합니다.	26-9페이지의 현재 네트워크 분석 설정에 대한 보고서 생성
두 네트워크 분석 정책 또는 동일한 정책의 두 개정 설정 비교	**Compare Policies**를 클릭합니다.	26-9페이지의 두 가지 네트워크 분석 정책 또는 개정 비교
네트워크 분석 정책 삭제	삭제 아이콘( )을 클릭한 다음 정책을 삭제할 것임을 확인합니다. 액세스 제어 정책이 참조하는 네트워크 분석 정책은 삭제할 수 없습니다.	

FireSIGHT 시스템 사용자 계정 역할이 Intrusion Policy 또는 Modify Intrusion Policy로 제한된 경우 네트워크 정책과 침입 정책을 생성 및 수정할 수 있습니다. Network Analysis Policy 페이지에 액세스하려면 **Policies > Intrusion**을 선택하고 **Network Analysis Policy**를 클릭합니다. 자세한 내용은 61-51페이지의 사용자 지정 사용자 역할 관리을/를 참조하십시오.

네트워크 분석 정책 수정

라이센스: 보호

새 네트워크 분석 정책을 생성하면 생성된 정책은 기반 정책과 설정이 동일합니다. 다음 표에는 요구 사항에 새 정책을 맞춤화하기 위해 수행할 수 있는 가장 일반적인 작업이 나열되어 있습니다.

표 26-2 네트워크 분석 정책 수정 작업

목적	가능한 작업	참조
프리프로세서가 트래픽을 수정 또는 삭제하도록 허용	Policy Information 페이지에서 **Inline Mode** 확인란을 선택합니다.	26-5페이지의 인라인 구축에서 프리프로세서가 트래픽에 영향을 미치도록 허용
기반 정책 변경	Policy Information 페이지의 **Base Policy** 드롭다운 목록에서 기반 정책을 선택합니다.	24-4페이지의 기반 정책 변경
기반 정책의 설정 보기	Policy Information 페이지에서 **Manage Base Policy**를 클릭합니다.	24-3페이지의 기반 레이어 이해
프리프로세서에 대한 설정 활성화, 비활성화 또는 수정	탐색 패널에서 **Settings**를 클릭합니다.	26-6페이지의 네트워크 분석 정책에서 프리프로세서 구성
정책 레이어 관리	탐색 패널에서 **Policy Layers**를 클릭합니다.	24-1페이지의 네트워크 분석 또는 침입 정책에서 레이어 사용

네트워크 분석 정책을 맞춤화할 때, 특히 프리프로세서를 비활성화할 때, 일부 프리프로세서 및 침입 규칙에서는 특정 방법으로 트래픽을 먼저 디코딩하거나 전처리해야 한다는 점에 유의하십시오. 필수 프리프로세서를 비활성화하는 경우 네트워크 분석 정책 웹 인터페이스에서는 프리프로세서가 비활성 상태로 남아 있더라도, 시스템은 현재 설정을 이용해 프리프로세서를 자동으로 사용합니다.

참고 전처리 및 침입 검사는 밀접하게 관련되어 있으므로, 단일 패킷을 검토하는 네트워크 분석 및 침입 정책은 **반드시** 상호 보완 관계여야 합니다. 전처리를 맞춤화하는 작업 중에서도 특히 여러 개의 사용자 지정 네트워크 분석 정책을 사용하는 것은 **고급** 작업입니다. 자세한 내용은 23-12페이지의 사용자 지정 정책의 제한 사항을/를 참조하십시오.

시스템은 사용자당 하나의 네트워크 분석 정책을 캐시합니다. 네트워크 분석 정책을 수정하는 동안 메뉴를 선택하거나 다른 페이지에 대한 다른 경로를 선택하면, 페이지를 나가더라도 변경 사항이 시스템 캐시에 남아 있습니다. 위의 표에 있는 수행 가능한 작업 외에도 23-1페이지의 네트워크 분석 및 침입 정책 이해에서는 탐색 패널 사용, 충돌 해결, 변경 사항 커밋 등에 대한 정보를 제공합니다.

네트워크 분석 정책을 수정하려면

액세스: Admin/Intrusion Admin

1단계 **Policies > Access Control**을 선택하여 Access Control Policy 페이지를 표시한 다음 **Network Analysis Policy**를 클릭합니다.

Network Analysis Policy 페이지가 나타납니다.

2단계 구성할 네트워크 분석 정책 옆에 있는 수정 아이콘( )을 클릭합니다.

네트워크 분석 정책 편집기가 나타나며, Policy Information 페이지에 초점이 맞춰지고 탐색 패널이 왼쪽에 표시됩니다.

3단계 정책을 수정합니다. 위에 요약된 작업 중 하나를 수행합니다.

4단계 정책을 저장하거나, 계속 수정하거나, 변경 사항을 취소하거나, 시스템 캐시에 변경 사항이 남아 있는 상태로 종료합니다. 자세한 내용은 23-15페이지의 충돌 해결 및 정책 변경 사항 커밋을/를 참조하십시오.

인라인 구축에서 프리프로세서가 트래픽에 영향을 미치도록 허용

라이센스: 보호

인라인 구축에서 일부 프리프로세서는 트래픽을 수정 및 차단할 수 있습니다. 예를 들면 다음과 같습니다.

- 인라인 표준화 프리프로세서는 다른 프리프로세서 및 침입 규칙 엔진에서 분석할 수 있도록 패킷을 표준화합니다. 또한 특정 패킷을 차단하려면 프리프로세서의 **Allow These TCP Options** 및 **Block Unrecoverable TCP Header Anomalies** 옵션을 사용할 수 있습니다. 자세한 내용은 29-7페이지의 인라인 트래픽 표준화을/를 참조하십시오.
- 시스템은 잘못된 체크섬이 있는 패킷을 삭제할 수 있습니다. 29-5페이지의 체크섬 확인을/를 참조하십시오.
- 시스템은 속도 기반 공격 방지 설정과 일치하는 패킷을 삭제할 수 있습니다. 34-9페이지의 속도 기반 공격 방지을/를 참조하십시오.

트래픽에 영향을 미치도록 네트워크 분석 정책에서 구성한 프리프로세서의 경우 프리프로세서를 활성화하고 올바르게 구성하는 것은 물론, 관리되는 디바이스를 인라인으로(즉, 인라인 인터페이스 설정으로) 올바르게 구축해야 합니다. 마지막으로, 네트워크 분석 정책의 **Inline Mode** 설정을 활성화해야 합니다.

트래픽을 실제로 수정하지 않은 채 인라인 구축에서 컨피그레이션이 어떻게 작동하는지를 평가하려면 인라인 모드를 비활성화할 수 있습니다. 인라인 모드와 상관없이, 패시브 구축 또는 탭 모드의 인라인 구축에서는 시스템이 트래픽에 영향을 줄 수 없습니다.

인라인 모드를 비활성화하면 침입 이벤트 성능 통계 그래프에 영향을 줄 수 있습니다. 인라인 구축에서 인라인 모드가 활성화된 경우 Intrusion Event Performance 페이지(**Overview > Summary > Intrusion Event Performance**)에는 표준화 및 차단된 패킷을 나타내는 그래프가 표시됩니다. 인라인 모드를 비활성화하면(즉, 패시브 구축에서는), 시스템이 표준화 또는 삭제했을 트래픽에 대한 데이터가 다수의 그래프에 표시됩니다. 자세한 내용은 41-5페이지의 침입 이벤트 성능 통계 그래프 생성을/를 참조하십시오.

팁 인라인 구축의 경우 Cisco는 인라인 모드를 활성화하고 **Normalize TCP Payload** 옵션을 활성화하여 인라인 표준화 프리프로세서를 구성할 것을 권장합니다. 패시브 구축의 경우 Cisco는 적응형 프로필을 구성할 것을 권장합니다.

프리프로세서가 인라인 구축에서 트래픽에 영향을 미치도록 허용하려면

액세스: Admin/Intrusion Admin

1단계 **Policies > Access Control**을 선택하여 Access Control Policy 페이지를 표시한 다음 **Network Analysis Policy**를 클릭합니다.

Network Analysis Policy 페이지가 나타납니다.

2단계 수정할 정책 옆에 있는 수정 아이콘( )을 클릭합니다.

Policy Information 페이지가 나타납니다.

3단계 프리프로세서가 트래픽에 영향을 미치도록 허용할지 여부를 지정합니다.

- 프리프로세서가 트래픽에 영향을 미치도록 허용하려면 **Inline Mode**를 활성화합니다.
- 프리프로세서가 트래픽에 영향을 미치지 못하도록 하려면 **Inline Mode**를 비활성화합니다.

4단계 정책을 저장하거나, 계속 수정하거나, 변경 사항을 취소하거나, 시스템 캐시에 변경 사항이 남아 있는 상태로 종료합니다. 자세한 내용은 23-15페이지의 충돌 해결 및 정책 변경 사항 커밋을/를 참조하십시오.

네트워크 분석 정책에서 프리프로세서 구성

라이센스: 보호

*프리프로세서*는 트래픽 표준화 및 프로토콜 변칙 식별을 통해 추가로 트래픽을 검사할 수 있도록 준비합니다. 프리프로세서는 패킷이 사용자가 구성한 프리프로세서 옵션을 트리거할 때 프리프로세서 이벤트를 생성할 수 있습니다(41-39페이지의 프리프로세서 이벤트 읽기 참조). 네트워크 분석 정책의 기반 정책은 기본적으로 활성화되는 프리프로세서 및 각각에 대한 기본 컨피그레이션을 결정합니다.

네트워크 분석 정책의 탐색 패널에서 **Settings**를 선택하면 유형별 프리프로세서가 정책에 나열됩니다. Settings 페이지에서는 네트워크 분석 정책의 프리프로세서를 활성화 또는 비활성화할 수 있으며 프리프로세서 컨피그레이션 페이지에 액세스할 수 있습니다.

프리프로세서를 구성하려면 먼저 활성화해야 합니다. 프리프로세서를 활성화하면, 탐색 패널에서 프리프로세서에 대한 컨피그레이션 페이지의 하위 링크가 **Settings** 링크 아래에 나타납니다. 또한 컨피그레이션 페이지에 대한 **Edit** 링크가 Settings 페이지의 프리프로세서 옆에 나타납니다.

팁 프리프로세서의 컨피그레이션을 기반 정책의 설정으로 되돌리려면 프리프로세서 컨피그레이션 페이지에서 **Revert to Defaults**를 클릭합니다. 확인 메시지가 표시되면 설정을 되돌릴 것임을 확인합니다.

프리프로세서를 비활성화하면 하위 링크와 **Edit** 링크가 더 이상 나타나지 않지만 컨피그레이션은 그대로 유지됩니다. 특별 분석을 수행하려는 경우 다수의 프리프로세서 및 침입 규칙에서는 트래픽을 특정 방법으로 디코딩 또는 전처리하도록 요구합니다. 필수 프리프로세서를 비활성화하는 경우 네트워크 분석 정책 웹 인터페이스에서는 프리프로세서가 비활성 상태로 남아 있더라도, 시스템은 현재 설정을 이용해 프리프로세서를 자동으로 사용합니다.

참고 대부분의 경우 프리프로세서는 구성을 위한 특정 전문성을 요구하며, 일반적으로 수정은 거의 또는 전혀 요구하지 않습니다. 전처리를 맞춤화하는 작업 중에서도 특히 여러 개의 사용자 지정 네트워크 분석 정책을 사용하는 것은 **고급** 작업입니다. 전처리 및 침입 검사는 밀접하게 관련되어 있으므로, 단일 패킷을 검토하는 네트워크 분석 및 침입 정책은 **반드시** 상호 보완 관계여야 합니다. 자세한 내용은 23-12페이지의 사용자 지정 정책의 제한 사항을/를 참조하십시오.

프리프로세서 컨피그레이션을 수정하려면 컨피그레이션 및 네트워크에서 잠재적 영향력을 이해해야 합니다. 다음 절에서는 각 프리프로세서의 특정 컨피그레이션 세부사항에 대한 링크를 제공합니다.

Application Layer Preprocessors

애플리케이션 레이어 프로토콜 디코더는 특정 패킷 데이터 유형을 침입 규칙 엔진이 분석할 수 있는 형식으로 표준화합니다.

표 26-3 애플리케이션 레이어 프리프로세서 설정

다음에 대한 정보	참조
DCE/RPC 컨피그레이션	27-2페이지의 DCE/RPC 트래픽 디코딩
DNS 컨피그레이션	27-14페이지의 DNS 이름 서버 응답에서 익스플로잇 탐지
FTP 및 텔넷 컨피그레이션	27-18페이지의 FTP 및 텔넷 트래픽 디코딩
HTTP 컨피그레이션	27-30페이지의 HTTP 트래픽 디코딩
Sun RPC 컨피그레이션	27-45페이지의 Sun RPC 프리프로세서 사용
SIP 컨피그레이션	27-46페이지의 SIP(Session Initiation Protocol) 디코딩
GTP 명령 채널 컨피그레이션	27-51페이지의 GTP 명령 채널 구성
IMAP 컨피그레이션	27-52페이지의 IMAP 트래픽 디코딩
POP 컨피그레이션	27-55페이지의 POP 트래픽 디코딩
SMTP 컨피그레이션	27-58페이지의 SMTP 트래픽 디코딩
SSH 컨피그레이션	27-66페이지의 SSH 프리프로세서를 사용하여 익스플로잇 탐지
SSL 컨피그레이션	27-70페이지의 SSL 프리프로세서 사용

SCADA Preprocessors

Modbus 및 DNP3 프리프로세서는 트래픽 변칙을 탐지하고 침입에 대한 침입 규칙 엔진에 데이터를 제공합니다.

표 26-4 SCADA 프리프로세서 설정

다음에 대한 정보	참조
Modbus 컨피그레이션	28-1페이지의 Modbus 프리프로세서 구성
DNP3 컨피그레이션	28-3페이지의 DNP3 프리프로세서 구성

Transport/Network Layer Preprocessors

네트워크 및 전송 레이어 프리프로세서는 네트워크 및 전송 레이어에서 익스플로잇을 탐지합니다. 패킷이 프리프로세서로 전송되기 전, 패킷 디코더는 프리프로세서 및 침입 규칙 엔진이 쉽게 사용할 수 있는 형식으로 패킷 헤더 및 페이로드를 변환하고 패킷 헤더에서 비정상적인 각종 동작을 탐지합니다.

표 26-5 전송 및 네트워크 레이어 프리프로세서 설정

다음에 대한 정보	참조
체크섬 확인	29-5페이지의 체크섬 확인
인라인 표준화	29-7페이지의 인라인 트래픽 표준화
IP 디프래그먼트화	29-12페이지의 IP 패킷 디프래그먼트
패킷 디코딩	29-17페이지의 패킷 디코딩 이해
TCP 스트림 컨피그레이션	29-21페이지의 TCP 스트림 전처리 사용
UDP 스트림 컨피그레이션	29-32페이지의 UDP 스트림 전처리 사용

일부 고급 전송 및 네트워크 프리프로세서 설정은 액세스 제어 정책을 적용하는 모든 네트워크, 영역 및 VLAN에 전역적으로 적용됩니다. 이러한 고급 설정은 네트워크 분석 정책보다는 액세스 제어 정책에서 구성합니다. 29-2페이지의 고급 Transport/Network 설정 구성을/를 참조하십시오.

Specific Threat Detection

Back Orifice 프리프로세서는 UDP 트래픽에서 Back Orifice magic cookie를 분석합니다. 스캔 활동을 보고하도록 포트스캔 탐지기를 구성할 수 있습니다. 속도 기반 공격 방지는 네트워크를 마비시키도록 설계된 굉장히 많은 수의 동시 연결 및 SYN 플러드로부터 네트워크를 보호하는 데 도움이 될 수 있습니다.

표 26-6 Specific Threat Detection 설정

다음에 대한 정보	참조
Back Orifice Detection	34-1페이지의 Back Orifice 탐지
Portscan Detection	34-3페이지의 포트스캔 탐지
Rate-Based Attack Prevention	34-9페이지의 속도 기반 공격 방지

침입 정책에서 ASCII 텍스트의 신용카드 번호 및 주민등록번호 같은 민감한 데이터를 탐지하는 민감한 데이터 프리프로세서를 구성할 수 있습니다. 자세한 내용은 34-18페이지의 민감한 데이터 탐지을/를 참조하십시오.

현재 네트워크 분석 설정에 대한 보고서 생성

라이센스: 보호

네트워크 분석 정책 보고서는 특정 시점의 정책 컨피그레이션에 대한 기록입니다. 시스템은 기반 정책의 설정을 정책 레이어의 설정과 결합하고, 기반 정책에서 시작된 설정과 정책 레이어에서 시작된 설정을 구분하지 않습니다.

감사의 목적으로 또는 현재 컨피그레이션을 검사하는 데 다음 정보를 포함하는 이 보고서를 사용할 수 있습니다.

표 26-7 네트워크 분석 정책 보고서 섹션

섹션	설명
Policy Information	정책의 이름과 설명, 마지막으로 정책을 수정한 사용자의 이름, 정책이 마지막으로 수정된 날짜와 시간을 제공합니다. 또한 인라인 표준화의 활성화 가능 여부, 현재 규칙 업데이트 버전, 기반 정책이 현재 규칙 업데이트로 잠겼는지 여부도 나타납니다.
Settings	활성화된 모든 프리프로세서 설정 및 해당 컨피그레이션을 나열합니다.

두 가지 네트워크 분석 정책 또는 동일한 정책의 두 개정을 비교하는 비교 보고서를 생성할 수도 있습니다. 자세한 내용은 26-9페이지의 두 가지 네트워크 분석 정책 또는 개정 비교을/를 참조하십시오.

네트워크 분석 정책 보고서를 보려면

액세스: Admin/Intrusion Admin

1단계 **Policies > Access Control**을 선택하여 Access Control Policy 페이지를 표시한 다음 **Network Analysis Policy**를 클릭합니다.

Network Analysis Policy 페이지가 나타납니다.

2단계 보고서를 생성할 정책 옆의 보고서 아이콘( )을 클릭합니다. 네트워크 분석 정책 보고서를 생성하기 전에 모든 변경 사항을 커밋해야 합니다. 커밋된 변경 사항만 보고서에 나타납니다.

시스템에서 보고서를 생성합니다. 브라우저 설정에 따라 보고서가 팝업 창에 나타날 수 있으며, 컴퓨터에 보고서를 저장하는 프롬프트가 표시될 수도 있습니다.

두 가지 네트워크 분석 정책 또는 개정 비교

라이센스: 보호

조직의 표준을 준수하거나 시스템 성능을 최적화하기 위해 정책 변경 사항을 검토할 경우 두 네트워크 분석 정책 간의 차이를 확인할 수 있습니다. 두 네트워크 분석 정책 또는 동일한 네트워크 분석 정책의 두 개정을 비교할 수 있습니다. 선택적으로, 비교 후 두 정책 또는 정책 개정의 차이를 기록하는 PDF 보고서를 생성할 수도 있습니다.

네트워크 분석 정책 또는 정책 개정의 비교에 사용할 수 있는 두 가지 툴이 있습니다.

- 비교 보기에는 두 네트워크 분석 정책 또는 네트워크 분석 정책 개정 간의 차이점만 나란히 표시됩니다. 각 정책 또는 정책 개정의 이름은 비교 보기 왼쪽과 오른쪽의 제목 표시줄에 나타납니다.

이를 사용하여 웹 인터페이스에서 차이점이 강조 표시된 상태로 두 정책 개정을 모두 보고 탐색할 수 있습니다.

- 비교 보고서는 두 네트워크 분석 정책 또는 네트워크 분석 정책 개정의 차이점에 대해서만 기록을 생성하는데, 그 형식은 네트워크 분석 정책 보고서와 비슷하지만 PDF 형식입니다.

  이를 사용하여 향후 점검을 위해 정책 비교를 저장, 복사, 인쇄, 공유할 수 있습니다.

정책 비교 툴을 이해하고 사용하는 것에 대한 자세한 내용은 다음을 참조하십시오.

- 26-10페이지의 네트워크 분석 정책 비교 보기 사용
- 26-11페이지의 네트워크 분석 정책 비교 보고서 사용

네트워크 분석 정책 비교 보기 사용

라이센스: 보호

비교 보기에서는 두 정책 또는 정책 개정을 나란히 표시하며, 각 정책 또는 정책 개정은 비교 보기의 좌우 제목 표시줄에 있는 이름으로 식별됩니다. 마지막 수정 시간 및 마지막 수정자가 정책 이름과 함께 표시됩니다.

두 정책 간의 차이점이 강조 표시됩니다.

- 파란색은 강조 표시된 설정이 두 정책에서 다름을 의미하며, 그 차이점이 빨간색 텍스트로 표시됩니다.
- 녹색은 강조 표시된 설정이 둘 중 한 정책에만 나타남을 의미합니다.

다음 표의 작업을 수행할 수 있습니다.

표 26-8 네트워크 분석 정책 비교 보기 작업

목적	가능한 작업
개별 변경 사항 탐색	제목 표시줄 위의 **Previous** 또는 **Next**를 클릭합니다. 왼쪽과 오른쪽 사이의 중앙에 있는 이중 화살표 아이콘()이 움직이고, 어떤 차이점을 보고 있는지 식별할 수 있도록 **Difference** 번호가 조정됩니다.
특정 프리프로세서에 대한 컨피그레이션이 포함된 레이어 확인	보려는 컨피그레이션 옆에 있는 고급 컨피그레이션 아이콘() 위로 포인터를 가져갑니다. 창에는 프리프로세서 컨피그레이션을 포함하는 레이어의 이름이 표시됩니다.
새 정책 비교 보기 생성	**New Comparison**을 클릭합니다. **Select Comparison** 창이 나타납니다. 자세한 내용은 26-11페이지의 네트워크 분석 정책 비교 보고서 사용을/를 참조하십시오.
정책 비교 보고서 생성	**Comparison Report**를 클릭합니다. 정책 비교 보고서에서는 두 정책 또는 정책 개정의 차이점만 나열하는 PDF 문서를 생성합니다.

네트워크 분석 정책 비교 보고서 사용

라이센스: 보호

네트워크 분석 정책 비교 보고서는 두 네트워크 분석 정책 또는 동일한 네트워크 분석 정책의 두 개정 간 모든 차이점을 PDF에서 네트워크 분석 정책 비교 보기 형태로 기록한 것입니다. 두 네트워크 분석 정책 컨피그레이션의 차이점을 더 자세히 살펴보고 조사 결과를 저장하여 배포하는 데 이 보고서를 사용할 수 있습니다.

액세스 권한이 있는 모든 네트워크 분석 정책에 대해 비교 보기에서 정책 비교 보고서를 생성할 수 있습니다. 정책 보고서를 생성하기 전에 모든 변경 사항을 저장해야 합니다. 저장된 변경 사항만 보고서에 나타납니다.

정책 비교 보고서의 형식은 한 가지 점만 제외하면 정책 보고서와 동일합니다. 정책 보고서에는 정책의 모든 컨피그레이션이 포함되지만, 정책 비교 보고서에는 정책 간에 서로 다른 컨피그레이션만 나열됩니다. 네트워크 분석 정책 비교 보고서는 26-9 페이지의 표 26-7에 설명된 섹션으로 구성됩니다.

팁 SSL, 액세스 제어, 침입, 파일, 시스템 또는 상태 정책을 비교하는 데에도 비슷한 절차를 사용할 수 있습니다.

두 개의 네트워크 분석 정책 또는 정책 개정을 비교하려면

액세스: Admin/Intrusion Admin

1단계 **Policies > Access Control**을 선택하여 Access Control Policy 페이지를 표시한 다음 **Network Analysis Policy**를 클릭합니다.

Network Analysis Policy 페이지가 나타납니다.

2단계 **Compare Policies**를 클릭합니다.

Select Comparison 창이 나타납니다.

3단계 **Compare Against** 드롭다운 목록에서 원하는 비교 유형을 선택합니다.

- 두 개의 다른 정책을 비교하려면 **Other Policy**를 선택합니다.

  페이지가 새로 고쳐지고 Policy A 및 Policy B 드롭다운 목록이 나타납니다.
- 동일한 정책의 두 개정을 비교하려면 **Other Revision**을 선택합니다.

  페이지가 새로 고쳐지고 Policy, Revision A 및 Revision B 드롭다운 목록이 나타납니다.

4단계 선택한 비교 유형에 따라 다음을 선택할 수 있습니다.

- 두 개의 다른 정책을 비교할 경우 비교할 정책을 Policy A 및 Policy B 드롭다운 목록에서 각각 선택합니다.
- 동일한 정책의 두 개정을 비교하는 경우 Policy를 선택한 다음, Revision A 및 Revision B 드롭다운 목록에서 비교할 타임스탬프된 개정을 선택합니다.

5단계 **OK**를 클릭하여 정책 비교 보기를 표시합니다.

비교 보기가 나타납니다.

6단계 선택적으로, **Comparison Report**를 클릭하여 네트워크 분석 정책 비교 보고서를 생성합니다.

네트워크 분석 정책 비교 보고서가 나타납니다. 브라우저 설정에 따라 보고서가 팝업 창에 나타날 수 있으며, 컴퓨터에 보고서를 저장하는 프롬프트가 표시될 수도 있습니다.

27장 애플리케이션 레이어 프리프로세서 사용

네트워크 분석 정책에서 애플리케이션 레이어 프리프로세서를 구성하며, 이를 통해 침입 정책에서 활성화된 규칙을 사용하여 트래픽을 검사할 준비를 하게 됩니다. 자세한 내용은 23-1페이지의 네트워크 분석 및 침입 정책 이해을/를 참조하십시오.

애플리케이션 레이어 프로토콜은 다양한 방법으로 동일한 데이터를 표현할 수 있습니다. Cisco에서는 특정 패킷 데이터 유형을 침입 규칙 엔진이 분석할 수 있는 형식으로 표준화하는 애플리케이션 레이어 프로토콜 디코더를 제공합니다. 애플리케이션 레이어 프로토콜 인코딩을 정규화함으로써 규칙 엔진에서는 데이터가 다르게 표현된 패킷에 동일한 콘텐츠 관련 규칙을 효과적으로 적용하고 의미 있는 결과를 얻을 수 있습니다.

침입 규칙 또는 규칙 인수에서 비활성화된 프리프로세서를 요구하면, 네트워크 분석 정책의 웹 인터페이스에서 비활성 상태로 있더라도 시스템에서는 자동으로 현재의 컨피그레이션과 함께 해당 프리프로세서를 사용합니다. 자세한 내용은 23-12페이지의 사용자 지정 정책의 제한 사항을/를 참조하십시오.

주의 사용자 지정 사용자 역할이 있는 일부 사용자는 표준 메뉴 경로(**Policies > Access Control > Network Analysis Policy**)를 통해 네트워크 분석 정책에 액세스할 수 없습니다. 이러한 사용자는 침입 정책을 통해 네트워크 분석 정책에 액세스할 수 있습니다(**Policies > Intrusion > Intrusion Policy > Network Analysis Policy**). 사용자 지정 사용자 역할에 대한 자세한 내용은 61-51페이지의 사용자 지정 사용자 역할 관리을/를 참조하십시오.

침입 정책에서 동반 프리프로세서 규칙을 활성화하지 않는 한 프리프로세서는 대부분의 경우 이벤트를 생성하지 않습니다. 자세한 내용은 32-20페이지의 규칙 상태 설정을/를 참조하십시오.

자세한 내용은 다음 절을 참조하십시오.

- 27-2페이지의 DCE/RPC 트래픽 디코딩 - DCE/RPC 프리프로세서를 소개하고, 회피 시도를 방지하고 DCE/RPC 트래픽에서 변칙을 탐지하도록 이 프리프로세서를 구성하는 방법에 대해 설명합니다.
- 27-14페이지의 DNS 이름 서버 응답에서 익스플로잇 탐지 - DNS 프리프로세서를 소개하고, DNS 이름 서버 응답에서 세 가지 특정 익스플로잇을 탐지하도록 이 프리프로세서를 구성하는 방법에 대해 설명합니다.
- 27-18페이지의 FTP 및 텔넷 트래픽 디코딩 - FTP/Telnet 디코더를 소개하고, FTP 및 텔넷 트래픽을 표준화 및 디코딩하도록 이 디코더를 구성하는 방법에 대해 설명합니다.
- 27-30페이지의 HTTP 트래픽 디코딩 - HTTP 디코더를 소개하고, HTTP 트래픽을 표준화도록 이 디코더를 구성하는 방법에 대해 설명합니다.
- 27-45페이지의 Sun RPC 프리프로세서 사용 - RPC 디코더를 소개하고, RPC 트래픽을 표준화도록 이 디코더를 구성하는 방법에 대해 설명합니다.

- 27-46페이지의 SIP(Session Initiation Protocol) 디코딩 - SIP 프리프로세서를 사용하여 SIP 트래픽에서 변칙을 디코딩 및 탐지하는 방법에 대해 설명합니다.
- 27-51페이지의 GTP 명령 채널 구성 - GTP 프리프로세서를 사용하여 규칙 엔진에 패킷 디코더가 추출한 GTP 명령 채널 메시지를 제공하는 방법에 대해 설명합니다.
- 27-52페이지의 IMAP 트래픽 디코딩 - IMAP 프리프로세서를 사용하여 IMAP 트래픽에서 변칙을 디코딩 및 탐지하는 방법에 대해 설명합니다.
- 27-55페이지의 POP 트래픽 디코딩 - POP 프리프로세서를 사용하여 POP 트래픽에서 변칙을 디코딩 및 탐지하는 방법에 대해 설명합니다.
- 27-58페이지의 SMTP 트래픽 디코딩 - SMTP 디코더를 소개하고, SMTP 트래픽을 디코딩 및 표준화도록 이 디코더를 구성하는 방법에 대해 설명합니다.
- 27-66페이지의 SSH 프리프로세서를 사용하여 익스플로잇 탐지 - SSH 암호화 트래픽에서 익스플로잇을 식별 및 처리하는 방법에 대해 설명합니다.
- 27-70페이지의 SSL 프리프로세서 사용 - SSL 프리프로세서를 사용하여, 암호화된 트래픽을 식별하고 해당 트래픽의 검사를 중지하여 오탐을 없애는 방법에 대해 설명합니다.
- 28-1페이지의 SCADA 전처리 구성 - Modbus 및 DNP3 프리프로세서를 사용하여 해당 트래픽에서 변칙을 탐지하고, 특정 프로토콜 필드의 검사를 위해 데이터를 침입 규칙 엔진에 제공하는 방법에 대해 설명합니다.

DCE/RPC 트래픽 디코딩

라이센스: 보호

DCE/RPC 프로토콜을 사용하면 서로 다른 네트워크 호스트의 프로세스가 마치 동일한 호스트에 있는 것처럼 통신할 수 있습니다. 프로세스 간 통신은 일반적으로 TCP 및 UDP를 통해 호스트 간에 전송됩니다. TCP 전송 내에서 DCE/RPC가 Windows SMB(Server Message Block) 프로토콜 또는 Samba로 더 캡슐화될 수 있습니다. Samba는 Windows와 UNIX 또는 Linux 같은 운영 체제로 구성된 혼합 환경에서 프로세스 간 통신에 사용되는 오픈 소스 SMB 구현입니다. 또한 네트워크의 Windows IIS 웹 서버는 방화벽을 통해 프록시 TCP 전송 DCE/RPC 트래픽에 분산 통신을 제공하는 IIS RPC over HTTP를 사용할 수도 있습니다.

DCE/RPC 프리프로세서 옵션과 기능에 대한 설명에는 Microsoft의 DCE/RPC 구현(MSRPC라고 알려짐)이 포함되고, SMB 옵션과 기능에 대한 설명에서는 SMB와 Samba를 모두 다룹니다.

대부분의 DCE/RPC 익스플로잇은 DCE/RPC 서버를 대상으로 하는 DCE/RPC 클라이언트 요청에서 발생하지만(실제로 Windows나 Samba를 실행하는 네트워크의 호스트일 수도 있음) 익스플로잇은 서버 응답에서 발생할 수도 있습니다. DCE/RPC 프리프로세서는 버전 1 RPC over HTTP를 사용하는 TCP 전송 DCE/RPC를 포함하여 TCP, UDP 및 SMB 전송에서 캡슐화된 DCE/RPC 요청 및 응답을 탐지합니다. 이 프리프로세서는 DCE/RPC 데이터 스트림을 분석하고, DCE/RPC 트래픽에서 이상 동작 및 회피 기법을 탐지합니다. 또한 SMB 데이터 스트림을 분석하고, SMB 이상 동작 및 회피 기법을 탐지합니다.

IP 디프래그먼트화 프리프로세서에서 제공하는 IP 디프래그먼트화 및 TCP 스트림 프리프로세서에서 제공하는 TCP 스트림 리어셈블리 외에도 DCE/RPC 프리프로세서는 SMB를 디세그먼트하고 DCE/RPC를 디프래그먼트합니다. 29-21페이지의 TCP 스트림 전처리 사용 및 29-12페이지의 IP 패킷 디프래그먼트을/를 참조하십시오.

마지막으로, DCE/RPC 프리프로세서는 규칙 엔진에서 처리할 수 있도록 DCE/RPC 트래픽을 표준화합니다. DCE/RPC 서비스, 운영 및 스텁 데이터 탐지를 위해 특정 DCE/RPC 규칙 키워드를 사용하는 방법에 대한 자세한 내용은 36-60페이지의 DCE/RPC 키워드을/를 참조하십시오.

프리프로세서 작동 방식을 제어하는 전역 옵션을 수정하여, 그리고 IP 주소 또는 실행 중인 Windows나 Samba 버전으로 네트워크에서 DCE/RPC 서버를 식별하는 하나 이상의 대상 기반 서버 정책을 지정하여 DCE/RPC 프리프로세서를 구성합니다.

GID(generator ID)가 132 또는 133인 DCE/RPC 프리프로세서 규칙을 활성화해야 이러한 규칙에서 이벤트를 생성할 수 있습니다. 자세한 내용은 32-20페이지의 규칙 상태 설정을/를 참조하십시오.

자세한 내용은 다음 절을 참조하십시오.

- 27-3페이지의 전역 DCE/RPC 옵션 선택
- 27-4페이지의 대상 기반 DCE/RPC 서버 정책 이해
- 27-5페이지의 DCE/RPC 전송 이해
- 27-8페이지의 DCE/RPC 대상 기반 정책 옵션 선택
- 27-11페이지의 DCE/RPC 프리프로세서 구성

전역 DCE/RPC 옵션 선택

라이센스: 보호

전역 DCE/RPC 프리프로세서 옵션은 프리프로세서의 작동 방식을 제어합니다. **Memory Cap Reached** 옵션을 제외하고, 이러한 옵션을 수정하면 성능 또는 탐지 기능에 부정적인 영향이 미칠 수 있습니다. 프리프로세서 및 프리프로세서와 활성화된 DCE/RPC 규칙 간 상호 작용을 철저히 이해하고 있는 경우가 아니면 이러한 옵션을 수정해서는 안 됩니다. 특히, **Maximum Fragment Size** 옵션과 **Reassembly Threshold** 옵션은 규칙이 탐지해야 하는 깊이와 같거나 더 커야 합니다. 자세한 내용은 36-17페이지의 내용 일치 제한 및 36-30페이지의 Byte_Jump and Byte_Test 사용을/를 참조하십시오.

다음 설명에서 프리프로세서 규칙이 언급되지 않은 경우 해당 옵션은 프리프로세서 규칙과 관련되지 않은 것입니다.

Maximum Fragment Size

Enable Defragmentation을 선택한 경우, 1514~65535바이트 범위에서 허용되는 최대 DCE/RPC 프래그먼트 길이를 지정합니다. 프리프로세서는 디프래그먼트 전에 처리 목적으로 더 큰 프래그먼트를 지정된 크기로 자르지만, 실제 패킷을 변경하지는 않습니다. 필드를 비워 두면 이 옵션이 비활성화됩니다.

Reassembly Threshold

Enable Defragmentation을 선택한 경우, 0은 이 옵션을 비활성화하고 1~65535바이트 값은 리어셈블된 패킷을 규칙 엔진으로 전송하기 전 프래그먼트된 DCE/RPC 바이트, 그리고 해당되는 경우 세그먼트된 SMB 바이트의 최소 수를 지정합니다. 낮은 값을 입력하면 조기 탐지 가능성이 높아지지만 성능이 저하될 수 있습니다. 이 옵션을 활성화하는 경우 성능 영향을 테스트해야 합니다.

Enable Defragmentation

프래그먼트된 DCE/RPC 트래픽을 디프래그먼트해야 할지 여부를 지정합니다. 비활성화된 경우 프리프로세서는 여전히 변칙을 탐지하고 규칙 엔진에 DCE/RPC 데이터를 전송하지만, 프래그먼트된 DCE/RPC 데이터에서 익스플로잇을 놓칠 위험이 있습니다.

이 옵션은 DCE/RPC 트래픽을 디프래그먼트하지 않는 유연성을 제공하지만, 대부분의 DCE/RPC 익스플로잇은 프래그먼트를 이용하여 익스플로잇을 숨기려고 시도합니다. 이 옵션을 비활성화하면 대부분의 알려진 익스플로잇을 우회하게 되므로 상당히 많은 오탐이 발생할 수 있습니다.

Memory Cap Reached

프리프로세서에 할당된 최대 메모리 제한에 도달하거나 이를 초과하는 경우를 탐지합니다. 최대 메모리 용량에 도달하거나 이를 초과하는 경우 프리프로세서는 메모리 용량 이벤트를 일으킨 세션과 관련된 보류 중인 모든 데이터를 비우고 해당 세션의 나머지를 무시합니다.

이 옵션에 대한 이벤트를 생성하려면 규칙 133:1을 활성화할 수 있습니다. 자세한 내용은 32-20 페이지의 규칙 상태 설정을/를 참조하십시오.

Auto-Detect Policy on SMB Session

SMB `Session Setup AndX` 요청과 응답에서 식별되는 Windows 또는 Samba 버전을 탐지합니다. 탐지된 버전이 **Policy** 컨피그레이션 옵션에 대해 구성된 Windows 또는 Samba 버전과 다른 경우, 해당 세션에 대해서만 탐지된 버전이 구성된 버전을 재정의합니다. 자세한 내용은 27-4페이지의 대상 기반 DCE/RPC 서버 정책 이해을/를 참조하십시오.

예를 들어 **Policy**를 Windows XP로 설정했는데 Windows Vista가 탐지된 경우, 프리프로세서는 해당 세션에 대해 Windows Vista 정책을 사용합니다. 다른 설정은 그대로 유효합니다.

DCE/RPC 전송이 SMB가 아닌 경우(즉, 전송이 TCP나 UDP인 경우), 버전을 탐지할 수 없으며 정책이 자동으로 구성되지 않습니다.

이 옵션을 활성화하는 경우 드롭다운 목록에서 다음 중 하나를 선택합니다.

- 정책 유형에 대해 서버-클라이언트 트래픽을 검사하려면 **Client**를 선택합니다.
- 정책 유형에 대해 클라이언트-서버 트래픽을 검사하려면 **Server**를 선택합니다.
- 정책 유형에 대해 서버-클라이언트 및 클라이언트-서버 트래픽을 검사하려면 **Both**를 선택합니다.

대상 기반 DCE/RPC 서버 정책 이해

라이센스: 보호

지정된 서버 유형이 처리하는 것과 동일한 DCE/RPC 트래픽을 검사하려면 DCE/RPC 프리프로세서를 구성하기 위한 하나 이상의 대상 기반 서버 정책을 생성할 수 있습니다. 대상 기반 정책 컨피그레이션에는 네트워크에서 사용자가 식별하는 호스트에서 실행 중인 Windows 또는 Samba 버전 식별하기, 전송 프로토콜을 활성화하고 DCE/RPC 트래픽을 이러한 호스트로 전달하는 포트 지정하기, 기타 서버 관련 옵션 설정하기 등이 포함됩니다.

Windows 및 Samba DCE/RPC 구현은 크게 다릅니다. 예를 들어 모든 Windows 버전은 DCE/RPC 트래픽을 디프래그먼트할 때 첫 번째 프래그먼트에 DCE/RPC 컨텍스트 ID를 사용하고, 모든 Samba 버전은 마지막 프래그먼트에 컨텍스트 ID를 사용합니다. 또 다른 예로 Windows Vista는 특정 함수 호출을 식별하기 위해 첫 번째 프래그먼트에 opnum(operation number) 헤더 필드를 사용하고, Samba 및 다른 모든 Windows 버전은 마지막 프래그먼트에 opnum 필드를 사용합니다.

또한 Windows 및 Samba SMB 구현에는 중요한 차이점이 있습니다. 예를 들어, Windows는 명명된 파이프로 작업할 때 SMB OPEN 및 READ 명령을 인식하지만 Samba는 이러한 명령을 인식하지 못합니다.

DCE/RPC 프리프로세서를 활성화하는 경우 기본 대상 기반 정책도 자동으로 활성화됩니다. 선택적으로, **Policy** 드롭다운 목록에서 올바른 버전을 선택하여 다른 Windows 또는 Samba 버전을 실행 중인 다른 호스트를 대상으로 하는 대상 기반 정책을 추가할 수 있습니다. 기본 대상 기반 정책은 다른 대상 기반 정책에 포함되지 않은 호스트에 적용됩니다.

각 대상 기반 정책에서 하나 이상의 전송을 활성화하고 각각에 대한 *탐지 포트*를 지정할 수 있습니다. 또한 *자동 탐지 포트*를 활성화 및 지정할 수 있습니다. 자세한 내용은 27-5페이지의 DCE/RPC 전송 이해을/를 참조하십시오.

다른 대상 기반 정책 옵션을 구성할 수도 있습니다. 지정한 하나 이상의 공유 SMB 리소스에 연결하려는 시도가 있는 경우 이를 탐지하도록 프리프로세서를 설정할 수 있습니다. SMB 트래픽에서 파일을 탐지하고, 탐지된 파일에서 지정된 바이트 수를 검사하도록 프리프로세서를 구성할 수 있습니다. 고급 옵션의 경우 SMB 프로토콜 전문 지식을 갖춘 사용자만이 수정하도록 해야 합니다. 이 옵션을 사용하면 chained SMB AndX 명령 수가 지정된 최대 수를 초과하는 경우를 탐지하도록 프리프로세서를 설정할 수 있습니다.

각 대상 기반 정책에서 다음과 같이 할 수 있습니다.

- 하나 이상의 전송을 활성화하고 각각에 대해 *탐지 포트*를 활성화할 수 있습니다.
- *자동 탐지 포트*를 활성화 및 지정할 수 있습니다. 자세한 내용은 27-5페이지의 DCE/RPC 전송 이해을/를 참조하십시오.
- 지정한 하나 이상의 공유 SMB 리소스에 연결하려는 시도가 있는 경우 이를 탐지하도록 프리프로세서를 설정할 수 있습니다.
- SMB 트래픽에서 파일을 탐지하고, 탐지된 파일에서 지정된 바이트 수를 검사하도록 프리프로세서를 구성할 수 있습니다.
- 고급 옵션의 경우 SMB 프로토콜 전문 지식을 갖춘 사용자만이 수정하도록 해야 합니다. 이 옵션을 사용하면 chained SMB AndX 명령 수가 지정된 최대 수를 초과하는 경우를 탐지하도록 프리프로세서를 설정할 수 있습니다.

SMB가 DCE/RPC 전송일 경우 세션 단위 기반으로 대상 정책에 대해 구성된 정책 유형을 자동으로 재정의하려면 **Auto-Detect Policy on SMB Session** 전역 옵션을 활성화할 수 있습니다. 27-4페이지의 Auto-Detect Policy on SMB Session을/를 참조하십시오.

DCE/RPC 프리프로세서에서 SMB 트래픽 파일 탐지를 활성화하는 것 외에도 선택적으로 이러한 파일을 캡처 및 차단하거나 동적 분석을 위해 종합 보안 인텔리전스 클라우드에 제출하려면 파일 정책을 구성할 수 있습니다. 해당 정책 내에서 **Action**(**Detect Files** 또는 **Block Files**) 및 선택한 **Application Protocol**(**Any** 또는 **NetBIOS-ssn (SMB)**)로 파일 규칙을 생성해야 합니다. 자세한 내용은 37-16페이지의 파일 정책 생성 및 37-17페이지의 파일 규칙 작업을/를 참조하십시오.

DCE/RPC 전송 이해

라이센스: 보호

각 대상 기반 정책에서 하나 이상의 TCP, UDP, SMB 및 RPC over HTTP 전송을 활성화할 수 있습니다. 전송을 활성화할 때, DCE/RPC 트래픽을 전달하는 것으로 알려진 포트인 *탐지 포트*를 하나 이상 지정해야 합니다. 선택적으로, 프리프로세서가 먼저 테스트를 통해 해당 포트에서 DCE/RPC 트래픽을 전달하는지를 확인하고 DCE/RPC 트래픽을 탐지하는 경우에만 계속해서 처리하는 포트인 *자동 탐지 포트*를 활성화 및 지정할 수도 있습니다.

Cisco에서는 잘 알려진 포트이거나 각 프로토콜에 대해 일반적으로 사용되는 포트인 기본 탐지 포트를 사용할 것을 권장합니다. 기본 포트가 아닌 포트에서 DCE/RPC 트래픽을 탐지한 경우에만 탐지 포트를 추가하면 됩니다.

자동 탐지 포트를 활성화하는 경우, 전체 임시 포트 범위를 수용할 수 있도록 1024~65535의 포트 범위를 설정해야 합니다. RPC over HTTP Proxy Auto-Detect Ports 옵션 또는 SMB Auto-Detect Ports 옵션에 대해서는 자동 탐지 포트를 설정하지 않을 수 있습니다. 지정된 기본 탐지 포트를 제외하면 이러한 포트에서 트래픽이 발생할 가능성이 거의 없기 때문입니다. 자동 탐지는 전송 탐지 포트에 의해 아직 식별되지 않은 포트에 대해서만 발생한다는 점에 유의하십시오. 각 포트에 대해 자동 탐지 포트를 활성화 또는 비활성화하기 위한 권장 사항은 27-8페이지의 DCE/RPC 대상 기반 정책 옵션 선택을/를 참조하십시오.

Windows 대상 기반 정책에서는 네트워크의 트래픽을 매칭하기 위해 임의의 조합으로 하나 이상의 전송에 대해 포트를 지정할 수 있지만, Samba 대상 기반 정책에서는 SMB 전송에 대해서만 포트를 지정할 수 있습니다.

하나 이상의 전송이 활성화된 DCE/RPC 대상 기반 정책을 추가한 경우를 제외하고, 기본 대상 기반 정책에서는 하나 이상의 DCE/RPC 전송을 활성화해야 합니다. 예를 들어 모든 DCE/RPC 구현에 대해 호스트를 지정하고, 지정되지 않은 호스트에는 기본 대상 기반 정책을 적용하지 않을 수 있습니다. 이 경우 기본 대상 기반 정책에 대해 전송을 활성화하지 않을 수 있습니다.

자세한 내용은 다음 절을 참조하십시오.

- 27-6페이지의 연결 없는/연결 지향 DCE/RPC 트래픽 이해
- 27-7페이지의 RPC over HTTP 전송 이해

연결 없는/연결 지향 DCE/RPC 트래픽 이해

라이센스: 보호

DCE/RPC 메시지는 두 가지 서로 다른 DCE/RPC PDU(Protocol Data Unit) 프로토콜 중 하나를 준수합니다.

- 연결 지향 DCE/RPC PDU 프로토콜

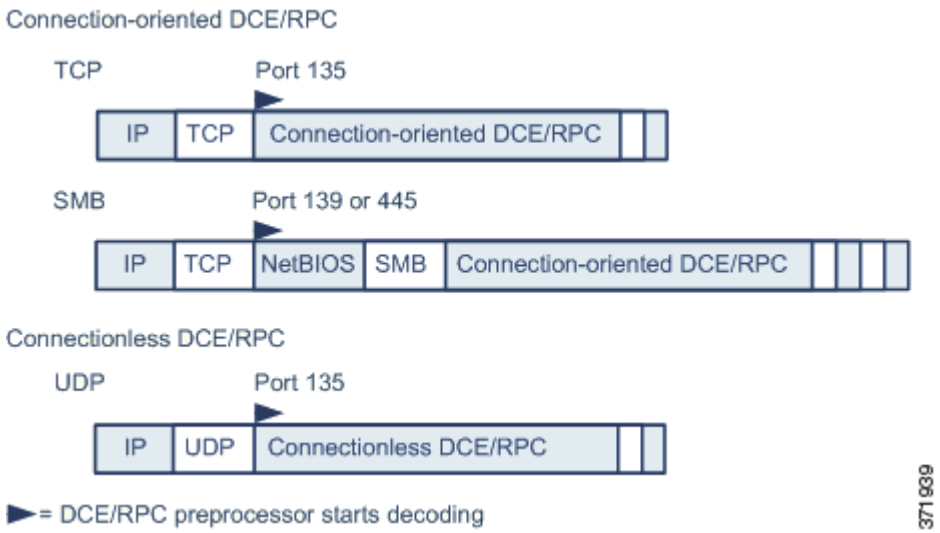
  DCE/RPC 프리프로세서는 TCP, SMB 및 RPC over HTTP 전송에서 연결 지향 DCE/RPC를 탐지합니다.

- 연결 없는 DCE/RPC PDU 프로토콜

  DCE/RPC 프리프로세서는 UDP 전송에서 연결 없는 DCE/RPC를 탐지합니다.

두 개의 DCE/RPC PDU 프로토콜에는 각각의 고유한 헤더 및 데이터 특성이 있습니다. 예를 들어 연결 지향 DCE/RPC 헤더 길이는 일반적으로 24바이트이며 연결 없는 DCE/RPC 헤더 길이는 80바이트로 고정되어 있습니다. 또한 프래그먼트된 연결 없는 DCE/RPC의 올바른 프래그먼트 순서는 연결 없는 전송으로 처리할 수 없으며, 대신 연결 없는 DCE/RPC 헤더 값으로 보장해야 합니다. 반대로 전송 프로토콜은 연결 지향 DCE/RPC에 대한 올바른 프래그먼트 순서를 보장합니다. DCE/RPC 프리프로세서는 이러한 특성 및 기타 프로토콜 관련 특성을 사용하여 두 프로토콜에서 변칙이나 기타 회피 기법을 모니터링하고, 규칙 엔진으로 전달되기 전에 트래픽을 디코딩 및 디프래그먼트합니다.

다음 다이어그램은 DCE/RPC 프리프로세서가 서로 다른 전송에 대해 DCE/RPC 트래픽 처리를 시작하는 지점을 설명합니다.



이 그림에서 다음에 유의하십시오.

- 잘 알려진 TCP 또는 UDP 포트 135는 TCP 및 UDP 전송에서 DCE/RPC 트래픽을 식별합니다.
- 그림에는 RPC over HTTP가 포함되지 않았습니다.

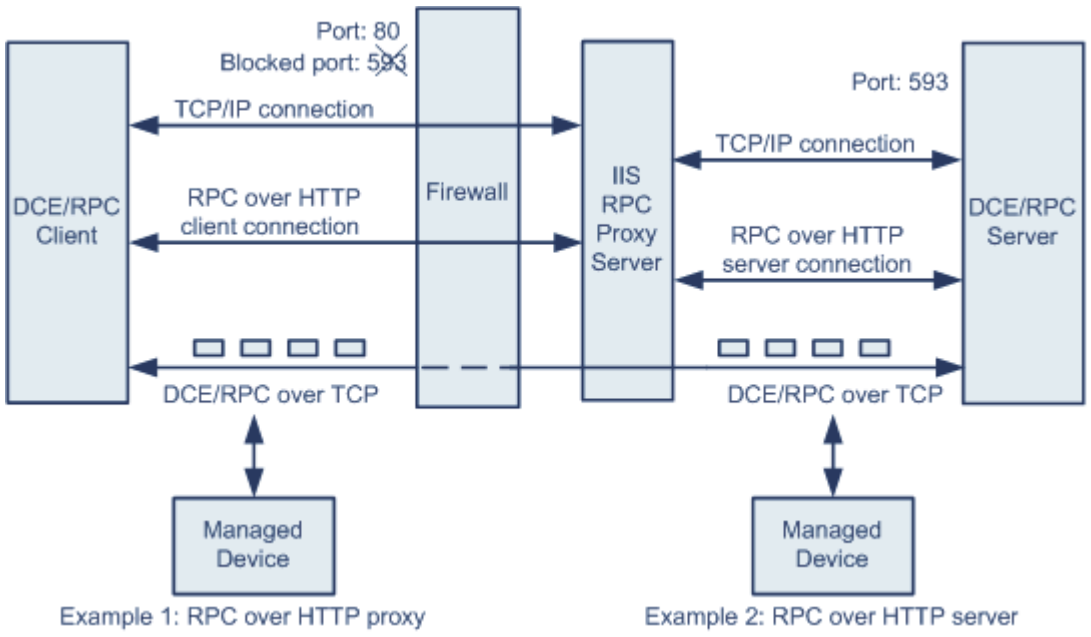
  RPC over HTTP의 경우, 연결 지향 DCE/RPC는 HTTP를 통한 초기 설정 시퀀스 후 그림에 나와 있듯이 TCP를 통해 직접 전송됩니다. 자세한 내용은 27-7페이지의 RPC over HTTP 전송 이해을/를 참조하십시오.
- DCE/RPC 프리프로세서는 일반적으로 NetBIOS Session Service에 대해 잘 알려진 TCP 포트 139에서 SMB 트래픽을 수신하거나, 잘 알려진 Windows 포트 445에서 유사하게 구현합니다.

  SMB에는 DCE/RPC 전송 외에도 많은 기능이 있기 때문에 프리프로세서는 먼저 SMB 트래픽이 DCE/RPC 트래픽을 전달하는지 테스트한 다음, 전달하지 않는 경우 처리를 중지하고 전달하는 경우 처리를 계속 진행합니다.
- IP는 모든 DCE/RPC 전송을 캡슐화합니다.
- TCP는 모든 연결 지향 DCE/RPC를 전송합니다.
- UDP는 연결 없는 DCE/RPC를 전송합니다.

RPC over HTTP 전송 이해

라이센스: 보호

Microsoft RPC over HTTP를 사용하면 다음 그림에 보이는 것처럼 방화벽을 통해 DCE/RPC 트래픽을 터널링할 수 있습니다. DCE/RPC 프리프로세서는 Microsoft RPC over HTTP의 버전 1을 탐지합니다.



Example 1: RPC over HTTP proxy

Example 2: RPC over HTTP server

Microsoft IIS 프록시 서버 및 DCE/RPC 서버는 같은 호스트에 있을 수도 있고 다른 호스트에 있을 수도 있습니다. 두 경우에 대해 각기 다른 프록시 및 서버 옵션이 제공됩니다. 이 그림에서 다음에 유의하십시오.

- DCE/RPC 서버는 포트 593에서 DCE/RPC 클라이언트 트래픽을 모니터링하지만, 방화벽은 포트 593을 차단합니다.

  대개 방화벽은 기본적으로 포트 593을 차단합니다.
- RPC over HTTP는 잘 알려진 HTTP 포트 80을 사용하여 DCE/RPC over HTTP를 전송하며, 방화벽에서는 이를 허용할 수 있습니다.
- Example 1에서는 DCE/RPC 클라이언트와 Microsoft IIS RPC 프록시 서버 간 트래픽을 모니터링하기 위해 **RPC over HTTP proxy** 옵션을 선택합니다.
- Example 2에서는 Microsoft IIS RPC 프록시 서버 및 DCE/RPC 서버가 서로 다른 호스트에 있고 디바이스가 두 서버 간 트래픽을 모니터링할 때 **RPC over HTTP server** 옵션을 선택합니다.
- RPC over HTTP가 DCE/RPC 클라이언트와 서버 간 프록시된 설정을 완료한 후 트래픽은 연결 지향 DCE/RPC over TCP로만 구성됩니다.

DCE/RPC 대상 기반 정책 옵션 선택

라이센스: 보호

각 대상 기반 정책에서는 다음과 같은 다양한 옵션을 지정할 수 있습니다. **Memory Cap Reached** 및 **Auto-Detect Policy on SMB Session** 옵션을 제외하고, 이러한 옵션을 수정하면 성능 또는 탐지 기능에 부정적인 영향이 미칠 수 있습니다. 프리프로세서 및 프리프로세서와 활성화된 DCE/RPC 규칙 간 상호 작용을 철저히 이해하고 있는 경우가 아니면 이러한 옵션을 수정해서는 안 됩니다.

다음 설명에서 프리프로세서 규칙이 언급되지 않은 경우 해당 옵션은 프리프로세서 규칙과 관련되지 않은 것입니다.

네트워크

DCE/RPC 대상 기반 서버 정책을 적용하려는 호스트 IP 주소.

단일 IP 주소나 주소 블록 또는 쉼표로 구분된 목록을 지정할 수 있습니다(둘 중 하나 또는 모두). 기본 정책을 포함하여 최대 255개의 총 프로필을 지정할 수 있습니다. FireSIGHT 시스템에서 IPv4 및 IPv6 주소 블록을 지정하는 방법에 대한 자세한 내용은 을/를 참조하십시오.

기본 정책의 `default` 설정은 다른 대상 기반 정책에서 처리되지 않는 모니터링되는 네트워크 세그먼트의 모든 IP 주소를 지정합니다. 따라서 기본 정책에 대해서는 IP 주소 또는 CIDR 블록/접두사 길이를 지정할 수 없고 지정할 필요도 없으며, 다른 정책에서 이 설정을 비워둘 수 없거나 `any`를 나타내는 주소 표기법(예: 0.0.0.0/0 또는 ::/0)을 사용할 수 없습니다.

또한 트래픽 처리를 위한 대상 기반 정책의 경우, 식별하는 네트워크는 대상 기반 정책을 구성하는 네트워크 분석 정책에서 처리되는 네트워크, 영역, VLAN의 하위 집합과 일치하거나 하위 집합이어야 합니다. 자세한 내용은 25-3페이지의 네트워크 분석 정책으로 전처리 맞춤화을/를 참조하십시오.

정책

대상 호스트 또는 모니터링되는 네트워크 세그먼트의 호스트에서 사용하는 Windows 또는 Samba DCE/RPC 구현. 이러한 정책에 대한 자세한 내용은 27-4페이지의 대상 기반 DCE/RPC 서버 정책 이해을/를 참조하십시오.

SMB가 DCE/RPC 전송일 경우 세션 단위 기반으로 이 옵션에 대한 설정을 자동으로 재정의하려면 **Auto-Detect Policy on SMB Session** 전역 옵션을 활성화할 수 있습니다. 27-4페이지의 Auto-Detect Policy on SMB Session을/를 참조하십시오.

SMB Invalid Shares

하나 이상의 SMB 공유 리소스를 식별하는 대/소문자 구분 영숫자 텍스트 문자열. 프리프로세서는 사용자가 지정한 공유 리소스에 연결하려는 시도가 있는 경우 이를 탐지합니다. 쉼표로 구분된 목록에서 여러 공유를 지정할 수 있으며, 선택적으로 공유를 따옴표로 감쌀 수 있습니다. 이는 이전 소프트웨어 버전에서 필요했지만 더 이상 그럴 필요가 없습니다. 예를 들면 다음과 같습니다.

```
"C$", D$, "admin", private
```

SMB 포트 및 SMB 트래픽 탐지를 모두 활성화한 경우 프리프로세서는 SMB 트래픽에서 잘못된 공유를 탐지합니다.

대부분의 경우 잘못된 공유로 식별하는, Windows에서 명명된 드라이브에 달러 기호를 추가해야 합니다. 예를 들면 드라이브 C를 C$ 또는 "C$"로 식별합니다.

이 옵션에 대한 이벤트를 생성하려면 규칙 133:26을 활성화할 수 있습니다. 자세한 내용은 32-20페이지의 규칙 상태 설정을/를 참조하십시오.

SMB Maximum AndX Chain

허용할 chained SMB AndX 명령의 최대 수(0~255). 일반적으로 비교적 많은 chained AndX 명령이 이상 행동을 보이며, 회피 시도를 나타낼 수 있습니다. chained 명령을 허용하지 않으려면 1을 지정하고, chained 명령 수의 탐지를 비활성화하려면 0을 지정합니다.

프리프로세서는 먼저 chained 명령의 수를 세고, 동반 SMB 프리프로세서 규칙이 활성화되고 chained 명령 수가 구성된 값과 같거나 큰 경우 이벤트를 생성합니다. 그런 다음 계속해서 처리합니다.

참고 SMB 프로토콜에 대한 전문 지식을 보유한 사용자만이 이 옵션의 기본 설정을 수정해야 합니다.

이 옵션에 대한 이벤트를 생성하려면 규칙 133:20을 활성화할 수 있습니다. 자세한 내용은 32-20페이지의 규칙 상태 설정을/를 참조하십시오.

RPC proxy traffic only

RPC over HTTP Proxy Ports가 활성화된 경우 탐지된 클라이언트 측 RPC over HTTP 트래픽이 프록시 트래픽 전용인지 다른 웹 서버 트래픽도 포함할 수 있는지를 나타냅니다. 예를 들어 포트 80은 프록시 및 기타 웹 서버 트래픽을 수행할 수 있습니다.

이 옵션이 비활성화되면 프록시와 기타 웹 서버 트래픽이 모두 예상됩니다. 예를 들어 서버가 전용 프록시 서버인 경우 이 옵션을 활성화하십시오. 활성화된 경우 프리프로세서는 트래픽이 DCE/RPC를 전달하는지를 테스트하고, 전달하지 않는 경우 트래픽을 무시하고 전달하는 경우 처리를 계속 진행합니다. 이 옵션과 함께 **RPC over HTTP Proxy Ports**도 활성화한 경우에만 기능이 추가됩니다.

RPC over HTTP Proxy Ports

관리되는 디바이스가 DCE/RPC 클라이언트와 Microsoft IIS RPC 프록시 서버 사이에 있는 경우, 지정된 각 포트를 통해 RPC over HTTP에 의해 터널링된 DCE/RPC 트래픽의 탐지를 활성화합니다. 27-7페이지의 RPC over HTTP 전송 이해을/를 참조하십시오.

활성화된 경우 DCE/RPC 트래픽을 확인할 포트를 추가할 수 있습니다. 웹 서버는 일반적으로 DCE/RPC 및 기타 트래픽에 대해 기본 포트를 사용하므로 이 작업이 반드시 필요한 것은 아닙니다. 활성화된 경우 **RPC over HTTP Proxy Auto-Detect Ports**는 활성화하지 않을 수 있지만, 탐지된 클라이언트 측 RPC over HTTP 트래픽이 프록시 트래픽 전용이며 다른 웹 서버 트래픽을 포함하지 않는 경우에는 **RPC Proxy Traffic Only**를 활성화할 수 있습니다.

RPC over HTTP Server Ports

Microsoft IIS RPC 프록시 서버 및 DCE/RPC 서버가 서로 다른 호스트에 있고 디바이스가 두 서버 간 트래픽을 모니터링하는 경우, 지정된 각 포트에서 RPC over HTTP에 의해 터널링된 DCE/RPC 트래픽의 탐지를 활성화합니다. 27-7페이지의 RPC over HTTP 전송 이해을/를 참조하십시오.

일반적으로 이 옵션을 활성화한 경우에는, 네트워크에서 프록시 웹 서버를 인지하지 못하더라도 해당 옵션에 대해 1025~65535의 포트 범위로 **RPC over HTTP Server Auto-Detect Ports**도 활성화해야 합니다. RPC over HTTP 서버 포트는 때때로 다시 구성됩니다. 그런 경우 이 옵션에 대한 포트 목록에 다시 구성된 서버 포트를 추가해야 합니다.

TCP Ports

지정된 각 포트의 TCP에서 DCE/RPC 트래픽의 탐지를 활성화합니다.

합법적인 DCE/RPC 트래픽과 익스플로잇이 광범위한 포트를 사용할 수 있으며, 이 경우 일반적으로 포트 1024 위의 다른 포트가 사용됩니다. 이 옵션을 활성화하는 경우 해당 옵션에 대해 1025~65535 포트 범위로 **TCP Auto-Detect Ports**도 활성화합니다.

UDP Ports

지정된 각 포트의 UDP에서 DCE/RPC 트래픽의 탐지를 활성화합니다.

합법적인 DCE/RPC 트래픽과 익스플로잇이 광범위한 포트를 사용할 수 있으며, 이 경우 일반적으로 포트 1024 위의 다른 포트가 사용됩니다. 이 옵션을 활성화하는 경우 해당 옵션에 대해 1025~65535 포트 범위로 **UDP Auto-Detect Ports**도 활성화합니다.

SMB 포트

지정된 각 포트의 SMB에서 DCE/RPC 트래픽의 탐지를 활성화합니다.

기본 탐지 포트를 사용하는 SMB 트래픽이 발견될 수 있습니다. 다른 포트는 거의 발견되지 않습니다. 대개 기본 설정을 사용합니다.

RPC over HTTP Proxy Auto-Detect Ports

관리되는 디바이스가 DCE/RPC 클라이언트와 Microsoft IIS RPC 프록시 서버 사이에 있는 경우, 지정된 포트를 통해 RPC over HTTP에 의해 터널링된 DCE/RPC 트래픽의 자동 탐지를 활성화합니다. 27-7페이지의 RPC over HTTP 전송 이해을/를 참조하십시오.

활성화된 경우 전체 임시 포트 범위를 수용할 수 있도록 대개 1025~65535의 포트 범위를 지정합니다.

RPC over HTTP Server Auto-Detect Ports

Microsoft IIS RPC 프록시 서버 및 DCE/RPC 서버가 서로 다른 호스트에 있고 디바이스가 두 서버 간 트래픽을 모니터링하는 경우, 지정된 포트에서 RPC over HTTP에 의해 터널링된 DCE/RPC 트래픽의 자동 탐지를 활성화합니다. 27-7페이지의 RPC over HTTP 전송 이해을/를 참조하십시오.

TCP Auto-Detect 포트

지정된 포트의 TCP에서 DCE/RPC 트래픽의 자동 탐지를 활성화합니다.

UDP Auto-Detect 포트

지정된 각 포트의 UDP에서 DCE/RPC 트래픽의 자동 탐지를 활성화합니다.

SMB Auto-Detect 포트

SMB에서 DCE/RPC 트래픽의 자동 탐지를 활성화합니다.

SMB File Inspection

파일 탐지를 위한 SMB 트래픽의 검사를 활성화합니다. 다음 옵션을 이용할 수 있습니다.

- 파일 검사를 비활성화하려면 **Off**를 선택합니다.
- SMB에서 DCE/RPC 트래픽을 검사하지 않고 파일 데이터를 검사하려면 **Only**를 선택합니다. 이 옵션을 선택하면 파일과 DCE/RPC 트래픽 모두의 검사 성능이 개선될 수 있습니다.
- SMB에서 파일과 DCE/RPC 트래픽을 모두 검사하려면 **On**을 선택합니다. 이 옵션을 선택하면 성능이 저하될 수 있습니다.

다음에 대한 SMB 트래픽의 검사는 지원되지 않습니다.

- SMB 2.x 및 SMB 3.x에서 전송되는 파일
- 이 옵션이 활성화되고 정책이 적용되기 전에 기존의 TCP 또는 SMB 세션에서 전송되는 파일
- 단일 TCP 또는 SMB 세션에서 동시에 전송되는 파일
- 여러 TCP 또는 SMB 세션 간에 전송되는 파일
- 메시지 서명이 협상된 경우처럼 비연속 데이터와 함께 전송되는 파일
- 데이터를 중첩하는, 동일한 오프셋의 서로 다른 데이터와 함께 전송되는 파일
- 수정을 위해 원격 클라이언트에서 열었으며 해당 클라이언트가 파일 서버에 저장한 파일

SMB File Inspection Depth

SMB File Inspection이 **Only** 또는 **On**으로 설정된 경우 SMB 트래픽에서 파일이 탐지될 때 검사하는 바이트 수. 다음 중 하나를 지정합니다.

- `1~2147483647`(약 2GB)의 정수
- 전체 파일을 검사하려는 경우 `0`
- 파일 검사를 비활성화하려는 경우 `-1`

액세스 제어 정책에서 정의한 것과 같거나 더 작은 값을 이 필드에 입력하십시오. 이 옵션의 값을 **Limit the number of bytes inspected when doing file type detection**에 대해 정의한 것보다 크게 설정하는 경우 시스템은 최대 기능으로 액세스 제어 정책 설정을 사용합니다. 자세한 내용은 18-20페이지의 파일 및 악성코드 검사 성능과 저장 조정을/를 참조하십시오.

SMB File Inspection이 **Off**로 설정된 경우 이 필드는 비활성화됩니다.

DCE/RPC 프리프로세서 구성

라이센스: 보호

DCE/RPC 프리프로세서 전역 옵션 및 하나 이상의 대상 기반 서버 정책을 구성할 수 있습니다.

GID(generator ID) 133으로 규칙을 활성화하지 않는 한 프리프로세서는 이벤트를 생성하지 않습니다. 특정 탐지 옵션과 관련된 규칙은 27-3페이지의 전역 DCE/RPC 옵션 선택 및 27-8페이지의 DCE/RPC 대상 기반 정책 옵션 선택을 참조하고, 32-20페이지의 규칙 상태 설정도 참조하십시오.

또한 대부분의 DCE/RPC 프리프로세서 규칙은 SMB, 연결 지향 DCE/RPC 또는 연결 없는 DCE/RPC 트래픽에서 탐지된 변칙 및 회피 기법에 대해 이벤트를 생성합니다. 다음 표는 각 트래픽 유형에 대해 활성화할 수 있는 규칙을 식별합니다.

표 27-1 트래픽 관련 DCE/RPC 규칙

트래픽	프리프로세서 규칙 GID:SID
SMB	133:2~133:26 및 133:48~133:57
Connection-Oriented DCE/RPC	133:27~133:39
연결 없는 DCE/RPC 탐지	133:40~133:43

DCE/RPC 프리프로세서를 구성하려면

액세스: Admin/Intrusion Admin

1단계 **Policies > Access Control**을 선택하여 Access Control Policy 페이지를 표시한 다음 **Network Analysis Policy**를 클릭합니다.

Network Analysis Policy 페이지가 나타납니다.

2단계 수정할 정책 옆에 있는 수정 아이콘()을 클릭합니다.

다른 정책에 저장하지 않은 변경 사항이 있는 경우 변경 사항을 취소하고 계속 진행하려면 **OK**를 클릭합니다. 저장되지 않은 변경 사항을 다른 정책에 저장하는 방법에 대한 자세한 내용은 23-15페이지의 충돌 해결 및 정책 변경 사항 커밋을/를 참조하십시오.

Policy Information 페이지가 나타납니다.

3단계 왼쪽의 탐색 패널에서 **Settings**를 클릭합니다.

Settings 페이지가 나타납니다.

4단계 Application Layer Preprocessors 아래에서 **DCE/RPC Configuration**이 활성화되었는지 여부에 따라 두 가지 선택 사항이 있습니다.

- 컨피그레이션이 활성화되어 있으면 **Edit**를 클릭합니다.
- 컨피그레이션이 비활성화되어 있으면 **Enabled**를 클릭한 다음 **Edit**를 클릭합니다.

DCE/RPC Configuration(IP 컨피그레이션) 페이지가 나타납니다. 페이지 하단에 있는 메시지는 컨피그레이션이 포함된 네트워크 분석 정책 레이어를 식별합니다. 자세한 내용은 24-1페이지의 네트워크 분석 또는 침입 정책에서 레이어 사용을/를 참조하십시오.

5단계 27-3페이지의 전역 DCE/RPC 옵션 선택에 설명된 옵션 중 하나를 수정할 수 있습니다.

6단계 다음 2가지 옵션을 사용할 수 있습니다.

- 새로운 대상 기반 정책을 추가합니다. 페이지 왼쪽의 **Servers** 옆에 있는 추가 아이콘()을 클릭합니다. Add Target 팝업 창이 나타납니다. **Server Address** 필드에서 하나 이상의 IP 주소를 지정하고 **OK**를 클릭합니다.

  단일 IP 주소나 주소 블록 또는 쉼표로 구분된 목록을 지정할 수 있습니다(둘 중 하나 또는 모두). FireSIGHT 시스템에서 IPv4 및 IPv6 주소 블록을 사용하는 방법에 대한 자세한 내용은 1-19페이지의 IP 주소 표기 규칙을/를 참조하십시오.

  기본 정책을 포함하여 최대 255개의 정책을 구성할 수 있습니다.

  트래픽 처리를 위한 대상 기반 정책의 경우, 식별하는 네트워크는 대상 기반 정책을 구성하는 네트워크 분석 정책에서 처리되는 네트워크, 영역, VLAN의 하위 집합과 일치하거나 하위 집합이어야 합니다. 자세한 내용은 25-3페이지의 네트워크 분석 정책으로 전처리 맞춤화을/를 참조하십시오.

  새 항목이 페이지 왼쪽의 서버 목록에 나타나서 선택된 것을 알 수 있도록 강조 표시되며, 추가한 프로필에 대한 현재 컨피그레이션을 반영하여 Configuration 섹션이 업데이트됩니다.

- 기존의 대상 기반 정책에 대한 설정을 수정합니다. 페이지 왼쪽의 **Servers** 아래에서 추가한 정책에 대해 구성된 주소를 클릭하거나 **default**를 클릭합니다.

  선택 항목이 강조 표시되고, 선택한 정책에 대한 현재 컨피그레이션을 표시하기 위해 Configuration 섹션이 업데이트됩니다. 기존의 정책을 삭제하려면 제거할 정책 옆에 있는 삭제 아이콘( )을 클릭합니다.

7단계 다음의 대상 기반 정책 옵션을 수정할 수 있습니다.

- DCE/RPC 대상 기반 서버 정책을 적용할 하나 이상의 호스트를 지정하려면 단일 IP 주소나 주소 블록 또는 둘 중 하나나 둘 모두의 쉼표로 구분된 목록을 **Networks** 필드에 입력합니다.

  기본 정책을 포함하여 최대 255개의 총 프로필을 지정할 수 있습니다. 기본 정책에서는 **Networks**에 대한 설정을 수정할 수 없습니다. 기본 정책은 다른 정책에서 식별되지 않는 네트워크의 모든 서버에 적용됩니다.

- 네트워크 세그먼트의 지정된 호스트에 적용할 정책 유형을 지정하려면 **Policy** 드롭다운 목록에서 Windows 또는 Samba 정책 유형 중 하나를 선택합니다.

  SMB가 DCE/RPC 전송일 경우 세션 단위 기반으로 이 옵션에 대한 설정을 자동으로 재정의하려면 **Auto-Detect Policy on SMB Session** 전역 옵션을 활성화할 수 있습니다. 27-4페이지의 Auto-Detect Policy on SMB Session을/를 참조하십시오.

- 지정된 공유 SMB 리소스에 연결하려는 시도가 있을 때 이를 탐지하도록 프리프로세서를 설정하려면 공유 리소스를 식별할 단일 또는 쉼표로 구분된 목록의 대/소문자 구분 문자열을 **SMB Invalid Shares** 필드에 입력합니다. 선택적으로, 개별 문자열을 따옴표로 감쌉니다. 이는 이전 소프트웨어 버전에서 필요했지만 더 이상 그럴 필요가 없습니다.

  예를 들어 C$, D$, admin, private 이름의 공유 리소스를 탐지하려면 다음을 입력할 수 있습니다.

  ```
  "C$", D$, "admin", private
  ```

  잘못된 SMB 공유를 탐지하려면 **SMB Ports** 또는 **SMB Auto-Detect Ports**를 활성화하고 전역 **SMB Traffics** 옵션을 활성화해야 합니다.

  또한 대부분의 경우 잘못된 공유로 식별하는, Windows에서 명명된 드라이브에 달러 기호를 추가해야 합니다. 예를 들어 드라이브 C를 식별하려면 `C$` 또는 `"C$"`를 입력합니다.

- DCE/RPC 트래픽을 분석하지 않은 채 SMB의 DCE/RPC 트래픽에서 탐지된 파일을 검사하려면 **SMB File Inspection** 드롭다운 목록에서 **Only**를 선택합니다. DCE/RPC 트래픽과 SMB의 DCE/RPC 트래픽에서 탐지된 파일을 모두 검사하려면 **SMB File Inspection** 드롭다운 목록에서 **On**을 선택합니다. 탐지된 파일에서 검사할 바이트 수를 **SMB File Inspection Depth** 필드에 입력합니다. 탐지된 파일을 모두 검사하려면 `0`을 입력합니다.

- 허용할 chained SMB AndX 명령의 최대 수를 지정하려면 **SMB Maximum AndX Chains** 필드에 0~255 범위의 값을 입력합니다. chained 명령을 허용하지 않으려면 `1`을 지정합니다. 이 기능을 비활성화하려면 `0`을 입력하거나 옵션을 비워 둡니다.

참고 SMB 프로토콜에 대한 전문 지식을 보유한 사용자만이 **SMB Maximum AndX Chains** 옵션의 설정을 수정해야 합니다.

- Windows 정책 전송용 DCE/RPC 트래픽을 전달하는 것으로 알려진 포트를 통한 DCE/RPC 트래픽의 처리를 활성화하려면 탐지 포트 옆에 있는 확인란을 선택하거나 선택 취소하고, 선택적으로 전송용 포트를 추가하거나 삭제합니다.

  Windows 정책용 **RPC over HTTP Proxy Ports**, **RPC over HTTP Server Ports**, **TCP Ports** 및 **UDP Ports** 중 하나 또는 임의의 조합을 선택합니다. **RPC over HTTP proxy**가 활성화되고 탐지된 클라이언트 측 RPC over HTTP 트래픽이 프록시 트래픽 전용인 경우(즉, 다른 웹 서버 트래픽이 포함되지 않음) **RPC Proxy Traffic Only**를 선택합니다.

  Samba 정책에는 **SMB Ports**를 선택합니다.

대부분의 경우 기본 설정을 사용합니다. 자세한 내용은 27-5페이지의 DCE/RPC 전송 이해, 27-7페이지의 RPC over HTTP 전송 이해 및 27-8페이지의 DCE/RPC 대상 기반 정책 옵션 선택을/를 참조하십시오.

단일 포트, 대시(-)로 구분된 포트 번호의 범위 또는 포트 번호와 범위의 쉼표로 구분된 목록을 입력할 수 있습니다.

- 지정된 포트가 DCE/RPC 트래픽을 전달하는지 테스트하고 전달하는 경우 처리를 계속 진행하려면 자동 탐지 전송 옆에 있는 확인란을 선택하거나 선택 취소하고, 선택적으로 전송에 대한 포트를 추가하거나 삭제합니다.

  Windows 정책용 **RPC over HTTP Server Auto-Detect Ports**, **TCP Auto-Detect Ports** 및 **UDP Auto-Detect Ports** 중 하나 또는 임의의 조합을 선택합니다.

  매우 드문 경우이기는 하지만 **RPC over HTTP Proxy Auto-Detect Ports** 또는 **SMB Auto-Detect Ports**를 선택합니다.

  전체 임시 포트 범위를 수용할 수 있도록 활성화하는 자동 탐지 포트에 대해 대개 1025~65535의 포트 범위를 지정합니다. 자세한 내용은 27-5페이지의 DCE/RPC 전송 이해, 27-7페이지의 RPC over HTTP 전송 이해 및 27-8페이지의 DCE/RPC 대상 기반 정책 옵션 선택을/를 참조하십시오.

자세한 내용은 27-8페이지의 DCE/RPC 대상 기반 정책 옵션 선택을/를 참조하십시오.

8단계 정책을 저장하거나, 계속 수정하거나, 변경 사항을 취소하거나, 기반 정책의 기본 컨피그레이션 설정으로 돌아가거나, 시스템 캐시에 변경 사항이 남아 있는 상태로 종료합니다. 자세한 내용은 23-15페이지의 충돌 해결 및 정책 변경 사항 커밋을/를 참조하십시오.

DNS 이름 서버 응답에서 익스플로잇 탐지

라이센스: 보호

DNS 프리프로세서는 DNS 이름 서버 응답에서 다음과 같은 특정 익스플로잇을 검사합니다.

- RData 텍스트 필드에 대한 오버플로 시도
- 오래된 DNS 리소스 레코드 유형
- 실험적인 DNS 리소스 레코드 유형

자세한 내용은 다음 절을 참조하십시오.

- 27-15페이지의 DNS 프리프로세서 리소스 레코드 검사 이해
- 27-16페이지의 RData 텍스트 필드에서 오버플로 시도 탐지
- 27-16페이지의 오래된 DNS 리소스 레코드 유형 탐지
- 27-16페이지의 실험적인 DNS 리소스 레코드 유형 탐지
- 27-17페이지의 DNS 프리프로세서 구성

DNS 프리프로세서 리소스 레코드 검사 이해

라이센스: 보호

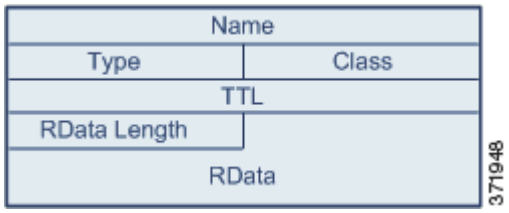
DNS 이름 서버 응답의 가장 일반적인 유형은 응답을 요청하는 쿼리의 도메인 이름에 해당하는 하나 이상의 IP 주소를 제공합니다. 다른 서버 응답 유형은 예를 들면 이메일 메시지의 목적지, 또는 원래 쿼리된 서버에서 사용할 수 없는 정보를 제공할 수 있는 이름 서버의 위치를 제공합니다.

DNS 응답은 메시지 헤더, 하나 이상의 요청이 포함된 Question 섹션, 그리고 Question 섹션의 요청에 응답하는 세 섹션(Answer, Authority 및 Additional Information)으로 구성됩니다. 이 세 섹션의 응답은 이름 서버에서 유지 관리되는 RR(*리소스 레코드*)의 정보를 반영합니다. 다음 표에서는 이러한 섹션에 대해 설명합니다.

표 27-2 DNS 이름 서버 RR 응답

섹션	포함	예
대답	선택적으로, 쿼리에 대한 특정 답을 제공하는 하나 이상의 리소스 레코드	도메인 이름에 해당하는 IP 주소
권한	선택적으로, 권한 있는 이름 서버를 가리키는 하나 이상의 리소스 레코드	응답에 대한 권한 있는 이름 서버의 이름
추가 정보	선택적으로, Answer 섹션과 관련된 추가 정보를 제공하는 하나 이상의 리소스 레코드	쿼리할 또 다른 서버의 IP 주소

다음 구조를 모두 준수하는 많은 리소스 레코드 유형이 있습니다.



이론적으로 이름 서버 응답 메시지의 Answer, Authority 또는 Additional Information 섹션에는 모든 리소스 레코드 유형을 사용할 수 있습니다. DNS 프리프로세서는 익스플로잇을 탐지하는 세 응답 섹션 각각에서 리소스 레코드를 검사합니다.

Type 및 RData 리소스 레코드 필드는 DNS 프리프로세서에서 특히 중요합니다. Type 필드는 리소스 레코드의 유형을 식별합니다. RData(resource data) 필드는 응답 내용을 제공합니다. RData 필드의 크기와 내용은 리소스 레코드의 유형에 따라 다릅니다.

DNS 메시지는 일반적으로 UDP 전송 프로토콜을 사용하지만, 메시지 유형이 안전한 배달을 요구하거나 메시지 크기가 UDP 용량을 초과하는 경우에는 TCP도 사용합니다. DNS 프리프로세서는 UDP 및 TCP 트래픽에서 DNS 서버 응답을 검사합니다.

DNS 프리프로세서는 중간에 선택된 TCP 세션을 검사하지 않으며, 패킷 삭제 때문에 세션이 상태를 손실하면 검사를 중지합니다.

DNS 프리프로세서에 대해 구성할 일반 포트는 잘 알려진 포트 53이며, DNS 이름 서버는 UDP 및 TCP에서 모두 DNS 메시지에 대해 이 포트를 사용합니다.

RData 텍스트 필드에서 오버플로 시도 탐지

라이센스: 보호

리소스 레코드 유형이 TXT(텍스트)이면 RData 필드는 변수 길이의 ASCII 텍스트 필드입니다.

Detect Overflow attempts on RData Text fields 옵션을 선택하면 DNS 프리프로세서는 MITRE의 Current Vulnerabilities and Exposures 데이터베이스에 있는 CVE-2006-3441 항목으로 식별되는 특정 취약성을 탐지합니다. 이것은 Microsoft Windows 2000 서비스 팩 4, Windows XP 서비스 팩 1 및 서비스 팩 2, Windows Server 2003 서비스 팩 1의 알려진 취약성입니다. 공격자는 이 취약성을 악용하여 악의적으로 조작된 이름 서버 응답을 전송하거나 호스트가 이를 수신하도록 함으로써 호스트를 완전히 제어할 수 있습니다. 이 경우 RData 텍스트 필드의 길이가 잘못 계산되어 버퍼 오버플로가 발생합니다.

이 취약성을 수정하도록 업그레이드되지 않은 운영 체제를 실행하는 호스트가 네트워크에 있는 경우 이 기능을 활성화해야 합니다.

이 옵션에 대한 이벤트를 생성하려면 규칙 131:3을 활성화할 수 있습니다. 자세한 내용은 32-20페이지의 규칙 상태 설정을/를 참조하십시오.

오래된 DNS 리소스 레코드 유형 탐지

라이센스: 보호

RFC 1035는 여러 리소스 레코드 유형을 오래된 것으로 식별합니다. 이들은 폐기된 레코드 유형이므로 일부 시스템은 이들을 고려하지 않으며 익스플로잇에 노출될 수 있습니다. 이러한 레코드 유형을 포함하도록 고의로 네트워크를 구성하지 않는 한 일반 DNS 응답에서는 이러한 레코드 유형을 찾을 수 없습니다.

알려진 오래된 리소스 레코드 유형을 탐지하도록 시스템을 구성할 수 있습니다. 다음 표에서는 이러한 레코드 유형을 나열 및 설명합니다.

표 27-3 오래된 DNS 리소스 레코드 유형

RR 유형	코드	설명
0.3	MD	메일 목적지
4	MF	메일 전달자

이 옵션에 대한 이벤트를 생성하려면 규칙 131:1을 활성화할 수 있습니다. 자세한 내용은 32-20페이지의 규칙 상태 설정을/를 참조하십시오.

실험적인 DNS 리소스 레코드 유형 탐지

라이센스: 보호

RFC 1035는 여러 리소스 레코드 유형을 실험적인 것으로 식별합니다. 이들은 실험적인 레코드 유형이므로 일부 시스템은 이들을 고려하지 않으며 익스플로잇에 노출될 수 있습니다. 이러한 레코드 유형을 포함하도록 고의로 네트워크를 구성하지 않는 한 일반 DNS 응답에서는 이러한 레코드 유형을 찾을 수 없습니다.

알려진 실험적인 리소스 레코드 유형을 탐지하도록 시스템을 구성할 수 있습니다. 다음 표에서는 이러한 레코드 유형을 나열 및 설명합니다.

표 27-4 실험적인 DNS 리소스 레코드 유형

RR 유형	코드	설명
7	MB	사서함 도메인 이름
8	MG	메일 그룹 멤버
9	MR	메일 이름 변경 도메인 이름
10	NUL	Null 리소스 레코드

이 옵션에 대한 이벤트를 생성하려면 규칙 131:2를 활성화할 수 있습니다. 자세한 내용은 32-20페이지의 규칙 상태 설정을/를 참조하십시오.

DNS 프리프로세서 구성

라이센스: 보호

DNS 프리프로세서를 구성하려면 다음 절차를 사용할 수 있습니다. 이 페이지의 옵션 구성에 대한 자세한 내용은 27-16페이지의 RData 텍스트 필드에서 오버플로 시도 탐지, 27-16페이지의 오래된 DNS 리소스 레코드 유형 탐지 및 27-16페이지의 실험적인 DNS 리소스 레코드 유형 탐지을/를 참조하십시오.

DNS 프리프로세서를 구성하려면

액세스: Admin/Intrusion Admin

1단계 **Policies > Access Control**을 선택하여 Access Control Policy 페이지를 표시한 다음 **Network Analysis Policy**를 클릭합니다.

Network Analysis Policy 페이지가 나타납니다.

2단계 수정할 정책 옆에 있는 수정 아이콘( )을 클릭합니다.

다른 정책에 저장하지 않은 변경 사항이 있는 경우 변경 사항을 취소하고 계속 진행하려면 **OK**를 클릭합니다. 저장되지 않은 변경 사항을 다른 정책에 저장하는 방법에 대한 자세한 내용은 23-15페이지의 충돌 해결 및 정책 변경 사항 커밋을/를 참조하십시오.

Policy Information 페이지가 나타납니다.

3단계 왼쪽의 탐색 패널에서 **Settings**를 클릭합니다.

Settings 페이지가 나타납니다.

4단계 Application Layer Preprocessors 아래에서 **DNS Configuration**이 활성화되었는지 여부에 따라 두 가지 선택 사항이 있습니다.

- 컨피그레이션이 활성화되어 있으면 **Edit**를 클릭합니다.
- 컨피그레이션이 비활성화되어 있으면 **Enabled**를 클릭한 다음 **Edit**를 클릭합니다.

DNS Configuration(IP 컨피그레이션) 페이지가 나타납니다. 페이지 하단에 있는 메시지는 컨피그레이션이 포함된 네트워크 분석 정책 레이어를 식별합니다. 자세한 내용은 24-1페이지의 네트워크 분석 또는 침입 정책에서 레이어 사용을/를 참조하십시오.

5단계 선택적으로, Settings 영역에서 다음을 수정할 수 있습니다.

- DNS 프리프로세서가 DNS 서버 응답에 대해 모니터링해야 할 하나 이상의 소스 포트를 **Ports** 필드에 지정합니다. 포트가 여러 개인 경우 쉼표로 구분하십시오.
- RData 텍스트 필드에서 버퍼 오버플로 시도의 탐지를 활성화하려면 **Detect Overflow Attempts on RData Text fields** 확인란을 선택합니다.
- 오래된 리소스 레코드 유형의 탐지를 활성화하려면 **Detect Obsolete DNS RR Types** 확인란을 선택합니다.
- 실험적인 리소스 레코드 유형을 탐지하려면 **Detect Experimental DNS RR Types** 확인란을 선택합니다.

6단계 정책을 저장하거나, 계속 수정하거나, 변경 사항을 취소하거나, 기반 정책의 기본 컨피그레이션 설정으로 돌아가거나, 시스템 캐시에 변경 사항이 남아 있는 상태로 종료합니다. 자세한 내용은 23-15 페이지의 충돌 해결 및 정책 변경 사항 커밋을/를 참조하십시오.

FTP 및 텔넷 트래픽 디코딩

라이센스: 보호

FTP/Telnet 디코더는 FTP 및 텔넷 데이터 스트림을 분석하여, 규칙 엔진이 처리하기 전에 FTP 및 텔넷 명령을 표준화합니다.

GID(generator ID)가 125 또는 126인 FTP 및 텔넷 프리프로세서 규칙을 활성화해야 이러한 규칙에서 이벤트를 생성할 수 있습니다. 자세한 내용은 32-20페이지의 규칙 상태 설정을/를 참조하십시오.

자세한 내용은 다음 항목을 참조하십시오.

전역 FTP 및 텔넷 옵션

라이센스: 보호

FTP/Telnet 디코더가 패킷의 스테이트풀 또는 스테이트리스 검사를 수행할지 여부, 암호화된 FTP 또는 텔넷 세션을 탐지할지 여부, 그리고 암호화된 데이터를 발견한 후 데이터 스트림 검사를 계속할지 여부를 결정하는 전역 옵션을 설정할 수 있습니다.

다음 설명에서 프리프로세서 규칙이 언급되지 않은 경우 해당 옵션은 프리프로세서 규칙과 관련되지 않은 것입니다.

Stateful Inspection

이 옵션을 선택하면, FTP/Telnet 디코더는 상태를 저장하고 개별 패킷에 대한 세션 컨텍스트를 제공하며, 리어셈블된 세션만 검사합니다. 이 옵션을 선택하지 않으면, 세션 컨텍스트 없이 각 개별 패킷을 분석합니다.

FTP 데이터 전송을 검사하려면 이 옵션을 선택해야 합니다.

Detect Encrypted Traffic

암호화된 텔넷 및 FTP 세션을 탐지합니다.

이 옵션에 대한 이벤트를 생성하려면 규칙 125:7 및 126:2를 활성화할 수 있습니다. 자세한 내용은 32-20페이지의 규칙 상태 설정을/를 참조하십시오.

Continue to Inspect Encrypted Data

암호화된 후에도 데이터 스트림을 계속 검사하여 해독된 최종 데이터를 찾도록 프리프로세서에 지시합니다.

전역 FTP/Telnet 옵션 구성

라이센스: 보호

FTP/Telnet 디코더가 스테이트풀 또는 스테이트리스 검사를 수행할지 여부, 암호화된 트래픽을 탐지할지 여부, 그리고 암호화된 것으로 식별한 데이터 스트림에서 해독된 데이터를 계속 검사할지 여부를 제어하기 위한 전역 옵션을 구성해야 합니다. 전역 설정에 대한 자세한 내용은 27-18페이지의 전역 FTP 및 텔넷 옵션을/를 참조하십시오.

전역 옵션을 구성하려면

액세스: Admin/Intrusion Admin

1단계 **Policies > Access Control**을 선택하여 Access Control Policy 페이지를 표시한 다음 **Network Analysis Policy**를 클릭합니다.

Network Analysis Policy 페이지가 나타납니다.

2단계 수정할 정책 옆에 있는 수정 아이콘( )을 클릭합니다.

다른 정책에 저장하지 않은 변경 사항이 있는 경우 변경 사항을 취소하고 계속 진행하려면 **OK**를 클릭합니다. 저장되지 않은 변경 사항을 다른 정책에 저장하는 방법에 대한 자세한 내용은 23-15페이지의 충돌 해결 및 정책 변경 사항 커밋을/를 참조하십시오.

Policy Information 페이지가 나타납니다.

3단계 왼쪽의 탐색 패널에서 **Settings**를 클릭합니다.

Settings 페이지가 나타납니다.

Advanced Settings 페이지가 나타납니다.

4단계 Application Layer Preprocessors 아래에서 **FTP and Telnet Configuration**이 활성화되었는지 여부에 따라 두 가지 선택 사항이 있습니다.

- 컨피그레이션이 활성화되어 있으면 **Edit**를 클릭합니다.
- 컨피그레이션이 비활성화되어 있으면 **Enabled**를 클릭한 다음 **Edit**를 클릭합니다.

FTP and Telnet Configuration 페이지가 나타납니다.

페이지 하단에 있는 메시지는 컨피그레이션이 포함된 네트워크 분석 정책 레이어를 식별합니다. 자세한 내용은 24-1페이지의 네트워크 분석 또는 침입 정책에서 레이어 사용을/를 참조하십시오.

팁 이 페이지의 다른 옵션 구성에 대한 자세한 내용은 27-21페이지의 텔넷 옵션 구성, 27-25페이지의 서버 레벨 FTP 옵션 구성 및 27-28페이지의 클라이언트 레벨 FTP 옵션 구성을/를 참조하십시오.

5단계 선택적으로, Global Settings 페이지 영역에서 다음을 수정할 수 있습니다.

- FTP 패킷을 포함하는 리어셈블된 TCP 스트림을 검사하려면 **Stateful Inspection**을 선택합니다. 리어셈블되지 않은 패킷만 검사하려면 **Stateful Inspection**의 선택을 취소합니다.
- 암호화된 트래픽을 탐지하려면 **Detect Encrypted Traffic**을 선택합니다. 암호화된 트래픽을 무시하려면 **Detect Encrypted Traffic**의 선택을 취소합니다.
- 필요한 경우, 암호화된 후에도 스트림을 계속 검사하려면 **Continue to Inspect Encrypted Data**를 선택합니다. 이 경우 스트림은 다시 해독되고 계속 처리할 수 있게 됩니다.

6단계 정책을 저장하거나, 계속 수정하거나, 변경 사항을 취소하거나, 기반 정책의 기본 컨피그레이션 설정으로 돌아가거나, 시스템 캐시에 변경 사항이 남아 있는 상태로 종료합니다. 자세한 내용은 23-15페이지의 충돌 해결 및 정책 변경 사항 커밋을/를 참조하십시오.

텔넷 옵션 이해

라이센스: 보호

FTP/Telnet 디코더에 의한 텔넷 명령의 표준화를 활성화 또는 비활성화하고, 특정 변칙 사례를 활성화 또는 비활성화하고, 허용할 AYT(Are You There) 공격의 임계값 수를 설정할 수 있습니다.

다음 설명에서 프리프로세서 규칙이 언급되지 않은 경우 해당 옵션은 프리프로세서 규칙과 관련되지 않은 것입니다.

Ports

텔넷 트래픽을 표준화할 포트를 나타냅니다. 인터페이스에서 여러 포트를 쉼표로 구분하여 나열합니다.

Normalize

텔넷 트래픽을 지정된 포트로 표준화합니다.

Detect Anomalies

해당 SE(subnegotiation end)가 없는 Telnet SB(subnegotiation begin)의 탐지를 활성화합니다.

텔넷은 subnegotiation을 지원하는데, subnegotiation은 SB(subnegotiation begin)로 시작하며 SE(subnegotiation end)로 끝나야 합니다. 그러나 텔넷 서버의 특정 구현에서는 해당 SE가 없는 SB를 무시합니다. 이는 회피 사례라고 할 수 있는 이상 행동입니다. FTP는 제어 연결에서 텔넷 프로토콜을 사용하므로 이러한 행동을 의심합니다.

텔넷 트래픽에서 이러한 변칙이 탐지될 때 이벤트를 생성하려면 규칙 126:3을 활성화하고, FTP 명령 채널에서 탐지될 때 이벤트를 생성하려면 규칙 125:9를 활성화할 수 있습니다. 자세한 내용은 32-20페이지의 규칙 상태 설정을/를 참조하십시오.

Are You There Attack Threshold Number

연속 AYT 명령 수가 지정된 임계값을 초과하는 경우를 탐지합니다. Cisco에서는 AYT 임계값을 20보다 크게 설정하지 않을 것을 권장합니다.

이 옵션에 대한 이벤트를 생성하려면 규칙 126:1을 활성화할 수 있습니다. 자세한 내용은 32-20페이지의 규칙 상태 설정을/를 참조하십시오.

텔넷 옵션 구성

라이센스: 보호

표준화를 활성화 또는 비활성화하고, 특정 변칙 사례를 활성화 또는 비활성화하고, 허용할 AYT(Are You There) 공격의 임계값 수를 제어할 수 있습니다. 텔넷 옵션에 대한 자세한 내용은 27-20페이지의 텔넷 옵션 이해을/를 참조하십시오.

텔넷 옵션을 구성하려면

액세스: Admin/Intrusion Admin

1단계 **Policies > Access Control**을 선택하여 Access Control Policy 페이지를 표시한 다음 **Network Analysis Policy**를 클릭합니다.

Network Analysis Policy 페이지가 나타납니다.

2단계 수정할 정책 옆에 있는 수정 아이콘()을 클릭합니다.

다른 정책에 저장하지 않은 변경 사항이 있는 경우 변경 사항을 취소하고 계속 진행하려면 **OK**를 클릭합니다. 저장되지 않은 변경 사항을 다른 정책에 저장하는 방법에 대한 자세한 내용은 23-15페이지의 충돌 해결 및 정책 변경 사항 커밋을/를 참조하십시오.

Policy Information 페이지가 나타납니다.

3단계 왼쪽의 탐색 패널에서 **Settings**를 클릭합니다.

Settings 페이지가 나타납니다.

4단계 Application Layer Preprocessors 아래에서 **FTP and Telnet Configuration**이 활성화되었는지 여부에 따라 두 가지 선택 사항이 있습니다.

- 컨피그레이션이 활성화되어 있으면 **Edit**를 클릭합니다.
- 컨피그레이션이 비활성화되어 있으면 **Enabled**를 클릭한 다음 **Edit**를 클릭합니다.

FTP and Telnet Configuration 페이지가 나타납니다.

페이지 하단에 있는 메시지는 컨피그레이션이 포함된 네트워크 분석 정책 레이어를 식별합니다. 자세한 내용은 24-1페이지의 네트워크 분석 또는 침입 정책에서 레이어 사용을/를 참조하십시오.

팁 이 페이지의 다른 옵션 구성에 대한 자세한 내용은 27-19페이지의 전역 FTP/Telnet 옵션 구성, 27-25페이지의 서버 레벨 FTP 옵션 구성 및 27-28페이지의 클라이언트 레벨 FTP 옵션 구성을/를 참조하십시오.

5단계 선택적으로, Telnet Settings 페이지 영역에서 다음을 수정할 수 있습니다.

- 텔넷 트래픽을 디코딩해야 할 포트를 **Ports** 필드에 지정합니다. 텔넷은 일반적으로 TCP 포트 23에 연결됩니다. 포트가 여러 개인 경우 쉼표로 구분하십시오.

주의 암호화된 트래픽(SSL)은 디코딩할 수 없으므로 포트 22(SSH)를 추가하면 예기치 못한 결과가 발생할 수 있습니다.

- 텔넷 표준화를 활성화 또는 비활성화하려면 **Normalize** 텔넷 프로토콜 옵션을 선택하거나 선택 취소합니다.
- 변칙 탐지를 활성화 또는 비활성화하려면 **Detect Anomalies** 텔넷 프로토콜 옵션을 선택하거나 선택 취소합니다.
- 허용할 연속 AYT 명령의 **Are You There Attack Threshold Number**를 지정합니다.

팁 Cisco에서는 AYT 임계값을 기본값보다 크게 설정하지 않을 것을 권장합니다.

6단계 정책을 저장하거나, 계속 수정하거나, 변경 사항을 취소하거나, 기반 정책의 기본 컨피그레이션 설정으로 돌아가거나, 시스템 캐시에 변경 사항이 남아 있는 상태로 종료합니다. 자세한 내용은 23-15 페이지의 충돌 해결 및 정책 변경 사항 커밋을/를 참조하십시오.

서버 레벨 FTP 옵션 이해

라이센스: 보호

여러 FTP 서버를 디코딩하기 위한 옵션을 설정할 수 있습니다. 생성하는 각 서버 프로필에는 트래픽을 모니터링해야 할 서버의 서버 IP 주소 및 포트가 포함됩니다. 특정 서버에 대해 어떤 FTP 명령을 검증하고 어떤 것을 무시할지를 지정할 수 있으며 명령의 최대 매개 변수 길이를 설정할 수 있습니다. 디코더가 특정 명령에 대해 검증해야 할 특정 명령 구문 및 대체 최대 명령 매개 변수 길이를 설정할 수 있습니다.

다음 설명에서 프리프로세서 규칙이 언급되지 않은 경우 해당 옵션은 프리프로세서 규칙과 관련되지 않은 것입니다.

Networks

FTP 서버의 IP 주소를 하나 이상 지정하려면 이 옵션을 사용합니다.

단일 IP 주소나 주소 블록 또는 쉼표로 구분된 목록을 지정할 수 있습니다(둘 중 하나 또는 모두로 구성). 최대 1024자를 지정할 수 있으며, 기본 프로필을 포함하여 최대 255개의 프로필을 구성할 수 있습니다. FireSIGHT 시스템에서 IPv4 및 IPv6 주소 블록을 사용하는 방법에 대한 자세한 내용은 1-19페이지의 IP 주소 표기 규칙을/를 참조하십시오.

기본 정책의 `default` 설정은 다른 대상 기반 정책에서 처리되지 않는 모니터링되는 네트워크 세그먼트의 모든 IP 주소를 지정합니다. 따라서 기본 정책에 대해서는 IP 주소 또는 주소 블록을 지정할 수 없고 지정할 필요도 없으며, 다른 정책에서 이 설정을 비워둘 수 없거나 `any`를 나타내는 주소 표기법(예: 0.0.0.0/0 또는 ::/0)을 사용할 수 없습니다.

또한 트래픽 처리를 위한 대상 기반 정책의 경우, 식별하는 네트워크는 대상 기반 정책을 구성하는 네트워크 분석 정책에서 처리되는 네트워크, 영역, VLAN의 하위 집합과 일치하거나 하위 집합이어야 합니다. 자세한 내용은 25-3페이지의 네트워크 분석 정책으로 전처리 맞춤화을/를 참조하십시오.

Ports

관리되는 디바이스가 트래픽을 모니터링해야 할 FTP 서버의 포트를 지정하려면 이 옵션을 사용합니다. 인터페이스에서 여러 포트를 쉼표로 구분하여 나열합니다.

File Get Commands

서버에서 클라이언트로 파일을 전송하는 데 사용할 FTP 명령을 정의하려면 이 옵션을 사용합니다. 고객 지원의 지침 없이는 이러한 값을 변경하지 마십시오.

File Put Commands

클라이언트에서 서버로 파일을 전송하는 데 사용할 FTP 명령을 정의하려면 이 옵션을 사용합니다. 고객 지원의 지침 없이는 이러한 값을 변경하지 마십시오.

Additional FTP Commands

디코더가 탐지해야 할 추가 명령을 지정하려면 이 줄을 사용합니다. 추가 명령은 공백으로 구분하십시오.

Default Max Parameter Length

대체 최대 매개 변수 길이를 설정하지 않은 경우 명령의 최대 매개 변수 길이를 탐지하려면 이 옵션을 사용합니다.

이 옵션에 대한 이벤트를 생성하려면 규칙 125:3을 활성화할 수 있습니다. 자세한 내용은 32-20 페이지의 규칙 상태 설정을/를 참조하십시오.

Alternate Max Parameter Length

다른 최대 매개 변수 길이를 탐지하려는 경우 명령을 지정하고 그러한 명령의 최대 매개 변수 길이를 지정하려면 이 옵션을 사용합니다. 특별한 명령에 대해 탐지하기 위해 다른 최대 매개 변수 길이를 지정하려는 경우 줄을 추가하려면 **Add**를 클릭합니다.

Check Commands for String Format Attacks

문자열 형식 공격에 대해 지정된 명령을 검사하려면 이 옵션을 사용합니다.

이 옵션에 대한 이벤트를 생성하려면 규칙 125:5를 활성화할 수 있습니다. 자세한 내용은 32-20 페이지의 규칙 상태 설정을/를 참조하십시오.

Command Validity

특정 명령에 대해 유효한 형식을 입력하려면 이 옵션을 사용합니다. FTP 통신의 일부로 수신한 매개 변수의 구문을 검증하기 위한 FTP 명령 매개 변수 검증 문을 생성하는 방법에 대한 자세한 내용은 27-24페이지의 FTP 명령 매개 변수 검증 문 생성을/를 참조하십시오. 명령 검증 줄을 추가하려면 **Add**를 클릭합니다.

이 옵션에 대한 이벤트를 생성하려면 규칙 125:2 및 125:4를 활성화할 수 있습니다. 자세한 내용은 32-20페이지의 규칙 상태 설정을/를 참조하십시오.

Ignore FTP Transfers

데이터 전송 채널에 대한 상태 검사 외의 모든 검사를 비활성화함으로써 FTP 데이터 전송의 성능을 개선하려면 이 옵션을 사용합니다.

Detect Telnet Escape Codes within FTP Commands

Telnet 명령이 FTP 명령 채널을 통해 사용되는 경우를 탐지하려면 이 옵션을 사용합니다.

이 옵션에 대한 이벤트를 생성하려면 규칙 125:1을 활성화할 수 있습니다. 자세한 내용은 32-20 페이지의 규칙 상태 설정을/를 참조하십시오.

Ignore Erase Commands during Normalization

Detect Telnet Escape Codes within FTP Commands를 선택한 경우 FTP 트래픽을 표준화할 때 텔넷 문자 및 줄 지우기 명령을 무시하려면 이 옵션을 사용합니다. 이 설정은 FTP 서버가 텔넷 지우기 명령을 처리하는 방법과 일치해야 합니다. 좀 더 이전 FTP 서버는 일반적으로 텔넷 지우기 명령을 처리하는 반면 좀 더 최신 FTP 서버는 이러한 명령을 무시합니다.

Troubleshooting Options: Log FTP Command Validation Configuration

고객 지원에서 문제 해결 통화 중에 서버에 대해 나열된 각 FTP 명령에 대한 컨피그레이션 정보를 인쇄하도록 시스템을 구성하라고 요청할 수 있습니다.

주의 이 문제 해결 옵션에 대한 설정의 변경은 고객 지원의 지침에 의해서만 수행할 수 있으며 성능에 영향을 미치게 됩니다.

FTP 명령 매개 변수 검증 문 생성

라이센스: 보호

FTP 명령에 대한 검증 문을 설정할 때 공백으로 매개 변수를 구분하여 대체 매개 변수의 그룹을 지정할 수 있습니다. 검증 문에서 파이프 문자(|)로 구분하여 두 매개 변수 간 이진 OR 관계를 생성할 수도 있습니다. 대괄호([])로 감싼 매개 변수는 해당 매개 변수가 선택 사항임을 나타냅니다. 중괄호({})로 감싼 매개 변수는 해당 매개 변수가 필수임을 나타냅니다.

FTP 통신의 일부로 수신한 매개 변수의 구문을 검증하기 위한 FTP 명령 매개 변수 검증 문을 생성할 수 있습니다. 자세한 내용은 27-22페이지의 서버 레벨 FTP 옵션 이해을/를 참조하십시오.

다음 표에 나열된 매개 변수는 FTP 명령 매개 변수 검증 문에 사용할 수 있습니다.

표 27-5 FTP 명령 매개 변수

매개 변수	검증 내용
`int`	표시되는 매개 변수는 정수여야 합니다.
`number`	표시되는 매개 변수는 1과 255 사이의 정수여야 합니다.
`char` *`_chars`*	표시되는 매개 변수는 단일 문자이며 *`_chars`* 인수에 지정된 문자의 멤버여야 합니다. 예를 들어 검증 문 `char` *`SBC`*로 `MODE`의 명령 유효성을 정의하면 `MODE` 명령에 대한 매개 변수가 `S`(Stream 모드를 나타냄), `B`(Block 모드를 나타냄) 또는 `C`(Compressed 모드를 나타냄) 문자로 구성되어 있는지에 대한 검사가 수행됩니다.
`date` *`_datefmt`*	*`_datefmt`*에 `#`이 포함된 경우 표시되는 매개 변수는 숫자여야 합니다. *`_datefmt`*에 `C`가 포함된 경우 표시되는 매개 변수는 문자여야 합니다. *`_datefmt`*에 리터럴 문자열이 포함된 경우 표시되는 매개 변수는 리터럴 문자열과 일치해야 합니다.
`문자열`	표시되는 매개 변수는 문자열이어야 합니다.
`host_port`	표시되는 매개 변수는 Network Working Group의 File Transfer Protocol 사양인 RFC 959에 정의된 대로, 유효한 호스트 포트 지정자여야 합니다.

필요에 따라 위의 표에 있는 구문을 결합하여 트래픽 검증이 필요할 때 각 FTP 명령을 올바르게 확인하는 매개 변수 검증 문을 생성할 수 있습니다.

참고 TYPE 명령에 복잡한 식을 포함하는 경우 공백으로 감싸십시오. 또한 식 내에서 각 연산자를 공백으로 감싸십시오. 예를 들면 `char A|B`가 아니라 `char A | B`를 입력하십시오.

서버 레벨 FTP 옵션 구성

라이센스: 보호

서버 레벨에서 여러 옵션을 구성할 수 있습니다. 추가하는 각 FTP 서버에 대해 모니터링할 포트, 검증할 명령, 명령의 기본 최대 매개 변수 길이, 특정 명령의 대체 매개 변수 길이, 특정 명령의 검증 구문 등을 지정할 수 있습니다. 또한 FTP 채널에서 문자열 형식 공격 및 텔넷 명령의 확인 여부, 그리고 각 명령에서 컨피그레이션 정보를 인쇄할지 여부를 선택할 수 있습니다. 서버 레벨 FTP 옵션에 대한 자세한 내용은 27-22페이지의 서버 레벨 FTP 옵션 이해을/를 참조하십시오.

서버 레벨 FTP 옵션을 구성하려면

액세스: Admin/Intrusion Admin

1단계 **Policies > Access Control**을 선택하여 Access Control Policy 페이지를 표시한 다음 **Network Analysis Policy**를 클릭합니다.

Network Analysis Policy 페이지가 나타납니다.

2단계 수정할 정책 옆에 있는 수정 아이콘()을 클릭합니다.

다른 정책에 저장하지 않은 변경 사항이 있는 경우 변경 사항을 취소하고 계속 진행하려면 **OK**를 클릭합니다. 저장되지 않은 변경 사항을 다른 정책에 저장하는 방법에 대한 자세한 내용은 23-15페이지의 충돌 해결 및 정책 변경 사항 커밋을/를 참조하십시오.

Policy Information 페이지가 나타납니다.

3단계 왼쪽의 탐색 패널에서 **Settings**를 클릭합니다.

Settings 페이지가 나타납니다.

4단계 Application Layer Preprocessors 아래에서 **FTP and Telnet Configuration**이 활성화되었는지 여부에 따라 두 가지 선택 사항이 있습니다.

- 컨피그레이션이 활성화되어 있으면 **Edit**를 클릭합니다.
- 컨피그레이션이 비활성화되어 있으면 **Enabled**를 클릭한 다음 **Edit**를 클릭합니다.

FTP and Telnet Configuration 페이지가 나타납니다.

페이지 하단에 있는 메시지는 컨피그레이션이 포함된 네트워크 분석 정책 레이어를 식별합니다. 자세한 내용은 24-1페이지의 네트워크 분석 또는 침입 정책에서 레이어 사용을/를 참조하십시오.

팁 이 페이지의 다른 옵션 구성에 대한 자세한 내용은 27-19페이지의 전역 FTP/Telnet 옵션 구성, 27-21페이지의 텔넷 옵션 구성 및 27-28페이지의 클라이언트 레벨 FTP 옵션 구성을/를 참조하십시오.

5단계 다음 2가지 옵션을 사용할 수 있습니다.

- 새 서버 프로필을 추가합니다. 페이지 왼쪽의 **FTP Server** 옆에 있는 추가 아이콘()을 클릭합니다. Add Target 팝업 창이 나타납니다. **Server Address** 필드에서 클라이언트에 대한 하나 이상의 IP 주소를 지정하고 **OK**를 클릭합니다.

  단일 IP 주소나 주소 블록 또는 쉼표로 구분된 목록을 지정할 수 있습니다(둘 중 하나 또는 모두). 최대 1024자를 지정할 수 있으며, 기본 정책을 포함하여 최대 255개의 정책을 구성할 수 있습니다. FireSIGHT 시스템에서 IPv4 및 IPv6 주소 블록을 사용하는 방법에 대한 자세한 내용은 1-19페이지의 IP 주소 표기 규칙을/를 참조하십시오.

트래픽 처리를 위한 대상 기반 정책의 경우, 식별하는 네트워크는 대상 기반 정책을 구성하는 네트워크 분석 정책에서 처리되는 네트워크, 영역, VLAN의 하위 집합과 일치하거나 하위 집합이어야 합니다. 자세한 내용은 25-3페이지의 네트워크 분석 정책으로 전처리 맞춤화을/를 참조하십시오.

새 항목이 페이지 왼쪽의 FTP 서버 목록에 나타나서 선택된 것을 알 수 있도록 강조 표시되며, 추가한 프로필에 대한 현재 컨피그레이션을 반영하여 Configuration 섹션이 업데이트됩니다.

- 기존의 서버 프로필에 대한 설정을 수정합니다. 페이지 왼쪽의 **FTP Server** 아래에서 추가한 프로필에 대해 구성된 주소를 클릭하거나 **default**를 클릭합니다.

  선택 항목이 강조 표시되고, 선택한 프로필에 대한 현재 컨피그레이션을 표시하기 위해 Configuration 섹션이 업데이트됩니다. 기존의 프로필을 삭제하려면 제거할 프로필 옆에 있는 삭제 아이콘( )을 클릭합니다.

6단계 선택적으로, Configuration 페이지 영역에서 다음을 수정할 수 있습니다.

- **Networks** 필드에 나열된 주소를 수정하고 페이지의 다른 영역을 클릭합니다.

  페이지의 왼쪽에서 강조 표시된 주소가 업데이트됩니다.

  기본 프로필에서는 **Network**에 대한 설정을 수정할 수 없습니다. 기본 프로필은 다른 프로필에서 식별되지 않는 네트워크의 모든 서버에 적용됩니다.

- FTP 트래픽을 모니터링할 **Ports**를 지정합니다. Port 21은 잘 알려진 FTP 트래픽용 포트입니다.
- 서버에서 클라이언트로의 파일 전송에 사용되는 FTP 명령을 **File Get Commands** 필드에서 업데이트합니다.
- 클라이언트에서 서버로의 파일 전송에 사용되는 FTP 명령을 **File Put Commands** 필드에서 업데이트합니다.

참고 고객 지원의 지침 없이는 **File Get Commands** 및 **File Put Commands** 필드의 값을 변경하지 마십시오.

- FTP/Telnet 프리프로세서에서 기본적으로 확인하는 명령 외 추가 FTP 명령을 탐지하려면, 공백으로 구분하여 **Additional FTP Commands** 필드에 명령을 입력합니다.

  기타 FTP 명령을 필요한 만큼 추가할 수 있습니다.

참고 추가할 수 있는 기타 명령에는 `XPWD`, `XCWD`, `XCUP`, `XMKD` 및 `XRMD`가 포함됩니다. 이러한 명령에 대한 자세한 내용은 Network Working Group의 Directory oriented FTP 명령 사양인 RFC 775을/를 참조하십시오.

- 명령 매개 변수에 대한 기본 최대 바이트 수를 **Default Max Parameter Length** 필드에 지정합니다.
- 특정 명령에 대해 다른 최대 매개 변수 길이를 탐지하려면 **Alternate Max Parameter Length** 옆에 있는 **Add**를 클릭합니다. 나타나는 첫 번째 행 텍스트 상자에 최대 매개 변수 길이를 지정합니다. 두 번째 텍스트 상자에, 이 대체 최대 매개 변수 길이를 적용해야 할 명령을 공백으로 구분하여 지정합니다.

  대체 최대 매개 변수 길이를 필요한 만큼 추가할 수 있습니다.

- 특정 명령에 대한 문자열 형식 공격을 확인하려면 명령을 공백으로 구분하여 **Check Commands for String Format Attacks** 텍스트 상자에 지정합니다.
- 명령에 대한 유효한 형식을 지정하려면 **Command Validity** 옆에 있는 **Add**를 클릭합니다. 검증할 명령을 지정한 다음 명령 매개 변수에 대한 검증 문을 입력합니다. 검증 문 구문에 대한 자세한 내용은 27-22페이지의 서버 레벨 FTP 옵션 이해을/를 참조하십시오.

- 데이터 전송 채널에 대한 상태 검사 외의 모든 검사를 비활성화함으로써 FTP 데이터 전송의 성능을 개선하려면 **Ignore FTP Transfers**를 활성화합니다.

참고 데이터 전송을 검사하려면 전역 FTP/Telnet **Stateful Inspection** 옵션을 선택해야 합니다. 전역 옵션 설정에 대한 자세한 내용은 27-18페이지의 전역 FTP 및 텔넷 옵션을/를 참조하십시오.

- 텔넷 명령이 FTP 명령 채널을 통해 사용되는 경우를 탐지하려면 **Detect Telnet Escape Codes within FTP Commands**를 선택합니다.
- FTP 트래픽을 표준화할 때 텔넷 문자 및 줄 지우기 명령을 무시하려면 **Ignore Erase Commands during Normalization**을 활성화합니다.

7단계 선택적으로, 고객 지원에서 요청하는 경우에만 관련 문제 해결 옵션을 수정합니다. **Troubleshooting Options** 옆에 있는 **+** 기호를 클릭하여 문제 해결 옵션 섹션을 확장합니다.

8단계 정책을 저장하거나, 계속 수정하거나, 변경 사항을 취소하거나, 기반 정책의 기본 컨피그레이션 설정으로 돌아가거나, 시스템 캐시에 변경 사항이 남아 있는 상태로 종료합니다. 자세한 내용은 23-15페이지의 충돌 해결 및 정책 변경 사항 커밋을/를 참조하십시오.

클라이언트 레벨 FTP 옵션 이해

라이센스: 보호

FTP 클라이언트용 프로필을 생성할 수 있습니다. 각 프로필 내에서, 클라이언트의 FTP 응답에 대한 최대 응답 길이를 지정할 수 있습니다. 또한 특정 클라이언트에 대해 FTP 명령 채널에서 바운스 공격 및 텔넷 명령 사용을 탐지할지 여부를 구성할 수 있습니다.

다음 설명에서 프리프로세서 규칙이 언급되지 않은 경우 해당 옵션은 프리프로세서 규칙과 관련되지 않은 것입니다.

Networks

FTP 클라이언트의 IP 주소를 하나 이상 지정하려면 이 옵션을 사용합니다.

단일 IP 주소나 주소 블록 또는 쉼표로 구분된 목록을 지정할 수 있습니다(둘 중 하나 또는 모두로 구성). 최대 1024자를 지정할 수 있으며, 기본 프로필을 포함하여 최대 255개의 프로필을 지정할 수 있습니다. FireSIGHT 시스템에서 IPv4 및 IPv6 주소 블록을 사용하는 방법에 대한 자세한 내용은 1-19페이지의 IP 주소 표기 규칙을/를 참조하십시오.

기본 정책의 `default` 설정은 다른 대상 기반 정책에서 처리되지 않는 모니터링되는 네트워크 세그먼트의 모든 IP 주소를 지정합니다. 따라서 기본 정책에 대해서는 IP 주소 또는 주소 블록을 지정할 수 없고 지정할 필요도 없으며, 다른 정책에서 이 설정을 비워둘 수 없거나 `any`를 나타내는 주소 표기법(예: 0.0.0.0/0 또는 ::/0)을 사용할 수 없습니다.

또한 트래픽 처리를 위한 대상 기반 정책의 경우, 식별하는 네트워크는 대상 기반 정책을 구성하는 네트워크 분석 정책에서 처리되는 네트워크, 영역, VLAN의 하위 집합과 일치하거나 하위 집합이어야 합니다. 자세한 내용은 25-3페이지의 네트워크 분석 정책으로 전처리 맞춤화을/를 참조하십시오.

Max Response Length

FTP 클라이언트에서 응답 문자열의 최대 길이를 지정하려면 이 옵션을 사용합니다.

이 옵션에 대한 이벤트를 생성하려면 규칙 125:6을 활성화할 수 있습니다. 자세한 내용은 32-20페이지의 규칙 상태 설정을/를 참조하십시오.

Detect FTP Bounce Attempts

FTP 바운스 공격을 탐지하려면 이 옵션을 사용합니다.

이 옵션에 대한 이벤트를 생성하려면 규칙 125:8을 활성화할 수 있습니다. 자세한 내용은 32-20 페이지의 규칙 상태 설정을/를 참조하십시오.

Allow FTP Bounce to

FTP PORT 명령을 FTP 바운스 공격으로 취급해서는 안 되는 추가 호스트 및 그러한 호스트의 포트 목록을 구성하려면 이 옵션을 사용합니다.

Detect Telnet Escape Codes within FTP Commands

Telnet 명령이 FTP 명령 채널을 통해 사용되는 경우를 탐지하려면 이 옵션을 사용합니다.

이 옵션에 대한 이벤트를 생성하려면 규칙 125:1을 활성화할 수 있습니다. 자세한 내용은 32-20 페이지의 규칙 상태 설정을/를 참조하십시오.

Ignore Erase Commands During Normalization

Detect Telnet Escape Codes within FTP Commands를 선택한 경우 FTP 트래픽을 표준화할 때 텔넷 문자 및 줄 지우기 명령을 무시하려면 이 옵션을 사용합니다. 이 설정은 FTP 클라이언트가 텔넷 지우기 명령을 처리하는 방법과 일치해야 합니다. 좀 더 이전 FTP 클라이언트는 일반적으로 텔넷 지우기 명령을 처리하는 반면 좀 더 최신 FTP 클라이언트는 이러한 명령을 무시합니다.

클라이언트 레벨 FTP 옵션 구성

라이센스: 보호

FTP 클라이언트가 클라이언트의 FTP 트래픽을 모니터링하도록 클라이언트 프로필을 구성할 수 있습니다. 클라이언트 모니터링에 대해 설정할 수 있는 옵션에 대한 자세한 내용은 27-27페이지의 클라이언트 레벨 FTP 옵션 이해을/를 참조하십시오. 텔넷 옵션에 대한 자세한 내용은 27-20페이지의 텔넷 옵션 이해을/를 참조하십시오. 추가 FTP 옵션에 대한 자세한 내용은 27-22페이지의 서버 레벨 FTP 옵션 이해 및 27-18페이지의 전역 FTP 및 텔넷 옵션을/를 참조하십시오.

클라이언트 레벨 FTP 옵션을 구성하려면

액세스: Admin/Intrusion Admin

1단계 **Policies > Access Control**을 선택하여 Access Control Policy 페이지를 표시한 다음 **Network Analysis Policy**를 클릭합니다.

Network Analysis Policy 페이지가 나타납니다.

2단계 수정할 정책 옆에 있는 수정 아이콘( )을 클릭합니다.

다른 정책에 저장하지 않은 변경 사항이 있는 경우 변경 사항을 취소하고 계속 진행하려면 **OK**를 클릭합니다. 저장되지 않은 변경 사항을 다른 정책에 저장하는 방법에 대한 자세한 내용은 23-15페이지의 충돌 해결 및 정책 변경 사항 커밋을/를 참조하십시오.

Policy Information 페이지가 나타납니다.

3단계 왼쪽의 탐색 패널에서 **Settings**를 클릭합니다.

Settings 페이지가 나타납니다.

4단계 Application Layer Preprocessors 아래에서 **FTP and Telnet Configuration**이 활성화되었는지 여부에 따라 두 가지 선택 사항이 있습니다.

- 컨피그레이션이 활성화되어 있으면 **Edit**를 클릭합니다.
- 컨피그레이션이 비활성화되어 있으면 **Enabled**를 클릭한 다음 **Edit**를 클릭합니다.

FTP and Telnet Configuration 페이지가 나타납니다.

5단계 다음 2가지 옵션을 사용할 수 있습니다.

- 새 클라이언트 프로필을 추가합니다. 페이지 왼쪽의 **FTP Client** 옆에 있는 추가 아이콘( )을 클릭합니다. Add Target 팝업 창이 나타납니다. **Client Address** 필드에서 클라이언트에 대한 하나 이상의 IP 주소를 지정하고 **OK**를 클릭합니다.

  단일 IP 주소나 주소 블록 또는 쉼표로 구분된 목록을 지정할 수 있습니다(둘 중 하나 또는 모두). 최대 1024자를 지정할 수 있으며, 기본 정책을 포함하여 최대 255개의 정책을 구성할 수 있습니다. FireSIGHT 시스템에서 IPv4 및 IPv6 주소 블록을 사용하는 방법에 대한 자세한 내용은 1-19페이지의 IP 주소 표기 규칙을/를 참조하십시오.

  트래픽 처리를 위한 대상 기반 정책의 경우, 식별하는 네트워크는 대상 기반 정책을 구성하는 네트워크 분석 정책에서 처리되는 네트워크, 영역, VLAN의 하위 집합과 일치하거나 하위 집합이어야 합니다. 자세한 내용은 25-3페이지의 네트워크 분석 정책으로 전처리 맞춤화을/를 참조하십시오.

  새 항목이 페이지 왼쪽의 FTP 클라이언트 목록에 나타나서 선택된 것을 알 수 있도록 강조 표시되며, 추가한 프로필에 대한 현재 컨피그레이션을 반영하여 Configuration 섹션이 업데이트됩니다.

- 기존의 클라이언트 프로필에 대한 설정을 수정합니다. 페이지 왼쪽의 **FTP Client** 아래에서 추가한 프로필에 대해 구성된 주소를 클릭하거나 **default**를 클릭합니다.

  선택 항목이 강조 표시되고, 선택한 프로필에 대한 현재 컨피그레이션을 표시하기 위해 Configuration 섹션이 업데이트됩니다. 기존의 프로필을 삭제하려면 제거할 프로필 옆에 있는 삭제 아이콘( )을 클릭합니다.

6단계 선택적으로, Configuration 페이지 영역에서 다음을 수정할 수 있습니다.

- 선택적으로, **Networks** 필드에 나열된 주소를 수정하고 페이지의 다른 영역을 클릭합니다.

  페이지의 왼쪽에서 강조 표시된 주소가 업데이트됩니다.

  기본 프로필에서는 **Network**에 대한 설정을 수정할 수 없습니다. 기본 프로필은 다른 프로필에서 식별되지 않는 네트워크의 모든 클라이언트 호스트에 적용됩니다.

- FTP 클라이언트에서 오는 응답의 최대 길이를 **Max Response Length** 필드에 바이트 단위로 지정합니다.

- FTP 바운스 공격을 탐지하려면 **Detect FTP Bounce attempts**를 선택합니다.

  FTP/Telnet 디코더는 FTP PORT 명령이 실행되는 경우를 탐지하며, 지정된 호스트는 클라이언트의 지정된 호스트를 매칭하지 않습니다.

- FTP PORT 명령을 FTP 바운스 공격으로 취급해서는 안 되는 추가 호스트 및 포트의 목록을 구성하려면 각 호스트(또는 CIDR 형식의 네트워크)와 콜론(:) 그리고 포트 또는 포트 범위를 **Allow FTP Bounce to** 필드에 지정합니다. 호스트에 대한 포트 범위를 입력하려면 범위의 시작 포트와 끝 포트를 대시(-)로 구분합니다. 호스트에 대한 항목을 쉼표로 구분하여 여러 호스트를 입력할 수 있습니다.

  예를 들어 FTP PORT 명령을 포트 21에서 호스트 192.168.1.1로 전달하고, 22에서 1024의 임의의 포트에서 호스트 192.168.1.2로 전달하려면 다음을 입력합니다.

  ```
  192.168.1.1:21, 192.168.1.2:22-1024
  ```

  FireSIGHT 시스템에서 CIDR 표기법 및 접두사 길이를 사용하는 방법에 대한 자세한 내용은 1-19페이지의 IP 주소 표기 규칙을/를 참조하십시오.

참고 한 호스트에 대해 여러 개별 포트를 지정하려면 각 포트 정의에 대해 호스트 IP 주소를 반복해야 합니다. 예를 들어 192.168.1.1에서 포트 22와 25를 지정하려면 `192.168.1.1:22, 192.168.1.1:25`를 입력합니다.

- 텔넷 명령이 FTP 명령 채널을 통해 사용되는 경우를 탐지하려면 **Detect Telnet Escape Codes within FTP Commands**를 선택합니다.
- FTP 트래픽을 표준화할 때 텔넷 문자 및 줄 지우기 명령을 무시하려면 **Ignore Erase Commands During Normalization**을 선택합니다.

7단계 정책을 저장하거나, 계속 수정하거나, 변경 사항을 취소하거나, 기반 정책의 기본 컨피그레이션 설정으로 돌아가거나, 시스템 캐시에 변경 사항이 남아 있는 상태로 종료합니다. 자세한 내용은 23-15 페이지의 충돌 해결 및 정책 변경 사항 커밋을/를 참조하십시오.

HTTP 트래픽 디코딩

라이센스: 보호

HTTP Inspect 프리프로세서는 다음을 수행합니다.

- 네트워크의 웹 서버로 전송되는 HTTP 요청 및 웹 서버에서 수신하는 HTTP 응답을 디코딩 및 표준화
- HTTP 관련 침입 규칙의 성능 향상을 위해 웹 서버로 전송되는 메시지를 URI, 비 쿠키 헤더, 쿠키 헤더 및 메시지 본문 구성 요소로 구분
- HTTP 관련 침입 규칙의 성능 향상을 위해 웹 서버에서 수신되는 메시지를 상태 코드, 상태 메시지, non-set-cookie 헤더, 쿠키 헤더 및 응답 본문 구성 요소로 구분
- URI 인코딩 공격 가능성 탐지
- 표준화된 데이터를 추가 규칙 처리에 이용하도록 지정

HTTP 트래픽은 다양한 형식으로 인코딩할 수 있으므로, 규칙에서 적절히 검사하기가 쉽지 않습니다. HTTP Inspect는 HTTP 트래픽을 최대한 잘 검사할 수 있도록 14개 인코딩 유형을 디코딩합니다.

HTTP Inspect 옵션을 전체적으로, 단일 서버에서 또는 서버 목록에 대해 구성할 수 있습니다.

HTTP Inspect 프리프로세서를 사용할 때에는 다음에 유의하십시오.

- 프리프로세서 엔진은 HTTP 표준화를 *스테이트리스 방식으로* 수행합니다. 즉, HTTP 문자열을 패킷 단위로 표준화하며, TCP 스트림 프리프로세서에 의해 리어셈블된 HTTP 문자열만 처리할 수 있습니다.
- GID(generator ID)가 119인 HTTP 프리프로세서 규칙을 활성화해야 이러한 규칙에서 이벤트를 생성할 수 있습니다. 자세한 내용은 32-20페이지의 규칙 상태 설정을/를 참조하십시오.

자세한 내용은 다음 절을 참조하십시오.

- 27-31페이지의 전역 HTTP 표준화 옵션 선택
- 27-32페이지의 전역 HTTP 컨피그레이션 옵션 구성
- 27-32페이지의 서버 레벨 HTTP 표준화 옵션 선택
- 27-40페이지의 서버 레벨 HTTP 표준화 인코딩 옵션 선택
- 27-42페이지의 HTTP 서버 옵션 구성
- 27-44페이지의 추가 HTTP Inspect 프리프로세서 규칙 활성화

전역 HTTP 표준화 옵션 선택

라이센스: 보호

HTTP Inspect 프리프로세서에서 제공하는 전역 HTTP 옵션은 프리프로세서의 작동 방식을 제어합니다. 웹 서버 포트로 지정되지 않은 포트가 HTTP 트래픽을 수신할 때 HTTP 표준화를 활성화 또는 비활성화하려면 이러한 옵션을 사용합니다.

다음에 유의하십시오.

- **Unlimited Decompression**을 활성화한 경우 변경 사항을 커밋하면 **Maximum Compressed Data Depth** 및 **Maximum Decompressed Data Depth** 옵션은 자동으로 65535로 설정됩니다. 자세한 내용은 27-32페이지의 서버 레벨 HTTP 표준화 옵션 선택을/를 참조하십시오.
- **Maximum Compressed Data Depth** 및 **Maximum Decompressed Data Depth** 옵션에 대한 값이 액세스 제어 정책의 기본 작업과 관련된 침입 정책 및 액세스 제어 규칙과 관련된 침입 정책에서 서로 다른 경우 가장 큰 값이 사용됩니다.

다음 설명에서 프리프로세서 규칙이 언급되지 않은 경우 해당 옵션은 프리프로세서 규칙과 관련되지 않은 것입니다.

Detect Anomalous HTTP Servers

웹 서버 포트로 지정되지 않은 포트에서 주고받는 HTTP 트래픽을 탐지합니다.

참고 이 옵션을 활성화하는 경우 HTTP Configuration 페이지에서 서버 프로필의 HTTP 트래픽을 수신하는 모든 포트를 나열하십시오. 그렇게 하지 않고 이 옵션 및 동반 프리프로세서 규칙을 활성화하는 경우, 서버를 왕래하는 표준 트래픽이 이벤트를 생성하게 됩니다. 기본 서버 프로필에는 HTTP 트래픽에 일반적으로 사용되는 모든 포트가 포함되지만, 이 프로필을 수정하는 경우 이벤트 생성을 방지하려면 해당 포트를 다른 프로필에 추가해야 할 수 있습니다.

이 옵션에 대한 이벤트를 생성하려면 규칙 120:1을 활성화할 수 있습니다. 자세한 내용은 32-20페이지의 규칙 상태 설정을/를 참조하십시오.

Detect HTTP Proxy Servers

Allow HTTP Proxy Use 옵션으로 정의하지 않은 프록시 서버를 사용하는 HTTP 트래픽을 탐지합니다.

이 옵션에 대한 이벤트를 생성하려면 규칙 119:17을 활성화할 수 있습니다. 자세한 내용은 32-20페이지의 규칙 상태 설정을/를 참조하십시오.

Maximum Compressed Data Depth

Inspect Compressed Data(그리고 선택적으로 **Decompress SWF File (LZMA)**, **Decompress SWF File (Deflate)** 또는 **Decompress PDF File (Deflate)**) 옵션이 활성화된 경우 압축 해제할 압축 데이터의 최대 크기를 설정합니다. 1~65535바이트 범위로 지정할 수 있습니다.

Maximum Decompressed Data Depth

Inspect Compressed Data(그리고 선택적으로 **Decompress SWF File (LZMA)**, **Decompress SWF File (Deflate)** 또는 **Decompress PDF File (Deflate)**) 옵션이 활성화된 경우 표준화된 압축 해제 데이터의 최대 크기를 설정합니다. 1~65535바이트 범위로 지정할 수 있습니다.

전역 HTTP 컨피그레이션 옵션 구성

라이센스: 보호

비표준 포트에 대한 HTTP 트래픽의 탐지 및 프록시 서버를 사용하는 HTTP 트래픽에 대한 탐지를 구성할 수 있습니다. 전역 HTTP 컨피그레이션 옵션에 대한 자세한 내용은 27-31페이지의 전역 HTTP 표준화 옵션 선택을/를 참조하십시오.

전역 HTTP 컨피그레이션 옵션을 구성하려면

액세스: Admin/Intrusion Admin

1단계 **Policies > Access Control**을 선택하여 Access Control Policy 페이지를 표시한 다음 **Network Analysis Policy**를 클릭합니다.

Network Analysis Policy 페이지가 나타납니다.

2단계 수정할 정책 옆에 있는 수정 아이콘()을 클릭합니다.

다른 정책에 저장하지 않은 변경 사항이 있는 경우 변경 사항을 취소하고 계속 진행하려면 **OK**를 클릭합니다. 저장되지 않은 변경 사항을 다른 정책에 저장하는 방법에 대한 자세한 내용은 23-15페이지의 충돌 해결 및 정책 변경 사항 커밋을/를 참조하십시오.

Policy Information 페이지가 나타납니다.

3단계 왼쪽의 탐색 패널에서 **Settings**를 클릭합니다.

Settings 페이지가 나타납니다.

4단계 Application Layer Preprocessors 아래에서 **HTTP Configuration**이 활성화되었는지 여부에 따라 두 가지 선택 사항이 있습니다.

- 컨피그레이션이 활성화되어 있으면 **Edit**를 클릭합니다.
- 컨피그레이션이 비활성화되어 있으면 **Enabled**를 클릭한 다음 **Edit**를 클릭합니다.

HTTP Configuration(IP 컨피그레이션) 페이지가 나타납니다.

5단계 27-31페이지의 전역 HTTP 표준화 옵션 선택에 설명된 전역 옵션을 수정할 수 있습니다.

6단계 정책을 저장하거나, 계속 수정하거나, 변경 사항을 취소하거나, 기반 정책의 기본 컨피그레이션 설정으로 돌아가거나, 시스템 캐시에 변경 사항이 남아 있는 상태로 종료합니다. 자세한 내용은 23-15페이지의 충돌 해결 및 정책 변경 사항 커밋을/를 참조하십시오.

서버 레벨 HTTP 표준화 옵션 선택

라이센스: 보호

모니터링하는 각 서버에 대해, 모든 서버에 대해 전체적으로 또는 서버 목록에 대해 서버 레벨 옵션을 설정할 수 있습니다. 또한 이러한 옵션을 사전 정의된 서버 프로필을 사용하여 설정하거나, 환경 요구에 맞게 개별적으로 설정할 수 있습니다. 트래픽을 표준화할 HTTP 서버 포트, 표준화할 서버 응답 페이로드의 양, 표준화할 인코딩의 유형 등을 지정하려면 이러한 옵션을 사용하거나 이러한 옵션에 대해 설정된 기본 프로필 중 하나를 사용하십시오.

다음 설명에서 프리프로세서 규칙이 언급되지 않은 경우 해당 옵션은 프리프로세서 규칙과 관련되지 않은 것입니다.

Networks

하나 이상의 서버에 대한 IP 주소를 지정하려면 이 옵션을 사용합니다. 단일 IP 주소나 주소 블록 또는 쉼표로 구분된 목록을 지정할 수 있습니다(둘 중 하나 또는 모두로 구성).

기본 프로필을 비롯한 총 프로필 수가 255개로 제한되는 것 외에도 HTTP 서버 목록에는 문자를 최대 496자(약 26개 항목)까지 포함할 수 있으며, 모든 서버 프로필에 대해 총 256개의 주소 항목을 지정할 수 있습니다. FireSIGHT 시스템에서 IPv4 CIDR 표기법 및 IPv6 접두사 길이 사용에 대한 자세한 내용은 1-19페이지의 IP 주소 표기 규칙을/를 참조하십시오.

기본 정책의 `default` 설정은 다른 대상 기반 정책에서 처리되지 않는 모니터링되는 네트워크 세그먼트의 모든 IP 주소를 지정합니다. 따라서 기본 정책에 대해서는 IP 주소 또는 CIDR 블록/접두사 길이를 지정할 수 없고 지정할 필요도 없으며, 다른 정책에서 이 설정을 비워둘 수 없거나 `any`를 나타내는 주소 표기법(예: 0.0.0.0/0 또는 ::/0)을 사용할 수 없습니다.

또한 트래픽 처리를 위한 대상 기반 정책의 경우, 식별하는 네트워크는 대상 기반 정책을 구성하는 네트워크 분석 정책에서 처리되는 네트워크, 영역, VLAN의 하위 집합과 일치하거나 하위 집합이어야 합니다. 자세한 내용은 25-3페이지의 네트워크 분석 정책으로 전처리 맞춤화을/를 참조하십시오.

Ports

프리프로세서 엔진이 HTTP 트래픽을 표준화할 포트. 포트 번호가 여러 개인 경우 쉼표로 구분하십시오.

Oversize Dir Length

지정된 값보다 긴 URL 디렉토리를 탐지합니다.

이 옵션에 대한 이벤트를 생성하려면 규칙 119:15를 활성화할 수 있습니다. 자세한 내용은 32-20페이지의 규칙 상태 설정을/를 참조하십시오.

Client Flow Depth

Ports에 정의된 클라이언트 측 HTTP 트래픽에 있는 원시 HTTP 패킷(헤더 및 페이로드 데이터 포함)에서 검사할 규칙의 바이트 수를 지정합니다. 규칙 내 HTTP content 규칙 옵션이 요청 메시지의 특정 부분을 검사할 때에는 Client Flow Depth가 적용되지 않습니다. 자세한 내용은 36-23페이지의 HTTP Content 옵션을/를 참조하십시오.

-1~1460 범위의 값을 지정할 수 있습니다. Cisco에서는 Client Flow Depth를 최대값으로 설정할 것을 권장합니다. 다음과 같이 지정합니다.

- 1~1460은 첫 번째 패킷에서 지정된 바이트 수를 검사합니다. 첫 번째 패킷에 있는 바이트 수가 지정된 값보다 적으면 전체 패킷이 검사됩니다. 지정된 값은 세그먼트된 패킷과 리어셈블된 패킷에 모두 적용됩니다.

  값을 300으로 지정하는 경우 많은 클라이언트 요청 헤더의 끝에 나타나는 큰 HTTP Cookies에 대한 검사가 대개 생략됩니다.
- 0은 한 세션의 여러 패킷을 포함하여 모든 클라이언트 측 트래픽을 검사하며, 필요 시 1460 바이트 제한을 초과합니다. 이 값은 성능에 영향을 미칠 수 있습니다.
- -1은 모든 클라이언트 측 트래픽을 무시합니다.

Server Flow Depth

Ports에 정의된 서버 측 HTTP 트래픽에 있는 원시 HTTP 패킷에서 검사할 규칙의 바이트 수를 지정합니다. **Inspect HTTP Responses**가 비활성화된 경우 원시 헤더와 페이로드가 검사에 포함되고, **Inspect HTTP Response**가 활성화된 경우 원시 응답 본문만 검사에 포함됩니다.

Server Flow Depth는 **Ports**에 정의된 서버 측 HTTP 트래픽을 검사할 규칙에 대해 세션에서 원시 서버 응답 데이터의 바이트 수를 지정합니다. HTTP 서버 응답 데이터의 성능과 검사 수준 간에 균형을 유지하려면 이 옵션을 사용할 수 있습니다. 규칙 내 HTTP content 옵션이 응답 메시지의 특정 부분을 검사할 때에는 Server Flow Depth가 적용되지 않습니다. 자세한 내용은 36-23페이지의 HTTP Content 옵션을/를 참조하십시오.

Client Flow Depth와 달리 Server Flow Depth는 검사할 규칙에 대해 HTTP 요청 패킷당 바이트 수가 아니라 HTTP 응답당 바이트 수를 지정합니다.

-1~65535 범위의 값을 지정할 수 있습니다. Cisco에서는 Server Flow Depth를 최대값으로 설정할 것을 권장합니다. 다음과 같이 지정할 수 있습니다.

- 1~65535:

  Inspect HTTP Responses가 **활성화**된 경우 원시 HTTP 응답 본문만 검사하고 원시 HTTP 헤더는 검사하지 않습니다. **Inspect Compressed Data**가 활성화된 경우 압축 해제 데이터도 검사합니다.

  Inspect HTTP Responses가 **비활성화**된 경우 원시 패킷 헤더 및 페이로드를 검사합니다.

  세션에 포함된 응답 바이트 수가 지정된 값보다 작은 경우, 규칙은 지정된 세션에서 모든 응답 패킷을 전체적으로 검사합니다(필요 시 여러 패킷에 걸쳐). 세션에 포함된 응답 바이트 수가 지정된 값보다 큰 경우, 규칙은 해당 세션에 대해 지정된 바이트 수만 검사합니다(필요 시 여러 패킷에 걸쳐).

  Flow Depth 값이 작으면 **Ports**에 정의된 서버 측 트래픽을 대상으로 하는 규칙에서 오탐이 발생할 수 있습니다. 이러한 규칙은 대부분 비 헤더 데이터의 처음 100바이트 정도에 있을 수 있는 HTTP 헤더 또는 HTTP content를 대상으로 합니다. 헤더 길이는 대개 300바이트 미만이지만, 헤더 크기는 다양할 수 있습니다.

  지정된 값은 세그먼트된 패킷과 리어셈블된 패킷에 모두 적용됩니다.

- 0은 65535바이트가 넘는 세션의 응답 데이터를 포함하여 **Ports**에 정의된 모든 HTTP 서버 측 트래픽의 전체 패킷을 검사합니다.

  이 값은 성능에 영향을 미칠 수 있습니다.

- -1:

  Inspect HTTP Responses가 **활성화**된 경우 원시 HTTP 헤더만 검사하고 원시 HTTP 응답 본문은 검사하지 않습니다.

  Inspect HTTP Responses가 **비활성화**된 경우 **Ports**에 정의된 모든 서버 측 트래픽을 무시합니다.

Maximum Header Length

HTTP 요청에서(그리고 **Inspect HTTP Responses**가 활성화된 경우 HTTP 응답에서) 지정된 최대 바이트 수보다 긴 헤더 필드를 탐지합니다. 값을 0으로 지정하면 이 옵션이 비활성화됩니다. 옵션을 활성화하려면 1~65535 범위의 값을 지정합니다.

이 옵션에 대한 이벤트를 생성하려면 규칙 119:19를 활성화할 수 있습니다. 자세한 내용은 32-20페이지의 규칙 상태 설정을/를 참조하십시오.

Maximum Number of Headers

헤더의 수가 HTTP 요청에 있는 이 설정을 초과하는 경우를 탐지합니다. 옵션을 활성화하려면 1~1024 범위의 값을 지정합니다.

이 옵션에 대한 이벤트를 생성하려면 규칙 119:20을 활성화할 수 있습니다. 자세한 내용은 32-20페이지의 규칙 상태 설정을/를 참조하십시오.

Maximum Number of Spaces

축소된 줄의 공백 수가 HTTP 요청에 있는 이 설정과 같거나 큰 경우를 탐지합니다. 값을 0으로 지정하면 이 옵션이 비활성화됩니다. 옵션을 활성화하려면 1~65535 범위의 값을 지정합니다.

이 옵션에 대한 이벤트를 생성하려면 규칙 119:26을 활성화할 수 있습니다. 자세한 내용은 32-20페이지의 규칙 상태 설정을/를 참조하십시오.

HTTP Client Body Extraction Depth

HTTP 클라이언트 요청의 메시지 본문에서 추출할 바이트 수를 지정합니다. 침입 규칙을 사용하면 `content` 또는 `protected_content` 키워드 **HTTP Client Body** 옵션을 선택하여 추출된 데이터를 검사할 수 있습니다. 자세한 내용은 36-23페이지의 HTTP Content 옵션을/를 참조하십시오.

-1~65495 범위의 값을 지정합니다. -1을 지정하면 클라이언트 본문이 무시됩니다. 0을 지정하면 전체 클라이언트 본문이 추출됩니다. 추출할 특정 바이트를 식별하면 시스템 성능이 향상될 수 있습니다. 침입 규칙에서 **HTTP Client Body** 옵션이 작동하도록 하려면 0~65495 범위의 값을 지정해야 합니다.

Small Chunk Size

작은 청크로 간주할 최대 바이트 수를 지정합니다. 1~255 범위의 값을 지정합니다. 값을 0으로 지정하면 비정상적으로 연속된 작은 세그먼트의 탐지가 비활성화됩니다. 자세한 내용은 **Consecutive Small Chunks** 옵션을/를 참조하십시오.

Consecutive Small Chunks

청크된 전송 인코딩을 사용하는 클라이언트 또는 서버 트래픽에서 연속된 작은 청크가 몇 개일 때 비정상적으로 큰 수를 나타내는지를 지정합니다. **Small Chunk Size** 옵션은 작은 청크의 최대 크기를 지정합니다.

예를 들어 10바이트 이하의 연속된 청크 5개를 탐지하려면 **Small Chunk Size**를 10으로 설정하고 **Consecutive Small Chunks**를 5로 설정합니다.

지나치게 작은 청크에 대해 이벤트를 트리거하려면 클라이언트 트래픽에서는 프리프로세서 규칙 119:27, 서버 트래픽에서는 규칙 120:7을 활성화할 수 있습니다. **Small Chunk Size**가 활성화되고 이 옵션이 0 또는 1로 설정된 경우 이러한 규칙을 활성화하면 지정된 크기 이하의 모든 청크에 대해 이벤트가 트리거됩니다. 자세한 내용은 32-20페이지의 규칙 상태 설정을/를 참조하십시오.

HTTP Methods

GET 및 POST 외에 시스템이 트래픽에서 발견하는 HTTP 요청 메서드를 지정합니다. 여러 개의 값을 구분하려면 쉼표를 사용하십시오.

침입 규칙은 HTTP 메서드에서 내용을 검색하기 위해 `content` 또는 `protected_content` 키워드와 **HTTP Method** 인수를 사용합니다. 36-23페이지의 HTTP Content 옵션을/를 참조하십시오. GET, POST 또는 이 옵션에 대해 구성된 메서드 이외의 메서드가 트래픽에서 발견될 때 이벤트를 생성하려면 규칙 119:31을 활성화할 수 있습니다.

No Alerts

동반 프리프로세서 규칙이 활성화된 경우 침입 이벤트를 비활성화합니다.

참고 이 옵션은 HTTP 표준 텍스트 규칙 및 공유 객체 규칙을 비활성화하지 **않습니다**.

Normalize HTTP Headers

Inspect HTTP Responses가 활성화된 경우 요청 및 응답 헤더에서 비 쿠키 데이터의 표준화를 활성화합니다. **Inspect HTTP Responses**가 활성화되지 **않은** 경우 요청 및 응답 헤더에서 쿠키를 비롯한 전체 HTTP 헤더의 표준화를 활성화합니다.

Inspect HTTP Cookies

HTTP 요청 헤더에서 쿠키의 추출을 활성화합니다. 또한 **Inspect HTTP Responses**가 활성화된 경우 응답 헤더에서 set-cookie 데이터의 추출을 활성화합니다. 쿠키 추출이 필요하지 않을 때 이 옵션을 비활성화하면 성능이 향상됩니다.

`Cookie:` 및 `Set-Cookie:` 헤더 이름, 헤더 줄의 선행 공백, 헤더 줄을 종료하는 `CRLF`는 쿠키의 일부가 아니라 헤더의 일부로서 검사됩니다.

Normalize Cookies in HTTP headers

HTTP 요청 헤더에서 쿠키의 표준화를 활성화합니다. **Inspect HTTP Responses**가 활성화된 경우 응답 헤더에서 set-cookie 데이터의 표준화도 활성화합니다. 이 옵션을 선택하기 전에 **Inspect HTTP Cookies**를 선택해야 합니다.

Allow HTTP Proxy Use

모니터링되는 웹 서버를 HTTP 프록시로서 사용하도록 허용합니다. 이 옵션은 HTTP 요청 검사에만 사용됩니다.

Inspect URI Only

표준화된 HTTP 요청 패킷의 URI 부분만 검사합니다.

Inspect HTTP Responses

프리프로세서에서 HTTP 요청 메시지의 디코딩 및 표준화 외에 규칙 엔진이 검사할 응답 필드도 추출하도록 HTTP 응답의 확장 검사를 활성화합니다. 이 옵션을 활성화하면 시스템은 응답 헤더, 본문, 상태 코드 등을 추출하며, **Inspect HTTP Cookies**가 활성화된 경우 set-cookie 데이터도 추출합니다. 자세한 내용은 36-23페이지의 HTTP Content 옵션, 36-96페이지의 HTTP 인코딩 유형 및 위치에서 이벤트 생성, 36-99페이지의 특정 페이로드 유형 가리키기을/를 참조하십시오.

이 옵션에 대한 이벤트를 생성하려면 규칙 120:2 및 120:3을 활성화할 수 있습니다. 자세한 내용은 32-20페이지의 규칙 상태 설정을/를 참조하십시오.

Normalize UTF Encodings to UTF-8

Inspect HTTP Responses가 활성화된 경우 HTTP 응답에서 UTF-16LE, UTF-16BE, UTF-32LE 및 UTF32-BE 인코딩을 탐지하고 UTF-8로 표준화합니다.

이 옵션에 대한 이벤트를 생성하려면 규칙 120:4를 활성화할 수 있습니다. 자세한 내용은 32-20페이지의 규칙 상태 설정을/를 참조하십시오.

Inspect Compressed Data

Inspect HTTP Responses가 활성화된 경우 HTTP 응답 본문에 있는 gzip 및 deflate 호환 압축 데이터의 압축 해제 및 표준화된 압축 해제 데이터의 검사를 활성화합니다. 시스템은 청크 및 비 청크 HTTP 응답 데이터를 검사합니다. 시스템은 필요에 따라 여러 패킷에서 패킷 단위로 압축 해제 데이터를 검사합니다. 즉, 시스템은 검사를 위해 서로 다른 패킷의 압축 해제 데이터를 결합하지 않습니다. **Maximum Compressed Data Depth**, **Maximum Decompressed Data Depth** 또는 압축된 데이터의 끝에 도달하면 압축 해제가 종료됩니다. **Unlimited Decompression**도 함께 선택하지 않은 경우에는 **Server Flow Depth**에 도달하면 압축 해제된 데이터의 검사가 종료됩니다. 압축 해제된 데이터를 검사하려면 `file_data` 규칙 키워드를 사용할 수 있습니다. 자세한 내용은 36-99페이지의 특정 페이로드 유형 가리키기을/를 참조하십시오.

Unlimited Decompression

Inspect Compressed Data(그리고 선택적으로 **Decompress SWF File (LZMA)**, **Decompress SWF File (Deflate)** 또는 **Decompress PDF File (Deflate)**)가 활성화된 경우 여러 패킷에서 **Maximum Decompressed Data Depth**를 재정의합니다. 즉, 이 옵션은 여러 패킷에서 무제한 압축 해제를 활성화합니다. 이 옵션의 활성화는 단일 패킷 내에서 **Maximum Compressed Data Depth** 또는 **Maximum Decompressed Data Depth**에 영향을 미치지 않습니다. 이 옵션을 활성화하면, 변경 사항을 커밋하는 경우 **Maximum Compressed Data Depth** 및 **Maximum Decompressed Data Depth**가 65535로 설정됩니다. 27-31페이지의 전역 HTTP 표준화 옵션 선택을/를 참조하십시오.

Normalize Javascript

Inspect HTTP Responses가 활성화된 경우 HTTP 응답 본문 내에서 Javascript의 탐지 및 표준화를 활성화합니다. 프리프로세서는 unescape 및 decodeURI 함수, String.fromCharCode 메서드 등 난독 Javascript 데이터를 표준화합니다. 프리프로세서는 unescape, decodeURI 및 decodeURIComponent 함수 내에서 다음 인코딩을 표준화합니다.

- %XX
- %uXXXX
- 0xXX
- \xXX
- \uXXXX

프리프로세서는 연속 공백을 탐지하고 이를 단일 공백으로 표준화합니다. 이 옵션이 활성화된 경우 난독 Javascript 데이터에서 허용할 연속 공백의 최대 수를 컨피그레이션 필드에 지정할 수 있습니다. 1~65535 범위의 값을 입력할 수 있습니다. 이 필드와 연결된 프리프로세서 규칙 (120:10)의 활성화 여부와 상관없이, 값을 0으로 지정하면 이벤트 생성이 비활성화됩니다.

프리프로세서는 또한 Javascript 더하기(+) 연산자 및 이 연산자를 사용하는 연결 문자열을 표준화합니다.

침입 규칙이 표준화된 Javascript 데이터를 가리키도록 하려면 `file_data` 키워드를 사용할 수 있습니다. 자세한 내용은 36-99페이지의 특정 페이로드 유형 가리키기을/를 참조하십시오.

이 옵션에 대한 이벤트를 생성하려면 다음과 같이 규칙 120:9, 120:10 및 120:11을 활성화할 수 있습니다.

표 27-6 Normalize Javascript 옵션 규칙

규칙	이벤트가 트리거되는 경우
120:9	프리프로세서 내 난독 수준이 2보다 크거나 같음
120:10	Javascript 난독 데이터의 연속 공백 수가 허용되는 최대 연속 공백 수에 대해 구성된 값보다 크거나 같음
120:11	이스케이프된 또는 인코딩된 데이터에 여러 개의 인코딩 유형이 포함됨

자세한 내용은 32-20페이지의 규칙 상태 설정을/를 참조하십시오.

Decompress SWF File (LZMA) 및 Decompress SWF File (Deflate)

HTTP Inspect Responses가 활성화된 경우 이러한 옵션은 HTTP 요청의 HTTP 응답 본문에 있는 파일의 압축 부분을 압축 해제합니다.

참고 HTTP GET 응답에서 발견된 파일의 압축 **부분만** 압축 해제할 수 있습니다.

- **Decompress SWF File (LZMA)**은 Adobe ShockWave Flash(`.swf`) 파일의 LZMA 호환 압축 부분을 압축 해제합니다.
- **Decompress SWF File (Deflate)**은 Adobe ShockWave Flash(`.swf`) 파일의 deflate 호환 압축 부분을 압축 해제합니다.

Maximum Compressed Data Depth, **Maximum Decompressed Data Depth** 또는 압축된 데이터의 끝에 도달하면 압축 해제가 종료됩니다. **Unlimited Decompression**도 함께 선택하지 않은 경우에는 **Server Flow Depth**에 도달하면 압축 해제된 데이터의 검사가 종료됩니다. 압축 해제된 데이터를 검사하려면 `file_data` 규칙 키워드를 사용할 수 있습니다. 자세한 내용은 36-99페이지의 특정 페이로드 유형 가리키기을/를 참조하십시오.

이 옵션에 대한 이벤트를 생성하려면 다음과 같이 규칙 120:12 및 120:13을 활성화할 수 있습니다.

표 27-7 Decompress SWF File 옵션 규칙

규칙	이벤트가 트리거되는 경우
120:12	deflate 파일 압축 해제가 실패함
120:13	LZMA 파일 압축 해제가 실패함

Decompress PDF File (Deflate)

HTTP Inspect Responses가 활성화된 경우 **Decompress PDF File (Deflate)**은 HTTP 요청의 HTTP 응답 본문에 있는 Portable Document Format(`.pdf`) 파일의 deflate 호환 압축 부분을 압축 해제합니다. 시스템은 `/FlateDecode` 스트림 필터가 있는 PDF 파일만 압축 해제할 수 있습니다. 다른 스트림 필터(`/FlateDecode /FlateDecode` 포함)는 지원되지 않습니다.

참고 HTTP GET 응답에서 발견된 파일의 압축 **부분만** 압축 해제할 수 있습니다.

Maximum Compressed Data Depth, **Maximum Decompressed Data Depth** 또는 압축된 데이터의 끝에 도달하면 압축 해제가 종료됩니다. **Unlimited Decompression**도 함께 선택하지 않은 경우에는 **Server Flow Depth**에 도달하면 압축 해제된 데이터의 검사가 종료됩니다. 압축 해제된 데이터를 검사하려면 `file_data` 규칙 키워드를 사용할 수 있습니다. 자세한 내용은 36-99페이지의 특정 페이로드 유형 가리키기을/를 참조하십시오.

이 옵션에 대한 이벤트를 생성하려면 다음과 같이 규칙 120:14, 120:15, 120:16 및 120:17을 활성화할 수 있습니다.

표 27-8 Decompress PDF File (Deflate) 옵션 규칙

규칙	이벤트가 트리거되는 경우
120:14	파일 압축 해제가 실패함
120:15	지원되지 않는 압축 유형 때문에 파일 압축 해제가 실패함

표 27-8 Decompress PDF File (Deflate) 옵션 규칙(계속)

규칙	이벤트가 트리거되는 경우
120:16	지원되지 않는 PDF 스트림 필터 때문에 파일 압축 해제가 실패함
120:17	파일 구문 분석이 실패함

Extract Original Client IP Address

XFF(X-Forwarded-For), True-Client-IP 또는 사용자 정의 HTTP 헤더에서의 원래 클라이언트 IP 주소 추출을 활성화합니다. 추출된 원래 클라이언트 IP 주소를 침입 이벤트 테이블 보기에 표시할 수 있습니다. 자세한 내용은 41-10페이지의 침입 이벤트 이해을/를 참조하십시오.

이 옵션에 대한 이벤트를 생성하려면 규칙 119:23, 119:29 및 119:30을 활성화할 수 있습니다. 자세한 내용은 32-20페이지의 규칙 상태 설정을/를 참조하십시오.

XFF Header Priority

Extract Original Client IP Address가 활성화된 경우 시스템이 원래 클라이언트 IP HTTP 헤더를 처리하는 순서를 지정합니다. 모니터링되는 네트워크에서 XFF(X-Forwarded-For) 또는 True-Client-IP 이외의 원래 클라이언트 IP 헤더가 발견될 수 있는 경우, **Add**를 클릭하여 우선순위 목록에 다른 헤더 이름을 추가할 수 있습니다. 그런 다음 각 헤더 유형 옆에 있는 위쪽 또는 아래쪽 화살표 아이콘을 사용하여 우선순위를 조정할 수 있습니다. HTTP 요청에 여러 XFF 헤더가 나타나는 경우 시스템은 우선순위가 가장 높은 헤더만 처리합니다.

Log URI

HTTP 요청 패킷에서 원시 URI(있는 경우)의 추출을 활성화하고, URI를 세션에 대해 생성된 모든 침입 이벤트와 연결합니다.

이 옵션이 활성화된 경우 침입 이벤트 테이블 보기의 HTTP URI 열에서 추출된 URI의 처음 50개 문자를 표시할 수 있습니다. 패킷 보기에서 최대 2048바이트까지 전체 URI를 표시할 수 있습니다. 자세한 내용은 41-10페이지의 침입 이벤트 이해 및 41-24페이지의 이벤트 정보 보기을/를 참조하십시오.

Log Hostname

HTTP 요청 Host 헤더에서 호스트 이름(있는 경우)의 추출을 활성화하고, 호스트 이름을 세션에 대해 생성된 모든 침입 이벤트와 연결합니다. 여러 Host 헤더가 있는 경우 첫 번째 헤더에서 호스트 이름을 추출합니다.

이 옵션이 활성화된 경우 침입 이벤트 테이블 보기의 HTTP 호스트 이름 열에서 추출된 호스트 이름의 처음 50개 문자를 표시할 수 있습니다. 패킷 보기에서 최대 256바이트까지 전체 호스트 이름을 표시할 수 있습니다. 자세한 내용은 41-10페이지의 침입 이벤트 이해 및 41-24페이지의 이벤트 정보 보기을/를 참조하십시오.

이 옵션에 대한 이벤트를 생성하려면 규칙 119:25를 활성화할 수 있습니다. 자세한 내용은 32-20페이지의 규칙 상태 설정을/를 참조하십시오.

프리프로세서 및 규칙 119:24가 활성화된 경우 이 옵션의 설정과 상관없이 프리프로세서는 HTTP 요청에서 여러 Host 헤더를 탐지하는 경우 침입 이벤트를 생성합니다. 자세한 내용은 27-44페이지의 추가 HTTP Inspect 프리프로세서 규칙 활성화을/를 참조하십시오.

Profile

HTTP 트래픽에 대해 표준화되는 인코딩 유형을 지정합니다. 시스템은 대부분의 서버에 적절한 기본 프로필, Apache 및 IIS 서버의 기본 프로필, 모니터링되는 트래픽의 요구를 충족시키기 위해 맞춤화할 수 있는 사용자 지정 기본 설정을 제공합니다. 자세한 내용은 27-40페이지의 서버 레벨 HTTP 표준화 인코딩 옵션 선택을/를 참조하십시오.

서버 레벨 HTTP 표준화 인코딩 옵션 선택

라이센스: 보호

서버 레벨 HTTP 표준화 옵션을 선택하여 HTTP 트래픽에 대해 표준화되는 인코딩의 유형을 지정하고, 이 인코딩 유형이 포함된 트래픽에 대해 시스템이 이벤트를 생성하도록 지정할 수 있습니다.

다음 설명에서 프리프로세서 규칙이 언급되지 않은 경우 해당 옵션은 프리프로세서 규칙과 관련되지 않은 것입니다.

ASCII Encoding

인코딩된 ASCII 문자를 디코딩하고 ASCII로 인코딩된 URI에 대해 규칙 엔진이 이벤트를 생성할지 여부를 지정합니다.

이 옵션에 대한 이벤트를 생성하려면 규칙 119:1을 활성화할 수 있습니다. 자세한 내용은 32-20 페이지의 규칙 상태 설정을/를 참조하십시오.

UTF-8 Encoding

URI에서 표준 UTF-8 유니코드 시퀀스를 디코딩합니다.

이 옵션에 대한 이벤트를 생성하려면 규칙 119:6을 활성화할 수 있습니다. 자세한 내용은 32-20 페이지의 규칙 상태 설정을/를 참조하십시오.

Microsoft %U Encoding

%u 및 네 문자 형식을 사용하는 IIS %u 인코딩 체계를 디코딩합니다. 여기서 네 문자는 IIS 유니코드 코드포인트와 상호 연결되는 16진수로 인코딩된 값입니다.

팁 합법적인 클라이언트는 %u 인코딩을 거의 사용하지 않으므로, Cisco에서는 %u 인코딩으로 인코딩된 HTTP 트래픽을 디코딩할 것을 권장합니다.

이 옵션에 대한 이벤트를 생성하려면 규칙 119:3을 활성화할 수 있습니다. 자세한 내용은 32-20 페이지의 규칙 상태 설정을/를 참조하십시오.

Bare Byte UTF-8 Encoding

비 ASCII 문자를 UTF-8 값 디코딩에서 유효한 값으로 사용하는 Bare Byte 인코딩을 디코딩합니다.

팁 Bare Byte 인코딩을 사용하면 사용자는 IIS 서버를 에뮬레이트하고 비표준 인코딩을 정확하게 해석할 수 있습니다.합법적인 클라이언트는 이런 방식으로 UTF-8을 인코딩하지 않으므로 Cisco에서는 이 옵션을 활성화할 것을 권장합니다.

이 옵션에 대한 이벤트를 생성하려면 규칙 119:4를 활성화할 수 있습니다. 자세한 내용은 32-20 페이지의 규칙 상태 설정을/를 참조하십시오.

Microsoft IIS Encoding

유니코드 코드포인트 매핑을 사용하여 디코딩합니다.

팁 이는 주로 공격 및 회피 시도에서 발견되므로 Cisco에서는 이 옵션을 활성화할 것을 권장합니다.

이 옵션에 대한 이벤트를 생성하려면 규칙 119:7을 활성화할 수 있습니다. 자세한 내용은 32-20 페이지의 규칙 상태 설정을/를 참조하십시오.

Double Encoding

둘 모두 각각에서 디코딩을 수행하는 요청 URI를 통과하도록 하여 IIS 이중 인코딩 트래픽을 디코딩합니다.이는 주로 공격 시나리오에서 발견되므로 Cisco에서는 이 옵션을 활성화할 것을 권장합니다.

이 옵션에 대한 이벤트를 생성하려면 규칙 119:2를 활성화할 수 있습니다. 자세한 내용은 32-20 페이지의 규칙 상태 설정을/를 참조하십시오.

Multi-Slash Obfuscation

한 행의 여러 슬래시를 단일 슬래시로 표준화합니다.

이 옵션에 대한 이벤트를 생성하려면 규칙 119:8을 활성화할 수 있습니다. 자세한 내용은 32-20 페이지의 규칙 상태 설정을/를 참조하십시오.

IIS Backslash Obfuscation

백슬래시를 슬래시로 표준화합니다.

이 옵션에 대한 이벤트를 생성하려면 규칙 119:9를 활성화할 수 있습니다. 자세한 내용은 32-20 페이지의 규칙 상태 설정을/를 참조하십시오.

Directory Traversal

디렉토리 통과 및 자체 참조 디렉토리를 표준화합니다. 일부 웹사이트는 디렉토리 통과를 사용하여 파일을 참조하므로, 동반 프리프로세서 규칙이 이 유형의 트래픽에 대해 이벤트를 생성하도록 활성화하는 경우 오탐이 생성될 수 있습니다.

이 옵션에 대한 이벤트를 생성하려면 규칙 119:10 및 119:11을 활성화할 수 있습니다. 자세한 내용은 32-20페이지의 규칙 상태 설정을/를 참조하십시오.

Tab Obfuscation

공백 구분 기호에 탭을 사용하는 비 RFC 표준을 표준화합니다. Apache 및 기타 비 IIS 웹 서버는 탭 문자(0x09)를 URL의 구분 기호로 사용합니다.

참고 이 옵션의 컨피그레이션과 상관없이 HTTP Inspect 프리프로세서는 공백 문자(0x20)가 앞에 오는 경우 탭을 공백으로 취급합니다.

이 옵션에 대한 이벤트를 생성하려면 규칙 119:12를 활성화할 수 있습니다. 자세한 내용은 32-20페이지의 규칙 상태 설정을/를 참조하십시오.

Invalid RFC Delimiter

URI 데이터에서 줄 바꿈(\n)을 표준화합니다.

이 옵션에 대한 이벤트를 생성하려면 규칙 119:13을 활성화할 수 있습니다. 자세한 내용은 32-20페이지의 규칙 상태 설정을/를 참조하십시오.

Webroot Directory Traversal

URL에서 초기 디렉토리를 가로지르는 디렉토리 통과를 탐지합니다.

이 옵션에 대한 이벤트를 생성하려면 규칙 119:18을 활성화할 수 있습니다. 자세한 내용은 32-20페이지의 규칙 상태 설정을/를 참조하십시오.

Tab URI Delimiter

탭 문자(0x09)를 URI의 구분 기호로 사용하도록 설정합니다. Apache, IIS의 최신 버전 및 기타 일부 웹 서버는 탭 문자를 URL의 구분 기호로 사용합니다.

참고 이 옵션의 컨피그레이션과 상관없이 HTTP Inspect 프리프로세서는 공백 문자(0x20)가 앞에 오는 경우 탭을 공백으로 취급합니다.

Non-RFC characters

들어오거나 나가는 URI 데이터 내에 나타날 때 해당 필드에 추가하는 비 RFC 문자 목록을 탐지합니다. 이 필드를 수정하는 경우 바이트 문자를 나타내는 16진수 형식을 사용하십시오. 이 옵션을 구성하는 경우 값을 신중하게 설정해야 합니다. 매우 일반적인 문자를 사용하면 이벤트가 너무 많이 발생할 수 있습니다.

이 옵션에 대한 이벤트를 생성하려면 규칙 119:14를 활성화할 수 있습니다. 자세한 내용은 32-20페이지의 규칙 상태 설정을/를 참조하십시오.

Max Chunk Encoding Size

URI 데이터에서 비정상적으로 큰 청크 크기를 탐지합니다.

이 옵션에 대한 이벤트를 생성하려면 규칙 119:16 및 119:22를 활성화할 수 있습니다. 자세한 내용은 32-20페이지의 규칙 상태 설정을/를 참조하십시오.

Disable Pipeline Decoding

파이프라인된 요청에 대한 HTTP 디코딩을 비활성화합니다. 이 옵션을 비활성화하면, 파이프라인에서 대기하는 HTTP 요청이 디코딩 또는 분석되지 않으며 일반적인 패턴 매칭만을 사용하여 검사되므로 성능이 향상됩니다.

Non-Strict URI Parsing

엄격하지 않은 URI 구문 분석을 활성화합니다. "GET /index.html abc xo qr \n" 형식의 비표준 URI를 허용하는 서버에서만 이 옵션을 사용하십시오. 이 옵션을 사용하면, 두 번째 공백 뒤에 유효한 HTTP 식별자가 없더라도 디코더는 URI가 첫 번째와 두 번째 공백 사이에 있다고 가정합니다.

Extended ASCII Encoding

HTTP 요청 URI에 있는 확장 ASCII 문자의 구문 분석을 활성화합니다. 이 옵션은 Apache, IIS 또는 모든 서버에서 제공하는 기본 프로필이 아니라 사용자 지정 서버 프로필에서만 사용할 수 있습니다.

HTTP 서버 옵션 구성

라이센스: 보호

HTTP 서버 옵션을 구성하려면 다음 절차를 사용할 수 있습니다. HTTP 서버 옵션에 대한 자세한 내용은 27-32페이지의 서버 레벨 HTTP 표준화 옵션 선택 및 27-40페이지의 서버 레벨 HTTP 표준화 인코딩 옵션 선택을/를 참조하십시오.

서버 레벨 HTTP 컨피그레이션 옵션을 구성하려면

액세스: Admin/Intrusion Admin

1단계 **Policies > Access Control**을 선택하여 Access Control Policy 페이지를 표시한 다음 **Network Analysis Policy**를 클릭합니다.

Network Analysis Policy 페이지가 나타납니다.

2단계 수정할 정책 옆에 있는 수정 아이콘( )을 클릭합니다.

다른 정책에 저장하지 않은 변경 사항이 있는 경우 변경 사항을 취소하고 계속 진행하려면 **OK**를 클릭합니다. 저장되지 않은 변경 사항을 다른 정책에 저장하는 방법에 대한 자세한 내용은 23-15페이지의 충돌 해결 및 정책 변경 사항 커밋을/를 참조하십시오.

Policy Information 페이지가 나타납니다.

3단계 왼쪽의 탐색 패널에서 **Settings**를 클릭합니다.

Settings 페이지가 나타납니다.

4단계 Application Layer Preprocessors 아래에서 **HTTP Configuration**이 활성화되었는지 여부에 따라 두 가지 선택 사항이 있습니다.

- 컨피그레이션이 활성화되어 있으면 **Edit**를 클릭합니다.
- 컨피그레이션이 비활성화되어 있으면 **Enabled**를 클릭한 다음 **Edit**를 클릭합니다.

HTTP Configuration(IP 컨피그레이션) 페이지가 나타납니다. 페이지 하단에 있는 메시지는 컨피그레이션이 포함된 네트워크 분석 정책 레이어를 식별합니다. 자세한 내용은 24-1페이지의 네트워크 분석 또는 침입 정책에서 레이어 사용을/를 참조하십시오.

5단계 다음 2가지 옵션을 사용할 수 있습니다.

- 새 서버 프로필을 추가합니다. 페이지 왼쪽의 **Servers** 옆에 있는 추가 아이콘( )을 클릭합니다. Add Target 팝업 창이 나타납니다. **Server Address** 필드에서 클라이언트에 대한 하나 이상의 IP 주소를 지정하고 **OK**를 클릭합니다.

  단일 IP 주소나 주소 블록 또는 쉼표로 구분된 목록을 지정할 수 있습니다(둘 중 하나 또는 모두). 목록에 최대 496자를 포함하고, 모든 서버 프로필에 대해 총 256개의 주소 항목을 지정하고, 기본 프로필을 포함하여 총 255개의 프로필을 생성할 수 있습니다. FireSIGHT 시스템에서 IPv4 및 IPv6 주소 블록을 사용하는 방법에 대한 자세한 내용은 1-19페이지의 IP 주소 표기 규칙을/를 참조하십시오.

  트래픽 처리를 위한 대상 기반 정책의 경우, 식별하는 네트워크는 대상 기반 정책을 구성하는 네트워크 분석 정책에서 처리되는 네트워크, 영역, VLAN의 하위 집합과 일치하거나 하위 집합이어야 합니다. 자세한 내용은 25-3페이지의 네트워크 분석 정책으로 전처리 맞춤화을/를 참조하십시오.

  새 항목이 페이지 왼쪽의 서버 목록에 나타나서 선택된 것을 알 수 있도록 강조 표시되며, 추가한 프로필에 대한 현재 컨피그레이션을 반영하여 Configuration 섹션이 업데이트됩니다.

- 기존의 프로필에 대한 설정을 수정합니다. 페이지 왼쪽의 **Servers** 아래에서 추가한 프로필에 대해 구성된 주소를 클릭하거나 **default**를 클릭합니다.

  선택 항목이 강조 표시되고, 선택한 프로필에 대한 현재 컨피그레이션을 표시하기 위해 Configuration 섹션이 업데이트됩니다. 기존의 프로필을 삭제하려면 제거할 프로필 옆에 있는 삭제 아이콘( )을 클릭합니다.

6단계 선택적으로, **Networks** 필드에 나열된 주소를 수정하고 페이지의 다른 영역을 클릭합니다.

페이지의 왼쪽에서 강조 표시된 주소가 업데이트됩니다.

기본 프로필에서는 **Networks**에 대한 설정을 수정할 수 없습니다. 기본 프로필은 다른 프로필에서 식별되지 않는 네트워크의 모든 서버에 적용됩니다.

7단계 HTTP Inspect로 트래픽을 검사하려는 포트를 **Ports** 필드에 나열합니다. 포트가 여러 개인 경우 쉼표로 구분하십시오.

8단계 27-32페이지의 서버 레벨 HTTP 표준화 옵션 선택에 설명된 다른 옵션을 수정할 수 있습니다.

9단계 다음과 같이 서버 프로필을 선택합니다.

- 자체 서버 프로필을 생성하려면 **Custom**을 선택합니다(자세한 내용은 27-40페이지의 서버 레벨 HTTP 표준화 인코딩 옵션 선택 참조).
- 모든 서버에 적합한 표준 기본 프로필을 사용하려면 **All**을 선택합니다.
- 기본 IIS 프로필을 사용하려면 **IIS**를 선택합니다.
- 기본 Apache 프로필을 사용하려면 **Apache**를 선택합니다.

10단계 **Custom**을 선택하면 사용자 지정 옵션이 나타납니다.

11단계 프로필에서 원하는 HTTP 디코딩 옵션을 구성합니다.

사용 가능한 표준화 옵션에 대한 자세한 내용은 27-32페이지의 서버 레벨 HTTP 표준화 옵션 선택을/를 참조하십시오.

12단계 정책을 저장하거나, 계속 수정하거나, 변경 사항을 취소하거나, 기반 정책의 기본 컨피그레이션 설정으로 돌아가거나, 시스템 캐시에 변경 사항이 남아 있는 상태로 종료합니다. 자세한 내용은 23-15페이지의 충돌 해결 및 정책 변경 사항 커밋을/를 참조하십시오.

추가 HTTP Inspect 프리프로세서 규칙 활성화

라이센스: 보호

특정 컨피그레이션 옵션과 연결되지 않은 HTTP Inspect 프리프로세서 규칙에 대한 이벤트를 생성하려면 다음 표의 **Preprocessor Rule GID:SID** 열에서 규칙을 활성화할 수 있습니다. 자세한 내용은 32-20페이지의 규칙 상태 설정을/를 참조하십시오.

표 27-9 추가 HTTP Inspect 프리프로세서 규칙

프리프로세서 규칙 GID:SID	설명
120:5	HTTP 응답 트래픽에서 UTF-7 인코딩이 발견되는 경우 이벤트를 생성합니다. UTF-7은 7비트 패리티가 필요한 경우(예: SMTP 트래픽)에만 나타나야 합니다.
119:21	HTTP 요청 헤더에 `content-length` 필드가 여러 개 있는 경우 이벤트를 생성합니다.
119:24	HTTP 요청에 여러 개의 Host 헤더가 있는 경우 이벤트를 생성합니다.
119:28 120:8	활성화된 경우 이러한 규칙은 이벤트를 생성하지 않습니다.
119:32	트래픽에서 HTTP 버전 0.9가 발견되는 경우 이벤트를 생성합니다. TCP 스트림 컨피그레이션도 활성화되어야 합니다. 29-21페이지의 TCP 스트림 전처리 사용을/를 참조하십시오.
119:33	HTTP URI에 이스케이프되지 않은 공백이 포함된 경우 이벤트를 생성합니다.
119:34	TCP 연결에 24개 이상의 HTTP 요청이 포함된 경우 이벤트를 생성합니다.

Sun RPC 프리프로세서 사용

라이센스: 보호

RPC(Remote Procedure Call) 표준화는 규칙 엔진이 전체 레코드를 검사할 수 있도록, 프래그먼트된 RPC 레코드를 가져와서 단일 레코드로 표준화합니다. 예를 들어 공격자는 RPC `admind`가 실행되는 포트를 검색하려고 시도할 수 있습니다. 일부 UNIX 호스트는 RPC `admind`를 사용하여 원격 배포된 시스템 작업을 수행합니다. 호스트가 약한 인증을 수행하면 악의적인 사용자가 원격 관리를 제어할 수 있습니다. Snort ID 575의 표준 텍스트 규칙(generator ID: 1)은 부적절한 `portmap GETPORT` 요청을 식별하기 위해 특정 위치에서 내용을 검색하여 이 공격을 탐지합니다.

Ports

트래픽을 표준화할 포트를 지정합니다. 인터페이스에서 여러 포트를 쉼표로 구분하여 나열합니다. 일반적인 RPC 포트는 111 및 32771입니다. 네트워크가 다른 포트에 RPC 트래픽을 전송하는 경우 이들의 추가를 고려해보십시오.

Detect fragmented RPC records

RPC 프래그먼트된 레코드를 탐지합니다.

이 옵션에 대한 이벤트를 생성하려면 규칙 106:1 및 106:5를 활성화할 수 있습니다. 자세한 내용은 32-20페이지의 규칙 상태 설정을/를 참조하십시오.

Detect multiple records in one packet

패킷(또는 리어셈블된 패킷)당 둘 이상의 RPC 요청을 탐지합니다.

이 옵션에 대한 이벤트를 생성하려면 규칙 106:2를 활성화할 수 있습니다. 자세한 내용은 32-20 페이지의 규칙 상태 설정을/를 참조하십시오.

Detect fragmented record sums which exceed one fragment

현재 패킷 길이를 초과하는 리어셈블된 프래그먼트 레코드 길이를 탐지합니다.

이 옵션에 대한 이벤트를 생성하려면 규칙 106:3을 활성화할 수 있습니다. 자세한 내용은 32-20 페이지의 규칙 상태 설정을/를 참조하십시오.

Detect single fragment records which exceed the size of one packet

부분 레코드를 탐지합니다.

이 옵션에 대한 이벤트를 생성하려면 규칙 106:4를 활성화할 수 있습니다. 자세한 내용은 32-20 페이지의 규칙 상태 설정을/를 참조하십시오.

Sun RPC 프리프로세서 구성

라이센스: 보호

Sun RPC 프리프로세서를 구성하려면 다음 절차를 사용할 수 있습니다. Sun RPC 프리프로세서 컨피그레이션 옵션에 대한 자세한 내용은 27-45페이지의 Sun RPC 프리프로세서 사용을/를 참조하십시오.

Sun RPC 프리프로세서를 구성하려면

액세스: Admin/Intrusion Admin

1단계 **Policies > Access Control**을 선택하여 Access Control Policy 페이지를 표시한 다음 **Network Analysis Policy**를 클릭합니다.

Network Analysis Policy 페이지가 나타납니다.

2단계 수정할 정책 옆에 있는 수정 아이콘()을 클릭합니다.

다른 정책에 저장하지 않은 변경 사항이 있는 경우 변경 사항을 취소하고 계속 진행하려면 **OK**를 클릭합니다. 저장되지 않은 변경 사항을 다른 정책에 저장하는 방법에 대한 자세한 내용은 23-15페이지의 충돌 해결 및 정책 변경 사항 커밋을/를 참조하십시오.

Policy Information 페이지가 나타납니다.

3단계 왼쪽의 탐색 패널에서 **Settings**를 클릭합니다.

Settings 페이지가 나타납니다.

4단계 Application Layer Preprocessors 아래에서 **Sun RPC Configuration**이 활성화되었는지 여부에 따라 두 가지 선택 사항이 있습니다.

- 컨피그레이션이 활성화되어 있으면 **Edit**를 클릭합니다.
- 컨피그레이션이 비활성화되어 있으면 **Enabled**를 클릭한 다음 **Edit**를 클릭합니다.

Sun RPC Configuration 페이지가 나타납니다. 페이지 하단에 있는 메시지는 컨피그레이션이 포함된 네트워크 분석 정책 레이어를 식별합니다. 자세한 내용은 24-1페이지의 네트워크 분석 또는 침입 정책에서 레이어 사용을/를 참조하십시오.

5단계 RPC 트래픽을 디코딩할 포트 번호를 **Ports** 필드에 입력합니다. 포트가 여러 개인 경우 쉼표로 구분하십시오.

6단계 Sun RPC Configuration 페이지에서 다음 탐지 옵션을 선택하거나 선택 취소할 수 있습니다.

- **Detect fragmented RPC records**
- **Detect multiple records in one packet**
- **Detect fragmented record sums which exceed one packet**
- **Detect single fragment records which exceed the size of one packet**

7단계 정책을 저장하거나, 계속 수정하거나, 변경 사항을 취소하거나, 기반 정책의 기본 컨피그레이션 설정으로 돌아가거나, 시스템 캐시에 변경 사항이 남아 있는 상태로 종료합니다. 자세한 내용은 23-15페이지의 충돌 해결 및 정책 변경 사항 커밋을/를 참조하십시오.

SIP(Session Initiation Protocol) 디코딩

라이센스: 보호

SIP(Session Initiation Protocol)는 한 명 이상의 클라이언트 애플리케이션(인터넷 전화 통화, 멀티미디어 컨퍼런싱, 인스턴트 메시징, 온라인 게임, 파일 전송 등) 사용자에 대해 하나 이상의 세션 해체, 통화 설정 및 수정을 제공합니다. 각 SIP 요청의 *method* 필드는 요청의 목적을 식별하며, Request-URI는 요청을 전송할 곳을 지정합니다. 각 SIP 응답의 상태 코드는 요청된 작업의 출력을 나타냅니다.

SIP를 사용한 통화가 설정되면, RTP(Real-time Transport Protocol)는 이후의 오디오 및 비디오 통신을 담당합니다. 세션의 이 부분을 통화 채널, 데이터 채널 또는 오디오/비디오 데이터 채널이라고 부르기도 합니다. RTP는 데이터 채널 매개 변수 협상, 세션 선언 및 세션 초대에 대한 SIP 메시지 본문 내에서 SDP(Session Description Protocol)를 사용합니다.

SIP 프리프로세서는 다음을 수행합니다.

- SIP 2.0 트래픽 디코딩 및 분석
- SDP 데이터(있는 경우)를 포함한 SIP 헤더 및 메시지 본문 추출, 추가 검사를 위해 추출된 데이터를 규칙 엔진으로 전달
- 다음 조건이 탐지되고 해당 프리프로세서 규칙이 활성화되는 경우 이벤트 생성: SIP 패킷의 변칙 및 알려진 취약성, 순서가 틀리거나 유효하지 않은 통화 시퀀스
- 선택적으로 통화 채널 무시

프리프로세서는 SIP 메시지 본문에는 포함되지만 프리프로세서가 RTP 프로토콜 검사를 제공하지 않는 SDP 메시지에서 식별된 포트를 기반으로 RTP 채널을 식별합니다.

SIP 프리프로세서를 사용할 때에는 다음에 유의하십시오.

- UDP는 일반적으로 SIP에서 지원되지 않는 미디어 세션을 전달합니다. UDP 스트림 전처리는 SIP 프리프로세서에 대한 SIP 세션 추적을 제공합니다.
- SIP 규칙 키워드를 사용하면 SIP 패킷 헤더 또는 메시지 본문을 가리키고, 특정 SIP 메서드나 상태 코드에 대한 패킷으로 탐지를 제한할 수 있습니다. 자세한 내용은 36-63페이지의 SIP 키워드을/를 참조하십시오.
- 활성화된 경우 GID(generator ID) 140의 동반 규칙도 활성화하지 않는 한, 프리프로세서는 추출된 데이터를 규칙 엔진으로 전송하기 전에 이벤트를 생성하지 않습니다. 자세한 내용은 32-20페이지의 규칙 상태 설정을/를 참조하십시오.

자세한 내용은 다음 절을 참조하십시오.

- 27-47페이지의 SIP 프리프로세서 옵션 선택
- 27-49페이지의 SIP 프리프로세서 구성
- 27-50페이지의 추가 SIP 프리프로세서 규칙 활성화

SIP 프리프로세서 옵션 선택

라이센스: 보호

다음 목록에서는 수정할 수 있는 SIP 프리프로세서 옵션에 대해 설명합니다.

Maximum Request URI Length, **Maximum Call ID Length**, **Maximum Request Name Length**, **Maximum From Length**, **Maximum To Length**, **Maximum Via Length**, **Maximum Contact Length** 및 **Maximum Content Length** 옵션의 경우 1~65535바이트 범위로 지정할 수 있습니다. 또는 관련 규칙의 활성화 여부와 상관없이 옵션에 대한 이벤트 생성을 비활성화하려면 0을 지정할 수 있습니다.

다음 설명에서 프리프로세서 규칙이 언급되지 않은 경우 해당 옵션은 프리프로세서 규칙과 관련되지 않은 것입니다.

Ports

SIP 트래픽을 검사할 포트를 지정합니다. 0~65535의 정수를 지정할 수 있습니다. 포트 번호가 여러 개인 경우 쉼표로 구분하십시오.

Methods to Check

탐지할 SIP 메서드를 지정합니다. 현재 정의된 다음과 같은 SIP 메서드 중에서 지정할 수 있습니다.

```
ack, benotify, bye, cancel, do, info, invite, join, message,
notify, options, prack, publish, quath, refer, register,
service, sprack, subscribe, unsubscribe, update
```

메서드는 대/소문자를 구분하지 않습니다. 메서드 이름에는 알파벳 문자, 숫자 및 밑줄 문자를 사용할 수 있습니다. 다른 특수 문자는 허용되지 않습니다. 메서드가 여러 개인 경우 쉼표로 구분하십시오.

향후 새 SIP 메서드가 정의될 수 있으므로 현재 정의되지 않은 알파벳 문자열을 컨피그레이션에 포함할 수 있습니다. 시스템은 21개의 현재 정의된 메서드 및 11개의 추가 메서드를 포함하여 최대 32개의 메서드를 지원합니다. 시스템은 사용자가 구성할 수 있는 정의되지 않은 메서드는 무시합니다.

이 옵션에 대해 지정하는 메서드 외에, 침입 규칙에서 `sip_method` 키워드를 사용하여 지정된 총 32개의 메서드가 포함되어 있습니다. 자세한 내용은 36-63페이지의 sip_method을/를 참조하십시오.

Maximum Dialogs within a Session

한 스트림 세션 내 허용되는 최대 대화 상자 수를 지정합니다. 이 숫자보다 더 많은 대화 상자가 생성되면, 대화 상자 수가 지정된 최대 수를 초과하지 않을 때까지 가장 오래된 대화 상자부터 삭제됩니다. 또한 규칙 140:27이 활성화된 경우 이벤트가 트리거됩니다.

1~4194303의 정수를 지정할 수 있습니다.

Maximum Request URI Length

Request-URI 헤더 필드에서 허용할 최대 바이트 수를 지정합니다. 140:3이 활성화된 경우 더 긴 URI가 이벤트를 트리거합니다. 요청 URI 필드는 요청의 목적지 경로 또는 페이지를 나타냅니다.

Maximum Call ID Length

요청 또는 응답 Call-ID 헤더 필드에서 허용할 최대 바이트 수를 지정합니다. 140:5가 활성화된 경우 더 긴 Call-ID가 이벤트를 트리거합니다. Call-ID 필드는 요청 및 응답에서 SIP 세션을 고유하게 식별합니다.

Maximum Request Name Length

CSeq 트랜잭션 식별자에 지정하는 메서드의 이름인 요청 이름에서 허용할 최대 바이트 수를 지정합니다. 140:7이 활성화된 경우 더 긴 요청 이름이 이벤트를 트리거합니다.

Maximum From Length

요청 또는 응답 From 헤더 필드에서 허용할 최대 바이트 수를 지정합니다. 140:9가 활성화된 경우 더 긴 From이 이벤트를 트리거합니다. From 필드는 메시지 initiator를 식별합니다.

Maximum To Length

요청 또는 응답 To 헤더 필드에서 허용할 최대 바이트 수를 지정합니다. 140:11이 활성화된 경우 더 긴 To가 이벤트를 트리거합니다. To 필드는 메시지 recipient를 식별합니다.

Maximum Via Length

요청 또는 응답 Via 헤더 필드에서 허용할 최대 바이트 수를 지정합니다. 140:13이 활성화된 경우 더 긴 Via가 이벤트를 트리거합니다. Via 필드는 경로와 함께 요청을 제공하며, 응답에서는 수신 정보를 제공합니다.

Maximum Contact Length

요청 또는 응답 Contact 헤더 필드에서 허용할 최대 바이트 수를 지정합니다. 140:15가 활성화된 경우 더 긴 Contact가 이벤트를 트리거합니다. Contact 필드는 후속 메시지와 함께 연락처 위치를 지정하는 URI를 제공합니다.

Maximum Content Length

요청 또는 응답 메시지 본문의 내용에서 허용할 최대 바이트 수를 지정합니다. 140:16이 활성화된 경우 더 긴 내용이 이벤트를 트리거합니다.

Ignore Audio/Video Data Channel

데이터 채널 트래픽의 검사를 활성화 및 비활성화합니다. 이 옵션을 활성화하면 프리프로세서는 다른 비 데이터 채널 SIP 트래픽을 계속해서 검사합니다.

SIP 프리프로세서 구성

라이센스: 보호

SIP 프리프로세서를 구성하려면 다음 절차를 사용할 수 있습니다.

SIP 프리프로세서를 구성하려면

액세스: Admin/Intrusion Admin

1단계 **Policies > Access Control**을 선택하여 Access Control Policy 페이지를 표시한 다음 **Network Analysis Policy**를 클릭합니다.

Network Analysis Policy 페이지가 나타납니다.

2단계 수정할 정책 옆에 있는 수정 아이콘( )을 클릭합니다.

다른 정책에 저장하지 않은 변경 사항이 있는 경우 변경 사항을 취소하고 계속 진행하려면 **OK**를 클릭합니다. 저장되지 않은 변경 사항을 다른 정책에 저장하는 방법에 대한 자세한 내용은 23-15페이지의 충돌 해결 및 정책 변경 사항 커밋을/를 참조하십시오.

Policy Information 페이지가 나타납니다.

3단계 왼쪽의 탐색 패널에서 **Settings**를 클릭합니다.

Settings 페이지가 나타납니다.

4단계 Application Layer Preprocessors 아래에서 **SIP Configuration**이 활성화되었는지 여부에 따라 두 가지 선택 사항이 있습니다.

- 컨피그레이션이 활성화되어 있으면 **Edit**를 클릭합니다.
- 컨피그레이션이 비활성화되어 있으면 **Enabled**를 클릭한 다음 **Edit**를 클릭합니다.

SIP Configuration(IP 컨피그레이션) 페이지가 나타납니다. 페이지 하단에 있는 메시지는 컨피그레이션이 포함된 네트워크 분석 정책 레이어를 식별합니다. 자세한 내용은 24-1페이지의 네트워크 분석 또는 침입 정책에서 레이어 사용을/를 참조하십시오.

5단계 27-47페이지의 SIP 프리프로세서 옵션 선택에 설명된 옵션 중 하나를 수정할 수 있습니다.

6단계 정책을 저장하거나, 계속 수정하거나, 변경 사항을 취소하거나, 기반 정책의 기본 컨피그레이션 설정으로 돌아가거나, 시스템 캐시에 변경 사항이 남아 있는 상태로 종료합니다. 자세한 내용은 23-15페이지의 충돌 해결 및 정책 변경 사항 커밋을/를 참조하십시오.

추가 SIP 프리프로세서 규칙 활성화

라이센스: 보호

다음 표의 SIP 프리프로세서 규칙은 특정 컨피그레이션 옵션과 연결되어 있지 않습니다. 다른 SIP 프리프로세서 규칙과 마찬가지로, 이벤트를 생성하도록 하려면 이러한 규칙을 활성화해야 합니다. 규칙 활성화에 대한 자세한 내용은 32-20페이지의 규칙 상태 설정을/를 참조하십시오.

표 27-10 추가 SIP 프리프로세서 규칙

프리프로세서 규칙 GID:SID	설명
140:1	프리프로세서가 시스템에서 허용하는 SIP 세션의 최대 수를 모니터링하는 경우 이벤트를 생성합니다.
140:2	필수 Request_URI 필드가 SIP 요청에서 비어 있을 때 이벤트를 생성합니다.
140:4	Call-ID 헤더 필드가 SIP 요청 또는 응답에서 비어 있을 때 이벤트를 생성합니다.
140:6	SIP 요청 또는 응답 CSeq 필드의 시퀀스 번호 값이 231보다 작은 32비트 서명되지 않은 정수가 아닌 경우 이벤트를 생성합니다.
140:8	From 헤더 필드가 SIP 요청 또는 응답에서 비어 있을 때 이벤트를 생성합니다.
140:10	To 헤더 필드가 SIP 요청 또는 응답에서 비어 있을 때 이벤트를 생성합니다.
140:12	Via 헤더 필드가 SIP 요청 또는 응답에서 비어 있을 때 이벤트를 생성합니다.
140:14	필수 Contact 헤더 필드가 SIP 요청 또는 응답에서 비어 있을 때 이벤트를 생성합니다.
140:17	UDP 트래픽의 단일 SIP 요청 또는 응답 패킷에 여러 메시지가 포함되어 있을 때 이벤트를 생성합니다. 이전 SIP 버전에서는 다수의 메시지를 지원했지만 SIP 2.0에서는 패킷당 하나의 메시지만 지원합니다.
140:18	UDP 트래픽에서 SIP 요청 또는 응답의 메시지 본문 실제 길이가 SIP 요청 또는 응답의 Content-Length 헤더 필드에 지정된 값과 일치하지 않는 경우 이벤트를 생성합니다.
140:19	프리프로세서가 SIP 응답의 CSeq 필드에서 메서드 이름을 인식하지 못하는 경우 이벤트를 생성합니다.
140:20	SIP 서버가 인증된 초대 메시지에 대해 질문하지 않는 경우 이벤트를 생성합니다. 이는 InviteReplay billing 공격의 경우 발생합니다.
140:21	통화가 설정되기 전 세션 정보가 변경되는 경우 이벤트를 생성합니다. 이는 FakeBusy billing 공격의 경우 발생합니다.
140:22	응답 상태 코드가 3자리수가 아닌 경우 이벤트를 생성합니다.
140:23	Content-Type 헤더 필드가 콘텐츠 유형을 지정하지 않고 메시지 본문에 데이터가 포함되지 않은 경우 이벤트를 생성합니다.
140:24	SIP 버전이 1, 1.1 또는 2.0이 아닌 경우 이벤트를 생성합니다.
140:25	CSeq 헤더에 지정된 메서드와 메서드 필드가 SIP 요청에서 일치하지 않는 경우 이벤트를 생성합니다.
140:26	프리프로세서가 SIP 요청 메서드 필드에 명명된 메서드를 인식하지 못하는 경우 이벤트를 생성합니다.

GTP 명령 채널 구성

라이센스: 보호

GPRS(General Service Packet Radio) GTP(Tunneling Protocol)는 GTP 핵심 네트워크를 통한 통신을 제공합니다. GTP 프리프로세서는 GTP 트래픽에서 변칙을 탐지하고, 검사를 위해 명령 채널 신호 메시지를 규칙 엔진으로 전달합니다. GTP 명령 채널 트래픽에서 익스플로잇을 검사하려면 `gtp_version`, `gtp_type` 및 `gtp_info` 규칙 키워드를 사용할 수 있습니다.

단일 컨피그레이션 옵션을 사용하면 프리프로세서가 GTP 명령 채널 메시지에 대해 검사하는 포트의 기본 설정을 수정할 수 있습니다.

GTP 프리프로세서 규칙이 이벤트를 생성하도록 하려면 다음 표에 나와 있는 해당 규칙을 활성화해야 합니다. 규칙 활성화에 대한 자세한 내용은 32-20페이지의 규칙 상태 설정을/를 참조하십시오.

표 27-11 GTP 프리프로세서 규칙

프리프로세서 규칙 GID:SID	설명
143:1	프리프로세서가 잘못된 메시지 길이를 탐지하는 경우 이벤트를 생성합니다.
143:2	프리프로세서가 잘못된 정보 요소 길이를 탐지하는 경우 이벤트를 생성합니다.
143:3	프리프로세서가 순서가 잘못된 정보 요소를 탐지하는 경우 이벤트를 생성합니다.

GTP 프리프로세서가 GTP 명령 메시지를 모니터링하는 포트를 수정하려면 다음 절차를 사용할 수 있습니다.

GTP 명령 채널을 구성하려면

액세스: Admin/Intrusion Admin

1단계 **Policies > Access Control**을 선택하여 Access Control Policy 페이지를 표시한 다음 **Network Analysis Policy**를 클릭합니다.

Network Analysis Policy 페이지가 나타납니다.

2단계 수정할 정책 옆에 있는 수정 아이콘( )을 클릭합니다.

다른 정책에 저장하지 않은 변경 사항이 있는 경우 변경 사항을 취소하고 계속 진행하려면 **OK**를 클릭합니다. 저장되지 않은 변경 사항을 다른 정책에 저장하는 방법에 대한 자세한 내용은 23-15페이지의 충돌 해결 및 정책 변경 사항 커밋을/를 참조하십시오.

Policy Information 페이지가 나타납니다.

3단계 왼쪽의 탐색 패널에서 **Settings**를 클릭합니다.

Settings 페이지가 나타납니다.

4단계 Application Layer Preprocessors 아래에서 **GTP Command Channel Configuration**이 활성화되었는지 여부에 따라 두 가지 선택 사항이 있습니다.

- 컨피그레이션이 활성화되어 있으면 **Edit**를 클릭합니다.
- 컨피그레이션이 비활성화되어 있으면 **Enabled**를 클릭한 다음 **Edit**를 클릭합니다.

GTP Command Channel Configuration 페이지가 나타납니다.

5단계 선택적으로, 프리프로세서가 GTP 명령 메시지에 대해 검사하는 포트를 수정합니다. 0~65535의 정수를 지정할 수 있습니다. 여러 포트를 구분하려면 쉼표를 사용하십시오.

6단계 정책을 저장하거나, 계속 수정하거나, 변경 사항을 취소하거나, 기반 정책의 기본 컨피그레이션 설정으로 돌아가거나, 시스템 캐시에 변경 사항이 남아 있는 상태로 종료합니다. 자세한 내용은 23-15 페이지의 충돌 해결 및 정책 변경 사항 커밋을/를 참조하십시오.

IMAP 트래픽 디코딩

라이센스: 보호

IMAP(Internet Message Application Protocol)는 원격 IMAP 서버에서 이메일을 검색하는 데 사용됩니다. IMAP 프리프로세서는 서버-클라이언트 IMAP4 트래픽을 검사하며, 관련 프리프로세서 규칙이 활성화된 경우 비정상적인 트래픽에 대해 이벤트를 생성합니다. 프리프로세서는 또한 클라이언트-서버 IMAP4 트래픽의 이메일 첨부 파일을 추출 및 디코딩하고, 첨부 데이터를 규칙 엔진으로 전송할 수 있습니다. 첨부 데이터를 가리키려면 침입 규칙에서 `file_data` 키워드를 사용할 수 있습니다. 자세한 내용은 36-99페이지의 특정 페이로드 유형 가리키기을/를 참조하십시오.

추출 및 디코딩에는 여러 첨부 파일(있는 경우)이 포함되며, 여러 패킷에 걸쳐 있는 대규모 첨부 파일도 포함됩니다.

IMAP 프리프로세서 규칙이 이벤트를 생성하도록 하려면 규칙을 활성화해야 합니다. IMAP 프리프로세서 규칙은 GID(generator ID)가 141입니다. 자세한 내용은 32-20페이지의 규칙 상태 설정을/를 참조하십시오.

자세한 내용은 다음 절을 참조하십시오.

- 27-52페이지의 IMAP 프리프로세서 옵션 선택
- 27-53페이지의 IMAP 프리프로세서 구성
- 27-55페이지의 추가 IMAP 프리프로세서 규칙 활성화

IMAP 프리프로세서 옵션 선택

라이센스: 보호

다음 목록에서는 수정할 수 있는 IMAP 프리프로세서 옵션에 대해 설명합니다.

디코딩(MIME 이메일 첨부 파일에 디코딩이 필요하지 않은 경우 추출)에는 여러 첨부 파일 및 여러 패킷에 걸친 대형 첨부 파일이 포함됩니다.

Base64 Decoding Depth, **7-Bit/8-Bit/Binary Decoding Depth**, **Quoted-Printable Decoding Depth** 또는 **Unix-to-Unix Decoding Depth** 옵션에 대한 값이 다음에서 서로 다른 경우 가장 큰 값이 사용됩니다.

- 기본 네트워크 분석 정책
- 동일한 액세스 제어 정책의 네트워크 분석 규칙에 의해 호출된 다른 사용자 지정 네트워크 분석 정책

자세한 내용은 25-4페이지의 액세스 제어에 대한 기본 네트워크 분석 정책 설정 및 25-4페이지의 네트워크 분석 규칙을 사용하여 전처리할 트래픽 지정을/를 참조하십시오.

다음 설명에서 프리프로세서 규칙이 언급되지 않은 경우 해당 옵션은 프리프로세서 규칙과 관련되지 않은 것입니다.

Ports

IMAP 트래픽을 검사할 포트를 지정합니다. 0~65535의 정수를 지정할 수 있습니다. 포트 번호가 여러 개인 경우 쉼표로 구분하십시오.

Base64 Decoding Depth

각 Base64 인코딩 MIME 이메일 첨부 파일에서 추출하고 디코딩할 최대 바이트 수를 지정합니다. 1~65535바이트 범위로 지정할 수 있습니다. 또는 모든 Base64 데이터를 디코딩하려면 0을 지정합니다. Base64 데이터를 무시하려면 -1을 지정합니다.

4로 나누어지지 않는 양의 값은 다음 4의 배수로 반올림됩니다. 단, 65533, 65534 및 65535는 65532로 내림됩니다.

Base64 디코딩이 활성화된 경우 디코딩 실패 시 이벤트를 생성하려면 규칙 141:4를 활성화할 수 있습니다. 예를 들면 잘못된 인코딩 또는 손상된 데이터 때문에 디코딩이 실패할 수 있습니다.

7-Bit/8-Bit/Binary Decoding Depth

디코딩이 필요하지 않은 각 MIME 이메일 첨부 파일에서 추출할 최대 데이터 바이트를 수를 지정합니다. 이러한 첨부 파일 유형에는 7비트, 8비트, 이진 및 각종 multipart 콘텐츠 유형(예: 일반 텍스트, jpeg 이미지, mp3 파일 등)이 포함됩니다. 1~65535바이트 범위로 지정할 수 있습니다. 또는 패킷의 모든 데이터를 추출하려면 0을 지정합니다. 디코딩되지 않은 데이터를 무시하려면 -1을 지정합니다.

Quoted-Printable Decoding Depth

각 QP(quoted-printable) 인코딩 MIME 이메일 첨부 파일에서 추출하고 디코딩할 최대 바이트 수를 지정합니다. 1~65535바이트 범위로 지정할 수 있습니다. 또는 패킷의 모든 QP 인코딩 데이터를 디코딩하려면 0을 지정합니다. QP 인코딩 데이터를 무시하려면 -1을 지정합니다.

QP 디코딩이 활성화된 경우 디코딩 실패 시 이벤트를 생성하려면 규칙 141:6을 활성화할 수 있습니다. 예를 들면 잘못된 인코딩 또는 손상된 데이터 때문에 디코딩이 실패할 수 있습니다.

Unix-to-Unix Decoding Depth

각 Unix-to-Unix 인코딩(uuencoded) 이메일 첨부 파일에서 추출하고 디코딩할 최대 바이트 수를 지정합니다. 1~65535바이트 범위로 지정할 수 있습니다. 또는 패킷의 모든 uuencoded 데이터를 디코딩하려면 0을 지정합니다. Uuencoded 데이터를 무시하려면 -1을 지정합니다.

Unix-to-Unix 디코딩이 활성화된 경우 디코딩 실패 시 이벤트를 생성하려면 규칙 141:7을 활성화할 수 있습니다. 예를 들면 잘못된 인코딩 또는 손상된 데이터 때문에 디코딩이 실패할 수 있습니다.

IMAP 프리프로세서 구성

라이센스: 보호

IMAP 프리프로세서를 구성하려면 다음 절차를 사용할 수 있습니다. IMAP 프리프로세서 컨피그레이션 옵션에 대한 자세한 내용은 27-52페이지의 IMAP 프리프로세서 옵션 선택을/를 참조하십시오.

IMAP 프리프로세서를 구성하려면

액세스: Admin/Intrusion Admin

1단계 **Policies > Access Control**을 선택하여 Access Control Policy 페이지를 표시한 다음 **Network Analysis Policy**를 클릭합니다.

Network Analysis Policy 페이지가 나타납니다.

2단계 수정할 정책 옆에 있는 수정 아이콘( )을 클릭합니다.

다른 정책에 저장하지 않은 변경 사항이 있는 경우 변경 사항을 취소하고 계속 진행하려면 **OK**를 클릭합니다. 저장되지 않은 변경 사항을 다른 정책에 저장하는 방법에 대한 자세한 내용은 23-15페이지의 충돌 해결 및 정책 변경 사항 커밋을/를 참조하십시오.

Policy Information 페이지가 나타납니다.

3단계 왼쪽의 탐색 패널에서 **Settings**를 클릭합니다.

Settings 페이지가 나타납니다.

4단계 Application Layer Preprocessors 아래에서 **IMAP Configuration**이 활성화되었는지 여부에 따라 두 가지 선택 사항이 있습니다.

- 컨피그레이션이 활성화되어 있으면 **Edit**를 클릭합니다.
- 컨피그레이션이 비활성화되어 있으면 **Enabled**를 클릭한 다음 **Edit**를 클릭합니다.

IMAP Configuration(IP 컨피그레이션) 페이지가 나타납니다. 페이지 하단에 있는 메시지는 컨피그레이션이 포함된 네트워크 분석 정책 레이어를 식별합니다. 자세한 내용은 24-1페이지의 네트워크 분석 또는 침입 정책에서 레이어 사용을/를 참조하십시오.

5단계 IMAP 트래픽을 디코딩할 하는 **Ports**를 지정합니다. 포트 번호가 여러 개인 경우 쉼표로 구분하십시오.

6단계 다음 이메일 첨부 파일 유형의 조합에서 추출 및 디코딩할 데이터의 최대 바이트 수를 지정합니다.

- **Base64 Decoding Depth**
- **7-Bit/8-Bit/Binary Decoding Depth**(일반 텍스트, jpeg 이미지, mp3 파일 등 각종 multipart 콘텐츠 유형 포함)
- **Quoted-Printable Decoding Depth**
- **Unix-to-Unix Decoding Depth**

각 유형에 대해 1~65535바이트 범위로 지정할 수 있습니다. 또는 패킷의 모든 데이터를 추출 및 디코딩(필요 시)하려면 0을 지정합니다. 첨부 파일 유형의 데이터를 무시하려면 -1을 지정합니다.

첨부 데이터를 검사하려면 침입 규칙에서 `file_data` 규칙 키워드를 사용할 수 있습니다. 자세한 내용은 36-99페이지의 특정 페이로드 유형 가리키기을/를 참조하십시오.

7단계 정책을 저장하거나, 계속 수정하거나, 변경 사항을 취소하거나, 기반 정책의 기본 컨피그레이션 설정으로 돌아가거나, 시스템 캐시에 변경 사항이 남아 있는 상태로 종료합니다. 자세한 내용은 23-15페이지의 충돌 해결 및 정책 변경 사항 커밋을/를 참조하십시오.

추가 IMAP 프리프로세서 규칙 활성화

라이센스: 보호

다음 표의 IMAP 프리프로세서 규칙은 특정 컨피그레이션 옵션과 연결되어 있지 않습니다. 다른 IMAP 프리프로세서 규칙과 마찬가지로, 이벤트를 생성하도록 하려면 이러한 규칙을 활성화해야 합니다. 규칙 활성화에 대한 자세한 내용은 32-20페이지의 규칙 상태 설정을/를 참조하십시오.

표 27-12 추가 IMAP 프리프로세서 규칙

프리프로세서 규칙 GID:SID	설명
141:1	프리프로세서가 RFC 3501에 정의되지 않은 클라이언트 명령을 탐지하는 경우 이벤트를 생성합니다.
141:2	프리프로세서가 RFC 3501에 정의되지 않은 서버 응답을 탐지하는 경우 이벤트를 생성합니다.
141:3	프리프로세서가 시스템에서 허용하는 최대 데이터 양을 사용하는 경우 이벤트를 생성합니다. 이 시점에서 프리프로세서는 메모리가 사용 가능해질 때까지 디코딩을 중지합니다.

POP 트래픽 디코딩

라이센스: 보호

POP(Post Office Protocol)는 원격 POP 메일 서버에서 이메일을 검색하는 데 사용됩니다. POP 프리프로세서는 서버-클라이언트 POP3 트래픽을 검사하며, 관련 프리프로세서 규칙이 활성화된 경우 비정상적인 트래픽에 대해 이벤트를 생성합니다. 프리프로세서는 또한 클라이언트-서버 POP3 트래픽의 이메일 첨부 파일을 추출 및 디코딩하고, 첨부 데이터를 규칙 엔진으로 전송할 수 있습니다. 첨부 데이터를 가리키려면 침입 규칙에서 `file_data` 키워드를 사용할 수 있습니다. 자세한 내용은 36-99페이지의 특정 페이로드 유형 가리키기을/를 참조하십시오.

추출 및 디코딩에는 여러 첨부 파일(있는 경우)이 포함되며, 여러 패킷에 걸쳐 있는 대규모 첨부 파일도 포함됩니다.

POP 프리프로세서 규칙이 이벤트를 생성하도록 하려면 규칙을 활성화해야 합니다. POP 프리프로세서 규칙은 GID(generator ID)가 142입니다. 자세한 내용은 32-20페이지의 규칙 상태 설정을/를 참조하십시오.

자세한 내용은 다음 절을 참조하십시오.

- 27-56페이지의 POP 프리프로세서 옵션 선택
- 27-57페이지의 POP 프리프로세서 구성
- 27-58페이지의 추가 POP 프리프로세서 규칙 활성화

POP 프리프로세서 옵션 선택

라이센스: 보호

다음 목록에서는 수정할 수 있는 POP 프리프로세서 옵션에 대해 설명합니다.

디코딩(MIME 이메일 첨부 파일에 디코딩이 필요하지 않은 경우 추출)에는 여러 첨부 파일 및 여러 패킷에 걸친 대형 첨부 파일이 포함됩니다.

Base64 Decoding Depth, **7-Bit/8-Bit/Binary Decoding Depth**, **Quoted-Printable Decoding Depth** 또는 **Unix-to-Unix Decoding Depth** 옵션에 대한 값이 액세스 제어 정책의 기본 작업과 관련된 침입 정책 및 액세스 제어 규칙과 관련된 침입 정책에서 서로 다른 경우 가장 큰 값이 사용됩니다.

다음 설명에서 프리프로세서 규칙이 언급되지 않은 경우 해당 옵션은 프리프로세서 규칙과 관련되지 않은 것입니다.

Ports

POP 트래픽을 검사할 포트를 지정합니다. 0~65535의 정수를 지정할 수 있습니다. 포트 번호가 여러 개인 경우 쉼표로 구분하십시오.

Base64 Decoding Depth

각 Base64 인코딩 MIME 이메일 첨부 파일에서 추출하고 디코딩할 최대 바이트 수를 지정합니다. 1~65535바이트 범위로 지정할 수 있습니다. 또는 모든 Base64 데이터를 디코딩하려면 0을 지정합니다. Base64 데이터를 무시하려면 -1을 지정합니다.

4로 나누어지지 않는 양의 값은 다음 4의 배수로 반올림됩니다. 단, 65533, 65534 및 65535는 65532로 내림됩니다.

Base64 디코딩이 활성화된 경우 디코딩 실패 시 이벤트를 생성하려면 규칙 142:4를 활성화할 수 있습니다. 예를 들면 잘못된 인코딩 또는 손상된 데이터 때문에 디코딩이 실패할 수 있습니다. 자세한 내용은 32-20페이지의 규칙 상태 설정을/를 참조하십시오.

7-Bit/8-Bit/Binary Decoding Depth

디코딩이 필요하지 않은 각 MIME 이메일 첨부 파일에서 추출할 최대 데이터 바이트를 수를 지정합니다. 이러한 첨부 파일 유형에는 7비트, 8비트, 이진 및 각종 multipart 콘텐츠 유형(예: 일반 텍스트, jpeg 이미지, mp3 파일 등)이 포함됩니다. 1~65535바이트 범위로 지정할 수 있습니다. 또는 패킷의 모든 데이터를 추출하려면 0을 지정합니다. 디코딩되지 않은 데이터를 무시하려면 -1을 지정합니다.

Quoted-Printable Decoding Depth

각 QP(quoted-printable) 인코딩 MIME 이메일 첨부 파일에서 추출하고 디코딩할 최대 바이트 수를 지정합니다. 1~65535바이트 범위로 지정할 수 있습니다. 또는 패킷의 모든 QP 인코딩 데이터를 디코딩하려면 0을 지정합니다. QP 인코딩 데이터를 무시하려면 -1을 지정합니다.

QP 디코딩이 활성화된 경우 디코딩 실패 시 이벤트를 생성하려면 규칙 142:6을 활성화할 수 있습니다. 예를 들면 잘못된 인코딩 또는 손상된 데이터 때문에 디코딩이 실패할 수 있습니다. 자세한 내용은 32-20페이지의 규칙 상태 설정을/를 참조하십시오.

Unix-to-Unix Decoding Depth

각 Unix-to-Unix 인코딩(uuencoded) 이메일 첨부 파일에서 추출하고 디코딩할 최대 바이트 수를 지정합니다. 1~65535바이트 범위로 지정할 수 있습니다. 또는 패킷의 모든 uuencoded 데이터를 디코딩하려면 0을 지정합니다. Uuencoded 데이터를 무시하려면 -1을 지정합니다.

Unix-to-Unix 디코딩이 활성화된 경우 디코딩 실패 시 이벤트를 생성하려면 규칙 142:7을 활성화할 수 있습니다. 예를 들면 잘못된 인코딩 또는 손상된 데이터 때문에 디코딩이 실패할 수 있습니다. 자세한 내용은 32-20페이지의 규칙 상태 설정을/를 참조하십시오.

POP 프리프로세서 구성

라이센스: 보호

POP 프리프로세서를 구성하려면 다음 절차를 사용할 수 있습니다. POP 프리프로세서 컨피그레이션 옵션에 대한 자세한 내용은 27-56페이지의 POP 프리프로세서 옵션 선택을/를 참조하십시오.

POP 프리프로세서를 구성하려면

액세스: Admin/Intrusion Admin

1단계 **Policies > Access Control**을 선택하여 Access Control Policy 페이지를 표시한 다음 **Network Analysis Policy**를 클릭합니다.

Network Analysis Policy 페이지가 나타납니다.

2단계 수정할 정책 옆에 있는 수정 아이콘()을 클릭합니다.

다른 정책에 저장하지 않은 변경 사항이 있는 경우 변경 사항을 취소하고 계속 진행하려면 **OK**를 클릭합니다. 저장되지 않은 변경 사항을 다른 정책에 저장하는 방법에 대한 자세한 내용은 23-15페이지의 충돌 해결 및 정책 변경 사항 커밋을/를 참조하십시오.

Policy Information 페이지가 나타납니다.

3단계 왼쪽의 탐색 패널에서 **Settings**를 클릭합니다.

Settings 페이지가 나타납니다.

4단계 Application Layer Preprocessors 아래에서 **POP Configuration**이 활성화되었는지 여부에 따라 두 가지 선택 사항이 있습니다.

- 컨피그레이션이 활성화되어 있으면 **Edit**를 클릭합니다.
- 컨피그레이션이 비활성화되어 있으면 **Enabled**를 클릭한 다음 **Edit**를 클릭합니다.

POP Configuration(IP 컨피그레이션) 페이지가 나타납니다. 페이지 하단에 있는 메시지는 컨피그레이션이 포함된 네트워크 분석 정책 레이어를 식별합니다. 자세한 내용은 24-1페이지의 네트워크 분석 또는 침입 정책에서 레이어 사용을/를 참조하십시오.

5단계 IMAP 트래픽을 디코딩할 하는 **Ports**를 지정합니다. 포트 번호가 여러 개인 경우 쉼표로 구분하십시오.

6단계 다음 이메일 첨부 파일 유형의 조합에서 추출 및 디코딩할 데이터의 최대 바이트 수를 지정합니다.

- **Base64 Decoding Depth**
- **7-Bit/8-Bit/Binary Decoding Depth**(일반 텍스트, jpeg 이미지, mp3 파일 등 각종 multipart 콘텐츠 유형 포함)
- **Quoted-Printable Decoding Depth**
- **Unix-to-Unix Decoding Depth**

각 유형에 대해 1~65535바이트 범위로 지정할 수 있습니다. 또는 패킷의 모든 데이터를 추출 및 디코딩(필요 시)하려면 0을 지정합니다. 첨부 파일 유형의 데이터를 무시하려면 -1을 지정합니다.

첨부 데이터를 검사하려면 침입 규칙에서 `file_data` 규칙 키워드를 사용할 수 있습니다. 자세한 내용은 36-99페이지의 특정 페이로드 유형 가리키기을/를 참조하십시오.

7단계 정책을 저장하거나, 계속 수정하거나, 변경 사항을 취소하거나, 기반 정책의 기본 컨피그레이션 설정으로 돌아가거나, 시스템 캐시에 변경 사항이 남아 있는 상태로 종료합니다. 자세한 내용은 23-15페이지의 충돌 해결 및 정책 변경 사항 커밋을/를 참조하십시오.

추가 POP 프리프로세서 규칙 활성화

라이센스: 보호

다음 표의 POP 프리프로세서 규칙은 특정 컨피그레이션 옵션과 연결되어 있지 않습니다. 다른 POP 프리프로세서 규칙과 마찬가지로, 이벤트를 생성하도록 하려면 이러한 규칙을 활성화해야 합니다. 규칙 활성화에 대한 자세한 내용은 32-20페이지의 규칙 상태 설정을/를 참조하십시오.

표 27-13 추가 POP 프리프로세서 규칙

프리프로세서 규칙 GID:SID	설명
142:1	프리프로세서가 RFC 1939에 정의되지 않은 클라이언트 명령을 탐지하는 경우 이벤트를 생성합니다.
142:2	프리프로세서가 RFC 1939에 정의되지 않은 서버 응답을 탐지하는 경우 이벤트를 생성합니다.
142:3	프리프로세서가 시스템에서 허용하는 최대 데이터 양을 사용하는 경우 이벤트를 생성합니다. 이 시점에서 프리프로세서는 메모리가 사용 가능해질 때까지 디코딩을 중지합니다.

SMTP 트래픽 디코딩

라이센스: 보호

SMTP 프리프로세서는 규칙 엔진에 SMTP 명령을 표준화하도록 지시합니다. 프리프로세서는 또한 클라이언트-서버 트래픽에서 이메일 첨부 파일을 추출 및 디코딩할 수 있으며, 소프트웨어 버전에 따라 SMTP 트래픽에서 트리거한 침입 이벤트를 표시할 때 컨텍스트를 제공하기 위해 이메일 파일 이름, 주소 및 헤더 데이터를 추출할 수 있습니다.

SMTP 프리프로세서를 사용할 때에는 다음에 유의하십시오.

- GID(generator ID)가 124인 SMTP 프리프로세서 규칙을 활성화해야 이러한 규칙에서 이벤트를 생성할 수 있습니다. 자세한 내용은 32-20페이지의 규칙 상태 설정을/를 참조하십시오.

자세한 내용은 다음 절을 참조하십시오.

- 27-58페이지의 SMTP 디코딩 이해
- 27-63페이지의 SMTP 디코딩 구성
- 27-65페이지의 SMTP 최대 디코딩 메모리 알림 활성화

SMTP 디코딩 이해

라이센스: 보호

표준화를 활성화 또는 비활성화할 수 있으며, SMTP 디코더가 탐지하는 비정상적인 트래픽의 유형을 제어하기 위해 옵션을 구성할 수 있습니다.

디코딩(MIME 이메일 첨부 파일에 디코딩이 필요하지 않은 경우 추출)에는 여러 첨부 파일 및 여러 패킷에 걸친 대형 첨부 파일이 포함됩니다.

Base64 Decoding Depth, **7-Bit/8-Bit/Binary Decoding Depth**, **Quoted-Printable Decoding Depth** 또는 **Unix-to-Unix Decoding Depth** 옵션에 대한 값이 액세스 제어 정책의 기본 작업과 관련된 침입 정책 및 액세스 제어 규칙과 관련된 침입 정책에서 서로 다른 경우 가장 큰 값이 사용됩니다.

다음 설명에서 프리프로세서 규칙이 언급되지 않은 경우 해당 옵션은 프리프로세서 규칙과 관련되지 않은 것입니다.

Ports

SMTP 트래픽을 표준화할 포트를 지정합니다. 0~65535의 정수를 지정할 수 있습니다. 포트가 여러 개인 경우 쉼표로 구분하십시오.

Stateful Inspection

이 옵션을 선택하면, SMTP 디코더는 상태를 저장하고 개별 패킷에 대한 세션 컨텍스트를 제공하며, 리어셈블된 세션만 검사합니다. 이 옵션을 선택하지 않으면, 세션 컨텍스트 없이 각 개별 패킷을 분석합니다.

Normalize

All로 설정하면 모든 명령이 표준화됩니다. 명령 뒤에 공백 문자가 두 개 이상 있는지 확인합니다.

None으로 설정하면 명령을 표준화하지 않습니다.

Cmds로 설정하면 **Custom Commands**에 나열된 명령만 표준화합니다.

Custom Commands

Normalize가 Cmds로 설정된 경우 나열된 명령을 표준화합니다.

텍스트 상자에 표준화해야 할 명령을 지정합니다. 명령 뒤에 공백 문자가 두 개 이상 있는지 확인합니다.

공백(ASCII 0x20) 및 탭(ASCII 0x09) 문자는 표준화 과정에서 공백 문자로 계산됩니다.

Ignore Data

메일 데이터는 처리하지 않고, MIME 메일 헤더 데이터만 처리합니다.

Ignore TLS Data

Transport Layer Security 프로토콜에서 암호화된 데이터를 처리하지 않습니다.

No Alerts

동반 프리프로세서 규칙이 활성화된 경우 침입 이벤트를 비활성화합니다.

Detect Unknown Commands

SMTP 트래픽에서 알려지지 않은 명령을 탐지합니다.

이 옵션에 대한 이벤트를 생성하려면 규칙 124:5 및 124:6을 활성화할 수 있습니다. 자세한 내용은 32-20페이지의 규칙 상태 설정을/를 참조하십시오.

Max Command Line Len

SMTP 명령줄이 이 값보다 긴 경우를 탐지합니다. 명령줄 길이를 탐지하지 않으려면 0을 지정합니다.

Simple Mail Transfer Protocol의 Network Working Group 사양인 RFC 2821에서는 최대 명령줄 길이로 512를 권장합니다.

이 옵션에 대한 이벤트를 생성하려면 규칙 124:1을 활성화할 수 있습니다. 자세한 내용은 32-20 페이지의 규칙 상태 설정을/를 참조하십시오.

Max Header Line Len

SMTP 데이터 헤더 줄이 이 값보다 긴 경우를 탐지합니다. 데이터 헤더 줄을 탐지하지 않으려면 0을 지정합니다.

이 옵션에 대한 이벤트를 생성하려면 규칙 124:2 및 124:7을 활성화할 수 있습니다. 자세한 내용은 32-20페이지의 규칙 상태 설정을/를 참조하십시오.

Max Response Line Len

SMTP 응답 줄이 이 값보다 긴 경우를 탐지합니다. 응답 줄 길이를 탐지하지 않으려면 0을 지정합니다.

RFC 2821에서는 최대 응답 줄 길이로 512를 권장합니다.

이 옵션에 대한 이벤트를 생성하려면 규칙 124:3을 활성화할 수 있습니다. 자세한 내용은 32-20 페이지의 규칙 상태 설정을/를 참조하십시오.

Alt Max Command Line Len

지정된 명령에 대한 SMTP 명령줄이 이 값보다 긴 경우를 탐지합니다. 지정된 명령에 대한 명령줄 길이를 탐지하지 않으려면 0을 지정합니다. 여러 명령에 대해 서로 다른 기본 줄 길이가 설정됩니다.

이 설정은 지정된 명령에 대한 Max Command Line Len 설정을 재정의합니다.

이 옵션에 대한 이벤트를 생성하려면 규칙 124:3을 활성화할 수 있습니다. 자세한 내용은 32-20 페이지의 규칙 상태 설정을/를 참조하십시오.

Invalid Commands

이러한 명령이 클라이언트 측에서 전송되는지 여부를 탐지합니다.

이 옵션에 대한 이벤트를 생성하려면 규칙 124:5 및 124:6을 활성화할 수 있습니다. 자세한 내용은 32-20페이지의 규칙 상태 설정을/를 참조하십시오.

Valid Commands

이 목록에 있는 명령을 허용합니다.

이 목록이 비어 있더라도 프리프로세서는 다음의 유효한 명령을 허용합니다. ATRN AUTH BDAT DATA DEBUG EHLO EMAL ESAM ESND ESOM ETRN EVFY EXPN HELO HELP IDENT MAIL NOOP ONEX QUEU QUIT RCPT RSET SAML SEND SIZE SOML STARTTLS TICK TIME TURN TURNME VERB VRFY XADR XAUTH XCIR XEXCH50 X-EXPS XGEN XLICENSE X-LINK2STATE XQUE XSTA XTRN XUSR

참고 RCPT TO 및 MAIL FROM은 SMTP 명령입니다. 프리프로세서 컨피그레이션은 각각 RCPT 및 MAIL 명령 이름을 사용합니다. 코드 내에서 프리프로세서는 RCPT 및 MAIL을 올바른 명령 이름에 매핑합니다.

이 옵션에 대한 이벤트를 생성하려면 규칙 124:4를 활성화할 수 있습니다. 자세한 내용은 32-20 페이지의 규칙 상태 설정을/를 참조하십시오.

Data Commands

SMTP DATA 명령이 RFC 5321에 따라 데이터를 전송하는 것과 동일한 방법으로 데이터 전송을 시작하는 명령을 나열합니다. 공백을 사용하여 여러 명령을 구분하십시오.

Binary Data Commands

BDAT 명령이 RFC 3030에 따라 데이터를 전송하는 것과 유사한 방법으로 데이터 전송을 시작하는 명령을 나열합니다. 공백을 사용하여 여러 명령을 구분하십시오.

Authentication Commands

클라이언트와 서버 간 인증 교환을 시작하는 명령을 나열합니다. 공백을 사용하여 여러 명령을 구분하십시오.

Detect xlink2state

X-Link2State Microsoft Exchange 버퍼 데이터 오버플로 공격의 일부인 패킷을 탐지합니다. 인라인 구축에서 시스템은 그러한 패킷도 삭제합니다.

이 옵션에 대한 이벤트를 생성하려면 규칙 124:8을 활성화할 수 있습니다. 자세한 내용은 32-20 페이지의 규칙 상태 설정을/를 참조하십시오.

Base64 Decoding Depth

Ignore Data가 비활성화된 경우 각 Base64 인코딩 MIME 이메일 첨부 파일에서 추출하고 디코딩할 최대 바이트 수를 지정합니다. 1~65535바이트 범위로 지정할 수 있습니다. 또는 모든 Base64 데이터를 디코딩하려면 0을 지정합니다. Base64 데이터를 무시하려면 -1을 지정합니다. **Ignore Data**가 선택된 경우 프리프로세서는 데이터를 디코딩하지 않습니다.

4로 나누어지지 않는 양의 값은 다음 4의 배수로 반올림됩니다. 단, 65533, 65534 및 65535는 65532로 내림됩니다.

Base64 디코딩이 활성화된 경우 디코딩 실패 시 이벤트를 생성하려면 규칙 124:10을 활성화할 수 있습니다. 예를 들면 잘못된 인코딩 또는 손상된 데이터 때문에 디코딩이 실패할 수 있습니다. 자세한 내용은 32-20페이지의 규칙 상태 설정을/를 참조하십시오.

이 옵션은 폐기된 옵션인 **Enable MIME Decoding** 및 **Maximum MIME Decoding Depth**를 교체합니다. 이 두 옵션은 이전 버전과의 호환성을 위해 기존 침입 정책에서 여전히 지원됩니다.

7-Bit/8-Bit/Binary Decoding Depth

Ignore Data가 비활성화된 경우 디코딩이 필요하지 않은 각 MIME 이메일 첨부 파일에서 추출할 최대 데이터 바이트를 수를 지정합니다. 이러한 첨부 파일 유형에는 7비트, 8비트, 이진 및 각종 multipart 콘텐츠 유형(예: 일반 텍스트, jpeg 이미지, mp3 파일 등)이 포함됩니다. 1~65535바이트 범위로 지정할 수 있습니다. 또는 패킷의 모든 데이터를 추출하려면 0을 지정합니다. 디코딩되지 않은 데이터를 무시하려면 -1을 지정합니다. **Ignore Data**가 선택된 경우 프리프로세서는 데이터를 추출하지 않습니다.

Quoted-Printable Decoding Depth

Ignore Data가 비활성화된 경우 각 QP(quoted-printable) 인코딩 MIME 이메일 첨부 파일에서 추출하고 디코딩할 최대 바이트 수를 지정합니다.

1~65535바이트 범위로 지정할 수 있습니다. 또는 패킷의 모든 QP 인코딩 데이터를 디코딩하려면 0을 지정합니다. QP 인코딩 데이터를 무시하려면 -1을 지정합니다. **Ignore Data**가 선택된 경우 프리프로세서는 데이터를 디코딩하지 않습니다.

QP 디코딩이 활성화된 경우 디코딩 실패 시 이벤트를 생성하려면 규칙 124:11을 활성화할 수 있습니다. 예를 들면 잘못된 인코딩 또는 손상된 데이터 때문에 디코딩이 실패할 수 있습니다. 자세한 내용은 32-20페이지의 규칙 상태 설정을/를 참조하십시오.

Unix-to-Unix Decoding Depth

Ignore Data가 비활성화된 경우 각 Unix-to-Unix 인코딩(uuencoded) 이메일 첨부 파일에서 추출하고 디코딩할 최대 바이트 수를 지정합니다. 1~65535바이트 범위로 지정할 수 있습니다. 또는 패킷의 모든 uuencoded 데이터를 디코딩하려면 0을 지정합니다. Uuencoded 데이터를 무시하려면 -1을 지정합니다. **Ignore Data**가 선택된 경우 프리프로세서는 데이터를 디코딩하지 않습니다.

Unix-to-Unix 디코딩이 활성화된 경우 디코딩 실패 시 이벤트를 생성하려면 규칙 124:13을 활성화할 수 있습니다. 예를 들면 잘못된 인코딩 또는 손상된 데이터 때문에 디코딩이 실패할 수 있습니다. 자세한 내용은 32-20페이지의 규칙 상태 설정을/를 참조하십시오.

Log MIME Attachment Names

MIME Content-Disposition 헤더에서 MIME 첨부 파일 이름의 추출을 활성화하고, 파일 이름을 해당 세션에 대해 생성된 모든 침입 이벤트와 연결합니다. 여러 파일 이름이 지원됩니다.

이 옵션이 활성화된 경우 침입 이벤트 테이블 보기의 Email Attachment 열에서 이벤트와 관련된 파일 이름을 볼 수 있습니다. 자세한 내용은 41-10페이지의 침입 이벤트 이해을/를 참조하십시오.

Log To Addresses

SMTP RCPT TO 명령에서 수신자 이메일 주소의 추출을 활성화하고, 수신자 주소를 해당 세션에 대해 생성된 모든 침입 이벤트와 연결합니다. 여러 수신자가 지원됩니다.

이 옵션이 활성화된 경우 침입 이벤트 테이블 보기의 Email Recipient 열에서 이벤트와 관련된 수신자를 볼 수 있습니다. 자세한 내용은 41-10페이지의 침입 이벤트 이해을/를 참조하십시오.

Log From Addresses

SMTP MAIL FROM 명령에서 전송자 이메일 주소의 추출을 활성화하고, 전송자 주소를 해당 세션에 대해 생성된 모든 침입 이벤트와 연결합니다. 여러 전송자 주소가 지원됩니다.

이 옵션이 활성화된 경우 침입 이벤트 테이블 보기의 Email Sender 열에서 이벤트와 관련된 전송자를 볼 수 있습니다. 자세한 내용은 41-10페이지의 침입 이벤트 이해을/를 참조하십시오.

Log Headers

이메일 헤더의 추출을 활성화합니다. 추출할 바이트 수는 **Header Log Depth**에 대해 지정된 값으로 결정됩니다.

이메일 헤더 데이터를 패턴으로 사용하는 침입 규칙을 작성하려면 `content` 또는 `protected_content` 키워드를 사용할 수 있습니다. 침입 이벤트 패킷 보기에서도 추출된 이메일 헤더를 볼 수 있습니다. 자세한 내용은 36-17페이지의 내용 일치 제한 및 41-22페이지의 패킷 보기 사용을/를 참조하십시오.

Header Log Depth

Log Headers가 활성화된 경우 추출할 이메일 헤더의 바이트 수를 지정합니다. 0~20480바이트를 지정할 수 있습니다. 값을 0으로 지정하면 **Log Headers**가 비활성화됩니다.

SMTP 디코딩 구성

라이센스: 보호

침입 정책의 SMTP Configuration 페이지를 사용하여 SMTP 표준화를 구성할 수 있습니다. SMTP 프리프로세서 컨피그레이션 옵션에 대한 자세한 내용은 27-58페이지의 SMTP 디코딩 이해을/를 참조하십시오.

SMTP 디코딩 옵션을 구성하려면

액세스: Admin/Intrusion Admin

1단계 **Policies > Access Control**을 선택하여 Access Control Policy 페이지를 표시한 다음 **Network Analysis Policy**를 클릭합니다.

Network Analysis Policy 페이지가 나타납니다.

2단계 수정할 정책 옆에 있는 수정 아이콘()을 클릭합니다.

다른 정책에 저장하지 않은 변경 사항이 있는 경우 변경 사항을 취소하고 계속 진행하려면 **OK**를 클릭합니다. 저장되지 않은 변경 사항을 다른 정책에 저장하는 방법에 대한 자세한 내용은 23-15페이지의 충돌 해결 및 정책 변경 사항 커밋을/를 참조하십시오.

Policy Information 페이지가 나타납니다.

3단계 왼쪽의 탐색 패널에서 **Settings**를 클릭합니다.

Settings 페이지가 나타납니다.

4단계 Application Layer Preprocessors 아래에서 **SMTP Configuration**이 활성화되었는지 여부에 따라 두 가지 선택 사항이 있습니다.

- 컨피그레이션이 활성화되어 있으면 **Edit**를 클릭합니다.
- 컨피그레이션이 비활성화되어 있으면 **Enabled**를 클릭한 다음 **Edit**를 클릭합니다.

SMTP Configuration(IP 컨피그레이션) 페이지가 나타납니다. 다음 그림에서는 방어 센터 패킷 보기를 보여줍니다. 페이지 하단에 있는 메시지는 컨피그레이션이 포함된 네트워크 분석 정책 레이어를 식별합니다. 자세한 내용은 24-1페이지의 네트워크 분석 또는 침입 정책에서 레이어 사용을/를 참조하십시오.

5단계 SMTP 트래픽을 디코딩해야 할 **Ports**를 쉼표로 구분하여 지정합니다.

6단계 SMTP 패킷을 포함하는 리어셈블된 TCP 스트림을 검사하려면 **Stateful Inspection**을 선택합니다. 리어셈블되지 않은 SMTP 패킷만 검사하려면 **Stateful Inspection**의 선택을 취소합니다.

7단계 표준화 옵션을 구성합니다.

- 모든 명령을 표준화하려면 **All**을 선택합니다.
- **Custom Commands**에 지정된 명령만 표준화하려면 **Cmds**를 선택하고 표준화할 명령을 지정합니다. 공백을 사용하여 명령을 구분하십시오.
- 명령을 표준화하지 않으려면 **None**을 선택합니다.
- MIME 메일 헤더 데이터를 제외한 메일 데이터를 무시하려면 **Ignore Data**를 선택합니다.
- Transport Security Layer 프로토콜에서 암호화된 데이터를 무시하려면 **Ignore TLS Data**를 선택합니다.
- 동반 프리프로세서 규칙이 활성화된 경우 이벤트 생성을 비활성화하려면 **No Alerts**를 선택합니다.
- SMTP 데이터에서 알려지지 않은 명령을 탐지하려면 **Detect Unknown Commands**를 선택합니다.

8단계 **Max Command Line Len** 필드에 최대 명령줄 길이를 지정합니다.

9단계 **Max Header Line Len** 필드에 최대 데이터 헤더 줄 길이를 지정합니다.

10단계 **Max Response Line Len** 필드에 최대 응답 줄 길이를 지정합니다.

참고 RCPT TO 및 MAIL FROM은 SMTP 명령입니다. 프리프로세서 컨피그레이션은 각각 RCPT 및 MAIL 명령 이름을 사용합니다. 코드 내에서 프리프로세서는 RCPT 및 MAIL을 올바른 명령 이름에 매핑합니다.

11단계 필요 시 대체 최대 명령 줄 길이를 지정할 명령을 추가하려면 **Alt Max Command Line Len** 옆에 있는 **Add**를 클릭한 다음, 줄 길이 및 해당 길이를 적용할 명령을 지정합니다. 둘 이상의 명령은 공백으로 구분하여 지정할 수 있습니다.

12단계 유효하지 않은 것으로 취급하여 탐지할 명령을 **Invalid Commands** 필드에 지정합니다. 공백을 사용하여 명령을 구분하십시오.

13단계 유효한 것으로 취급하여 탐지할 명령을 **Valid Commands** 필드에 지정합니다. 공백을 사용하여 명령을 구분하십시오.

참고 **Valid Commands** 목록이 비어 있더라도 프리프로세서는 다음 명령을 유효한 것으로 취급합니다. ATRN, AUTH, BDAT, DATA, DEBUG, EHLO, EMAL, ESAM, ESND, ESOM, ETRN, EVFY, EXPN, HELO, HELP, IDENT, MAIL, NOOP, QUIT, RCPT, RSET, SAML, SOML, SEND, ONEX, QUEU, STARTTLS, TICK, TIME, TURN, TURNME, VERB, VRFY, X-EXPS, X-LINK2STATE, XADR, XAUTH, XCIR, XEXCH50, XGEN, XLICENSE, XQUE, XSTA, XTRN 또는 XUSR.

14단계 SMTP DATA 명령이 RFC 5321에 따라 데이터를 전송하는 것과 동일한 방법으로 데이터 전송을 시작할 명령을 **Data Commands** 필드에 지정합니다. 공백을 사용하여 명령을 구분하십시오.

15단계 BDAT 명령이 RFC 3030에 따라 데이터를 전송하는 것과 유사한 방법으로 데이터 전송을 시작할 명령을 **Binary Data Commands** 필드에 지정합니다. 공백을 사용하여 명령을 구분하십시오.

16단계 클라이언트와 서버 간 인증 교환을 시작할 명령을 **Authentication Commands** 필드에 지정합니다. 공백을 사용하여 명령을 구분하십시오.

17단계 X-Link2State Microsoft Exchange 버퍼 데이터 오버플로 공격의 일부인 패킷을 탐지하려면 **Detect xlink2state**를 선택합니다.

18단계 서로 다른 유형의 이메일 첨부 파일에 대해 추출 및 디코딩할 데이터의 최대 바이트 수를 지정하려면 다음 첨부 파일 유형에 대한 값을 지정합니다.

- **Base64 Decoding Depth**
- **7-Bit/8-Bit/Binary Decoding Depth**(일반 텍스트, jpeg 이미지, mp3 파일 등 각종 multipart 콘텐츠 유형 포함)
- **Quoted-Printable Decoding Depth**
- **Unix-to-Unix Decoding Depth**

1~65535바이트 범위로 지정할 수 있습니다. 또는 해당 유형 패킷의 모든 데이터를 추출 및 디코딩(필요 시)하려면 0을 지정합니다. 첨부 파일 유형의 데이터를 무시하려면 -1을 지정합니다.

추출된 데이터를 검사하려면 침입 규칙에서 `file_data` 규칙 키워드를 사용할 수 있습니다. 자세한 내용은 36-99페이지의 특정 페이로드 유형 가리키기을/를 참조하십시오.

또한 패킷 간 데이터 또는 여러 TCP 세그먼트를 가로지르는 데이터를 추출 및 디코딩하려면 SMTP **Stateful Inspection** 옵션을 선택해야 합니다.

19단계 컨텍스트 정보를 SMTP 트래픽에 의해 트리거된 침입 이벤트와 연결하기 위한 옵션을 구성합니다.

- 침입 이벤트와 연결하기 위한 MIME 첨부 파일 이름의 추출을 활성화하려면 **Log MIME Attachment Names**를 선택합니다.
- 수신자 이메일 주소의 추출을 활성화하려면 **Log To Addresses**를 선택합니다.
- 침입 이벤트와 연결할 전송자 이메일 주소의 추출을 활성화하려면 **Log From Addresses**를 선택합니다.
- 침입 이벤트와 연결하고 이메일 헤더를 검사하는 규칙을 작성하기 위해 이메일 주소의 추출을 활성화하려면 **Log Headers**를 선택합니다.

  헤더 정보는 침입 이벤트 패킷 보기에 표시됩니다. 또한 `content` 또는 `protected_content` 키워드와 이메일 헤더 데이터를 패턴으로 사용하는 침입 규칙을 작성할 수도 있습니다. 자세한 내용은 41-24페이지의 이벤트 정보 보기 및 36-14페이지의 내용 일치 검색을/를 참조하십시오.

  선택적으로, 0~20480바이트의 추출할 이메일 헤더의 **Header Log Depth**를 지정할 수 있습니다. 값을 0으로 지정하면 **Log Headers**가 비활성화됩니다.

20단계 정책을 저장하거나, 계속 수정하거나, 변경 사항을 취소하거나, 기반 정책의 기본 컨피그레이션 설정으로 돌아가거나, 시스템 캐시에 변경 사항이 남아 있는 상태로 종료합니다. 자세한 내용은 23-15페이지의 충돌 해결 및 정책 변경 사항 커밋을/를 참조하십시오.

SMTP 최대 디코딩 메모리 알림 활성화

라이센스: 보호

활성화된 프리프로세서가 다음의 인코딩된 데이터 유형을 디코딩하기 위해 시스템에서 허용하는 최대 메모리 양을 사용하는 경우 이벤트를 생성하려면 SMTP 프리프로세서 규칙 124:9를 활성화할 수 있습니다.

- Base64
- 7-bit/8-bit/binary
- Quoted-printable
- Unix-to-Unix

최대 디코딩 메모리가 초과되면 프리프로세서는 메모리가 사용 가능해질 때까지 이러한 유형의 인코딩된 데이터의 디코딩을 중지합니다. 이 프리프로세서 규칙은 특정 단일 컨피그레이션 옵션과 연결되어 있지 않습니다. 규칙 활성화에 대한 자세한 내용은 32-20페이지의 규칙 상태 설정을/를 참조하십시오.

SSH 프리프로세서를 사용하여 익스플로잇 탐지

라이센스: 보호

SSH 프리프로세서는 Challenge-Response Buffer Overflow 익스플로잇, CRC-32 익스플로잇, SecureCRT SSH Client Buffer Overflow 익스플로잇, 프로토콜 불일치, 잘못된 SSH 메시지 방향 등을 탐지합니다. 프리프로세서는 또한 버전 1 또는 2 이외의 버전 문자열을 탐지합니다.

Challenge-Response Buffer Overflow 및 CRC-32 공격이 키 교환 후 발생하며, 따라서 암호화됩니다. 두 공격 모두 인증 질문 직후 20KB가 넘는 이례적으로 큰 페이로드를 서버에 전송합니다. CRC-32 공격은 SSH 버전 1에만 적용되고, Challenge-Response Buffer Overflow 익스플로잇은 SSH 버전 2에만 적용됩니다. 버전 문자열은 세션 초기에 확인됩니다. 버전 문자열의 차이점을 제외하면 두 공격은 동일한 방식으로 처리됩니다.

SecureCRT SSH 익스플로잇 및 프로토콜 불일치 공격은 키 교환 전에 연결을 보호하려고 시도할 때 발생합니다. SecureCRT 익스플로잇은 지나치게 긴 프로토콜 식별자 문자열을 클라이언트에 전송하여 버퍼 오버플로를 일으킵니다. 비 SSH 클라이언트 애플리케이션이 보안 SSH 서버에 연결하려고 시도하거나 서버와 클라이언트 버전 번호가 일치하지 않는 경우 프로토콜 불일치가 발생합니다.

지정된 포트 또는 포트 목록에서 트래픽을 검사하거나 SSH 트래픽을 자동으로 탐지하도록 프리프로세서를 구성할 수 있습니다. 지정된 바이트 수 내에서 암호화된 패킷의 지정된 수가 지나갈 때까지 또는 지정된 패킷 수 내에서 지정된 최대 바이트 수가 초과될 때까지 계속해서 SSH 트래픽을 검사합니다. 최대 바이트 수가 초과되면 CRC-32(SSH 버전 1) 또는 Challenge-Response Buffer Overflow(SSH 버전 2) 공격이 발생한 것으로 간주됩니다. 또한 SecureCRT 익스플로잇, 프로토콜 불일치 및 잘못된 메시지 방향을 탐지할 수 있습니다. 프리프로세서는 컨피그레이션 없이 버전 1 또는 2 이외의 버전 문자열 값을 탐지합니다.

SSH 프리프로세서를 사용할 때에는 다음에 유의하십시오.

- GID(generator ID)가 128인 SSH 프리프로세서 규칙을 활성화해야 이러한 규칙에서 이벤트를 생성할 수 있습니다. 자세한 내용은 32-20페이지의 규칙 상태 설정을/를 참조하십시오.
- SSH 프리프로세서는 무차별 암호 대입 공격(brute force attack)을 처리하지 않습니다. 무차별 암호 대입 공격 시도에 대한 자세한 내용은 32-29페이지의 동적 규칙 상태 추가을/를 참조하십시오.

자세한 내용은 다음 절을 참조하십시오.

- 27-66페이지의 SSH 프리프로세서 옵션 선택
- 27-69페이지의 SSH 프리프로세서 구성

SSH 프리프로세서 옵션 선택

라이센스: 보호

이 섹션에서는 SSH 프리프로세서를 구성하기 위해 사용할 수 있는 옵션에 대해 설명합니다.

다음 중 하나가 발생하면 프리프로세서는 세션에서 트래픽 검사를 중지합니다.

- 이 암호화된 패킷의 수에 대해 서버와 클라이언트 간 유효한 교환이 발생했으며, 연결이 계속 유지됩니다.
- 검사할 암호화된 패킷 수에 도달하기 전에 **Number of Bytes Sent Without Server Response**에 도달하여, 공격이 있다고 가정할 수 있습니다.

Number of Encrypted Packets to Inspect 중 각각의 유효한 서버 응답은 **Number of Bytes Sent Without Server Response**를 재설정하며, 패킷 카운트가 계속됩니다.

다음의 SSH 프리프로세서 컨피그레이션 예를 고려해볼 수 있습니다.

- **Server Ports**: 22
- **Autodetect Ports**: off
- **Maximum Length of Protocol Version String**: 80
- **Number of Encrypted Packets to Inspect**: 25
- **Number of Bytes Sent Without Server Response**: 19,600
- 모든 탐지 옵션이 활성화됨

이 예에서 프리프로세서는 포트 22를 검사합니다. 즉, 자동 탐지가 비활성화되어 있으므로 지정된 포트에서만 검사합니다.

또한 이 예의 프리프로세서는 다음 중 하나가 발생하면 트래픽 검사를 중지합니다.

- 클라이언트가 25개의 암호화된 패킷을 전송하며, 여기에 포함된 바이트 수는 19,600바이트(누적)를 넘지 않습니다. 이 경우 공격이 없다고 가정할 수 있습니다.
- 클라이언트가 25개의 암호화된 패킷 내에서 전송하는 바이트 수가 19,600바이트를 초과합니다. 이 예의 세션은 SSH 버전 2 세션이므로, 이 경우 프리프로세서는 공격을 Challenge-Response Buffer Overflow 익스플로잇이라고 간주합니다.

이 예에서 프리프로세서는 트래픽 처리 중에 발생하는 다음 내용도 탐지합니다.

- 80바이트보다 큰 버전 문자열에 의해 트리거되고 SecureCRT 익스플로잇을 나타내는 서버 오버플로
- 프로토콜 불일치
- 잘못된 방향의 패킷 흐름

마지막으로, 프리프로세서는 버전 1 또는 2 이외의 버전 문자열을 자동으로 탐지합니다.

다음 설명에서 프리프로세서 규칙이 언급되지 않은 경우 해당 옵션은 프리프로세서 규칙과 관련되지 않은 것입니다.

Server Ports

SSH 프리프로세서가 트래픽을 검사해야 할 포트를 지정합니다.

단일 포트 또는 쉼표로 구분된 포트 목록을 구성할 수 있습니다.

Autodetect Ports

SSH 트래픽을 자동으로 탐지하도록 프리프로세서를 설정합니다.

이 옵션이 활성화된 경우 프리프로세서는 모든 트래픽에서 SSH 버전 번호를 검사합니다. 클라이언트 패킷에도 서버 패킷에도 버전 번호가 포함되지 않은 경우 처리가 중지됩니다. 비활성화된 경우 프리프로세서는 **Server Ports** 옵션으로 식별된 트래픽만 검사합니다.

Number of Encrypted Packets to Inspect

세션당 검사해야 할 암호화된 패킷의 수를 지정합니다.

이 옵션을 0으로 설정하면 모든 트래픽이 통과됩니다.

검사할 암호화된 패킷의 수를 줄이면 일부 공격이 탐지를 회피할 수 있습니다. 검사할 암호화된 패킷의 수를 높이면 성능이 저하될 수 있습니다.

Number of Bytes Sent Without Server Response

Challenge-Response Buffer Overflow 또는 CRC-32 공격으로 간주하기 전 클라이언트가 응답을 받지 않고 서버로 전송할 수 있는 SSH의 최대 바이트 수를 지정합니다.

프리프로세서가 Challenge-Response Buffer Overflow 또는 CRC-32 익스플로잇에서 오탐을 생성하는 경우 이 옵션의 값을 높이십시오.

Maximum Length of Protocol Version String

SecureCRT 익스플로잇으로 간주하기 전 서버의 버전 문자열에서 허용되는 최대 바이트 수를 지정합니다.

Detect Challenge-Response Buffer Overflow Attack

Challenge-Response Buffer Overflow 익스플로잇의 탐지를 활성화 또는 비활성화합니다.

이 옵션에 대한 이벤트를 생성하려면 규칙 128:1을 활성화할 수 있습니다. 자세한 내용은 32-20 페이지의 규칙 상태 설정을/를 참조하십시오.

Detect SSH1 CRC-32 Attack

CRC-32 익스플로잇의 탐지를 활성화 또는 비활성화합니다.

이 옵션에 대한 이벤트를 생성하려면 규칙 128:2를 활성화할 수 있습니다. 자세한 내용은 32-20 페이지의 규칙 상태 설정을/를 참조하십시오.

Detect Server Overflow

SecureCRT SSH Client Buffer Overflow 익스플로잇의 탐지를 활성화 또는 비활성화합니다.

이 옵션에 대한 이벤트를 생성하려면 규칙 128:3을 활성화할 수 있습니다. 자세한 내용은 32-20 페이지의 규칙 상태 설정을/를 참조하십시오.

Detect Protocol Mismatch

프로토콜 불일치의 탐지를 활성화 또는 비활성화합니다.

이 옵션에 대한 이벤트를 생성하려면 규칙 128:4를 활성화할 수 있습니다. 자세한 내용은 32-20 페이지의 규칙 상태 설정을/를 참조하십시오.

Detect Bad Message Direction

트래픽 플로우의 방향이 잘못된 경우(즉, 서버라고 생각되는 곳에서 클라이언트 트래픽을 생성하거나, 클라이언트에서 서버 트래픽을 생성하는 경우)의 탐지를 활성화 또는 비활성화합니다.

이 옵션에 대한 이벤트를 생성하려면 규칙 128:5를 활성화할 수 있습니다. 자세한 내용은 32-20 페이지의 규칙 상태 설정을/를 참조하십시오.

Detect Payload Size Incorrect for the Given Payload

SSH 패킷에 지정된 길이가 IP 헤더에 지정된 총 길이와 일치하지 않거나 메시지가 잘린 경우(즉, 전체 SSH 헤더에 대한 데이터가 충분하지 않은 경우) 등 페이로드 크기가 잘못된 패킷의 탐지를 활성화 또는 비활성화합니다.

이 옵션에 대한 이벤트를 생성하려면 규칙 128:6을 활성화할 수 있습니다. 자세한 내용은 32-20 페이지의 규칙 상태 설정을/를 참조하십시오.

Detect Bad Version String

활성화된 경우 프리프로세서는 컨피그레이션 없이 버전 1 또는 2 이외의 버전 문자열을 탐지합니다.

이 옵션에 대한 이벤트를 생성하려면 규칙 128:7을 활성화할 수 있습니다. 자세한 내용은 32-20 페이지의 규칙 상태 설정을/를 참조하십시오.

SSH 프리프로세서 구성

라이센스: 보호

이 절에서는 SSH 프리프로세서를 구성하는 방법에 대해 설명합니다.

SSH 프리프로세서를 구성하려면

액세스: Admin/Intrusion Admin

1단계 **Policies > Access Control**을 선택하여 Access Control Policy 페이지를 표시한 다음 **Network Analysis Policy**를 클릭합니다.

Network Analysis Policy 페이지가 나타납니다.

2단계 수정할 정책 옆에 있는 수정 아이콘( )을 클릭합니다.

다른 정책에 저장하지 않은 변경 사항이 있는 경우 변경 사항을 취소하고 계속 진행하려면 **OK**를 클릭합니다. 저장되지 않은 변경 사항을 다른 정책에 저장하는 방법에 대한 자세한 내용은 23-15페이지의 충돌 해결 및 정책 변경 사항 커밋을/를 참조하십시오.

Policy Information 페이지가 나타납니다.

3단계 왼쪽의 탐색 패널에서 **Settings**를 클릭합니다.

Settings 페이지가 나타납니다.

4단계 Application Layer Preprocessors 아래에서 **SSH Configuration**이 활성화되었는지 여부에 따라 두 가지 선택 사항이 있습니다.

- 컨피그레이션이 활성화되어 있으면 **Edit**를 클릭합니다.
- 컨피그레이션이 비활성화되어 있으면 **Enabled**를 클릭한 다음 **Edit**를 클릭합니다.

SSH Configuration(IP 컨피그레이션) 페이지가 나타납니다. 페이지 하단에 있는 메시지는 컨피그레이션이 포함된 네트워크 분석 정책 레이어를 식별합니다. 자세한 내용은 24-1페이지의 네트워크 분석 또는 침입 정책에서 레이어 사용을/를 참조하십시오.

5단계 SSH Configuration 프리프로세서 페이지의 옵션을 수정할 수 있습니다. 자세한 내용은 27-66페이지의 SSH 프리프로세서 옵션 선택을/를 참조하십시오.

6단계 정책을 저장하거나, 계속 수정하거나, 변경 사항을 취소하거나, 기반 정책의 기본 컨피그레이션 설정으로 돌아가거나, 시스템 캐시에 변경 사항이 남아 있는 상태로 종료합니다. 자세한 내용은 23-15페이지의 충돌 해결 및 정책 변경 사항 커밋을/를 참조하십시오.

SSL 프리프로세서 사용

라이센스: 기능에 따라 다름

SSL 프리프로세서는 SSL 검사의 구성을 허용합니다. 이를 통해 암호화된 트래픽을 차단 또는 해독하거나 액세스 제어로 트래픽을 검사할 수 있습니다. SSL 검사의 구성 여부와 상관없이 SSL 프리프로세서는 트래픽에서 탐지된 SSL 핸드셰이크 메시지를 분석하고 세션이 암호화되는 시기를 결정합니다. 암호화된 트래픽을 식별하면 시스템은 암호화된 페이로드의 침입 및 파일 검사를 중지하는데, 이는 오탐을 줄이고 성능을 향상하는 데 도움이 됩니다. 자세한 내용은 19-1페이지의 트래픽 해독 이해 및 14-3페이지의 액세스 제어 규칙 생성 및 수정을/를 참조하십시오.

SSL 프리프로세서는 또한 암호화된 트래픽에서 Heartbleed 버그를 악용하려는 시도를 탐지하고, 그러한 익스플로잇을 탐지하는 경우 이벤트를 생성합니다.

암호화된 트래픽을 해독하기 위해 SSL 프리프로세서를 사용하는 데에는 라이센스가 필요하지 않습니다. 악성코드 및 침입에 대한 암호화된 페이로드의 검사 정지, Heartbleed 버그 익스플로잇 탐지 등 다른 모든 SSL 프리프로세서 기능에는 보호 라이센스가 필요합니다.

참고 시스템 제공 네트워크 분석 정책은 기본적으로 SSL 프리프로세서를 활성화합니다. 암호화된 트래픽이 네트워크를 통과할 것으로 예상하는 경우 사용자 지정 구축에서 SSL 프리프로세서를 비활성화하지 않는 것이 좋습니다.

자세한 내용은 다음 절을 참조하십시오.

- 27-70페이지의 SSL 전처리 이해
- 27-71페이지의 SSL 프리프로세서 규칙 활성화
- 27-72페이지의 SSL 프리프로세서 구성

SSL 전처리 이해

라이센스: 보호

SSL 검사를 구성한 경우, SSL 프리프로세서는 암호화된 데이터의 침입 및 파일 검사를 중지하고 SSL 정책으로 암호화된 트래픽을 검사합니다. 이는 오탐을 줄이는 데 도움이 될 수 있습니다. SSL 프리프로세서는 SSL 핸드셰이크를 검사할 때 상태 정보를 유지 관리하여, 세션의 상태와 SSL 버전을 모두 추적합니다. 프리프로세서에서 세션 상태가 암호화된 것을 탐지하면 시스템은 해당 세션의 트래픽을 암호화된 것으로 표시합니다. 암호화가 설정된 경우 암호화된 세션의 모든 패킷에 대한 처리를 중지하도록, 그리고 Heartbleed 버그를 악용하려는 시도를 탐지할 경우 이벤트를 생성하도록 시스템을 구성할 수 있습니다.

각 패킷에 대해 SSL 프리프로세서는 트래픽에 IP 헤더, TCP 헤더 및 TCP 페이로드가 포함되어 있는지, 그리고 트래픽이 SSL 전처리를 위해 지정된 포트에서 발생하는지를 확인합니다. 적격 트래픽에 대해 다음 시나리오를 통해 트래픽의 암호화 여부가 결정됩니다.

- 시스템이 세션의 모든 패킷 관찰 - **Server side data is trusted**가 활성화되지 않고, 세션에 서버와 클라이언트 모두에서 오는 Finished 메시지 및 각각에서 오는 하나 이상의 패킷(Application 레코드 포함, Alert 레코드 포함하지 않음)이 포함됨
- 시스템이 트래픽의 일부 손실 - **Server side data is trusted**가 활성화되지 않고, 세션에 각각에서 오는 하나 이상의 패킷(Alert 레코드로 답하지 않은 Application 레코드 포함)이 포함됨
- 시스템이 세션의 모든 패킷 관찰 - **Server side data is trusted**가 활성화되고, 세션에 클라이언트에서 오는 Finished 메시지 및 클라이언트에서 오는 하나 이상의 패킷(Application 레코드 포함, Alert 레코드 포함하지 않음)이 포함됨

- 시스템이 트래픽의 일부 손실 - **Server side data is trusted**가 활성화되고, 세션에 클라이언트에서 오는 하나 이상의 패킷(Alert 레코드로 답하지 않은 Application 레코드 포함)이 포함됨

암호화된 트래픽에 대한 처리를 중지하기로 선택하면 시스템은 세션을 암호화된 것으로 표시한 후 이후 세션의 패킷을 무시합니다.

또한 SSL 핸드셰이크 중에 프리프로세서는 하트비트 요청과 응답을 모니터링합니다. 프리프로세서는 다음을 탐지하는 경우 이벤트를 생성합니다.

- 페이로드 자체보다 큰 페이로드 길이 값을 포함하는 하트비트 요청
- Max Heartbeat Length 필드에 저장된 값보다 큰 하트비트 응답

참고 규칙 내에서 SSL 상태 또는 버전 정보를 사용하려면 `ssl_state` 및 `ssl_version` 키워드를 규칙에 추가할 수 있습니다. 자세한 내용은 36-55페이지의 세션에서 SSL 정보 추출을/를 참조하십시오.

SSL 프리프로세서 규칙 활성화

라이센스: 보호

활성화된 경우 SSL 프리프로세서는 SSL 세션 초기에 교환되는 핸드셰이크와 키 교환 메시지의 내용을 검사합니다. 세션이 암호화되면 트래픽에서 침입 및 악성코드 검사를 일시 중단할 수 있습니다. SSL 검사를 구성하는 경우 SSL 프리프로세서는 또한 액세스 제어로 차단, 해독 또는 검사할 수 있는 암호화된 트래픽을 식별합니다.

GID(generator ID)가 137인 SSL 프리프로세서 규칙을 활성화해야 이러한 규칙에서 이벤트를 생성할 수 있습니다. 자세한 내용은 32-20페이지의 규칙 상태 설정을/를 참조하십시오.

다음 표에서는 활성화할 수 있는 SSL 프리프로세서 규칙에 대해 설명합니다.

표 27-14 SSL 프리프로세서 규칙

프리프로세서 규칙 GID:SID	설명
137:1	서버 hello 이후 클라이언트 hello를 탐지합니다. 이는 유효하지 않으며 이상 행동으로 간주됩니다.
137:2	**Server side data is trusted**가 비활성화된 경우 클라이언트 hello 없는 서버 hello를 탐지합니다. 이는 유효하지 않으며 이상 행동으로 간주됩니다. 자세한 내용은 27-72페이지의 SSL 프리프로세서 구성을/를 참조하십시오.
137:3	**Max Heartbeat Length**에 0이 아닌 값이 포함된 경우 페이로드 길이가 페이로드 자체보다 큰 하트비트 요청을 탐지합니다. 이는 Heartbleed 버그를 악용하려는 시도를 나타냅니다.
137:4	**Max Heartbeat Length**에 지정된 0이 아닌 값보다 큰 하트비트 응답을 탐지합니다. 이는 Heartbleed 버그를 악용하려는 시도를 나타냅니다.

SSL 프리프로세서 구성

라이센스: 보호

SSL 검사를 구성하지 않으면 시스템은 암호화된 트래픽에서 해독 없이 악성코드와 침입을 검사하려고 시도합니다. SSL 프리프로세서는 활성화되면 세션이 암호화되는 경우를 탐지합니다. SSL 프리프로세서가 활성화되면, 규칙 엔진은 SSL 상태 및 버전 정보를 얻기 위해 프리프로세서를 호출할 수 있습니다. 침입 정책에서 `ssl_state` 및 `ssl_version` 키워드를 사용하여 규칙을 활성화하는 경우 SSL 프리프로세서도 활성화해야 합니다.

또한 암호화된 세션의 검사 및 리어셈블을 비활성화하려면 **Stop inspecting encrypted traffic** 옵션을 활성화할 수 있습니다. SSL 프리프로세서는 세션의 상태를 유지 관리하므로 세션에서 모든 트래픽의 검사를 비활성화할 수 있습니다. 시스템은 SSL 전처리가 활성화되고 **Stop inspecting encrypted traffic** 옵션이 선택된 **경우에만** 암호화된 세션에서 트래픽 검사를 중지합니다. **Stop inspecting encrypted traffic** 옵션의 선택을 취소하는 경우 **Server side data is trusted** 옵션을 수정할 수 없습니다.

암호화된 트래픽의 식별 기반을 서버 트래픽에만 두려면 **Server side data is trusted** 옵션을 활성화할 수 있습니다. 즉, 서버 측 데이터가 신뢰되어 트래픽이 암호화되었음을 나타냅니다. SSL 프리프로세서는 일반적으로 세션이 암호화되었는지를 확인하기 위해 클라이언트 트래픽 및 해당 트래픽에 대한 서버 응답을 모두 검사합니다. 그러나 시스템은 세션의 양쪽을 모두 탐지할 수 없으면 트랜잭션을 암호화된 것으로 표시하지 않을 수 있으므로, 세션의 암호화 여부를 나타내려면 SSL 서버에 의존할 수 있습니다. 암호화된 세션에서 시스템이 트래픽을 계속 검사하지 않도록 하려면 **Server side data is trusted** 옵션을 활성화할 때 **Stop inspecting encrypted traffic** 옵션도 활성화해야 합니다.

SSL 핸드셰이크 내에서 하트비트 요청과 응답을 검사함으로써 Heartbleed 버그를 악용하려는 시도를 탐지하도록 프리프로세서 **Max Heartbeat Length** 옵션을 구성할 수 있습니다. 페이로드 길이가 실제 페이로드 길이보다 큰 하트비트 요청 또는 **Max Heartbeat Length** 값보다 큰 하트비트 응답을 탐지하면 프리프로세서는 이벤트를 생성합니다.

프리프로세서가 트래픽에서 암호화된 세션을 모니터링하는 포트를 지정할 수 있습니다.

참고 SSL 모니터링을 위해 지정된 포트에서 비 SSL 트래픽을 탐지하면 SSL 프리프로세서는 트래픽을 SSL 트래픽으로 디코딩하려고 시도한 후 손상된 것으로 플래그 처리합니다.

SSL 프리프로세서를 구성하려면

액세스: Admin/Intrusion Admin

1단계 **Policies > Access Control**을 선택하여 Access Control Policy 페이지를 표시한 다음 **Network Analysis Policy**를 클릭합니다.

Network Analysis Policy 페이지가 나타납니다.

2단계 수정할 정책 옆에 있는 수정 아이콘()을 클릭합니다.

다른 정책에 저장하지 않은 변경 사항이 있는 경우 변경 사항을 취소하고 계속 진행하려면 **OK**를 클릭합니다. 저장하지 않은 변경 사항을 다른 정책에 저장하는 방법에 대한 자세한 내용은 23-15페이지의 충돌 해결 및 정책 변경 사항 커밋을/를 참조하십시오.

Policy Information 페이지가 나타납니다.

3단계 왼쪽의 탐색 패널에서 **Settings**를 클릭합니다.

Settings 페이지가 나타납니다.

4단계 Application Layer Preprocessors 아래에서 **SSL Configuration**이 활성화되었는지 여부에 따라 두 가지 선택 사항이 있습니다.

- 컨피그레이션이 활성화되어 있으면 **Edit**를 클릭합니다.
- 컨피그레이션이 비활성화되어 있으면 **Enabled**를 클릭한 다음 **Edit**를 클릭합니다.

SSL Configuration(IP 컨피그레이션) 페이지가 나타납니다. 페이지 하단에 있는 메시지는 컨피그레이션이 포함된 네트워크 분석 정책 레이어를 식별합니다. 자세한 내용은 24-1페이지의 네트워크 분석 또는 침입 정책에서 레이어 사용을/를 참조하십시오.

5단계 SSL 프리프로세서가 트래픽에서 암호화된 세션을 모니터링해야 할 포트를 쉼표로 구분하여 입력합니다. **Ports** 필드에 포함된 포트에 대해서만 암호화된 트래픽 검사가 수행됩니다.

6단계 세션이 암호화된 것으로 표시된 후 해당 세션에서 트래픽 검사를 활성화 또는 비활성화하려면 **Stop inspecting encrypted traffic** 확인란을 클릭합니다.

7단계 클라이언트 측 트래픽만을 기반으로 암호화된 트래픽의 식별을 활성화 또는 비활성화하려면 **Server side data is trusted** 확인란을 클릭합니다.

8단계 Heartbleed 버그 익스플로잇 시도를 위한 SSL 핸드셰이크 내에서 하트비트 요청 및 응답의 검사를 활성화하려면 **Max Heartbeat Length** 필드에 바이트 수를 입력합니다. 옵션을 비활성화하려면 1~65535의 정수 또는 0을 지정할 수 있습니다.

9단계 정책을 저장하거나, 계속 수정하거나, 변경 사항을 취소하거나, 기반 정책의 기본 컨피그레이션 설정으로 돌아가거나, 시스템 캐시에 변경 사항이 남아 있는 상태로 종료합니다. 자세한 내용은 23-15페이지의 충돌 해결 및 정책 변경 사항 커밋을/를 참조하십시오.

28장 SCADA 전처리 구성

네트워크 분석 정책에서 SCADA(Supervisory Control and Data Acquisition) 프리프로세서를 구성하며, 이를 통해 침입 정책에서 활성화된 규칙을 사용하여 트래픽을 검사할 준비를 하게 됩니다. 자세한 내용은 23-1페이지의 네트워크 분석 및 침입 정책 이해을/를 참조하십시오.

SCADA 프로토콜은 산업, 인프라 및 설비 공정(예: 제조, 생산, 물 처리, 전력 분배, 공항 및 배송 시스템 등)에서 데이터를 모니터링하고 제어하고 수집합니다. FireSIGHT 시스템은 네트워크 분석 정책의 일부로서 구성할 수 있는 Modbus 및 DNP3 SCADA 프로토콜용 프리프로세서를 제공합니다.

주의 사용자 지정 사용자 역할이 있는 일부 사용자는 표준 메뉴 경로(**Policies > Access Control > Network Analysis Policy**)를 통해 네트워크 분석 정책에 액세스할 수 없습니다. 이러한 사용자는 침입 정책을 통해 네트워크 분석 정책에 액세스할 수 있습니다(**Policies > Intrusion > Intrusion Policy > Network Analysis Policy**). 사용자 지정 사용자 역할에 대한 자세한 내용은 61-51페이지의 사용자 지정 사용자 역할 관리을/를 참조하십시오.

Modbus 또는 DNP3 키워드를 포함하는 규칙을 해당 침입 정책에서 활성화하면, 프리프로세서가 네트워크 분석 정책 웹 인터페이스에서 비활성 상태로 유지되더라도 시스템은 자동으로 현재 설정을 통해 각각 Modbus 또는 DNP3 프로세서를 사용합니다. 자세한 내용은 36-75페이지의 Modbus 키워드 및 36-77페이지의 DNP3 키워드을/를 참조하십시오.

자세한 내용은 다음 절을 참조하십시오.

- 28-1페이지의 Modbus 프리프로세서 구성
- 28-3페이지의 DNP3 프리프로세서 구성

Modbus 프리프로세서 구성

라이센스: 보호

Modicon에서 1979년 처음 발표한 Modbus 프로토콜은 널리 사용되는 SCADA 프로토콜입니다. Modbus 프리프로세서는 Modbus 트래픽에서 변칙을 탐지하며, Modbus 키워드를 사용하여 특정 프로토콜 필드에 액세스하는 규칙 엔진에 의해 처리되도록 Modbus 프로토콜을 디코딩합니다. 자세한 내용은 36-75페이지의 Modbus 키워드을/를 참조하십시오.

단일 컨피그레이션 옵션을 사용하면 프리프로세서가 Modbus 트래픽에 대해 검사하는 포트의 기본 설정을 수정할 수 있습니다.

Modbus 프리프로세서 규칙이 이벤트를 생성하도록 하려면 다음 표에 나와 있는 해당 규칙을 활성화해야 합니다. 규칙 활성화에 대한 자세한 내용은 32-20페이지의 규칙 상태 설정을/를 참조하십시오.

표 28-1 Modbus 프리프로세서 규칙

프리프로세서 규칙 GID:SID	설명
144:1	Modbus 헤더의 길이가 Modbus 함수 코드에 필요한 길이와 일치하지 않는 경우 이벤트를 생성합니다. 각 Modbus 함수에는 요청 및 응답을 위한 예상 형식이 있습니다. 메시지의 길이가 예상 형식과 일치하지 않으면 이 이벤트가 생성됩니다.
144:2	Modbus 프로토콜 ID가 0이 아닌 경우 이벤트가 생성됩니다. 프로토콜 ID 필드는 다른 프로토콜을 Modbus와 멀티플렉싱하는 데 사용됩니다. 프리프로세서는 이러한 다른 프로토콜을 처리하지 않으므로 대신 이 이벤트가 생성됩니다.
144:3	프리프로세서가 예약된 Modbus 함수 코드를 탐지하는 경우 이벤트가 생성됩니다.

Modbus 프리프로세서의 사용과 관련하여, 네트워크에 Modbus 활성화 디바이스가 포함되어 있지 않으면 트래픽에 적용하는 네트워크 분석 정책에서 이 프리프로세서를 활성화하지 않아야 합니다.

Modbus 프리프로세서가 모니터링하는 포트를 수정하려면 다음 절차를 사용할 수 있습니다.

Modbus 프리프로세서를 구성하려면

액세스: Admin/Intrusion Admin

1단계 **Policies > Access Control**을 선택하여 Access Control Policy 페이지를 표시한 다음 **Network Analysis Policy**를 클릭합니다.

Network Analysis Policy 페이지가 나타납니다.

2단계 수정할 정책 옆에 있는 수정 아이콘( )을 클릭합니다.

다른 정책에 저장하지 않은 변경 사항이 있는 경우 변경 사항을 취소하고 계속 진행하려면 **OK**를 클릭합니다. 저장하지 않은 변경 사항을 다른 정책에 저장하는 방법에 대한 자세한 내용은 23-15페이지의 충돌 해결 및 정책 변경 사항 커밋을/를 참조하십시오.

Policy Information 페이지가 나타납니다.

3단계 왼쪽의 탐색 패널에서 **Settings**를 클릭합니다.

Settings 페이지가 나타납니다.

4단계 **SCADA Preprocessors** 아래에서 **Modbus Configuration**이 활성화되었는지 여부에 따라 두 가지 선택 사항이 있습니다.

- 컨피그레이션이 활성화되어 있으면 **Edit**를 클릭합니다.
- 컨피그레이션이 비활성화되어 있으면 **Enabled**를 클릭한 다음 **Edit**를 클릭합니다.

Modbus Configuration 페이지가 나타납니다. 페이지 하단에 있는 메시지는 컨피그레이션이 포함된 네트워크 분석 정책 레이어를 식별합니다. 자세한 내용은 24-1페이지의 네트워크 분석 또는 침입 정책에서 레이어 사용을/를 참조하십시오.

5단계 선택적으로, 프리프로세서가 Modbus 트래픽에 대해 검사하는 **Ports**를 수정합니다. 0~65535의 정수를 지정할 수 있습니다. 여러 포트를 구분하려면 쉼표를 사용하십시오.

6단계 정책을 저장하거나, 계속 수정하거나, 변경 사항을 취소하거나, 기반 정책의 기본 컨피그레이션 설정으로 돌아가거나, 시스템 캐시에 변경 사항이 남아 있는 상태로 종료합니다. 자세한 내용은 23-15페이지의 충돌 해결 및 정책 변경 사항 커밋을/를 참조하십시오.

DNP3 프리프로세서 구성

라이센스: 보호

Distributed Network Protocol(DNP3)은 원래 발전소 사이의 일관된 통신을 제공하기 위해 개발된 SCADA 프로토콜입니다. DNP3은 또한 물, 쓰레기, 통신 및 기타 여러 산업 부문에 널리 사용되었습니다.

DNP3 프리프로세서는 DNP3 트래픽에서 변칙을 탐지하며, DNP3 키워드를 사용하여 특정 프로토콜 필드에 액세스하는 규칙 엔진에 의해 처리되도록 DNP3 프로토콜을 디코딩합니다. 자세한 내용은 36-77페이지의 DNP3 키워드을/를 참조하십시오.

DNP3 프리프로세서 규칙이 이벤트를 생성하도록 하려면 다음 표에 나와 있는 해당 규칙을 활성화해야 합니다. 규칙 활성화에 대한 자세한 내용은 32-20페이지의 규칙 상태 설정을/를 참조하십시오.

표 28-2 DNP3 프리프로세서 규칙

프리프로세서 규칙 GID:SID	설명
145:1	**Log bad CRC**가 활성화된 경우 프리프로세서가 잘못된 체크섬이 있는 링크 레이어 프레임을 탐지하면 이벤트를 생성합니다.
145:2	프리프로세서가 잘못된 길이의 DNP3 링크 레이어 프레임을 탐지하면 이벤트를 생성하고 패킷을 차단합니다.
145:3	프리프로세서가 잘못된 시퀀스 번호의 전송 레이어 세그먼트를 탐지하면 리어셈블리 중에 이벤트를 생성하고 패킷을 차단합니다.
145:4	완전한 프래그먼트를 리어셈블하기 전에 DNP3 리어셈블리 버퍼가 지워지는 경우 이벤트를 생성합니다. 이는 다른 세그먼트가 대기열에 추가된 이후 FIR 플래그를 전달하는 세그먼트가 나타나는 경우 발생합니다.
145:5	프리프로세서가 예약된 주소를 사용하는 DNP3 링크 레이어 프레임을 탐지할 때 이벤트를 생성합니다.
145:6	프리프로세서가 예약된 함수 코드를 사용하는 DNP3 요청 또는 응답을 탐지할 때 이벤트를 생성합니다.

DNP3 프리프로세서의 사용과 관련하여, 네트워크에 DNP3 활성화 디바이스가 포함되어 있지 않으면 트래픽에 적용하는 네트워크 분석 정책에서 이 프리프로세서를 활성화하지 않아야 합니다. 자세한 내용은 29-30페이지의 TCP 스트림 전처리 구성을/를 참조하십시오.

다음 목록에서는 구성할 수 있는 DNP3 프리프로세서 옵션에 대해 설명합니다.

Ports

지정된 각 포트에서 DNP3 트래픽의 검사를 활성화합니다. 단일 포트 또는 쉼표로 구분된 포트 목록을 지정할 수 있습니다. 각 포트에 대해 0~65535의 값을 지정할 수 있습니다.

Log bad CRCs

활성화되면 DNP3 링크 레이어 프레임에 포함된 체크섬을 검증합니다. 잘못된 체크섬이 있는 프레임은 무시됩니다.

잘못된 체크섬이 탐지될 때 이벤트를 생성하려면 규칙 145:1을 활성화할 수 있습니다.

DNP3 프리프로세서를 구성하려면

액세스: Admin/Intrusion Admin

1단계 **Policies > Access Control**을 선택하여 Access Control Policy 페이지를 표시한 다음 **Network Analysis Policy**를 클릭합니다.

Network Analysis Policy 페이지가 나타납니다.

2단계 수정할 정책 옆에 있는 수정 아이콘( )을 클릭합니다.

다른 정책에 저장하지 않은 변경 사항이 있는 경우 변경 사항을 취소하고 계속 진행하려면 **OK**를 클릭합니다. 저장하지 않은 변경 사항을 다른 정책에 저장하는 방법에 대한 자세한 내용은 23-15페이지의 충돌 해결 및 정책 변경 사항 커밋을/를 참조하십시오.

Policy Information 페이지가 나타납니다.

3단계 왼쪽의 탐색 패널에서 **Settings**를 클릭합니다.

Settings 페이지가 나타납니다.

4단계 **SCADA Preprocessors** 아래에서 **DNP3 Configuration**이 활성화되었는지 여부에 따라 두 가지 선택 사항이 있습니다.

- 컨피그레이션이 활성화되어 있으면 **Edit**를 클릭합니다.
- 컨피그레이션이 비활성화되어 있으면 **Enabled**를 클릭한 다음 **Edit**를 클릭합니다.

DNP3 Configuration(IP 컨피그레이션) 페이지가 나타납니다. 페이지 하단에 있는 메시지는 컨피그레이션이 포함된 네트워크 분석 정책 레이어를 식별합니다. 자세한 내용은 24-1페이지의 네트워크 분석 또는 침입 정책에서 레이어 사용을/를 참조하십시오.

5단계 선택적으로, 프리프로세서가 DNP3 트래픽에 대해 검사하는 **Ports**를 수정합니다. 0~65535의 정수를 지정할 수 있습니다. 여러 포트를 구분하려면 쉼표를 사용하십시오.

6단계 선택적으로, DNP3 링크 레이어 프레임에 포함된 체크섬을 검증하고 잘못된 체크섬의 프레임을 무시할지 여부를 지정하려면 **Log bad CRCs** 확인란을 선택하거나 지웁니다.

7단계 정책을 저장하거나, 계속 수정하거나, 변경 사항을 취소하거나, 기반 정책의 기본 컨피그레이션 설정으로 돌아가거나, 시스템 캐시에 변경 사항이 남아 있는 상태로 종료합니다. 자세한 내용은 네트워크 분석 정책 수정 작업 표를 참조하십시오.

29장 전송 및 네트워크 레이어 전처리 구성

네트워크 분석 정책의 네트워크 레이어 프리프로세서에서 대부분의 전송을 구성하며, 이를 통해 침입 정책에서 활성화된 규칙을 사용하여 트래픽을 검사할 준비를 하게 됩니다. 자세한 내용은 23-1페이지의 네트워크 분석 및 침입 정책 이해을/를 참조하십시오.

전송 및 네트워크 레이어 프리프로세서는 IP 프래그먼트화, 체크섬 검증, TCP 및 UDP 세션 전처리를 악용하는 공격을 탐지합니다. 패킷이 프리프로세서로 전송되기 전, 패킷 디코더는 프리프로세서 및 침입 규칙 엔진이 쉽게 사용할 수 있는 형식으로 패킷 헤더 및 페이로드를 변환하고 패킷 헤더에서 비정상적인 각종 동작을 탐지합니다. 패킷을 디코딩한 후 그리고 다른 프리프로세서로 패킷을 전송하기 전, 인라인 표준화 프리프로세서는 인라인 구축을 위해 패킷을 표준화합니다.

침입 규칙 또는 규칙 인수에서 비활성화된 프리프로세서를 요구하면, 네트워크 분석 정책의 웹 인터페이스에서 비활성 상태로 있더라도 시스템에서는 자동으로 현재의 컨피그레이션과 함께 해당 프리프로세서를 사용합니다. 자세한 내용은 23-12페이지의 사용자 지정 정책의 제한 사항을/를 참조하십시오.

주의 사용자 지정 사용자 역할이 있는 일부 사용자는 표준 메뉴 경로(**Policies > Access Control > Network Analysis Policy**)를 통해 네트워크 분석 정책에 액세스할 수 없습니다. 이러한 사용자는 침입 정책을 통해 네트워크 분석 정책에 액세스할 수 있습니다(**Policies > Intrusion > Intrusion Policy > Network Analysis Policy**). 사용자 지정 사용자 역할에 대한 자세한 내용은 61-51페이지의 사용자 지정 사용자 역할 관리을/를 참조하십시오.

네트워크 분석 정책에서 구성하는 전송 및 네트워크 레이어 프리프로세서 설정을 VLAN, 영역 또는 네트워크 단위로 맞춤화할 수 있습니다. 모든 트래픽에 전역적으로 적용되는 일부 전송 및 네트워크 레이어 설정은 액세스 제어 정책에서 구성합니다.

고급 Transport/Network 설정 구성

라이센스: 보호

고급 전송 및 네트워크 프리프로세서 설정은 액세스 제어 정책을 적용하는 모든 네트워크, 영역, VLAN에 전역으로 적용됩니다. 네트워크 분석 정책이 아닌 액세스 제어 정책에서 이러한 고급 설정을 구성합니다.

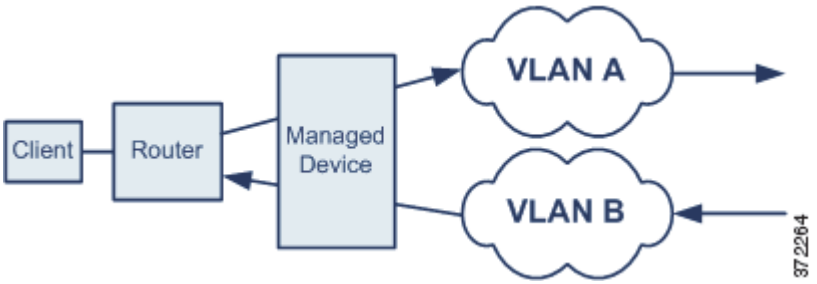
다음 섹션에서는 이러한 설정에 대해 설명합니다.

VLAN 헤더 무시

라이센스: 보호

지원되는 디바이스: ASA FirePOWER를 제외한 모두

동일한 연결에 대해 다른 방향으로 이동하는 트래픽의 서로 다른 VLAN 태그는 트래픽 리어셈블리 및 규칙 처리에 영향을 미칠 수 있습니다. 예를 들어 다음 그림에서는 동일한 연결에 대한 트래픽을 VLAN A를 통해 전송하고 VLAN B를 통해 수신할 수 있습니다.



Ignore the VLAN header when tracking connections를 활성화하면 시스템은 구축에서 패킷이 올바르게 처리되도록 VLAN 헤더를 무시합니다.

VLAN 헤더를 무시하려면

액세스: Admin/Access Admin/Network Admin

1단계 **Policies > Access Control**을 선택합니다.

Access Control Policy 페이지가 나타납니다.

2단계 수정할 액세스 제어 정책 옆에 있는 수정 아이콘()을 클릭합니다.

액세스 제어 정책 편집기가 나타납니다.

3단계 **Advanced** 탭을 선택합니다.

Access control policy advanced settings 페이지가 나타납니다.

4단계 **Transport/Network Layer Preprocessor Settings** 옆에 있는 수정 아이콘()을 클릭합니다.

Transport/Network Layer Preprocessor Settings 팝업 창이 나타납니다.

5단계 다음 옵션을 이용할 수 있습니다.

- 서로 다른 방향으로 이동하는 트래픽의 동일한 연결에 대해 서로 다른 VLAN 태그를 탐지할 수 있는 구축된 디바이스의 경우, 트래픽을 식별할 때 VLAN 헤더를 무시하려면 **Ignore the VLAN header when tracking connections** 확인란을 선택합니다.
- 서로 다른 방향으로 이동하는 트래픽의 동일한 연결에 대해 서로 다른 VLAN 태그를 탐지할 수 없는 구축된 디바이스의 경우, 트래픽을 식별할 때 VLAN 헤더를 무시하려면 **Ignore the VLAN header when tracking connections** 확인란의 선택을 취소합니다.

6단계 **OK** 를 클릭합니다.

변경 사항을 적용하려면 액세스 제어 정책을 적용해야 합니다. 12-15페이지의 액세스 제어 정책 적용을/를 참조하십시오.

침입 삭제 규칙으로 능동 응답 시작

라이센스: 보호

삭제 규칙은 규칙 상태가 Drop and Generate Events로 설정된 침입 규칙 또는 프리프로세서 규칙입니다. 인라인 구축에서 시스템은 트리거링 패킷을 삭제하거나 패킷이 시작된 세션을 차단하여 TCP 또는 UDP 삭제 규칙에 응답합니다. 패시브 구축에서 시스템은 능동 응답을 사용하는 경우가 아니면 패킷을 삭제할 수 없으며 세션을 차단할 수도 없습니다.

팁 UDP 데이터 스트림은 일반적으로 *세션*의 관점에서 고려되지 않으므로, 스트림 프리프로세서가 캡슐화하는 IP 데이터그램 헤더의 소스 및 목적지 IP 주소 필드를 사용하고 UDP 헤더의 포트 필드를 사용하여 플로우의 방향을 결정하고 UDP 세션을 식별하는 방법에 대해 자세히 알아보려면 29-32페이지의 UDP 스트림 전처리 사용을/를 참조하십시오.

위반 패킷이 TCP 또는 UDP 삭제 규칙을 트리거할 때 하나 이상의 *능동 응답*을 시작하여 TCP 연결 또는 UDP 세션을 좀 더 정확하게 구체적으로 종료하도록 **Maximum Active Responses** 옵션을 구성할 수 있습니다.

능동 응답이 인라인 구축에서 활성화되면, 시스템은 트리거링 패킷을 삭제하고 TCP 재설정(RST) 패킷을 클라이언트와 서버 트래픽에 모두 삽입하여 TCP 삭제 규칙에 응답합니다. 패시브 구축에서는 시스템이 패킷을 삭제할 수 없습니다. 패시브 구축에서 능동 응답이 활성화되면, 시스템은 TCP 연결의 클라이언트 및 서버 양쪽 끝으로 TCP 재설정을 전송하여 TCP 삭제 규칙에 응답합니다. 능동 응답이 인라인 또는 패시브 구축에서 활성화되면, 시스템은 세션의 양쪽 끝으로 ICMP 도달 불가 패킷을 전송하여 UDP 세션을 종료합니다. 연결 또는 세션에 영향을 주기 위해 재설정이 제시간에 도달할 수 있을 것이므로 능동 응답은 인라인 구축에서 가장 효과적입니다.

Maximum Active Responses 옵션의 구성 방법에 따라, 연결 또는 세션의 어느 한쪽 끝에서 추가 트래픽이 발생하는 경우 시스템은 추가 능동 응답을 시작할 수도 있습니다. 이전 응답 이후 일정 기간(초)이 경과하면 시스템은 지정된 최대값까지 각각의 추가 능동 응답을 시작합니다.

능동 응답의 최대 수를 설정하는 방법에 대한 자세한 내용은 29-22페이지의 TCP 전역 옵션 선택을/를 참조하십시오.

Maximum Active Responses의 컨피그레이션과 상관없이, 트리거된 **resp** 또는 **react** 규칙도 능동 응답을 시작할 수 있습니다. 그러나 **Maximum Active Responses**는 시스템이 삭제 규칙에 대한 능동 응답의 최대 수를 제어하는 것과 동일한 방식으로 **resp** 및 **react** 규칙에 대해 추가 능동 응답을 시작할지 여부를 제어합니다. 자세한 내용은 36-85페이지의 규칙 키워드로 능동 응답 시작을/를 참조하십시오.

또한 패시브 구축에서 사용할 능동 응답 인터페이스 및 시도할 TCP 재설정 횟수를 구성하려면 `config response` 명령을 사용할 수 있습니다. 자세한 내용은 36-88페이지의 능동 응답 재설정 시도 및 인터페이스 설정을/를 참조하십시오.

다음 옵션과 연결된 프리프로세서 규칙은 없습니다.

Maximum Active Responses

TCP 연결당 최대 1~25개의 능동 응답을 지정합니다. 능동 응답이 시작된 연결에서 추가 트래픽이 발생하면, 능동 응답 이후 **Minimum Response Seconds**가 지난 다음에 트래픽이 발생하며, 지정된 최대값에 도달하지 않은 경우 시스템은 또 다른 능동 응답을 전송합니다. 설정이 0이면 삭제 규칙에 의해 트리거된 능동 응답이 비활성화되고, **resp** 또는 **react** 규칙에 의해 트리거된 추가 능동 응답이 비활성화됩니다. 자세한 내용은 29-3페이지의 침입 삭제 규칙으로 능동 응답 시작 및 36-85페이지의 규칙 키워드로 능동 응답 시작을/를 참조하십시오.

Minimum Response Seconds

Maximum Active Responses에 도달할 때까지, 시스템이 능동 응답을 시작한 연결에 대한 추가 트래픽이 후속 능동 응답으로 이어지기 전 대기 시간을 1~300초 범위로 지정합니다.

삭제 규칙으로 능동 응답을 시작하려면

액세스: Admin/Access Admin/Network Admin

1단계 **Policies > Access Control**을 선택합니다.

Access Control Policy 페이지가 나타납니다.

2단계 수정할 액세스 제어 정책 옆에 있는 수정 아이콘( )을 클릭합니다.

액세스 제어 정책 편집기가 나타납니다.

3단계 **Advanced** 탭을 선택합니다.

Access control policy advanced settings 페이지가 나타납니다.

4단계 **Transport/Network Layer Preprocessor Settings** 옆에 있는 수정 아이콘( )을 클릭합니다.

Transport/Network Layer Preprocessor Settings 팝업 창이 나타납니다.

5단계 다음 옵션을 이용할 수 있습니다.

- TCP 연결당 **Maximum Active Responses**의 값을 1~25 범위로 지정합니다. 설정이 0이면 삭제 규칙에 의해 트리거된 능동 응답이 비활성화되고, **resp** 또는 **react** 규칙에 의해 트리거된 추가 능동 응답이 비활성화됩니다.
- **Maximum Active Responses**에 도달할 때까지 또는 시스템이 능동 응답을 시작한 연결에 대한 추가 트래픽이 후속 능동 응답으로 이어지기까지 대기할 **Minimum Response Seconds**의 값을 1~300 범위로 지정합니다.

6단계 **OK**를 클릭합니다.

변경 사항을 적용하려면 액세스 제어 정책을 적용해야 합니다. 12-15페이지의 액세스 제어 정책 적용을/를 참조하십시오.

문제 해결: 세션 종료 메시지 로깅

라이센스: 보호

고객 지원과의 문제 해결 통화 중에, 개별 연결이 지정된 임계값을 초과할 경우의 메시지를 로깅하도록 시스템을 구성하라고 요청할 수 있습니다. 이 옵션에 대한 설정의 변경은 고객 지원의 지침에 의해서만 수행할 수 있으며 성능에 영향을 미치게 됩니다.

세션 종료 메시지를 로깅하려면

액세스: Admin/Access Admin/Network Admin

1단계 **Policies > Access Control**을 선택합니다.

Access Control Policy 페이지가 나타납니다.

2단계 수정할 액세스 제어 정책 옆에 있는 수정 아이콘( )을 클릭합니다.

액세스 제어 정책 편집기가 나타납니다.

3단계 **Advanced** 탭을 선택합니다.

Access control policy advanced settings 페이지가 나타납니다.

4단계 **Transport/Network Layer Preprocessor Settings** 옆에 있는 수정 아이콘( )을 클릭합니다.

Transport/Network Layer Preprocessor Settings 팝업 창이 나타납니다.

5단계 **Troubleshooting Options**를 확장합니다.

6단계 세션이 종료되고 지정된 수를 초과했을 때 로깅된 메시지에 나타나는 바이트 수인 **Session Termination Logging Threshold**를 지정합니다.

상한은 1GB이지만, 스트림 처리에 할당된 관리되는 디바이스의 메모리 양에 의해서도 제한을 받습니다.

7단계 **OK** 를 클릭합니다.

변경 사항을 적용하려면 액세스 제어 정책을 적용해야 합니다. 12-15페이지의 액세스 제어 정책 적용을/를 참조하십시오.

체크섬 확인

라이센스: 보호

IP, TCP, UDP 및 ICMP 전송이 완전히 수신되도록 보장하고, 기본적인 수준에서 패킷이 변조되거나 전송 중에 실수로 변경되지 않도록 보장하기 위해 시스템은 모든 프로토콜 레벨 체크섬을 확인할 수 있습니다. 체크섬은 패킷에서 프로토콜의 무결성을 확인하기 위한 알고리즘을 사용합니다. 최종 호스트가 패킷에 기록한 동일한 값을 시스템이 계산하는 경우 패킷은 변경되지 않아야 합니다.

체크섬 확인을 비활성화하면 네트워크가 삽입 공격에 취약해질 수 있습니다. 시스템은 체크섬 확인 이벤트를 생성하지 않습니다. 인라인 구축에서, 체크섬이 잘못된 패킷을 시스템이 삭제하도록 구성할 수 있습니다.

체크섬 확인을 구성하려면

액세스: Admin/Intrusion Admin

1단계 **Policies > Access Control**을 선택하여 Access Control Policy 페이지를 표시한 다음 **Network Analysis Policy**를 클릭합니다.

Network Analysis Policy 페이지가 나타납니다.

2단계 수정할 정책 옆에 있는 수정 아이콘( )을 클릭합니다.

다른 정책에 저장하지 않은 변경 사항이 있는 경우 변경 사항을 취소하고 계속 진행하려면 **OK**를 클릭합니다. 저장하지 않은 변경 사항을 다른 정책에 저장하는 방법에 대한 자세한 내용은 23-15페이지의 충돌 해결 및 정책 변경 사항 커밋을/를 참조하십시오.

Edit Policy 페이지가 나타납니다.

3단계 왼쪽의 탐색 패널에서 **Settings**를 클릭합니다.

Settings 페이지가 나타납니다.

4단계 Transport/Network Layer Preprocessors 아래에서 **Checksum Verification**이 활성화되었는지 여부에 따라 두 가지 선택 사항이 있습니다.

- 컨피그레이션이 활성화되어 있으면 **Edit**를 클릭합니다.
- 컨피그레이션이 비활성화되어 있으면 **Enabled**를 클릭한 다음 **Edit**를 클릭합니다.

Checksum Verification 페이지가 나타납니다. 페이지 하단에 있는 메시지는 컨피그레이션이 포함된 정책 레이어를 식별합니다. 자세한 내용은 24-1페이지의 네트워크 분석 또는 침입 정책에서 레이어 사용을/를 참조하십시오.

5단계 Checksum Verification 섹션의 다음 옵션을 패시브 또는 인라인 구축에서는 **Enabled** 또는 **Disabled**로 설정하고 인라인 구축에서는 **Drop**으로 설정할 수 있습니다.

- **ICMP Checksums**
- **IP Checksums**
- **TCP Checksums**
- **UDP Checksums**

옵션을 **Drop**으로 설정하고 위반 패킷을 삭제하려면 관련 네트워크 분석 정책에서 **Inline Mode**를 활성화해야 합니다. 자세한 내용은 26-5페이지의 인라인 구축에서 프리프로세서가 트래픽에 영향을 미치도록 허용을/를 참조하십시오. 패시브 구축에서 이러한 옵션을 **Drop**으로 설정하거나 인라인 구축에서 탭 모드로 설정하는 것은 옵션을 **Enabled**로 설정하는 것과 같습니다.

6단계 정책을 저장하거나, 계속 수정하거나, 변경 사항을 취소하거나, 기반 정책의 기본 컨피그레이션 설정으로 돌아가거나, 시스템 캐시에 변경 사항이 남아 있는 상태로 종료합니다. 자세한 내용은 23-15페이지의 충돌 해결 및 정책 변경 사항 커밋을/를 참조하십시오.

인라인 트래픽 표준화

라이센스: 보호

인라인 구축에서 인라인 표준화 프리프로세서는 공격자가 탐지를 회피할 가능성을 최소화하기 위해 트래픽을 표준화합니다. 사용자가 네트워크 분석 정책에서 인라인 표준화 프리프로세서를 활성화하면, 시스템은 인라인 구축이 사용 중인지 확인하기 위해 다음 두 가지 조건을 테스트합니다.

- **Inline Mode**가 정책에서 활성화되었는지 확인합니다. 26-5페이지의 인라인 구축에서 프리프로세서가 트래픽에 영향을 미치도록 허용을/를 참조하십시오.
- 인라인 표준화가 활성화된 액세스 제어 정책이 인라인으로 구축되었고 인라인 집합을 사용하는 디바이스에 적용되었는지 확인합니다.

두 가지 조건이 충족되면 프리프로세서는 지정된 트래픽을 표준화합니다.

IPv4, IPv6, ICMPv4, ICMPv6 및 TCP 트래픽의 임의의 조합에 대한 표준화를 지정할 수 있습니다. 대부분의 표준화는 패킷 기준이며 인라인 표준화 프리프로세서에 의해 수행됩니다. 그러나 TCP 스트림 프리프로세서는 TCP 페이로드 표준화를 포함하여 대부분의 상태 관련 패킷과 스트림 표준화를 처리합니다.

인라인 표준화는 패킷 디코더에 의한 디코딩 직후 및 기타 프리프로세서에 의한 처리 전에 발생합니다. 표준화는 패킷 레이어의 안쪽에서 바깥쪽으로 진행됩니다.

인라인 표준화 프리프로세서는 이벤트를 생성하지 않고, 다른 프리프로세서 및 규칙 엔진이 인라인 구축에 사용할 패킷을 준비합니다. 이 프리프로세서는 또한 시스템이 처리하는 패킷이 네트워크의 호스트에서 수신하는 패킷과 동일한지를 확인하도록 지원합니다.

팁 인라인 구축의 경우 Cisco는 **Normalize TCP Payload** 옵션을 활성화하여 인라인 표준화 프리프로세서를 구성할 것을 권장합니다. 패시브 구축 시 Cisco의 권장 사항은 적응형 프로필을 구성하는 것입니다. 자세한 내용은 30-1페이지의 수동 구축 시 전처리 튜닝을/를 참조하십시오.

Minimum TTL

Reset TTL이 이 옵션에 대해 설정된 1~255 값보다 크거나 같으면 다음을 지정합니다.

- **Normalize IPv4**가 활성화되었을 때 시스템이 IPv4 Time to Live (TTL) 필드에서 허용할 최소값. 값이 더 낮으면 TTL에 대한 패킷 값이 **Reset TTL**에 대해 설정된 값으로 표준화됩니다.
- **Normalize IPv6**이 활성화되었을 때 시스템이 IPv6 Hop Limit 필드에서 허용할 최소값. 값이 더 낮으면 Hop Limit에 대한 패킷 값이 **Reset TTL**에 대해 설정된 값으로 표준화됩니다.

  값이 1이면 시스템은 필드가 비어 있는 것으로 간주합니다.

  이 옵션에 대한 이벤트를 생성하려면 디코더 규칙 카테고리에서 다음 규칙을 활성화할 수 있습니다.

- 시스템이 지정된 최소값보다 더 낮은 TTL의 IPv4 패킷을 탐지할 때 이벤트를 생성하려면 규칙 116:428을 활성화할 수 있습니다.
- 시스템이 지정된 최소값보다 더 낮은 Hop Limit의 IPv6 패킷을 탐지할 때 이벤트를 생성하려면 규칙 116:270을 활성화할 수 있습니다.

  자세한 내용은 29-20페이지의 패킷 디코딩 구성의 패킷 디코더 **Detect Protocol Header Anomalies** 옵션을/를 참조하십시오.

Reset TTL

Minimum TTL보다 크거나 같은 1~255 값으로 설정된 경우 다음을 표준화합니다.

- **Normalize IPv4**가 활성화된 경우 IPv4 TTL 필드
- **Normalize IPv6**이 활성화된 경우 IPv6 Hop Limit 필드

패킷 값이 **Minimum TTL**보다 작은 경우 시스템은 TTL 또는 Hop Limit 값을 이 옵션에 대해 설정된 값으로 변경하여 패킷을 표준화합니다. 이 옵션을 0 또는 **Minimum TTL**보다 작은 값으로 설정하면 이 옵션이 비활성화됩니다. 값이 0이면 시스템은 필드가 비어 있는 것으로 간주합니다.

Normalize IPv4

IPv4 트래픽의 표준화를 활성화합니다. 시스템은 또한 이 옵션이 활성화되고 **Reset TTL**에 대해 설정된 값이 TTL 표준화를 활성화하면 필요에 따라 TTL 필드를 표준화합니다. 이 옵션이 활성화되면 **Normalize Don't Fragment Bits** 및 **Normalize Reserved Bits**도 활성화할 수 있습니다.

이 옵션이 활성화되면 시스템은 다음의 기반 IPv4 표준화를 수행합니다.

- 초과 페이로드의 패킷을 IP 헤더에 지정된 데이터그램 길이로 절단
- 전에 Type of Service (TOS) 필드로 알려진 Differentiated Services (DS) 필드 지우기
- 모든 옵션 옥텟을 1(No Operation)로 설정

Normalize Don't Fragment Bit

IPv4 Flags 헤더 필드의 단일 비트 Don't Fragment 하위 필드를 지웁니다. 이 옵션을 활성화하면 다운스트림 라우터에서 필요 시 패킷을 삭제하는 대신 프래그먼트할 수 있습니다. 또한 삭제할 가공 패킷을 기반으로 하는 회피를 방지할 수도 있습니다. 이 옵션을 선택하려면 **Normalize IPv4**를 활성화해야 합니다.

Normalize Reserved Bit

IPv4 Flags 헤더 필드의 단일 비트 Reserved 하위 필드를 지웁니다. 이 옵션은 일반적으로 활성화합니다. 이 옵션을 선택하려면 **Normalize IPv4**를 활성화해야 합니다.

Normalize TOS Bit

전에 Type of Service로 알려진 1바이트 Differentiated Services 필드를 지웁니다. 이 옵션을 선택하려면 **Normalize IPv4**를 활성화해야 합니다.

Normalize Excess Payload

초과 페이로드의 패킷을 IP 헤더 및 Layer 2(예: Ethernet) 헤더에 지정된 데이터그램 길이로 자르지만, 최소 프레임 길이 아래로는 자르지 않습니다. 이 옵션을 선택하려면 **Normalize IPv4**를 활성화해야 합니다.

Normalize IPv6

Hop-by-Hop Options and Destination Options 확장 헤더의 모든 Option Type 필드를 00(Skip and continue processing)으로 설정합니다. 시스템은 또한 이 옵션이 활성화되고 **Reset TTL**에 대해 설정된 값이 Hop Limit 표준화를 활성화하면 필요에 따라 Hop Limit 필드를 표준화합니다.

Normalize ICMPv4

ICMPv4 트래픽의 Echo (Request) 및 Echo Reply 메시지에서 8-bit Code 필드를 지웁니다.

Normalize ICMPv6

ICMPv6 트래픽의 Echo (Request) 및 Echo Reply 메시지에서 8-bit Code 필드를 지웁니다.

Normalize/Clear Reserved Bits

TCP 헤더에서 Reserved 비트를 지웁니다.

Normalize/Clear Option Padding Bytes

모든 TCP 옵션 패딩 바이트를 지웁니다.

Clear Urgent Pointer if URG=0

Urgent(URG) 제어 비트가 설정되지 않은 경우 16비트 TCP 헤더 Urgent Pointer 필드를 지웁니다.

Clear Urgent Pointer/URG on Empty Payload

페이로드가 없는 경우 TCP 헤더 Urgent Pointer 필드 및 URG 제어 비트를 지웁니다.

Clear URG if Urgent Pointer is Not Set

Urgent Pointer가 설정되지 않은 경우 TCP 헤더 URG 제어 비트를 지웁니다.

Normalize Urgent Pointer

포인터가 페이로드 길이보다 긴 경우 2바이트 TCP 헤더 Urgent Pointer 필드를 페이로드 길이로 설정합니다.

Normalize TCP Payload

재전송된 데이터에서 일관성이 보장되도록 TCP Data 필드의 표준화를 활성화합니다. 적절히 리어셈블할 수 없는 세그먼트는 삭제됩니다.

Remove Data on SYN

TCP 운영 체제 정책이 Mac OS가 아닌 경우 동기화(SYN) 패킷에서 데이터를 제거합니다.

이 옵션은 또한 규칙 129:2에 대한 이벤트 생성을 비활성화합니다.

Remove Data on RST

TCP 재설정(RST) 패킷에서 데이터를 제거합니다.

Trim Data to Window

Window 필드에 지정된 크기로 TCP Data 필드를 자릅니다.

Trim Data to MSS

페이로드가 MSS(Maximum Segment Size)보다 긴 경우 TCP Data 필드를 MSS로 자릅니다.

Block Unrecoverable TCP Header Anomalies

이 옵션을 활성화하면 시스템은 표준화할 경우 잘못될 수 있거나 수신 호스트에서 차단될 수 있는 비정상적인 TCP 패킷을 차단합니다. 예를 들어 시스템은 설정된 세션에 이어서 전송되는 SYN 패킷을 차단합니다.

시스템은 또한 다음 TCP 스트림 프리프로세서 규칙(규칙의 활성화 여부와 상관없이) 중 하나와 일치하는 패킷을 삭제합니다.

- 129:1
- 129:3
- 129:4
- 129:6
- 129.8

- 129:11
- 129:14~129:19

Total Blocked Packets 성능 그래프는 인라인 구축에서 차단된 패킷 수, 그리고 탭 모드의 패시브 구축 및 인라인 구축에서, 인라인 구축에서였다면 차단되었을 수를 추적합니다. 자세한 내용은 41-5페이지의 침입 이벤트 성능 통계 그래프 생성을/를 참조하십시오.

Explicit Congestion Notification

ECN(Explicit Congestion Notification) 플래그의 패킷당 또는 스트림당 표준화를 다음과 같이 활성화합니다.

- 협상과 상관없이 패킷 단위 기준으로 ECN 플래그를 지우려면 **Packet** 선택
- ECN이 협상되지 않은 경우 스트림 단위 기준으로 ECN 플래그를 지우려면 **Stream** 선택

Stream을 선택하는 경우, 이 표준화가 발생하도록 하려면 TCP 스트림 프리프로세서 **Require TCP 3-Way Handshake** 옵션도 활성화되었는지 확인해야 합니다. 자세한 내용은 29-23페이지의 TCP 정책 옵션 선택을/를 참조하십시오.

Allow These TCP Options

트래픽에서 허용하는 특정 TCP 옵션의 표준화를 비활성화합니다.

명시적으로 허용하는 옵션은 시스템에서 표준화하지 않습니다. 옵션을 No Operation(TCP Option 1)으로 설정하여 명시적으로 허용하지 않는 옵션은 시스템에서 표준화합니다.

MSS(Maximum Segment Size), Window Scale 및 Time Stamp TCP 옵션은 최적의 TCP 성능을 위해 일반적으로 사용되므로 시스템은 이러한 옵션을 항상 허용합니다. **Allow These TCP Options**의 컨피그레이션과 상관없이 시스템은 일반적으로 사용되는 이러한 옵션을 표준화합니다. 기타 덜 일반적으로 사용되는 옵션은 시스템에서 자동으로 허용하지 않습니다.

다음 예에 나와 있는 것처럼 옵션 키워드, 옵션 번호 또는 둘 모두를 쉼표로 구분된 목록으로 구성하여 특정 옵션을 허용할 수 있습니다.

```
sack, echo, 19
```

옵션 키워드를 지정하는 것은 키워드와 관련된 하나 이상의 TCP 옵션에 대한 수를 지정하는 것과 같습니다. 예를 들어 `sack`를 지정하는 것은 TCP 옵션 4(Selective Acknowledgment Permitted) 및 5(Selective Acknowledgment)를 지정하는 것과 같습니다. 옵션 키워드는 대/소문자를 구분하지 않습니다.

모든 TCP 옵션을 허용하고 모든 TCP 옵션의 표준화를 효과적으로 비활성화하는 `any`를 지정할 수도 있습니다.

다음 표에는 허용되는 TCP 옵션을 지정하는 방법이 요약되어 있습니다. 필드를 비워두면 시스템은 MSS, Window Scale 및 Time Stamp 옵션만 허용합니다.

지정	허용
sack	TCP 옵션 4(Selective Acknowledgment Permitted) 및 5(Selective Acknowledgment)
echo	TCP 옵션 6(Echo Request) 및 7(Echo Reply)
partial_order	TCP 옵션 9(Partial Order Connection Permitted) 및 10 (Partial Order Service Profile)
conn_count	TCP Connection Count 옵션 11(CC), 12(CC.New) 및 13(CC.Echo)
alt_checksum	TCP 옵션 14(Alternate Checksum Request) 및 15(Alternate Checksum)

지정	허용
md5	TCP 옵션 19(MD5 Signature)
옵션 번호 2~255	키워드가 없는 옵션을 비롯한 특정 옵션
모든	모든 TCP 옵션. 이 설정은 TCP 옵션 표준화를 효과적으로 비활성화함

이 옵션에 대해 any를 지정하지 않으면 표준화에 다음이 포함됩니다.

- MSS, Window Scale, Time Stamp 및 기타 명시적으로 허용된 옵션을 제외한 모든 옵션 바이트는 No Operation(TCP Option 1)으로 설정됨
- Time Stamp가 존재하지만 유효하지 않거나, 유효하지만 협상되지 않은 경우 Time Stamp 옥텟을 No Operation으로 설정함
- Time Stamp가 협상되었지만 존재하지 않는 경우 패킷을 차단함
- Acknowledgment(ACK) 제어 비트가 설정되지 않은 경우 Time Stamp Echo Reply (TSecr) 옵션 필드를 지움
- SYN 제어 비트가 설정되지 않은 경우 MSS 및 Window Scale 옵션을 No Operation(TCP Option 1)으로 설정함

인라인 표준화 프리프로세서를 구성하려면

액세스: Admin/Intrusion Admin

1단계 **Policies > Access Control**을 선택하여 Access Control Policy 페이지를 표시한 다음 **Network Analysis Policy**를 클릭합니다.

Network Analysis Policy 페이지가 나타납니다.

2단계 수정할 정책 옆에 있는 수정 아이콘()을 클릭합니다.

다른 정책에 저장하지 않은 변경 사항이 있는 경우 변경 사항을 취소하고 계속 진행하려면 **OK**를 클릭합니다. 저장하지 않은 변경 사항을 다른 정책에 저장하는 방법에 대한 자세한 내용은 23-15페이지의 충돌 해결 및 정책 변경 사항 커밋을/를 참조하십시오.

Edit Policy 페이지가 나타납니다.

3단계 왼쪽의 탐색 패널에서 **Settings**를 클릭합니다.

Settings 페이지가 나타납니다.

4단계 Transport/Network Layer Preprocessors 아래에서 **Inline Normalization**이 활성화되었는지 여부에 따라 두 가지 선택 사항이 있습니다.

- 컨피그레이션이 활성화되어 있으면 **Edit**를 클릭합니다.
- 컨피그레이션이 비활성화되어 있으면 **Enabled**를 클릭한 다음 **Edit**를 클릭합니다.

Inline Normalization 페이지가 나타납니다. 페이지 하단에 있는 메시지는 컨피그레이션이 포함된 정책 레이어를 식별합니다. 자세한 내용은 24-1페이지의 네트워크 분석 또는 침입 정책에서 레이어 사용을/를 참조하십시오.

5단계 29-7페이지의 인라인 트래픽 표준화에 설명된 옵션 중 하나를 설정할 수 있습니다.

6단계 정책을 저장하거나, 계속 수정하거나, 변경 사항을 취소하거나, 기반 정책의 기본 컨피그레이션 설정으로 돌아가거나, 시스템 캐시에 변경 사항이 남아 있는 상태로 종료합니다. 자세한 내용은 23-15페이지의 충돌 해결 및 정책 변경 사항 커밋을/를 참조하십시오.

IP 패킷 디프래그먼트

라이센스: 보호

IP 데이터그램이 MTU(최대 전송 단위)보다 크기 때문에 둘 이상의 더 작은 IP 데이터그램으로 나뉘는 경우 *프래그먼트*되는 것입니다. 단일 IP 데이터그램 프래그먼트에는 숨겨진 공격을 식별하기 위한 충분한 정보가 포함되어 있지 않습니다. 공격자들은 프래그먼트된 패킷으로 공격 데이터를 전송하여 탐지를 회피하려고 시도할 수 있습니다. 해당 패킷에서 규칙이 공격을 좀 더 적절히 식별할 수 있도록, IP 디프래그먼트화 프리프로세서는 규칙 엔진이 규칙을 실행하기 전에 프래그먼트된 IP 데이터그램을 리어셈블합니다. 프래그먼트된 데이터그램을 리어셈블할 수 없으면 규칙이 실행되지 않습니다.

GID(generator ID)가 123인 IP 디프래그먼트화 프리프로세서 규칙을 활성화해야 이러한 규칙에서 이벤트를 생성할 수 있습니다. 자세한 내용은 32-20페이지의 규칙 상태 설정을/를 참조하십시오.

자세한 내용은 다음 절을 참조하십시오.

- 29-12페이지의 IP 프래그먼트화 익스플로잇 이해
- 29-13페이지의 대상 기반 디프래그먼트화 정책
- 29-14페이지의 디프래그먼트화 옵션 선택
- 29-15페이지의 IP 디프래그먼트화 구성

IP 프래그먼트화 익스플로잇 이해

라이센스: 보호

IP 디프래그먼트화를 활성화하면 네트워크의 호스트에서 Teardrop 공격 또는 시스템 자체에 대한 리소스 소모 공격(예: Jolt2 공격)과 같은 공격을 탐지하는 데 도움이 됩니다.

Teardrop 공격은 중복 IP 프래그먼트를 리어셈블하려고 시도할 때 충돌을 일으키는 특정 운영 체제의 버그를 악용합니다. 활성화 및 구성된 IP 디프래그먼트화 프리프로세서는 중복 프래그먼트를 식별합니다. IP 디프래그먼트화 프리프로세서는 Teardrop과 같은 중복 프래그먼트 공격에서 첫 번째 패킷을 탐지하지만, 동일한 공격의 후속 패킷은 탐지하지 않습니다.

Jolt2 공격은 IP defragmentor의 과다 사용으로 서비스 거부 공격을 일으키기 위해 동일한 프래그먼트된 IP 패킷의 매우 많은 복사본을 전송합니다. 메모리 usage cap 기능은 IP 디프래그먼트화 프리프로세서에서 이 공격 및 유사한 공격을 중단하고, 철저한 검사로 시스템이 자체 보존을 구현하도록 지원합니다. 시스템은 공격으로 혼란에 빠지지 않으며, 운영 상태를 유지하고, 계속해서 네트워크 트래픽을 검사합니다.

운영 체제마다 각기 다른 방법으로 프래그먼트된 패킷을 리어셈블합니다. 호스트에서 실행되는 운영 체제를 확인할 수 있는 공격자는 대상 호스트가 특정 방법으로 리어셈블하도록 악의적인 패킷을 프래그먼트할 수 있습니다. 모니터링되는 네트워크의 호스트가 실행하는 운영 체제가 무엇인지를 시스템은 알지 못하므로 프리프로세서에서 패킷을 정확하지 않게 리어셈블 및 검사함으로써 익스플로잇이 탐지되지 않고 통과될 수 있습니다. 이러한 종류의 공격을 완화하려면 네트워크의 각 호스트에 대해 적절한 패킷 디프래그먼트 방법을 사용하도록 디프래그먼트화 프리프로세서를 구성할 수 있습니다. 자세한 내용은 29-13페이지의 대상 기반 디프래그먼트화 정책을/를 참조하십시오.

또한패킷의 대상 호스트에 대한 호스트 운영 체제 정보를 사용하여 IP 디프래그먼트화 프리프로세서에 대한 대상 기반 정책을 동적으로 선택하려면 적응형 프로필을 사용할 수 있습니다. 자세한 내용은 30-1페이지의 수동 구축 시 전처리 튜닝을/를 참조하십시오.

대상 기반 디프래그먼트화 정책

라이센스: 보호

호스트 운영 체제는 패킷을 리어셈블할 때 어떤 코드 프래그먼트를 사용할지 결정하기 위해 세 가지 기준을 사용합니다. 프래그먼트가 운영 체제에서 수신된 순서, 오프셋(바이트 단위로 패킷 시작부터 프래그먼트의 거리), 그리고 중복 프래그먼트와 비교한 시작 및 종료 위치가 그것입니다. 모든 운영 체제가 이 기준을 사용하지만, 운영 체제마다 프래그먼트된 패킷을 리어셈블할 때 선호하는 프래그먼트가 다릅니다. 따라서 네트워크에서 운영 체제가 다른 두 호스트는 동일한 중복 프래그먼트를 완전히 다른 방식으로 리어셈블할 수 있습니다.

호스트 중 하나의 운영 체제를 알고 있는 공격자는 악의적인 내용을 중복 패킷 프래그먼트에 숨겨 전송하여 탐지를 회피하고 호스트를 악용하려고 시도할 수 있습니다. 이 패킷을 리어셈블하여 검사하면 무해한 것처럼 보이지만, 대상 호스트에서 리어셈블될 경우 악의적인 익스플로잇을 포함하게 됩니다. 그러나 모니터링되는 네트워크 세그먼트에서 실행 중인 운영 체제를 인식하도록 IP 디프래그먼트화 프리프로세서를 구성하면, 대상 호스트가 하는 것과 동일한 방식으로 프래그먼트가 리어셈블되므로 공격을 식별할 수 있습니다.

대상 호스트의 운영 체제에 따라 7개의 디프래그먼트화 정책 중 하나를 사용하도록 IP 디프래그먼트화 프리프로세서를 구성할 수 있습니다. 다음 표에는 7개의 정책 및 각각을 사용하는 운영 체제가 나열되어 있습니다. First 및 Last 정책 이름은 해당 정책이 원래의 중복 패킷을 선호하는지 후속 중복 패킷을 선호하는지를 반영합니다.

표 29-1 대상 기반 디프래그먼트화 정책

정책	운영 체제
BSD	AIX
	FreeBSD
	IRIX
	VAX/VMS
BSD-right	HP JetDirect
First	Mac OS
	HP-UX
Linux	Linux
	OpenBSD
Last	Cisco IOS
Solaris	SunOS
Windows	Windows

디프래그먼트화 옵션 선택

라이센스: 보호

단순히 IP 디프래그먼트화를 활성화 또는 비활성화하도록 선택할 수도 있습니다. 그러나 Cisco에서는 활성화된 IP 디프래그먼트화 프리프로세서의 동작을 좀 더 세부적으로 지정할 것을 권장합니다.

다음 설명에서 프리프로세서 규칙이 언급되지 않은 경우 해당 옵션은 프리프로세서 규칙과 관련되지 않은 것입니다.

글로벌 **Preallocated Fragments** 옵션을 구성할 수 있습니다.

Preallocated Fragments

프리프로세서가 동시에 처리할 수 있는 개별 프래그먼트의 최대 수. 사전 할당할 프래그먼트 노드의 수를 지정하면 고정 메모리를 할당할 수 있습니다.

주의 개별 프래그먼트를 처리하는 데 약 1550바이트의 메모리가 사용됩니다. 프리프로세서가 개별 프래그먼트를 처리하는 데 관리되는 디바이스에 대해 사전 결정된 허용 메모리 제한보다 더 많은 메모리가 필요한 경우, 디바이스에 대한 메모리 제한이 우선적으로 적용됩니다.

각 IP 디프래그먼트화 정책에 대해 다음 옵션을 구성할 수 있습니다.

Networks

디프래그먼트화 정책을 적용할 하나 이상의 호스트의 IP 주소.

단일 IP 주소나 주소 블록 또는 쉼표로 구분된 목록을 지정할 수 있습니다(둘 중 하나 또는 모두). 기본 정책을 포함하여 최대 255개의 총 프로필을 지정할 수 있습니다. FireSIGHT 시스템에서 IPv4 및 IPv6 주소 블록을 사용하는 방법에 대한 자세한 내용은 1-19페이지의 IP 주소 표기 규칙을/를 참조하십시오.

기본 정책의 `default` 설정은 다른 대상 기반 정책에서 처리되지 않는 모니터링되는 네트워크 세그먼트의 모든 IP 주소를 지정합니다. 따라서 기본 정책에 대해서는 IP 주소 또는 CIDR 블록/접두사 길이를 지정할 수 없고 지정할 필요도 없으며, 다른 정책에서 이 설정을 비워둘 수 없거나 `any`를 나타내는 주소 표기법(예: 0.0.0.0/0 또는 ::/0)을 사용할 수 없습니다.

또한 트래픽 처리를 위한 대상 기반 정책의 경우, 식별하는 네트워크는 대상 기반 정책을 구성하는 네트워크 분석 정책에서 처리되는 네트워크, 영역, VLAN의 하위 집합과 일치하거나 하위 집합이어야 합니다. 자세한 내용은 25-3페이지의 네트워크 분석 정책으로 전처리 맞춤화을/를 참조하십시오.

Policy

모니터링되는 네트워크 세그먼트에서 호스트 집합에 대해 사용할 디프래그먼트화 정책. 7가지 정책인 BSD, BSD-Right, First, Linux, Last, Solaris, Windows 중에서 선택할 수 있습니다. 이러한 정책에 대한 자세한 내용은 29-13페이지의 대상 기반 디프래그먼트화 정책을/를 참조하십시오.

Timeout

프래그먼트된 패킷을 리어셈블할 때 프리프로세서 엔진이 사용할 수 있는 시간(초)을 지정합니다. 지정된 시간 내에 패킷을 리어셈블하지 못하면 프리프로세서 엔진은 리어셈블 시도를 중지하고 수신된 프래그먼트를 폐기합니다.

Minimum TTL

패킷이 가질 수 있는 허용되는 최소 TTL 값을 지정합니다. 이 옵션은 TTL 기반 삽입 공격을 탐지합니다.

이 옵션에 대한 이벤트를 생성하려면 규칙 123:1을 활성화할 수 있습니다. 자세한 내용은 32-20 페이지의 규칙 상태 설정을/를 참조하십시오.

Detect Anomalies

중복 프래그먼트와 같은 프래그먼트화 문제를 식별합니다.

이 옵션에 대한 이벤트를 생성하려면 다음 규칙을 활성화할 수 있습니다.

- 123:1~123:4
- 123:5(BSD 정책)
- 123:6~123:8

Overlap Limit

세션의 중복 세그먼트에서 0(무제한)과 255 사이로 구성된 숫자가 탐지된 경우 해당 세션에 대해 디프래그먼트화가 중지됩니다. 이 옵션을 구성하려면 **Detect Anomalies**를 활성화해야 합니다. 값을 비워 두면 이 옵션이 비활성화됩니다.

이 옵션에 대한 이벤트를 생성하려면 규칙 123:12를 활성화할 수 있습니다. 자세한 내용은 32-20페이지의 규칙 상태 설정을/를 참조하십시오.

Minimum Fragment Size

0(무제한)과 255바이트 사이로 구성된 숫자보다 작은, 최종이 아닌 프래그먼트가 탐지된 경우 패킷이 악의적인 것으로 간주됩니다. 이 옵션을 구성하려면 **Detect Anomalies**를 활성화해야 합니다. 값을 비워 두면 이 옵션이 비활성화됩니다.

이 옵션에 대한 이벤트를 생성하려면 규칙 123:13을 활성화할 수 있습니다. 자세한 내용은 32-20페이지의 규칙 상태 설정을/를 참조하십시오.

IP 디프래그먼트화 구성

라이센스: 보호

IP 디프래그먼트화 프리프로세서를 구성하려면 다음 절차를 사용할 수 있습니다. IP 디프래그먼트화 프리프로세서 컨피그레이션 옵션에 대한 자세한 내용은 29-14페이지의 디프래그먼트화 옵션 선택을/를 참조하십시오.

IP 디프래그먼트화를 구성하려면

액세스: Admin/Intrusion Admin

1단계 **Policies > Access Control**을 선택하여 Access Control Policy 페이지를 표시한 다음 **Network Analysis Policy**를 클릭합니다.

Network Analysis Policy 페이지가 나타납니다.

2단계 수정할 정책 옆에 있는 수정 아이콘( )을 클릭합니다.

다른 정책에 저장하지 않은 변경 사항이 있는 경우 변경 사항을 취소하고 계속 진행하려면 **OK**를 클릭합니다. 저장하지 않은 변경 사항을 다른 정책에 저장하는 방법에 대한 자세한 내용은 23-15페이지의 충돌 해결 및 정책 변경 사항 커밋을/를 참조하십시오.

Edit Policy 페이지가 나타납니다.

3단계 왼쪽의 탐색 패널에서 **Settings**를 클릭합니다.

Settings 페이지가 나타납니다.

4단계 Transport/Network Layer Preprocessors 아래에서 **IP Defragmentation**이 활성화되었는지 여부에 따라 두 가지 선택 사항이 있습니다.

- 컨피그레이션이 활성화되어 있으면 **Edit**를 클릭합니다.
- 컨피그레이션이 비활성화되어 있으면 **Enabled**를 클릭한 다음 **Edit**를 클릭합니다.

IP Defragmentation 페이지가 나타납니다. 페이지 하단에 있는 메시지는 컨피그레이션이 포함된 정책 레이어를 식별합니다. 자세한 내용은 24-1페이지의 네트워크 분석 또는 침입 정책에서 레이어 사용을/를 참조하십시오.

5단계 선택적으로, Global Settings 페이지 영역에서 **Preallocated Fragments**에 대한 설정을 수정할 수 있습니다.

6단계 다음 2가지 옵션을 사용할 수 있습니다.

- 새로운 대상 기반 정책을 추가합니다. 페이지 왼쪽의 **Servers** 옆에 있는 추가 아이콘( )을 클릭합니다. Add Target 팝업 창이 나타납니다. **Host Address** 필드에서 하나 이상의 IP 주소를 지정하고 **OK**를 클릭합니다.

  단일 IP 주소나 주소 블록 또는 쉼표로 구분된 목록을 지정할 수 있습니다(둘 중 하나 또는 모두). 기본 정책을 포함하여 총 255개의 대상 기반 정책을 생성할 수 있습니다. FireSIGHT 시스템에서 IP 주소 블록을 사용하는 방법에 대한 자세한 내용은 1-19페이지의 IP 주소 표기 규칙을/를 참조하십시오.

  트래픽 처리를 위한 대상 기반 정책의 경우, 식별하는 네트워크는 대상 기반 정책을 구성하는 네트워크 분석 정책에서 처리되는 네트워크, 영역, VLAN의 하위 집합과 일치하거나 하위 집합이어야 합니다. 자세한 내용은 25-3페이지의 네트워크 분석 정책으로 전처리 맞춤화을/를 참조하십시오.

  새 항목이 페이지 왼쪽의 대상 목록에 나타나서 선택된 것을 알 수 있도록 강조 표시되며, 추가한 정책에 대한 현재 컨피그레이션을 반영하여 Configuration 섹션이 업데이트됩니다.

- 기존의 대상 기반 정책에 대한 설정을 수정합니다. 페이지 왼쪽의 **Hosts** 아래에서 추가한 정책에 대해 구성된 주소를 클릭하거나 **default**를 클릭합니다.

  선택 항목이 강조 표시되고, 선택한 정책에 대한 현재 컨피그레이션을 표시하기 위해 Configuration 섹션이 업데이트됩니다. 기존의 대상 기반 정책을 삭제하려면 제거할 정책 옆에 있는 삭제 아이콘( )을 클릭합니다.

7단계 선택적으로, Configuration 페이지 영역에서 옵션을 수정할 수 있습니다.

8단계 정책을 저장하거나, 계속 수정하거나, 변경 사항을 취소하거나, 기반 정책의 기본 컨피그레이션 설정으로 돌아가거나, 시스템 캐시에 변경 사항이 남아 있는 상태로 종료합니다. 자세한 내용은 23-15페이지의 충돌 해결 및 정책 변경 사항 커밋을/를 참조하십시오.

패킷 디코딩 이해

라이센스: 보호

캡처된 패킷을 프리프로세서로 전송하기 전에 시스템은 먼저 패킷을 패킷 디코더로 전송합니다. 패킷 디코더는 패킷 헤더와 페이로드를 프리프로세서와 규칙 엔진이 쉽게 사용할 수 있는 형식으로 변환합니다. 각 스택 레이어는 데이터 링크 레이어로 시작하여 계속해서 네트워크 및 전송 레이어를 통해 차례로 디코딩됩니다.

GID(generator ID)가 116인 IP 패킷 디코더 규칙을 활성화해야 이러한 규칙에서 이벤트를 생성할 수 있습니다. 자세한 내용은 32-20페이지의 규칙 상태 설정을/를 참조하십시오.

다음 설명에서 프리프로세서 규칙이 언급되지 않은 경우 해당 옵션은 프리프로세서 규칙과 관련되지 않은 것입니다.

Decode GTP Data Channel

캡슐화된 GTP(General Packet Radio Service[GPRS] Tunneling Protocol) 데이터 채널을 디코딩합니다. 기본적으로 디코더는 포트 3386에서 버전 0 데이터를, 포트 2152에서 버전 1 데이터를 디코딩합니다. 캡슐화된 GTP 트래픽을 식별하는 포트를 수정하려면 `GTP_PORTS` 기본 변수를 사용할 수 있습니다. 자세한 내용은 3-18페이지의 사전 정의된 기본 변수 최적화을/를 참조하십시오.

이 옵션에 대한 이벤트를 생성하려면 규칙 116:297 및 116:298을 활성화할 수 있습니다.

Detect Teredo on Non-Standard Ports

포트 3544 이외의 UDP 포트에서 식별된 IPv6 트래픽의 Teredo 터널링을 검사합니다.

시스템은 IPv6 트래픽이 있을 때 항상 이를 검사합니다. 기본적으로 IPv6 검사에는 4in6, 6in4, 6to4 및 6in6 터널링 체계가 포함되며, UDP 헤더가 포트 3544를 지정하는 경우 Teredo 터널링도 포함됩니다.

IPv4 네트워크에서 IPv4 호스트는 IPv4 NAT(Network Address Translation) 디바이스를 통해 IPv6 트래픽을 터널링하기 위해 Teredo 프로토콜을 사용할 수 있습니다 Teredo는 IPv4 NAT 디바이스 뒤에서 IPv6 연결을 허용하기 위해 IPv4 UDP 데이터그램 내에 IPv6 패킷을 캡슐화합니다. 시스템은 Teredo 트래픽을 식별하기 위해 일반적으로 UDP 포트 3544를 사용합니다. 그러나 공격자는 탐지를 피하기 위해 비표준 포트를 사용할 수 있습니다. 시스템이 Teredo 터널링에서 모든 UDP 페이로드를 검사하도록 하려면 **Detect Teredo on Non-Standard Ports**를 활성화할 수 있습니다.

Teredo 디코딩은 첫 번째 UDP 헤더에서만, 그리고 IPv4가 외부 네트워크 레이어에 사용된 경우에만 발생합니다. IPv6 데이터에 캡슐화된 UDP 데이터 때문에 Teredo IPv6 레이어 이후 두 번째 UDP 레이어가 존재하는 경우 규칙 엔진은 UDP 침입 규칙을 사용하여 내부 및 외부 UDP 레이어를 모두 분석합니다.

policy-other 규칙 카테고리의 침입 규칙 12065, 12066, 12067 및 12068은 Teredo 트래픽을 탐지하지만 디코딩하지는 않습니다. 선택적으로, 이러한 규칙을 사용하여 인라인 구축에서 Teredo 트래픽을 삭제할 수 있습니다. 그러나 **Detect Teredo on Non-Standard Ports**를 활성화하는 경우에는 이러한 규칙을 비활성화하거나, 트래픽 삭제 없이 이벤트를 생성하도록 설정해야 합니다. 자세한 내용은 32-10페이지의 침입 정책의 규칙 필터링 및 32-20페이지의 규칙 상태 설정을/를 참조하십시오.

Detect Excessive Length Value

패킷 헤더가 실제 패킷 길이보다 긴 패킷 길이를 지정하는 경우를 탐지합니다.

이 옵션에 대한 이벤트를 생성하려면 규칙 116:6, 116:47, 116:97 및 116:275를 활성화할 수 있습니다.

Detect Invalid IP Options

잘못된 IP 옵션을 사용하는 익스플로잇을 식별하기 위해 잘못된 IP 헤더 옵션을 탐지합니다. 예를 들면 시스템 중단을 일으키는, 방화벽에 대한 서비스 거부 공격이 있습니다. 방화벽은 잘못된 Timestamp 및 Security IP 옵션을 구문 분석하려고 시도하며 제로 길이 확인에 실패하는데, 이로 인해 복구 불가능한 무한 루프가 발생합니다. 규칙 엔진은 제로 길이 옵션을 식별하고, 방화벽에서의 공격을 완화하기 위해 사용할 수 있는 정보를 제공합니다.

이 옵션에 대한 이벤트를 생성하려면 규칙 116:4 및 116:5를 활성화할 수 있습니다. 자세한 내용은 32-20페이지의 규칙 상태 설정을/를 참조하십시오.

Detect Experimental TCP Options

실험적 TCP 옵션으로 TCP 헤더를 탐지합니다. 다음 표에서는 이러한 옵션에 대해 설명합니다.

TCP 옵션	설명
9	Partial Order Connection Permitted
10	Partial Order Service Profile
14	Alternate Checksum Request
15	Alternate Checksum Data
18	Trailer Checksum
20	Space Communications Protocol Standards(SCPS)
21	Selective Negative Acknowledgements(SCPS)
22	Record Boundaries(SCPS)
23	Corruption(SPCS)
24	SNAP
26	TCP Compression Filter

이들은 실험적 옵션이므로 일부 시스템은 이들을 고려하지 않으며 익스플로잇에 노출될 수 있습니다.

참고 위의 표에 나열된 실험적 옵션 외에도 시스템은 26보다 큰 옵션 번호의 TCP 옵션을 실험적 옵션으로 간주합니다.

이 옵션에 대한 이벤트를 생성하려면 규칙 116:58을 활성화할 수 있습니다. 자세한 내용은 32-20페이지의 규칙 상태 설정을/를 참조하십시오.

Detect Obsolete TCP Options

폐기된 TCP 옵션으로 TCP 헤더를 탐지합니다. 이들은 폐기된 옵션이므로 일부 시스템은 이들을 고려하지 않으며 익스플로잇에 노출될 수 있습니다. 다음 표에서는 이러한 옵션에 대해 설명합니다.

TCP 옵션	설명
6	에코
7	Echo Reply
16	Skeeter
17	Bubba
19	MD5 Signature
25	할당되지 않음

이 옵션에 대한 이벤트를 생성하려면 규칙 116:57을 활성화할 수 있습니다. 자세한 내용은 32-20페이지의 규칙 상태 설정을/를 참조하십시오.

Detect T/TCP

CC.ECHO 옵션으로 TCP 헤더를 탐지합니다. CC.ECHO 옵션은 TCP for Transactions(T/TCP)가 사용 중임을 확인합니다. T/TCP 헤더 옵션은 널리 사용되지 않으므로 일부 시스템은 이들을 고려하지 않으며 익스플로잇에 노출될 수 있습니다.

이 옵션에 대한 이벤트를 생성하려면 규칙 116:56을 활성화할 수 있습니다. 자세한 내용은 32-20페이지의 규칙 상태 설정을/를 참조하십시오.

Detect Other TCP Options

다른 TCP 디코딩 이벤트 옵션으로 탐지되지 않는 잘못된 TCP 옵션의 TCP 헤더를 탐지합니다. 예를 들어 이 옵션은 잘못된 길이 또는 TCP 헤더 외부에 옵션 데이터를 두는 길이의 TCP 옵션을 탐지합니다.

이 옵션에 대한 이벤트를 생성하려면 규칙 116:54, 116:55 및 116:59를 활성화할 수 있습니다. 자세한 내용은 32-20페이지의 규칙 상태 설정을/를 참조하십시오.

Detect Protocol Header Anomalies

좀 더 구체적인 IP 및 TCP 디코더 옵션으로 탐지되지 않는 기타 디코딩 오류를 탐지합니다. 예를 들어, 디코더는 잘못된 형식의 데이터 링크 프로토콜 헤더를 탐지할 수 있습니다.

이 옵션에 대한 이벤트를 생성하려면 다른 패킷 디코더 옵션과 특별히 연결된 규칙 이외의 패킷 디코더 규칙을 활성화할 수 있습니다. 자세한 내용은 32-20페이지의 규칙 상태 설정을/를 참조하십시오.

116:270~116:274, 116:275 through 116:283, 116:291, 116:292, 116:295, 116:296, 116:406, 116:458, 116:460, 116:461 규칙은 비정상적인 IPv6 트래픽에 의해 트리거되는 이벤트를 생성합니다.

인라인 표준화 프리프로세서 **Minimum TTL** 옵션과 연결된 다음 규칙도 참조하십시오.

- 시스템이 지정된 최소값보다 더 낮은 TTL의 IPv4 패킷을 탐지할 때 이벤트를 생성하려면 규칙 116:428을 활성화할 수 있습니다.
- 시스템이 지정된 최소값보다 더 낮은 Hop Limit의 IPv6 패킷을 탐지할 때 이벤트를 생성하려면 규칙 116:270을 활성화할 수 있습니다.

자세한 내용은 29-7페이지의 인라인 트래픽 표준화의 인라인 표준화 **Minimum TTL** 옵션을/를 참조하십시오.

패킷 디코딩 구성

라이센스: 보호

Packet Decoding 컨피그레이션 페이지에서 패킷 디코딩을 구성할 수 있습니다. 패킷 디코딩 컨피그레이션 옵션에 대한 자세한 내용은 29-17페이지의 패킷 디코딩 이해을/를 참조하십시오.

패킷 디코딩을 구성하려면

액세스: Admin/Intrusion Admin

1단계 **Policies > Access Control**을 선택하여 Access Control Policy 페이지를 표시한 다음 **Network Analysis Policy**를 클릭합니다.

Network Analysis Policy 페이지가 나타납니다.

2단계 수정할 정책 옆에 있는 수정 아이콘( )을 클릭합니다.

다른 정책에 저장하지 않은 변경 사항이 있는 경우 변경 사항을 취소하고 계속 진행하려면 **OK**를 클릭합니다. 저장하지 않은 변경 사항을 다른 정책에 저장하는 방법에 대한 자세한 내용은 23-15페이지의 충돌 해결 및 정책 변경 사항 커밋을/를 참조하십시오.

Edit Policy 페이지가 나타납니다.

3단계 왼쪽의 탐색 패널에서 **Settings**를 클릭합니다.

Settings 페이지가 나타납니다.

4단계 Transport/Network Layer Preprocessors 아래에서 **Packet Decoding**이 활성화되었는지 여부에 따라 두 가지 선택 사항이 있습니다.

- 컨피그레이션이 활성화되어 있으면 **Edit**를 클릭합니다.
- 컨피그레이션이 비활성화되어 있으면 **Enabled**를 클릭한 다음 **Edit**를 클릭합니다.

Packet Decoding 페이지가 나타납니다. 페이지 하단에 있는 메시지는 컨피그레이션이 포함된 정책 레이어를 식별합니다. 자세한 내용은 23-15페이지의 충돌 해결 및 정책 변경 사항 커밋을/를 참조하십시오.

5단계 Packet Decoding 페이지에서 탐지 옵션을 활성화 또는 비활성화할 수 있습니다. 자세한 내용은 29-17페이지의 패킷 디코딩 이해을/를 참조하십시오.

6단계 정책을 저장하거나, 계속 수정하거나, 변경 사항을 취소하거나, 기반 정책의 기본 컨피그레이션 설정으로 돌아가거나, 시스템 캐시에 변경 사항이 남아 있는 상태로 종료합니다. 자세한 내용은 23-15페이지의 충돌 해결 및 정책 변경 사항 커밋을/를 참조하십시오.

TCP 스트림 전처리 사용

라이센스: 보호

TCP 프로토콜은 연결이 존재할 수 있는 여러 상태를 정의합니다. 각 TCP 연결은 소스/목적지 IP 주소 및 소스/목적지 포트로 식별됩니다. TCP는 동일한 연결 매개 변수 값과의 연결이 한 번에 하나만 존재하도록 허용합니다.

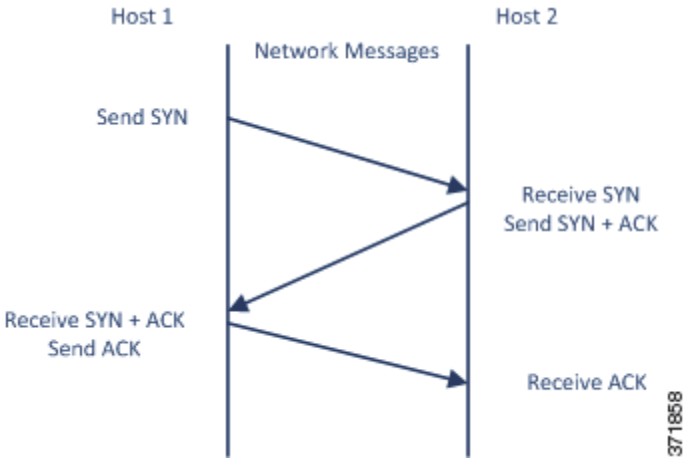
GID(generator ID)가 129인 TCP 스트림 프리프로세서 규칙을 활성화해야 이러한 규칙에서 이벤트를 생성할 수 있습니다. 자세한 내용은 32-20페이지의 규칙 상태 설정을/를 참조하십시오.

자세한 내용은 다음 절을 참조하십시오.

State-Related TCP 익스플로잇 이해

라이센스: 보호

침입 규칙에 `flow` 키워드와 `established` 인수를 추가하는 경우, 침입 규칙 엔진은 스테이트풀 모드에서 rule 및 flow 지시문과 일치하는 패킷을 검사합니다. 스테이트풀 모드는 클라이언트와 서버 간 합법적인 3-way 핸드셰이크로 설정된 TCP 세션의 일부인 트래픽만 평가합니다. 다음 데이터그램은 3-way 핸드셰이크를 보여줍니다.



설정된 TCP 세션의 일부로 식별할 수 없는 TCP 트래픽을 프리프로세서가 탐지하도록 시스템을 구성할 수 있습니다. 이 경우 이벤트가 빠르게 시스템 과부하를 일으킬 수 있고 의미 있는 데이터를 제공하지 않을 수 있으므로 이 방법은 권장되지 않습니다.

Stick 및 snot 같은 공격은 시스템의 폭넓은 규칙 집합 및 패킷 검사를 사용합니다. 이러한 툴은 Snort 기반 침입 규칙의 패턴을 기반으로 패킷을 생성하고 네트워크를 통해 전송합니다. 스테이트풀 검사를 위해 구성하기 위한 `flow` 또는 `flowbits` 키워드가 규칙에 포함되어 있지 않으면, 각 패킷이 규칙을 트리거하여 시스템이 혼란에 빠질 수 있습니다. 스테이트풀 검사를 사용하면 이러한 패킷을 무시할 수 있습니다. 이러한 패킷은 설정된 TCP 세션의 일부가 아니며 의미 있는 정보를 제공하지 않기 때문입니다. 스테이트풀 검사를 수행할 때 규칙 엔진은 설정된 TCP 세션의 일부인 공격만 탐지하므로, 분석가들은 stick 또는 snot으로 인한 다량의 이벤트 대신 이러한 공격에 집중할 수 있습니다.

TCP 전역 옵션 선택

라이센스: 보호

TCP 스트림 프리프로세서에는 TCP 스트림 프리프로세서의 작동 방식을 제어하는 하나의 전역 옵션이 있습니다.

이 옵션과 연결된 프리프로세서 규칙은 없습니다.

Packet Type Performance Boost

활성화된 침입 규칙에 지정되지 않은 모든 포트 및 애플리케이션 프로토콜에 대한 TCP 트래픽 무시를 활성화합니다. 단, 소스 및 목적지 포트가 모두 `any`로 설정된 TCP 규칙에 `flow` 또는 `flowbits` 옵션이 있는 경우는 예외입니다. 이렇게 성능을 개선할 경우 공격을 놓칠 수 있습니다.

대상 기반 TCP 정책 이해

라이센스: 보호

운영 체제마다 각기 다른 방법으로 TCP를 구현합니다. 예를 들어 Windows 및 일부 기타 운영 체제는 세션 재설정을 위한 정확한 TCP 시퀀스 번호를 보유하려면 TCP 재설정 세그먼트가 필요합니다. 반면 Linux 및 기타 운영 체제는 일정한 범위의 시퀀스 번호를 허용합니다. 이 예에서 시스템 프리프로세서는 목적지 호스트가 시퀀스 번호를 기반으로 재설정에 반응하는 방법을 정확히 이해해야 합니다. 스트림 프리프로세서는 목적지 호스트에서 재설정이 유효하다고 간주하는 경우에만 세션 추적을 중지합니다. 따라서 프리프로세서가 스트림 검사를 중지한 후 패킷을 전송하여 탐지를 회피하는 공격을 수행할 수 없습니다. TCP 구현의 다른 방법에는 운영 체제가 TCP 타임스탬프 옵션을 사용할지 여부와 사용할 경우 타임스탬프를 처리하는 방법, 운영 체제가 SYN 패킷의 데이터를 수용할지 거부할지 여부 등이 포함됩니다.

각 운영 체제는 각기 다른 방법으로 중복 TCP 세그먼트를 리어셈블합니다. 중복 TCP 세그먼트는 미승인 TCP 트래픽의 정상적인 재전송을 반영할 수 있습니다. 또한 호스트 중 하나의 운영 체제를 알고 있으며 악의적인 내용을 중복 세그먼트에 숨겨 전송하여 탐지를 회피하고 호스트를 악용하려 하는 공격자의 시도를 나타낼 수도 있습니다. 그러나 모니터링되는 네트워크 세그먼트에서 실행 중인 운영 체제를 인식하도록 스트림 프리프로세서를 구성할 수 있으며, 이 경우 대상 호스트가 하는 것과 동일한 방식으로 세그먼트가 리어셈블되므로 공격을 식별할 수 있습니다.

모니터링되는 네트워크 세그먼트의 다른 운영 체제에 대해 TCP 스트림 검사와 리어셈블리를 맞춤화하기 위해 하나 이상의 TCP 정책을 생성할 수 있습니다. 각 정책에 대해 13개의 운영 체제 정책 중 하나를 식별합니다. 다른 운영 체제를 사용하는 하나 또는 모든 호스트를 식별하기 위해 필요한 만큼의 TCP 정책을 사용하여 각 TCP 정책을 특정 IP 주소 및 주소 블록에 바인딩합니다. 기본 TCP 정책은 다른 TCP 정책에서 식별하지 않는 모니터링되는 네트워크의 모든 호스트에 적용됩니다. 따라서 기본 TCP 정책에 대해서는 IP 주소, CIDR 블록 또는 접두사 길이를 지정할 필요가 없습니다.

또한패킷의 대상 호스트에 대한 호스트 운영 체제 정보를 사용하여 TCP 스트림 프리프로세서에 대한 대상 기반 정책을 동적으로 선택하려면 적응형 프로필을 사용할 수 있습니다. 자세한 내용은 30-1페이지의 수동 구축 시 전처리 튜닝을/를 참조하십시오.

다음 표에는 운영 체제 정책 및 각각을 사용하는 호스트 운영 체제가 나열되어 있습니다.

표 29-2 TCP 운영 체제 정책

정책	운영 체제
First	알 수 없는 OS
Last	Cisco IOS
BSD	AIX
	FreeBSD
	OpenBSD
Linux	Linux 2.4 커널
	Linux 2.6 커널
Old Linux	Linux 2.2 및 이전 커널
Windows	Windows 98
	Windows NT
	Windows 2000
	Windows XP
Windows 2003	Windows 2003
Windows Vista	Windows Vista
Solaris	Solaris OS
	SunOS
IRIX	SGI Irix
HPUX	HP-UX 11.0 이상
HPUX 10	HP-UX 10.2 이하
Mac OS	Mac OS 10(Mac OS X)

팁 First 운영 체제 정책은 호스트 운영 체제를 모르는 경우 어느 정도의 보호 기능을 제공할 수 있습니다. 그러나 공격을 놓칠 수도 있습니다. 올바른 운영 체제를 알고 있는 경우 정확히 지정하여 정책을 수정해야 합니다.

TCP 정책 옵션 선택

라이센스: 보호

다음 목록에서는 스트림 프리프로세서가 검사하는 TCP 트래픽을 식별 및 제어하기 위해 설정할 수 있는 옵션에 대해 설명합니다.

다음 설명에서 프리프로세서 규칙이 언급되지 않은 경우 해당 옵션은 프리프로세서 규칙과 관련되지 않은 것입니다.

Network

TCP 스트림 리어셈블리 정책을 적용할 호스트 IP 주소를 지정합니다.

단일 IP 주소 또는 주소 블록을 지정할 수 있습니다. 기본 정책을 포함하여 최대 255개의 총 프로필을 지정할 수 있습니다. FireSIGHT 시스템에서 IPv4 및 IPv6 주소 블록을 사용하는 방법에 대한 자세한 내용은 1-19페이지의 IP 주소 표기 규칙을/를 참조하십시오.

기본 정책의 `default` 설정은 다른 대상 기반 정책에서 처리되지 않는 모니터링되는 네트워크 세그먼트의 모든 IP 주소를 지정합니다. 따라서 기본 정책에 대해서는 IP 주소 또는 CIDR 블록/접두사 길이를 지정할 수 없고 지정할 필요도 없으며, 다른 정책에서 이 설정을 비워둘 수 없거나 `any`를 나타내는 주소 표기법(예: 0.0.0.0/0 또는 ::/0)을 사용할 수 없습니다.

또한 트래픽 처리를 위한 대상 기반 정책의 경우, 식별하는 네트워크는 대상 기반 정책을 구성하는 네트워크 분석 정책에서 처리되는 네트워크, 영역, VLAN의 하위 집합과 일치하거나 하위 집합이어야 합니다. 자세한 내용은 25-3페이지의 네트워크 분석 정책으로 전처리 맞춤화을/를 참조하십시오.

Policy

대상 호스트의 TCP 정책 운영 체제를 식별합니다. **Mac OS** 외의 정책을 선택하는 경우, 시스템은 동기화(SYN) 패킷에서 데이터를 제거하고 규칙 129:2에 대한 이벤트 생성을 비활성화합니다.

자세한 내용은 29-22페이지의 대상 기반 TCP 정책 이해을/를 참조하십시오.

Timeout

침입 규칙 엔진이 상태 테이블에 비활성 스트림을 유지하는 1~86400 사이의 초 단위 시간. 스트림이 지정된 시간에 리어셈블되지 않으면 침입 규칙 엔진은 상태 테이블에서 스트림을 삭제합니다.

참고 네트워크 트래픽이 디바이스의 대역폭 제한에 도달할 것 같은 세그먼트에 관리되는 디바이스가 구축된 경우, 처리 오버헤드의 양을 줄이려면 이 값을 더 높게 설정하는 것을 고려해야 합니다(예: 600초).

Maximum TCP Window

수신 호스트에 지정된 대로, 허용되는 1~1073725440바이트 범위의 최대 TCP 창 크기를 지정합니다. 값을 0으로 설정하면 TCP 창 크기에 대한 확인이 비활성화됩니다.

주의 상한은 RFC에서 허용하는 최대 창 크기이며 공격자의 탐지 회피를 방지하는 것이 목적이지만, 최대 창 크기를 너무 크게 설정하면 자체적으로 서비스 거부가 발생할 수 있습니다.

이 옵션에 대한 이벤트를 생성하려면 규칙 129:6을 활성화할 수 있습니다. 자세한 내용은 32-20페이지의 규칙 상태 설정을/를 참조하십시오.

Overlap Limit

세션의 중복 세그먼트에서 0(무제한)과 255 사이로 구성된 숫자가 탐지된 경우 해당 세션에 대해 세그먼트 리어셈블리가 중지되며, **Stateful Inspection Anomalies**가 활성화되고 동반 프리프로세서 규칙도 활성화된 경우 이벤트가 생성됩니다.

이 옵션에 대한 이벤트를 생성하려면 규칙 129:7을 활성화할 수 있습니다. 자세한 내용은 32-20페이지의 규칙 상태 설정을/를 참조하십시오.

Flush Factor

인라인 구축에서, 비감소 크기의 세그먼트 1~2048 사이로 구성된 수에 이어 감소 크기의 세그먼트가 탐지된 경우 시스템은 탐지를 위해 누적된 세그먼트 데이터를 플러시합니다. 값을 0으로 설정하면 이 세그먼트 패턴의 탐지가 비활성화되며, 이는 요청 또는 응답의 종료를 나타낼 수 있습니다. 이 옵션을 사용할 수 있으려면 Inline Normalization **Normalize TCP Payload** 옵션을 활성화해야 합니다. 자세한 내용은 29-7페이지의 인라인 트래픽 표준화을/를 참조하십시오.

Stateful Inspection Anomalies

TCP 스택에서 비정상적인 동작을 탐지합니다. 동반 프리프로세서 규칙이 활성화된 경우 TCP/IP 스택이 제대로 작성되지 않으면 많은 이벤트가 생성될 수 있습니다.

이 옵션에 대한 이벤트를 생성하려면 다음 규칙을 활성화할 수 있습니다.

- 129:1~129:5
- 129:6(Mac OS 전용)
- 129:8~129:11
- 129:13~129:19

자세한 내용은 32-20페이지의 규칙 상태 설정을/를 참조하십시오.

TCP Session Hijacking

세션에서 수신된 후속 패킷에 대한 3-way 핸드셰이크 중에 TCP 연결의 양쪽에서 탐지된 하드웨어(MAC) 주소를 검증함으로써 TCP 세션 하이재킹을 탐지합니다. 한쪽 또는 다른 쪽의 MAC 주소가 일치하지 않으면, **Stateful Inspection Anomalies**가 활성화되고 두 개의 해당 프리프로세서 규칙 중 하나가 활성화된 경우 시스템이 이벤트를 생성합니다.

이 옵션에 대한 이벤트를 생성하려면 규칙 129:9 및 129:10을 활성화할 수 있습니다. 자세한 내용은 32-20페이지의 규칙 상태 설정을/를 참조하십시오.

Consecutive Small Segments

Stateful Inspection Anomalies가 활성화된 경우, 허용되는 연속 소형 TCP 세그먼트의 최대 수를 1~2048 범위로 지정합니다. 값을 0으로 설정하면 연속 소형 세그먼트에 대한 확인이 비활성화됩니다.

이 옵션은 **Small Segment Size** 옵션과 함께 설정해야 합니다. 둘 다 비활성화하거나 둘 다 0이 아닌 값으로 설정합니다. 연속 세그먼트 2000개를 수신하면, 개입하는 ACK 없이 각 세그먼트 길이가 1바이트일지라도, 일반적으로 예상하는 것보다 훨씬 많은 연속 세그먼트가 됩니다.

이 옵션에 대한 이벤트를 생성하려면 규칙 129:12를 활성화할 수 있습니다. 자세한 내용은 32-20페이지의 규칙 상태 설정을/를 참조하십시오.

Small Segment Size

Stateful Inspection Anomalies가 활성화된 경우, 소형으로 간주되는 1~2048바이트의 TCP 세그먼트 크기를 지정합니다. 값을 0으로 설정하면 소형 세그먼트의 크기 지정이 비활성화됩니다.

이 옵션은 **Consecutive Small Segments** 옵션과 함께 설정해야 합니다. 둘 다 비활성화하거나 둘 다 0이 아닌 값으로 설정합니다. 2048바이트 TCP 세그먼트가 정상적인 1500바이트 이더넷 프레임보다 큽니다.

Ports Ignoring Small Segments

Stateful Inspection Anomalies, **Consecutive Small Segments** 및 **Small Segment Size**가 활성화된 경우 선택적으로, 소형 TCP 세그먼트 탐지를 무시하는 하나 이상의 포트에 대한 쉼표로 구분된 목록을 지정합니다. 이 옵션을 비워 두면 무시되는 포트가 없습니다.

목록에 어떤 포트든 추가할 수 있지만, 목록은 TCP 정책의 **Perform Stream Reassembly on** 포트 목록 중 하나에 지정된 포트에만 영향을 줍니다.

Require TCP 3-Way Handshake

TCP 3-way 핸드셰이크가 완료된 경우에만 세션을 설정된 것으로 취급하도록 지정합니다. 성능을 높이고, SYN 플러드 공격에서 보호하고, 부분적 비동기 환경에서 운영을 허용하려면 이 옵션을 비활성화하십시오. 설정된 TCP 세션의 일부가 아닌 정보를 전송하여 오탐을 생성하려고 시도하는 공격을 피하려면 이 옵션을 활성화하십시오.

이 옵션에 대한 이벤트를 생성하려면 규칙 129:20을 활성화할 수 있습니다. 자세한 내용은 32-20페이지의 규칙 상태 설정을/를 참조하십시오.

3-Way Handshake Timeout

Require TCP 3-Way Handshake가 활성화되었을 때 핸드셰이크를 완료해야 할, 0(무제한)과 86400(24시간) 사이의 시간을 초 단위로 지정합니다. 이 옵션의 값을 수정하려면 **Require TCP 3-Way Handshake**를 활성화해야 합니다.

Packet Size Performance Boost

리어셈블리 버퍼의 큰 패킷을 대기열에 추가하지 않도록 프리프로세서를 설정합니다. 이렇게 성능을 개선할 경우 공격을 놓칠 수 있습니다. 1~20바이트의 소형 패킷을 사용하는 회피 시도를 방지하려면 이 옵션을 비활성화하십시오. 모든 트래픽이 매우 큰 패킷으로 구성되어 있어서 그러한 공격이 없을 것이라고 확신하는 경우 이 옵션을 활성화하십시오.

Legacy Reassembly

패킷을 리어셈블할 때 사용되지 않는 Stream 4 프리프로세서를 에뮬레이트하도록 스트림 프리프로세서를 설정합니다. 그러면 스트림 프리프로세서에 의해 리어셈블된 이벤트를 Stream 4 프리프로세서에 의해 리어셈블된 동일한 데이터 스트림 기반의 이벤트와 비교할 수 있습니다.

Asynchronous Network

모니터링되는 네트워크가 비동기 네트워크인지, 즉 시스템이 트래픽 절반만 관찰하는 네트워크인지를 지정합니다. 이 옵션이 활성화되면 시스템은 성능을 높이기 위해 TCP 스트림을 리어셈블하지 않습니다.

Perform Stream Reassembly on Client Ports, Server Ports, Both Ports

클라이언트 포트, 서버 포트 또는 둘 모두에 대해, 리어셈블할 스트림 프리프로세서에 대한 트래픽을 식별하기 위한 쉼표로 구분된 포트 목록을 지정합니다. 29-27페이지의 스트림 리어셈블리 옵션 선택을/를 참조하십시오.

Perform Stream Reassembly on Client Services, Server Services, Both Services

클라이언트 서비스, 서버 서비스 또는 둘 모두에 대해, 리어셈블할 스트림 프리프로세서에 대한 트래픽에서 식별하기 위한 서비스를 지정합니다. 29-27페이지의 스트림 리어셈블리 옵션 선택을/를 참조하십시오.

Troubleshooting Options: Maximum Queued Bytes

고객 지원과의 문제 해결 통화 중에, TCP 연결의 한쪽에서 대기열에 추가할 수 있는 데이터의 양을 지정하도록 요구할 수 있습니다. 값 0은 무제한의 바이트를 지정합니다.

주의 이러한 문제 해결 옵션에 대한 설정 변경은 성능에 영향을 미치므로 지원 안내에 따라서만 수행해야 합니다.

Troubleshooting Options: Maximum Queued Segments

고객 지원과의 문제 해결 통화 중에, TCP 연결의 한쪽에서 대기열에 추가할 수 있는 데이터 세그먼트의 최대 바이트 수를 지정하도록 요구할 수 있습니다. 값 0은 무제한의 데이터 세그먼트 바이트를 지정합니다.

주의 이러한 문제 해결 옵션에 대한 설정 변경은 성능에 영향을 미치므로 지원 안내에 따라서만 수행해야 합니다.

TCP 스트림 리어셈블

라이센스: 보호

스트림 프리프로세서는 TCP 세션의 서버-클라이언트 통신 스트림, 클라이언트-서버 통신 스트림 또는 둘 모두의 일부인 모든 패킷을 수집 및 리어셈블합니다. 이렇게 하면 규칙 엔진이 지정된 스트림의 일부인 개별 패킷만 검사하는 것이 아니라, 스트림을 리어셈블된 단일 엔티티로서 검사할 수 있습니다.

자세한 내용은 다음 절을 참조하십시오.

- 29-27페이지의 스트림 기반 공격 이해
- 29-27페이지의 스트림 리어셈블리 옵션 선택

스트림 기반 공격 이해

라이센스: 보호

스트림 리어셈블리는 규칙 엔진이 개별 패킷을 검사할 때에는 탐지하지 못할 수 있는 스트림 기반 공격을 식별하도록 허용합니다. 네트워크 요구를 기반으로 어떤 통신 스트림을 규칙 엔진이 리어셈블할지를 지정할 수 있습니다. 예를 들어 웹 서버에서 트래픽을 모니터링하는 경우 자체 웹 서버에서는 악성 트래픽을 수신할 가능성이 매우 낮으므로 클라이언트 트래픽만 검사하고자 할 수 있습니다.

스트림 리어셈블리 옵션 선택

라이센스: 보호

각 TCP 정책에서, 리어셈블할 스트림 프리프로세서용 트래픽을 식별하려면 쉼표로 구분된 포트 목록을 지정할 수 있습니다. 적응형 프로필이 활성화된 경우, 포트에 대한 대안으로서 또는 포트와의 조합으로 리어셈블할 트래픽을 식별하는 서비스를 나열할 수 있습니다. 적응형 프로필의 활성화 및 사용에 대한 자세한 내용은 30-1페이지의 수동 구축 시 전처리 튜닝을/를 참조하십시오.

포트, 서비스 또는 둘 모두를 지정할 수 있습니다. 클라이언트 포트, 서버 포트 및 둘 모두의 임의의 조합에 대해 별도의 포트 목록을 지정할 수 있습니다. 또한 클라이언트 서비스, 서버 서비스 및 둘 모두의 임의의 조합에 대해 별도의 서비스 목록을 지정할 수 있습니다. 예를 들어 다음을 리어셈블하려 한다고 가정해보겠습니다.

- 클라이언트로부터의 SMTP(포트 25) 트래픽
- FTP 서버 응답(포트 21)
- 양방향의 텔넷(포트 23) 트래픽

다음을 구성할 수 있습니다.

- 클라이언트 포트의 경우 `23, 25` 지정
- 서버 포트의 경우 `21, 23` 지정

또는 대신 다음을 구성할 수 있습니다.

- 클라이언트 포트의 경우 `25` 지정
- 서버 포트의 경우 `21` 지정
- 두 포트의 경우 `23` 지정

추가로, 포트와 서비스를 결합하며 적응형 프로필이 활성화될 때 유효할 수 있는 다음 예를 고려해 보십시오.

- 클라이언트 포트의 경우 `23` 지정
- 클라이언트 서비스의 경우 `smtp` 지정
- 서버 포트의 경우 `21` 지정
- 서버 서비스의 경우 `telnet` 지정

포트를 부정하면(예: `!80`) TCP 스트림 프리프로세서가 해당 포트에 대해 트래픽을 처리하지 않도록 하여 성능을 향상할 수 있습니다.

모든 포트에 대해 리어셈블리를 제공하려면 `all`을 인수로 지정할 수도 있지만, 그렇게 하면 이 프리프로세서에서 검사하는 트래픽의 양이 증가하여 불필요하게 성능이 저하될 수 있으므로 Cisco에서는 포트를 `all`로 설정하는 것을 권장하지 **않습니다**.

TCP 리어셈블리는 다른 프리프로세서에 추가하는 포트를 자동으로 투명하게 포함합니다. 그러나 다른 프리프로세서 컨피그레이션에 추가한 TCP 리어셈블리 목록에 포트를 명시적으로 추가하면 이러한 추가 포트는 정상적으로 처리됩니다. 여기에는 다음 프리프로세서에 대한 포트 목록이 포함됩니다.

- FTP/Telnet(서버 레벨 FTP)
- DCE/RPC
- HTTP Inspect
- SMTP
- 세션 시작 프로토콜
- POP
- IMAP
- SSL

추가 트래픽 유형(클라이언트, 서버, 둘 다)을 리어셈블하면 리소스 수요가 증가합니다.

다음 설명에서 프리프로세서 규칙이 언급되지 않은 경우 해당 옵션은 프리프로세서 규칙과 관련되지 않은 것입니다.

Perform Stream Reassembly on Client Ports

연결의 클라이언트 측에 대해 포트를 기반으로 스트림 리어셈블리를 활성화합니다. 다시 말하면, 웹 서버, 메일 서버 또는 일반적으로 $HOME_NET에 지정된 IP 주소로 정의되는 기타 IP 주소로 이동하는 스트림이 리어셈블됩니다. 클라이언트에서 악성 트래픽이 발생할 것으로 예상하는 경우 이 옵션을 사용하십시오.

Perform Stream Reassembly on Client Services

연결의 클라이언트 측에 대해 서비스를 기반으로 스트림 리어셈블리를 활성화합니다. 클라이언트에서 악성 트래픽이 발생할 것으로 예상하는 경우 이 옵션을 사용하십시오.

선택한 각 클라이언트 서비스에 대해 하나 이상의 클라이언트 탐지기가 활성화되어야 합니다(46-27페이지의 탐지기 활성화 및 비활성화 참조). 기본적으로 모든 Cisco 제공 탐지기는 활성화되어 있습니다. 어떤 관련 클라이언트 애플리케이션에 대해 활성화된 탐지기가 없을 경우 자동으로 모든 Cisco 제공 탐지기가 해당 애플리케이션에 대해 활성화됩니다. 탐지기가 하나도 없을 경우 가장 최근에 수정된 사용자 정의 탐지기가 이 애플리케이션에 대해 활성화됩니다.

이 기능을 사용하려면 보호 및 제어 라이센스가 필요합니다.

Perform Stream Reassembly on Server Ports

연결의 서버 측에 대해 포트를 기반으로 스트림 리어셈블리를 활성화합니다. 다시 말하면, 웹 서버, 메일 서버 또는 일반적으로 $EXTERNAL_NET에 지정된 IP 주소로 정의되는 기타 IP 주소에서 오는 스트림이 리어셈블됩니다. 서버 측 공격을 관찰하려는 경우 이 옵션을 사용하십시오. 포트를 지정하지 않음으로써 이 옵션을 비활성화할 수 있습니다.

Perform Stream Reassembly on Server Services

연결의 서버 측에 대해 서비스를 기반으로 스트림 리어셈블리를 활성화합니다. 서버 측 공격을 관찰하려는 경우 이 옵션을 사용하십시오. 서비스를 지정하지 않음으로써 이 옵션을 비활성화할 수 있습니다.

선택한 각 서비스에 대해 하나 이상의 탐지기가 활성화되어야 합니다(46-27페이지의 탐지기 활성화 및 비활성화 참조). 기본적으로 모든 Cisco 제공 탐지기는 활성화되어 있습니다. 어떤 서비스에 대해 활성화된 탐지기가 없을 경우 연결된 애플리케이션 프로토콜에 대해 자동으로 모든 Cisco 제공 탐지기가 활성화됩니다. 탐지기가 하나도 없을 경우 가장 최근에 수정된 사용자 정의 탐지기가 이 애플리케이션 프로토콜에 대해 활성화됩니다.

이 기능을 사용하려면 보호 및 제어 라이센스가 필요합니다.

Perform Stream Reassembly on Both Ports

연결의 클라이언트 및 서버 측 모두에 대해 포트를 기반으로 스트림 리어셈블리를 활성화합니다. 클라이언트와 서버 사이의 어느 한 방향으로 동일한 포트에 대한 악성 트래픽이 이동할 것으로 예상하는 경우 이 옵션을 사용하십시오. 포트를 지정하지 않음으로써 이 옵션을 비활성화할 수 있습니다.

Perform Stream Reassembly on Both Services

연결의 클라이언트 및 서버 측 모두에 대해 서비스를 기반으로 스트림 리어셈블리를 활성화합니다. 클라이언트와 서버 사이의 어느 한 방향으로 동일한 서비스에 대한 악성 트래픽이 이동할 것으로 예상하는 경우 이 옵션을 사용하십시오. 서비스를 지정하지 않음으로써 이 옵션을 비활성화할 수 있습니다.

선택한 각 서비스에 대해 하나 이상의 탐지기가 활성화되어야 합니다(46-27페이지의 탐지기 활성화 및 비활성화 참조). 기본적으로 모든 Cisco 제공 탐지기는 활성화되어 있습니다. 어떤 관련 클라이언트 애플리케이션 또는 애플리케이션 프로토콜에 대해 활성화된 탐지기가 없을 경우 해당 애플리케이션 또는 애플리케이션 프로토콜에 대해 자동으로 모든 Cisco 제공 탐지기가 활성화됩니다. 탐지기가 하나도 없을 경우 가장 최근에 수정된 사용자 정의 탐지기가 이 애플리케이션 또는 애플리케이션 프로토콜에 대해 활성화됩니다.

이 기능을 사용하려면 보호 및 제어 라이센스가 필요합니다.

TCP 스트림 전처리 구성

라이센스: 보호

TCP 정책을 포함하여 TCP 스트림 전처리를 구성할 수 있습니다. TCP 스트림 프리프로세서 컨피그레이션 옵션에 대한 자세한 내용은 29-23페이지의 TCP 정책 옵션 선택을/를 참조하십시오.

TCP 세션을 추적하도록 스트림 프리프로세서를 구성하려면

액세스: Admin/Intrusion Admin

1단계 **Policies > Access Control**을 선택하여 Access Control Policy 페이지를 표시한 다음 **Network Analysis Policy**를 클릭합니다.

Network Analysis Policy 페이지가 나타납니다.

2단계 수정할 정책 옆에 있는 수정 아이콘( )을 클릭합니다.

다른 정책에 저장하지 않은 변경 사항이 있는 경우 변경 사항을 취소하고 계속 진행하려면 **OK**를 클릭합니다. 저장하지 않은 변경 사항을 다른 정책에 저장하는 방법에 대한 자세한 내용은 23-15페이지의 충돌 해결 및 정책 변경 사항 커밋을/를 참조하십시오.

Edit Policy 페이지가 나타납니다.

3단계 왼쪽의 탐색 패널에서 **Settings**를 클릭합니다.

Settings 페이지가 나타납니다.

4단계 Transport/Network Layer Preprocessors 아래에서 **TCP Stream Configuration**이 활성화되었는지 여부에 따라 두 가지 선택 사항이 있습니다.

- 컨피그레이션이 활성화되어 있으면 **Edit**를 클릭합니다.
- 컨피그레이션이 비활성화되어 있으면 **Enabled**를 클릭한 다음 **Edit**를 클릭합니다.

TCP Stream Configuration 페이지가 나타납니다. 페이지 하단에 있는 메시지는 컨피그레이션이 포함된 정책 레이어를 식별합니다. 자세한 내용은 24-1페이지의 네트워크 분석 또는 침입 정책에서 레이어 사용을/를 참조하십시오.

5단계 선택적으로, Global Settings 아래에서 **Packet Type Performance Boost**를 수정합니다. 자세한 내용은 29-22페이지의 TCP 전역 옵션 선택을/를 참조하십시오.

6단계 다음 2가지 옵션을 사용할 수 있습니다.

- 새로운 대상 기반 정책을 추가합니다. 페이지 왼쪽의 **Hosts** 옆에 있는 추가 아이콘( )을 클릭합니다. Add Target 팝업 창이 나타납니다. **Host Address** 필드에서 하나 이상의 IP 주소를 지정하고 **OK**를 클릭합니다.

  단일 IP 주소 또는 주소 블록을 지정할 수 있습니다. 기본 정책을 포함하여 총 255개의 대상 기반 정책을 생성할 수 있습니다. FireSIGHT 시스템에서 IP 주소 블록을 사용하는 방법에 대한 자세한 내용은 1-19페이지의 IP 주소 표기 규칙을/를 참조하십시오.

  트래픽 처리를 위한 대상 기반 정책의 경우, 식별하는 네트워크는 대상 기반 정책을 구성하는 네트워크 분석 정책에서 처리되는 네트워크, 영역, VLAN의 하위 집합과 일치하거나 하위 집합이어야 합니다. 자세한 내용은 25-3페이지의 네트워크 분석 정책으로 전처리 맞춤화을/를 참조하십시오.

  새 항목이 페이지 왼쪽의 대상 목록에 나타나서 선택된 것을 알 수 있도록 강조 표시되며, 추가한 정책에 대한 현재 컨피그레이션을 반영하여 Configuration 섹션이 업데이트됩니다.

- 기존의 대상 기반 정책에 대한 설정을 수정합니다. 페이지 왼쪽의 **Hosts** 아래에서 추가한 정책에 대해 구성된 주소를 클릭하거나 **default**를 클릭합니다.

  선택 항목이 강조 표시되고, 선택한 정책에 대한 현재 컨피그레이션을 표시하기 위해 Configuration 섹션이 업데이트됩니다. 기존의 대상 기반 정책을 삭제하려면 제거할 정책 옆에 있는 삭제 아이콘( )을 클릭합니다.

7단계 선택적으로, Configuration 아래에서 TCP 정책 옵션을 수정합니다.

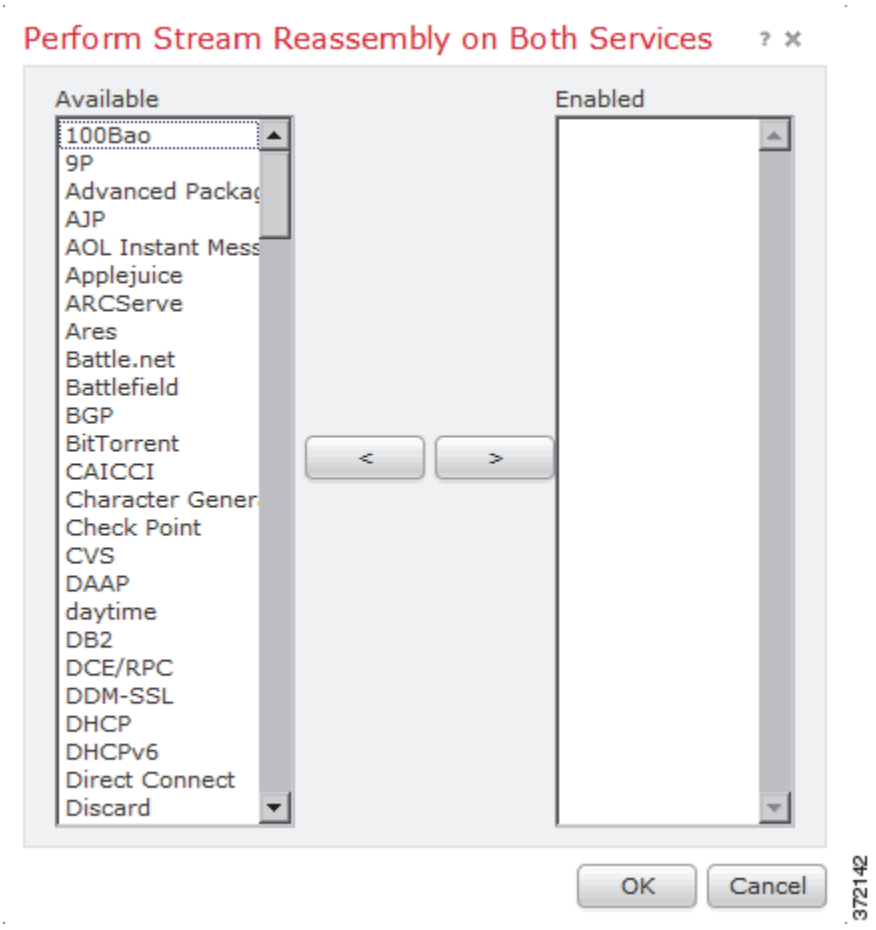
클라이언트 서비스, 서버 서비스 또는 둘 모두를 기반으로 스트림 리어셈블리에 대한 설정을 수정하는 특별한 지침을 보려면 8단계로 이동하십시오. 아니면 11단계로 이동하십시오.

자세한 내용은 29-23페이지의 TCP 정책 옵션 선택 및 29-27페이지의 스트림 리어셈블리 옵션 선택을/를 참조하십시오.

8단계 클라이언트, 서버 또는 두 서비스를 기반으로 스트림 리어셈블리에 대한 설정을 수정하려면 수정할 필드 내부를 클릭하고 필드 옆에 있는 **Edit**를 클릭합니다.

선택한 필드에 대한 팝업 창이 나타납니다.

예를 들어 다음 그림에서는 Perform Stream Reassembly on Both Services 팝업 창을 보여줍니다.



네트워크에서 검색된 서비스를 기반으로 리어셈블할 스트림 프리프로세서에 대한 트래픽을 모니터링하려면 적응형 프로필을 활성화할 수 있습니다. 자세한 내용은 50-36페이지의 서버 작업 및 30-1페이지의 수동 구축 시 전처리 튜닝을/를 참조하십시오.

9단계 2가지 옵션이 있습니다.

- 모니터링할 서비스를 추가하려면 왼쪽의 **Available** 목록에서 하나 이상의 서비스를 선택한 다음 오른쪽 화살표(**>**) 버튼을 클릭합니다.
- 서비스를 제거하려면 오른쪽의 **Enabled** 목록에서 서비스를 선택한 다음 왼쪽 화살표(**<**) 버튼을 클릭합니다.

여러 서비스 탐지기를 선택하려면 Ctrl 또는 Shift 키를 누른 채 클릭합니다. 또는 클릭하고 드래그하여 인접한 여러 서비스 탐지기를 선택할 수 있습니다.

10단계 선택을 추가하려면 **OK**를 클릭합니다.

TCP Stream Configuration 페이지가 표시되고 서비스가 업데이트됩니다.

11단계 선택적으로, **Troubleshooting Options**를 확장하고 고객 지원에서 지시하는 경우에만 TCP 스트림 전처리 정책 설정 중 하나를 수정합니다. 자세한 내용은 29-23페이지의 TCP 정책 옵션 선택을/를 참조하십시오.

12단계 정책을 저장하거나, 계속 수정하거나, 변경 사항을 취소하거나, 기반 정책의 기본 컨피그레이션 설정으로 돌아가거나, 시스템 캐시에 변경 사항이 남아 있는 상태로 종료합니다. 자세한 내용은 23-15 페이지의 충돌 해결 및 정책 변경 사항 커밋을/를 참조하십시오.

UDP 스트림 전처리 사용

라이센스: 보호

UDP 스트림 전처리는 규칙 엔진이 다음 인수 중 하나를 사용하여 `flow` 키워드(36-52페이지의 TCP나 UDP 클라이언트 또는 서버 플로우에 규칙 적용 참조)를 포함하는 UDP 규칙에 대해 패킷을 처리할 때 발생합니다.

- `Established`
- `To Client`
- `From Client`
- `To Server`
- `From Server`

UDP는 두 엔드포인트가 통신 채널을 설정하고 데이터를 교환하고 채널을 닫기 위해 필요한 수단을 제공하지 않는 연결 없는 프로토콜입니다. UDP 데이터 스트림은 일반적으로 *세션*의 관점에서 고려되지 않습니다. 그러나 스트림 프리프로세서는 캡슐화하는 IP 데이터그램 헤더의 소스 및 목적지 IP 주소 필드를 사용하고 UDP 헤더의 포트 필드를 사용하여 플로우의 방향을 결정하고 세션을 식별합니다. 구성 가능한 타이머가 초과될 때, 또는 두 엔드포인트 중 하나가 다른 엔드포인트에 도달할 수 없다거나 요청한 서비스를 사용할 수 없다는 ICMP 메시지를 수신할 때 세션이 종료됩니다.

시스템은 UDP 스트림 전처리와 관련된 이벤트를 생성하지 않습니다. 그러나 UDP 프로토콜 헤더 변칙을 탐지하려면 관련 패킷 디코더 규칙을 활성화할 수 있습니다. 패킷 디코더에 의해 생성되는 이벤트에 대한 자세한 내용은 29-17페이지의 패킷 디코딩 이해을/를 참조하십시오.

UDP 스트림 전처리 구성

라이센스: 보호

UDP 스트림 전처리를 구성할 수 있습니다.

UDP 세션을 추적하도록 스트림 프리프로세서를 구성하려면

액세스: Admin/Intrusion Admin

1단계 **Policies > Access Control**을 선택하여 Access Control Policy 페이지를 표시한 다음 **Network Analysis Policy**를 클릭합니다.

Network Analysis Policy 페이지가 나타납니다.

2단계 수정할 정책 옆에 있는 수정 아이콘()을 클릭합니다.

다른 정책에 저장하지 않은 변경 사항이 있는 경우 변경 사항을 취소하고 계속 진행하려면 **OK**를 클릭합니다. 저장하지 않은 변경 사항을 다른 정책에 저장하는 방법에 대한 자세한 내용은 23-15페이지의 충돌 해결 및 정책 변경 사항 커밋을/를 참조하십시오.

Edit Policy 페이지가 나타납니다.

3단계 왼쪽의 탐색 패널에서 **Settings**를 클릭합니다.

Settings 페이지가 나타납니다.

4단계 Transport/Network Layer Preprocessors 아래에서 **UDP Stream Configuration**이 활성화되었는지 여부에 따라 두 가지 선택 사항이 있습니다.

- 컨피그레이션이 활성화되어 있으면 **Edit**를 클릭합니다.
- 컨피그레이션이 비활성화되어 있으면 **Enabled**를 클릭한 다음 **Edit**를 클릭합니다.

UDP Stream Configuration 페이지가 나타납니다. 페이지 하단에 있는 메시지는 컨피그레이션이 포함된 정책 레이어를 식별합니다. 자세한 내용은 24-1페이지의 네트워크 분석 또는 침입 정책에서 레이어 사용을/를 참조하십시오.

5단계 선택적으로, 프리프로세서가 상태 테이블에 비활성 스트림을 유지하는 1~86400 사이의 초 단위 시간을 지정하려면 **Timeout** 값을 구성합니다. 지정된 시간에 추가 데이터그램이 나타나지 않으면 프리프로세서는 상태 테이블에서 스트림을 삭제합니다.

6단계 선택적으로, 활성화된 규칙에 지정되지 않은 모든 포트 및 애플리케이션 프로토콜에 대한 UDP 트래픽을 무시하려면 **Packet Type Performance Boost**를 선택합니다. 단, 소스 및 목적지 포트가 모두 `any`로 설정된 UDP 규칙에 `flow` 또는 `flowbits` 옵션이 있는 경우는 예외입니다. 이렇게 성능을 개선할 경우 공격을 놓칠 수 있습니다.

7단계 정책을 저장하거나, 계속 수정하거나, 변경 사항을 취소하거나, 기반 정책의 기본 컨피그레이션 설정으로 돌아가거나, 시스템 캐시에 변경 사항이 남아 있는 상태로 종료합니다. 자세한 내용은 23-15페이지의 충돌 해결 및 정책 변경 사항 커밋을/를 참조하십시오.

30장 수동 구축 시 전처리 튜닝

일반적으로 시스템에서는 네트워크 분석 정책에 고정 설정을 사용하여 트래픽을 전처리하고 분석합니다. 그러나 적응형 프로필 기능이 있을 경우 시스템에서는 트래픽을 네트워크 맵의 호스트 정보와 연결한 다음 이에 따라 트래픽을 처리하여 네트워크 트래픽에 맞출 수 있습니다.

호스트에 트래픽이 수신되면 호스트에서 실행 중인 운영 체제에서는 IP 프래그먼트를 다시 재결합합니다. 이러한 재결합에 사용되는 순서는 운영 체제에 따라 다릅니다. 이와 마찬가지로, 각 운영 체제는 여러 가지 방법으로 TCP를 구현할 수 있으므로 TCP 스트림은 다양한 방식으로 재결합됩니다. 프리프로세서가 대상 호스트의 운영 체제에서 사용되는 것과 다른 형식을 사용하여 데이터를 재결합할 경우, 수신 호스트에서 재결합 작업이 수행될 때 악성일 가능성이 있는 콘텐츠를 놓칠 수 있습니다.

팁 패시브 구축 시 Cisco의 권장 사항은 적응형 프로필을 구성하는 것입니다. 인라인 구축의 경우 Cisco는 **Normalize TCP Payload** 옵션을 활성화하여 인라인 표준화 프리프로세서를 구성할 것을 권장합니다. 자세한 내용은 29-7페이지의 인라인 트래픽 표준화을/를 참조하십시오.

적응형 프로필을 사용하여 패킷 프래그먼트 및 TCP 스트림의 재결합을 개선하는 방법에 대한 자세한 내용은 다음 주제을/를 참조하십시오.

- 30-1페이지의 적응형 프로필 이해
- 30-3페이지의 적응형 프로필 구성

적응형 프로필 이해

라이센스: 보호

적응형 프로필은 IP 프래그먼트 모음 및 TCP 스트림 전처리에 가장 알맞은 운영 체제를 사용할 수 있도록 지원합니다. 적응형 프로필의 영향을 받는 네트워크 분석 정책의 측면에 대한 자세한 내용은 29-12페이지의 IP 패킷 디프래그먼트 및 29-21페이지의 TCP 스트림 전처리 사용을/를 참조하십시오.

시스템에서는 네트워크 검색에서 탐지되거나, Nmap 검사를 통해 얻거나, 처리 동작을 적응시키기 위한 호스트 입력 기능을 통해 추가된 호스트 정보를 사용할 수 있습니다.

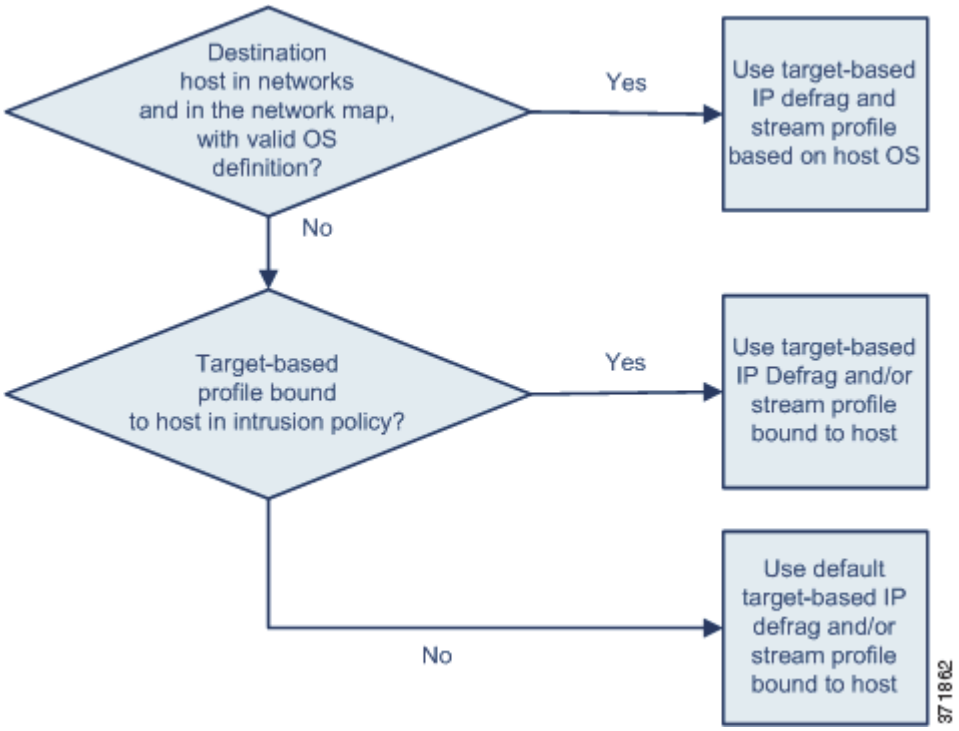
참고 명령줄 가져오기 유틸리티 또는 호스트 입력 API를 사용하여 타사 애플리케이션에서 호스트 정보를 입력할 경우, 우선 데이터를 제품 정의에 매핑하여 시스템에서 적응형 프로필을 사용할 수 있도록 해야 합니다. 자세한 내용은 46-30페이지의 서드파티 제품 매핑 관리을/를 참조하십시오.

프리프로세서로 적응형 프로필 사용

라이센스: 보호

Target-Based 프로필 같은 적응형 프로필을 네트워크 분석 정책에서 구성하면, 대상 호스트의 운영 체제에서 수행하는 것과 동일한 방식으로 IP 패킷 프래그먼트를 모으고 스트림을 재결합할 수 있습니다. 그런 다음 침입 규칙 엔진은 대상 호스트에서 사용된 것과 동일한 형식으로 된 데이터를 분석합니다.

수동으로 구성된 대상 기반 프로필은 사용자가 선택하는 기본 운영 체제 프로필 또는 특정 호스트에 바인딩하는 프로필에만 적용됩니다. 그러나 적응형 프로필의 경우에는 아래 다이어그램에 나온 것처럼, 대상 호스트에 대한 호스트 프로필의 운영 체제를 기반으로 알맞은 운영 체제 프로필로 전환합니다.



10.6.0.0/16 서브넷에 대한 적응형 프로필을 구성하고 Linux에 대한 기본 IP 프래그먼트 모음 Target-Based 정책을 설정하는 경우를 예로 들어보겠습니다. 방어 센터에서 10.6.0.0/16 서브넷이 포함된 네트워크 맵이 있는 설정을 구성합니다.

디바이스에서 10.6.0.0/16 서브넷에 없는 호스트 A의 트래픽을 탐지할 경우, 해당 디바이스는 Linux Target-Based 정책을 사용하여 IP 프래그먼트를 재결합합니다. 그러나 디바이스에서 10.6.0.0/16 서브넷에 있는 호스트 B의 트래픽을 탐지할 경우, 해당 디바이스는 호스트 B가 Microsoft Windows XP Professional을 실행 중인 것으로 나열된 네트워크 맵에서 호스트 B의 운영 체제 데이터를 수신합니다. 시스템에서는 Windows Target-Based 프로필을 사용하여 호스트 B로 향하는 트래픽의 IP 프래그먼트 모음을 수행합니다.

IP 프래그먼트 모음 프리프로세서에 대한 자세한 내용은 29-12페이지의 IP 패킷 디프래그먼트을/를 참조하십시오. 스트림 프리프로세서에 대한 자세한 내용은 29-21페이지의 TCP 스트림 전처리 사용을/를 참조하십시오.

적응형 프로필과 FireSIGHT 권장 규칙

라이센스: 보호

적응형 프로필 기능은 액세스 제어 정책에 의해 호출되는 모든 침입 정책에 전체적으로 적용되는 액세스 제어 정책의 고급 설정입니다. FireSIGHT에서는 개별 침입 정책을 구성할 경우 이러한 정책에 규칙 기능을 적용하도록 권장합니다.

FireSIGHT 권장 규칙과 마찬가지로, 적응형 프로필은 규칙의 메타데이터를 호스트 정보와 비교하여 특정 호스트에 규칙을 적용해야 할지 여부를 결정합니다. 그러나 FireSIGHT 권장 규칙에서는 해당 정보를 사용하여 규칙의 활성화 또는 비활성화를 위한 권장 사항을 제공하는 반면, 적응형 프로필은 해당 정보를 사용하여 특정 트래픽에 특정 규칙을 적용합니다.

FireSIGHT 권장 규칙을 사용하려면 규칙 상태를 권장 사항으로 변경해야 합니다. 이와 달리 적응형 프로필은 침입 정책을 수정하지 않습니다. 규칙을 적응형 방식으로 처리할 경우 패킷별로 이루어집니다.

또한 FireSIGHT 권장 규칙은 비활성화된 규칙을 활성화할 수 있습니다. 이와 반대로 적응형 프로필은 침입 정책에 이미 활성화된 규칙의 적용에만 영향을 미칩니다. 적응형 프로필은 규칙 상태를 변경하지 않습니다.

적응형 프로필 및 FireSIGHT 권장 규칙을 조합하여 사용할 수 있습니다. 적응형 프로필은 침입 정책이 적용될 때 규칙에 대한 규칙 상태를 사용하여 해당 정책을 적용 후보로 포함할지 여부를 결정하며, 권장 사항을 승인하거나 거부하도록 선택하면 이러한 결과가 규칙 상태에 반영됩니다. 두 가지 기능을 모두 사용하여 모니터링하는 각 네트워크에 가장 알맞은 규칙이 활성화 또는 비활성화되었는지 확인할 수 있으며, 그런 다음 활성화된 규칙을 특정 트래픽에 가장 효율적으로 적용할 수 있습니다.

자세한 내용은 33-1페이지의 네트워크 자산에 대한 침입 방지 맞춤화을/를 참조하십시오.

적응형 프로필 구성

라이센스: 보호

호스트 정보를 사용하여 IP 프래그먼트 모음 및 TCP 스트림 전처리에 어떤 Target-Based 프로필이 사용되었는지 확인하기 위해 적응형 프로필을 구성할 수 있습니다.

참고 적응형 프로필을 사용하려면 보호하려는 네트워크에 대한 네트워크 검색 정책에서 호스트 검색을 활성화한 다음, 네트워크 검색 정책을 다시 적용해야 합니다. 자세한 내용은 45-23페이지의 네트워크 검색 정책 생성을/를 참조하십시오.

적응형 프로필을 구성할 경우, 적응형 프로필 설정을 특정 네트워크에 바인딩해야 합니다. 적응형 프로필을 올바르게 사용하려면 해당 네트워크가 네트워크 맵에 있어야 하며, 액세스 제어 정책을 적용할 디바이스에서 모니터링하는 세그먼트에 있어야 합니다.

IP 주소, 주소 블록 또는 액세스 제어 정책에 대한 기본 침입 정책과 연결된 변수 집합에 구성된 원하는 값이 포함된 네트워크 변수를 지정함으로써 적응형 프로필을 사용하여 트래픽을 처리해야 하는 네트워크 맵에서 호스트를 표시할 수 있습니다. 자세한 내용은 25-1페이지의 액세스 제어에 대한 기본 침입 정책 설정을/를 참조하십시오.

이러한 주소 지정 방법만 단독으로 사용하거나 아래 예시에 나온 것처럼 IP 주소, 주소 블록 또는 변수 목록을 쉼표로 구분하여 함께 사용할 수 있습니다.

```
192.168.1.101, 192.168.4.0/24, $HOME_NET
```

FireSIGHT 시스템에서 주소 블록 지정에 대한 자세한 내용은 1-19페이지의 IP 주소 표기 규칙을/를 참조하십시오.

팁 임의의 값이 포함된 변수를 사용하거나 0.0.0.0/0을 네트워크 값으로 지정하여 적응형 프로필을 네트워크 맵의 모든 호스트에 적용할 수 있습니다.

또한 방어 센터에서 매니지드 디바이스로 네트워크 맵 데이터가 동기화되는 빈도를 제어할 수 있습니다. 시스템에서는 데이터를 사용하여 트래픽을 처리할 때 어떤 프로필을 사용해야 할지 결정할 수 있습니다.

적응형 프로필을 구성하려면

액세스: Admin/Access Admin/Network Admin

1단계 **Policies > Access Control**을 선택합니다.

Access Control Policy 페이지가 나타납니다.

2단계 수정할 액세스 제어 정책 옆에 있는 수정 아이콘()을 클릭합니다.

액세스 제어 정책 편집기가 나타납니다.

3단계 **Advanced** 탭을 선택합니다.

Access control policy advanced settings 페이지가 나타납니다.

4단계 **Detection Enhancement Settings** 옆에 있는 수정 아이콘()을 클릭합니다.

Detection Enhancement Settings 팝업 창이 표시됩니다.

5단계 적응형 프로필을 사용하려면 **Adaptive Profiles - Enabled**를 선택합니다.

6단계 원하는 경우 **Adaptive Profiles - Attribute Update Interval** 필드에 방어 센터에서 매니지드 디바이스로 네트워크 맵 데이터를 동기화하는 데 소요되는 시간(분)을 입력합니다.

참고 이 옵션의 값을 늘리면 대규모 네트워크의 성능을 향상할 수 있습니다.

7단계 **Adaptive Profiles - Networks** 필드에 특정 IP 주소, 주소 블록, 변수 또는 이러한 주소 지정 방법이 쉼표로 구분되어 포함된 목록을 입력하여 적응형 프로필을 사용할 네트워크 맵의 호스트를 식별합니다.

변수 구성에 대한 자세한 내용은 3-17페이지의 변수 집합 작업을/를 참조하십시오. 네트워크 맵 구성에 대한 자세한 내용은 45-23페이지의 네트워크 검색 정책 생성을/를 참조하십시오.

8단계 **OK**를 클릭하여 설정을 유지합니다.

31장

침입 정책 시작하기

*침입 정책*은 트래픽에서 보안 위반을 검사하고 인라인 구축에서 악성 트래픽을 차단 또는 변경할 수 있는 침입 탐지 및 방지 컨피그레이션의 정의된 집합입니다. 침입 정책은 액세스 제어 정책에 의해 호출되며, 목적지로 트래픽이 허용되기 전 시스템의 마지막 방어선입니다.

Cisco에서는 FireSIGHT 시스템을 통해 몇 가지 침입 정책을 제공합니다. 시스템 제공 정책을 사용하면 Cisco VRT(Vulnerability Research Team)의 경험을 활용할 수 있습니다. 이러한 정책에 대해 VRT는 침입 및 프리프로세서 규칙 상태(enabled 또는 disabled)를 설정하며, 기타 고급 설정에 대한 초기 컨피그레이션을 제공합니다. 규칙을 활성화하면 시스템은 규칙과 일치하는 트래픽에 대해 침입 이벤트를 생성(선택적으로 차단)합니다. 규칙을 비활성화하면 규칙의 처리가 중지됩니다.

팁 시스템 제공 침입 및 네트워크 분석 정책은 이름은 비슷하지만 컨피그레이션은 다릅니다. 예를 들어, Balanced Security and Connectivity 네트워크 분석 정책과 Balanced Security and Connectivity 침입 정책은 함께 작동하며 둘 다 침입 규칙 업데이트에서 업데이트할 수 있습니다. 그러나 네트워크 분석 정책은 주로 전처리 옵션을 제어하는 반면, 침입 정책은 주로 침입 규칙을 제어합니다. 23-1페이지의 네트워크 분석 및 침입 정책 이해에서는 네트워크 분석과 침입 정책이 트래픽 검토를 위해 함께 작동하는 방식의 개요는 물론 탐색 패널 사용, 충돌 해결, 변경 사항 커밋 등의 기본 사항에 대해서도 설명합니다.

사용자 지정 침입 정책을 생성하면 다음을 수행할 수 있습니다.

- 규칙을 활성화 및 비활성화하여, 그리고 자신의 고유한 규칙을 작성 및 추가하여 탐지를 조정합니다.
- FireSIGHT 권장 사항을 사용하여, 네트워크에서 탐지되는 운영 체제, 서버 및 클라이언트 애플리케이션 프로토콜을 이러한 자산 보호를 위해 특별히 작성된 규칙과 연결합니다.
- 외부 변경, 민감한 데이터 전처리 및 전역 규칙 임계값 등 다양한 고급 설정을 구성합니다.
- 여러 침입 정책을 효율적으로 관리하기 위해 레이어를 구성 요소로 사용합니다.

침입 정책을 맞춤화할 때, 특히 규칙을 활성화하고 추가할 때, 일부 침입 규칙에서는 특정 방법으로 트래픽을 먼저 디코딩하거나 전처리해야 한다는 점에 유의하십시오. 침입 정책이 패킷을 검토하기 전에, 네트워크 분석 정책의 컨피그레이션에 따라 패킷이 전처리됩니다. 필수 프리프로세서를 비활성화하는 경우 네트워크 분석 정책 웹 인터페이스에서는 프리프로세서가 비활성 상태로 남아 있더라도, 시스템은 현재 설정을 이용해 프리프로세서를 자동으로 사용합니다.

참고 전처리 및 침입 검사는 밀접하게 관련되어 있으므로, 단일 패킷을 검토하는 네트워크 분석 및 침입 정책은 **반드시** 상호 보완 관계여야 합니다. 전처리를 맞춤화하는 작업 중에서도 특히 여러 개의 사용자 지정 네트워크 분석 정책을 사용하는 것은 **고급** 작업입니다. 자세한 내용은 23-12페이지의 사용자 지정 정책의 제한 사항을/를 참조하십시오.

사용자 지정 침입 정책을 구성한 후에는, 해당 침입 정책을 하나 이상의 액세스 제어 규칙 또는 액세스 제어 정책의 기본 작업과 연결하여 액세스 제어 컨피그레이션의 일부로서 사용할 수 있습니다. 그러면 트래픽이 최종 목적지로 전달되기 전에 시스템은 침입 정책을 사용하여 특정 허용 트래픽을 검토합니다. 침입 정책과 연결하는 변수 집합을 사용하면 홈 및 외부 네트워크, 그리고 해당되는 경우 네트워크의 서버를 정확히 반영할 수 있습니다. 자세한 내용은 18-1페이지의 침입 정책 및 파일 정책을 사용하여 트래픽 제어을/를 참조하십시오.

기본적으로 시스템은 암호화된 페이로드의 침입 검사를 비활성화합니다. 이는 암호화 연결이 침입 검사가 구성된 액세스 제어 규칙과 일치하는 경우 오탐을 줄이고 성능을 높이는 데 도움이 됩니다. 자세한 내용은 19-1페이지의 트래픽 해독 이해 및 27-70페이지의 SSL 프리프로세서 사용을/를 참조하십시오.

이 장에서는 간단한 사용자 지정 침입 정책을 생성하는 방법에 대해 설명합니다. 또한 침입 정책 관리(수정, 비교 등)에 대한 기본적인 정보도 제공합니다. 자세한 내용은 다음 링크를 참고하십시오.

사용자 지정 침입 정책 생성

라이센스: 보호

새 침입 정책을 생성할 때에는 고유한 이름과 기반 정책 및 삭제 동작을 지정해야 합니다.

기반 정책은 침입 정책의 기본 설정을 정의합니다. 새 정책에서 설정을 수정하면 기반 정책의 설정이 재정의됩니다(변경되지는 않음). 시스템 제공 정책 또는 사용자 지정 정책을 기반 정책으로 사용할 수 있습니다. 자세한 내용은 24-3페이지의 기반 레이어 이해을/를 참조하십시오.

침입 정책의 삭제 동작 또는 **Drop when Inline** 설정은 시스템이 삭제 규칙을 처리하는 방법(규칙 상태가 Drop and Generate Events로 설정되는 침입 또는 프리프로세서 규칙) 및 트래픽에 영향을 미치는 기타 침입 정책 컨피그레이션을 결정합니다. 악의적인 패킷을 삭제 또는 교체하려는 경우 인라인 구축에서 삭제 동작을 활성화해야 합니다. 삭제 동작과 상관없이, 패시브 구축에서는 시스템이 트래픽 플로우에 영향을 줄 수 없습니다. 자세한 내용은 31-6페이지의 인라인 구축에서 삭제 동작 설정을/를 참조하십시오.

침입 정책을 생성하려면

액세스: Admin/Intrusion Admin

1단계 **Policies > Intrusion Policy > Intrusion Policy**를 선택합니다.

Intrusion Policy 페이지가 나타납니다.

팁 또 다른 방어 센터에서도 정책을 가져올 수 있습니다. A-1페이지의 컨피그레이션 가져오기 및 내보내기을/를 참조하십시오.

2단계 **Create Policy**를 클릭합니다.

다른 정책에 저장하지 않은 변경 사항이 있는 경우 Intrusion Policy 페이지로 돌아갈지 묻는 대화 상자가 나타나면 **Cancel**을 클릭합니다. 저장하지 않은 변경 사항을 다른 정책에 저장하는 방법에 대한 자세한 내용은 23-15페이지의 충돌 해결 및 정책 변경 사항 커밋을/를 참조하십시오.

Create Intrusion Policy 팝업 창이 나타납니다.

3단계 정책에 고유한 **Name**을 지정하고 선택 사항인 **Description**도 입력합니다.

4단계 초기 **Base Policy**를 지정합니다.

시스템 제공 정책 또는 사용자 지정 정책을 기반 정책으로 사용할 수 있습니다.

주의 Cisco 담당자의 지침이 없는 한 `Experimental Policy 1`을 사용하지 **마십시오**. Cisco에서는 테스트 목적으로 이 정책을 사용합니다.

5단계 인라인 구축에서 시스템의 삭제 동작을 설정합니다.

- 침입 정책이 트래픽에 영향을 미치고 이벤트를 생성하도록 하려면 **Drop when Inline**을 활성화합니다.
- 이벤트를 생성하는 동안 침입 정책이 트래픽에 영향을 미치지 못하도록 하려면 **Drop when Inline**을 비활성화합니다.

6단계 정책을 생성합니다.

- 새 정책을 생성하고 Intrusion Policy 페이지로 돌아가려면 **Create Policy**를 클릭합니다. 새 정책은 기반 정책과 설정이 동일합니다.
- 정책을 생성한 후 고급 침입 정책 편집기에서 수정하기 위해 열려면 **Create and Edit Policy**를 클릭합니다. 31-4페이지의 침입 정책 수정을/를 참조하십시오.

침입 정책 관리

라이센스: 보호

Intrusion Policy 페이지(**Policies > Intrusion > Intrusion Policy**)에서 다음 정보와 함께 현재의 사용자 지정 침입 정책을 볼 수 있습니다.

- 정책이 마지막으로 수정된 시간과 날짜(현지 시간) 및 수정한 사용자
- 인라인 구축에서 트래픽을 삭제 및 수정할 수 있도록 해주는 **Drop when Inline** 설정의 활성화 여부
- 트래픽 검사를 위해 침입 정책을 사용 중인 액세스 제어 정책 및 디바이스
- 정책에 저장되지 않은 변경 사항이 있는지, 현재 정책을 수정 중인 사용자(있는 경우)에 대한 정보가 있는지 여부

생성하는 사용자 지정 정책 외에도 시스템에서는 두 가지 사용자 지정 정책인 Initial Inline Policy 및 Initial Passive Policy를 제공합니다. 이러한 두 가지 침입 정책에서는 Balanced Security and Connectivity Intrusion 정책을 기본으로 사용합니다. 두 정책의 유일한 차이점은 **Drop When Inline** 설정이며, 이 설정은 인라인 정책의 동작을 삭제하고 패시브 정책에서 이를 비활성화합니다. 이러한 시스템 제공 사용자 지정 정책을 수정 및 사용할 수 있습니다.

Intrusion Policy 페이지의 옵션을 사용하면 다음 표의 작업을 수행할 수 있습니다.

표 31-1 침입 정책 관리 작업

목적	가능한 작업	참조
새 침입 정책 생성	**Create Policy**를 클릭합니다.	31-2페이지의 사용자 지정 침입 정책 생성
기존 침입 정책 수정	수정 아이콘( )을 클릭합니다.	31-4페이지의 침입 정책 수정
관리되는 디바이스에 침입 정책 다시 적용	적용 아이콘( )을 클릭합니다.	31-8페이지의 침입 정책 적용
또 다른 방어 센터에서 가져오기 위해 침입 정책 내보내기	내보내기 아이콘( )을 클릭합니다.	A-2페이지의 컨피그레이션 내보내기
침입 정책의 현재 컨피그레이션 설정을 나열하는 PDF 보고서 보기	보고서 아이콘( )을 클릭합니다.	31-9페이지의 현재 침입 설정 보고서 생성
두 침입 정책 또는 동일한 정책의 두 개정 설정 비교	**Compare Policies**를 클릭합니다.	31-10페이지의 두 가지 침입 정책 또는 개정 비교
침입 정책 삭제	삭제 아이콘( )을 클릭한 다음 정책을 삭제할 것임을 확인합니다. 액세스 제어 정책이 참조하는 침입 정책은 삭제할 수 없습니다.	

침입 정책 수정

라이센스: 보호

새 침입 정책을 생성하면 생성된 정책은 기반 정책과 침입 규칙 및 고급 설정이 동일합니다. 다음 표에서는 침입 정책 수정 시 수행하는 가장 일반적인 작업에 대해 설명합니다.

표 31-2 침입 정책 수정 작업

목적	가능한 작업	참조
인라인 구축에서 삭제 동작 지정	Policy Information 페이지에서 **Drop when Inline** 확인란을 선택하거나 선택을 취소합니다.	31-6페이지의 인라인 구축에서 삭제 동작 설정
기반 정책 변경	Policy Information 페이지의 **Base Policy** 드롭다운 목록에서 기반 정책을 선택합니다.	24-4페이지의 기반 정책 변경
기반 정책의 설정 보기	Policy Information 페이지에서 **Manage Base Policy**를 클릭합니다.	24-3페이지의 기반 레이어 이해
침입 규칙 표시 또는 구성	Policy Information 페이지에서 **Manage Rules**를 클릭합니다.	32-3페이지의 침입 정책의 규칙 보기
현재 규칙 상태를 기준으로 침입 규칙의 필터링된 보기를 표시하고 선택적으로 그러한 규칙 구성	Policy Information 페이지에서 Generate Events 또는 Drop and Generate Events로 설정된 **Manage Rules** 아래의 규칙 수 옆에 있는 **View**를 클릭합니다.	32-10페이지의 침입 정책의 규칙 필터링
FireSIGHT 권장 규칙 구성	탐색 패널에서 **FireSIGHT Recommendations**를 클릭합니다.	33-4페이지의 권장FireSIGHT 사항 사용

표 31-2 침입 정책 수정 작업(계속)

목적	가능한 작업	참조
현재 권장 규칙 상태를 기준으로 침입 규칙의 필터링된 보기를 표시하고 선택적으로 그러한 규칙 구성	Policy Information 페이지에서 권장을 생성한 후 • 이벤트 생성, 이벤트 삭제 및 생성, 또는 규칙 비활성화 권장 사항의 수 옆에 있는 **View**를 클릭합니다. • 모든 권장 사항을 보려면 **View Recommended Changes**를 클릭합니다.	33-4페이지의 권장FireSIGHT 사항 사용
고급 설정 활성화, 비활성화 또는 수정	탐색 패널에서 **Advanced Settings**를 클릭합니다.	31-7페이지의 침입 정책에서 고급 설정 구성
정책 레이어 관리	탐색 패널에서 **Policy Layers**를 클릭합니다.	24-1페이지의 네트워크 분석 또는 침입 정책에서 레이어 사용

침입 정책을 맞춤화할 때, 특히 규칙을 활성화하고 추가할 때, 일부 침입 규칙에서는 특정 방법으로 트래픽을 먼저 해독하거나 전처리해야 한다는 점에 유의하십시오. 침입 정책이 패킷을 검토하기 전에, 네트워크 분석 정책의 컨피그레이션에 따라 패킷이 전처리됩니다. 필수 프리프로세서를 비활성화하는 경우 네트워크 분석 정책 웹 인터페이스에서는 프리프로세서가 비활성 상태로 남아 있더라도, 시스템은 현재 설정을 이용해 프리프로세서를 자동으로 사용합니다.

참고 전처리 및 침입 검사는 밀접하게 관련되어 있으므로, 단일 패킷을 검토하는 네트워크 분석 및 침입 정책은 **반드시** 상호 보완 관계여야 합니다. 전처리를 맞춤화하는 작업 중에서도 특히 여러 개의 사용자 지정 네트워크 분석 정책을 사용하는 것은 **고급** 작업입니다. 자세한 내용은 23-12페이지의 사용자 지정 정책의 제한 사항을/를 참조하십시오.

시스템은 사용자당 하나의 침입 정책을 캐시합니다. 침입 정책을 수정하는 동안 메뉴를 선택하거나 다른 페이지에 대한 다른 경로를 선택하면, 페이지를 나가더라도 변경 사항이 시스템 캐시에 남아 있습니다. 위의 표에 있는 수행 가능한 작업 외에도 23-1페이지의 네트워크 분석 및 침입 정책 이해에서는 탐색 패널 사용, 충돌 해결, 변경 사항 커밋 등에 대한 정보를 제공합니다.

침입 정책을 수정하려면

액세스: Admin/Intrusion Admin

1단계 **Policies > Intrusion > Intrusion Policy**를 선택합니다.

Intrusion Policy 페이지가 나타납니다.

2단계 구성하려는 침입 정책 옆의 수정 아이콘( )을 클릭합니다.

침입 정책 편집기가 나타나며, Policy Information 페이지에 초점이 맞춰지고 탐색 패널이 왼쪽에 표시됩니다.

3단계 정책을 수정합니다. 위에 요약된 작업 중 하나를 수행합니다.

4단계 정책을 저장하거나, 계속 수정하거나, 변경 사항을 취소하거나, 시스템 캐시에 변경 사항이 남아 있는 상태로 종료합니다. 자세한 내용은 23-15페이지의 충돌 해결 및 정책 변경 사항 커밋을/를 참조하십시오.

인라인 구축에서 삭제 동작 설정

라이센스: 보호

인라인 구축에서 침입 정책은 트래픽을 차단 및 수정할 수 있습니다.

- *삭제 규칙*은 일치하는 패킷을 삭제하고 침입 이벤트를 생성할 수 있습니다. 침입 또는 프리프로세서 삭제 규칙을 구성하려면 상태를 Drop and Generate Events로 설정합니다. 32-20페이지의 규칙 상태 설정을/를 참조하십시오.
- 침입 규칙은 `replace` 키워드를 사용하여 악의적인 내용을 교체할 수 있습니다. 36-29페이지의 인라인 구축에서 내용 교체을/를 참조하십시오.

침입 규칙이 트래픽에 영향을 주려면, 삭제 규칙 및 내용을 교체하는 규칙을 올바르게 구성해야 하며, 관리되는 디바이스를 인라인으로(즉, 인라인 인터페이스 설정으로) 올바르게 구축해야 합니다. 마지막으로, 침입 정책의 *drop behavior* 또는 **Drop when Inline** 설정을 활성화해야 합니다.

참고 FTP를 통한 악성코드 파일의 전송을 차단하려면, 네트워크 기반 AMP를 올바르게 구성하는 것은 물론, 액세스 제어 정책의 기본 침입 정책에서 **Drop when Inline**을 활성화해야 합니다. 기본 침입 정책을 결정하거나 변경하려면 25-1페이지의 액세스 제어에 대한 기본 침입 정책 설정을/를 참조하십시오.

트래픽에 실제로 영향을 주지 않은 채 인라인 구축에서 컨피그레이션이 어떻게 작동하는지를 평가하려면 삭제 동작을 비활성화할 수 있습니다. 이 경우 시스템은 침입 이벤트를 생성하지만, 삭제 규칙을 트리거하는 패킷을 삭제하지 않습니다. 결과에 만족하면 삭제 동작을 활성화할 수 있습니다.

삭제 동작과 상관없이, 패시브 구축 또는 탭 모드의 인라인 구축에서는 시스템이 트래픽에 영향을 줄 수 없습니다. 다시 말하면 패시브 구축에서, Generate Events로 설정된 규칙은 Generate Events로 설정된 규칙과 동일하게 작동합니다(시스템은 침입 이벤트를 생성하지만 패킷을 삭제하지 않음).

침입 이벤트를 볼 때 트래픽이 실제로 삭제되었는지 또는 삭제되었을 것인지를 나타내는 *인라인 결과*를 워크플로에 포함할 수 있습니다. 패킷이 삭제 규칙과 일치하면 인라인 결과는 다음이 될 수 있습니다.

- `Dropped` - 삭제 동작이 활성화되어 올바르게 구성된 인라인 구축에서 삭제된 패킷의 경우
- `Would have dropped` - 디바이스가 패시브 구축되었거나 삭제 동작이 비활성화되어 삭제되지 않은 패킷의 경우 구축과 상관없이 시스템 정리 중 표시된 패킷에 대해서는 인라인 결과가 항상 `Would have dropped`입니다.

인라인 구축에서 침입 정책의 삭제 동작을 설정하려면

액세스: Admin/Intrusion Admin

1단계 **Policies > Intrusion > Intrusion Policy**를 선택합니다.

Intrusion Policy 페이지가 나타납니다.

2단계 수정할 정책 옆에 있는 수정 아이콘( )을 클릭합니다.

Policy Information 페이지가 나타납니다.

3단계 정책의 삭제 동작을 설정합니다.

- 침입 규칙이 트래픽에 영향을 미치고 이벤트를 생성하도록 하려면 **Drop when Inline**을 활성화합니다.
- 이벤트를 생성하는 동안 침입 규칙이 트래픽에 영향을 미치지 못하도록 하려면 **Drop when Inline**을 비활성화합니다.

4단계 정책을 저장하거나, 계속 수정하거나, 변경 사항을 취소하거나, 시스템 캐시에 변경 사항이 남아 있는 상태로 종료합니다. 자세한 내용은 23-15페이지의 충돌 해결 및 정책 변경 사항 커밋을/를 참조하십시오.

침입 정책에서 고급 설정 구성

라이센스: 보호

침입 정책의 *고급 설정*을 구성하려면 특정 전문 지식이 필요합니다. 침입 정책의 기반 정책은 기본적으로 활성화되는 고급 설정 및 각각에 대한 기본 컨피그레이션을 결정합니다.

침입 정책의 탐색 패널에서 **Advanced Settings**를 선택하면 유형별 고급 설정이 정책에 나열됩니다. Advanced Settings 페이지에서는 침입 정책의 고급 설정을 활성화 또는 비활성화할 수 있으며, 고급 설정 컨피그레이션 페이지에 액세스할 수 있습니다.

고급 설정을 구성하려면 먼저 활성화해야 합니다. 고급 설정을 활성화하면, 탐색 패널에서 고급 설정에 대한 컨피그레이션 페이지의 하위 링크가 **Advanced Settings** 링크 아래에 나타납니다. 또한 컨피그레이션 페이지에 대한 **Edit** 링크가 Advanced Settings 페이지의 고급 설정 옆에 나타납니다.

팁 고급 설정의 컨피그레이션을 기반 정책의 설정으로 되돌리려면 고급 설정에 대한 컨피그레이션 페이지에서 **Revert to Defaults**를 클릭합니다. 확인 메시지가 표시되면 설정을 되돌릴 것임을 확인합니다.

고급 설정을 비활성화하면 하위 링크와 **Edit** 링크가 더 이상 나타나지 않지만 컨피그레이션은 그대로 유지됩니다. 일부 침입 정책 컨피그레이션(민감한 데이터 규칙, 침입 규칙에 대한 SNMP 알림)에는 활성화되고 올바르게 구성된 고급 설정이 필요합니다. 이렇게 잘못 구성된 침입 정책은 저장할 수 없습니다. 23-15페이지의 충돌 해결 및 정책 변경 사항 커밋을/를 참조하십시오.

고급 설정의 컨피그레이션을 수정하려면 수정할 컨피그레이션과 네트워크에서 미칠 영향에 대해 잘 알고 있어야 합니다. 다음 절에서는 각 고급 설정의 특정 컨피그레이션 세부사항에 대한 링크를 제공합니다.

Specific Threat Detection

민감한 데이터 프리프로세서는 ASCII 텍스트의 신용카드 번호 및 주민등록번호 같은 민감한 데이터를 탐지합니다. 이러한 프리프로세서 구성에 대한 자세한 내용은 34-18페이지의 민감한 데이터 탐지을/를 참조하십시오.

후면 구멍 공격, 몇몇 포트 스캔 유형, 과도한 트래픽으로 네트워크의 무력화를 시도하는 속도 기반 공격 등 특정 위협을 탐지하는 기타 프리프로세서는 네트워크 분석 정책에서 구성됩니다. 자세한 내용은 34-1페이지의 특정 위협 탐지을/를 참조하십시오.

Intrusion Rule Thresholds

전역 규칙 임계값 기능을 사용하면 시스템이 침입 이벤트를 로깅 및 표시하는 횟수를 제한하는 임계값을 통해 시스템이 다수의 이벤트로 무력화되는 것을 방지할 수 있습니다. 자세한 내용은 35-1페이지의 전체적으로 침입 이벤트 로깅 제한을/를 참조하십시오.

External Responses

웹 인터페이스 내의 다양한 침입 이벤트 보기 외에도 시스템 로그(syslog) 장소에 로깅하는 기능을 활성화하거나 이벤트 데이터를 SNMP 트랩 서버로 전송할 수 있습니다. 정책 단위로 침입 이벤트 알림 제한을 지정하고, 외부 로깅 장소에 대한 침입 이벤트 알림을 설정하고, 침입 이벤트에 대한 외부 응답을 구성할 수 있습니다. 자세한 내용은 다음 링크를 참고하십시오.

- 44-3페이지의 SNMP 응답 구성
- 44-6페이지의 Syslog 응답 구성

이러한 정책 단위 알림 컨피그레이션 외에도 각 규칙이나 규칙 그룹에 대해 침입 이벤트의 이메일 알림을 전역적으로 활성화 또는 비활성화할 수 있습니다. 어떤 침입 정책이 패킷을 처리하는지와 상관없이 이메일 알림 설정이 사용됩니다. 자세한 내용은 44-7페이지의 이메일 알림 이해을/를 참조하십시오.

침입 정책 적용

라이센스: 보호

액세스 제어를 사용하여 관리되는 디바이스에 침입 정책을 적용한 후(12-15페이지의 액세스 제어 정책 적용 참조) 언제든 침입 정책을 다시 적용할 수 있습니다. 이 기능을 사용하면 액세스 제어 정책을 다시 적용하지 않고도 모니터링되는 네트워크에서 침입 정책 변경 사항을 구현할 수 있습니다. 다시 적용할 때, 침입 정책이 마지막으로 적용된 후 변경된 내용을 확인할 수 있는 비교 보고서도 볼 수 있습니다.

침입 정책을 다시 적용할 때 다음을 참조하십시오.

- 침입 정책 다시 적용 작업을 정기적으로 반복되도록 예약할 수 있습니다. 62-6페이지의 침입 정책 적용 자동화을/를 참조하십시오.
- 잘못된 대상 디바이스에서는 침입 정책 다시 적용이 실패합니다. 예를 들어 전에 적용된 침입 정책을 디바이스에서 제거하는 액세스 제어 정책을 적용한 다음, 액세스 제어 정책 적용 작업이 해결되기 전에 침입 정책을 다시 적용하려고 시도하면 침입 정책 다시 적용이 실패합니다.
- FireSIGHT 시스템의 서로 다른 버전을 실행하는(예: 디바이스 중 하나에 대한 업그레이드가 실패한 경우) 스태킹된 디바이스에는 침입 정책을 적용할 수 없습니다. 침입 정책을 디바이스 스택에는 다시 적용할 수 있지만, 스택 내 개별 디바이스에는 다시 적용할 수 없습니다.
- 규칙 업데이트를 가져올 때 가져오기가 완료되면 침입 정책을 자동으로 적용할 수 있습니다. 이 옵션을 활성화하지 않은 경우 규칙 업데이트에 의해 변경된 정책을 수동으로 다시 적용해야 합니다. 자세한 내용은 66-14페이지의 규칙 업데이트 및 로컬 규칙 파일 가져오기을/를 참조하십시오.
- 방어 센터의 Snort 버전이 관리되는 디바이스의 버전과 다르면 액세스 제어 정책을 적용하지 않은 채 디바이스에 침입 정책을 적용할 수 없습니다. 이 이유 때문에 침입 정책 적용이 실패하는 경우, 대신 전체 액세스 제어 정책을 다시 적용하십시오.

침입 정책을 다시 적용하려면

액세스: Admin/Security Approver

1단계 **Policies > Intrusion > Intrusion Policy**를 선택합니다.

Intrusion Policy 페이지가 나타납니다.

2단계 다시 적용할 정책 옆에 있는 적용 아이콘( )을 클릭합니다.

Reapply Intrusion Policy 창이 나타나며, 정책이 현재 적용된 디바이스가 나열됩니다.

3단계 정책을 다시 적용할 디바이스를 지정합니다.

팁 선택적으로, 디바이스가 **Out-of-date**로 나열되면 비교 아이콘( )을 클릭하여 현재 적용된 침입 정책과 업데이트된 침입 정책을 비교하는 보고서를 봅니다.

4단계 **Reapply**를 클릭합니다.

정책이 다시 적용됩니다. 작업 대기열을 사용하여 적용의 상태를 모니터링할 수 있습니다(**System > Monitoring > Task Status**). 자세한 내용은 C-1페이지의 작업 대기열 보기을/를 참조하십시오.

현재 침입 설정 보고서 생성

라이센스: 보호

침입 정책 보고서는 특정 시점의 정책 컨피그레이션에 대한 기록입니다. 시스템은 기반 정책의 설정을 정책 레이어의 설정과 결합하고, 기반 정책에서 시작된 설정과 정책 레이어에서 시작된 설정을 구분하지 않습니다.

감사의 목적으로 또는 현재 컨피그레이션을 검사하는 데 다음 정보를 포함하는 이 보고서를 사용할 수 있습니다.

표 31-3 침입 정책 보고서 섹션

섹션	설명
Policy Information	침입 정책의 이름과 설명, 마지막으로 정책을 수정한 사용자의 이름, 정책이 마지막으로 수정된 날짜와 시간을 제공합니다. 또한 인라인 구축에서 패킷 삭제 기능이 활성화되었는지 여부, 현재 규칙 업데이트 버전, 기반 정책이 현재 규칙 업데이트로 잠겼는지 여부도 나타납니다.
FireSIGHT Recommendations	네트워크의 호스트와 애플리케이션을 기반으로 권장 규칙 상태에 대한 정보를 제공합니다. 선택적으로, FireSIGHT 권장 사항을 구성할 때 해당 설정을 활성화한 경우 정책 보고서에 권장 사항과 규칙 상태 간 차이가 포함됩니다.
Established	활성화된 모든 침입 정책 고급 설정과 컨피그레이션을 나열합니다.
Rules	활성화된 모든 규칙 및 작업의 목록을 제공합니다.

두 가지 침입 정책 또는 동일한 정책의 두 개정을 비교하는 비교 보고서를 생성할 수도 있습니다. 자세한 내용은 31-10페이지의 두 가지 침입 정책 또는 개정 비교을/를 참조하십시오.

침입 정책 보고서를 보려면

액세스: Admin/Intrusion Admin

1단계 **Policies > Intrusion > Intrusion Policy**를 선택합니다.

Intrusion Policy 페이지가 나타납니다.

2단계 보고서를 생성할 침입 정책 옆의 보고서 아이콘( )을 클릭합니다. 침입 정책 보고서를 생성하기 전에 모든 잠재적 변경 사항을 커밋해야 합니다. 커밋된 변경 사항만 보고서에 나타납니다.

시스템에서 침입 정책 보고서를 생성합니다. 브라우저 설정에 따라 보고서가 팝업 창에 나타날 수 있으며, 컴퓨터에 보고서를 저장하는 프롬프트가 표시될 수도 있습니다.

두 가지 침입 정책 또는 개정 비교

라이센스: 보호

조직의 표준을 준수하거나 시스템 성능을 최적화하기 위해 정책 변경 사항을 검토할 경우 두 침입 정책 간의 차이를 확인할 수 있습니다. 액세스할 수 있는 침입 정책에 대해 두 가지 침입 정책 또는 동일한 침입 정책의 두 가지 개정을 비교할 수 있습니다. 선택적으로, 비교 후 두 정책 또는 정책 개정의 차이를 기록하는 PDF 보고서를 생성할 수도 있습니다.

침입 정책 또는 침입 정책 개정의 비교에 사용할 수 있는 두 가지 툴이 있습니다.

- 비교 보기에는 두 침입 정책 또는 침입 정책 개정 간의 차이점만 나란히 표시됩니다. 각 정책 또는 정책 개정의 이름은 비교 보기 왼쪽과 오른쪽의 제목 표시줄에 나타납니다.

  이를 사용하여 웹 인터페이스에서 차이점이 강조 표시된 상태로 두 정책 개정을 모두 보고 탐색할 수 있습니다.
- 비교 보고서는 두 침입 정책 또는 침입 정책 개정의 차이점에 대해서만 기록을 생성하는데, 그 형식은 침입 정책 보고서와 비슷하지만 PDF 형식입니다.

  이를 사용하여 향후 점검을 위해 정책 비교를 저장, 복사, 인쇄, 공유할 수 있습니다.

침입 정책 비교 툴을 이해하고 사용하는 방법에 대한 자세한 내용은 다음을 참조하십시오.

- 31-10페이지의 침입 정책 비교 보기 사용
- 31-11페이지의 침입 정책 비교 보고서 사용

침입 정책 비교 보기 사용

라이센스: 보호

비교 보기에서는 두 침입 정책 또는 정책 개정을 나란히 표시하며, 각 정책 또는 정책 개정은 비교 보기의 좌우 제목 표시줄에 있는 이름으로 식별됩니다. 마지막 수정 시간 및 마지막 수정자가 정책 이름의 오른쪽에 표시됩니다. Intrusion Policy 페이지에는 정책의 마지막 수정 시간이 현지 시간으로 표시되지만, 침입 정책 보고서에는 수정 시간이 UTC로 표시됩니다. 두 가지 침입 정책 또는 정책 개정 간의 차이점이 강조 표시됩니다.

- 파란색은 강조 표시된 설정이 두 정책 또는 정책 개정에서 다름을 의미하며, 그 차이점이 빨간색 텍스트로 표시됩니다.
- 녹색은 강조 표시된 설정이 둘 중 한 정책 또는 정책 개정에만 나타남을 의미합니다.

다음 표에 설명된 작업을 수행할 수 있습니다.

표 31-4 침입 정책 비교 보기의 작업

목적	가능한 작업
개별 변경 사항 탐색	제목 표시줄 위의 **Previous** 또는 **Next**를 클릭합니다. 왼쪽과 오른쪽 사이의 중앙에 있는 이중 화살표 아이콘()이 움직이고, 어떤 차이점을 보고 있는지 식별할 수 있도록 **Difference** 번호가 조정됩니다.
특정 고급 설정에 대한 컨피그레이션이 포함된 레이어 확인	보려는 컨피그레이션 옆에 있는 고급 컨피그레이션 아이콘() 위로 포인터를 가져갑니다. 창에는 고급 컨피그레이션을 포함하는 레이어의 이름이 표시됩니다.

표 31-4 침입 정책 비교 보기의 작업(계속)

목적	가능한 작업
새 침입 정책 비교 보기 생성	**New Comparison**을 클릭합니다. **Select Comparison** 창이 나타납니다. 자세한 내용은 침입 정책 비교 보고서 사용을/를 참조하십시오.
침입 정책 비교 보고서 생성	**Comparison Report**를 클릭합니다. 정책 비교 보고서에서는 두 정책 또는 정책 개정의 차이점만 나열하는 PDF 문서를 생성합니다.

침입 정책 비교 보고서 사용

라이센스: 보호

침입 정책 비교 보고서는 두 침입 정책 또는 동일한 침입 정책의 두 개정 간 모든 차이점을 PDF에서 침입 정책 비교 보기 형태로 기록한 것입니다. 두 침입 정책 컨피그레이션의 차이점을 더 자세히 살펴보고 조사 결과를 저장하여 배포하는 데 이 보고서를 사용할 수 있습니다.

액세스 권한이 있는 어떤 침입 정책에 대해서도 비교 보기에서 침입 정책 비교 보고서를 생성할 수 있습니다. 침입 정책 보고서를 생성하기 전에 모든 잠재적 변경 사항을 커밋해야 합니다. 커밋된 변경 사항만 보고서에 나타납니다.

침입 정책 비교 보고서의 형식은 침입 정책 보고서와 동일합니다. 단, 침입 정책 보고서는 침입 정책의 모든 설정을 포함하는 것과 달리 침입 정책 비교 보고서는 두 정책 간에 다른 설정만 나열합니다.

컨피그레이션에 따라, 침입 정책 비교 보고서는 침입 정책 보고서 섹션 표에 설명된 것처럼 하나 이상의 섹션을 포함할 수 있습니다.

팁 SSL, 액세스 제어, 네트워크 분석, 파일, 시스템 또는 상태 정책을 비교하는 데에도 비슷한 절차를 사용할 수 있습니다.

두 침입 정책 또는 동일한 정책의 두 개정을 비교하려면

액세스: Admin/Intrusion Admin

1단계 **Policies > Intrusion > Intrusion Policy**를 선택합니다.

Intrusion Policy 페이지가 나타납니다.

2단계 **Compare Policies**를 클릭합니다.

Select Comparison 창이 나타납니다.

3단계 **Compare Against** 드롭다운 목록에서 원하는 비교 유형을 선택합니다.

- 두 개의 다른 정책을 비교하려면 **Other Policy**를 선택합니다.
- 동일한 정책의 두 개정을 비교하려면 **Other Revision**을 선택합니다.

침입 정책 보고서를 생성하기 전에 모든 변경 사항을 커밋해야 합니다. 커밋된 변경 사항만 보고서에 나타납니다.

4단계 선택한 비교 유형에 따라 다음을 선택할 수 있습니다.

- 두 개의 다른 정책을 비교할 경우 비교할 정책을 **Policy A** 및 **Policy B** 드롭다운 목록에서 각각 선택합니다.
- 동일한 정책의 두 개정을 비교하는 경우 **Policy** 드롭다운 목록에서 정책을 선택한 다음, **Revision A** 및 **Revision B** 드롭다운 목록에서 비교할 개정을 선택합니다.

5단계 침입 정책 비교 보기를 표시하려면 **OK**를 클릭합니다.

비교 보기가 나타납니다.

6단계 침입 정책 비교 보고서를 생성하려면 **Comparison Report**를 클릭합니다.

7단계 침입 정책 보고서가 나타납니다. 브라우저 설정에 따라 보고서가 팝업 창에 나타날 수 있으며, 컴퓨터에 보고서를 저장하는 프롬프트가 표시될 수도 있습니다.

32장

규칙을 사용하여 침입 정책 조정

침입 정책의 Rules 페이지에서는 공유 객체 규칙, 표준 텍스트 규칙 및 프리프로세서 규칙을 위한 규칙 상태 및 기타 설정을 구성할 수 있습니다.

상태를 Generate Events 또는 Drop and Generate Events로 설정하여 규칙을 활성화합니다. 규칙을 활성화하면 시스템은 규칙과 일치하는 트래픽에 대해 이벤트를 생성합니다. 규칙을 비활성화하면 규칙의 처리가 중지됩니다. 선택적으로, 인라인 구축에서 Drop and Generate Events로 설정된 규칙이 일치하는 트래픽에 대해 이벤트를 생성하거나 해당 트래픽을 삭제하도록 침입 정책을 설정할 수 있습니다. 자세한 내용은 31-6페이지의 인라인 구축에서 삭제 동작 설정을/를 참조하십시오. 패시브 구축에서 Drop and Generate Events로 설정된 규칙은 일치하는 규칙에 대해 이벤트를 생성합니다.

하위 집합을 표시하도록 규칙을 필터링하면 규칙 상태 또는 규칙 설정을 변경하고자 하는 정확한 규칙 집합을 선택할 수 있습니다.

침입 규칙 또는 규칙 인수에서 비활성화된 프리프로세서를 요구하면, 네트워크 분석 정책의 웹 인터페이스에서 비활성 상태로 있더라도 시스템에서는 자동으로 현재의 컨피그레이션과 함께 해당 프리프로세서를 사용합니다. 자세한 내용은 23-12페이지의 사용자 지정 정책의 제한 사항을/를 참조하십시오.

자세한 내용은 다음 절을 참조하십시오.

- 32-2페이지의 침입 방지 규칙 유형 이해 - 침입 정책에서 보고 구성할 수 있는 침입 규칙 및 프리프로세서 규칙에 대해 설명합니다.
- 32-3페이지의 침입 정책의 규칙 보기 - Rules 페이지에서 규칙의 순서를 변경하고, 페이지에서 아이콘을 해석하고, 규칙 세부사항에 집중하는 방법에 대해 설명합니다.
- 32-10페이지의 침입 정책의 규칙 필터링 - 규칙 필터를 사용하여 규칙 설정을 적용할 규칙을 찾는 방법에 대해 설명합니다.
- 32-20페이지의 규칙 상태 설정 - Rules 페이지에서 규칙을 활성화 및 비활성화하는 방법에 대해 설명합니다.
- 32-22페이지의 정책당 침입 이벤트 알림 필터링 - 특정 규칙에 대한 이벤트 필터링 임계값을 설정하고 특정 규칙에서 억제를 설정하는 방법에 대해 설명합니다.
- 32-29페이지의 동적 규칙 상태 추가 - 일치하는 트래픽에서 규칙 변칙이 탐지될 때 동적으로 트리거되는 규칙 상태를 설정하는 방법에 대해 설명합니다.
- 32-33페이지의 SNMP 알림 추가 - SNMP 알림을 특정 규칙과 연결하는 방법에 대해 설명합니다.
- 32-34페이지의 규칙 코멘트 추가 - 침입 정책에서 규칙에 코멘트를 추가하는 방법에 대해 설명합니다.

침입 방지 규칙 유형 이해

라이센스: 보호

침입 정책에는 침입 규칙과 프리프로세서 규칙이라는 두 가지 규칙 유형이 포함됩니다.

침입 규칙은 네트워크에서 취약성 악용 시도를 탐지하는 키워드와 인수의 지정된 집합이며, 네트워크 트래픽을 분석하여 규칙의 기준과 일치하는지를 확인합니다. 시스템은 패킷을 각 규칙에 지정된 조건과 비교하고, 패킷이 규칙에 지정된 모든 조건과 일치하면 규칙을 트리거합니다. 시스템에는 Cisco VRT(Vulnerability Research Team)에서 생성한 다음 두 가지 유형의 침입 규칙이 포함되어 있습니다. 공유 객체 규칙은 컴파일되며 수정할 수 없습니다(소스 및 목적지 포트, IP 주소 등의 규칙 헤더 정보 제외). 표준 텍스트 규칙은 규칙에 대한 새 사용자 지정 인스턴스로서 저장 및 수정할 수 있습니다.

시스템에는 또한 프리프로세서 및 패킷 디코더 탐지 옵션과 연결된 규칙인 프리프로세서 규칙도 포함됩니다. 프리프로세서 규칙은 복사 또는 수정할 수 없습니다. 대부분의 프리프로세서 규칙은 기본적으로 비활성화되어 있습니다. 시스템이 프리프로세서 규칙에 대해 이벤트를 생성하고 인라인 구축에서 위반 패킷을 삭제하도록 하려면 프리프로세서 규칙을 활성화(즉, Generate Events 또는 Drop and Generate Events로 설정)해야 합니다.

VRT는 시스템에 포함된 각 기본 침입 정책에 대해 Cisco의 공유 객체 규칙, 표준 텍스트 규칙 및 프리프로세서 규칙에 대한 기본 규칙 상태를 결정합니다.

다음 표에서는 FireSIGHT 시스템에 포함된 각 규칙 유형에 대해 설명합니다.

표 32-1 규칙 유형

유형	설명
공유 객체 규칙	C 소스 코드에서 컴파일된 이진 모듈로 제공되며 Cisco VRT(Vulnerability Research Team)에서 생성하는 침입 규칙. 공유 객체 규칙을 사용하면 표준 텍스트 규칙에서 할 수 없는 방법으로 공격을 탐지할 수 있습니다. 공유 객체 규칙에서는 규칙 키워드와 인수를 수정할 수 없습니다. 규칙에서 사용되는 변수를 수정하거나, 소스/목적지 포트 및 IP 주소와 같은 정보를 수정하고 규칙의 새 인스턴스를 사용자 지정 공유 객체 규칙으로서 저장할 수 있을 뿐입니다. 공유 객체 규칙에는 GID(generator ID) 3이 있습니다. 자세한 내용은 36-104페이지의 기존 규칙 수정을/를 참조하십시오.
표준 텍스트 규칙	VRT에서 생성하거나, 새 사용자 지정 규칙으로서 복사 및 저장하거나, 규칙 편집기를 사용하여 생성하거나, 로컬 시스템에서 생성하여 가져오는 로컬 규칙으로서 가져온 침입 규칙. VRT에서 생성한 표준 규칙에서는 규칙 키워드와 인수를 수정할 수 없습니다. 규칙에서 사용되는 변수를 수정하거나, 소스/목적지 포트 및 IP 주소와 같은 정보를 수정하고 규칙의 새 인스턴스를 사용자 지정 표준 텍스트 규칙으로서 저장할 수 있을 뿐입니다. 자세한 내용은 36-104페이지의 기존 규칙 수정, 36-1페이지의 침입 규칙 이해 및 작성 및 66-20페이지의 로컬 규칙 파일 가져오기을/를 참조하십시오. VRT에서 생성한 표준 텍스트 규칙에는 GID(generator ID) 1이 있습니다. 규칙 편집기를 사용하여 생성하거나 로컬 규칙으로서 가져오는 사용자 지정 표준 텍스트 규칙에는 SID(Signature ID) 1000000 이상이 있습니다.
프리프로세서 규칙	패킷 디코더의 탐지 옵션과 관련되거나 FireSIGHT 시스템에 포함된 프리프로세서 중 하나와 관련된 규칙. 프리프로세서 규칙에서 이벤트를 생성하도록 하려면 해당 규칙을 활성화해야 합니다. 이러한 규칙에는 디코더별 또는 프리프로세서별 GID(generator ID)가 있습니다. 자세한 내용은 Generator ID 표를 참조하십시오.

침입 정책의 규칙 보기

라이센스: 보호

침입 정책에서 규칙이 표시되는 방법을 조정할 수 있으며, 여러 기준으로 규칙을 정렬할 수 있습니다. 또한 규칙 설정, 규칙 문서 및 기타 규칙 사양을 보려면 특정 규칙에 대한 세부사항을 표시할 수 있습니다.

Rules 페이지에는 네 개의 주요 기능 영역이 있습니다.

- 필터링 기능 - 자세한 내용은 32-10페이지의 침입 정책의 규칙 필터링 참조
- 규칙 특성 메뉴 - 자세한 내용은 32-20페이지의 규칙 상태 설정, 32-22페이지의 정책당 침입 이벤트 알림 필터링, 32-29페이지의 동적 규칙 상태 추가, 32-33페이지의 SNMP 알림 추가 및 32-34페이지의 규칙 코멘트 추가 참조
- 규칙 목록 - 자세한 내용은 Rules 페이지 열 표 참조
- 규칙 세부사항 - 자세한 내용은 32-5페이지의 규칙 세부사항 보기 참조

또한 서로 다른 기준으로 규칙을 정렬할 수 있습니다. 자세한 내용은 32-4페이지의 규칙 표시 정렬을/를 참조하십시오.

열 제목으로 사용되는 아이콘은 메뉴 모음의 메뉴에 해당하며, 여기에서 해당 컨피그레이션 항목에 액세스할 수 있습니다. 예를 들어 Rule State 메뉴는 Rule State 열과 동일한 아이콘(➡)으로 표시됩니다.

다음 표에서는 Rules 페이지의 열에 대해 설명합니다.

표 32-2 Rules 페이지 열

머리글	설명	참조 섹션
GID	규칙의 GID(Generator ID)를 나타내는 정수.	41-40페이지의 프리프로세서 Generator ID 읽기
SID	SID(Snort ID)를 나타내는 정수로, 규칙의 고유한 식별자 역할을 합니다.	41-40페이지의 프리프로세서 Generator ID 읽기
Message	이 규칙에 의해 생성되는 이벤트에 포함된 메시지로, 규칙의 이름 역할도 합니다.	36-11페이지의 이벤트 메시지 정의
➡	규칙의 규칙 상태로, 다음 세 가지 상태 중 하나일 수 있습니다. • 이벤트 삭제 및 생성(✖) • 이벤트 생성(➡) • 비활성(➡) 규칙 상태 아이콘을 클릭하여 규칙에 대한 Set rule state 대화 상자에 액세스할 수 있습니다.	32-20페이지의 규칙 상태 설정
🌐	규칙에 대한 FireSIGHT 권장 규칙 상태.	33-1페이지의 네트워크 자산에 대한 침입 방지 맞춤화
▼	규칙에 적용되는 이벤트 필터로, 이벤트 임계값 및 이벤트 억제를 포함합니다.	32-22페이지의 정책당 침입 이벤트 알림 필터링
🕒	규칙에 대한 동적 규칙 상태로, 지정된 속도 변칙이 발생하면 작동합니다.	32-29페이지의 동적 규칙 상태 추가

표 32-2 Rules 페이지 열(계속)

머리글	설명	참조 섹션
	규칙에 대해 구성된 알림(현재 SNMP 알림만 있음).	32-33페이지의 SNMP 알림 추가
	규칙에 추가된 코멘트.	32-34페이지의 규칙 코멘트 추가

정책의 다른 레이어에 대한 Rules 페이지로 전환하려면 레이어 드롭다운 목록을 사용할 수도 있습니다. 정책에 레이어를 추가하지 않는 한, 드롭다운 목록에 나열되는 수정 가능한 보기는 정책 Rules 페이지 및 정책 레이어에 대한 Rules 페이지(원래 이름은 `My Changes`)뿐입니다. 이 두 보기 중 하나에서 변경하는 것은 다른 보기에서 변경하는 것과 동일합니다. 자세한 내용은 24-1페이지의 네트워크 분석 또는 침입 정책에서 레이어 사용을/를 참조하십시오. 드롭다운 목록에는 읽기 전용 기반 정책에 대한 Rules 페이지도 나열됩니다. 기반 정책에 대한 자세한 내용은 24-3페이지의 기반 레이어 이해을/를 참조하십시오.

침입 정책에서 규칙을 보려면

액세스: Admin/Intrusion Admin

1단계 **Policies > Intrusion > Intrusion Policy**를 선택합니다.

Intrusion Policy 페이지가 나타납니다.

2단계 수정할 정책 옆에 있는 수정 아이콘( )을 클릭합니다.

다른 정책에 저장하지 않은 변경 사항이 있는 경우 변경 사항을 취소하고 계속 진행하려면 **OK**를 클릭합니다. 저장하지 않은 변경 사항을 다른 정책에 저장하는 방법에 대한 자세한 내용은 23-15페이지의 충돌 해결 및 정책 변경 사항 커밋을/를 참조하십시오.

Policy Information 페이지가 나타납니다.

3단계 Policy Information 페이지에서 **Rules**를 클릭합니다.

Rules 페이지가 나타납니다. 기본적으로 페이지에는 규칙이 메시지별 알파벳순으로 나열됩니다.

탐색 패널의 구분선 위에 있는 **Rules**를 선택하면 동일한 규칙 목록 보기로 이동하게 됩니다. 이 보기에서 정책의 모든 규칙 속성을 보고 설정할 수 있습니다.

규칙 표시 정렬

라이센스: 보호

열 제목 또는 아이콘을 클릭하여 Rules 페이지의 열을 기준으로 규칙을 정렬할 수 있습니다.

제목 또는 아이콘의 위쪽(▲) 또는 아래쪽(▼) 화살표는 해당 열에서 그 방향으로 정렬될 것임을 나타냅니다.

침입 정책에서 규칙을 정렬하려면

액세스: Admin/Intrusion Admin

1단계 **Policies > Intrusion > Intrusion Policy**를 선택합니다.

Intrusion Policy 페이지가 나타납니다.

2단계 수정할 정책 옆에 있는 수정 아이콘( )을 클릭합니다.

다른 정책에 저장하지 않은 변경 사항이 있는 경우 변경 사항을 취소하고 계속 진행하려면 **OK**를 클릭합니다. 저장하지 않은 변경 사항을 다른 정책에 저장하는 방법에 대한 자세한 내용은 23-15페이지의 충돌 해결 및 정책 변경 사항 커밋을/를 참조하십시오.

Policy Information 페이지가 나타납니다.

3단계 **Rules**를 클릭합니다.

Rules 페이지가 나타납니다. 기본적으로 페이지에는 규칙이 메시지별 알파벳순으로 나열됩니다.

4단계 정렬하려는 열의 상단에서 제목 또는 아이콘을 클릭합니다.

열 머리글에 나타나는 화살표의 방향으로 규칙이 열에서 정렬됩니다. 반대 방향으로 정렬하려면 머리글을 다시 클릭합니다. 정렬 순서 및 화살표가 반전됩니다.

규칙 세부사항 보기

라이센스: 보호

Rule Detail 보기에서는 규칙 문서, FireSIGHT 권장 사항 및 규칙 오버헤드를 볼 수 있습니다. 또한 규칙 관련 기능을 보고 추가할 수도 있습니다.

취약성에 매핑되지 않는 한 로컬 규칙에는 오버헤드가 없습니다.

표 32-3 규칙 세부사항

소항목	설명	참조 섹션
Summary	규칙 요약. 규칙 기반 이벤트의 경우, 규칙 문서에 요약 정보가 포함되어 있으면 이 행이 나타납니다.	41-24페이지의 이벤트 정보 보기
Rule State	규칙에 대한 현재 규칙 상태. 규칙 상태가 설정된 레이어를 나타내기도 합니다.	32-20페이지의 규칙 상태 설정, 24-1페이지의 네트워크 분석 또는 침입 정책에서 레이어 사용
FireSIGHT Recommendation	FireSIGHT 권장 사항이 생성된 경우 규칙에 대한 권장 규칙 상태.	33-1페이지의 네트워크 자산에 대한 침입 방지 맞춤화
Rule Overhead	시스템 성능에 대한 규칙의 잠재적 영향력 및 규칙이 오탐을 생성할 가능성.	33-3페이지의 규칙 오버헤드 이해
Thresholds	이 규칙에 대해 현재 설정된 임계값 및 규칙에 대한 임계값을 추가하기 위한 기능.	32-6페이지의 규칙에 대해 임계값 설정
Suppressions	이 규칙에 대해 현재 설정된 억제 설정 및 규칙에 대한 억제를 추가하기 위한 기능.	32-7페이지의 규칙에 대해 억제 설정
Dynamic State	이 규칙에 대해 현재 설정된 규칙 기반 규칙 상태 및 규칙에 대한 동적 규칙 상태를 추가하기 위한 기능.	32-8페이지의 규칙에 대한 동적 규칙 상태 설정
Alerts	이 규칙에 대해 현재 설정된 알림 및 규칙에 대한 알림을 추가하기 위한 기능. 현재 SNMP 알림만 지원됩니다.	32-9페이지의 규칙에 대해 SNMP 알림 설정

표 32-3 규칙 세부사항(계속)

소항목	설명	참조 섹션
Comments	이 규칙에 추가된 코멘트 및 규칙에 대한 코멘트를 추가하기 위한 기능.	32-9페이지의 규칙에 대한 규칙 코멘트 추가
Documentation	Cisco VRT(Vulnerability Research Team)에서 제공하는, 현재 규칙에 대한 규칙 문서.	41-27페이지의 패킷 보기 작업 사용

규칙 세부사항을 보려면

액세스: Admin/Intrusion Admin

1단계 **Policies > Intrusion > Intrusion Policy**를 선택합니다.

Intrusion Policy 페이지가 나타납니다.

2단계 수정할 정책 옆에 있는 수정 아이콘( )을 클릭합니다.

다른 정책에 저장하지 않은 변경 사항이 있는 경우 변경 사항을 취소하고 계속 진행하려면 **OK**를 클릭합니다. 저장하지 않은 변경 사항을 다른 정책에 저장하는 방법에 대한 자세한 내용은 23-15페이지의 충돌 해결 및 정책 변경 사항 커밋을/를 참조하십시오.

Policy Information 페이지가 나타납니다.

3단계 **Rules**를 클릭합니다.

Rules 페이지가 나타납니다. 기본적으로 페이지에는 규칙이 메시지별 알파벳순으로 나열됩니다.

4단계 세부사항을 보려는 규칙을 강조 표시합니다.

5단계 **Show details**를 클릭합니다.

Rule Detail 보기가 나타납니다. 세부사항을 다시 숨기려면 **Hide details**를 클릭합니다.

팁 Rules 보기에서 규칙을 두 번 클릭하여 Rule Detail을 열 수도 있습니다.

규칙에 대해 임계값 설정

라이센스: 보호

Rule Detail 페이지에서 규칙에 대한 단일 임계값을 설정할 수 있습니다. 임계값을 추가하면 규칙에 대한 기존 임계값을 덮어씁니다. 임계값에 대한 자세한 내용은 32-22페이지의 이벤트 임계값 구성을/를 참조하십시오.

잘못된 값을 입력하면 필드에 되돌리기 아이콘( )이 나타납니다. 이 아이콘을 클릭하면 해당 필드에 대한 마지막으로 유효한 값으로 돌아가거나, 이전 값이 없는 경우 필드가 지워집니다.

규칙 세부사항에서 임계값을 설정하려면

액세스: Admin/Intrusion Admin

1단계 **Thresholds** 옆에 있는 **Add**를 클릭합니다.

Set Threshold 대화 상자가 나타납니다.

2단계 **Type** 드롭다운 목록에서 설정하려는 임계값의 유형을 선택합니다.

- 기간당 지정된 이벤트 인스턴스의 수로 알림을 제한하려면 **Limit**를 선택합니다.
- 기간당 지정된 각 이벤트 인스턴스의 수에 대해 알림을 제공하려면 **Threshold**를 선택합니다.
- 지정된 이벤트 인스턴스의 수 이후 기간당 한 번 알림을 제공하려면 **Both**를 선택합니다.

3단계 이벤트 인스턴스를 소스 또는 목적지 IP 주소로 추적할지를 나타내려면 **Track By** 드롭다운 목록에서 **Source** 또는 **Destination**을 선택합니다.

4단계 임계값으로 사용할 이벤트 인스턴스의 수를 **Count** 필드에 입력합니다.

5단계 이벤트 인스턴스를 추적할 기간(초 단위)을 지정하는 0~2147483647의 숫자를 **Seconds** 필드에 입력합니다.

6단계 **OK**를 클릭합니다.

시스템은 임계값을 추가하고 Event Filtering 열의 규칙 옆에 이벤트 필터 아이콘( )을 표시합니다. 규칙에 여러 이벤트 필터를 추가하는 경우 이벤트 필터 개수가 아이콘 위에 표시됩니다.

규칙에 대해 억제 설정

라이센스: 보호

Rule Detail 페이지에서 규칙에 대한 하나 이상의 억제를 설정할 수 있습니다. 억제에 대한 자세한 내용은 32-26페이지의 침입 정책당 억제 구성을/를 참조하십시오.

잘못된 값을 입력하면 필드에 되돌리기 아이콘( )이 나타납니다. 이 아이콘을 클릭하면 해당 필드에 대한 마지막으로 유효한 값으로 돌아가거나, 이전 값이 없는 경우 필드가 지워집니다.

규칙 세부사항에서 억제를 설정하려면

액세스: Admin/Intrusion Admin

1단계 **Suppressions** 옆에 있는 **Add**를 클릭합니다.

Add Suppression 대화 상자가 나타납니다.

2단계 **Suppression Type** 드롭다운 목록에서 다음 옵션 중 하나를 선택합니다.

- 선택한 규칙에 대한 이벤트를 완전히 억제하려면 **Rule**을 선택합니다.
- 지정된 소스 IP 주소에서 나온 패킷에 의해 생성된 이벤트를 억제하려면 **Source**를 선택합니다.
- 지정된 목적지 IP 주소로 이동하는 패킷에 의해 생성된 이벤트를 억제하려면 **Destination**을 선택합니다.

3단계 억제 유형에 대해 **Source** 또는 **Destination**을 선택한 경우 Network 필드가 나타납니다. IP 주소, 주소 블록 또는 이러한 항목 조합의 쉼표로 구분된 목록을 **Network** 필드에 입력합니다. 침입 정책이 액세스 제어 정책의 기본 작업과 연결된 경우 기본 작업 변수 집합에서 네트워크 변수를 지정하거나 나열할 수도 있습니다.

FireSIGHT 시스템에서 IPv4 CIDR 및 IPv6 접두사 길이 주소 블록의 사용에 대한 자세한 내용은 1-19페이지의 IP 주소 표기 규칙을/를 참조하십시오.

4단계 **OK**를 클릭합니다.

시스템은 억제 조건을 추가하고 억제된 규칙 옆 Event Filtering 열의 규칙 옆에 이벤트 필터 아이콘( )을 표시합니다. 규칙에 여러 이벤트 필터를 추가하는 경우 아이콘 위의 숫자는 필터의 수를 나타냅니다.

규칙에 대한 동적 규칙 상태 설정

라이센스: 보호

Rule Detail 페이지에서 규칙에 대한 하나 이상의 동적 규칙 상태를 설정할 수 있습니다. 나열되는 첫 번째 동적 규칙 상태의 우선순위가 가장 높습니다. 두 개의 동적 규칙 상태가 충돌하면 첫 번째 작업이 구현됩니다. 동적 규칙 상태에 대한 자세한 내용은 32-30페이지의 동적 규칙 상태 이해을/를 참조하십시오.

잘못된 값을 입력하면 필드에 되돌리기 아이콘( )이 나타납니다. 이 아이콘을 클릭하면 해당 필드에 대한 마지막으로 유효한 값으로 돌아가거나, 이전 값이 없는 경우 필드가 지워집니다.

규칙 세부사항에서 동적 규칙 상태를 설정하려면

액세스: Admin/Intrusion Admin

1단계 **Dynamic State** 옆에 있는 **Add**를 클릭합니다.

Add Rate-Based Rule State 대화 상자가 나타납니다.

2단계 **Track By** 드롭다운 목록에서 규칙 일치를 추적할 방법을 나타내는 옵션을 선택합니다.

- 특정 소스 또는 소스 집합에서 해당 규칙과 일치하는 수를 추적하려면 **Source**를 선택합니다.
- 특정 목적지 또는 목적지 집합에서 해당 규칙과 일치하는 수를 추적하려면 **Destination**을 선택합니다.
- 해당 규칙에 대한 모든 일치 항목을 추적하려면 **Rule**을 선택합니다.

3단계 선택적으로, **Track By**를 **Source** 또는 **Destination**으로 설정하는 경우 추적하려는 각 호스트의 IP 주소를 **Network** 필드에 입력합니다.

FireSIGHT 시스템에서 IPv4 CIDR 및 IPv6 접두사 길이 표기법 사용에 대한 자세한 내용은 1-19페이지의 IP 주소 표기 규칙을/를 참조하십시오.

4단계 공격 속도를 설정하기 위한 기간당 규칙 일치 수를 **Rate** 옆에 지정합니다.

- 0~2147483647의 정수를 사용하여 임계값으로 사용할 규칙 일치의 수를 **Count** 필드에 지정합니다.
- 0~2147483647의 정수를 사용하여 공격이 추적되는 기간의 값(초 단위)을 **Seconds** 필드에 입력합니다.

5단계 조건이 일치할 때 수행할 새 작업을 **New State** 드롭다운 목록에서 선택합니다.

- 이벤트를 생성하려면 **Generate Events**를 선택합니다.
- 인라인 구축에서 이벤트를 생성하고 이벤트를 트리거한 패킷을 삭제하려면 또는 패시브 구축에서 이벤트를 생성하려면 **Drop and Generate Events**를 선택합니다.
- 작업을 수행하지 않으려면 **Disabled**를 선택합니다.

6단계 1~2147483647(약 68년)의 정수를 사용하여 새 작업이 유효한 상태를 유지할 기간의 값(초 단위)을 **Timeout** 필드에 입력합니다. 시간이 초과되면 규칙이 원래 상태로 돌아갑니다. 새 작업의 시간 초과를 금지하려면 0을 지정합니다.

7단계 **OK**를 클릭합니다.

시스템은 동적 규칙 상태를 추가하고 Dynamic State 열의 규칙 옆에 동적 상태 아이콘( )을 표시합니다. 규칙에 여러 동적 규칙 상태 필터를 추가하는 경우 아이콘 위의 숫자는 필터의 수를 나타냅니다.

필수 필드 중 비어 있는 것이 있으면 필드를 작성해야 한다는 오류 메시지가 표시됩니다.

규칙에 대해 SNMP 알림 설정

라이센스: 보호

Rule Detail 페이지에서 규칙에 대한 SNMP 알림을 설정할 수 있습니다. SNMP 알림에 대한 자세한 내용은 32-33페이지의 SNMP 알림 추가을/를 참조하십시오.

규칙 세부사항에서 SNMP 알림을 추가하려면

액세스: Admin/Intrusion Admin

1단계 **Alerts** 옆에 있는 **Add SNMP Alert**를 클릭합니다.

시스템은 알림을 추가하고 Alerting 열의 규칙 옆에 알림 아이콘( )을 표시합니다. 규칙에 여러 알림을 추가하는 경우 알림 개수가 아이콘 위에 표시됩니다.

규칙에 대한 규칙 코멘트 추가

라이센스: 보호

Rule Detail 페이지에서 규칙에 대한 규칙 코멘트를 추가할 수 있습니다. 규칙 코멘트에 대한 자세한 내용은 32-34페이지의 규칙 코멘트 추가를 참고하십시오.

규칙 세부사항에서 코멘트를 추가하려면

액세스: Admin/Intrusion Admin

1단계 **Comments** 옆에 있는 **Add**를 클릭합니다.

Add Comment 대화 상자가 나타납니다.

2단계 **Comment** 필드에 규칙 코멘트를 입력합니다.

3단계 **OK**를 클릭합니다.

시스템은 코멘트를 추가하고 Comments 열의 규칙 옆에 코멘트 아이콘( )을 표시합니다. 규칙에 여러 코멘트를 추가하는 경우 아이콘 위의 숫자는 코멘트의 수를 나타냅니다.

팁 규칙 코멘트를 삭제하려면 규칙 코멘트 섹션에서 **Delete**를 클릭합니다. 코멘트되지 않은 침입 정책 변경 사항과 함께 코멘트가 캐시된 경우에만 코멘트를 삭제할 수 있습니다. 침입 정책 변경 사항이 커밋되면 규칙 코멘트는 영구적인 상태가 됩니다.

침입 정책의 규칙 필터링

라이센스: 보호

Rules 페이지에 표시된 규칙을 단일 기준 또는 여러 기준의 조합으로 필터링할 수 있습니다.

구성한 필터는 Filter 텍스트 상자에 표시됩니다. 필터 패널에서 키워드 및 키워드 인수를 클릭하여 필터를 구성할 수 있습니다. 여러 키워드를 선택하면 시스템에서는 AND 논리를 사용하여 결합한 다음 복합 검색 필터를 생성합니다. 예를 들어 **Category** 아래에서 **preprocessor**를 선택한 다음 **Rule Content > GID**를 선택하고 `116`을 입력하면 `Category: "preprocessor" GID:"116"` 필터가 구성됩니다. 이 필터는 프리프로세서 규칙 **및(and)** GID 116인 모든 규칙을 검색합니다.

Category, Microsoft Vulnerabilities, Microsoft Worms, Platform Specific, Preprocessor 및 Priority 필터 그룹을 사용하면 키워드에 대한 여러 개의 인수를 쉼표로 구분하여 제출할 수 있습니다. 예를 들어 Shift 키를 누르고 **Category**에서 **os-linux** 및 **os-windows**를 선택하면 `Category:"os-windows,os-linux"` 필터가 구성됩니다. 이 필터는 `os-linux` 카테고리 또는 `os-windows` 카테고리의 규칙을 검색합니다.

필터 패널을 표시하려면 표시 아이콘( )을 클릭합니다.

필터 패널을 숨기려면 숨기기 아이콘( )을 클릭합니다.

자세한 내용은 다음 항목을 참조하십시오.

- 32-10페이지의 침입 정책의 규칙 필터링 이해
- 32-18페이지의 침입 정책에서 규칙 필터 설정

침입 정책의 규칙 필터링 이해

라이센스: 보호

규칙 필터 키워드를 사용하면 규칙 설정(예: 규칙 상태 또는 이벤트 필터)을 적용할 규칙을 쉽게 찾을 수 있습니다. 키워드로 필터링하고 동시에 Rules 페이지 필터 패널에서 원하는 인수를 선택하여 키워드에 대한 인수를 선택할 수 있습니다.

자세한 내용은 다음 절을 참조하십시오.

- 32-10페이지의 침입 정책 규칙 필터 구성을 위한 지침
- 32-13페이지의 규칙 컨피그레이션 필터 이해
- 32-15페이지의 규칙 내용 필터 이해
- 32-17페이지의 규칙 카테고리 이해
- 32-17페이지의 규칙 필터 직접 수정

침입 정책 규칙 필터 구성을 위한 지침

라이센스: 보호

대부분의 경우 필터를 작성할 때 침입 정책에서 Rules 페이지의 왼쪽에 있는 필터 패널을 사용하여 원하는 키워드/인수를 선택합니다.

Rule 필터는 필터 패널의 규칙 필터 그룹으로 그룹화됩니다. 많은 규칙 필터 그룹에 하위 기준이 포함되어 있어서 원하는 특정 규칙을 손쉽게 찾을 수 있습니다. 일부 규칙 필터에는 개별 규칙으로 드릴다운하기 위해 확장할 수 있는 여러 레벨이 있습니다.

필터 패널의 항목은 때로는 필터 유형 그룹, 때로는 키워드, 그리고 때로는 키워드에 대한 인수를 나타냅니다. 다음의 대략적인 방법을 사용하면 필터를 작성하는 데 도움이 됩니다.

- 키워드가 아닌 필터 유형 그룹 제목(Rule Configuration, Rule Content, Platform Specific 및 Priority)을 선택하면 해당 제목이 확장되어 사용 가능한 키워드가 나열됩니다.

  기준 목록의 노드를 클릭하여 키워드를 선택하면 팝업 창이 나타나는데, 여기에서 필터링할 인수를 제공합니다.

  해당 키워드가 필터에서 이미 사용되고 있는 경우, 새로 제공하는 인수가 키워드의 기존 인수를 교체합니다.

  예를 들어 필터 패널의 **Rule Configuration > Recommendation** 아래에서 **Drop and Generate Events**를 클릭하면 필터 텍스트 상자에 `Recommendation:"Drop and Generate Events"`가 추가됩니다. 그런 다음 **Rule Configuration > Recommendation** 아래에서 **Generate Events**를 클릭하면 필터가 `Recommendation:"Generate Events"`로 변경됩니다.

- 키워드인 필터 유형 그룹 제목(Category, Classifications, Microsoft Vulnerabilities, Microsoft Worms, Priority 및 Rule Update)을 선택하면 사용 가능한 인수가 나열됩니다.

  이 그룹 유형에서 항목을 선택하면, 적용하는 인수와 키워드가 필터에 즉시 추가됩니다. 키워드가 필터에 이미 있는 경우, 그룹에 해당하는 키워드에 대한 기존 인수를 교체합니다.

  예를 들어 필터 패널의 **Category** 아래에서 **os-linux**를 클릭하면 필터 텍스트 상자에 `Category:"os-linux"`가 추가됩니다. **Category** 아래에서 **os-windows**를 클릭하면 필터가 `Category:"os-windows"`로 바뀝니다.

- Rule Content 아래의 Reference는 키워드이며, 그 아래에 나열된 참조 ID 유형도 마찬가지입니다. 참조 키워드를 선택하면 팝업 창이 나타납니다. 여기서 인수를 제공하면 기존 필터에 키워드가 추가됩니다. 해당 키워드가 필터에서 이미 사용되고 있는 경우, 새로 제공하는 인수가 기존 인수를 교체합니다.

  예를 들어 필터 패널에서 **Rule Content > Reference > CVE ID**를 클릭하면 CVE ID를 입력하라는 팝업 창이 나타납니다. `2007`을 입력하면 필터 텍스트 상자에 `CVE:"2007"`이 추가됩니다. 예를 들어 필터 패널에서 **Rule Content > Reference**를 클릭하면 참조를 입력하라는 팝업 창이 나타납니다. `2007`을 입력하면 필터 텍스트 상자에 `Reference:"2007"`이 추가됩니다.

- 서로 다른 그룹에서 규칙 필터 키워드를 선택하면 각 필터 키워드가 필터에 추가되며 기존 키워드는 유지됩니다(동일한 키워드의 새 값으로 덮어쓰지 않는 한).

  예를 들어 필터 패널의 **Category** 아래에서 **os-linux**를 클릭하면 필터 텍스트 상자에 `Category:"os-linux"`가 추가됩니다. **Microsoft Vulnerabilities** 아래에서 **MS00-006**을 클릭하면 필터는 `Category:"os-linux" MicrosoftVulnerabilities:"MS00-006"`으로 변경됩니다.

- 여러 키워드를 선택하면 시스템에서는 AND 논리를 사용하여 결합한 다음 복합 검색 필터를 생성합니다. 예를 들어 **Category** 아래에서 **preprocessor**를 선택한 다음 **Rule Content > GID**를 선택하고 `116`을 입력하면 `Category: "preprocessor" GID:"116"` 필터가 구성됩니다. 이 필터는 프리프로세서 규칙 **및(and)** GID 116인 모든 규칙을 검색합니다.

- Category, Microsoft Vulnerabilities, Microsoft Worms, Platform Specific 및 Priority 필터 그룹을 사용하면 키워드에 대한 여러 개의 인수를 쉼표로 구분하여 제출할 수 있습니다. 예를 들어 Shift 키를 누르고 **Category**에서 **os-linux** 및 **os-windows**를 선택하면 `Category:"os-windows,app-detect"` 필터가 구성됩니다. 이 필터는 `os-linux` 카테고리 또는 `os-windows` 카테고리의 규칙을 검색합니다.

둘 이상의 필터 키워드/인수 쌍으로 동일한 규칙을 검색할 수 있습니다. 예를 들어 규칙을 **dos** 카테고리로 필터링하면 DOS Cisco 시도 규칙(SID 1545)이 나타나며, **High** 우선순위로 필터링하는 경우에도 마찬가지입니다.

참고 Cisco에서는 규칙 필터를 추가 및 제거하기 위해 규칙 업데이트 메커니즘을 사용할 수 있습니다.

Rules 페이지의 규칙은 공유 객체 규칙(generator ID 3) 또는 표준 텍스트 규칙(generator ID 1)일 수 있습니다. 다음 표에서는 서로 다른 규칙 필터에 대해 설명합니다.

표 32-4 규칙 필터 그룹

필터 그룹	설명	다중인수 지원 여부	제목	목록의 항목
Rule Configuration	규칙의 컨피그레이션에 따라 규칙을 찾습니다. 32-13페이지의 규칙 컨피그레이션 필터 이해을/를 참조하십시오.	아니요	그룹화	키워드
Rule Content	규칙의 내용에 따라 규칙을 찾습니다. 32-15페이지의 규칙 내용 필터 이해을/를 참조하십시오.	아니요	그룹화	키워드
Category	규칙 편집기에 사용되는 규칙 카테고리에 따라 규칙을 찾습니다. 로컬 규칙은 로컬 하위 그룹에 나타납니다. 32-17페이지의 규칙 카테고리 이해을/를 참조하십시오.	예	키워드	인수
Classifications	규칙에 의해 생성된 이벤트의 패킷 표시에 나타나는 공격 분류에 따라 규칙을 찾습니다. 41-42페이지의 침입 이벤트 검색 및 36-12페이지의 침입 이벤트 분류 정의을/를 참조하십시오.	아니요	키워드	인수
Microsoft Vulnerabilities	Microsoft 게시판 번호에 따라 규칙을 찾습니다.	예	키워드	인수
Microsoft Worms	Microsoft Windows 호스트에 영향을 주는 특정 웜을 기반으로 규칙을 찾습니다.	예	키워드	인수
Platform Specific	특정 운영 체제 버전에 대한 연관성에 따라 규칙을 찾습니다. 규칙 하나가 둘 이상의 운영 체제 또는 둘 이상의 운영 체제 버전에 영향을 미칠 수 있습니다. 예를 들어 SID 2260의 활성화는 Mac OS X, IBM AIX 및 기타 운영 체제의 여러 버전에 영향을 미칩니다.	예	키워드	인수 하위 목록에서 항목 중 하나를 선택하면 인수에 수정자가 추가됩니다.
Preprocessors	개별 프리프로세서에 대한 규칙을 찾습니다. 프리프로세서가 활성화되었을 때 옵션에 대한 이벤트를 생성하려면 프리프로세서 옵션과 연결된 프리프로세서 규칙을 활성화해야 합니다. 32-20페이지의 규칙 상태 설정을/를 참조하십시오.	예	그룹화	하위 그룹화
Priority	높음, 중간, 낮음 우선순위에 따라 규칙을 찾습니다. 규칙에 할당된 분류가 우선순위를 결정합니다. 이러한 그룹은 규칙 카테고리로 더 그룹화됩니다. 로컬 규칙(즉, 사용자가 생성하는 규칙)은 우선순위 그룹에 나타나지 않습니다.	예	키워드	인수 하위 목록에서 항목 중 하나를 선택하면 인수에 수정자가 추가됩니다.
Rule Update	특정 규칙 업데이트를 통해 추가 또는 수정된 규칙을 찾습니다. 각 규칙 업데이트에 대해 모든 규칙을 보거나, 가져온 규칙만 보거나, 업데이트에 의해 변경된 기존 규칙만 볼 수 있습니다.	아니요	키워드	인수

규칙 컨피그레이션 필터 이해

라이센스: 보호

Rules 페이지에 나열되는 규칙을 여러 규칙 컨피그레이션 설정으로 필터링할 수 있습니다. 규칙 상태가 권장 규칙 상태와 일치하지 않는 규칙의 집합을 보려면 **Does not match recommendation**을 선택하여 규칙 상태로 필터링할 수 있습니다.

기준 목록의 노드를 클릭하여 키워드를 선택하면 팝업 창이 나타나는데, 여기에서 필터링할 인수를 제공합니다.

해당 키워드가 필터에서 이미 사용되고 있는 경우, 새로 제공하는 인수가 키워드의 기존 인수를 교체합니다.

예를 들어 필터 패널의 **Rule Configuration > Recommendation** 아래에서 **Drop and Generate Events**를 클릭하면 필터 텍스트 상자에 `Recommendation:"Drop and Generate Events"`가 추가됩니다. 그런 다음 **Rule Configuration > Recommendation** 아래에서 **Generate Events**를 클릭하면 필터가 `Recommendation:"Generate Events"`로 변경됩니다.

필터링하기 위해 사용할 수 있는 규칙 컨피그레이션 설정에 대한 자세한 내용은 다음 절차를 참조하십시오.

Rule State 필터를 사용하려면

액세스: Admin/Intrusion Admin

1단계 **Rule Configuration** 아래에서 **Rule State**를 클릭합니다.

2단계 **Rule State** 드롭다운 목록에서 필터링할 규칙 상태를 선택합니다.

- 이벤트를 생성하기만 하는 규칙을 찾으려면 **Generate Events**를 선택하고 **OK**를 클릭합니다.
- 이벤트를 생성하고 일치하는 패킷을 삭제하도록 설정된 규칙을 찾으려면 **Drop and Generate Events**를 선택하고 **OK**를 클릭합니다.
- 비활성화된 규칙을 찾으려면 **Disabled**를 선택하고 **OK**를 클릭합니다.
- 규칙 상태가 권장 상태와 일치하지 않는 규칙을 찾으려면 **Does not match recommendation**을 선택한 다음 **OK**를 클릭합니다.

현재 규칙 상태에 따라 규칙을 표시하도록 Rules 페이지가 업데이트됩니다.

Recommendation 필터를 사용하려면

액세스: Admin/Intrusion Admin

1단계 **Rule Configuration** 아래에서 **Recommendation**을 클릭합니다.

2단계 **Recommendation** 드롭다운 목록에서 필터링할 FireSIGHT 규칙 상태 권장 사항을 선택한 다음 **OK**를 클릭합니다.

권장 규칙 상태에 따라 규칙을 표시하도록 Rules 페이지가 업데이트됩니다.

Threshold 필터를 사용하려면

액세스: Admin/Intrusion Admin

1단계 **Rule Configuration** 아래에서 **Threshold**를 클릭합니다.

2단계 **Threshold** 드롭다운 목록에서 필터링할 임계값 설정을 선택합니다.

- 임계값 유형 `limit`의 규칙을 찾으려면 **Limit**를 선택한 다음 **OK**를 클릭합니다.
- 임계값 유형 `threshold`의 규칙을 찾으려면 **Threshold**를 선택한 다음 **OK**를 클릭합니다.
- 임계값 유형 `both`의 규칙을 찾으려면 **Both**를 선택한 다음 **OK**를 클릭합니다.
- `source`에 의해 추적되는 임계값으로 규칙을 찾으려면 **Source**를 선택한 다음 **OK**를 클릭합니다.
- `destination`에 의해 추적되는 임계값으로 규칙을 찾으려면 **Destination**을 선택한 다음 **OK**를 클릭합니다.
- 임계값 설정으로 규칙을 찾으려면 **All**을 선택한 다음 **OK**를 클릭합니다.

Rules 페이지가 업데이트되면서 필터에 나타난 임계값 유형이 적용된 규칙이 표시됩니다.

Suppression 필터를 사용하려면

액세스: Admin/Intrusion Admin

1단계 **Rule Configuration** 아래에서 **Suppression**을 클릭합니다.

2단계 **Suppression** 드롭다운 목록에서 필터링할 억제 설정을 선택합니다.

- 이벤트가 해당 규칙으로 조사된 패킷에 대해 억제된 규칙을 찾으려면 **By Rule**을 선택한 다음 **OK**를 클릭합니다.
- 이벤트가 트래픽의 소스를 기반으로 억제된 규칙을 찾으려면 **By Source**를 선택한 다음 **OK**를 클릭합니다.
- 트래픽의 목적지를 기반으로 이벤트가 억제된 규칙을 찾으려면 **By Destination**을 선택한 다음 **OK**를 클릭합니다.
- 억제 설정으로 규칙을 찾으려면 **All**을 선택한 다음 **OK**를 클릭합니다.

Rules 페이지가 업데이트되면서 필터에 나타난 억제 유형이 적용된 규칙이 표시됩니다.

Dynamic State 필터를 사용하려면

액세스: Admin/Intrusion Admin

1단계 **Rule Configuration** 아래에서 **Dynamic State**를 클릭합니다.

2단계 **Dynamic State** 드롭다운 목록에서 필터링할 억제 설정을 선택합니다.

- 동적 상태가 해당 규칙으로 조사된 패킷에 대해 구성된 규칙을 찾으려면 **By Rule**을 선택한 다음 **OK**를 클릭합니다.
- 동적 상태가 트래픽의 소스를 기반으로 패킷에 대해 구성된 규칙을 찾으려면 **By Source**를 선택한 다음 **OK**를 클릭합니다.
- 동적 상태가 트래픽의 목적지를 기반으로 구성된 규칙을 찾으려면 **By Destination**을 선택한 다음 **OK**를 클릭합니다.

- Generate Events의 동적 상태가 구성된 규칙을 찾으려면 **Generate Events**를 선택한 다음 **OK**를 클릭합니다.
- Drop and Generate Events의 동적 상태가 구성된 규칙을 찾으려면 **Drop and Generate Events**를 선택한 다음 **OK**를 클릭합니다.
- Disabled의 동적 상태가 구성된 규칙을 찾으려면 **Disabled**를 선택한 다음 **OK**를 클릭합니다.
- 억제 설정으로 규칙을 찾으려면 **All**을 선택한 다음 **OK**를 클릭합니다.

Rules 페이지가 업데이트되면서 필터에 나타난 동적 규칙 상태가 적용된 규칙이 표시됩니다.

Alert 필터를 사용하려면

액세스: Admin/Intrusion Admin

1단계 **Rule Configuration** 아래에서 **Alert**를 클릭합니다.

2단계 **Alert** 드롭다운 목록에서 필터링할 알림 설정(**SNMP**)을 선택합니다.

3단계 **OK**를 클릭합니다.

Rules 페이지가 업데이트되어 알림 필터가 적용된 규칙이 표시됩니다.

Comment 필터를 사용하려면

액세스: Admin/Intrusion Admin

1단계 **Rule Configuration** 아래에서 **Comment**를 클릭합니다.

2단계 필터링할 코멘트 텍스트 문자열을 **Comment** 필드에 입력한 다음 **OK**를 클릭합니다.

Rules 페이지가 업데이트되어 규칙에 적용된 코멘트가 필터에 표시된 문자열을 포함하는 규칙이 표시됩니다.

규칙 내용 필터 이해

라이센스: 보호

Rules 페이지에 나열되는 규칙을 여러 규칙 내용 항목으로 필터링할 수 있습니다. 예를 들어 규칙의 SID를 사용하여 규칙을 빠르게 검색할 수 있습니다. 또한 특정 목적지 포트로 가는 트래픽을 검사하는 모든 규칙을 찾을 수 있습니다.

기준 목록의 노드를 클릭하여 키워드를 선택하면 팝업 창이 나타나는데, 여기에서 필터링할 인수를 제공합니다.

해당 키워드가 필터에서 이미 사용되고 있는 경우, 새로 제공하는 인수가 키워드의 기존 인수를 교체합니다.

예를 들어 필터 패널의 **Rule Content** 아래에서 **SID**를 클릭하면 SID를 입력하라는 팝업 창이 나타납니다. 1045를 입력하면 필터 텍스트 상자에 SID:"1045"가 추가됩니다. 그런 다음 **SID**를 다시 클릭하고 SID 필터를 1044로 변경하면 필터가 SID:"1044"로 바뀝니다.

필터링에 사용할 수 있는 규칙 내용에 대해 자세히 알아보려면 다음 표를 참조하십시오.

표 32-5 규칙 내용 필터

사용할 필터	수행할 작업	결과
Message	필터링할 메시지 문자열을 입력하고 **OK**를 클릭합니다.	메시지 필드에 제공된 문자열을 포함하는 규칙을 찾습니다.
SID	필터링할 SID 번호를 입력하고 **OK**를 클릭합니다.	지정된 SID가 있는 규칙을 찾습니다.
GID	필터링할 GID 번호를 입력하고 **OK**를 클릭합니다.	지정된 GID가 있는 규칙을 찾습니다.
Reference	필터링할 참조 문자열을 입력하고 **OK**를 클릭합니다. 필터링할 특정 참조 유형에 대한 문자열을 입력하려면 **CVE ID**, **URL**, **Bugtraq ID**, **Nessus ID**, **Arachnids ID** 또는 **Mcafee ID**를 선택한 다음 문자열을 입력하고 **OK**를 클릭합니다.	참조 필드에 제공된 문자열을 포함하는 규칙을 찾습니다.
Action	필터링할 작업을 선택합니다. • 알림 규칙을 찾으려면 **Alert**를 선택하고 **OK**를 클릭합니다. • 통과 규칙을 찾으려면 **Pass**를 선택하고 **OK**를 클릭합니다.	`alert` 또는 `pass`로 시작되는 규칙을 찾습니다.
Protocol	필터링할 프로토콜 **ICMP**, **IP**, **TCP** 또는 **UDP**를 선택한 다음 **OK**를 클릭합니다.	선택한 프로토콜을 포함하는 규칙을 찾습니다.
Direction	필터링할 방향 설정을 선택합니다. • 특정 방향으로 이동하는 트래픽을 검사하는 규칙을 찾으려면 **Directional**을 선택한 다음 **OK**를 클릭합니다. • 소스와 목적지 간 양방향으로 이동하는 트래픽을 검사하는 규칙을 찾으려면 **Bidirectional**을 선택한 다음 **OK**를 클릭합니다.	규칙에 표시된 방향 설정이 포함되어 있는지를 기반으로 규칙을 찾습니다.
Source IP	필터링할 소스 IP 주소를 입력하고 **OK**를 클릭합니다. 유효한 IP 주소, CIDR 불록/접두사 길이로 필터링하거나 `$HOME_NET` 또는 `$EXTERNAL_NET` 같은 변수를 사용하여 필터링할 수 있습니다.	규칙에서 소스 IP 주소 지정에 특정 주소나 변수를 사용하는 규칙을 찾습니다.
Destination IP	필터링할 목적지 IP 주소를 입력하고 **OK**를 클릭합니다. 유효한 IP 주소, CIDR 불록/접두사 길이로 필터링하거나 `$HOME_NET` 또는 `$EXTERNAL_NET` 같은 변수를 사용하여 필터링할 수 있습니다.	규칙에서 소스 IP 주소 지정에 특정 주소나 변수를 사용하는 규칙을 찾습니다.

표 32-5 규칙 내용 필터(계속)

사용할 필터	수행할 작업	결과
Source port	필터링할 소스 포트를 입력하고 **OK**를 클릭합니다. 값은 1과 65535 사이의 정수 또는 포트 변수여야 합니다.	지정된 소스 포트를 포함하는 규칙을 찾습니다.
Destination port	필터링할 목적지 포트를 입력하고 **OK**를 클릭합니다. 값은 1과 65535 사이의 정수 또는 포트 변수여야 합니다.	지정된 목적지 포트를 포함하는 규칙을 찾습니다.
Rule Overhead	**Low**, **Medium**, **High** 또는 **Very High**로 필터링할 규칙 오버헤드의 양을 선택하고 **OK**를 클릭합니다.	선택한 규칙 오버헤드의 규칙을 찾습니다.
Metadata	필터링할 메타데이터 키-값 쌍을 공백으로 구분하여 입력한 다음 **OK**를 클릭합니다. 예를 들어 HTTP 애플리케이션 프로토콜과 관련된 메타데이터로 규칙을 찾으려면 `metadata:"service http"`를 입력합니다.	일치하는 키-값 쌍을 포함하는 메타데이터로 규칙을 찾습니다.

규칙 카테고리 이해

라이센스: 보호

FireSIGHT 시스템은 규칙이 탐지하는 트래픽의 유형을 기반으로 카테고리에 규칙을 배치합니다. Rules 페이지에서 규칙 카테고리로 필터링하여, 한 카테고리의 모든 규칙에 대해 규칙 속성을 설정할 수 있습니다. 예를 들어 네트워크에 Linux 호스트가 없으면 **os-linux** 카테고리로 필터링한 다음, 표시되는 모든 규칙을 비활성화하여 전체 **os-linux** 카테고리를 비활성화할 수 있습니다.

포인터를 카테고리 이름 위로 이동하면 해당 카테고리의 규칙 수가 표시됩니다.

참고 Cisco에서는 규칙 카테고리를 추가 및 제거하기 위해 규칙 업데이트 메커니즘을 사용할 수 있습니다.

규칙 필터 직접 수정

라이센스: 보호

필터 패널에서 필터를 클릭할 때 제공되는 특수 키워드 및 해당 인수를 변경하려면 필터를 수정할 수 있습니다. Rules 페이지의 사용자 지정 필터는 규칙 편집기에서 사용되는 것과 유사하게 작동하지만, 필터 패널을 통해 필터를 선택할 때 표시되는 구문을 사용하여 Rules 페이지 필터에서 제공하는 키워드를 사용할 수 있습니다. 나중에 사용할 키워드를 결정하려면 필터 패널 오른쪽에서 적절한 인수를 클릭합니다. 필터 텍스트 상자에 필터 키워드와 인수 구문이 나타납니다.

특정 값만 지원하는 키워드의 인수 목록을 보려면 32-13페이지의 규칙 컨피그레이션 필터 이해, 32-15페이지의 규칙 내용 필터 이해 및 32-17페이지의 규칙 카테고리 이해을/를 참조하십시오. 키워드에 대한 쉼표로 구분된 다중 인수는 Category 및 Priority 필터 유형에 대해서만 지원됩니다.

키워드와 인수, 문자 문자열, 따옴표의 리터럴 문자 문자열을 사용할 수 있으며 여러 필터 조건을 공백으로 구분할 수 있습니다. 필터에는 정규식이나 와일드카드 문자 또는 부정 문자(!), 보다 큼 기호(>), 보다 작음 기호(<) 등의 특수 연산자를 포함할 수 없습니다. 키워드 없이, 키워드의 첫 글자 대문자 없이 또는 인수 앞뒤의 따옴표 없이 검색할 용어를 입력하면 검색은 문자열 검색으로 처리되며, 지정된 용어가 카테고리, 메시지 및 SID 필드에서 검색됩니다.

모든 키워드, 키워드 인수 및 문자 문자열은 대/소문자를 구분하지 않습니다. `gid` 및 `sid` 키워드를 제외하고 모든 인수 및 문자열은 부분 문자열로 취급됩니다. `gid` 및 `sid`에 대한 인수는 정확한 일치 항목만 반환합니다.

각 규칙 필터는 다음과 같은 형식으로 하나 이상의 키워드를 포함할 수 있습니다.

Keyword:"*argument*"

여기서 *keyword*는 규칙 유형 표에서 설명한 키워드 그룹의 키워드 중 하나이며 *argument*는 키워드와 관련된 하나 이상의 특정 필드에서 검색할, 대/소문자를 구분하지 않는 단일 영숫자 문자열로서 큰따옴표로 둘러싸입니다. 키워드의 첫 글자는 대문자로 입력해야 합니다.

`gid` 및 `sid`를 제외한 모든 키워드의 인수는 부분 문자열로 취급됩니다. 예를 들어 인수 `123`은 `"12345"`, `"41235"`, `"45123"` 등을 반환합니다. `gid` 및 `sid`에 대한 인수는 정확한 일치 항목만 반환합니다. 예를 들어 `sid:3080`은 `SID 3080`만 반환합니다.

각 규칙 필터는 또한 하나 이상의 영숫자 문자 문자열을 포함할 수 있습니다. 문자 문자열은 규칙 Message 필드, Signature ID 및 Generator ID를 검색합니다. 예를 들어 문자열 `123`은 규칙 메시지에 있는 `"Lotus123"`, `"123mania"` 등의 문자열을 반환하며 `SID 6123`, `SID 12375` 등도 반환합니다. 규칙 Message 필드에 대한 자세한 내용은 36-11페이지의 이벤트 메시지 정의을/를 참조하십시오. 규칙 SID 및 GID에 대한 자세한 내용은 41-40페이지의 프리프로세서 Generator ID 읽기을/를 참조하십시오. 하나 이상의 문자 문자열로 필터링하여 부분 SID를 검색할 수 있습니다.

모든 문자 문자열은 대/소문자를 구분하지 않으며 부분 문자열로 취급됩니다. 예를 들어 `ADMIN`, `admin` 또는 `Admin` 문자열은 `"admin"`, `"CFADMIN"`, `"Administrator"` 등을 반환합니다.

정확한 일치 항목을 반환하려면 문자 문자열을 따옴표로 감쌀 수 있습니다. 예를 들어 따옴표로 감싼 리터럴 문자열 `"overflow attempt"`는 정확한 문자열만을 반환하는 반면, 따옴표 없이 `overflow` 및 `attempt`의 두 문자열로 구성된 필터는 `"overflow attempt"`, `"overflow multipacket attempt"`, `"overflow with evasion attempt"` 등을 반환합니다.

키워드, 문자 문자열 또는 둘 모두의 임의의 조합을 공백으로 구분하여 입력함으로써 필터링 결과의 범위를 좁힐 수 있습니다. 모든 필터 조건과 일치하는 규칙이 결과에 포함됩니다.

원하는 순서로 여러 필터 조건을 입력할 수 있습니다. 다음의 각 필터는 동일한 규칙을 반환합니다.

- `url:at login attempt cve:200`
- `login attempt cve:200 url:at`
- `login cve:200 attempt url:at`

침입 정책에서 규칙 필터 설정

라이센스: 보호

규칙의 하위 집합을 표시하려면 Rule 페이지에서 규칙을 필터링할 수 있습니다. 그런 다음 컨텍스트 메뉴에서 사용 가능한 기능 선택을 포함하여 원하는 페이지 기능을 사용할 수 있습니다. 이 기능은 예를 들어 특정 카테고리의 모든 규칙에 대해 임계값을 설정하고자 할 때 유용할 수 있습니다. 필터링된 목록 또는 필터링되지 않은 목록에서 규칙에 동일한 기능을 사용할 수 있습니다. 예를 들어 필터링된 목록 또는 필터링되지 않은 목록에서 규칙에 새 규칙 상태를 적용할 수 있습니다.

침입 정책의 Rules 페이지 왼쪽에 있는 필터 패널에서 사전 정의된 필터 키워드를 선택할 수 있습니다. 필터를 선택하면 페이지에 모든 일치하는 규칙이 표시되거나 일치하는 규칙이 없음이 표시됩니다.

사용할 수 있는 모든 키워드와 인수 및 필터 패널에서 필터를 구성하는 방법에 대한 자세한 내용은 32-10페이지의 침입 정책의 규칙 필터링 이해을/를 참조하십시오.

추가로 제한하려면 필터에 키워드를 추가할 수 있습니다. 입력한 필터는 전체 규칙 데이터베이스를 검색하며 일치하는 모든 규칙을 반환합니다. 페이지에 이전 필터의 결과가 표시되어 있는 상태에서 필터를 입력하면, 페이지가 지워지고 새 필터의 결과가 대신 반환됩니다.

필터를 선택할 때 제공된 동일한 키워드 및 인수 구문을 사용하여 필터를 입력할 수도 있고, 선택한 후 필터에서 인수 값을 수정할 수도 있습니다. 키워드 없이, 키워드의 첫 글자 대문자 없이 또는 인수 앞뒤의 따옴표 없이 검색할 용어를 입력하면 검색은 문자열 검색으로 처리되며, 지정된 용어가 카테고리, 메시지 및 SID 필드에서 검색됩니다.

침입 정책에서 특정 규칙을 필터링하려면

액세스: Admin/Intrusion Admin

1단계 **Policies > Intrusion > Intrusion Policy**를 선택합니다.

Intrusion Policy 페이지가 나타납니다.

2단계 수정할 정책 옆에 있는 수정 아이콘( )을 클릭합니다.

다른 정책에 저장하지 않은 변경 사항이 있는 경우 변경 사항을 취소하고 계속 진행하려면 **OK**를 클릭합니다. 저장하지 않은 변경 사항을 다른 정책에 저장하는 방법에 대한 자세한 내용은 23-15페이지의 충돌 해결 및 정책 변경 사항 커밋을/를 참조하십시오.

Policy Information 페이지가 나타납니다.

3단계 **Rules**를 클릭합니다.

Rules 페이지가 나타납니다. 기본적으로 페이지에는 규칙이 메시지별 알파벳순으로 나열됩니다.

4단계 왼쪽에 있는 필터 패널에서 키워드나 인수를 클릭하여 필터를 구성합니다. 필터에 이미 있는 키워드에 대한 인수를 클릭하면 기존 인수가 교체됩니다. 자세한 내용은 다음 링크을/를 참조하십시오.

- 32-10페이지의 침입 정책 규칙 필터 구성을 위한 지침
- 32-13페이지의 규칙 컨피그레이션 필터 이해
- 32-15페이지의 규칙 내용 필터 이해
- 32-17페이지의 규칙 카테고리 이해
- 32-17페이지의 규칙 필터 직접 수정

페이지가 새로 고쳐지고 일치하는 모든 규칙이 표시되며, 필터와 일치하는 규칙의 수가 필터 텍스트 상자 위에 표시됩니다.

5단계 새 설정을 적용하고자 하는 규칙을 선택합니다. 다음 옵션을 이용할 수 있습니다.

- 특정 규칙을 선택하려면 규칙 옆에 있는 확인란을 선택합니다.
- 현재 목록의 모든 규칙을 선택하려면 열 맨 위에 있는 확인란을 선택합니다.

6단계 선택적으로, 페이지에서 일반적으로 하는 것처럼 규칙을 변경합니다. 자세한 내용은 다음 절을 참조하십시오.

- Rules 페이지에서 규칙을 활성화 및 비활성화하는 방법에 대한 자세한 내용은 32-20페이지의 규칙 상태 설정을/를 참조하십시오.
- 규칙에 임계값과 억제를 추가하는 방법에 대한 자세한 내용은 32-22페이지의 정책당 침입 이벤트 알림 필터링을/를 참조하십시오.
- 일치하는 트래픽에서 속도 변칙이 발생할 때 트리거되는 동적 규칙 상태 설정에 대한 자세한 내용은 32-29페이지의 동적 규칙 상태 추가을/를 참조하십시오.

- 특정 규칙에 SNMP 알림을 추가하는 방법에 대한 자세한 내용은 32-33페이지의 SNMP 알림 추가을/를 참조하십시오.
- 규칙 코멘트를 규칙에 추가하는 방법에 대한 자세한 내용은 32-34페이지의 규칙 코멘트 추가을/를 참조하십시오.

7단계 정책을 저장하거나, 계속 수정하거나, 변경 사항을 취소하거나, 시스템 캐시에 변경 사항이 남아 있는 상태로 종료합니다.

자세한 내용은 31-3페이지의 침입 정책 관리 및 31-4페이지의 침입 정책 수정을/를 참조하십시오.

규칙 상태 설정

라이센스: 보호

Cisco VRT(Vulnerability Research Team)는 각 기본 정책에서 각 침입 및 프리프로세서 규칙의 기본 상태를 설정합니다. 예를 들어 Security over Connectivity 기본 정책에서는 규칙을 활성화하고 Connectivity over Security 기본 정책에서는 규칙을 비활성화할 수 있습니다. 생성하는 침입 정책 규칙은 정책을 생성하기 위해 사용하는 기본 정책에 있는 규칙의 기본 상태를 상속합니다.

Generate Events, Drop and Generate Events 또는 Disable에 대해 개별적으로 규칙을 설정하거나, 다양한 요소로 규칙을 필터링하여 상태를 수정할 규칙을 선택할 수 있습니다. 인라인 구축에서 인라인 침입 구축의 Drop and Generate Events 규칙 상태를 사용하여 악의적인 패킷을 삭제할 수 있습니다. Drop and Generate Events 규칙 상태의 규칙은 이벤트를 생성하지만, 3D9900 또는 Series 3 디바이스 인라인 인터페이스 집합이 탭 모드에 있는 경우를 비롯하여 패시브 구축에서 패킷을 삭제하지 않습니다. 규칙을 Generate Events 또는 Drop and Generate Events로 설정하면 규칙이 활성화되고, 규칙을 Disable로 설정하면 규칙이 비활성화됩니다.

두 가지 시나리오를 생각해볼 수 있습니다. 첫 번째 시나리오에서 특정 규칙에 대한 규칙 상태는 Generate Events로 설정됩니다. 악의적인 패킷이 네트워크를 이동하여 규칙을 트리거하면 규칙이 목적지로 전송되고 시스템이 침입 이벤트를 생성합니다. 두 번째 시나리오에서는 동일한 규칙에 대한 규칙 상태가 인라인 구축에서 Drop and Generate Events로 설정됩니다. 이 경우 악의적인 패킷이 네트워크를 이동하면 시스템은 이를 삭제하고 침입 이벤트를 생성합니다. 패킷은 대상에 도달하지 못합니다.

침입 정책에서 규칙의 상태를 다음 중 하나로 설정할 수 있습니다.

- 시스템이 특정 침입 시도를 탐지하고 일치하는 트래픽을 찾을 경우 침입 이벤트를 생성하도록 하려면 규칙 상태를 **Generate Events**로 설정합니다.
- 시스템이 특정 침입 시도를 탐지한 다음 인라인 구축의 일치하는 트래픽을 발견하면 공격을 포함하는 패킷을 삭제하고 침입 이벤트를 생성하며, 패시브 구축(3D9900 또는 Series 3 디바이스 인라인 인터페이스 집합이 탭 모드인 경우 포함)의 일치하는 트래픽을 발견하면 침입 이벤트를 생성하도록 하려면 규칙 상태를 **Drop and Generate Events**로 설정합니다.

  시스템이 패킷을 삭제하도록 하려면 인라인 구축에서 규칙을 삭제하도록 침입 정책을 설정해야 합니다. 자세한 내용은 31-6페이지의 인라인 구축에서 삭제 동작 설정을/를 참조하십시오.
- 시스템이 일치하는 트래픽을 평가하지 않도록 하려면 규칙 상태를 **Disable**로 설정합니다.

삭제 규칙을 사용하려면 다음과 같이 해야 합니다.

- 침입 정책에서 **Drop when Inline** 옵션을 활성화합니다.
- 규칙과 일치하는 모든 패킷을 삭제해야 하는 규칙에 대해 규칙 상태를 **Drop and Generate Events**로 설정합니다.
- 침입 정책과 관련된 액세스 제어 규칙을 포함하는 액세스 제어 정책을 인라인 집합을 사용하는 관리되는 디바이스에 적용합니다.

Rules 페이지에서 규칙을 필터링하면 삭제 규칙으로 설정할 규칙을 찾는 데 도움이 될 수 있습니다. 자세한 내용은 32-10페이지의 침입 정책의 규칙 필터링을/를 참조하십시오.

규칙 구조, 규칙 키워드와 옵션, 규칙 작성 구문에 대한 자세한 내용은 36-1페이지의 침입 규칙 이해 및 작성을/를 참조하십시오.

VRT에서는 때때로 규칙 업데이트를 사용하여 기본 정책에 있는 하나 이상의 규칙의 기본 상태를 변경합니다. 규칙 업데이트가 기반 정책을 업데이트하도록 허용하면, 정책을 생성하기 위해 사용한 기본 정책(또는 기반으로 하는 기본 정책)에서 기본 상태가 변경될 때 정책에 있는 규칙의 기본 상태를 변경하는 것도 허용됩니다. 그러나 규칙 상태를 변경한 경우 규칙 업데이트가 변경 사항을 재정의하지 않습니다.

하나 이상의 규칙의 규칙 상태를 변경하려면

액세스: Admin/Intrusion Admin

1단계 **Policies > Intrusion > Intrusion Policy**를 선택합니다.

Intrusion Policy 페이지가 나타납니다.

2단계 수정할 정책 옆에 있는 수정 아이콘( )을 클릭합니다.

다른 정책에 저장하지 않은 변경 사항이 있는 경우 변경 사항을 취소하고 계속 진행하려면 **OK**를 클릭합니다. 저장하지 않은 변경 사항을 다른 정책에 저장하는 방법에 대한 자세한 내용은 23-15페이지의 충돌 해결 및 정책 변경 사항 커밋을/를 참조하십시오.

Policy Information 페이지가 나타납니다.

이 페이지에는 활성화된 총 규칙 수, Generate Events로 설정된 활성화된 총 규칙 수, Drop and Generate Events로 설정된 총 규칙 수가 표시됩니다. 패시브 구축에서는 Drop and Generate Events로 설정된 규칙만이 이벤트를 생성합니다.

3단계 **Rules**를 클릭합니다.

Rules 페이지가 나타납니다. 기본적으로 페이지에는 규칙이 메시지별 알파벳순으로 나열됩니다.

4단계 규칙 상태를 설정하고자 하는 규칙을 찾습니다. 다음 옵션을 이용할 수 있습니다.

- 현재 표시를 정렬하려면 열 머리글이나 아이콘을 클릭합니다. 정렬 순서를 반대로 하려면 다시 클릭합니다.
- 왼쪽에 있는 필터 패널에서 키워드나 인수를 클릭하여 필터를 구성합니다. 자세한 내용은 32-10페이지의 침입 정책의 규칙 필터링 이해 및 32-18페이지의 침입 정책에서 규칙 필터 설정 항목을 참조하십시오.

  페이지가 새로 고쳐지고 일치하는 모든 규칙이 표시됩니다.

5단계 규칙 상태를 설정하고자 하는 규칙을 선택합니다. 다음 옵션을 이용할 수 있습니다.

- 특정 규칙을 선택하려면 규칙 옆에 있는 확인란을 선택합니다.
- 현재 목록의 모든 규칙을 선택하려면 열 맨 위에 있는 확인란을 선택합니다.

6단계 다음 옵션을 이용할 수 있습니다.

- 트래픽이 선택한 규칙과 일치하는 경우 이벤트를 생성하려면 **Rule State > Generate Events**를 선택합니다.
- 트래픽이 선택한 규칙과 일치하는 경우 이벤트를 생성하고 인라인 구축에서 트래픽을 삭제하려면 **Rule State > Drop and Generate Events**를 선택합니다.
- 선택한 규칙과 일치하는 트래픽을 검사하지 않으려면 **Rule State > Disable**을 선택합니다.

참고 Cisco에서는 침입 정책에서 모든 침입 규칙을 활성화하지는 **않을** 것을 **적극** 권장합니다. 모든 규칙이 활성화될 경우 관리되는 디바이스의 성능이 저하될 수 있습니다. 대신 네트워크 환경과 가능한 한 일치하도록 규칙 설정을 조정하십시오.

7단계 정책을 저장하거나, 계속 수정하거나, 변경 사항을 취소하거나, 시스템 캐시에 변경 사항이 남아 있는 상태로 종료합니다. 자세한 내용은 31-3페이지의 침입 정책 관리 및 31-4페이지의 침입 정책 수정을/를 참조하십시오.

정책당 침입 이벤트 알림 필터링

라이센스: 보호

침입 이벤트의 중요성은 발생 빈도 또는 소스나 목적지 IP 주소를 기반으로 할 수 있습니다. 어떤 경우에는 특정 횟수가 발생할 때까지 이벤트에 대해 신경 쓰지 않아도 됩니다. 예를 들어, 어떤 사용자가 서버에 로그인을 시도하는 경우 특정 횟수만큼 실패할 때까지는 염려하지 않아도 됩니다. 다른 경우에는 소수의 발생 상황만 확인해도 광범위한 문제의 존재 여부를 파악할 수 있습니다. 예를 들어 웹 서버에 대해 DoS 공격이 시작된 경우, 상황을 해결해야 하는지를 파악하려면 침입 이벤트의 발생 상황을 몇 번만 확인해보면 됩니다. 동일한 이벤트를 수백 번 확인하면 시스템에 부담을 줄 뿐입니다.

자세한 내용은 다음 절을 참조하십시오.

- 32-22페이지의 이벤트 임계값 구성 - 발생 횟수를 기반으로, 이벤트가 표시되는 빈도를 나타내는 임계값을 설정하는 방법에 대해 설명합니다. 이벤트당 및 정책당 임계값을 구성할 수 있습니다.
- 32-26페이지의 침입 정책당 억제 구성 - 소스/목적지 IP 주소당, 정책당 지정된 이벤트의 알림을 억제하는 방법에 대해 설명합니다.

이벤트 임계값 구성

라이센스: 보호

지정된 기간 내 이벤트 생성 횟수를 기반으로 시스템이 침입 이벤트를 로깅 및 표시하는 횟수를 제한하도록 침입 정책당 개별 규칙에 대한 임계값을 설정할 수 있습니다. 이렇게 하면 동일한 이벤트 수가 너무 많아서 혼란스러워지는 상황을 피할 수 있습니다. 임계값을 공유 객체 규칙, 표준 텍스트 규칙 또는 프리프로세서 규칙당 설정할 수 있습니다.

자세한 내용은 다음 절을 참조하십시오.

- 32-23페이지의 이벤트 임계값 이해
- 32-24페이지의 침입 이벤트 임계값 추가 및 수정
- 32-25페이지의 침입 이벤트 임계값 보기 및 삭제
- 32-6페이지의 규칙에 대해 임계값 설정

이벤트 임계값 이해

라이센스: 보호

먼저 임계값 유형을 지정해야 합니다. 다음 표에서 설명하는 옵션 중에서 선택할 수 있습니다.

표 32-6 임계값 옵션

옵션	설명
Limit	지정된 기간 중 규칙을 트리거하는 지정된 패킷 수(Count 인수로 지정)에 대한 이벤트를 로깅 및 표시합니다. 예를 들어 유형을 **Limit**, **Count**를 10, **Seconds**를 60으로 설정한 경우 14개 패킷으로 규칙이 트리거되면 시스템은 지정된 기간 내 발생하는 처음 10개를 표시한 후 규칙에 대한 이벤트 로깅을 중지합니다.
Threshold	지정된 기간 중 지정된 패킷 수(Count 인수로 지정)가 규칙을 트리거하면 단일 이벤트를 로깅 및 표시합니다. 이벤트의 임계값 카운트에 도달하고 시스템이 해당 이벤트를 로깅하면 시간에 대한 카운터가 다시 시작됩니다. 예를 들어 유형을 **Threshold**, **Count**를 10, **Seconds**를 60으로 설정했는데, 33초에 10회 규칙이 트리거됩니다. 시스템은 이벤트를 한 번 생성한 다음 Seconds 및 Count 카운터를 0으로 재설정합니다. 다음 25초에 10회가 더 발생하면 규칙이 트리거됩니다. 33초에 카운터가 0으로 재설정되므로 시스템은 또 다른 이벤트를 로깅합니다.
Both	지정된 패킷 수(카운트)가 규칙을 트리거한 후 지정된 기간당 한 번 이벤트를 로깅 및 표시합니다. 예를 들어 유형을 **Both**, **Count**를 2, **Seconds**를 10으로 설정하면 이벤트 카운트는 다음과 같습니다. • 10초에 한 번 규칙이 트리거되면 시스템은 이벤트를 생성하지 않습니다(임계값이 충족되지 않음). • 규칙이 10초에 두 번 트리거되면 시스템은 이벤트를 한 번 생성합니다(규칙이 두 번째 트리거될 때 임계값이 충족됨). • 규칙이 10초에 네 번 트리거되면 시스템은 이벤트를 한 번 생성합니다(규칙이 두 번째 트리거될 때 임계값이 충족되고 이후 이벤트는 무시됨).

다음으로 추적을 지정합니다. 이는 이벤트 임계값을 소스 IP 주소당 계산할지, 목적지 IP 주소당 계산할지를 결정합니다. 시스템이 이벤트 인스턴스를 추적하는 방법을 지정하려면 다음 표의 옵션 중 하나를 선택합니다.

표 32-7 임계값 IP 옵션

옵션	설명
Source	소스 IP 주소당 이벤트 인스턴스 수를 계산합니다.
Destination	목적지 IP 주소당 이벤트 인스턴스 수를 계산합니다.

마지막으로, 임계값을 정의하는 인스턴스 수 및 기간을 지정해야 합니다.

표 32-8 임계값 지정 인스턴스/시간 옵션

옵션	설명
Count	임계값 충족에 필요한 추적 IP 주소당 지정된 기간의 이벤트 인스턴스 수.
Seconds	카운트가 재설정될 때까지 경과하는 시간(초). 임계값 유형을 **limit**, 추적을 **Source IP**, **count**를 10, **seconds**를 10으로 설정하면 시스템은 지정된 소스 포트에서 10초간 발생하는 처음 10개 이벤트를 로깅 및 표시합니다. 처음 10초간 이벤트가 7개만 발생하면 시스템은 이를 로깅 및 표시하고, 처음 10초간 이벤트가 40개 발생하면 시스템은 10개만 로깅 및 표시한 다음 10초 기간 경과 후 카운팅을 다시 시작합니다.

침입 이벤트 임계값만 사용할 수도 있고 속도 기반 공격 방지, `detection_filter` 키워드 및 침입 이벤트 억제를 조합하여 사용할 수도 있습니다. 자세한 내용은 32-29페이지의 동적 규칙 상태 추가, 36-89페이지의 이벤트 필터링 및 32-26페이지의 침입 정책당 억제 구성을/를 참조하십시오.

자세한 내용은 다음 절을 참조하십시오.

- 32-24페이지의 침입 이벤트 임계값 추가 및 수정
- 32-6페이지의 규칙에 대해 임계값 설정
- 32-25페이지의 침입 이벤트 임계값 보기 및 삭제

팁 침입 이벤트의 패킷 보기 내에서 임계값을 추가할 수도 있습니다. 자세한 내용은 41-24페이지의 이벤트 정보 보기을/를 참조하십시오.

침입 이벤트 임계값 추가 및 수정

라이센스: 보호

하나 이상의 특정 규칙에 대해 임계값을 설정할 수 있습니다. 기존 임계값 설정을 별도로 또는 동시에 수정할 수도 있습니다. 각각에 대해 단일 임계값을 설정할 수 있습니다. 임계값을 추가하면 규칙에 대한 기존 임계값을 덮어씁니다.

임계값 컨피그레이션을 보고 삭제하는 방법에 대한 자세한 내용은 32-25페이지의 침입 이벤트 임계값 보기 및 삭제을/를 참조하십시오.

모든 규칙 및 프리프로세서 생성 이벤트에 의해 적용되는 전역 임계값을 수정할 수도 있습니다. 자세한 내용은 35-1페이지의 전체적으로 침입 이벤트 로깅 제한을/를 참조하십시오.

잘못된 값을 입력하면 필드에 되돌리기 아이콘()이 나타납니다. 이 아이콘을 클릭하면 해당 필드에 대한 마지막으로 유효한 값으로 돌아가거나, 이전 값이 없는 경우 필드가 지워집니다.

팁 다중 CPU가 있는 관리되는 디바이스에 대한 전역 또는 개별 임계값을 사용하면 이벤트 수가 예상보다 더 많아질 수 있습니다.

이벤트 임계값을 추가 또는 수정하려면

액세스: Admin/Intrusion Admin

1단계 **Policies > Intrusion > Intrusion Policy**를 선택합니다.

Intrusion Policy 페이지가 나타납니다.

2단계 수정할 정책 옆에 있는 수정 아이콘()을 클릭합니다.

다른 정책에 저장하지 않은 변경 사항이 있는 경우 변경 사항을 취소하고 계속 진행하려면 **OK**를 클릭합니다. 저장하지 않은 변경 사항을 다른 정책에 저장하는 방법에 대한 자세한 내용은 23-15페이지의 충돌 해결 및 정책 변경 사항 커밋을/를 참조하십시오.

Policy Information 페이지가 나타납니다.

3단계 **Rules**를 클릭합니다.

Rules 페이지가 나타납니다. 기본적으로 페이지에는 규칙이 메시지별 알파벳순으로 나열됩니다.

4단계 임계값을 설정하고자 하는 규칙을 찾습니다. 다음 옵션을 이용할 수 있습니다.

- 현재 표시를 정렬하려면 열 머리글이나 아이콘을 클릭합니다. 정렬 순서를 반대로 하려면 다시 클릭합니다.
- 왼쪽에 있는 필터 패널에서 키워드나 인수를 클릭하여 필터를 구성합니다. 자세한 내용은 32-10페이지의 침입 정책의 규칙 필터링 이해 및 32-18페이지의 침입 정책에서 규칙 필터 설정 항목을 참조하십시오.

페이지가 새로 고쳐지고 일치하는 모든 규칙이 표시됩니다.

5단계 임계값을 설정하고자 하는 규칙을 선택합니다. 다음 옵션을 이용할 수 있습니다.

- 특정 규칙을 선택하려면 규칙 옆에 있는 확인란을 선택합니다.
- 현재 목록의 모든 규칙을 선택하려면 열 맨 위에 있는 확인란을 선택합니다.

6단계 **Event Filtering > Threshold**를 선택합니다.

Thresholding 팝업 창이 나타납니다.

7단계 **Type** 드롭다운 목록에서 설정하려는 임계값의 유형을 선택합니다.

- 기간당 지정된 이벤트 인스턴스의 수로 알림을 제한하려면 **Limit**를 선택합니다.
- 기간당 지정된 각 이벤트 인스턴스의 수에 대해 알림을 제공하려면 **Threshold**를 선택합니다.
- 지정된 이벤트 인스턴스의 수 이후 기간당 한 번 알림을 제공하려면 **Both**를 선택합니다.

8단계 **Track By** 드롭다운 목록에서 이벤트 인스턴스를 **Source** IP 주소로 추적할지 **Destination** IP 주소로 추적할지를 선택합니다.

9단계 임계값으로 사용할 이벤트 인스턴스의 수를 **Count** 필드에 지정합니다.

10단계 이벤트 인스턴스가 추적되는 기간의 값(초 단위)을 **Seconds** 필드에 입력합니다.

11단계 **OK**를 클릭합니다.

시스템은 임계값을 추가하고 Event Filtering 열의 규칙 옆에 이벤트 필터 아이콘()을 표시합니다. 규칙에 여러 이벤트 필터를 추가하는 경우 아이콘 위의 숫자는 이벤트 필터의 수를 나타냅니다.

12단계 정책을 저장하거나, 계속 수정하거나, 변경 사항을 취소하거나, 시스템 캐시에 변경 사항이 남아 있는 상태로 종료합니다.

자세한 내용은 31-3페이지의 침입 정책 관리 및 31-4페이지의 침입 정책 수정을/를 참조하십시오.

침입 이벤트 임계값 보기 및 삭제

라이센스: 보호

기존 임계값 설정을 보거나 삭제하고자 할 수 있습니다. 임계값에 대해 구성된 설정을 표시하여 시스템에 적절한지 확인하려면 Rules Details 보기를 사용할 수 있습니다. 적절하지 않은 경우 새 임계값을 추가하여 기존 값을 덮어쓸 수 있습니다.

모든 규칙 및 프리프로세서 생성 이벤트에 의해 적용되는 전역 임계값을 수정할 수도 있습니다. 자세한 내용은 35-1페이지의 전체적으로 침입 이벤트 로깅 제한을/를 참조하십시오.

임계값을 보거나 삭제하려면

액세스: Admin/Intrusion Admin

1단계 **Policies > Intrusion > Intrusion Policy**를 선택합니다.

Intrusion Policy 페이지가 나타납니다.

2단계 수정할 정책 옆에 있는 수정 아이콘( )을 클릭합니다.

다른 정책에 저장하지 않은 변경 사항이 있는 경우 변경 사항을 취소하고 계속 진행하려면 **OK**를 클릭합니다. 저장하지 않은 변경 사항을 다른 정책에 저장하는 방법에 대한 자세한 내용은 23-15페이지의 충돌 해결 및 정책 변경 사항 커밋을/를 참조하십시오.

Policy Information 페이지가 나타납니다.

3단계 **Rules**를 클릭합니다.

Rules 페이지가 나타납니다. 기본적으로 페이지에는 규칙이 메시지별 알파벳순으로 나열됩니다.

4단계 보거나 삭제할 구성된 임계값이 있는 규칙을 찾습니다. 다음 옵션을 이용할 수 있습니다.

- 현재 표시를 정렬하려면 열 머리글이나 아이콘을 클릭합니다. 정렬 순서를 반대로 하려면 다시 클릭합니다.
- 왼쪽에 있는 필터 패널에서 키워드나 인수를 클릭하여 필터를 구성합니다. 자세한 내용은 32-10페이지의 침입 정책의 규칙 필터링 이해 및 32-18페이지의 침입 정책에서 규칙 필터 설정 항목을 참조하십시오.

  페이지가 새로 고쳐지고 일치하는 모든 규칙이 표시됩니다.

5단계 보거나 삭제할 구성된 임계값이 있는 규칙을 선택합니다. 다음 옵션을 이용할 수 있습니다.

- 특정 규칙을 선택하려면 규칙 옆에 있는 확인란을 선택합니다.
- 현재 목록의 모든 규칙을 선택하려면 열 맨 위에 있는 확인란을 선택합니다.

6단계 선택한 각 규칙에 대한 모든 임계값을 제거하려면 **Event Filtering > Remove Thresholds** 를 선택합니다. 표시되는 확인 팝업 창에서 **OK**를 클릭합니다.

팁 또한 특정 임계값을 제거하려면 규칙을 강조 표시하고 **Show details**를 클릭할 수 있습니다. 임계값 설정을 확장한 다음 제거할 임계값 설정 옆에 있는 **Delete**를 클릭합니다. **OK**를 클릭하여 컨피그레이션을 삭제할 것임을 확인합니다.

페이지가 새로 고쳐지고 임계값이 삭제됩니다.

7단계 정책을 저장하거나, 계속 수정하거나, 변경 사항을 취소하거나, 시스템 캐시에 변경 사항이 남아 있는 상태로 종료합니다. 자세한 내용은 31-3페이지의 침입 정책 관리 및 31-4페이지의 침입 정책 수정을/를 참조하십시오.

침입 정책당 억제 구성

라이센스: 보호

특정 IP 주소 또는 IP 주소 범위가 특정 규칙 또는 프리프로세서를 트리거할 때 침입 이벤트 알림을 억제할 수 있습니다. 이렇게 하면 오탐을 없애는 데 도움이 됩니다. 특정 익스플로잇처럼 보이는 패킷을 전송하는 메일 서버가 있는 경우, 메일 서버에 의해 이벤트가 트리거될 때 해당 이벤트에 대한 이벤트 알림을 억제할 수 있습니다. 규칙은 모든 패킷에 대해 트리거되지만, 기준에 맞는 공격에 대한 이벤트만 표시됩니다.

침입 이벤트 억제만 사용할 수도 있고 속도 기반 공격 방지, `detection_filter` 키워드 및 침입 이벤트 임계값을 조합하여 사용할 수도 있습니다. 자세한 내용은 32-29페이지의 동적 규칙 상태 추가, 36-89페이지의 이벤트 필터링 및 32-22페이지의 이벤트 임계값 구성을/를 참조하십시오.

자세한 내용은 다음 절을 참조하십시오.

- 32-27페이지의 침입 이벤트 억제
- 32-28페이지의 억제 조건 보기 및 삭제

팁 침입 이벤트의 패킷 보기 내에서 억제를 추가할 수도 있습니다. 자세한 내용은 41-24페이지의 이벤트 정보 보기을/를 참조하십시오. Rule Editor 페이지 및 침입 이벤트 페이지(이벤트가 침입 규칙에 의해 트리거된 경우)에서 마우스 오른쪽 버튼을 클릭하면 나타나는 컨텍스트 메뉴를 사용하여 억제 설정에 액세스할 수도 있습니다.

침입 이벤트 억제

라이센스: 보호

하나 이상의 규칙에 대해 침입 이벤트 알림을 억제할 수 있습니다. 규칙에 대해 알림이 억제되면 규칙이 트리거되더라도 이벤트가 생성되지 않습니다. 규칙에 대해 하나 이상의 억제를 설정할 수 있습니다. 나열되는 첫 번째 억제의 우선순위가 가장 높습니다. 두 개의 억제가 충돌하면 첫 번째 작업이 구현됩니다.

잘못된 값을 입력하면 필드에 되돌리기 아이콘()이 나타납니다. 이 아이콘을 클릭하면 해당 필드에 대한 마지막으로 유효한 값으로 돌아가거나, 이전 값이 없는 경우 필드가 지워집니다.

이벤트 표시를 억제하려면

액세스: Admin/Intrusion Admin

1단계 **Policies > Intrusion > Intrusion Policy**를 선택합니다.

Intrusion Policy 페이지가 나타납니다.

2단계 수정할 정책 옆에 있는 수정 아이콘()을 클릭합니다.

다른 정책에 저장하지 않은 변경 사항이 있는 경우 변경 사항을 취소하고 계속 진행하려면 **OK**를 클릭합니다. 저장하지 않은 변경 사항을 다른 정책에 저장하는 방법에 대한 자세한 내용은 23-15페이지의 충돌 해결 및 정책 변경 사항 커밋을/를 참조하십시오.

Policy Information 페이지가 나타납니다.

3단계 **Rules**를 클릭합니다.

Rules 페이지가 나타납니다. 기본적으로 페이지에는 규칙이 메시지별 알파벳순으로 나열됩니다.

4단계 억제를 설정하고자 하는 규칙을 찾습니다. 다음 옵션을 이용할 수 있습니다.

- 현재 표시를 정렬하려면 열 머리글이나 아이콘을 클릭합니다. 정렬 순서를 반대로 하려면 다시 클릭합니다.
- 왼쪽에 있는 필터 패널에서 키워드나 인수를 클릭하여 필터를 구성합니다. 자세한 내용은 32-10페이지의 침입 정책의 규칙 필터링 이해 및 32-18페이지의 침입 정책에서 규칙 필터 설정 항목을 참조하십시오.

  페이지가 새로 고쳐지고 일치하는 모든 규칙이 표시됩니다.

5단계 억제 조건을 구성할 하나 이상의 규칙을 선택합니다. 다음 옵션을 이용할 수 있습니다.

- 특정 규칙을 선택하려면 규칙 옆에 있는 확인란을 선택합니다.
- 현재 목록의 모든 규칙을 선택하려면 열 맨 위에 있는 확인란을 선택합니다.

6단계 **Event Filtering > Suppression**을 선택합니다.

Suppression 팝업 창이 나타납니다.

7단계 다음 **Suppression Type** 옵션 중 하나를 선택합니다.

- 선택한 규칙에 대한 이벤트를 완전히 억제하려면 **Rule**을 선택합니다.
- 지정된 소스 IP 주소에서 나온 패킷에 의해 생성된 이벤트를 억제하려면 **Source**를 선택합니다.
- 지정된 목적지 IP 주소로 이동하는 패킷에 의해 생성된 이벤트를 억제하려면 **Destination**을 선택합니다.

8단계 억제 유형에 대해 **Source** 또는 **Destination**을 선택한 경우 **Network** 필드에 소스/목적지 IP 주소로 지정할 IP 주소, 주소 블록 또는 변수를 입력하거나 이들의 조합을 입력합니다.

FireSIGHT 시스템에서 IPv4 CIDR 및 IPv6 접두사 길이 주소 블록의 사용에 대한 자세한 내용은 1-19페이지의 IP 주소 표기 규칙을/를 참조하십시오.

9단계 **OK**를 클릭합니다.

시스템은 억제 조건을 추가하고 억제된 규칙 옆 Event Filtering 열의 규칙 옆에 이벤트 필터 아이콘()을 표시합니다. 규칙에 여러 이벤트 필터를 추가하는 경우 아이콘 위의 숫자는 이벤트 필터의 수를 나타냅니다.

10단계 정책을 저장하거나, 계속 수정하거나, 변경 사항을 취소하거나, 시스템 캐시에 변경 사항이 남아 있는 상태로 종료합니다.

자세한 내용은 31-3페이지의 침입 정책 관리 및 31-4페이지의 침입 정책 수정을/를 참조하십시오.

억제 조건 보기 및 삭제

라이센스: 보호

기존 억제 조건을 보거나 삭제하고자 할 수 있습니다. 예를 들어, 메일 서버는 일반적으로 익스플로잇처럼 보이는 패킷을 전송하므로 메일 서버 IP 주소에서 시작되는 패킷에 대한 이벤트 알림을 억제할 수 있습니다. 해당 메일 서버에 대한 설정을 취소한 후 IP 주소를 다른 호스트에 다시 할당하는 경우 해당 소스 IP 주소에 대한 억제 조건을 삭제해야 합니다.

정의된 억제 조건을 보거나 삭제하려면

액세스: Admin/Intrusion Admin

1단계 **Policies > Intrusion > Intrusion Policy**를 선택합니다.

Intrusion Policy 페이지가 나타납니다.

2단계 수정할 정책 옆에 있는 수정 아이콘()을 클릭합니다.

다른 정책에 저장하지 않은 변경 사항이 있는 경우 변경 사항을 취소하고 계속 진행하려면 **OK**를 클릭합니다. 저장하지 않은 변경 사항을 다른 정책에 저장하는 방법에 대한 자세한 내용은 23-15페이지의 충돌 해결 및 정책 변경 사항 커밋을/를 참조하십시오.

Policy Information 페이지가 나타납니다.

3단계 **Rules**를 클릭합니다.

Rules 페이지가 나타납니다. 기본적으로 페이지에는 규칙이 메시지별 알파벳순으로 나열됩니다.

4단계 억제를 보거나 삭제하고자 하는 규칙을 찾습니다. 다음 옵션을 이용할 수 있습니다.

- 현재 표시를 정렬하려면 열 머리글이나 아이콘을 클릭합니다. 정렬 순서를 반대로 하려면 다시 클릭합니다.
- 왼쪽에 있는 필터 패널에서 키워드나 인수를 클릭하여 필터를 구성합니다. 자세한 내용은 32-10페이지의 침입 정책의 규칙 필터링 이해 및 32-18페이지의 침입 정책에서 규칙 필터 설정 항목을 참조하십시오.

  페이지가 새로 고쳐지고 일치하는 모든 규칙이 표시됩니다.

5단계 억제를 보거나 삭제하고자 하는 규칙을 선택합니다. 다음 옵션을 이용할 수 있습니다.

- 특정 규칙을 선택하려면 규칙 옆에 있는 확인란을 선택합니다.
- 현재 목록의 모든 규칙을 선택하려면 열 맨 위에 있는 확인란을 선택합니다.

6단계 다음 2가지 옵션을 사용할 수 있습니다.

- 규칙에 대한 모든 억제를 제거하려면 **Event Filtering > Remove Suppressions** 를 선택합니다.표시되는 확인 팝업 창에서 **OK**를 클릭합니다.
- 특정 억제 설정을 제거하려면 규칙을 강조 표시하고 **Show details**를 클릭합니다. 억제 설정을 확장한 다음 제거할 억제 설정 옆에 있는 **Delete**를 클릭합니다. **OK**를 클릭하여 선택한 설정을 삭제할 것임을 확인합니다.

페이지가 새로 고쳐지고 억제 설정이 삭제됩니다.

7단계 정책을 저장하거나, 계속 수정하거나, 변경 사항을 취소하거나, 시스템 캐시에 변경 사항이 남아 있는 상태로 종료합니다. 자세한 내용은 31-3페이지의 침입 정책 관리 및 31-4페이지의 침입 정책 수정을/를 참조하십시오.

동적 규칙 상태 추가

라이센스: 보호

속도 기반 공격은 네트워크나 호스트로 과도한 트래픽을 전송하여 속도를 저하시키고 적법한 요청을 거부하게 함으로써 네트워크나 호스트를 혼란에 빠뜨리려고 시도합니다. 특정 규칙에 대한 과도한 규칙 일치에 대응하여 규칙의 작업을 변경하려면 속도 기반 방지를 사용할 수 있습니다.

자세한 내용은 다음 절을 참조하십시오.

- 32-30페이지의 동적 규칙 상태 이해
- 32-31페이지의 동적 규칙 상태 설정

동적 규칙 상태 이해

라이센스: 보호

지정된 기간에 규칙에 대해 너무 많은 일치가 발생할 때 이를 탐지하는 속도 기반 필터를 포함하도록 침입 정책을 구성할 수 있습니다. 이 기능은 지정된 시간 동안 속도 기반 공격을 차단하기 위해 인라인으로 구축된 관리되는 디바이스에서 사용하고, 그런 다음 규칙이 일치할 때 이벤트만 생성하고 트래픽을 삭제하지 않는 규칙 상태로 돌아갈 수 있습니다.

속도 기반 공격 방지는 비정상적인 트래픽 패턴을 식별하고, 합법적인 요청에 대한 해당 트래픽의 영향을 최소화하도록 시도합니다. 하나 이상의 특정 목적지 IP 주소로 나가거나 하나 이상의 특정 소스 IP 주소에서 들어오는 과도한 규칙 일치를 식별할 수 있습니다. 탐지된 모든 트래픽에서 특정 규칙에 대해 발생하는 과도한 일치에 대응할 수도 있습니다.

침입 정책에서 침입 또는 프리프로세서 규칙에 대해 속도 기반 필터를 구성할 수 있습니다. 속도 기반 필터에는 세 가지 구성 요소가 포함되어 있습니다.

- 특정 시간(초) 내에 규칙 일치 카운트로서 구성하는 규칙 매칭 속도
- 속도 초과 시 수행할 수 있는 새 작업으로 다음 세 가지 중 하나: Generate Events, Drop and Generate Events 및 Disable
- 시간 초과 값으로 구성할 수 있는 작업의 기간

시작되면, 해당 기간 중에 속도가 구성된 값 아래로 떨어지더라도 시간 초과에 도달할 때까지 새 작업이 발생합니다. 시간 초과에 도달하여 속도가 임계값 아래로 떨어지면 규칙에 대한 작업이 규칙에 대해 처음 구성한 작업으로 복구됩니다.

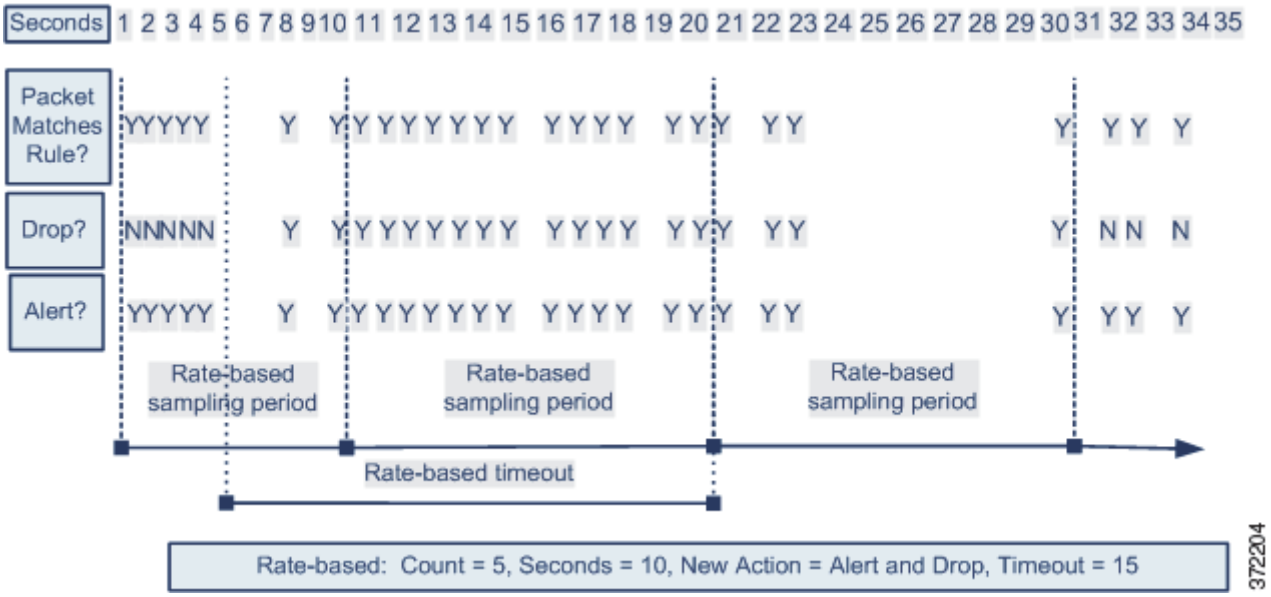
일시적으로 또는 영구적으로 공격을 차단하기 위해 인라인 구축에서 속도 기반 공격 방지를 구성할 수 있습니다. 속도 기반 컨피그레이션 없이 Generate Events로 설정된 규칙은 이벤트를 생성하지만 시스템은 해당 규칙의 패킷을 삭제하지 않습니다. 그러나 공격 트래픽이 속도 기반 기준을 구성한 규칙과 일치하면, 해당 규칙이 처음부터 Drop and Generate Events로 설정되지 않았더라도 속도 작업이 활성 상태로 유지되는 기간에 패킷 삭제가 발생할 수 있습니다.

참고 속도 기반 작업은 비활성화된 규칙을 활성화하거나, 비활성화된 규칙과 일치하는 트래픽을 삭제할 수 없습니다.

동일한 규칙에서 여러 속도 기반 필터를 정의할 수 있습니다. 침입 정책에 첫 번째로 나열되는 필터의 우선순위가 가장 높습니다. 두 개의 속도 기반 필터 작업이 충돌하면 첫 번째 속도 기반 필터의 작업이 구현됩니다.

다음 다이어그램은 공격자가 호스트에 액세스를 시도하는 예를 보여줍니다. 비밀번호를 찾으려는 시도가 반복되면 속도 기반 공격 방지가 구성된 규칙이 트리거됩니다. 10초 동안 규칙 일치가 5회 발생한 후 속도 기반 설정은 규칙 특성을 Drop and Generate Events로 변경합니다. 새 규칙 특성은 15초 후에 시간 초과됩니다.

시간 초과 후 이어지는 속도 기반 샘플링 기간에도 패킷은 계속 삭제됩니다. 샘플링된 속도가 현재 또는 이전 샘플링 기간의 임계값보다 높으면 새 작업이 계속됩니다. 샘플링된 속도가 임계값 속도 아래로 내려오고 샘플링 기간이 완료된 후에야 비로소 새 작업이 Generate Events로 되돌아갑니다.



동적 규칙 상태 설정

라이센스: 보호

규칙과 일치하는 모든 패킷을 삭제하지는 않을 것이지만 지정된 시간에 특정 일치 속도가 발생하면 규칙과 일치하는 패킷을 삭제하려는 경우, 규칙을 Drop and Generate Events 상태로 설정하지 않을 수 있습니다. 동적 규칙 상태를 사용하면 규칙에 대한 작업에서 변경을 트리거하는 속도, 속도가 충족될 때 작업에서 변경해야 할 내용, 새 작업의 지속 시간 등을 구성할 수 있습니다.

카운트와 초(작업 변경을 트리거하기 위해 히트 수가 발생해야 하는 시간)를 지정하여 규칙에 대한 히트 수를 설정할 수 있습니다. 또한 시간 초과를 설정하여 만료 시 작업이 규칙에 대한 이전 상태로 돌아가도록 할 수 있습니다.

동일한 규칙에서 여러 동적 규칙 상태 필터를 정의할 수 있습니다. 침입 정책의 규칙 세부사항에 첫 번째로 나열되는 필터의 우선순위가 가장 높습니다. 두 개의 속도 기반 필터 작업이 충돌하면 첫 번째 속도 기반 필터의 작업이 구현됩니다.

잘못된 값을 입력하면 필드에 되돌리기 아이콘( )이 나타납니다. 이 아이콘을 클릭하면 해당 필드에 대한 마지막으로 유효한 값으로 돌아가거나, 이전 값이 없는 경우 필드가 지워집니다.

참고 동적 규칙 상태는 비활성화된 규칙을 활성화하거나, 비활성화된 규칙과 일치하는 트래픽을 삭제할 수 없습니다.

동적 규칙 상태를 추가하려면

액세스: Admin/Intrusion Admin

1단계 **Policies > Intrusion > Intrusion Policy**를 선택합니다.

Intrusion Policy 페이지가 나타납니다.

2단계 수정할 정책 옆에 있는 수정 아이콘( )을 클릭합니다.

다른 정책에 저장하지 않은 변경 사항이 있는 경우 변경 사항을 취소하고 계속 진행하려면 **OK**를 클릭합니다. 저장하지 않은 변경 사항을 다른 정책에 저장하는 방법에 대한 자세한 내용은 23-15페이지의 충돌 해결 및 정책 변경 사항 커밋을/를 참조하십시오.

Policy Information 페이지가 나타납니다.

3단계 **Rules**를 클릭합니다.

Rules 페이지가 나타납니다.

4단계 동적 규칙 상태를 추가하고자 하는 규칙을 찾습니다. 다음 옵션을 이용할 수 있습니다.

- 현재 표시를 정렬하려면 열 머리글이나 아이콘을 클릭합니다. 정렬 순서를 반대로 하려면 다시 클릭합니다.
- 왼쪽에 있는 필터 패널에서 키워드나 인수를 클릭하여 필터를 구성합니다. 자세한 내용은 32-10페이지의 침입 정책의 규칙 필터링 이해 및 32-18페이지의 침입 정책에서 규칙 필터 설정 항목을 참조하십시오.

  페이지가 새로 고쳐지고 일치하는 모든 규칙이 표시됩니다.

5단계 동적 규칙 상태를 추가하고자 하는 규칙을 선택합니다. 다음 옵션을 이용할 수 있습니다.

- 특정 규칙을 선택하려면 규칙 옆에 있는 확인란을 선택합니다.
- 현재 목록의 모든 규칙을 선택하려면 열 맨 위에 있는 확인란을 선택합니다.

6단계 **Dynamic State > Add Rate-Based Rule State**를 선택합니다.

Add Rate-Based Rule State 대화 상자가 나타납니다.

7단계 **Track By** 드롭다운 목록에서 규칙 일치를 추적할 방법을 선택합니다.

- 특정 소스 또는 소스 집합에서 해당 규칙과 일치하는 수를 추적하려면 **Source**를 선택합니다.
- 특정 목적지 또는 목적지 집합에서 해당 규칙과 일치하는 수를 추적하려면 **Destination**을 선택합니다.
- 해당 규칙에 대한 모든 일치 항목을 추적하려면 **Rule**을 선택합니다.

8단계 **Track By**를 **Source** 또는 **Destination**으로 설정하는 경우 추적하려는 각 호스트의 주소를 **Network** 필드에 입력합니다.

단일 IP 주소나 주소 블록, 변수 또는 이러한 항목의 조합으로 구성된 쉼표로 구분된 목록을 지정할 수 있습니다. FireSIGHT 시스템에서 IPv4 CIDR 및 IPv6 접두사 길이 주소 블록의 사용에 대한 자세한 내용은 1-19페이지의 IP 주소 표기 규칙을/를 참조하십시오.

9단계 공격 속도를 설정하기 위한 기간당 규칙 일치 수를 **Rate** 옆에 지정합니다.

- 1~2147483647의 정수를 사용하여 임계값으로 사용할 규칙 일치의 수를 **Count** 필드에 지정합니다.
- 1~2147483647의 정수를 사용하여 공격이 추적되는 기간의 값(초 단위)을 **Seconds** 필드에 입력합니다.

10단계 조건이 일치할 때 수행할 새 작업을 **New State** 드롭다운 목록에서 지정합니다.

- 이벤트를 생성하려면 **Generate Events**를 선택합니다.
- 인라인 구축에서 이벤트를 생성하고 이벤트를 트리거한 패킷을 삭제하려면 또는 패시브 구축에서 이벤트를 생성하려면 **Drop and Generate Events**를 선택합니다.
- 작업을 수행하지 않으려면 **Disabled**를 선택합니다.

11단계 새 작업이 유효한 상태를 유지할 기간의 값(초 단위)을 **Timeout** 필드에 입력합니다. 시간이 초과되면 규칙이 원래 상태로 돌아갑니다. 새 작업의 시간 초과를 금지하려면 0을 지정하거나 **Timeout** 필드를 비워둡니다.

12단계 **OK**를 클릭합니다.

시스템은 동적 규칙 상태를 추가하고 Dynamic State 열의 규칙 옆에 동적 상태 아이콘()을 표시합니다. 규칙에 여러 동적 규칙 상태 필터를 추가하는 경우 아이콘 위의 숫자는 필터의 수를 나타냅니다.

필수 필드 중 비어 있는 것이 있으면 필드를 작성해야 한다는 오류 메시지가 표시됩니다.

팁 규칙의 집합에 대한 모든 동적 규칙 설정을 삭제하려면 Rules 페이지에서 규칙을 선택한 다음 **Dynamic State > Remove Rate-Based States**를 선택합니다. 규칙을 선택하고, **Show details**를 클릭한 다음, 제거하려는 속도 기반 필터 옆에 있는 **Delete**를 차례로 클릭하여 규칙 상세정보에서 개별 속도 기반 규칙 상태 필터를 삭제할 수도 있습니다.

13단계 정책을 저장하거나, 계속 수정하거나, 변경 사항을 취소하거나, 시스템 캐시에 변경 사항이 남아 있는 상태로 종료합니다.

자세한 내용은 31-3페이지의 침입 정책 관리 및 31-4페이지의 침입 정책 수정을/를 참조하십시오.

SNMP 알림 추가

라이센스: 보호

FireSIGHT 시스템에 대한 SNMP 알림을 구성하려면, 규칙이 이벤트를 생성할 때 SNMP 알림을 제공하기 위한 특정 규칙을 구성할 수 있습니다. 자세한 내용은 44-1페이지의 SNMP 응답 사용을/를 참조하십시오.

SNMP 알림을 설정하려면

액세스: Admin/Intrusion Admin

1단계 **Policies > Intrusion > Intrusion Policy**를 선택합니다.

Intrusion Policy 페이지가 나타납니다.

2단계 수정할 정책 옆에 있는 수정 아이콘()을 클릭합니다.

다른 정책에 저장하지 않은 변경 사항이 있는 경우 변경 사항을 취소하고 계속 진행하려면 **OK**를 클릭합니다. 저장하지 않은 변경 사항을 다른 정책에 저장하는 방법에 대한 자세한 내용은 23-15페이지의 충돌 해결 및 정책 변경 사항 커밋을/를 참조하십시오.

Policy Information 페이지가 나타납니다.

3단계 **Rules**를 클릭합니다.

Rules 페이지가 나타납니다.

4단계 SNMP 알림을 설정하고자 하는 규칙을 찾습니다. 다음 옵션을 이용할 수 있습니다.

- 현재 표시를 정렬하려면 열 머리글이나 아이콘을 클릭합니다. 정렬 순서를 반대로 하려면 다시 클릭합니다.
- 왼쪽에 있는 필터 패널에서 키워드나 인수를 클릭하여 필터를 구성합니다. 자세한 내용은 32-10페이지의 침입 정책의 규칙 필터링 이해 및 32-18페이지의 침입 정책에서 규칙 필터 설정 항목을 참조하십시오.

  페이지가 새로 고쳐지고 일치하는 모든 규칙이 표시됩니다.

5단계 SNMP 알림을 설정하고자 하는 규칙을 선택합니다.

- 특정 규칙을 선택하려면 규칙 옆에 있는 확인란을 선택합니다.
- 현재 목록의 모든 규칙을 선택하려면 열 맨 위에 있는 확인란을 선택합니다.

6단계 **Alerting > Add SNMP Alert**를 선택합니다.

시스템은 알림을 추가하고 Alerting 열의 규칙 옆에 알림 아이콘( )을 표시합니다. 규칙에 여러 알림 유형을 추가하는 경우 아이콘 위의 숫자는 알림 유형의 수를 나타냅니다.

팁 규칙에서 SNMP 알림을 제거하려면 규칙 옆에 있는 확인란을 클릭하고 **Alerting > Remove SNMP Alerts**를 선택한 다음 **OK**를 클릭하여 삭제를 확인합니다.

7단계 정책을 저장하거나, 계속 수정하거나, 변경 사항을 취소하거나, 시스템 캐시에 변경 사항이 남아 있는 상태로 종료합니다. 자세한 내용은 31-3페이지의 침입 정책 관리 및 31-4페이지의 침입 정책 수정을/를 참조하십시오.

규칙 코멘트 추가

라이센스: 보호

규칙에 코멘트를 추가할 수 있습니다. 추가하는 코멘트는 Rules 페이지의 Rule Details 보기에서 볼 수 있습니다.

코멘트가 포함된 침입 정책 변경 사항을 커밋한 후에는 또한 규칙 Edit 페이지에서 **Rule Comment**를 클릭하여 코멘트를 볼 수 있습니다. 규칙 수정에 대한 자세한 내용은 36-104페이지의 기존 규칙 수정을/를 참조하십시오.

규칙에 코멘트를 추가하려면

액세스: Admin/Intrusion Admin

1단계 **Policies > Intrusion > Intrusion Policy**를 선택합니다.

Intrusion Policy 페이지가 나타납니다.

2단계 수정할 정책 옆에 있는 수정 아이콘( )을 클릭합니다.

다른 정책에 저장하지 않은 변경 사항이 있는 경우 변경 사항을 취소하고 계속 진행하려면 **OK**를 클릭합니다. 저장하지 않은 변경 사항을 다른 정책에 저장하는 방법에 대한 자세한 내용은 23-15페이지의 충돌 해결 및 정책 변경 사항 커밋을/를 참조하십시오.

Policy Information 페이지가 나타납니다.

3단계 **Rules**를 클릭합니다.

Rules 페이지가 나타납니다.

4단계 코멘트를 추가하고자 하는 규칙을 찾습니다. 다음 옵션을 이용할 수 있습니다.

- 현재 표시를 정렬하려면 열 머리글이나 아이콘을 클릭합니다. 정렬 순서를 반대로 하려면 다시 클릭합니다.
- 왼쪽에 있는 필터 패널에서 키워드나 인수를 클릭하여 필터를 구성합니다. 자세한 내용은 32-10페이지의 침입 정책의 규칙 필터링 이해 및 32-18페이지의 침입 정책에서 규칙 필터 설정 항목을 참조하십시오.

  페이지가 새로 고쳐지고 일치하는 모든 규칙이 표시됩니다.

5단계 코멘트를 추가하고자 하는 규칙을 선택합니다.

- 특정 규칙을 선택하려면 규칙 옆에 있는 확인란을 선택합니다.
- 현재 목록의 모든 규칙을 선택하려면 열 맨 위에 있는 확인란을 선택합니다.

6단계 **Comments > Add Rule Comment**를 선택합니다.

Add Comment 대화 상자가 나타납니다.

7단계 **Comment** 필드에 규칙 코멘트를 입력합니다.

8단계 **OK**를 클릭합니다.

시스템은 코멘트를 추가하고 Comments 열의 규칙 옆에 코멘트 아이콘( )을 표시합니다. 규칙에 여러 코멘트를 추가하는 경우 아이콘 위의 숫자는 코멘트의 수를 나타냅니다.

팁 규칙 코멘트를 삭제하려면 규칙을 강조 표시하고 **Show Details**를 클릭한 다음, **Comments** 섹션에서 **Delete**를 클릭합니다. 코멘트되지 않은 침입 정책 변경 사항과 함께 코멘트가 캐시된 경우에만 코멘트를 삭제할 수 있습니다. 침입 정책 변경 사항이 커밋되면 규칙 코멘트는 영구적인 상태가 됩니다.

9단계 정책을 저장하거나, 계속 수정하거나, 변경 사항을 취소하거나, 시스템 캐시에 변경 사항이 남아 있는 상태로 종료합니다.

자세한 내용은 31-3페이지의 침입 정책 관리 및 31-4페이지의 침입 정책 수정을/를 참조하십시오.

33장 네트워크 자산에 대한 침입 방지 맞춤화

네트워크에서 탐지된 운영 체제, 서버 및 클라이언트 애플리케이션 프로토콜(45-1페이지의 네트워크 검색 소개 참조)을 이러한 자산의 보호를 위해 특별히 작성된 규칙과 침입 정책 단위로 연결하려면 FireSIGHT 권장 규칙 기능을 사용할 수 있습니다. 이렇게 하면 모니터링되는 네트워크의 특정 요구에 맞게 침입 정책을 맞춤화할 수 있습니다. FireSIGHT 권장 규칙 기능을 사용하려면 FireSIGHT 및 보호 라이센스가 필요합니다.

FireSIGHT 권장 규칙 기능을 구성하면, 시스템은 네트워크 자산과 연결된 취약성으로부터 보호하는 규칙의 기반 정책을 검색하고 기반 정책에서 규칙의 현재 상태를 식별합니다. 그런 다음 시스템은 규칙 상태를 권장하고, 선택적으로 다음 표의 기준을 사용하여 규칙을 권장 상태로 설정합니다.

표 33-1 취약성을 기준으로 한 FireSIGHT 규칙 상태 권장 사항

기반 정책 규칙 상태	규칙이 검색된 자산을 보호합니까?	권장 규칙 상태
이벤트 생성 또는 Disable	예	이벤트 생성
이벤트 삭제 및 생성	예	이벤트 삭제 및 생성
모든	아니요	Disable

Cisco VRT(Vulnerability Research Team)는 Cisco에서 제공하는 기본 정책에서 각 규칙의 적절한 상태를 결정합니다. 따라서 기반 정책이 Cisco에서 제공하는 기본 정책일 때 시스템이 규칙을 FireSIGHT 권장 규칙 상태로 설정하도록 허용하는 경우의 순 효과는, 침입 정책의 규칙이 Cisco에서 네트워크 자산에 대해 권장하는 설정과 일치한다는 것입니다. 자세한 내용은 23-8페이지의 시스템 제공 정책 이해을/를 참조하십시오.

규칙 상태 권장 사항 생성은 권장 사항을 생성할 때 또는 나중에, 권장 규칙 상태의 사용 여부를 선택하는 것만큼 간단할 수 있습니다. 고급 권장 옵션을 사용하면 컨피그레이션을 더 세부적으로 맞춤화할 수 있습니다. 권장 규칙 상태를 사용하도록 선택하면 읽기 전용 FireSIGHT 권장 사항 레이어가 침입 정책에 추가되며, 그 후에 권장 규칙 상태를 사용하지 않도록 선택하면 레이어가 제거됩니다. 여러 침입 정책을 좀 더 효과적으로 관리하기 위해 정책 레이어를 사용하는 방법에 대한 자세한 내용은 24-1페이지의 네트워크 분석 또는 침입 정책에서 레이어 사용을/를 참조하십시오.

대개 시스템은 표준 텍스트 규칙 및 공유 객체 규칙에 대한 규칙 상태 변경을 권장하지만, 프리프로세서와 디코더 규칙에 대한 변경도 권장할 수 있습니다.

침입 정책에서 가장 최근에 저장한 컨피그레이션 설정을 기반으로 권장 사항을 자동으로 생성하도록 작업을 예약할 수 있습니다. 권장 규칙 상태를 생성하기 위한 작업 예약에 대한 자세한 내용은 62-9페이지의 권장FireSIGHT 사항 자동화을/를 참조하십시오.

자세한 내용은 다음 절을 참조하십시오.

- 기본 규칙 상태 권장 사항 이해
- 고급 규칙 상태 권장 사항 이해
- 권장FireSIGHT 사항 사용

기본 규칙 상태 권장 사항 이해

라이센스: 보호 + FireSIGHT

정책의 권장 규칙 상태를 사용하지 않고도 권장 사항을 생성할 수 있습니다. 그러면 Rules 페이지의 세 가지 필터링된 보기(Generate Events, Drop and Generate Events 또는 Disable) 중 하나를 표시하여 시스템에서 설정하도록 권장하는 규칙을 볼 수 있습니다. 이렇게 하면 권장 규칙 상태를 사용하도록 선택할 경우 어떤 규칙이 수정될지를 미리 알 수 있습니다. 또한 권장 사항을 생성하고 즉시 사용하도록 선택할 수도 있습니다.

권장 사항을 필터링한 Rules 페이지가 표시되는 동안에 또는 탐색 패널이나 Policy Information 페이지에서 Rules 페이지에 직접 액세스한 후에, 규칙 상태를 수동으로 설정하고, 규칙을 정렬하고, Rules 페이지에서 사용할 수 있는 기타 작업(예: 규칙 억제, 규칙 임계값 설정 등)을 수행할 수 있습니다. 선택한 규칙의 상태를 수동으로 변경하는 방법에 대한 자세한 내용은 32-20페이지의 규칙 상태 설정을/를 참조하십시오. 침입 정책에서 규칙을 맞춤화하기 위해 Rules 페이지에서 사용할 수 있는 기타 작업에 대한 자세한 내용은 32-1페이지의 규칙을 사용하여 침입 정책 조정을/를 참조하십시오.

시스템은 수동으로 설정한 규칙 상태를 변경하지 않습니다. 권장 사항을 생성하는 동안 권장 규칙 상태를 사용하기로 선택하는 경우

- 권장 사항을 생성하기 전에 지정된 규칙의 상태를 수동으로 설정하면 향후 시스템은 그러한 규칙의 상태를 수정할 수 없게 됩니다.
- 권장 사항을 생성한 후에 지정된 규칙의 상태를 수동으로 설정하면 해당 규칙의 권장 상태가 재정의됩니다.

팁 규칙 상태가 권장 상태와 다른 경우 규칙의 침입 정책 보고서에 목록을 포함할 수 있습니다. 자세한 내용은 31-9페이지의 현재 침입 설정 보고서 생성을/를 참조하십시오.

FireSIGHT 권장 규칙에 대한 고급 설정을 변경하지 않고 권장 사항을 생성하면 시스템은 검색된 전체 네트워크의 모든 호스트에 대해 규칙 상태를 변경하도록 권장합니다. 또한 시스템은 기본적으로 low 또는 medium 오버헤드의 규칙에 대해서만 권장 사항을 생성하며, 규칙을 비활성화할 권장 사항을 생성합니다. 자세한 내용은 33-3페이지의 고급 규칙 상태 권장 사항 이해을/를 참조하십시오.

고급 규칙 상태 권장 사항 이해

라이센스: 보호 또는 보호 + FireSIGHT

고급 설정을 사용하면 시스템이 네트워크의 어떤 호스트에서 취약성을 모니터링할지를 다시 정의하고, 규칙 오버헤드를 기반으로 시스템이 어떤 규칙을 권장할지에 영향을 미치고, 규칙을 비활성화할 권장 사항의 생성 여부를 지정할 수 있습니다.

호스트 정보를 기반으로 특정 패킷에 대해 활성 규칙 프로세싱을 동적으로 수정하려면 적응형 프로필을 활성화할 수도 있습니다. 자세한 내용은 30-3페이지의 적응형 프로필과 FireSIGHT 권장 규칙을/를 참조하십시오.

자세한 내용은 다음 절을 참조하십시오.

- 33-3페이지의 검사할 네트워크 이해
- 33-3페이지의 규칙 오버헤드 이해

검사할 네트워크 이해

라이센스: 보호 + FireSIGHT

네트워크 맵에서 검토할 네트워크를 식별하여 FireSIGHT 권장 규칙 기능을 구성합니다. 그러면 시스템은 네트워크 보호를 위해 활성화할 수 있는 규칙을 권장합니다. 네트워크 맵에 대한 자세한 내용은 48-1페이지의 네트워크 맵 사용을/를 참조하십시오.

권장에 대해 검토할 호스트와 함께 **Networks** 필드를 구성합니다. 단일 IP 주소나 주소 블록 또는 쉼표로 구분된 목록을 지정할 수 있습니다(둘 중 하나 또는 모두로 구성).

지정하는 호스트 내 주소의 목록은 부정을 제외하고 OR 연산으로 연결되며, 모든 OR 연산이 계산되면 AND 연산으로 연결됩니다.

규칙 오버헤드 이해

라이센스: 보호

Cisco는 규칙이 시스템 성능에 미칠 수 있는 영향 및 규칙이 오탐을 생성할 가능성을 기반으로 각 침입 규칙의 오버헤드를 none, low, medium 또는 high로 평가합니다. Rules 페이지의 규칙 세부사항 보기에서 규칙에 대한 오버헤드 등급을 볼 수 있습니다. 자세한 내용은 32-5페이지의 규칙 세부사항 보기을/를 참조하십시오.

지정된 오버헤드 등급을 포함하여 그 등급까지. 예를 들어 오버헤드가 medium인 규칙에 대한 권장 사항을 생성하면 시스템은 오버헤드 등급이 none, low 또는 medium인 모든 규칙을 기반으로 권장 사항을 만들며, high 오버헤드에 대해서는 규칙의 권장 사항을 만들지 않습니다.

시스템은 이벤트를 생성할 권장 사항 또는 이벤트를 삭제하고 생성할 권장 사항에 대해 규칙 오버헤드를 고려합니다. 시스템은 규칙을 비활성화할 권장 사항에 대해서는 규칙 오버헤드를 고려하지 않습니다. 서드파티 취약성으로 매핑되지 않는 한 로컬 규칙에는 오버헤드가 없습니다. 자세한 내용은 66-20페이지의 로컬 규칙 파일 가져오기 및 46-30페이지의 서드파티 제품 매핑 관리을/를 참조하십시오.

특정 설정의 오버헤드 등급이 있는 규칙에 대한 권장 사항을 생성할 경우, 다른 오버헤드의 권장 사항을 생성한 다음 원래 오버헤드 설정에 대해 다시 권장 사항을 생성하는 것이 차단되지 않습니다. 권장 사항의 생성 횟수 또는 생성에 사용할 서로 다른 오버헤드 설정의 수와 상관없이, 동일한 규칙 설정에 대해 권장 사항을 생성할 때마다 각 오버헤드 설정에 대해 동일한 규칙 상태 권장 사항을 얻게 됩니다. 예를 들면 오버헤드를 medium으로, 그다음에는 high로, 그런 다음 최종적으로 다시 medium으로 설정하여 권장 사항을 생성할 수 있습니다. 네트워크의 호스트와 애플리케이션이 변경되지 않은 경우, 오버헤드가 medium으로 설정된 권장 사항의 두 집합은 해당 규칙 집합에 대해 동일합니다.

권장FireSIGHT 사항 사용

라이센스: FireSIGHT + 보호

권장 규칙 상태를 사용하거나 사용하지 않고, 권장 사항 생성을 위한 고급 설정을 수정하거나 수정하지 않고 권장 사항을 생성할 수 있습니다. 자세한 내용은 33-2페이지의 기본 규칙 상태 권장 사항 이해 및 33-3페이지의 고급 규칙 상태 권장 사항 이해을/를 참조하십시오.

권장 사항을 생성한 후에는 권장 규칙 상태를 사용할 수 있습니다. 또한 권장 상태를 보고 Rules 페이지에서 사용 가능한 기능을 사용할 수 있습니다.

FireSIGHT 규칙 상태 권장 사항을 사용하려면

액세스: Admin/Intrusion Admin

1단계 **Policies > Intrusion > Intrusion Policy**를 선택합니다.

Intrusion Policy 페이지가 나타납니다.

2단계 수정할 정책 옆에 있는 수정 아이콘( )을 클릭합니다.

다른 정책에 저장하지 않은 변경 사항이 있는 경우 변경 사항을 취소하고 계속 진행하려면 **OK**를 클릭합니다. 저장하지 않은 변경 사항을 다른 정책에 저장하는 방법에 대한 자세한 내용은 23-15페이지의 충돌 해결 및 정책 변경 사항 커밋을/를 참조하십시오.

Policy Information 페이지가 나타납니다.

3단계 다음 2가지 옵션을 사용할 수 있습니다.

- 권장 사항을 생성하지 않은 경우 **No recommendations have been generated. Click here to set up FireSIGHT recommendations**를 선택합니다.
- 권장 사항을 생성한 경우 **Click to change recommendations**를 선택합니다.

FireSIGHT Recommended Rules Configuration 페이지가 나타납니다.

4단계 다음 옵션을 이용할 수 있습니다.

- 해당 침입 정책 보고서에 실제 상태가 권장 상태와 다른 모든 규칙에 대한 규칙 메시지, 권장 상태 및 실제 상태를 나열하려면 **Include all differences between recommendations and rule states in policy reports**를 선택합니다. 자세한 내용은 31-9페이지의 현재 침입 설정 보고서 생성을/를 참조하십시오.
- 기본 설정을 사용하여 권장 사항을 생성하려면 9단계로 이동합니다.
- 고급 권장 옵션을 수정하려면 5단계로 이동합니다.

5단계 더하기 아이콘()을 클릭하여 **Advanced Settings** 섹션을 확장합니다.

고급 FireSIGHT 권장 사항 옵션이 나타납니다.

6단계 **Networks to Examine**의 **Networks** 필드에 권장 사항에 대해 검토할 네트워크를 지정합니다.

FireSIGHT 시스템에서 IP 주소 표기법을 사용하는 방법에 대한 자세한 내용은 1-19페이지의 IP 주소 표기 규칙을/를 참조하십시오.

주소의 목록은 부정을 제외하고 OR 연산으로 연결되며, 모든 OR 연산이 계산되면 AND 연산으로 연결됩니다. 자세한 내용은 33-3페이지의 검사할 네트워크 이해을/를 참조하십시오.

7단계 선택적으로, 생성하는 권장 사항에 포함하기 위해 규칙에 필요한 오버헤드의 양을 지정하려면 **FireSIGHT Recommended Rules Configuration**에서 **Recommendation Threshold (By Rule Overhead)** 슬라이드 바를 끕니다.

슬라이드 바를 오른쪽으로 끌면 오버헤드가 높아지고 권장 사항이 더 많아질 수 있지만, 시스템 성능에 더 많은 영향을 미칠 수 있습니다. 자세한 내용은 33-3페이지의 규칙 오버헤드 이해을/를 참조하십시오.

8단계 다음 옵션을 이용할 수 있습니다.

- 규칙을 비활성화할 권장 사항을 생성하려면 **Accept Recommendations to Disable Rules** 확인란을 선택합니다.

  규칙을 비활성화할 권장 사항을 수용하면 규칙 적용 범위가 제한됩니다.

- 규칙을 비활성화할 권장 사항을 차단하려면 **Accept Recommendations to Disable Rules** 확인란을 선택하지 않습니다.

  규칙을 비활성화할 권장 사항을 생략하면 규칙 적용 범위가 증가합니다.

9단계 여러 옵션이 있습니다.

- 권장 사항을 아직 생성하지 않았으며 권장 사항 생성 중에 시스템이 규칙 상태를 자동으로 권장 상태로 변경하도록 하려면 **Generate and Use Recommendations**를 클릭합니다.

  시스템은 권장 규칙 상태 변경을 생성하고 규칙을 자동으로 권장 상태로 설정합니다.

- 규칙 상태를 권장 상태로 자동으로 변경하지 않은 채 시스템이 권장 사항을 생성하도록 하려면 **Generate Recommendations**를 클릭합니다.

  시스템은 권장 규칙 상태 변경을 생성합니다.

- 전에 권장 사항을 생성한 경우 기존 권장 사항을 업데이트하려면 **Update Recommendations**를 클릭합니다.

  시스템은 권장 규칙 상태 변경을 생성하고, 권장 사항이 사용 중이면 규칙을 자동으로 권장 상태로 설정합니다. 권장 사항의 수, 권장 규칙 상태가 변경된 호스트의 수, 이벤트의 생성, 이벤트의 삭제 및 생성 또는 규칙 비활성화에 대한 권장 사항의 수에 대한 상태가 업데이트됩니다.

- 전에 권장 사항을 생성한 경우, 생성되었지만 사용되지 않은 권장 사항을 사용하려면 **Use Recommendations**를 클릭합니다.

  시스템은 규칙을 자동으로 권장 상태로 설정합니다.

- 권장 사항을 생성했으며 이미 사용 중인 경우 현재 사용 중인 권장 사항의 사용을 중지하려면 **Do Not Use Recommendations**를 클릭합니다.

  권장 사항을 사용하기 전 특정 규칙 상태가 규칙에 적용되지 않았다면 시스템은 규칙을 자동으로 기본 규칙 상태로 재설정합니다. 이 경우 규칙은 특정 규칙 상태로 되돌아갑니다.

시스템은 Impact Qualification 기능을 사용하여 비활성화한 취약성을 기반으로 하는 침입 규칙에 대해 규칙 상태를 권장하지 않습니다. 자세한 내용은 49-28페이지의 취약성 영향 자격 설정을/를 참조하십시오.

네트워크 및 규칙 집합의 규모에 따라, 권장 사항을 사용하거나 사용하지 않도록 정책을 업데이트하는 데에 몇 분 정도 걸릴 수 있습니다.

참고 시스템은 항상 호스트에 매핑된 서드파티 취약성과 관련된 로컬 규칙을 활성화하도록 권장합니다. 시스템은 매핑되지 않은 로컬 규칙에 대해서는 상태 권장 사항을 만들지 않습니다. 자세한 내용은 46-30페이지의 서드파티 제품 매핑 관리을/를 참조하십시오.

10단계 선택적으로, 선택한 권장 사항 유형에 대해 Rules 페이지에 권장 사항으로 필터링한 보기를 표시하려면 권장 사항 유형 옆에 있는 **View**를 클릭합니다.

11단계 정책을 저장하거나, 계속 수정하거나, 변경 사항을 취소하거나, 시스템 캐시에 변경 사항이 남아 있는 상태로 종료합니다. 자세한 내용은 23-15페이지의 충돌 해결 및 정책 변경 사항 커밋을/를 참조하십시오.

34장 특정 위협 탐지

네트워크 분석 정책에 있는 여러 프리프로세서를 사용하면 모니터링되는 네트워크에 대한 특정 위협(예: Back Orifice 공격), 여러 포트스캔 유형, 과도한 트래픽으로 네트워크를 무력화하려는 속도 기반 공격 등을 탐지할 수 있습니다. 침입 규칙 또는 규칙 인수에서 비활성화된 프리프로세서를 요구하면, 네트워크 분석 정책의 웹 인터페이스에서 비활성 상태로 있더라도 시스템에서는 자동으로 현재의 컨피그레이션과 함께 해당 프리프로세서를 사용합니다. 자세한 내용은 23-12페이지의 사용자 지정 정책의 제한 사항을/를 참조하십시오.

주의 사용자 지정 사용자 역할이 있는 일부 사용자는 표준 메뉴 경로(**Policies > Access Control > Network Analysis Policy**)를 통해 네트워크 분석 정책에 액세스할 수 없습니다. 이러한 사용자는 침입 정책을 통해 네트워크 분석 정책에 액세스할 수 있습니다(**Policies > Intrusion > Intrusion Policy > Network Analysis Policy**). 사용자 지정 사용자 역할에 대한 자세한 내용은 61-51페이지의 사용자 지정 사용자 역할 관리을/를 참조하십시오.

안전하지 않게 전송되는 민감한 수치 데이터를 탐지하려면 침입 정책에서 구성하는 민감한 데이터 탐지 기능을 사용할 수도 있습니다.

특정 위협 탐지에 대한 자세한 내용은 다음 절을 참조하십시오.

- 34-1페이지의 Back Orifice 탐지 - Back Orifice 공격의 탐지에 대해 설명합니다.
- 34-3페이지의 포트스캔 탐지 - 포트스캔의 여러 유형에 대해 설명하고, 네트워크에 대한 위협이 공격으로 발전하기 전에 포트스캔 탐지를 사용하는 방법에 대해 설명합니다.
- 34-9페이지의 속도 기반 공격 방지 - DoS(서비스 거부) 및 SYN 플러드 공격을 제한하는 방법에 대해 설명합니다.
- 34-18페이지의 민감한 데이터 탐지 - ASCII 텍스트의 신용카드 번호 및 주민등록번호 같은 민감한 데이터를 탐지하고 이벤트를 생성하는 방법에 대해 설명합니다.

Back Orifice 탐지

라이센스: 보호

FireSIGHT 시스템은 Back Orifice 프로그램의 존재를 탐재하는 프리프로세서를 제공합니다. Windows 호스트에 대한 관리자 액세스를 얻는 데 이 프로그램을 사용할 수 있습니다. Back Orifice 프리프로세서는 Back Orifice magic cookie, "*!*QWTY?"(패킷의 처음 8바이트에 있으며 XOR로 암호화됨)에 대한 UDP 트래픽을 분석합니다.

Back Orifice 프리프로세서에는 컨피그레이션 페이지가 있지만 컨피그레이션 옵션은 없습니다. 활성화된 경우, 프리프로세서가 해당 이벤트를 생성하도록 하려면 다음 표의 프리프로세서 규칙도 활성화해야 합니다. 자세한 내용은 32-20페이지의 규칙 상태 설정을/를 참조하십시오.

표 34-1 Back Orifice GID:SID

프리프로세서 규칙 GID:SID	설명
105:1	Back Orifice 트래픽이 탐지됨
105:2	Back Orifice 클라이언트 트래픽이 탐지됨
105:3	Back Orifice 서버 트래픽이 탐지됨
105:4	Back Orifice snort 버퍼 공격이 탐지됨

Back Orifice Detection 페이지를 보려면

액세스: Admin/Intrusion Admin

1단계 **Policies > Access Control > Access Control Policy**를 선택하여 Access Control Policy 페이지를 표시한 다음 **Network Analysis Policy**를 클릭합니다.

Network Analysis Policy 페이지가 나타납니다.

2단계 수정할 정책 옆에 있는 수정 아이콘( )을 클릭합니다.

다른 정책에 저장하지 않은 변경 사항이 있는 경우 변경 사항을 취소하고 계속 진행하려면 **OK**를 클릭합니다. 저장하지 않은 변경 사항을 다른 정책에 저장하는 방법에 대한 자세한 내용은 23-15페이지의 충돌 해결 및 정책 변경 사항 커밋을/를 참조하십시오.

Policy Information 페이지가 나타납니다.

3단계 왼쪽의 탐색 패널에서 **Settings**를 클릭합니다.

Settings 페이지가 나타납니다.

4단계 **Specific Threat Detection** 아래에서 **Back Orifice Detection**이 활성화되었는지 여부에 따라 두 가지 선택 사항이 있습니다.

- 프리프로세서가 활성화되어 있으면 **Edit**를 클릭합니다.
- 프리프로세서가 비활성화되어 있으면 **Enabled**를 클릭한 다음 **Edit**를 클릭합니다.

Back Orifice Detection 페이지가 나타납니다. 페이지 하단에 있는 메시지는 컨피그레이션이 포함된 침입 정책 레이어를 식별합니다. 자세한 내용은 24-1페이지의 네트워크 분석 또는 침입 정책에서 레이어 사용을/를 참조하십시오.

5단계 정책을 저장하거나, 계속 수정하거나, 변경 사항을 취소하거나, 시스템 캐시에 변경 사항이 남아 있는 상태로 종료합니다. 자세한 내용은 23-15페이지의 충돌 해결 및 정책 변경 사항 커밋을/를 참조하십시오.

포트스캔 탐지

라이센스: 보호

포트스캔은 공격에 앞서 공격자가 종종 사용하는 네트워크 정찰의 형태입니다. 포트스캔에서 공격자는 특별히 고안된 패킷을 대상 호스트로 전송합니다. 호스트가 응답하는 패킷을 검사하여 공격자는 종종 호스트에서 어떤 포트가 열려 있는지, 그리고 직접적으로 또는 추론에 의해 이러한 포트에서 어떤 애플리케이션 프로토콜이 실행 중인지 확인할 수 있습니다.

포트스캔 탐지가 활성화된 경우 포트스캔 탐지기의 활성화된 포트스캔 유형이 포트스캔 이벤트를 생성하도록 하려면 침입 정책 Rules 페이지에서 GID(generator ID) 122로 규칙을 활성화해야 합니다. 자세한 내용은 32-20페이지의 규칙 상태 설정 및 34-7 페이지의 표 34-5을/를 참조하십시오.

포트스캔 자체는 공격의 증거가 되지 못합니다. 실제로, 공격자가 사용하는 포트스캔 기법 중 일부는 네트워크의 합법적인 사용자들도 사용할 수 있습니다. Cisco의 포트스캔 탐지기는 활동의 패턴을 탐지하여 어떤 포트스캔이 악의적일 수 있는지를 확인하도록 설계되었습니다.

공격자들은 네트워크에 대한 프로브를 위해 여러 방법을 사용할 것입니다. 이들은 종종, 하나의 프로토콜 유형이 차단되면 다른 것을 사용할 수 있도록 대상 호스트에서 서로 다른 응답을 이끌어내기 위해 여러 프로토콜을 사용합니다. 다음 표에서는 포트스캔 탐지기에서 활성화할 수 있는 프로토콜에 대해 설명합니다.

표 34-2 프로토콜 유형

프로토콜	설명
TCP	SYN 스캔, ACK 스캔, TCP connect() 스캔, 그리고 Xmas tree, FIN, NULL 등 특이한 플래그 조합의 스캔과 같은 TCP 프로브를 탐지합니다.
UDP	제로바이트 UDP 패킷과 같은 UDP 프로브를 탐지합니다.
ICMP	ICMP 에코 요청(ping)을 탐지합니다.
IP	IP 프로토콜 스캔을 탐지합니다. 이 스캔은 TCP 및 UDP 스캔과 다릅니다. 공격자가 열린 포트를 찾는 대신 대상 호스트에서 어떤 IP 프로토콜이 지원되는지를 알아보려고 하기 때문입니다.

참고 포트스캔 연결 탐지기가 생성하는 이벤트의 경우 프로토콜 번호는 255로 설정됩니다. 포트스캔에는 기본적으로 연결된 특정 프로토콜이 없기 때문에 IANA(Internet Assigned Numbers Authority)에서는 프로토콜 번호를 할당하지 않습니다. IANA에서는 255를 예약 번호로 지정하므로, 이벤트에 대해 연결된 프로토콜이 없음을 나타내기 위해 프로토콜 이벤트에 해당 번호가 사용됩니다.

포트스캔은 일반적으로 대상 호스트의 수, 스캔하는 호스트의 수, 스캔되는 포트의 수를 기반으로 네 가지 유형으로 구분됩니다. 다음 표에서는 탐지할 수 있는 포트스캔 활동 유형에 대해 설명합니다.

표 34-3 포트스캔 유형

유형	설명
Portscan Detection	공격자가 단일 대상 호스트에서 여러 포트를 스캔하기 위해 하나 또는 소수의 호스트를 사용하는 일대일 포트스캔. 일대일 포트 스캔의 특성: • 스캔하는 호스트 수가 적음 • 단일 호스트가 스캔됨 • 스캔되는 포트 수가 많음 이 옵션은 TCP, UDP 및 IP 포트스캔을 탐지합니다.
Port Sweep	공격자가 여러 대상 호스트에서 단일 포트를 스캔하기 위해 하나 또는 소수의 호스트를 사용하는 일대다 포트스윕. 포트스윕의 특성: • 스캔하는 호스트 수가 적음 • 스캔되는 호스트 수가 많음 • 스캔되는 고유한 포트 수가 적음 이 옵션은 TCP, UDP, ICMP 및 IP 포트스윕을 탐지합니다.
Decoy Portscan	공격자가 스푸핑된 소스 IP 주소를 실제 스캔하는 IP 주소와 혼합하는 일대일 포트스캔. Decoy Portscan의 특성: • 스캔하는 호스트 수가 많음 • 한 번만 스캔되는 포트 수가 적음 • 단일(또는 소수의) 스캔되는 호스트 Decoy Portscan 옵션은 TCP, UDP 및 IP 프로토콜 포트스캔을 탐지합니다.
Distributed Portscan	다수의 호스트가 열린 포트에 대해 단일 호스트를 쿼리하는 다대일 포트스캔. Distributed Portscan의 특성: • 스캔하는 호스트 수가 많음 • 한 번만 스캔되는 포트 수가 많음 • 단일(또는 소수의) 스캔되는 호스트 Distributed Portscan 옵션은 TCP, UDP 및 IP 프로토콜 포트스캔을 탐지합니다.

포트스캔 탐지기가 프로브에 대해 학습하는 정보는 프로브된 호스트에서 부정적인 응답을 확인하는 것에 크게 기반을 둡니다. 예를 들어 웹 클라이언트가 웹 서버에 연결하려고 시도하는 경우 클라이언트는 포트 80/tcp를 사용하고 서버는 열려 있는 해당 포트에 의존할 수 있습니다. 그러나 공격자는 서버를 프로브할 때 서버에서 웹 서비스를 제공하는지 여부를 미리 알지 못합니다. 포트스캔 탐지기는 부정적인 응답(즉, ICMP 도달 불가 또는 TCP RST 패킷)을 확인하면 잠재적인 포트스캔으로 기록합니다. 대상 호스트가 디바이스의 다른 쪽(예: 부정적인 응답을 필터링하는 방화벽 또는 라우터)에 있으면 이 프로세스가 한층 어려워집니다. 이 경우 포트스캔은 사용자가 선택한 민감도 레벨을 기반으로 *필터링된* 포트스캔 이벤트를 생성할 수 있습니다.

다음 표에서는 사용자가 선택할 수 있는 세 가지 민감도 레벨에 대해 설명합니다.

표 34-4 민감도 레벨

수준	설명
Low	대상 호스트에서 부정적인 응답만 탐지합니다. 이 민감도 레벨을 선택하면 오탐을 억제할 수 있지만, 일부 포트스캔 유형(느린 스캔, 필터링된 스캔)을 놓칠 수 있습니다. 이 레벨은 포트스캔 탐지에 가장 짧은 시간 창을 사용합니다.
Medium	호스트에 대한 연결 수를 기반으로 포트스캔을 탐지합니다. 즉, 필터링된 포트스캔을 탐지할 수 있습니다. 그러나 네트워크 주소 변환기와 프록시 등 매우 활동적인 호스트는 오탐을 생성할 수 있습니다. 이 유형의 오탐을 완화하려면 이러한 활동적인 호스트의 IP 주소를 **Ignore Scanned** 필드에 추가할 수 있습니다. 이 레벨은 포트스캔 탐지에 좀 더 긴 시간 창을 사용합니다.
High	시간 창을 기반으로 포트스캔을 탐지합니다. 즉, 시간 기반 포트스캔을 탐지할 수 있습니다. 그러나 이 옵션을 사용할 경우 **Ignore Scanned** 및 **Ignore Scanner** 필드에 IP 주소를 지정하여 시간에 따라 탐지기를 신중하게 조정해야 합니다. 이 레벨은 포트스캔 탐지에 훨씬 긴 시간 창을 사용합니다.

자세한 내용은 다음 절을 참조하십시오.

- 34-5페이지의 포트스캔 탐지 구성
- 34-7페이지의 포트스캔 이벤트 이해

포트스캔 탐지 구성

라이센스: 보호

포트스캔 탐지 컨피그레이션 옵션을 사용하면 포트스캔 탐지기가 스캔 활동을 보고하는 방식을 세부적으로 조정할 수 있습니다.

포트스캔 탐지가 활성화된 경우 포트스캔 탐지기의 활성화된 포트스캔 유형이 포트스캔 이벤트를 생성하도록 하려면 Rules 페이지에서 GID(generator ID) 122로 규칙을 활성화해야 합니다. 자세한 내용은 32-20페이지의 규칙 상태 설정 및 포트스캔 탐지 SID(GID:122) 표를 참조하십시오.

포트스캔 탐지를 구성하려면

Admin/Intrusion Admin

1단계 **Policies > Access Control > Access Control Policy**를 선택하여 Access Control Policy 페이지를 표시한 다음 **Network Analysis Policy**를 클릭합니다.

Network Analysis Policy 페이지가 나타납니다.

2단계 수정할 정책 옆에 있는 수정 아이콘()을 클릭합니다.

다른 정책에 저장하지 않은 변경 사항이 있는 경우 변경 사항을 취소하고 계속 진행하려면 **OK**를 클릭합니다. 다른 정책에 있는 저장하지 않은 변경 사항을 저장하는 방법에 대한 자세한 내용은 [was Committing Intrusion Policy Changes; update xref]을/를 참조하십시오.

Policy Information 페이지가 나타납니다.

3단계 왼쪽의 탐색 패널에서 **Settings**를 클릭합니다.

Settings 페이지가 나타납니다.

4단계 **Specific Threat Detection** 아래에서 **Portscan Detection**이 활성화되었는지 여부에 따라 두 가지 선택 사항이 있습니다.

- 컨피그레이션이 활성화되어 있으면 **Edit**를 클릭합니다.
- 컨피그레이션이 비활성화되어 있으면 **Enabled**를 클릭한 다음 **Edit**를 클릭합니다.

  Portscan Detection 페이지가 나타납니다. 페이지 하단에 있는 메시지는 컨피그레이션이 포함된 침입 정책 레이어를 식별합니다. 자세한 내용은 24-1페이지의 네트워크 분석 또는 침입 정책에서 레이어 사용을/를 참조하십시오.

5단계 다음 중 활성화할 프로토콜을 **Protocol** 필드에서 지정합니다.

- TCP
- UDP
- ICMP
- IP

여러 프로토콜을 선택하거나 개별 프로토콜을 지우려면 Ctrl 또는 Shift 키를 누른 채 클릭합니다. 자세한 내용은 프로토콜 유형 표를 참조하십시오.

TCP를 통해 스캔을 탐지할 수 있도록 TCP 스트림 프로세싱이 활성화되었는지, 그리고 UDP를 통해 스캔을 탐지할 수 있도록 UDP 스트림 프로세싱이 활성화되었는지 확인해야 합니다.

6단계 다음 중 탐지할 포트스캔을 **Scan Type** 필드에서 지정합니다.

- Portscan Detection
- Port Sweep
- Decoy Portscan
- Distributed Portscan

여러 프로토콜을 선택하거나 선택 취소하려면 Ctrl 또는 Shift 키를 누른 채 클릭합니다. 자세한 내용은 포트스캔 유형 표를 참조하십시오.

7단계 사용할 레벨을 **Sensitivity Level** 목록에서 선택합니다(low, medium, high).

자세한 내용은 민감도 레벨 표를 참조하십시오.

8단계 선택적으로, 포트스캔 활동의 징후를 관찰할 호스트를 **Watch IP** 필드에서 지정합니다. 모든 네트워크 트래픽을 관찰하려면 이 필드를 비워둡니다.

단일 IP 주소나 주소 블록 또는 쉼표로 구분된 목록(둘 중 하나 또는 모두)을 지정할 수 있습니다. FireSIGHT 시스템에서 IPv4 및 IPv6 주소 블록을 사용하는 방법에 대한 자세한 내용은 1-19페이지의 IP 주소 표기 규칙을/를 참조하십시오.

9단계 선택적으로, 스캐너로서 무시할 호스트를 **Ignore Scanners** 필드에서 지정합니다. 특별히 활동적인 네트워크의 호스트를 표시하려면 이 필드를 사용합니다. 이 목록은 시간이 지남에 따라 수정해야 할 수 있습니다.

단일 IP 주소나 주소 블록 또는 쉼표로 구분된 목록(둘 중 하나 또는 모두)을 지정할 수 있습니다. FireSIGHT 시스템에서 IPv4 및 IPv6 주소 블록을 사용하는 방법에 대한 자세한 내용은 1-19페이지의 IP 주소 표기 규칙을/를 참조하십시오.

10단계 선택적으로, 스캔 대상으로서 무시할 호스트를 **Ignore Scanned** 필드에서 지정합니다. 특별히 활동적인 네트워크의 호스트를 표시하려면 이 필드를 사용합니다. 이 목록은 시간이 지남에 따라 수정해야 할 수 있습니다.

단일 IP 주소나 주소 블록 또는 쉼표로 구분된 목록(둘 중 하나 또는 모두)을 지정할 수 있습니다. FireSIGHT 시스템에서 IPv4 및 IPv6 주소 블록을 사용하는 방법에 대한 자세한 내용은 1-19페이지의 IP 주소 표기 규칙을/를 참조하십시오.

11단계 선택적으로, 스트림 중간에 선택한 세션의 모니터링을 중단하려면 **Detect Ack Scans** 확인란의 선택을 취소합니다.

참고 스트림 중간 세션의 탐지는 ACK 스캔 식별에 도움이 되지만, 특히 트래픽이 많거나 삭제된 패킷이 있는 네트워크에서 잘못된 이벤트를 발생시킬 수 있습니다.

12단계 정책을 저장하거나, 계속 수정하거나, 변경 사항을 취소하거나, 시스템 캐시에 변경 사항이 남아 있는 상태로 종료합니다. 자세한 내용은 23-15페이지의 충돌 해결 및 정책 변경 사항 커밋을/를 참조하십시오.

포트스캔 이벤트 이해

라이센스: 보호

포트스캔 탐지가 활성화된 경우 활성화된 각 포트스캔 유형에 대해 이벤트를 생성하려면 GID(generator ID) 122 및 SID(Snort® ID) 범위 1~27을 사용하여 규칙을 활성화해야 합니다. 자세한 내용은 32-20페이지의 규칙 상태 설정을/를 참조하십시오. 다음 표의 **Preprocessor Rule SID** 열에는 각 포트스캔 유형에 대해 활성화해야 할 프리프로세서 규칙의 SID가 나열되어 있습니다.

표 34-5 포트스캔 탐지 SID(GID:122)

포트스캔 유형	프로토콜:	민감도 레벨	프리프로세서 규칙 SID
Portscan Detection	TCP	Low	1
		Medium or High	5
	UDP	Low	17
		Medium or High	21
	ICMP	Low	이벤트를 생성하지 않음
		Medium or High	이벤트를 생성하지 않음
	IP	Low	9
		Medium or High	13
Port Sweep	TCP	Low	3, 27
		Medium or High	7
	UDP	Low	19
		Medium or High	23
	ICMP	Low	25
		Medium or High	26
	IP	Low	11
		Medium or High	15

표 34-5 포트스캔 탐지 SID(GID:122)(계속)

포트스캔 유형	프로토콜:	민감도 레벨	프리프로세서 규칙 SID
Decoy Portscan	TCP	Low	2
		Medium or High	6
	UDP	Low	18
		Medium or High	22
	ICMP	Low	이벤트를 생성하지 않음
		Medium or High	이벤트를 생성하지 않음
	IP	Low	10
		Medium or High	14
Distributed Portscan	TCP	Low	4
		Medium or High	8
	UDP	Low	20
		Medium or High	24
	ICMP	Low	이벤트를 생성하지 않음
		Medium or High	이벤트를 생성하지 않음
	IP	Low	12
		Medium or High	16

동반 프리프로세서 규칙을 활성화하는 경우 포트스캔 탐지기는 침입 이벤트를 생성하며, 이 이벤트는 다른 침입 이벤트와 같은 방식으로 볼 수 있습니다. 그러나 패킷 보기에 표시되는 정보는 기타 침입 이벤트 유형과 다릅니다. 이 섹션에서는 포트스캔 이벤트에 대한 패킷 보기에 나타나는 필드, 그리고 해당 정보를 사용하여 네트워크에서 발생하는 프로브 유형을 이해하는 방법에 대해 설명합니다.

포트스캔 이벤트의 패킷 보기로 드릴다운하려면 침입 이벤트 보기를 사용하는 것으로 시작하십시오. 41-1페이지의 침입 이벤트 작업의 절차를 수행할 수 있습니다.

단일 포트스캔 이벤트는 여러 패킷을 기반으로 하기 때문에 포트스캔 패킷을 다운로드할 수 없습니다. 그러나 포트스캔 패킷 보기는 사용할 만한 모든 패킷 정보를 제공합니다.

참고 포트스캔 연결 탐지기가 생성하는 이벤트의 경우 프로토콜 번호는 255로 설정됩니다. 포트스캔에는 기본적으로 연결된 특정 프로토콜이 없기 때문에 IANA(Internet Assigned Numbers Authority)에서는 프로토콜 번호를 할당하지 않습니다. IANA에서는 255를 예약 번호로 지정하므로, 이벤트에 대해 연결된 프로토콜이 없음을 나타내기 위해 프로토콜 이벤트에 해당 번호가 사용됩니다.

다음 표에서는 포트스캔 이벤트용 패킷 보기에서 제공하는 정보에 대해 설명합니다. 임의의 IP 주소를 클릭하여 컨텍스트 메뉴를 표시한 다음, 해당 IP 주소에 대해 조회하려면 **whois**를 선택하고 해당 호스트의 호스트 프로필을 보려면 **View Host Profile**을 선택합니다.

표 34-6 포트스캔 패킷 보기

정보	설명
디바이스	이벤트를 탐지한 디바이스.
Time	이벤트가 발생한 시간.
메시지	프리프로세서에 의해 생성된 이벤트 메시지.
소스 IP	스캔하는 호스트의 IP 주소.
대상 IP	스캔되는 호스트의 IP 주소.

표 34-6 포트스캔 패킷 보기(계속)

정보	설명
Priority Count	스캔되는 호스트에서 오는 부정적인 응답(예: TCP RST 및 ICMP 도달 불가)의 수. 부정적인 응답의 수가 많을수록 우선순위 카운트가 높습니다.
Connection Count	호스트의 활성 연결의 수. 이 값은 연결 기반 스캔(예: TCP 및 IP)에 대해 더욱 정확합니다.
IP 수	스캔되는 호스트에 연결하는 IP 주소가 바뀐 횟수. 예를 들어 첫 번째 IP 주소가 10.1.1.1, 두 번째 IP 주소가 10.1.1.2, 세 번째 IP 주소가 10.1.1.1이면 IP Count는 3입니다. 이 숫자는 프록시 및 DNS 서버와 같은 활성 호스트에 대해 덜 정확합니다.
Scanner/Scanned IP Range	스캔 유형에 따라, 스캔되는 호스트 또는 스캔하는 호스트의 IP 주소 범위. 포트스윕의 경우 이 필드에는 스캔되는 호스트의 IP 범위가 표시됩니다. 포트스캔의 경우 이 필드에는 스캔하는 호스트의 IP 범위가 표시됩니다.
Port/Proto 수	TCP 및 UDP 포트스캔의 경우 스캔되는 포트가 변경된 횟수. 예를 들어 첫 번째 스캔되는 포트가 80, 두 번째 스캔되는 포트가 8080, 세 번째 스캔되는 포트가 다시 80이면 Port Count는 3입니다. IP 프로토콜 포트스캔의 경우 스캔되는 호스트에 연결하는 데 사용되는 프로토콜이 변경된 횟수.
Port/Proto 범위	TCP 및 UDP 포트스캔의 경우 스캔된 포트의 범위. IP 프로토콜 포트스캔의 경우 스캔되는 호스트에 연결하려고 시도하는 데 사용된 IP 프로토콜 번호의 범위.
Open Ports	스캔되는 호스트에 열려 있던 TCP 포트. 이 필드는 포트스캔이 하나 이상의 열린 포트를 탐지하는 경우에만 나타납니다.

속도 기반 공격 방지

라이센스: 보호

속도 기반 공격은 반복적인 시도 또는 연결 빈도에 의존하여 자행되는 공격입니다. 속도 기반 공격을 탐지하려면 속도 기반 탐지 기준을 사용하고(공격이 발생하면 발생한 공격에 대응하므로), 그런 다음 공격이 중지되면 일반적인 탐지 설정으로 돌아갈 수 있습니다. 속도 기반 탐지를 구성하는 방법에 대한 자세한 내용은 다음 항목을 참조하십시오.

- 34-10페이지의 속도 기반 공격 방지 이해
- 34-12페이지의 속도 기반 공격 방지 및 기타 필터
- 34-17페이지의 속도 기반 공격 방지 구성
- 32-30페이지의 동적 규칙 상태 이해
- 32-31페이지의 동적 규칙 상태 설정

속도 기반 공격 방지 이해

라이센스: 보호

네트워크의 호스트에서 발생하는 과도한 활동을 탐지하는 속도 기반 필터를 포함하도록 네트워크 분석 정책을 구성할 수 있습니다. 이 기능은 지정된 시간 동안 속도 기반 공격을 차단하기 위해 인라인 모드에서 구축된 관리되는 디바이스에서 사용하고, 그런 다음 이벤트만 생성하고 트래픽을 삭제하지 않는 상태로 돌아갈 수 있습니다.

속도 기반 공격 방지는 비정상적인 트래픽 패턴을 식별하고, 합법적인 요청에 대한 해당 트래픽의 영향을 최소화하도록 시도합니다. 속도 기반 공격은 일반적으로 다음 특성 중 하나를 가지고 있습니다.

- 네트워크의 호스트에 대한 과도하고 불완전한 연결을 포함하는 트래픽(SYN 플러드 공격을 나타냄)

  SYN 공격 탐지를 구성하려면 34-11페이지의 SYN 공격 방지을/를 참조하십시오.

- 네트워크의 호스트에 대한 과도하고 완전한 연결을 포함하는 트래픽(TCP/IP 연결 플러드 공격을 나타냄)

  동시 연결 탐지를 구성하려면 34-12페이지의 동시 연결 제어을/를 참조하십시오.

- 하나 이상의 특정 목적지 IP 주소로 나가거나 하나 이상의 특정 소스 IP 주소에서 들어오는 과도한 규칙 일치.

  소스 또는 목적지 기반 동적 규칙 상태를 구성하려면 32-31페이지의 동적 규칙 상태 설정을/를 참조하십시오.

- 모든 트래픽에서 특정 규칙에 대한 과도한 일치

  규칙 기반 동적 규칙 상태를 구성하려면 32-31페이지의 동적 규칙 상태 설정을/를 참조하십시오.

네트워크 분석 정책에서는 전체 정책에 대해 SYN 플러드 또는 TCP/IP 연결 플러드 탐지를 구성할 수 있습니다. 침입 정책에서는 개별 침입 또는 프리프로세서 규칙에 대해 속도 기반 필터를 설정할 수 있습니다. 규칙 135:1 및 135:2에 수동으로 속도 기반 필터를 추가하면 아무 효과도 없습니다. GID:135의 규칙은 클라이언트를 소스 값으로 사용하고 서버를 목적지 값으로 사용합니다. 자세한 내용은 34-11페이지의 SYN 공격 방지 및 34-12페이지의 동시 연결 제어을/를 참조하십시오.

각 속도 기반 필터에는 여러 구성 요소가 포함되어 있습니다.

- 정책 전반 또는 규칙 기반 소스나 목적지 설정을 위한 네트워크 주소 지정
- 특정 시간(초) 내에 규칙 일치 카운트로서 구성하는 규칙 매칭 속도
- 속도가 초과될 때 수행할 새 작업

  전체 정책에 대해 속도 기반 설정을 구성하면 시스템은 속도 기반 공격 탐지 시 이벤트를 생성하며, 선택적으로 인라인 구축에서 트래픽을 삭제할 수 있습니다. 개별 규칙에 대해 속도 기반 작업을 설정할 경우 Generate Events, Drop and Generate Events 및 Disable의 세 가지 사용 가능한 작업이 있습니다.

- 시간 초과 값으로 구성할 수 있는 작업의 기간

시작되면, 해당 기간 중에 속도가 구성된 값 아래로 떨어지더라도 시간 초과에 도달할 때까지 새 작업이 발생합니다. 시간 초과 기간이 만료되어 속도가 임계값 아래로 떨어지면 규칙에 대한 작업이 규칙에 대해 처음 구성한 작업으로 복구됩니다. 정책 전반 설정의 경우, 작업은 트래픽과 일치하는 각 규칙의 작업으로 돌아갑니다. 일치하는 규칙이 없는 경우 작업이 중지됩니다.

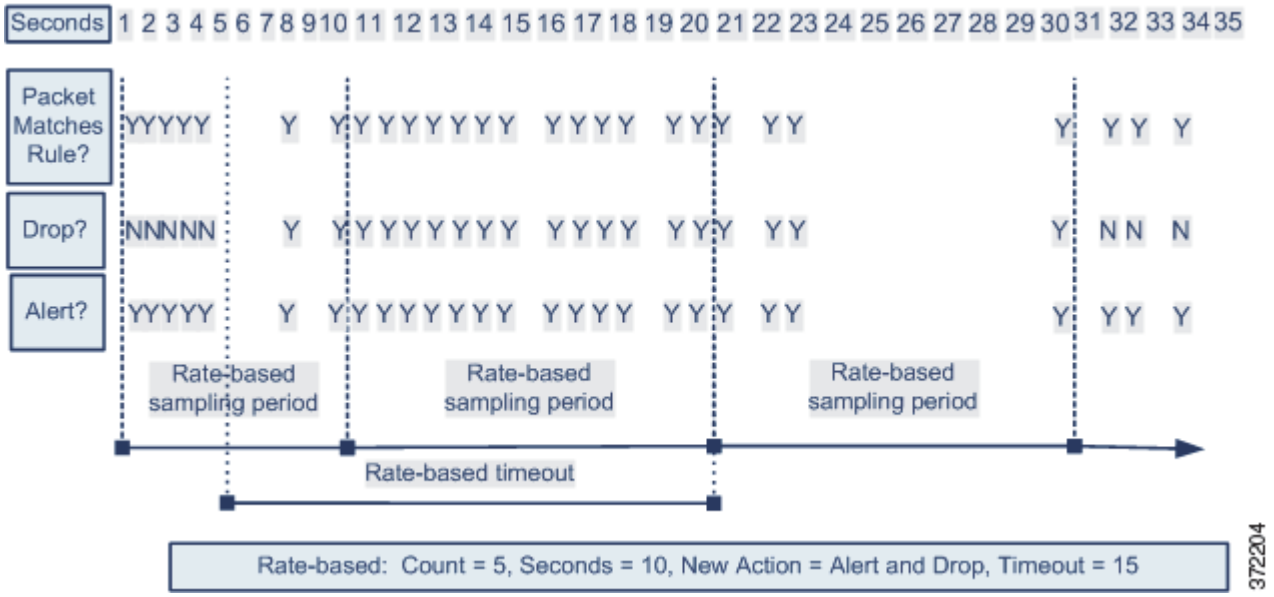
일시적으로 또는 영구적으로 공격을 차단하기 위해 인라인 구축에서 속도 기반 공격 방지를 구성할 수 있습니다. 속도 기반 컨피그레이션 없이 Generate Events로 설정된 규칙은 이벤트를 생성하지만 시스템은 해당 규칙의 패킷을 삭제하지 않습니다. 그러나 공격 트래픽이 속도 기반 기준을 구성한 규칙과 일치하면, 해당 규칙이 처음부터 Drop and Generate Events로 설정되지 않았더라도 속도 작업이 활성 상태로 유지되는 기간에 패킷 삭제가 발생할 수 있습니다.

참고 속도 기반 작업은 비활성화된 규칙을 활성화하거나, 비활성화된 규칙과 일치하는 트래픽을 삭제할 수 없습니다. 그러나 정책 레벨에서 속도 기반 필터를 설정하면, 지정된 기간 내에 과도한 수량의 SYN 패킷 또는 SYN/ACK 상호 작용을 포함하는 트래픽이 발생할 경우 이벤트를 생성하고 해당 트래픽을 삭제할 수 있습니다.

동일한 규칙에서 여러 속도 기반 필터를 정의할 수 있습니다. 침입 정책에 첫 번째로 나열되는 필터의 우선순위가 가장 높습니다. 두 개의 속도 기반 필터 작업이 충돌하면 시스템은 첫 번째 속도 기반 필터의 작업을 구현합니다. 마찬가지로, 필터가 충돌하는 경우 정책 전반의 속도 기반 필터가 개별 규칙에 대해 설정된 속도 기반 필터를 재정의합니다.

다음 다이어그램은 공격자가 호스트에 액세스를 시도하는 예를 보여줍니다. 비밀번호를 찾으려는 시도가 반복되면 속도 기반 공격 방지가 구성된 규칙이 트리거됩니다. 10초 동안 규칙 일치가 5회 발생한 후 속도 기반 설정은 규칙 특성을 Drop and Generate Events로 변경합니다. 새 규칙 특성은 15초 후에 시간 초과됩니다.

시간 초과 후 이어지는 속도 기반 샘플링 기간에도 패킷은 계속 삭제됩니다. 샘플링된 속도가 현재 또는 이전 샘플링 기간의 임계값보다 높으면 새 작업이 계속됩니다. 샘플링된 속도가 임계값 속도 아래로 내려오고 샘플링 기간이 완료된 후에야 비로소 새 작업이 이벤트 생성으로 되돌아갑니다.



SYN 공격 방지

라이센스: 보호

SYN 공격 방지 옵션을 사용하면 SYN 플러드로부터 네트워크 호스트를 보호하는 데 도움이 됩니다. 일정한 기간에 나타나는 패킷 수를 기반으로 개별 호스트 또는 전체 네트워크를 보호할 수 있습니다. 디바이스가 수동적으로 구축된 경우 이벤트를 생성할 수 있습니다. 디바이스가 인라인으로 배치된 경우 악의적인 패킷을 삭제할 수도 있습니다. 시간 초과 기간이 경과한 후 속도 조건이 중지되면 이벤트 생성과 패킷 삭제가 중지됩니다.

예를 들어 어느 한 IP 주소에서 최대 10개의 SYN 패킷을 허용하고, 해당 IP 주소에서 60초 동안 추가 연결을 차단하도록 설정을 구성할 수 있습니다.

이 옵션을 활성화하면 규칙 135:1도 활성화됩니다. 이 규칙을 수동으로 활성화하면 아무 효과도 없습니다. 규칙 상태가 항상 Disabled로 표시되며 절대 바뀌지 않습니다. 이 옵션이 활성화되고 정의된 규칙 조건이 초과되면 규칙이 이벤트를 생성합니다.

동시 연결 제어

라이센스: 보호

DoS(서비스 거부) 공격 또는 사용자의 과도한 활동을 방지하려면 네트워크에 있는 호스트에서 TCP/IP 연결을 제한할 수 있습니다. 시스템은 지정된 IP 주소 또는 주소 범위에서 구성된 수의 성공적인 연결을 탐지하면 추가 연결에 대해 이벤트를 생성합니다. 속도 조건 발생 없이 시간 초과 기간이 경과할 때까지 속도 기반 이벤트 생성이 계속됩니다. 인라인 구축에서 속도 조건이 시간 초과될 때까지 패킷을 삭제하도록 선택할 수 있습니다.

예를 들어 어느 한 IP 주소에서 최대 10개의 성공적인 동시 연결을 허용하고, 해당 IP 주소에서 60초 동안 추가 연결을 차단하도록 설정을 구성할 수 있습니다.

이 옵션을 활성화하면 규칙 135:2도 활성화됩니다. 이 규칙을 수동으로 활성화하면 아무 효과도 없습니다. 규칙 상태가 항상 Disabled로 표시되며 절대 바뀌지 않습니다. 이 옵션이 활성화되고 정의된 규칙 조건이 초과되면 규칙이 이벤트를 생성합니다.

속도 기반 공격 방지 및 기타 필터

라이센스: 보호

`detection_filter` 필터링과 임계값 지정 및 억제 기능은 트래픽 자체 또는 시스템이 생성하는 이벤트를 필터링할 다른 방법을 제공합니다. 속도 기반 공격 방지를 단독으로 사용할 수도 있고 임계값 지정, 억제 또는 `detection_filter` 키워드와 함께 사용할 수도 있습니다.

자세한 내용은 다음 예을/를 참조하십시오.

- 34-12페이지의 속도 기반 공격 방지 및 탐지 필터링
- 34-13페이지의 동적 규칙 상태 및 임계값 지정 또는 억제
- 34-14페이지의 정책 전반의 속도 기반 탐지 임계값 지정 또는 억제
- 34-16페이지의 속도 기반 탐지 및 여러 필터링 방법

속도 기반 공격 방지 및 탐지 필터링

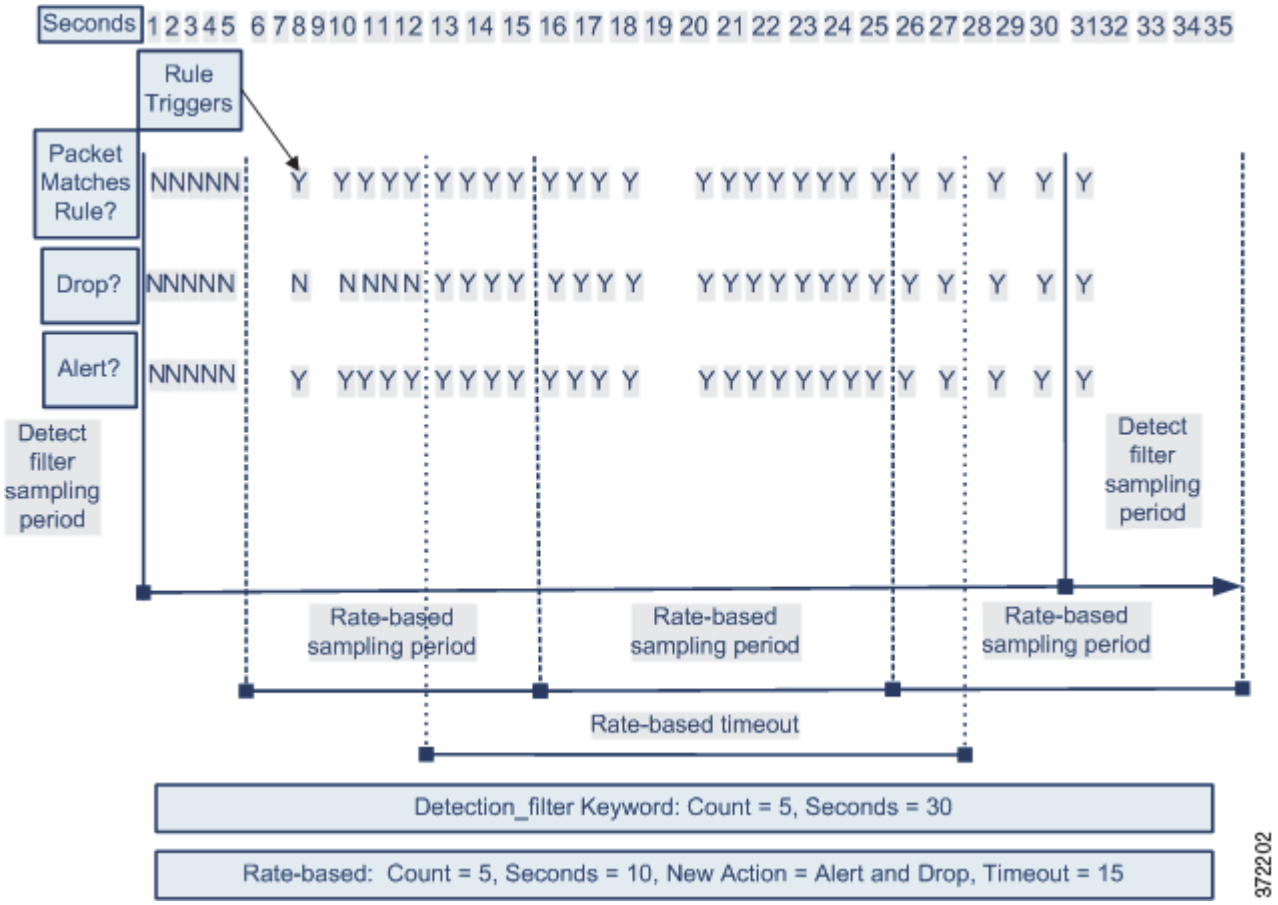
라이센스: 보호

`detection_filter` 키워드는 지정된 시간 내에 임계값 수의 규칙 일치가 발생할 때까지 규칙이 트리거되는 것을 방지합니다. 규칙에 `detection_filter` 키워드가 포함되면 시스템은 시간 초과 기간당 규칙의 패턴과 일치하는 수신 패킷의 수를 추적합니다. 시스템은 특정 소스 또는 목적지 IP 주소에서 해당 규칙에 대한 히트 수를 계산할 수 있습니다. 속도가 규칙의 속도를 초과하면 해당 규칙에 대한 이벤트 알림이 시작됩니다.

다음 예는 공격자의 무차별 암호 대입(brute-force) 로그인 시도를 보여줍니다. 비밀번호를 찾으려는 시도가 반복되면 카운트가 5로 설정된 `detection_filter` 키워드가 포함된 규칙이 트리거됩니다. 이 규칙에는 속도 기반 공격 방지가 구성되어 있습니다. 10초 동안 규칙에 대한 히트가 5회 발생하는 경우 속도 기반 설정은 20초 동안 규칙 특성을 Drop and Generate Events로 변경합니다.

다이어그램에 나와 있듯이, `detection_filter` 키워드로 표시된 속도를 초과할 때까지 규칙이 트리거되지 않으므로 규칙과 일치하는 처음 5개 패킷은 이벤트를 생성하지 않습니다. 규칙이 트리거된 후 이벤트 알림이 시작되지만, 속도 기반 기준은 5개 패킷이 더 전달될 때까지 Drop and Generate Events의 새 작업을 트리거하지 않습니다.

속도 기반 기준이 충족되면 속도 기반 시간 초과 기간이 만료되고 속도가 임계값 아래로 떨어질 때까지 이벤트가 생성되고 패킷이 삭제됩니다. 20초 경과 후에는 속도 기반 작업이 시간 초과됩니다. 시간 초과 후 이어지는 속도 기반 샘플링 기간에도 패킷은 계속 삭제됩니다. 시간 초과가 발생할 경우 샘플링된 속도는 이전 샘플링 기간의 임계값 속도보다 높으므로 속도 기반 작업이 계속됩니다.



예제에는 이 내용이 없지만, Drop and Generate Events 규칙 상태를 `detection_filter` 키워드와 함께 사용하여 규칙에 대한 히트 수가 지정된 속도에 도달할 때 트래픽 삭제를 시작할 수 있습니다. 규칙에 대한 속도 기반 설정의 구성 여부를 결정할 때에는 규칙을 Drop and Generate Events로 설정하고 `detection_filter` 키워드를 포함할 경우 동일한 결과를 얻을 수 있는지, 침입 정책에서 속도 및 시간 초과 설정을 관리하고자 하는지를 고려하십시오. 자세한 내용은 32-20페이지의 규칙 상태 설정을/를 참조하십시오.

동적 규칙 상태 및 임계값 지정 또는 억제

라이센스: 보호

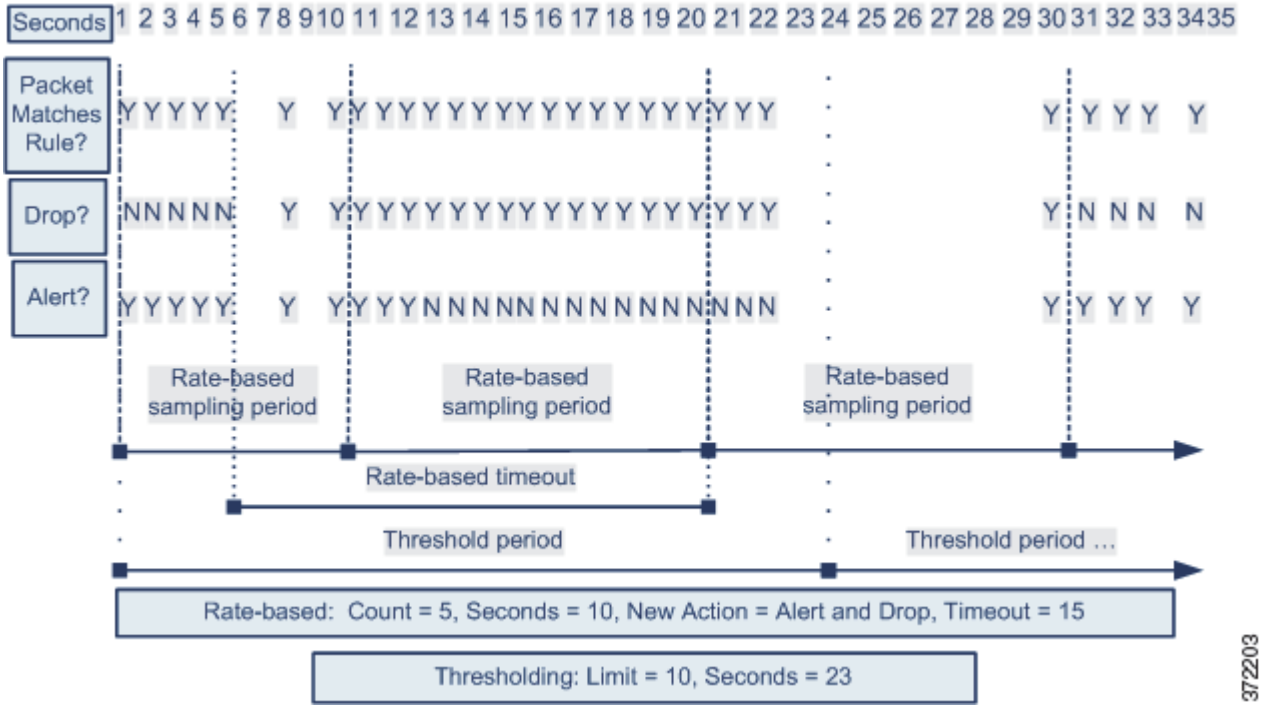
임계값 지정 및 억제를 사용하면 규칙에 대한 이벤트 알림의 수를 제한하고 해당 규칙에 대한 알림을 완전히 억제함으로써 과도한 이벤트를 줄일 수 있습니다. 임계값 지정 및 억제에 사용할 수 있는 옵션에 대한 자세한 내용은 32-22페이지의 이벤트 임계값 구성 및 32-26페이지의 침입 정책당 억제 구성을/를 참조하십시오.

규칙에 억제를 적용하면 시스템은 속도 기반 작업 변경이 발생하더라도 모든 해당 IP 주소에 대해 해당 규칙의 이벤트 알림을 억제합니다. 그러나 임계값 지정과 속도 기반 기준의 상호 작용은 좀 더 복잡해집니다.

다음 예는 공격자의 무차별 암호 대입(brute-force) 로그인 시도를 보여줍니다. 비밀번호를 찾으려는 시도가 반복되면 속도 기반 공격 방지가 구성된 규칙이 트리거됩니다. 10초 동안 규칙에 대한 히트가 5회 발생하는 경우 속도 기반 설정은 15초 동안 규칙 특성을 Drop and Generate Events로 변경합니다. 또한 제한 임계값은 규칙이 생성할 수 있는 이벤트의 수를 23초에 10개로 제한합니다.

다이어그램에 나와 있듯이 규칙은 처음 5개의 일치하는 패킷에 대해 이벤트를 생성합니다. 5개 패킷 이후 속도 기반 기준은 Drop and Generate Events의 새 작업을 트리거하며, 다음 5개 패킷에 대해 규칙은 이벤트를 생성하고 시스템은 패킷을 삭제합니다. 10번째 패킷 이후 제한 임계값에 도달하면, 시스템은 나머지 패킷에 대해 이벤트를 생성하지 않지만 패킷은 삭제합니다.

시간 초과 후 이어지는 속도 기반 샘플링 기간에도 패킷은 계속 삭제됩니다. 샘플링된 속도가 현재 또는 이전 샘플링 기간의 임계값 속도보다 높으면 새 작업이 계속됩니다. 샘플링된 속도가 임계값 속도 아래로 내려오고 샘플링 기간이 완료된 후에야 비로소 새 작업이 Generate Events로 되돌아갑니다.



이 예에는 나와 있지 않지만, 임계값에 도달한 *이후* 속도 기반 기준 때문에 새 작업이 트리거되면 시스템은 작업 변경을 알리는 단일 이벤트를 생성합니다. 예를 들어 제한 임계값 10에 도달하여 시스템이 이벤트 생성을 중지하고 14번째 패킷에서 작업이 Generate Events에서 Drop and Generate Events로 변경되면, 시스템은 작업 변경을 알리는 11번째 이벤트를 생성합니다.

정책 전반의 속도 기반 탐지 임계값 지정 또는 억제

라이센스: 보호

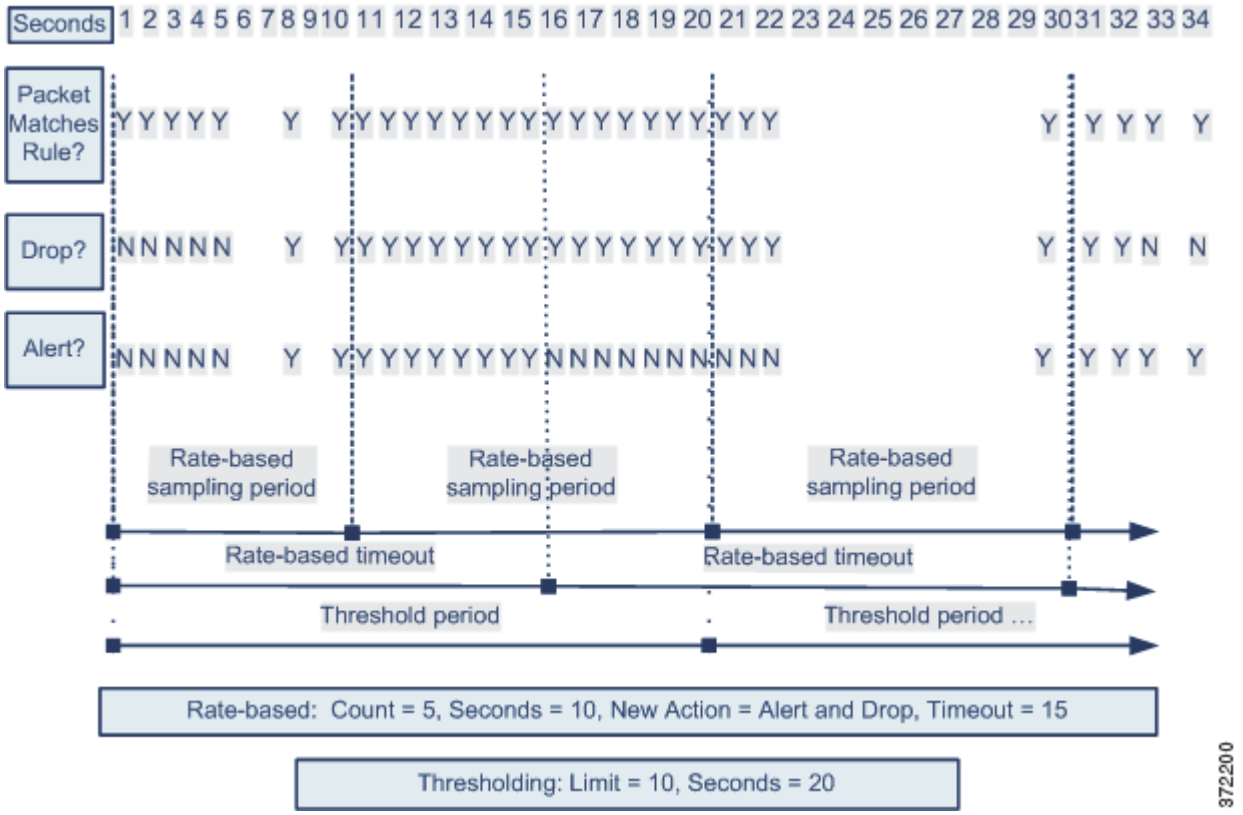
임계값 지정 및 억제를 사용하면 소스나 목적지에 대한 이벤트 알림의 수를 제한하고 해당 규칙에 대한 알림을 완전히 억제함으로써 과도한 이벤트를 줄일 수 있습니다. 임계값 지정 및 억제에 사용할 수 있는 옵션에 대한 자세한 내용은 35-3페이지의 전역 임계값 구성, 32-22페이지의 이벤트 임계값 구성 및 32-26페이지의 침입 정책당 억제 구성을/를 참조하십시오.

규칙에 억제가 적용되면, 정책 전반의 또는 규칙 단위의 속도 기반 설정 때문에 속도 기반 작업 변경이 발생하더라도 모든 해당 IP 주소에 대해 해당 규칙의 이벤트 알림이 억제됩니다. 그러나 임계값 지정과 속도 기반 기준의 상호 작용은 좀 더 복잡해집니다.

다음 예는 공격자가 네트워크의 호스트에서 DoS(서비스 거부) 공격을 시도하는 경우를 보여줍니다. 동일한 소스에서 호스트에 동시에 다수가 연결하면 정책 전반의 Control Simultaneous Connections 설정이 트리거됩니다. 10초에 한 소스에서 5개 연결이 발생하면 이벤트가 생성되고 악성 트래픽이 삭제됩니다. 또한 전역 제한 임계값은 규칙 또는 설정이 생성할 수 있는 이벤트의 수를 20초에 10개로 제한합니다.

다이어그램에 나와 있듯이, 정책 전반의 설정은 처음 10개의 일치하는 패킷에 대해 이벤트를 생성하고 트래픽을 삭제합니다. 10번째 패킷 이후 제한 임계값에 도달하면, 나머지 패킷에 대해 이벤트는 생성되지 않지만 패킷은 삭제됩니다.

시간 초과 후 이어지는 속도 기반 샘플링 기간에도 패킷은 계속 삭제됩니다. 샘플링된 속도가 현재 또는 이전 샘플링 기간의 임계값 속도보다 높으면, 이벤트를 생성하고 트래픽을 삭제하는 속도 기반 작업이 계속됩니다. 샘플링된 속도가 임계값 속도 아래로 내려오고 샘플링 기간이 완료된 후에야 비로소 속도 기반 작업이 중지됩니다.



이 예에는 나와 있지 않지만, 임계값에 도달한 *이후* 속도 기반 기준 때문에 새 작업이 트리거되면 시스템은 작업 변경을 알리는 단일 이벤트를 생성합니다. 예를 들어 제한 임계값 10에 도달하여 시스템이 이벤트 생성을 중지하고 14번째 패킷에서 작업이 Drop and Generate Events로 변경되면, 시스템은 작업 변경을 알리는 11번째 이벤트를 생성합니다.

속도 기반 탐지 및 여러 필터링 방법

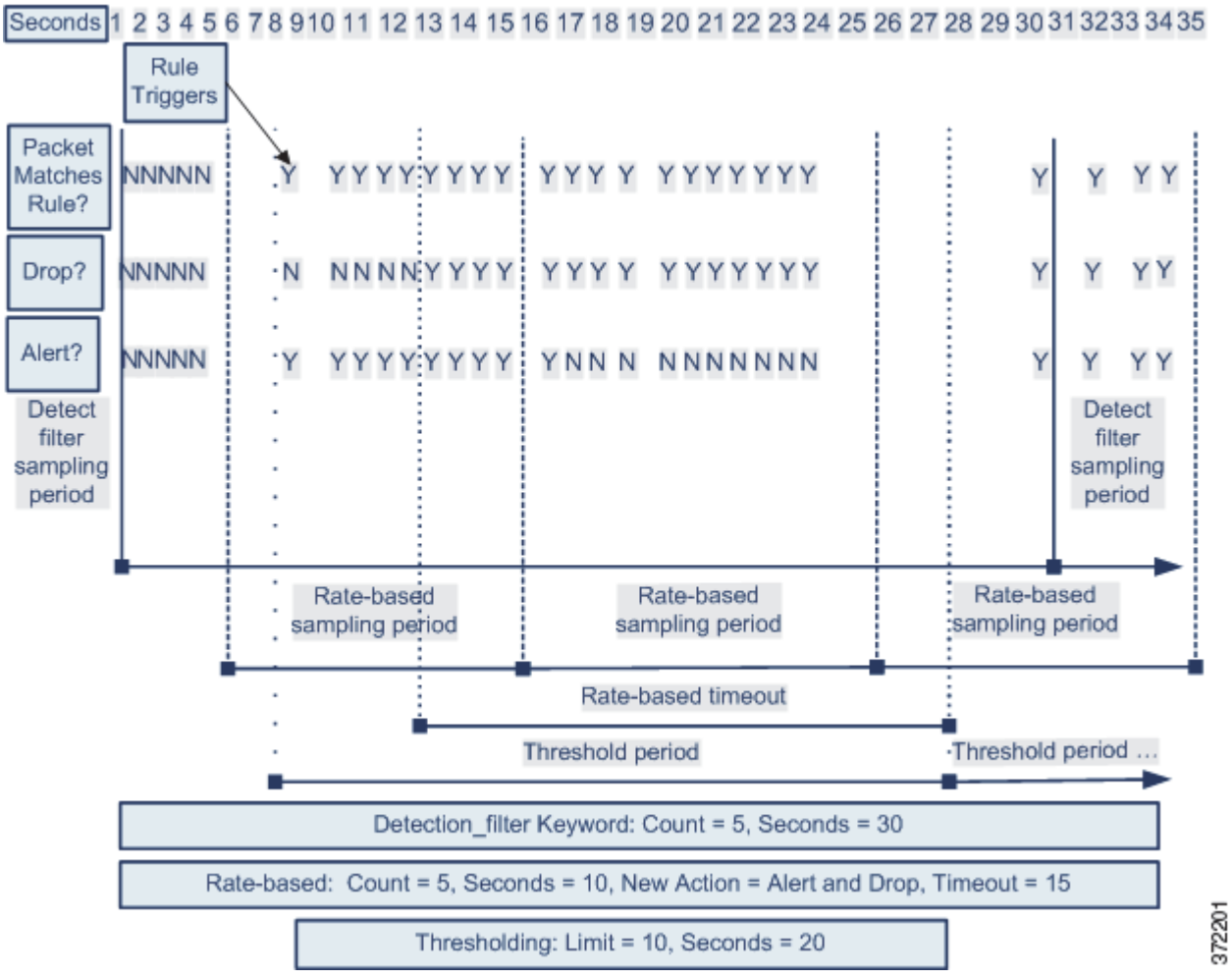
라이센스: 보호

`detection_filter` 키워드, 임계값 지정 또는 억제, 속도 기반 기준이 동일한 트래픽이 모드 적용되는 상황이 발생할 수 있습니다. 규칙에 대해 억제를 활성화하면 속도 기반 변경이 발생하더라도 지정된 IP 주소에 대해 이벤트가 억제됩니다.

다음 예에서는 공격자가 무차별 암호 대입 로그인을 시도하는 경우를 보여주며, `detection_filter` 키워드, 속도 기반 필터링, 임계값 지정이 상호 작용하는 경우에 대해 설명합니다. 비밀번호를 찾으려는 시도가 반복되면 카운트가 5로 설정된 `detection_filter` 키워드가 포함된 규칙이 트리거됩니다. 이 규칙은 또한 15초 동안 규칙 히트가 5회 발생하는 경우 30초 동안 규칙 특성을 Drop and Generate Events로 변경하는 속도 기반 공격 방지 설정을 가지고 있습니다. 또한 제한 임계값은 30초에 이벤트 10개로 규칙을 제한합니다.

다이어그램에 나와 있듯이, `detection_filter` 키워드로 표시된 속도를 초과할 때까지 규칙이 트리거되지 않으므로 규칙과 일치하는 처음 5개 패킷은 이벤트 알림을 생성하지 않습니다. 규칙이 트리거된 후 이벤트 알림이 시작되지만, 속도 기반 기준은 5개 패킷이 더 전달될 때까지 Drop and Generate Events의 새 작업을 트리거하지 않습니다. 속도 기반 기준이 충족되면 시스템은 패킷 11-15에 대해 이벤트를 생성하고 패킷을 삭제합니다. 15번째 패킷 이후 제한 임계값에 도달하면, 시스템은 나머지 패킷에 대해 이벤트를 생성하지 않지만 패킷은 삭제합니다.

규칙 기반 시간 초과 후 이어지는 속도 기반 샘플링 기간에도 패킷은 계속 삭제됩니다. 샘플링된 속도가 이전 샘플링 기간의 임계값 속도보다 높으므로 새 작업이 계속됩니다.



속도 기반 공격 방지 구성

라이센스: 보호

SYN 플러드 공격을 중지하려면 정책 레벨에서 속도 기반 공격 방지를 구성할 수 있습니다. 특정 소스에서의 과도한 연결 또는 특정 목적지로의 과도한 연결도 중지할 수 있습니다.

속도 기반 공격 방지를 구성하려면

Admin/Intrusion Admin

1단계 **Policies > Access Control > Access Control Policy**를 선택하여 Access Control Policy 페이지를 표시한 다음 **Network Analysis Policy**를 클릭합니다.

Network Analysis Policy 페이지가 나타납니다.

2단계 수정할 정책 옆에 있는 수정 아이콘( )을 클릭합니다.

다른 정책에 저장하지 않은 변경 사항이 있는 경우 변경 사항을 취소하고 계속 진행하려면 **OK**를 클릭합니다. 저장하지 않은 변경 사항을 다른 정책에 저장하는 방법에 대한 자세한 내용은 23-15페이지의 충돌 해결 및 정책 변경 사항 커밋을/를 참조하십시오.

Policy Information 페이지가 나타납니다.

3단계 왼쪽의 탐색 패널에서 **Settings**를 클릭합니다.

Settings 페이지가 나타납니다.

4단계 **Specific Threat Detection** 아래에서 **Rate-Based Attack Prevention**이 활성화되었는지 여부에 따라 두 가지 선택 사항이 있습니다.

- 컨피그레이션이 활성화되어 있으면 **Edit**를 클릭합니다.
- 컨피그레이션이 비활성화되어 있으면 **Enabled**를 클릭한 다음 **Edit**를 클릭합니다.

Rate-Based Attack Prevention 페이지가 나타납니다. 페이지 하단에 있는 메시지는 컨피그레이션이 포함된 침입 정책 레이어를 식별합니다. 자세한 내용은 24-1페이지의 네트워크 분석 또는 침입 정책에서 레이어 사용을/를 참조하십시오.

5단계 다음 2가지 옵션을 사용할 수 있습니다.

- 호스트 플러드를 의도하는 불완전한 연결을 방지하려면 **SYN Attack Prevention** 아래에서 **Add**를 클릭합니다.

  SYN Attack Prevention 대화 상자가 나타납니다.

- 과도한 수의 연결을 방지하려면 **Control Simultaneous Connections** 아래에서 **Add**를 클릭합니다.

  Control Simultaneous Connections 대화 상자가 나타납니다.

6단계 트래픽을 추적할 방법을 선택합니다.

- 특정 소스 또는 소스 범위의 모든 트래픽을 추적하려면 **Track By** 드롭다운 목록에서 **Source**를 선택하고 **Network** 필드에 단일 IP 주소 또는 주소 블록을 입력합니다.
- 특정 목적지 또는 목적지 범위의 모든 트래픽을 추적하려면 **Track By** 드롭다운 목록에서 **Destination**을 선택하고 **Network** 필드에 단일 IP 주소 또는 주소 블록을 입력합니다.

시스템은 Network 필드에 포함된 각 IP 주소에 대해 별도로 트래픽을 추적합니다. 특정 IP 주소의 트래픽이 구성된 속도를 초과하면 해당 IP 주소에 대해서만 이벤트가 생성됩니다. 예를 들어 네트워크 설정에 대해 소스 CIDR 블록 `10.1.0.0/16`을 설정하고, 10개의 동시 연결이 열릴 때 이벤트를 생성하도록 시스템을 구성한다고 가정해보겠습니다. 10.1.4.21에서 8개의 연결이 열리고 10.1.5.10에서 6개가 열리면, 두 소스 모두 열린 연결의 트리거링 수에 도달하지 않았으므로 이벤트가 생성되지 않습니다. 그러나 10.1.4.21에서 11개의 동시 연결이 열리면 10.1.4.21의 연결에 대해서만 이벤트가 생성됩니다.

FireSIGHT 시스템에서 CIDR 표기법 및 접두사 길이를 사용하는 방법에 대한 자세한 내용은 1-19 페이지의 IP 주소 표기 규칙을/를 참조하십시오.

7단계 속도 추적 설정에 대한 트리거링 속도를 지정합니다.

- SYN 공격 컨피그레이션의 경우 **Rate** 필드에 초당 SYN 패킷 수를 지정합니다.
- 동시 연결 컨피그레이션의 경우 **Count** 필드에 연결 수를 지정합니다.

8단계 속도 기반 공격 방지 설정과 일치하는 패킷을 삭제하려면 **Drop**을 선택합니다.

9단계 SYN의 일치 패턴 또는 동시 연결이 있는 트래픽에 대해 이벤트 생성 및 삭제(해당되는 경우)를 중지할 경과 시간을 **Timeout** 필드에 입력합니다.

주의 Timeout 값은 1~1,000,000의 정수입니다. 그러나 시간 초과 값을 높게 설정하면 인라인 구축의 호스트에 대한 연결이 완전히 차단될 수 있습니다.

10단계 정책을 저장하거나, 계속 수정하거나, 변경 사항을 취소하거나, 시스템 캐시에 변경 사항이 남아 있는 상태로 종료합니다. 자세한 내용은 23-15페이지의 충돌 해결 및 정책 변경 사항 커밋을/를 참조하십시오.

민감한 데이터 탐지

라이센스: 보호

주민등록번호, 신용카드 번호, 운전면허증 번호 같은 민감한 정보가 인터넷에 고의적으로 또는 실수로 유출될 수 있습니다. 이 시스템에서는 ASCII 텍스트로 된 민감한 데이터에 대한 이벤트를 탐지하고 생성할 수 있는 민감한 데이터 프리프로세서를 제공하며, 이는 실수로 인한 데이터 유출을 탐지할 때 특히 유용합니다.

시스템에서는 암호화되거나 위장된 형태의 민감한 데이터나 압축 또는 인코딩된 형식(예: Base64 인코딩 이메일 첨부 파일)의 민감한 데이터를 탐지하지 않습니다. 예를 들어 시스템이 전화 번호 (555)123-4567을 탐지했지만, (5 5 5) 1 2 3 - 4 5 6 7과 같이 공백으로 각 번호가 구분되거나 (555)-123-4567과 같이 HTML 코드가 포함된 애매한 버전이 아닌 경우를 가정해보겠습니다. 그러나 시스템은 중간 코드가 번호 패턴을 방해하지 않는 HTML 코드 번호 (555)-123-4567을 탐지할 수 있습니다.

팁 민감한 데이터 프리프로세서는 FTP 또는 HTTP를 사용하여 업로드 및 다운로드되는 암호화되지 않은 Microsoft Word 파일에서 민감한 데이터를 탐지할 수 있습니다. 이는 ASCII 텍스트 및 형식 지정 명령을 별도로 그룹화하는 방식 때문에 가능합니다.

시스템에서는 개별 데이터 유형을 트래픽과 일치시켜 TCP 세션당 민감한 데이터를 탐지합니다. 각 데이터 유형에 대한 기본 설정 및 침입 정책의 모든 데이터 유형에 적용되는 전역 옵션에 대한 기본 설정을 수정할 수 있습니다. Cisco에서는 일반적으로 사용되는 사전 정의된 데이터 유형을 제공합니다. 사용자 지정 데이터 유형을 생성할 수도 있습니다.

민감한 데이터 프리프로세서 규칙은 각 데이터 유형과 연결됩니다. 데이터 유형에 해당하는 프리프로세서 규칙을 활성화하여 각 데이터 유형에 민감한 데이터 탐지 및 이벤트 생성을 활성화할 수 있습니다. 컨피그레이션 페이지의 링크를 클릭하면 Rules 페이지에 있는 민감한 데이터 규칙의 필터링된 보기가 나타납니다. 여기에서 규칙을 활성화 및 비활성화하고 다른 규칙 특성을 구성할 수 있습니다.

침입 정책에 대한 변경 사항을 저장하면, 데이터 유형과 관련된 규칙이 활성화되고 민감한 데이터 탐지가 비활성화되는 경우 민감한 데이터 프리프로세서를 자동으로 활성화할 수 있는 옵션이 제공됩니다.

자세한 내용은 다음 절을 참조하십시오.

민감한 데이터 탐지 구축

라이센스: 보호

민감한 데이터 탐지는 FireSIGHT 시스템의 성능에 큰 영향을 미칠 수 있으므로 Cisco에서는 다음 지침을 따를 것을 권장합니다.

- 기본 침입 정책으로 No Rules Active 기본 정책을 선택합니다. 자세한 내용은 24-3페이지의 시스템 제공 기반 정책 이해을/를 참조하십시오.
- 다음 설정이 해당 네트워크 분석 정책에서 활성화되었는지 확인합니다.
  - **Application Layer Preprocessors** 아래의 **FTP and Telnet Configuration**
  - **Transport/Network Layer Preprocessors** 아래의 **IP Defragmentation** 및 **TCP Stream Configuration**
- 민감한 데이터 컨피그레이션이 포함된 침입 정책을 포함하는 액세스 제어 정책을 민감한 데이터 탐지에 예약된 별도의 디바이스에 적용합니다. 자세한 내용은 12-15페이지의 액세스 제어 정책 적용을/를 참조하십시오.

전역 민감한 데이터 탐지 옵션 선택

라이센스: 보호

글로벌 민감한 데이터 프리프로세서 옵션은 프리프로세서의 작동 방식을 제어합니다. 다음을 지정하는 전역 옵션을 수정할 수 있습니다.

- 프리프로세서가 트리거링 패킷에서 신용카드 번호 마지막 4자리를 제외한 모두 또는 주민등록번호를 교체할지 여부
- 민감한 데이터를 모니터링할 네트워크의 목적지 호스트
- 이벤트가 되기 위해 단일 세션에서 발생해야 하는 모든 데이터 유형의 수

전역 민감한 데이터 옵션은 정책 단위이며 모든 데이터 유형에 적용됩니다.

다음과 같은 전역 민감한 데이터 탐지 옵션을 구성할 수 있습니다.

Mask

트리거링 패킷에서 신용카드 번호의 마지막 4자리를 제외한 모두 및 주민등록번호를 X로 교체합니다. 웹 인터페이스의 침입 이벤트 패킷 보기 및 다운로드된 패킷에 마스크 처리된 숫자가 나타납니다. 자세한 내용은 41-22페이지의 패킷 보기 사용을/를 참조하십시오.

Networks

민감한 데이터를 모니터링할 하나 이상의 목적지 호스트를 지정합니다. 단일 IP 주소나 주소 블록 또는 쉼표로 구분된 목록(둘 중 하나 또는 모두)을 지정할 수 있습니다. 시스템은 빈 필드를 any, 즉 모든 목적지 IP 주소로 해석합니다. FireSIGHT 시스템에서 IPv4 및 IPv6 주소 블록을 사용하는 방법에 대한 자세한 내용은 1-19페이지의 IP 주소 표기 규칙을/를 참조하십시오.

Global Threshold

전역 임계값 이벤트를 생성하기 전에 프리프로세서가 탐지해야 하는, 단일 세션 중 발생하는 모든 데이터 유형의 총수를 지정합니다. 1~65535를 지정할 수 있습니다.

Cisco에서는 이 옵션의 값을 정책에서 활성화하는 개별 데이터 유형에 대한 가장 높은 임계값보다 더 높게 설정할 것을 권장합니다. 자세한 내용은 34-21페이지의 개별 데이터 유형 옵션 선택을/를 참조하십시오.

전역 임계값에 대한 다음 사항에 유의하십시오.

- 데이터 유형 발생을 조합하여 이벤트를 탐지 및 생성하려면 프리프로세서 규칙 139:1을 활성화해야 합니다. 침입 규칙에서 규칙을 활성화하는 방법에 대한 자세한 내용은 32-20페이지의 규칙 상태 설정을/를 참조하십시오.
- 프리프로세서는 세션당 최대 하나의 전역 임계값 이벤트를 생성합니다.
- 전역 임계값 이벤트는 개별 데이터 유형 이벤트와는 별개입니다. 즉, 개별 데이터 유형에 대한 이벤트 임계값에 도달했는지와 상관없이 프리프로세서는 전역 임계값에 도달할 때 이벤트를 생성합니다. 그 반대의 경우도 마찬가지입니다.

개별 데이터 유형 옵션 선택

라이센스: 보호

개별 데이터 유형은 사용자가 탐지할 수 있는 민감한 데이터를 식별하고, 지정된 목적지 네트워크 트래픽에서 이벤트를 생성합니다. 다음을 지정하는 데이터 유형 옵션에 대한 기본 설정을 수정할 수 있습니다.

- 단일 세션당 이벤트 생성을 위해 탐지된 데이터 유형에 대해 충족해야 하는 임계값
- 각 데이터 유형을 모니터링할 목적지 포트
- 각 데이터 유형을 모니터링할 애플리케이션 프로토콜

최소한 각 데이터 유형은 이벤트 임계값 및 모니터링할 하나 이상의 포트 또는 애플리케이션 프로토콜을 지정해야 합니다.

Cisco에서 제공하는 사전 정의된 각 데이터 유형은 달리 액세스할 수 없는 `sd_pattern` 키워드를 사용하여, 트래픽에서 탐지할 내장형 데이터 패턴을 정의합니다. 사전 정의된 데이터 유형 목록은 34-23 페이지의 표 34-8을/를 참조하십시오. 고유한 데이터 패턴을 지정하기 위해 단순한 정규식을 사용할 사용자 지정 데이터 유형을 생성할 수도 있습니다. 자세한 내용은 34-28페이지의 사용자 지정 데이터 유형 사용을/를 참조하십시오.

데이터 유형 이름 및 패턴은 시스템 전체에 적용되며, 다른 모든 데이터 유형 옵션은 정책에만 적용됩니다.

다음 표에서는 구성할 수 있는 데이터 유형 옵션에 대해 설명합니다.

표 34-7 개별 데이터 유형 옵션

옵션	설명
데이터유형	데이터 유형의 고유한 이름을 표시합니다.
임계값	시스템이 이벤트를 생성할 때 발생해야 할 데이터 유형의 수를 지정합니다. 활성화된 데이터 유형에 대한 임계값을 설정하지 않으면 정책을 저장할 때 오류 메시지가 표시됩니다. 1~255를 지정할 수 있습니다. 프리프로세서는 세션당 탐지된 데이터 유형에 대해 하나의 이벤트를 생성합니다. 전역 임계값 이벤트는 개별 데이터 유형 이벤트와는 별개입니다. 즉, 전역 이벤트 임계값에 도달했는지와 상관없이 프리프로세서는 데이터 유형 이벤트 임계값에 도달할 때 이벤트를 생성합니다. 그 반대의 경우도 마찬가지입니다.

표 34-7 개별 데이터 유형 옵션(계속)

옵션	설명
대상 포트	데이터 유형을 모니터링할 목적지 포트를 지정합니다. 단일 포트, 쉼표로 구분된 포트 목록 또는 any(모든 목적지 포트)를 지정할 수 있습니다. 데이터 유형에 대해 하나 이상의 포트 또는 애플리케이션 프로토콜을 설정하지 않고 데이터 유형에 대한 규칙을 활성화하면 정책을 저장할 때 오류 메시지가 표시됩니다.
애플리케이션 프로토콜 이 기능을 사용하려면 제어 라이센스가 필요합니다.	데이터 유형을 모니터링할 최대 8개의 애플리케이션 프로토콜을 지정합니다. 데이터 유형에 대해 하나 이상의 포트 또는 애플리케이션 프로토콜을 설정하지 않고 데이터 유형에 대한 규칙을 활성화하면 정책을 저장할 때 오류 메시지가 표시됩니다. 선택한 각 애플리케이션 프로토콜에 대해 하나 이상의 탐지기가 활성화되어야 합니다(46-27페이지의 탐지기 활성화 및 비활성화 참조). 기본적으로 모든 Cisco 제공 탐지기는 활성화되어 있습니다. 어떤 애플리케이션 프로토콜에 대해 활성화된 탐지기가 없을 경우 자동으로 모든 Cisco 제공 탐지기가 해당 애플리케이션에 대해 활성화됩니다. 탐지기가 하나도 없을 경우 가장 최근에 수정된 사용자 정의 탐지기가 이 애플리케이션에 대해 활성화됩니다. 데이터 유형에 대해 애플리케이션 프로토콜을 선택하는 방법에 대한 자세한 내용은 34-26페이지의 모니터링할 애플리케이션 프로토콜 선택을/를 참조하십시오.
패턴	사용자 지정 데이터 유형에서 탐지하도록 지정된 패턴(Cisco에서 제공하는 데이터 유형의 데이터 패턴은 미리 정의됨). 자세한 내용은 34-28페이지의 사용자 지정 데이터 유형 사용을/를 참조하십시오. 웹 인터페이스에는 사전 정의된 데이터 유형에 대한 내장형 패턴이 표시되지 않습니다. 사용자 지정 및 사전 정의된 데이터 패턴은 시스템 전체에 적용됩니다.

사전 정의된 데이터 유형 사용

라이센스: 보호

각 침입 정책에는 신용카드 번호, 이메일 주소, 전화 번호, 주민등록번호(대시 포함 또는 포함하지 않음) 등 일반적으로 사용되는 데이터 패턴을 탐지하기 위한 사전 정의된 데이터 유형이 포함되어 있습니다. 사전 정의된 각 데이터 유형은 GID(generator ID) 138의 단일 민감한 데이터 프리프로세서 규칙과 연결됩니다. 정책에서 사용할 각 데이터 유형에 대해, 탐지를 활성화할 침입 정책의 관련된 민감한 데이터 규칙 및 이벤트 생성을 활성화해야 합니다. 침입 규칙에서 규칙을 활성화하는 방법에 대한 자세한 내용은 32-20페이지의 규칙 상태 설정을/를 참조하십시오.

민감한 데이터 규칙의 활성화에 도움이 되도록 컨피그레이션 페이지에서 제공되는 링크를 클릭하면 모든 사용자 지정 및 사전 정의된 민감한 데이터 규칙을 표시하는 Rules 페이지의 필터링된 보기가 나타납니다. Rules 페이지에서 민감한 데이터 규칙 필터링 카테고리를 선택하여 사전 정의된 민감한 데이터 규칙만 표시할 수도 있습니다. 자세한 내용은 32-10페이지의 침입 정책의 규칙 필터링을/를 참조하십시오. 사전 정의된 민감한 데이터 규칙은 Rule Editor 페이지(**Policies > Intrusion > Rule Editor**)에도 나열됩니다. 이곳의 민감한 데이터 규칙 카테고리에서는 규칙을 볼 수는 있지만 수정할 수는 없습니다.

다음 표에서는 각 데이터 유형에 대해 설명하고, 데이터 유형에 대한 탐지와 이벤트 생성을 위해 활성화해야 할 해당 프리프로세서 규칙을 나열합니다.

표 34-8 민감한 데이터 유형

데이터유형	설명	프리프로세서 규칙 GID:SID
신용 카드 번호	표준 구분 대시나 공백을 사용하거나 사용하지 않고 Visa®, MasterCard®, Discover® 및 American Express® 15/16자리 신용카드 번호를 매칭합니다. 또한 Luhn 알고리즘을 사용하여 신용카드 체크 숫자를 확인합니다.	138:2
이메일 주소	이메일 주소를 매칭합니다.	138:5
미국 전화 번호	미국 전화 번호를 `(\d{3}) ?\d{3}-\d{4}` 패턴에 따라 매칭합니다.	138:6
미국 Social Security 번호(대시 없음)	9자리 미국 Social Security 번호를 매칭합니다(유효한 3자리 지역 숫자, 유효한 2자리 그룹 번호, 대시 없음).	138:4
미국 Social Security 번호(대시 있음)	9자리 미국 Social Security 번호를 매칭합니다(유효한 3자리 지역 숫자, 유효한 2자리 그룹 번호, 대시 있음).	138:3
사용자 지정	지정된 트래픽에서 사용자 정의 데이터 패턴을 매칭합니다. 자세한 내용은 34-28페이지의 사용자 지정 데이터 유형 사용을/를 참조하십시오.	138:>999999

Social Security 번호 외 9자리 번호에서 오탐을 줄이기 위해 프리프로세서는 각 Social Security 번호에서 4자리 일련 번호 앞에 오는 3자리 지역 번호와 2자리 그룹 번호를 검증하는 알고리즘을 사용합니다. 프리프로세서는 2009년 11월까지 Social Security 그룹 번호를 검증합니다.

민감한 데이터 탐지 구성

라이센스: 보호

기본 전역 설정 및 개별 데이터 유형에 대한 설정을 수정할 수 있습니다. 또한 탐지할 각 데이터 유형에 대해 프리프로세서 규칙을 활성화해야 합니다.

민감한 데이터 탐지를 활성화하지 않은 채 정책에서 민감한 데이터 프리프로세서 규칙을 활성화하면, 정책에 변경 사항을 저장할 때 민감한 데이터 탐지를 활성화하라는 메시지가 표시됩니다. 자세한 내용은 23-15페이지의 충돌 해결 및 정책 변경 사항 커밋을/를 참조하십시오.

다음 표에서는 Sensitive Data Detection 페이지에서 선택할 수 있는 작업에 대해 설명합니다.

표 34-9 민감한 데이터 컨피그레이션 작업

목적	가능한 작업
전역 설정 수정	수정할 수 있는 전역 설정에 대한 자세한 내용은 34-8 페이지의 표 34-6을/를 참조하십시오.
데이터 유형 옵션 수정	Targets 페이지 영역에서 데이터 유형 이름을 클릭합니다. Configuration 페이지 영역이 업데이트되며 데이터 유형에 대한 현재 설정이 표시됩니다. 수정할 수 있는 옵션에 대한 자세한 내용은 개별 데이터 유형 옵션을/를 참조하십시오.
데이터 유형을 모니터링할 애플리케이션 프로토콜 추가 또는 제거 이 기능을 사용하려면 제어 라이센스가 필요합니다.	**Application Protocols** 필드의 내부를 클릭하거나 필드 옆의 **Edit**를 클릭합니다. Application Protocols 팝업 창이 나타납니다. • 모니터링할 최대 8개의 애플리케이션 프로토콜을 추가하려면 왼쪽의 **Available** 목록에서 하나 이상의 애플리케이션 프로토콜을 선택한 다음 오른쪽 화살표(**>**) 버튼을 클릭합니다. • 애플리케이션 프로토콜을 제거하려면 오른쪽의 **Enabled** 목록에서 애플리케이션 프로토콜을 선택한 다음 왼쪽 화살표(**<**) 버튼을 클릭합니다. 여러 애플리케이션 프로토콜을 선택하려면 Ctrl 또는 Shift 키를 누른 채 클릭합니다. 또는 클릭하고 드래그하여 인접한 여러 애플리케이션 프로토콜을 선택할 수 있습니다. 선택한 각 애플리케이션 프로토콜에 대해 하나 이상의 탐지기가 활성화되어야 합니다 (46-27페이지의 탐지기 활성화 및 비활성화 참조). 기본적으로 모든 Cisco 제공 탐지기는 활성화되어 있습니다. 어떤 애플리케이션 프로토콜에 대해 활성화된 탐지기가 없을 경우 자동으로 모든 Cisco 제공 탐지기가 해당 애플리케이션에 대해 활성화됩니다. 탐지기가 하나도 없을 경우 가장 최근에 수정된 사용자 정의 탐지기가 이 애플리케이션에 대해 활성화됩니다. **참고** FTP 트래픽에서 민감한 데이터를 탐지하려면 `Ftp data` 애플리케이션 프로토콜을 추가해야 합니다. 자세한 내용은 34-27페이지의 특별한 경우: FTP 트래픽에서 민감한 데이터 탐지을/를 참조하십시오.
사용자 지정 데이터 유형 생성	페이지 왼쪽의 **Data Types** 옆에 있는 **+** 기호를 클릭합니다. Add Data Type 팝업 창이 나타납니다. 고유한 데이터 유형 이름 및 이 데이터 유형으로 탐지할 패턴을 지정하고 **OK**를 클릭합니다. 수정 사항을 취소하려면 **Cancel**을 클릭합니다. 자세한 내용은 34-28페이지의 사용자 지정 데이터 유형 사용을/를 참조하십시오.

표 34-9 민감한 데이터 컨피그레이션 작업(계속)

목적	가능한 작업
민감한 데이터 프리프로세서 규칙 표시	Global Settings 페이지 영역 위에서 **Configure Rules for Sensitive Data Detection** 링크를 클릭합니다. 모든 민감한 데이터 프리프로세서 규칙 목록이 Rules 페이지의 필터링된 표시에 나타납니다. 선택적으로, 나열된 규칙에서 원하는 항목을 활성화 또는 비활성화할 수 있습니다. 침입 정책에서 사용할 각 데이터 유형에 대해 민감한 데이터 프리프로세서 규칙을 활성화해야 합니다. 자세한 내용은 32-20페이지의 규칙 상태 설정을/를 참조하십시오. Rules 페이지에서 사용할 수 있는 다른 작업(예: 규칙 억제, 속도 기반 공격 방지 등)에 대해서도 민감한 데이터 규칙을 구성할 수 있습니다. 자세한 내용은 32-1페이지의 규칙을 사용하여 침입 정책 조정을/를 참조하십시오. Sensitive Data Detection 페이지로 돌아가려면 **Back**을 클릭합니다.

민감한 데이터 탐지를 구성하려면

액세스: Admin/Intrusion Admin

1단계 **Policies > Intrusion > Intrusion Policy**를 선택합니다.

Intrusion Policy 페이지가 나타납니다.

2단계 수정할 정책 옆에 있는 수정 아이콘( )을 클릭합니다.

다른 정책에 저장하지 않은 변경 사항이 있는 경우 변경 사항을 취소하고 계속 진행하려면 **OK**를 클릭합니다. 저장하지 않은 변경 사항을 다른 정책에 저장하는 방법에 대한 자세한 내용은 23-15페이지의 충돌 해결 및 정책 변경 사항 커밋을/를 참조하십시오.

Policy Information 페이지가 나타납니다.

3단계 왼쪽의 탐색 패널에서 **Advanced Settings**를 클릭합니다.

Advanced Settings 페이지가 나타납니다.

4단계 **Specific Threat Detection** 아래에서 **Sensitive Data Detection**이 활성화되었는지 여부에 따라 두 가지 선택 사항이 있습니다.

- 컨피그레이션이 활성화되어 있으면 **Edit**를 클릭합니다.
- 컨피그레이션이 비활성화되어 있으면 **Enabled**를 클릭한 다음 **Edit**를 클릭합니다.

Sensitive Data Detection 페이지가 나타납니다. 페이지 하단에 있는 메시지는 컨피그레이션이 포함된 침입 정책 레이어를 식별합니다. 자세한 내용은 24-1페이지의 네트워크 분석 또는 침입 정책에서 레이어 사용을/를 참조하십시오.

5단계 민감한 데이터 컨피그레이션 작업 표에 설명된 작업을 수행할 수 있습니다.

6단계 정책을 저장하거나, 계속 수정하거나, 변경 사항을 취소하거나, 시스템 캐시에 변경 사항이 남아 있는 상태로 종료합니다. 자세한 내용은 23-15페이지의 충돌 해결 및 정책 변경 사항 커밋을/를 참조하십시오.

모니터링할 애플리케이션 프로토콜 선택

라이센스: 제어

데이터 유형을 모니터링할 최대 8개의 애플리케이션 프로토콜을 지정할 수 있습니다. 시스템이 네트워크에서 탐지할 수 있는 애플리케이션 프로토콜에 대한 자세한 내용은 50-36페이지의 서버 작업을/를 참조하십시오.

선택한 각 애플리케이션 프로토콜에 대해 하나 이상의 탐지기가 활성화되어야 합니다(46-27페이지의 탐지기 활성화 및 비활성화 참조). 기본적으로 모든 Cisco 제공 탐지기는 활성화되어 있습니다. 어떤 애플리케이션 프로토콜에 대해 활성화된 탐지기가 없을 경우 자동으로 모든 Cisco 제공 탐지기가 해당 애플리케이션에 대해 활성화됩니다. 탐지기가 하나도 없을 경우 가장 최근에 수정된 사용자 정의 탐지기가 이 애플리케이션에 대해 활성화됩니다.

각 데이터 유형을 모니터링할 애플리케이션 프로토콜 또는 포트를 하나 이상 지정해야 합니다. 그러나 FTP 트래픽에서 민감한 데이터를 탐지하려는 경우를 제외하고, Cisco에서는 애플리케이션 프로토콜을 지정할 때 가장 완전한 해당 포트의 적용 범위를 지정할 것을 권장합니다. 예를 들어 HTTP를 지정하는 경우 잘 알려진 HTTP 포트 80도 구성할 수 있습니다. 네트워크의 새 호스트가 HTTP를 구현하면, 시스템은 새 HTTP 애플리케이션 프로토콜을 검색하는 사이에 포트 80을 모니터링합니다.

FTP 트래픽에서 민감한 데이터를 탐지하려는 경우 `FTP data` 애플리케이션 프로토콜을 지정해야 합니다. 포트 번호를 지정하는 데 따른 이점은 없습니다. 자세한 내용은 34-27페이지의 특별한 경우: FTP 트래픽에서 민감한 데이터 탐지을/를 참조하십시오.

민감한 데이터 탐지를 위해 애플리케이션 프로토콜을 수정하려면

Admin/Intrusion Admin

1단계 **Policies > Intrusion > Intrusion Policy**를 선택합니다.

Intrusion Policy 페이지가 나타납니다.

2단계 수정할 정책 옆에 있는 수정 아이콘( )을 클릭합니다.

다른 정책에 저장하지 않은 변경 사항이 있는 경우 변경 사항을 취소하고 계속 진행하려면 **OK**를 클릭합니다. 저장하지 않은 변경 사항을 다른 정책에 저장하는 방법에 대한 자세한 내용은 23-15페이지의 충돌 해결 및 정책 변경 사항 커밋을/를 참조하십시오.

Policy Information 페이지가 나타납니다.

3단계 왼쪽의 탐색 패널에서 **Advanced Settings**를 클릭합니다.

Advanced Settings 페이지가 나타납니다.

4단계 **Specific Threat Detection** 아래에서 **Sensitive Data Detection**이 활성화되었는지 여부에 따라 두 가지 선택 사항이 있습니다.

- 컨피그레이션이 활성화되어 있으면 **Edit**를 클릭합니다.
- 컨피그레이션이 비활성화되어 있으면 **Enabled**를 클릭한 다음 **Edit**를 클릭합니다.

Sensitive Data Detection 페이지가 나타납니다.

페이지 하단에 있는 메시지는 컨피그레이션이 포함된 침입 정책 레이어를 식별합니다. 자세한 내용은 24-1페이지의 네트워크 분석 또는 침입 정책에서 레이어 사용을/를 참조하십시오.

5단계 수정할 데이터 유형을 선택하려면 **Data Types** 아래에서 데이터 유형 이름을 클릭합니다.

Configuration 영역이 업데이트되며 선택한 데이터 유형에 대한 현재 설정이 표시됩니다.

6단계 **Application Protocols** 필드의 내부를 클릭하거나 필드 옆의 **Edit**를 클릭합니다.

Application Protocols 팝업 창이 나타납니다.

7단계 2가지 옵션이 있습니다.

- 모니터링할 최대 8개의 애플리케이션 프로토콜을 추가하려면 왼쪽의 **Available** 목록에서 하나 이상의 애플리케이션 프로토콜을 선택한 다음 오른쪽 화살표(**>**) 버튼을 클릭합니다.
- 애플리케이션 프로토콜을 제거하려면 오른쪽의 **Enabled** 목록에서 애플리케이션 프로토콜을 선택한 다음 왼쪽 화살표(**<**) 버튼을 클릭합니다.

여러 애플리케이션 프로토콜을 선택하려면 Ctrl 또는 Shift 키를 누른 채 클릭합니다. 또는 클릭하고 드래그하여 인접한 여러 애플리케이션 프로토콜을 선택할 수 있습니다.

참고 FTP 트래픽에서 민감한 데이터를 탐지하려면 `FTP data` 애플리케이션 프로토콜을 추가해야 합니다. 자세한 내용은 34-27페이지의 특별한 경우: FTP 트래픽에서 민감한 데이터 탐지을/를 참조하십시오.

8단계 애플리케이션 프로토콜을 추가하려면 **OK**를 클릭합니다.

Sensitive Data Detection 페이지가 표시되고 애플리케이션 프로토콜이 업데이트됩니다.

특별한 경우: FTP 트래픽에서 민감한 데이터 탐지

라이센스: 제어

어떤 트래픽에서 민감한 데이터를 모니터링할지를 결정할 때에는 일반적으로 모니터링할 포트를 지정하거나, 선택적으로 구축에서 애플리케이션 프로토콜을 지정합니다. 그러나 FTP 트래픽에서 민감한 데이터를 탐지하는 경우 포트나 애플리케이션 프로토콜을 지정하는 것만으로는 충분하지 않습니다. FTP 트래픽의 민감한 데이터는 FTP 애플리케이션 프로토콜에 대한 트래픽에서 발견되지 않습니다. 이 트래픽은 간헐적으로 발생하며 임시 포트 번호를 사용하므로 탐지가 어렵습니다. FTP 트래픽에서 민감한 데이터를 탐지하려면 컨피그레이션에 다음을 **포함해야** 합니다.

- `FTP data` 애플리케이션 프로토콜을 지정합니다.

  `FTP data` 애플리케이션 프로토콜을 지정하면 FTP 트래픽에서 민감한 데이터 탐지가 활성화됩니다. 자세한 내용은 34-26페이지의 모니터링할 애플리케이션 프로토콜 선택을/를 참조하십시오.

  FTP 트래픽에서 민감한 데이터를 탐지하는 특별한 경우 `FTP data` 애플리케이션 프로토콜이 탐지를 호출하지는 않습니다. 대신 FTP 트래픽에서 민감한 데이터를 탐지할 수 있도록 FTP/텔넷 프로세서의 신속한 처리를 호출합니다. 자세한 내용은 27-18페이지의 FTP 및 텔넷 트래픽 디코딩을/를 참조하십시오.

- FTP Data 탐지기(기본적으로 활성화됨)가 활성화되었는지 확인합니다.

  46-27페이지의 탐지기 활성화 및 비활성화을/를 참조하십시오.

- 민감한 데이터를 모니터링할 하나 이상의 포트가 컨피그레이션에 포함되었는지 확인합니다.

  FTP 트래픽에서만 민감한 데이터를 탐지하고자 하는 특별한 경우가 아니면 FTP 포트를 지정할 필요가 없습니다. 대부분의 민감한 데이터 컨피그레이션에는 HTTP나 이메일 포트 등 다른 포트가 포함됩니다. 모니터링할 포트로 FTP 포트 하나만 지정하고 다른 포트는 지정하지 않으려는 경우 Cisco에서는 FTP 명령 포트 `23`을 지정할 것을 권장합니다. 자세한 내용은 34-24페이지의 민감한 데이터 탐지 구성을/를 참조하십시오.

사용자 지정 데이터 유형 사용

라이센스: 보호

지정한 데이터 패턴을 탐지하려면 사용자 지정 데이터 유형을 생성 및 수정할 수 있습니다. 예를 들어 병원에서는 환자 번호를 보호하기 위한 데이터 유형을 생성할 수 있고, 대학에서는 고유한 번호 지정 패턴이 있는 학생 번호를 탐지하기 위한 데이터 유형을 생성할 수 있습니다.

각 사용자 지정 데이터 유형을 생성하면 GID(generator ID) 138과 Snort ID 1000000 이상(즉, 로컬 규칙용 SID)의 단일 민감한 데이터 프리프로세서 규칙도 생성됩니다. 정책에서 사용할 각 사용자 지정 데이터 유형에 대해, 탐지를 활성화할 관련된 민감한 데이터 규칙 및 이벤트 생성을 활성화해야 합니다. 침입 규칙에서 규칙을 활성화하는 방법에 대한 자세한 내용은 32-20페이지의 규칙 상태 설정을/를 참조하십시오.

민감한 데이터 규칙의 활성화에 도움이 되도록 컨피그레이션 페이지에서 제공되는 링크를 클릭하면 모든 사용자 지정 및 사전 정의된 민감한 데이터 규칙을 표시하는 Rules 페이지의 필터링된 보기가 나타납니다. Rules 페이지에서 로컬 규칙 필터링 카테고리를 선택하여 사용자 지정 민감한 데이터 규칙만 표시할 수도 있습니다. 자세한 내용은 32-10페이지의 침입 정책의 규칙 필터링을/를 참조하십시오. 사용자 지정 민감한 데이터 규칙은 Rule Editor 페이지에 나열되지 않습니다.

생성하는 사용자 지정 데이터 유형은 모든 침입 정책에 추가됩니다. 특정 사용자 지정 데이터 유형에 대한 이벤트를 탐지하고 생성하고자 하는 정책에서 관련된 민감한 데이터 규칙을 활성화해야 합니다.

데이터 유형 및 관련 규칙을 생성하려면 Sensitive Data Detection 컨피그레이션 페이지를 사용해야 합니다. 민감한 데이터 규칙을 생성하는 데에는 규칙 편집기를 사용할 수 없습니다.

자세한 내용은 다음 절을 참조하십시오.

- 34-28페이지의 사용자 지정 데이터 유형에서 데이터 패턴 정의
- 34-30페이지의 사용자 지정 데이터 유형 구성
- 34-32페이지의 사용자 지정 데이터 유형 이름 및 탐지 패턴 수정

사용자 지정 데이터 유형에서 데이터 패턴 정의

라이센스: 보호

다음으로 구성된 간단한 정규식 집합을 사용하여 사용자 지정 데이터 유형용 데이터 패턴을 정의할 수 있습니다.

- 메타 문자 3개
- 메타 문자를 리터럴 문자로 사용하기 위한 이스케이프된 문자
- 문자 클래스 6개

메타 문자는 정규식 내에서 특별한 의미를 갖는 리터럴 문자입니다. 다음 표에서는 사용자 지정 데이터 패턴을 정의할 때 사용할 수 있는 메타 문자에 대해 설명합니다.

표 34-10 민감한 데이터 패턴 메타 문자

메타 문자	설명	예
?	선행 문자 또는 이스케이프 시퀀스가 0번 또는 1번 나타나는 경우와 일치합니다. 즉, 선행 문자나 이스케이프 문자는 선택 사항입니다.	colou?r - color 또는 colour와 일치
{*n*}	선행 문자 또는 이스케이프 시퀀스가 *n*번 나타나는 경우와 일치합니다.	예를 들어, \d{2} - 55, 12 등과 일치 \l{3} - AbC, www 등과 일치 \w{3} - a1B, 25C 등과 일치 x{5} - xxxxx와 일치
\	메타 문자를 실제 문자로서 사용할 수 있으며, 사전 정의된 문자 클래스를 지정하는 데에도 사용됩니다. 민감한 데이터 패턴에서 사용할 수 있는 문자 클래스의 설명은 34-29 페이지의 표 34-12을/를 참조하십시오.	\? - 물음표와 일치 \\ - 백슬래시와 일치 \d - 숫자 문자와 일치 등

민감한 데이터 프리프로세서가 다음 표에 있는 문자를 리터럴 문자로 정확히 해석하도록 하려면 백슬래시를 사용하여 해당 문자를 이스케이프해야 합니다.

표 34-11 이스케이프된 민감한 데이터 패턴 문자

다음 이스케이프된 문자 사용	다음 리터럴 문자 표시
\?	?
\{	{
\}	}
\\	\

다음 표에서는 사용자 지정 민감한 데이터 패턴을 정의할 때 사용할 수 있는 문자 클래스에 대해 설명합니다.

표 34-12 민감한 데이터 패턴 문자 클래스

문자 클래스	설명	문자 클래스 정의
\d	숫자 ASCII 문자 0-9와 일치	0-9
\D	숫자 ASCII 문자가 아닌 바이트와 일치	not 0-9
\l(소문자 "엘")	ASCII 문자와 일치	a-zA-Z
\L	ASCII 문자가 아닌 바이트와 일치	not a-zA-Z
\w	ASCII 영숫자 문자와 일치 PCRE 정규식과는 달리 여기에는 밑줄(_)이 포함되지 않습니다.	a-zA-Z0-9
\W	ASCII 영숫자 문자가 아닌 바이트와 일치	not a-zA-Z0-9

프리프로세서는 직접 입력된 문자(정규식의 일부 대신)를 리터럴 문자로 취급합니다. 예를 들어 데이터 패턴 1234는 1234와 일치합니다.

사전 정의된 민감한 데이터 규칙 138:4에서 사용되는 다음 데이터 패턴 예에서는 이스케이프된 숫자 문자 클래스, 승수와 옵션 지정자 메타 문자, 리터럴 대시(-)와 좌우 괄호() 문자를 사용하여 미국 전화 번호를 탐지합니다.

```
(\d{3}) ?\d{3}-\d{4}
```

사용자 지정 데이터 패턴을 생성할 때에는 각별히 주의해야 합니다. 전호 번호를 탐지하는 다음의 대체 데이터 패턴을 고려해보십시오. 여기에서는 유효한 구문이 사용되지만 다수의 오탐이 발생할 수 있습니다.

```
(?\d{3})? ?\d{3}-?\d{4}
```

두 번째 예에서는 옵션 괄호, 옵션 공백, 옵션 대시를 조합하므로 다음과 같은 바람직한 패턴의 전화 번호를 탐지할 수 있습니다.

- `(555)123-4567`
- `555123-4567`
- `5551234567`

그러나 두 번째 예제 패턴은 다음과 같이 잠재적으로 유효하지 않은 패턴도 탐지함으로써 오탐을 일으킬 수 있습니다.

- `(555 1234567`
- `555)123-4567`
- `555) 123-4567`

마지막으로 설명을 목적으로, 소규모 회사 네트워크의 모든 목적지 트래픽에서 낮은 이벤트 임계값을 사용하여 소문자 `a`를 탐지하는 데이터 패턴을 생성하는 극단적인 예를 생각해볼 수 있습니다. 그러한 데이터 패턴은 불과 몇 분 만에 수백만 개의 이벤트로 시스템을 혼란에 빠뜨릴 수 있습니다.

사용자 지정 데이터 유형 구성

라이센스: 보호

기본적으로 사전 정의된 데이터 유형에 대해 구성하는 것과 동일한 데이터 유형 옵션을 사용자 지정 데이터 유형에 대해서도 구성합니다. 모든 데이터 유형에 공통된 옵션을 설정하는 방법에 대한 자세한 내용은 34-21페이지의 개별 데이터 유형 옵션 선택을/를 참조하십시오. 또한 사용자 지정 데이터 유형에 대한 이름과 데이터 패턴도 지정해야 합니다.

사용자 지정 데이터 유형을 생성하면 관련된 사용자 지정 민감한 데이터 전처리 규칙도 생성됩니다. 해당 데이터 유형을 사용하고자 하는 각 정책에서 이를 활성화해야 합니다. 침입 규칙에서 규칙을 활성화하는 방법에 대한 자세한 내용은 32-20페이지의 규칙 상태 설정을/를 참조하십시오.

사용자 지정 데이터 유형을 생성 또는 수정하려면

Admin/Intrusion Admin

1단계 **Policies > Intrusion > Intrusion Policy**를 선택합니다.

Intrusion Policy 페이지가 나타납니다.

2단계 수정할 정책 옆에 있는 수정 아이콘( )을 클릭합니다.

다른 정책에 저장하지 않은 변경 사항이 있는 경우 변경 사항을 취소하고 계속 진행하려면 **OK**를 클릭합니다. 저장하지 않은 변경 사항을 다른 정책에 저장하는 방법에 대한 자세한 내용은 23-15페이지의 충돌 해결 및 정책 변경 사항 커밋을/를 참조하십시오.

Policy Information 페이지가 나타납니다.

3단계 왼쪽의 탐색 패널에서 **Advanced Settings**를 클릭합니다.

Advanced Settings 페이지가 나타납니다.

4단계 **Specific Threat Detection** 아래에서 **Sensitive Data Detection**이 활성화되었는지 여부에 따라 두 가지 선택 사항이 있습니다.

- 컨피그레이션이 활성화되어 있으면 **Edit**를 클릭합니다.
- 컨피그레이션이 비활성화되어 있으면 **Enabled**를 클릭한 다음 **Edit**를 클릭합니다.

Sensitive Data Detection 페이지가 나타납니다.

페이지 하단에 있는 메시지는 컨피그레이션이 포함된 침입 정책 레이어를 식별합니다. 자세한 내용은 24-1페이지의 네트워크 분석 또는 침입 정책에서 레이어 사용을/를 참조하십시오.

5단계 다음 옵션을 이용할 수 있습니다.

- 사용자 지정 데이터 유형을 생성하려면 페이지 왼쪽의 **Data Types** 옆에 있는 **+** 기호를 클릭합니다. Add Data Type 팝업 창이 나타납니다.

  고유한 데이터 유형 이름 및 이 데이터 유형으로 탐지할 패턴을 지정하고 **OK**를 클릭합니다. 수정 사항을 취소하려면 **Cancel**을 클릭합니다. 자세한 내용은 34-32페이지의 사용자 지정 데이터 유형 이름 및 탐지 패턴 수정을/를 참조하십시오.

  Sensitive Data Detection 페이지가 나타납니다. **OK**를 클릭하면 페이지가 업데이트되면서 변경 사항이 표시됩니다.

- 사전 정의된 데이터 유형과 사용자 지정 데이터 유형에 공통된 옵션을 수정하려면 **Targets** 페이지 영역에서 데이터 유형 이름을 클릭합니다.

  Configuration 페이지 영역이 업데이트되며 데이터 유형에 대한 현재 설정이 표시됩니다. 자세한 내용은 34-24페이지의 민감한 데이터 탐지 구성을/를 참조하십시오.

- 사용자 지정 데이터 유형에 대한 시스템 전반의 이름과 데이터 패턴을 수정하려면 34-32페이지의 사용자 지정 데이터 유형 이름 및 탐지 패턴 수정을/를 참조하십시오.
- 사용자 지정 데이터 유형을 삭제하려면 제거하려는 데이터 유형 옆에 있는 삭제 아이콘( )을 클릭하고 **OK**를 클릭합니다. 데이터 유형의 삭제를 취소하려면 **Cancel**을 클릭합니다.

  침입 정책에서 데이터 유형에 대한 민감한 데이터 규칙이 활성화된 경우에는 해당 데이터 유형을 삭제할 수 없습니다. 사용자 지정 데이터 유형을 삭제하면 모든 침입 정책에서 삭제됩니다.

사용자 지정 데이터 유형 이름 및 탐지 패턴 수정

라이센스: 보호

사용자 지정 민감한 데이터 규칙에 대한 시스템 전반의 이름 및 탐지 패턴을 수정할 수 있습니다. 이러한 설정을 변경하면 시스템의 다른 모든 정책에서도 변경됩니다. 적용된 액세스 제어 정책에 수정한 사용자 지정 데이터 유형을 사용하는 침입 정책이 포함된 경우 해당 액세스 제어 정책을 다시 적용해야 합니다.

사용자 지정 데이터 유형 이름 및 데이터 패턴을 제외한 모든 데이터 유형 옵션은 사용자 지정 데이터 유형과 사전 정의된 데이터 유형 모두에서 정책 단위로 적용됩니다. 사용자 지정 데이터 유형에서 이름과 데이터 패턴 이외의 옵션을 수정하는 방법에 대한 자세한 내용은 34-21페이지의 개별 데이터 유형 옵션 선택을/를 참조하십시오.

사용자 지정 데이터 유형 이름 및 데이터 패턴을 수정하려면

Admin/Intrusion Admin

1단계 **Policies > Intrusion > Intrusion Policy**를 선택합니다.

Intrusion Policy 페이지가 나타납니다.

2단계 수정할 정책 옆에 있는 수정 아이콘( )을 클릭합니다.

다른 정책에 저장하지 않은 변경 사항이 있는 경우 변경 사항을 취소하고 계속 진행하려면 **OK**를 클릭합니다. 저장하지 않은 변경 사항을 다른 정책에 저장하는 방법에 대한 자세한 내용은 23-15페이지의 충돌 해결 및 정책 변경 사항 커밋을/를 참조하십시오.

Policy Information 페이지가 나타납니다.

3단계 왼쪽의 탐색 패널에서 **Advanced Settings**를 클릭합니다.

Advanced Settings 페이지가 나타납니다.

4단계 **Specific Threat Detection** 아래에서 **Sensitive Data Detection**이 활성화되었는지 여부에 따라 두 가지 선택 사항이 있습니다.

- 컨피그레이션이 활성화되어 있으면 **Edit**를 클릭합니다.
- 컨피그레이션이 비활성화되어 있으면 **Enabled**를 클릭한 다음 **Edit**를 클릭합니다.

Sensitive Data Detection 페이지가 나타납니다.

페이지 하단에 있는 메시지는 컨피그레이션이 포함된 침입 정책 레이어를 식별합니다. 자세한 내용은 24-1페이지의 네트워크 분석 또는 침입 정책에서 레이어 사용을/를 참조하십시오.

5단계 **Targets** 페이지 영역에서 수정하려는 사용자 지정 데이터 유형의 이름을 클릭합니다.

페이지가 업데이트되며 데이터 유형에 대한 현재 설정이 표시되고, Configuration 페이지 영역의 오른쪽 위에 **Edit Data Type Name and Pattern** 링크가 나타납니다.

6단계 **Edit Data Type Name and Pattern** 링크를 클릭합니다.

Edit Data Type 팝업 창이 나타납니다.

7단계 데이터 유형 이름, 패턴 또는 둘을 모두 수정하고 **OK**를 클릭합니다. 수정을 취소하려면 **Cancel**을 클릭합니다. 데이터 패턴 지정에 대한 자세한 내용은 34-28페이지의 사용자 지정 데이터 유형에서 데이터 패턴 정의을/를 참조하십시오.

Sensitive Data Detection 페이지가 나타납니다. **OK**를 클릭하면 페이지에 변경 사항이 표시됩니다.

전체적으로 침입 이벤트 로깅 제한

시스템이 침입 이벤트를 로깅하고 표시하는 횟수를 제한하기 위해 임계값을 사용할 수 있습니다. 침입 정책의 일부로 구성되는 임계값을 지정하면, 규칙과 일치하는 트래픽이 지정된 기간 내에 특정 주소나 주소 범위에서 발생하거나 그러한 주소나 주소 범위로 이동하는 횟수를 기반으로 시스템은 이벤트를 생성합니다. 이렇게 하면 이벤트 수가 너무 많아서 혼란스러워지는 상황을 피할 수 있습니다. 이 기능을 사용하려면 보호 라이센스가 필요합니다.

이벤트 알림 임계값은 두 가지 방법으로 설정할 수 있습니다.

- 특정 소스나 목적지의 이벤트가 지정된 기간에 로깅 및 표시되는 빈도를 제한하려면 모든 트래픽에 대해 전역 임계값을 설정할 수 있습니다. 자세한 내용은 35-1페이지의 임계값 이해 및 35-3페이지의 전역 임계값 구성을/를 참조하십시오.
- 32-22페이지의 이벤트 임계값 구성에 설명된 대로 침입 정책 컨피그레이션에서 공유 객체 규칙, 표준 텍스트 규칙 또는 프리프로세서 규칙당 임계값을 설정할 수 있습니다.

임계값 이해

라이센스: 보호

기본적으로 모든 침입 정책에는 전역 규칙 임계값이 포함되어 있습니다. 기본 임계값은 각 규칙에 대해 동일한 목적지로 가는 트래픽에 대한 이벤트 생성을 60초당 1회로 제한합니다. 이 전역 임계값은 기본적으로 모든 침입 규칙 및 프리프로세서 규칙에 적용됩니다. 침입 정책의 Advanced Settings 페이지에서 임계값을 비활성화할 수 있습니다.

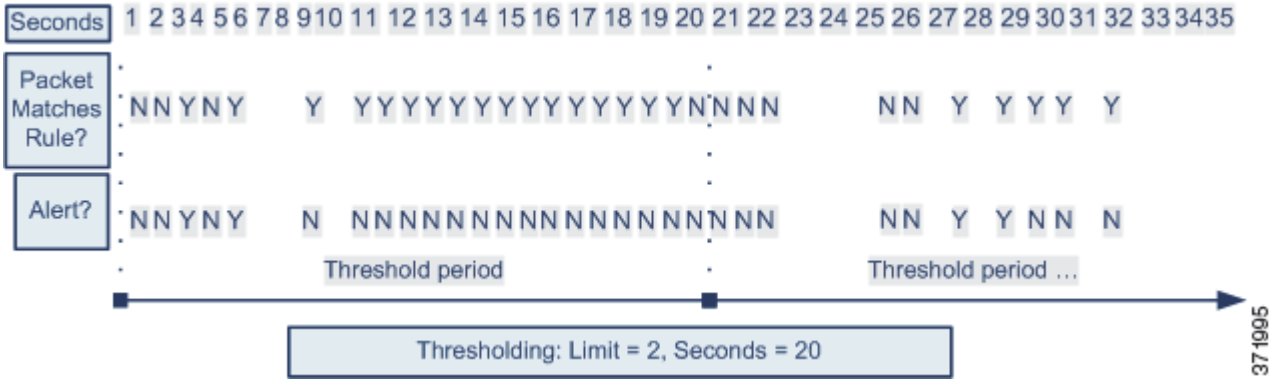
특정 규칙에 대해 개별 임계값을 설정하여 이 임계값을 재정의할 수도 있습니다. 예를 들어 전역 제한 임계값은 60초당 이벤트 5회이지만, SID 1315에 대해서는 60초당 이벤트 10회의 특정 임계값을 설정할 수 있습니다. 다른 모든 규칙은 60초당 생성되는 이벤트가 5회를 넘지 않지만, SID 1315의 경우 시스템은 60초당 이벤트를 최대 10회 생성합니다.

규칙 기반 임계값 설정에 대한 자세한 내용은 32-22페이지의 이벤트 임계값 구성을/를 참조하십시오.

팁 다중 CPU가 있는 관리되는 디바이스에 대한 전역 또는 개별 임계값을 사용하면 이벤트 수가 예상보다 더 많아질 수 있습니다.

다음 다이어그램은 특정 규칙에 대해 진행되는 공격의 예를 보여줍니다. 전역 제한 임계값은 각 규칙에 대한 이벤트 생성을 20초당 이벤트 2회로 제한합니다.

기간은 1초에 시작하여 21초에 끝납니다. 기간이 끝나면 주기가 다시 시작되고 다음 두 규칙 일치가 이벤트를 생성하며, 시스템은 해당 기간 중에 더 이상 이벤트를 생성하지 않습니다.



임계값 옵션 이해

라이센스: 보호

임계값을 사용하면 특정 기간에 특정 수의 이벤트만을 생성하여 또는 이벤트 집합에 대해 하나의 이벤트만 생성하여 침입 이벤트 생성을 제한할 수 있습니다. 전역 임계값을 구성할 때에는 다음 표에 설명된 대로 먼저 임계값 유형을 지정해야 합니다.

표 35-1 임계값 옵션

옵션	설명
제한	지정된 기간 중 규칙을 트리거하는 지정된 패킷 수(count 인수로 지정)에 대한 이벤트를 로깅 및 표시합니다. 예를 들어 유형을 **Limit**, **Count**를 `10`, **Seconds**를 `60`으로 설정한 경우 14개 패킷으로 규칙이 트리거되면 시스템은 지정된 기간 내 발생하는 처음 10개를 표시한 후 규칙에 대한 이벤트 로깅을 중지합니다.
임계값	지정된 기간 중 지정된 패킷 수(count 인수로 지정)가 규칙을 트리거하면 단일 이벤트를 로깅 및 표시합니다. 이벤트의 임계값 카운트에 도달하고 시스템이 해당 이벤트를 로깅하면 시간에 대한 카운터가 다시 시작됩니다. 예를 들어 유형을 **Threshold**, **Count**를 `10`, **Seconds**를 `60`으로 설정했는데, 33초에 10회 규칙이 트리거됩니다. 시스템은 이벤트를 한 번 생성한 다음 Seconds 및 Count 카운터를 `0`으로 재설정합니다. 다음 25초에 10회가 더 발생하면 규칙이 트리거됩니다. 33초에 카운터가 `0`으로 재설정되므로 시스템은 또 다른 이벤트를 로깅합니다.
모두	지정된 패킷 수(카운트)가 규칙을 트리거한 후 지정된 기간당 한 번 이벤트를 로깅 및 표시합니다. 예를 들어 유형을 **Both**, **Count**를 `2`, **Seconds**를 `10`으로 설정하면 이벤트 카운트는 다음과 같습니다. • 10초에 한 번 규칙이 트리거되면 시스템은 이벤트를 생성하지 않습니다(임계값이 충족되지 않음). • 규칙이 10초에 두 번 트리거되면 시스템은 이벤트를 한 번 생성합니다(규칙이 두 번째 트리거될 때 임계값이 충족됨). • 규칙이 10초에 네 번 트리거되면 시스템은 이벤트를 한 번 생성합니다(규칙이 두 번째 트리거될 때 임계값이 충족되고 이후 이벤트는 무시됨).

다음으로 추적을 지정합니다. 이는 이벤트 인스턴스 카운트를 소스 IP 주소당 계산할지, 목적지 IP 주소당 계산할지를 결정합니다. 마지막으로, 임계값을 정의하는 인스턴스 수 및 기간을 지정합니다.

표 35-2 임계값 지정 인스턴스/시간 옵션

옵션	설명
개수	임계값 충족에 필요한 추적 IP 주소 또는 주소 범위당 지정된 기간의 이벤트 인스턴스 수.
초	카운트가 재설정될 때까지 경과하는 시간(초). 임계값 유형을 **Limit**, 추적을 **Source**, **Count**를 10, **Seconds**를 10으로 설정하면 시스템은 지정된 소스 포트에서 10초간 발생하는 처음 10개 이벤트를 로깅 및 표시합니다. 처음 10초간 이벤트가 7개만 발생하면 시스템은 이를 로깅 및 표시하고, 처음 10초간 이벤트가 40개 발생하면 시스템은 10개만 로깅 및 표시한 다음 10초 기간 경과 후 카운팅을 다시 시작합니다.

전역 임계값 구성

라이센스: 보호

일정 기간 동안 각 규칙에 의해 생성되는 이벤트 수를 관리하려면 전역 임계값을 설정할 수 있습니다. 전역 임계값을 설정하면 해당 임계값은 특정 임계값을 재정의하지 않는 각 규칙에 적용됩니다. 임계값 구성에 대한 자세한 내용은 35-1페이지의 임계값 이해을/를 참조하십시오.

전역 임계값은 시스템에서 기본적으로 구성됩니다. 기본값은 다음과 같습니다.

- **Type** — Limit
- **Track By** — Destination
- **Count** — 1
- **Seconds** — 60

전역 임계값을 구성하려면

액세스: Admin/Intrusion Admin

1단계 **Policies > Intrusion > Intrusion Policy**를 선택합니다.

Intrusion Policy 페이지가 나타납니다.

2단계 수정할 정책 옆에 있는 수정 아이콘( )을 클릭합니다.

다른 정책에 저장하지 않은 변경 사항이 있는 경우 변경 사항을 취소하고 계속 진행하려면 **OK**를 클릭합니다. 저장하지 않은 변경 사항을 다른 정책에 저장하는 방법에 대한 자세한 내용은 23-15페이지의 충돌 해결 및 정책 변경 사항 커밋을/를 참조하십시오.

Policy Information 페이지가 나타납니다.

3단계 왼쪽의 탐색 패널에서 **Advanced Settings**를 클릭합니다.

Advanced Settings 페이지가 나타납니다.

4단계 **Intrusion Rule Thresholds** 아래에서 **Global Rule Thresholding**이 활성화되었는지 여부에 따라 두 가지 선택 사항이 있습니다.

- 컨피그레이션이 활성화되어 있으면 **Edit**를 클릭합니다.
- 컨피그레이션이 비활성화되어 있으면 **Enabled**를 클릭한 다음 **Edit**를 클릭합니다.

Global Rule Thresholding 페이지가 나타납니다. 페이지 하단에 있는 메시지는 컨피그레이션이 포함된 침입 정책 레이어를 식별합니다. 자세한 내용은 24-1페이지의 네트워크 분석 또는 침입 정책에서 레이어 사용을/를 참조하십시오.

5단계 **Type** 라디오 버튼에서 seconds 인수로 지정된 기간 동안 적용할 임계값 유형을 선택합니다. 자세한 내용은 임계값 옵션 표를 참조하십시오.

- count 인수로 지정된 제한이 초과될 때까지 규칙을 트리거하는 각 패킷에 대한 이벤트를 로깅 및 표시하려면 **Limit**를 선택합니다.
- 규칙을 트리거하는 각 패킷 및 count 인수로 설정한 임계값과 일치하는 인스턴스 또는 임계값의 배수인 인스턴스를 나타내는 각 패킷에 대해 단일 이벤트를 로깅 및 표시하려면 **Threshold**를 선택합니다.
- count 인수로 지정된 패킷 수가 규칙을 트리거한 후 단일 이벤트를 로깅 및 표시하려면 **Both**를 선택합니다.

6단계 **Track By** 라디오 버튼에서 추적 방법을 선택합니다.

- 하나 이상의 특정 소스 IP 주소에서 오는 트래픽에서 규칙 일치를 식별하려면 **Source**를 선택합니다.
- 특정 목적지 IP 주소로 가는 트래픽에서 규칙 일치를 식별하려면 **Source**를 선택합니다.

7단계 **Count** 필드에서

- **Limit** 임계값 - 임계값 충족에 필요한 추적 IP 주소당 지정된 기간의 이벤트 인스턴스 수를 지정합니다.
- **Threshold** 임계값 - 임계값으로 사용할 규칙 일치의 수를 지정합니다.

8단계 **Seconds** 필드에서

- **Limit** 임계값 - 공격이 추적되는 기간을 구성하는 초 단위의 시간을 지정합니다.
- **Threshold** 임계값 - 카운트가 재설정되기까지 경과하는 초 단위의 시간을 지정합니다. 지정된 시간(초)이 경과하기 전 **Count** 필드에 표시된 규칙 일치 수가 발생하는 경우 카운트가 재설정됩니다.

9단계 정책을 저장하거나, 계속 수정하거나, 변경 사항을 취소하거나, 시스템 캐시에 변경 사항이 남아 있는 상태로 종료합니다. 자세한 내용은 23-15페이지의 충돌 해결 및 정책 변경 사항 커밋을/를 참조하십시오.

전역 임계값 비활성화

라이센스: 보호

기본적으로 전역 제한 임계값은 목적지로 가는 트래픽에 대한 이벤트의 수를 60초당 1개로 제한합니다. 특정 규칙의 이벤트에 임계값을 적용하고 기본적으로 모든 규칙에 임계값을 적용하지는 않으려는 경우 최고 정책 레이어에서 전역 임계값 지정을 비활성화할 수 있습니다.

전역 임계값 지정을 비활성화하려면

액세스: Admin/Intrusion Admin

1단계 **Policies > Intrusion > Intrusion Policy**를 선택합니다.

Intrusion Policy 페이지가 나타납니다.

2단계 수정할 정책 옆에 있는 수정 아이콘( )을 클릭합니다.

다른 정책에 저장하지 않은 변경 사항이 있는 경우 변경 사항을 취소하고 계속 진행하려면 **OK**를 클릭합니다. 저장하지 않은 변경 사항을 다른 정책에 저장하는 방법에 대한 자세한 내용은 23-15페이지의 충돌 해결 및 정책 변경 사항 커밋을/를 참조하십시오.

Policy Information 페이지가 나타납니다.

3단계 왼쪽의 탐색 패널에서 **Settings**를 클릭합니다.

Settings 페이지가 나타납니다.

4단계 **Intrusion Rule Thresholds**에서 **Global Rule Thresholding**을 비활성화합니다.

5단계 정책을 저장하거나, 계속 수정하거나, 변경 사항을 취소하거나, 시스템 캐시에 변경 사항이 남아 있는 상태로 종료합니다. 자세한 내용은 23-15페이지의 충돌 해결 및 정책 변경 사항 커밋을/를 참조하십시오.

36장

침입 규칙 이해 및 작성

*침입(intrusion) 규칙*은 네트워크 트래픽을 분석하여 규칙의 기준과 일치하는지 확인함으로써 네트워크에서 취약성 악용 시도를 탐지하는 키워드와 인수의 지정된 집합입니다. 시스템은 패킷을 각 규칙에 지정된 조건과 비교하고, 패킷이 규칙에 지정된 모든 조건과 일치하면 규칙을 트리거합니다. 규칙이 *알림(alert) 규칙*이면 침입 이벤트가 생성됩니다. 규칙이 *통과(pass) 규칙*이면 트래픽이 무시됩니다. 방어 센터 웹 인터페이스에서 침입 이벤트를 보고 평가할 수 있습니다.

주의 프로덕션 환경에서 작성된 침입 규칙을 사용하기 전에 먼저 테스트해볼 수 있는 제어된 네트워크 환경이 있어야 합니다. 잘못 작성된 침입 규칙은 시스템 성능에 심각한 영향을 미칠 수 있습니다.

다음에 유의하십시오.

- 인라인 구축에서 *삭제(drop)* 규칙의 경우 시스템은 패킷을 삭제하고 이벤트를 생성합니다. 삭제 규칙에 대한 자세한 내용은 32-20페이지의 규칙 상태 설정을/를 참조하십시오.
- Cisco는 두 가지 침입 규칙 유형인 공유 객체 규칙 및 표준 텍스트 규칙을 제공합니다. Cisco VRT(Vulnerability Research Team)는 공유 객체 규칙을 사용하여 취약성에 대한 공격을 탐지할 수 있는데, 이 방법은 기존의 표준 텍스트 규칙에서 할 수 없는 방법입니다. 공유 객체 규칙은 생성할 수 없습니다. 고유한 침입 규칙을 작성하면 표준 텍스트 규칙을 생성할 수 있습니다.

보려는 이벤트 유형을 조정하려면 사용자 지정 표준 텍스트 규칙을 작성할 수 있습니다. 이 문서에서는 더러 특정 익스플로잇을 탐지하기 위한 규칙에 대해 설명하지만, 대부분의 성공적인 규칙은 알려진 특정 익스플로잇보다는 알려진 취약성의 악용을 시도할 수 있는 트래픽을 대상으로 합니다. 규칙을 작성하고 규칙의 이벤트 메시지를 지정하면 공격 및 정책 회피를 나타내는 트래픽을 좀 더 쉽게 식별할 수 있습니다. 이벤트 평가에 대한 자세한 내용은 41-1페이지의 침입 이벤트 작업을/를 참조하십시오.

사용자 지정 침입 정책에서 사용자 지정 표준 텍스트 규칙을 활성화할 때에는, 일부 규칙 키워드 및 인수에서 트래픽을 우선 특정 방법으로 디코딩 또는 전처리하도록 요구한다는 점에 유의해야 합니다. 이 장에서는 전처리를 제어하는 네트워크 분석 정책에서 구성해야 하는 옵션에 대해 설명합니다. 필수 프리프로세서를 비활성화하는 경우 네트워크 분석 정책 웹 인터페이스에서는 프리프로세서가 비활성 상태로 남아 있더라도, 시스템은 현재 설정을 이용해 프리프로세서를 자동으로 사용합니다.

참고 전처리 및 침입 검사는 밀접하게 관련되어 있으므로, 단일 패킷을 검토하는 네트워크 분석 및 침입 정책은 **반드시** 상호 보완 관계여야 합니다. 전처리를 맞춤화하는 작업 중에서도 특히 여러 개의 사용자 지정 네트워크 분석 정책을 사용하는 것은 **고급** 작업입니다. 자세한 내용은 23-12페이지의 사용자 지정 정책의 제한 사항을/를 참조하십시오.

자세한 내용은 다음 절을 참조하십시오.

- 36-2페이지의 규칙 구조 이해 - 유효한 표준 텍스트 규칙을 구성하는, 규칙 헤더와 규칙 옵션을 비롯한 구성 요소에 대해 설명합니다.
- 36-3페이지의 규칙 헤더 이해 - 규칙 헤더의 부분에 대해 자세히 설명합니다.
- 36-9페이지의 규칙의 키워드 및 인수 이해 - FireSIGHT 시스템에서 사용할 수 있는 침입 규칙 키워드의 사용법 및 구문에 대해 설명합니다.
- 36-102페이지의 규칙 작성 - 규칙 편집기를 사용하여 새 규칙을 작성하는 방법에 대해 설명합니다.
- 36-107페이지의 규칙 검색 - 기존 규칙을 검색하는 방법에 대해 설명합니다.
- 36-109페이지의 Rule Editor 페이지에서 규칙 필터링 - 특정 규칙을 찾기 위해 규칙의 하위 집합을 표시하는 방법에 대해 설명합니다.

규칙 구조 이해

라이센스: 보호

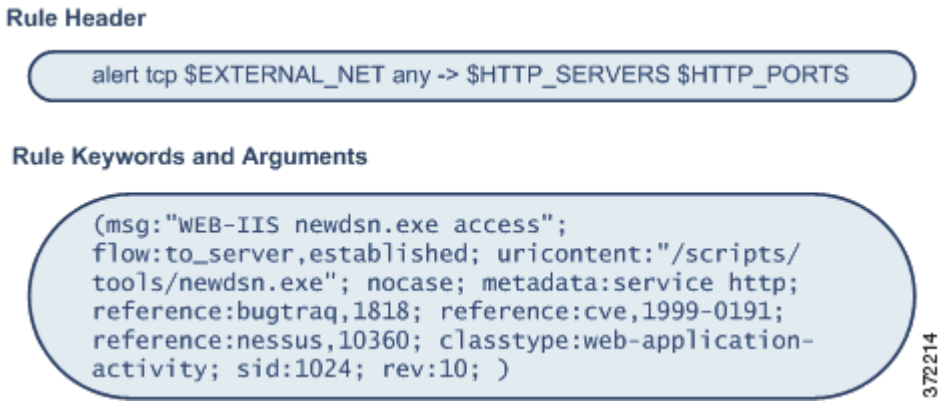
모든 표준 텍스트 규칙에는 두 개의 논리 섹션, 즉 규칙 헤더와 규칙 옵션이 있습니다. 규칙 헤더에는 다음이 포함되어 있습니다.

- 규칙의 작업 또는 유형
- 프로토콜
- 소스 및 목적지 IP 주소와 넷마스크
- 소스에서 목적지로 트래픽 플로우를 보여주는 방향 표시기
- 소스 및 목적지 포트

규칙 옵션 섹션에는 다음이 포함되어 있습니다.

- 이벤트 메시지
- 키워드와 해당 매개 변수 및 인수
- 규칙을 트리거하기 위해 패킷의 페이로드와 일치해야 하는 패턴
- 규칙 엔진이 검사해야 하는 패킷의 부분에 대한 사양

다음 다이어그램에서는 규칙의 부분에 대해 설명합니다.

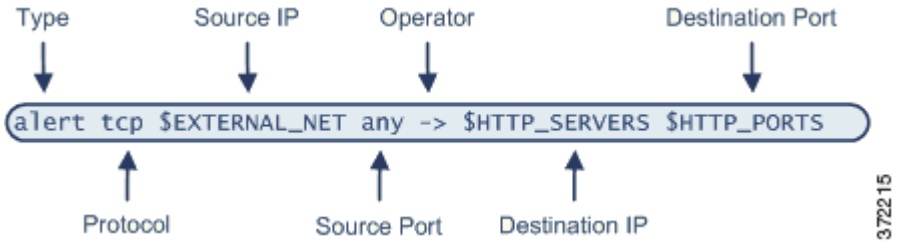


규칙의 옵션 섹션은 괄호로 표시된 부분입니다. 규칙 편집기는 표준 텍스트 규칙 작성에 도움이 되는 사용하기 쉬운 인터페이스를 제공합니다.

규칙 헤더 이해

라이센스: 보호

모든 표준 텍스트 규칙 및 공유 객체 규칙에는 매개 변수와 인수가 포함된 규칙 헤더가 있습니다. 다음은 규칙 헤더의 부분에 대한 설명입니다.



다음 표에서는 위에 나와 있는 규칙 헤더의 각 부분에 대해 설명합니다.

표 36-1 규칙 헤더 값

규칙 헤더 구성 요소	값의 예	역할
작업	경고	트리거될 때 침입 이벤트를 생성합니다.
프로토콜	tcp	TCP 트래픽만 테스트합니다.
소스 IP 주소	$EXTERNAL_NET	내부 네트워크가 아닌 호스트에서 오는 트래픽을 테스트합니다.
소스 포트	모든	시작 호스트의 포트에서 오는 트래픽을 테스트합니다.
운영자	->	외부 트래픽(네트워크의 웹 서버로 가는 트래픽)을 테스트합니다.
대상 IP 주소	$HTTP_SERVERS	내부 네트워크에서 웹 서버로 지정된 호스트로 전달되는 트래픽을 테스트합니다.
대상 포트	$HTTP_PORTS	내부 네트워크에서 HTTP 포트로 전달되는 트래픽을 테스트합니다.

참고 위의 예에서는 대부분의 침입 규칙이 그러하듯 기본 변수를 사용합니다. 변수의 의미, 구성 방법 등 변수에 대한 자세한 내용은 3-17페이지의 변수 집합 작업을/를 참조하십시오.

규칙 헤더 매개 변수에 대한 자세한 내용은 다음 절을 참조하십시오.

- 36-4페이지의 규칙 작업 지정 - 규칙 유형과 규칙이 트리거될 때 발생하는 작업을 지정하는 방법에 대해 설명합니다.
- 36-4페이지의 프로토콜 지정 - 규칙이 테스트해야 하는 트래픽에 대한 트래픽 프로토콜을 정의하는 방법에 대해 설명합니다.
- 36-5페이지의 침입 규칙에서 IP 주소 지정 - 규칙 헤더에서 개별 IP 주소와 IP 주소 블록을 정의하는 방법에 대해 설명합니다.
- 36-8페이지의 침입 규칙에서 포트 정의 - 규칙 헤더에서 개별 포트와 포트 범위를 정의하는 방법에 대해 설명합니다.
- 36-9페이지의 방향 지정 - 사용 가능한 연산자와 규칙에서 테스트하기 위해 트래픽이 이동해야 하는 방향을 지정하는 방법에 대해 설명합니다.

규칙 작업 지정

라이센스: 보호

각 규칙 헤더에는 패킷이 규칙을 트리거할 때 시스템이 수행하는 작업을 지정하는 매개 변수가 포함되어 있습니다. *알림(alert)*으로 설정된 작업의 규칙은 규칙을 트리거한 패킷에 대해 침입 이벤트를 생성하고 해당 패킷의 세부사항을 로깅합니다. *통과(pass)*로 설정된 규칙은 규칙을 트리거한 패킷에 대해 이벤트를 생성하지 않거나 세부사항을 로깅하지 않습니다.

참고 인라인 구축에서, 상태가 *Drop and Generate Events*로 설정된 규칙은 규칙을 트리거한 패킷에 대해 침입 이벤트를 생성합니다. 또한 패시브 구축에서 삭제 규칙을 적용하면 규칙이 알림 규칙 역할을 합니다. 삭제 규칙에 대한 자세한 내용은 32-20페이지의 규칙 상태 설정을/를 참조하십시오.

기본적으로 통과 규칙은 알림 규칙을 재정의합니다. 통과 규칙에 정의된 기준을 충족하는 패킷이 특정 상황에서 알림 규칙을 비활성화하는 것이 아니라 알림 규칙을 트리거하는 상황을 피하도록 통과 규칙을 생성할 수 있습니다. 예를 들어 FTP 서버에 "anonymous" 사용자로 로그인하려는 시도를 찾는 규칙을 활성 상태로 유지하고자 할 수 있습니다. 그러나 네트워크에 하나 이상의 공식적인 익명 FTP 서버가 있으면 그러한 특정 서버의 경우 익명 사용자가 원래 규칙을 트리거하지 않도록 지정하는 통과 규칙을 작성하여 활성화할 수 있습니다.

규칙 편집기 내 **Action** 목록에서 규칙 유형을 선택합니다. 규칙 편집기를 사용하여 규칙 헤더를 작성하기 위한 절차에 대한 자세한 내용은 36-102페이지의 규칙 작성을/를 참조하십시오.

프로토콜 지정

라이센스: 보호

각 규칙 헤더에서, 규칙이 검사하는 트래픽의 프로토콜을 지정해야 합니다. 분석할 다음 네트워크 프로토콜을 지정할 수 있습니다.

- ICMP(Internet Control Message Protocol)
- IP(Internet Protocol)

참고 프로토콜이 `ip`로 설정된 경우 시스템은 침입 규칙 헤더에서 포트 정의를 무시합니다. 자세한 내용은 36-8페이지의 침입 규칙에서 포트 정의을/를 참조하십시오.

- TCP(Transmission Control Protocol)
- UDP(User Datagram Protocol)

IANA에서 할당한 모든 프로토콜(TCP, UDP, ICMP, IGMP 등)을 검토하려면 프로토콜 유형으로 **IP**를 사용하십시오. IANA 할당 프로토콜의 전체 목록은 http://www.iana.org/assignments/protocol-numbers을/를 참조하십시오.

참고 IP 페이로드의 다음 헤더(예: TCP 헤더)에서 패턴을 매칭하는 규칙은 현재 작성할 수 없습니다. 대신 내용 매칭은 마지막으로 디코딩된 프로토콜로 시작됩니다. 대안으로, 규칙 옵션을 사용하여 TCP 헤더에서 패턴을 매칭할 수 있습니다.

규칙 편집기 내 **Protocol** 목록에서 프로토콜 유형을 선택합니다. 규칙 편집기를 사용하여 규칙 헤더를 작성하기 위한 절차에 대한 자세한 내용은 36-102페이지의 규칙 작성을/를 참조하십시오.

침입 규칙에서 IP 주소 지정

라이센스: 보호

패킷 검사를 특정 IP 주소에서 오는 패킷 또는 특정 IP 주소로 가는 패킷으로 제한하면 시스템이 수행해야 할 패킷 검사의 양이 줄어듭니다. 이 경우 규칙이 좀 더 구체화되고, 소스 및 목적지 IP 주소가 의심스러운 동작으로 표시하지 않는 패킷에 대해 규칙이 트리거될 가능성이 사라지므로 오탐도 줄어듭니다.

팁 시스템은 IP 주소만을 인식하며 소스 또는 목적지 IP 주소의 호스트 이름은 수용하지 않습니다.

규칙 편집기의 **Source IPs** 및 **Destination IPs** 필드에는 소스 및 목적지 IP 주소를 지정합니다. 규칙 편집기를 사용하여 규칙 헤더를 작성하기 위한 절차에 대한 자세한 내용은 36-102페이지의 규칙 작성을/를 참조하십시오.

표준 텍스트 규칙을 작성할 때 필요에 따라 다양한 방법으로 IPv4 및 IPv6 주소를 지정할 수 있습니다. 단일 IP 주소, `any`, IP 주소 목록, CIDR 표기법, 접두사 길이, 네트워크 변수 또는 네트워크 객체나 네트워크 객체 그룹을 지정할 수 있습니다. 또한 특정 IP 주소 또는 IP 주소 집합을 제외하고자 함을 나타낼 수도 있습니다. IPv6 주소를 지정할 때 RFC 4291에 정의된 주소 표기 규칙을 사용할 수 있습니다.

다음 표에는 소스 및 목적지 IP 주소를 지정할 수 있는 다양한 방법이 요약되어 있습니다.

표 36-2 소스/목적지 IP 주소 구문

지정할 내용	사용	예
임의의 IP 주소	`any`	`any`
특정 IP 주소	IP 주소 동일한 규칙에서 IPv4와 IPv6의 소스 및 목적지 주소를 함께 사용해서는 안 됩니다.	`192.168.1.1` `2001:db8::abcd`
IP 주소의 목록	IP 주소를 묶으려면 대괄호(`[]`), 분리하려면 쉼표	`[192.168.1.1,192.168.1.15]` `[2001:db8::b3ff, 2001:db8::0202]`
IP 주소의 블록	IPv4 CIDR 블록 또는 IPv6 주소 접두사 표기법	`192.168.1.0/24` `2001:db8::/32`
특정 IP 주소 또는 주소 집합을 제외한 모든 주소	부정할 하나 이상의 IP 주소 앞에 `!` 문자	`!192.168.1.15` `!2001:db8::0202:b3ff:fe1e`
하나 이상의 특정 IP 주소를 제외한 IP 주소 블록 내 임의의 주소	주소의 블록 뒤에 부정되는 주소 또는 블록의 목록	`[10.0.0/8, !10.2.3.4, !10.1.0.0/16]` `[2001:db8::/32, !2001:db8::8329, !2001:db8::0202]`
네트워크 변수로 정의된 IP 주소	대문자 변수 이름 앞에 `$` 침입 규칙에 사용된 네트워크 변수로 정의한 호스트와 상관없이 프리프로세서 규칙은 이벤트를 트리거할 수 있습니다. 자세한 내용은 3-17페이지의 변수 집합 작업을/를 참조하십시오.	`$HOME_NET`
IP 주소 변수로 정의한 주소를 제외한 모든 IP 주소	대문자 변수 이름 앞에 `!$` 자세한 내용은 36-7페이지의 침입 규칙에서 IP 주소 제외을/를 참조하십시오.	`!$HOME_NET`

표 36-2 소스/목적지 IP 주소 구문(계속)

지정할 내용	사용	예
네트워크 객체 또는 네트워크 객체 그룹으로 정의된 IP 주소	`!{object_name}` 형식을 사용하는 객체 또는 그룹 이름. 자세한 내용은 3-4페이지의 네트워크 객체 작업을/를 참조하십시오.	`${192.168sub16}`
네트워크 객체 또는 네트워크 객체 그룹으로 정의된 주소를 제외한 모든 IP 주소	중괄호({})로 묶은 객체 또는 그룹 이름과 그 앞에 `!$`. 자세한 내용은 3-4페이지의 네트워크 객체 작업을/를 참조하십시오.	`!${192.168sub16}`

소스 및 목적지 IP 주소를 지정하는 데 사용할 수 있는 구문 및 IP 주소를 지정하기 위해 변수를 사용하는 방법에 대한 자세한 내용은 다음 절을 참조하십시오.

- 1-19페이지의 IP 주소 표기 규칙.
- 3-17페이지의 변수 집합 작업
- 36-6페이지의 IP 주소 지정
- 36-6페이지의 여러 IP 주소 지정
- 36-7페이지의 네트워크 객체 지정
- 36-7페이지의 침입 규칙에서 IP 주소 제외

IP 주소 지정

라이센스: 보호

임의의 IPv4 또는 IPv6 주소를 나타내기 위한 규칙 소스 또는 목적지 IP 주소로 `any`라는 단어를 지정할 수 있습니다.

예를 들어 다음 규칙은 **Source IPs** 및 **Destination IPs** 필드에 **`any`** 인수를 사용하며 IPv4 또는 IPv6 소스/목적지 주소로 패킷을 평가합니다.

```
alert tcp any any -> any any
```

임의의 IPv6 주소를 나타내기 위해 `::`을 지정할 수도 있습니다.

여러 IP 주소 지정

라이센스: 보호

IP 주소를 쉼표로 구분하여 개별 IP 주소를 나열할 수 있습니다. 선택적으로, 다음 예에 보이는 것처럼 부정하지 않을 목록을 대괄호로 감쌀 수도 있습니다.

```
[192.168.1.100,192.168.1.103,192.168.1.105]
```

IPv4 및 IPv6 주소만 나열할 수도 있고 다음 예와 같이 임의의 조합을 사용할 수도 있습니다.

```
[192.168.1.100,2001:db8::1234,192.168.1.105]
```

IP 주소 목록을 대괄호로 감싸는 것이 이전 소프트웨어 릴리스에서는 필수 사항이었지만 지금은 필수 사항이 아닙니다. 또한 선택적으로, 목록에서 각 쉼표 앞뒤에 공백을 넣을 수 있습니다.

참고 부정되는 목록은 대괄호로 감싸야 합니다. 자세한 내용은 36-7페이지의 침입 규칙에서 IP 주소 제외을/를 참조하십시오.

또한 IPv4 CIDR(Classless Inter-Domain Routing) 표기법 또는 IPv6 접두사 길이를 사용하여 주소 블록을 지정할 수 있습니다. 예를 들면 다음과 같습니다.

- 192.168.1.0/24는 192.168.1.0 네트워크에서 서브넷 마스크 255.255.255.0(즉, 192.168.1.0~192.168.1.255)의 IPv4 주소를 지정합니다. 자세한 내용은 1-19페이지의 IP 주소 표기 규칙을/를 참조하십시오.
- 2001:db8::/32는 2001:db8:: 네트워크에서 접두사 길이 32비트(즉, 2001:db8::~2001:db8:ffff:ffff:ffff:ffff:ffff:ffff)의 IPv6 주소를 지정합니다.

팁 IP 주소의 블록을 지정해야 하지만 CIDR 또는 접두사 길이 표기법만으로 표현할 수 없는 경우 IP 주소 목록에서 CIDR 블록 및 접두사 길이를 사용할 수 있습니다.

네트워크 객체 지정

라이센스: 보호

다음 구문을 사용하여 네트워크 객체 또는 네트워크 객체 그룹을 지정할 수 있습니다.

```
${object_name | group_name}
```

여기서 각 항목은 다음을 나타냅니다.

- *object_name*은 네트워크 객체의 이름입니다.
- *group_name*은 네트워크 객체 그룹의 이름입니다.

네트워크 객체 및 네트워크 객체 그룹 생성에 대한 자세한 내용은 3-4페이지의 네트워크 객체 작업을/를 참조하십시오.

`192.168sub16`이라는 네트워크 객체 및 `all_subnets`라는 네트워크 객체 그룹을 생성했다고 가정해 보겠습니다. 네트워크 객체를 사용하는 IP 주소를 지정하는 데 다음을 사용할 수 있습니다.

```
${192.168sub16}
```

네트워크 객체 그룹을 사용하는 데에는 다음을 지정할 수 있습니다.

```
${all_subnets}
```

또한 네트워크 개체 및 네트워크 객체 그룹의 부정을 사용할 수 있습니다. 예를 들면 다음과 같습니다.

```
!${192.168sub16}
```

자세한 내용은 36-7페이지의 침입 규칙에서 IP 주소 제외을/를 참조하십시오.

침입 규칙에서 IP 주소 제외

라이센스: 보호

지정된 IP 주소를 부정하려면 느낌표(`!`)를 사용할 수 있습니다. 즉, 하나 이상의 지정된 IP 주소를 제외하고 임의의 IP 주소를 매칭할 수 있습니다. 예를 들어 `!192.168.1.1`은 192.168.1.1 이외의 IP 주소를 지정하며, `!2001:db8:ca2e::fa4c`는 2001:db8:ca2e::fa4c 이외의 IP 주소를 지정합니다.

IP 주소 목록을 부정하려면 IP 주소 목록 대괄호 앞에 `!`를 둡니다. 예를 들어 `![192.168.1.1,192.168.1.5]`는 192.168.1.1 또는 192.168.1.5 외의 IP 주소를 정의합니다.

참고 IP 주소의 목록을 부정하려면 대괄호를 사용해야 합니다.

IP 주소 목록과 함께 부정 문자를 사용하려면 주의를 기울여야 합니다. 예를 들어, 192.168.1.1 또는 192.168.1.5가 아닌 주소를 매칭하기 위해 `[!192.168.1.1,!192.168.1.5]`를 사용하면, 시스템은 이 구문을 "192.168.1.1이 아닌 임의의 주소, **또는** 192.168.1.5가 아닌 임의의 주소"로 해석합니다.

192.168.1.5는 192.168.1.1이 아니고 192.168.1.1은 192.168.1.5가 아니므로 두 IP 주소는 `[!192.168.1.1,!192.168.1.5]`의 IP 주소 값과 일치하며 결과적으로 "any"를 사용하는 것과 마찬가지가 됩니다.

대신 `![192.168.1.1,192.168.1.5]`를 사용하십시오. 시스템은 이를 "192.168.1.1이 **아니고** 192.168.1.5**도 아닌** 주소"로 해석합니다. 즉, 대괄호 안에 나열된 주소 이외의 IP 주소를 매칭합니다.

논리적으로 부정에는 any를 사용할 수 없습니다. any의 부정은 no address를 나타내기 때문입니다.

침입 규칙에서 포트 정의

라이센스: 보호

규칙 편집기의 **Source Port** 및 **Destination Port** 필드에는 소스 및 목적지 포트를 지정합니다. 규칙 편집기를 사용하여 규칙 헤더를 작성하기 위한 절차에 대한 자세한 내용은 36-102페이지의 규칙 작성을/를 참조하십시오.

FireSIGHT 시스템은 규칙 헤더에 사용되는 포트 번호를 정의하기 위해 특정 유형의 구문을 사용합니다.

참고 프로토콜이 ip로 설정된 경우 시스템은 침입 규칙 헤더에서 포트 정의를 무시합니다. 자세한 내용은 36-4페이지의 프로토콜 지정을/를 참조하십시오.

다음 예에 보이는 것처럼 쉼표로 구분하여 포트를 나열할 수 있습니다.

```
80, 8080, 8138, 8600-9000, !8650-8675
```

선택적으로, 다음 예는 대괄호로 포트 목록을 감싸는 방법을 보여줍니다. 이전 소프트웨어 버전에서는 필수 사항이었지만 지금은 필수 사항이 아닙니다.

```
[80, 8080, 8138, 8600-9000, !8650-8675]
```

다음 예에 보이는 것처럼 부정되는 포트 목록은 **반드시** 대괄호로 감싸야 합니다.

```
![20, 22, 23]
```

침입 규칙의 소스 및 목적지 포트 목록에는 최대 64자를 포함할 수 있습니다.

다음 표에는 사용할 수 있는 구문이 요약되어 있습니다.

표 36-3 소스/목적지 포트 구문

지정할 내용	사용	예
임의의 포트	any	any
특정 포트	포트 번호	80
포트 범위	범위의 처음 포트와 마지막 포트 번호 사이에 대시	80-443
특정 포트보다 작거나 같은 모든 포트	포트 번호 앞에 대시	-21
특정 포트보다 크거나 같은 모든 포트	포트 번호 뒤에 대시	80-
특정 포트 또는 포트 범위를 제외한 모든 포트	부정할 포트, 포트 목록 또는 포트 범위 앞에 ! 문자 논리적으로 *any*(부정되는 경우 *no port*를 나타냄)를 제외한 모든 포트 지정에 부정을 사용할 수 있습니다.	!20

표 36-3 소스/목적지 포트 구문(계속)

지정할 내용	사용	예
포트 변수로 정의된 모든 포트	대문자 변수 이름 앞에 `$` 자세한 내용은 3-30페이지의 포트 변수 작업을/를 참조하십시오.	`$HTTP_PORTS`
포트 변수로 정의된 포트 외의 모든 포트	대문자 변수 이름 앞에 `!$`	`!$HTTP_PORTS`

방향 지정

라이센스: 보호

규칙의 검사를 위해 패킷이 이동해야 할 방향을 규칙 헤더 내에 지정할 수 있습니다. 다음 표에서는 이러한 옵션에 대해 설명합니다.

표 36-4 규칙 헤더에서의 방향 옵션

사용	테스트할 내용
Directional	지정한 소스 IP 주소에서 지정한 목적지 IP 주소로의 트래픽만
Bidirectional	지정한 소스 및 목적지 IP 주소 간에 이동하는 모든 트래픽

규칙 편집기를 사용하여 규칙 헤더를 작성하기 위한 절차에 대한 자세한 내용은 36-102페이지의 규칙 작성을/를 참조하십시오.

규칙의 키워드 및 인수 이해

라이센스: 보호

규칙 언어를 사용할 때 키워드를 조합하여 규칙의 동작을 지정할 수 있습니다. 키워드 및 관련 값(*arguments*라고 함)은 규칙 엔진에서 테스트하는 패킷 및 패킷 관련 값을 시스템이 평가하는 방법을 지시합니다. FireSIGHT 시스템은 현재 내용 매칭, 프로토콜별 패턴 매칭, 상태별 매칭 등의 검사 기능 수행을 허용하는 키워드를 지원합니다. 키워드당 최대 100개의 인수를 정의할 수 있으며, 원하는 수의 호환 키워드를 조합하여 훨씬 구체적인 규칙을 생성할 수 있습니다. 그러면 오탐과 미탐의 가능성이 감소하며, 수신하는 침입 정보에 집중할 수 있습니다.

또한 적응형 프로필을 사용하여 규칙 메타데이터 및 호스트 정보를 기반으로 특정 패킷에 대해 활성 규칙 처리를 동적으로 조정할 수 있습니다. 자세한 내용은 30-1페이지의 수동 구축 시 전처리 튜닝을/를 참조하십시오.

자세한 내용은 다음 절을 참조하십시오.

- 36-11페이지의 침입 이벤트 세부사항 정의 - 이벤트의 메시지, 우선순위 정보, 규칙이 탐지한 익스플로잇에 대한 외부 정보 참조 등을 정의할 수 있는 키워드의 구문과 사용에 대해 설명합니다.
- 36-14페이지의 내용 일치 검색 - `content` 또는 `protected_content` 키워드를 사용하여 패킷 페이로드의 내용을 테스트하는 방법에 대해 설명합니다.
- 36-17페이지의 내용 일치 제한 - `content` 또는 `protected_content` 키워드에 대한 수정 키워드를 사용하는 방법에 대해 설명합니다.

- 36-29페이지의 인라인 구축에서 내용 교체 - 인라인 구축에서 `replace` 키워드를 사용하여 동일한 길이의 지정된 내용을 교체하는 방법에 대해 설명합니다.
- 36-30페이지의 Byte_Jump and Byte_Test 사용 - `byte_jump` 및 `byte_test` 키워드를 사용하여 규칙 엔진이 패킷에서 내용 일치에 대한 테스트를 시작해야 하는 곳을 계산하고 바이트를 평가하는 방법에 대해 설명합니다.
- 36-35페이지의 PCRE를 사용하여 내용 검색 - `pcre` 키워드를 사용하여 규칙에서 PCRE를 사용하는 방법에 대해 설명합니다.
- 36-41페이지의 규칙에 메타데이터 추가 - `metadata` 키워드를 사용하여 규칙에 정보를 추가하는 방법에 대해 설명합니다.
- 36-46페이지의 IP 헤더 값 검사- 패킷의 IP 헤더에서 값을 테스트하는 키워드의 구문 및 사용법에 대해 설명합니다.
- 36-49페이지의 ICMP 헤더 값 검사- 패킷의 ICMP 헤더에서 값을 테스트하는 키워드의 구문 및 사용법에 대해 설명합니다.
- 36-50페이지의 TCP 헤더 값 및 스트림 크기 검사- 패킷의 TCP 헤더에서 값을 테스트하는 키워드의 구문 및 사용법에 대해 설명합니다.
- 36-54페이지의 TCP 스트림 리어셈블리 활성화 및 비활성화 - 연결에서 검사된 트래픽이 규칙의 조건과 일치할 때 단일 연결에 대해 스트림 리어셈블리를 활성화 및 비활성화하는 방법에 대해 설명합니다.
- 36-55페이지의 세션에서 SSL 정보 추출 - 암호화된 트래픽에서 버전과 상태 정보를 추출하는 키워드의 구문 및 사용법에 대해 설명합니다.
- 36-83페이지의 키워드 인수로 패킷 데이터 읽어오기 - 다른 특정 키워드의 인수에 대한 값을 지정하기 위해 동일한 규칙에서 나중에 사용할 수 있는 변수로 패킷의 값을 읽어오는 방법에 대해 설명합니다.
- 36-57페이지의 애플리케이션 레이어 프로토콜 값 검사 - 애플리케이션 레이어 프로토콜 속성을 테스트하는 키워드의 구문 및 사용법에 대해 설명합니다.
- 36-80페이지의 패킷 특성 검사 - `dsize`, `sameIP`, `isdataat`, `fragoffset` 및 `cvs` 키워드의 구문 및 사용법에 대해 설명합니다.
- 36-85페이지의 규칙 키워드로 능동 응답 시작 - `resp` 키워드를 사용하여 TCP 연결 또는 UDP 세션을 능동적으로 닫고, `react` 키워드를 사용하여 HTML 페이지를 전송한 다음 TCP 연결을 능동적으로 닫고, `config response` 명령을 사용하여 능동 응답 인터페이스 및 패시브 구축에서 시도할 TCP 재설정의 횟수를 지정하는 방법에 대해 설명합니다.
- 36-89페이지의 이벤트 필터링 - 지정된 시간 내에 지정된 패킷 수가 규칙의 탐지 기준을 충족하지 않는 한 규칙이 이벤트를 트리거하지 못하게 하는 방법에 대해 설명합니다.
- 36-90페이지의 공격 이후 트래픽 평가 - 호스트 또는 세션에 대한 추가 트래픽을 로깅하는 방법에 대해 설명합니다.
- 36-91페이지의 여러 패킷에서 수행되는 공격 탐지 - 단일 세션에서 여러 패킷에 걸친 공격의 패킷에 상태 이름을 할당한 다음, 상태에 따라 패킷을 분석하고 알림을 보내는 방법에 대해 설명합니다.
- 36-96페이지의 HTTP 인코딩 유형 및 위치에서 이벤트 생성 - 표준화 전에 HTTP 요청 또는 응답 URI, 헤더 또는 쿠키(set-cookies 포함)에서 인코딩 유형에 대해 이벤트를 생성하는 방법에 대해 설명합니다.
- 36-97페이지의 파일 유형 및 버전 탐지 - `file_type` 또는 `file_group` 키워드를 사용하여 특정 파일 형식 또는 파일 버전을 가리키는 방법에 대해 설명합니다.
- 36-99페이지의 특정 페이로드 유형 가리키기 - HTTP 응답 엔티티 본문, SMTP 페이로드 또는 인코딩된 이메일 첨부 파일의 시작 부분을 가리키는 방법에 대해 설명합니다.

- 36-100페이지의 패킷 페이로드의 시작 부분 가리키기 - 패킷 페이로드의 시작 부분을 가리키는 방법에 대해 설명합니다.
- 36-101페이지의 Base64 데이터 디코딩 및 검사 - `base64_decode` 및 `base64_data` 키워드를 사용하여 특히 HTTP 요청에서 Base64 데이터를 디코딩 및 검사하는 방법에 대해 설명합니다.

침입 이벤트 세부사항 정의

라이센스: 보호

표준 텍스트 규칙을 구성할 때 규칙이 익스플로잇 시도를 탐지한 취약성을 설명하는 컨텍스트 정보를 포함할 수 있습니다. 또한 취약성 데이터베이스에 대한 외부 참조를 포함하고 조직에서 이벤트의 우선순위를 정의할 수 있습니다. 분석가들은 이벤트를 볼 때 즉시 사용 가능한 우선순위, 익스플로잇 및 알려진 완화에 대한 정보를 얻을 수 있습니다.

이벤트 관련 키워드에 대한 자세한 내용은 다음 절을 참조하십시오.

- 36-11페이지의 이벤트 메시지 정의
- 36-11페이지의 이벤트 우선순위 정의
- 36-12페이지의 침입 이벤트 분류 정의
- 36-14페이지의 이벤트 참조 정의

이벤트 메시지 정의

라이센스: 보호

규칙이 트리거될 때 메시지로서 나타나는 의미 있는 텍스트를 지정할 수 있습니다. 메시지를 보면 규칙이 익스플로잇의 시도를 탐지하는 취약성의 본성을 즉시 파악할 수 있습니다. 중괄호({})를 제외한 인쇄 가능한 표준 ASCII 문자를 사용할 수 있습니다. 시스템은 메시지를 완전히 둘러싼 따옴표를 제거합니다.

팁 규칙 메시지를 지정해야 합니다. 또한 메시지는 공백으로만, 하나 이상의 따옴표로만, 하나 이상의 아포스트로피로만 구성할 수 없으며, 공백이나 따옴표나 아포스트로피의 조합으로 구성할 수도 없습니다.

규칙 편집기에서 이벤트 메시지를 정의하려면 **Message** 필드에 이벤트 메시지를 입력하십시오. 규칙 편집기를 사용하여 규칙을 작성하는 방법에 대한 자세한 내용은 36-102페이지의 규칙 작성을/를 참조하십시오.

이벤트 우선순위 정의

라이센스: 보호

기본적으로 규칙의 우선순위는 규칙에 대한 이벤트 분류에서 파생됩니다. 그러나 규칙에 `priority` 키워드를 추가하여 규칙에 대한 분류 우선순위를 재정의할 수 있습니다.

규칙 편집기에 대한 우선순위를 지정하려면 **Detection Options** 목록에서 **priority**를 선택하고 드롭다운 목록 **high**, **medium** 또는 **low**를 선택합니다. 예를 들어, 웹 애플리케이션 공격을 탐지하는 규칙에 대해 **high** 우선순위를 할당하려면 규칙에 `priority` 키워드를 추가하고 우선순위로 **high**를 선택합니다. 규칙 편집기를 사용하여 규칙을 작성하는 방법에 대한 자세한 내용은 36-102페이지의 규칙 작성을/를 참조하십시오.

침입 이벤트 분류 정의

라이센스: 보호

각 규칙에 대해 이벤트의 패킷 표시에 나타나는 공격 분류를 지정할 수 있습니다. 다음 표에는 각 분류의 이름과 번호가 나열되어 있습니다.

표 36-5 규칙 분류

번호	분류 이름	설명
1	not-suspicious	의심스럽지 않은 트래픽
2	unknown	알 수 없는 트래픽
0.3	bad-unknown	잠재적으로 나쁜 트래픽
4	attempted-recon	정보 유출 시도
5	successful-recon-limited	정보 유출
6	successful-recon-largescale	대규모 정보 유출
7	attempted-dos	서비스 거부 시도
8	successful-dos	서비스 거부
9	attempted-user	사용자 권한 확보 시도
10	unsuccessful-user	사용자 권한 확보 실패
11	successful-user	사용자 권한 확보 성공
12	attempted-admin	관리자 권한 확보 시도
13	successful-admin	관리자 권한 확보 성공
14	rpc-portmap-decode	RPC 쿼리 디코딩
15	shellcode-detect	실행 코드가 탐지됨
16	string-detect	의심스러운 문자열이 탐지됨
17	suspicious-filename-detect	의심스러운 파일 이름이 탐지됨
18	suspicious-login	의심스러운 사용자 이름을 사용한 로그인 시도가 탐지됨
19	system-call-detect	시스템 호출이 탐지됨
20	tcp-connection	TCP 연결이 탐지됨
21	trojan-activity	네트워크 트로이 목마 탐지
22	unusual-client-port-connection	클라이언트가 특이한 포트 사용
23	network-scan	네트워크 스캔 탐지
24	denial-of-service	서비스 거부 공격 탐지
25	non-standard-protocol	비표준 프로토콜 또는 이벤트 탐지
26	protocol-command-decode	일반 프로토콜 명령 디코딩
27	web-application-activity	잠재적으로 취약한 웹 애플리케이션에 액세스
28	web-application-attack	웹 애플리케이션 공격
29	misc-activity	기타 활동
30	misc-attack	기타 공격
31	icmp-event	일반 ICMP 이벤트

표 36-5 규칙 분류(계속)

번호	분류 이름	설명
32	inappropriate-content	부적절한 내용이 탐지됨
33	policy-violation	잠재적인 회사 비공개 정보 보호 위반
34	default-login-attempt	기본 사용자 이름 및 비밀번호로 로그인 시도
35	sdf	민감한 데이터
36	malware-cnc	알려진 악성코드 명령 및 제어 트래픽
37	client-side-exploit	알려진 클라이언트 측 익스플로잇 시도
38	file-format	알려진 악의적인 파일 및 파일 기반 익스플로잇

규칙 편집기에서 분류를 지정하려면 **Classification** 목록에서 분류를 선택합니다. 규칙 편집기에 대한 자세한 내용은 36-103페이지의 새 규칙 작성을/를 참조하십시오.

사용자 지정 분류 추가

라이센스: 보호

정의한 규칙에 의해 생성되는 이벤트의 패킷 표시 설명 내용을 좀 더 세부적으로 사용자 지정하려면 사용자 지정 분류를 생성할 수 있습니다.

Classification 목록에 분류를 추가하려면

액세스: Admin/Intrusion Admin

1단계 **Policies > Intrusion > Rule Editor**를 선택합니다.

Rule Editor 페이지가 나타납니다.

2단계 **Create Rule**을 클릭합니다.

Create Rule 페이지가 나타납니다.

3단계 **Classification** 드롭다운 목록에서 **Edit Classifications**를 클릭합니다.

팝업 창이 나타납니다.

4단계 **Classification Name** 필드에 분류의 이름을 입력합니다.

최대 255자의 영숫자 문자를 사용할 수 있지만, 40자가 넘을 경우 페이지에서 읽는 데 어려움이 있습니다. `<>()\'"&$;` 및 공백 문자는 지원되지 않습니다.

5단계 **Classification Description** 필드에 분류의 설명을 입력합니다.

영숫자와 공백을 포함하여 최대 255자로 입력할 수 있습니다. `<>()\'"&$;` 문자는 지원되지 않습니다.

6단계 **Priority** 목록에서 우선순위를 선택합니다.

high, **medium**, 또는 **low**를 선택할 수 있습니다.

7단계 **Add**를 클릭합니다.

새 분류가 목록에 추가되고 규칙 편집기에서 사용할 수 있게 됩니다.

8단계 **Done**을 클릭합니다.

이벤트 참조 정의

라이센스: 보호

외부 웹사이트에 대한 참조 및 이벤트에 대한 정보를 추가하려면 `reference` 키워드를 사용할 수 있습니다. 참조를 추가하면 분석가들은 패킷이 규칙을 트리거한 이유를 파악하는 데 도움이 되는 즉시 사용 가능한 리소스를 얻을 수 있습니다. 다음 표에는 알려진 익스플로잇 및 공격에 대한 데이터를 제공할 수 있는 몇몇 외부 시스템이 나열되어 있습니다.

표 36-6 외부 공격 식별 시스템

시스템 ID	설명	예?ID
`bugtraq`	Bugtraq 페이지	`8550`
`cve`	Common Vulnerabilities and Exposure 페이지	`CAN-2003-0702`
`mcafee`	McAfee 페이지	`98574`
`url`	웹사이트 참조	`www.example.com?exploit=14`
`msb`	Microsoft 보안 게시판	`MS11-082`
`nessus`	Nessus 페이지	`10039`
`secure-url`	보안 웹사이트 참조 (https://...)	`intranet/exploits/exploit=14` 보안 웹사이트에는 `secure-url`을 사용할 수 있습니다.

규칙 편집기를 사용하여 참조를 지정하려면 **Detection Options** 목록에서 **reference**를 선택하고 다음과 같이 해당 필드에 값을 입력합니다.

id_system,*id*

여기서 *id_system*은 접두사로 사용되고 있는 시스템이고, *id*는 Bugtraq ID, CVE 번호, Arachnids ID 또는 URL(`http://` 없음)입니다.

예를 들어, Bugtraq ID 17134에 설명된 Microsoft Commerce Server 2002 서버에 대한 인증 우회 취약성을 지정하려면 **reference** 필드에 다음을 입력합니다.

```
bugtraq,17134
```

규칙에 참조를 추가할 때는 다음에 유의하십시오.

- 쉼표 뒤에는 공백을 사용하지 않습니다.
- 시스템 ID에는 대문자를 사용하지 않습니다.

규칙 편집기를 사용하여 규칙을 작성하는 방법에 대한 자세한 내용은 36-102페이지의 규칙 작성을/를 참조하십시오.

내용 일치 검색

라이센스: 보호

패킷에서 탐지할 내용을 지정하려면 `content` 키워드 또는 `protected_content` 키워드를 사용합니다. 자세한 내용은 다음 절을 참조하십시오.

- 36-15페이지의 content 키워드 사용
- 36-15페이지의 protected_content 키워드 사용
- 36-16페이지의 내용 일치 구성

content 키워드 사용

content 키워드를 사용하면 규칙 엔진은 패킷 페이로드를 검색하거나 해당 문자열을 스트리밍합니다. 예를 들어 content 키워드 중 하나의 값으로 /bin/sh를 입력하면 규칙 엔진은 패킷 페이로드에서 문자열 /bin/sh를 검색합니다.

ASCII 문자열, 16진수 내용(이진 바이트 코드) 또는 둘의 조합을 사용하여 내용을 매칭합니다. 키워드 값에서 파이프 문자(|)로 16진수 내용을 감쌉니다. 예를 들면 |90C8 C0FF FFFF|/bin/sh에서와 같이 16진수 내용과 ASCII 내용을 혼합할 수 있습니다.

단일 규칙에서 여러 내용 일치를 지정할 수 있습니다. 이렇게 하려면 content 키워드의 추가 인스턴스를 사용합니다. 각 내용 일치에 대해, 규칙을 트리거하려면 내용 일치가 패킷 페이로드에서 또는 스트림에서 발견되어야 한다고 지정할 수 있습니다.

protected_content 키워드 사용

protected_content 키워드를 사용하면 규칙 인수를 구성하기 전에 검색 내용을 인코딩할 수 있습니다. 원래 규칙 작성자는 키워드를 구성하기 전 문자열을 인코딩하기 위해 해시 함수(SHA-512, SHA-256 또는 MD5)를 사용합니다.

content 키워드 대신 protected_content 키워드를 사용할 경우, 규칙 엔진이 해당 문자열에 대해 패킷 페이로드 또는 스트림을 검색하는 방법에는 변화가 없으며 키워드 옵션 기능은 대부분 예상대로 작동합니다. 다음 표에는 예외가 요약되어 있습니다. 여기서 protected_content 키워드 옵션은 content 키워드 옵션과 다릅니다.

표 36-7 protected_content 옵션 예외

옵션	설명
Hash Type	protected_content 규칙 키워드에 대한 새 옵션. 자세한 내용은 36-18페이지의 Hash Type을/를 참조하십시오.
Case Insensitive	지원되지 않음
Within	지원되지 않음
Depth	지원되지 않음
Length	protected_content 규칙 키워드에 대한 새 옵션. 자세한 내용은 36-21페이지의 Length을/를 참조하십시오.
Use Fast Pattern Matcher	지원되지 않음
Fast Pattern Matcher Only	지원되지 않음
Fast Pattern Matcher Offset and Length	지원되지 않음

Cisco에서는, 규칙 엔진이 fast pattern matcher를 사용하도록 하려면 protected_content 키워드가 포함된 규칙에 하나 이상의 content 키워드를 포함할 것을 권장합니다. 이렇게 하면 처리 속도가 빨라지고 성능이 향상됩니다. 규칙에서 content 키워드를 protected_content 키워드 앞에 두십시오. Use Fast Pattern Matcher 인수에서 content 키워드의 활성화 여부와 상관없이, 규칙에 content 키워드가 하나 이상 포함되어 있으면 규칙 엔진은 fast pattern matcher를 사용합니다.

내용 일치 구성

거의 항상 content 또는 protected_content 키워드 뒤에는 내용을 검색해야 할 위치, 검색의 대/소문자 구분 여부 및 기타 옵션을 나타내는 수정자를 사용해야 합니다. content 및 protected_content 키워드의 수정자에 대한 자세한 내용은 내용 일치 제한을/를 참조하십시오.

규칙이 이벤트를 트리거하려면 모든 내용 일치가 참이어야 합니다. 즉, 각 내용 일치에는 다른 내용 일치와의 AND 관계가 있어야 합니다.

또한 인라인 구축에서는 악의적인 내용과 일치하는 규칙을 설정한 다음 동일한 길이의 고유한 텍스트 문자열과 교체할 수 있습니다. 자세한 내용은 36-29페이지의 인라인 구축에서 내용 교체을/를 참조하십시오.

매칭할 content를 입력하려면

액세스: Admin/Intrusion Admin

1단계 content 필드에 찾으려는 내용(예: |90C8 C0FF FFFF|/bin/sh)을 입력합니다.

지정한 내용이 **아닌** 내용을 검색하려면 **Not** 확인란을 선택합니다.

주의 content 키워드가 하나만 포함된 규칙을 생성하고 키워드에 대해 **Not** 옵션을 선택한 경우 침입 정책을 무효화할 수 있습니다. 자세한 내용은 36-19페이지의 Not을/를 참조하십시오.

2단계 선택적으로, content 키워드를 수정하는 키워드를 더 추가하거나 키워드에 대한 제한 사항을 추가합니다. 기타 키워드에 대한 자세한 내용은 36-9페이지의 규칙의 키워드 및 인수 이해을/를 참조하십시오.

content 키워드 제한에 대한 자세한 내용은 36-17페이지의 내용 일치 제한을/를 참조하십시오.

3단계 계속해서 규칙을 생성 또는 수정합니다.

자세한 내용은 36-103페이지의 새 규칙 작성 또는 36-104페이지의 기존 규칙 수정을/를 참조하십시오.

매칭할 protected content를 입력하려면

액세스: Admin/Intrusion Admin

1단계 SHA-512, SHA-256 또는 MD5 해시 생성기를 사용하여 찾으려는 내용을 인코딩합니다(예: SHA-512 해시 생성기를 통해 문자열 Sample1 실행).

생성기는 문자열에 대한 해시를 출력합니다.

2단계 1단계에서 생성한 해시를 protected_content 필드에 입력합니다(예: B20AABAF59605118593404BD42FE69BD8D6506EE7F1A71CE6BB470B1DF848C814BC5DBEC2081999F15691A71FAECA5FBA4A3F8B8AB56B7F04585DA6D73E5DD15).

지정한 내용이 **아닌** 내용을 검색하려면 **Not** 확인란을 선택합니다.

주의 protected_content 키워드가 하나만 포함된 규칙을 생성하고 키워드에 대해 **Not** 옵션을 선택한 경우 침입 정책을 무효화할 수 있습니다. 자세한 내용은 36-19페이지의 Not을/를 참조하십시오.

3단계 1단계에서 사용한 해시 함수를 **Hash Type** 드롭다운 목록에서 선택합니다(예: **SHA-512**). 2단계에서 입력한 해시의 비트 수는 해시 유형과 **반드시** 일치해야 합니다. 그렇지 않으면 시스템에서 규칙을 저장하지 않습니다. 자세한 내용은 36-18페이지의 Hash Type을/를 참조하십시오.

팁 Cisco 설정 **Default**를 선택하면 시스템은 SHA-512를 해시 함수로 간주합니다.

4단계 필수 **Length** 필드에 값을 입력합니다. 이 값은 찾으려고 하는 원래의 해시되지 않은 문자열 길이와 **반드시** 일치해야 합니다(예: 2단계의 문자열 `Sample1`은 길이가 7).

자세한 내용은 36-21페이지의 Length을/를 참조하십시오.

5단계 **Offset** 또는 **Distance** 필드에 값을 입력합니다. 단일 키워드 컨피그레이션 내에 **Offset** 및 **Distance** 옵션을 혼합할 수 없습니다.

자세한 내용은 36-22페이지의 protected_content 키워드에서 검색 위치 옵션 사용을/를 참조하십시오.

6단계 선택적으로, `protected_content` 키워드를 수정하는 제한 옵션을 더 추가합니다.

자세한 내용은 36-17페이지의 내용 일치 제한을/를 참조하십시오.

7단계 선택적으로, `protected_content` 키워드를 수정하는 키워드를 더 추가합니다.

자세한 내용은 36-9페이지의 규칙의 키워드 및 인수 이해을/를 참조하십시오.

8단계 계속해서 규칙을 생성 또는 수정합니다.

자세한 내용은 36-103페이지의 새 규칙 작성 또는 36-104페이지의 기존 규칙 수정을/를 참조하십시오.

내용 일치 제한

라이센스: 보호

`content` 또는 `protected_content` 키워드를 수정하는 매개 변수로 내용 검색의 위치 및 대/소문자 구분을 제한할 수 있습니다. `content` 또는 `protected_content` 키워드를 수정하여 검색할 내용을 지정할 수 있는 옵션을 구성합니다.

자세한 내용은 다음 절을 참조하십시오.

- 36-18페이지의 Case Insensitive
- 36-18페이지의 Hash Type
- 36-19페이지의 Raw Data
- 36-19페이지의 Not
- 36-20페이지의 검색 위치 옵션
- 36-23페이지의 HTTP Content 옵션
- 36-26페이지의 Fast Pattern Matcher 사용

Case Insensitive

라이센스: 보호

참고 `protected_content` 키워드를 구성하면 이 옵션은 지원되지 **않습니다**. 자세한 내용은 36-15페이지의 protected_content 키워드 사용을/를 참조하십시오.

ASCII 문자열에서 내용 일치를 검색할 때 대/소문자를 무시하도록 검색 엔진에 지시할 수 있습니다. 검색에서 대/소문자를 구분하도록 하려면 내용 검색을 지정할 때 **Case Insensitive**를 선택합니다.

내용을 검색할 때 Case Insensitive를 지정하려면

액세스: Admin/Intrusion Admin

1단계 추가하는 `content` 키워드에 대해 **Case Insensitive**를 선택합니다.

2단계 계속해서 규칙을 생성 또는 수정합니다.

자세한 내용은 내용 일치 제한, 36-14페이지의 내용 일치 검색, 36-103페이지의 새 규칙 작성 또는 36-104페이지의 기존 규칙 수정을/를 참조하십시오.

Hash Type

라이센스: 보호

참고 이 옵션은 `protected_content` 키워드**에서만** 구성할 수 있습니다. 자세한 내용은 36-15페이지의 protected_content 키워드 사용을/를 참조하십시오.

검색 문자열 인코딩에 사용한 해시 함수를 식별하려면 **Hash Type** 드롭다운을 사용합니다. `protected_content` 검색 문자열에 대해서는 SHA-512, SHA-256 및 MD5 해싱이 지원됩니다. 해시된 내용의 길이가 선택한 해시 유형과 일치하지 않으면 시스템은 규칙을 저장하지 **않습니다**.

시스템은 자동으로 Cisco 설정 기본값을 선택합니다. **Default**가 선택되면 규칙에 특정 해시 함수가 기록되지 않으며 시스템은 SHA-512를 해시 함수로 간주합니다.

protected content 검색 중에 해시 함수를 지정하려면

1단계 **Hash Type** 드롭다운 목록에서 추가하는 `protected_content` 키워드에 대한 해시로 **Default**, **SHA-512**, **SHA-256** 또는 **MD5**를 선택합니다.

팁 Cisco 설정 **Default**를 선택하면 시스템은 SHA-512를 해시 함수로 간주합니다. 자세한 내용은 36-18페이지의 Hash Type을/를 참조하십시오.

2단계 계속해서 규칙을 생성 또는 수정합니다. 자세한 내용은 내용 일치 제한, 36-14페이지의 내용 일치 검색, 36-103페이지의 새 규칙 작성 또는 36-104페이지의 기존 규칙 수정을/를 참조하십시오.

Raw Data

라이센스: 보호

Raw Data 옵션은 표준화된 페이로드 데이터(네트워크 분석 정책으로 디코딩된)를 분석하기 전에 원래 패킷 페이로드를 분석하도록 규칙 엔진에 지시하며 인수 값을 사용하지 않습니다. 텔넷 트래픽을 분석할 때 표준화 전에 페이로드에서 텔넷 협상 옵션을 확인하려면 이 키워드를 사용할 수 있습니다.

Raw Data 옵션은 동일한 `content` 또는 `protected_content` 키워드에서 HTTP content 옵션과 함께 사용할 수 없습니다. 자세한 내용은 36-23페이지의 HTTP Content 옵션을/를 참조하십시오.

팁 원시 데이터를 HTTP 트래픽에서 검사할지 여부 및 검사해야 할 원시 데이터의 양을 결정하려면 HTTP Inspect 프리프로세서 **Client Flow Depth** 및 **Server Flow Depth** 옵션을 구성할 수 있습니다. 자세한 내용은 27-32페이지의 서버 레벨 HTTP 표준화 옵션 선택을/를 참조하십시오.

원시 데이터를 분석하려면

액세스: Admin/Intrusion Admin

1단계 추가하는 `content` 또는 `protected_content` 키워드에 대해 **Raw Data** 확인란을 선택합니다.

2단계 계속해서 규칙을 생성 또는 수정합니다. 자세한 내용은 내용 일치 제한, 36-14페이지의 내용 일치 검색, 36-103페이지의 새 규칙 작성 또는 36-104페이지의 기존 규칙 수정을/를 참조하십시오.

Not

라이센스: 보호

지정한 내용과 일치하지 않는 내용을 검색하려면 **Not** 옵션을 선택합니다. **Not** 옵션을 선택한 상태로 `content` 또는 `protected_content` 키워드가 포함된 규칙을 생성하는 경우, **Not** 옵션을 선택하지 않은 상태로 하나 이상의 `content` 또는 `protected_content` 키워드를 규칙에 포함해야 합니다.

주의 **Not** 옵션을 선택한 경우 `content` 또는 `protected_content` 키워드가 하나만 포함된 규칙을 생성해서는 안 됩니다. 침입 정책이 무효화될 수 있습니다.

예를 들어 SMTP rule 1:2541:9에는 세 개의 `content` 키워드가 포함되어 있으며, 그중 하나에 대해서만 **Not** 옵션이 선택되어 있습니다. **Not** 옵션이 선택된 하나를 제외하고 모든 `content` 키워드를 제거하면 이 규칙을 기반으로 하는 사용자 지정 규칙은 무효가 됩니다. 그런 규칙을 침입 정책에 추가하면 정책이 무효화될 수 있습니다.

지정한 내용과 일치하지 않는 내용을 검색하려면

액세스: Admin/Intrusion Admin

1단계 추가하는 `content` 또는 `protected_content` 키워드에 대해 **Not** 확인란을 선택합니다.

팁 동일한 `content` 키워드에서 **Not** 확인란과 **Use Fast Pattern Matcher** 확인란을 모두 선택할 수는 없습니다.

2단계 **Not** 옵션이 선택되지 않은 하나 이상의 다른 `content` 또는 `protected_content` 키워드를 규칙에 포함합니다.

3단계 계속해서 규칙을 생성 또는 수정합니다. 자세한 내용은 내용 일치 제한, 36-14페이지의 내용 일치 검색, 36-103페이지의 새 규칙 작성 또는 36-104페이지의 기존 규칙 수정을/를 참조하십시오.

검색 위치 옵션

라이센스: 보호

지정된 내용에 대한 검색을 어디에서 시작할지, 어디까지 계속해야 할지를 지정하려면 검색 위치 옵션을 사용할 수 있습니다. 각 옵션에 대한 자세한 내용은 다음을 참조하십시오.

- 36-20페이지의 Depth
- 36-20페이지의 Distance
- 36-21페이지의 Length
- 36-21페이지의 Offset
- 36-21페이지의 Within

`content` 또는 `protected_content` 키워드 내에서 검색 위치 옵션을 사용하는 방법에 대한 자세한 내용은 다음을 참조하십시오.

- 36-21페이지의 content 키워드에서 검색 위치 옵션 사용
- 36-22페이지의 protected_content 키워드에서 검색 위치 옵션 사용

Depth

참고 이 옵션은 `content` 키워드를 구성하는 **경우에만** 지원됩니다. 자세한 내용은 36-15페이지의 content 키워드 사용을/를 참조하십시오.

오프셋 값의 시작부터 최대 내용 검색 깊이를 바이트 단위로 지정합니다. 오프셋을 구성하지 않으면 패킷 페이로드의 처음부터 검색이 시작됩니다.

예를 들어 content 값 `cgi-bin/phf`, `offset` 값 `3`, `depth` 값 `22`의 규칙에서는, 규칙 헤더에 지정된 매개 변수를 충족하는 패킷에서 `cgi-bin/phf` 문자열에 대한 일치 검색이 3바이트에서 시작되고 22바이트를 처리한 후(25바이트에서) 중지됩니다.

지정된 내용의 길이보다 크거나 같은 값을 최대 65535바이트까지 지정해야 합니다. 값 0은 지정할 수 없습니다.

기본값은 패킷의 끝까지 검색하는 것입니다.

Distance

전에 성공한 내용 일치 이후 지정된 바이트에서 발생하는 후속 내용 일치를 식별하도록 규칙 엔진에 지시합니다.

Distance 카운터는 0에서 시작하므로 마지막으로 성공한 내용 일치 이후 진행할 바이트 수보다 1 작은 수를 지정합니다. 예를 들어 4를 지정하면 검색은 5번째 바이트에서 시작됩니다.

범위 -65535~65535바이트의 값을 지정할 수 있습니다. 음의 `Distance` 값을 지정하면 검색을 시작하는 바이트가 패킷의 시작 밖이 될 수 있습니다. 검색은 실제로 패킷의 첫 번째 바이트부터 시작되지만 계산에서는 패킷 외부의 바이트 값이 나올 수 있습니다. 예를 들어 패킷의 현재 위치가 5번째 바이트이고 다음 내용 규칙 옵션에서 `Distance` 값 -10이며 `Within` 값이 20이면, 검색은 페이로드의 처음부터 시작되며 `Within` 옵션은 15로 조정됩니다.

기본값은 0, 즉 마지막 내용 일치 이후 패킷의 현재 위치입니다.

Length

참고 이 옵션은 `protected_content` 키워드를 구성하는 **경우에만** 지원됩니다. 자세한 내용은 36-15페이지의 protected_content 키워드 사용을/를 참조하십시오.

Length `protected_content` 키워드 옵션은 해시되지 않은 검색 문자열의 길이를 바이트 단위로 나타냅니다.

예를 들어 안전한 해시를 생성하기 위해 내용 `Sample1` 을 사용한 경우 **Length** 값에 `7`을 사용하십시오. 이 필드에는 **반드시** 값을 입력해야 합니다.

Offset

패킷 페이로드의 처음을 기준으로 내용 검색을 시작할 패킷 페이로드의 위치를 바이트 단위로 지정합니다. 범위 -65535~65535바이트의 값을 지정할 수 있습니다.

Offset 카운터는 0에서 시작하므로 패킷 페이로드의 시작 부분에서 진행할 바이트 수보다 1 작은 수를 지정합니다. 예를 들어 7을 지정하면 검색은 8번째 바이트에서 시작됩니다.

기본값은 0, 즉 패킷의 처음입니다.

Within

참고 이 옵션은 `content` 키워드를 구성하는 **경우에만** 지원됩니다. 자세한 내용은 36-15페이지의 content 키워드 사용을/를 참조하십시오.

Within 옵션은, 규칙을 트리거하려면 다음 내용 일치가 마지막으로 성공한 내용 일치의 끝으로부터 지정한 바이트 수 이내에 발생해야 함을 의미합니다. 예를 들어 **Within** 값으로 `8`을 지정하면 다음 내용 일치는 패킷 페이로드의 다음 8바이트 이내에 발생해야 합니다. 그렇지 않으면 규칙 트리거 기준이 충족되지 않습니다.

지정된 내용의 길이보다 크거나 같은 값을 최대 65535바이트까지 지정할 수 있습니다.

Within의 기본값은 패킷의 끝까지 검색하는 것입니다.

content 키워드에서 검색 위치 옵션 사용

지정된 내용에 대한 검색을 어디에서 시작할지, 어디까지 계속해야 할지를 지정하려면 다음과 같이 두 가지 `content` 위치 쌍 중 하나를 사용할 수 있습니다.

- 패킷 페이로드의 시작을 기준으로 검색하려면 **Offset** 및 **Depth**를 함께 사용합니다.
- 현재 검색 위치를 기준으로 검색하려면 **Distance** 및 **Within**을 함께 사용합니다.

한 쌍에서 한 옵션만 지정하면 나머지 옵션은 기본값으로 간주됩니다.

Offset 및 **Depth** 옵션을 **Distance** 및 **Within** 옵션과 혼합하여 사용할 수 없습니다. 예를 들어 **Offset** 및 **Within** 쌍은 사용할 수 없습니다. 규칙에서 위치 옵션은 원하는 만큼 사용할 수 있습니다.

위치가 지정되지 않으면 **Offset** 및 **Depth**의 기본값이 사용됩니다. 즉, 내용 검색은 패킷 페이로드의 처음부터 시작되고 패킷의 끝까지 계속됩니다.

위치 옵션에 대한 값을 지정하는 데 기존의 `byte_extract` 변수를 사용할 수도 있습니다. 자세한 내용은 36-83페이지의 키워드 인수로 패킷 데이터 읽어오기을/를 참조하십시오.

웹 인터페이스를 통해 content 키워드에서 검색 위치를 지정하려면

액세스: Admin/Intrusion Admin

1단계 추가하는 `content` 키워드에 대해 필드에 값을 입력합니다. 다음 옵션을 이용할 수 있습니다.

- **Offset**
- **Depth**
- **Distance**
- **Within**

규칙에서 위치 옵션은 원하는 만큼 사용할 수 있습니다.

2단계 계속해서 규칙을 생성 또는 수정합니다. 자세한 내용은 36-17페이지의 내용 일치 제한, 36-14페이지의 내용 일치 검색, 36-103페이지의 새 규칙 작성 또는 36-104페이지의 기존 규칙 수정을/를 참조하십시오.

protected_content 키워드에서 검색 위치 옵션 사용

지정된 내용에 대한 검색을 어디에서 시작할지, 어디까지 계속해야 할지를 지정하려면 다음과 같이 필수 **Length** `protected_content` 위치 옵션을 **Offset** 또는 **Distance** 위치 옵션 중 하나와 함께 사용하십시오.

- 패킷 페이로드의 시작을 기준으로 보호되는 문자열을 검색하려면 **Length** 및 **Offset**을 함께 사용합니다.
- 현재 검색 위치를 기준으로 보호되는 문자열을 검색하려면 **Length** 및 **Distance**를 함께 사용합니다.

팁 단일 키워드 컨피그레이션에서는 **Offset** 및 **Distance** 옵션을 혼합하여 사용할 수 없지만, 규칙에서는 위치 옵션을 원하는 만큼 사용할 수 있습니다.

위치가 지정되지 않으면 기본값이 사용됩니다. 즉, 내용 검색은 패킷 페이로드의 처음부터 시작되고 패킷의 끝까지 계속됩니다.

위치 옵션에 대한 값을 지정하는 데 기존의 `byte_extract` 변수를 사용할 수도 있습니다. 자세한 내용은 36-83페이지의 키워드 인수로 패킷 데이터 읽어오기을/를 참조하십시오.

웹 인터페이스를 통해 protected_content 키워드에서 검색 위치를 지정하려면

액세스: Admin/Intrusion Admin

1단계 추가하는 `protected_content` 키워드에 대해 필드에 값을 입력합니다. 다음 옵션을 이용할 수 있습니다.

- **Length**(필수)
- **Offset**
- **Distance**

단일 protected_content 키워드에서는 **Offset** 및 **Distance** 옵션을 혼합하여 사용할 수 없지만, 규칙에서는 위치 옵션을 원하는 만큼 사용할 수 있습니다.

2단계 계속해서 규칙을 생성 또는 수정합니다. 자세한 내용은 36-17페이지의 내용 일치 제한, 36-14페이지의 내용 일치 검색, 36-103페이지의 새 규칙 작성 또는 36-104페이지의 기존 규칙 수정을/를 참조하십시오.

HTTP Content 옵션

라이센스: 보호

HTTP content 또는 protected_content 키워드 옵션을 사용하면 HTTP Inspect 프리프로세서에 의해 디코딩된 HTTP 메시지 내의 어디에서 내용 일치를 검색할지를 지정할 수 있습니다.

HTTP 응답의 두 가지 옵션 검색 상태 필드

- **HTTP Status Code**
- **HTTP Status Message**

규칙 엔진은 원시의 표준화되지 않은 상태 필드를 검색하지만, 다른 원시 HTTP 필드 및 표준화된 HTTP 필드를 조합할 때 고려해야 할 제한 사항에 따라 설명을 간소화하기 위해 여기에서는 이러한 옵션이 별도로 나열되어 있습니다.

HTTP 요청, 응답 또는 둘 모두에서 사용되는 5가지 옵션 검색 표준화 필드(자세한 내용은 36-23페이지의 HTTP Content 옵션 참조)

- **HTTP URI**
- **HTTP 방법**
- **HTTP헤더**
- **HTTP Cookie**
- **HTTP Client Body**

HTTP 요청, 응답 또는 둘 모두에서 사용되는 3가지 옵션 검색 원시(비표준화) 비상태 필드(자세한 내용은 36-23페이지의 HTTP Content 옵션 참조)

- **HTTP Raw URI**
- **HTTP Raw Header**
- **HTTP Raw Cookie**

HTTP content 옵션을 선택할 경우 다음 지침을 사용하십시오.

- HTTP content 옵션은 TCP 트래픽에만 적용됩니다.
- 성능에 악영향을 주지 않으려면 지정된 내용이 나타날 것 같은 메시지의 부분만 선택합니다.

  예를 들어 트래픽에 장바구니 메시지의 쿠키처럼 대규모 쿠키가 포함되었을 것 같으면, 지정된 내용을 HTTP 쿠키가 아니라 HTTP 헤더에서 검색할 수 있습니다.
- HTTP Inspect 프리프로세서 표준화를 이용하고 성능을 개선하려면, 생성하는 HTTP 관련 규칙에는 최소한 하나 이상의 content 또는 protected_content 키워드가 포함되어 있어야 하며 **HTTP URI**, **HTTP Method**, **HTTP Header** 또는 **HTTP Client Body** 옵션이 선택되어 있어야 합니다.
- replace 키워드는 HTTP content 또는 protected_content 키워드 옵션과 함께 사용할 수 없습니다.

일치하는 내용 영역을 대상으로 하려면 단일 표준화 HTTP 옵션 또는 상태 필드를 지정하거나, 표준화 HTTP 옵션과 상태 필드를 원하는 조합으로 사용할 수 있습니다. 그러나 HTTP 필드 옵션을 사용할 때는 다음 제한 사항에 유의해야 합니다.

- **Raw Data** 옵션은 동일한 `content` 또는 `protected_content` 키워드에서 HTTP 옵션과 함께 사용할 수 없습니다.
- 원시 HTTP 필드 옵션(**HTTP Raw URI**, **HTTP Raw Header** 또는 **HTTP Raw Cookie**)을 동일한 `content` 또는 `protected_content` 키워드에서 해당 표준화 옵션(각각 **HTTP URI**, **HTTP Header** 또는 **HTTP Cookie**)과 함께 사용할 수 없습니다.
- 하나 이상의 다음 HTTP 필드 옵션과 함께 **Use Fast Pattern Matcher**를 선택할 수 없습니다.

  HTTP Raw URI, **HTTP Raw Header**, **HTTP Raw Cookie**, **HTTP Cookie**, **HTTP Method**, **HTTP Status Message** 또는 **HTTP Status Code**

  그러나 다음의 표준화 필드 중 하나를 검색하는 데 역시 fast pattern matcher를 사용하는 `content` 또는 `protected_content` 키워드에는 위의 옵션을 포함할 수 있습니다.

  HTTP URI, **HTTP Header** 또는 **HTTP Client Body**

  예를 들어 **HTTP Cookie**, **HTTP Header** 및 **Use Fast Pattern Matcher**를 선택하면 규칙 엔진은 HTTP 쿠키와 HTTP 헤더에서 모두 내용을 검색하지만, fast pattern matcher는 HTTP 쿠키가 아니라 HTTP 헤더에만 적용됩니다.
- 제한 옵션과 비제한 옵션을 결합하면 fast pattern matcher는 사용자가 지정한 비제한 필드만 검색하여, 제한된 필드에 대한 평가를 비롯한 완전한 평가를 위해 규칙 편집기로 규칙을 전달할지 여부를 테스트합니다. 자세한 내용은 36-26페이지의 Fast Pattern Matcher 사용을/를 참조하십시오.

위의 제한 사항은 HTTP `content` 및 `protected_content` 키워드 옵션을 설명하는 다음 목록의 각 옵션에 대한 설명에도 반영됩니다.

HTTP URI

표준화된 요청 URI 필드에서 내용 일치를 검색하려면 이 옵션을 선택합니다.

이 옵션은 `pcre` 키워드 HTTP URI (U) 옵션과 함께 동일한 내용을 검색하는 데 사용할 수 없습니다. 자세한 내용은 Snort 전용 Post 정규식 수정자 표를 참조하십시오.

참고 파이프라인된 HTTP 요청 패킷에는 여러 URI가 포함되어 있습니다. **HTTP URI**가 선택된 상태에서 파이프라인된 HTTP 요청 패킷이 탐지되면 규칙 엔진은 패킷의 모든 URI에서 내용 일치를 검색합니다.

HTTP Raw URI

표준화된 요청 URI 필드에서 내용 일치를 검색하려면 이 옵션을 선택합니다.

이 옵션은 `pcre` 키워드 HTTP URI (U) 옵션과 함께 동일한 내용을 검색하는 데 사용할 수 없습니다. 자세한 내용은 Snort 전용 Post 정규식 수정자 표를 참조하십시오.

참고 파이프라인된 HTTP 요청 패킷에는 여러 URI가 포함되어 있습니다. **HTTP URI**가 선택된 상태에서 파이프라인된 HTTP 요청 패킷이 탐지되면 규칙 엔진은 패킷의 모든 URI에서 내용 일치를 검색합니다.

HTTP Method

요청 메서드 필드에서 내용 일치를 검색하려면, URI에서 식별된 리소스에 대해 수행할 GET 및 POST 같은 작업을 식별하는 이 옵션을 선택합니다.

HTTP Header

HTTP 요청의 표준화된 헤더 필드에서(쿠키 제외), 그리고 HTTP Inspect 프리프로세서 **Inspect HTTP Responses** 옵션이 활성화되었을 때 응답에서 내용 일치를 검색하려면 이 옵션을 선택합니다.

이 옵션은 `pcre` 키워드 HTTP header (H) 옵션과 함께 동일한 내용을 검색하는 데 사용할 수 없습니다. 자세한 내용은 Snort 전용 Post 정규식 수정자 표를 참조하십시오.

HTTP Raw Header

HTTP 요청의 원시 헤더 필드에서(쿠키 제외), 그리고 HTTP Inspect 프리프로세서 **Inspect HTTP Responses** 옵션이 활성화되었을 때 응답에서 내용 일치를 검색하려면 이 옵션을 선택합니다.

이 옵션은 `pcre` 키워드 HTTP raw header (D) 옵션과 함께 동일한 내용을 검색하는 데 사용할 수 없습니다. 자세한 내용은 Snort 전용 Post 정규식 수정자 표를 참조하십시오.

HTTP Cookie

표준화된 HTTP 클라이언트 요청 헤더에서 식별된 쿠키에서, 그리고 HTTP Inspect 프리프로세서 **Inspect HTTP Responses** 옵션이 활성화되었을 때 응답 set-cookie 데이터에서 내용 일치를 검색하려면 이 옵션을 선택합니다. 시스템은 메시지 본문에 포함된 쿠키를 본문 내용으로 취급합니다.

일치 내용을 쿠키에서만 검색하려면 HTTP Inspect 프리프로세서 **Inspect HTTP Cookies** 옵션을 활성화해야 합니다. 그렇게 하지 않으면 규칙 엔진은 쿠키를 포함하여 전체 헤더를 검색합니다. 자세한 내용은 27-32페이지의 서버 레벨 HTTP 표준화 옵션 선택을/를 참조하십시오.

다음에 유의하십시오.

- 이 옵션은 `pcre` 키워드 HTTP cookie (C) 옵션과 함께 동일한 내용을 검색하는 데 사용할 수 없습니다. 자세한 내용은 Snort 전용 Post 정규식 수정자 표를 참조하십시오.
- `Cookie:` 및 `Set-Cookie:` 헤더 이름, 헤더 줄의 선행 공백, 헤더 줄을 종료하는 `CRLF`는 쿠키의 일부가 아니라 헤더의 일부로서 검사됩니다.

HTTP Raw Cookie

원시 HTTP 클라이언트 요청 헤더에서 식별된 쿠키에서, 그리고 HTTP Inspect 프리프로세서 **Inspect HTTP Responses** 옵션이 활성화되었을 때 응답 set-cookie 데이터에서 내용 일치를 검색하려면 이 옵션을 선택합니다. 시스템은 메시지 본문에 포함된 쿠키를 본문 내용으로 취급합니다.

일치 내용을 쿠키에서만 검색하려면 HTTP Inspect 프리프로세서 **Inspect HTTP Cookies** 옵션을 활성화해야 합니다. 그렇게 하지 않으면 규칙 엔진은 쿠키를 포함하여 전체 헤더를 검색합니다. 자세한 내용은 27-32페이지의 서버 레벨 HTTP 표준화 옵션 선택을/를 참조하십시오.

다음에 유의하십시오.

- 이 옵션은 `pcre` 키워드 HTTP raw cookie (K) 옵션과 함께 동일한 내용을 검색하는 데 사용할 수 없습니다. 자세한 내용은 Snort 전용 Post 정규식 수정자 표를 참조하십시오.
- `Cookie:` 및 `Set-Cookie:` 헤더 이름, 헤더 줄의 선행 공백, 헤더 줄을 종료하는 `CRLF`는 쿠키의 일부가 아니라 헤더의 일부로서 검사됩니다.

HTTP Client Body

HTTP 클라이언트 요청의 메시지 본문에서 내용 일치를 검색하려면 이 옵션을 선택합니다.

이 옵션이 작동하려면 HTTP Inspect 프리프로세서 **HTTP Client Body Extraction Depth** 옵션에 대해 0~65535의 값을 지정해야 합니다. 자세한 내용은 27-32페이지의 서버 레벨 HTTP 표준화 옵션 선택을/를 참조하십시오.

HTTP Status Code

HTTP 응답의 3자리 상태 코드에서 내용 일치를 검색하려면 이 옵션을 선택합니다.

이 옵션이 일치 항목을 반환하도록 하려면 HTTP Inspect 프리프로세서 **Inspect HTTP Responses** 옵션을 활성화해야 합니다. 자세한 내용은 27-32페이지의 서버 레벨 HTTP 표준화 옵션 선택을/를 참조하십시오.

HTTP Status Message

HTTP 응답의 상태 코드와 함께 표시되는 텍스트 설명에서 내용 일치를 검색하려면 이 옵션을 선택합니다.

이 옵션이 일치 항목을 반환하도록 하려면 HTTP Inspect 프리프로세서 **Inspect HTTP Responses** 옵션을 활성화해야 합니다. 자세한 내용은 27-32페이지의 서버 레벨 HTTP 표준화 옵션 선택을/를 참조하십시오.

TCP 트래픽의 내용 검색을 수행할 때 HTTP content 옵션을 지정하려면

액세스: Admin/Intrusion Admin

1단계 선택적으로, HTTP Inspect 프리프로세서 표준화를 활용하고 성능을 개선하려면 다음을 선택합니다.

- 추가하는 `content` 또는 `protected_content` 키워드에 대해 **HTTP URI**, **HTTP Raw URI**, **HTTP Method**, **HTTP Header**, **HTTP Raw Header** 또는 **HTTP Client Body** 옵션 중 하나 이상
- **HTTP Cookie** 또는 **HTTP Raw Cookie** 옵션

2단계 계속해서 규칙을 생성 또는 수정합니다. 자세한 내용은 36-17페이지의 내용 일치 제한, 36-14페이지의 내용 일치 검색, 36-103페이지의 새 규칙 작성 또는 36-104페이지의 기존 규칙 수정을/를 참조하십시오.

Fast Pattern Matcher 사용

라이센스: 보호

참고 `protected_content` 키워드를 구성하면 이러한 옵션은 지원되지 **않습니다**. 자세한 내용은 36-15페이지의 protected_content 키워드 사용을/를 참조하십시오.

Fast pattern matcher는 패킷이 규칙 엔진에 전달되기 전에 어떤 규칙을 평가할지를 빠르게 결정합니다. 이 초기 결정은 패킷 평가에 사용되는 규칙 수를 크게 줄여 성능을 개선합니다.

기본적으로 fast pattern matcher는 패킷에서 규칙에 지정된 가장 긴 내용을 검색합니다. 이렇게 하면 규칙의 불필요한 평가가 최대한 해소됩니다. 다음과 같은 규칙 프래그먼트를 가정해보겠습니다.

```
alert tcp any any -> any 80 (msg:"Exploit"; content:"GET";
http_method; nocase; content:"/exploit.cgi"; http_uri;
nocase;)
```

거의 모든 HTTP 클라이언트 요청에는 `GET` 내용이 있지만, `/exploit.cgi` 내용이 있는 경우는 별로 없습니다. `GET`을 빠른 패턴 내용으로 사용하면 검색 엔진은 이 규칙을 대부분의 경우 평가할 것이고 일치하는 결과는 거의 없을 것입니다. 그러나 대부분의 클라이언트 `GET` 요청은 `/exploit.cgi`를 사용하여 평가되지 않을 것이므로 성능이 증가할 것입니다.

규칙 엔진은 fast pattern matcher가 지정된 내용을 탐지하는 경우에만 규칙을 기준으로 패킷을 평가합니다. 예를 들어, 규칙에 있는 한 `content` 키워드가 `short` 내용을 지정하고, 두 번째 키워드가 `longer`, 세 번째가 `longest`를 지정한 경우 fast pattern matcher는 `longest` 내용을 사용하며, 규칙 엔진이 페이로드에서 `longest`를 찾은 경우에만 규칙이 평가됩니다.

Fast pattern matcher가 사용할 더 짧은 검색 패턴을 지정하려면 **Use Fast Pattern Matcher** 옵션을 사용할 수 있습니다. 사용자가 지정하는 패턴은 가장 긴 패턴보다 패킷에서 발견될 가능성이 적으며, 따라서 좀 더 구체적으로 대상 익스플로잇을 식별합니다.

Use Fast Pattern Matcher 및 동일한 `content` 키워드의 다른 옵션을 선택할 때는 다음 제한 사항에 유의하십시오.

- 규칙당 한 번만 **Use Fast Pattern Matcher**를 지정할 수 있습니다.
- **Use Fast Pattern Matcher**를 **Not**과 함께 선택하는 경우에는 **Distance**, **Within**, **Offset** 또는 **Depth**를 사용할 수 없습니다.
- 다음 HTTP 필드 옵션과 함께 Use Fast Pattern Matcher를 선택할 수 없습니다.

  HTTP Raw URI, **HTTP Raw Header**, **HTTP Raw Cookie**, **HTTP Cookie**, **HTTP Method**, **HTTP Status Message** 또는 **HTTP Status Code**

  그러나 다음의 표준화 필드 중 하나를 검색하는 데 역시 fast pattern matcher를 사용하는 `content` 키워드에는 위의 옵션을 포함할 수 있습니다.

  HTTP URI, **HTTP Header** 또는 **HTTP Client Body**

  예를 들어 **HTTP Cookie**, **HTTP Header** 및 **Use Fast Pattern Matcher**를 선택하면 규칙 엔진은 HTTP 쿠키와 HTTP 헤더에서 모두 내용을 검색하지만, fast pattern matcher는 HTTP 쿠키가 아니라 HTTP 헤더에만 적용됩니다.

  원시 HTTP 필드 옵션(**HTTP Raw URI**, **HTTP Raw Header** 또는 **HTTP Raw Cookie**)을 동일한 `content` 키워드에서 해당 표준화 옵션(각각 **HTTP URI**, **HTTP Header** 또는 **HTTP Cookie**)과 함께 사용할 수 없습니다. 자세한 내용은 36-23페이지의 HTTP Content 옵션을/를 참조하십시오.

  제한 옵션과 비제한 옵션을 결합하면 fast pattern matcher는 사용자가 지정한 비제한 필드만 검색하여, 제한된 필드에 대한 평가를 비롯한 완전한 평가를 위해 규칙 엔진으로 패킷을 전달할지 여부를 테스트합니다.
- 선택적으로, **Use Fast Pattern Matcher**를 선택하면 **Fast Pattern Matcher Only** 또는 **Fast Pattern Matcher Offset and Length**를 선택할 수 있지만 둘을 모두 선택할 수는 없습니다.
- Base64 데이터를 검사할 경우에는 fast pattern matcher를 사용할 수 없습니다. 자세한 내용은 36-101페이지의 Base64 데이터 디코딩 및 검사을/를 참조하십시오.

Fast Pattern Matcher만 사용

Fast Pattern Matcher Only 옵션을 선택하면 `content` 키워드를 fast pattern matcher 옵션이 아니라 규칙 옵션으로만 사용할 수 있습니다. 지정된 내용을 규칙 엔진으로 평가할 필요가 없을 때 리소스를 절약하려면 이 옵션을 사용할 수 있습니다. 페이로드 어디에든 `12345` 내용이 있으면 된다고 하는 규칙이 있다고 가정해보겠습니다. Fast pattern matcher가 패턴을 탐지하면 규칙의 추가 키워드에 대해 패킷이 평가될 수 있습니다. 규칙 엔진은 패킷에 `12345` 패턴이 포함되어 있는지를 판단하기 위해 패킷을 다시 평가할 필요가 없습니다.

규칙에 지정된 내용에 대해 다른 조건이 포함된 경우 이 옵션을 사용하지 않을 수 있습니다. 예를 들어, `abcd`가 `1234` 앞에 나타나는지를 다른 규칙 조건이 확인하는 경우 `1234` 내용을 검색하기 위해 이 옵션을 사용하지 않을 수 있습니다. 이 경우 규칙 엔진은 상대적인 위치를 파악할 수 없습니다. **Fast Pattern Matcher Only**를 지정하면 규칙 엔진은 지정된 내용을 검색하지 않기 때문입니다.

이 옵션을 사용할 때는 다음 조건에 유의하십시오.

- 지정된 내용은 위치에 의존하지 않습니다. 즉, 페이로드의 어디에 나타나도 됩니다. 따라서 위치 옵션(**Distance**, **Within**, **Offset**, **Depth** 또는 **Fast Pattern Matcher Offset and Length**)을 사용할 수 없습니다.
- 이 옵션은 **Not**과 함께 사용할 수 없습니다.
- 이 옵션은 **Fast Pattern Matcher Offset and Length**와 함께 사용할 수 없습니다.

- 모든 패턴이 fast pattern matcher에 대/소문자 구분 없이 입력되므로 지정된 내용에서는 대/소문자가 구분되지 않습니다. 이는 자동으로 처리되므로 이 옵션을 선택할 때 **Case Insensitive**를 선택할 필요가 없습니다.
- **Fast Pattern Matcher Only** 옵션을 사용하는 `content` 키워드 바로 뒤에는 현재 검색 위치를 기준으로 검색 위치를 설정하는 다음 키워드를 사용할 수 없습니다.
- `isdataat`
- `pcre`
- `content` - **Distance** 또는 **Within** 선택 시
- `content` - **HTTP URI** 선택 시
- `asn1`
- `byte_jump`
- `byte_test`
- `byte_extract`
- `base64_decode`

Fast Pattern Matcher Offset and Length 지정

Fast Pattern Matcher Offset and Length 옵션을 사용하면 검색할 내용의 부분을 지정할 수 있습니다. 이 옵션은 패턴이 매우 길거나 패턴의 일부만으로 규칙의 일치 여부를 충분히 식별할 수 있는 경우 메모리 사용을 줄일 수 있습니다. Fast pattern matcher로 규칙을 선택하면 규칙에 대해 전체 패턴이 평가됩니다.

검색을 어디에서 시작할지(offset), 어디까지 계속해야 할지(length)를 바이트 단위로 지정하여 fast pattern matcher에 사용할 부분을 결정할 수 있습니다. 다음 구문을 사용합니다.

```
offset,length
```

예를 들어 다음 내용의 경우

```
1234567
```

offset과 length 바이트 숫자를 다음으로 지정하면

```
1,5
```

Fast pattern matcher는 `23456` 내용만 검색합니다.

이 옵션은 **Fast Pattern Matcher Only**와 함께 사용할 수 없습니다.

Fast pattern matcher로 검색할 내용을 지정하려면

액세스: Admin/Intrusion Admin

1단계 추가하는 `content` 키워드에 대해 **Use Fast Pattern Matcher**를 선택합니다.

2단계 선택적으로, 지정된 패턴이 패킷에 존재하는지를 규칙 엔진 평가 없이 판단하려면 **Fast Pattern Matcher Only**를 선택합니다.

Fast pattern matcher가 지정된 내용을 탐지하는 경우에만 평가가 진행됩니다.

3단계 선택적으로, 내용을 검색할 패턴의 일부를 **Fast Pattern Matcher Offset and Length**에서 지정합니다. 다음 구문을 사용합니다.

```
offset,length
```

여기서 *offset*은 내용의 처음을 기준으로 몇 바이트 떨어진 곳에서 검색을 시작할지를 지정하고 *length*는 몇 바이트까지 계속할지를 지정합니다.

4단계 계속해서 규칙을 생성 또는 수정합니다. 자세한 내용은 36-17페이지의 내용 일치 제한, 36-35페이지의 PCRE를 사용하여 내용 검색, 36-103페이지의 새 규칙 작성 또는 36-104페이지의 기존 규칙 수정을/를 참조하십시오.

인라인 구축에서 내용 교체

라이센스: 보호

지정된 내용을 교체하려면 인라인 구축에서 `replace` 키워드를 사용할 수 있습니다.

참고 Cisco SSL Appliance에 의해 탐지된 SSL 트래픽의 내용을 교체하는 데에는 `replace` 키워드를 사용할 수 **없습니다**. 교체 데이터가 아니라 원래 암호화된 데이터가 전송됩니다. 자세한 내용은 *Cisco SSL Appliance Administration and Deployment Guide*를 참조하십시오.

`replace` 키워드를 사용하려면 특정 문자열을 찾는 데 `content` 키워드를 사용하는 사용자 지정 표준 텍스트 규칙을 작성합니다. 그런 다음 `replace` 키워드를 사용하여 content를 교체할 문자열을 지정합니다. replace 값과 content 값은 길이가 같아야 합니다.

참고 `protected_content` 키워드의 해시된 내용을 교체하는 데에는 `replace` 키워드를 사용할 수 **없습니다**. 자세한 내용은 36-15페이지의 protected_content 키워드 사용을/를 참조하십시오.

선택적으로, 이전 FireSIGHT 시스템 소프트웨어 버전과의 호환을 위해 교체 문자열을 따옴표로 감쌀 수 있습니다. 따옴표를 포함하지 않으면 규칙이 올바른 구문이 되도록 자동으로 규칙에 따옴표가 추가됩니다. 교체 텍스트의 일부로서 앞이나 뒤에 따옴표를 포함하려면 다음 예에 보이는 것처럼 백슬래시를 사용하여 이스케이프해야 합니다.

```
"replacement text plus \"quotation\" marks""
```

규칙에는 여러 `replace` 키워드를 포함할 수 있지만 `content` 키워드당 하나만 가능합니다. 규칙에서 찾는 첫 번째 content 인스턴스만 교체됩니다.

다음은 `replace` 키워드의 사용 예에 대한 설명입니다.

- 시스템에서 익스플로잇이 포함된 수신 패킷을 탐지하면, 악의적인 문자열을 무해한 문자열로 교체할 수 있습니다. 때로는 이 방법이 위반 패킷을 단순히 삭제하는 것보다 더 성공적입니다. 일부 공격 시나리오에서 공격자는 네트워크 방어선을 우회하거나 네트워크를 플러딩할 때까지 삭제된 패킷을 단순히 재전송합니다. 패킷을 삭제하는 것이 아니라 한 문자열을 다른 문자열로 교체하면, 취약하지 않은 대상에 대해 공격이 시작된 것으로 공격자가 믿게 만들 수 있습니다.
- 예를 들어 웹 서버의 취약한 버전을 실행 중인지 알아보려고 시도하는 정찰 공격이 우려되는 경우, 발신 패킷을 탐지하고 배너를 자신의 고유한 텍스트로 교체할 수 있습니다.

참고 교체 규칙을 사용하고자 하는 인라인 침입 정책에서 규칙 상태를 Generate Events로 설정해야 합니다. 규칙을 Drop and Generate 이벤트로 설정하면 패킷이 삭제될 수 있으며, 이 경우 내용을 교체하지 못하게 됩니다.

문자열 교체 프로세스의 일부로서 시스템은 목적지 호스트가 오류 없이 패킷을 수신할 수 있도록 패킷 체크섬을 자동으로 업데이트합니다.

`replace` 키워드는 HTTP 요청 메시지 `content` 키워드 옵션과 함께 사용할 수 없습니다. 자세한 내용은 36-14페이지의 내용 일치 검색 및 36-23페이지의 HTTP Content 옵션을/를 참조하십시오.

인라인 구축에서 내용을 교체하려면

액세스: Admin/Intrusion Admin

1단계 Create Rule 페이지의 드롭다운 목록에서 **content**를 선택하고 **Add Option**을 클릭합니다.

`content` 키워드가 나타납니다.

2단계 탐지하려는 내용을 **content** 필드에 입력하고 선택적으로 해당 인수를 선택합니다. HTTP 요청 메시지 `content` 키워드 옵션은 `replace` 키워드와 함께 사용할 수 없습니다.

3단계 드롭다운 목록에서 **replace**를 선택하고 **Add Option**을 클릭합니다.

`replace` 키워드가 `content` 키워드 아래에 나타납니다.

4단계 지정한 내용에 대한 교체 문자열을 **replace:** 필드에 입력합니다.

Byte_Jump and Byte_Test 사용

라이센스: 보호

`byte_jump` 및 `byte_test` 키워드를 사용하면 규칙 엔진이 패킷에서 데이터 일치에 대한 테스트를 시작해야 하는 곳을 계산하고 바이트를 평가하는 방법에 대해 설명할 수 있습니다.

또한 `byte_jump` 및 `byte_test` **DCE/RPC** 인수를 사용하여 DCE/RPC 프리프로세서에 의해 처리되는 트래픽에 대해 두 키워드 중 하나를 맞춤화할 수 있습니다. **DCE/RPC** 인수를 사용하면 `byte_jump` 및 `byte_test`를 다른 특정 DCE/RPC 키워드와 함께 사용할 수도 있습니다. 자세한 내용은 27-2페이지의 DCE/RPC 트래픽 디코딩 및 36-60페이지의 DCE/RPC 키워드을/를 참조하십시오.

자세한 내용은 다음 절을 참조하십시오.

- 36-30페이지의 byte_jump
- 36-33페이지의 byte_test

byte_jump

라이센스: 보호

`byte_jump` 키워드는 지정된 바이트 세그먼트에 정의된 바이트 수를 계산한 다음, 지정한 옵션에 따라 지정된 바이트 세그먼트의 끝에서부터 또는 패킷 페이로드의 처음부터 패킷 내에서 해당 바이트 수만큼 건너뜁니다. 특정 바이트 세그먼트가 패킷 내 변수 데이터에 포함된 바이트 수를 설명하는 패킷에서는 이 기능이 유용합니다.

다음 표에서는 `byte_jump` 키워드에 필요한 인수에 대해 설명합니다.

표 36-8 필수 byte_jump 인수

인수	설명
Bytes	패킷에서 계산할 바이트 수.
Offset	처리를 시작하기 위한 페이로드에 대한 바이트 수. `offset` 카운터는 0바이트부터 시작되므로, `offset` 값을 계산할 때는 패킷 페이로드의 처음부터 또는 마지막으로 성공한 내용 일치로부터 앞으로 이동하려는 바이트 수에서 1을 빼야 합니다. 이 인수에 대한 값을 지정하는 데 기존의 `byte_extract` 변수를 사용할 수도 있습니다. 자세한 내용은 36-83페이지의 키워드 인수로 패킷 데이터 읽어오기을/를 참조하십시오.

다음 표에서는 필수 인수에 대해 지정한 값을 시스템이 해석하는 방법을 정의하기 위해 사용할 수 있는 옵션에 대해 설명합니다.

표 36-9 선택적인 추가 byte_jump 인수

인수	설명
Relative	마지막으로 성공한 내용 일치에서 발견된 마지막 패턴을 기준으로 offset을 설정합니다.
Align	변환된 바이트의 수를 다음 32비트 경계로 반올림합니다.
Multiplier	규칙 엔진이 최종 `byte_jump` 값을 얻기 위해 패킷에서 얻은 `byte_jump` 값에 곱해야 하는 값을 나타냅니다. 이 경우 규칙 엔진은 지정된 바이트 세그먼트에 정의된 바이트 수를 건너뛰는 대신, Multiplier 인수로 지정한 정수를 곱한 바이트 수를 건너뜁니다.
Post Jump Offset	다른 `byte_jump` 인수를 적용한 후 앞이나 뒤로 건너뛸 -63535~63535 범위의 바이트 수. 양의 값은 앞으로 건너뛰고 음의 값은 뒤로 건너뜁니다. 비활성화하려면 필드를 비워두거나 `0`을 입력합니다. **DCE/RPC** 인수를 선택할 경우 적용할 수 없는 `byte_jump` 인수에 대해서는 Endianness 인수 표의 **DCE/RPC** 인수을/를 참조하십시오.
From Beginning	규칙 엔진이, 건너뛸 바이트 수를 지정하는 바이트 세그먼트의 끝부터가 아니라 패킷 페이로드의 처음부터 시작하여 페이로드에서 지정된 바이트 수를 건너뛰어야 함을 나타냅니다.

DCE/RPC, **Endian** 또는 **Number Type** 중 하나만 지정할 수 있습니다.

`byte_jump` 키워드가 바이트를 계산하는 방법을 정의하려면 다음 표에 설명된 인수 중에서 선택할 수 있습니다(지정된 인수가 없으면 네트워크 바이트 순서가 사용됨).

표 36-10 Endianness 인수

인수	설명
Big Endian	Big Endian 바이트 순서로 데이터를 처리합니다. 이것이 기본 네트워크 바이트 순서입니다.
Little Endian	Little Endian 바이트 순서로 데이터를 처리합니다.
DCE/RPC	DCE/RPC 프리프로세서에 의해 처리되는 트래픽에 대해 `byte_jump` 키워드를 지정합니다. 자세한 내용은 27-2페이지의 DCE/RPC 트래픽 디코딩을/를 참조하십시오. DCE/RPC 프리프로세서는 big endian 또는 little endian 바이트 순서를 결정하며, **Number Type**, **Endian** 및 **From Beginning** 인수는 적용되지 않습니다. 이 인수를 활성화하면 `byte_jump`를 다른 특정 DCE/RPC 키워드와 함께 사용할 수도 있습니다. 자세한 내용은 36-60페이지의 DCE/RPC 키워드을/를 참조하십시오.

다음 표에 있는 인수 중 하나를 사용하여 시스템이 패킷의 데이터를 보는 방법을 정의합니다.

표 36-11 숫자 유형 인수

인수	설명
Hexadecimal String	변환된 문자열 데이터를 16진수 형식으로 나타냅니다.
Decimal String	변환된 문자열 데이터를 10진수 형식으로 나타냅니다.
Octal String	변환된 문자열 데이터를 8진수 형식으로 나타냅니다.

예를 들어 byte_jump에 대해 설정한 값이 다음과 같으면

- Bytes = 4
- Offset = 12
- Relative enabled
- Align enabled

규칙 엔진은 마지막으로 성공한 내용 일치에서 13바이트 뒤에 나타나는 4바이트에 설명된 숫자를 계산하고, 패킷에서 해당 바이트 수만큼 앞으로 건너뜁니다. 예를 들어 특정 패킷에서 계산된 4바이트가 00 00 00 1F이면 규칙 엔진은 이를 31로 변환합니다. 엔진에 다음 32비트 경계로 이동하도록 지시하는 align이 지정되었으므로 규칙 엔진은 패킷에서 32바이트 앞으로 건너뜁니다.

또는 byte_jump에 대해 설정한 값이 다음과 같으면

- Bytes = 4
- Offset = 12
- From Beginning enabled
- Multiplier = 2

규칙 엔진은 패킷의 시작에서 13바이트 뒤에 나타나는 4바이트에 설명된 숫자를 계산합니다. 그런 다음 그 숫자에 2를 곱하여 건너뛸 총 바이트 수를 얻습니다. 예를 들어 특정 패킷에서 계산된 4바이트가 00 00 00 1F이면 규칙 엔진은 이를 31로 변환한 다음 2를 곱해 62를 얻습니다. From Beginning이 활성화되었으므로 규칙 엔진은 패킷의 처음 63바이트를 건너뜁니다.

byte_jump를 사용하려면

액세스: Admin/Intrusion Admin

1단계 드롭다운 목록에서 byte_jump를 선택하고 **Add Option**을 클릭합니다.

마지막으로 선택한 키워드 아래에 byte_jump 섹션이 나타납니다.

byte_test

라이센스: 보호

byte_test 키워드는 지정된 바이트 세그먼트에서 바이트 수를 계산하고, 지정한 연산자 및 값에 따라 이들을 비교합니다.

다음 표에서는 byte_test 키워드에 필요한 인수에 대해 설명합니다.

표 36-12 필수 byte_test 인수

인수	설명
Bytes	패킷에서 계산할 바이트 수. 1~10바이트를 지정할 수 있습니다.
Operator and Value	지정한 값을 <, >, =, !, &, ^, !>, !<, !=, !& 또는 !^과 비교합니다. 예를 들어 !1024를 지정하면 byte_test는 지정된 숫자를 변환하고, 이 숫자가 1024와 같지 않으면 이벤트를 생성합니다(다른 모든 키워드 매개 변수가 일치하는 경우). !와 !=는 동일합니다. 이 인수에 대한 값을 지정하는 데 기존의 byte_extract 변수를 사용할 수도 있습니다. 자세한 내용은 36-83페이지의 키워드 인수로 패킷 데이터 읽어오기을/를 참조하십시오.
Offset	처리를 시작하기 위한 페이로드에 대한 바이트 수. offset 카운터는 0바이트부터 시작되므로, offset 값을 계산할 때는 패킷 페이로드의 처음부터 또는 마지막으로 성공한 내용 일치로부터 앞으로 이동하려는 바이트 수에서 1을 빼야 합니다. 이 인수에 대한 값을 지정하는 데 기존의 byte_extract 변수를 사용할 수도 있습니다. 자세한 내용은 36-83페이지의 키워드 인수로 패킷 데이터 읽어오기을/를 참조하십시오.

시스템에서 다음 표에 설명된 인수와 함께 byte_test 인수를 사용하는 방법을 더 정의할 수 있습니다.

표 36-13 선택적인 추가 byte_test 인수

인수	설명
Relative	마지막으로 성공한 패턴 일치를 기준으로 offset을 설정합니다.
Align	변환된 바이트의 수를 다음 32비트 경계로 반올림합니다.

DCE/RPC, **Endian** 또는 **Number Type** 중 하나만 지정할 수 있습니다.

byte_test 키워드가 테스트할 바이트를 계산하는 방법을 정의하려면 다음 표의 인수 중에서 선택하십시오. 지정된 인수가 없으면 네트워크 바이트 순서가 사용됩니다.

표 36-14 Endianness byte_test 인수

인수	설명
Big Endian	Big Endian 바이트 순서로 데이터를 처리합니다. 이것이 기본 네트워크 바이트 순서입니다.

표 36-14 Endianness byte_test 인수(계속)

인수	설명
Little Endian	Little Endian 바이트 순서로 데이터를 처리합니다.
DCE/RPC	DCE/RPC 프리프로세서에 의해 처리되는 트래픽에 대해 `byte_test` 키워드를 지정합니다. 자세한 내용은 27-2페이지의 DCE/RPC 트래픽 디코딩을/를 참조하십시오. DCE/RPC 프리프로세서는 big endian 또는 little endian 바이트 순서를 결정하며, **Number Type** 및 **Endian** 인수는 적용되지 않습니다. 이 인수를 활성화하면 `byte_test`를 다른 특정 DCE/RPC 키워드와 함께 사용할 수도 있습니다. 자세한 내용은 36-60페이지의 DCE/RPC 키워드을/를 참조하십시오.

다음 표에 있는 인수 중 하나를 사용하여 시스템이 패킷의 문자열 데이터를 보는 방법을 정의할 수 있습니다.

표 36-15 Number Type byte-test 인수

인수	설명
Hexadecimal String	변환된 문자열 데이터를 16진수 형식으로 나타냅니다.
Decimal String	변환된 문자열 데이터를 10진수 형식으로 나타냅니다.
Octal String	변환된 문자열 데이터를 8진수 형식으로 나타냅니다.

예를 들어, `byte_test`의 값이 다음과 같이 지정된 경우

- Bytes = 4
- Operator and Value > 128
- Offset = 8
- Relative enabled

규칙 엔진은 마지막으로 성공한 내용 일치에서 9바이트 떨어진 곳에 나타나는 4바이트에 설명된 숫자를 계산하고, 계산된 숫자가 128바이트보다 크면 규칙을 트리거합니다.

byte_test를 사용하려면

액세스: Admin/Intrusion Admin

1단계 Create Rule 페이지의 드롭다운 목록에서 `byte_test`를 선택하고 **Add Option**을 클릭합니다.

마지막으로 선택한 키워드 아래에 `byte_test` 섹션이 나타납니다.

PCRE를 사용하여 내용 검색

라이센스: 보호

pcre 키워드를 사용하면 PCRE(Perl-compatible regular expressions)를 사용하여 패킷 페이로드에서 지정된 내용을 검사할 수 있습니다. 동일한 내용에서 약간 변경된 내용을 매칭하기 위해 여러 규칙을 작성하지 않으려면 PCRE를 사용할 수 있습니다.

정규식은 다양한 방식으로 표시되는 내용을 검색할 때 유용합니다. 내용에는 패킷 페이로드 내에서 위치를 찾으려는 시도에 대해 설명하려는 특성과 다른 특성이 있을 수 있습니다.

침입 규칙에 사용되는 정규식 구문은 전체 정규식 라이브러리의 하위 집합이며, 전체 라이브러리의 명령에 사용되는 구문과는 다소 다릅니다. 규칙 편집기를 사용하여 pcre 키워드를 추가할 때에는 다음 형식으로 전체 값을 입력합니다.

```
!/pcre/ ismxAEGRBUIPHDMCKSY
```

여기서 각 항목은 다음을 나타냅니다.

- ! - 옵션 부정(정규식과 일치하지 **않는** 패턴을 매칭하려는 경우 사용)
- /*pcre*/ - PCRE(Perl-compatible regular expression)
- ismxAEGRBUIPHDMCKSY - 수정자 옵션의 조합

또한 패킷 페이로드에서 특정 내용을 검색하기 위해 다음 표에 나열된 문자를 PCRE에서 사용할 때 규칙 엔진이 올바르게 해석하도록 하려면 해당 문자를 이스케이프해야 합니다.

표 36-16 이스케이프된 PCRE 문자

이스케이프 대상	백슬래시와	16진수 코드와
#(해시 마크)	\#	\x23
;(세미콜론)	\;	\x3B
|(세로 막대)	\\|	\x7C
:(콜론)	\:	\x3A

팁 선택적으로 PCRE를 따옴표로 감쌀 수 있습니다(예: *pcre_expression* 또는 "*pcre_expression*"). 이 옵션은 따옴표가 선택이 아니라 필수였던 이전 버전에 익숙한 기존 사용자를 위해 남겨둔 것입니다. 규칙 편집기는 규칙을 저장한 후 표시할 때 따옴표를 표시하지 않습니다.

또한 m?regex?를 사용할 수 있는데, 여기서 ?는 / 이외의 구분 기호입니다. 정규식 내에서 슬래시를 매칭해야 하지만 백슬래시를 사용하여 이스케이프하고 싶지 않은 경우 이 기호를 사용할 수 있습니다. 예를 들어 m?*regex*? ismxAEGRBUIPHDMCKSY를 사용하려는 경우, *regex*는 PCRE이고 ismxAEGRBUIPHDMCKSY는 수정자 옵션의 조합입니다. 정규식 구문에 대한 자세한 내용은 36-36페이지의 PCRE 기본 사항을/를 참조하십시오.

다음 절에서는 pcre 키워드에 대한 유효한 값을 작성하는 방법에 대해 설명합니다.

- 36-36페이지의 PCRE 기본 사항 - PCRE에서 사용되는 일반 구문에 대해 설명합니다.
- 36-37페이지의 PCRE 수정자 옵션 - 정규식을 수정하기 위해 사용할 수 있는 옵션에 대해 설명합니다.
- 36-40페이지의 예제 PCRE 키워드 값 - 규칙에서 pcre 키워드의 사용법 예를 제공합니다.

PCRE 기본 사항

라이센스: 보호

pcre 키워드는 표준 PCRE(Perl-compatible regular expression) 구문을 수용합니다. 다음 절에서는 이러한 구문에 대해 설명합니다.

팁 다음 절에서는 PCRE에 대해 사용할 수 있는 기본 구문에 대해 설명하지만, 고급 정보를 알아보려면 Perl 및 PCRE 전용 온라인 참고 자료나 책을 찾아볼 수 있습니다.

메타 문자

라이센스: 보호

메타 문자는 정규식 내에서 특별한 의미를 갖는 리터럴 문자입니다. 정규식 내에서 메타 문자를 사용할 경우 앞에 백슬래시를 입력하여 "이스케이프"해야 합니다.

다음 표에서는 PCRE와 함께 사용할 수 있는 메타 문자 및 각각에 대한 예를 제공합니다.

표 36-17 PCRE 메타 문자

메타 문자	설명	예
.	새 줄 이외의 문자와 일치합니다. 수정 옵션으로 s가 사용되면 새 줄 문자도 포함할 수 있습니다.	abc. - abcd, abc1, abc# 등과 일치합니다.
*	0번 이상의 문자 또는 식과 일치합니다.	abc* - abc, abcc, abccc, abcccccc 등과 일치합니다.
	0번 또는 1번의 문자 또는 식과 일치합니다.	abc? - abc와 일치합니다.
+	1번 이상의 문자 또는 식과 일치합니다.	abc+ - abc, abcc, abccc, abcccccc 등과 일치합니다.
()	식을 그룹화합니다.	(abc)+ - abc, abcabc, abcabcabc 등과 일치합니다.
{}	문자 또는 식에 대한 일치 수의 제한을 지정합니다. 상한 및 하한을 설정하려면 쉼표로 구분합니다.	a{4,6} - aaaa, aaaaa 또는 aaaaaa와 일치합니다. (ab){2} - abab와 일치합니다.
[]	문자 클래스를 정의할 수 있으며, 집합에 설명된 대로 문자 또는 문자 조합과 일치합니다.	[abc123] - a 또는 b 또는 c 등과 일치합니다.
^	문자열의 시작 부분에서 내용과 일치합니다. 문자 클래스 내에서 사용하는 경우 부정에도 사용할 수 있습니다.	^in - info의 "in"과는 일치하지만 bin의 "in"과는 일치하지 않습니다. [^a] - a가 포함되지 않은 모든 것과 일치합니다.
$	문자열의 끝 부분에서 내용과 일치합니다.	ce$ - announce의 "ce"와는 일치하지만 cent의 "ce"와는 일치하지 않습니다.
|	OR 식을 나타냅니다.	(MAILTO|HELP) - MAILTO 또는 HELP와 일치합니다.
\	메타 문자를 실제 문자로서 사용할 수 있으며, 사전 정의된 문자 클래스를 지정하는 데에도 사용됩니다.	\. - 마침표와 일치, * - 별표와 일치, \\ - 백슬래시와 일치 등. \d - 숫자 문자와 일치, \w - 영숫자 문자와 일치 등. PCRE에서 문자 클래스를 사용하는 방법에 대한 자세한 내용은 36-37페이지의 문자 클래스을/를 참조하십시오.

문자 클래스

라이센스: 보호

문자 클래스에는 알파벳 문자, 숫자 문자, 영숫자 문자 및 공백 문자가 포함됩니다. 대괄호 내에 고유한 문자 클래스를 생성하는 동안(36-36페이지의 메타 문자 참조), 서로 다른 문자 유형에 대한 바로 가기로서 사전 정의된 클래스를 사용할 수 있습니다. 추가 한정자 없이 사용할 경우 문자 클래스는 단일 숫자 또는 문자와 일치합니다.

다음 표에서는 PCRE에서 허용되는 사전 정의된 문자 클래스의 예를 설명하고 제공합니다.

표 36-18 PCRE 문자 클래스

문자 클래스	설명	문자 클래스 정의
\d	숫자 문자("digit")와 일치합니다.	[0-9]
\D	숫자 문자 외의 문자와 일치합니다.	[^0-9]
\w	영숫자 문자("word")와 일치합니다.	[a-zA-Z0-9_]
\W	영숫자 문자 외의 문자와 일치합니다.	[^a-zA-Z0-9_]
\s	공백, 캐리지 리턴, 탭, 새 줄, 폼피드 등의 공백 문자와 일치합니다.	[\r\t\n\f]
\S	공백 문자 외의 문자와 일치합니다.	[^ \r\t\n\f]

PCRE 수정자 옵션

라이센스: 보호

`pcre` 키워드 값에서 정규식 구문을 지정한 후 수정 옵션을 사용할 수 있습니다. 이러한 수정자는 Perl, PCRE 및 Snort 관련 처리 기능을 수행합니다. 수정자는 항상 PCRE 값의 끝에 다음 형식으로 나타납니다.

`/pcre/ismxAEGRBUIPHDMCKSY`

여기서 `ismxAEGRBUPHMC`는 다음 표에 나타나는 수정 옵션 중 하나를 포함할 수 있습니다.

팁 선택적으로, 정규식 및 수정 옵션을 따옴표로 감쌀 수 있습니다(예: `"/pcre/ismxAEGRBUIPHDMCKSY"`). 이 옵션은 따옴표가 선택이 아니라 필수였던 이전 버전에 익숙한 기존 사용자를 위해 남겨둔 것입니다. 규칙 편집기는 규칙을 저장한 후 표시할 때 따옴표를 표시하지 않습니다.

다음 표에서는 Perl 처리 기능을 수행하기 위해 사용할 수 있는 옵션에 대해 설명합니다.

표 36-19 Perl 관련 Post 정규식 옵션

옵션	설명
i	정규식에서 대/소문자를 구분하지 않도록 합니다.
s	점 문자(.)는 새 줄 또는 `\n` 문자 외의 모든 문자를 설정합니다. 이를 재정의하고 점 문자가 새 줄 문자를 비롯한 모든 문자와 일치하도록 하려면 `"s"`를 옵션으로 사용할 수 있습니다.
m	기본적으로 문자열은 단일 문자 줄로 취급되며 ^ 및 $ 는 특정 문자열의 시작 및 끝과 일치합니다. `"m"`을 옵션으로 사용하면 ^ 및 $는 버퍼의 새 줄 문자 바로 앞 또는 뒤에 오는 내용은 물론 버퍼의 시작 또는 끝에 있는 내용과도 일치합니다.
x	패턴 내에 나타날 수 있는 공백 데이터 문자를 무시합니다. 단, 이스케이프되거나(앞에 백슬래시 사용) 문자 클래스 내에 포함된 경우는 제외입니다.

다음 표에서는 정규식 뒤에 사용할 수 있는 PCRE 수정자에 대해 설명합니다.

표 36-20 PCRE 관련 Post 정규식 옵션

옵션	설명
A	패턴은 문자열의 시작 부분에서 매칭합니다(정규식에서 ^을 사용하는 것과 동일).
E	주제 문자열의 끝에서만 매칭하려면 $를 설정합니다. (E가 없으면 $는 새 줄일 경우 마지막 문자 바로 앞에서 매칭하지만, 다른 새 줄 문자 앞에서는 매칭하지 않습니다).
G	기본적으로 * + 및 ?는 "greedy"입니다. 즉, 둘 이상의 일치가 발견되면 더 긴 것을 선택합니다. 이를 변경하여, 물음표 문자(?)가 뒤따르지 않는 한 이러한 문자가 항상 첫 번째 일치를 선택하도록 하려면 G 문자를 사용합니다. 예를 들어 *? +? 및 ??는 G 수정자를 사용하는 구성에서 greedy이고, 추가 물음표가 없는 *, + 또는 ?의 경우는 greedy가 아닙니다.

다음 표에서는 정규식 뒤에 사용할 수 있는 Snort 전용 수정자에 대해 설명합니다.

표 36-21 Snort 전용 Post 정규식 수정자

옵션	설명
R	규칙 엔진에 의해 발견되는 마지막 일치의 끝을 기준으로 일치 내용을 검색합니다.
B	프리프로세서에 의해 디코딩되기 전에 데이터 내에서 내용을 검색합니다(이 옵션은 content 또는 protected_content 키워드와 함께 Raw Data 인수를 사용하는 것과 유사합니다).
U	HTTP Inspect 프리프로세서로 디코딩된 표준화 HTTP 요청 메시지의 URI 내에서 내용을 검색합니다. 이 옵션은 content 또는 protected_content 키워드 **HTTP URI** 옵션과 함께 동일한 내용을 검색하는 데 사용할 수 없습니다. 자세한 내용은 36-23페이지의 HTTP Content 옵션을/를 참조하십시오. **참고** 파이프라인된 HTTP 요청 패킷에는 여러 URI가 포함되어 있습니다. U 옵션이 포함된 PCRE 식을 사용하면 규칙 엔진은 파이프라인된 HTTP 요청 패킷의 첫 번째 URI에서만 내용 일치를 검색합니다. 패킷의 모든 URI를 검색하려면 U 옵션을 사용하는 동반 PCRE 식의 유무와 상관없이 content 또는 protected_content 키워드와 함께 **HTTP URI**를 선택하십시오.
I	HTTP Inspect 프리프로세서로 디코딩된 원시 HTTP 요청 메시지의 URI 내에서 내용을 검색합니다. 이 옵션은 content 또는 protected_content 키워드 **HTTP Raw URI** 옵션과 함께 동일한 내용을 검색하는 데 사용할 수 없습니다. 자세한 내용은 36-23페이지의 HTTP Content 옵션을/를 참조하십시오.
P	HTTP Inspect 프리프로세서에 의해 디코딩된 표준화 HTTP 요청 메시지의 본문 내에서 내용을 검색합니다. 자세한 내용은 36-23페이지의 HTTP Content 옵션에서 content 및 protected_content 키워드 **HTTP Client Body** 옵션을/를 참조하십시오.
H	HTTP Inspect 프리프로세서로 디코딩된 HTTP 요청 또는 응답 메시지의 헤더(쿠키 포함) 내에서 내용을 검색합니다. 이 옵션은 content 또는 protected_content 키워드 **HTTP Header** 옵션과 함께 동일한 내용을 검색하는 데 사용할 수 없습니다. 자세한 내용은 36-23페이지의 HTTP Content 옵션을/를 참조하십시오.
D	HTTP Inspect 프리프로세서로 디코딩된 원시 HTTP 요청 또는 응답 메시지의 헤더(쿠키 포함) 내에서 내용을 검색합니다. 이 옵션은 content 또는 protected_content 키워드 **HTTP Raw Header** 옵션과 함께 동일한 내용을 검색하는 데 사용할 수 없습니다. 자세한 내용은 36-23페이지의 HTTP Content 옵션을/를 참조하십시오.

표 36-21 Snort 전용 Post 정규식 수정자(계속)

옵션	설명
M	HTTP Inspect 프리프로세서로 디코딩된 표준화 HTTP 요청 메시지의 메서드 필드 내에서 내용을 검색합니다. 메서드 필드는 GET, PUT, CONNECT 등의 작업을 식별하며 URI에서 식별된 리소스를 이용합니다. 자세한 내용은 36-23페이지의 HTTP Content 옵션에서 `content` 및 `protected_content` 키워드 **HTTP Method** 옵션을/를 참조하십시오.
C	HTTP Inspect 프리프로세서 **Inspect HTTP Cookies** 옵션이 활성화될 때 HTTP 요청 헤더의 쿠키 내에서, 그리고 프리프로세서 **Inspect HTTP Responses** 옵션이 활성화될 때 HTTP 응답 헤더의 set-cookie 내에서 표준화된 내용을 검색합니다. **Inspect HTTP Cookies**가 활성화되지 않으면 쿠키 또는 set-cookie 데이터를 비롯한 전체 헤더를 검색합니다. 다음에 유의하십시오. • 메시지 본문에 포함된 쿠키는 본문 내용으로 취급됩니다. • 이 옵션은 `content` 또는 `protected_content` 키워드 **HTTP Cookie** 옵션과 함께 동일한 내용을 검색하는 데 사용할 수 없습니다. 자세한 내용은 36-23페이지의 HTTP Content 옵션을/를 참조하십시오. • `Cookie:` 및 `Set-Cookie:` 헤더 이름, 헤더 줄의 선행 공백, 헤더 줄을 종료하는 `CRLF`는 쿠키의 일부가 아니라 헤더의 일부로서 검사됩니다.
K	HTTP Inspect 프리프로세서 **Inspect HTTP Cookies** 옵션이 활성화될 때 HTTP 요청 헤더의 쿠키 내에서, 그리고 프리프로세서 **Inspect HTTP Responses** 옵션이 활성화될 때 HTTP 응답 헤더의 set-cookie 내에서 원시 내용을 검색합니다. **Inspect HTTP Cookies**가 활성화되지 않으면 쿠키 또는 set-cookie 데이터를 비롯한 전체 헤더를 검색합니다. 다음에 유의하십시오. • 메시지 본문에 포함된 쿠키는 본문 내용으로 취급됩니다. • 이 옵션은 `content` 또는 `protected_content` 키워드 **HTTP Raw Cookie** 옵션과 함께 동일한 내용을 검색하는 데 사용할 수 없습니다. 자세한 내용은 36-23페이지의 HTTP Content 옵션을/를 참조하십시오. • `Cookie:` 및 `Set-Cookie:` 헤더 이름, 헤더 줄의 선행 공백, 헤더 줄을 종료하는 `CRLF`는 쿠키의 일부가 아니라 헤더의 일부로서 검사됩니다.
S	HTTP 응답에서 3자리 상태 코드를 검색합니다. 자세한 내용은 36-23페이지의 HTTP Content 옵션에서 `content` 및 `protected_content` 키워드 **HTTP Status Code** 옵션을/를 참조하십시오.
Y	HTTP 응답의 상태 코드와 함께 제공되는 텍스트 설명을 검색합니다. 자세한 내용은 36-23페이지의 HTTP Content 옵션에서 `content` 및 `protected_content` 키워드 **HTTP Status Message** 옵션을/를 참조하십시오.

참고 U 옵션은 R 옵션과 함께 사용하지 마십시오. 성능 문제가 발생할 수 있습니다. 또한 U 옵션을 다른 HTTP 내용 옵션(I, P, H, D, M, C, K, S 또는 Y)과 함께 사용하지 마십시오.

예제 PCRE 키워드 값

라이센스: 보호

다음 예제에서는 pcre에 대해 입력할 수 있는 값을 각 예제에서 매칭할 내용에 대한 설명과 함께 보여줍니다.

- **/feedback[(\d{0,1})]?\.cgi/U**

  이 예제는 패킷 페이로드에서 feedback, 그 뒤에 0개 또는 1개의 숫자 문자, 그리고 그 뒤에 .cgi를 URI 데이터에서만 검색합니다.

  다음 예는 일치합니다.

- feedback.cgi
- feedback1.cgi
- feedback2.cgi
- feedback3.cgi

  다음 예는 일치하지 **않습니다**.

- feedbacka.cgi
- feedback11.cgi
- feedback21.cgi
- feedbackzb.cgi
- **/^ez(\w{3,5})\.cgi/iU**

  이 예제는 패킷 페이로드에서 문자열의 처음에 나오는 ez, 그 뒤에 3~5개의 문자로 구성된 단어, 그리고 그 뒤에 .cgi를 검색합니다. 검색에서 대/소문자는 구분되지 않으며 URI 데이터만 검색됩니다.

  다음 예는 일치합니다.

- EZBoard.cgi
- ezman.cgi
- ezadmin.cgi
- EZAdmin.cgi

  다음 예는 일치하지 **않습니다**.

- ezez.cgi
- fez.cgi
- abcezboard.cgi
- ezboardman.cgi
- **/mail(file|seek)\.cgi/U**

  이 예제는 패킷 페이로드에서 mail, 그 뒤에 file 또는 seek를 URI 데이터에서 검색합니다.

  다음 예는 일치합니다.

- mailfile.cgi
- mailseek.cgi

  다음 예는 일치하지 **않습니다**.

- MailFile.cgi
- mailfilefile.cgi
- **m?http\\x3a\x2f\x2f.*(\n|\t)+?U**

  이 예제는 패킷 페이로드에서 URI 내용 중 임의의 문자 수 뒤에 나오는 HTTP 요청 중 탭 또는 새 줄 문자를 검색합니다. 이 예제는 m?*regex*?를 사용하여 식에서 http\:\/\/의 사용을 피합니다. 콜론 앞에 백슬래시가 오는 것에 유의하십시오.

다음 예는 일치합니다.

- `http://www.example.com?scriptvar=x&othervar=\n\..\..`
- `http://www.example.com?scriptvar=\t`

다음 예는 일치하지 **않습니다**.

- `ftp://ftp.example.com?scriptvar=&othervar=\n\..\..`
- `http://www.example.com?scriptvar=|/bin/sh -i|`
- **`m?http\\x3a\x2f\x2f.*=\|.*\|+?sU`**

  이 예제는 패킷 페이로드에서 임의의 문자 수의 URL(새 줄 포함), 그 뒤에 등호, 그리고 임의의 문자 수 또는 공백을 포함한 파이프 문자를 검색합니다. 이 예제는 `m?`*`regex`*`?`를 사용하여 식에서 `http\:\/\/`의 사용을 피합니다.

  다음 예는 일치합니다.

- `http://www.example.com?value=|/bin/sh/ -i|`
- `http://www.example.com?input=|cat /etc/passwd|`

  다음 예는 일치하지 **않습니다**.

- `ftp://ftp.example.com?value=|/bin/sh/ -i|`
- `http://www.example.com?value=x&input?|cat /etc/passwd|`
- **`/[0-9a-f]{2}\:[0-9a-f]{2}\:[0-9a-f]{2}\:[0-9a-f]{2}\:[0-9a-f]{2}\:[0-9a-f]{2}/i`**

  이 예제는 패킷 페이로드에서 MAC 주소를 검색합니다. 여기서는 콜론 문자를 백슬래시로 이스케이프합니다.

규칙에 메타데이터 추가

라이센스: 보호

`metadata` 키워드를 사용하여 규칙에 설명 정보를 추가할 수 있습니다. 추가한 정보를 사용하여 요구에 맞게 규칙을 구성 또는 식별할 수 있으며, 규칙을 검색할 수도 있습니다.

시스템은 다음 형식을 기반으로 메타데이터를 검증합니다.

```
key value
```

여기서 *key* 및 *value*는 공백으로 구분된 설명 조합을 제공합니다. 이것은 Cisco에서 제공하는 규칙에 메타데이터를 추가하기 위해 Cisco VRT에서 사용하는 형식입니다.

또는 다음 형식을 사용할 수도 있습니다.

```
key=value
```

예를 들어, *key value* 형식에서 다음과 같이 카테고리 및 하위 카테고리를 사용하여 작성자와 날짜별로 규칙을 식별할 수 있습니다.

```
author SnortGuru_20050406
```

하나의 규칙에 여러 `metadata` 키워드를 사용할 수 있습니다. 또한 다음 예에서와 같이 단일 `metadata` 키워드에서 여러 *key value* 문을 쉼표로 구분하여 사용할 수 있습니다.

```
author SnortGuru_20050406, revised_by SnortUser1_20050707,
revised_by SnortUser2_20061003, revised_by
SnortUser1_20070123
```

key value 또는 *key=value* 형식만 사용하도록 제한되지 않습니다. 그러나 이러한 형식 기반의 검증에서 오는 제한 사항에 대해 알고 있어야 합니다.

제한되는 문자 피하기

라이센스: 보호

다음과 같은 문자 제한 사항에 유의하십시오.

- 세미콜론(;) 또는 콜론(:)을 `metadata` 키워드에 사용하지 마십시오.
- 쉼표를 사용할 때에는 시스템이 *`key value`* 또는 *`key=value`* 문에서 쉼표를 구분 기호로 해석한다는 점에 유의해야 합니다. 예를 들면 다음과 같습니다.

```
key value, key value, key value
```

- 등호(=) 문자 또는 공백 문자를 사용할 때에는 시스템이 이러한 문자를 *`key`* 및 *`value`* 값 사이의 구분 기호로 해석한다는 점에 유의해야 합니다. 예를 들면 다음과 같습니다.

```
key value
key=value
```

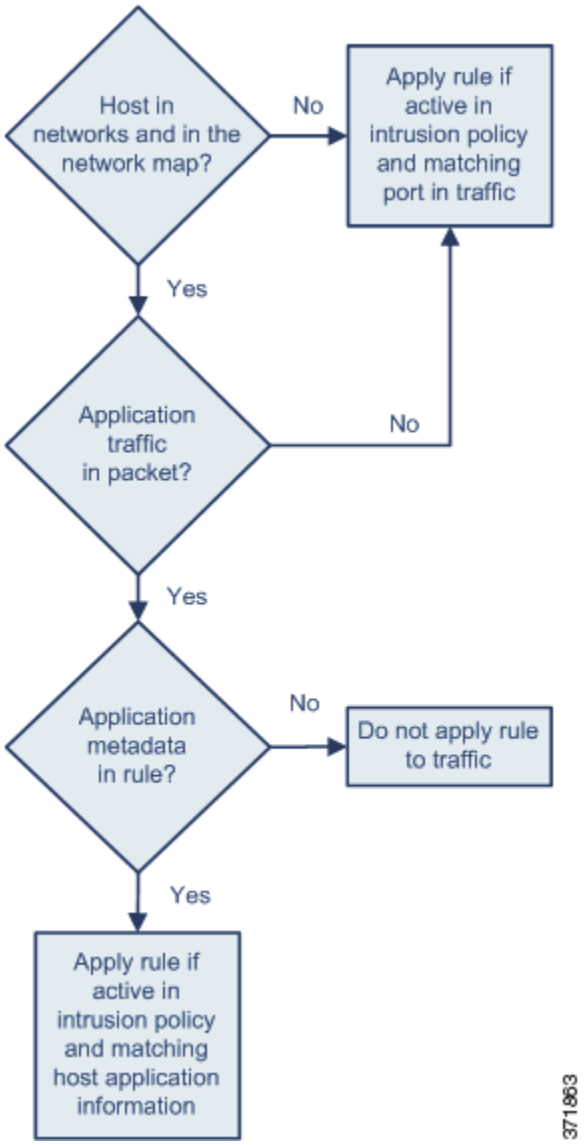
다른 모든 문자는 허용됩니다.

service 메타데이터 추가

라이센스: 보호

규칙 엔진은 트래픽을 분석하고 처리하는 데 패킷에서 호스트에 대한 애플리케이션 프로토콜 정보와 일치하는 `service` 메타데이터가 포함된 활성 규칙을 적용합니다. 일치하지 않으면 시스템은 트래픽에 규칙을 적용하지 않습니다. 호스트에 애플리케이션 프로토콜 정보가 없거나 규칙에 `service` 메타데이터가 없으면, 시스템은 트래픽에 규칙을 적용할지를 결정하기 위해 규칙의 포트를 기준으로 트래픽의 포트를 점검합니다.

다음 다이어그램은 애플리케이션 정보를 기반으로 규칙을 트래픽에 매칭하는 방법을 보여줍니다.



식별된 애플리케이션 프로토콜이 있는 규칙을 매칭하려면 `metadata` 키워드와 *`key value`* 문을 정의해야 하며 *`key`*에는 `service`를 사용하고 *`value`*에는 애플리케이션을 사용해야 합니다. 예를 들어 `metadata` 키워드의 다음 *`key value`* 문은 규칙을 HTTP 트래픽과 연결합니다.

```
service http
```

다음 표에서는 가장 일반적인 애플리케이션 값에 대해 설명합니다.

참고 아래의 표에 없는 애플리케이션을 정의하는 데 도움이 필요하면 지원 팀에 문의하십시오.

표 36-22 service 값

가치	설명
`dcerpc`	분산된 컴퓨팅 환경/원격 절차 호출 시스템
`dns`	도메인 이름 시스템

표 36-22 service 값(계속)

가치	설명
finger	Finger 사용자 정보 프로토콜
ftp	파일 전송 프로토콜
ftp-data	File Transfer Protocol(데이터 채널)
HTTP	하이퍼텍스트 전송 프로토콜
IMAP	인터넷 메시지 액세스 프로토콜
isakmp	Internet Security Association and Key Management Protocol
netbios-dgm	NETBIOS Datagram Service
netbios-ns	NETBIOS Name Service
NetBIOS ssn	NETBIOS Session Service
nntp	Network News Transfer Protocol
oracle	Oracle Net Services
pop2	Post Office Protocol, 버전 2
POP3	Post Office Protocol, 버전 3
SMTP	간단한 메일 전송 프로토콜 (SMTP)
SSH	Secure Shell 네트워크 프로토콜
telnet	Telnet 네트워크 프로토콜
tftp	Trivial File Transfer Protocol
x11	X Window System

예약된 메타데이터 피하기

라이센스: 보호

다음 단어는 VRT에서 사용하도록 예약되어 있으므로 `metadata` 키워드에서 단일 인수로서 또는 *`key value`* 문의 키로서 사용하지 마십시오.

```
application
engine
impact_flag
OS
policy
rule-type
rule-flushing
soid
```

참고 예상대로 작동하지 않을 수 있는 로컬 규칙에 제한된 메타데이터를 추가하는 데 도움이 필요하면 지원 팀에 문의하십시오. 자세한 내용은 66-20페이지의 로컬 규칙 파일 가져오기을/를 참조하십시오.

메타데이터로 규칙 검색

라이센스: 보호

`metadata` 키워드를 사용하는 규칙을 검색하려면 규칙 Search 페이지에서 `metadata` 키워드를 선택하고, 선택적으로 메타데이터의 일부를 입력합니다. 예를 들어 다음을 입력할 수 있습니다.

- `author` - *key*에 `author`를 사용한 모든 규칙 표시
- `author snortguru` - *key*에 `author`를 사용하고 *value*에 `SnortGuru`를 사용한 모든 규칙 표시
- `author s` - *key*에 `author`를 사용하고 *value*에 `SnortGuru` 또는 `SnortUser1` 또는 `SnortUser2` 등의 용어를 사용한 모든 규칙 표시

팁

*key*와 *value*를 모두 검색하는 경우 규칙의 *key value* 문에서 사용된 것과 동일한 연결 연산자(등호 [=] 또는 공백 문자)를 검색에 사용하십시오. *key* 뒤에 등호(=) 문자를 사용하는지 공백 문자를 사용하는지에 따라 검색에서 다른 결과가 반환됩니다.

메타데이터를 추가하는 데 사용하는 형식과 상관없이, 시스템은 메타데이터 검색 용어를 *key value* 또는 *key=value* 문의 전체 또는 일부로 해석합니다. 예를 들어 다음은 *key value* 또는 *key=value* 형식을 따르지 않는 유효한 메타데이터일 수 있습니다.

```
ab cd ef gh
```

그러나 시스템은 예제의 각 공백을 key와 value 사이의 구분 기호로 해석합니다. 따라서 병렬 용어 및 단일 용어에 대해 다음 검색 중 하나를 사용하여 예제 메타데이터를 포함하는 규칙을 성공적으로 찾을 수 있습니다.

```
cd ef
ef gh
ef
```

그러나 다음 검색을 사용하면 규칙을 찾을 수 없습니다. 시스템이 이를 단일 *key value* 문으로 해석하기 때문입니다.

```
ab ef
```

자세한 내용은 36-107페이지의 규칙 검색을/를 참조하십시오.

영향 레벨 1 설정

라이센스: 보호

`metadata` 키워드에서 다음의 예약된 *key value* 문을 사용할 수 있습니다.

```
impact_flag red
```

key value 문은 가져온 로컬 규칙 또는 규칙 편집기를 사용하여 생성한 사용자 지정 규칙에 대해 영향 플래그를 red(레벨 1)로 설정합니다.

Cisco에서 제공하는 규칙에 `impact_flag red` 문이 포함된다면 이는 규칙을 트리거한 패킷이 소스 또는 목적지 호스트가 바이러스, 트로이 목마 또는 기타 악성 소프트웨어에 의해 손상되었을 가능성이 있음을 나타내는 것이라고 VRT에서 판단한 것입니다. 자세한 내용은 41-38페이지의 이벤트를 평가하기 위한 영향 레벨 사용을/를 참조하십시오.

IP 헤더 값 검사

라이센스: 보호

패킷의 IP 헤더에서 공격 또는 보안 정책 위반 가능성을 식별하기 위한 키워드를 사용할 수 있습니다. 자세한 내용은 다음 절을 참조하십시오.

프래그먼트 및 예약된 비트 검사

라이센스: 보호

`fragbits` 키워드는 IP 헤더에서 프래그먼트 및 예약된 비트를 검사합니다. 각 패킷에서 Reserved Bit, More Fragments 비트 및 Don't Fragment 비트를 임의의 조합으로 확인할 수 있습니다.

표 36-23 Fragbits 인수 값

인수	설명
R	Reserved bit
M	More Fragments bit
D	Don’t Fragment bit

`fragbits` 키워드를 사용하여 규칙을 더 자세히 수정하려면 다음 표에서 설명하는 연산자를 규칙의 인수 값 뒤에 지정할 수 있습니다.

표 36-24 Fragbit 연산자

운영자	설명
더하기 기호(+)	패킷이 지정된 모든 비트에 대해 매칭해야 합니다.
별표(*)	패킷이 지정된 비트의 일부에 대해서만 매칭할 수 있습니다.
느낌표(!)	지정된 비트 중 아무것도 설정되어 있지 않으면 패킷이 기준을 충족합니다.

예를 들어 Reserved Bit이 설정된(다른 비트도 설정될 수 있음) 패킷에 대해 이벤트를 생성하려면 `fragbits` 값으로 `R+`를 사용합니다.

IP 헤더 식별 값 검사

라이센스: 보호

id 키워드는 키워드 인수에서 지정하는 값을 기준으로 IP 헤더 프래그먼트 식별 필드를 테스트합니다. 일부 서비스 거부 툴 및 스캐너는 이 필드를 탐지하기 쉬운 특정 번호로 설정합니다. 예를 들어 Synscan 포트스캔을 탐지하는 SID 630에서 id 값은 39426으로 설정됩니다. 이 값은 스캐너에서 전송한 패킷에서 ID 번호로 사용되는 고정 값입니다.

참고 id 인수 값은 숫자여야 합니다.

지정된 IP 옵션 식별

라이센스: 보호

IPopts 키워드를 사용하면 지정된 IP 헤더 옵션에 대한 패킷을 검색할 수 있습니다. 다음 표에는 사용 가능한 인수 값이 나열되어 있습니다.

표 36-25 IPoption 인수

인수	설명
rr	record route(레코드 경로)
eol	end of list(파일의 끝)
nop	no operation(작업 없음)
ts	time stamp(타임스탬프)
초	IP security option(IP 보안 옵션)
lsrr	loose source routing(느슨한 소스 라우팅)
ssrr	strict source routing(엄격한 소스 라우팅)
satid	stream identifier(스트림 식별자)

분석가들은 엄격한 소스 라우팅과 느슨한 소스 라우팅을 가장 자주 감시합니다. 이 두 옵션은 스푸핑된 소스 IP 주소를 나타낼 수 있기 때문입니다.

지정된 IP 프로토콜 번호 식별

라이센스: 보호

ip_proto 키워드를 사용하면 키워드의 값으로 지정된 IP 프로토콜로 패킷을 식별할 수 있습니다. IP 프로토콜은 0~255의 숫자로 지정할 수 있습니다. 전체 프로토콜 번호 목록은 http://www.iana.org/assignments/protocol-numbers에서 확인할 수 있습니다. 이러한 번호를 <, >, ! 등의 연산자와 함께 사용할 수 있습니다. 예를 들어, ICMP가 아닌 프로토콜로 트래픽을 검사하려면 ip_proto 키워드에 대한 값으로 !1을 사용합니다. 단일 규칙에서 ip_proto 키워드를 여러 번 사용할 수도 있습니다. 그러나 규칙 엔진은 키워드의 여러 인스턴스를 부울 AND 관계로 해석합니다. 예를 들어 ip_proto:!3; ip_proto:!6이 포함된 규칙을 생성하면 규칙은 GGP 프로토콜 AND TCP 프로토콜을 사용하는 트래픽을 무시합니다.

패킷의 Type of Service 검사

라이센스: 보호

일부 네트워크는 네트워크를 이동하는 패킷의 우선순위를 설정하기 위해 ToS(type of service) 값을 사용합니다. `tos` 키워드를 사용하면 키워드의 인수로 지정한 값을 기준으로 패킷의 IP 헤더 ToS 값을 테스트할 수 있습니다. `tos` 키워드를 사용하는 규칙은 ToS가 지정된 값으로 설정되어 있으며 규칙에 지정된 나머지 기준을 충족하는 패킷에서 트리거됩니다.

참고 `tos` 인수 값은 숫자여야 합니다.

ToS 필드는 IP 헤더 프로토콜에서 사용되지 않게 되었으며 Differentiated Services Code Point (DSCP) 필드로 교체되었습니다.

패킷의 Time-To-Live 값 검사

라이센스: 보호

패킷의 ttl(time-to-live) 값은 삭제되기 전에 만들 수 있는 홉의 수를 나타냅니다. `ttl` 키워드를 사용하면 키워드의 인수로 지정한 값 또는 값의 범위를 기준으로 패킷의 IP 헤더 ttl 값을 테스트할 수 있습니다. 낮은 ttl 값은 때때로 traceroute 또는 침입 회피 시도를 나타내므로 `ttl` 키워드 매개 변수를 0 또는 1과 같은 낮은 값으로 설정하는 것이 도움이 될 수 있습니다. (이 키워드의 적절한 값은 관리되는 디바이스 위치 및 네트워크 토폴로지에 따라 달라집니다.) 구문은 다음과 같이 사용할 수 있습니다.

- TTL 값으로 특정 값을 설정하려면 0~255의 정수를 사용합니다. 값 앞에 등호(=)를 사용할 수도 있습니다(예를 들어 `5` 또는 `=5`를 지정할 수 있습니다).
- TTL 값의 범위를 지정하려면 하이픈(-)을 사용합니다(예를 들어 `0-2`는 0에서 2까지의 모든 값, `-5`는 0에서 5까지의 모든 값, `5-`는 5에서 255까지의 모든 값을 지정합니다).
- 특정 값보다 큰 TTL 값을 지정하려면 보다 큼(>) 기호를 사용합니다(예를 들어 `>3`은 3보다 큰 모든 값을 지정합니다).
- 특정 값보다 크거나 같은 TTL 값을 지정하려면 보다 큼 및 같음(>=) 기호를 사용합니다(예를 들어 `>=3`은 3보다 크거나 같은 모든 값을 지정합니다).
- 특정 값보다 작은 TTL 값을 지정하려면 보다 작음(>) 기호를 사용합니다(예를 들어 `<3`은 3보다 작은 모든 값을 지정합니다).
- 특정 값보다 작거나 같은 TTL 값을 지정하려면 보다 작음 및 같음(<=) 기호를 사용합니다(예를 들어 `<=3`은 3보다 작거나 같은 모든 값을 지정합니다).

ICMP 헤더 값 검사

라이센스: 보호

FireSIGHT 시스템은 ICMP 패킷의 헤더에서 공격 및 보안 정책 위반을 식별하기 위해 사용할 수 있는 키워드를 지원합니다. 그러나 대부분의 ICMP 유형 및 코드를 탐지하는 사전 정의된 규칙이 존재합니다. 기존 규칙을 활성화하거나 기존 규칙을 기반으로 로컬 규칙을 생성하는 방법을 고려해 보십시오. 처음부터 ICMP 규칙을 작성하는 것보다 요구에 맞는 규칙을 더 빠르게 찾을 수 있을 것입니다.

ICMP 전용 키워드에 대한 자세한 내용은 다음 절을 참조하십시오.

- 36-49페이지의 고정 ICMP ID 및 시퀀스 값 식별
- 36-49페이지의 ICMP 메시지 유형 검사
- 36-50페이지의 ICMP 메시지 코드 검사

고정 ICMP ID 및 시퀀스 값 식별

라이센스: 보호

ICMP 식별 및 시퀀스 번호는 ICMP 응답을 ICMP 요청과 연결하는 데 도움이 됩니다. 일반 트래픽에서 이러한 값은 패킷에 동적으로 할당됩니다. 일부 숨김 채널 및 DDoS(Distributed Denial of Server) 프로그램은 고정 ICMP ID 및 시퀀스 값을 사용합니다. 다음 키워드를 사용하면 고정 값으로 ICMP 패킷을 식별할 수 있습니다.

icmp_id

`icmp_id` 키워드는 ICMP 에코 요청 또는 응답 패킷의 ICMP ID 번호를 검사합니다. `icmp_id` 키워드에 대한 인수로 ICMP ID 번호에 해당하는 숫자 값을 사용합니다.

icmp_seq

`icmp_seq` 키워드는 ICMP 에코 요청 또는 응답 패킷의 ICMP 시퀀스를 검사합니다. `icmp_seq` 키워드에 대한 인수로 ICMP 시퀀스 번호에 해당하는 숫자 값을 사용합니다.

ICMP 메시지 유형 검사

라이센스: 보호

특정 ICMP 메시지 유형 값이 있는 패킷을 찾으려면 `itype` 키워드를 사용합니다. 서로 다른 트래픽 유형을 테스트하려면 유효한 ICMP 유형 값(ICMP 유형 번호의 전체 목록은 http://www.iana.org/assignments/icmp-parameters 또는 http://www.faqs.org/rfcs/rfc792.html 참조) 또는 유효하지 않은 ICMP 유형 값을 지정할 수 있습니다. 예를 들어 공격자는 서비스 거부 및 플러딩 공격을 일으키기 위해 ICMP 유형 값을 범위 밖으로 설정할 수 있습니다.

보다 작음(<) 및 보다 큼(>)을 사용하여 `itype` 인수의 범위를 지정할 수 있습니다.

예를 들면 다음과 같습니다.

- <35
- >36
- 3<>55

팁 ICMP 유형 번호의 전체 목록은 http://www.iana.org/assignments/icmp-parameters 또는 http://www.faqs.org/rfcs/rfc792.html을/를 참조하십시오.

ICMP 메시지 코드 검사

라이센스: 보호

ICMP 메시지에는 때때로 목적지에 도달할 수 없을 때 세부사항을 제공하는 코드 값이 포함됩니다. (사용 가능한 메시지 유형과 상호 관련된 ICMP 메시지 코드의 전체 목록은 http://www.iana.org/assignments/icmp-parameters의 두 번째 절을 참조하십시오.)

특정 ICMP 코드 값으로 패킷을 식별하려면 `icode` 키워드를 사용할 수 있습니다. 서로 다른 트래픽 유형을 테스트하려면 유효한 ICMP 코드 값 또는 유효하지 않은 ICMP 코드 값을 지정하도록 선택할 수 있습니다.

보다 작음(<) 및 보다 큼(>)을 사용하여 `icode` 인수의 범위를 지정할 수 있습니다.

예를 들면 다음과 같습니다.

- 35보다 작은 값을 찾으려면 `<35`를 지정합니다.
- 36보다 큰 값을 찾으려면 `<36`을 지정합니다.
- 3과 55 사이의 값을 찾으려면 `3<>55`를 지정합니다.

팁 `icode` 및 `itype` 키워드를 함께 사용하여 둘 모두와 일치하는 트래픽을 식별할 수 있습니다. 예를 들어 ICMP Destination Unreachable 코드 유형과 ICMP Port Unreachable 코드 유형을 포함하는 ICMP 트래픽을 식별하려면 `itype` 키워드와 값 3(Destination Unreachable에 대해) 및 `icode` 키워드와 값 3(Port Unreachable에 대해)을 지정합니다.

TCP 헤더 값 및 스트림 크기 검사

라이센스: 보호

FireSIGHT 시스템은 패킷의 TCP 헤더 및 TCP 스트림 크기를 사용하려고 시도하는 공격을 식별하도록 설계된 키워드를 지원합니다. TCP 전용 키워드에 대한 자세한 내용은 다음 절을 참조하십시오.

- 36-50페이지의 TCP 승인 값 검사
- 36-51페이지의 TCP 플래그 조합 검사
- 36-52페이지의 TCP나 UDP 클라이언트 또는 서버 플로우에 규칙 적용
- 36-53페이지의 고정 TCP 시퀀스 번호 식별
- 36-53페이지의 지정된 크기의 TCP 창 식별
- 36-53페이지의 지정된 크기의 TCP 스트림 식별

TCP 승인 값 검사

라이센스: 보호

패킷의 TCP 승인 번호를 기준으로 값을 비교하려면 `ack` 키워드를 사용할 수 있습니다. 패킷의 TCP 승인 번호가 `ack` 키워드에 대해 지정된 값과 일치하면 규칙이 트리거됩니다.

`ack` 인수 값은 숫자여야 합니다.

TCP 플래그 조합 검사

라이센스: 보호

검사된 패킷에서 설정할 때 규칙을 트리거하는 TCP 플래그의 조합을 지정하려면 `flags` 키워드를 사용할 수 있습니다.

참고 전에 `flags`에 대해 `A+`를 사용하던 상황에서는 `flow` 키워드와 `established` 값을 대신 사용해야 합니다. 모든 플래그 조합이 탐지되도록 하기 위해 플래그를 사용할 때에는 일반적으로 `flow` 키워드와 `stateless` 값을 사용해야 합니다. `flow` 키워드에 대한 자세한 내용은 36-52페이지의 TCP나 UDP 클라이언트 또는 서버 플로우에 규칙 적용을/를 참조하십시오.

`flag` 키워드에 대해 다음 표에 설명한 값을 확인하거나 무시할 수 있습니다.

표 36-26 flag 인수

인수	TCP 플래그
Ack	데이터를 승인합니다.
Psh	이 패킷의 데이터는 전송해야 합니다.
Syn	새 연결.
Urg	패킷에 긴급 데이터가 포함되어 있습니다.
Fin	닫힌 연결.
Rst	취소된 연결.
CWR	ECN 혼잡 창이 축소되었습니다. 전에는 이것이 R1 인수였으며, 여전히 이전 버전과의 호환성이 지원됩니다.
ECE	ECN 에코. 전에는 이것이 R2 인수였으며, 여전히 이전 버전과의 호환성이 지원됩니다.

팁 ECN(Explicit Congestion Notification)에 대한 자세한 내용은 http://www.faqs.org/rfcs/rfc3168.html에서 제공하는 정보를 참조하십시오.

`flags` 키워드를 사용할 때에는 여러 플래그를 기준으로 시스템이 매칭을 수행하는 방법을 나타내기 위해 연산자를 사용할 수 있습니다. 다음 표에서는 이러한 연산자에 대해 설명합니다.

표 36-27 flags와 함께 사용하는 연산자

운영자	설명	예
all	패킷이 지정된 모든 플래그를 포함해야 합니다.	패킷이 Urgent 플래그는 반드시 포함해야 하며 다른 플래그는 포함할 수도 있다고 지정하려면 `Urg` 및 `all`을 선택합니다.
any	패킷이 지정된 플래그를 포함할 수 있습니다.	규칙을 트리거하려면 `Ack` 및 `Psh` 플래그 중 하나 또는 둘 모두를 설정해야 하며 패킷에서 다른 플래그를 설정할 수도 있다고 지정하려면 `Ack`, `Psh` 및 `any`를 선택합니다.
not	패킷은 지정된 플래그 설정을 포함해서는 **안** 됩니다.	이 규칙을 트리거하는 패킷에 대해 Urgent 플래그가 설정되지 **않도록** 지정하려면 `Urg` 및 `not`을 선택합니다.

TCP나 UDP 클라이언트 또는 서버 플로우에 규칙 적용

라이센스: 보호

세션 특성을 기반으로 규칙에서 검사할 패킷을 선택하려면 `flow` 키워드를 사용할 수 있습니다. `flow` 키워드를 사용하면 규칙이 적용되는 트래픽 플로우의 방향(규칙을 클라이언트 플로우에 적용할지 서버 플로우에 적용할지)을 지정할 수 있습니다. `flow` 키워드가 패킷을 검사하는 방법을 지정하려면 분석할 트래픽의 방향, 검사할 패킷의 상태, 패킷이 재작성된 스트림의 일부인지 여부 등을 설정할 수 있습니다.

규칙이 처리될 때 패킷의 스테이트풀 검사가 발생합니다. TCP 규칙이 스테이트리스 트래픽을 무시하도록 하려면(설정된 세션 컨텍스트가 없는 트래픽) 규칙에 `flow` 키워드를 추가하고 키워드에 대해 **Established** 인수를 선택해야 합니다. UDP 규칙이 스테이트리스 트래픽을 무시하도록 하려면 규칙에 `flow` 키워드를 추가하고 **Established** 인수나 방향 인수 또는 둘 모두를 선택해야 합니다. 이렇게 하면 TCP 또는 UDP 규칙이 패킷의 스테이트풀 검사를 수행합니다.

방향 인수를 추가하면 규칙 엔진은 지정한 방향과 일치하는 플로우의 기존 상태가 있는 패킷만 검사합니다. 예를 들어 `established` 인수 및 `From Client` 인수의 `flow` 키워드를 TCP 또는 UDP 연결이 탐지될 때 트리거되는 규칙에 추가하면, 규칙 엔진은 클라이언트에서 전송되는 패킷만 검사합니다.

팁 성능을 최대화하려면 TCP 규칙 또는 UDP 세션 규칙에 항상 `flow` 키워드를 포함하십시오.

플로우를 지정하려면 Create Rule 페이지의 **Detection Options** 목록에서 `flow` 키워드를 선택하고 **Add Option**을 클릭합니다. 그런 다음 각 필드에 대해 제공되는 목록에서 인수를 선택합니다.

다음 표에서는 `flow` 키워드에 대해 지정할 수 있는 스트림 관련 인수에 대해 설명합니다.

표 36-28 상태 관련 flow 인수

인수	설명
Established	설정된 연결에서 트리거됩니다.
Stateless	스트림 프로세서의 상태와 상관없이 트리거됩니다.

다음 표에서는 `flow` 키워드에 대해 지정할 수 있는 방향 옵션에 대해 설명합니다.

표 36-29 flow 방향 인수

인수	설명
To Client	서버 응답에 대해 트리거됩니다.
To Server	클라이언트 응답에 대해 트리거됩니다.
From Client	클라이언트 응답에 대해 트리거됩니다.
From Server	서버 응답에 대해 트리거됩니다.

`From Server` 및 `To Client`는 동일한 기능을 수행하며, `To Server` 및 `From Client`도 마찬가지입니다. 이러한 옵션은 규칙에 컨텍스트와 가독성을 더해줍니다. 예를 들어 서버에서 클라이언트로의 공격을 탐지하도록 설계된 규칙을 생성하는 경우 `From Server`를 사용합니다. 그러나 클라이언트에서 서버로의 공격을 탐지하도록 설계된 규칙을 생성하는 경우 `From Client`를 사용합니다.

다음 표에서는 flow 키워드에 대해 지정할 수 있는 스트림 관련 인수에 대해 설명합니다.

표 36-30 스트림 관련 flow 인수

인수	설명
Ignore Stream Traffic	재작성된 스트림 패킷에 대해 트리거되지 않습니다.
Only Stream Traffic	재작성된 스트림 패킷에 대해서만 트리거됩니다.

예를 들어, 스트림 프리프로세서에 의해 리어셈블된, 설정된 세션에서 클라이언트에서 서버로 이동하는 트래픽을 탐지하려면 flow 키워드에 대해 To Server, Established, Only Stream Traffic을 사용할 수 있습니다.

고정 TCP 시퀀스 번호 식별

라이센스: 보호

seq 키워드를 사용하면 고정 시퀀스 번호 값을 지정할 수 있습니다. 시퀀스 번호가 지정된 인수와 일치하는 패킷은 키워드가 포함된 규칙을 트리거합니다. 이 키워드는 거의 사용되지 않지만 고정 시퀀스 번호와 함께 생성된 패킷을 사용하는 공격 및 네트워크 스캔을 식별하는 데 도움이 됩니다.

지정된 크기의 TCP 창 식별

라이센스: 보호

관심이 있는 TCP 창 크기를 지정하려면 window 키워드를 사용할 수 있습니다. 지정된 TCP 창 크기의 패킷이 발견될 때마다 이 키워드를 포함하는 규칙이 트리거됩니다. 이 키워드는 거의 사용되지 않지만 고정 TCP 창 크기와 함께 생성된 패킷을 사용하는 공격 및 네트워크 스캔을 식별하는 데 도움이 됩니다.

지정된 크기의 TCP 스트림 식별

라이센스: 보호

스트림 프리프로세서와 함께 stream_size 키워드를 사용하면, 다음 형식으로 TCP 스트림의 크기를 바이트 단위로 확인할 수 있습니다.

direction,*operator*,*bytes*

여기서 *bytes*는 바이트의 수입니다. 인수의 각 옵션은 쉼표(,)로 구분해야 합니다.

다음 표에서는 stream_size 키워드에 대해 지정할 수 있는 방향 옵션(대/소문자 구분 없음)에 대해 설명합니다.

표 36-31 stream_size 키워드 방향 인수

인수	설명
client	지정된 스트림 크기와 일치하는 클라이언트의 스트림에서 트리거됩니다.
server	지정된 스트림 크기와 일치하는 서버의 스트림에서 트리거됩니다.

표 36-31 stream_size 키워드 방향 인수(계속)

인수	설명
both	지정된 스트림 크기와 일치하는 클라이언트의 스트림 및 서버의 스트림에서 트리거됩니다. 예를 들어 인수 `both, >, 200`은 클라이언트의 트래픽이 200바이트보다 크고(AND) 서버의 트래픽이 200바이트보다 클 때 트리거됩니다.
either	지정된 스트림 크기와 일치하는 클라이언트 또는 서버의 트래픽 중 먼저 발생하는 것에서 트리거됩니다. 예를 들어 인수 `either, >, 200`은 클라이언트의 트래픽이 200바이트보다 크거나(OR) 서버의 트래픽이 200바이트보다 클 때 트리거됩니다.

다음 표에서는 `stream_size` 키워드와 함께 사용할 수 있는 연산자에 대해 설명합니다.

표 36-32 stream_size 키워드 인수 연산자

운영자	설명
=	같음
!=	같지 않음
>	보다 큼
<	보다 작음
>=	보다 크거나 같음
<=	보다 작거나 같음

예를 들어 클라이언트에서 서버로 이동하며 5001216바이트보다 크거나 같은 TCP 스트림을 탐지하려면 `stream_size` 키워드에 대한 인수로 `client, >=, 5001216`을 사용할 수 있습니다.

TCP 스트림 리어셈블리 활성화 및 비활성화

라이센스: 보호

연결에서 검사된 트래픽이 규칙의 조건과 일치할 때 단일 연결에 대해 TCP 스트림 리어셈블리를 활성화 또는 비활성화하려면 `stream_reassemble` 키워드를 사용할 수 있습니다. 선택적으로, 하나의 규칙에서 이 키워드를 여러 번 사용할 수 있습니다.

스트림 리어셈블리를 활성화 또는 비활성화하려면 다음 구문을 사용합니다.

```
enable|disable, server|client|both, option, option
```

다음 표에서는 `stream_reassemble` 키워드와 함께 사용할 수 있는 선택적 인수에 대해 설명합니다.

표 36-33 stream_reassemble 선택적 인수

인수	설명
noalert	규칙에서 지정한 다른 탐지 옵션과 상관없이 이벤트를 생성하지 않습니다.
fastpath	일치가 있을 경우 연결 트래픽의 나머지를 무시합니다.

예를 들어 다음 규칙은 HTTP 응답에서 200 OK 상태 코드가 탐지된 연결에 대해 이벤트를 생성하지 않은 채 TCP 클라이언트 측 스트림 리어셈블리를 비활성화합니다.

```
alert tcp any 80 -> any any (flow:to_client, established; content: "200 OK";
stream_reassemble:disable, client, noalert
```

stream_reassemble을 사용하려면

액세스: Admin/Intrusion Admin

1단계 Create Rule 페이지의 드롭다운 목록에서 `stream_reassemble`을 선택하고 **Add Option**을 클릭합니다. `stream_reassemble` 섹션이 나타납니다.

세션에서 SSL 정보 추출

라이센스: 보호

SSL(Secure Sockets Layer) 프리프로세서를 호출하고 암호화된 세션의 패킷에서 SSL 버전 및 세션 상태에 대한 정보를 추출하려면 SSL 규칙 키워드를 사용할 수 있습니다.

클라이언트와 서버는 SSL 또는 TLS(Transport Layer Security)를 사용하여 암호화된 세션을 설정하기 위해 통신할 때 핸드셰이크 메시지를 교환합니다. 세션에서 전송되는 데이터는 암호화되지만 핸드셰이크 메시지는 암호화되지 않습니다.

SSL 프리프로세서는 특정 핸드셰이크 필드에서 상태 및 버전 정보를 추출합니다. 핸드셰이크 내 두 필드는 핸드셰이크의 세션 및 단계를 암호화하는 데 사용되는 SSL 또는 TLS의 버전을 나타냅니다.

자세한 내용은 다음 절을 참조하십시오.

- 36-55페이지의 ssl_state
- 36-56페이지의 ssl_version

ssl_state

라이센스: 보호

암호화된 세션에 대한 상태 정보에 대해 매칭하려면 `ssl_state` 키워드를 사용할 수 있습니다. 동시에 사용된 둘 이상의 SSL 버전을 확인하려면 하나의 규칙에 여러 `ssl_version` 키워드를 사용합니다.

규칙이 `ssl_state` 키워드를 사용하면 규칙 엔진은 트래픽에서 SSL 상태 정보를 확인할 수 있도록 SSL 프리프로세서를 호출합니다.

예를 들어, 지나치게 길고 양이 많은 데이터의 `ClientHello` 메시지를 전송하여 서버에서 버퍼 오버플로를 일으키려는 공격자의 시도를 탐지하려면 `ssl_state` 키워드와 `client_hello` 인수를 사용한 다음 비정상적으로 큰 패킷을 검토할 수 있습니다.

SSL 상태에 대한 여러 인수를 지정하려면 쉼표로 구분된 목록을 사용합니다. 여러 인수를 나열하면 시스템은 OR 연산자를 사용하여 평가합니다. 예를 들어 `client_hello` 및 `server_hello`를 인수로 지정하면 시스템은 `client_hello` 또는(OR) `server_hello`가 있는 트래픽에 대해 규칙을 평가합니다.

다음 예와 같이 인수를 부정할 수도 있습니다.

```
!client_hello, !unknown
```

연결이 상태 집합 각각에 도달하도록 보장하려면 ssl_state 규칙 옵션을 사용하는 여러 규칙을 사용해야 합니다. ssl_state 키워드는 다음 식별자를 인수로 사용합니다.

표 36-34 ssl_state *인수*

인수	목적
client_hello	메시지 유형이 ClientHello인 핸드셰이크 메시지에 대해 매칭합니다. 여기서 클라이언트는 암호화된 세션을 요청합니다.
server_hello	메시지 유형이 ServerHello인 핸드셰이크 메시지에 대해 매칭합니다. 여기서 서버는 암호화된 세션에 대한 클라이언트의 요청에 응답합니다.
client_keyx	메시지 유형이 ClientKeyExchange인 핸드셰이크 메시지에 대해 매칭합니다. 여기서 클라이언트는 서버에 키를 전송하고, 서버로부터 키 수신을 확인합니다.
server_keyx	메시지 유형이 ServerKeyExchange인 핸드셰이크 메시지에 대해 매칭합니다. 여기서 클라이언트는 서버에 키를 전송하고, 서버로부터 키 수신을 확인합니다.
unknown	핸드셰이크 메시지 유형에 대해 매칭합니다.

ssl_version

라이센스: 보호

암호화된 세션에 대한 버전 정보에 대해 매칭하려면 ssl_version 키워드를 사용할 수 있습니다. 규칙이 ssl_version 키워드를 사용하면 규칙 엔진은 트래픽에서 SSL 버전 정보를 확인할 수 있도록 SSL 프리프로세서를 호출합니다.

예를 들어 SSL 버전 2에 버퍼 오버플로 취약성이 있음을 알고 있는 경우, SSL의 해당 버전을 사용하는 트래픽을 식별하려면 ssl_version 키워드와 sslv2 인수를 사용할 수 있습니다.

SSL 버전에 대한 여러 인수를 지정하려면 쉼표로 구분된 목록을 사용합니다. 여러 인수를 나열하면 시스템은 OR 연산자를 사용하여 평가합니다. 예를 들어 SSLv2를 사용하지 않은 암호화된 트래픽을 식별하려면 규칙에 ssl_version:ssl_v3,tls1.0,tls1.1,tls1.2를 추가할 수 있습니다. 규칙은 SSL 버전 3, TLS 버전 1.0, TLS 버전 1.1 또는 TLS 버전 1.2를 사용하는 트래픽을 평가할 수 있습니다.

ssl_version 키워드는 다음 SSL/TLS 버전 식별자를 인수로 사용합니다.

표 36-35 ssl_version *인수*

인수	목적
sslv2	SSL(Secure Sockets Layer) 버전 2를 사용하여 인코딩된 트래픽에 대해 매칭합니다.
sslv3	SSL(Secure Sockets Layer) 버전 3을 사용하여 인코딩된 트래픽에 대해 매칭합니다.
tls1.0	TLS(Transport Layer Security) 버전 1.0을 사용하여 인코딩된 트래픽에 대해 매칭합니다.
tls1.1	TLS(Transport Layer Security) 버전 1.1을 사용하여 인코딩된 트래픽에 대해 매칭합니다.
tls1.2	TLS(Transport Layer Security) 버전 1.2를 사용하여 인코딩된 트래픽에 대해 매칭합니다.

애플리케이션 레이어 프로토콜 값 검사

라이센스: 보호

프리프로세서는 애플리케이션 레이어 프로토콜 값의 표준화 및 검사의 대부분을 수행하지만, 다음 섹션에 설명된 키워드를 사용하여 애플리케이션 레이어 값을 계속 검사할 수 있습니다.

- 36-57페이지의 RPC
- 36-58페이지의 ASN.1
- 36-59페이지의 urilen
- 36-60페이지의 DCE/RPC 키워드
- 36-63페이지의 SIP 키워드
- 36-65페이지의 GTP 키워드
- 36-75페이지의 Modbus 키워드
- 36-77페이지의 DNP3 키워드

RPC

라이센스: 보호

`rpc` 키워드는 TCP 또는 UDP 패킷에서 ONC RPC(Open Network Computing Remote Procedure Call) 서비스를 식별합니다. 이렇게 하면 호스트에서 RPC 프로그램을 식별하려는 시도를 탐지할 수 있습니다. 침입자는 네트워크에서 실행 중인 RPC 서비스 중에 악용 가능한 서비스가 있는지 확인하기 위해 RPC 포트매퍼를 사용할 수 있습니다. 침입자는 또한 포트매퍼를 사용하지 않은 채 RPC를 실행 중인 다른 포트에 액세스하려고 시도할 수 있습니다. 다음 표에는 `rpc` 키워드가 허용하는 인수가 나열되어 있습니다.

표 36-36 rpc 키워드 인수

인수	설명
application	RPC 애플리케이션 번호
procedure	호출된 RPC 절차
version	RPC 버전

`rpc` 키워드에 대한 인수를 지정하려면 다음 구문을 사용합니다.

`application``,`*`procedure`*`,`*`version`*

여기서 *`application`*은 RPC 애플리케이션 번호, *`procedure`*는 RPC 프로시저 번호, *`version`*은 RPC 버전 번호입니다. `rpc` 키워드에 대해서는 모든 인수를 지정해야 합니다. 인수 중 하나를 지정할 수 없으면 별표(`*`)로 교체할 수 있습니다.

예를 들어, 임의의 절차 또는 버전으로 RPC 포트매퍼(번호 100000으로 표시되는 RPC 애플리케이션)를 검색하려면 인수로 `100000,*,*`를 사용합니다.

ASN.1

라이센스: 보호

asn1 키워드를 사용하면 패킷 또는 패킷의 일부를 디코딩하여 각종 악의적인 인코딩을 찾아볼 수 있습니다.

다음 표에서는 asn1 키워드의 인수에 대해 설명합니다.

표 36-37 asn.1 키워드 인수

인수	설명
Bitstring Overflow	원격으로 악용 가능한 유효하지 않은 bitstring 인코딩을 탐지합니다.
Double Overflow	표준 버퍼보다 큰 double ASCII 인코딩을 탐지합니다. 이는 Microsoft Windows에서는 악용 가능한 함수로 알려지지만, 서비스를 악용할 수 있는 시점에는 알려지지 않습니다.
Oversize Length	제공된 인수보다 큰 ASN.1 유형 길이를 탐지합니다. 예를 들어 Oversize Length를 500으로 설정하면 500보다 큰 ASN.1 유형이 규칙을 트리거합니다.
Absolute Offset	패킷 페이로드의 처음부터 시작되는 절대 오프셋을 설정합니다. (offset 카운터는 0바이트에서 시작됩니다.) 예를 들어 SNMP 패킷을 디코딩하려면 Absolute Offset을 0으로 설정하고 Relative Offset을 설정하지 마십시오. Absolute Offset은 양수 또는 음수일 수 있습니다.
Relative Offset	마지막으로 성공한 내용 일치, pcre 또는 byte_jump에서 시작되는 상대 오프셋입니다. "foo" 내용 직후 ASN.1 시퀀스를 디코딩하려면 Relative Offset을 0으로 설정하고 Absolute Offset을 설정하지 마십시오. Relative Offset은 양수 또는 음수일 수 있습니다. (offset 카운터는 0에서 시작됩니다.)

예를 들어 버퍼 오버플로를 생성하는 Microsoft ASN.1 Library에 알려진 취약성이 있으면 공격자는 특별히 고안된 인증 패킷을 사용하여 조건을 악용할 수 있습니다. 시스템이 asn.1 데이터를 디코딩할 때 패킷의 익스플로잇 코드가 시스템 레벨 권한으로 호스트에서 실행되거나 DoS 조건을 일으킵니다. 다음 규칙에서는 asn1 키워드를 사용하여 이 취약성을 악용하려는 시도를 탐지합니다.

```
alert tcp $EXTERNAL_NET any -> $HOME_NET 445
(flow:to_server, established; content:"|FF|SMB|73|"; nocase;
offset:4; depth:5;
asn1:bitstring_overflow,double_overflow,oversize_length
100,relative_offset 54;)
```

위 규칙은 $EXTERNAL_NET 변수에 정의된 IP 주소(임의의 포트)에서 $HOME_NET 변수에 포트 445로 정의된 IP 주소로 이동하는 TCP 트래픽에 대한 이벤트를 생성합니다. 또한 서버에 대한 기존의 TCP 연결에서만 규칙이 실행됩니다. 그런 다음 특정 위치의 특정 내용에 대해 규칙이 테스트됩니다. 마지막으로 규칙은 asn1 키워드를 사용하여 bitstring 인코딩 및 double ASCII 인코딩을 탐지하고, 마지막으로 성공한 내용 일치의 끝에서 55바이트 위치부터 시작하여 100바이트 길이까지 asn.1 유형 길이를 식별합니다 (offset 카운터는 0바이트에서 시작됩니다.).

urilen

라이센스: 보호

HTTP Inspect 프리프로세서와 함께 `urilen` 키워드를 사용하면 HTTP 트래픽에서 특정 길이, 즉 최대 길이 미만, 최소 길이 초과 또는 지정된 범위 내의 URI를 검사할 수 있습니다.

HTTP Inspect 프리프로세서가 패킷을 표준화 및 검사한 후 규칙 엔진은 규칙에 대해 패킷을 평가하고 URI가 `urilen` 키워드로 지정한 길이 조건과 일치하는지를 확인합니다. 예를 들어 공격자가 DoS 조건을 만들거나 시스템 레벨 권한으로 호스트에서 코드를 실행하도록 허용하는 버퍼 오버플로를 생성하는 방법으로 URI 길이 취약성을 이용하려고 시도하는 익스플로잇을 탐지하려면 이 키워드를 사용할 수 있습니다.

규칙에서 `urilen` 키워드를 사용할 때에는 다음에 유의하십시오.

- 실무에서는 항상 `urilen` 키워드를 `flow:established` 키워드 또는 하나 이상의 다른 키워드와 함께 사용합니다.
- 규칙 프로토콜은 항상 TCP입니다. 자세한 내용은 36-4페이지의 프로토콜 지정을/를 참조하십시오.
- 목적지 포트는 항상 HTTP 포트입니다. 자세한 내용은 36-8페이지의 침입 규칙에서 포트 정의 및 3-18페이지의 사전 정의된 기본 변수 최적화을/를 참조하십시오.

바이트 단위 10진수와 보다 작음(<) 및 보다 큼(>)을 사용하여 URI 길이를 지정합니다.

예를 들면 다음과 같습니다.

- 5바이트 길이의 URI를 탐지하려면 `5`를 지정합니다.
- 5바이트 길이보다 작은 URI를 탐지하려면 `< 5`(공백 문자 하나로 구분)를 지정합니다.
- 5바이트 길이보다 큰 URI를 탐지하려면 `> 5`(공백 문자 하나로 구분)를 지정합니다.
- 3과 5바이트 사이의(포함) URI를 탐지하려면 `3 <> 5`(`<>` 전후에 공백 문자 하나씩)를 지정합니다.

예를 들어, eDirectory 버전 8.8과 함께 제공되는 Novell의 서버 모니터링 및 진단 유틸리티인 iMonitor 버전 2.4에는 알려진 취약성이 있습니다. 지나치게 긴 URI가 포함된 패킷은 버퍼 오버플로를 생성하며, 따라서 공격자는 시스템 레벨 권한으로 호스트에서 실행하거나 DoS 조건을 일으킬 수 있는 특별히 고안된 패킷으로 상황을 악용할 수 있습니다. 다음 규칙에서는 `urilen` 키워드를 사용하여 이 취약성을 악용하려는 시도를 탐지합니다.

```
alert tcp $EXTERNAL_NET any -> $HOME_NET $HTTP_PORTS
(msg:"EXPLOIT eDirectory 8.8 Long URI iMonitor buffer
overflow attempt";flow:to_server,established;
urilen:> 8192; uricontent:"/nds/"; nocase;
classtype:attempted-admin; sid:x; rev:1;)
```

위 규칙은 $EXTERNAL_NET 변수에 정의된 IP 주소(임의의 포트)에서 $HOME_NET 변수에 정의된 IP 주소($HTTP_PORTS 변수에 정의된 포트)로 이동하는 TCP 트래픽에 대한 이벤트를 생성합니다. 또한 패킷은 서버에 대한 기존의 TCP 연결에서만 규칙에 대해 평가됩니다. 규칙은 `urilen` 키워드를 사용하여 URI 길이가 8192바이트보다 큰 URI를 탐지합니다. 마지막으로, 규칙은 URI에서 대/소문자 구분 없이 특정 내용 `/nds/`를 검색합니다.

DCE/RPC 키워드

라이센스: 보호

다음 표에서 설명하는 세 개의 DCE/RPC 키워드를 사용하면 DCE/RPC 세션 트래픽에서 익스플로잇을 모니터링할 수 있습니다. 시스템은 이러한 키워드로 규칙을 처리할 때 DCE/RPC 프리프로세서를 호출합니다. 자세한 내용은 27-2페이지의 DCE/RPC 트래픽 디코딩을/를 참조하십시오.

표 36-38 DCE/RPC 키워드

사용	방법	탐지할 내용
`dce_iface`	단독으로	특정 DCE/RPC 서비스를 식별하는 패킷
`dce_opnum`	`dce_iface`가 앞에 옴	특정 DCE/RPC 서비스 작업을 식별하는 패킷
`dce_stub_data`	`dce_iface` + `dce_opnum`이 앞에 옴	특정 작업 요청 또는 응답을 정의하는 스텁 데이터

항상 `dce_opnum` 앞에 `dce_iface`를 두고 `dce_stub_data` 앞에 `dce_iface` + `dce_opnum`을 두어야 합니다.

또한 이러한 DCE/RPC 키워드를 다른 규칙 키워드와 함께 사용할 수 있습니다. DCE/RPC 규칙의 경우 `byte_jump`, `byte_test` 및 `byte_extract` 키워드를 선택한 **DCE/RPC** 인수와 함께 사용합니다. 자세한 내용은 36-30페이지의 Byte_Jump and Byte_Test 사용 및 36-83페이지의 키워드 인수로 패킷 데이터 읽어오기을/를 참조하십시오.

Cisco에서는, 규칙 엔진이 fast pattern matcher를 사용하도록 하려면 DCE/RPC 키워드가 포함된 규칙에 하나 이상의 `content` 키워드를 포함할 것을 권장합니다. 이렇게 하면 처리 속도가 빨라지고 성능이 향상됩니다. **Use Fast Pattern Matcher** 인수에서 `content` 키워드의 활성화 여부와 상관없이, 규칙에 `content` 키워드가 하나 이상 포함되어 있으면 규칙 엔진은 fast pattern matcher를 사용합니다. 자세한 내용은 36-14페이지의 내용 일치 검색 및 36-26페이지의 Fast Pattern Matcher 사용을/를 참조하십시오.

다음과 같은 경우 DCE/RPC 버전 및 인접 헤더 정보를 일치 내용으로 사용할 수 있습니다.

- 규칙에 다른 `content` 키워드가 포함되지 않음
- 규칙에 다른 `content` 키워드가 포함되어 있지만 DCE/RPC 버전 및 인접 정보가 다른 내용보다 더 고유한 패턴을 나타냄

  예를 들어 DCE/RPC 버전 및 인접 정보가 단일 바이트 내용보다 더 고유할 수 있습니다.

다음 버전 및 인접 정보 내용 일치 중 하나로 자격 규칙을 종료해야 합니다.

- 연결 지향 DCE/RPC 규칙의 경우 내용 `|05 00 00|`을 사용합니다(주 버전 05, 부 버전 00, 요청 PDU(protocol data unit) 유형 00).
- 연결 없는 DCE/RPC 규칙의 경우 `|04 00|`을 사용합니다(버전 04, 요청 PDU 유형 00).

어떤 경우든 DCE/RPC 프리프로세서에 의해 이미 완료된 처리를 반복하지 않고 fast pattern matcher를 호출하려면 버전 및 인접 정보에 대한 `content` 키워드를 규칙의 마지막 키워드로 배치하십시오. `content` 키워드를 규칙의 끝에 두는 것은 fast pattern matcher를 호출하기 위한 디바이스로 사용되는 버전 내용에 적용되며, 규칙의 다른 내용 일치에는 적용할 필요가 없습니다.

자세한 내용은 다음 절을 참조하십시오.

- 36-61페이지의 dce_iface
- 36-62페이지의 dce_opnum
- 36-62페이지의 dce_stub_data

dce_iface

라이센스: 보호

특정 DCE/RPC 서비스를 식별하려면 `dce_iface` 키워드를 사용할 수 있습니다.

선택적으로, 검사할 DCE/RPC 트래픽을 더 제한하려면 `dce_iface`를 `dce_opnum` 및 `dce_stub_data` 키워드와 함께 사용할 수 있습니다. 자세한 내용은 36-62페이지의 dce_opnum 및 36-62페이지의 dce_stub_data을/를 참조하십시오.

고정된 16바이트 UUID(Universally Unique Identifier) 식별자는 각 DCE/RPC 서비스에 할당된 애플리케이션 인터페이스를 식별합니다. 예를 들어 UUID 4b324fc8-670-01d3-1278-5a47bf6ee188은 피어 투 피어 프린터, 파일 및 SMB 명명된 파이프 등을 위한 다양한 관리 기능을 제공하는 DCE/RPC lanmanserver 서비스(srvsvc 서비스라고도 함)를 식별합니다. DCE/RPC 프리프로세서는 UUID 및 관련된 헤더 값을 사용하여 DCE/RPC 세션을 추적합니다.

인터페이스 UUID는 하이픈으로 구분된 5개의 16진수 문자열로 구성됩니다.

```
<4hexbytes>-<2hexbytes>-<2hexbytes>-<2hexbytes>-<6hexbytes>
```

인터페이스에 대한 다음 UUID에 보이는 것처럼 하이픈을 포함한 전체 UUID를 입력하여 인터페이스를 지정합니다.

```
12345678-1234-abcd-ef00-01234567cffb
```

Big endian 바이트 순서의 UUID에서 처음 세 문자열을 지정해야 합니다. 게시된 인터페이스 목록 및 프로토콜 애널라이저에서는 일반적으로 올바른 바이트 순서로 UUID를 표시하지만, 입력하기 전에 UUID 바이트 순서를 다시 정돈해야 할 수 있습니다. 다음의 메신저 서비스 UUID를 고려해보십시오. 이 UUID는 little endian 바이트 순서로 처음 세 문자열과 함께 원시 ASCII 텍스트로 표시될 수 있습니다.

```
f8 91 7b 5a 00 ff d0 11 a9 b2 00 c0 4f b6 e6 fc
```

하이픈을 삽입하고 big endian 바이트 순서로 처음 세 문자열을 입력하여 `dce_iface` 키워드에 대해 동일한 UUID를 지정할 수 있습니다.

```
5a7b91f8-ff00-11d0-a9b2-00c04fb6e6fc
```

DCE/RPC 세션은 여러 인터페이스에 대한 요청을 포함할 수 있지만 하나의 규칙에는 `dce_iface` 키워드를 하나만 포함해야 합니다. 추가 인터페이스를 탐지하려면 추가 규칙을 생성하십시오.

DCE/RPC 애플리케이션 인터페이스에는 인터페이스 버전 번호도 있습니다. 선택적으로, 버전이 지정된 값과 같은지, 같지 않은지, 작은지 또는 큰지를 나타내는 연산자와 함께 인터페이스 버전을 지정할 수 있습니다.

TCP 세그멘테이션 또는 IP 프래그먼트화 외에도 연결 지향 DCE/RPC 및 연결 없는 DCE/RPC를 모두 프래그먼트화할 수 있습니다. 일반적으로 첫 번째 외의 DCE/RPC 프래그먼트를 지정된 인터페이스와 연결하는 것은 유용하지 않습니다. 이렇게 하면 다수의 오탐이 발생할 수 있습니다. 그러나 선택적으로, 지정된 인터페이스에 대해 모든 프래그먼트를 평가할 수 있습니다.

다음 표에는 `dce_iface` 키워드 인수가 요약되어 있습니다.

표 36-39 `dce_iface` ***인수***

인수	설명
Interface UUID	DCE/RPC 트래픽에서 탐지할 특정 서비스의 애플리케이션 인터페이스를 식별하는, 하이픈을 포함한 UUID. 지정된 인터페이스와 관련된 요청은 인터페이스 UUID를 매칭하게 됩니다.
Version	선택적으로, 0~65535의 애플리케이션 인터페이스 버전 번호 및 지정된 값보다 큰 버전(>), 작은 버전(<), 같은 버전(=), 같지 않은 버전(!) 중 무엇을 탐지할지를 나타내는 연산자.

표 36-39 dce_iface 인수(계속)

인수	설명
All Fragments	선택적으로, 모든 관련 DCE/RPC 프래그먼트의 인터페이스에 대해, 그리고 지정된 경우 인터페이스 버전에 대해 매칭할 수 있습니다. 이 인수는 기본적으로 비활성화됩니다. 즉, 첫 번째 프래그먼트 또는 프래그먼트되지 않은 전체 패킷이 지정된 인터페이스와 연결된 경우에만 키워드 매칭이 수행됩니다. 이 인수를 활성화하면 오탐이 발생할 수 있습니다.

dce_opnum

라이센스: 보호

DCE/RPC 서비스가 제공하는 하나 이상의 특정 작업을 식별하는 패킷을 탐지하려면 DCE/RPC 프리프로세서와 함께 dce_opnum 키워드를 사용할 수 있습니다.

클라이언트 기능 호출은 DCE/RPC 사양에서 *operations*라고 하는 특정 서비스 기능을 요청합니다. 작업 번호(opnum)는 DCE/RPC 헤더에서 특정 작업을 식별합니다. 익스플로잇은 특정 작업을 대상으로 할 수 있습니다.

예를 들어 UUID 12345678-1234-abcd-ef00-01234567cffb는 수십 개의 서로 다른 작업을 제공하는 netlogon 서비스에 대한 인터페이스를 식별합니다. 이들 중 하나가 작업 6, 즉 NetrServerPasswordSet 작업입니다.

작업에 대한 서비스를 식별하려면 dce_opnum 키워드 앞에 dce_iface 키워드를 배치해야 합니다. 자세한 내용은 36-61페이지의 dce_iface을/를 참조하십시오.

특정 작업, 하이픈으로 구분된 작업 범위, 쉼표로 구분된 작업과 범위의 목록에 대해 0~65535의 단일 10진수 값을 임의의 순서로 지정할 수 있습니다.

다음 예 중 하나는 유효한 netlogon 작업 번호를 지정합니다.

```
15
15-18
15, 18-20
15, 20-22, 17
15, 18-20, 22, 24-26
```

dce_stub_data

라이센스: 보호

다른 규칙 옵션과 상관없이 규칙 엔진이 스텁 데이터의 처음부터 검사를 시작해야 한다고 지정하려면 dce_stub_data 키워드를 DCE/RPC 프리프로세서와 함께 사용할 수 있습니다. dce_stub_data 키워드 뒤에 나오는 패킷 페이로드 규칙 옵션은 스텁 데이터 버퍼를 기준으로 적용됩니다.

DCE/RPC 스텁 데이터는 DCE/RPC 중심의 서비스와 루틴을 제공하는 메커니즘인 클라이언트 절차 호출과 DCE/RPC 런타임 시스템 간 인터페이스를 제공합니다. DCE/RPC 익스플로잇은 DCE/RPC 패킷의 stub 데이터 부분에서 식별됩니다. 스텁 데이터는 특정 작업 또는 기능과 관련되어 있으므로 관련 서비스 및 작업을 식별하려면 항상 dce_stub_data 앞에 dce_iface 및 dce_opnum을 두어야 합니다.

dce_stub_data 키워드에는 인수가 없습니다. 자세한 내용은 36-61페이지의 dce_iface 및 36-62페이지의 dce_opnum을/를 참조하십시오.

SIP 키워드

라이센스: 보호

4개의 SIP 키워드를 사용하면 SIP 세션 트래픽에서 익스플로잇을 모니터링할 수 있습니다.

SIP 프로토콜은 DoS(서비스 거부) 공격에 취약합니다. 이러한 공격을 해결하는 규칙은 속도 기반 공격 방지로 혜택을 얻을 수 있습니다. 자세한 내용은 32-29페이지의 동적 규칙 상태 추가 및 34-9페이지의 속도 기반 공격 방지을/를 참조하십시오.

자세한 내용은 다음 절을 참조하십시오.

- 36-63페이지의 sip_header
- 36-63페이지의 sip_body
- 36-63페이지의 sip_method
- 36-64페이지의 sip_stat_code

sip_header

라이센스: 보호

추출된 SIP 요청 또는 응답 헤더의 처음부터 검사를 시작하고 헤더 필드에 대한 검사를 제한하려면 `sip_header` 키워드를 사용할 수 있습니다.

`sip_header` 키워드에는 인수가 없습니다. 자세한 내용은 36-63페이지의 sip_method 및 36-64페이지의 sip_stat_code을/를 참조하십시오.

다음의 예제 규칙 프래그먼트는 SIP 헤더를 가리키며 CSeq 헤더 필드를 매칭합니다.

```
alert udp any any -> any 5060 ( sip_header; content:"CSeq"; )
```

sip_body

라이센스: 보호

추출된 SIP 요청 또는 응답 메시지 본문의 처음부터 검사를 시작하고 메시지 본문에 대한 검사를 제한하려면 `sip_body` 키워드를 사용할 수 있습니다.

`sip_body` 키워드에는 인수가 없습니다.

다음의 예제 규칙 프래그먼트는 SIP 메시지 본문을 가리키며 추출된 SDP 데이터의 c(연결 정보) 필드에서 특정 IP 주소를 매칭합니다.

```
alert udp any any -> any 5060 ( sip_body; content:"c=IN 192.168.12.14"; )
```

규칙은 SDP 내용 검색으로 제한되지 않습니다. SIP 프리프로세서는 전체 메시지 본문을 추출하고 규칙 엔진에서 사용할 수 있도록 합니다.

sip_method

라이센스: 보호

각 SIP 요청의 *method* 필드는 요청의 목적을 식별합니다. 특정 메서드에 대해 SIP 요청을 테스트하려면 `sip_method` 키워드를 사용할 수 있습니다. 메서드가 여러 개인 경우 쉼표로 구분하십시오.

현재 정의된 다음과 같은 SIP 메서드 중에서 지정할 수 있습니다.

```
ack, benotify, bye, cancel, do, info, invite, join, message, notify, options, prack,
publish, quath, refer, register, service, sprack, subscribe, unsubscribe, update
```

메서드는 대/소문자를 구분하지 않습니다. 메서드가 여러 개인 경우 쉼표로 구분할 수 있습니다.

앞으로 새로운 SIP 메서드가 정의될 수 있으므로 사용자 지정 메서드, 즉 현재 정의되지 않은 SIP 메서드를 지정할 수도 있습니다. 허용되는 필드 값은 RFC 2616에 정의되어 있으며 =, (,) 등의 구분 기호 및 제어 문자를 제외한 모든 문자가 허용됩니다. 제외된 구분 기호의 전체 목록은 RFC 2616을/를 참조하십시오. 시스템은 트래픽에서 지정된 사용자 지정 메서드를 발견하면 패킷 헤더를 검사하지만 메시지는 검사하지 않습니다.

시스템은 21개의 현재 정의된 메서드 및 11개의 추가 메서드를 포함하여 최대 32개의 메서드를 지원합니다. 시스템은 사용자가 구성할 수 있는 정의되지 않은 메서드는 무시합니다. 32개의 총 메서드에는 **Methods to Check** SIP 프리프로세서 옵션을 사용하여 지정한 메서드가 포함됩니다. 자세한 내용은 27-47페이지의 SIP 프리프로세서 옵션 선택을/를 참조하십시오.

부정을 사용할 때에는 메서드를 하나만 지정할 수 있습니다. 예를 들면 다음과 같습니다.

```
!invite
```

그러나 한 규칙의 여러 `sip_method` 키워드는 **AND** 연산으로 연결됩니다. 예를 들어 `invite` 및 `cancel` 외의 모든 추출된 메서드를 테스트하려면 두 개의 부정 `sip_method` 키워드를 사용할 수 있습니다.

```
sip_method: !invite
sip_method: !cancel
```

Cisco에서는, 규칙 엔진이 fast pattern matcher를 사용하도록 하려면 `sip_method` 키워드가 포함된 규칙에 하나 이상의 `content` 키워드를 포함할 것을 권장합니다. 이렇게 하면 처리 속도가 빨라지고 성능이 향상됩니다. **Use Fast Pattern Matcher** 인수에서 `content` 키워드의 활성화 여부와 상관없이, 규칙에 `content` 키워드가 하나 이상 포함되어 있으면 규칙 엔진은 fast pattern matcher를 사용합니다. 자세한 내용은 36-14페이지의 내용 일치 검색 및 36-26페이지의 Fast Pattern Matcher 사용을/를 참조하십시오.

sip_stat_code

라이센스: 보호

각 SIP 응답의 세 자리 상태 코드는 요청된 작업의 출력을 나타냅니다. 특정 상태 코드에 대해 SIP 응답을 테스트하려면 `sip_stat_code` 키워드를 사용할 수 있습니다.

1-9의 1자리 응답 유형 숫자, 100-999의 특정 3자리 숫자, 또는 각각의 쉼표로 구분된 조합의 목록을 지정할 수 있습니다. 목록의 단일 숫자가 SIP 응답의 코드와 일치하면 목록이 일치합니다.

다음 표에서는 지정할 수 있는 SIP 상태 코드 값에 대해 설명합니다.

표 36-40 `sip_stat_code` ***값***

탐지할 내용	지정	예	탐지 결과
특정 상태 코드	3자리 상태 코드	189	189
지정한 단일 숫자로 시작되는 3자리 코드	단일 숫자	1	1xx, 즉 100, 101, 102 등
값의 목록	특정 코드 및 단일 숫자를 쉼표로 구분한 조합	222, 3	222 더하기 300, 301, 302 등

규칙에 `content` 키워드가 포함되었는지 여부와 상관없이, 규칙 엔진은 `sip_stat_code` 키워드로 지정한 값을 검색하는 데 fast pattern matcher를 사용하지 않습니다.

GTP 키워드

라이센스: 보호

GTP(GSRP Tunneling Protocol) 키워드를 사용하면 GTP 버전, 메시지 유형 및 정보 요소에 대해 GTP 명령 채널을 검사할 수 있습니다. GTP 키워드는 다른 침입 규칙 키워드(예: `content` 또는 `byte_jump`)와 함께 사용할 수 없습니다. `gtp_info` 또는 `gtp_type` 키워드를 사용하는 각 규칙에서는 `gtp_version` 키워드를 사용해야 합니다.

자세한 내용은 다음 절을 참조하십시오.

- 36-65페이지의 gtp_version
- 36-65페이지의 gtp_type
- 36-70페이지의 gtp_info

gtp_version

GTP 버전 0, 1 또는 2에 대한 GTP 제어 메시지를 검사하려면 `gtp_version` 키워드를 사용할 수 있습니다.

서로 다른 GTP 버전은 서로 다른 메시지 유형 및 정보 요소를 정의하므로 `gtp_type` 또는 `gtp_info` 키워드를 사용할 때는 이 키워드를 사용해야 합니다. 값 0, 1 또는 2를 지정할 수 있습니다.

GTP 버전을 지정하려면

액세스: Admin/Intrusion Admin

1단계 Create Rule 페이지의 드롭다운 목록에서 **gtp_version**을 선택하고 **Add Option**을 클릭합니다.

`gtp_version` 키워드가 나타납니다.

2단계 GTP 버전을 식별하려면 `0`, `1` 또는 `2`를 지정합니다.

gtp_type

각 GTP 메시지는 메시지 유형별로 식별되며, 숫자 값 및 문자열로 구성됩니다. 트래픽에서 특정 GTP 메시지 유형을 검사하려면 `gtp_type` 키워드를 `gtp_version` 키워드와 함께 사용할 수 있습니다.

다음 예에 보이는 것처럼 메시지 유형에 대해 정의된 10진수 값, 정의된 문자열, 둘 중 하나 또는 둘 모두의 쉼표로 구분된 조합의 목록을 지정할 수 있습니다.

```
10, 11, echo_request
```

시스템은 나열된 각 값 또는 문자열을 매칭하기 위해 OR 연산을 사용합니다. 값과 문자열을 나열하는 순서는 중요하지 않습니다. 목록에 있는 모든 단일 값 또는 문자열이 키워드와 매칭됩니다. 인식되지 않은 문자열 또는 범위를 벗어난 값이 포함된 규칙을 저장하려고 하면 오류가 표시됩니다.

다음 표에서 서로 다른 GTP 버전은 동일한 메시지 유형에 대해 서로 다른 값을 사용합니다. 예를 들어 `sgsn_context_request` 메시지 유형은 GTPv0 및 GTPv1의 값이 50이지만 GTPv2의 값은 130입니다.

패킷의 버전 번호에 따라 `gtp_type` 키워드는 서로 다른 값을 매칭합니다. 위의 예에서 키워드는 GTPv0 또는 GTPv1 패킷에서는 메시지 유형 값 30을 매칭하고, GTPv2 패킷에서는 값 130을 매칭합니다. 패킷의 메시지 유형 값이 패킷에 지정된 버전에 대한 알려진 값이 아니면 키워드는 패킷을 매칭하지 않습니다.

메시지 유형에 대해 정수를 지정하면 패킷에 지정된 버전과 상관없이, 키워드의 메시지 유형이 GTP 패킷의 값과 일치하는 경우 키워드가 매칭됩니다.

다음 표에는 각 GTP 메시지 유형에 대해 시스템이 인식하는 정의된 값과 문자열이 나열되어 있습니다.

표 36-41 GTP 메시지 유형

가치	버전 0	버전 1	버전 2
1	echo_request	echo_request	echo_request
2	echo_response	echo_response	echo_response
3	version_not_supported	version_not_supported	version_not_supported
4	node_alive_request	node_alive_request	해당 없음
5	node_alive_response	node_alive_response	해당 없음
6	redirection_request	redirection_request	해당 없음
7	redirection_response	redirection_response	해당 없음
16	create_pdp_context_request	create_pdp_context_request	해당 없음
17	create_pdp_context_response	create_pdp_context_response	해당 없음
18	update_pdp_context_request	update_pdp_context_request	해당 없음
19	update_pdp_context_response	update_pdp_context_response	해당 없음
20	delete_pdp_context_request	delete_pdp_context_request	해당 없음
21	delete_pdp_context_response	delete_pdp_context_response	해당 없음
22	create_aa_pdp_context_request	init_pdp_context_activation_request	해당 없음
23	create_aa_pdp_context_response	init_pdp_context_activation_response	해당 없음
24	delete_aa_pdp_context_request	해당 없음	해당 없음
25	delete_aa_pdp_context_response	해당 없음	해당 없음
26	error_indication	error_indication	해당 없음
27	pdu_notification_request	pdu_notification_request	해당 없음
28	pdu_notification_response	pdu_notification_response	해당 없음
29	pdu_notification_reject_request	pdu_notification_reject_request	해당 없음
30	pdu_notification_reject_response	pdu_notification_reject_response	해당 없음
31	해당 없음	supported_ext_header_notification	해당 없음
32	send_routing_info_request	send_routing_info_request	create_session_request
33	send_routing_info_response	send_routing_info_response	create_session_response
34	failure_report_request	failure_report_request	modify_bearer_request
35	failure_report_response	failure_report_response	modify_bearer_response
36	note_ms_present_request	note_ms_present_request	delete_session_request
37	note_ms_present_response	note_ms_present_response	delete_session_response
38	해당 없음	해당 없음	change_notification_request
39	해당 없음	해당 없음	change_notification_response
48	identification_request	identification_request	해당 없음
49	identification_response	identification_response	해당 없음
50	sgsn_context_request	sgsn_context_request	해당 없음

표 36-41 GTP 메시지 유형(계속)

가치	버전 0	버전 1	버전 2
51	sgsn_context_response	sgsn_context_response	해당 없음
52	sgsn_context_ack	sgsn_context_ack	해당 없음
53	해당 없음	forward_relocation_request	해당 없음
54	해당 없음	forward_relocation_response	해당 없음
55	해당 없음	forward_relocation_complete	해당 없음
56	해당 없음	relocation_cancel_request	해당 없음
57	해당 없음	relocation_cancel_response	해당 없음
58	해당 없음	forward_srns_contex	해당 없음
59	해당 없음	forward_relocation_complete_ack	해당 없음
60	해당 없음	forward_srns_contex_ack	해당 없음
64	해당 없음	해당 없음	modify_bearer_command
65	해당 없음	해당 없음	modify_bearer_failure_indication
66	해당 없음	해당 없음	delete_bearer_command
67	해당 없음	해당 없음	delete_bearer_failure_indication
68	해당 없음	해당 없음	bearer_resource_command
69	해당 없음	해당 없음	bearer_resource_failure_indication
70	해당 없음	ran_info_relay	downlink_failure_indication
71	해당 없음	해당 없음	trace_session_activation
72	해당 없음	해당 없음	trace_session_deactivation
73	해당 없음	해당 없음	stop_paging_indication
95	해당 없음	해당 없음	create_bearer_request
96	해당 없음	mbms_notification_request	create_bearer_response
97	해당 없음	mbms_notification_response	update_bearer_request
98	해당 없음	mbms_notification_reject_request	update_bearer_response
99	해당 없음	mbms_notification_reject_response	delete_bearer_request
100	해당 없음	create_mbms_context_request	delete_bearer_response
101	해당 없음	create_mbms_context_response	delete_pdn_request
102	해당 없음	update_mbms_context_request	delete_pdn_response
103	해당 없음	update_mbms_context_response	해당 없음
104	해당 없음	delete_mbms_context_request	해당 없음
105	해당 없음	delete_mbms_context_response	해당 없음
112	해당 없음	mbms_register_request	해당 없음
113	해당 없음	mbms_register_response	해당 없음
114	해당 없음	mbms_deregister_request	해당 없음
115	해당 없음	mbms_deregister_response	해당 없음
116	해당 없음	mbms_session_start_request	해당 없음

표 36-41 GTP 메시지 유형(계속)

가치	버전 0	버전 1	버전 2
117	해당 없음	mbms_session_start_response	해당 없음
118	해당 없음	mbms_session_stop_request	해당 없음
119	해당 없음	mbms_session_stop_response	해당 없음
120	해당 없음	mbms_session_update_request	해당 없음
121	해당 없음	mbms_session_update_response	해당 없음
128	해당 없음	ms_info_change_request	identification_request
129	해당 없음	ms_info_change_response	identification_response
130	해당 없음	해당 없음	sgsn_context_request
131	해당 없음	해당 없음	sgsn_context_response
132	해당 없음	해당 없음	sgsn_context_ack
133	해당 없음	해당 없음	forward_relocation_request
134	해당 없음	해당 없음	forward_relocation_response
135	해당 없음	해당 없음	forward_relocation_complete
136	해당 없음	해당 없음	forward_relocation_complete_ack
137	해당 없음	해당 없음	forward_access
138	해당 없음	해당 없음	forward_access_ack
139	해당 없음	해당 없음	relocation_cancel_request
140	해당 없음	해당 없음	relocation_cancel_response
141	해당 없음	해당 없음	configuration_transfer_tunnel
149	해당 없음	해당 없음	detach
150	해당 없음	해당 없음	detach_ack
151	해당 없음	해당 없음	cs_paging
152	해당 없음	해당 없음	ran_info_relay
153	해당 없음	해당 없음	alert_mme
154	해당 없음	해당 없음	alert_mme_ack
155	해당 없음	해당 없음	ue_activity
156	해당 없음	해당 없음	ue_activity_ack
160	해당 없음	해당 없음	create_forward_tunnel_request
161	해당 없음	해당 없음	create_forward_tunnel_response
162	해당 없음	해당 없음	suspend
163	해당 없음	해당 없음	suspend_ack
164	해당 없음	해당 없음	resume
165	해당 없음	해당 없음	resume_ack
166	해당 없음	해당 없음	create_indirect_forward_tunnel_request
167	해당 없음	해당 없음	create_indirect_forward_tunnel_response
168	해당 없음	해당 없음	delete_indirect_forward_tunnel_request

표 36-41 GTP 메시지 유형(계속)

가치	버전 0	버전 1	버전 2
169	해당 없음	해당 없음	delete_indirect_forward_tunnel_response
170	해당 없음	해당 없음	release_access_bearer_request
171	해당 없음	해당 없음	release_access_bearer_response
176	해당 없음	해당 없음	downlink_data
177	해당 없음	해당 없음	downlink_data_ack
179	해당 없음	해당 없음	pgw_restart
180	해당 없음	해당 없음	pgw_restart_ack
200	해당 없음	해당 없음	update_pdn_request
201	해당 없음	해당 없음	update_pdn_response
211	해당 없음	해당 없음	modify_access_bearer_request
212	해당 없음	해당 없음	modify_access_bearer_response
231	해당 없음	해당 없음	mbms_session_start_request
232	해당 없음	해당 없음	mbms_session_start_response
233	해당 없음	해당 없음	mbms_session_update_request
234	해당 없음	해당 없음	mbms_session_update_response
235	해당 없음	해당 없음	mbms_session_stop_request
236	해당 없음	해당 없음	mbms_session_stop_response
240	data_record_transfer_request	data_record_transfer_request	해당 없음
241	data_record_transfer_response	data_record_transfer_response	해당 없음
254	해당 없음	end_marker	해당 없음
255	pdu	pdu	해당 없음

GTP 메시지 유형을 지정하려면

액세스: Admin/Intrusion Admin

1단계 Create Rule 페이지의 드롭다운 목록에서 **gtp_type**을 선택하고 **Add Option**을 클릭합니다.

`gtp_type` 키워드가 나타납니다.

2단계 메시지 유형에 대해 0~255의 정의된 10진수 값, 정의된 문자열, 둘 중 하나 또는 둘 모두의 쉼표로 구분된 조합의 목록을 지정합니다. 시스템에서 인식하는 값 및 문자열은 GTP 메시지 유형 표를 참조하십시오.

gtp_info

GTP 메시지는 여러 정보 요소를 포함할 수 있으며, 각 요소는 정의된 숫자 값 및 정의된 문자열로 식별됩니다. 지정된 정보 요소의 처음부터 검사를 시작하고 지정된 정보 요소에 대해 검사를 제한하려면 `gtp_info` 키워드를 `gtp_version` 키워드와 함께 사용할 수 있습니다.

정보 요소에 대해 정의된 10진수 값 또는 정의된 문자열을 지정할 수 있습니다. 여러 정보 요소를 검사하려면 단일 값 또는 문자열을 지정하고, 하나의 규칙에 여러 `gtp_info` 키워드를 사용할 수 있습니다.

메시지가 동일한 유형의 여러 정보 요소를 포함하면 모두에 대해 매칭이 검사됩니다. 정보 요소가 잘못된 순서로 나타나면 마지막 인스턴스만 검사됩니다.

서로 다른 GTP 버전은 동일한 정보 요소에 대해 서로 다른 값을 사용합니다. 예를 들어 `cause` 정보 요소는 GTPv0 및 GTPv1의 값이 1이지만 GTPv2의 값은 2입니다.

패킷의 버전 번호에 따라 `gtp_info` 키워드는 서로 다른 값을 매칭합니다. 위의 예에서 키워드는 GTPv0 또는 GTPv1 패킷에서는 정보 요소 값 1을 매칭하고, GTPv2 패킷에서는 2를 매칭합니다. 패킷의 정보 요소 값이 패킷에 지정된 버전에 대한 알려진 값이 아니면 키워드는 패킷을 매칭하지 않습니다.

정보 요소에 대해 정수를 지정하면 패킷에 지정된 버전과 상관없이, 키워드의 메시지 유형이 GTP 패킷의 값과 일치하는 경우 키워드가 매칭됩니다.

다음 표에는 각 GTP 정보 요소에 대해 시스템이 인식하는 값과 문자열이 나열되어 있습니다.

표 36-42 GTP 정보 요소

가치	버전 0	버전 1	버전 2
1	cause	cause	imsi
2	imsi	imsi	cause
3	rai	rai	recovery
4	tlli	tlli	해당 없음
5	p_tmsi	p_tmsi	해당 없음
6	qos	해당 없음	해당 없음
8	recording_required	recording_required	해당 없음
9	authentication	authentication	해당 없음
11	map_cause	map_cause	해당 없음
12	p_tmsi_sig	p_tmsi_sig	해당 없음
13	ms_validated	ms_validated	해당 없음
14	recovery	recovery	해당 없음
15	selection_mode	selection_mode	해당 없음
16	flow_label_data_1	teid_1	해당 없음
17	flow_label_signalling	teid_control	해당 없음
18	flow_label_data_2	teid_2	해당 없음
19	ms_unreachable	teardown_ind	해당 없음
20	해당 없음	nsapi	해당 없음
21	해당 없음	ranap	해당 없음
22	해당 없음	rab_context	해당 없음

표 36-42 GTP 정보 요소(계속)

가치	버전 0	버전 1	버전 2
23	해당 없음	radio_priority_sms	해당 없음
24	해당 없음	radio_priority	해당 없음
25	해당 없음	packet_flow_id	해당 없음
26	해당 없음	charging_char	해당 없음
27	해당 없음	trace_ref	해당 없음
28	해당 없음	trace_type	해당 없음
29	해당 없음	ms_unreachable	해당 없음
71	해당 없음	해당 없음	apn
72	해당 없음	해당 없음	ambr
73	해당 없음	해당 없음	ebi
74	해당 없음	해당 없음	ip_addr
75	해당 없음	해당 없음	mei
76	해당 없음	해당 없음	msisdn
77	해당 없음	해당 없음	indication
78	해당 없음	해당 없음	pco
79	해당 없음	해당 없음	paa
80	해당 없음	해당 없음	bearer_qos
80	해당 없음	해당 없음	flow_qos
82	해당 없음	해당 없음	rat_type
83	해당 없음	해당 없음	serving_network
84	해당 없음	해당 없음	bearer_tft
85	해당 없음	해당 없음	tad
86	해당 없음	해당 없음	uli
87	해당 없음	해당 없음	f_teid
88	해당 없음	해당 없음	tmsi
89	해당 없음	해당 없음	cn_id
90	해당 없음	해당 없음	s103pdf
91	해당 없음	해당 없음	s1udf
92	해당 없음	해당 없음	delay_value
93	해당 없음	해당 없음	bearer_context
94	해당 없음	해당 없음	charging_id
95	해당 없음	해당 없음	charging_char
96	해당 없음	해당 없음	trace_info
97	해당 없음	해당 없음	bearer_flag
99	해당 없음	해당 없음	pdn_type
100	해당 없음	해당 없음	pti

표 36-42 GTP 정보 요소(계속)

가치	버전 0	버전 1	버전 2
101	해당 없음	해당 없음	drx_parameter
103	해당 없음	해당 없음	gsm_key_tri
104	해당 없음	해당 없음	umts_key_cipher_quin
105	해당 없음	해당 없음	gsm_key_cipher_quin
106	해당 없음	해당 없음	umts_key_quin
107	해당 없음	해당 없음	eps_quad
108	해당 없음	해당 없음	umts_key_quad_quin
109	해당 없음	해당 없음	pdn_connection
110	해당 없음	해당 없음	pdn_number
111	해당 없음	해당 없음	p_tmsi
112	해당 없음	해당 없음	p_tmsi_sig
113	해당 없음	해당 없음	hop_counter
114	해당 없음	해당 없음	ue_time_zone
115	해당 없음	해당 없음	trace_ref
116	해당 없음	해당 없음	complete_request_msg
117	해당 없음	해당 없음	guti
118	해당 없음	해당 없음	f_container
119	해당 없음	해당 없음	f_cause
120	해당 없음	해당 없음	plmn_id
121	해당 없음	해당 없음	target_id
123	해당 없음	해당 없음	packet_flow_id
124	해당 없음	해당 없음	rab_contex
125	해당 없음	해당 없음	src_rnc_pdcp
126	해당 없음	해당 없음	udp_src_port
127	charge_id	charge_id	apn_restriction
128	end_user_address	end_user_address	selection_mode
129	mm_context	mm_context	src_id
130	pdp_context	pdp_context	해당 없음
131	apn	apn	change_report_action
132	protocol_config	protocol_config	fq_csid
133	gsn	gsn	channel
134	msisdn	msisdn	emlpp_pri
135	해당 없음	qos	node_type
136	해당 없음	authentication_qu	fqdn
137	해당 없음	tft	ti
138	해당 없음	target_id	mbms_session_duration

표 36-42 GTP 정보 요소(계속)

가치	버전 0	버전 1	버전 2
139	해당 없음	utran_trans	mbms_service_area
140	해당 없음	rab_setup	mbms_session_id
141	해당 없음	ext_header	mbms_flow_id
142	해당 없음	trigger_id	mbms_ip_multicast
143	해당 없음	omc_id	mbms_distribution_ack
144	해당 없음	ran_trans	rfsp_index
145	해당 없음	pdp_context_pri	uci
146	해당 없음	addi_rab_setup	csg_info
147	해당 없음	sgsn_number	csg_id
148	해당 없음	common_flag	cmi
149	해당 없음	apn_restriction	service_indicator
150	해당 없음	radio_priority_lcs	detach_type
151	해당 없음	rat_type	ldn
152	해당 없음	user_loc_info	node_feature
153	해당 없음	ms_time_zone	mbms_time_to_transfer
154	해당 없음	imei_sv	throttling
155	해당 없음	camel	arp
156	해당 없음	mbms_ue_context	epc_timer
157	해당 없음	tmp_mobile_group_id	signalling_priority_indication
158	해당 없음	rim_routing_addr	tmgi
159	해당 없음	mbms_config	mm_srvcc
160	해당 없음	mbms_service_area	flags_srvcc
161	해당 없음	src_rnc_pdcp	nmbr
162	해당 없음	addi_trace_info	해당 없음
163	해당 없음	hop_counter	해당 없음
164	해당 없음	plmn_id	해당 없음
165	해당 없음	mbms_session_id	해당 없음
166	해당 없음	mbms_2g3g_indicator	해당 없음
167	해당 없음	enhanced_nsapi	해당 없음
168	해당 없음	mbms_session_duration	해당 없음
169	해당 없음	addi_mbms_trace_info	해당 없음
170	해당 없음	mbms_session_repetition_num	해당 없음
171	해당 없음	mbms_time_to_data	해당 없음
173	해당 없음	bss	해당 없음
174	해당 없음	cell_id	해당 없음
175	해당 없음	pdu_num	해당 없음

표 36-42 GTP 정보 요소(계속)

가치	버전 0	버전 1	버전 2
177	해당 없음	mbms_bearer_capab	해당 없음
178	해당 없음	rim_routing_disc	해당 없음
179	해당 없음	list_pfc	해당 없음
180	해당 없음	ps_xid	해당 없음
181	해당 없음	ms_info_change_report	해당 없음
182	해당 없음	direct_tunnel_flags	해당 없음
183	해당 없음	correlation_id	해당 없음
184	해당 없음	bearer_control_mode	해당 없음
185	해당 없음	mbms_flow_id	해당 없음
186	해당 없음	mbms_ip_multicast	해당 없음
187	해당 없음	mbms_distribution_ack	해당 없음
188	해당 없음	reliable_inter_rat_handover	해당 없음
189	해당 없음	rfsp_index	해당 없음
190	해당 없음	fqdn	해당 없음
191	해당 없음	evolved_allocation1	해당 없음
192	해당 없음	evolved_allocation2	해당 없음
193	해당 없음	extended_flags	해당 없음
194	해당 없음	uci	해당 없음
195	해당 없음	csg_info	해당 없음
196	해당 없음	csg_id	해당 없음
197	해당 없음	cmi	해당 없음
198	해당 없음	apn_ambr	해당 없음
199	해당 없음	ue_network	해당 없음
200	해당 없음	ue_ambr	해당 없음
201	해당 없음	apn_ambr_nsapi	해당 없음
202	해당 없음	ggsn_backoff_timer	해당 없음
203	해당 없음	signalling_priority_indication	해당 없음
204	해당 없음	signalling_priority_indication_nsapi	해당 없음
205	해당 없음	high_bitrate	해당 없음
206	해당 없음	max_mbr	해당 없음
251	charging_gateway_addr	charging_gateway_addr	해당 없음
255	private_extension	private_extension	private_extension

GTP 정보 요소를 지정하려면 다음 절차를 사용할 수 있습니다.

GTP 정보 요소를 지정하려면

액세스: Admin/Intrusion Admin

1단계 Create Rule 페이지의 드롭다운 목록에서 **gtp_info**를 선택하고 **Add Option**을 클릭합니다.

`gtp_info` 키워드가 나타납니다.

2단계 정보 요소에 대해 0~255의 정의된 단일 10진수 값 또는 정의된 단일 문자열을 지정합니다. 시스템에서 인식하는 값 및 문자열은 GTP 정보 요소 표를 참조하십시오.

Modbus 키워드

라이센스: 보호

Modbus Function Code에 대해 또는 Modbus Unit ID에 대해 매칭하기 위해 Modbus 요청 또는 응답의 Data 필드 시작 부분을 가리키려면 Modbus 키워드를 사용할 수 있습니다. Modbus 키워드는 단독으로 또는 다른 키워드(예: `content` 또는 `byte_jump`)와 함께 사용할 수 있습니다.

자세한 내용은 다음 절을 참조하십시오.

- 36-75페이지의 modbus_data
- 36-75페이지의 modbus_func
- 36-76페이지의 modbus_unit

modbus_data

Modbus 요청 또는 응답의 Data 필드 시작 부분을 가리키려면 `modbus_data` 키워드를 사용할 수 있습니다.

Modbus Data 필드 시작 부분을 가리키려면

액세스: Admin/Intrusion Admin

1단계 Create Rule 페이지의 드롭다운 목록에서 **modbus_data**를 선택하고 **Add Option**을 클릭합니다.

`modbus_data` 키워드가 나타납니다.

`modbus_data` 키워드에는 인수가 없습니다.

modbus_func

Modbus 애플리케이션 레이어 요청 또는 응답 헤더의 Function Code 필드에 대해 매칭하려면 `modbus_func` 키워드를 사용할 수 있습니다. Modbus 함수 코드에 대해 정의된 단일 10진수 값 또는 정의된 단일 문자열을 지정할 수 있습니다.

다음 표에는 Modbus 함수 코드에 대해 시스템이 인식하는 정의된 값과 문자열이 나열되어 있습니다.

표 36-43 Modbus 함수 코드

가치	문자열
1	read_coils
2	read_discrete_inputs

표 36-43 Modbus 함수 코드(계속)

가치	문자열
3	read_holding_registers
4	read_input_registers
5	write_single_coil
6	write_single_register
7	read_exception_status
8	diagnostics
11	get_comm_event_counter
12	get_comm_event_log
15	write_multiple_coils
16	write_multiple_registers
17	report_slave_id
20	read_file_record
21	write_file_record
22	mask_write_register
23	read_write_multiple_registers
24	read_fifo_queue
43	encapsulated_interface_transport

Modbus 함수 코드를 지정하려면

액세스: Admin/Intrusion Admin

1단계 Create Rule 페이지의 드롭다운 목록에서 **modbus_func**를 선택하고 **Add Option**을 클릭합니다.

`modbus_func` 키워드가 나타납니다.

2단계 함수 코드에 대해 0~255의 정의된 단일 10진수 값 또는 정의된 단일 문자열을 지정합니다. 시스템에서 인식하는 값 및 문자열은 Modbus 함수 코드 표를 참조하십시오.

modbus_unit

Modbus 요청 또는 응답 헤더의 Unit ID 필드에 대해 단일 10진수 값을 매칭하려면 `modbus_unit` 키워드를 사용할 수 있습니다.

Modbus unit ID를 지정하려면

액세스: Admin/Intrusion Admin

1단계 Create Rule 페이지의 드롭다운 목록에서 **modbus_unit**을 선택하고 **Add Option**을 클릭합니다.

`modbus_unit` 키워드가 나타납니다.

2단계 0~255의 10진수 값을 지정합니다.

DNP3 키워드

라이센스: 보호

애플리케이션 레이어 프래그먼트의 시작 부분을 가리키고, DNP3 응답 및 요청에서 DNP3 함수 코드 및 객체에 대해 매칭하고, DNP3 응답의 내부 표시 플래그에 대해 매칭하려면 DNP3 키워드를 사용할 수 있습니다. DNP3 키워드는 단독으로 또는 다른 키워드(예: `content` 또는 `byte_jump`)와 함께 사용할 수 있습니다.

자세한 내용은 다음 절을 참조하십시오.

- 36-77페이지의 dnp3_data
- 36-77페이지의 dnp3_func
- 36-79페이지의 dnp3_ind
- 36-80페이지의 dnp3_obj

dnp3_data

리어셈블된 DNP3 애플리케이션 레이어 프래그먼트의 시작 부분을 가리키려면 `dnp3_data` 키워드를 사용할 수 있습니다.

DNP3 프리프로세서는 링크 레이어 프레임을 애플리케이션 레이어 프래그먼트로 리어셈블합니다. `dnp3_data` 키워드는 각 애플리케이션 레이어 프래그먼트의 시작 부분을 가리킵니다. 다른 규칙 옵션은 데이터를 분리하고 16초마다 체크섬을 추가하지 않은 채 프래그먼트 내에서 리어셈블된 데이터에 대해 매칭할 수 있습니다.

리어셈블된 DNP3 프래그먼트의 시작 부분을 가리키려면

액세스: Admin/Intrusion Admin

1단계 Create Rule 페이지의 드롭다운 목록에서 **modbus_data**를 선택하고 **Add Option**을 클릭합니다.

`dnp3_data` 키워드가 나타납니다.

`dnp3_data` 키워드에는 인수가 없습니다.

dnp3_func

DNP3 애플리케이션 레이어 요청 또는 응답 헤더의 Function Code 필드에 대해 매칭하려면 `dnp3_func` 키워드를 사용할 수 있습니다. DNP3 함수 코드에 대해 정의된 단일 10진수 값 또는 정의된 단일 문자열을 지정할 수 있습니다.

다음 표에는 DNP3 함수 코드에 대해 시스템이 인식하는 정의된 값과 문자열이 나열되어 있습니다.

표 36-44 DNP3 함수 코드

가치	문자열
0	confirm
1	read
2	write
3	select
4	operate

표 36-44 DNP3 함수 코드(계속)

가치	문자열
5	direct_operate
6	direct_operate_nr
7	immed_freeze
8	immed_freeze_nr
9	freeze_clear
10	freeze_clear_nr
11	freeze_at_time
12	freeze_at_time_nr
13	cold_restart
14	warm_restart
15	initialize_data
16	initialize_appl
17	start_appl
18	stop_appl
19	save_config
20	enable_unsolicited
21	disable_unsolicited
22	assign_class
23	delay_measure
24	record_current_time
25	open_file
26	close_file
27	delete_file
28	get_file_info
29	authenticate_file
30	abort_file
31	activate_config
32	authenticate_req
33	authenticate_err
129	response
130	unsolicited_response
131	authenticate_resp

DNP3 함수 코드를 지정하려면

액세스: Admin/Intrusion Admin

1단계 Create Rule 페이지의 드롭다운 목록에서 **dnp3_func**를 선택하고 **Add Option**을 클릭합니다.

`dnp3_func` 키워드가 나타납니다.

2단계 함수 코드에 대해 0~255의 정의된 단일 10진수 값 또는 정의된 단일 문자열을 지정합니다. 시스템에서 인식하는 값 및 문자열은 DNP3 함수 코드 표를 참조하십시오.

dnp3_ind

DNP3 애플리케이션 레이어 응답 헤더의 Internal Indications 필드에 있는 플래그에 대해 매칭하려면 `dnp3_ind` 키워드를 사용할 수 있습니다.

다음 예와 같이 알려진 단일 플래그 또는 쉼표로 구분된 플래그 목록에 대한 문자열을 지정할 수 있습니다.

```
class_1_events, class_2_events
```

여러 플래그를 지정하면 목록에 있는 임의의 플래그에 대해 키워드가 매칭됩니다. 플래그의 조합을 탐지하려면 하나의 규칙에 `dnp3_ind` 키워드를 여러 번 사용합니다.

다음 목록은 정의된 DNP3 내부 표시 플래그에 대해 시스템에서 인식하는 문자열 구문을 제공합니다.

```
class_1_events
class_2_events
class_3_events
need_time
local_control
device_trouble
device_restart
no_func_code_support
object_unknown
parameter_error
event_buffer_overflow
already_executing
config_corrupt
reserved_2
reserved_1
```

DNP3 내부 표시 플래그를 지정하려면

액세스: Admin/Intrusion Admin

1단계 Create Rule 페이지의 드롭다운 목록에서 **dnp3_ind**를 선택하고 **Add Option**을 클릭합니다.

`dnp3_ind` 키워드가 나타납니다.

2단계 알려진 단일 플래그 또는 쉼표로 구분된 플래그 목록에 대한 문자열을 지정할 수 있습니다.

dnp3_obj

요청 또는 응답의 DNP3 객체 헤더에 대해 매칭하려면 `dnp3_obj` 키워드를 사용할 수 있습니다.

DNP3 데이터는 아날로그 입력, 이진 입력 등 유형이 서로 다른 일련의 DNP3 객체로 구성되어 있습니다. 각 유형은 *그룹*(아날로그 입력 그룹, 이진 입력 그룹 등)으로 식별되며, 이들 각각은 10진수 값으로 식별할 수 있습니다. 각 그룹의 객체는 16비트 정수, 32비트 정수, 짧은 부동 소수점 등 *객체 변형*에 의해 더 식별되며, 이들 각각은 객체의 데이터 형식을 지정합니다. 객체 변형의 각 유형 역시 10진수 값으로 식별할 수 있습니다.

객체 헤더 그룹의 유형 및 객체 변형의 유형에 대해 10진수를 지정함으로써 객체 헤더를 식별합니다. 이 둘의 조합으로 DNP3 객체의 특정 유형을 정의합니다.

DNP3 객체를 지정하려면

액세스: Admin/Intrusion Admin

1단계 Create Rule 페이지의 드롭다운 목록에서 **dnp3_obj**를 선택하고 **Add Option**을 클릭합니다.

`dnp3_obj` 키워드가 나타납니다.

2단계 알려진 객체 그룹을 식별하기 위한 10진수 값(0~255)을 지정하고, 알려진 객체 변형 유형을 식별하기 위한 또 다른 10진수 값(0~255)을 지정합니다.

패킷 특성 검사

라이센스: 보호

특정 패킷 특성이 있는 패킷에 대해서만 이벤트를 생성하는 규칙을 작성할 수 있습니다. FireSIGHT 시스템은 패킷 특성을 평가하기 위해 다음 키워드를 제공합니다.

- 36-80페이지의 dsize
- 36-81페이지의 isdataat
- 36-81페이지의 sameip
- 36-82페이지의 fragoffset
- 36-82페이지의 cvs

dsize

라이센스: 보호

`dsize` 키워드는 패킷 페이로드 크기를 테스트합니다. 값의 범위를 지정하려면 보다 큼 및 보다 작음 연산자(`<` 및 `>`)를 사용할 수 있습니다. 다음 구문으로 범위를 지정할 수 있습니다.

```
>number_of_bytes
<number_of_bytes
number_of_bytes<>number_of_bytes
```

예를 들어 400바이트보다 큰 패킷 크기를 나타내려면 `dtype` 값으로 `>400`을 사용합니다. 500바이트보다 작은 패킷 크기를 나타내려면 `<500`을 사용합니다. 400~500바이트 사이(포함)의 패킷에 대해 규칙이 트리거되도록 지정하려면 `400<>500`을 사용합니다.

주의 `dsize` 키워드는 프리프로세서에 의해 디코딩되기 전에 패킷을 테스트합니다.

isdataat

라이센스: 보호

isdataat 키워드는 페이로드의 특정 위치에 데이터가 상주하는지 확인하도록 규칙 엔진에 지시합니다.

다음 표에는 isdataat 키워드와 함께 사용할 수 있는 인수가 나열되어 있습니다.

표 36-45 isdataat 인수

인수	유형	설명
Offset	필수	페이로드의 특정 위치. 데이터가 패킷 페이로드의 50바이트 위치에 나타나는지 테스트하려면 오프셋 값으로 50을 지정합니다. ! 수정자는 isdataat 테스트의 결과를 부정하고, 페이로드 내에 특정 데이터 양이 없으면 알림을 표시합니다. 이 인수에 대한 값을 지정하는 데 기존의 byte_extract 변수를 사용할 수도 있습니다. 자세한 내용은 36-83페이지의 키워드 인수로 패킷 데이터 읽어오기을/를 참조하십시오.
Relative	옵션	마지막으로 성공한 내용 일치를 기준으로 위치를 설정합니다. 상대적 위치를 지정하는 경우 카운터는 0바이트부터 시작되므로, 위치를 계산할 때는 마지막으로 성공한 내용 일치로부터 앞으로 이동하려는 바이트 수에서 1을 빼야 합니다. 예를 들어 마지막으로 성공한 내용 일치 후 9번째 바이트에서 데이터가 나타나야 한다고 지정하려면 relative offset 8을 지정합니다.
Raw Data	옵션	FireSIGHT 시스템 프리프로세서에 의한 디코딩 또는 애플리케이션 레이어 표준화 전에 데이터가 원래 패킷 페이로드에 있음을 지정합니다. 이전 내용 일치가 원시 패킷 데이터에 있는 경우 이 인수를 **Relative**와 함께 사용할 수 있습니다.

예를 들어 내용 foo를 검색하는 규칙에서 isdataat에 대한 값이 다음과 같이 지정되면

- Offset = !10
- Relative = enabled

규칙 엔진이 페이로드가 끝나기 전 10바이트 떨어진 곳에서 foo를 탐지하지 못하면 시스템이 알림을 표시합니다.

isdataat를 사용하려면

액세스: Admin/Intrusion Admin

1단계 Create Rule 페이지의 드롭다운 목록에서 isdataat를 선택하고 **Add Option**을 클릭합니다.

isdataat 섹션이 나타납니다.

sameip

라이센스: 보호

sameip 키워드는 패킷의 소스 및 목적지 IP 주소가 동일한지 테스트합니다. 이 키워드는 인수를 사용하지 않습니다.

fragoffset

라이센스: 보호

fragoffset 키워드는 프래그먼트된 패킷의 오프셋을 테스트합니다. 일부 익스플로잇(에: WinNuke DoS 공격)은 특정 오프셋이 있는, 수동으로 생성된 패킷 프래그먼트를 사용하므로 이 키워드가 유용합니다.

예를 들어 프래그먼트된 패킷의 오프셋이 31337바이트인지 테스트하려면 fragoffset 값으로 31337을 지정합니다.

fragoffset 키워드에 대해 인수를 지정할 때는 다음 연산자를 사용할 수 있습니다.

표 36-46 fragoffset 키워드 인수 연산자

운영자	설명
!	not
>	보다 큼
<	보다 작음

not(!) 연산자는 < 또는 > 연산자와 함께 사용할 수 없습니다.

cvs

라이센스: 보호

cvs 키워드는 CVS(Concurrent Versions System) 트래픽에서 형식이 잘못된 CVS 항목을 테스트합니다. 공격자는 형식이 잘못된 항목을 사용하여 CVS 서버에서 힙 오버플로를 적용하고 악의적인 코드를 실행할 수 있습니다. 이 키워드는 두 가지 알려진 CVS 취약성인 CVE-2004-0396(CVS 1.11.x - 최대 1.11.15, 1.12.x - 최대 1.12.7) 및 CVS-2004-0414(CVS 1.12.x~1.12.8, 1.11.x~1.11.16)에 대해 공격을 식별하는 데 사용할 수 있습니다. cvs 키워드는 올바른 형식의 항목을 점검하고 잘못된 형식의 항목이 탐지되면 알림을 생성합니다.

규칙에는 CVS가 실행되는 포트를 포함해야 합니다. 또한 CVS 세션에 대해 상태가 유지될 수 있도록, 트래픽이 발생할 수 있는 포트를 TCP 정책의 스트림 리어셈블리용 포트 목록에 추가해야 합니다. TCP 포트 2401(pserver) 및 514(rsh)는 스트림 리어셈블리가 발생하는 클라이언트 포트 목록에 포함됩니다. 그러나 xinetd 서버(즉, pserver)로서 실행되는 서버는 어떤 TCP 포트에서나 실행할 수 있습니다. 비표준 포트는 스트림 리어셈블리 **Client Ports** 목록에 추가합니다. 자세한 내용은 29-27페이지의 스트림 리어셈블리 옵션 선택을/를 참조하십시오.

형식이 잘못된 CVS 항목을 탐지하려면

액세스: Admin/Intrusion Admin

1단계 규칙에 cvs 옵션을 추가하고 키워드 인수로 invalid-entry를 입력합니다.

키워드 인수로 패킷 데이터 읽어오기

라이센스: 보호

패킷에서 변수로 지정된 바이트 수를 읽어오려면 byte_extract 키워드를 사용할 수 있습니다. 그러면 일부 다른 탐지 키워드의 특정 인수에 대한 값으로 동일한 규칙에서 나중에 변수를 사용할 수 있습니다.

예를 들어, 특정 바이트 세그먼트가 패킷 내 데이터에 포함된 바이트 수를 설명하는 패킷에서 데이터 크기를 추출하는 경우 유용합니다. 예를 들어, 특정 바이트 세그먼트는 이후 데이터가 4바이트로 구성되어 있다고 알려줄 수 있습니다. 그러면 변수 값으로 사용하기 위해 4바이트의 데이터 크기를 추출할 수 있습니다.

하나의 규칙에서 최대 2개의 서로 다른 변수를 생성하려면 byte_extract를 사용할 수 있습니다. byte_extract 변수는 몇 번이든 다시 정의할 수 있습니다. 동일한 변수 이름과 다른 변수 정의로 새 byte_extract 키워드를 입력하면 해당 변수의 이전 정의를 덮어쓰게 됩니다.

다음 표에서는 byte_extract 키워드에 필요한 인수에 대해 설명합니다.

표 36-47 필수 byte_extract 인수

인수	설명
Bytes to Extract	패킷에서 추출할 바이트 수. 1, 2, 3 또는 4바이트를 지정할 수 있습니다.
Offset	데이터 추출을 시작하기 위한 페이로드에 대한 바이트 수. -65534~65535바이트 범위로 지정할 수 있습니다. offset 카운터는 0바이트부터 시작되므로, offset 값을 계산할 때는 앞으로 이동하려는 바이트 수에서 1을 빼야 합니다. 예를 들어 8바이트를 이동하려면 7을 지정합니다. 규칙 엔진은 패킷 페이로드의 시작 부분부터, 또는 **Relative**를 지정한 경우 마지막으로 성공한 내용 일치 이후부터 계산을 시작합니다. 음수는 **Relative**를 지정한 경우에만 지정할 수 있습니다. 자세한 내용은 선택적인 추가 byte_extract 인수 표를 참조하십시오.
Variable Name	인수에서 다른 탐지 키워드에 대해 사용할 변수 이름. 영숫자 문자열을 지정할 수 있지만, 반드시 문자로 시작해야 합니다.

시스템이 추출할 데이터를 찾는 방법을 더 세부적으로 정의하려면 다음 표에 설명된 인수를 사용할 수 있습니다.

표 36-48 선택적인 추가 byte_extract 인수

인수	설명
Multiplier	패킷에서 추출된 값에 대한 승수. 0~65535를 지정할 수 있습니다. 승수를 지정하지 않으면 기본값 1이 사용됩니다.
Align	추출된 값을 가장 가까운 2바이트 또는 4바이트 경계로 반올림합니다. **Multiplier**도 선택한 경우 Align 전에 Multiplier가 적용됩니다.
Relative	페이로드의 시작 대신 마지막으로 성공한 내용 일치의 끝을 기준으로 **Offset**을 지정합니다. 자세한 내용은 필수 byte_extract 인수 표를 참조하십시오.

DCE/RPC, **Endian** 또는 **Number Type** 중 하나만 지정할 수 있습니다.

byte_extract 키워드가 테스트할 바이트를 계산하는 방법을 정의하려면 다음 표의 인수 중에서 선택할 수 있습니다. 두 인수 중 하나를 선택하지 않으면 규칙 엔진은 big endian 바이트 순서를 사용합니다.

표 36-49 Endianness byte_extract 인수

인수	설명
Big Endian	Big Endian 바이트 순서로 데이터를 처리합니다. 이것이 기본 네트워크 바이트 순서입니다.
Little Endian	Little Endian 바이트 순서로 데이터를 처리합니다.
DCE/RPC	DCE/RPC 프리프로세서에 의해 처리되는 트래픽에 대해 byte_extract 키워드를 지정합니다. 자세한 내용은 27-2페이지의 DCE/RPC 트래픽 디코딩을/를 참조하십시오. DCE/RPC 프리프로세서는 big endian 또는 little endian 바이트 순서를 결정하며, **Number Type** 및 **Endian** 인수는 적용되지 않습니다. 이 인수를 활성화하면 byte_extract를 다른 특정 DCE/RPC 키워드와 함께 사용할 수도 있습니다. 자세한 내용은 36-60페이지의 DCE/RPC 키워드을/를 참조하십시오.

ASCII 문자열로 데이터를 읽으려면 숫자 유형을 지정할 수 있습니다. 시스템이 패킷의 문자열 데이터를 보는 방법을 정의하려면 다음 표에 있는 인수 중 하나를 선택할 수 있습니다.

표 36-50 숫자 유형 byte_extract 인수

인수	설명
Hexadecimal String	추출된 문자열 데이터를 16진수 형식으로 읽습니다.
Decimal String	추출된 문자열 데이터를 10진수 형식으로 읽습니다.
Octal String	추출된 문자열 데이터를 8진수 형식으로 읽습니다.

예를 들어, byte_extract의 값이 다음과 같이 지정된 경우

- Bytes to Extract = 4
- Variable Name = var
- Offset = 8
- Relative = enabled

규칙 엔진은 마지막으로 성공한 내용 일치를 기준으로 9바이트 떨어진 곳에 나타나는 4바이트에 설명된 숫자를 이름이 var인 변수로 읽어오는데, 이를 특정 키워드 인수에 대한 값으로 규칙에서 나중에 지정할 수 있습니다.

다음 표에는 byte_extract 키워드에 정의되는 변수를 지정할 수 있는 키워드 인수가 나열되어 있습니다.

표 36-51 byte_extract 변수를 허용하는 인수

키워드	인수	참조 섹션
content	Depth, Offset, Distance, Within	36-17페이지의 내용 일치 제한
byte_jump	Offset	36-30페이지의 byte_jump
byte_test	Offset, Value	36-33페이지의 byte_test
isdataat	Offset	36-81페이지의 isdataat

byte_extract를 사용하려면

액세스: Admin/Intrusion Admin

1단계 Create Rule 페이지의 드롭다운 목록에서 byte_extract를 선택하고 **Add Option**을 클릭합니다. 마지막으로 선택한 키워드 아래에 byte_extract 섹션이 나타납니다.

규칙 키워드로 능동 응답 시작

라이센스: 보호

시스템은 트리거된 TCP 규칙에 대한 응답에서 또는 트리거된 UDP 규칙에 대한 응답에서 TCP 연결을 종료하기 위해 능동 응답을 시작할 수 있습니다. 능동 응답을 시작하기 위한 별도의 접근법을 제공하는 두 가지 키워드가 있습니다. 패킷이 두 키워드 중 하나가 포함된 규칙을 트리거하면 시스템은 단일 능동 응답을 시작합니다. 또한 패시브 구축에서 사용할 능동 응답 인터페이스 및 시도할 TCP 재설정 횟수를 구성하려면 config response 명령을 사용할 수 있습니다.

연결 또는 세션에 영향을 주기 위해 재설정이 제시간에 도달할 수 있을 것이므로 능동 응답은 인라인 구축에서 가장 효과적입니다. 예를 들어 인라인 구축의 react 키워드에 대한 응답에서 시스템은 각 연결 끝부분에서 TCP 재설정(RST) 패킷을 트래픽에 직접 삽입하며, 이를 통해 연결이 종료됩니다.

몇 가지 이유 때문에 능동 응답은 방화벽을 대신하지 않습니다. 예를 들어 패시브 구축에서 시스템이 패킷을 삽입할 수 없으며, 공격자가 능동 응답을 무시하거나 회피하기로 선택했을 수 있습니다.

능동 응답은 다시 라우팅될 수 있으므로 시스템은 TCP 재설정이 TCP 재설정을 시작하도록 허용하지 않습니다. 이에 따라 능동 응답의 끝없는 시퀀스가 방지됩니다. 시스템은 또한 표준 방식을 유지하면서 ICMP 도달 불가 패킷이 ICMP 도달 불가 패킷을 시작하도록 허용하지 않습니다.

침입 규칙이 능동 응답을 트리거한 후 연결 또는 세션에서 추가 트래픽을 탐지하도록 TCP 스트림 프리프로세서를 구성할 수 있습니다. 프리프로세서는 추가 트래픽을 탐지하면 지정된 최대값까지 연결 또는 세션의 양쪽 끝으로 추가 능동 응답을 전송합니다. 자세한 내용은 29-3페이지의 침입 삭제 규칙으로 능동 응답 시작을/를 참조하십시오.

능동 응답을 시작하는 데 사용할 수 있는 키워드와 관련된 정보는 다음 절을 참조하십시오.

- 36-86페이지의 유형 및 방향별로 능동 응답 시작
- 36-87페이지의 TCP 재설정 전에 HTML 페이지 보내기
- 36-88페이지의 능동 응답 재설정 시도 및 인터페이스 설정

유형 및 방향별로 능동 응답 시작

라이센스: 보호

규칙 헤더에서 TCP 프로토콜을 지정하는지 UDP 프로토콜을 지정하는지에 따라 TCP 연결 또는 UDP 세션에 적극적으로 응답하려면 `resp` 키워드를 사용할 수 있습니다. 자세한 내용은 36-4페이지의 프로토콜 지정을/를 참조하십시오.

키워드 인수를 사용하여 패킷 방향을 지정하고, 능동 응답으로 TCP 재설정(RST) 패킷을 사용할지 ICMP 도달 불가 패킷을 사용할지를 지정할 수 있습니다.

TCP 연결을 종료하려면 TCP 재설정 또는 ICMP 도달 불가 인수를 사용할 수 있습니다. UDP 세션을 닫으려면 ICMP 도달 불가 인수만 사용할 수 있습니다.

서로 다른 TCP 재설정 인수를 사용하면 능동 응답의 타겟을 패킷 소스, 목적지 또는 둘 다로 지정할 수도 있습니다. 모든 ICMP 도달 불가 인수는 패킷 소스를 타겟으로 삼으며, 사용자는 ICMP 네트워크, 호스트, 포트 도달 불가 패킷을 사용할지 셋을 모두 사용할지를 지정할 수 있습니다.

다음 표에는 규칙이 트리거될 때 FireSIGHT 시스템에서 무엇을 할지를 정확히 지정하기 위해 `resp` 키워드와 함께 사용할 수 있는 인수가 나열되어 있습니다.

표 36-52 resp 인수

인수	설명
reset_source	규칙을 트리거한 패킷을 전송한 엔드포인트로 TCP 재설정 패킷을 전달합니다. 또는 이전 버전과의 호환성을 위해 지원되는 `rst_snd`를 지정할 수 있습니다.
reset_dest	규칙을 트리거한 패킷의 의도된 목적지 엔드포인트로 TCP 재설정 패킷을 전달합니다. 또는 이전 버전과의 호환성을 위해 지원되는 `rst_rcv`를 지정할 수 있습니다.
reset_both	전송 및 수신 엔드포인트 모두로 TCP 재설정 패킷을 전달합니다. 또는 이전 버전과의 호환성을 위해 지원되는 `rst_all`을 지정할 수 있습니다.
icmp_net	ICMP 네트워크 도달 불가 메시지를 전송자에게 전달합니다.
icmp_host	ICMP 호스트 도달 불가 메시지를 전송자에게 전달합니다.
icmp_port	ICMP 포트 도달 불가 메시지를 전송자에게 전달합니다. 이 인수는 UDP 트래픽을 종료하는 데 사용됩니다.
icmp_all	다음 ICMP 메시지를 전송자에게 전달합니다. • 네트워크 도달 불가 • 호스트 도달 불가 • 포트 도달 불가

예를 들어 규칙이 트리거될 때 연결의 양쪽을 재설정하도록 규칙을 구성하려면 `resp` 키워드에 대한 값으로 `reset_both`를 사용합니다.

다음과 같이 여러 인수를 지정하려면 쉼표로 구분된 목록을 사용합니다.

`argument,argument,argument`

또한 `config response` 명령을 사용하여 패시브 구축에서 사용할 능동 응답 인터페이스 및 시도할 TCP 재설정 횟수를 구성하는 방법에 대한 자세한 내용은 36-88페이지의 능동 응답 재설정 시도 및 인터페이스 설정을/를 참조하십시오.

능동 응답을 지정하려면

액세스: Admin/Intrusion Admin

1단계 Create Rule 페이지의 드롭다운 목록에서 **resp**를 선택하고 **Add Option**을 클릭합니다.

`resp` 키워드가 나타납니다.

2단계 resp 인수 표에 나와 있는 인수를 **resp** 필드에서 지정합니다. 여러 인수를 지정하려면 쉼표로 구분된 목록을 사용합니다.

TCP 재설정 전에 HTML 페이지 보내기

라이센스: 보호

패킷이 규칙을 트리거할 때 기본 HTML 페이지를 TCP 연결 클라이언트로 전송하려면 `react` 키워드를 사용할 수 있습니다. HTML 페이지를 전송하면 시스템은 TCP 재설정 패킷을 사용하여 연결의 양쪽 끝에 대한 능동 응답을 시작합니다. `react` 키워드는 UDP 트래픽에 대해 능동 응답을 트리거하지 않습니다.

선택적으로, 다음과 같은 인수를 지정할 수 있습니다.

`msg`

패킷이 `msg` 인수를 사용하는 `react` 규칙을 트리거하면 HTML 페이지에 규칙 이벤트 메시지가 포함됩니다. 이벤트 메시지 필드에 대한 설명은 36-2페이지의 규칙 구조 이해을/를 참조하십시오.

`msg` 인수를 지정하지 않으면 HTML 페이지에 다음 메시지가 포함됩니다.

```
You are attempting to access a forbidden site.
Consult your system administrator for details.
```

참고 능동 응답은 다시 라우팅되므로 HTML 응답 페이지가 `react` 규칙을 트리거하지 않도록 해야 합니다. 이로 인해 능동 응답의 끝없는 시퀀스가 발생할 수 있습니다. Cisco에서는 `react` 규칙을 프로덕션 환경에서 활성화하기 전에 폭넓게 테스트해볼 것을 권장합니다.

또한 `config response` 명령을 사용하여 패시브 구축에서 사용할 능동 응답 인터페이스 및 시도할 TCP 재설정 횟수를 구성하는 방법에 대한 자세한 내용은 36-88페이지의 능동 응답 재설정 시도 및 인터페이스 설정을/를 참조하십시오.

능동 응답을 시작하기 전에 HTML 페이지를 전송하려면

액세스: Admin/Intrusion Admin

1단계 Create Rule 페이지의 드롭다운 목록에서 **react**를 선택하고 **Add Option**을 클릭합니다.

`react` 키워드가 나타납니다.

2단계 2가지 옵션이 있습니다.

- 연결이 종료되기 전에 규칙에 대해 구성된 이벤트 메시지를 포함하는 HTML 페이지를 클라이언트로 전송하려면 **react** 필드에 `msg`를 입력합니다.
- 연결이 종료되기 전에 다음과 같은 기본 메시지를 포함하는 HTML 페이지를 클라이언트로 전송하려면 **react** 필드를 비워둡니다.

```
You are attempting to access a forbidden site.
Consult your system administrator for details
```

능동 응답 재설정 시도 및 인터페이스 설정

라이센스: 보호

resp 및 react 규칙에 의해 시작되는 TCP 재설정의 동작을 더 구성하려면 **config response** 명령을 사용할 수 있습니다. 이 명령도 삭제 규칙에 의해 시작되는 능동 응답에 영향을 줍니다. 자세한 내용은 29-3페이지의 침입 삭제 규칙으로 능동 응답 시작을/를 참조하십시오.

USER_CONF 고급 변수에서 별도의 줄에 삽입하여 **config response** 명령을 사용합니다. USER_CONF 변수 사용에 대한 자세한 내용은 3-32페이지의 고급 변수 이해을/를 참조하십시오.

주의 기능 설명에 나와 있거나 지원 팀에서 안내한 경우가 아니면 침입 정책 기능을 구성하는 데 USER_CONF 고급 변수를 사용하지 **마십시오**. 컨피그레이션이 충돌하거나 중복되면 시스템이 중단됩니다.

능동 응답 재설정 시도, 능동 응답 인터페이스 또는 둘 모두를 지정하려면

액세스: Admin/Intrusion Admin

1단계 능동 응답의 횟수만 지정할지, 능동 응답 인터페이스만 지정할지, 아니면 둘 모두를 지정할지에 따라 USER_CONF 고급 변수에서 별도의 줄에 config response 명령의 형식을 삽입합니다. 다음 옵션을 이용할 수 있습니다.

- 능동 응답 시도의 횟수만 지정하려면 다음 명령을 입력합니다.
  `config response: attempts att`

  예: `config response: attempts 10`
- 능동 응답 인터페이스만 지정하려면 다음 명령을 입력합니다.
  `config response: device dev`

  예: `config response: device eth0`
- 능동 응답 시도의 횟수와 능동 응답 인터페이스를 모두 지정하려면 다음 명령을 입력합니다.
  `config response: attempts att, device dev`

  예: `config response: attempts 10, device eth0`

  여기서 각 항목은 다음을 나타냅니다.

  *att*는 수신 호스트가 패킷을 허용하도록 현재 연결 창 내에서 각 TCP 재설정 패킷을 실행하기 위한 1~20의 시도 횟수입니다. 이러한 연속 *수행*은 패시브 구축에서만 유용합니다. 인라인 구축에서는 시스템이 트리거링 패킷 대신 스트림에 재설정 패킷을 직접 삽입합니다. 시스템은 ICMP 도달 가능 능동 응답을 하나만 전송합니다.

  *dev*는 시스템이 패시브 구축에서 능동 응답을 전송하거나 인라인 구축에서 능동 응답을 삽입하도록 할 대체 인터페이스입니다.

이벤트 필터링

라이센스: 보호

지정된 시간 내에 지정된 패킷 수가 규칙을 트리거하지 않는 한 규칙의 이벤트 생성을 방지하려면 `detection_filter` 키워드를 사용할 수 있습니다. 이 키워드는 규칙의 때 이른 이벤트 생성을 중지합니다. 예를 들어, 몇 초 내에 로그인 시도가 2~3번 실패할 수는 있지만 같은 시간 내에 다수의 시도가 발생하면 무차별 암호 대입 공격(brute force attack)을 나타내는 것일 수 있습니다.

`detection_filter` 키워드에는 소스 또는 목적지 IP 주소를 추적하는지 여부, 이벤트 트리거 전에 탐지 기준을 충족해야 하는 횟수, 카운트를 지속해야 할 기간 등을 정의하는 인수가 필요합니다.

이벤트의 트리거를 지연시키려면 다음 구문을 사용합니다.

```
track by_src/by_dst, count count, seconds number_of_seconds
```

`track` 인수는 규칙의 탐지 기준을 충족하는 패킷의 수를 셀 때 패킷의 소스 또는 목적지 IP 주소를 사용할지 여부를 지정합니다. 시스템이 이벤트 인스턴스를 추적하는 방법을 지정하려면 다음 표에 설명된 인수 값 중에서 선택합니다.

표 36-53 detection_filter 추적 인수

인수	설명
by_src	소스 IP 주소별 탐지 기준 카운트
by_dst	목적지 IP 주소별 탐지 기준 카운트

`count` 인수는 규칙이 이벤트를 생성하기 전 지정된 시간 내에 지정된 IP 주소에 대한 규칙을 트리거해야 하는 패킷의 수를 지정합니다.

`seconds` 인수는 규칙이 이벤트를 생성하기 전에 지정된 패킷 수가 규칙을 트리거해야 하는 시간(초)을 지정합니다.

패킷에서 내용 `foo`를 검색하고 `detection_filter` 키워드를 다음 인수와 함께 사용하는 규칙이 있다고 가정해보겠습니다.

```
track by_src, count 10, seconds 20
```

이 예에서는 지정된 소스 IP 주소에서 20초 이내에 10개의 패킷에서 `foo`를 탐지할 때까지 규칙은 이벤트를 생성하지 않습니다. 시스템이 처음 20초 내에 `foo`가 포함된 패킷을 7개만 탐지하면 이벤트가 생성되지 않습니다. 그러나 처음 20초 동안 `foo`가 40번 발생하면 규칙은 이벤트를 30번 생성하며, 20초가 경과되면 카운트가 다시 시작됩니다.

임계값 및 detection_filter 키워드 비교

사용되지 않는 `threshold` 키워드를 `detection_filter` 키워드가 대신합니다. 이전 버전과의 호환성을 위해 `threshold` 키워드는 계속 지원되며, 침입 정책 내에 설정한 임계값과 동일하게 작동합니다.

`detection_filter` 키워드는 패킷이 규칙을 트리거하기 전에 적용되는 탐지 기능입니다. 규칙은 지정된 패킷 카운트 전에 탐지된 트리거링 패킷에 대해 이벤트를 생성하지 않으며, 인라인 구축에서는 규칙이 패킷을 삭제하도록 설정된 경우 해당 패킷을 삭제하지 않습니다. 반대로, 규칙은 규칙을 트리거하고 지정된 패킷 카운트 뒤에 발생하는 패킷에 대해서는 이벤트를 생성하며, 인라인 구축에서는 규칙이 패킷을 삭제하도록 설정된 경우 해당 패킷을 삭제합니다.

임계값 지정은 탐지 작업으로 귀결되지 않는 이벤트 알림 기능으로, 패킷이 이벤트를 트리거한 후 적용됩니다. 인라인 구축에서, 패킷을 삭제하도록 설정된 규칙은 규칙 임계값과 상관없이 규칙을 트리거하는 모든 패킷을 삭제합니다.

침입 정책에서 침입 이벤트 임계값 지정, 침입 이벤트 억제, 속도 기반 공격 방지 기능을 원하는 대로 조합하여 `detection_filter` 키워드를 사용할 수 있습니다. 사용되지 않는 `threshold` 키워드를 침입 정책에서 침입 이벤트 임계값 지정 기능과 함께 사용하는 가져온 로컬 규칙을 활성화하면 정책 검증이 실패합니다. 자세한 내용은 32-22페이지의 이벤트 임계값 구성, 32-26페이지의 침입 정책당 억제 구성, 32-31페이지의 동적 규칙 상태 설정 및 66-20페이지의 로컬 규칙 파일 가져오기을/를 참조하십시오.

공격 이후 트래픽 평가

라이센스: 보호

호스트 또는 세션에 대한 추가 트래픽을 로깅하도록 시스템에 알리려면 `tag` 키워드를 사용합니다. `tag` 키워드를 사용하여 캡처하려는 트래픽의 양과 유형을 지정하려면 다음 구문을 사용합니다.

`tagging_type, count, metric, optional_direction`

다음 세 개의 표에서는 사용 가능한 기타 인수에 대해 설명합니다.

두 가지 태그 지정 유형 중에서 선택할 수 있습니다. 다음 표에서는 두 가지 태그 지정 유형에 대해 설명합니다. 침입 규칙에서 규칙 헤더 옵션만 구성하는 경우, 세션 태그 인수 유형을 선택하면 시스템은 동일한 세션의 패킷을 마치 다른 세션에서 온 것처럼 로깅합니다. 동일한 세션에서 온 패킷을 그룹화하려면 동일한 침입 규칙 내에서 하나 이상의 규칙 옵션(예: `flag` 키워드 또는 `content` 키워드)을 구성하십시오.

표 36-54 태그 인수

인수	설명
session	규칙을 트리거한 세션의 패킷을 로깅합니다.
host	규칙을 트리거한 패킷을 전송한 호스트의 패킷을 로깅합니다. 호스트에서 오는(`src`) 또는 호스트로 가는(`dst`) 트래픽만 로깅하려면 방향 수정자를 추가할 수 있습니다.

로깅할 트래픽의 양을 나타내려면 다음 인수를 사용합니다.

표 36-55 카운트 인수

인수	설명
count	규칙이 트리거된 후 로깅할 패킷의 수 또는 시간(초). 이 측정 단위는 카운트 인수 뒤에 오는 메트릭 인수로 지정됩니다.

시간을 기준으로 또는 트래픽의 양을 기준으로 로깅하기 위해 사용할 메트릭을 다음 표에 설명된 인수 중에서 선택합니다.

주의 고대역 네트워크에서는 초당 패킷 수가 수천 개에 이를 수 있으며 많은 양의 패킷에 태깅하려면 성능이 크게 저하될 수 있으므로, 네트워크 환경에 맞게 이 설정을 조정하십시오.

표 36-56 로깅 메트릭 인수

인수	설명
packets	규칙이 트리거된 후 카운트에 의해 지정된 패킷의 수를 로깅합니다.
seconds	규칙이 트리거된 후 카운트에 의해 지정된 시간(초) 동안의 트래픽을 로깅합니다.

예를 들어 다음 tag 키워드 값의 규칙이 트리거되면

```
host, 30, seconds, dst
```

클라이언트에서 호스트로 다음 30초 동안 전송되는 모든 패킷이 로깅됩니다.

여러 패킷에서 수행되는 공격 탐지

라이센스: 보호

세션에 상태 이름을 할당하려면 flowbits 키워드를 사용합니다. 전에 명명된 상태에 따라 세션에서 후속 패킷을 분석함으로써 시스템은 단일 세션의 여러 패킷에서 수행되는 익스플로잇을 탐지하고 알릴 수 있습니다.

flowbits 상태 이름은 세션의 특정 부분에서 패킷에 할당된 사용자 정의 레이블입니다. 패킷 내용을 기반으로 하는 상태 이름으로 패킷에 레이블을 지정할 수 있습니다. 이렇게 하면 악의적인 패킷과 알리지 않으려는 패킷을 구분할 수 있습니다. 관리되는 디바이스당 최대 1024개의 상태 이름을 정의할 수 있습니다. 예를 들어 성공적으로 로그인해야만 발생함을 알고 있는 악의적인 패킷에 대해 알리려는 경우 flowbits 키워드를 사용하면, 악의적인 패킷에만 집중할 수 있도록 초기 로그인 시도를 구성하는 패킷을 필터링할 수 있습니다. 이렇게 하려면 먼저 설정된 로그인이 있는 세션의 모든 패킷에 logged_in 상태로 레이블을 지정하는 규칙을 생성한 다음, flowbits가 첫 번째 규칙에서 설정한 상태의 패킷을 검사하고 해당 패킷에 대해서만 작업을 수행하는 두 번째 규칙을 생성하면 됩니다. 사용자가 로그인했는지를 확인하기 위해 flowbits를 사용하는 예를 보려면 36-93페이지의 state_name을 사용하는 flowbits 예을/를 참조하십시오.

선택적인 *그룹 이름*을 사용하면 상태 그룹에 상태 이름을 포함할 수 있습니다. 하나의 상태 이름이 여러 그룹에 속할 수 있습니다. 그룹과 연결되지 않은 상태는 상호 배타적이지 않으므로, 그룹과 연결되지 않은 상태를 트리거하고 설정하는 규칙은 현재 설정된 다른 상태에 영향을 미치지 않습니다. 그룹에 상태 이름을 포함하여 동일한 그룹에 있는 또 다른 상태의 설정을 해제함으로써 오탐을 방지하는 방법을 보여주는 예는 36-93페이지의 오탐이 된 flowbits 예을/를 참조하십시오.

다음 표에서는 flowbits 키워드에서 사용할 수 있는 연산자, 상태 및 그룹의 다양한 조합에 대해 설명합니다. 상태 이름에는 영숫자 문자, 마침표(.), 밑줄(_) 및 대시(-)를 포함할 수 있습니다.

표 36-57 flowbits 옵션

운영자	상태 옵션	그룹	설명
set	state_name	옵션	패킷에 대해 하나의 지정된 상태를 설정합니다. 그룹이 정의된 경우 지정된 그룹에서 하나의 상태를 설정합니다.
	state_name&state_name	옵션	패킷에 대해 여러 지정된 상태를 설정합니다. 그룹이 정의된 경우 지정된 그룹에서 여러 상태를 설정합니다.
setx	state_name	필수	패킷에 대해 지정된 하나의 그룹에서 지정된 하나의 상태를 설정하고, 그룹의 다른 모든 상태를 설정 취소합니다.
	state_name&state_name	필수	패킷에 대해 지정된 여러 그룹에서 지정된 여러 상태를 설정하고, 그룹의 다른 모든 상태를 설정 취소합니다.
unset	state_name	그룹 없음	패킷에 대해 하나의 지정된 상태를 설정 취소합니다.
	state_name&state_name	그룹 없음	패킷에 대해 여러 지정된 상태를 설정 취소합니다.
	all	필수	지정된 그룹에서 모든 상태를 설정 취소합니다.

표 36-57 flowbits 옵션(계속)

운영자	상태 옵션	그룹	설명
toggle	state_name	그룹 없음	설정된 경우 하나의 지정된 상태를 설정 취소하고, 설정 취소된 경우 하나의 지정된 상태를 설정합니다.
	state_name&state_name	그룹 없음	설정된 경우 여러 지정된 상태를 설정 취소하고, 설정 취소된 경우 여러 지정된 상태를 설정합니다.
	all	필수	지정된 그룹에서 설정된 모든 상태를 설정 취소하고, 지정된 그룹에서 설정 취소된 모든 상태를 설정합니다.
isset	state_name	그룹 없음	하나의 지정된 상태가 패킷에 설정되어 있는지 확인합니다.
	state_name&state_name	그룹 없음	여러 지정된 상태가 패킷에 설정되어 있는지 확인합니다.
	state_name|state_name	그룹 없음	여러 지정된 상태 중 하나가 패킷에 설정되어 있는지 확인합니다.
	any	필수	지정된 그룹에 어느 한 상태가 설정되어 있는지 확인합니다.
	all	필수	지정된 그룹에 모든 상태가 설정되어 있는지 확인합니다.
isnotset	state_name	그룹 없음	하나의 지정된 상태가 패킷에 설정되어 있지 않은지 확인합니다.
	state_name&state_name	그룹 없음	여러 지정된 상태가 패킷에 설정되어 있지 않은지 확인합니다.
	state_name|state_name	그룹 없음	여러 지정된 상태 중 하나가 패킷에 설정되어 있지 않은지 확인합니다.
	any	필수	패킷에 어느 한 상태가 설정되어 있지 않은지 확인합니다.
	all	필수	패킷에 모든 상태가 설정되어 있지 않은지 확인합니다.
reset	(상태 없음)	옵션	모든 패킷의 모든 상태를 설정 취소합니다. 그룹이 지정된 경우 그룹의 모든 상태를 설정 취소합니다.
noalert	(상태 없음)	그룹 없음	이벤트 생성을 억제하려면 다른 연산자와 함께 사용하십시오.

flowbits 키워드를 사용할 때에는 다음에 유의하십시오.

- setx 연산자를 사용할 때 지정된 상태는 지정된 그룹에만 속할 수 있고, 다른 그룹에는 속할 수 없습니다.
- 서로 다른 상태 및 각 인스턴스의 동일한 그룹을 지정하려면 setx 연산자를 여러 번 정의할 수 있습니다.
- setx 연산자를 사용하여 그룹을 지정할 경우 해당 지정된 그룹에서 set, toggle 또는 unset 연산자는 사용할 수 없습니다.
- 상태가 그룹에 있는지 여부와 상관없이 isset 및 isnotset 연산자는 지정된 상태를 평가합니다.
- 침입 정책을 저장하고 침입 정책을 다시 적용하고 액세스 제어 정책을 적용하는 동안(액세스 제어 정책이 침입 정책 하나를 참조하든 여러 개를 참조하든 상관없이), 지정된 그룹 **없이** isset 또는 isnotset 연산자가 포함된 규칙을 활성화하고 해당 상태 이름과 프로토콜에 대한 flowbits 할당(set, setx, unset, toggle)에 영향을 주는 규칙을 하나 이상 활성화하지 않으면, 해당 상태 이름에 대한 flowbits 할당에 영향을 주는 모든 규칙이 활성화됩니다.
- 침입 정책을 저장하고 침입 정책을 다시 적용하고 액세스 제어 정책을 적용하는 동안(액세스 제어 정책이 침입 정책 하나를 참조하든 여러 개를 참조하든 상관없이), 지정된 그룹과 **함께** isset 또는 isnotset 연산자가 포함된 규칙을 활성화하면, flowbits 할당(set, setx, unset, toggle)에 영향을 주고 해당 그룹 이름을 정의하는 모든 규칙도 활성화됩니다.

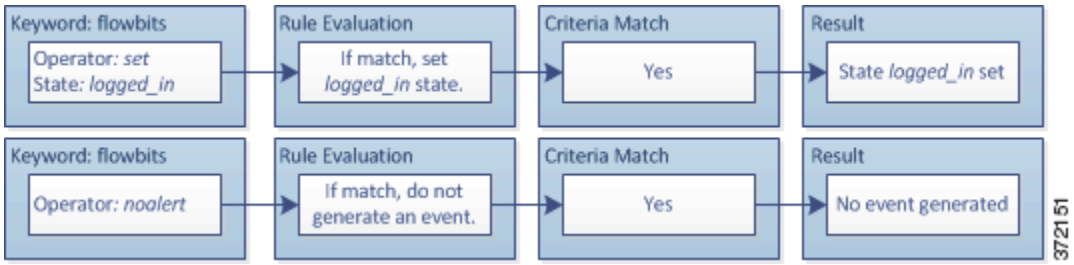
state_name을 사용하는 flowbits 예

Bugtraq ID #1110에 설명된 IMAP 취약성을 생각해 보십시오. 이 취약성은 IMAP의 구현, 특히 LIST, LSUB, RENAME, FIND 및 COPY 명령에 존재합니다. 그러나 취약성을 활용하려면 공격자는 IMAP 서버에 로그인해야 합니다. IMAP 서버로부터의 LOGIN 확인 및 이를 따르는 익스플로잇은 서로 다른 패킷에 있어야 하므로 이러한 익스플로잇을 포착하는 비 플로우 기반(non-flow-based) 규칙을 작성하기는 어렵습니다. `flowbits` 키워드를 사용하면, 사용자가 IMAP 서버에 로그인했는지를 추적하고, 로그인한 경우 공격 중 하나가 탐지될 때 이벤트를 생성하는 일련의 규칙을 작성할 수 있습니다. 사용자가 로그인하지 않았으면 공격은 취약성을 악용할 수 없고 이벤트가 생성되지 않습니다.

이어지는 두 가지 규칙 프래그먼트가 이 예를 설명합니다. 첫 번째 규칙 프래그먼트는 IMAP 서버로부터 IMAP 로그인 확인을 찾습니다.

```
alert tcp any 143 -> any any (msg:"IMAP login"; content:"OK
LOGIN"; flowbits:set,logged_in; flowbits:noalert;)
```

다음 다이어그램은 위 규칙 프래그먼트에 나오는 `flowbits` 키워드의 효과를 보여줍니다.

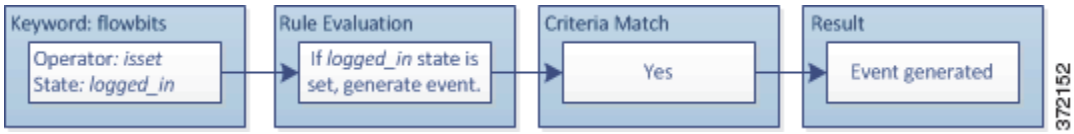


IMAP 서버에 많은 무해한 로그인 세션이 있을 것이므로 `flowbits:set`은 `logged_in`의 상태를 설정하는 반면 `flowbits:noalert`은 알림을 억제합니다.

다음 규칙 프래그먼트는 LIST 문자열을 찾지만, 세션의 일부 이전 패킷의 결과로 logged_in 상태가 설정되지 않았다면 이벤트를 생성하지 않습니다.

```
alert tcp any any -> any 143 (msg:"IMAP LIST";
content:"LIST"; flowbits:isset,logged_in;)
```

다음 다이어그램은 위 규칙 프래그먼트에 나오는 `flowbits` 키워드의 효과를 보여줍니다.



이 경우 이전 패킷이 첫 번째 프래그먼트가 포함된 규칙을 트리거했다면, 두 번째 프래그먼트가 포함된 규칙이 트리거되고 이벤트가 생성됩니다.

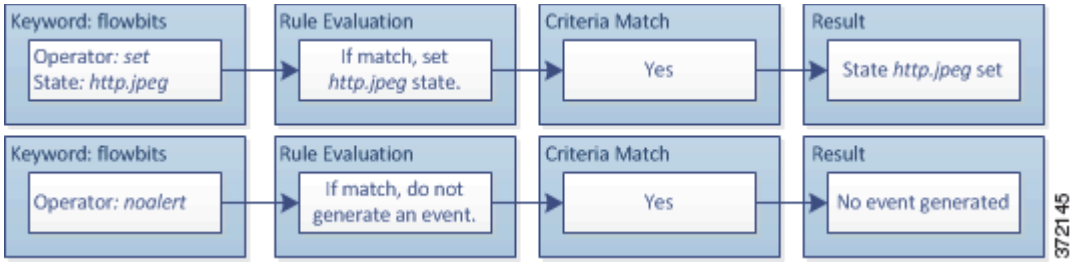
오탐이 된 flowbits 예

그룹의 서로 다른 규칙에 설정된 서로 다른 상태 이름을 포함하면, 후속 패킷의 내용이 더 이상 상태가 유효하지 않은 규칙과 일치하는 경우 발생할 수도 있을 오탐 이벤트를 방지할 수 있습니다. 다음 예는 그룹에 여러 상태 이름을 포함하지 않을 때 어떻게 오탐이 발생할 수 있는지를 보여줍니다.

단일 세션 중에 다음의 세 규칙 프래그먼트가 표시된 순서로 트리거되는 경우를 가정해보겠습니다.

```
(msg:"JPEG transfer"; content:"image/";pcre:"/^Content-
Type\x3a(\s*|\s*\r?\n\s+)image\x2fp?jpe?g/smi";
flowbits:set,http.jpeg; flowbits:noalert;)
```

다음 다이어그램은 위 규칙 프래그먼트에 나오는 flowbits 키워드의 효과를 보여줍니다.

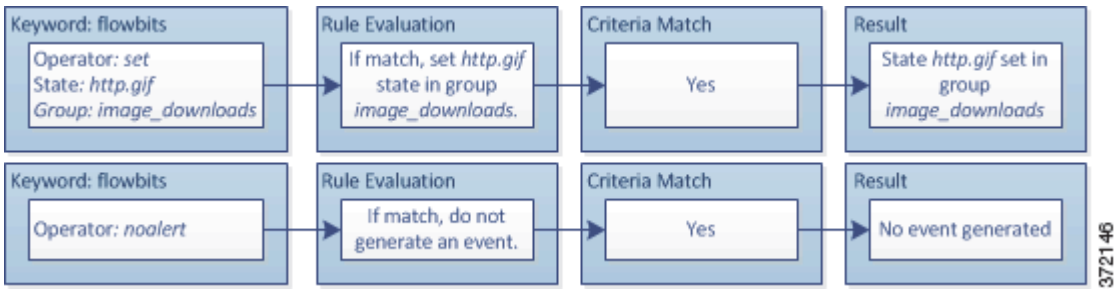


첫 번째 규칙 프래그먼트의 content 및 pcre 키워드는 JPEG 파일 다운로드를 매칭하고, flowbits:set,http.jpeg는 http.jpeg flowbits 상태를 설정하며, flowbits:noalert은 규칙의 이벤트 생성을 중지합니다. 규칙의 목적은 파일 다운로드를 탐지하고, 하나 이상의 동반 규칙이 악의적인 내용과 결합된 상태 이름을 테스트하고 악의적인 내용이 탐지될 때 이벤트를 생성할 수 있도록 flowbits 상태를 설정하는 것이기 때문에 이벤트가 생성되지 않습니다.

다음 규칙 프래그먼트는 위의 JPEG 파일 다운로드에 이어 GIF 파일 다운로드를 탐지합니다.

```
(msg:"GIF transfer"; content:"image/"; pcre:"/^Content-
Type\x3a(\s*|\s*\r?\n\s+)image\x2fgif/smi";
flowbits:set,http.tif,image_downloads; flowbits:noalert;)
```

다음 다이어그램은 위 규칙 프래그먼트에 나오는 flowbits 키워드의 효과를 보여줍니다.

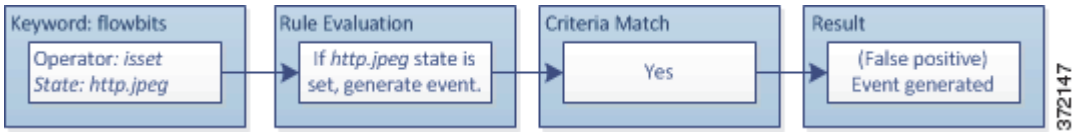


두 번째 규칙의 content 및 pcre 키워드는 GIF 파일 다운로드를 매칭하고, flowbits:set,http.tif는 http.tif flowbits 상태를 설정하며, flowbits:noalert은 규칙의 이벤트 생성을 중지합니다. 첫 번째 규칙 프래그먼트에 의해 설정된 http.jpeg 상태는 더 이상 필요하지 않더라도 계속 설정 상태가 유지됩니다. 후속 GIF 다운로드가 탐지되면 JPEG 다운로드를 종료해야 하기 때문입니다.

세 번째 규칙 프래그먼트는 첫 번째 규칙 프래그먼트와 짝을 이룹니다.

```
(msg:"JPEG exploit";
flowbits:isset,http.jpeg;content:"|FF|"; pcre:"
/\xFF[\xE1\xE2\xED\xFE]\x00[\x00\x01]/";)
```

다음 다이어그램은 위 규칙 프래그먼트에 나오는 flowbits 키워드의 효과를 보여줍니다.



세 번째 규칙 프래그먼트에서 flowbits:isset,http.jpeg는 이제 관련이 없는 http.jpeg 상태가 설정되었는지, 그리고 content 및 pcre가 JPEG 파일에서는 악성이지만 GIF 파일에서는 악성이 아닌 내용과 일치하는지를 확인합니다. 세 번째 규칙 프래그먼트는 JPEG 파일에 존재하지 않는 익스플로잇에 대해 오탐 이벤트가 됩니다.

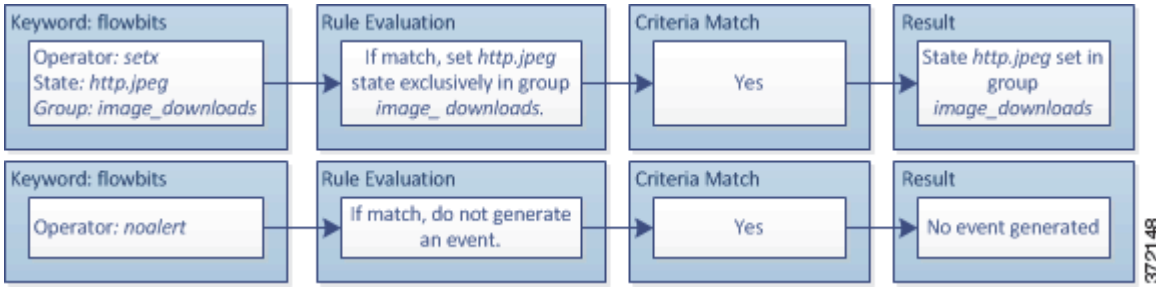
오탐 방지를 위한 flowbits 예

다음 예는 그룹에 상태 이름을 포함하고 `setx` 연산자를 사용하여 오탐을 방지하는 방법을 보여줍니다.

위의 예와 같지만, 이제 처음 두 규칙이 동일한 상태 그룹에 두 개의 서로 다른 상태 이름을 가지고 있는 경우를 가정해보겠습니다.

```
(msg:"JPEG transfer"; content:"image/";pcre:"/^Content-
Type\x3a(\s*|\s*\r?\n\s+)image\x2fp?jpe?g/smi";
flowbits:setx,http.jpeg,image_downloads; flowbits:noalert;)
```

다음 다이어그램은 위 규칙 프래그먼트에 나오는 `flowbits` 키워드의 효과를 보여줍니다.

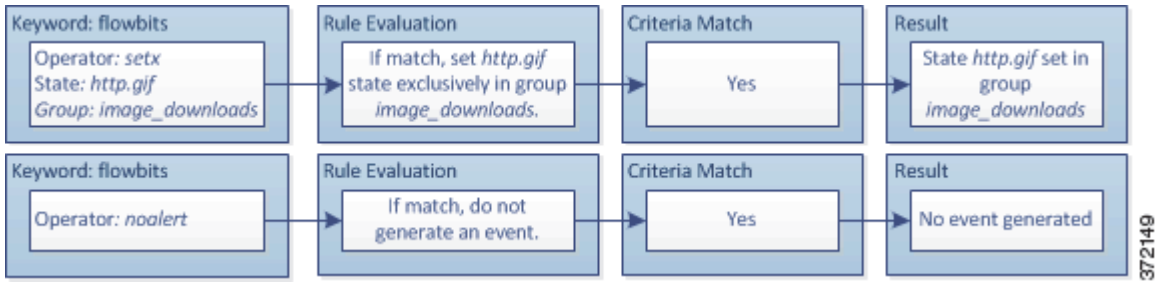


첫 번째 규칙 프래그먼트가 JPEG 파일 다운로드를 탐지하면 `flowbits:setx,http.jpeg,image_downloads` 키워드는 `flowbits` 상태를 `http.jpeg`로 설정하고 `image_downloads` 그룹에 상태를 포함합니다.

그러면 다음 규칙이 후속 GIF 파일 다운로드를 탐지합니다.

```
(msg:"GIF transfer"; content:"image/"; pcre:"/^Content-
Type\x3a(\s*|\s*\r?\n\s+)image\x2fgif/smi";
flowbits:setx,http.tif,image_downloads; flowbits:noalert;)
```

다음 다이어그램은 위 규칙 프래그먼트에 나오는 `flowbits` 키워드의 효과를 보여줍니다.

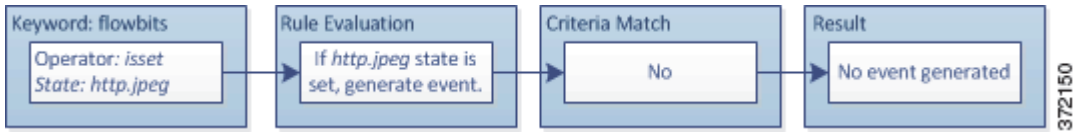


두 번째 규칙 프래그먼트가 GIF 다운로드와 일치하면 `flowbits:setx,http.tif,image_downloads` 키워드는 `http.tif` `flowbits` 상태를 설정하고 그룹의 다른 상태인 `http.jpeg`를 설정 취소합니다.

세 번째 규칙 프래그먼트는 오탐으로 귀결되지 않습니다.

```
(msg:"JPEG exploit";
flowbits:isset,http.jpeg;content:"|FF|"; pcre:"/
\xFF[\xE1\xE2\xED\xFE]\x00[\x00\x01]/";)
```

다음 다이어그램은 위 규칙 프래그먼트에 나오는 `flowbits` 키워드의 효과를 보여줍니다.



`flowbits:isset,http.jpeg`는 거짓이므로 규칙 엔진은 규칙 처리를 중지하며 이벤트가 생성되지 않습니다. 따라서 GIF 파일의 내용이 JPEG 파일의 익스플로잇 내용과 일치하는 경우에도 오탐을 피할 수 있습니다.

HTTP 인코딩 유형 및 위치에서 이벤트 생성

라이센스: 보호

HTTP URI, HTTP 헤더의 non-cookie 데이터, HTTP 요청 헤더의 쿠키 또는 HTTP 응답의 set-cookie 데이터에서 표준화 이전의 HTTP 요청 또는 응답을 인코딩하는 유형에 대한 이벤트를 생성하려면 `http_encode` 키워드를 사용할 수 있습니다.

`http_encode` 키워드를 사용하여 규칙에 대한 일치를 반환하기 위해 HTTP 응답 또는 HTTP 쿠키를 검사하려면 HTTP Inspect 프리프로세서를 구성해야 합니다. 자세한 내용은 27-30페이지의 HTTP 트래픽 디코딩 및 27-32페이지의 서버 레벨 HTTP 표준화 옵션 선택을/를 참조하십시오.

인코딩 유형에 대한 이벤트를 트리거하려면 침입 규칙의 `http_encode` 키워드에 대한 HTTP Inspect 프리프로세서 컨피그레이션에서 각각의 특정 인코딩 유형에 대해 디코딩 및 알림 옵션을 활성화해야 합니다. 자세한 내용은 27-40페이지의 서버 레벨 HTTP 표준화 인코딩 옵션 선택을/를 참조하십시오.

base36 인코딩 유형은 사용되지 않습니다. 이전 버전과의 호환성을 위해 기존 규칙에서는 base36 인수가 허용되지만, 규칙 엔진이 base36 트래픽을 검사하지는 않습니다.

다음 표에서는 이 옵션이 HTTP URI, 헤더, 쿠키 및 set-cookies에 대해 이벤트를 생성할 수 있는 인코딩 유형에 대해 설명합니다.

표 36-58 http_encode 인코딩 유형

인코딩 유형	설명
utf8	HTTP Inspect 프리프로세서에서 디코딩하도록 UTF-8 인코딩 유형이 활성화된 경우 지정된 위치에서 이 인코딩을 탐지합니다.
double_encode	HTTP Inspect 프리프로세서에서 디코딩하도록 double 인코딩 유형이 활성화된 경우 지정된 위치에서 이 인코딩을 탐지합니다.
non_ascii	non-ASCII 문자가 탐지되지만 탐지된 인코딩 유형이 활성화되지 않은 경우 지정된 위치에서 non-ASCII 문자를 탐지합니다.
uencode	HTTP Inspect 프리프로세서에서 디코딩하도록 Microsoft %u 인코딩 유형이 활성화된 경우 지정된 위치에서 이 인코딩을 탐지합니다.
bare_byte	HTTP Inspect 프리프로세서에서 디코딩하도록 bare byte 인코딩 유형이 활성화된 경우 지정된 위치에서 이 인코딩을 탐지합니다.

침입 규칙에서 HTTP 인코딩 유형 및 위치를 식별하려면

액세스: Admin/Intrusion Admin

1단계 규칙에 `http_encode` 키워드를 추가합니다.

2단계 HTTP URI, 헤더 또는 쿠키(set-cookie 포함)에서 지정된 인코딩 유형을 검색할지 여부를 **Encoding Location** 드롭다운 목록에서 선택합니다.

3단계 다음 형식 중 하나를 사용하여 하나 이상의 인코딩 유형을 지정합니다.

```
encode_type
encode_type|encode_type|encode_type...
!encode_type
```

여기서 *encode_type*은 다음 중 하나입니다.

```
utf8, double_encode, non_ascii, uencode, bare_byte
```

부정(!) 및 OR(|) 연산자는 함께 사용할 수 없습니다.

4단계 선택적으로, 동일한 규칙에 여러 `http_encode` 키워드를 추가하고(AND) 각각에 대한 조건을 추가합니다. 예를 들어 다음 조건의 두 키워드를 입력합니다.

첫 번째 `http_encode` 키워드:

- **Encoding Location**: `HTTP URI`
- **Encoding Type**: `utf8`

추가 `http_encode` 키워드:

- **Encoding Location**: `HTTP URI`
- **Encoding Type**: `uencode`

예제 컨피그레이션에서는 HTTP URI에서 UTF-8 AND Microsoft IIS %u 인코딩을 검색합니다.

파일 유형 및 버전 탐지

라이센스: 보호

`file_type` 및 `file_group` 키워드를 사용하면 유형과 버전을 기반으로 FTP, HTTP, SMTP, IMAP, POP3 및 NetBIOS-ssn(SMB)을 통해 전송된 파일을 탐지할 수 있습니다. 단일 침입 규칙에서 `file_type` 또는 `file_group` 키워드를 둘 이상 사용하지 **마십시오**.

팁 VDB(취약성 데이터베이스)를 업데이트하면 규칙 편집기가 최신 파일 형식, 버전 및 그룹으로 채워집니다. 자세한 내용은 66-13페이지의 취약성 데이터베이스 업데이트을/를 참조하십시오.

`file_type` 또는 `file_group` 키워드와 일치하는 트래픽에 대한 침입 이벤트를 생성하려면 특정 프리프로세서를 **활성화해야** 합니다.

표 36-59 file_type and file_group 침입 이벤트 생성

전송 프로토콜	필수 프리프로세서 또는 프리프로세서 옵션
FTP	FTP/Telnet 프리프로세서 및 **Normalize TCP Payload** 인라인 표준화 프리프로세서 옵션. 27-18페이지의 FTP 및 텔넷 트래픽 디코딩 및 29-7페이지의 인라인 트래픽 표준화 참조.
HTTP	HTTP Inspect 프리프로세서. 27-30페이지의 HTTP 트래픽 디코딩 참조.
SMTP	SMTP 프리프로세서. 27-58페이지의 SMTP 트래픽 디코딩 참조.
IMAP	IMAP 프리프로세서. 27-52페이지의 IMAP 트래픽 디코딩 참조.
POP3	POP 프리프로세서. 27-55페이지의 POP 트래픽 디코딩 참조.
NetBIOS-ssn(SMB)	**SMB File Inspection** DCE/RPC 프리프로세서 옵션. 27-2페이지의 DCE/RPC 트래픽 디코딩 참조.

자세한 내용은 다음 절을 참조하십시오.

- 36-98페이지의 file_type
- 36-98페이지의 file_group

file_type

file_type 키워드를 사용하면 트래픽에서 탐지할 파일의 형식 및 버전을 지정할 수 있습니다. 파일 형식 인수(예: **JPEG** 및 **PDF**)는 트래픽에서 찾으려는 파일의 형식을 식별합니다.

참고 file_type 키워드를 동일한 침입 규칙의 또 다른 file_type 또는 file_group 키워드와 사용해서는 **안 됩니다**.

시스템은 기본적으로 **Any Version**을 선택하지만, 일부 파일 형식의 경우 트래픽에서 찾을 특정 파일 형식 버전을 식별하려면 버전 옵션(예: PDF 버전 **1.7**)을 선택할 수 있습니다.

최신 파일 형식 및 버전을 보고 구성하려면 VDB를 업데이트하십시오. 자세한 내용은 66-13페이지의 취약성 데이터베이스 업데이트을/를 참조하십시오.

침입 규칙에서 파일 형식 및 버전을 선택하려면

액세스: Admin/Intrusion Admin

1단계 Create Rule 페이지의 드롭다운 목록에서 **file_type**을 선택하고 **Add Option**을 클릭합니다.

file_type 키워드가 나타납니다.

2단계 드롭다운 목록에서 파일 형식을 하나 이상 선택합니다. 파일 형식을 선택하면 인수가 규칙에 자동으로 추가됩니다.

규칙에서 파일 형식 인수를 제거하려면 제거할 파일 형식 옆에 있는 삭제 아이콘( )을 클릭합니다.

3단계 선택적으로, 각 파일 형식의 대상 버전을 사용자 지정합니다. 시스템은 기본적으로 **Any Version**을 선택하지만, 일부 파일 형식의 경우 개별 대상 버전을 선택할 수 있습니다.

참고 VDB를 업데이트하면 규칙 편집기가 최신 파일 형식 및 버전으로 채워집니다. 사용자가 **Any Version**을 선택하면 시스템은 나중에 VDB 업데이트에 추가될 때 새 버전을 포함하도록 규칙을 구성합니다.

file_group

file_group 키워드를 사용하면 Cisco에서 정의한 유사한 파일 형식의 그룹(예: **multimedia** 또는 **audio**)을 트래픽에서 찾도록 선택할 수 있습니다. 파일 그룹은 또한 그룹의 각 파일 형식에 대해 Cisco 정의 버전을 포함합니다.

참고 file_group 키워드를 동일한 침입 규칙의 또 다른 file_group 또는 file_type 키워드와 사용해서는 **안 됩니다**.

최신 파일 그룹을 보고 구성하려면 VDB를 업데이트하십시오. 자세한 내용은 66-13페이지의 취약성 데이터베이스 업데이트을/를 참조하십시오.

침입 규칙에서 파일 그룹을 선택하려면

액세스: Admin/Intrusion Admin

1단계 Create Rule 페이지의 드롭다운 목록에서 **file_group**을 선택하고 **Add Option**을 클릭합니다.

`file_group` 키워드가 나타납니다.

2단계 선택적으로, 그룹의 파일 형식에 대한 버전 정보를 보려면 포인터를 파일 그룹 위로 이동하고 **(Show Version Info)**를 클릭합니다.

파일 그룹 정보가 버전을 표시하도록 확장됩니다.

3단계 규칙을 추가할 파일 그룹을 선택합니다.

특정 페이로드 유형 가리키기

라이센스: 보호

`file_data` 키워드는 `content`, `byte_jump`, `byte_test`, `pcre` 등의 기타 키워드에 사용할 수 있는 위치 인수에 대한 참조 역할을 하는 포인터를 제공합니다. 탐지된 트래픽은 `file_data` 키워드가 가리키는 데이터 형식을 결정합니다. 다음 페이로드 유형의 시작 부분을 가리키려면 `file_data` 키워드를 사용할 수 있습니다.

- HTTP 응답 본문

  HTTP 응답 패킷을 검사하려면 HTTP Inspect 프리프로세서를 활성화하고, HTTP 응답을 검사하도록 프리프로세서를 구성해야 합니다. 자세한 내용은 27-30페이지의 HTTP 트래픽 디코딩과 27-32페이지의 서버 레벨 HTTP 표준화 옵션 선택의 **Inspect HTTP Responses**을/를 참조하십시오. `file_data` 키워드는 HTTP Inspect 프리프로세서가 HTTP 응답 본문 데이터를 탐지하는지 여부를 매칭합니다.

- 압축되지 않은 gzip 파일 데이터

  HTTP 응답 본문에서 압축되지 않은 gzip 파일을 검사하려면 HTTP Inspect 프리프로세서를 활성화해야 하며, HTTP 응답을 검사하고 HTTP 응답 본문에서 gzip으로 압축된 파일을 압축 해제하도록 프리프로세서를 구성해야 합니다. 자세한 내용은 27-30페이지의 HTTP 트래픽 디코딩과 27-32페이지의 서버 레벨 HTTP 표준화 옵션 선택의 **Inspect HTTP Responses** 및 **Inspect Compressed Data** 옵션을/를 참조하십시오. `file_data` 키워드는 HTTP Inspect 프리프로세서가 HTTP 응답 본문에서 압축 해제된 gzip 데이터를 탐지하는지 여부를 매칭합니다.

- 표준화된 JavaScript

  표준화된 JavaScript 데이터를 검사하려면 HTTP Inspect 프리프로세서를 활성화하고, HTTP 응답을 검사하도록 프리프로세서를 구성해야 합니다. 자세한 내용은 27-30페이지의 HTTP 트래픽 디코딩과 27-32페이지의 서버 레벨 HTTP 표준화 옵션 선택의 **Inspect HTTP Responses**을/를 참조하십시오. `file_data` 키워드는 HTTP Inspect 프리프로세서가 응답 본문 데이터에서 JavaScript를 탐지하는지 여부를 매칭합니다.

- SMTP페 이로드

  SMTP 페이로드를 검사하려면 SMTP 프리프로세서를 활성화해야 합니다. 자세한 내용은 27-63페이지의 SMTP 디코딩 구성을/를 참조하십시오. `file_data` 키워드는 SMTP 프리프로세서가 SMTP 데이터를 탐지하는지 여부를 매칭합니다.

- SMTP, POP 또는 IMAP 트래픽의 인코딩된 이메일 첨부 파일

SMTP, POP 또는 IMAP 트래픽에서 이메일 첨부 파일을 검사하려면 각각 SMTP, POP 또는 IMAP 프리프로세서를 별도로 활성화하거나 임의의 조합으로 활성화해야 합니다. 그런 다음 각각의 활성화된 프리프로세서에 대해, 원하는 각 첨부 파일 인코딩 유형을 디코딩하도록 프리프로세서가 구성되어 있는지 확인해야 합니다. 각 프리프로세서에 대해 구성할 수 있는 첨부 파일 디코딩 옵션은 **Base64 Decoding Depth**, **7-Bit/8-Bit/Binary Decoding Depth**, **Quoted-Printable Decoding Depth** 및 **Unix-to-Unix Decoding Depth**입니다. 자세한 내용은 27-52페이지의 IMAP 트래픽 디코딩, 27-55페이지의 POP 트래픽 디코딩 및 27-58페이지의 SMTP 트래픽 디코딩을/를 참조하십시오.

하나의 규칙에 여러 `file_data` 키워드를 사용할 수 있습니다.

특정 페이로드 유형의 시작 부분을 가리키려면

액세스: Admin/Intrusion Admin

1단계 Create Rule 페이지의 드롭다운 목록에서 **file_data**를 선택하고 **Add Option**을 클릭합니다.

`file_data` 키워드가 나타납니다.

`file_data` 키워드에는 인수가 없습니다.

패킷 페이로드의 시작 부분 가리키기

라이센스: 보호

`pkt_data` 키워드는 `content`, `byte_jump`, `byte_test`, `pcre` 등의 기타 키워드에 사용할 수 있는 위치 인수에 대한 참조 역할을 하는 포인터를 제공합니다.

표준화된 FTP, 텔넷 또는 SMTP 트래픽이 탐지되면 `pkt_data` 키워드는 표준화된 패킷 페이로드의 시작 부분을 가리킵니다. 다른 트래픽이 탐지되면 `pkt_data` 키워드는 원시 TCP 또는 UDP 페이로드의 시작 부분을 가리킵니다.

침입 규칙으로 검사할 해당 트래픽을 표준화하려면 시스템에 대해 다음 표준화 옵션을 활성화해야 합니다.

- 검사할 FTP 트래픽을 표준화하려면 FTP 및 Telnet 프리프로세서 **Detect Telnet Escape codes within FTP commands** 옵션을 활성화해야 합니다. 27-25페이지의 서버 레벨 FTP 옵션 구성을/를 참조하십시오.
- 검사할 텔넷 트래픽을 표준화하려면 FTP 및 Telnet 프리프로세서 **Normalize** 텔넷 옵션을 활성화해야 합니다. 27-20페이지의 텔넷 옵션 이해을/를 참조하십시오.
- 검사할 SMTP 트래픽을 표준화하려면 SMTP 프리프로세서 **Normalize** 옵션을 활성화해야 합니다. 27-58페이지의 SMTP 디코딩 이해을/를 참조하십시오.

하나의 규칙에 여러 `pkt_data` 키워드를 사용할 수 있습니다.

패킷 페이로드의 시작 부분을 가리키려면

액세스: Admin/Intrusion Admin

1단계 Create Rule 페이지의 드롭다운 목록에서 **pkt_data**를 선택하고 **Add Option**을 클릭합니다.

`pkt_data` 키워드가 나타납니다.

`pkt_data` 키워드에는 인수가 없습니다.

Base64 데이터 디코딩 및 검사

라이센스: 보호

지정된 데이터를 Base64 데이터로 디코딩 및 검사하도록 규칙 엔진에 지시하려면 `base64_decode` 및 `base64_data` 키워드를 함께 사용할 수 있습니다. 이 방법은 예를 들면 HTTP PUT 요청과 POST 요청에서 Base64로 인코딩된 HTTP Authentication 요청 헤더 및 Base64로 인코딩된 데이터를 검사하는 경우 유용할 수 있습니다.

이러한 키워드는 HTTP 요청에서 Base64 데이터를 디코딩 및 검사하는 데 특히 유용합니다. 그러나 긴 헤더를 여러 줄로 확장하기 위해 HTTP와 같은 방식으로 공백 및 탭 문자를 사용하는 SMTP와 같은 프로토콜에서도 이러한 키워드를 사용할 수 있습니다. 접기(folding)라고도 알려진 이러한 줄 확장이 해당 프로토콜에 없는 경우, 검사는 캐리지 리턴에서 끝나거나 공백 또는 탭이 이어지지 않는 라인 피드에서 끝납니다.

자세한 내용은 다음 절을 참조하십시오.

- 36-101페이지의 base64_decode
- 36-102페이지의 base64_data

base64_decode

라이센스: 보호

`base64_decode` 키워드는 패킷 데이터를 Base64 데이터로 디코딩하도록 규칙 엔진에 지시합니다. 선택적인 인수를 사용하면 디코딩할 바이트 수 및 디코딩을 시작할 데이터의 위치를 지정할 수 있습니다.

규칙에서 `base64_decode` 키워드를 한 번 사용할 수 있으며, `base64_data` 키워드보다 적어도 한 인스턴스 앞에 나타나야 합니다. 자세한 내용은 36-102페이지의 base64_data을/를 참조하십시오.

Base64 데이터를 디코딩하기 전에 규칙 엔진은 여러 줄에 접혀 있는 긴 헤더를 펼칩니다. 규칙 엔진이 다음 중 하나를 발견하면 디코딩이 종료됩니다.

- 헤더 줄의 끝
- 디코딩할 지정된 바이트 수
- 패킷의 끝

다음 표에서는 `base64_decode` 키워드와 함께 사용할 수 있는 인수에 대해 설명합니다.

표 36-60 선택적인 base64_decode 인수

인수	설명
Bytes	디코딩할 바이트 수를 지정합니다. 이 인수를 지정하지 않으면 디코딩은 헤더 줄의 끝이나 패킷 페이로드의 끝 중 먼저 나타나는 것까지 계속됩니다. 0이 아닌 양의 값을 지정할 수 있습니다.
Offset	패킷 페이로드의 처음을 기준으로, 또는 **Relative**를 지정한 경우 현재 검사 위치를 기준으로 오프셋을 결정합니다. 0이 아닌 양의 값을 지정할 수 있습니다.
Relative	현재 검사 위치를 기준으로 검사를 지정합니다.

Base64 데이터를 디코딩하려면

액세스: Admin/Intrusion Admin

1단계 Create Rule 페이지의 드롭다운 목록에서 **base64_decode**를 선택하고 **Add Option**을 클릭합니다.

`base64_decode` 키워드가 나타납니다.

2단계 선택적으로, 선택적인 base64_decode 인수 표에 설명된 인수 중 하나를 선택합니다.

base64_data

라이센스: 보호

`base64_data` 키워드는 `base64_decode` 키워드를 사용하여 디코딩된 Base64 데이터를 검사하기 위한 참조를 제공합니다. `base64_data` 키워드는 검사가 디코딩된 Base64 데이터의 처음부터 시작되도록 설정합니다. 선택적으로, 검사할 위치를 추가로 지정하려면 `content` 또는 `byte_test`와 같은 기타 키워드에서 사용 가능한 위치 인수를 사용할 수 있습니다.

`base64_data` 키워드는 `base64_decode` 키워드 뒤에서 적어도 한 번 사용해야 합니다. 선택적으로, 디코딩된 Base64 데이터의 시작 부분으로 돌아가려면 `base64_data`를 여러 번 사용할 수 있습니다.

Base64 데이터를 검사할 때에는 다음에 유의하십시오.

- Fast pattern matcher를 사용할 수 없습니다. 자세한 내용은 36-26페이지의 Fast Pattern Matcher 사용을/를 참조하십시오.
- 중개 HTTP content 인수가 있는 규칙에서 Base64 검사를 중단하려면 Base64 데이터를 추가로 검사하기 전에 규칙에 또 다른 `base64_data` 키워드를 삽입해야 합니다. 자세한 내용은 36-23 페이지의 HTTP Content 옵션을/를 참조하십시오.

디코딩된 Base64 데이터를 검사하려면

액세스: Admin/Intrusion Admin

1단계 Create Rule 페이지의 드롭다운 목록에서 **base64_data**를 선택하고 **Add Option**을 클릭합니다.

`base64_data` 키워드가 나타납니다.

규칙 작성

라이센스: 보호

사용자 지정 표준 텍스트 규칙을 생성할 수 있는 것처럼, Cisco에서 제공하는 표준 텍스트 규칙 및 공유 객체 규칙을 수정하고 변경 사항을 새 규칙으로 저장할 수 있습니다. Cisco에서 제공하는 공유 객체 규칙의 경우, 소스 및 목적지 포트와 IP 주소 등 규칙 헤더 정보를 수정하는 것으로 제한됩니다. 공유 객체 규칙에서는 규칙 키워드와 인수를 수정할 수 없습니다.

자세한 내용은 다음 절을 참조하십시오.

- 36-103페이지의 새 규칙 작성
- 36-104페이지의 기존 규칙 수정
- 36-106페이지의 규칙에 코멘트 추가
- 36-106페이지의 사용자 지정 규칙 삭제

새 규칙 작성

라이센스: 보호

자신의 고유한 표준 텍스트 규칙을 작성할 수 있습니다.

사용자 지정 표준 텍스트 규칙에서는 규칙 헤더 설정과 규칙 키워드 및 인수를 설정합니다. 선택적으로, 규칙 헤더 설정을 사용하면 특정 프로토콜을 사용하며 특정 IP 주소나 포트를 이동하는 트래픽만을 매칭하도록 규칙의 범위를 좁힐 수 있습니다.

새 규칙을 생성한 후, `GID:SID:Rev` 형식의 규칙 번호를 사용하여 신속하게 다시 찾을 수 있습니다 모든 표준 텍스트 규칙의 규칙 번호는 1부터 시작합니다. 규칙 번호의 두 번째 부분인 SID(Snort ID) 번호는 규칙이 로컬 규칙인지 Cisco에서 제공한 규칙인지를 나타냅니다. 새 규칙을 생성하면 시스템은 로컬 규칙에 대해 사용 가능한 다음 Snort ID 번호를 할당하고 로컬 규칙 카테고리에 저장합니다. 로컬 규칙용 Snort ID 번호는 1,000,000부터 시작하며(고가용성 쌍의 보조 방어 센터에서 생성된 침입 규칙은 1,000,000,000부터 시작) 새로운 각 로컬 규칙의 SID는 1씩 증가합니다. 규칙 번호의 마지막 부분은 개정 번호입니다. 새 규칙의 개정 번호는 0입니다. 사용자 지정 규칙을 수정할 때마다 개정 번호가 1씩 증가합니다.

참고 시스템은 사용자가 가져온 침입 정책의 사용자 지정 규칙에 새 SID를 할당합니다. 자세한 내용은 A-1페이지의 컨피그레이션 가져오기 및 내보내기을/를 참조하십시오.

규칙 편집기를 사용하여 사용자 지정 표준 텍스트 규칙을 작성하려면

액세스: Admin/Intrusion Admin

1단계 **Policies > Intrusion > Rule Editor**를 선택합니다.

Rule Editor 페이지가 나타납니다.

2단계 **Create Rule**을 클릭합니다.

Create Rule 페이지가 나타납니다.

3단계 이벤트와 함께 표시할 메시지를 **Message** 필드에 입력합니다.

이벤트 메시지에 대한 자세한 내용은 36-11페이지의 이벤트 메시지 정의을/를 참조하십시오.

팁 규칙 메시지를 지정해야 합니다. 또한 메시지는 공백으로만, 하나 이상의 따옴표로만, 하나 이상의 아포스트로피로만 구성할 수 없으며, 공백이나 따옴표나 아포스트로피의 조합으로 구성할 수도 없습니다.

4단계 이벤트 유형을 설명하기 위한 분류를 **Classification** 목록에서 선택합니다.

사용 가능한 분류에 대한 자세한 내용은 36-12페이지의 침입 이벤트 분류 정의을/를 참조하십시오.

5단계 생성하고자 하는 규칙의 유형을 **Action** 목록에서 선택합니다. 다음 중 하나를 사용할 수 있습니다.

- 트래픽이 규칙을 트리거할 때 이벤트를 생성하는 규칙을 생성하려면 **alert**을 선택합니다.
- 규칙을 트리거하는 트래픽을 무시하는 규칙을 생성하려면 **pass**를 선택합니다.

6단계 규칙이 검사할 패킷의 트래픽 프로토콜(**tcp**, **udp**, **icmp** 또는 **ip**)을 **Protocol** 목록에서 선택합니다.

프로토콜 유형 선택에 대한 자세한 내용은 36-4페이지의 프로토콜 지정을/를 참조하십시오.

7단계 규칙을 트리거해야 하는 트래픽의 원래 IP 주소 또는 주소 블록을 **Source IPs** 필드에 입력합니다. 규칙을 트리거해야 하는 트래픽의 목적지 IP 주소 또는 주소 블록을 **Destination IPs** 필드에 입력합니다.

규칙 편집기가 수용하는 IP 주소 구문에 대한 자세한 내용은 36-5페이지의 침입 규칙에서 IP 주소 지정을/를 참조하십시오.

8단계 규칙을 트리거해야 하는 트래픽의 원래 포트 번호를 **Source Port** 필드에 입력합니다. 규칙을 트리거해야 하는 트래픽의 수신 포트 번호를 **Destination Port** 필드에 입력합니다.

참고 프로토콜이 `ip`로 설정된 경우 시스템은 침입 규칙 헤더에서 포트 정의를 무시합니다.

규칙 편집기가 수용하는 포트 구문에 대한 자세한 내용은 36-8페이지의 침입 규칙에서 포트 정의을/를 참조하십시오.

9단계 규칙을 트리거할 트래픽의 방향을 나타내는 연산자를 **Direction** 목록에서 선택합니다. 다음 중 하나를 사용할 수 있습니다.

- **Directional** - 소스 IP 주소에서 목적지 IP 주소로 이동하는 트래픽을 매칭합니다.
- **Bidirectional** - 둘 중 한 방향으로 이동하는 트래픽을 매칭합니다.

10단계 사용할 키워드를 **Detection Options** 목록에서 선택합니다.

11단계 **Add Option**을 클릭합니다.

12단계 추가한 키워드에 대해 지정할 인수를 입력합니다. 규칙 키워드와 그 사용 방법에 관한 자세한 내용은 36-9페이지의 규칙의 키워드 및 인수 이해을/를 참조하십시오.

키워드와 인수를 추가할 때 다음을 수행할 수 있습니다.

- 키워드를 추가한 후 순서를 변경하려면 이동할 키워드 옆에 있는 위쪽 또는 아래쪽 화살표를 클릭합니다.
- 키워드를 삭제하려면 해당 키워드 옆에 있는 **X**를 클릭합니다.

추가할 각 키워드 옵션에 대해 10단계~12단계를 반복합니다.

13단계 규칙을 저장하려면 **Save As New**를 클릭합니다.

시스템은 로컬 규칙에 대한 규칙 번호 시퀀스에서 가능한 다음 SID(Snort ID) 번호를 할당하고 로컬 규칙 카테고리에 저장합니다.

새 규칙 또는 변경된 규칙을 적절한 침입 정책 내에서 활성화하기 전에는 시스템이 이러한 규칙에 대해 트래픽의 평가를 시작하지 않습니다. 활성화 후에는 액세스 제어 정책의 일부로서 침입 정책을 적용합니다. 자세한 내용은 12-15페이지의 액세스 제어 정책 적용을/를 참조하십시오.

기존 규칙 수정

라이센스: 보호

사용자 지정 표준 텍스트 규칙을 수정할 수 있습니다. 또한 Cisco에서 제공하는 표준 텍스트 규칙 또는 공유 객체 규칙을 수정한 후 저장하여 하나 이상의 새로운 규칙 인스턴스를 생성할 수도 있습니다.

규칙을 생성하거나 Cisco 규칙을 수정하면 새 규칙 또는 개정이 로컬 규칙 카테고리에 복사되고, 규칙에 100000보다 큰 사용 가능한 다음 SID(Snort ID)가 할당됩니다.

공유 객체 규칙에 대해서는 헤더 정보만 수정할 수 있습니다. 공유 객체 규칙 또는 해당 인수에 사용되는 규칙 키워드는 수정할 수 없습니다. 공유 객체 규칙에 대한 헤더 정보를 수정하고 변경 사항을 저장하면, GID(Generator ID) 3 및 사용자 지정 규칙에 사용 가능한 다음 SID와 함께 규칙의 새 인스턴스가 생성됩니다. Rule Editor는 공유 객체 규칙의 새 인스턴스를 예약된 `soid` 키워드에 연결하는데, 이 경우 사용자가 생성한 규칙이 VRT에 의해 생성된 규칙에 매핑됩니다. 자신이 생성한 공유 객체 규칙의 인스턴스는 삭제할 수 있지만 Cisco에서 제공한 공유 객체 규칙은 삭제할 수 없습니다. 자세한 내용은 36-3페이지의 규칙 헤더 이해 및 36-106페이지의 사용자 지정 규칙 삭제을/를 참조하십시오.

참고 공유 객체 규칙에 대한 프로토콜을 수정하지 마십시오. 수정할 경우 규칙이 무효화됩니다.

규칙을 수정하려면

액세스: Admin/Intrusion Admin

1단계 **Policies > Intrusion > Rule Editor**를 선택합니다.

Rule Editor 페이지가 나타납니다.

2단계 수정할 하나 이상의 규칙을 찾습니다. 다음 옵션을 이용할 수 있습니다.

- 규칙 카테고리를 탐색하여 규칙을 찾으려면 원하는 규칙에 대한 폴더를 살펴보고 규칙 옆에 있는 수정 아이콘( )을 클릭합니다.
- 규칙을 검색하여 찾으려면 원하는 하나 이상의 규칙에 대한 검색 기준(가장 단순하게 SID)을 입력하고 **Search**를 클릭합니다. 검색에 의해 반환된 알맞은 규칙을 클릭합니다. 자세한 내용은 36-107페이지의 규칙 검색을/를 참조하십시오.
- 페이지에 표시된 규칙을 필터링하여 하나 이상의 규칙을 찾으려면, 규칙 목록의 왼쪽 위에 필터 아이콘( )으로 표시되는 텍스트 상자에 규칙 필터를 입력합니다. 원하는 규칙을 찾고 규칙 옆에 있는 수정 아이콘( )을 클릭합니다. 자세한 내용은 36-109페이지의 Rule Editor 페이지에서 규칙 필터링을/를 참조하십시오.

선택한 규칙과 함께 규칙 편집기가 열립니다.

공유 객체 규칙을 선택하면 규칙 편집기에 규칙 헤더 정보만 표시됩니다. GID 번호 3(예: 3:1000004)으로 시작되는 목록으로 Rule Editor 페이지에서 공유 객체 규칙을 식별할 수 있습니다.

3단계 원하는 대로 규칙을 수정하고(규칙 옵션에 대한 자세한 내용은 36-103페이지의 새 규칙 작성 참조) **Save As New**를 클릭합니다.

로컬 규칙 카테고리에 규칙이 저장됩니다.

팁 시스템 규칙 대신 로컬에서 수정한 규칙을 사용하려면 32-20페이지의 규칙 상태 설정의 절차에 따라 시스템 규칙을 비활성화하고 로컬 규칙을 활성화하십시오.

4단계 변경 사항을 적용하려면 12-15페이지의 액세스 제어 정책 적용에 설명된 대로 침입 정책을 액세스 제어 정책의 일부로 적용하여 활성화합니다.

규칙에 코멘트 추가

라이센스: 보호

침입 규칙에 코멘트를 추가할 수 있습니다. 그러면 규칙과 익스플로잇 또는 식별하는 정책 위반에 대한 추가 컨텍스트와 정보를 제공할 수 있습니다.

규칙에 코멘트를 추가하려면

액세스: Admin/Intrusion Admin

1단계 **Policies > Intrusion > Rule Editor**를 선택합니다.

Rule Editor 페이지가 나타납니다.

2단계 주석을 달 규칙을 찾습니다. 다음 옵션을 이용할 수 있습니다.

- 규칙 카테고리를 탐색하여 규칙을 찾으려면 원하는 규칙에 대한 폴더를 살펴보고 규칙 옆에 있는 수정 아이콘( )을 클릭합니다.
- 규칙을 검색하여 찾으려면 원하는 규칙에 대한 검색 기준(가장 단순하게 SID)을 입력하고 **Search**를 클릭합니다. 검색에 의해 반환된 알맞은 규칙을 클릭합니다. 자세한 내용은 36-107페이지의 규칙 검색을/를 참조하십시오.
- 페이지에 표시된 규칙을 필터링하여 규칙을 찾으려면, 규칙 목록의 왼쪽 위에 필터 아이콘( )으로 표시되는 텍스트 상자에 규칙 필터를 입력합니다. 원하는 규칙을 찾고 규칙 옆에 있는 수정 아이콘( )을 클릭합니다. 자세한 내용은 36-109페이지의 Rule Editor 페이지에서 규칙 필터링을/를 참조하십시오.

규칙 편집기가 나타납니다.

3단계 **Rule Comment**를 클릭합니다.

Rule Comment 페이지가 나타납니다.

4단계 텍스트 상자에 코멘트를 입력하고 **Add Comment**를 클릭합니다.

코멘트 텍스트 상자에 코멘트가 저장됩니다.

팁 또한 침입 이벤트의 패킷 보기에서 규칙 코멘트를 추가하고 볼 수 있습니다. 자세한 내용은 41-24페이지의 이벤트 정보 보기을/를 참조하십시오.

사용자 지정 규칙 삭제

라이센스: 보호

침입 정책에서 현재 활성화되지 않은 사용자 지정 규칙을 삭제할 수 있습니다. Cisco에서 제공하는 표준 텍스트 규칙 또는 공유 객체 규칙은 삭제할 수 없습니다.

삭제된 규칙은 Deleted 카테고리에 저장되며, 삭제된 규칙을 새 규칙의 기반으로 사용할 수 있습니다. 규칙의 수정에 대한 자세한 내용은 36-104페이지의 기존 규칙 수정을/를 참조하십시오.

침입 정책의 Rules 페이지에는 Deleted 카테고리가 표시되지 않으므로, 삭제된 사용자 지정 규칙은 활성화할 수 없습니다.

Rule Updates 페이지에서 모든 로컬 규칙을 삭제할 수도 있습니다. 예제를 보려면 66-16페이지의 1회 규칙 업데이트 사용을/를 참조하십시오.

자세한 내용은 다음 절을 참조하십시오.

- 사용자 지정 테이블 생성에 대한 자세한 내용은 36-103페이지의 새 규칙 작성을/를 참조하십시오.
- 로컬 규칙 가져오기에 대한 자세한 내용은 66-14페이지의 규칙 업데이트 및 로컬 규칙 파일 가져오기을/를 참조하십시오.
- 규칙 상태 설정에 대한 자세한 내용은 32-20페이지의 규칙 상태 설정을/를 참조하십시오.

사용자 지정 규칙을 삭제하려면

액세스: Admin/Intrusion Admin

1단계 **Policies > Intrusion > Rule Editor**를 선택합니다.

Rule Editor 페이지가 나타납니다.

2단계 2가지 옵션이 있습니다.

- **Delete Local Rules**와 **OK**를 차례로 클릭합니다.

  변경 사항을 저장했지만 침입 정책에서 현재 활성화되지 않은 모든 규칙이 로컬 규칙 카테고리에서 삭제되고 Deleted 카테고리로 이동합니다.

- 로컬 규칙 카테고리에 대한 폴더를 탐색하고, 로컬 규칙 카테고리를 클릭하여 확장한 다음 삭제할 규칙 옆에 있는 삭제 아이콘( )을 클릭합니다.

  규칙이 로컬 규칙 카테고리에서 삭제되고 Deleted 카테고리로 이동합니다.

  사용자 지정 표준 텍스트 규칙의 GID(Generator ID)는 1(예: 1:1000012)이고 사용자 지정 공유 객체 규칙의 GID는 3(예: 3:1000005)입니다.

팁 또한 수정된 헤더 정보로 저장된 공유 객체 규칙은 로컬 규칙 카테고리에 저장되며 GID는 3입니다. 공유 객체 규칙의 수정된 버전은 삭제할 수 있지만 원래 공유 객체 규칙은 삭제할 수 없습니다.

규칙 검색

라이센스: 보호

FireSIGHT 시스템에서는 수천 개의 표준 텍스트 규칙을 제공하며, Cisco Vulnerability Research Team에서는 새로운 취약성 및 익스플로잇이 검색될 때마다 계속해서 규칙을 추가합니다. 특정 규칙을 손쉽게 검색하여 활성화, 비활성화 또는 수정할 수 있습니다.

다음 표에서는 사용 가능한 검색 옵션에 대해 설명합니다.

표 36-61 규칙 검색 기준

옵션	설명
Signature ID	Snort ID(Signature ID라고도 함)를 기반으로 단일 규칙을 검색하려면 Snort ID 번호를 입력합니다. 여러 규칙을 검색하려면 쉼표로 구분된 Snort ID 번호 목록을 입력합니다. 이 필드의 문자 제한은 80자입니다.
Generator ID	표준 텍스트 규칙을 검색하려면 **1**을 선택합니다. 공유 객체 규칙을 검색하려면 **3**을 선택합니다.

표 36-61 규칙 검색 기준(계속)

옵션	설명
메시지	특정 메시지가 있는 규칙을 검색하려면 규칙 메시지의 한 단어를 **Message** 필드에 입력합니다. 예를 들어 DNS 익스플로잇을 검색하려면 `DNS`, 버퍼 오버플로 익스플로잇을 검색하려면 `overflow`를 입력합니다.
프로토콜	특정 프로토콜의 트래픽을 평가하는 규칙을 검색하려면 프로토콜을 선택합니다. 프로토콜을 선택하지 않으면 검색 결과에 모든 프로토콜에 대한 규칙이 포함됩니다.
소스 포트	지정된 포트에서 오는 패킷을 검사하는 규칙을 검색하려면 소스 포트 번호 또는 포트 관련 변수를 입력합니다.
대상 포트	특정 포트로 향하는 패킷을 검사하는 규칙을 검색하려면 목적지 포트 번호 또는 포트 관련 변수를 입력합니다.
소스 IP	지정된 IP 주소에서 오는 패킷을 검사하는 규칙을 검색하려면 소스 IP 주소 또는 IP 주소 관련 변수를 입력합니다.
대상 IP	지정된 IP 주소로 향하는 패킷을 검사하는 규칙을 검색하려면 목적지 IP 주소 또는 IP 주소 관련 변수를 입력합니다.
키워드	특정 키워드를 검색하려면 키워드 검색 옵션을 사용할 수 있습니다. 검색할 키워드 및 키워드 값을 선택합니다. 지정된 값 이외의 값을 매칭하려면 키워드 값 앞에 느낌표(!)를 입력할 수도 있습니다.
카테고리	특정 카테고리의 규칙을 검색하려면 **Category** 목록에서 카테고리를 선택합니다.
분류	특정 분류가 있는 규칙을 검색하려면 **Classification** 목록에서 분류 이름을 선택합니다.
Rule State	특정 정책 및 규칙 상태 내의 규칙을 검색하려면, 첫 번째 **Rule State** 목록에서 정책을 선택하고 규칙을 검색하기 위한 두 번째 목록에서 상태를 선택합니다 (**Generate Events**, **Drop and Generate Events** 또는 **Disabled**).

특정 규칙을 검색하려면

액세스: Admin/Intrusion Admin

1단계 **Policies > Intrusion > Rule Editor**를 선택합니다.

Rule Editor 페이지가 나타납니다.

2단계 툴바에서 **Search**를 클릭합니다.

Search 페이지가 나타납니다.

3단계 규칙 검색 기준 표에 설명된 필드 중 하나를 사용하여 검색 기준을 추가합니다.

참고 규칙을 검색하려면 검색 기준을 하나 이상 지정해야 합니다.

4단계 특정 키워드가 포함된 규칙을 검색하려면 다음 단계를 수행하십시오.

- **Keyword** 섹션의 드롭다운 목록에서 검색할 키워드를 선택합니다.
  사용 가능한 각 키워드의 목록은 36-9페이지의 규칙의 키워드 및 인수 이해을/를 참조하십시오.
- 검색할 인수를 **Keyword** 필드에 입력합니다.

5단계 **Search**를 클릭합니다.

검색 기준과 일치하는 규칙 목록과 함께 페이지가 다시 로드됩니다.

6단계 규칙(시스템 규칙인 경우 규칙의 복사본)을 보거나 수정하려면 하이퍼링크가 있는 규칙 메시지를 클릭합니다. 규칙의 수정에 대한 자세한 내용은 36-104페이지의 기존 규칙 수정을/를 참조하십시오.

Rule Editor 페이지에서 규칙 필터링

라이센스: 보호

규칙의 하위 집합을 표시하려면 Rule Editor 페이지에서 규칙을 필터링할 수 있습니다. 필터링 기능은 예를 들어, 규칙을 수정하거나 규칙 상태를 변경하고자 하지만 수천 개의 사용 가능한 규칙 중 원하는 규칙을 찾는 데 어려움이 있는 경우 유용할 수 있습니다.

필터를 입력하면 하나 이상의 일치하는 규칙이 포함된 폴더가 표시되거나, 일치하는 규칙이 없는 경우 메시지가 표시됩니다. 필터에는 특수 키워드와 인수, 문자 문자열, 따옴표의 리터럴 문자 문자열을 포함할 수 있으며 여러 필터 조건을 공백으로 구분할 수 있습니다. 필터에는 정규식이나 와일드카드 문자 또는 부정 문자(!), 보다 큼 기호(>), 보다 작음 기호(<) 등의 특수 연산자를 포함할 수 없습니다.

모든 키워드, 키워드 인수 및 문자 문자열은 대/소문자를 구분하지 않습니다. `gid` 및 `sid` 키워드를 제외하고 모든 인수 및 문자열은 부분 문자열로 취급됩니다. `gid` 및 `sid`에 대한 인수는 정확한 일치 항목만 반환합니다.

선택적으로, 필터링되지 않은 원래 페이지에서 폴더를 확장할 수 있으며, 후속 필터가 해당 폴더에서 일치 항목을 반환하면 폴더는 확장된 상태로 유지됩니다. 이 방법은 찾으려는 규칙이 다수의 규칙을 포함하는 폴더에 있는 경우 유용할 수 있습니다.

필터를 후속 필터로 제한할 수 없습니다. 입력한 필터는 전체 규칙 데이터베이스를 검색하며 일치하는 모든 규칙을 반환합니다. 페이지에 이전 필터의 결과가 표시되어 있는 상태에서 필터를 입력하면, 페이지가 지워지고 새 필터의 결과가 대신 반환됩니다.

필터링된 목록 또는 필터링되지 않은 목록에서 규칙에 동일한 기능을 사용할 수 있습니다. 예를 들어 Rule Editor 페이지의 필터링된 또는 필터링되지 않은 목록에서 규칙을 수정할 수 있습니다. 페이지에 대한 컨텍스트 메뉴에서 원하는 옵션을 사용할 수도 있습니다.

자세한 내용은 다음 절을 참조하십시오.

- 36-110페이지의 규칙 필터에서 키워드 사용
- 36-111페이지의 규칙 필터에서 문자 문자열 사용
- 36-111페이지의 규칙 필터에서 키워드와 문자 문자열 조합
- 36-112페이지의 규칙 필터링

규칙 필터에서 키워드 사용

라이센스: 보호

각 규칙 필터는 다음과 같은 형식으로 하나 이상의 키워드를 포함할 수 있습니다.

keyword:*argument*

여기서 *keyword*는 규칙 필터 키워드 표에 있는 키워드 중 하나이며 *argument*는 키워드와 관련된 하나 이상의 특정 필드에서 검색할, 대/소문자를 구분하지 않는 단일 영숫자 문자열입니다.

`gid` 및 `sid`를 제외한 모든 키워드의 인수는 부분 문자열로 취급됩니다. 예를 들어 인수 `123`은 `"12345"`, `"41235"`, `"45123"` 등을 반환합니다. `gid` 및 `sid`에 대한 인수는 정확한 일치 항목만 반환합니다. 예를 들어 `sid:3080`은 SID 3080만 반환합니다.

팁 하나 이상의 문자 문자열로 필터링하여 부분 SID를 검색할 수 있습니다. 자세한 내용은 36-111페이지의 규칙 필터에서 문자 문자열 사용을/를 참조하십시오.

다음 표에서는 규칙 필터링에 사용할 수 있는 특정 필터링 키워드 및 인수에 대해 설명합니다.

표 36-62 규칙 필터 키워드

키워드	설명	예
`arachnids`	규칙 참조에서 Arachnids ID의 전체 또는 일부를 기반으로 하나 이상의 규칙을 반환합니다. 자세한 내용은 36-14페이지의 이벤트 참조 정의을/를 참조하십시오.	`arachnids:181`
`bugtraq`	규칙 참조에서 Bugtraq ID의 전체 또는 일부를 기반으로 하나 이상의 규칙을 반환합니다. 자세한 내용은 36-14페이지의 이벤트 참조 정의을/를 참조하십시오.	`bugtraq:2120`
`cve`	규칙 참조에서 CVE 번호의 전체 또는 일부를 기반으로 하나 이상의 규칙을 반환합니다. 자세한 내용은 36-14페이지의 이벤트 참조 정의을/를 참조하십시오.	`cve:2003-0109`
`gid`	인수 `1`은 표준 텍스트 규칙을 반환합니다. 인수 `3`은 공유 객체 규칙을 반환합니다. 자세한 내용은 41-40페이지의 프리프로세서 Generator ID 읽기 및 32-2 페이지의 표 32-1을/를 참조하십시오.	`gid:3`
`mcafee`	규칙 참조에서 McAfee ID의 전체 또는 일부를 기반으로 하나 이상의 규칙을 반환합니다. 자세한 내용은 36-14페이지의 이벤트 참조 정의을/를 참조하십시오.	`mcafee:10566`
`msg`	규칙 Message 필드(이벤트 메시지라고도 함)의 전체 또는 일부를 기반으로 하나 이상의 규칙을 반환합니다. 자세한 내용은 36-11페이지의 이벤트 메시지 정의을/를 참조하십시오.	`msg:chat`
`nessus`	규칙 참조에서 Nessus ID의 전체 또는 일부를 기반으로 하나 이상의 규칙을 반환합니다. 자세한 내용은 36-14페이지의 이벤트 참조 정의을/를 참조하십시오.	`nessus:10737`
`ref`	규칙 참조 또는 규칙 Message 필드에서 단일 영숫자 문자열의 전체 또는 일부를 기반으로 하나 이상의 규칙을 반환합니다. 자세한 내용은 36-14페이지의 이벤트 참조 정의 및 36-11페이지의 이벤트 메시지 정의을/를 참조하십시오.	`ref:MS03-039`

표 36-62 규칙 필터 키워드(계속)

키워드	설명	예
sid	정확한 Signature ID의 규칙을 반환합니다. 자세한 내용은 41-40페이지의 프리프로세서 Generator ID 읽기을/를 참조하십시오.	sid:235
url	규칙 참조에서 URL의 전체 또는 일부를 기반으로 하나 이상의 규칙을 반환합니다. 자세한 내용은 36-14페이지의 이벤트 참조 정의을/를 참조하십시오.	url:faqs.org

규칙 필터에서 문자 문자열 사용

라이센스: 보호

각 규칙 필터는 하나 이상의 영숫자 문자 문자열을 포함할 수 있습니다. 문자 문자열은 규칙 **Message** 필드, Signature ID 및 Generator ID를 검색합니다. 예를 들어 문자열 `123`은 규칙 메시지에 있는 `"Lotus123"`, `"123mania"` 등의 문자열을 반환하며 SID 6123, SID 12375 등도 반환합니다. 규칙 **Message** 필드에 대한 자세한 내용은 36-11페이지의 이벤트 메시지 정의을/를 참조하십시오. 규칙 SID 및 GID에 대한 자세한 내용은 41-40페이지의 프리프로세서 Generator ID 읽기을/를 참조하십시오.

모든 문자 문자열은 대/소문자를 구분하지 않으며 부분 문자열로 취급됩니다. 예를 들어 `ADMIN`, `admin` 또는 `Admin` 문자열은 `"admin"`, `"CFADMIN"`, `"Administrator"` 등을 반환합니다.

정확한 일치 항목을 반환하려면 문자 문자열을 따옴표로 감쌀 수 있습니다. 예를 들어 따옴표로 감싼 리터럴 문자열 `"overflow attempt"`는 정확한 문자열만을 반환하는 반면, 따옴표 없이 `overflow` 및 `attempt`의 두 문자열로 구성된 필터는 `"overflow attempt"`, `"overflow multipacket attempt"`, `"overflow with evasion attempt"` 등을 반환합니다.

규칙 필터에서 키워드와 문자 문자열 조합

라이센스: 보호

키워드, 문자 문자열 또는 둘 모두의 임의의 조합을 공백으로 구분하여 입력함으로써 필터링 결과의 범위를 좁힐 수 있습니다. 모든 필터 조건과 일치하는 규칙이 결과에 포함됩니다.

원하는 순서로 여러 필터 조건을 입력할 수 있습니다. 다음의 각 필터는 동일한 규칙을 반환합니다.

- `url:at login attempt cve:200`
- `login attempt cve:200 url:at`
- `login cve:200 attempt url:at`

규칙 필터링

라이센스: 보호

특정 규칙을 좀 더 쉽게 찾을 수 있도록 규칙의 하위 집합을 표시하려면 Rule Editor 페이지에서 규칙을 필터링할 수 있습니다. 그런 다음 컨텍스트 메뉴에서 사용 가능한 기능 선택을 포함하여 원하는 페이지 기능을 사용할 수 있습니다.

특정 규칙을 필터링하려면

액세스: Admin/Intrusion Admin

1단계 **Policies > Intrusion > Rule Editor**를 선택합니다.

Rule Editor 페이지가 나타납니다.

규칙 필터링은 수정할 규칙을 찾고자 하는 Rule Editor 페이지에서 특히 유용할 수 있습니다. 자세한 내용은 36-104페이지의 기존 규칙 수정을/를 참조하십시오.

2단계 선택적으로, Group Rules By 목록에서 다른 그룹화 방법을 선택할 수 있습니다.

팁 모든 하위 그룹의 규칙을 포함한 총 규칙 수가 클 경우 규칙이 여러 카테고리에 나타날 수 있기 때문에 고유한 총 규칙 수가 훨씬 적더라도 필터링에 상당한 시간이 소요될 수 있습니다.

3단계 선택적으로, 확장할 그룹 옆에 있는 폴더를 클릭합니다.

폴더가 확장되며 해당 그룹의 규칙이 표시됩니다. 일부 규칙 그룹에는 역시 확장 가능한 하위 그룹이 있습니다.

필터링되지 않은 원래 페이지에서 그룹을 확장하면 해당 그룹에 규칙이 있을 것으로 예상되는 경우 유용할 수 있습니다. 후속 필터로 해당 폴더에서 일치 항목이 검색되는 경우, 그리고 필터 지우기 아이콘( )을 클릭하여 필터링되지 않은 원래 페이지로 돌아갈 경우 그룹은 확장된 상태로 유지됩니다.

4단계 필터 텍스트 상자를 활성화하려면 규칙 목록의 왼쪽 위 텍스트 상자 내부에 있는 필터 아이콘( )의 오른쪽을 클릭합니다.

5단계 필터 제약 조건을 입력하고 Enter를 누릅니다.

필터에는 키워드와 인수, 문자 문자열(따옴표 포함 또는 없이) 및 여러 조건을 구분하는 공백을 포함할 수 있습니다. 자세한 내용은 36-109페이지의 Rule Editor 페이지에서 규칙 필터링을/를 참조하십시오.

페이지가 새로 고쳐지며 하나 이상의 일치하는 규칙이 포함된 그룹이 표시됩니다.

6단계 선택적으로, 아직 열리지 않은 폴더를 열어 일치하는 규칙을 표시합니다. 다음 필터링 옵션을 이용할 수 있습니다.

- 새 필터를 입력하려면 커서를 필터 텍스트 상자 내부에 두고 클릭하여 활성화한 다음, 필터를 입력하고 Enter를 누릅니다.
- 현재의 필터링된 목록을 지우고 필터링되지 않은 원래 페이지로 돌아가려면 필터 지우기 아이콘( )을 클릭합니다.

7단계 선택적으로, 페이지에서 일반적으로 하는 것처럼 규칙을 변경합니다. 36-104페이지의 기존 규칙 수정을/를 참조하십시오.

변경 사항을 반영하려면 12-15페이지의 액세스 제어 정책 적용에 설명된 대로 액세스 제어 정책의 침입 정책 부분을 적용합니다.

37장

악성코드 및 금지된 파일 차단

악성 소프트웨어나 *악성코드*는 여러 경로를 통해 조직의 네트워크에 침입할 수 있습니다. 악성코드의 효과를 식별 및 감소할 수 있도록 FireSIGHT 시스템의 파일 제어, 네트워크 파일 전파 흔적 분석(File trajectory), AMP 구성 요소는 네트워크 트래픽 내에서 악성코드 및 기타 유형의 파일 전송을 감지, 추적, 저장, 분석하고, 선택적으로 차단할 수 있습니다. 또한 시스템에서는 아카이브 파일(예: formats `.zip` 또는 `.rar` 형식의 아카이브 파일) 내부의 중첩된 파일을 분석하고 작업을 수행합니다.

전체 액세스 제어 컨피그레이션에 악성코드 차단 및 파일 제어를 포함하여 이를 수행하도록 시스템을 구성합니다. 사용자가 생성하고 액세스 제어 규칙과 연결하는 *파일 정책*은 규칙과 매칭되는 네트워크 트래픽을 처리합니다. 트래픽에서 탐지된 파일을 다운로드한 다음, 파일 시그니처의 *동적 분석*을 위해 이를 Cisco의 악성코드 네트워크(*종합 보안 인텔리전스 클라우드*라고 함)에 제출하여 해당 파일에 악성코드가 포함되어 있는지 확인할 수 있습니다.

Context Explorer 및 대시보드에서는 조직의 내트워크 트래픽에서 탐지된 파일(악성코드 파일 포함)에 대해 다양한 유형의 심층적인 보기를 제공합니다. 더 세밀하게 분석 대상을 지정하기 위해, 악성코드 파일의 *네트워크 파일 전파 흔적 분석* 페이지를 사용하여 시간의 추이에 따라 호스트 전반의 개별 위협 확산을 추적할 수 있으며, 이를 통해 가장 효율적인 곳에서 침투를 제어하고 차단하는 작업에 주력할 수 있습니다.

모든 라이센스로 파일 정책을 생성할 수 있으나, 다음 표에 설명된 것처럼 악성코드 차단 및 파일 제어의 특정 부분에는 대상 디바이스의 특정 라이센스 기능을 사용해야 합니다.

표 37-1 침입 및 파일 검사를 위한 라이센스와 어플라이언스 요건

기능	설명	다음 라이센스 추가	다음 방어 센터 중 하나에 추가	다음 디바이스 중 하나에서 사용
침입 방지	침입 및 익스플로잇을 탐지하고 선택적으로 차단	보호	모든	모든
파일 제어	파일 유형의 전송을 탐지하고 선택적으로 차단	보호	모든	모든
AMP(Advanced Malware Protection)	악성코드의 전송을 탐지, 저장, 추적 및 선택적으로 차단 악성코드 분석을 위해 캡처 파일을 Cisco 클라우드에 제출	악성코드	DC500을 제외한 모두	Series 2 또는 X-Series를 제외한 모두

조직에 FireAMP 서브스크립션이 있는 경우, 방어 센터는 퍼블릭 Cisco 클라우드에서 엔드포인트 기반의 악성코드 탐지 데이터를 수신할 수도 있습니다. 방어 센터는 이러한 데이터를 시스템에서 생성된 네트워크 기반 파일 및 악성코드 데이터와 함께 제공합니다. FireAMP 데이터를 가져올 경우 FireAMP 서브스크립션 외에 라이센스가 필요하지 않습니다. 자세한 내용은 37-24페이지의 FireAMP를 위한 클라우드 연결 작업을/를 참조하십시오.

조직에 추가 보안이 필요하거나 외부 연결을 제한하려는 경우, 파일 및 악성코드 클라우드 기반 기능을 위해 표준 클라우드 연결 대신 FireAMP Private Cloud를 사용할 수 있습니다. 모든 파일 및 악성코드 클라우드를 조회하고, FireAMP 엔드포인트에서 이벤트 데이터를 수집 및 전달하는 작업은 프라이빗 클라우드를 통해 처리됩니다. 프라이빗 클라우드가 퍼블릭 Cisco 클라우드에 연결할 경우, 엔드포인트 이벤트 데이터를 전송하지 않는 익명 프록시 연결을 통해 이러한 작업을 수행합니다.

자세한 내용은 다음 링크를 참고하십시오.

- 37-2페이지의 악성코드 차단 및 파일 제어 이해
- 37-9페이지의 파일 정책 이해 및 생성
- 37-24페이지의 FireAMP를 위한 클라우드 연결 작업

악성코드 차단 및 파일 제어와 관련된 이벤트 데이터 평가에 대한 자세한 내용은 40-1페이지의 악성코드 및 파일 활동 분석을/를 참조하십시오.

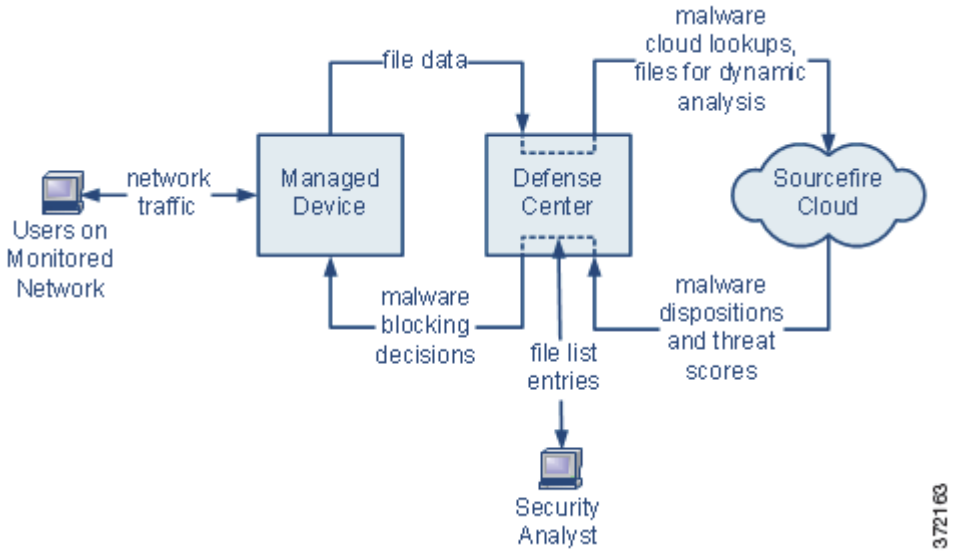
악성코드 차단 및 파일 제어 이해

라이센스: 보호, 악성코드, 또는 모두

지원되는 디바이스: 기능에 따라 다름

지원되는 Defense Center: 기능에 따라 다름

고급 악성코드 차단 기능을 사용하면 아래 다이어그램에 나온 것처럼, 네트워크에 전송되는 악성코드 파일을 탐지, 저장, 추적, 분석하고 선택에 따라 차단하도록 FireSIGHT 시스템을 구성할 수 있습니다.



시스템은 PDF, Microsoft Office 문서 및 기타 파일을 비롯한 다양한 유형의 파일에 있는 악성코드를 탐지하고 선택에 따라 차단합니다. 매니지드 디바이스는 이러한 파일 유형의 전송을 위해 애플리케이션 프로토콜 기반의 네트워크 트래픽을 모니터링합니다. 디바이스가 적합한 파일을 탐지하면, 파일의 SHA-256 해시 값이 방어 센터에 전송되며 여기에서는 해당 정보를 사용하여 *악성코드 클라우드 조회*를 수행합니다. 이러한 결과를 바탕으로, Cisco 클라우드는 파일 속성을 방어 센터에 반환합니다.

시스템이 네트워크 트래픽에서 파일을 탐지한 경우, *파일 저장* 기능을 사용하면 디바이스가 적합한 파일을 하드 드라이브 또는 악성코드 스토리지 팩에 저장할 수 있습니다. 속성이 Unknown인 실행 파일의 경우, 디바이스의 파일 저장 여부에 상관없이 디바이스에서는 *동적 분석*을 위해 해당 파일을 제출할 수 있습니다. 클라우드는 방어 센터에 다음 결과를 반환합니다.

- 위협 점수 — 파일에 악성코드가 포함되어 있을 가능성 설명
- 동적 분석 요약 보고서 — 클라우드에서 해당 위협 점수를 할당한 이유를 세부적으로 설명

파일이 적합한 실행 파일인 경우, 디바이스는 파일 구조에 대해 Spero 분석을 수행하고 결과로 제공된 Spero 시그니처를 클라우드에 제출할 수 있습니다. 이 시그니처를 사용하여 동적 분석을 보완할 경우, 클라우드는 파일이 악성코드인지 확인합니다.

클라우드의 파일에 잘못된 속성이 있는 경우, 파일의 SHA-256 값을 파일 목록에 추가할 수 있습니다.

- 클라우드가 정상 성향을 할당한 것처럼 파일을 취급하려면 *정상 목록*에 파일을 추가합니다.
- 클라우드가 악성코드 성향을 할당한 것처럼 파일을 취급하려면 *사용자 지정 탐지 목록*에 파일을 추가합니다.

시스템이 파일 목록에서 파일의 SHA-256 값을 탐지한 경우, 시스템은 악성코드 조회 또는 파일 속성 확인을 수행하지 않고 적절한 조치를 취합니다. 파일 정책에서 규칙을 **Malware Cloud Lookup** 또는 **Block Malware** 작업으로 구성해야 하며, 파일의 SHA 값을 계산하도록 일치하는 파일 형식을 구성해야 합니다. 파일 정책을 기준으로 안전 목록 또는 사용자 지정 탐지 목록의 사용을 활성화할 수 있습니다. 파일 목록 관리에 대한 자세한 내용은 3-33페이지의 파일 목록 작업을/를 참조하십시오.

시스템은 압축되지 않은 일반 파일을 분석하고 작업을 수행하는 것과 동일한 방식으로, 아카이브 파일(예: `.zip` 또는 `.rar` 아카이브 파일) 내부의 중첩된 파일을 검사하고 차단할 수 있습니다. 그러나 시스템이 모든 중첩된 파일을 차단할 경우, 해당 파일이 포함된 전체 아카이브 파일이 차단됩니다. 시스템은 가장 바깥의 아카이브 파일(수준 0) 아래에 있는 최대 3가지 수준의 중첩된 파일을 검사할 수 있습니다. 지정된 중첩 수준(최대 3가지 수준)을 초과하는 아카이브 파일을 차단하도록 파일 정책을 구성할 수 있습니다.

또한 내용이 암호화된 아카이브 파일을 차단하거나, 그렇지 않을 경우 검사할 수 없도록 파일 정책을 구성할 수도 있습니다. 아카이브 파일 검사에 대한 자세한 내용은 37-20페이지의 아카이브 파일 검사 옵션 구성을/를 참조하십시오.

파일을 검사하거나 차단하려면 정책을 적용하는 매니지드 디바이스에 대한 보호 라이센스를 활성화해야 합니다. 파일을 저장하고, 악성코드 클라우드 조회를 수행하고 악성코드 파일을 선택적으로 차단하고, 동적 분석을 위해 파일을 클라우드에 제출하거나, 파일 목록에 파일을 추가하려면 해당 디바이스에 대한 악성코드 라이센스를 활성화해야 합니다.

파일 속성 이해

시스템은 Cisco 클라우드에 의해 반환된 속성을 기준으로 파일 속성을 확인합니다. 파일 목록에 파일을 추가하거나 위협 점수가 제공된 결과로 인해, 파일에는 Cisco 클라우드에 의해 반환된 다음과 같은 파일 속성 중 하나가 포함될 수 있습니다.

- `Malware` — 클라우드가 파일을 악성코드로 분류했으며 파일의 위협 점수가 파일 정책에 정의된 악성코드 임계값을 초과했음을 나타냅니다.
- `Clean` — 클라우드가 파일을 정상으로 분류했거나, 사용자가 파일을 정상 목록에 추가했음을 나타냅니다.

- Unknown — 클라우드가 성향을 할당하기 전에 악성코드 클라우드 조회가 발생했음을 나타냅니다. 클라우드에서 파일의 카테고리를 분류하지 않았습니다.
- Custom Detection — 사용자가 파일을 사용자 지정 탐지 목록에 추가했음을 나타냅니다.
- Unavailable — 방어 센터에서 악성코드 클라우드 조회를 수행할 수 없음을 나타냅니다. 이 성향의 이벤트는 비율이 낮을 수 있는데, 이는 정상적인 상황입니다.

팁 빠른 세션에서 여러 개의 Unavailable 악성코드 이벤트가 표시될 경우, 클라우드 연결 및 포트 컨피그레이션을 확인하십시오. 자세한 내용은 E-1페이지의 보안, 인터넷 액세스, 통신 포트을/를 참조하십시오.

아카이브 파일의 속성은 아카이브 내부의 파일에 할당된 속성을 기준으로 합니다. 아래의 내용별 아카이브 파일 속성 표에는 아카이브에 포함된 여러 가지 가능한 파일 조합을 위해 아카이브 파일에 제공되는 속성이 나열되어 있습니다. 식별된 악성코드 파일을 포함하는 **모든** 아카이브는 Malware라는 속성이 제공됩니다. 식별된 악성코드 파일이 없는 아카이브의 경우 알 수 없는 파일이 포함되어 있으면 Unknown이라는 속성이 제공되고, 안전한 파일만 포함되어 있으면 Clean이라는 속성이 제공됩니다. 아카이브 파일 검사에 대한 자세한 내용은 37-20페이지의 아카이브 파일 검사 옵션 구성을/를 참조하십시오. 다른 파일과 마찬가지로, 아카이브 파일은 Custom Detection 또는 Unavailable 속성에 조건이 적용될 경우 해당 속성이 포함될 수 있습니다.

표 37-2 내용별 아카이브 파일 속성

아카이브 파일 속성	알 수 없는 파일 수	안전한 파일 수	악성코드 파일 수
Unknown	1개 이상	모든	0
Clean	0	1개 이상	0
Malware	모든	모든	1개 이상

파일 속성을 기준으로, 방어 센터는 매니지드 디바이스가 파일을 차단하거나 파일의 업로드 또는 다운로드를 허용하도록 지시합니다. 아카이브 파일 내부의 중첩된 파일이 차단된 경우, 시스템에서는 전체 아카이브 파일을 차단합니다. 시스템이 SHA-256 값에 기반하여 파일의 속성을 이미 알고 있는 경우, 방어 센터는 성능을 개선하기 위해 Cisco 클라우드에 쿼리하는 대신 캐싱된 속성을 사용합니다.

파일 속성은 변경할 수 있습니다. 예를 들어, 클라우드는 이전에 안전한 것으로 간주된 파일이 현재 악성코드로 식별된 경우, 또는 그 반대로 악성코드로 식별된 파일이 사실은 안전한 파일로 드러난 경우를 확인할 수 있습니다. 지난주에 악성코드를 조회한 파일의 속성이 변경된 경우, 클라우드에서 방어 센터에 이를 알려 시스템이 다음번에 해당 파일의 전송을 탐지할 경우 적절한 조치를 취할 수 있도록 합니다. 변경된 파일 속성은 *회귀적* 속성이라고 합니다.

악성코드 클라우드 조회에서 반환된 파일 속성 및 모든 관련 위협 점수에는 TTL(time-to-live) 값이 포함됩니다. TTL 값에 지정된 기간 동안 파일 속성이 업데이트되지 않고 유지될 경우, 시스템에서는 캐싱된 정보를 삭제합니다. 속성 및 관련 위협 점수에는 다음과 같은 TTL 값이 포함됩니다.

- Clean — 4시간
- Unknown — 1시간
- Malware — 1시간

캐시에 대한 악성코드 클라우드 조회를 통해 캐싱된 속성이 시간을 초과한 것으로 식별된 경우, 시스템은 새로운 조회를 수행하여 파일 속성을 확인합니다.

파일 제어 이해

조직에서 악성코드뿐만 아니라 특정 유형의 모든 파일(파일의 악성코드 여부 포함 여부에 상관없이)의 전송을 차단하려는 경우, *파일 제어* 기능을 사용하면 폭넓은 범위를 포괄할 수 있습니다. 악성코드 차단과 마찬가지로, 매니지드 디바이스는 특정 유형의 파일 전송에 대해 네트워크 트래픽을 모니터링하고 파일을 차단하거나 허용합니다.

파일 제어는 시스템이 악성코드와 더불어 다양한 추가 파일 유형을 탐지할 수 있는 경우 모든 파일 유형을 지원합니다. 이러한 파일 유형은 멀티미디어(swf, mp3), 실행 파일(exe, torrent), PDF를 비롯한 기본적인 카테고리로 그룹화됩니다. 파일 제어는 악성코드 차단과 달리 Cisco 클라우드의 쿼리가 필요하지 않습니다.

캡처 파일, 파일 이벤트, 악성코드 이벤트를 분석에 사용

시스템에서는 파일이 전송되거나 차단된 경우 악성코드 및 파일 이벤트를 생성합니다. 이와 더불어 매니지드 디바이스에서 캡처한 모든 파일에 대한 정보를 수집하기도 합니다. 방어 센터의 웹 인터페이스를 사용하여 이러한 이벤트 및 정보를 볼 수 있습니다. 또한 Context Explorer 및 대시보드에서는 조직에서 탐지한 파일(악성코드 파일 포함)에 대해 다양한 유형의 심층적인 보기를 제공합니다.

분석 대상을 더 세밀하게 지정하려는 경우, *네트워크 파일 전파 흔적 분석* 기능을 사용하여 개별 파일의 전송 경로를 추적할 수 있습니다. 파일의 전파 흔적 분석 페이지에는 파일에 대한 요약 정보, 호스트에서 호스트로 전송된 파일의 그래픽 맵(차단된 전송 포함), 해당 파일의 탐지 또는 차단과 관련된 악성코드 또는 파일 이벤트 목록이 표시됩니다.

악성코드 라이센스를 DC500에 사용할 수 없고 악성코드 라이센스를 Series 2 디바이스 또는 Cisco NGIPS for Blue Coat X-Series에서 활성화할 수 없으므로 이러한 어플라이언스를 사용하여 개별 파일을 캡처 또는 차단하거나, 동적 분석을 위해 파일을 제출하거나, 악성코드 클라우드 조회를 시행할 파일의 파일 전파 흔적 분석을 볼 수 없습니다.

자세한 내용은 다음 절을 참조하십시오.

- 37-5페이지의 악성코드 차단 및 파일 제어 구성
- 37-6페이지의 악성코드 차단 및 파일 제어를 기반으로 이벤트 로깅
- 37-7페이지의 FireSIGHT 시스템와 FireAMP통합
- 37-8페이지의 네트워크 기반 AMP와 엔드포인트 기반 FireAMP 비교
- 40-36페이지의 네트워크 파일 전파 흔적 작업

악성코드 차단 및 파일 제어 구성

라이센스: 보호 또는 악성코드

지원되는 디바이스: 기능에 따라 다름

지원되는 Defense Center: 기능에 따라 다름

파일 정책을 액세스 제어 규칙과 연결하여 악성코드 차단 및 파일 제어를 전반적 액세스 제어 컨피그레이션의 일부로 구성합니다. 이러한 연결은 시스템이 액세스 제어 규칙의 조건과 매칭되는 트래픽의 파일을 전달하기 전에, 우선 파일을 검사하도록 합니다.

상위 액세스 제어 정책과 마찬가지로, 파일 정책에는 각 규칙의 조건과 일치하는 파일을 처리하는 방식을 결정하는 규칙이 포함됩니다. 별도의 파일 규칙을 구성하여 각기 다른 파일 유형, 애플리케이션 프로토콜, 또는 전송 방향마다 다른 작업을 실행할 수 있습니다.

파일이 규칙과 매칭될 경우, 규칙에서는 다음을 수행할 수 있습니다.

- 간단한 파일 유형 매칭을 기준으로 파일 허용 또는 차단
- 악성코드 파일 속성을 기준으로 파일 차단
- 파일을 캡처하고 디바이스에 저장
- 동적 분석을 위해 캡처 파일 제출

또한 파일 정책으로 다음을 수행할 수 있습니다.

- 안전 목록 또는 사용자 지정 탐지 목록의 항목을 기준으로 파일을 안전한 파일 또는 악성코드로 자동 처리
- 파일의 위협 점수가 구성 가능한 임계값을 초과할 경우 파일을 악성코드로 처리
- 아카이브 파일(예: `.zip` 또는 `.rar`)의 내용 검사
- 내용이 암호화 및 중첩된 아카이브 파일이 지정된 최대 아카이브 깊이를 넘을 경우 차단하거나, 검사할 수 없도록 구성

간단한 예를 들자면, 사용자가 실행 파일을 다운로드하는 것을 차단하는 파일 정책을 구현할 수 있습니다. 다른 예로, 다운로드한 PDF 파일의 악성코드 여부를 검사하고 발견된 모든 인스턴스를 차단할 수 있습니다. 파일 정책 및 이를 액세스 제어 규칙과 연결하는 방법에 대한 자세한 내용은 37-9페이지의 파일 정책 이해 및 생성 및 18-8페이지의 침입 방지 성능 조정을/를 참조하십시오.

악성코드 라이센스를 DC500에 사용할 수 없으므로, 해당 어플라이언스를 사용하여 네트워크 기반 악성코드 차단을 수행하거나 아카이브 파일의 내용을 검사하는 파일 정책을 적용할 수 없습니다. 이와 마찬가지로, 악성코드 라이센스를 Series 2 디바이스 또는 Cisco NGIPS for Blue Coat X-Series에서 활성화할 수 없으므로 네트워크 기반 악성코드 차단을 수행하거나 아카이브 파일의 내용을 검사하는 어플라이언스에 파일 정책을 적용할 수 없습니다.

악성코드 차단 및 파일 제어를 기반으로 이벤트 로깅

라이센스: 보호 또는 악성코드

지원되는 디바이스: 기능에 따라 다름

지원되는 Defense Center: 기능에 따라 다름

방어 센터에서는 시스템의 파일 검사 및 처리에 대한 레코드를 캡처된 파일, 파일 이벤트 및 악성코드 이벤트로 기록합니다.

- *캡처된 파일* — 시스템에 의해 캡처된 파일을 나타냅니다.
- *파일 이벤트* — 네트워크 트래픽에서 시스템에 의해 탐지되고 선택적으로 차단된 파일을 나타냅니다.
- *악성코드 이벤트* — 네트워크 트래픽에서 시스템에 의해 탐지되고 선택적으로 차단된 악성코드 파일을 나타냅니다.
- *소급 악성코드 이벤트* — 악성코드 파일 속성이 변경된 파일을 나타냅니다.

시스템에서 네트워크 트래픽의 악성코드 탐지 또는 차단을 기준으로 악성코드 이벤트를 생성할 경우, 파일의 악성코드를 탐지하려면 우선 파일 자체를 탐지해야 하므로 파일 이벤트도 같이 생성됩니다. FireAMP Connector(37-7페이지의 FireSIGHT 시스템와 FireAMP통합 참조)에서 생성된 엔드포인트 기반 악성코드 이벤트에는 해당 파일 이벤트가 없습니다. 이와 마찬가지로, 시스템이 네트워크 트래픽에서 파일을 캡처할 경우 파일을 먼저 탐지하므로 파일 이벤트가 함께 생성됩니다.

방어 센터를 사용하여 캡처 파일, 파일 이벤트, 악성코드 이벤트를 보고, 조작하고, 분석한 후 이러한 분석 결과를 다른 사용자에게 전달할 수 있습니다. Context Explorer, 대시보드, 이벤트 뷰어, 네트워크 파일 전파 흔적 분석, 보고 기능을 사용하면 탐지, 캡처, 차단된 파일 및 악성코드에 대한 내용을 심층적으로 파악할 수 있습니다. 이벤트를 사용하여 상관관계 정책 위반을 트리거하거나 이메일, SMTP 또는 syslog를 통해 알림을 제공할 수도 있습니다. 파일 및 악성코드 이벤트에 대한 자세한 내용은 40-8페이지의 파일 이벤트 작업 및 40-17페이지의 악성코드 이벤트 작업을/를 참조하십시오.

악성코드 라이센스를 DC500에 사용할 수 없고 악성코드 라이센스를 Series 2 디바이스 또는 Cisco NGIPS for Blue Coat X-Series에서 활성화할 수 없으므로 이러한 어플라이언스를 사용해서는 악성코드 클라우드 조회와 연결되거나 아카이브 파일의 내용과 연결되어 있는 캡처 파일, 파일 이벤트, 악성코드 이벤트를 생성하거나 분석할 수 없습니다.

FireSIGHT 시스템와 FireAMP통합

라이센스: 모든

FireAMP는 첨단 악성코드 침투, APT(Advanced Persistent Threat), 표적 공격을 발견, 이해 및 차단하는 Cisco의 엔터프라이즈급 고급 악성코드 분석 및 보호 솔루션입니다.

조직에서 FireAMP 서브스크립션을 보유한 경우 개별 사용자는 *엔드포인트* 즉, 컴퓨터와 모바일 디바이스에 *FireAMP Connector*를 설치할 수 있습니다. FireAMP Connector는 다른 기능 중에서도 업로드, 다운로드, 실행, 열기, 복사, 이동 등의 작업을 수행할 경우 파일을 검사할 수 있는 경량 에이전트입니다. 이러한 커넥터는 Cisco 클라우드와 통신을 수행하여 검사한 파일에 악성코드가 포함되었는지 확인합니다.

파일이 악성코드로 식별되면, 클라우드는 위협 식별 정보를 방어 센터에 전송합니다. 또한 클라우드는 검사, 격리, 차단된 실행, 클라우드 회수를 비롯한 다른 종류의 정보도 방어 센터에 전송할 수 있습니다. 방어 센터는 이러한 정보를 악성코드 이벤트로 로깅합니다.

FireAMP가 구축된 경우, 악성코드 이벤트를 기준으로 방어 센터에서 시작한 위협 요소 제거 및 알림을 구성할 수 있을 뿐만 아니라, FireAMP포털(http://amp.sourcefire.com/)을 사용하여 악성코드가 미치는 영향을 완화할 수 있습니다. 포털에서는 FireAMP 구축의 모든 부분을 제어하고, 침투의 모든 단계를 관리하는 강력하고 유연한 웹 인터페이스를 제공합니다. 다음이 가능합니다:

- 조직 전체에 알맞은 사용자 지정 악성코드 탐지 정책 및 프로필을 구성하고, 모든 사용자의 파일에 신속한 전체 검사 수행
- 보기 히트 맵, 자세한 파일 정보, 네트워크 파일 전파 흔적 분석, 위협 근본 원인을 비롯한 악성코드 분석 수행
- 자동 격리, 비 격리 실행 파일의 실행을 중단하는 애플리케이션 차단, 제외 목록을 비롯하여 침투 제어의 다양한 요소 구성
- 사용자 지정 보호 생성, 그룹 정책에 기반을 둔 특정 애플리케이션의 실행 차단, 사용자 지정 화이트리스트 생성

자세한 내용은 다음 절을 참조하십시오.

- 37-8페이지의 네트워크 기반 AMP와 엔드포인트 기반 FireAMP 비교에서는 Cisco 제품군에서 제공되는 악성코드 차단 전략을 비교합니다.
- 37-24페이지의 FireAMP를 위한 클라우드 연결 작업에서는 방어 센터와 Cisco 클라우드 간에 직접적으로 또는 FireAMP Private Cloud 연결을 통해 통신을 설정하는 방법을 설명합니다.

팁 FireAMP에 대한 자세한 내용은 FireAMP 포털의 온라인 도움말을 참조하십시오.

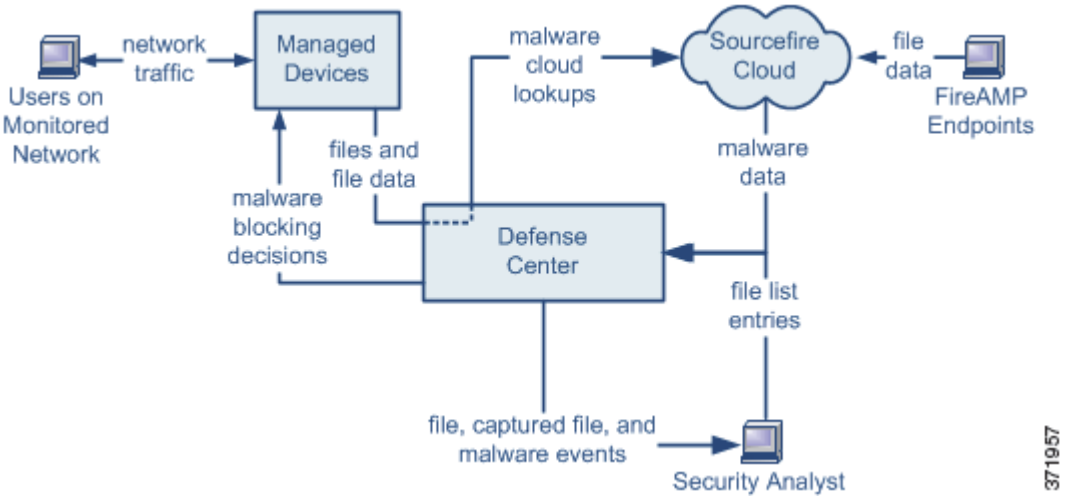
네트워크 기반 AMP와 엔드포인트 기반 FireAMP 비교

라이센스: 악성코드 또는 모두

지원되는 디바이스: 기능에 따라 다름

지원되는 Defense Center: 기능에 따라 다름

다음 다이어그램에는 방어 센터를 사용하여 네트워크 기반 고급 악성코드 차단 전략 및 엔드포인트 기반 FireAMP 전략에서 도출된 데이터를 모두 활용하는 방법이 나와 있습니다.



FireAMPFireAMP 악성코드 탐지는 다운로드 시 또는 실행 시 엔드포인트에서 수행되므로, 관리되는 디바이스가 네트워크 트래픽에서 악성코드를 탐지한다 하더라도 두 가지 유형의 악성코드 이벤트에 있는 정보가 다릅니다. 예를 들어, 엔드포인트 기반 악성코드 이벤트에는 파일 경로, 클라이언트 애플리케이션 호출 등에 대한 정보가 포함됩니다. 반면 네트워크 트래픽의 악성코드 탐지에는 포트, 애플리케이션 프로토콜, 파일 전송에 사용되는 연결에 대한 원래 IP 주소 정보가 포함됩니다.

또 다른 예를 들자면, 네트워크 기반 악성코드 이벤트의 경우 사용자 정보에는 네트워크 검색에서 확인된 내용에 따라, 악성코드가 목표로 한 호스트에 가장 최근 로그인한 사용자가 사용자 정보에 표시됩니다. 반면 FireAMP에서 보고된 사용자 정보에는 로컬 커넥터에서 확인된 내용에 따라, 악성코드가 탐지된 엔드포인트에 최근 로그인한 사용자가 표시됩니다.

참고 엔드포인트 기반 악성코드 이벤트에서 보고된 IP 주소는 네트워크 맵에 없을 수 있으며, 모니터링된 네트워크에도 없을 수 있습니다. 구축 환경, 네트워크 아키텍처, 규정준수 수준 및 기타 요인에 따라, 커넥터가 설치된 엔드포인트는 매니지드 디바이스에서 모니터링하는 호스트와 동일하지 않을 수 있습니다.

악성코드 라이센스를 DC500에 사용할 수 없고 악성코드 라이센스를 Series 2 디바이스 또는 Cisco NGIPS for Blue Coat X-Series에서 활성화할 수 없으므로 이러한 어플라이언스를 사용하여 개별 파일을 캡처 또는 차단하거나, 동적 분석을 위해 파일을 제출하거나, 아카이브 파일의 내용을 검사하거나, 악성코드 클라우드 조회를 시행할 파일의 파일 전파 흔적 분석을 볼 수 없습니다.

다음 표에는 두 가지 전략의 차이점이 요약되어 있습니다.

표 37-3 네트워크 기반과 엔드포인트 기반 악성코드 전략 비교

기능	네트워크 기반	엔드포인트 기반(FireAMP)
파일 유형 탐지 및 차단 방법(파일 제어)	네트워크 트래픽 내부에서 수행, 액세스 제어 및 파일 정책 사용	지원되지 않음
악성코드 탐지 및 차단 방법	네트워크 트래픽 내부에서 수행, 액세스 제어 및 파일 정책 사용	개별 엔드포인트에서 수행, Cisco 클라우드와 통신을 수행하는 설치된 커넥터 사용
네트워크 트래픽 검사	트래픽이 매니지드 트래픽을 통과함	없음, 엔드포인트에 설치된 커넥터가 파일을 직접 검사
악성코드 탐지 안정성	제한된 파일 유형	모든 파일 유형
악성코드 분석 선택	방어 센터 기반, 클라우드 내 분석 포함	방어 센터 기반, FireAMP 포털의 추가 옵션 포함
악성코드 완화	네트워크 트래픽의 악성코드 차단, 방어 센터에서 위협 요소 제거 시작	FireAMP 기반 격리 및 침투 제어 옵션, 방어 센터에서 위협 요소 제거 시작
이벤트 생성	파일 이벤트, 캡처 파일, 악성코드 이벤트, 회귀적 악성코드 이벤트	악성코드 이벤트
악성코드 이벤트에 대한 정보	기본적인 악성코드 이벤트 정보, 연결 데이터 포함(IP 주소, 포트, 애플리케이션 프로토콜)	심층적인 악성코드 이벤트 정보, 연결 데이터 없음
네트워크 파일 전파 흔적 분석	방어 센터 기반	방어 센터 기반, FireAMP 포털의 추가 옵션 포함
필수 라이센스 또는 서브스크립션	보호 라이센스로 파일 제어 수행, 악성코드 라이센스로 악성코드 차단 수행	FireAMP 서브스크립션(라이센스 기반 아님)

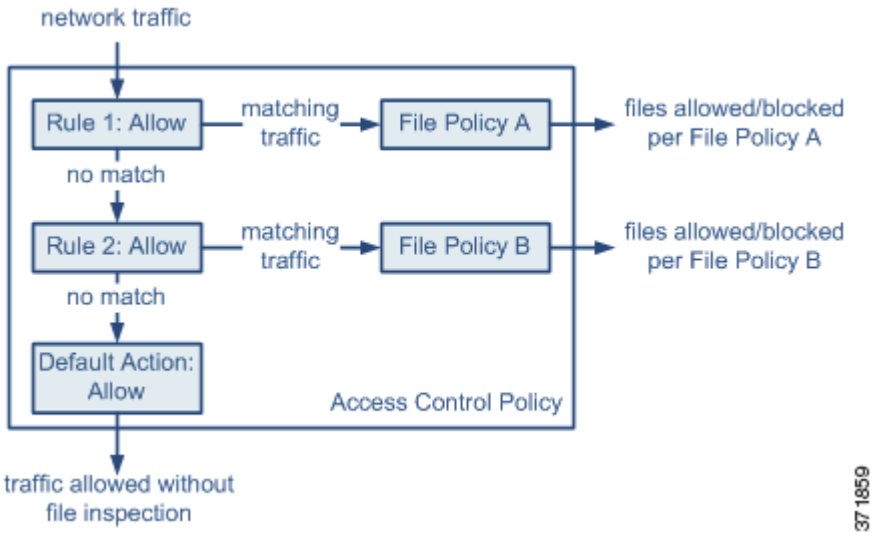
파일 정책 이해 및 생성

라이센스: 보호 또는 악성코드

지원되는 디바이스: 기능에 따라 다름

지원되는 Defense Center: 기능에 따라 다름

파일 정책은 지능형 악성코드 차단 및 파일 제어를 수행하기 위해 시스템에서 전체 액세스 제어 구성의 일부로 사용하는 컨피그레이션 집합입니다. 인라인 구축의 간단한 액세스 제어 정책을 나타낸 아래 다이어그램을 살펴보십시오.



정책에 두 개의 액세스 제어 규칙이 있으며, 두 규칙 모두 Allow 작업을 사용하고 파일 정책과 연결되어 있습니다. 정책의 기본 작업은 파일 정책 검사 없이 트래픽을 허용하는 것입니다. 이 시나리오에서 트래픽은 다음과 같이 처리됩니다.

- `Rule 1`과 매칭되는 트래픽은 `File Policy A`에서 검사합니다.
- `Rule 1`과 매칭되지 않는 트래픽은 `Rule 2`로 평가합니다. `Rule 2`와 매칭되는 트래픽은 `File Policy B`에서 검사합니다.
- 각 규칙과 매칭되지 않는 트래픽이 허용되며, 파일 정책을 기본 작업과 연결할 수 없습니다.

상위 액세스 제어 정책과 마찬가지로, 파일 정책에는 각 규칙의 조건과 일치하는 파일을 처리하는 방식을 결정하는 규칙이 포함됩니다. 별도의 파일 규칙을 구성하여 각기 다른 파일 유형, 애플리케이션 프로토콜, 또는 전송 방향마다 다른 작업을 실행할 수 있습니다.

파일이 규칙과 일치할 경우, 규칙에서는 다음을 수행할 수 있습니다.

- 간단한 파일 유형 매칭을 기준으로 파일 허용 또는 차단
- 악성코드 파일 속성을 기준으로 파일 차단
- 캡처 파일을 디바이스에 저장
- 동적 분석을 위해 캡처 파일 제출

또한 파일 정책으로 다음을 수행할 수 있습니다.

- 안전 목록 또는 사용자 지정 탐지 목록의 항목을 기준으로 파일을 안전한 파일 또는 악성코드로 자동 처리
- 파일의 위협 점수가 구성 가능한 임계값을 초과할 경우 파일을 악성코드로 처리
- 아카이브 파일(예: `.zip` 또는 `.rar`)의 내용 검사
- 내용이 암호화 및 중첩된 아카이브 파일이 지정된 최대 아카이브 깊이를 넘을 경우 차단하거나, 검사할 수 없도록 구성

단일 파일 정책을 **Allow**, **Interactive Block**, **Interactive Block with reset** 작업이 포함된 액세스 제어 규칙과 연결할 수 있습니다. 그런 다음 시스템에서는 해당 파일 정책을 사용하여 액세스 제어 규칙의 조건에 부합하는 네트워크 트래픽을 검사합니다. 다양한 파일 정책을 서로 다른 액세스 제어 규칙과 연결할 경우, 네트워크에 전송된 파일을 식별하고 차단하는 방법을 세부적으로 제어할 수 있습니다. 그러나 파일 정책을 사용하여 액세스 제어 기본 작업에 의해 처리된 트래픽을 검사할 수는 **없습니다**. 자세한 내용은 18-2페이지의 침입 및 악성코드에 대해 허용된 트래픽 검사을/를 참조하십시오.

파일 규칙

파일 정책을 파일 규칙으로 채웁니다. 다음 표에는 파일 규칙의 구성 요소가 설명되어 있습니다.

표 37-4 파일 규칙 구성 요소

파일 규칙 구성 요소	설명
애플리케이션 프로토콜	시스템에서는 FTP, HTTP, SMTP, IMAP, POP3, NetBIOS-ssn(SMB)을 통해 전송된 파일을 탐지하고 검사할 수 있습니다. 성능을 개선하려는 경우, 파일 규칙당 해당 애플리케이션 프로토콜 중 하나만 대상으로 하여 파일 탐지를 제한할 수 있습니다.
전송 방향	다운로드한 파일의 수신 FTP, HTTP, IMAP, POP3, NetBIOS-ssn(SMB) 트래픽을 검사할 수 있으며, 업로드한 파일의 발신 FTP, HTTP, SMTP, NetBIOS-ssn(SMB) 트래픽을 검사할 수 있습니다.
파일 카테고리 및 유형	시스템에서는 다양한 유형의 파일을 탐지할 수 있습니다. 이러한 파일 유형은 멀티미디어(swf, mp3), 실행 파일(exe, torrent), PDF를 비롯한 기본적인 카테고리로 그룹화됩니다. 개별 파일 유형을 탐지하거나, 파일 유형의 전체 카테고리를 탐지하는 파일 규칙을 구성할 수 있습니다. 예를 들어, 모든 멀티미디어 파일을 차단하거나 ShockWave Flash(swf) 파일만 차단하도록 할 수 있습니다. 또는 사용자가 BitTorrent(torrent) 파일을 다운로드할 경우 알림을 제공하도록 시스템을 구성할 수 있습니다. ⚠ **주의** 자주 트리거되는 파일 규칙은 시스템 성능에 영향을 미칠 수 있습니다. 예를 들어, HTTP 트래픽(예: 상당량의 Flash 콘텐츠를 전송하는 YouTube)의 멀티미디어 파일을 탐지할 경우 지나치게 많은 이벤트가 생성될 수 있습니다.
파일 규칙 작업	파일 규칙 작업에서는 규칙의 조건과 일치하는 트래픽을 처리하는 방법을 결정합니다. **참고** 파일 규칙은 숫자나 순서가 아닌 규칙 작업으로 평가됩니다. 자세한 내용은 다음 절, 파일 규칙 작업 및 평가 순서을/를 참조하십시오.

파일 규칙 작업 및 평가 순서

각 파일 규칙에는 시스템이 규칙의 조건과 매칭되는 트래픽을 처리하는 방법을 결정하는 관련 작업이 포함됩니다. 파일 정책 내에 별도의 규칙을 설정하여 서로 다른 파일 유형, 애플리케이션 프로토콜 또는 전송 방향에 맞는 다양한 조치를 취할 수 있습니다. 규칙 작업은 다음과 같이 규칙-작업의 순서로 이루어집니다.

- *Block Files* 규칙을 사용하면 특정 파일 유형을 차단할 수 있습니다.
- *Block Malware* 규칙을 사용하면 특정 파일 유형의 SHA-256 해시 값을 계산한 후, 클라우드 조회 프로세스를 사용하여 네트워크를 통과하는 파일에 악성코드가 포함되어 있는지 확인한 다음, 위협이 나타난 파일을 차단할 수 있습니다.
- *Malware Cloud Lookup* 규칙을 사용하면 네트워크를 통과하는 파일의 악성코드 속성을 클라우드 조회를 기준으로 로깅하는 동시에, 해당 파일의 전송은 계속 허용할 수 있습니다.
- *Detect Files* 규칙을 사용하면 특정 파일 유형의 탐지 내역을 데이터베이스에 로깅하는 동시에, 해당 파일의 전송은 계속 허용할 수 있습니다.

각 파일 규칙에는 파일 전송이 차단될 때 연결을 재설정하고, 매니지드 디바이스에 캡처 파일을 저장하고, 동적 및 Spero 분석을 위해 캡처 파일을 클라우드에 제출하는 옵션을 구성할 수 있습니다. 다음 표에는 각 파일 작업에 사용할 수 있는 옵션의 세부 정보가 나와 있습니다.

표 37-5 파일 규칙 작업

작업	연결 재설정	파일 저장	동적 분석	MSEXE의 Spero 분석
Block Files	예(권장)	예, 매칭되는 모든 파일 유형을 저장할 수 있음	아니요	아니요
Block Malware	예(권장)	예, 선택한 파일 속성과 매칭되는 파일 유형을 저장할 수 있음	예, 파일 속성이 Unknown인 실행 파일을 제출할 수 있음	예, 실행 파일을 제출할 수 있음
Detect Files	아니요	예, 매칭되는 모든 파일 유형을 저장할 수 있음	아니요	아니요
Malware Cloud Lookup	아니요	예, 선택한 파일 속성과 매칭되는 파일 유형을 저장할 수 있음	예, 파일 속성이 Unknown인 실행 파일을 제출할 수 있음	예, 실행 파일을 제출할 수 있음

파일 및 악성코드 탐지, 캡처, 차단 참고 사항 및 제한 사항

다음 내용은 파일 및 악성코드 탐지, 캡처, 차단 동작에 대한 세부 정보 및 제한 사항입니다.

- 파일의 파일 끝 마커가 탐지되지 않을 경우 전송 프로토콜에 상관없이, 해당 파일은 **Block Malware** 규칙 또는 사용자 지정 탐지 목록에 의해 차단되지 않습니다. 시스템은 파일 끝 마커에 표시된 대로 전체 파일이 수신될 때까지 파일의 차단을 보류하며, 마커가 탐지된 후에 파일을 차단합니다.
- FTP 파일 전송의 파일 끝 마커가 최종 데이터 세그먼트와 별도로 전송된 경우, 해당 마커는 차단되며 FTP 클라이언트는 파일 전송이 실패한 것으로 표시합니다. 그러나 파일은 실제로는 디스크에 완전히 전송됩니다.
- FTP는 다양한 채널을 통해 명령 및 데이터를 전송합니다. 패시브 또는 인라인 탭 모드 구축의 경우, FTP 데이터 세션 및 제어 세션의 트래픽은 동일한 Snort에 대해 로드 밸런싱이 이루어지지 않을 수 있습니다.
- 파일이 애플리케이션 프로토콜 조건이 포함된 규칙과 매치될 경우, 시스템에서 파일의 애플리케이션 프로토콜을 확인한 후 파일 이벤트가 생성됩니다. 확인되지 않은 파일은 파일 이벤트가 생성되지 않습니다.
- FTP용 **Block Malware** 규칙이 포함된 파일 정책을 사용하는 액세스 제어 정책의 경우, **Drop when Inline**이 비활성화된 침입 정책에 기본 작업을 설정하면 시스템에서는 해당 규칙과 매치되는 탐지된 파일 또는 악성코드에 대한 이벤트를 생성하지만 해당 파일을 삭제하지는 않습니다. 파일 정책을 선택할 경우 FTP 파일 전송을 차단하고, 침입 정책을 액세스 제어 정책의 기본 작업으로 사용하려면 **Drop when Inline**이 활성화된 침입 정책을 선택해야 합니다.
- **Block Files** 및 **Block Malware** 작업이 포함된 파일 규칙은 최초 파일 전송 시도가 발생한 후 24시간 동안 탐지된 동일한 파일, URL, 서버, 클라이언트 애플리케이션이 포함된 새로운 세션을 차단함으로써 HTTP를 통해 파일 다운로드가 자동으로 다시 시작되는 것을 차단합니다.
- 드문 경우지만 HTTP 업로드 세션의 트래픽이 순서가 뒤바뀐 경우, 시스템에서는 트래픽을 올바르게 재결합할 수 없으며 결과적으로 이를 차단하거나 파일 이벤트를 생성할 수 없습니다.

- **Block Files** 규칙으로 차단된 NetBIOS-ssn을 통해 파일을 전송할 경우(예: SMB 파일 전송), 대상 호스트에 파일이 표시될 수 있습니다. 그러나 해당 파일은 다운로드가 시작된 후에 차단되었으므로 사용할 수 없으며, 파일 전송이 완료되지 않습니다.
- NetBIOS-ssn을 통해 전송된 파일(예: SMB 파일 전송)을 탐지하거나 차단하는 파일 규칙을 생성할 경우, 시스템에서는 파일 정책을 호출하는 액세스 제어 정책을 적용하기 전에는 설정된 TCP 또는 SMB 세션에서 전송된 파일을 검사하지 않으므로 이러한 파일은 탐지되거나 차단되지 않습니다.
- 패시브 구축 시 파일을 차단하도록 구성된 규칙은 매칭되는 파일을 차단하지 않습니다. 이러한 연결은 파일 전송을 계속 진행하므로, 연결의 시작을 로깅하는 규칙을 구성할 경우 이러한 연결에 대해 로깅한 여러 이벤트가 표시될 수 있습니다.
- POP3, POP, SMTP, IMAP 세션에 있는 파일의 모든 파일 이름의 총 바이트 수가 1024를 초과할 경우, 해당 세션의 파일 이벤트에는 파일 이름 버퍼가 작성된 후 탐지된 파일의 파일 이름이 올바르게 나타나지 않을 수 있습니다.
- SMTP를 통해 텍스트 기반 파일을 전송할 경우, 일부 메일 클라이언트에서는 새 줄을 CRLF 새 줄 문자 표준으로 변환합니다. MAC 기반 호스트는 캐리지 리턴(CR) 문자를 사용하고 Unix/Linux 기반 호스트는 라인 피드(LF) 문자를 사용하므로, 메일 클라이언트에서 새 줄을 변환할 경우 파일의 크기가 수정될 수 있습니다. 일부 메일 클라이언트는 인식할 수 없는 파일 유형을 처리할 경우 새 줄 변환을 기본값으로 설정합니다.
- Cisco 권장 사항에 따르면 **Block Files** 및 **Block Malware** 작업에 **Reset Connection**을 활성화하여, 차단된 애플리케이션 세션이 TCP 연결이 재설정될 때까지 열려 있지 않도록 하는 것이 좋습니다. 연결을 재설정하지 않으면, TCP 연결이 자체적으로 재설정될 때까지 클라이언트 세션이 계속 열려 있게 됩니다.
- **Malware Cloud Lookup** 또는 **Block Malware** 작업이 포함된 파일 규칙이 구성되어 있고 방어 센터에서 클라우드와의 연결을 설정할 수 없는 경우, 시스템에서는 클라우드 연결이 복원될 때까지 구성된 규칙 작업 옵션을 수행할 수 없습니다.
- 많은 양의 트래픽을 모니터링할 경우 모든 캡처 파일을 저장하거나, 동적 분석을 위해 모든 캡처 파일을 제출하지 **마십시오**. 이렇게 하면 시스템 성능이 저하될 수 있습니다.

참고 세션에서 파일이 탐지되고 차단될 때까지, 세션의 패킷은 침입 검사 대상이 될 수 있습니다.

파일 규칙 평가 예

액세스 제어 정책과 달리, 규칙은 숫자 순서로 평가되며 파일 정책은 파일을 37-11페이지의 파일 규칙 작업 및 평가 순서(으)로 처리합니다. 즉, 간단한 차단은 악성코드 검사 및 차단보다 우선하며, 간단한 탐지 및 로깅보다 우선합니다. 단일한 파일 정책에서 PDF 파일을 처리하는 네 가지 규칙의 예를 들어보겠습니다. 웹 인터페이스에 표시되는 순서에 관계없이, 이러한 규칙은 다음과 같은 순서로 평가됩니다.

표 37-6 파일 규칙 평가 순서 예

애플리케이션 프로토콜	방향	작업	작업 옵션	결과
SMTP	업로드	Block Files	연결 재설정	사용자가 PDF 파일을 이메일로 전송하지 못하도록 차단하고 연결을 재설정합니다.
FTP	다운로드	Block Malware	속성이 Unknown인 파일 저장, 연결 재설정	파일 전송을 통한 악성코드 PDF 파일의 다운로드를 차단하고, 파일 속성이 Unknown인 파일을 디바이스에 저장하며, 연결을 재설정합니다.

표 37-6 파일 규칙 평가 순서 예(계속)

애플리케이션 프로토콜	방향	작업	작업 옵션	결과
POP3 IMAP	다운로드	Malware Cloud Lookup	속성이 Unknown인 파일 저장, 동적 분석	이메일을 통해 전송된 PDF 파일의 악성코드 여부를 검사하고, 속성이 Unknown인 파일을 디바이스에 저장합니다. 동적 분석을 위해 파일을 Cisco 클라우드에 제출합니다.
Any	모든	Detect Files	없음	사용자가 웹에서(HTTP를 통해) PDF 파일을 볼 경우, 트래픽을 탐지하고 로깅하되 이를 허용합니다.

방어 센터는 경고 아이콘(⚠)을 사용하여 충돌하는 파일 규칙을 나타냅니다. 자세한 내용은 경고 아이콘 위에 포인터를 두면 확인할 수 있습니다.

시스템에서 탐지한 모든 파일 유형에 악성코드 분석을 수행할 수는 없습니다. **Application Protocol**, **Direction of Transfer**, **Action** 드롭다운 목록에서 값을 선택하면 시스템에서 파일 유형 목록을 제한합니다.

악성코드 라이센스를 DC500에 사용할 수 없으므로, Block Malware 또는 Malware Cloud Lookup 작업을 사용하는 파일 규칙을 생성하거나, 해당 어플라이언스를 사용하여 이러한 작업이 포함된 규칙이 있는 파일 정책을 적용할 수 없습니다. 이와 마찬가지로, 악성코드 라이센스를 Series 2 디바이스 또는 Cisco NGIPS for Blue Coat X-Series에서 활성화할 수 없으므로 이러한 작업이 포함된 규칙이 있는 파일 정책을 해당 어플라이언스에 적용할 수 없습니다.

캡처 파일, 파일 이벤트, 악성코드 이벤트 및 알림 로깅

파일 정책을 액세스 제어 규칙과 연결할 경우, 시스템에서는 매칭되는 트래픽에 대한 파일 및 악성코드 이벤트 로깅을 자동으로 활성화합니다. 파일을 캡처하고 저장하도록 파일 정책을 구성한 경우, 시스템에서는 파일 캡처 시 캡처 파일 로깅도 자동으로 활성화합니다. 시스템이 파일을 검사할 경우, 다음과 같은 유형의 이벤트가 생성됩니다.

- *파일 이벤트* — 탐지되거나 차단된 파일, 탐지된 악성코드 파일을 나타냄
- *악성코드 이벤트* — 탐지된 악성코드 파일을 나타냄
- *회귀적 악성코드 이벤트* — 이전에 탐지된 파일의 Malware 파일 속성이 변경될 경우 생성됨

파일 정책이 파일 또는 악성코드 이벤트를 생성하거나 파일을 캡처할 경우, 시스템에서는 연결된 연결의 끝을 방어 센터 데이터베이스에 자동으로 로깅하며 이는 호출 액세스 제어 규칙의 로깅 컨피그레이션에 상관없이 이루어집니다.

참고 NetBIOS-ssn(SMB) 트래픽을 검사하여 생성되는 파일 이벤트의 경우, 클라이언트와 서버가 지속적인 연결을 설정하므로 연결 이벤트를 즉시 생성하지 않습니다. 시스템에서는 클라이언트 또는 서버 세션이 종료된 후에 연결 이벤트를 생성합니다.

이러한 각 연결 이벤트는 다음과 같습니다.

- **Files** 필드에는 연결에서 탐지된 파일(악성코드 파일 포함)의 개수를 나타내는 아이콘(📄)이 포함됩니다. 해당 파일 및 악성코드 파일, 파일의 속성을 보려면 아이콘을 클릭합니다.
- **Reason** 필드에는 연결 이벤트가 로깅된 사유가 표시되며, 이는 파일 작업 규칙에 따라 다릅니다.
- `File Monitor`는 Detect Files 및 Malware Cloud Lookup 파일 규칙, 안전 목록의 파일에 사용됩니다.
- `File Block`은 Block Files 또는 Block Malware 파일 규칙에 사용됩니다.

- `File Custom Detection`은 시스템이 사용자 지정 탐지 목록에 있는 파일을 발견한 경우 사용됩니다.
- `File Resume Allow`는 처음에 Block Files 또는 Block Malware 파일 규칙에 의해 차단된 파일을 전송할 경우 사용됩니다. 파일을 허용하는 새로운 액세스 제어 정책이 적용되면, HTTP 세션이 자동으로 다시 시작됩니다.
- `File Resume Block`은 처음에 Detect Files 또는 Malware Cloud Lookup 파일 규칙에 의해 허용된 파일을 전송할 경우 사용됩니다. 파일을 차단하는 새로운 액세스 제어 정책이 적용되면, HTTP 세션이 자동으로 중단됩니다.
- 파일 또는 악성코드가 차단된 연결의 경우, 해당하는 **Action**은 `Block`입니다.

FireSIGHT 시스템에 의해 생성된 모든 종류의 이벤트와 마찬가지로, 방어 센터의 웹 인터페이스를 사용하여 파일 및 악성코드 이벤트를 보고, 조작하고, 분석할 수 있습니다. 또한 악성코드 이벤트를 사용하여 상관관계 정책 위반 사항을 트리거하거나 이메일, SMTP 또는 syslog를 통해 알림을 받을 수도 있습니다.

참고 방어 센터는 조직의 FireAMP 서브스크립션을 사용하여 악성코드 이벤트를 수신합니다. 이러한 악성코드 이벤트는 다운로드 또는 실행 시 엔드포인트에서 생성되므로, 해당 정보는 네트워크 기반 악성코드 이벤트와 다릅니다.

연결, 파일, 악성코드 이벤트에 대한 자세한 내용 및 이러한 이벤트를 로깅하는 방법에 대한 추가 정보는 다음을 참조하십시오.

- 38-1페이지의 네트워크 트래픽의 연결 로깅
- 40-8페이지의 파일 이벤트 작업
- 40-17페이지의 악성코드 이벤트 작업
- 39-2페이지의 연결 및 보안 인텔리전스 데이터 이해

인터넷 액세스 및 고가용성

시스템에서는 네트워크 기반 AMP에 포트 443을 사용하여 악성코드 클라우드 조회를 수행합니다. 방어 센터에서 포트 아웃바운드를 열어야 합니다.

파일 정책 및 관련 컨피그레이션은 공유하지만, 고가용성 쌍의 방어 센터는 클라우드 연결이나 캡처 파일, 파일 이벤트, 악성코드 이벤트를 공유하지 않습니다. 운영 연속성을 보장하고, 탐지된 파일의 악성코드 속성을 두 방어 센터에서 동일하게 유지하려면 기본 및 보조 방어 센터에 클라우드에 대한 액세스 권한이 모두 있어야 합니다.

동적 분석을 위해 파일을 클라우드에 제출하려면 디바이스에서 포트 443 아웃바운드를 열어야 합니다.

참고 FireAMP Private Cloud의 열린 포트 및 고가용성 제한 사항은 퍼블릭 Cisco 클라우드 연결과 동일해야 합니다.

파일 정책 관리

기존 파일 정책 목록 및 이러한 정책의 최종 수정 날짜가 함께 표시되는 File Policies 페이지(**Policies > Files**)에서 파일 정책을 생성, 수정, 삭제, 비교합니다.

파일 정책의 적용 아이콘( )을 클릭하면 어떤 액세스 제어 정책이 파일 정책을 사용하는지 알려주는 대화 상자가 표시되며, Access Control Policy 페이지로 리디렉션됩니다. 그 이유는 파일 정책의 경우 상위 액세스 제어 정책의 일부로 간주되므로, 사용자가 파일 정책을 개별적으로 적용할 수 없기 때문입니다. 새로운 파일 정책을 사용하거나, 기존 파일 정책에 구현된 변경 사항을 적용하려면 상위 액세스 제어 정책을 적용하거나 다시 적용해야 합니다.

다음에 유의하십시오.

- 시스템에서는 동적 분석에 적합한 파일 유형의 목록이 업데이트되었는지 클라우드를 확인합니다(하루에 한 번만 수행). 적합한 파일 유형 목록이 변경된 경우, 이는 파일 정책의 변경 사항을 구성합니다. 또한 디바이스에 적용된 경우, 파일 정책을 사용하는 모든 액세스 제어 정책은 기한이 지난 것으로 표시됩니다. 상위 액세스 제어 정책을 다시 적용하여 업데이트된 파일 정책을 디바이스에 적용해야 합니다.
- 저장 또는 적용된 액세스 제어 정책에 사용된 파일 정책은 삭제할 수 없습니다.

파일 정책 관리에 대한 자세한 내용은 다음 절을 참조하십시오.

- 37-16페이지의 파일 정책 생성
- 37-17페이지의 파일 규칙 작업
- 37-23페이지의 두 가지 정책 비교

파일 정책 생성

라이센스: 보호 또는 악성코드

지원되는 디바이스: 기능에 따라 다름

지원되는 Defense Center: 기능에 따라 다름

파일 정책을 생성하고 이를 규칙으로 채운 후에는 액세스 제어 규칙에서 해당 정책을 사용할 수 있습니다.

악성코드 라이센스를 DC500에 사용할 수 없으므로, Block Malware 또는 Malware Cloud Lookup 작업을 사용하는 파일 규칙을 생성하거나, 해당 어플라이언스를 사용하여 이러한 작업이 포함된 규칙이 있는 파일 정책을 적용할 수 없습니다. 이와 마찬가지로, 악성코드 라이센스를 Series 2 디바이스 또는 Cisco NGIPS for Blue Coat X-Series에서 활성화할 수 없으므로 이러한 작업이 포함된 규칙이 있는 파일 정책을 해당 어플라이언스에 적용할 수 없습니다.

팁 기존 파일 정책의 복사본을 만들려면, 복사 아이콘( )을 클릭한 다음, 표시되는 대화 상자에 새 정책의 고유한 이름을 입력합니다. 그런 다음 복사본을 수정할 수 있습니다.

파일 정책을 생성하려면

액세스: Admin/Access Admin

1단계 **Policies > Files**를 선택합니다.

File Policies 페이지가 나타납니다.

2단계 **New File Policy**를 클릭합니다.

New File Policy 대화 상자가 나타납니다.

새 정책의 경우, 웹 인터페이스에 정책이 사용 중이 아닌 것으로 표시됩니다. 사용 중인 파일 정책을 수정하려는 경우, 해당 파일 정책을 사용 중인 액세스 제어 정책의 수가 웹 인터페이스에 표시됩니다. 어떤 경우이든 텍스트를 클릭하여 Access Control Policies 페이지로 이동할 수 있습니다(12-1페이지의 액세스 제어 정책 시작 참조).

3단계 새 정책의 **Name** 및 선택에 따라 **Description**을 입력한 다음 **Save**를 클릭합니다.

File Policy Rules 탭이 나타납니다.

4단계 하나 이상의 규칙을 파일 정책에 추가합니다.

파일 규칙은 악성코드 여부를 로깅, 차단 또는 검사할 파일 유형을 세부적으로 제어할 수 있도록 합니다. 파일 규칙 추가에 대한 자세한 내용은 37-17페이지의 파일 규칙 작업을/를 참조하십시오.

악성코드 라이센스를 DC500에 사용할 수 없으므로, Block Malware 또는 Malware Cloud Lookup 작업을 사용하는 파일 규칙을 생성하거나, 해당 어플라이언스를 사용하여 이러한 작업이 포함된 규칙이 있는 파일 정책을 적용할 수 없습니다. 이와 마찬가지로, 악성코드 라이센스를 Series 2 디바이스 또는 Cisco NGIPS for Blue Coat X-Series에서 활성화할 수 없으므로 이러한 작업이 포함된 규칙이 있는 파일 정책을 해당 어플라이언스에 적용할 수 없습니다.

5단계 고급 옵션을 구성합니다. 자세한 내용은 37-19페이지의 고급 파일 정책의 일반 옵션 구성 및 37-20페이지의 아카이브 파일 검사 옵션 구성을/를 참조하십시오.

6단계 **Save**를 클릭합니다.

새로운 정책을 사용하려면, 파일 정책을 액세스 제어 규칙에 추가한 다음 액세스 제어 정책을 적용해야 합니다. 기존 파일 정책을 수정할 경우, 해당 파일 정책을 사용하는 모든 액세스 제어 정책을 다시 적용해야 합니다.

파일 규칙 작업

라이센스: 보호 또는 악성코드

지원되는 디바이스: 기능에 따라 다름

지원되는 Defense Center: 기능에 따라 다름

효율성을 높이려면 파일 정책에 하나 이상의 규칙을 포함해야 합니다. File Policy Rules 페이지에서 규칙을 생성, 수정, 삭제할 수 있으며 이 페이지는 새로운 파일 정책을 생성하거나 기존 정책을 수정할 때 표시됩니다. 이 페이지에는 정책의 모든 규칙 및 각 규칙의 기본 특성이 함께 나열됩니다.

또한 이 페이지에는 이 파일 정책을 사용하는 액세스 제어 정책의 수가 표시됩니다. 알림을 클릭하여 상위 정책 목록을 표시할 수 있으며, 선택에 따라 Access Control Policies 페이지를 계속 진행할 수 있습니다.

파일 규칙을 생성하려면

액세스: Admin/Access Admin

1단계 **Policies > Files**를 선택합니다.

File Policies 페이지가 나타납니다.

2단계 다음 옵션을 이용할 수 있습니다.

- 규칙을 새로운 정책에 추가하려면 **New File Policy**를 클릭하여 새 정책을 생성합니다(37-16페이지의 파일 정책 생성 참조).
- 규칙을 기존 정책에 추가하려면 정책 옆의 수정 아이콘( )을 클릭합니다.

3단계 표시되는 File Policy Rules 페이지에서 **Add File Rule**을 클릭합니다.

Add File Rule 대화 상자가 나타납니다.

4단계 **Application Protocol**을 선택합니다.

기본값인 **Any**는 HTTP, SMTP, IMAP, POP3, FTP, NetBIOS-ssn (SMB) 트래픽의 파일을 탐색합니다.

5단계 **Direction of Transfer**를 선택합니다.

다운로드한 파일에 대한 다음과 같은 유형의 수신 트래픽을 검사할 수 있습니다.

- HTTP
- IMAP
- POP3
- FTP
- NetBIOS-ssn(SMB)

업로드한 파일에 대한 다음과 같은 유형의 발신 트래픽을 검사할 수 있습니다.

- HTTP
- FTP
- SMTP
- NetBIOS-ssn(SMB)

사용자의 발신 또는 수신 여부에 상관없이, **Any**를 사용하여 여러 애플리케이션 프로토콜의 파일을 탐지합니다.

6단계 파일 규칙 **Action**을 선택합니다. 자세한 내용은 파일 규칙 작업 표를 참조하십시오.

Block Files 또는 Block Malware를 선택할 경우, **Reset Connection**이 기본적으로 활성화됩니다. 차단된 파일의 전송이 이루어지는 연결을 재설정하지 **않으려면** 이 옵션의 선택을 취소합니다.

참고 Cisco 권장 사항에 따르면 **Reset Connection**을 활성화된 상태로 유지하여, 차단된 애플리케이션 세션이 TCP 연결이 재설정될 때까지 열려 있지 않도록 하는 것이 좋습니다.

파일 규칙 작업에 대한 자세한 내용은 37-11페이지의 파일 규칙 작업 및 평가 순서을/를 참조하십시오.

악성코드 라이센스를 DC500에 사용할 수 없으므로, Block Malware 또는 Malware Cloud Lookup 작업을 사용하는 파일 규칙을 생성하거나, 해당 어플라이언스를 사용하여 이러한 작업이 포함된 규칙이 있는 파일 정책을 적용할 수 없습니다. 이와 마찬가지로, 악성코드 라이센스를 Series 2 디바이스 또는 Cisco NGIPS for Blue Coat X-Series에서 활성화할 수 없으므로 이러한 작업이 포함된 규칙이 있는 파일 정책을 해당 어플라이언스에 적용할 수 없습니다.

7단계 하나 이상의 **File Types**를 선택합니다. Shift + Ctrl 키를 사용하여 여러 파일 유형을 선택합니다. 다음과 같은 방법으로 파일 유형 목록을 필터링할 수 있습니다.

- 하나 이상의 **File Type Categories**를 선택합니다.
- 이름 또는 설명으로 파일 유형을 검색합니다. 예를 들어, **Search name and description** 필드에 `Windows`를 입력하여 Microsoft Windows 관련 파일 목록을 표시합니다.

팁 해당 설명을 보려면 파일 유형 위에 마우스 포인터를 올려놓습니다.

파일 규칙에서 사용할 수 있는 파일 유형은 **Application Protocol**, **Direction of Transfer**, **Action**의 선택 사항에 따라 달라집니다.

예를 들어, **Direction of Transfer**로 **Download**를 선택할 경우 **Graphics** 카테고리에서 `GIF`, `PNG`, `JPEG`, `TIFF`, `ICO`가 제거되어 파일 이벤트의 초과를 방지합니다.

8단계 선택한 파일 유형을 **Selected Files Categories and Types** 목록에 추가합니다.

- **Add**를 클릭하여 선택한 파일 유형을 규칙에 추가합니다.
- 하나 이상의 파일 유형을 **Selected Files Categories and Types** 목록에 끌어서 놓습니다.
- 카테고리를 선택한 상태에서 **All types in selected Categories**를 클릭한 다음, **Add**를 클릭하거나 선택 항목을 **Selected Files Categories and Types** 목록에 끌어서 놓습니다.

9단계 **Save**를 클릭합니다.

파일 규칙이 정책에 추가됩니다. 기존 파일 정책을 수정할 경우, 변경 사항을 구현하려면 해당 파일 정책을 사용하는 모든 액세스 제어 정책을 다시 적용해야 합니다.

고급 파일 정책의 일반 옵션 구성

라이센스: 악성코드

지원되는 디바이스: 기능에 따라 다름

지원되는 Defense Center: 기능에 따라 다름

파일 정책의 경우, General 섹션에서 다음 고급 옵션을 설정할 수 있습니다. 고급 Archive File Inspection 옵션에 대한 자세한 내용은 37-20페이지의 아카이브 파일 검사 옵션 구성을/를 참조하십시오.

표 37-7 고급 파일 정책의 일반 옵션

필드	설명	기본값
Enable Custom Detection List	탐지된 경우 이 필드를 선택하여 사용자 지정 탐지 목록의 파일을 차단합니다.	활성화
Enable Clean List	탐지된 경우 이 필드를 선택하여 안전 목록의 파일을 허용합니다.	활성화
Mark files as malware based on dynamic analysis threat score	위협 점수가 있거나 높은 경우, 파일을 자동으로 악성코드로 처리하기 위한 임계값을 선택합니다. 이 필드를 사용하지 않으려면 **Disabled**를 선택합니다. 낮은 임계값을 선택하면 악성코드로 처리되는 파일 수가 늘어납니다. 파일 정책에서 선택한 작업에 따라, 이렇게 하면 차단되는 파일의 수가 늘어날 수 있습니다.	매우 높음 (76 이상)

악성코드 라이센스를 DC500에 사용할 수 없으므로, 이러한 설정을 사용하거나 수정할 수 없습니다. 이와 마찬가지로, 악성코드 라이센스를 Series 2 디바이스 또는 Cisco NGIPS for Blue Coat X-Series에서 활성화할 수 없으므로 이러한 설정이 활성화된 상태에서는 파일 정책을 적용할 수 없습니다.

고급 파일 정책의 일반 옵션을 구성하려면

액세스: Admin/Access Admin

1단계 **Policies > Files**를 선택합니다.

File Policies 페이지가 나타납니다.

2단계 수정할 정책 옆에 있는 수정 아이콘( )을 클릭합니다.

File Policy Rule 페이지가 나타납니다.

3단계 **Advanced** 탭을 선택합니다.

Advanced 탭이 나타납니다.

4단계 **General** 섹션에서, 고급 파일 정책의 일반 옵션 표에 설명된 대로 옵션을 수정합니다.

5단계 **Save**를 클릭합니다.

수정한 파일 정책을 사용하는 모든 액세스 제어 정책을 다시 적용해야 합니다.

아카이브 파일 검사 옵션 구성

라이센스: 악성코드

지원되는 디바이스: Series 2 또는 X-Series를 제외한 모두

지원되는 Defense Center: DC500을 제외한 모두

아카이브 파일(예: `.zip` 또는 `.rar`)이 모니터링된 트래픽에 나타나는 경우가 종종 있습니다. 일부 파일은 합법적인 정보를 압축하고 전송할 수 있는 편리한 수단에 불과하지만, 어떤 파일은 악성코드를 숨기려고 하거나 바람직하지 않은 파일인 경우가 있습니다. 아카이브 파일의 내용을 검사하도록 파일 정책을 구성하여, 조직의 요구 사항에 따라 아카이브 파일을 분석하고 선택에 따라 차단할 수 있습니다. 압축되지 않은 파일에 적용 가능한 모든 기능(예: 동적 분석 및 파일 저장)은 아카이브 파일 내부의 중첩된 파일에도 사용할 수 있습니다. 컨텍스트 메뉴를 사용하여 이벤트 뷰어 또는 파일 전파 흔적 분석 뷰어에서 아카이브 파일의 내용을 볼 수 있습니다. 자세한 내용은 다음 섹션 37-22페이지의 아카이브 파일의 내용 보기을/를 참조하십시오.

참고 보안 인텔리전스에 의해 블랙리스트 또는 화이트리스트에 추가된 아카이브 파일이 트래픽에 포함되어 있거나, 최상위 아카이브 파일의 SHA-256 값이 사용자 지정 탐지 목록에 있는 경우 시스템에서는 아카이브 파일의 내용을 검사하지 않습니다. 중첩된 파일이 블랙리스트에 추가되면 전체 아카이브가 차단됩니다. 그러나 중첩된 파일이 화이트리스트에 추가되면 아카이브가 자동으로 통과되지 않습니다(기타 중첩된 파일 및 특성에 따라 달라짐). 자세한 내용은 3-7페이지의 전역 화이트리스트 및 블랙리스트 작업을/를 참조하십시오.

일부 아카이브 파일에는 추가 아카이브 파일 등이 포함됩니다. 파일이 중첩되는 수준은 *아카이브 파일 깊이*에 해당합니다. 최상위 아카이브 파일은 깊이 계산 시 고려되지 않으며, 깊이는 처음 중첩된 파일을 기점으로 1부터 시작합니다. 시스템은 최대 3가지 수준의 중첩된 아카이브 파일만 검사할 수 있으나, 해당 깊이를 넘는(또는 지정된 하위 최대 깊이) 아카이브 파일을 차단하도록 파일 정책을 구성할 수 있습니다. 중첩된 아카이브를 더 세밀하게 제한하려면, 하위 최대 파일 깊이인 2 또는 1로 옵션을 구성합니다. 최대 아카이브 파일 깊이인 3을 초과하는 파일을 차단하지 않도록 선택하면, 추출 가능한 내용이 아카이브 파일에 포함되고 3보다 큰 깊이로 중첩된 내용이 모니터링 트래픽에 표시될 경우 시스템에서는 검사할 수 있는 파일에 대해서만 데이터를 검사하고 보고합니다.

아카이브 파일은 포함된 파일의 속성을 기준으로 파일 속성을 수신합니다. 식별된 악성코드 파일을 포함하는 **모든** 아카이브는 `Malware`라는 속성이 제공됩니다. 식별된 악성코드 파일이 없는 아카이브의 경우 알 수 없는 파일이 포함되어 있으면 `Unknown`이라는 속성이 제공되고, 안전한 파일만 포함되어 있으면 `Clean`이라는 속성이 제공됩니다. 파일 속성에 대한 자세한 내용은 37-3페이지의 파일 속성 이해을/를 참조하십시오.

다음 표에는 파일 정책에서 구성할 수 있는 아카이브 파일 검사 옵션이 나열되어 있습니다.

표 37-8 아카이브 파일 검사 옵션

필드	설명	기본값
Inspect Archives	아카이브 파일의 내용을 검사하려면 이 필드를 선택합니다. 이 옵션을 선택하지 않으면 아래 옵션이 회색으로 표시되고 사용할 수 없습니다.	비활성화
Block Encrypted Archives	암호화된 내용이 포함된 아카이브 파일을 차단하려면 이 필드를 선택합니다.	비활성화
Block Uninspectable Archives	시스템에서 암호화 이외의 이유로 검사를 수행할 수 없는 내용이 포함된 아카이브 파일을 차단하려면 이 필드를 선택합니다(이러한 현상은 주로 손상된 파일 또는 지정된 최대 아카이브 깊이를 초과하는 파일에 적용됨).	활성화
Max Archive Depth	중첩된 아카이브 파일의 최대 깊이를 지정합니다. 이 깊이를 초과하는 아카이브 파일은 차단됩니다. `1`, `2`, `3` 사이의 값이어야 합니다. 최상위 아카이브 파일은 이 계산에서 고려되지 않으며, 깊이는 처음 중첩된 파일을 기점으로 1부터 시작합니다.	2

아카이브 파일 검사 옵션을 구성하려면

액세스: Admin/Access Admin

1단계 **Policies > Files**를 선택합니다.

File Policies 페이지가 나타납니다.

2단계 수정할 정책 옆에 있는 수정 아이콘()을 클릭합니다.

File Policy Rule 페이지가 나타납니다.

3단계 **Advanced** 탭을 선택합니다.

Advanced 탭이 나타납니다.

4단계 **Archive File Inspection** 섹션에서, 아카이브 파일 검사 옵션에 설명된 대로 옵션을 수정합니다.

5단계 **Save**를 클릭합니다.

수정한 파일 정책을 사용하는 모든 액세스 제어 정책을 다시 적용해야 합니다.

아카이브 파일의 내용 보기

라이센스: 악성코드

지원되는 디바이스: Series 2 또는 X-Series를 제외한 모두

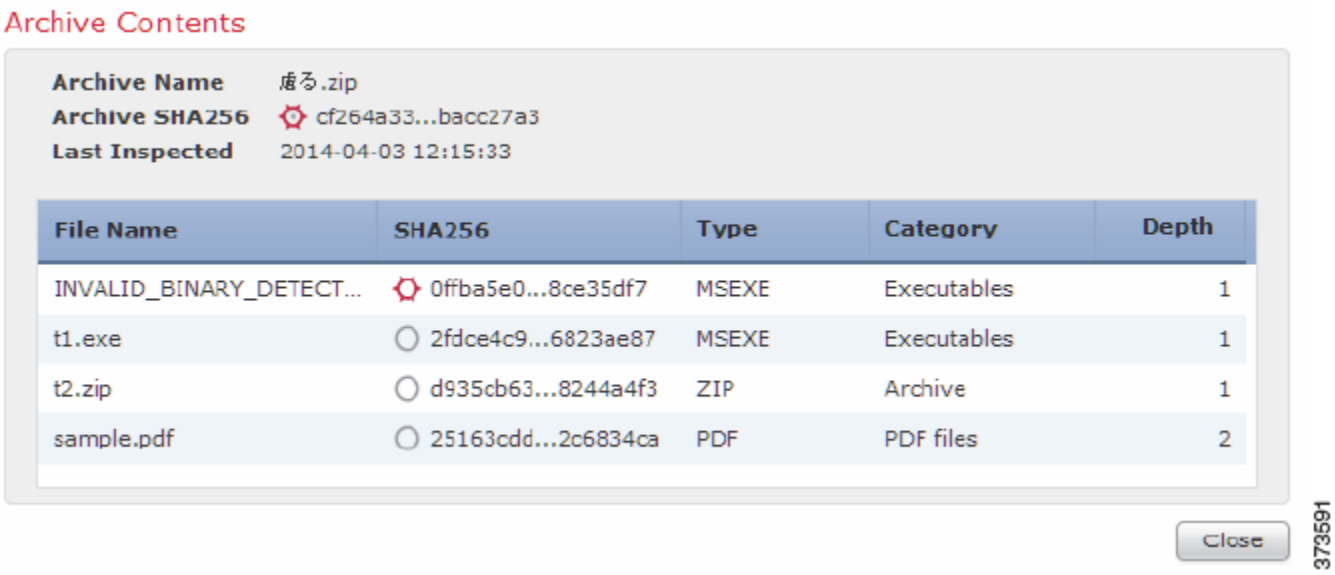
지원되는 Defense Center: DC500을 제외한 모두

아카이브 파일 내용을 검사하도록 파일 정책을 구성할 경우, 이벤트 뷰어 컨텍스트 메뉴 및 네트워크 파일 전파 흔적 분석 뷰어를 사용하면 아카이브 파일이 파일 이벤트, 악성코드 이벤트에 표시되거나 캡처 파일로 표시될 때 아카이브 내부의 파일에 대한 정보를 볼 수 있습니다.

자세한 내용은 다음 링크를 참고하십시오.

- 2-5페이지의 컨텍스트 메뉴 사용
- 40-8페이지의 파일 이벤트 보기
- 40-19페이지의 악성코드 이벤트 보기
- 40-31페이지의 캡처된 파일 보기
- 40-37페이지의 네트워크 파일 전파 흔적 검토

Archive Contents 창을 두 가지 방식으로 볼 수 있습니다. 이벤트 뷰어에서 마우스 오른쪽 버튼으로 적합한 아카이브 파일을 클릭한 후 컨텍스트 메뉴에서 **View Archive Contents**를 선택하거나, 아카이브 파일의 파일 전파 흔적 분석 뷰에서 **Archive Contents** 아래의 보기 아이콘( )을 클릭합니다. 두 경우 모두 동일한 창이 표시됩니다. 다음 그래픽은 Archive Contents 창의 예입니다.



아카이브의 모든 파일 내용은 표 형식으로 나열되며, 관련 정보(이름, SHA-256 해시 값, 유형, 카테고리, 아카이브 깊이)가 짧게 요약되어 있습니다. 네트워크 파일 전파 흔적 분석 아이콘은 각 파일에 표시되며, 이를 클릭하면 Network Trajectory 기능에 따라 특정 파일에 대한 추가 정보를 볼 수 있습니다.

이벤트 뷰어에서 아카이브 파일의 내용을 보려면

액세스: Admin/Access Admin

1단계 선택한 이벤트 뷰어로 이동합니다. 3가지 옵션이 제공됩니다.

- 악성코드 이벤트의 경우 **Analysis > Files > Malware Events**를 선택합니다.
- 파일 이벤트의 경우 **Analysis > Files> File Events**를 선택합니다.
- 캡처 파일의 경우 **Analysis > Files > Captured Files**를 선택합니다.

기본 이벤트 워크플로의 첫 번째 페이지가 표시됩니다.

2단계 검사할 아카이브 파일이 표시되는 표 행을 마우스 오른쪽 버튼으로 클릭합니다.

컨텍스트 메뉴가 나타납니다.

3단계 컨텍스트 메뉴에서 **View Archive Contents**를 클릭합니다.

Archive Contents 창이 나타납니다.

파일 전파 흔적 분석 뷰어에서 아카이브 파일의 내용을 보려면

액세스: Admin/Access Admin

1단계 **Analysis > Files > Network File Trajectory**를 선택합니다.

Network File Trajectory List 페이지가 나타납니다.

2단계 검사할 아카이브 파일의 파일 전파 흔적 분석 아이콘( )을 클릭합니다.

해당 파일의 파일 전파 흔적 분석 페이지가 표시됩니다.

3단계 **Archive Contents** 아래에서 보기 아이콘( )을 클릭합니다.

Archive Contents 창이 나타납니다.

두 가지 정책 비교

라이센스: 보호

정책 변경 사항이 조직의 표준을 준수하거나 시스템 성능을 최적화하는지 검토하려는 경우, 두 가지 파일 정책의 차이점을 살펴보거나 동일한 정책의 두 가지 수정 버전을 살펴볼 수 있습니다.

파일 정책 *비교 보기*에는 두 가지 파일 정책 또는 수정 버전이 나란히 표시되며, 각 정책의 이름 옆에 최종 수정 시간 및 최종 수정한 사용자가 함께 표시됩니다. 두 정책 간의 차이점이 강조 표시됩니다.

- 파란색은 강조 표시된 설정이 두 정책에서 다름을 의미하며, 그 차이점이 빨간색 텍스트로 표시됩니다.
- 녹색은 강조 표시된 설정이 둘 중 한 정책에만 나타남을 의미합니다.

Previous 및 **Next**를 클릭하여 차이점을 탐색할 수 있습니다. 왼쪽과 오른쪽 사이의 중앙에 있는 이중 화살표 아이콘( )이 움직이고, 어떤 차이점을 보고 있는지 식별할 수 있도록 **Difference** 번호가 조정됩니다. 선택에 따라, 비교 보기의 PDF 버전인 파일 정책 *비교 보고서*를 생성할 수 있습니다.

두 가지 파일 정책을 비교하려면

액세스: Admin/Access Admin

1단계 **Policies > Files**를 선택합니다.

File Policies 페이지가 나타납니다.

2단계 **Compare Policies**를 클릭합니다.

Select Comparison 대화 상자가 표시됩니다.

3단계 **Compare Against** 드롭다운 목록에서 원하는 비교 유형을 선택합니다.

- 두 가지 다른 정책을 비교하려면 **Running Configuration** 또는 **Other Policy**를 선택합니다. 두 옵션의 실제 차이점은 **Running Configuration**을 선택할 경우, 비교 선택 항목 중 하나가 현재 적용된 파일 정책 집합으로 제한된다는 점입니다.
- 동일한 정책의 수정 버전을 비교하려면 **Other Revision**을 선택합니다.

대화 상자가 새로 고쳐지고 비교 옵션이 표시됩니다.

4단계 선택한 비교 유형에 따라 다음을 선택할 수 있습니다.

- 두 가지 다른 정책을 비교할 경우, **Policy A** 또는 **Target/Running Configuration A** 및 **Policy B** 중에서 비교할 정책을 선택합니다.
- 동일한 정책의 수정 버전을 비교할 경우, 사용할 **Policy**를 선택한 다음 두 가지 수정 버전인 **Revision A** 및 **Revision B**를 선택합니다. 수정 버전은 날짜 및 사용자 이름을 기준으로 나열됩니다.

5단계 **OK**를 클릭합니다.

비교 보기가 나타납니다.

6단계 선택에 따라, **Comparison Report**를 클릭하여 액세스 제어 정책 비교 보고서를 생성합니다.

비교 보고서가 표시됩니다. 브라우저 설정에 따라 보고서가 팝업 창에 나타날 수 있으며, 컴퓨터에 보고서를 저장하는 프롬프트가 표시될 수도 있습니다.

FireAMP를 위한 클라우드 연결 작업

라이센스: 모든

FireAMP는 Cisco의 엔터프라이즈급 고급 악성코드 분석 및 보호 솔루션입니다. 조직에서 FireAMP 서브스크립션을 보유한 경우 개별 사용자는 컴퓨터와 모바일 디바이스에 FireAMP Connector를 설치할 수 있습니다. 이와 같이 가벼운 에이전트는 Cisco 클라우드와 통신하며, Cisco 클라우드는 방어 센터와 통신합니다. 방어 센터를 클라우드에 연결하도록 구성한 후 검사, 악성코드 탐지, 격리에 대한 레코드를 수신할 수 있습니다. 이러한 레코드는 방어 센터 데이터베이스에 악성코드 이벤트로 저장됩니다. 자세한 내용은 37-2페이지의 악성코드 차단 및 파일 제어 이해을/를 참조하십시오.

조직의 보안 정책이 기존 클라우드 서버 연결의 사용을 허용하지 않는 경우 Cisco의 프라이빗 온프레미스 클라우드 솔루션인 FireAMP Private Cloud를 구입하여 구성할 수 있습니다. 이 솔루션은 퍼블릭 Cisco 클라우드의 압축된 로컬 버전 역할을 하는 가상 머신입니다. 이 경우, 일반적으로 클라우드 연결이 수반되는 데이터 및 작업(예: FireAMP 커넥터의 이벤트, 파일 속성 조회, 회귀적 이벤트 등)은 프라이빗 클라우드에 대한 로컬 연결로 대신 처리됩니다. 외부 클라우드에 연결해야 할 경우(예: 파일 속성 조회), 프라이빗 클라우드는 방어 센터와 Cisco 클라우드 간의 익명 프록시 역할을 수행합니다. 프라이빗 클라우드를 사용할 경우, 외부 연결을 통해 엔드포인트 이벤트 데이터가 공유되지 않습니다. 프라이빗 클라우드 구성에 대한 자세한 내용은 37-27페이지의 FireAMP Private Cloud 작업을/를 참조하십시오.

참고 프라이빗 클라우드는 동적 분석을 지원하지 않습니다.

FireAMP Connector가 설치된 호스트에서는 해당 호스트에서 탐지된 엔드포인트 기반 악성코드 탐지 작업을 통해 호스트의 보안이 침해되었을 수 있음을 알 수 있는 경우 IOC(보안 침해 지표) 태그를 생성할 수도 있습니다. 방어 센터에서 호스트에 대한 엔드포인트 IOC 정보를 보려면 해당 호스트가 방어 센터의 네트워크 맵에 표시되어야 합니다. Cisco에서는 수시로 엔드포인트 기반 악성코드 이벤트의 새로운 IOC 유형을 개발하며, 이 유형은 Cisco 클라우드에서 해당 시스템으로 자동으로 다운로드됩니다. IOC에 대한 자세한 내용은 45-20페이지의 IOC 이해 및 45-20페이지의 엔드포인트 기반 악성코드 이벤트 IOC 유형을/를 참조하십시오.

구축 환경의 각 방어 센터는 Cisco 클라우드에 연결할 수 있습니다. 기본적으로 클라우드는 조직 내의 모든 그룹에 대한 악성코드 이벤트를 전송할 수 있으나, 연결 구성 시 이를 그룹별로 제한할 수 있습니다.

인터넷 액세스 및 고가용성

시스템에서는 포트 443/HTTPS를 사용해 Cisco 클라우드(퍼블릭 또는 프라이빗)에 연결하여 엔드포인트 기반 악성코드 이벤트를 수신합니다. 인바운드 및 아웃바운드 모두 방어 센터에서 포트를 열어야 합니다. 또한 방어 센터는 인터넷에 직접 액세스해야 합니다. 기본 상태 정책에는 FireAMP Status Monitor가 포함되며, 이는 방어 센터가 처음 연결에 성공한 후 클라우드에 연결할 수 없는 경우 또는 FireAMP 포털을 사용하여 연결의 등록이 취소된 경우 경고 메시지를 제공합니다.

엔드포인트 기반 악성코드 이벤트를 수신하는 클라우드 연결은 고가용성 쌍의 구성원 간에 이벤트를 공유하지 **않습니다**. 운영 연속성을 보장하기 위해, 기본 및 보조 방어 센터를 클라우드에 연결합니다.

클라우드 연결 관리

방어 센터의 AMP Management 페이지(**AMP > AMP Management**)를 사용하여 Cisco 클라우드 또는 프라이빗 클라우드에 대한 연결을 보고 생성할 뿐만 아니라, 해당 연결을 비활성화하고 삭제할 수 있습니다.

회전하는 상태의 아이콘은 연결이 보류 중임을 나타냅니다. 이를테면, 방어 센터에서 연결을 구성했으나, 이제 FireAMP 포털을 사용하여 연결에 권한을 부여해야 하는 경우를 예로 들 수 있습니다. 오류 또는 거부 아이콘( )은 클라우드에서 연결을 거부했거나 다른 이유로 인해 연결이 실패했음을 나타냅니다.

팁 새 브라우저 창에서 FireAMP 포털을 열려면 임의의 클라우드 이름을 클릭합니다.

자세한 내용은 다음 링크를 참고하십시오.

- 37-26페이지의 클라우드 Cisco연결 생성
- 37-27페이지의 클라우드 연결 삭제 또는 비활성화
- 37-27페이지의 FireAMP Private Cloud 작업

클라우드 Cisco연결 생성

라이센스: 모든

방어 센터와 Cisco 클라우드 간의 연결을 생성하는 작업은 두 단계의 프로세스로 구성됩니다. 우선, 방어 센터를 클라우드에 연결합니다. 그런 다음 FireAMP 포털에 로그인하여 연결에 권한을 부여합니다. FireAMP 서브스크립션이 없는 경우, 등록 프로세스를 완료할 수 없습니다.

공장 기본값으로 복원되었거나 클라우드에 등록될 때 변환된 방어 센터를 다시 등록하려면, FireAMP를 연결하고 이를 다시 등록하기 전에 방어 센터를 제거해야 합니다.

FireAMP에 대한 Cisco 클라우드 연결을 생성하려면

액세스: 관리자

1단계 **AMP > AMP Management**를 선택합니다.

AMP Management 페이지가 나타납니다.

2단계 **Create FireAMP Connection**을 클릭합니다.

Create FireAMP Connection 대화 상자가 나타납니다.

3단계 **Cloud Name** 드롭다운 상자에서 사용할 클라우드를 선택합니다.

- 유럽 연합 클라우드의 경우 **EU Cloud**를 선택합니다.
- 미국 클라우드의 경우 **US Cloud**를 선택합니다.
- 프라이빗 클라우드의 경우 **Private Cloud**를 선택한 다음 37-27페이지의 FireAMP Private Cloud 작업에 따라 추가 단계를 수행합니다.

4단계 **Register**를 클릭합니다.

5단계 FireAMP 포털을 계속 진행할 것인지 확인하고 포털에 로그인합니다.

포털에 Applications 페이지가 표시됩니다. 이 페이지를 사용하여 악성코드 이벤트를 방어 센터에 전송할 수 있도록 Cisco에 권한을 부여합니다.

6단계 선택에 따라, 악성코드 이벤트를 수신할 조직 내에서 특정 그룹을 선택합니다.

수신하는 이벤트를 제한하려는 경우에만 그룹을 선택합니다. 기본적으로 방어 센터에서는 모든 그룹의 악성코드 이벤트를 수신합니다.

팁 그룹을 관리하려면 FireAMP 포털에서 **Management > Groups**를 선택합니다. 자세한 내용은 포털의 온라인 도움말을 참조하십시오.

7단계 **Allow**를 클릭합니다.

방어 센터의 FireAMP Management 페이지로 돌아갑니다. 연결이 활성화되며 방어 센터는 클라우드에서 악성코드 이벤트를 수신하기 시작합니다.

Deny를 클릭할 경우에도 방어 센터로 돌아오며, 이 경우 클라우드 연결이 거부된 것으로 표시됩니다. 이와 마찬가지로, FireAMP 포털에서 Applications 페이지를 벗어나 연결을 거부하거나 허용할 경우, 방어 센터의 웹 인터페이스에 연결이 보류 중인 것으로 표시됩니다. 상태 모니터링은 이러한 상황에 대해 알림을 제공하지 **않습니다**. 나중에 클라우드에 연결하려면 실패하거나 보류 중인 연결을 삭제한 다음 다시 생성해야 합니다.

클라우드 연결 삭제 또는 비활성화

라이센스: 모든

클라우드에서 악성코드 이벤트를 더 이상 수신하지 않으려면 Cisco 클라우드 연결 또는 프라이빗 클라우드 연결을 삭제합니다. 특정 연결에 대한 악성코드 이벤트 수신을 일시적으로 중단하려면, 연결을 삭제하는 대신 이를 비활성화할 수 있습니다. 이 경우 클라우드는 연결이 다시 활성화될 때까지 이벤트를 저장하며, 클라우드는 그 후에야 저장된 이벤트를 전송합니다.

주의 드문 경우지만 이벤트 속도가 매우 빠르거나 연결이 장기적으로 비활성화된 경우, 클라우드에서는 연결이 비활성화된 동안 생성된 모든 이벤트를 저장하지 못할 수 있습니다.

방어 센터의 웹 인터페이스 대신 FireAMP 포털을 사용하여 연결의 등록을 취소할 경우, 이벤트 전송이 중단되지만 방어 센터의 연결은 제거되지 않습니다. 등록 취소된 연결은 FireAMP Management 페이지에 실패 상태가 표시되며 해당 연결은 삭제해야 합니다.

방어 센터를 사용하여 클라우드 연결을 활성화 또는 비활성화하려면

액세스: Admin

1단계 AMP Management 페이지에서, 삭제할 연결 옆의 슬라이더를 클릭한 다음 연결을 활성화 또는 비활성화할 것을 확인합니다.

연결을 활성화하면 클라우드가 방어 센터로 이벤트 수신을 시작하며, 여기에는 연결이 비활성화된 동안 일어난 모든 이벤트가 포함됩니다. 클라우드는 비활성화된 연결에는 이벤트를 전송하지 않습니다.

방어 센터를 사용하여 클라우드 연결을 삭제하려면

액세스: Admin

1단계 AMP Management 페이지에서, 삭제할 연결 옆의 삭제 아이콘( )을 클릭한 다음 연결을 제거할 것을 확인합니다.

연결이 제거되며 클라우드는 방어 센터로 이벤트 전송을 중단합니다.

FireAMP Private Cloud 작업

라이센스: 모든

조직에 개인 정보 또는 보안 문제가 있을 경우, 이는 모니터링된 네트워크와 외부 클라우드 서버 간에 연결이 잘되지 않거나 아예 불가능한 상황이 자주 발생하는 원인이 됩니다. 이 경우 네트워크와 Cisco FireAMP 클라우드 간의 보안 중재자 역할을 하는 독점적인 Cisco 가상 머신인 FireAMP Private Cloud를 구입하여 구성할 수 있습니다. 많은 어플라이언스의 식별 가능한 연결 대신, 퍼블릭 외부 Cisco 클라우드에 대한 모든 필요한 연결은 프라이빗 클라우드를 통해 이동되며, 이러한 프라이빗 클라우드는 모니터링된 네트워크의 보안과 개인 정보를 보장하는 익명 프록시 역할을 합니다. 각 프라이빗 클라우드는 최대 10,000개의 개별 커넥터를 지원할 수 있습니다. 네트워크에 여러 프라이빗 클라우드를 구성하여 조직의 요구 사항을 충족할 수 있습니다.

FireAMP Private Cloud는 파일 속성 조회, 엔드포인트 기반 FireAMP 이벤트 검색, 회귀적 악성코드 이벤트 생성의 클라우드 기반 작업을 처리합니다. 퍼블릭 클라우드 대신 역할을 수행하는 프라이빗 클라우드는 FireAMP Connector 엔드포인트에서 악성코드 이벤트를 수집하고 이를 방어 센터에 전송합니다. 익명화되고 프록시화된 클라우드 연결을 통해, 퍼블릭 Cisco 클라우드에 대한 쿼리(파일 속성, SHA-256 값 등 확인)만 네트워크에 유지됩니다. 엔드포인트 이벤트 데이터는 네트워크를 벗어나지 않습니다.

클라우드 기반 파일 및 악성코드 기능에 대한 자세한 내용은 다음을 참조하십시오.

- 37-2페이지의 악성코드 차단 및 파일 제어 이해
- 37-7페이지의 FireSIGHT 시스템와 FireAMP통합
- 40-4페이지의 동적 분석 작업
- 40-17페이지의 엔드포인트 기반(FireAMP) 악성코드 이벤트
- 40-18페이지의 소급 악성코드 이벤트

프라이빗 클라우드의 지원되는 기능과 관련된 본 설명서 및 다른 설명서에서, "클라우드" 또는 "Cisco 클라우드"에 대한 모든 참조는 달리 명시되지 않는 한 프라이빗 클라우드를 통한 연결에 해당됩니다. 프라이빗 클라우드의 열린 포트 및 고가용성 제한 사항은 표준 클라우드 연결과 동일해야 합니다.

참고 FireAMP Private Cloud는 악성코드 및 파일과 관련된 클라우드 기반 기능만 지원합니다. URL 또는 보안 인텔리전스 같은 클라우드 연결을 사용하는 다른 FireSIGHT 시스템 기능은 지원하지 않습니다. 또한 프라이빗 클라우드를 사용하여 Cisco에서 기존에 동적으로 분석한 파일의 위협 점수를 검색할 수는 있으나, 프라이빗 클라우드에서는 동적 분석 기능을 지원하지 않습니다.

방어 센터와 FireAMP Private Cloud 간에 연결을 생성하려면, 지원 사이트에서 제공되는 *FireAMP Private Cloud Administration Portal User Guide*의 절차에 따라 FireAMP Private Cloud를 먼저 구성해야 합니다. 이 컨피그레이션을 수행하는 동안, **FireAMP Console** 필드에 프라이빗 클라우드 호스트 이름이 표시되는지 확인해야 합니다. 프라이빗 클라우드를 방어 센터에 연결하려면 이 호스트 이름이 있어야 합니다. 프라이빗 클라우드가 올바르게 구성되면 이전에 구성된 모든 퍼블릭 클라우드 연결이 자동으로 비활성화됩니다.

방어 센터와 FireAMP Private Cloud 간에 연결을 생성하려면

액세스: Admin

1단계 **AMP > AMP Management**를 선택합니다.

AMP Management 페이지가 나타납니다.

2단계 **Create FireAMP Connection**을 클릭합니다.

Create FireAMP Connection 대화 상자가 나타납니다.

3단계 **Cloud Name** 드롭다운 목록에서 **Private Cloud**를 선택합니다.

추가 필드가 대화 상자에 표시됩니다.

4단계 **Name** 필드에 프라이빗 클라우드 연결의 이름을 입력합니다. 이 이름은 악성코드 이벤트를 볼 때 FireAMP Cloud 이벤트 필드에 표시됩니다.

5단계 FireAMP Private Cloud 가상 머신을 구성할 때 FireAMP Console 필드에 표시되는 프라이빗 클라우드의 호스트 이름을 **Host** 필드에 입력합니다.

6단계 **Certificate Upload Path** 필드에서 프라이빗 클라우드에 대한 TLS 또는 SSL 암호화 인증서 정보의 위치를 찾습니다. 자세한 내용은 *FireAMP Private Cloud Administration Portal User Guide*를 참조하십시오.

7단계 모니터링된 네트워크에 여러 개의 프라이빗 클라우드를 구성한 상태이고 어떤 프라이빗 클라우드에서 네트워크 기반 악성코드 조회를 처리하는지 확인하려면, **Use For NetworkAMP** 확인란을 선택하거나 취소합니다. 프라이빗 클라우드를 하나만 구성한 경우, 이 확인란은 기본적으로 선택되어 있으며 취소할 수 없습니다.

8단계 방어 센터에 프록시 연결을 구성한 상태이고 프라이빗 클라우드에 프록시 연결을 사용하려는 경우, **Use Proxy for Connection** 확인란을 선택합니다. 이 옵션을 선택하지 않으면, 프라이빗 클라우드에서는 구성된 프록시를 통신에 사용하지 **않습니다**.

9단계 **Register**를 클릭합니다.

프라이빗 클라우드 컨피그레이션을 생성할 경우 기존에 구성한 모든 퍼블릭 클라우드 연결이 비활성화된다는 내용을 알리는 대화 상자가 표시됩니다.

10단계 **Yes**를 클릭합니다.

FireAMP 포털을 계속 진행할 것인지 확인하고 포털에 로그인합니다.

11단계 시스템은 프라이빗 클라우드 정보를 처리하고 FireAMP 사이트로 사용자를 리디렉션하여 컨피그레이션을 완료합니다. 추가 지침을 보려면 *FireAMP Private Cloud Administration Portal User Guide*를 참조하십시오.

38장

네트워크 트래픽의 연결 로깅

관리 대상 디바이스는 네트워크의 호스트에서 생성되는 트래픽을 모니터링하면서 탐지한 연결에 대한 로그를 생성할 수 있습니다. 액세스 제어 및 SSL 정책의 다양한 설정을 통해 어떤 연결을 로깅하고 언제 로깅하며 그 데이터를 어디에 저장하는가를 세부적으로 제어할 수 있습니다. 액세스 제어 규칙의 구체적인 로깅 컨피그레이션에 의해 연결과 관련된 파일 및 악성코드 이벤트의 로깅 여부도 결정됩니다.

대부분의 경우, 연결의 시작, 종료 또는 둘 다에서 로깅할 수 있습니다. 어떤 연결을 로깅하면 *연결 이벤트*가 생성됩니다. 또한 평판 기반의 Security Intelligence 기능에서 어떤 연결을 블랙리스트에 포함할 때마다, 즉 차단할 때마다 *Security Intelligence 이벤트*라는 특별한 종류의 연결 이벤트를 로깅할 수 있습니다.

연결 이벤트는 탐지된 세션에 대한 데이터를 포함합니다. 임의의 개별 연결 이벤트에 대해 제공되는 이 정보는 여러 요인에 좌우되지만, 일반적으로 여기에는 다음 항목이 포함됩니다.

- 기본 연결 속성: 타임스탬프, 소스 및 목적지 IP 주소, 인그레스 및 이그레스 영역, 연결을 처리한 디바이스 등
- 시스템에서 검색했거나 추론한 추가 연결 속성: 연결과 관련된 애플리케이션, 요청된 URL, 사용자 등
- 연결이 로깅된 이유에 대한 메타데이터: 정책에서 트래픽을 처리하는 데 적용한 액세스 제어 규칙(또는 기타 컨피그레이션), 연결 허용 또는 차단 여부, 암호화되고 해독된 연결에 대한 세부사항 등

조직의 보안 및 규정준수 요구 사항에 따라 연결을 로깅해야 합니다. 액세스 제어에 앞서 디바이스 레벨에서 빠른 경로가 설정된(fast-pathed) 연결을 제외하고 **어떤** 연결도 로깅할 수 있습니다.

방어 센터 데이터베이스에 연결 이벤트를 저장하면 FireSIGHT 시스템의 각종 보고, 분석, 데이터 상관관계 기능을 활용할 수 있습니다. 39-1페이지의 연결 및 보안 인텔리전스 데이터 작업를 참조하십시오. 또는 외부 시스템 로그(syslog)나 SNMP 트랩 서버에 연결 데이터를 보낼 수 있습니다.

관리 대상 디바이스에서 수집한 연결 데이터를 보완할 목적으로 NetFlow 지원 디바이스에서 생성한 레코드를 활용하여 연결 이벤트를 생성할 수 있습니다. 이는 FireSIGHT 시스템이 관리하는 디바이스에서 모니터링하지 못하는 네트워크에 NetFlow 지원 디바이스가 구축된 경우 특히 유용합니다.

참고 NetFlow 데이터 수집이 액세스 제어와 연결되지 않으므로 어떤 NetFlow 연결을 로깅할 것인가는 세밀하게 제어하지 않습니다. FireSIGHT 시스템이 관리하는 디바이스가 NetFlow 지원 디바이스에서 내보낸 레코드를 탐지하고 이 레코드의 데이터를 기반으로 단일 방향 연결 종료(end-of-connection) 이벤트를 생성하며 최종적으로는 방어 센터에 이벤트를 보내 데이터베이스에 로깅되게 합니다. NetFlow 레코드는 보안 인텔리전스 이벤트를 생성할 수 없으며 외부 서버에 로깅될 수도 없습니다. 자세한 내용은 45-16페이지의 NetFlow 이해를 참조하십시오.

연결 데이터 로깅에 대한 자세한 내용은 다음을 참조하십시오.

로깅할 연결 결정

라이센스: 모두

액세스 제어 및 SSL 정책의 다양한 설정을 사용하여 디바이스에서 모니터링하는, 빠른 경로가 설정되지 않은 어떤 연결도 로깅할 수 있습니다. 대개는 연결의 시작, 종료 또는 둘 다에서 로깅할 수 있습니다. 그러나 차단된 트래픽은 더 이상의 검사 없이 즉시 거부되므로, 차단되었거나 블랙리스트에 포함된 트래픽에 대해서는 대개 연결 시작(beginning-of-connection) 이벤트만 로깅할 수 있습니다. 로깅해야 하는 특별한 연결 종료는 없습니다.

연결 이벤트를 로깅할 때 방어 센터 데이터베이스에 저장한 다음 FireSIGHT 시스템으로 추가 분석할 수 있습니다. 또는 외부 syslog나 SNMP 트랩 서버에 연결 데이터를 보낼 수 있습니다.

팁 FireSIGHT 시스템을 사용하여 연결 데이터를 상세 분석하려는 경우 Cisco는 중요 연결의 종료를 방어 센터 데이터베이스에 로깅하는 것을 권장합니다.

자세한 내용은 다음 링크를 참조하십시오.

중요 연결 로깅

라이센스: 모두

조직의 보안 및 규정준수 요구 사항에 따라 연결을 로깅해야 합니다. 생성하는 연결의 수를 제한하여 성능을 개선하는 것이 목적이라면 분석에 필요한 연결에 대해서만 로깅을 활성화합니다. 그러나 프로필 생성을 위해 네트워크 트래픽을 포괄적으로 파악하고자 하는 경우에는 다른 연결에 대해 로깅을 활성화할 수 있습니다. 액세스 제어 및 SSL 정책의 다양한 설정을 통해 어떤 연결을 로깅하고 언제 로깅하며 그 데이터를 어디에 저장하는가를 세부적으로 제어할 수 있습니다.

주의 DoS(Denial of Service) 공격 중에 차단된 TCP 연결을 로깅하면 시스템 성능에 영향을 미치고 다수의 유사 이벤트로 인해 데이터베이스에 부담을 줄 수 있습니다. 차단 규칙에 대한 로깅을 활성화하기 전에 이 규칙이 인터넷 연결 인터페이스 또는 DoS 공격에 취약한 다른 인터페이스의 트래픽을 모니터링하는지 여부를 고려하십시오.

사용자가 구성하는 로깅 외에도 시스템에서 금지된 파일, 악성코드 또는 침입 시도를 탐지한 연결도 대부분 자동으로 로깅됩니다. 시스템 정책을 사용하여 연결 이벤트 저장을 완전히 비활성화하지 않는 한, 다른 로깅 컨피그레이션과 무관하게 이 연결 종료 이벤트가 방어 센터 데이터베이스에 자동으로 저장되어 추가 분석이 이루어집니다. 모든 연결 이벤트는 자동으로 로깅된 이유를 Action 및 Reason 필드로 나타냅니다. 39-5페이지의 Action 및 39-8페이지의 Reason을/를 참조하십시오.

보안 인텔리전스 블랙리스팅 결정(선택 사항)

평판 기반 보안 인텔리전스 기능에 의해 연결이 블랙리스트에 포함될(차단될) 때마다 연결을 로깅할 수 있습니다. 원한다면 보안 인텔리전스 필터링에 대한 모니터 전용 설정을 사용할 수 있으며, 이는 패시브 구축에서 권장 사항입니다. 그러면 시스템은 블랙리스트에 포함되는 연결을 추가 분석할 수 있으나, 블랙리스트와의 매칭은 계속 로깅됩니다. 보안 인텔리전스 모니터링에서는 보안 인텔리전스 정보를 사용하여 트래픽 프로필을 생성하는 것도 허용합니다.

보안 인텔리전스 로깅을 활성화할 경우, 블랙리스트 매칭 시 보안 인텔리전스 이벤트와 연결 이벤트가 생성됩니다. 보안 인텔리전스 이벤트는 특별한 종류의 연결 이벤트로서 별도로 보고 분석할 수 있으며 또한 별도로 저장 및 정리(prune)가 이루어집니다. 자세한 내용은 38-10페이지의 보안 인텔리전스(블랙리스팅) 결정 로깅을/를 참조하십시오.

암호화 연결(선택 사항)

SSL 정책의 설정에 따라 암호화된 세션이 차단될 때 연결을 로깅할 수 있습니다. 또한 트래픽 해독 여부 및 시스템에서 추후 트래픽을 처리하거나 검사하는지 여부와 무관하게, 추가 평가를 위해 액세스 제어 규칙을 통해 반드시 연결을 로깅하게 할 수도 있습니다. 이러한 로깅은 SSL 규칙에 따라 구성하여 중요한 연결만 로깅하도록 합니다. 자세한 내용은 38-12페이지의 암호화 연결 로깅을/를 참조하십시오.

액세스 제어 처리(선택 사항)

액세스 제어 규칙 또는 액세스 제어 기본 작업에 의해 연결이 처리될 때 이를 로깅할 수 있습니다. 이러한 로깅은 액세스 제어 규칙에 따라 구성하므로 중요한 연결만 로깅하도록 합니다. 자세한 내용은 38-15페이지의 액세스 제어 처리 기반 연결 로깅을/를 참조하십시오.

침입 관련 연결(자동)

액세스 제어 규칙에 의해 호출된 침입 정책(14-1페이지의 액세스 제어 규칙을 사용하여 트래픽 플로우 조정 참조)이 침입을 탐지하고 침입 이벤트를 생성하면, 규칙의 로깅 컨피그레이션과 무관하게 침입이 발생한 연결의 종료가 자동으로 방어 센터 데이터베이스에 로깅됩니다.

그러나 액세스 제어 기본 작업과 연결된 침입 정책(12-6페이지의 네트워크 트래픽의 기본 처리 및 검사 설정 참조)에서 침입 이벤트를 생성할 경우에는 해당 연결의 종료가 자동으로 로깅되지 **않습니다**. 그 대신 기본 작업 연결 로깅을 명시적으로 활성화해야 합니다. 이는 어떤 연결 데이터도 로깅하지 않을 침입 방지 전용 구축에서 유용합니다.

침입이 차단된 연결의 경우, 연결 로그에서 이 연결에 대한 작업은 `Block`이고 사유는 `Intrusion Block`입니다. 그러나 침입 조사를 수행하려면 허용(Allow) 규칙을 사용해야 합니다.

팁 Series 3 또는 가상 디바이스에서 이러한 연결 로깅을 비활성화하려면 CLI를 사용합니다. D-31페이지의 log-ips-connections을/를 참조하십시오.

파일 및 악성코드 이벤트 관련 연결(자동)

액세스 제어 규칙에 의해 호출된 파일 정책에서 금지된 파일(악성코드 포함)을 탐지하고 파일 또는 악성코드 이벤트를 생성할 경우, 액세스 제어 규칙의 로깅 컨피그레이션과 무관하게 파일이 탐지된 연결의 종료가 자동으로 방어 센터 데이터베이스에 로깅됩니다. 이 로깅은 비활성화할 수 **없습니다**.

참고 NetBIOS-ssn(SMB) 트래픽 검사에 의해 생성된 파일 이벤트는 즉시 연결 이벤트를 생성하지 않습니다. 클라이언트와 서버가 지속적인 연결을 설정하기 때문입니다. 클라이언트 또는 서버가 세션을 종료하면 연결 이벤트가 생성됩니다.

어떤 파일이 차단된 연결의 경우 연결 로그에서 이 연결에 대한 작업은 `Block`입니다. 그러나 파일 및 악성코드 검사를 수행하려면 허용 규칙을 사용해야 합니다. 연결 사유는 `File Monitor`(파일 유형 또는 악성코드가 탐지됨)이거나 `Malware Block` 또는 `File Block`(파일이 차단됨)입니다.

연결 시작 또는 종료 로깅

라이센스: 모두

연결이 탐지되면 대개는 그 시작이나 종료에서 연결을 로깅할 수 있습니다.

그러나 차단된 트래픽은 추가 검사 없이 즉시 거부되므로, 차단되었거나 블랙리스트에 포함된 트래픽에 대해서는 대개 연결 시작(beginning-of-connection) 이벤트만 로깅할 수 있습니다. 로깅해야 하는 특별한 연결 종료는 없습니다. 암호화 트래픽을 차단할 경우에는 예외가 발생합니다. SSL 정책에서 연결 로깅을 활성화하면 연결 시작이 아닌 연결 종료가 로깅됩니다. 이는 시스템에서 세션의 첫 번째 패킷을 사용하여 연결의 암호화 여부를 확인할 수 없고 따라서 즉시 암호화 세션을 차단할 수 없기 때문입니다.

참고 차단되지 않은 단일 연결의 경우 연결 종료 이벤트는 연결 시작 이벤트의 모든 정보 및 세션 과정에서 수집된 정보를 포함합니다.

성능 최적화를 위해서는 연결 시작 또는 종료 중 하나만 로깅하십시오. 연결 시작 또는 종료 이벤트에 따라 상관관계 규칙을 트리거할 수 있습니다. 어떤 이유로든 연결을 모니터링하면 반드시 연결 종료가 로깅됩니다. 38-6페이지의 모니터링되는 연결에 대한 로깅 이해을/를 참조하십시오.

다음 표에서는 연결 시작 및 연결 종료 이벤트의 차이점과 각 로깅의 장점을 설명합니다.

표 38-1 연결 시작 이벤트와 종료 이벤트 비교

	연결 시작 이벤트	연결 종료 이벤트
생성되는 경우	연결 시작이 탐지될 때(또는 애플리케이션이나 URL 식별에 따라 이벤트가 생성되는 경우 처음 몇 개의 패킷 이후에)	시스템에서 • 연결 종료를 탐지할 때 • 일정 기간이 지나도 연결 종료를 탐지하지 않을 때 • 메모리 제약으로 더 이상 세션을 추적할 수 없을 때
로깅 대상	보안 인텔리전스 또는 액세스 제어 규칙에 의해 평가된 모든 연결. 단, 연결 종료 로깅을 구성할 수 없는 경우도 있습니다.	모든 연결. 단, 연결 종료 로깅을 구성할 수 없는 경우도 있습니다.

표 38-1 연결 시작 이벤트와 종료 이벤트 비교(계속)

	연결 시작 이벤트	연결 종료 이벤트
내용	첫 번째 패킷(애플리케이션 또는 URL 식별에 따라 이벤트가 생성되는 경우에는 처음 몇 개 패킷)에서 확인할 수 있는 정보만	연결 시작 이벤트의 모든 정보와 세션 기간에 트래픽을 검사하여 확인한 정보(예: 총 데이터 전송량, 연결의 마지막 패킷의 타임스탬프)
유용한 경우	다음 항목을 로깅할 때 • 차단된 연결(보안 인텔리전스 블랙리스팅 결정 포함) • 연결 시작만(연결 종료 정보가 중요하지 않아서)	다음 작업을 수행할 때 • SSL 정책에 의해 처리된 암호화 연결을 로깅할 때 • 세션 기간에 수집된 정보에 대해 상세 분석을 수행하거나 그 정보를 사용하여 상관관계 규칙을 트리거할 때 • 사용자 지정 워크플로에서 연결 요약(종합 연결 데이터)을 보거나 그래픽 형식으로 연결 데이터를 보거나 트래픽 프로필을 사용할 때

방어 센터 또는 외부 서버와의 연결 로깅

라이센스: 모두

방어 센터 데이터베이스뿐 아니라 외부 syslog 또는 SNMP 트랩 서버에 연결 이벤트를 로깅할 수 있습니다. 외부 서버에 연결 데이터를 로깅하려면 먼저 그 서버와 *알림 응답(alert response)*이라는 연결을 구성해야 합니다. 43-2페이지의 알림 응답 작업을/를 참조하십시오.

방어 센터 데이터베이스에 로깅하면 FireSIGHT 시스템의 각종 보고, 분석, 데이터 상관관계 기능을 활용할 수 있습니다. 예를 들면 다음과 같습니다.

- 대시보드 및 컨텍스트 탐색기에서는 시스템에서 로깅한 연결을 그래픽 화면에서 한눈에 볼 수 있습니다. 55-1페이지의 대시보드 사용 및 56-1페이지의 Context Explorer 사용을/를 참조하십시오.
- 이벤트 보기에서는 시스템에서 로깅한 연결에 대한 세부사항을 제공하며, 이는 그래픽 또는 표 형식으로 표시하거나 보고서 형태로 요약할 수 있습니다. 39-1페이지의 연결 및 보안 인텔리전스 데이터 작업을/를 참조하십시오.
- 트래픽 프로필에서는 정상적인 네트워크 트래픽에 대한 프로필을 생성하는 데 연결 데이터를 사용합니다. 그런 다음 이 프로필을 비정상적인 동작을 탐지하고 추적하는 데 기준으로 사용할 수 있습니다. 53-1페이지의 트래픽 프로필 생성을/를 참조하십시오.
- 상관관계 정책에서는 특정 유형의 연결 또는 트래픽 프로필 변경에 대한 이벤트를 생성하고 응답(예: 알림, 외부 교정)을 트리거할 수 있습니다. 51-3페이지의 상관관계 정책에 대한 규칙 생성을/를 참조하십시오.

참고 이 기능을 사용하려면 **반드시** 방어 센터 데이터베이스에 연결을 (대부분의 경우에는 연결 시작이 아닌 연결 종료를) 로깅해야 합니다. 따라서 중요한 연결, 즉 로깅된 침입, 금지된 파일, 악성코드와 관련된 연결은 자동으로 로깅됩니다.

방어 센터에서 저장할 수 있는 연결 및 보안 인텔리전스 이벤트의 수는 그 모델에 따라 달라집니다. 이러한 제한의 목록 및 연결 이벤트 저장 비활성화에 대한 정보는 63-15페이지의 데이터베이스 이벤트 제한 구성에서 확인하십시오.

액세스 제어 및 SSL 규칙 작업이 로깅에 미치는 영향 이해

라이센스: 기능에 따라

모든 액세스 제어 및 SSL 규칙에는 규칙과 매칭하는 트래픽을 검사하고 처리하는 방식뿐 아니라 매칭하는 트래픽의 세부사항을 로깅할 수 있는 시점과 방식을 결정하는 *작업*이 있습니다.

참고 액세스 제어 및 SSL 정책의 기본 작업에서 허용하는 연결 로깅은 약간 다르게 처리됩니다. 38-17페이지의 액세스 제어 기본 작업에 의해 처리되는 연결 로깅 및 38-14페이지의 암호화 연결 및 해독 불가 연결에 대한 기본 로깅 설정을/를 참조하십시오.

자세한 내용은 다음 링크를 참조하십시오.

- 14-8페이지의 규칙 작업을 사용하여 트래픽 처리 및 검사 확인
- 21-8페이지의 규칙 작업을 사용하여 암호화 트래픽 처리 및 조사 결정
- 38-6페이지의 모니터링되는 연결에 대한 로깅 이해
- 38-7페이지의 신뢰하는 연결에 대한 로깅 이해
- 38-7페이지의 차단된 연결 및 인터랙티브 차단된 연결에 대한 로깅 이해
- 38-8페이지의 허용된 연결에 대한 로깅 이해
- 38-8페이지의 허용된 연결에 대한 파일 및 악성코드 이벤트 로깅 비활성화

모니터링되는 연결에 대한 로깅 이해

라이센스: 기능에 따라

나중에 연결을 처리하는 규칙 또는 기본 작업의 로깅 컨피그레이션과 무관하게 다음 연결의 종료는 항상 방어 센터 데이터베이스에 로깅됩니다.

- 모니터링하도록 설정된 보안 인텔리전스 블랙리스트와 매칭하는 연결
- SSL 모니터 규칙과 매칭하는 연결
- 액세스 제어 모니터 규칙과 매칭하는 연결

즉 어떤 패킷이 모니터 규칙이나 보안 인텔리전스 모니터링 블랙리스트와 매칭할 경우, 패킷이 다른 어떤 규칙과도 매칭되지 않고 기본 작업에서 로깅을 활성화하지 않았더라도 그 연결은 항상 로깅됩니다. 보안 인텔리전스 필터링의 결과로 연결 이벤트가 로깅될 경우 매칭하는 보안 인텔리전스 이벤트도 로깅합니다. 이는 특별한 종류의 연결 이벤트로서 별도로 보고 분석할 수 있습니다. 38-10페이지의 보안 인텔리전스(블랙리스팅) 결정 로깅을/를 참조하십시오.

모니터링되는 트래픽은 항상 나중에 다른 규칙이나 기본 작업에 의해 처리되므로 모니터 규칙 때문에 로깅된 연결에 대한 작업은 `Monitor`가 될 수 없습니다. 그보다는 나중에 연결을 처리하는 규칙의 작업이나 기본 작업을 나타냅니다. 39-5페이지의 Action을/를 참조하십시오.

단일 연결이 SSL 또는 액세스 제어 모니터 규칙과 매칭할 때마다 별도의 이벤트를 생성하지는 **않습니다**. 단일 연결이 여러 모니터 규칙과 매칭할 수 있으므로, 방어 센터 데이터베이스에 로깅되는 각 연결 이벤트는 연결이 매칭하는 처음 8개 모니터 액세스 제어 규칙 및 첫 번째 매칭 모니터 SSL 규칙에 대한 정보를 포함하고 표시할 수 있습니다.

또한 외부 syslog나 SNMP 트랩 서버에 연결 이벤트를 보낼 경우 단일 연결이 모니터 규칙과 매칭할 때마다 별도의 알림을 보내지 않습니다. 그보다는 연결의 종료에 보내는 알림에 연결이 매칭한 모니터 규칙에 대한 정보가 들어 있습니다.

팁 연결 로그의 규칙 작업이 Monitor가 될 수 없지만, 모니터 규칙과 매칭하는 연결에 대해 상관관계 정책 위반을 트리거하는 것은 가능합니다. 자세한 내용은 51-5페이지의 상관관계 규칙 트리거 기준 지정을/를 참조하십시오.

신뢰하는 연결에 대한 로깅 이해

라이센스: 기능에 따라

신뢰하는 연결이란 신뢰 액세스 제어 규칙이나 액세스 제어 정책의 기본 작업에서 처리하는 연결입니다. 이 연결의 시작과 종료를 로깅할 수 있지만, 신뢰하는 연결은 암호화 여부와 무관하게 검색 데이터, 침입 또는 금지된 파일 및 악성코드에 대한 검사를 받지 않습니다. 따라서 신뢰하는 연결에 대한 연결 이벤트는 한정된 정보를 포함합니다.

신뢰 액세스 제어 규칙에서 처리하는 TCP 연결은 연결을 탐지하는 디바이스에 따라 다르게 로깅됩니다.

- Series 3 디바이스의 경우 첫 번째 패킷에서 신뢰 규칙에 의해 탐지된 TCP 연결은 선행 활성 모니터 규칙의 유무에 따라 다른 이벤트를 생성합니다. 모니터 규칙이 활성 상태일 경우 패킷을 평가하고 연결 시작 및 종료 이벤트를 모두 생성합니다. 활성 상태의 모니터 규칙이 없을 경우 연결 종료 이벤트만 생성합니다.
- 그 밖의 모든 모델에서는 첫 번째 패킷에서 신뢰 규칙에 의해 탐지된 TCP 연결은 연결 종료 이벤트만 생성합니다. 최종 세션 패킷의 1시간 후에 이벤트가 생성됩니다.

차단된 연결 및 인터랙티브 차단된 연결에 대한 로깅 이해

라이센스: 기능에 따라

차단된 연결을 로깅할 때 그 로깅 방식은 연결이 차단된 이유에 따라 달라집니다. 연결 로그를 기반으로 상관관계 규칙을 구성할 때 이 점을 기억해야 합니다.

- 암호화 트래픽을 차단하는 SSL 규칙 및 SSL 정책 기본 작업의 경우 연결 **종료** 이벤트가 로깅됩니다. 이는 세션의 첫 번째 패킷을 사용하여 연결의 암호화 여부를 확인할 수 없기 때문입니다.
- 해독된 트래픽 또는 암호화되지 않은 트래픽을 차단하는 액세스 제어 규칙 및 액세스 제어 정책 기본 작업(인터랙티브 차단 규칙 포함)의 경우 연결 **시작** 이벤트가 로깅됩니다. 매칭하는 트래픽은 추가 검사 없이 거부됩니다.

액세스 제어 또는 SSL 규칙에 의해 차단된 세션에 대한 연결 이벤트는 작업이 Block 또는 Block with reset입니다. 차단된 암호화 연결은 사유가 SSL Block입니다.

사용자가 금지된 웹 사이트로 이동할 때 경고 페이지를 표시하는 인터랙티브 차단 액세스 제어 규칙에서는 연결 종료 로깅을 구성할 수 있습니다. 이는 사용자가 경고 페이지를 클릭할 경우 모니터링 및 로깅 가능한 새로운 허용된 연결로 간주되기 때문입니다. 38-8페이지의 허용된 연결에 대한 로깅 이해을/를 참조하십시오.

따라서 인터랙티브 차단 또는 인터랙티브 차단 후 초기화 규칙과 매칭하는 패킷에 대해 다음 연결 이벤트가 생성될 수 있습니다.

- 사용자의 요청이 초기에 차단되고 경고 페지이가 표시될 경우 연결 시작 이벤트. 이 이벤트의 작업은 Interactive Block 또는 Interactive Block with reset입니다.
- 사용자가 경고 페이지를 클릭하고 원래 요청된 페이지를 로드할 경우 여러 개의 연결 시작 또는 종료 이벤트. 이 이벤트의 작업은 Allow이고, 사유는 User Bypass입니다.

인라인에 구축된 디바이스만 트래픽을 차단할 수 있습니다. 차단된 연결이 패시브 구축에서는 실제로 차단되지 않으므로 차단된 연결 각각에 대해 여러 개의 연결 시작 이벤트가 보고될 수 있습니다.

주의 DoS 공격 중에 차단된 TCP 연결을 로깅하면 시스템 성능에 영향을 미치고 다수의 유사 이벤트로 인해 데이터베이스에 부담을 줄 수 있습니다. 차단 규칙에 대한 로깅을 활성화하기 전에 이 규칙이 인터넷 연결 인터페이스 또는 DoS 공격에 취약한 다른 인터페이스의 트래픽을 모니터링하는지 여부를 고려하십시오.

허용된 연결에 대한 로깅 이해

라이센스: 기능에 따라

SSL 해독 규칙, SSL 해독 안 함 규칙, 허용 액세스 제어 규칙은 매칭하는 트래픽이 검사 및 트래픽 처리의 다음 단계로 진행할 수 있게 합니다.

SSL 규칙을 사용하여 암호화 트래픽을 해독하는지 여부와 무관하게 트래픽은 액세스 제어 규칙의 평가를 계속 받습니다. 이 SSL 규칙에 대한 로깅을 활성화할 경우, 액세스 제어 규칙이나 나중에 연결을 처리할 기본 작업의 로깅 컨피그레이션과 무관하게 매칭하는 연결의 종료가 로깅됩니다.

액세스 제어 규칙으로 트래픽을 허용할 경우, 트래픽이 최종 목적지에 도착하기 전에 관련 침입 또는 파일 정책(또는 둘 다)을 사용하여 트래픽을 추가 검사하고 침입, 금지된 파일, 악성코드를 차단할 수 있습니다. 그러나 암호화 페이로드에 대해서는 파일 및 침입 검사가 기본적으로 비활성화되어 있습니다.

허용 액세스 제어 규칙과 매칭하는 트래픽에 대한 연결은 다음과 같이 로깅됩니다.

- 액세스 제어 규칙에 의해 호출된 침입 정책이 침입을 탐지하고 침입 이벤트를 생성하면, 규칙의 로깅 컨피그레이션과 무관하게 침입이 발생한 연결의 종료가 자동으로 방어 센터 데이터베이스에 로깅됩니다.
- 액세스 제어 규칙에 의해 호출된 파일 정책에서 금지된 파일(악성코드 포함)을 탐지하고 파일 또는 악성코드 이벤트를 생성할 경우, 액세스 제어 규칙의 로깅 컨피그레이션과 무관하게 파일이 탐지된 연결의 종료가 자동으로 방어 센터 데이터베이스에 로깅됩니다.
- 원한다면 시스템에서 안전하다고 간주하는 트래픽, 침입 또는 파일 정책으로 검사하지 않는 트래픽을 포함하여 어떤 허용된 트래픽에 대해서도 연결 시작 및 종료 로깅을 활성화할 수 있습니다.

그에 따라 생성되는 모든 연결 이벤트의 Action 및 Reason 필드는 이벤트가 로깅된 사유를 나타냅니다. 39-5페이지의 Action 및 39-8페이지의 Reason을/를 참조하십시오. 다음 사항에 유의하십시오.

- `Allow` 작업은 최종 목적지에 도착한, 명시적으로 허용된 연결 및 사용자 바이패스 인터랙티브 차단 연결을 나타냅니다.
- `Block` 작업은 처음에는 액세스 제어 규칙에 의해 허용되었으나 침입, 금지된 파일 또는 악성코드가 탐지된 연결을 나타냅니다.

허용된 연결에 대한 파일 및 악성코드 이벤트 로깅 비활성화

라이센스: 보호 또는 악성코드

지원되는 디바이스: 기능에 따라

지원되는 Defense Center: 기능에 따라

액세스 제어 규칙으로 암호화되지 않은 트래픽이나 해독된 트래픽을 허용할 경우, 목적지에 도착하기 전에 관련 파일 정책을 사용하여 전송된 파일을 검사하고 금지된 파일 및 악성코드를 차단할 수 있습니다. 18-8페이지의 침입 방지 성능 조정을/를 참조하십시오. 악성코드 라이센스를 DC500에서 사용할 수 없고 악성코드 라이센스를 Series 2 디바이스 또는 Cisco NGIPS for Blue Coat X-Series에서 활성화할 수 없으므로 이 어플라이언스는 악성코드 차단에 사용하지 못합니다.

금지된 파일을 탐지하면 다음 유형의 이벤트 중 하나가 자동으로 방어 센터 데이터베이스에 로깅됩니다.

- *file events* - 악성코드 파일을 포함하여 탐지되었거나 차단된 파일을 나타냅니다.
- *malware events* - 탐지되었거나 차단된 악성코드 파일만 나타냅니다.
- *retrospective malware events* - 이전에 탐지된 파일의 악성코드 속성이 변경될 때 생성됩니다.

파일 또는 악성코드 이벤트를 로깅하지 않으려는 경우 액세스 제어 규칙별로 이 로깅을 비활성화할 수 있는데, 액세스 제어 규칙 편집기의 Logging 탭에서 **Log Files** 확인란의 선택을 취소하면 됩니다. 파일 및 악성코드 이벤트 저장을 완전히 비활성화하는 것에 대한 자세한 내용은 63-15페이지의 데이터베이스 이벤트 제한 구성을/를 참조하십시오.

참고 Cisco에서는 파일 및 악성코드 이벤트 로깅을 활성 상태로 두는 것을 권장합니다.

파일 및 악성코드 이벤트 저장 여부와 무관하게, 네트워크 트래픽에서 파일 정책을 위반하면 해당 연결의 종료가 방어 센터 데이터베이스에 자동으로 로깅됩니다. 호출하는 액세스 제어 규칙의 로깅 컨피그레이션에 구애받지 않습니다. 38-4페이지의 파일 및 악성코드 이벤트 관련 연결(자동)을/를 참조하십시오.

연결 로깅의 라이센스 및 모델 요구 사항

라이센스: 기능에 따라

액세스 제어 및 SSL 정책에서 연결 로깅을 구성하므로 이 정책에서 성공적으로 처리할 수 있는 어떤 연결도 로깅 가능합니다.

방어 센터의 라이센스와 무관하게 액세스 제어 및 SSL 정책을 생성할 수 있으나, 액세스 제어의 일부 요소는 대상 디바이스에서 어떤 라이센스 기능을 활성화해야 정책을 적용할 수 있습니다. 또한 어떤 기능은 특정 모듈에서만 사용 가능합니다.

방어 센터에 포함된 FireSIGHT 라이센스는 연결 로그의 정보를 기반으로 호스트, 사용자, 애플리케이션 데이터를 네트워크 맵에 추가할 뿐 아니라 연결 이벤트와 관련된 IOC(indication of compromise) 정보도 볼 수 있습니다. DC500을 제외하고 연결과 관련된 지오로케이션 데이터(소스 또는 목적지의 국가나 대륙)도 볼 수 있습니다.

다음 표에서는 성공적으로 액세스 제어를 구성하고 액세스 제어 정책에 의해 처리되는 연결을 로깅하는 데 필요한 라이센스에 대해 설명합니다.

표 38-2 액세스 제어 정책의 연결 로깅을 위한 라이센스 및 모델 요구 사항

로깅할 연결	라이센스	지원되는 방어 센터	지원되는 디바이스
네트워크, VLAN, 포트 또는 리터럴 URL 기준을 사용하여 처리되는 트래픽	모두	모두	다음을 제외하고 모두: • Series 2 디바이스는 URL 필터링을 수행할 수 없음 • ASA FirePOWER 디바이스는 VLAN 필터링을 수행할 수 없음
지오로케이션 데이터를 사용하여 처리되는 트래픽	FireSIGHT	DC500을 제외하고 모두	Series 2 또는 X-Series를 제외하고 모두

표 38-2 액세스 제어 정책의 연결 로깅을 위한 라이센스 및 모델 요구 사항(계속)

로깅할 연결	라이센스	지원되는 방어 센터	지원되는 디바이스
다음 항목과 관련된 연결: • 평판이 낮은 IP 주소(Security Intelligence 필터링) • 암호화되지 않았거나 해독된 트래픽의 침입 또는 금지된 파일	보호	모두	모두. 단, Series 2 디바이스는 보안 인텔리전스 필터링을 수행할 수 없음
암호화되지 않았거나 해독된 트래픽에서 탐지된 악성코드 관련	악성코드	DC500을 제외하고 모두	Series 2 또는 X-Series를 제외하고 모두
사용자 제어 또는 애플리케이션 제어에 의해 처리되는 트래픽	제어	모두. 단, DC500은 사용자 제어를 수행할 수 없음	Series 2 또는 X-Series를 제외하고 모두
URL 범주 및 평판 데이터를 사용하여 필터링하고 모니터링되는 호스트에서 요청한 URL의 URL 범주 및 URL 평판 정보를 표시하기 위해 필터링하는 트래픽	URL 필터링	DC500을 제외하고 모두	Series 2를 제외하고 모두

다음 표에서는 성공적으로 SSL 검사를 구성하고 SSL 정책에 의해 처리되는 연결을 로깅하는 데 필요한 라이센스에 대해 설명합니다. SSL 정책에 의해 암호화 연결이 로깅되지 않고 심지어 검사되지 않더라도 다른 사유로 로깅될 수도 있습니다.

표 38-3 SSL 정책의 연결 로깅을 위한 라이센스 및 모델 요구 사항

로깅할 연결	라이센스	지원되는 방어 센터	지원되는 디바이스
영역, 네트워크, VLAN, 포트 또는 SSL 관련 기준을 사용하여 처리되는 트래픽	모두	모두	Series 3
지오로케이션 데이터를 사용하여 처리되는 암호화 트래픽	FireSIGHT	DC500을 제외하고 모두	Series 3
애플리케이션 또는 사용자 기준을 사용하여 처리되는 암호화 트래픽	제어	모두. 단, DC500은 사용자 제어를 수행할 수 없음	Series 3
URL 범주 및 평판 데이터를 사용하여 필터링하는 암호화 트래픽	URL 필터링	DC500을 제외하고 모두	Series 3

보안 인텔리전스(블랙리스팅) 결정 로깅

라이센스: 보호

지원되는 디바이스: Series 2를 제외하고 모두

지원되는 Defense Center: 지원되는 Defense Center: DC500을 제외하고 모두

악성 인터넷 콘텐츠를 막는 2차 방어선인 FireSIGHT 시스템에서는 보안 인텔리전스 기능을 제공합니다. 이 기능으로 최신 평판 인텔리전스를 기반으로 즉시 연결을 블랙리스팅(차단)할 수 있으므로 더 많은 리소스가 필요한 심층 분석을 수행하지 않아도 됩니다. 이러한 트래픽 필터링은 다른 어떤 정책 기반 검사, 분석 또는 트래픽 처리가 이루어지기 **전에** 수행됩니다. 단, 하드웨어 레벨의 처리(예: 빠른 경로 설정)가 선행합니다.

원한다면 보안 인텔리전스 필터링에 대한 모니터 전용 설정을 사용할 수 있으며, 이는 패시브 구축에서 권장되는 사항입니다. 그러면 시스템은 블랙리스트에 포함되는 연결을 추가 분석할 수 있으나, 블랙리스트와의 매칭은 계속 로깅됩니다.

참고 보안 인텔리전스 정보를 기반으로 트래픽 프로필을 생성하거나 연결 종료 이벤트에서 보안 인텔리전스 정보를 사용하여 상관관계 규칙을 트리거하려면 **반드시** 이 정보를 방어 센터 데이터베이스에 로깅해야 합니다. 먼저 보안 인텔리전스 로깅을 활성화합니다. 그런 다음 모니터 전용 보안 인텔리전스 객체를 사용하여 블랙리스트를 작성합니다. 자세한 내용은 13-1페이지의 보안 인텔리전스 IP 주소 평판 블랙리스트에 추가을/를 참조하십시오.

보안 인텔리전스 로깅을 활성화하면 액세스 제어 정책의 대상 디바이스에서 처리한 모든 차단되고 모니터링된 연결이 로깅됩니다. 그러나 화이트리스트 매칭은 로깅하지 않습니다. 화이트리스트의 연결에 대한 로깅은 그 이벤트 속성에 따라 달라집니다.

보안 인텔리전스 필터링의 결과로 연결 이벤트가 로깅될 때마다 매칭하는 보안 인텔리전스 이벤트도 로깅합니다. 이는 특별한 종류의 연결 이벤트로서 별도로 보고 분석할 수 있습니다. 두 이벤트 유형 모두 **Action** 및 **Reason** 필드를 사용하여 블랙리스트 매칭을 나타냅니다. 또한 연결에서 블랙리스트의 IP 주소를 식별할 수 있도록 모니터링되는 블랙리스트 IP 주소는 이벤트 뷰어에서 그 옆에 있는 호스트 아이콘이 약간 다르게 표시됩니다.

차단된 블랙리스트 연결 로깅

차단된 연결은 연결 시작 보안 인텔리전스 및 연결 이벤트가 로깅됩니다. 블랙리스트 트래픽은 추가 검사 없이 즉시 거부되므로 로깅해야 할 특별한 연결 종료가 없습니다. 이러한 이벤트는 작업이 `Block`, 사유가 `IP Block`입니다.

`IP Block` 연결 이벤트는 고유 initiator-responder 쌍마다 임계값이 15초입니다. 즉 연결 차단으로 이벤트가 생성된 경우, 다음 15초 동안에는 이 두 호스트 간에 다시 연결이 차단되더라도 연결 이벤트가 생성되지 않습니다. 이는 포트 또는 프로토콜과 무관합니다.

모니터링되는 블랙리스트 연결의 로깅

보안 인텔리전스에서 (차단한 연결이 아니라) 모니터링하는 연결의 경우 연결 종료 보안 인텔리전스 및 연결 이벤트가 방어 센터 데이터베이스에 로깅됩니다. 이 로깅은 나중에 SSL 정책, 액세스 제어 규칙 또는 액세스 제어 기본 작업에서 연결을 처리하는 방식과 무관하게 일어납니다.

이러한 연결 이벤트의 작업은 연결의 이벤트 속성에 따라 달라집니다. **Reason** 필드에는 `IP Monitor`와 함께 연결이 로깅된 또 다른 사유가 포함됩니다.

모니터링되는 연결에 대해서는 나중에 연결을 처리하는 액세스 제어 규칙이나 기본 작업의 로깅 설정에 따라 연결 시작 이벤트도 생성될 수 있습니다.

블랙리스트 연결을 로깅하려면

액세스: Admin/Access Admin/Network Admin

1단계 **Policies > Access Control**을 선택합니다.

Access Control Policy 페이지가 나타납니다.

2단계 구성하려는 액세스 제어 정책 옆의 수정 아이콘()을 클릭합니다.

액세스 제어 정책 편집기가 나타납니다.

3단계 Security Intelligence 탭을 선택합니다.

액세스 제어 정책에 대한 보안 인텔리전스 설정이 나타납니다.

4단계 로깅 아이콘( )을 클릭합니다.

Blacklist Options 팝업 창이 나타납니다.

5단계 **Log Connections** 확인란을 선택합니다.

6단계 연결 및 보안 인텔리전스 이벤트를 어디로 보낼지 지정합니다. 다음과 같이 선택할 수 있습니다.

- 방어 센터에 이벤트를 보내려면 **Defense Center**를 선택합니다.
- 외부 syslog 서버에 이벤트를 보내려면 **Syslog**를 선택한 다음 드롭다운 목록에서 syslog 알림 응답을 선택합니다. 원한다면 추가 아이콘( )을 클릭하여 syslog 알림 응답을 추가할 수 있습니다. 43-5페이지의 Syslog 알림 응답 생성을/를 참조하십시오.
- SNMP 트랩 서버에 연결 이벤트를 보내려면 **SNMP Trap**을 선택하고 드롭다운 목록에서 SNMP 알림 응답을 선택합니다. 원한다면 추가 아이콘( )을 클릭하여 SNMP 알림 응답을 추가할 수 있습니다. 43-4페이지의 SNMP 알림 응답 생성를 참조하십시오.

블랙리스트 객체를 모니터 전용으로 설정하거나 보안 인텔리전스 필터링에 의해 생성된 연결 이벤트에 대해 또 다른 방어 센터 기반 분석을 수행하려는 경우 **반드시** 방어 센터에 이벤트를 보내야 합니다. 자세한 내용은 38-5페이지의 방어 센터 또는 외부 서버와의 연결 로깅을/를 참조하십시오.

7단계 로깅 옵션을 설정하려면 **OK**를 클릭합니다.

Security Intelligence 탭이 다시 나타납니다.

8단계 **Save**를 클릭합니다.

변경 사항이 적용되려면 액세스 제어 정책을 적용해야 합니다. 12-15페이지의 액세스 제어 정책 적용을/를 참조하십시오.

암호화 연결 로깅

라이센스: SSL

지원되는 디바이스: Series 3

액세스 제어의 일환으로 *SSL 검사* 기능에서는 SSL 정책을 사용하여 액세스 제어 규칙의 추가 평가를 받을 암호화 트래픽을 해독할 수 있습니다. 나중에 트래픽을 처리하거나 검사하는 방식과 무관하게 이 해독 연결을 반드시 로깅하도록 설정할 수 있습니다. 또한 암호화 트래픽을 차단할 때 또는 해독하지 않고 액세스 제어 규칙에 전달하는 것을 허용할 때에도 연결을 로깅할 수 있습니다.

암호화 세션의 연결 로그는 세션 암호화에 사용된 인증서와 같은 해독 세부 사항이 포함되어 있습니다. 중요한 연결만 로깅할 수 있도록 SSL 정책에서 SSL 규칙별로 암호화 세션에 대한 연결 로깅을 구성합니다.

자세한 내용은 다음 절을 참조하십시오.

- 38-13페이지의 SSL 규칙으로 해독 가능 연결 로깅
- 38-14페이지의 암호화 연결 및 해독 불가 연결에 대한 기본 로깅 설정

SSL 규칙으로 해독 가능 연결 로깅

라이센스: SSL

지원되는 디바이스: Series 3

SSL 정책에서 *SSL 규칙*은 여러 관리 대상 디바이스의 전 범위에서 암호화 트래픽을 처리하는 세부적인 방법을 제공합니다. 중요한 연결만 로깅할 수 있도록 SSL 규칙별로 연결 로깅을 활성화합니다. 어떤 규칙에 대해 연결 로깅을 활성화할 경우 그 규칙에서 처리하는 모든 연결이 로깅됩니다.

SSL 정책에 의해 검사되는 암호화 연결의 경우 방어 센터 데이터베이스에 또는 외부 syslog나 SNMP 트랩 서버에 연결 이벤트를 로깅할 수 있습니다. 그러나 연결 종료 이벤트만 로깅할 수 있습니다.

- 차단된 연결(Block, Block with reset)의 경우 즉시 세션을 종료하고 이벤트를 생성합니다.
- 모니터링되는 연결(Monitor)과 액세스 제어 규칙에 전달하는 연결(Decrypt, Do not decrypt)의 경우, 나중에 이를 처리하는 액세스 제어 규칙이나 기본 작업의 로깅 컨피그레이션과 무관하게 세션 종료 시 이벤트를 생성합니다.

자세한 내용은 38-6페이지의 액세스 제어 및 SSL 규칙 작업이 로깅에 미치는 영향 이해을/를 참조하십시오.

해독 가능 연결을 로깅하려면

액세스: Admin/Access Admin/Network Admin/Security Approver

1단계 **Policies > SSL**을 선택합니다.

SSL Policy 페이지가 나타납니다.

2단계 수정하려는 SSL 정책 옆의 수정 아이콘( )을 클릭합니다.

SSL 정책 편집기가 나타나며 Rules 탭에 포커스가 있습니다.

3단계 로깅을 구성하려는 규칙 옆의 수정 아이콘( )을 클릭합니다.

SSL 규칙 편집기가 나타납니다.

4단계 Logging 탭을 선택합니다.

Logging 탭이 나타납니다.

5단계 **Log at End of Connection**을 선택합니다.

6단계 연결 이벤트를 어디로 보낼지 지정합니다. 다음과 같이 선택할 수 있습니다.

- 방어 센터에 연결 이벤트를 보내려면 **Defense Center**를 선택합니다. 규칙 작업이 **Monitor**라면 방어 센터에 연결을 로깅해야 합니다.
- 외부 syslog에 이벤트를 보내려면 **Syslog**를 선택한 다음 드롭다운 목록에서 syslog 알림 응답을 선택합니다. 원한다면 추가 아이콘( )을 클릭하여 syslog 알림 응답을 추가할 수 있습니다. 43-5페이지의 Syslog 알림 응답 생성을/를 참조하십시오.
- SNMP 트랩 서버에 이벤트를 보내려면 **SNMP Trap**을 선택하고 드롭다운 목록에서 SNMP 알림 응답을 선택합니다. 원한다면 추가 아이콘( )을 클릭하여 SNMP 알림 응답을 추가할 수 있습니다. 43-4페이지의 SNMP 알림 응답 생성을/를 참조하십시오.

이 연결 이벤트에 대해 방어 센터 기반 분석을 수행하려면 **반드시** 방어 센터에 이벤트를 보내야 합니다. 자세한 내용은 38-5페이지의 방어 센터 또는 외부 서버와의 연결 로깅을/를 참조하십시오.

7단계 변경사항을 저장하려면 **Add**를 클릭합니다.

SSL 정책이 연결된 액세스 제어 정책을 적용해야 변경사항이 적용됩니다. 12-15페이지의 액세스 제어 정책 적용을/를 참조하십시오.

암호화 연결 및 해독 불가 연결에 대한 기본 로깅 설정

라이센스: SSL

지원되는 디바이스: Series 3

SSL 정책의 기본 작업에 의해 처리되는 트래픽에 대해 연결을 로깅할 수 있습니다. 이 로깅 설정은 해독 불가 세션을 로깅하는 방식에도 적용됩니다.

SSL 정책 기본 작업은 정책의 어떤 SSL 규칙과도 매칭하지 않는 암호화 트래픽의 처리 방식을 결정합니다. 단 모니터 규칙은 트래픽을 매칭하고 로깅하지만 트래픽을 처리하거나 검사하지 않습니다. SSL 정책에 어떤 SSL 규칙도 없을 경우 기본 작업은 네트워크의 모든 암호화 세션이 로깅되는 방식을 결정합니다. 자세한 내용은 20-4페이지의 암호화 트래픽에 대한 기본 처리 및 검사 설정을/를 참조하십시오.

SSL 정책의 기본 작업을 구성하여 방어 센터 데이터베이스에 또는 외부 syslog나 SNMP 트랩 서버에 연결을 로깅할 수 있습니다. 그러나 연결 종료 이벤트만 로깅할 수 있으나,

- 차단된 연결(Block, Block with reset)의 경우 시스템이 즉시 세션을 종료하고 이벤트를 생성합니다.
- 암호화되지 않은 채로 액세스 제어 규칙에 전달할 수 있는 연결의 경우(Do not decrypt) 세션 종료 시 이벤트가 생성됩니다.

SSL 정책 기본 작업에 대해 로깅을 비활성화하더라도, 해당 연결이 이전에 하나 이상의 SSL 모니터 규칙과 매칭한 적이 있거나 나중에 액세스 제어 규칙이나 액세스 제어 정책 기본 작업과 매칭할 경우 연결 종료 이벤트가 방어 센터 데이터베이스에 로깅될 수 있습니다.

암호화 및 해독 불가 트래픽에 대한 기본 처리를 설정하려면

액세스: Admin/Access Admin/Network Admin/Security Approver

1단계 **Policies > SSL**을 선택합니다.

SSL Policy 페이지가 나타납니다.

2단계 수정하려는 SSL 정책 옆의 수정 아이콘( )을 클릭합니다.

SSL 정책 편집기가 나타나며 Rules 탭에 포커스가 있습니다.

3단계 **Default Action** 드롭다운 목록 옆의 로깅 아이콘( )을 클릭합니다.

Logging 팝업 창이 나타납니다.

4단계 **Log at End of Connection**을 선택하여 연결 이벤트 로깅을 활성화합니다.

5단계 연결 이벤트를 어디로 보낼지 지정합니다. 다음과 같이 선택할 수 있습니다.

- 방어 센터에 연결 이벤트를 보내려면 **Defense Center**를 선택합니다.
- 외부 syslog 서버에 이벤트를 보내려면 **Syslog**를 선택한 다음 드롭다운 목록에서 syslog 알림 응답을 선택합니다. 원한다면 추가 아이콘( )을 클릭하여 syslog 알림 응답을 구성할 수 있습니다. 43-5페이지의 Syslog 알림 응답 생성을/를 참조하십시오.
- SNMP 트랩 서버에 이벤트를 보내려면 **SNMP Trap**을 선택하고 드롭다운 목록에서 SNMP 알림 응답을 선택합니다. 원한다면 추가 아이콘( )을 클릭하여 SNMP 알림 응답을 구성할 수 있습니다. 43-4페이지의 SNMP 알림 응답 생성을/를 참조하십시오.

이 연결 이벤트에 대해 방어 센터 기반 분석을 수행하려면 **반드시** 방어 센터에 이벤트를 보내야 합니다. 그러나 SSL 정책 기본 작업에 의해 처리되는 트래픽은 침입, 악성코드 또는 검색 데이터에 대한 추가 검사를 받지 않습니다. 자세한 내용은 38-5페이지의 방어 센터 또는 외부 서버와의 연결 로깅을/를 참조하십시오.

6단계 **OK**를 클릭하여 변경 사항을 저장합니다.

SSL 정책이 연결된 액세스 제어 정책을 적용해야 변경사항이 적용됩니다. 12-15페이지의 액세스 제어 정책 적용을/를 참조하십시오.

액세스 제어 처리 기반 연결 로깅

라이센스: 모두

액세스 제어 정책에 포함된 액세스 제어 규칙은 여러 관리 대상 디바이스의 전 범위에서 네트워크 트래픽을 처리하는 세부적인 방법을 제공합니다. 중요한 연결만 로깅할 수 있도록 액세스 제어 규칙별로 연결 로깅을 활성화합니다. 어떤 규칙에 대해 연결 로깅을 활성화할 경우 그 규칙에서 처리하는 모든 연결이 로깅됩니다.

또한 액세스 제어 정책의 기본 작업에 의해 처리되는 트래픽에 대해 연결을 로깅할 수 있습니다. 이 기본 작업은 정책의 어떤 액세스 제어 규칙과도 매칭하지 않는 트래픽의 처리 방식을 결정합니다. 단 모니터 규칙은 트래픽을 매칭하고 로깅하지만 트래픽을 처리하거나 검사하지 않습니다.

모든 액세스 제어 규칙과 기본 작업에서 로깅을 비활성화하더라도, 해당 연결이 어떤 액세스 제어 규칙과 매칭되고 침입 시도, 금지된 파일 또는 악성코드를 포함하는 경우이거나 해당 연결이 시스템에서 해독되었고 SSL 정책에서 이 연결에 대한 로깅이 활성화된 경우에는 연결 종료 이벤트가 방어 센터 데이터베이스에 로깅될 수 있습니다.

규칙 또는 기본 정책 작업 및 사용자가 구성하는 그 검사 옵션에 따라 로깅 옵션이 달라집니다. 자세한 내용은 다음 링크를 참조하십시오.

- 38-15페이지의 액세스 제어 규칙과 매칭하는 연결의 로깅
- 38-17페이지의 액세스 제어 기본 작업에 의해 처리되는 연결 로깅

액세스 제어 규칙과 매칭하는 연결의 로깅

라이센스: 모두

중요한 연결만 로깅하기 위해 액세스 제어 규칙별로 연결 로깅을 활성화합니다. 어떤 규칙에서 로깅을 활성화할 경우 그 규칙에서 처리하는 모든 연결이 로깅됩니다.

규칙 작업, 이 규칙의 침입 및 파일 검사 컨피그레이션에 따라 로깅 옵션이 달라집니다. 38-6페이지의 액세스 제어 및 SSL 규칙 작업이 로깅에 미치는 영향 이해을/를 참조하십시오. 또한 액세스 제어 규칙에 대한 로깅을 비활성화하더라도 연결이 다음 조건에 해당할 경우 그 규칙과 매칭하는 연결의 연결 종료 이벤트가 방어 센터 데이터베이스에 로깅될 수 있습니다.

- 침입 시도, 금지된 파일 또는 악성코드 포함
- SSL 정책에 의해 검사되고 로깅됨
- 하나 이상의 액세스 제어 모니터 규칙과 매칭한 적이 있음

연결, 파일, 악성코드 정보를 로깅하도록 액세스 제어 규칙을 구성하려면

액세스: Admin/Access Admin/Network Admin

1단계 **Policies > Access Control**을 선택합니다.

Access Control Policy 페이지가 나타납니다.

2단계 수정하려는 액세스 제어 정책 옆의 수정 아이콘( )을 클릭합니다.

액세스 제어 정책 편집기가 나타나며 Rules 탭에 포커스가 있습니다.

3단계 로깅을 구성하려는 규칙 옆의 수정 아이콘( )을 클릭합니다.

액세스 제어 규칙 편집기가 나타납니다.

4단계 Logging 탭을 선택합니다.

Logging 탭이 나타납니다.

5단계 **Log at Beginning of Connection** 또는 **Log at End of Connection**을 선택합니다.

성능 최적화를 위해서는 연결 시작 또는 종료 중 하나만 로깅하십시오.

차단되지 않은 단일 연결의 경우 연결 종료 이벤트는 연결 시작 이벤트의 모든 정보 및 세션 과정에서 수집된 정보를 포함합니다. 차단된 트래픽은 추가 검사 없이 즉시 거부되므로 차단 규칙에 대해서는 연결 시작 이벤트만 로깅할 수 있습니다.

또한 모니터 규칙의 목적은 매칭하는 트래픽을 로깅하는 것이므로 방어 센터 데이터베이스에 대한 연결 종료 로깅이 자동으로 활성화되며 이는 비활성화할 수 없습니다. 자세한 내용은 38-4페이지의 연결 시작 또는 종료 로깅을/를 참조하십시오.

6단계 연결과 관련된 모든 파일 및 악성코드 이벤트를 로깅할지 여부를 지정하려면 **Log Files** 확인란을 사용합니다.

파일 제어 또는 AMP를 수행하기 위해 파일 정책을 이 규칙과 연결할 경우 이 옵션이 자동으로 활성화됩니다. Cisco에서는 이 옵션을 활성 상태로 둘 것을 권장합니다. 38-8페이지의 허용된 연결에 대한 파일 및 악성코드 이벤트 로깅 비활성화을/를 참조하십시오.

7단계 연결 이벤트를 어디로 보낼지 지정합니다. 다음과 같이 선택할 수 있습니다.

- 방어 센터에 연결 이벤트를 보내려면 **방어 센터**를 선택합니다. 모니터 규칙에 대해서는 이 옵션을 비활성화할 수 없습니다.
- 외부 syslog 서버에 이벤트를 보내려면 **Syslog**를 선택한 다음 드롭다운 목록에서 syslog 알림 응답을 선택합니다. 원한다면 추가 아이콘( )을 클릭하여 syslog 알림 응답을 추가할 수 있습니다. 43-5페이지의 Syslog 알림 응답 생성을/를 참조하십시오.
- SNMP 트랩 서버에 이벤트를 보내려면 **SNMP Trap**을 선택하고 드롭다운 목록에서 SNMP 알림 응답을 선택합니다. 원한다면 추가 아이콘( )을 클릭하여 SNMP 알림 응답을 추가할 수 있습니다. 43-4페이지의 SNMP 알림 응답 생성을/를 참조하십시오.

연결 이벤트에 대해 방어 센터 기반 분석을 수행하려면 **반드시** 데이터베이스에 이벤트를 보내야 합니다. 자세한 내용은 38-5페이지의 방어 센터 또는 외부 서버와의 연결 로깅을/를 참조하십시오.

8단계 규칙을 저장하려면 **Save**를 클릭합니다.

규칙이 저장됩니다. 변경 사항이 적용되려면 액세스 제어 정책을 적용해야 합니다. 12-15페이지의 액세스 제어 정책 적용을/를 참조하십시오.

액세스 제어 기본 작업에 의해 처리되는 연결 로깅

라이센스: 모두

액세스 제어 정책의 기본 작업에 의해 처리되는 트래픽에 대해 연결을 로깅할 수 있습니다. 이 기본 작업은 정책의 어떤 액세스 제어 규칙과도 매칭하지 않는 트래픽의 처리 방식을 결정합니다. 단 모니터 규칙은 트래픽을 매칭하고 로깅하지만 트래픽을 처리하거나 검사하지 않습니다. 12-6페이지의 네트워크 트래픽의 기본 처리 및 검사 설정을/를 참조하십시오.

정책의 기본 작업에 의해 처리되는 연결 로깅의 메커니즘과 옵션은 다음 표에서 설명하는 것처럼 개별 액세스 제어 규칙에 의해 처리되는 연결의 로깅 옵션과 대체로 비슷합니다. 즉 차단된 트래픽을 제외하고 연결의 시작 및 종료를 로깅할 수 있으며, 방어 센터 데이터베이스에 또는 외부 syslog나 SNMP 트랩 서버에 연결 이벤트를 보낼 수 있습니다.

표 38-4 액세스 제어 기본 작업 로깅 옵션

기본 작업	비교 대상	참조
Access Control: Block All Traffic	차단 규칙	38-7페이지의 차단된 연결 및 인터랙티브 차단된 연결에 대한 로깅 이해
Access Control: Trust All Traffic	신뢰 규칙	38-7페이지의 신뢰하는 연결에 대한 로깅 이해
Intrusion Prevention	허용 규칙(관련 침입 정책 포함)	38-8페이지의 허용된 연결에 대한 로깅 이해
Network Discovery Only	허용 규칙(관련 침입 정책 제외)	

그러나 액세스 제어 규칙에서 처리하는 연결의 로깅과 기본 작업에서 처리하는 연결의 로깅은 몇 가지 차이점이 있습니다.

- 기본 작업은 파일 로깅 옵션이 없습니다. 기본 작업을 사용하여 파일 제어 또는 AMP를 수행할 수 없습니다.
- 액세스 제어 기본 작업과 연결된 침입 정책에서 침입 이벤트를 생성할 경우에는 해당 연결의 종료가 자동으로 로깅되지 **않습니다**. 이는 어떤 연결 데이터도 로깅하지 않을 침입 탐지 및 방지 전용 구축에서 유용합니다.

  기본 작업에 대해 연결 시작 로깅을 활성화할 경우 이 규칙의 예외가 적용됩니다. 그 경우에는 해당 침입 정책이 트리거되면 연결 시작뿐 아니라 연결 종료도 **로깅**됩니다.

기본 작업에 대한 로깅을 비활성화하더라도, 그 규칙과 매칭하는 연결이 하나 이상의 액세스 제어 모니터 규칙과 매칭된 적이 있거나 SSL 정책에 의해 검사 및 로깅된 경우 연결 종료 이벤트가 방어 센터 데이터베이스에 로깅될 수 있습니다.

액세스 제어 기본 작업에 의해 처리되는 트래픽에서 연결을 로깅하려면

액세스: Admin/Access Admin/Network Admin

1단계 **Policies > Access Control**을 선택합니다.

Access Control Policy 페이지가 나타납니다.

2단계 수정하려는 액세스 제어 정책 옆의 수정 아이콘( )을 클릭합니다.

액세스 제어 정책 편집기가 나타나며 Rules 탭에 포커스가 있습니다.

3단계 **Default Action** 드롭다운 목록 옆의 로깅 아이콘( )을 클릭합니다.

Logging 팝업 창이 나타납니다.

4단계 **Log at Beginning of Connection** 또는 **Log at End of Connection**을 선택합니다.

성능 최적화를 위해서는 이 연결의 시작 또는 종료 중 하나만 로깅하십시오. 차단되지 않은 단일 연결의 경우 연결 종료 이벤트는 연결 시작 이벤트의 모든 정보 및 세션 과정에서 수집된 정보를 포함합니다. 차단된 트래픽은 추가 검사 없이 즉시 거부되므로 Block All Traffic 기본 작업에 대해서는 연결 시작 이벤트만 로깅할 수 있습니다.

5단계 연결 이벤트를 어디로 보낼지 지정합니다. 다음과 같이 선택할 수 있습니다.

- 방어 센터에 연결 이벤트를 보내려면 **Defense Center**를 선택합니다. 모니터 규칙에 대해서는 이 옵션을 비활성화할 수 없습니다.
- 외부 syslog 서버에 이벤트를 보내려면 **Syslog**를 선택한 다음 드롭다운 목록에서 syslog 알림 응답을 선택합니다. 원한다면 추가 아이콘( )을 클릭하여 syslog 알림 응답을 추가할 수 있습니다. 43-5페이지의 Syslog 알림 응답 생성을/를 참조하십시오.
- SNMP 트랩 서버에 이벤트를 보내려면 **SNMP Trap**을 선택하고 드롭다운 목록에서 SNMP 알림 응답을 선택합니다. 원한다면 추가 아이콘( )을 클릭하여 SNMP 알림 응답을 추가할 수 있습니다. 43-4페이지의 SNMP 알림 응답 생성을/를 참조하십시오.

연결 이벤트에 대해 방어 센터 기반 분석을 수행하려면 **반드시** 데이터베이스에 이벤트를 보내야 합니다. 자세한 내용은 38-5페이지의 방어 센터 또는 외부 서버와의 연결 로깅을/를 참조하십시오.

6단계 정책을 저장하려면 **Save**를 클릭합니다.

정책이 저장됩니다. 변경 사항이 적용되려면 액세스 제어 정책을 적용해야 합니다. 12-15페이지의 액세스 제어 정책 적용을/를 참조하십시오.

연결에서 탐지된 URL 로깅

라이센스: FireSIGHT

HTTP 트래픽에 대해 연결 종료 이벤트를 방어 센터 데이터베이스에 로깅할 때 세션 중에 모니터링되는 호스트가 요청한 URL이 기록됩니다.

기본적으로 URL의 첫 1,024자가 연결 로그에 저장됩니다. 그러나 모니터링되는 호스트에서 요청한 전체 URL을 캡처하기 위해 URL당 최대 4,096자까지 저장하도록 구성할 수 있습니다. 또는 방문한 개별 URL이 중요하지 않을 경우 0개의 문자를 저장하는 방법으로 URL 저장을 완전히 비활성화할 수도 있습니다. 네트워크 트래픽에 따라 URL 문자 저장을 비활성화하거나 문자 수를 제한하면 시스템 성능이 향상될 수 있습니다.

URL 로깅을 비활성화하더라도 URL 필터링에 영향을 주지 않습니다. 액세스 제어 규칙은 요청된 URL, 그 범주, 평판에 따라 올바르게 트래픽을 필터링합니다. 이 규칙에서 처리하는 트래픽에 요청된 개별 URL을 기록하지 않더라도 마찬가지입니다. 자세한 내용은 16-8페이지의 URL 차단를 참조하십시오.

저장하는 URL 문자 수를 사용자 지정하려면

액세스: Admin/Access Admin/Network Admin

1단계 **Policies > Access Control**을 선택합니다.

Access Control Policy 페이지가 나타납니다.

2단계 구성하려는 액세스 제어 정책 옆의 수정 아이콘( )을 클릭합니다.

액세스 제어 정책 편집기가 나타납니다.

3단계 Advanced 탭을 선택합니다.

액세스 제어 정책에 대한 고급 설정이 나타납니다.

4단계 General Settings 옆의 수정 아이콘( )을 클릭합니다.

General Settings 팝업 창이 나타납니다.

5단계 **Maximum URL characters to store in connection events**를 입력합니다.

0에서 4096 사이의 숫자 중 하나로 지정할 수 있습니다. 저장할 문자 수가 0이면 URL 저장이 비활성화되지만 URL 필터링은 비활성화되지 않습니다.

6단계 **OK**를 클릭합니다.

액세스 제어 정책에 대한 고급 설정이 나타납니다.

7단계 정책을 저장하려면 **Save**를 클릭합니다.

정책이 저장됩니다. 변경 사항이 적용되려면 액세스 제어 정책을 적용해야 합니다. 12-15페이지의 액세스 제어 정책 적용을/를 참조하십시오.

39장

연결 및 보안 인텔리전스 데이터 작업

매니지드 디바이스는 네트워크의 호스트에서 생성된 트래픽을 모니터링하므로, 탐지하는 연결의 로그를 생성할 수 있습니다. 액세스 제어 및 SSL 정책의 다양한 설정은 로깅할 연결의 종류, 로깅을 실행할 시기, 데이터를 저장할 위치를 세부적으로 제어할 수 있도록 합니다. 대부분의 경우 연결이 로깅되는 때는 연결이 시작되거나 끝날 때, 또는 둘 다입니다.

연결을 로깅할 경우, 시스템에서는 *연결 이벤트*를 생성합니다. 또한 평판 기반의 보안 인텔리전스 기능에 의해 연결이 블랙리스트에 추가(차단)되거나 모니터링될 때마다, *보안 인텔리전스 이벤트*라고 하는 특수한 종류의 연결 이벤트를 로깅할 수 있습니다.

*연결 이벤트*라고 하는 연결 로그에는 탐지된 세션에 대한 데이터가 포함됩니다. 조직의 보안 및 규정준수 요구 사항에 따라 연결을 로깅해야 합니다. 액세스 제어에 도달하기 전에 디바이스 수준에서 fast-path가 설정된 경우를 제외하면, **모든** 연결을 로깅할 수 있습니다.

사용자가 구성하는 로깅 외에도 금지된 파일, 악성코드 또는 침입 시도가 탐지될 경우 시스템에서는 대부분의 연결을 자동으로 로깅합니다. 연결 이벤트 저장을 완전히 비활성화하지 않는 한, 시스템에서는 추가 분석을 위해 이러한 연결 종료 이벤트를 방어 센터 데이터베이스에 저장합니다. 연결 로깅 구성에 대한 자세한 내용은 38-1페이지의 네트워크 트래픽의 연결 로깅을/를 참조하십시오.

참고 모든 어플라이언스 및 라이센스를 사용하여 연결을 로깅할 수 있으나, 개별 연결 또는 보안 인텔리전스 이벤트에 제공되는 정보는 라이센스를 비롯한 여러 요인에 따라 달라집니다. 자세한 내용은 38-9페이지의 연결 로깅의 라이센스 및 모델 요구 사항을/를 참조하십시오.

매니지드 디바이스에서 수집한 연결 데이터를 보완하려는 경우, NetFlow 지원 디바이스에서 생성된 레코드를 사용하여 연결 이벤트를 생성할 수 있습니다. 이는 FireSIGHT 시스템 매니지드 디바이스를 모니터링할 수 없는 네트워크에 NetFlow 지원 디바이스를 구축한 경우 특히 유용합니다.

참고 NetFlow 데이터 수집은 액세스 제어와 연결되어 있지 않으므로, 로깅하려는 NetFlow 연결을 세부적으로 제어할 필요가 없습니다. FireSIGHT 시스템 매니지드 디바이스는 NetFlow 지원 디바이스에서 내보낸 레코드를 탐지하고, 해당 레코드의 데이터를 기준으로 단방향 연결 종료 이벤트를 생성하며, 최종적으로 이러한 이벤트를 방어 센터에 전송하여 데이터베이스 로깅합니다. NetFlow 레코드는 보안 인텔리전스 이벤트를 생성할 수 없으며, 외부 서버에도 로깅할 수 없습니다. 자세한 내용은 45-16페이지의 NetFlow 이해을/를 참조하십시오.

연결 및 보안 인텔리전스 이벤트 작업에 대한 자세한 내용은 다음을 참조하십시오.

연결 및 보안 인텔리전스 데이터 이해

라이센스: 모든

*연결 이벤트*라고 하는 연결 로그에는 탐지된 세션에 대한 데이터가 포함됩니다. 개별 연결 이벤트에 제공되는 정보는 일반적으로 다음과 같은 여러 요인에 따라 달라집니다.

- 기본 연결 속성: 타임스탬프, 소스 및 대상 IP 주소, 인그레스 및 이그레스 영역, 연결을 처리한 디바이스 등
- 시스템에서 검색 또는 유추한 추가 연결 속성: 애플리케이션, 요청 URL, 연결과 연결된 사용자 등
- 연결이 로깅된 사유에 대한 메타데이터: 어떤 정책의 어떤 액세스 제어 규칙(또는 다른 컨피그레이션)이 트래픽을 처리했는지, 연결이 허용 또는 차단되었는지, 암호화 및 해독된 연결에 대한 세부 정보 등

액세스 제어 및 SSL 정책의 다양한 설정은 로깅할 연결의 종류, 로깅을 실행할 시기, 데이터를 저장할 위치를 세부적으로 제어할 수 있도록 합니다. 액세스 제어 및 SSL 정책으로 올바르게 처리 가능한 모든 연결을 로깅할 수 있으며, 이 경우 특정 어플라이언스 모델 또는 라이센스 기능이 필요할 수 있습니다. 다음과 같은 상황에서 연결 로깅을 활성화할 수 있습니다.

- 평판 기반의 보안 인텔리전스 기능에 의해 연결이 블랙리스트에 추가(차단) 또는 모니터링된 경우
- 암호화된 세션이 SSL 정책에 의해 처리된 경우
- 액세스 제어 규칙 또는 액세스 제어 기본 작업에 의해 연결이 처리된 경우

사용자가 구성하는 로깅 외에도 금지된 파일, 악성코드 또는 침입 시도가 탐지될 경우 시스템에서는 대부분의 연결을 자동으로 로깅합니다. 시스템 정책을 사용하여 연결 이벤트 저장을 완전히 비활성화하지 않는 한, 기타 로깅 컨피그레이션에 상관없이 시스템에서는 추가 분석을 위해 이러한 연결 종료 이벤트를 방어 센터 데이터베이스에 저장합니다.

또한 보안 인텔리전스 로깅을 활성화할 경우, 블랙리스트가 매칭되면 *보안 인텔리전스 이벤트* 및 연결 이벤트를 자동으로 생성합니다. 보안 인텔리전스 이벤트는 개별적으로 보고 분석할 수 있는 특수한 종류의 연결 이벤트이며, 별도로 저장 및 삭제할 수도 있습니다. 보안 인텔리전스 블랙리스트 추가 결정을 비롯하여 연결 로깅을 구성하는 방법에 대한 자세한 내용은 38-1페이지의 네트워크 트래픽의 연결 로깅을/를 참조하십시오.

팁 연결 이벤트에 대한 일반적인 정보는 달리 명시되지 않는 한 보안 인텔리전스 이벤트에도 적용됩니다. 보안 인텔리전스에 대한 자세한 내용은 13-1페이지의 보안 인텔리전스 IP 주소 평판 블랙리스트에 추가을/를 참조하십시오.

다음 섹션에서는 탐지된 연결에 제공되는 여러 종류의 정보에 대한 추가적인 세부 정보를 제공합니다.

연결 요약 이해

라이센스: 모든

FireSIGHT 시스템에서는 5분 간격으로 수집된 연결 데이터를 연결 요약으로 취합하며, 시스템에서는 이 정보를 사용하여 연결 그래프 및 트래픽 프로필을 생성합니다. 선택에 따라, 연결 요약 데이터를 기준으로 사용자 지정 워크플로를 생성할 수 있으며 이는 개별 연결 이벤트에 기반한 워크플로를 사용할 때와 같은 방식으로 사용합니다.

해당하는 연결 종료 이벤트를 연결 요약 데이터로 취합할 수는 있지만, 보안 인텔리전스 이벤트에 대한 연결 요약 정보가 따로 제공되지는 않습니다.

여러 연결을 취합하려면 연결의 조건은 다음을 충족해야 합니다.

- 연결의 종료를 나타냄
- 소스 및 대상 IP 주소가 동일하며, 응답자(대상) 호스트에서 동일한 포트를 사용함
- 동일한 프로토콜을 사용함(TCP 또는 UDP)
- 동일한 애플리케이션 프로토콜을 사용함
- 동일한 Cisco 매니지드 디바이스로 탐지되거나 동일한 NetFlow 지원 디바이스에 의해 내보내기됨

각 연결 요약에는 총 트래픽 통계 및 요약에 나와 있는 연결 수가 포함됩니다. NetFlow 지원 디바이스는 단방향 연결을 생성하므로, 요약의 연결 수는 NetFlow 데이터를 기준으로 모든 연결마다 2배로 증가합니다.

연결 요약에는 요약의 취합된 연결과 관련된 모든 정보가 포함되지는 않습니다. 예를 들어, 클라이언트 정보는 연결 데이터를 연결 요약으로 취합하는 데 사용되지 않으므로 요약에는 클라이언트 정보가 포함되지 않습니다.

자세한 내용은 다음 절을 참조하십시오.

- 39-3페이지의 Long-Running 연결
- 39-4페이지의 외부 응답자의 연결 요약 통합
- 39-11페이지의 연결 및 보안 인텔리전스 이벤트에서 제공되는 정보

Long-Running 연결

라이센스: 모든

연결 데이터가 트리거되는 모니터링된 세션이 두 번 이상 5분 간격에 걸쳐 이루어질 경우, 해당 연결은 *long-running 연결*로 간주됩니다. 연결 요약의 연결 수를 계산할 경우, long-running 연결이 시작된 5분 간격에 대해서만 수가 증가합니다.

또한 long-running 연결에서 개시자 및 응답자가 전송한 패킷과 바이트 수를 계산할 경우, 각 5분 간격 동안 실제로 전송된 패킷과 바이트 수는 보고되지 않습니다. 그 대신, 시스템에서는 일정한 전송 속도를 추정하며 전송된 패킷과 바이트의 총 개수, 연결의 길이, 각 5분 간격 동안 발생한 연결의 부분을 기준으로 예측 수치를 계산합니다.

외부 응답자의 연결 요약 통합

라이센스: 모든

연결 데이터를 저장하는 데 필요한 공간을 줄이고 연결 그래프의 렌더링 속도를 높이기 위해, 시스템에서는 다음과 같은 경우 연결 요약을 통합합니다.

- 연결과 관련된 호스트 중 하나가 모니터링된 네트워크에 없을 경우
- 외부 호스트의 IP 주소 이외에, 요약의 연결이 39-3페이지의 연결 요약 이해에 나열된 취합 기준(프로토콜, 애플리케이션 프로토콜, 탐지 디바이스 등)에 부합할 경우

이벤트 뷰어에서 연결 요약을 보고 연결 그래프 작업을 수행할 경우, 시스템에서는 모니터링되지 않는 호스트의 IP 주소 대신 외부를 표시합니다.

이렇게 취합하면 외부 응답자와 관련된 연결 요약 또는 그래프에서 연결 데이터(즉, 개별 연결에 대한 액세스 데이터)의 테이블 보기로 드릴다운하려고 할 경우, 테이블 보기에 아무런 정보가 포함되지 않습니다.

연결 및 보안 인텔리전스 데이터 필드 이해

라이센스: 기능에 따라 다름

지원되는 디바이스: 기능에 따라 다름

지원되는 Defense Center: 기능에 따라 다름

각 연결 테이블 보기 또는 연결 그래프에는 사용자가 보는 연결 또는 연결 요약에 대한 정보(타임스탬프, IP 주소, 위치 정보, 애플리케이션 등)가 포함됩니다. 보안 인텔리전스 이벤트 보기에는 연결 이벤트 보기와 동일한 일반적인 정보가 포함되지만, **Security Intelligence Category** 값이 할당된 연결만 나열됩니다.

참고 개별 연결 또는 보안 인텔리전스 이벤트에 대해 사용 가능한 정보는 라이센스 및 어플라이언스 모델을 비롯한 여러 요소에 따라 달라집니다. 자세한 내용은 38-9페이지의 연결 로깅의 라이센스 및 모델 요구 사항을/를 참조하십시오.

다음 목록에는 FireSIGHT 시스템에 의해 로깅된 연결 데이터가 자세히 나와 있습니다. 정보가 개별 연결 또는 보안 인텔리전스 이벤트에 로깅되도록 결정하는 요인에 대한 내용은 다음 섹션 39-11페이지의 연결 및 보안 인텔리전스 이벤트에서 제공되는 정보을/를 참조하십시오.

Access Control Policy

연결을 모니터링하는 액세스 제어 정책입니다.

Access Control Rule

연결을 처리한 액세스 제어 규칙 또는 기본 작업이자, 해당 연결과 매칭된 최대 8개의 Monitor 규칙입니다.

연결이 하나의 Monitor 규칙과 매칭될 경우, 방어 센터에는 연결을 처리한 규칙의 이름이 표시되며 그 뒤에 Monitor 규칙 이름이 표시됩니다. 연결이 여러 개의 Monitor 규칙과 매칭될 경우, 이벤트 뷰어에는 매칭되는 Monitor 규칙의 개수가 표시됩니다(예: `기본 작업 + Monitor 규칙 2개`)

연결과 매칭되는 처음 8개의 Monitor 규칙이 포함된 팝업 창을 표시하려면, *N* **Monitor Rules**를 클릭합니다.

Action

연결을 로깅하는 액세스 제어 규칙 또는 기본 작업과 관련된 작업입니다.

- `Allow`는 명시적으로 허용되고, 사용자 우회를 통해 인터랙티브 방식으로 차단된 연결을 나타냅니다.
- `Trust`는 신뢰할 수 있는 연결을 나타냅니다. 시스템에서 로깅하는 Trust 규칙에 의해 탐지된 TCP 연결은 어플라이언스에 따라 달라집니다.

  Series 2, 가상 디바이스, Cisco NGIPS for Blue Coat X-Series의 경우 첫 번째 패킷의 Trust 규칙에 의해 탐지된 TCP 연결은 연결 종료 이벤트만 생성합니다. 시스템에서는 최종 세션 패킷이 끝난 지 한 시간 후에 이벤트를 생성합니다.

  Series 3 어플라이언스의 경우 첫 번째 패킷의 Trust 규칙에 의해 탐지된 TCP 연결은 Monitor 규칙의 존재 여부에 따라 다른 이벤트를 생성합니다. Monitor 규칙이 활성화된 경우 시스템에서는 패킷을 평가하며, 시작 및 연결 종료 이벤트를 모두 생성합니다. Monitor 규칙이 활성화되지 않은 경우, 시스템에서는 연결 종료 이벤트만 생성합니다.
- `Block` 및 `Block with reset`은 차단된 연결을 나타냅니다. 또한 시스템에서는 보안 인텔리전스에 의해 블랙리스트에 추가된 연결, SSL 정책에 의해 차단된 연결, 침입 정책에 의해 익스플로잇이 탐지된 연결, 파일 정책에 의해 파일이 차단된 연결을 `Block` 작업과 연결합니다.
- `Interactive Block` 및 `Interactive Block with reset`은시스템에서 Interactive Block 규칙을 사용하여 사용자의 HTTP 요청을 처음 차단할 때 로깅할 수 있는 beginning-of-connection 이벤트를 표시합니다. 사용자가 시스템에 표시된 경고 페이지를 클릭할 경우, 세션에 대해 로깅하는 모든 추가 연결 이벤트에는 `Allow` 작업이 포함됩니다.
- `Default Action` - 연결이 기본 작업에 의해 처리되었음을 나타냅니다.
- 보안 인텔리전스로 모니터링된 연결의 경우, 작업은 연결에 의해 트리거되는 첫 번째 비 Monitor 액세스 제어 규칙 또는 기본 작업입니다. 이와 마찬가지로, Monitor 규칙과 매칭되는 트래픽은 항상 후속 규칙 또는 기본 규칙에 의해 처리되므로 Monitor 규칙에 의해 로깅된 연결과 관련된 작업은 `Monitor`가 될 수 없습니다.

Application Protocol

호스트 간의 통신을 나타내는 애플리케이션 프로토콜이 연결에서 탐지됩니다.

Application Risk

연결에서 탐지된 애플리케이션 트래픽과 관련된 위험도(`Very High`, `High`, `Medium`, `Low`, `Very Low`)입니다. 연결에서 탐지된 각 유형의 애플리케이션에는 관련 위험도가 포함되며, 이 필드에는 가장 높은 순서부터 표시됩니다. 자세한 내용은 45-11 페이지의 표 45-2을/를 참조하십시오.

Business Relevance

연결에서 탐지된 애플리케이션 트래픽과 관련된 비즈니스 관련성(`Very High`, `High`, `Medium`, `Low`, `Very Low`)입니다. 연결에서 탐지된 각 애플리케이션 유형에는 관련된 비즈니스 연관성이 있습니다. 이 필드에는 그중 가장 낮은 값(가장 연관성이 적음)이 표시됩니다. 자세한 내용은 45-11 페이지의 표 45-2을/를 참조하십시오.

Category, Tag(Application Protocol, Client, Web Application)

애플리케이션의 기능을 파악하는 데 도움이 될 수 있도록 애플리케이션의 특성을 분류하는 기준입니다. 자세한 내용은 45-11 페이지의 표 45-2을/를 참조하십시오.

Client and Client Version

연결에서 탐지된 클라이언트 애플리케이션 및 클라이언트 버전입니다.

시스템이 연결에 사용된 특정 클라이언트를 식별하지 못할 경우, 이 필드에는 애플리케이션 프로토콜 이름에 추가된 클라이언트가 표시되어 일반 이름을 제공합니다(예: FTP 클라이언트).

Connections

연결 요약의 연결 개수입니다. 여러 연결 요약 간격에 걸쳐 있는 Long-Running 연결의 경우, 첫 번째 연결 요약 간격만 증가합니다.

Count

각 행에 표시되는 정보와 매칭되는 연결 개수입니다. 둘 이상의 동일한 행을 생성하는 제약 조건을 적용한 경우에만 **Count** 필드가 나타납니다.

참고 사용자 지정 워크플로를 생성하고 **Count** 열을 드릴다운 페이지에 추가하지 않은 경우, 각 연결은 개별적으로 나열되고 패킷과 바이트는 합산되지 않습니다.

Device

일반 연결 또는 NetFlow 지원 디바이스에서 내보낸 연결을 탐지하는 매니지드 디바이스, NetFlow 데이터를 처리하는 매니지드 디바이스입니다.

Files

연결과 관련된 파일 이벤트입니다. 파일 목록 대신, 방어 센터에서는 이 필드에 파일 보기 아이콘( )을 표시합니다. 아이콘의 숫자는 해당 연결에서 탐지되거나 차단된 파일(악성코드 파일 포함)의 수를 나타냅니다.

연결에서 탐지된 파일 목록은 물론, 해당 유형 및 악성코드 조회 속성이 포함된 팝업 창을 표시하려면 이 아이콘을 클릭합니다.

DC500 방어 센터 또는 Series 2 디바이스에서는 네트워크 기반의 악성코드 파일 탐지를 지원하지 않습니다.

자세한 내용은 39-30페이지의 연결에서 탐지된 파일 보기을/를 참조하십시오.

First Packet or Last Packet

세션의 첫 번째 또는 마지막 패킷이 표시된 날짜와 시간입니다.

HTTP Referrer

연결에서 탐지된 HTTP 트래픽에 대해 요청한 URL의 참조 페이지를 나타내는 HTTP 참조 페이지입니다(예: 다른 URL에 대한 링크를 제공하거나, 다른 URL에서 링크를 가져온 웹 사이트).

Ingress Interface or Egress Interface

연결과 관련된 인그레스 또는 이그레스 인터페이스입니다. 구축에 비동기식 라우팅 컨피그레이션이 포함된 경우, 인그레스 및 이그레스 인터페이스는 동일한 인터페이스 집합에 속할 수 있습니다.

Ingress Security Zone or Egress Security Zone

연결과 관련된 인그레스 또는 이그레스 보안 영역입니다.

Initiator Bytes or Responder Bytes

세션 개시자 또는 세션 응답자가 전송한 총 바이트 수입니다.

Initiator Country or Responder Country

라우팅 가능한 IP가 탐지된 경우, 세션을 시작한 호스트 IP 주소 또는 세션 응답자와 연결되는 국가입니다. 해당 국가의 국기 아이콘 및 ISO 3166-1 알파-3 국가 코드가 표시됩니다. 국가의 전체 이름을 보려면 국기 아이콘 위에 마우스 포인터를 올려놓습니다.

DC500 방어 센터에서는 이 기능을 지원하지 않습니다.

Initiator IP or Responder IP

시작하거나 세션 응답자에 응답한 호스트 IP 주소(또는 DNS 솔루션이 활성화된 경우에는 호스트 이름)입니다. 블랙리스트 연결에서 블랙리스트 IP 주소를 식별할 수 있도록 하기 위해, 블랙리스트 IP 주소 옆의 아이콘은 조금 다른 모양으로 표시됩니다.

Initiator Packets or Responder Packets

세션 개시자 또는 세션 응답자가 전송한 총 패킷 수입니다.

Initiator User

세션 개시자에 로그인한 사용자입니다.

Intrusion Events

연결과 관련된 침입 이벤트입니다. 이벤트 목록 대신, 방어 센터에서는 이 필드에 침입 이벤트 보기 아이콘(방어 센터)을 표시합니다.방어 센터

연결과 관련된 침입 이벤트 목록은 물론, 해당 이벤트의 우선순위 및 미치는 영향이 포함된 팝업 창을 표시하려면 이 아이콘을 클릭합니다. 자세한 내용은 39-31페이지의 연결과 관련된 침입 이벤트 보기을/를 참조하십시오.

IOC

이벤트가 연결과 관련된 호스트에 대해 IOC(보안 침해 지표)를 트리거했는지 여부를 나타냅니다. IOC에 대한 자세한 내용은 45-20페이지의 IOC 이해을/를 참조하십시오.

NetBIOS 도메인

세션에 사용된 NetBIOS 도메인입니다.

NetFlow Destination/Source Autonomous System

NetFlow 지원 디바이스에서 내보낸 연결을 위한 필드로, 연결의 트래픽 소스 또는 대상에 대한 경계 게이트웨이 프로토콜 자동 시스템 수입니다.

NetFlow Destination/Source Prefix

NetFlow 지원 디바이스에서 내보낸 연결을 위한 필드로, 소스 또는 대상 접두사 마스크가 포함된 소스 또는 대상 IP 주소 ANDed입니다.

NetFlow Destination/Source TOS

NetFlow 지원 디바이스에서 내보낸 연결을 위한 필드로, 연결 트래픽이 NetFlow 지원 디바이스에 들어오거나 나갈 경우 서비스 유형(TOS) 바이트에 대한 설정입니다.

NetFlow SNMP Input/Output

NetFlow 지원 디바이스에서 내보낸 연결을 위한 필드로, 연결 트래픽이 NetFlow 지원 디바이스에 들어오거나 나갈 경우 인터페이스에 대한 인터페이스 색인입니다.

Network Analysis Policy

네트워크 분석 정책(NAP)은 이벤트 생성과 연결됩니다.

Reason

다음과 같은 상황에서 연결이 로깅된 사유입니다.

- User Bypass는 시스템에서 사용자의 HTTP 요청을 처음에 차단했으나, 사용자가 경고 페이지를 클릭하여 원래 요청한 사이트를 계속 진행하도록 선택했음을 나타냅니다. User Bypass의 사유는 Allow 작업과 항상 쌍을 이룹니다.
- IP Block은 시스템에서 보안 인텔리전스 데이터를 기준으로 검사 없이 연결을 거부했음을 나타냅니다. IP Block의 사유는 Block 작업과 항상 쌍을 이룹니다.
- IP Monitor는 시스템에서 보안 인텔리전스 데이터를 기준으로 연결을 거부했을 수 있으나, 사용자가 연결을 거부하는 대신 모니터링하도록 시스템을 구성했음을 나타냅니다.
- File Monitor는 시스템이 연결에서 특정 유형의 파일을 탐지했음을 나타냅니다.
- File Block은 시스템에 의해 전송이 차단된 파일 또는 악성코드 파일이 연결에 포함되었음을 나타냅니다. File Block의 사유는 Block 작업과 항상 쌍을 이룹니다.
- File Custom Detection은 시스템에 의해 전송이 차단된 사용자 지정 탐지 목록의 파일이 연결에 포함되었음을 나타냅니다.
- File Resume Allow는 파일 전송이 원래 Block Files 또는 Block Malware 파일 규칙에 의해 차단되었음을 나타냅니다. 파일을 허용하는 새로운 액세스 제어 정책이 적용되면, HTTP 세션이 자동으로 다시 시작됩니다. 이 사유는 인라인 구축에서만 표시됩니다.
- File Resume Block은 파일 전송이 원래 Detect Files 또는 Malware Cloud Lookup 파일 규칙에 의해 허용되었음을 나타냅니다. 파일을 차단하는 새로운 액세스 제어 정책이 적용되면, HTTP 세션이 자동으로 중단됩니다. 이 사유는 인라인 구축에서만 표시됩니다.
- SSL Block은 시스템에서 SSL 검사 컨피그레이션을 기준으로 차단 및 암호화한 연결을 나타냅니다. SSL Block의 사유는 Block 작업과 항상 쌍을 이룹니다.
- Intrusion Block은 시스템이 연결에서 탐지된 익스플로잇(침입 정책 위반)을 차단했거나 차단했을 가능성이 있음을 나타냅니다. Intrusion Block의 사유는 차단된 익스플로잇의 경우 Block 작업과 쌍을 이루고, 차단되었을 수 있는 익스플로잇의 경우 Allow와 쌍을 이룹니다.
- Intrusion Monitor는 시스템이 연결에서 익스플로잇을 탐지했으나 이를 차단하지 않았음을 나타냅니다. 이러한 경우는 트리거된 침입 규칙의 상태가 **Generate Events**로 설정된 경우 발생합니다.

Referenced Host

연결의 프로토콜이 DNS, HTTP 또는 HTTPS인 경우 이 필드에는 해당 프로토콜을 사용 중인 호스트 이름이 표시됩니다.

Security Context

트래픽이 통과된 가상 방화벽 그룹을 식별하는 메타데이터입니다. 이 필드는 다중 컨텍스트 모드의 ASA FirePOWER 디바이스에 대해서만 채워집니다.

Security Intelligence Category

연결의 블랙리스트 IP 주소를 나타내거나 포함하는 블랙리스트 객체의 이름입니다. 보안 인텔리전스 카테고리는 네트워크 객체 또는 그룹의 이름, 전역 블랙리스트, 사용자 지정 인텔리전스 목록 또는 피드, 인텔리전스 피드의 카테고리 중 하나가 될 수 있습니다. 이 필드는 **Reason**이 IP Block 또는 IP Monitor인 경우에만 채워집니다. 보안 인텔리전스 이벤트 보기의 항목에는 항상 사유가 표시됩니다. 자세한 내용은 13-1페이지의 보안 인텔리전스 IP 주소 평판 블랙리스트에 추가을/를 참조하십시오.

DC500 방어 센터 또는 Series 2 디바이스에서는 이 기능을 지원하지 않습니다.

Source Device

연결에 대한 데이터를 내보낸 NetFlow 지원 디바이스의 IP 주소입니다. 매니지드 디바이스에서 연결을 탐지한 경우, 이 필드에는 `FireSIGHT`의 값이 포함됩니다.

Source Port/ICMP Type 또는 Destination Port/ICMP Code

세션 개시자 또는 세션 응답자가 사용한 포트, ICMP 유형 또는 ICMP 코드입니다.

SSL Status

SSL 규칙, 기본 작업 또는 암호화된 연결을 로깅한 해독 불가능한 트래픽 작업과 관련된 작업입니다.

- `Block` 및 `Block with reset` - 차단된 암호화 연결을 나타냅니다.
- `Decrypt (Resign)` - 다시 서명된 서버 인증서를 사용하여 해독된 발신 연결을 나타냅니다.
- `Decrypt (Replace Key)` - 대체된 공개 키가 있는 자체 서명된 서버 인증서를 사용하여 해독된 발신 연결을 나타냅니다.
- `Decrypt (Known Key)` - 알려진 개인 키를 사용하여 해독된 수신 연결을 나타냅니다.
- `Do not Decrypt` - 시스템이 해독하지 못한 연결을 나타냅니다.

시스템이 암호화된 연결을 해독하지 못할 경우, 해독 불가능한 트래픽 작업이 실행되었다는 내용과 함께 실패 사유가 표시됩니다. 예를 들어, 시스템이 알 수 없는 암호 그룹으로 암호화된 트래픽을 탐지하고 추가 검사 없이 이를 허용할 경우 이 필드는 `Do Not Decrypt (Unknown Cipher Suite)`로 표시됩니다.

인증서 세부사항을 보려면 잠금 아이콘( )을 클릭합니다. 자세한 내용은 39-32페이지의 암호화된 연결과 관련된 인증서 보기을/를 참조하십시오.

SSL Certificate Status

암호화된 트래픽이 SSL 규칙과 매칭될 경우, 이 필드에는 서버 인증서 상태가 표시됩니다. 해독 불가능한 트래픽이 SSL 규칙과 매칭될 경우, 이 필드는 `Not Checked`로 표시됩니다. 자세한 내용은 22-23페이지의 암호화된 트래픽을 인증서 상태로 제어을/를 참조하십시오.

SSL Flow Error

SSL 세션 도중 오류가 발생했을 때의 오류 이름 및 16진수 코드입니다. 오류가 발생하지 않은 경우 **Success**로 표시됩니다.

SSL Version

연결을 암호화하는 데 사용된 SSL 또는 TLS 프로토콜 버전입니다.

SSL Cipher Suite

연결을 암호화하는 데 사용된 암호 그룹입니다.

SSL Policy

연결을 처리한 SSL 정책입니다.

SSL Rule

연결을 처리한 SSL 규칙 또는 기본 작업이자, 해당 연결과 매칭된 첫 번째 Monitor 규칙입니다. 연결이 Monitor 규칙과 매칭될 경우, 방어 센터에는 연결을 처리한 규칙의 이름이 표시되며 그 뒤에 Monitor 규칙 이름이 표시됩니다.

SSL Session ID

SSL 핸드셰이크 도중 클라이언트와 서버 간에 협상된 16진수 Session ID입니다.

SSL Ticket ID

SSL 핸드셰이크 도중 전송된 세션 티켓 정보의 16진수 해시 값입니다.

SSL Flow Flags

암호화된 연결에 대한 처음 10개의 디버깅 수준 플래그입니다. 모든 플래그를 보려면 생략 부호(...)를 클릭합니다.

SSL Flow Messages

SSL 핸드셰이크 도중 클라이언트와 서버 간에 교환된 메시지입니다. 자세한 내용은 http://tools.ietf.org/html/rfc5246을/를 참조하십시오.

TCP Flags

연결에서 탐지된 TCP 플래그입니다.

시간

연결 요약에서 연결을 취합하는 데 사용된 5분 간격의 종료 시간입니다.

URL, URL Category, and URL Reputation

세션 도중 모니터링된 호스트에서 요청한 URL과 관련 카테고리 및 평판입니다.

시스템에서 SSL 애플리케이션을 식별하거나 차단한 경우, 요청한 URL은 암호화된 트래픽에 있으므로 시스템은 SSL 인증서를 기준으로 해당 트래픽을 식별합니다. 따라서 SSL 애플리케이션에 대해, 이 필드는 인증서에 포함된 공용 이름을 나타냅니다.

DC500 방어 센터 또는 Series 2 디바이스에서는 URL 카테고리 또는 평판 데이터를 지원하지 않습니다.

User Agent

연결에서 탐지된 HTTP 트래픽에서 추출된 사용자 에이전트 애플리케이션 정보입니다.

Web Application

연결에서 탐지된 HTTP 트래픽의 콘텐츠 또는 요청한 URL을 나타내는 웹 애플리케이션입니다.

웹 애플리케이션이 이벤트의 URL과 매칭되지 않을 경우, 해당 트래픽은 참조 트래픽(예: 광고 트래픽)일 가능성이 높습니다. 시스템이 참조 트래픽을 탐지할 경우, 시스템은 제공되는 참조 애플리케이션을 저장하고 해당 애플리케이션을 웹 애플리케이션으로 나열합니다.

시스템이 HTTP 트래픽에서 특정 웹 애플리케이션을 식별하지 못할 경우, 이 필드는 `Web Browsing`으로 표시됩니다.

연결 및 보안 인텔리전스 이벤트에서 제공되는 정보

라이센스: 기능에 따라 다름

지원되는 디바이스: 기능에 따라 다름

지원되는 Defense Center: 기능에 따라 다름

개별 연결, 연결 요약 또는 보안 인텔리전스 이벤트에 제공되는 정보는 여러 요인에 따라 달라집니다.

어플라이언스 모델 및 라이센스

액세스 제어 및 SSL 정책으로 올바르게 처리 가능한 모든 연결을 로깅할 수 있습니다. 그러나 대다수의 기능은 대상 디바이스에서 특정 라이센스 기능을 활성화해야 하며, 특정 모델에서만 사용 가능한 기능도 많습니다.

예를 들어, SSL 검사는 Series 3 디바이스가 있어야 합니다. 다른 어플라이언스 모델은 암호화된 트래픽을 검사할 수 없습니다. 로깅된 연결 이벤트에는 암호화된 연결에 대한 정보가 포함되지 않습니다. 또 다른 예를 들자면, DC500을 사용하여 연결 이벤트의 위치 데이터를 볼 수 없습니다. 자세한 내용은 38-9페이지의 연결 로깅의 라이센스 및 모델 요구 사항을/를 참조하십시오.

트래픽 특성

시스템은 네트워크 트래픽에 존재하고 탐지 가능한 정보만 보고합니다. 예를 들어, 사용자가 개시자 호스트와 연결되지 않거나 프로토콜이 DNS, HTTP 또는 HTTPS가 아닌 연결에서 참조 호스트가 탐지되지 않을 수 있습니다.

탐지 방법: FireSIGHT 시스템과 NetFlow 비교

TCP 플래그 및 NetFlow 자동 시스템, 접두사, TOS 데이터를 제외하면 NetFlow 레코드에서 제공되는 정보는 매니지드 디바이스를 사용하는 네트워크 트래픽을 모니터링하여 생성한 정보보다 더욱 제한적입니다. 자세한 내용은 45-17페이지의 NetFlow 및 FireSIGHT 데이터 간 차이점을/를 참조하십시오.

로깅 방법: 연결의 시작 또는 종료

시스템이 연결을 탐지한 경우, 연결의 시작/종료(또는 두 시점 모두) 시점 중 연결을 언제 로깅할 수 있는지는 사용자가 시스템의 연결 탐지 및 처리 방식을 어떻게 구성하느냐에 따라 달라집니다(38-4페이지의 연결 시작 또는 종료 로깅 참조).

Beginning-of-connection 이벤트에는 세션 기간 중에 트래픽을 검사하여 확인해야 하는 정보(예: 전송된 총 데이터의 양, 연결의 마지막 패킷의 타임스탬프)가 포함되지 않습니다.
Beginning-of-connection 이벤트에는 세션의 애플리케이션 또는 URL 트래픽에 대한 정보가 없을 수 있으며, 세션의 암호화에 대한 세부 정보도 포함되지 않습니다.

검사 방법: 관련 SSL, 파일, 침입 정책

SSL 정책에 따라 처리한 암호화된 연결에만 연결 로그에 SSL 관련 정보가 포함됩니다. 관련 파일 정책이 포함된 액세스 제어 규칙으로 로깅한 연결에만 파일 정보가 포함됩니다. 이와 마찬가지로, 연결 로그에서 침입 정보를 보려면 침입 정책을 액세스 제어 규칙 또는 기본 작업과 연결해야 합니다.

연결 이벤트 유형: 개별 또는 요약

연결 요약에는 취합된 연결과 관련된 모든 정보가 포함되지 않습니다. 예를 들어, 클라이언트 정보는 연결 데이터를 연결 요약으로 취합하는 데 사용되지 않으므로 요약에는 클라이언트 정보가 포함되지 않습니다.

연결 그래프는 연결 종료 로그만 사용하는 연결 요약 데이터를 기준으로 합니다. 연결 시작 데이터만 로깅할 경우, 연결 그래프 및 연결 요약 이벤트 보기에 데이터가 포함되지 않습니다.

기타 컨피그레이션

액세스 제어 정책의 고급 설정에서는 HTTP 세션에서 모니터링된 호스트에서 요청한 각 URL의 연결 로그에 저장되는 특성의 수를 제어합니다. 이 설정을 사용하여 URL 로깅을 비활성화할 경우, 카테고리 및 평판 데이터가 존재하고 이를 계속 볼 수 있는 경우에도 시스템에서는 연결 로그에 개별 URL을 표시하지 않습니다.

또한 일부 연결 이벤트에는 **Reason**이 포함되지 않습니다. 이는 사용자가 Interactive Block 컨피그레이션을 우회하는 경우처럼 특정한 상황에서만 채워지는 필드입니다(39-8페이지의 Reason 참조).

다음 표에는 각 연결 이벤트/보안 인텔리전스 이벤트 필드가 나열되며, 시스템에서 해당 필드에 정보를 표시하는지 여부는 탐지 방법, 로깅 방법, 연결 이벤트 유형에 따라 달라집니다. 보안 인텔리전스 이벤트는 취합되지 않으므로, Summary 열은 연결 이벤트 요약만 참조합니다.

팁 연결 이벤트 및 보안 인텔리전스 이벤트의 테이블 보기에서는 각 유형의 애플리케이션, NetFlow 관련 필드, SSL 관련 필드, 기타에 대한 Category 및 Tag 필드를 비롯하여 몇 가지 필드가 기본적으로 표시되지 않습니다. 이벤트 보기에서 숨겨진 필드를 표시하려면, 검색 제한 사항을 확장한 다음 **Disabled Columns** 아래에서 해당 필드 이름을 클릭합니다.

표 39-1 로깅 및 탐지 방법을 기준으로 한 연결 및 보안 인텔리전스 데이터

	탐지 방법:		로깅 방법:		연결 이벤트:	
필드	FireSIGHT	NetFlow	시작	끝	단일	요약
Time	예	예	아니요	예	아니요	예
First Packet	예	예	예	예	예	아니요
Last Packet	예	예	아니요	예	예	아니요
Action	예	아니요	예	예	예	아니요
Reason	예	아니요	예	예	예	아니요
Initiator IP	예	예	예	예	예	예
Initiator Country	예	아니요	예	예	예	예
Initiator User	예	예	예	예	예	예
Responder IP	예	예	예	예	예	예
Responder Country	예	아니요	예	예	예	예
Security Intelligence Category	예	아니요	예	예	예	아니요
Ingress Security Zone	예	아니요	예	예	예	예
Egress Security Zone	예	아니요	예	예	예	예
Source Port/ICMP Code	예	예	예	예	예	아니요
Destination Port/ICMP Type	예	예	예	예	예	예
SSL Status	예	아니요	아니요	예	예	아니요
SSL Certificate Status	예	아니요	아니요	예	예	아니요
SSL Version	예	아니요	아니요	예	예	아니요

표 39-1 로깅 및 탐지 방법을 기준으로 한 연결 및 보안 인텔리전스 데이터(계속)

	탐지 방법:		로깅 방법:		연결 이벤트:	
필드	FireSIGHT	NetFlow	시작	끝	단일	요약
SSL Policy	예	아니요	아니요	예	예	아니요
SSL Rule	예	아니요	아니요	예	예	아니요
SSL Cipher Suite	예	아니요	아니요	예	예	아니요
SSL Flow Flags	예	아니요	아니요	예	예	아니요
SSL Flow Messages	예	아니요	아니요	예	예	아니요
Application Protocol	예	예	사용 가능한 경우	예	예	예
Client	예	아니요	사용 가능한 경우	예	예	아니요
Client Version	예	아니요	사용 가능한 경우	예	예	아니요
Web Application	예	아니요	사용 가능한 경우	예	예	아니요
Category, Tag(Application Protocol, Client, Web Application)	예	아니요	사용 가능한 경우	예	예	아니요
Application Risk	예	아니요	사용 가능한 경우	예	예	아니요
Business Relevance	예	아니요	사용 가능한 경우	예	예	아니요
URL	예	아니요	사용 가능한 경우	예	예	아니요
URL Category	예	아니요	사용 가능한 경우	예	예	아니요
URL Reputation	예	아니요	사용 가능한 경우	예	예	아니요
VLAN ID	예	아니요	예	예	예	아니요
Referenced Host	예	아니요	아니요	예	예	아니요
User Agent	예	아니요	아니요	예	예	아니요
HTTP Referrer	예	아니요	아니요	예	예	아니요
IOC	예	아니요	예	예	예	아니요
Intrusion Events	예	아니요	아니요	예	예	아니요
Files	예	아니요	아니요	예	예	아니요
Intrusion Policy	예	아니요	예	예	예	아니요
Access Control Policy	예	아니요	예	예	예	아니요
Access Control Rule	예	아니요	예	예	예	아니요
Network Analysis Policy	예	아니요	예	예	예	아니요
Device	예	예	예	예	예	예
Ingress Interface	예	아니요	예	예	예	예

표 39-1 로깅 및 탐지 방법을 기준으로 한 연결 및 보안 인텔리전스 데이터(계속)

	탐지 방법:		로깅 방법:		연결 이벤트:	
필드	FireSIGHT	NetFlow	시작	끝	단일	요약
Egress Interface	예	아니요	예	예	예	예
Security Context (ASA only)	예	아니요	예	예	예	예
TCP Flags	아니요	예	아니요	예	예	아니요
NetFlow Destination/Source Autonomous System	아니요	예	아니요	예	예	아니요
NetFlow Destination/Source Prefix	아니요	예	아니요	예	예	아니요
NetFlow Destination/Source TOS	아니요	예	아니요	예	예	아니요
NetFlow SNMP Input/Output	아니요	예	아니요	예	예	아니요
Source Device	예	예	FireSIGHT	예	예	예
NetBIOS Domain	예	아니요	예	예	예	아니요
Initiator Packets	예	예	유용하지 않음	예	예	예
Responder Packets	예	예	유용하지 않음	예	예	예
Initiator Bytes	예	예	유용하지 않음	예	예	예
Responder Bytes	예	예	유용하지 않음	예	예	예
Connections	예	예	아니요	예	아니요	예
Count	예	예	예	예	예	아니요

연결 및 보안 인텔리전스 데이터 보기

라이센스: 기능에 따라 다름

지원되는 디바이스: 기능에 따라 다름

지원되는 Defense Center: 기능에 따라 다름

연결 데이터에 대한 심층적인 통찰력을 제공하기 위해, 시스템은 연결 데이터를 그래픽 및 테이블 형식으로 표시할 수 있습니다. 연결 데이터에 액세스할 때 표시되는 페이지는 사용 중인 워크플로에 따라 달라집니다. 미리 정의된 워크플로 중 하나를 사용하거나, 특정 요구 사항에 부합하는 정보만 표시하는 사용자 지정 워크플로를 생성할 수 있습니다.

보안 인텔리전스 이벤트는 보호 라이센스가 필요하며 테이블 형식으로만 표시됩니다. 보안 인텔리전스 데이터는 Series 2 매니지드 디바이스 또는 DC500 방어 센터에서 지원되지 않습니다. 보안 인텔리전스 이벤트의 연결 이벤트 데이터는 그래프 형식으로 볼 수 있으나, 보안 인텔리전스 이벤트에서 데이터 그래프를 생성할 수는 없습니다. 보안 인텔리전스 데이터의 인터랙티브 그래픽 보기를 보려는 경우, Context Explorer의 Security Intelligence 섹션을 볼 수 있습니다. 자세한 내용은 56-17페이지의 Security Intelligence 섹션 이해을/를 참조하십시오.

참고 개별 연결 또는 보안 인텔리전스 이벤트에 대해 사용 가능한 정보는 라이센스 및 어플라이언스 모델을 비롯한 여러 요소에 따라 달라집니다. 자세한 내용은 38-9페이지의 연결 로깅의 라이센스 및 모델 요구 사항을/를 참조하십시오.

각 테이블 보기 또는 그래프에는 사용자가 보는 연결 또는 연결 요약에 대한 정보(타임스탬프, IP 주소, 애플리케이션 등)가 포함됩니다. FireSIGHT 시스템에서 탐지된 개별 연결에 제공되는 정보는 탐지 방법 및 로깅 옵션을 비롯한 여러 요인에 따라 달라집니다. 자세한 내용은 39-4페이지의 연결 및 보안 인텔리전스 데이터 필드 이해 및 39-11페이지의 연결 및 보안 인텔리전스 이벤트에서 제공되는 정보을/를 참조하십시오.

팁 Connection Summary 대시보드에서는 시스템이 로깅한 연결을 한눈에 볼 수 있는 보기를 제공하며, Summary Dashboard에는 보안 인텔리전스 이벤트 데이터가 표시됩니다. 자세한 내용은 55-1페이지의 대시보드 사용을/를 참조하십시오.

연결 또는 보안 인텔리전스 데이터를 보려면

액세스: Admin/Any Security Analyst

1단계 다음 2가지 옵션을 사용할 수 있습니다.

- 연결 이벤트를 보려면 **Analysis > Connections > Events**를 선택합니다.
- 보안 인텔리전스 이벤트를 보려면 **Analysis > Connections > Security Intelligence Events**를 선택합니다.

기본 연결 또는 보안 인텔리전스 워크플로의 첫 번째 페이지가 표시됩니다. 연결 이벤트의 경우, 두 가지 가능성이 있습니다.

- 워크플로 페이지에 **그래프**가 표시됩니다. 수행할 수 있는 작업에 대한 내용을 보려면 39-16페이지의 연결 그래프 작업을/를 참조하십시오.
- 워크플로 페이지에 **테이블**이 표시됩니다. 수행할 수 있는 작업에 대한 내용을 보려면 39-28페이지의 연결 및 보안 인텔리전스 데이터 테이블 작업을/를 참조하십시오.

보안 인텔리전스 이벤트의 경우, 워크플로 페이지에 **테이블**이 표시됩니다.

사용자 지정 워크플로를 비롯한 다른 워크플로를 사용하려면 워크플로 제목 옆의 **(switch workflow)**를 클릭합니다. 다른 기본 워크플로 지정에 대한 자세한 내용은 71-3페이지의 이벤트 보기 설정 구성을/를 참조하십시오. 이벤트가 표시되지 않을 경우 시간 범위를 조정해야 할 수 있습니다. 58-22페이지의 이벤트 시간 제약 조건 설정을/를 참조하십시오.

연결 그래프 작업

라이센스: 모든

시스템에서 연결 데이터를 표시할 수 있는 방법 중 한 가지는 그래픽으로 표시하는 것입니다. 선 그래프, 막대 그래프, 원 그래프로 구성된 세 가지 다른 유형의 연결 그래프가 제공됩니다. 막대 그래프와 선 그래프는 여러 데이터세트를 표시할 수 있습니다. 즉, 각 x축 데이터 포인트의 y축에 여러 값을 표시할 수 있습니다.

다음과 같은 다양한 방법으로 연결 그래프를 조작할 수 있습니다.

- 그래프를 표시하는 데이터 유형 변경
- 그래프 유형 전환
- 그래프를 제한하여 특정 시간 범위, 호스트, 애플리케이션, 포트, 디바이스에 대한 데이터 표시

트래픽 프로필은 연결 데이터에 기반하므로(53-1페이지의 트래픽 프로필 생성 참조), 트래픽 프로필을 선 그래프로 볼 수 있습니다. 몇 가지 제한 사항을 추가하여, 이러한 그래프를 다른 연결 그래프와 동일한 방식으로 조작할 수 있습니다.

보안 인텔리전스 이벤트의 연결 이벤트 데이터는 그래프 형식으로 볼 수 있으나, 보안 인텔리전스 이벤트에서 데이터 그래프를 생성할 수는 없습니다. 보안 인텔리전스 데이터의 인터랙티브 그래픽 보기를 보려는 경우, Context Explorer의 Security Intelligence 섹션을 볼 수 있습니다. 자세한 내용은 56-17페이지의 Security Intelligence 섹션 이해을/를 참조하십시오.

참고 트래픽 프로필을 보려면 관리자 액세스 권한이 있어야 합니다. 이를 보안 전문가 또는 관리자 액세스 권한으로 볼 수 있는 다른 연결 그래프와 비교합니다.

39-14페이지의 연결 및 보안 인텔리전스 데이터 보기에 설명된 대로 연결 그래프를 볼 경우, 다음 표에 설명된 기본 작업을 수행할 수 있습니다.

액세스: Admin/Any Security Analyst

표 39-2 기본 연결 그래프 기능

목적	가능한 작업
표시되는 데이터 자세히 살펴보기	39-4페이지의 연결 및 보안 인텔리전스 데이터 필드 이해에서 자세히 알아보십시오.
시간 및 날짜 범위 수정	58-22페이지의 이벤트 시간 제약 조건 설정에서 자세히 알아보십시오.
호스트의 프로필 보기	개시자 또는 응답자를 기준으로 연결 데이터가 표시되는 그래프에서, 막대 그래프의 막대 또는 원 그래프의 쐐기 모양을 클릭하고 **View Host Profile**을 선택합니다.
사용자 지정 워크플로를 비롯한 다른 워크플로 사용	워크플로 제목 옆에 있는 **(switch workflow)**를 클릭합니다.
현재 워크플로에서 여러 페이지 이동	58-18페이지의 워크플로 페이지 사용에서 자세히 알아보십시오.
관련 이벤트를 보기 위해 다른 이벤트 보기로 이동	58-35페이지의 워크플로 간 이동에서 자세히 알아보십시오.

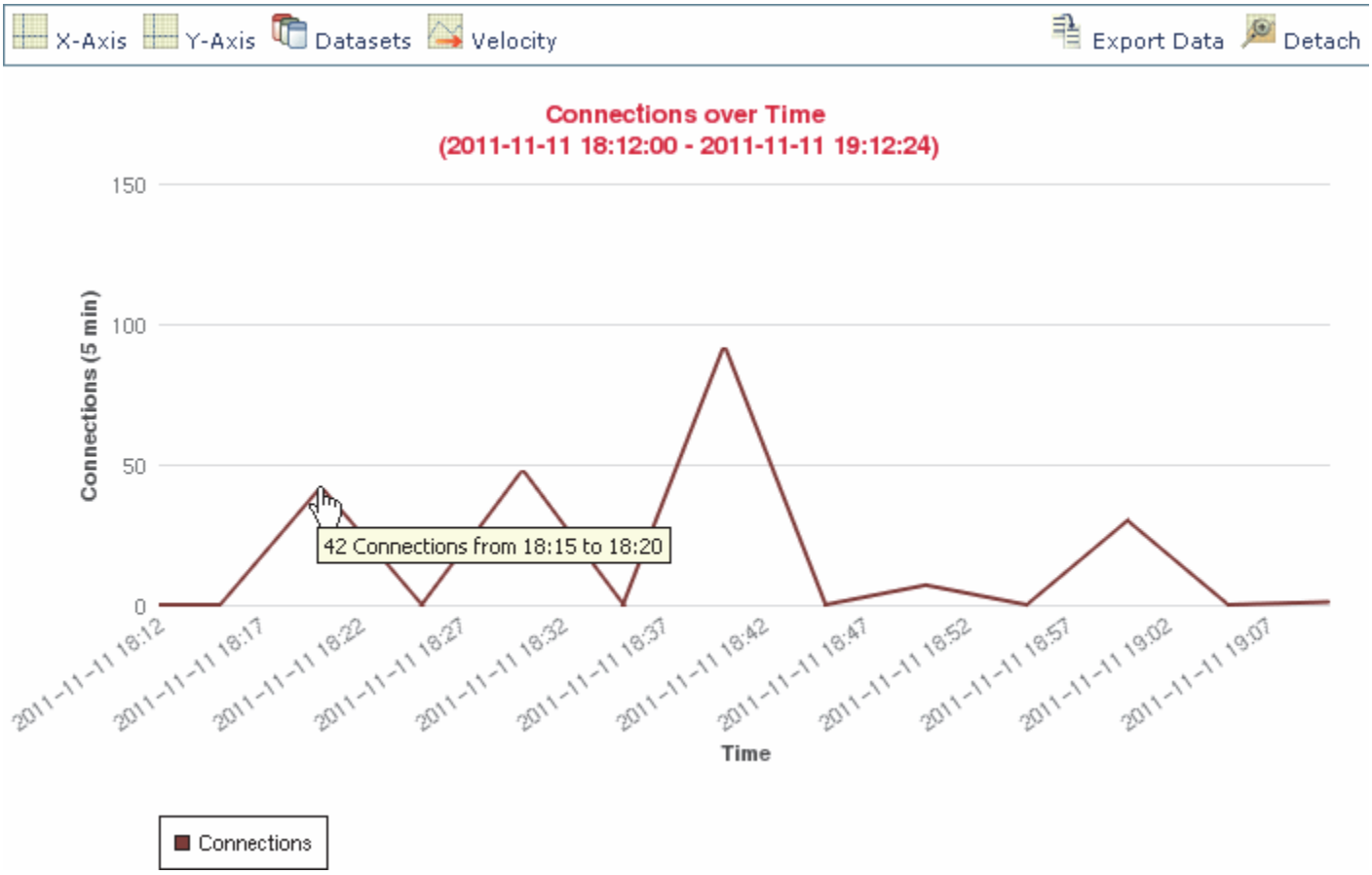
연결 데이터의 심층 분석을 수행할 경우 여러 가지 다른 방법으로 연결 그래프를 조작할 수 있습니다. 자세한 내용은 다음 링크를 참고하십시오.

- 39-18페이지의 그래프 유형 변경에서는 막대 그래프와 원 그래프 간에 전환하고, 표준 선 그래프와 속도 그래프 간에 전환하는 방법을 설명합니다.
- 39-21페이지의 데이터세트 선택에서는 선 그래프 및 막대 그래프에서 각 x축 데이터 포인트의 y축에 여러 값을 표시하는 방법을 설명합니다.
- 39-23페이지의 취합된 연결 데이터에 대한 정보 보기에서는 그래프의 데이터 포인트에 대한 추가 정보를 살펴보거나, 통계가 그래프로 작성되는 호스트의 호스트 프로필을 표시하는 방법을 설명합니다.
- 39-24페이지의 워크플로 페이지에서 연결 그래프 조작에서는 워크플로를 다음 페이지로 이동하지 않고 연결 그래프에 표시되는 데이터를 제한하는 방법을 설명합니다.
- 39-24페이지의 연결 데이터 그래프를 통해 드릴다운에서는 워크플로를 다음 페이지로 이동하는 동안 연결 그래프에 표시되는 데이터를 제한하는 방법을 설명합니다.
- 39-25페이지의 선 그래프 중심 재조정 및 확대/축소에서는 모든 시간 범위에 맞춰 선 그래프의 중심을 재조정하는 방법을 설명합니다.
- 39-25페이지의 그래프에 데이터 선택에서는 x축 또는 y축을 변경하여 연결 그래프에 표시된 데이터를 변경하는 방법을 설명합니다.
- 39-27페이지의 연결 그래프 분리에서는 연결 그래프를 새 브라우저 창에 분리하고, 방어 센터의 기본 시간 범위에 영향을 미치지 않으면서 추가 분석을 수행할 수 있는 방법을 설명합니다.
- 39-27페이지의 연결 데이터 내보내기에서는 그래프를 CSV(쉼표로 구분된 값) 파일로 구성하는 데 사용된 연결 데이터를 내보내는 방법을 설명합니다.

그래프 유형 변경

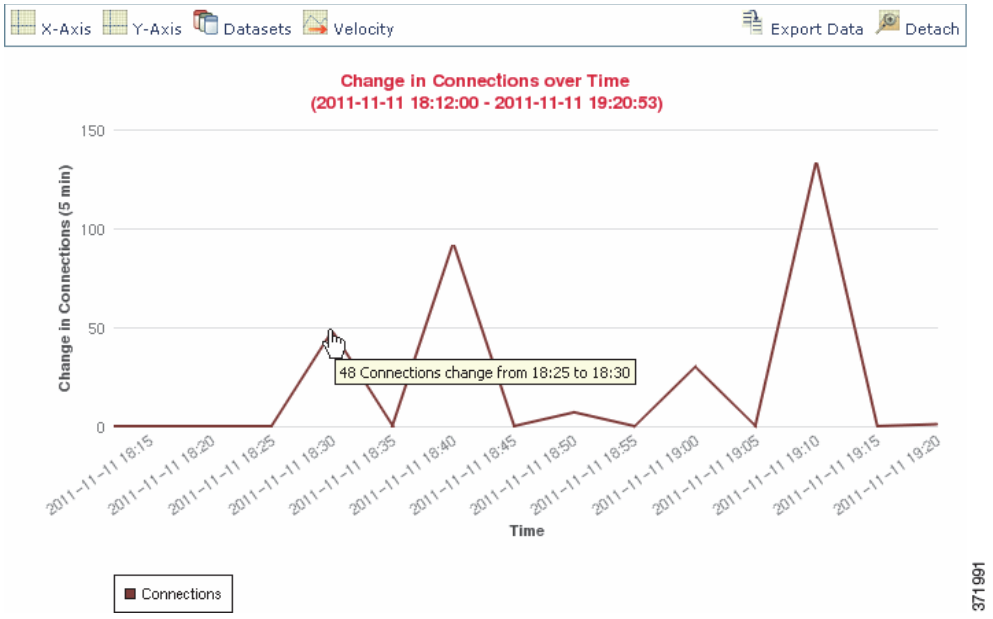
라이센스: 모든

선 그래프, 막대 그래프, 원 그래프로 구성된 세 가지 다른 유형의 연결 그래프가 제공됩니다. *선 그래프*는 데이터를 시간의 추이에 따라 선으로 나타냅니다. 예를 들어, 아래 선 그래프에는 1시간 동안 모니터링된 네트워크에서 탐지된 총 연결 수가 표시되어 있습니다. 트래픽 프로필은 항상 선 그래프로 표시됩니다.

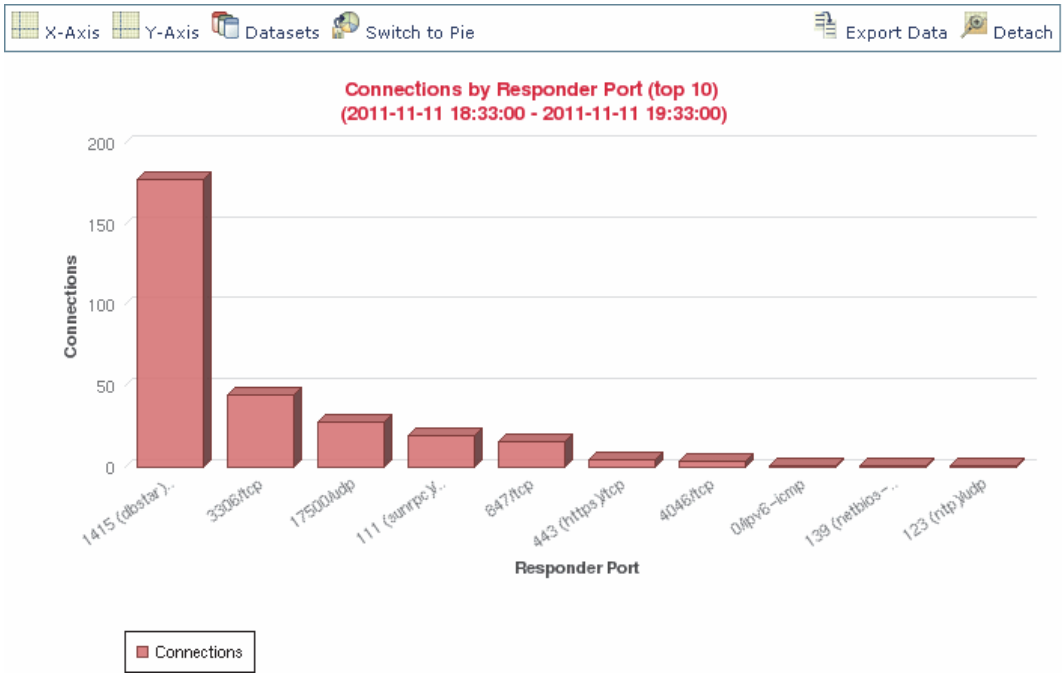


기본적으로 선 그래프는 *표준 보기*로 표시됩니다. 표준 선 그래프는 5분 간격을 통해 데이터를 취합하고, 취합된 데이터 포인트를 선으로 나타내고, 포인트를 연결합니다.

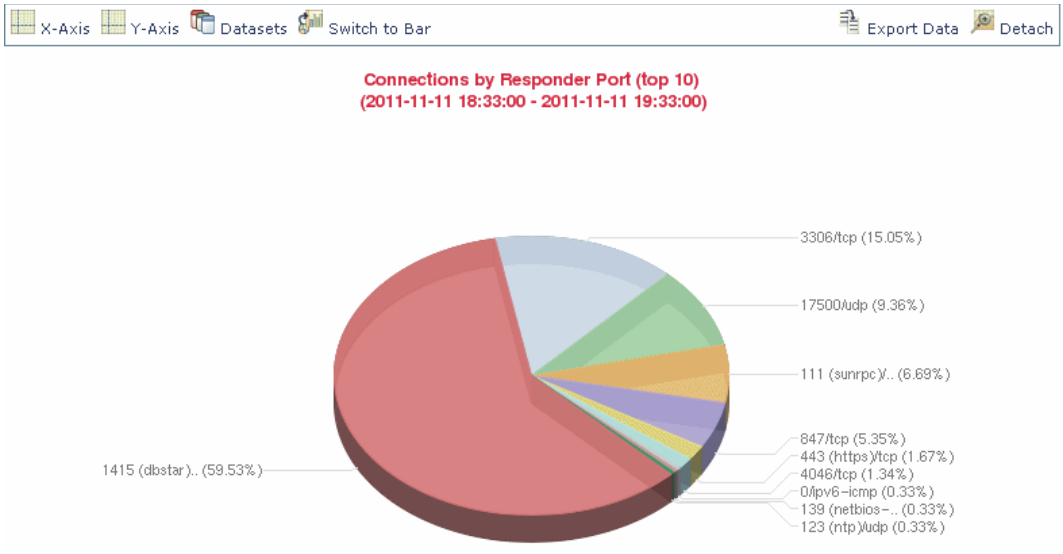
그러나 선 그래프를 표준 보기에서 *속도 보기*로 전환할 수 있습니다. 속도 선 그래프에서는 이러한 데이터 포인트의 변동률을 보여줍니다. 위 그래프를 속도 그래프로 전환할 경우, 연결 수를 나타내던 y축은 시간의 추이에 따른 연결 수의 변화를 나타내게 됩니다.



*막대 그래프*에는 데이터가 별도의 카테고리로 그룹화되어 표시됩니다. 예를 들어, 막대 그래프에는 1시간 동안 가장 활성화된 포트 10개에 대해 모니터링된 네트워크에서 탐지된 연결 수가 표시될 수 있습니다.



*원 그래프*는 막대 그래프와 마찬가지로, 별도의 카테고리로 그룹화된 데이터가 표시됩니다. 다음 원 그래프에는 위의 막대 그래프와 동일한 정보가 표시되어 있습니다.



표준 선 그래프를 속도 선 그래프로 전환하거나, 막대 그래프를 원 그래프로 전환할 경우 다음 표의 지침을 따르십시오.

액세스: Admin/Any Security Analyst

표 39-3 그래프 유형 전환

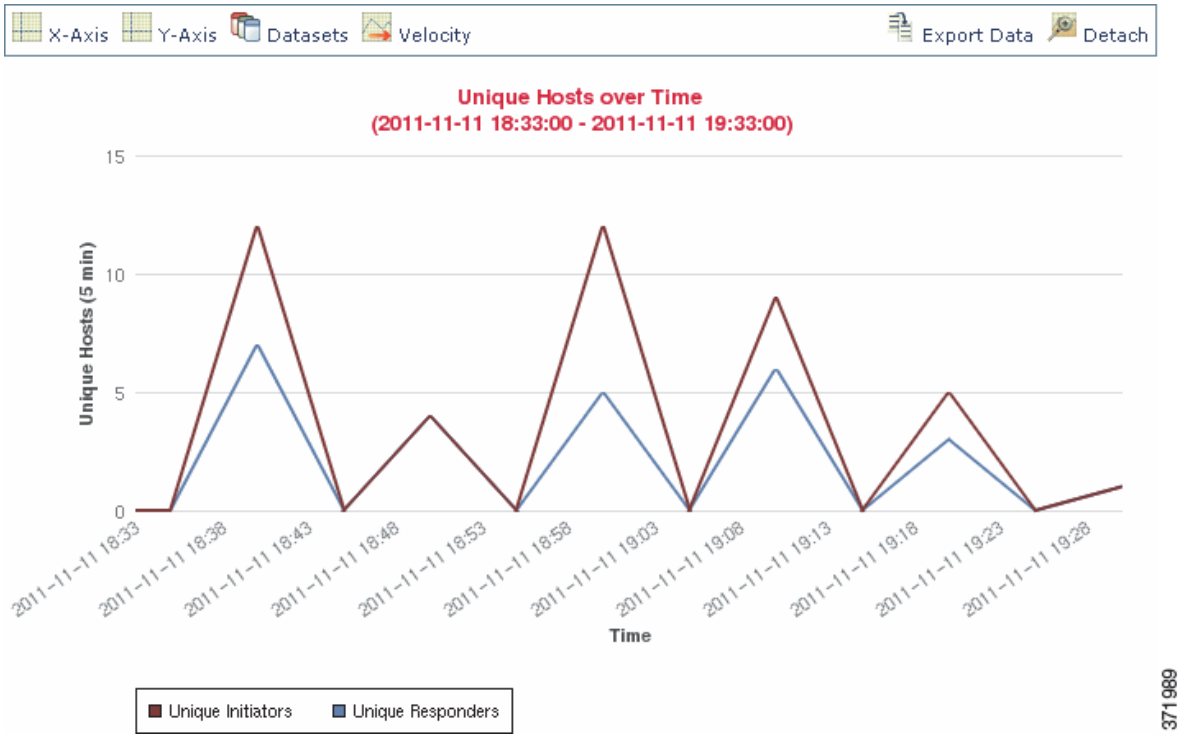
전환할 작업	가능한 작업
막대 그래프에서 원 그래프로	**Switch to Pie**를 클릭합니다. 원 그래프는 여러 데이터세트를 표시할 수 없습니다(39-21 페이지의 데이터세트 선택 참조).
원 그래프를 막대 그래프로	**Switch to Bar**를 클릭합니다.
표준 그래프의 선 그래프를 속도 그래프로	**Velocity**를 클릭하고 **Velocity**를 선택합니다.
속도 그래프의 선 그래프에서 표준 그래프로	**Velocity**를 클릭하고 **Standard**를 선택합니다.

데이터세트 선택

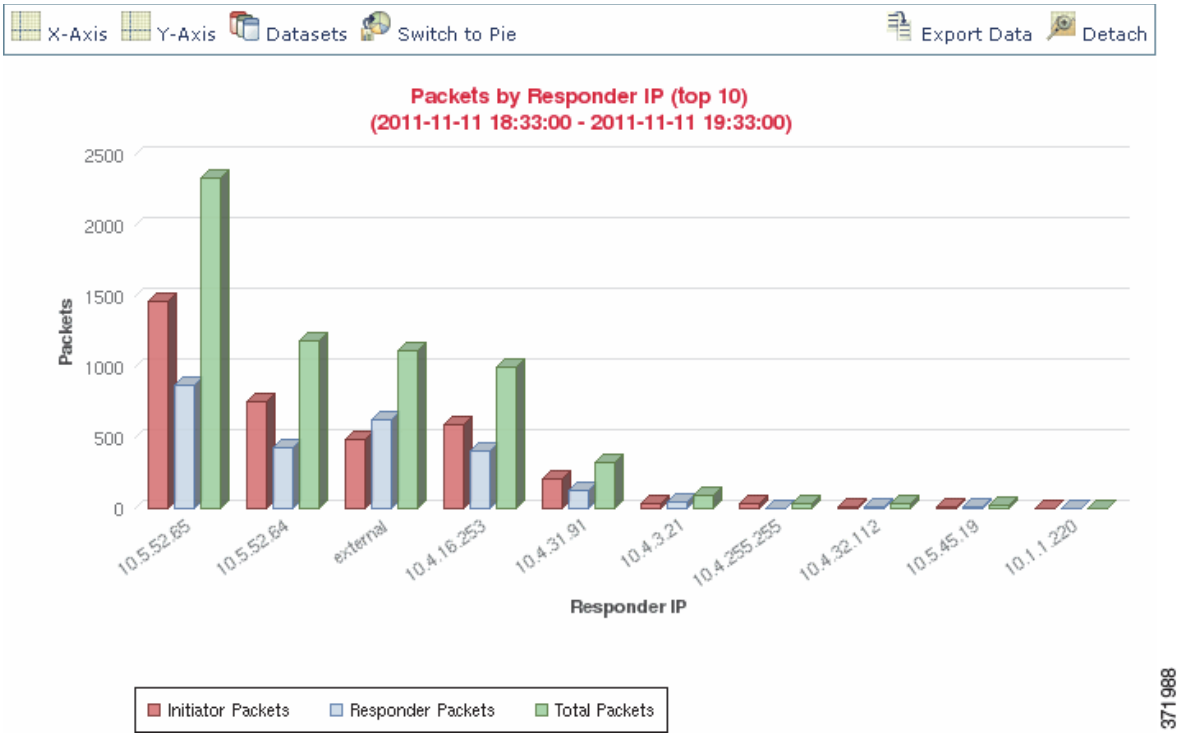
라이센스: 모든

막대 그래프와 선 그래프는 모두 여러 데이터세트를 표시할 수 있습니다. 즉, 각 x축 데이터 포인트의 y축에 여러 값을 표시할 수 있습니다. 예를 들어, 고유한 개시자의 총수를 표시할 수 있으며 고유한 원 그래프의 총수는 하나의 데이터세트만 표시할 수 있습니다.

선 그래프에서 여러 데이터세트는 각기 다른 색상의 여러 선으로 표시됩니다. 예를 들어, 다음 그래픽에는 1시간 간격 동안 모니터링된 네트워크에서 탐지된 고유한 개시자의 총수 및 고유한 응답자의 총수가 표시됩니다.



막대 그래프에서 여러 데이터세트는 각 x축 데이터 포인트의 색상 막대로 표시됩니다. 예를 들어, 다음 막대 그래프에는 모니터링된 네트워크에서 전송된 총 패킷, 개시자가 전송한 패킷, 응답자가 전송한 패킷이 표시됩니다.



원 그래프에서는 여러 데이터세트를 표시할 수 **없습니다**. 여러 데이터세트가 있는 막대 그래프에서 원 그래프로 전환할 경우, 원 그래프에는 자동으로 선택된 하나의 데이터세트만 표시됩니다. 표시할 데이터세트를 선택할 경우, 방어 센터는 개시자 및 응답자 통계보다 전체 통계를 우선시하고, 응답자 통계보다는 개시자 통계를 우선시합니다. 다음 표에는 연결 그래프의 x축에 표시할 수 있는 데이터세트가 설명되어 있습니다.

표 39-4 데이터세트 옵션

y축에 표시되는 내용	선택 가능한 데이터세트
연결	기본값 전용 - 모니터링되는 네트워크에서 탐지된 연결의 수(**Connections**) 이는 트래픽 프로필 그래프의 유일한 옵션입니다.
KB	다음을 조합하여 선택 • 모니터링되는 네트워크에서 전송된 총 킬로바이트(**Total KBytes**) • 모니터링되는 네트워크의 호스트 IP 주소에서 전송한 킬로바이트 수(**Initiator KBytes**) • 모니터링되는 네트워크의 호스트 IP 주소가 수신한 킬로바이트 수(**Responder KBytes**)
초당 KB	기본값 전용 - 모니터링되는 네트워크에서 전송된 초당 총 킬로바이트(**Total KBytes Per Second**)

표 39-4 데이터세트 옵션(계속)

y축에 표시되는 내용	선택 가능한 데이터세트
패킷	다음을 조합하여 선택 • 모니터링되는 네트워크에서 전송된 총 패킷(**Total Packets**) • 모니터링되는 네트워크의 호스트 IP 주소에서 전송한 패킷 수(**Initiator Packets**) • 모니터링되는 네트워크의 호스트 IP 주소가 수신한 패킷 수(**Responder Packets**)
고유한 호스트	다음을 조합하여 선택 • 모니터링되는 네트워크의 고유한 세션 개시자 수(**Unique Initiators**) • 모니터링되는 네트워크의 고유한 세션 응답자 수(**Unique Responders**)
고유한 애플리케이션 프로토콜	기본값 전용 - 모니터링되는 네트워크의 고유한 애플리케이션 프로토콜 수(**Unique Application Protocols**)
고유한 사용자	기본값 전용 - 모니터링되는 네트워크의 세션 개시자에 로깅된 고유한 사용자 수(**Unique Initiator Users**)

연결 그래프에 표시되는 데이터세트를 선택하려면

액세스: Admin/Any Security Analyst

1단계 **Datasets**를 클릭하고 그래프로 작성할 데이터세트를 선택합니다.

선택 가능한 데이터세트는 데이터세트 옵션 표에 설명되어 있습니다.

취합된 연결 데이터에 대한 정보 보기

라이센스: 모든

연결 그래프는 5분 간격 동안 취합된 데이터를 기준으로 하며, *연결 요약*이라고도 합니다. 연결 그래프를 구성하는 데 사용된 특정 연결 요약에 대한 추가 정보를 살펴볼 수 있습니다. 예를 들어, 시간의 추이에 따른 연결 그래프에서 특정 기간 동안 탐지된 연결이 정확히 몇 개인지 확인하고자 할 수 있습니다.

취합된 연결 데이터에 대한 세부 정보를 살펴보려면

액세스: Admin/Any Security Analyst

1단계 선 그래프의 포인트, 막대 그래프의 막대, 원 그래프의 쐐기 모양에 마우스 커서를 올려놓습니다. 그래프의 해당 부분을 구성하는 데 사용된 데이터에 대한 세부 정보가 포함된 툴팁이 표시됩니다.

워크플로 페이지에서 연결 그래프 조작

라이센스: 모든

연결 데이터 워크플로를 열 경우, 데이터는 처음에 시간 범위로만 제한됩니다. 워크플로를 다음 페이지로 이동하지 않고 추가 기준으로 연결 그래프를 제한할 수 있습니다.

팁 이러한 방식으로 연결 데이터를 제한하면 그래프의 x축(원 그래프를 볼 경우에는 독립 변수라고도 함)이 변경됩니다. 연결 데이터를 제한하지 않고 독립 변수를 변경하려면, **X-Axis** 및 **Y-Axis** 메뉴를 사용합니다. 자세한 내용은 39-25페이지의 그래프에 데이터 선택을/를 참조하십시오.

연결 데이터를 제한하려면

액세스: Admin/Any Security Analyst

1단계 선 그래프의 포인트, 막대 그래프의 막대, 원 그래프의 쐐기 모양을 클릭합니다.

2단계 **View by...** 옵션을 선택합니다.

X축 기능 표에 나열된 기준에 따라 연결 데이터를 제한할 수 있습니다.

예를 들어, 시간의 추이에 따른 연결 그래프를 생각해보십시오. 포트에 따라 그래프의 포인트를 제한할 경우, 탐지된 연결 이벤트 수를 기준으로 가장 활성화된 포트 10개가 제시되지만, 사용자가 클릭한 포인트를 중심으로 한 10분 간격으로 제한된 막대 그래프가 표시됩니다.

막대 중 하나를 클릭하고 **View by Initiator IP**를 선택하여 그래프를 추가로 제한할 경우, 이전과 동일한 10분 간격뿐만 아니라 클릭한 막대에 따라 표시되는 포트를 기준으로 제한된 새로운 막대 그래프가 표시됩니다.

참고 분리된 그래프로 작업하지 않는 한, 이러한 방식으로 연결 데이터를 구속하면 시간 범위가 변경됩니다. 분리된 그래프에 대한 자세한 내용은 39-27페이지의 연결 그래프 분리을/를 참조하십시오.

연결 데이터 그래프를 통해 드릴다운

라이센스: 모든

연결 데이터 워크플로를 열 경우, 데이터는 처음에 시간 범위로만 제한됩니다. 워크플로를 다음 페이지로 이동하는 동안 연결 그래프를 제한할 수 있습니다.

연결 데이터 워크플로를 드릴다운하려면

액세스: Admin/Any Security Analyst

1단계 선 그래프의 포인트, 막대 그래프의 막대, 원 그래프의 쐐기 모양을 클릭합니다.

2단계 **Drill-down**을 선택합니다.

다음 워크플로 페이지로 드릴다운하여, 클릭한 항목의 사용을 제한합니다.

- 선 그래프의 포인트를 클릭하면 이 클릭한 포인트를 중심으로, 다음 페이지의 시간 범위가 10분 간격으로 제한됩니다.

- 막대 그래프의 막대를 클릭하거나 원 그래프의 쐐기 모양을 클릭하면 막대 또는 쐐기 모양에 따라 표시된 기준에 의해 다음 페이지가 제한됩니다. 예를 들어, 포트 사용을 나타내는 막대를 클릭하면 워크플로의 다음 페이지로 드릴다운되며, 이는 사용자가 클릭한 막대에 따라 표시된 포트를 기준으로 제한됩니다.

선 그래프 중심 재조정 및 확대/축소

라이센스: 모든

모든 시간 범위에 맞춰 선 그래프의 중심을 재조정할 수 있습니다. 기본 시간 범위를 사용하여 중심을 재조정하거나, 다른 시간 범위를 선택할 수 있습니다.

참고 분리된 그래프로 작업하지 않는 한, 중심을 재조정하면 기본 시간 범위가 변경됩니다. 분리된 그래프에 대한 자세한 내용은 39-27페이지의 연결 그래프 분리을/를 참조하십시오.

기본 시간 범위를 사용하여 중심을 재조정하려면

액세스: Admin/Any Security Analyst

1단계 그래프의 중심을 재조정할 선 그래프의 포인트를 클릭하고, **recenter**를 클릭합니다.

그래프가 다시 작성되고, 클릭한 포인트가 중심이 되며, 기본 시간 범위와 길이가 동일한 시간 간격이 적용됩니다.

다른 시간 범위를 사용하여 중심을 재조정하려면

액세스: Admin/Any Security Analyst

1단계 그래프의 중심을 재조정할 포인트를 클릭하고 **Zoom**을 클릭합니다.

2단계 새 그래프의 시간 간격을 선택하며, 이 기간은 한 시간 또는 일주일처럼 짧거나 길 수 있습니다.

그래프가 다시 작성되고, 클릭한 포인트가 중심이 되며, 선택한 시간 간격이 적용됩니다.

그래프에 데이터 선택

라이센스: 모든

x축, y축 또는 두 축을 모두 변경하여 연결 그래프에 다른 데이터를 표시할 수 있습니다.

원 그래프의 경우, x축을 변경하면 독립 변수가 변경되고 y축을 변경하면 종속 변수가 변경됩니다. 일례로, 포트당 킬로바이트 단위로 그래프를 작성하는 원 그래프를 가정해보십시오. 이 경우 x축은 **Responder Port**이고 y축은 **KBytes**입니다. 이러한 원 그래프는 특정 간격 동안 모니터링되는 네트워크를 통해 전송된 데이터의 총 킬로바이트를 나타냅니다. 원형의 쐐기 모양은 각 포트에서 탐지된 데이터의 비율을 나타냅니다. **Application Protocol**에 대한 차트의 x축을 변경할 경우 원 그래프에는 전송된 총 킬로바이트가 계속 표시되지만, 원형의 쐐기 모양은 각 탐지된 애플리케이션 프로토콜에 전송된 데이터의 비율을 나타냅니다.

그러나 첫 번째 원 그래프의 y축을 **Packets**로 변경할 경우 원 그래프는 특정 간격 동안 모니터링되는 네트워크를 통해 전송된 총 패킷 수를 나타내며, 원형의 쐐기 모양은 각 포트에서 탐지된 총 패킷 수의 비율을 나타냅니다.

연결 그래프의 x축을 변경하려면 다음 표의 지침을 따르십시오.

표 39-5 X축 기능

그래프로 표시할 연결 데이터	가능한 작업
탐지된 연결 이벤트 수를 기준으로 모니터링되는 네트워크에서 가장 활성화된 애플리케이션 프로토콜 10개	**X-Axis**를 클릭하고 **Application Protocol**을 선택합니다.
탐지된 연결 이벤트 수를 기준으로 모니터링되는 네트워크에서 가장 활성화된 매니지드 디바이스 10개	**X-Axis**를 클릭하고 **Device**를 선택합니다.
호스트 IP 주소가 연결 트랜잭션을 시작한 연결 이벤트 수를 기준으로 모니터링되는 네트워크에서 가장 활성화된 호스트 IP 주소 10개	**X-Axis**를 클릭하고 **Initiator IP**를 선택합니다.
시작된 연결 트랜잭션에 사용자가 로깅한 호스트가 있는 연결 이벤트 수를 기준으로 모니터링되는 네트워크에서 가장 활성화된 사용자 10명	**X-Axis**를 클릭하고 **Initiator User**를 선택합니다.
연결 트랜잭션의 주소가 응답자인 연결 이벤트 수를 기준으로 모니터링되는 네트워크에서 가장 활성화된 호스트 IP 주소 10개	**X-Axis**를 클릭하고 **Responder IP**를 선택합니다.
연결 트랜잭션의 호스트가 응답자인 연결 이벤트 수를 기준으로 모니터링되는 네트워크에서 가장 활성화된 포트 IP 주소 10개	**X-Axis**를 클릭하고 **Responder Port**를 선택합니다.
가장 활성화된 소스 디바이스 10개(연결에 대한 연결 데이터를 내보낸 NetFlow 지원 디바이스, Cisco 매니지드 디바이스에서 탐지된 모든 연결의 명명된 소스 디바이스 FireSIGHT 포함)	**X-Axis**를 클릭하고 **Source Device**를 선택합니다.
시간의 추이	**X-Axis**를 클릭하고 **Time**을 선택합니다.

연결 그래프의 y축을 변경하려면 다음 표의 지침을 따르십시오.

표 39-6 Y-Axis 기능

목적	가능한 작업
x축에 선택한 기준에 따라 모니터링되는 네트워크의 연결 수를 그래프로 작성	**Y-Axis**를 클릭하고 **Connections**를 선택합니다.
x축에 선택한 기준에 따라 모니터링되는 네트워크에서 전송된 총 킬로바이트를 그래프로 작성	**Y-Axis**를 클릭하고 **KBytes**를 선택합니다.
x축에 선택한 기준에 따라 모니터링되는 네트워크에서 전송된 초당 총 킬로바이트를 그래프로 작성	**Y-Axis**를 클릭하고 **KBytes Per Second**를 선택합니다.
x축에 선택한 기준에 따라 모니터링되는 네트워크에서 전송된 총 패킷 수를 그래프로 작성	**Y-Axis**를 클릭하고 **Packets**를 선택합니다.
x축에 선택한 기준에 따라 모니터링되는 네트워크에서 전송된 고유한 호스트의 총 개수를 그래프로 작성	**Y-Axis**를 클릭하고 **Unique Hosts**를 선택합니다.

표 39-6 Y-Axis 기능(계속)

목적	가능한 작업
x축에 선택한 기준에 따라 모니터링되는 네트워크에서 탐지된 고유한 애플리케이션 프로토콜의 총 개수를 그래프로 작성	**Y-Axis**를 클릭하고 **Unique Application Protocols**를 선택합니다.
x축에 선택한 기준에 따라 모니터링되는 네트워크에서 탐지된 고유한 사용자의 총수를 그래프로 작성	**Y-Axis**를 클릭하고 **Unique Users**를 선택합니다.

연결 그래프 분리

라이센스: 모든

기본 시간 범위에 영향을 미치지 않고 연결 그래프에 추가 분석을 수행하려는 경우, 그래프를 새 브라우저 창으로 분리하면 됩니다. 내장된 연결 그래프에서 수행할 수 있는 작업은 분리된 연결 그래프에서도 모두 동일하게 수행할 수 있습니다. **Print**를 클릭하면 분리된 그래프를 인쇄할 수도 있습니다. 트래픽 프로필 그래프는 기본적으로 분리된 그래프입니다.

팁 분리된 그래프를 볼 경우, **New Window**를 클릭하면 분리된 그래프의 다른 복사본을 새 브라우저 창에 생성할 수 있습니다. 그런 다음 각각의 분리된 그래프에 서로 다른 분석을 수행할 수 있습니다.

그래프를 분리하려면

액세스: Admin/Any Security Analyst

1단계 **Detach**를 클릭합니다.

연결 데이터 내보내기

라이센스: 모든

연결 데이터를 CSV(쉼표로 구분된 값) 파일로 내보내 다른 사용자와 이를 쉽게 공유할 수 있습니다.

팁 또한 마우스 오른쪽 버튼으로 그래프를 클릭하고 브라우저의 프롬프트에 따라 연결 그래프를 이미지로 저장할 수도 있습니다.

연결 데이터를 내보내려면

액세스: Admin/Any Security Analyst

1단계 **Export Data**를 클릭합니다.

그래프의 데이터가 테이블 보기로 표시되는 팝업 창이 나타납니다.

2단계 **Download CSV File**을 클릭하고 파일을 저장합니다.

연결 및 보안 인텔리전스 데이터 테이블 작업

라이센스: 기능에 따라 다름

지원되는 디바이스: 기능에 따라 다름

지원되는 Defense Center: 기능에 따라 다름

FireSIGHT 시스템의 이벤트 뷰어를 사용하면 연결 데이터를 테이블로 볼 수 있을 뿐만 아니라, 분석과 관련된 정보에 따라 이벤트 뷰를 조작할 수도 있습니다. 보안 인텔리전스 보기 이벤트를 사용하면 확인된 보안 인텔리전스 평판을 통해 연결을 중점적으로 살펴볼 수 있습니다. (보안 인텔리전스는 보호 라이센스가 필요하며 Series 2 매니지드 디바이스 또는 DC500 방어 센터에서 지원되지 않습니다.) 연결 데이터에 액세스할 때 표시되는 페이지는 워크플로에 따라 달라지며, 이는 광범위한 보기를 보다 중점적인 보기로 전환하여 이벤트를 평가할 수 있는 페이지입니다.

참고 개별 연결 또는 보안 인텔리전스 이벤트에 대해 사용 가능한 정보는 라이센스 및 어플라이언스 모델을 비롯한 여러 요소에 따라 달라집니다. 자세한 내용은 38-9페이지의 연결 로깅의 라이센스 및 모델 요구 사항을/를 참조하십시오.

시스템에서 제공된 *Connection Events* 및 *Security Intelligence Events* 워크플로는 기본 연결 및 탐지된 애플리케이션 정보에 대한 요약 보기를 제공하며, 이를 사용하여 이벤트의 테이블 보기로 드릴다운할 수 있습니다. 또한 특정 요구 사항에 매칭되는 정보만 표시하는 사용자 지정 워크플로를 생성할 수도 있습니다.

이벤트 뷰어를 사용할 경우 다음을 수행할 수 있습니다.

- 이벤트 검색, 정렬 및 제한은 물론 표시된 이벤트에 대한 시간 범위를 변경할 수 있습니다.
- 나타나는 열을 지정할 수 있습니다(테이블 보기 전용).
- IP 주소와 연결된 호스트 프로필을 보거나, 사용자 ID와 연결된 사용자 세부사항 및 호스트 기록을 볼 수 있습니다.
- 연결에서 탐지된 파일(악성코드 파일 포함) 및 침입 보기
- IP 주소와 연결된 위치 정보 보기
- 연결 이벤트의 URL 전체 텍스트 보기
- 세션을 암호화하는 데 사용된 인증서에 대한 정보 보기
- 암호화된 세션 세부 정보 보기
- 동일한 워크플로 내에서 서로 다른 워크플로 페이지를 사용하여 이벤트를 볼 수 있습니다.
- 다른 워크플로를 사용하는 여러 이벤트를 함께 볼 수 있습니다.
- 특정 값으로 제한하여 워크플로 내에서 페이지 간에 드릴다운할 수 있습니다.
- 나중에 동일한 데이터(데이터가 그대로 있을 경우)로 돌아올 수 있도록 현재 페이지 및 제약 조건을 북마크 처리할 수 있습니다.
- 현재 제약 조건을 사용하여 보고서 템플릿을 생성할 수 있습니다.
- 데이터베이스에서 이벤트를 삭제할 수 있습니다.
- IP 주소 컨텍스트 메뉴를 사용하여 파일 이벤트와 연결된 호스트 또는 IP 주소의 추가 정보를 얻거나, 화이트리스트 또는 블랙리스트 작성

드릴다운 페이지에서 연결 이벤트를 제한할 경우, 동일한 이벤트의 패킷 및 바이트가 합산됩니다. 그러나 사용자 지정 워크플로를 사용하고 **Count** 열을 드릴다운 페이지에 추가하지 않은 경우, 이벤트가 개별적으로 나열되고 패킷과 바이트는 합산되지 않습니다.

다음 섹션에는 연결 및 보안 인텔리전스 이벤트 테이블을 보고 분석하는 방법에 대한 정보가 포함되어 있습니다.

- 58-1페이지의 워크플로의 이해 및 사용에서는 이벤트 뷰어 사용에 대한 자세한 지침을 제공합니다.
- 58-20페이지의 지오로케이션 사용에서는 연결 및 보안 인텔리전스 이벤트와 연결된 위치 정보를 보고 해석하는 방법에 대한 정보를 제공합니다.
- 71-3페이지의 이벤트 보기 설정 구성에서는 연결 및 보안 인텔리전스 이벤트 데이터를 볼 수 있는 기본 워크플로를 변경하는 방법을 설명합니다.
- 39-4페이지의 연결 및 보안 인텔리전스 데이터 필드 이해 및 39-11페이지의 연결 및 보안 인텔리전스 이벤트에서 제공되는 정보에서는 연결 및 보안 인텔리전스 이벤트의 데이터에 대한 세부 정보를 제공합니다.
- 39-29페이지의 Monitor 규칙과 연결된 이벤트 작업에서는 Monitor 규칙 기준을 사용하여 연결 이벤트를 제한하는 방법을 설명합니다.
- 39-30페이지의 연결에서 탐지된 파일 보기에서는 연결에서 탐지되거나 차단된 파일(악성코드 파일 포함)을 보는 방법을 설명합니다.
- 39-31페이지의 연결과 관련된 침입 이벤트 보기에서는 연결과 관련된 침입 이벤트를 보는 방법을 설명합니다.
- 39-32페이지의 암호화된 연결과 관련된 인증서 보기에서는 연결을 암호화하는 데 사용된 인증서에 대한 세부 정보를 보는 방법을 설명합니다.

Monitor 규칙과 연결된 이벤트 작업

라이센스: 모든

이벤트 뷰어를 사용하여 로깅된 연결을 볼 경우, 방어 센터에는 각 연결을 처리한 액세스 제어 규칙 또는 기본 작업, 그리고 해당 연결과 매칭된 최대 8개의 Monitor 규칙이 표시됩니다.

연결이 하나의 Monitor 규칙과 매칭될 경우, 방어 센터에는 연결을 처리한 규칙의 이름이 표시되며 그 뒤에 Monitor 규칙 이름이 표시됩니다. 연결이 여러 개의 Monitor 규칙과 매칭될 경우, 이벤트 뷰어에는 매칭되는 Monitor 규칙의 개수가 표시됩니다(예: `기본 작업 + Monitor 규칙 2개`)

다음 중 한 가지 방법을 사용하면, 매칭되는 Monitor 규칙을 사용하여 연결 이벤트 보기를 제한할 수 있습니다.

- 연결을 처리한 액세스 제어 규칙 또는 기본 작업
- 연결과 매칭된 개별 Monitor 규칙

Monitor 규칙 매칭을 사용하여 연결 이벤트를 제한하려면

액세스: Admin/Any Security Analyst

1단계 **Analysis > Connections > Events**를 선택합니다.

기본 연결 데이터 워크플로의 첫 번째 페이지가 표시됩니다.

2단계 분석에 사용할 워크플로를 표시합니다. 현재 사용 중인 드릴다운 페이지 또는 테이블 보기가 **Access Control Rule** 필드에 표시되는지 확인합니다.

3단계 이벤트를 어떤 방법으로 제한하시겠습니까?

- 연결을 처리한 액세스 제어 규칙 또는 기본 작업으로 제한하려면, 규칙 이름 또는 **Default Action**을 클릭합니다.
- 로깅된 연결을 매칭한 Monitor 규칙으로만 제한하려면 Monitor 규칙 이름을 클릭합니다.
- 로깅된 연결을 매칭한 여러 개의 Monitor 규칙 중 하나로 제한하려면 *N* **Monitor Rules** 값을 클릭합니다. 예를 들어, **2 Monitor Rules**를 클릭합니다.

  해당 연결 이벤트에 대한 Monitor Rules 팝업 창이 표시되며, 연결과 매칭되는 처음 8개의 Monitor 규칙이 나열됩니다. 연결 이벤트를 제한하는 데 사용할 Monitor 규칙 이름을 클릭합니다.

이벤트가 제한됩니다. 드릴다운 페이지를 사용 중일 경우, 이벤트 보기가 워크플로의 다음 페이지로 이동합니다.

연결에서 탐지된 파일 보기

라이센스: 보호 또는 악성코드

지원되는 디바이스: 기능에 따라 다름

지원되는 Defense Center: 기능에 따라 다름

파일 정책과 하나 이상의 액세스 제어 규칙을 연결할 경우, 시스템은 매칭 트래픽에서 파일(악성코드 포함)을 탐지할 수 있습니다. 이벤트 뷰어를 사용하면 해당 규칙에 의해 로깅된 연결과 관련된 파일 이벤트를 볼 수 있습니다.

파일 목록 대신, 방어 센터에서는 **Files** 필드에 파일 보기 아이콘( )을 표시합니다. 아이콘의 숫자는 해당 연결에서 탐지되거나 차단된 파일(악성코드 파일 포함)의 수를 나타냅니다. 이 아이콘을 클릭하면 다음 워크플로 페이지로 드릴다운하거나 연결 이벤트를 제한하지 않습니다. 그 대신 이 아이콘은 연결에서 탐지된 파일 목록은 물론, 해당 유형 및 악성코드 속성이 포함된 팝업 창을 표시합니다.

팝업 창에서 다음을 클릭할 수 있습니다.

- 파일 이벤트의 테이블 보기에 있는 세부 정보를 볼 수 있는 파일의 보기 아이콘( )
- 악성코드 이벤트의 테이블 보기에 있는 세부 정보를 볼 수 있는 악성코드 파일의 보기 아이콘( )
- 네트워크를 통한 파일의 전송을 추적할 수 있는 파일 전파 흔적 분석 아이콘( )
- **View File Events** 또는 **View Malware Events**에서는 연결의 모든 탐지된 파일 또는 네트워크 기반 악성코드 이벤트에 대한 세부 정보를 볼 수 있습니다.

팁 하나 이상의 연결과 관련된 파일 또는 악성코드 이벤트를 신속하게 보려면, 이벤트 뷰어의 확인란을 사용하여 연결을 선택한 다음 **Jump to** 드롭다운 목록에서 **Malware Events** 또는 **File Events**를 선택합니다. 파일을 전송하는 데 사용된 연결을 이와 비슷한 방법으로 볼 수 있습니다. 자세한 내용은 58-35페이지의 워크플로 간 이동을/를 참조하십시오.

연결된 이벤트를 볼 경우, 방어 센터에서는 해당 이벤트 유형에 대한 기본 워크플로를 사용합니다. 파일 및 악성코드 이벤트에 대한 자세한 내용은 40-8페이지의 파일 이벤트 작업 및 40-17페이지의 악성코드 이벤트 작업을/를 참조하십시오. 네트워크 파일 전파 흔적 분석 기능의 사용에 대한 자세한 내용은 40-36페이지의 네트워크 파일 전파 흔적 작업을/를 참조하십시오.

모든 파일 및 악성코드 이벤트는 다음과 같은 방식으로 연결과 관련됩니다.

- 엔드포인트 기반 악성코드 이벤트는 연결과 관련되지 않습니다. 이러한 이벤트는 네트워크 트래픽을 검사하는 시스템 대신 FireAMP Connector에 의해 생성됩니다.
- 많은 IMAP 지원 이메일 클라이언트에서는 단일 IMAP 세션을 사용하며, 이는 사용자가 애플리케이션을 종료하는 경우에만 종료됩니다. long-running 연결은 시스템에 의해 로깅되지만 (39-3페이지의 Long-Running 연결 참조), 세션에서 다운로드된 파일은 세션이 종료될 때까지 연결과 관련되지 않습니다.

Series 2 및 Cisco NGIPS for Blue Coat X-Series 디바이스와 DC500 방어 센터에서는 네트워크 기반 지능형 악성코드 차단을 지원하지 않습니다.

연결과 관련된 침입 이벤트 보기

라이센스: 보호

침입 정책을 액세스 제어 규칙 또는 기본 작업과 연결할 경우, 시스템은 매칭 트래픽에서 익스플로잇을 탐지할 수 있습니다. 이벤트 뷰어를 사용하면 로깅된 연결과 관련된 침입 이벤트를 볼 수 있습니다.

이벤트 목록 대신, 방어 센터에서는 **Intrusion Events** 열에 침입 이벤트 보기 아이콘( )을 표시합니다. 이 아이콘을 클릭하면 다음 워크플로 페이지로 드릴다운하거나 연결 이벤트를 제한하지 않습니다. 그 대신 이 아이콘은 연결과 관련된 침입 이벤트 목록은 물론, 해당 이벤트의 우선순위 및 미치는 영향이 포함된 팝업 창을 표시합니다.

팝업 창에서 나열된 이벤트의 보기 아이콘( )을 클릭하여 패킷 보기에서 세부 정보를 볼 수 있습니다. 또한 **View Intrusion Events**를 클릭하여 연결의 모든 관련 침입 이벤트에 대한 세부 정보를 볼 수 있습니다.

팁

하나 이상의 연결과 관련된 침입 이벤트를 신속하게 보려면, 이벤트 뷰어의 확인란을 사용하여 연결을 선택한 다음 **Jump to** 드롭다운 목록에서 **Intrusion Events**를 선택합니다. 침입 이벤트와 관련된 연결을 이와 비슷한 방법으로 볼 수 있습니다. 자세한 내용은 58-35페이지의 워크플로 간 이동을/를 참조하십시오.

관련 이벤트를 볼 경우 방어 센터에서는 기본 침입 이벤트 워크플로를 사용합니다. 침입 이벤트에 대한 자세한 내용은 41-1페이지의 침입 이벤트 작업을/를 참조하십시오.

암호화된 연결과 관련된 인증서 보기

라이센스: 모든

SSL 검사를 구성할 경우, 암호화된 연결을 로깅할 수 있습니다. 이벤트 뷰어를 사용하면 시스템이 트래픽에서 작업을 수행하고 인증서가 사용 가능한 경우, 연결을 암호화하는 데 사용된 공개 키 인증서의 세부 정보를 볼 수 있습니다.

인증서 자체 대신, 방어 센터의 **SSL Status** 열에는 잠금 아이콘()이 표시됩니다. 이 아이콘을 클릭하면 다음 표에 설명된 인증서 세부 정보가 포함된 팝업 창이 표시됩니다.

표 39-7 암호화된 연결 인증서 세부 정보

특성	설명
Subject/Issuer Common Name	인증서 주체 또는 인증서 발급자의 호스트 및 도메인 이름입니다.
Subject/Issuer Organization	인증서 주체 또는 인증서 발급자가 속한 조직입니다.
Subject/Issuer Organization Unit	인증서 주체 또는 인증서 발급자가 속한 조직의 부서입니다.
Not Valid Before/After	인증서가 유효한 날짜입니다.
Serial Number	발급 CA가 할당한 일련 번호입니다.
Certificate Fingerprint	인증서를 인증하는 데 사용되는 SHA 해시 값입니다.
Public Key Fingerprint	인증서 내에 있는 공개 키를 인증하는 데 사용되는 SHA 해시 값입니다.

제목을 두 번 클릭하면 팝업 창의 섹션을 확장하거나 축소할 수 있습니다.

시스템이 암호화된 트래픽에 작업을 수행했으나 인증서가 제공되지 않을 경우, 잠금 아이콘이 회색으로 표시됩니다. 예를 들어, 연결에 SSL 핸드셰이크 오류가 포함되어 있어 시스템이 해당 연결을 차단했으나 이를 해독하지 못한 경우, 시스템은 암호화 인증서 세부 정보를 볼 수 없으며 해당 연결의 잠금 아이콘은 회색으로 표시됩니다.

연결 및 보안 인텔리전스 데이터 검색

라이센스: 모든

방어 센터의 Search 페이지를 사용하면 특정 연결 이벤트, 보안 인텔리전스 이벤트 또는 연결 요약을 검색하고, 이벤트 뷰어에 해당 결과를 표시하며, 나중에 다시 사용하기 위해 검색 기준을 저장할 수 있습니다. Custom Analysis 대시보드 위젯, 보고서 템플릿, 사용자 지정 사용자 역할도 저장된 검색을 사용할 수 있습니다.

시스템에 제공된 검색은 Saved Searches 목록에 (`Cisco`)라는 레이블로 표시되며, 예시 역할을 수행합니다.

연결 그래프는 연결 요약에 기반하므로, 연결 요약을 제한하는 동일한 기준은 연결 그래프도 제한합니다. 별표(*)로 표시된 필드는 연결 그래프 및 연결 요약뿐만 아니라 개별 연결 또는 보안 인텔리전스 이벤트를 제한합니다.

잘못된 검색 제한을 사용하여 연결 요약을 검색하고 사용자 지정 워크플로의 연결 요약 페이지를 사용하여 결과를 볼 경우, 잘못된 제한은 아래 그래픽에 나온 것처럼 해당 사항 없음(N/A)이라는 레이블로 표시되고 취소선이 그어집니다.

또한 검색 결과는 검색할 이벤트에서 제공되는 데이터에 따라 달라진다는 사실을 유의하십시오. 다시 말하면, 사용 가능한 데이터에 따라 검색 제한이 적용되지 않을 수 있습니다. 각 연결 데이터 필드에 데이터가 언제 제공되는지에 대한 내용을 보려면 39-11페이지의 연결 및 보안 인텔리전스 이벤트에서 제공되는 정보을/를 참조하십시오.

일반 검색 구문

각 검색 필드 옆에는 유효한 구문의 예가 표시됩니다. 검색 기준을 입력할 경우, 다음 사항에 유의해야 합니다.

- 모든 필드에 부정(!)을 사용할 수 있습니다.
- 모든 필드에 쉼표로 구분된 검색 값의 목록을 사용할 수 있습니다. 지정된 필드에 나열된 값 중 하나를 포함하는 레코드는 검색 기준과 일치합니다.
- 모든 필드에 따옴표로 감싸고 쉼표로 구분한 목록을 검색 값으로 사용할 수 있습니다.
  - 단일 값만을 포함할 수 있는 필드의 경우, 따옴표 내에 지정된 정확한 문자열을 포함하는 지정된 필드의 레코드가 검색 기준과 일치합니다. 예를 들어 `A, B, "C, D, E"`에 대한 검색은 지정된 필드에 `"A"` 또는 `"B"` 또는 `"C, D, E"`가 포함된 레코드와 일치합니다. 따라서 가능한 값으로 쉼표를 포함하는 필드에서 일치를 확인할 수 있습니다.
  - 여러 값을 동시에 포함할 수 있는 필드의 경우, 따옴표로 감싸고 쉼표로 구분한 모든 값을 포함하는 지정된 필드의 레코드가 해당 검색 기준과 일치합니다.
  - 여러 값을 동시에 포함할 수 있는 필드의 경우, 검색 기준에 단일 값은 물론 따옴표로 감싸고 쉼표로 구분한 목록도 포함할 수 있습니다. 예를 들어 하나 이상의 이러한 문자를 포함할 수 있는 필드에서 `A, B, "C, D, E"`에 대한 검색은 지정된 필드에 `A` 또는 `B`, 또는 `C`, `D`, `E` 모두가 포함된 레코드와 일치합니다.
- 검색 결과에는 모든 필드에 지정된 검색 기준과 매칭되는 레코드만 반환됩니다.
- 많은 필드에서 와일드카드로 하나 이상의 별표(*)를 사용할 수 있습니다.
- 해당 필드에 대해 사용할 수 있는 정보가 없는 이벤트를 식별하려면 필드에 `n/a`를 지정합니다. 해당 필드가 채워지는 이벤트를 식별하려면 `!n/a`를 사용합니다.
- 특정 디바이스 및 그룹, 스택 또는 클러스터의 디바이스를 검색하려면 디바이스 필드를 사용합니다. FireSIGHT 시스템에서 검색 시 디바이스 필드를 취급하는 방법에 대한 자세한 내용은 60-7페이지의 검색에서 디바이스 지정을/를 참조하십시오.
- 검색 기준으로 객체를 사용하려면 검색 필드 옆에 나타나는 객체 추가 아이콘(+)을 클릭합니다.

검색에서 객체를 사용하는 방법을 포함하여 검색 구문에 대한 자세한 내용은 60-1페이지의 이벤트 검색을/를 참조하십시오.

연결 및 보안 인텔리전스 데이터에 대한 특수 검색 구문

위에 나열된 일반 검색 구문을 보완하기 위해, 다음 목록에서는 연결 및 보안 인텔리전스 데이터에 대한 몇 가지 특수 검색 구문을 설명합니다.

연결과 매칭되는 Monitor 규칙

Access Control Rule 기준을 사용하여 개별 Monitor 규칙과 매칭되는 연결을 검색할 수 있습니다.

Monitor 규칙은 항상 다른 규칙 또는 기본 작업에 의해 나중에 처리되므로, `Monitor` 작업과의 연결을 검색할 수 없습니다. Monitor 규칙의 이름을 검색하면 연결을 나중에 처리하는 규칙 또는 기본 작업에 상관없이, 해당 Monitor 규칙과 매칭되는 모든 연결이 반환됩니다.

숫자 값에 대한 기준(바이트, 패킷, 연결 수)

숫자 앞에 이상(`>`), 크거나 같음(`>=`), 이하(`<`), 작거나 같음(`<=`), 같음(`=`) 부호를 넣을 수 있습니다.

팁 **Connections** 기준을 사용하여 유의미한 검색 결과를 보려면, 연결 요약 페이지가 있는 사용자 지정 워크플로를 사용해야 합니다.

연결과 관련된 Files 또는 Intrusion Events

연결/보안 인텔리전스 이벤트 검색 페이지를 사용하여 연결과 관련된 파일, 악성코드, 침입 이벤트를 검색할 수 없습니다. 이러한 관련 이벤트를 보는 방법에 대한 자세한 내용은 39-30페이지의 연결에서 탐지된 파일 보기 및 39-31페이지의 연결과 관련된 침입 이벤트 보기을/를 참조하십시오.

연결의 Initiator User 또는 URL

시스템에서는 부분 매칭을 수행하므로, 별표를 사용하지 않고도 필드 내용의 전체 또는 부분을 검색할 수 있습니다.

연결에 사용된 총 트래픽(바이트 수) 또는 전송 프로토콜

연결 테이블 보기에 프로토콜 또는 트래픽 제한이 있는지 확인하려면, 검색 제한을 확장합니다.

특정 프로토콜을 검색하려면 http://www.iana.org/assignments/protocol-numbers에 나열된 이름 또는 숫자 프로토콜을 사용합니다.

이러한 열은 테이블 보기에 표시되지 않습니다.

NetFlow 연결의 TCP 플래그

이러한 플래그가 *최소한* 하나 이상(전체 대신) 포함된 모든 연결을 보려면 쉼표로 분리된 TCP 플래그 목록을 입력합니다. 또한 **Only** 확인란을 선택하여 TCP 플래그로만 지정한 모든 플래그가 포함된 연결을 검색할 수 있습니다.

연결에 적용된 SSL 암호화

SSL 암호화 또는 비암호화 연결을 보려면 `yes` 또는 `no`를 입력합니다.

이 열은 보안 인텔리전스 또는 연결 이벤트 테이블 보기에 표시되지 않습니다.

SSL 상태

시스템에서 작업을 적용하거나 조건을 확인한 암호화된 트래픽을 보려면 **SSL Actual Action** 및 **SSL Failure Reason**에 나열된 하나 이상의 키워드를 입력합니다. 이 필드에는 하나의 **SSL Actual Action** 값과 **SSL Failure Reason** 값이 동시에 포함될 수 있습니다.

해독이 올바르게 완료되면, 보안 인텔리전스 및 연결 이벤트 테이블 보기의 **SSL Status** 열에 **SSL Actual Action**의 값이 표시됩니다. 시스템이 트래픽을 해독하지 못한 경우, 보안 인텔리전스 및 연결 이벤트 테이블 보기의 **SSL Status** 열에 **SSL Actual Action** 및 **SSL Failure Reason** 사유가 표시됩니다.

수행한 SSL Actual Action

시스템에서 지정된 작업을 적용한 암호화된 트래픽을 보려면 다음 키워드를 입력합니다.

- `Do not Decrypt` - 시스템이 해독하지 못한 연결을 나타냅니다.
- `Block` 및 `Block with reset` - 차단된 암호화 연결을 나타냅니다.
- `Decrypt (Known Key)` - 알려진 개인 키를 사용하여 해독된 수신 연결을 나타냅니다.
- `Decrypt (Replace Key)` - 대체된 공개 키가 있는 자체 서명된 서버 인증서를 사용하여 해독된 발신 연결을 나타냅니다.
- `Decrypt (Resign)` - 다시 서명된 서버 인증서를 사용하여 해독된 발신 연결을 나타냅니다.

해독이 올바르게 완료되면, 보안 인텔리전스 및 연결 이벤트 테이블 보기의 **SSL Status** 열에 이 값이 표시됩니다. 시스템이 트래픽을 해독하지 못한 경우, 보안 인텔리전스 및 연결 이벤트 테이블 보기의 **SSL Status** 열에 **SSL Failure Reason** 사유가 표시됩니다.

SSL 예상 작업

SSL 규칙이 유효할 경우, 시스템이 지정된 방식으로 작업을 처리할 것으로 예상되는 암호화된 트래픽을 보려면 다음 키워드를 입력합니다.

- `Do not Decrypt` - 시스템이 해독하지 못한 연결을 나타냅니다.
- `Block` 및 `Block with reset` - 차단된 암호화 연결을 나타냅니다.
- `Decrypt (Known Key)` - 알려진 개인 키를 사용하여 해독된 수신 연결을 나타냅니다.
- `Decrypt (Replace Key)` - 대체된 공개 키가 있는 자체 서명된 서버 인증서를 사용하여 해독된 발신 연결을 나타냅니다.
- `Decrypt (Resign)` - 다시 서명된 서버 인증서를 사용하여 해독된 발신 연결을 나타냅니다.

이 열은 보안 인텔리전스 또는 연결 이벤트 테이블 보기에 표시되지 않습니다.

SSL 실패 사유

시스템이 지정된 사유로 인해 해독하지 못한 암호화된 트래픽을 보려면 다음 키워드를 입력합니다.

- `Unknown`
- `No Match`
- `Success`
- `Uncached Session`
- `Unknown Cipher Suite`
- `Unsupported Cipher Suite`
- `Unsupported SSL Version`
- `SSL Compression Used`
- `Session Undecryptable in Passive Mode`
- `Handshake Error`
- `Decryption Error`
- `Pending Server Name Category Lookup`
- `Pending Common Name Category Lookup`
- `Internal Error`
- `Network Parameters Unavailable`
- `Invalid Server Certificate Handle`
- `Server Certificate Fingerprint Unavailable`
- `Cannot Cache Subject DN`

- Cannot Cache Issuer DN
- Unknown SSL Version
- External Certificate List Unavailable
- External Certificate Fingerprint Unavailable
- Internal Certificate List Invalid
- Internal Certificate List Unavailable
- Internal Certificate Unavailable
- Internal Certificate Fingerprint Unavailable
- Server Certificate Validation Unavailable
- Server Certificate Validation Failure
- Invalid Action

시스템이 트래픽을 해독하지 못한 경우, 보안 인텔리전스 및 연결 이벤트 테이블 보기의 **SSL Status** 열에 **SSL Actual Action**과 함께 이 값이 표시됩니다.

사용된 SSL 암호 그룹

매크로 값을 입력하여 연결을 암호화하는 데 사용된 암호 그룹을 표시합니다. 암호 그룹 값 지정에 대한 내용은 www.iana.org/assignments/tls-parameters/tls-parameters.xhtml 을/를 참조하십시오.

SSL 주체 국가

암호화 인증서 주체 국가와 연결된 암호화된 트래픽을 보려면 두 개의 문자로 된 ISO 3166-1 알파-2 국가 코드를 입력합니다.

이 열은 보안 인텔리전스 또는 연결 이벤트 테이블 보기에 표시되지 않습니다.

SSL 발급자 국가

암호화 인증서 주체 국가와 연결된 암호화된 트래픽을 보려면 두 개의 문자로 된 ISO 3166-1 알파-2 국가 코드를 입력합니다.

이 열은 보안 인텔리전스 또는 연결 이벤트 테이블 보기에 표시되지 않습니다.

SSL 인증서 핑거프린트

인증서를 인증하고 해당 인증서와 연결된 트래픽을 보는 데 사용된 SHA 해시 값을 입력하거나 붙여넣습니다.

이 열은 보안 인텔리전스 또는 연결 이벤트 테이블 보기에 표시되지 않습니다.

SSL 공개 키 핑거프린트

공개 키를 인증하고 해당 인증서와 연결된 트래픽을 보는 데 사용된 SHA 해시 값을 입력하거나 붙여넣습니다.

이 열은 보안 인텔리전스 또는 연결 이벤트 테이블 보기에 표시되지 않습니다.

SSL 인증서 상태

이는 Certificate Status 규칙 조건을 구성한 경우에만 적용됩니다. 서버 인증서 상태와 연결된 암호화된 트래픽을 보려면 아래에 나열된 키워드를 하나 이상 입력합니다. 암호화된 트래픽은 여러 서버 인증서 상태와 동시에 매칭되지 않을 수 있습니다.

- Not Checked
- Self Signed
- Valid
- Invalid Signature

- Invalid Issuer
- Expired
- Unknown
- Not Valid Yet
- Revoked

SSL 흐름 메시지

SSL 핸드셰이크 도중 클라이언트와 서버 간에 교환된 다음 메시지와 연결된 암호화된 트래픽을 보려면 다음 키워드를 입력합니다.

- HELLO_REQUEST
- CLIENT_ALERT
- SERVER_ALERT
- CLIENT_HELLO
- SERVER_HELLO
- SERVER_CERTIFICATE
- SERVER_KEY_EXCHANGE
- CERTIFICATE_REQUEST
- SERVER_HELLO_DONE
- CLIENT_CERTIFICATE
- CLIENT_KEY_EXCHANGE
- CERTIFICATE_VERIFY
- CLIENT_CHANGE_CIPHER_SPEC
- CLIENT_FINISHED
- SERVER_CHANGE_CIPHER_SPEC
- SERVER_FINISHED
- NEW_SESSION_TICKET
- HANDSHAKE_OTHER
- APP_DATA_FROM_CLIENT
- APP_DATA_FROM_SERVER

SSL 버전

지정된 SSL 또는 TLS 프로토콜 버전과 연결된 암호화된 트래픽을 보려면 다음 키워드를 입력합니다.

- Unknown
- SSLv2.0
- SSLv3.0
- TLSv1.0
- TLSv1.1
- TSLv1.2

SSL 일련 번호

발급 CA가 공개 키 인증서에 할당한 일련 번호를 입력하거나 붙여넣습니다.

이 열은 보안 인텔리전스 또는 연결 이벤트 테이블 보기에 표시되지 않습니다.

연결 또는 보안 인텔리전스 데이터를 검색하려면

액세스: Admin/Any Security Analyst

1단계 **Analysis > Search**를 선택합니다.

Search 페이지가 나타납니다.

2단계 다음 옵션을 이용할 수 있습니다.

- 테이블 드롭다운 목록에서 **Connection Events**를 선택하여 연결 데이터를 검색합니다.
- 테이블 드롭다운 목록에서 **Security Intelligence Events**를 선택하여 보안 인텔리전스 데이터를 검색합니다.

해당 제약 조건으로 페이지가 업데이트됩니다.

3단계 해당 필드에 검색 기준을 입력합니다.

- 연결 및 보안 인텔리전스 테이블의 필드에 대한 자세한 내용은 39-4페이지의 연결 및 보안 인텔리전스 데이터 필드 이해을/를 참조하십시오.
- 공개 키 인증서와 관련된 필드에 대한 자세한 내용은 39-32페이지의 암호화된 연결과 관련된 인증서 보기을/를 참조하십시오.
- 연결 및 보안 인텔리전스 이벤트의 특수 검색 구문에 대한 내용은 39-33페이지의 연결 및 보안 인텔리전스 데이터에 대한 특수 검색 구문을/를 참조하십시오.

4단계 선택적으로, 검색을 저장하려면 **Private** 확인란을 선택하여 자신만 액세스할 수 있는 비공개로 검색을 저장할 수 있습니다. 또는 모든 사용자가 사용할 수 있도록 검색을 저장하려면 확인란을 선택하지 않습니다.

팁 사용자 지정 사용자 역할에 대한 데이터 제한으로서 검색을 사용하려면 **반드시** 비공개 검색으로 저장해야 합니다.

5단계 선택적으로, 나중에 다시 사용할 수 있도록 검색을 저장할 수 있습니다. 다음 옵션을 이용할 수 있습니다.

- 검색 기준을 저장하려면 **Save**를 클릭합니다.

  새 검색인 경우 검색 이름을 입력하도록 대화 상자가 나타납니다. 고유한 검색 이름을 입력하고 **Save**를 클릭합니다. 이미 존재하는 검색에 대한 새 조건을 저장하는 경우 프롬프트가 나타나지 않습니다. 나중에 실행할 수 있도록 검색이 저장됩니다(**Private**을 선택한 경우 자신만 볼 수 있음).

- 새 검색을 저장하거나, 저장된 기존 검색을 변경하여 만든 검색에 새 이름을 할당하려면 **Save As New**를 클릭합니다.

  검색 이름을 입력하도록 대화 상자가 나타납니다. 고유한 검색 이름을 입력하고 **Save**를 클릭합니다. 나중에 실행할 수 있도록 검색이 저장됩니다(**Private**을 선택한 경우 자신만 볼 수 있음).

6단계 검색을 시작하려면 **Search**를 클릭합니다.

검색 결과가 기본 연결 또는 보안 인텔리전스 워크플로에 표시되며, 현재 시간 범위로 제한됩니다.

연결 요약 페이지 보기

라이센스: 모든

Connection Summary 페이지에서는 여러 기준별로 구성된 모니터링되는 네트워크의 작업에 대한 그래프를 제공합니다. 예를 들어, Connections over Time 그래프에는 사용자가 선택한 간격에 따라 모니터링되는 네트워크의 총 연결 수가 표시됩니다.

참고 Connection Summary 페이지는 연결 이벤트에 대한 검색이 제한된 사용자 지정 역할을 보유하고 있고, Connection Summary 페이지에 명시적인 액세스 권한을 부여받은 사용자에게만 표시됩니다. 자세한 내용은 61-55페이지의 제한적 사용자 액세스 속성 이해 및 61-51페이지의 사용자 지정 사용자 역할 관리을/를 참조하십시오.

다음 표에는 Connection Summary 페이지에서 수행할 수 있는 여러 작업이 설명되어 있습니다.

표 39-8 Connection Summary 페이지 작업

목적	가능한 작업
Connection Summary 페이지의 시간 및 날짜 범위 수정	58-22페이지의 이벤트 시간 제약 조건 설정에서 자세히 알아보십시오.
연결 그래프 조작	39-16페이지의 연결 그래프 작업에서 자세히 알아보십시오.
페이지에서 연결 그래프 분리	분리하려는 그래프에서 **View**를 클릭합니다. 분리된 그래프에 대한 자세한 내용은 39-27페이지의 연결 그래프 분리을/를 참조하십시오.

연결 요약 그래프에서는 연결 그래프에서 수행할 수 있는 작업을 거의 모두 동일하게 수행할 수 있습니다. 그러나 Connection Summary 페이지의 그래프는 취합된 데이터를 기반으로 하므로, 그래프의 기준이 되는 개별 연결 이벤트를 검사할 수 없습니다. 즉, 연결 요약 그래프에서는 연결 데이터 테이블 보기로 드릴다운할 수 없습니다.

Connection Summary 페이지를 보려면

액세스: Custom

1단계 **Overview > Summary > Connection Summary**를 선택합니다.

Connection Summary 페이지가 방어 센터의 현재 시간 범위로 표시됩니다.

2단계 **Select Device** 목록에서, 보려는 요약이 포함된 디바이스를 선택하거나 **All**을 선택하여 모든 디바이스의 요약을 봅니다.

40장

악성코드 및 파일 활동 분석

방어 센터에서는 시스템의 파일 검사 및 처리에 대한 레코드를 캡처된 파일, 파일 이벤트 및 악성코드 이벤트로 기록합니다.

- *캡처된 파일* - 시스템에 의해 캡처된 파일을 나타냅니다.
- *파일 이벤트* - 네트워크 트래픽에서 시스템에 의해 탐지되고 선택적으로 차단된 파일을 나타냅니다.
- *악성코드 이벤트* - 네트워크 트래픽에서 시스템에 의해 탐지되고 선택적으로 차단된 악성코드 파일을 나타냅니다.
- *소급 악성코드 이벤트* - 악성코드 파일 속성이 변경된 파일을 나타냅니다.

시스템은 네트워크 트래픽에서 악성코드의 탐지 또는 차단을 기반으로 악성코드 이벤트를 생성할 때 파일 이벤트도 생성합니다. 파일에서 악성코드를 탐지하려면 우선 파일 자체를 탐지해야 하기 때문입니다. FireAMP Connector(37-7페이지의 FireSIGHT 시스템와 FireAMP통합 참조)에서 생성된 엔드포인트 기반 악성코드 이벤트에는 해당 파일 이벤트가 없습니다. 이와 마찬가지로, 시스템이 네트워크 트래픽에서 파일을 캡처할 경우 파일을 먼저 탐지하므로 파일 이벤트가 함께 생성됩니다.

방어 센터를 사용하여 캡처 파일, 파일 이벤트, 악성코드 이벤트를 보고, 조작하고, 분석한 후 이러한 분석 결과를 다른 사용자에게 전달할 수 있습니다. Context Explorer, 대시보드, 이벤트 뷰어, 컨텍스트 메뉴, 네트워크 파일 전파 흔적 맵 및 보고 기능을 사용하면 탐지, 캡처 및 차단된 파일과 악성코드를 더 깊이 이해할 수 있습니다. 이벤트를 사용하여 상관관계 정책 위반을 트리거하거나 이메일, SMTP 또는 syslog를 통해 알림을 제공할 수도 있습니다.

악성코드 라이센스를 DC500에서 사용할 수 없고 악성코드 라이센스를 Series 2 디바이스 또는 Cisco NGIPS for Blue Coat X-Series에서 활성화할 수 없으므로 악성코드 클라우드 조회 또는 아카이브 파일 콘텐츠와 관련된 악성코드 이벤트, 파일 이벤트 및 캡처된 파일을 생성하거나 분석하는 데 이러한 어플라이언스를 사용할 수 없습니다.

자세한 내용은 다음 링크를 참고하십시오.

이 장에서 설명하는 데이터를 생성하는 악성코드 차단 및 파일 제어 작업을 수행하기 위해 시스템을 구성하는 방법에 대한 자세한 내용은 37-1페이지의 악성코드 및 금지된 파일 차단을/를 참조하십시오.

파일 스토리지 작업

라이센스: 악성코드

지원되는 디바이스: Series 2 또는 X-Series를 제외한 모두

지원되는 Defense Center: DC500을 제외한 모든 방어 센터

파일 정책 컨피그레이션을 기반으로 파일을 탐지 및 차단하는 데 파일 제어 기능을 사용할 수 있습니다. 그러나 의심스러운 호스트나 네트워크에서 온 파일, 또는 네트워크의 모니터링되는 호스트로 전송된 파일에 대한 액세스의 경우 추가 분석이 필요할 수 있습니다. 파일 스토리지 기능을 사용하면 트래픽에서 탐지된 선택 파일을 캡처한 다음 디바이스의 하드 드라이브 또는 악성코드 스토리지 팩(설치된 경우)에 자동으로 저장할 수 있습니다.

디바이스는 트래픽에서 파일을 탐지하면 캡처할 수 있습니다. 시스템은 이렇게 생성된 복사본을 저장할 수도 있고 동적 분석을 위해 제출할 수도 있습니다. 디바이스가 파일을 캡처한 후에는 몇 가지 옵션이 있습니다.

- 나중에 분석하기 위해 캡처한 파일을 디바이스의 하드 드라이브에 저장합니다. 자세한 내용은 40-3페이지의 캡처된 파일 스토리지 이해을/를 참조하십시오.
- 저장된 파일을 추가 수동 분석 또는 아카이브를 위해 로컬 컴퓨터로 다운로드합니다. 자세한 내용은 40-4페이지의 다른 위치에 저장된 파일 다운로드을/를 참조하십시오.
- 캡처된 파일을 동적 분석을 위해 종합 보안 인텔리전스 클라우드에 제출합니다. 자세한 내용은 40-4페이지의 동적 분석 작업을/를 참조하십시오.

디바이스는 파일을 저장한 경우, 나중에 해당 파일이 탐지되었을 때 여전히 저장되어 있으면 다시 캡처하지 않습니다.

참고 처음으로 탐지된 파일은 방어 센터에서 클라우드 조회를 완료한 후 성향이 할당됩니다. 파일에 즉시 성향이 할당되지 않으면 시스템은 파일 이벤트를 생성하더라도 파일을 저장할 수 없습니다.

전에 탐지되지 않은 파일이 Block Malware 작업과 파일 규칙이 일치하면, 이어지는 클라우드 조회에서 즉시 성향을 반환하여 시스템이 파일을 저장하고 이벤트를 생성할 수 있도록 합니다.

전에 탐지되지 않은 파일이 Malware Cloud Lookup 작업과 파일 규칙이 일치하면, 시스템은 파일 이벤트를 생성하지만 클라우드 조회를 수행하고 성향을 반환하려면 추가 시간이 필요합니다. 이러한 지연 때문에 시스템은 Malware Cloud Lookup 작업과 파일 규칙이 일치하는 파일을, 네트워크에서 두 번째로 탐지될 때까지 저장할 수 없습니다.

시스템이 파일을 캡처하든 저장하든 사용자는 다음을 수행할 수 있습니다.

- 파일이 저장되었는지 아니면 동적 분석을 위해 제출되었는지 여부, 파일 성향, 위협 점수 등 캡처된 파일에 대한 정보를 이벤트 뷰어에서 검토할 수 있으며, 이를 통해 사용자는 네트워크에서 탐지된 악성코드 위협 가능성을 신속하게 검토할 수 있습니다. 자세한 내용은 40-30페이지의 캡처된 파일 작업을/를 참조하십시오.
- 파일의 전파 흔적을 보고 파일이 네트워크에서 어떻게 이동했는지, 어떤 호스트에 복사본이 있는지를 확인할 수 있습니다. 자세한 내용은 40-38페이지의 네트워크 파일 전파 흔적 분석을/를 참조하십시오.
- 향후 탐지에서 정상 또는 악성코드 성향이 있는 것으로 항상 취급하기 위해 파일을 정상 목록 또는 사용자 지정 탐지 목록에 추가할 수 있습니다. 자세한 내용은 3-33페이지의 파일 목록 작업을/를 참조하십시오.

특정 유형 또는 특정 성향(사용 가능한 경우)의 파일을 캡처 및 저장하도록 파일 정책에서 파일 규칙을 구성할 수 있습니다. 파일 정책을 액세스 제어 정책과 연결하고 디바이스에 적용하면, 트래픽에서 일치하는 파일이 캡처 및 저장됩니다. 또한 저장할 최소 및 최대 파일 크기를 제한할 수도 있습니다. 자세한 내용은 18-20페이지의 파일 및 악성코드 검사 성능과 저장 조정 및 37-17페이지의 파일 규칙 작업을/를 참조하십시오.

파일 스토리지 기능을 이용하려면 디바이스에 디스크 공간이 충분해야 합니다. 디바이스의 기본 하드 드라이브에 충분한 공간이 없으며 악성코드 스토리지 팩이 설치되어 있지 않으면 디바이스에 파일을 저장할 수 없습니다.

주의 Cisco에서 제공하지 않은 하드 드라이브를 디바이스에 설치하려고 하지 마십시오. 지원되지 않는 하드 드라이브를 설치하면 디바이스가 손상될 수 있습니다. 악성코드 스토리지 팩 키트는 Cisco **전용**으로만, 그리고 8000 Series 디바이스 **전용**으로만 사용할 수 있습니다. 악성코드 스토리지 팩과 관련하여 도움이 필요하면 고객 지원에 문의하십시오. 자세한 내용은 *FireSIGHT 시스템 Malware Storage Pack Guide*를 참조하십시오.

악성코드 라이센스를 DC500에서 사용할 수 없고 악성코드 라이센스를 Series 2 디바이스 또는 Cisco NGIPS for Blue Coat X-Series에서 활성화할 수 없으므로 파일을 캡처 또는 저장하는 데 이러한 어플라이언스를 사용할 수 없습니다.

자세한 내용은 다음 링크를 참고하십시오.

- 40-3페이지의 캡처된 파일 스토리지 이해
- 40-4페이지의 다른 위치에 저장된 파일 다운로드

캡처된 파일 스토리지 이해

라이센스: 악성코드

지원되는 디바이스: 8000 Series

디바이스에서는 파일 정책 컨피그레이션을 기반으로 상당한 양의 파일 데이터를 하드 드라이브에 저장할 수 있습니다. 디바이스에 악성코드 스토리지 팩을 설치할 수 있습니다. 시스템은 파일을 악성코드 스토리지 팩에 저장하므로, 기본 하드 드라이브에 이벤트와 컨피그레이션 파일을 저장하기 위한 공간이 좀 더 확보됩니다. 시스템은 주기적으로 오래된 파일을 삭제합니다.

주의 Cisco에서 제공하지 않은 하드 드라이브를 디바이스에 설치하려고 하지 마십시오. 지원되지 않는 하드 드라이브를 설치하면 디바이스가 손상될 수 있습니다. 악성코드 스토리지 팩 키트는 Cisco **전용**으로만, 그리고 8000 Series 디바이스 **전용**으로만 사용할 수 있습니다. 악성코드 스토리지 팩과 관련하여 도움이 필요하면 고객 지원에 문의하십시오. 자세한 내용은 FireSIGHT 시스템 *Malware Storage Pack Guide*를 참조하십시오.

악성코드 스토리지 팩이 설치되지 않은 상태에서 파일을 저장하도록 디바이스를 구성하면, 기본 하드 드라이브 공간의 일정 부분이 캡처된 파일 스토리지에만 할당됩니다. 디바이스에 악성코드 스토리지 팩을 설치하고 파일을 저장하도록 디바이스를 구성하면 전체 악성코드 스토리지 팩이 캡처된 파일을 저장하는 데 할당됩니다. 디바이스는 악성코드 스토리지 팩에 다른 정보를 저장할 수 없습니다.

캡처된 파일 스토리지의 할당된 공간이 꽉 차면 시스템은 할당된 공간이 시스템 정의 임계값에 도달할 때까지 저장된 파일 중 가장 오래된 파일을 삭제합니다. 저장된 파일 수를 기반으로, 시스템이 파일을 삭제한 후 디스크 사용량이 상당히 줄어든 것을 알 수 있을 것입니다.

디바이스가 이미 파일을 저장한 상태에서 악성코드 스토리지 팩을 설치하면, 디바이스를 다음에 다시 시작할 때 기본 하드 드라이브에 저장된 캡처된 파일이 악성코드 스토리지 팩으로 이동합니다. 이후 디바이스에서 저장하는 파일은 악성코드 스토리지 팩에 저장됩니다. 디바이스의 기본 하드 드라이브에 여유 공간이 충분하지 않거나 악성코드 스토리지 팩이 설치되어 있지 않으면 파일을 저장할 수 없습니다.

저장된 파일은 시스템 백업 파일에 포함할 수 없습니다. 자세한 내용은 70-2페이지의 백업 파일 생성을/를 참조하십시오.

다른 위치에 저장된 파일 다운로드

라이센스: 악성코드

지원되는 디바이스: Series 2 또는 X-Series를 제외한 모두

지원되는 Defense Center: DC500을 제외한 모든 방어 센터

디바이스가 파일을 저장한 경우 방어 센터가 해당 디바이스와 통신할 수 있고 파일을 삭제하지 않았다면 사용자는 해당 파일을 다운로드할 수 있습니다. 파일을 수동으로 분석할 수도 있고, 장기간 보관 및 분석을 위해 로컬 호스트로 다운로드할 수도 있습니다. 관련 파일 이벤트, 악성코드 이벤트, 캡처된 파일 보기 또는 파일 전파 흔적에서 파일을 다운로드할 수 있습니다. 자세한 내용은 2-5페이지의 컨텍스트 메뉴 사용 및 40-38페이지의 요약 정보을/를 참조하십시오.

기본적으로 악성코드는 유해하므로 모든 파일 다운로드를 확인해야 합니다. 그러나 파일 다운로드 프롬프트에서 확인을 비활성화할 수 있습니다. 확인을 다시 활성화하려면 71-5페이지의 파일 환경 설정을/를 참조하십시오.

주의 Cisco 사용자는 유해한 결과로 이어질 수 있는 악성코드를 다운로드해서는 **안 됩니다**. 어떤 파일을 다운로드할 때 악성코드를 포함했을 수도 있으므로 각별히 주의하십시오. 파일을 다운로드하기 전에 다운로드할 위치를 보호하기 위해 필요한 모든 예방 조치를 취해야 합니다.

Unknown 성향의 파일에는 악성코드가 포함되어 있을 수 있으므로, 파일을 다운로드할 때 시스템은 먼저 해당 파일을 `.zip` 패키지에 아카이브합니다. `.zip` 파일 이름에는 파일 성향과 파일 형식, 그리고 SHA-256 값(사용 가능한 경우)이 포함됩니다. 실수로 압축을 해제하지 못하도록 `.zip` 파일을 비밀번호로 보호할 수 있습니다. 기본 `.zip` 파일 비밀번호를 수정 또는 제거하려면 71-5페이지의 파일 환경 설정을/를 참조하십시오.

동적 분석 작업

라이센스: 악성코드

지원되는 디바이스: Series 2 또는 X-Series를 제외한 모두

지원되는 Defense Center: DC500을 제외한 모든 방어 센터

클라우드의 정확성을 높이고 추가 악성코드 분석 및 위협 식별을 제공하려면, 동적 분석을 위해 해당되는 캡처된 파일을 Cisco 클라우드에 제출할 수 있습니다. 클라우드는 테스트 환경에서 파일을 실행하고, 해당 결과를 바탕으로 위협 점수 및 동적 분석 요약 보고서를 방어 센터에 반환합니다. 해당 파일을 Spero 분석을 위해 클라우드로 제출할 수도 있습니다. 이 분석에서는 악성코드 식별을 보완하기 위해 파일의 구조를 검토합니다.

동적 분석을 위해 클라우드에 파일을 제출하는 작업은 캡처한 파일의 유형뿐만 아니라, 액세스 제어 정책에 구성된 허용 가능한 최소 및 최대 파일 크기에 따라 달라집니다. 다음과 같이 제출할 수 있습니다.

- 동적 분석을 위해 파일을 자동으로 제출 - 파일 규칙이 실행 파일에서 악성코드 클라우드 조회를 수행하는 경우 및 파일 성향을 알 수 없는 경우
- 동적 분석을 위해 한 번에 최대 25개의 파일을 수동으로 제출 - 저장 및 지원되는 파일 형식이 PDF, Microsoft Office 문서, 기타에 해당되는 경우

제출된 파일은 클라우드의 분석 대기열에 추가됩니다. 캡처된 파일 및 파일의 전파 흔적을 확인하여 파일이 동적 분석을 위해 제출되었는지 확인할 수 있습니다. 동적 분석을 위해 파일을 제출할 때마다 클라우드에서는 파일을 분석하며, 첫 번째 분석에서 결과가 생성된 경우에도 마찬가지입니다.

자세한 내용은 37-17페이지의 파일 규칙 작업 및 40-6페이지의 동적 분석을 위해 파일 제출을/를 참조하십시오.

참고 시스템은 클라우드에서 동적 분석 대상이 되는 파일 형식의 목록에 대한 업데이트 및 제출 가능한 (하루 1회를 넘지 않음) 파일의 최대/최소 크기를 확인합니다.

클라우드의 경우 샌드박스 환경에서 파일을 실행하여 동적 분석을 수행합니다. 다음이 반환됩니다.

- 위협 점수 - 파일에 악성코드가 포함될 가능성에 대해 세부적으로 설명.
- 동적 분석 요약 보고서 - 클라우드에서 해당 위협 점수를 할당한 이유를 세부적으로 설명.

파일 정책 컨피그레이션을 기준으로, 정의된 임계값보다 위협 점수가 높은 파일은 자동으로 차단할 수 있습니다. 또한 악성코드를 더 잘 식별하고 탐지 기능을 세부적으로 조정하기 위해 동적 분석 요약 보고서를 검토할 수 있습니다.

파일 규칙이 실행 파일에서 악성코드 클라우드 조회를 수행하는 경우, 동적 분석을 보완하려면 Spero 분석용 파일을 자동으로 제출할 수 있습니다. 클라우드는 메타데이터와 헤더 정보를 포함하여 실행 파일의 구조를 검토하고, 파일을 악성코드로 식별할 수 있습니다. 자세한 내용은 37-2페이지의 악성코드 차단 및 파일 제어 이해을/를 참조하십시오.

악성코드 라이센스를 DC500에서 사용할 수 없고 악성코드 라이센스를 Series 2 디바이스 또는 Cisco NGIPS for Blue Coat X-Series에서 활성화할 수 없으므로 동적 분석 또는 Spero 분석을 위해 파일을 제출하는 데 이러한 어플라이언스를 사용할 수 없습니다.

참고 HTTP 프록시를 통해 Cisco 클라우드에 파일을 제출하도록 관리되는 디바이스를 구성할 수 있습니다. 물리적 어플라이언스 구성 방법에 대한 자세한 내용은 64-8페이지의 관리 인터페이스 구성을/를 참조하십시오. 가상 어플라이언스 구성 방법은 D-33페이지의 http-proxy을/를 참조하십시오. Cisco NGIPS for Blue Coat X-Series는 프록시 설정을 지원하지 않습니다.

자세한 내용은 다음 링크를 참고하십시오.

- 40-6페이지의 Spero 분석 이해
- 40-6페이지의 동적 분석을 위해 파일 제출
- 40-6페이지의 위협 점수 및 동적 분석 요약 검토

Spero 분석 이해

라이센스: 악성코드

지원되는 디바이스: Series 2 또는 X-Series를 제외한 모두

지원되는 Defense Center: DC500을 제외한 모든 방어 센터

Spero 분석은 실행 파일에서 악성코드를 좀 더 완벽하게 식별할 수 있도록 SHA-256 해시의 분석을 보완합니다. Spero 분석에는 메타데이터 및 헤더 정보와 같은 파일 구조 특성을 검토하는 디바이스가 포함됩니다. 디바이스는 이 정보를 기반으로 Spero 서명을 생성한 후 Cisco 클라우드의 Spero 휴리스틱 엔진에 제출합니다. Spero 서명을 기반으로 Spero 엔진은 파일이 악성코드인지 여부를 반환합니다. 파일이 악성코드이며 파일 성향을 현재 알 수 없는 경우 시스템은 Malware 파일 성향을 할당합니다. 파일 성향에 대한 자세한 내용은 37-2페이지의 악성코드 차단 및 파일 제어 이해을/를 참조하십시오.

Spero 분석을 위해 실행 파일을 탐지 즉시 제출할 수 있으며, 나중에 수동으로 제출할 수 없습니다. 동적 분석을 위해 제출하지 않은 상태에서도 Spero 분석을 위해 파일을 제출할 수 있습니다. 자세한 내용은 37-17페이지의 파일 규칙 작업을/를 참조하십시오.

동적 분석을 위해 파일 제출

라이센스: 악성코드

지원되는 디바이스: Series 2 또는 X-Series를 제외한 모두

지원되는 Defense Center: DC500을 제외한 모든 방어 센터

이벤트 뷰어 컨텍스트 메뉴 또는 네트워크 파일 전파 흔적에서 동적 분석을 위해 파일을 수동으로 제출할 수 있습니다. 실행 파일 외에 자동 제출 대상이 아닌 파일 형식(예: PDF, Microsoft Office 문서 등)도 제출할 수 있습니다. 자세한 내용은 2-5페이지의 컨텍스트 메뉴 사용 및 40-38페이지의 요약 정보을/를 참조하십시오.

파일 성향과 상관없이, 인시던트 이후 여러 파일을 분석하려면 캡처된 파일 보기에서 동시에 최대 25개 파일(특정 형식)을 수동으로 제출할 수 있습니다. 이렇게 하면 광범위한 파일을 좀 더 빠르게 분석하고 인시던트의 원인을 정확히 파악할 수 있습니다. 자세한 내용은 40-30페이지의 캡처된 파일 작업 및 58-34페이지의 워크플로 페이지의 행 선택을/를 참조하십시오.

위협 점수 및 동적 분석 요약 검토

라이센스: 악성코드

지원되는 디바이스: Series 2 또는 X-Series를 제외한 모두

지원되는 Defense Center: DC500을 제외한 모든 방어 센터

동적 분석용 파일을 제출하면 Cisco 클라우드는 파일의 서명을 분석하고 위협 점수 및 동적 분석 요약을 반환합니다. 이를 통해 잠재적 악성코드 위협을 좀 더 면밀히 분석하고 탐지 전략을 세부적으로 조정할 수 있습니다.

위협 점수

가능성에서 네 가지 위협 점수 평가 중 하나에 속하는 파일은 악의적인 파일로 분류됩니다.

표 40-1 위협 점수 평가

위협 점수	아이콘	평가
Low	●○○○	1-25
Medium	●●○○	26-50
High	●●●○	51-75
Very High	●●●●	76-100

방어 센터은 파일의 성향과 동일한 시간에 대해 파일의 위협 점수를 로컬에서 캐시합니다. 시스템은 나중에 이러한 파일을 탐지하면 Cisco 클라우드에 다시 쿼리하는 대신 캐시된 위협 점수를 사용자에게 표시합니다. 파일 정책 컨피그레이션을 기반으로, 위협 점수가 정의된 악성코드 임계값 위협 점수를 초과하는 모든 파일에 대해 악성코드 파일 성향을 자동으로 할당할 수 있습니다. 자세한 내용은 37-16페이지의 파일 정책 생성을/를 참조하십시오.

동적 분석 요약

동적 분석 요약을 사용할 수 있는 경우 위협 점수 아이콘을 클릭하여 내용을 볼 수 있습니다. 동적 분석은 VRT(Vulnerability Research Team) 파일 분석에 의해 할당된 전체적인 위협 점수를 구성하는 다양한 구성 요소 등급 및 클라우드가 파일 실행을 시도했을 때 시작된 기타 프로세스에 대해 설명합니다.

여러 보고서가 존재하는 경우, 이 요약은 정확한 위협 점수와 일치하는 최근 보고서를 기반으로 합니다. 정확한 위협 점수와 일치하는 보고서가 없으면 가장 높은 위협 점수의 보고서가 표시됩니다. 보고서가 둘 이상이면 위협 점수를 선택하여 각각의 보고서를 볼 수 있습니다.

요약에는 위협 점수를 구성하는 각 구성 요소 위협이 나열되어 있습니다. VRT에서 발견한 내용 및 이 구성 요소 위협과 관련된 프로세스를 나열하기 위해 각 구성 요소 위협을 확장할 수 있습니다.

프로세스 트리에는 클라우드가 파일 실행을 시도했을 때 시작된 프로세스가 표시됩니다. 이는 악성코드가 포함된 파일이 예상을 뛰어넘어 프로세스 및 시스템 리소스에 대한 액세스를 시도했는지(예: Word 문서를 실행하여 Microsoft Word를 열고, Explorer를 시작한 다음 Java 시작) 여부를 파악하는 데 도움이 될 수 있습니다.

나열된 각 프로세스에는 실제 프로세스 확인에 사용할 수 있는 프로세스 식별자 및 md5 체크섬이 포함되어 있습니다. 프로세스 트리에는 상위 프로세스의 결과 하위 노드로서 시작된 프로세스가 표시됩니다.

동적 분석 요약에서 **View Full Report**를 클릭하여 VRT의 전체 분석이 포함된 VRT Analysis 보고서를 볼 수 있습니다. 여기에는 일반 파일 정보, 탐지된 모든 프로세스에 대한 좀 더 심층적인 검토, 파일 분석의 분류 및 기타 관련 정보가 자세히 나와 있습니다.

파일 이벤트 작업

라이센스: 보호

현재 적용된 파일 정책에 따라, 시스템은 관리되는 디바이스가 네트워크 트래픽에서 파일을 탐지 또는 차단할 때 생성되는 파일 이벤트를 기록합니다. 액세스 제어 규칙을 호출하는 로깅 컨피그레이션과 상관없이, 시스템은 파일 이벤트를 생성할 때 방어 센터 데이터베이스와 관련된 연결의 끝도 기록합니다. 자세한 내용은 37-9페이지의 파일 정책 이해 및 생성을/를 참조하십시오.

참고 네트워크에서 탐지되고 FireSIGHT 시스템에 의해 악성코드로 식별된 파일은 파일 이벤트와 악성코드 이벤트를 모두 생성합니다. 이는 시스템이 파일에서 악성코드를 탐지하려면 파일 자체를 먼저 탐지해야 하기 때문입니다. 엔드포인트 기반 악성코드 이벤트에는 해당하는 파일 이벤트가 없습니다. 자세한 내용은 40-17페이지의 악성코드 이벤트 작업 및 40-30페이지의 캡처된 파일 작업을/를 참조하십시오.

파일 이벤트를 보고 검색하고 삭제하려면 방어 센터의 이벤트 뷰어를 사용할 수 있습니다. 또한 Files Dashboard에서는 네트워크에서 탐지된 파일에 대한 자세한 정보를 차트 및 그래프를 통해 한눈에 볼 수 있습니다. 네트워크 파일 전파 흔적은 개별 파일을 좀 더 심층적으로 보여주며, 파일 및 파일이 시간에 따라 네트워크에서 이동한 방법에 대한 요약 정보를 제공합니다. 파일 식별 데이터를 사용하면 상관관계 규칙을 트리거하고 규칙을 생성할 수 있습니다. 규칙을 생성하는 데에는 사전 정의된 Files Report 템플릿 또는 사용자 지정 보고서 템플릿을 사용할 수 있습니다.

자세한 내용은 다음 링크를 참고하십시오.

- 40-8페이지의 파일 이벤트 보기
- 40-10페이지의 파일 이벤트 테이블 이해
- 58-20페이지의 지오로케이션 사용
- 40-13페이지의 파일 이벤트 검색

파일 이벤트 보기

라이센스: 보호

FireSIGHT 시스템의 이벤트 뷰어를 사용하면 테이블에서 파일 이벤트를 보는 것은 물론, 분석과 관련된 정보에 따라 이벤트 보기를 조작할 수도 있습니다. 모든 개별 파일 이벤트에 대해 사용 가능한 정보는 라이센스를 비롯한 여러 요소에 따라 달라집니다. 자세한 내용은 65-2페이지의 라이센스 유형 및 제한 사항을/를 참조하십시오.

파일 이벤트에 액세스할 때 볼 수 있는 페이지는, 넓은 보기에서 좀 더 집중된 보기로 이동하여 이벤트를 평가하는 데 사용할 수 있는 일련의 페이지인 워크플로에 따라 달라집니다. 시스템은 파일 이벤트에 대한 다음과 같은 사전 정의 워크플로와 함께 제공됩니다.

- *File Summary*(기본값) - 서로 다른 파일 이벤트 카테고리 및 유형을 관련 악성코드 파일 성향과 함께 빠르게 분류하여 제공합니다.
- *Hosts Receiving Files* 및 *Hosts Sending Files* - 파일을 받거나 보낸 호스트의 목록을 해당 파일과 관련된 악성코드 성향별로 그룹화하여 제공합니다.

참고 파일 성향은 시스템이 악성코드 클라우드 조회를 수행한 파일에 대해서만 나타납니다. 37-11페이지의 파일 규칙 작업 및 평가 순서을/를 참조하십시오.

특정 요구와 일치하는 정보만 표시하는 사용자 지정 워크플로를 생성할 수도 있습니다. 사용자 지정 워크플로를 비롯한 서로 다른 기본 워크플로 지정에 대한 자세한 내용은 71-3페이지의 이벤트 보기 설정 구성을/를 참조하십시오.

FireSIGHT 시스템은 이벤트 뷰어, 이벤트 검색, 대시보드, Context Explorer를 비롯한 웹 인터페이스의 모든 영역에서 유니코드(UTF-8) 문자를 사용하는 파일 이름의 표시와 입력을 지원합니다. 그러나 PDF 형식으로 생성하는 보고서는 유니코드를 지원하지 않습니다. 유니코드 파일 이름은 PDF 보고서에 음역 형태로 나타납니다. 자세한 내용은 57-26페이지의 보고서 생성 및 보기을/를 참조하십시오. SMB 프로토콜은 유니코드 파일 이름을 인쇄 가능한 문자로 변환합니다. SMB를 통해 탐지한, 유니코드 파일 이름이 있는 파일은 인쇄할 수 없는 문자 자리가 마침표(.)로 나타납니다.

이벤트 뷰어를 사용할 경우 다음을 수행할 수 있습니다.

- 이벤트 검색, 정렬 및 제한은 물론 표시된 이벤트에 대한 시간 범위를 변경할 수 있습니다.
- 나타나는 열을 지정할 수 있습니다(테이블 보기 전용).
- IP 주소와 연결된 호스트 프로필을 보거나, 사용자 ID와 연결된 사용자 세부사항 및 호스트 기록을 볼 수 있습니다.
- 특정 파일이 탐지된 연결을 볼 수 있습니다.
- 동일한 워크플로 내에서 서로 다른 워크플로 페이지를 사용하여 이벤트를 볼 수 있습니다.
- 다른 워크플로를 사용하는 여러 이벤트를 함께 볼 수 있습니다.
- 특정 값으로 제한하여 워크플로 내에서 페이지 간에 드릴다운할 수 있습니다.
- 나중에 동일한 데이터(데이터가 그대로 있을 경우)로 돌아올 수 있도록 현재 페이지 및 제약 조건을 북마크 처리할 수 있습니다.
- 파일과 관련된 라우팅 가능한 IP 주소에 대한 보내는/받는 국가와 대륙을 볼 수 있습니다.
- 파일의 전파 흔적을 볼 수 있습니다.
- 파일 목록에 파일을 추가하고, 파일을 다운로드하고, 동적 분석을 위해 파일을 제출하고, 파일의 SHA-256 값의 전체 텍스트를 볼 수 있습니다.
- 사용 가능한 경우 파일의 Dynamic Analysis Summary 보고서를 볼 수 있습니다.
- 아카이브 파일 내 중첩된 파일을 볼 수 있습니다.
- 현재 제약 조건을 사용하여 보고서 템플릿을 생성할 수 있습니다.
- 데이터베이스에서 이벤트를 삭제할 수 있습니다.
- IP 주소 컨텍스트 메뉴를 사용하여 파일 이벤트와 연결된 호스트 또는 IP 주소에 대해 사용 가능한 추가 정보를 얻거나, 화이트리스트 또는 블랙리스트를 작성할 수 있습니다.

사용자 지정 워크플로 생성을 포함하여 이벤트 뷰어 사용에 대한 자세한 내용은 58-1페이지의 워크플로의 이해 및 사용을/를 참조하십시오.

특정 파일이 탐지된 연결을 신속하게 보려면 이벤트 뷰어의 확인란을 사용하여 파일을 선택한 다음 **Jump to** 드롭다운 목록에서 **Connections Events**를 선택합니다. 자세한 내용은 58-35페이지의 워크플로 간 이동을/를 참조하십시오.

파일 이벤트를 보려면

액세스: Admin/Any Security Analyst

1단계 **Analysis > Files > File Events**를 선택합니다.

기본 파일 이벤트 워크플로의 첫 번째 페이지가 나타납니다. 나타나는 열에 대한 자세한 내용은 40-10페이지의 파일 이벤트 테이블 이해을/를 참조하십시오.

파일 이벤트 테이블 이해

라이센스: 보호

적용된 파일 정책의 설정에 따라, 방어 센터는 관리되는 디바이스가 모니터링되는 네트워크 트래픽에서 전송되는 파일을 탐지 또는 차단할 때 파일 이벤트를 기록합니다.

사전 정의된 파일 이벤트 워크플로의 마지막 페이지이며 사용자 지정 워크플로에 추가할 수 있는 파일 이벤트의 테이블 보기에는 파일 테이블의 각 필드에 대한 열이 포함됩니다. 파일 이벤트의 테이블 보기에서 일부 필드는 기본적으로 비활성화되어 있습니다. 세션 중에 필드를 활성화하려면 확장 화살표( )를 클릭하여 검색 제약 조건을 확장한 다음 **Disabled Columns** 아래에서 열 이름을 클릭합니다.

모든 개별 파일 이벤트에 대해 사용 가능한 정보는 라이센스를 비롯한 여러 요소에 따라 달라집니다. 예를 들어 파일 제어는 보호 라이센스로만 수행할 수 있지만, 악성코드 라이센스를 사용하면 특정 파일 형식에 대해 AMP를 수행하고 네트워크에서 전송된 파일을 추적할 수 있습니다.

다음 표에서는 파일 이벤트 필드에 대해 설명합니다.

표 40-2 파일 이벤트 필드

필드	설명
Time	이벤트가 생성된 날짜 및 시간.
Action	파일을 탐지한 파일 정책 규칙과 연결된 작업 및 관련된 모든 파일 작업 옵션.
Sending IP	탐지된 파일을 전송하는 호스트의 IP 주소.
Sending Country	탐지된 파일을 전송하는 호스트의 국가. DC500 방어 센터에서는 이 기능을 지원하지 않습니다.
Receiving IP	탐지된 파일을 수신하는 호스트의 IP 주소.
Receiving Country	탐지된 파일을 수신하는 호스트의 국가. DC500 방어 센터에서는 이 기능을 지원하지 않습니다.
Sending Port	파일이 탐지된 트래픽에 의해 사용된 소스 포트.
Receiving Port	파일이 탐지된 트래픽에 의해 사용된 목적지 포트.

표 40-2 파일 이벤트 필드(계속)

필드	설명
SSL Status	SSL 규칙, 기본 작업 또는 암호화된 연결을 로깅한 해독 불가능한 트래픽 작업과 관련된 작업입니다. • `Block` 및 `Block with reset` - 차단된 암호화 연결을 나타냅니다. • `Decrypt (Resign)` - 다시 서명된 서버 인증서를 사용하여 해독된 발신 연결을 나타냅니다. • `Decrypt (Replace Key)` - 대체된 공개 키가 있는 자체 서명된 서버 인증서를 사용하여 해독된 발신 연결을 나타냅니다. • `Decrypt (Known Key)` - 알려진 개인 키를 사용하여 해독된 수신 연결을 나타냅니다. • `Default Action` - 연결이 기본 작업에 의해 처리되었음을 나타냅니다. • `Do not Decrypt` - 시스템이 해독하지 못한 연결을 나타냅니다. 시스템이 암호화된 연결을 해독하지 못할 경우, 해독 불가능한 트래픽 작업이 실행되었다는 내용과 함께 실패 사유가 표시됩니다. 시스템이 알려지지 않은 암호 그룹으로 암호화 트래픽을 탐지한 후 추가 검사 없이 허용한 경우 이 필드에는 `Do Not Decrypt (Unknown Cipher Suite)`가 표시됩니다. 인증서 세부사항을 보려면 잠금 아이콘( )을 클릭합니다. 자세한 내용은 39-32페이지의 암호화된 연결과 관련된 인증서 보기을/를 참조하십시오.
User	파일의 목적지인 호스트(**Receiving IP**)에 로그인한 사용자. 사용자는 대상 호스트와 연결되어 있으므로, 파일을 업로드한 파일 이벤트와는 연결되지 않습니다.
File Name	파일의 이름.
Disposition	다음 파일 성향 중 하나: • `Malware` - 클라우드가 파일을 악성코드로 분류했으며 파일의 위협 점수가 파일 정책에 정의된 악성코드 임계값을 초과했음을 나타냅니다. • `Clean` - 클라우드가 파일을 정상으로 분류했거나, 사용자가 파일을 정상 목록에 추가했음을 나타냅니다. • `Unknown` - 클라우드가 성향을 할당하기 전에 악성코드 클라우드 조회가 발생했음을 나타냅니다. 파일이 분류되지 않습니다. • `Custom Detection` - 사용자가 파일을 사용자 지정 탐지 목록에 추가했음을 나타냅니다. • `Unavailable` - 방어 센터에서 악성코드 클라우드 조회를 수행할 수 없음을 나타냅니다. 이 성향의 이벤트는 비율이 낮을 수 있는데, 이는 정상적인 상황입니다. • `N/A` - Detect Files 또는 Block Files 규칙이 파일을 처리했으며 방어 센터에서 악성코드 클라우드 조회를 수행하지 않았음을 나타냅니다.

표 40-2 파일 이벤트 필드(계속)

필드	설명
SHA256	파일의 SHA-256 해시 값. 파일이 다음의 결과로 탐지된 경우 최근에 탐지된 파일 이벤트 및 파일 성향을 나타내는 네트워크 파일 전파 흔적 아이콘: • **Store Files**가 활성화된 Detect Files 파일 규칙 • **Store Files**가 활성화된 Block Files 파일 규칙 • Malware Cloud Lookup 파일 규칙 • Block Malware 파일 규칙 네트워크 파일 전파 흔적을 보려면 전파 흔적 아이콘을 클릭합니다. 자세한 내용은 40-38페이지의 네트워크 파일 전파 흔적 분석을/를 참조하십시오.
Threat Score	이 파일과 가장 최근에 연결된 위협 점수. • `Low`(●○○○) • `Medium`(●●○○) • `High`(●●●○) • `Very High`(●●●●) Dynamic Analysis Summary 보고서를 보려면 위협 점수 아이콘을 클릭합니다.
Type	`HTML` 또는 `MSEXE` 등의 파일 형식.
Category	다음과 같은 파일 형식의 일반 카테고리: `Office Documents`, `Archive`, `Multimedia`, `Executables`, `PDF files`, `Encoded`, `Graphics` 또는 `System Files`.
Size(KB)	킬로바이트 단위의 파일 크기. 파일을 완전히 수신하기 전에 시스템에서 파일의 형식을 결정하는 경우 파일 크기가 계산되지 않을 수 있고 따라서 이 필드는 비어 있게 됩니다.
URI	파일의 원래 URI(예: 사용자가 파일을 다운로드한 URL)
Archive Name	파일과 연결된 아카이브 파일(있는 경우)의 이름(예: `archive.zip`). 아카이브 파일의 내용을 보려면 아카이브 파일의 이벤트 뷰어 행을 마우스 오른쪽 버튼으로 클릭하여 컨텍스트 메뉴를 열고 **View Archive Contents**를 클릭합니다. 자세한 내용은 37-22페이지의 아카이브 파일의 내용 보기을/를 참조하십시오.
Archive SHA256	파일과 연결된 아카이브 파일(있는 경우)의 SHA-256 해시 값.
Archive Depth	아카이브 파일에서 파일이 중첩된 레벨(있는 경우)(예: `1` 또는 `3`).
Application Protocol	관리되는 디바이스가 파일을 탐지한 트래픽에 의해 사용된 애플리케이션 프로토콜.
Application Protocol, Client, Web Application Category or Tag	애플리케이션 기능 이해에 도움이 되도록 애플리케이션의 특성을 부여하는 기준. 45-11 페이지의 표 45-2을/를 참조하십시오.
Client	파일을 전송하기 위한 연결에서 사용된 클라이언트 애플리케이션.
Web Application	HTTP를 사용하여 전송된 파일의 경우, 연결에서 탐지되고 파일 전송에 사용된 웹 애플리케이션(콘텐츠 또는 요청된 URL).
Application Risk	연결에서 탐지된 애플리케이션 트래픽과 관련된 위험: `Very High`, `High`, `Medium`, `Low` 또는 `Very Low`. 연결에서 탐지된 각 유형의 애플리케이션에는 관련 위험도가 포함되며, 이 필드에는 가장 높은 순서부터 표시됩니다. 자세한 내용은 45-11 페이지의 표 45-2을/를 참조하십시오.

표 40-2 파일 이벤트 필드(계속)

필드	설명
Business Relevance	연결에서 탐지된 애플리케이션 트래픽과 관련된 비즈니스 관련성(Very High, High, Medium, Low, Very Low)입니다. 연결에서 탐지된 각 애플리케이션 유형에는 관련된 비즈니스 연관성이 있습니다. 이 필드에는 그중 가장 낮은 값(가장 연관성이 적음)이 표시됩니다. 자세한 내용은 45-11 페이지의 표 45-2을/를 참조하십시오.
Message	악성코드 성향이 변경된 파일의 경우, 즉 소급 악성코드 이벤트와 연결된 파일의 경우, 성향이 언제 어떻게 변경되었는지에 대한 정보.
File Policy	파일을 탐지한 파일 정책.
Device	파일을 탐지한 디바이스의 이름.
Security Context	트래픽이 통과된 가상 방화벽 그룹을 식별하는 메타데이터입니다. 이 필드는 다중 컨텍스트 모드의 ASA FirePOWER 디바이스에 대해서만 채워집니다.
Count	각 행의 정보와 일치하는 이벤트의 수. 둘 이상의 동일한 행을 생성하는 제약 조건을 적용한 경우에만 이 필드가 나타납니다.

파일 이벤트 검색

라이센스: 보호

방어 센터의 Search 페이지를 사용하면 특정 파일 이벤트를 검색하고, 이벤트 뷰어에 결과를 표시하고, 나중에 다시 사용할 수 있도록 검색 기준을 저장할 수 있습니다. Custom Analysis 대시보드 위젯, 보고서 템플릿, 사용자 지정 사용자 역할도 저장된 검색을 사용할 수 있습니다.

검색 결과는 검색 중인 이벤트에서 사용할 수 있는 데이터에 따라 달라집니다. 다시 말하면, 사용 가능한 데이터에 따라 검색 제한이 적용되지 않을 수 있습니다. 예를 들어 **Disposition** 및 **SHA256** 필드는 방어 센터에서 악성코드 클라우드 검색을 수행한 파일에 대해서만 채워집니다.

일반 검색 구문

각 검색 필드 옆에는 유효한 구문의 예가 표시됩니다. 검색 기준을 입력할 경우, 다음 사항에 유의해야 합니다.

- 모든 필드에 부정(!)을 사용할 수 있습니다.
- 모든 필드에 쉼표로 구분된 검색 값의 목록을 사용할 수 있습니다. 지정된 필드에 나열된 값 중 하나를 포함하는 레코드는 검색 기준과 일치합니다.
- 모든 필드에 따옴표로 감싸고 쉼표로 구분한 목록을 검색 값으로 사용할 수 있습니다.
  - 단일 값만을 포함할 수 있는 필드의 경우, 따옴표 내에 지정된 정확한 문자열을 포함하는 지정된 필드의 레코드가 검색 기준과 일치합니다. 예를 들어 `A, B, "C, D, E"`에 대한 검색은 지정된 필드에 `"A"` 또는 `"B"` 또는 `"C, D, E"`가 포함된 레코드와 일치합니다. 따라서 가능한 값으로 쉼표를 포함하는 필드에서 일치를 확인할 수 있습니다.
  - 여러 값을 동시에 포함할 수 있는 필드의 경우, 따옴표로 감싸고 쉼표로 구분한 모든 값을 포함하는 지정된 필드의 레코드가 해당 검색 기준과 일치합니다.
  - 여러 값을 동시에 포함할 수 있는 필드의 경우, 검색 기준에 단일 값은 물론 따옴표로 감싸고 쉼표로 구분한 목록도 포함할 수 있습니다. 예를 들어 하나 이상의 이러한 문자를 포함할 수 있는 필드에서 `A, B, "C, D, E"`에 대한 검색은 지정된 필드에 `A` 또는 `B`, 또는 `C`, `D`, `E` 모두가 포함된 레코드와 일치합니다.
- 검색 결과에는 모든 필드에 지정된 검색 기준과 매칭되는 레코드만 반환됩니다.
- 많은 필드에서 와일드카드로 하나 이상의 별표(*)를 사용할 수 있습니다.

- 해당 필드에 대해 사용할 수 있는 정보가 없는 이벤트를 식별하려면 필드에 n/a를 지정합니다. 해당 필드가 채워지는 이벤트를 식별하려면 !n/a를 사용합니다.
- 특정 디바이스 및 그룹, 스택 또는 클러스터의 디바이스를 검색하려면 디바이스 필드를 사용합니다. FireSIGHT 시스템에서 검색 시 디바이스 필드를 취급하는 방법에 대한 자세한 내용은 60-7페이지의 검색에서 디바이스 지정을/를 참조하십시오.
- 검색 기준으로 객체를 사용하려면 검색 필드 옆에 나타나는 객체 추가 아이콘(+)을 클릭합니다.

검색에서 객체를 사용하는 방법을 포함하여 검색 구문에 대한 자세한 내용은 60-1페이지의 이벤트 검색을/를 참조하십시오.

파일 이벤트용 특수 검색 구문

위에 나열된 일반 검색 구문을 보완하기 위해 다음 목록에서는 파일 이벤트용 특수 검색 구문 몇 가지에 대해 설명합니다.

Sending/Receiving Continent

시스템은 **Sending Continent** 또는 **Receiving Continent**가 사용자가 지정한 대륙과 일치하는 모든 이벤트를 반환합니다.

Sending/Receiving 국가

시스템은 **Sending Country** 또는 **Receiving Country**가 사용자가 지정한 국가와 일치하는 모든 이벤트를 반환합니다.

Sending/Receiving IP

시스템은 **Sending IP** 또는 **Receiving IP**가 사용자가 지정한 IP 주소와 일치하는 모든 이벤트를 반환합니다.

URI 또는 메시지

시스템에서는 부분 매칭을 수행하므로, 별표를 사용하지 않고도 필드 내용의 전체 또는 부분을 검색할 수 있습니다.

파일 스토리지

다음 중 하나 이상을 입력하십시오.

- Stored - 관련된 파일이 현재 저장되어 있는 모든 이벤트를 반환합니다.
- Stored in connection - 관련된 파일이 현재 저장되어 있는지와 상관없이, 시스템이 관련된 파일을 캡처 및 저장한 모든 이벤트를 반환합니다.
- Failed - 시스템이 관련된 파일을 저장하지 못한 모든 이벤트를 반환합니다.

수행한 SSL Actual Action

시스템이 지정된 작업을 적용한 암호화 트래픽에 대한 파일 이벤트를 보려면 다음 키워드 중 하나를 입력하십시오.

- Do Not Decrypt - 시스템이 해독하지 못한 연결을 나타냅니다.
- Block 및 Block with Reset - 차단된 암호화 연결을 나타냅니다.
- Decrypt (Known Key) - 알려진 개인 키를 사용하여 해독된 수신 연결을 나타냅니다.
- Decrypt (Replace Key) - 대체된 공개 키가 있는 자체 서명된 서버 인증서를 사용하여 해독된 발신 연결을 나타냅니다.
- Decrypt (Resign) - 다시 서명된 서버 인증서를 사용하여 해독된 발신 연결을 나타냅니다.

이 열은 파일 이벤트 테이블 보기에 나타나지 않습니다.

SSL Failure Reason

지정된 이유로 시스템이 해독에 실패한 암호화 트래픽에 대한 파일 이벤트를 보려면 다음 키워드 중 하나를 입력하십시오.

- Unknown
- No Match
- Success
- Uncached Session
- Unknown Cipher Suite
- Unsupported Cipher Suite
- Unsupported SSL Version
- SSL Compression Used
- Session Undecryptable in Passive Mode
- Handshake Error
- Decryption Error
- Pending Server Name Category Lookup
- Pending Common Name Category Lookup
- Internal Error
- Network Parameters Unavailable
- Invalid Server Certificate Handle
- Server Certificate Fingerprint Unavailable
- Cannot Cache Subject DN
- Cannot Cache Issuer DN
- Unknown SSL Version
- External Certificate List Unavailable
- External Certificate Fingerprint Unavailable
- Internal Certificate List Invalid
- Internal Certificate List Unavailable
- Internal Certificate Unavailable
- Internal Certificate Fingerprint Unavailable
- Server Certificate Validation Unavailable
- Server Certificate Validation Failure
- Invalid Action

이 열은 파일 이벤트 테이블 보기에 나타나지 않습니다.

SSL Subject Country

인증서 주체의 국가와 연결된 암호화 트래픽에 대한 파일 이벤트를 보려면 두 글자의 ISO 3166-1 alpha-2 국가 코드를 입력하십시오.

이 열은 파일 이벤트 테이블 보기에 나타나지 않습니다.

SSL Issuer Country

인증서 발급자의 국가와 연결된 암호화 트래픽에 대한 파일 이벤트를 보려면 두 글자의 ISO 3166-1 alpha-2 국가 코드를 입력하십시오.

이 열은 파일 이벤트 테이블 보기에 나타나지 않습니다.

SSL Certificate Fingerprint

인증서와 연결된 트래픽에 대한 파일 이벤트를 보려면 해당 인증서의 인증에 사용된 SHA 해시 값을 입력하거나 붙여넣으십시오.

이 열은 파일 이벤트 테이블 보기에 나타나지 않습니다.

SSL Public Key Fingerprint

인증서와 연결된 트래픽에 대한 파일 이벤트를 보려면 해당 인증서 내에 포함된 공개 키의 인증에 사용된 SHA 해시 값을 입력하거나 붙여넣으십시오.

이 열은 파일 이벤트 테이블 보기에 나타나지 않습니다.

파일 이벤트를 검색하려면

액세스: Admin/Any Security Analyst

1단계 **Analysis > Search**를 선택합니다.

Search 페이지가 나타납니다.

2단계 테이블 드롭다운 목록에서 **File Events**를 선택합니다.

해당 제약 조건으로 페이지가 업데이트됩니다.

3단계 다음 절의 설명에 따라 해당 필드에 검색 기준을 입력합니다.

- 파일 이벤트 테이블에 있는 필드에 대한 자세한 내용은 파일 이벤트 필드 표를 참조하십시오.
- 파일 이벤트용 특수 검색 구문은40-14페이지의 파일 이벤트용 특수 검색 구문을/를 참조하십시오.
- 공개 키 인증서와 관련된 필드는39-32페이지의 암호화된 연결과 관련된 인증서 보기을/를 참조하십시오.

4단계 선택적으로, 검색을 저장하려면 **Private** 확인란을 선택하여 자신만 액세스할 수 있는 비공개로 검색을 저장할 수 있습니다. 또는 모든 사용자가 사용할 수 있도록 검색을 저장하려면 확인란을 선택하지 않습니다.

팁 사용자 지정 사용자 역할에 대한 데이터 제한으로서 검색을 사용하려면 **반드시** 비공개 검색으로 저장해야 합니다.

5단계 선택적으로, 나중에 다시 사용할 수 있도록 검색을 저장할 수 있습니다. 다음 옵션을 이용할 수 있습니다.

- 검색 기준을 저장하려면 **Save**를 클릭합니다.

  새 검색인 경우 검색 이름을 입력하도록 대화 상자가 나타납니다. 고유한 검색 이름을 입력하고 **Save**를 클릭합니다. 이미 존재하는 검색에 대한 새 조건을 저장하는 경우 프롬프트가 나타나지 않습니다. 나중에 실행할 수 있도록 검색이 저장됩니다(**Private**을 선택한 경우 자신만 볼 수 있음).

- 새 검색을 저장하거나, 저장된 기존 검색을 변경하여 만든 검색에 새 이름을 할당하려면 **Save As New**를 클릭합니다.

  검색 이름을 입력하도록 대화 상자가 나타납니다. 고유한 검색 이름을 입력하고 **Save**를 클릭합니다. 나중에 실행할 수 있도록 검색이 저장됩니다(**Private**을 선택한 경우 자신만 볼 수 있음).

6단계 검색을 시작하려면 **Search**를 클릭합니다.

검색 결과는 현재의 시간 범위로 제한되어 기본 파일 이벤트 워크플로에 나타납니다.

악성코드 이벤트 작업

라이센스: 악성코드 또는 모두

지원되는 디바이스: 기능에 따라 다름

지원되는 Defense Center: 기능에 따라 다름

시스템은 다음과 같은 경우 악성코드 이벤트를 방어 센터 데이터베이스에 기록합니다.

- 관리되는 디바이스가 네트워크 트래픽에서 파일을 탐지했는데, 해당 파일이 악성코드 클라우드 조회에서 악성코드로 식별된 경우
- 관리되는 디바이스가 네트워크 트래픽의 사용자 지정 탐지 목록에서 파일을 탐지한 경우
- 파일의 악성코드 성향이 변경된 것을 시스템이 파악한 경우. 이를 소급 악성코드 이벤트라고 부릅니다.
- 조직의 엔드포인트에 설치된 FireAMP Connector가 위협을 탐지하고, 해당 위협을 Cisco 클라우드에 알린 경우

FireAMP 악성코드 탐지는 다운로드 시 또는 실행 시 엔드포인트에서 수행되며 관리되는 디바이스는 네트워크 트래픽에서 파일을 탐지하므로, 이러한 악성코드 이벤트에 있는 정보는 다릅니다. 소급 악성코드 이벤트는 다른 네트워크 기반 악성코드 이벤트 또는 엔드포인트 기반 악성코드 이벤트와 약간 다른 데이터를 포함할 수 있습니다.

다음 절에서는 서로 다른 종류의 악성코드 이벤트에 대해 간략하게 설명합니다. 전체적인 악성코드 탐지 프로세스에 대한 자세한 내용은 37-2페이지의 악성코드 차단 및 파일 제어 이해을/를 참조하십시오.

엔드포인트 기반(FireAMP) 악성코드 이벤트

조직에 FireAMP 서브스크립션이 있는 경우 개별 사용자는 컴퓨터와 모바일 디바이스에 FireAMP Connector를 설치할 수 있습니다. 이와 같이 가벼운 에이전트는 Cisco 클라우드와 통신하며, Cisco 클라우드는 방어 센터와 통신합니다. 37-24페이지의 FireAMP를 위한 클라우드 연결 작업을/를 참조하십시오. 클라우드는 위협의 알림은 물론 스캔, 격리, 차단된 실행, 클라우드 다시 호출에 대한 데이터 등 다른 유형의 정보도 전송할 수 있습니다. 방어 센터는 이러한 정보를 데이터베이스에 악성코드 이벤트로 기록합니다.

참고 엔드포인트 기반 악성코드 이벤트에서 보고된 IP 주소는 네트워크 맵에 없을 수 있으며, 모니터링되는 네트워크에도 없을 수 있습니다. 구축, 규정준수 레벨 및 기타 요소에 따라, FireAMP Connector가 설치된 조직의 엔드포인트는 관리되는 디바이스에서 모니터링하는 호스트와 같은 호스트가 아닐 수 있습니다.

네트워크 트래픽 기반 악성코드 이벤트

지원되는 디바이스: Series 2 또는 X-Series를 제외한 모두

지원되는 Defense Center: DC500을 제외한 모든 방어 센터

악성코드 라이센스의 경우 관리되는 디바이스는 전체적인 액세스 제어 컨피그레이션의 일부로서 네트워크 트래픽에서 악성코드를 탐지할 수 있습니다. 37-9페이지의 파일 정책 이해 및 생성을/를 참조하십시오.

다음 시나리오는 악성코드 이벤트 생성으로 이어질 수 있습니다.

- 관리되는 디바이스가 특정 파일 형식 집합 중 하나를 탐지한 경우 방어 센터는 악성코드 클라우드 조회를 수행하며, 그 결과 `Malware`, `Clean` 또는 `Unknown`의 파일 성향이 방어 센터에 반환됩니다.

- 방어 센터가 클라우드와 연결할 수 없거나 다른 이유로 클라우드를 사용할 수 없는 경우 파일 성향은 Unavailable이 됩니다. 이 성향의 이벤트는 비율이 낮을 수 있는데, 이는 정상적인 상황입니다.
- 파일과 관련된 위협 점수가 파일을 탐지한 파일 정책에 정의된 악성코드 임계값 위협 점수를 초과하면 방어 센터는 파일에 Malware의 파일 성향을 할당합니다.
- 관리되는 디바이스가 SHA-256 값이 사용자 지정 탐지 목록에 저장된 파일을 탐지하면 방어 센터는 파일에 Custom Detection의 파일 성향을 할당합니다.
- 관리되는 디바이스가 정상 목록의 파일을 탐지하면 방어 센터는 파일에 Clean의 파일 성향을 할당합니다.

방어 센터는 파일의 탐지 및 성향 레코드를 기타 컨텍스트 데이터와 함께 악성코드 이벤트로서 기록합니다.

참고 네트워크에서 탐지되고 FireSIGHT 시스템에 의해 악성코드로 식별된 파일은 파일 이벤트와 악성코드 이벤트를 모두 생성합니다. 이는 시스템이 파일에서 악성코드를 탐지하려면 파일 자체를 먼저 탐지해야 하기 때문입니다. 자세한 내용은 40-8페이지의 파일 이벤트 작업 및 40-30페이지의 캡처된 파일 작업을/를 참조하십시오.

소급 악성코드 이벤트

지원되는 디바이스: Series 3, 가상

지원되는 Defense Center: DC500을 제외한 모든 방어 센터

네트워크 트래픽에서 탐지된 악성코드 파일의 경우 파일 성향이 변경될 수 있습니다. 예를 들어, Cisco 클라우드는 전에 정상인 것으로 식별되었던 파일이 지금은 악성코드로 식별되는 경우 또는 그 반대의 경우(악성코드로 식별된 파일이 실제로 정상임)를 결정할 수 있습니다.

지난주에 악성코드 조회를 수행한 파일에 대해 파일 성향이 변경되면 클라우드는 이를 방어 센터에 알립니다. 그러면 두 가지가 발생합니다.

- 방어 센터는 새로운 소급 악성코드 이벤트를 생성합니다.

  이 새로운 소급 악성코드 이벤트는 동일한 SHA-256 해시 값을 갖는, 지난주 탐지된 모든 파일에 대한 성향 변경을 나타냅니다. 따라서 이러한 이벤트에는 방어 센터에서 성향 변경을 알린 날짜와 시간, 새로운 성향, 파일의 SHA-256 해시 값 및 위협 이름 등 제한된 정보가 포함됩니다. IP 주소나 기타 컨텍스트 정보는 포함되지 않습니다.

- 방어 센터는 전에 탐지된 파일에 대한 파일 성향을 소급 이벤트와 관련된 SHA-256 해시 값으로 변경합니다.

  파일의 성향이 Malware로 변경되면 방어 센터는 새 악성코드 이벤트를 데이터베이스에 기록합니다. 새 성향 외에도 이 새 악성코드 이벤트의 정보는 파일을 처음 탐지했을 때 생성된 파일 이벤트의 정보와 동일합니다.

  파일의 성향이 Clean으로 변경되면 방어 센터는 악성코드 이벤트를 악성코드 테이블에서 제거하지 않습니다. 대신 해당 이벤트는 단지 성향의 변경 사항을 반영합니다. 즉, Clean 성향의 파일은 악성코드 테이블에 나타날 수 있지만, 이는 원래 악성코드로 파악된 경우에 한합니다. 전에 악성코드로 식별된 적이 없는 파일은 파일 테이블에만 나타납니다.

  어느 경우든 악성코드 이벤트의 **Message**는 성향이 변경된 방법과 시기를 나타냅니다. 예를 들면 다음과 같습니다.

  ```
  Retrospective Event, Mon Oct 1 20:44:00 2012 (UTC), Old Disp: Unknown, New Disp:
  Malware
  ```

악성코드 이벤트 사용

악성코드 이벤트를 보고 검색하고 삭제하려면 방어 센터의 이벤트 뷰어를 사용할 수 있습니다. 또한 Files Dashboard 및 Context Explorer에서는 네트워크에서 탐지된 파일(악성코드 파일 포함)과 관련한 자세한 정보를 차트 및 그래프를 통해 한눈에 볼 수 있습니다. 네트워크 파일 전파 흔적은 개별 악성코드 파일을 좀 더 심층적으로 보여주며, 파일 및 파일이 시간에 따라 네트워크에서 이동한 방법에 대한 요약 정보를 제공합니다. 악성코드 탐지 데이터를 사용하면 상관관계 규칙을 트리거하고 규칙을 생성할 수 있습니다. 규칙을 생성하는 데에는 사전 정의된 Malware Report 템플릿 또는 사용자 지정 보고서 템플릿을 사용할 수 있습니다.

자세한 내용은 다음 링크를 참고하십시오.

- 40-19페이지의 악성코드 이벤트 보기
- 40-21페이지의 악성코드 이벤트 테이블 이해
- 40-26페이지의 악성코드 이벤트 검색

악성코드 이벤트 보기

라이센스: 악성코드 또는 모두

FireSIGHT 시스템의 이벤트 뷰어를 사용하면 테이블에서 악성코드 이벤트를 보는 것은 물론, 분석과 관련된 정보에 따라 이벤트 보기를 조작할 수도 있습니다. 모든 개별 악성코드 이벤트에 대해 사용 가능한 정보는 라이센스를 비롯한 여러 요소에 따라 달라집니다. 자세한 내용은 65-2페이지의 라이센스 유형 및 제한 사항을/를 참조하십시오.

악성코드 이벤트에 액세스할 때 볼 수 있는 페이지는, 넓은 보기에서 좀 더 집중된 보기로 이동하여 이벤트를 평가하는 데 사용할 수 있는 일련의 페이지인 워크플로에 따라 달라집니다. 시스템은 악성코드 이벤트에 대한 다음과 같은 사전 정의 워크플로와 함께 제공됩니다.

- *Malware Summary*(기본값) - 탐지된 악성코드의 목록을 개별 위협별로 그룹화하여 제공합니다.
- *Malware Event Summary* - 서로 다른 악성코드 이벤트 유형 및 하위 유형을 빠르게 분류하여 제공합니다.
- *Hosts Receiving Malware* 및 *Hosts Sending Malware* - 악성코드를 받거나 보낸 호스트의 목록을 해당 파일과 관련된 악성코드 성향별로 그룹화하여 제공합니다. 성향은 Malware Cloud Lookup 또는 Block Malware 파일 규칙의 결과로서 탐지된 파일에 대해서만 나타납니다.
- *Applications Introducing Malware* - 조직의 엔드포인트에서 탐지된 악성코드에 액세스하거나 악성코드를 실행한 클라이언트 애플리케이션의 목록을 제공합니다. 이 목록으로부터 각 상위 클라이언트에서 액세스한 개별 악성코드 파일로 드릴다운할 수 있습니다.

특정 요구와 일치하는 정보만 표시하는 사용자 지정 워크플로를 생성할 수도 있습니다. 사용자 지정 워크플로를 비롯한 서로 다른 기본 워크플로 지정에 대한 자세한 내용은 71-3페이지의 이벤트 보기 설정 구성을/를 참조하십시오.

FireSIGHT 시스템은 이벤트 뷰어, 이벤트 검색, 대시보드, Context Explorer를 비롯한 웹 인터페이스의 모든 영역에서 유니코드(UTF-8) 파일 이름의 표시와 입력을 지원합니다. 그러나 PDF 형식으로 생성하는 보고서는 유니코드를 지원하지 않습니다. 유니코드 파일 이름은 PDF 보고서에 음역 형태로 나타납니다. 자세한 내용은 57-26페이지의 보고서 생성 및 보기을/를 참조하십시오.

이벤트 뷰어를 사용할 경우 다음을 수행할 수 있습니다.

- 이벤트 검색, 정렬 및 제한은 물론 표시된 이벤트에 대한 시간 범위를 변경할 수 있습니다.
- 나타나는 열을 지정할 수 있습니다(테이블 보기 전용).
- IP 주소와 연결된 호스트 프로필을 보거나, 사용자 ID와 연결된 사용자 세부사항 및 호스트 기록을 볼 수 있습니다.

- 특정 악성코드가 탐지된 연결을 볼 수 있습니다(네트워크 기반 악성코드 이벤트 전용).
- 동일한 워크플로 내에서 서로 다른 워크플로 페이지를 사용하여 이벤트를 볼 수 있습니다.
- 다른 워크플로를 사용하는 여러 이벤트를 함께 볼 수 있습니다.
- 특정 값으로 제한하여 워크플로 내에서 페이지 간에 드릴다운할 수 있습니다.
- 나중에 동일한 데이터(데이터가 그대로 있을 경우)로 돌아올 수 있도록 현재 페이지 및 제약 조건을 북마크 처리할 수 있습니다.
- 파일과 연결된 라우팅 가능한 IP 주소에 대한 지오로케이션 정보를 볼 수 있습니다.
- 파일의 전파 흔적을 볼 수 있습니다.
- 아카이브 파일 내 중첩된 파일을 볼 수 있습니다.
- 현재 제약 조건을 사용하여 보고서 템플릿을 생성할 수 있습니다.
- 데이터베이스에서 이벤트를 삭제할 수 있습니다.
- 파일 목록에 파일을 추가하고, 파일을 다운로드하고, 동적 분석을 위해 파일을 제출하고, 파일의 SHA-256 값의 전체 텍스트를 볼 수 있습니다.
- 사용 가능한 경우 파일의 Dynamic Analysis Summary 보고서를 볼 수 있습니다.
- IP 주소 컨텍스트 메뉴를 사용하여 악성코드 이벤트와 연결된 호스트 또는 IP 주소에 대해 사용 가능한 추가 정보를 얻거나, 화이트리스트 또는 블랙리스트를 작성할 수 있습니다.

Series 2 디바이스, Cisco NGIPS for Blue Coat X-Series 및 DC500 방어 센터는 네트워크 기반 악성코드 차단 또는 아카이브 파일 검사를 지원하지 않으며, 이는 표시되는 데이터에 영향을 미칠 수 있습니다. Series 2 디바이스만 관리하는 Series 3 방어 센터는 엔드포인트 기반 악성코드 이벤트만 표시할 수 있습니다.

사용자 지정 워크플로 생성을 포함하여 이벤트 뷰어 사용에 대한 자세한 내용은 58-1페이지의 워크플로의 이해 및 사용을/를 참조하십시오.

악성코드 이벤트를 보려면

액세스: Admin/Any Security Analyst

1단계 **Analysis > Files > Malware Events**를 선택합니다.

기본 악성코드 이벤트 워크플로의 첫 번째 페이지가 나타납니다. 나타나는 열에 대한 자세한 내용은 40-21페이지의 악성코드 이벤트 테이블 이해을/를 참조하십시오.

악성코드 이벤트 테이블 이해

라이센스: 악성코드 또는 모두

지원되는 디바이스: 기능에 따라 다름

지원되는 Defense Center: 기능에 따라 다름

조직의 엔드포인트에 설치된 FireAMP Connector가 위협을 탐지하거나 관리되는 디바이스가 네트워크 트래픽에서 파일을 탐지한 후 해당 파일이 악성코드 클라우드 조회에 의해 악성코드로 식별된 경우, 시스템은 방어 센터 데이터베이스에 악성코드 이벤트를 기록합니다. 시스템은 또한 파일의 악성코드 성향이 변경된 것을 확인한 경우 소급 악성코드 이벤트를 기록합니다. Series 2 디바이스, Cisco NGIPS for Blue Coat X-Series 및 DC500 방어 센터는 네트워크 기반 악성코드 차단을 지원하지 않으며, 이는 표시되는 데이터에 영향을 미칠 수 있습니다. Series 2 디바이스만 관리하는 Series 3 방어 센터는 엔드포인트 기반 악성코드 이벤트만 표시할 수 있습니다. 자세한 내용은 37-2 페이지의 악성코드 차단 및 파일 제어 이해 및 40-17페이지의 악성코드 이벤트 작업을/를 참조하십시오.

사전 정의된 악성코드 이벤트 워크플로의 마지막 페이지이며 사용자 지정 워크플로에 추가할 수 있는 악성코드 이벤트의 테이블 보기에는 파일 테이블의 각 필드에 대한 열이 포함됩니다. 악성코드 이벤트의 테이블 보기에서 일부 필드는 기본적으로 비활성화되어 있습니다. 세션 중에 필드를 활성화하려면 확장 화살표( )를 클릭하여 검색 제약 조건을 확장한 다음 **Disabled Columns** 아래에서 열 이름을 클릭합니다.

모든 이벤트에 대해 모든 필드가 채워지는 것은 아닙니다. 서로 다른 유형의 악성코드 이벤트에는 서로 다른 정보가 포함될 수 있습니다. 예를 들어, FireAMP 악성코드 탐지는 다운로드 또는 실행 시 엔드포인트에서 수행되므로 엔드포인트 기반 악성코드 이벤트에는 파일 경로, 클라이언트 애플리케이션 호출 등에 대한 정보가 포함됩니다. 이와는 대조적으로, 관리되는 디바이스는 네트워크 트래픽에서 악성코드 파일을 탐지하며 이와 관련된 악성코드 이벤트에는 포트, 애플리케이션 프로토콜, 그리고 파일 전송에 사용된 연결에 대한 원래 IP 주소 정보가 포함됩니다.

다음 표에는 각 악성코드 이벤트 필드가 나열되어 있으며, 악성코드 이벤트 유형에 따라 시스템이 해당 필드에 정보를 표시하는지 여부가 나와 있습니다. DC500 방어 센터는 대륙 또는 국가 지오로케이션 정보의 보내기 또는 받기를 지원하지 않습니다.

표 40-3 악성코드 이벤트 필드

필드	설명	네트워크	엔드포인트	클라우드에서 소급
Time	이벤트가 생성된 날짜 및 시간.	예	예	예
Action	파일과 일치하는 규칙에 대한 규칙 작업과 관련된 파일 규칙 작업 및 관련된 파일 규칙 작업 옵션.	예	아니요	예
Sending IP	탐지된 악성코드를 전송하는 호스트의 IP 주소.	예	아니요	아니요
Sending Continent	탐지된 악성코드를 전송하는 호스트의 대륙.	예	아니요	예
Sending Country	탐지된 악성코드를 전송하는 호스트의 국가.	예	아니요	아니요
Receiving IP	네트워크 기반 악성코드 이벤트의 경우, 탐지된 악성코드를 수신하는 호스트의 IP 주소. 엔드포인트 기반 악성코드 이벤트의 경우, FireAMP Connector가 설치되고 악성코드 이벤트가 발생한 엔드포인트의 IP 주소.	예	예	아니요
Receiving Continent	탐지된 악성코드를 수신하는 호스트의 대륙.	예	아니요	예
Receiving Country	탐지된 악성코드를 수신하는 호스트의 국가.	예	아니요	아니요

표 40-3 악성코드 이벤트 필드(계속)

필드	설명	네트워크	엔드포인트	클라우드에서 소급
Sending Port	관리되는 디바이스가 악성코드를 탐지한 트래픽에 의해 사용된 소스 포트.	예	아니요	아니요
Receiving Port	관리되는 디바이스가 악성코드를 탐지한 트래픽에 의해 사용된 목적지 포트.	예	아니요	아니요
SSL Status	SSL 규칙, 기본 작업 또는 암호화된 연결을 로깅한 해독 불가능한 트래픽 작업과 관련된 작업입니다. • `Block` 및 `Block with reset` - 차단된 암호화 연결을 나타냅니다. • `Decrypt (Resign)` - 다시 서명된 서버 인증서를 사용하여 해독된 발신 연결을 나타냅니다. • `Decrypt (Replace Key)` - 대체된 공개 키가 있는 자체 서명된 서버 인증서를 사용하여 해독된 발신 연결을 나타냅니다. • `Decrypt (Known Key)` - 알려진 개인 키를 사용하여 해독된 수신 연결을 나타냅니다. • `Do not Decrypt` - 시스템이 해독하지 못한 연결을 나타냅니다. 시스템이 암호화된 연결을 해독하지 못할 경우, 해독 불가능한 트래픽 작업이 실행되었다는 내용과 함께 실패 사유가 표시됩니다. 시스템이 알려지지 않은 암호 그룹으로 암호화 트래픽을 탐지한 후 추가 검사 없이 허용한 경우 이 필드에는 `Do Not Decrypt (Unknown Cipher Suite)`가 표시됩니다. 인증서 세부사항을 보려면 잠금 아이콘()을 클릭합니다. 자세한 내용은 39-32페이지의 암호화된 연결과 관련된 인증서 보기을/를 참조하십시오.	예	아니요	아니요
User	악성코드 이벤트가 발생한 호스트(**Receiving IP**)의 사용자. 네트워크 기반 악성코드 이벤트의 경우 이 사용자는 네트워크 검색에 의해 결정됩니다. 사용자는 대상 호스트와 연결되어 있으므로, 악성코드 파일을 업로드한 악성코드 이벤트와는 연결되지 않습니다. 엔드포인트 기반 악성코드 이벤트의 경우 FireAMP Connector가 사용자 이름을 결정합니다. FireAMP 사용자는 사용자 검색 또는 제어에 연결할 수 **없습니다**. 이들은 Users 테이블에 나타나지 않으며 이들의 세부사항을 볼 수도 없습니다.	예	예	아니요
Event Type	악성코드 이벤트의 유형. 전체 이벤트 유형 목록은 40-25페이지의 악성코드 이벤트 유형을/를 참조하십시오.	예	예	예
Event Subtype	악성코드 탐지로 이어진 FireAMP 작업(예: `Create`, `Execute`, `Move` 또는 `Scan`).	아니요	예	아니요
Threat Name	탐지된 악성코드의 이름.	예	예	예
File Name	악성코드 파일의 이름.	예	예	아니요

표 40-3 악성코드 이벤트 필드(계속)

필드	설명	네트워크	엔드포인트	클라우드에서 소급
File Disposition	다음 파일 성향 중 하나: • `Malware` - 클라우드가 파일을 악성코드로 분류했으며 파일의 위협 점수가 파일 정책에 정의된 악성코드 임계값을 초과했음을 나타냅니다. • `Clean` - 클라우드가 파일을 정상으로 분류했거나, 사용자가 파일을 정상 목록에 추가했음을 나타냅니다. • `Unknown` - 클라우드가 성향을 할당하기 전에 악성코드 클라우드 조회가 발생했음을 나타냅니다. 파일이 분류되지 않습니다. • `Custom Detection` - 사용자가 파일을 사용자 지정 탐지 목록에 추가했음을 나타냅니다. • `Unavailable` - 방어 센터에서 악성코드 클라우드 조회를 수행할 수 없음을 나타냅니다. 이 성향의 이벤트는 비율이 낮을 수 있는데, 이는 정상적인 상황입니다. 정상(clean) 파일은 정상으로 변경된 경우에만 악성코드 테이블에 나타납니다. 40-18페이지의 소급 악성코드 이벤트을/를 참조하십시오.	예	아니요	예
File SHA256	파일의 SHA-256 해시 값, 그리고 최근에 탐지된 파일 이벤트 및 파일 성향을 나타내는 네트워크 파일 전파 흔적 아이콘. 네트워크 파일 전파 흔적을 보려면 전파 흔적 아이콘을 클릭합니다. 자세한 내용은 40-38페이지의 네트워크 파일 전파 흔적 분석을/를 참조하십시오.	예	예	예
Threat Score	이 파일과 가장 최근에 연결된 위협 점수. • `Low`(●○○○) • `Medium`(●●○○) • `High`(●●●○) • `Very High`(●●●●) Dynamic Analysis Summary 보고서를 보려면 위협 점수 아이콘을 클릭합니다.	예	아니요	아니요
File Path	악성코드 파일의 파일 경로이며, 파일 이름은 포함되지 않음.	아니요	예	아니요
File Type	악성코드 파일의 파일 형식(예: `HTML` 또는 `MSEXE`).	예	예	아니요
File Type Category	다음과 같은 파일 형식의 일반 카테고리: `Office Documents`, `Archive`, `Multimedia`, `Executables`, `PDF files`, `Encoded`, `Graphics` 또는 `System Files`.	예	예	아니요
File Timestamp	악성코드 파일이 생성된 시간과 날짜.	아니요	예	아니요
File Size (KB)	킬로바이트 단위의 악성코드 파일 크기.	예	예	아니요

표 40-3 악성코드 이벤트 필드(계속)

필드	설명	네트워크	엔드포인트	클라우드에서 소급
File URI	악성코드 파일의 원래 URI(예: 사용자가 파일을 다운로드한 URL)	예	아니요	아니요
Archive Name	악성코드 파일과 연결된 아카이브 파일(있는 경우)의 이름(예: `archive.zip`).	예	예	아니요
Archive SHA256	악성코드 파일과 연결된 아카이브 파일(있는 경우)의 SHA-256 해시 값. 아카이브 파일의 내용을 보려면 아카이브 파일의 이벤트 뷰어 행을 마우스 오른쪽 버튼으로 클릭하여 컨텍스트 메뉴를 열고 **View Archive Contents**를 클릭합니다. 자세한 내용은 37-22페이지의 아카이브 파일의 내용 보기을/를 참조하십시오.	예	예	아니요
Archive Depth	아카이브 파일에서 파일이 중첩된 레벨(있는 경우)(예: `1` 또는 `3`).	예	예	아니요
Application File Name	탐지가 발생했을 때 악성코드 파일에 액세스하는 클라이언트 애플리케이션. 이러한 애플리케이션은 네트워크 검색 또는 애플리케이션 제어에 연결되지 **않습니다**.	아니요	예	아니요
Application File SHA256	탐지가 발생했을 때 FireAMP에서 탐지한 또는 격리한 파일에 액세스한 부모 파일의 SHA-256 해시 값.	아니요	예	아니요
Application Protocol	관리되는 디바이스가 악성코드 파일을 탐지한 트래픽에 의해 사용된 애플리케이션 프로토콜.	예	아니요	아니요
Application Protocol, Client, Web Application Category or Tag	애플리케이션 기능 이해에 도움이 되도록 애플리케이션의 특성을 부여하는 기준. 45-11 페이지의 표 45-2을/를 참조하십시오.	예	아니요	예
Client	한 호스트에서 실행되며 서버에 의존하여 파일을 전송하는 클라이언트 애플리케이션.	예	아니요	예
Web Application	연결에서 탐지된 HTTP 트래픽에 대한 요청 URL 또는 내용을 나타내는 애플리케이션.	예	아니요	예
IOC	악성코드 이벤트가 연결과 관련된 호스트에 대해 IOC(indication of compromise)를 트리거했는지 여부. 엔드포인트 기반 악성코드 탐지가 IOC 규칙을 트리거하면 `FireAMP IOC` 유형과 함께 전체 악성코드 이벤트가 생성됩니다. IOC에 대한 자세한 내용은 45-20페이지의 IOC 이해을/를 참조하십시오.	예	예	예
Application Risk	연결에서 탐지된 애플리케이션 트래픽과 관련된 위험: `Very High`, `High`, `Medium`, `Low` 또는 `Very Low`. 연결에서 탐지된 각 유형의 애플리케이션에는 관련 위험도가 포함되며, 이 필드에는 가장 높은 순서부터 표시됩니다. 자세한 내용은 45-11 페이지의 표 45-2을/를 참조하십시오.	예	아니요	예
Business Relevance	연결에서 탐지된 애플리케이션 트래픽과 관련된 비즈니스 관련성(`Very High`, `High`, `Medium`, `Low`, `Very Low`)입니다. 연결에서 탐지된 각 애플리케이션 유형에는 관련된 비즈니스 연관성이 있습니다. 이 필드에는 그중 가장 낮은 값(가장 연관성이 적음)이 표시됩니다. 자세한 내용은 45-11 페이지의 표 45-2을/를 참조하십시오.	예	아니요	예

표 40-3 악성코드 이벤트 필드(계속)

필드	설명	네트워크	엔드포인트	클라우드에서 소급
Detector	악성코드를 식별하는 FireAMP detector(예: ClamAV, Spero 또는 SHA).	아니요	예	아니요
Message	악성코드 이벤트와 연결된 추가 정보. 네트워크 기반 악성코드 이벤트의 경우, 성향이 변경된 파일에 대해서만 이 필드가 채워집니다. 40-18페이지의 소급 악성코드 이벤트을/를 참조하십시오.	예	예	아니요
FireAMP Cloud	이벤트가 시작된 FireAMP 클라우드의 이름.	아니요	예	아니요
Device	네트워크 기반 악성코드 이벤트의 경우, 악성코드 파일을 탐지한 디바이스의 이름. 클라우드에 의해 생성된 네트워크 기반 악성코드 이벤트 및 소급 악성코드 이벤트의 경우, 방어 센터의 이름.	예	예	예
Security Context	트래픽이 통과된 가상 방화벽 그룹을 식별하는 메타데이터입니다. 이 필드는 다중 컨텍스트 모드의 ASA FirePOWER 디바이스에 대해서만 채워집니다.	예	예	예
Count	각 행의 정보와 일치하는 이벤트의 수. 둘 이상의 동일한 행을 생성하는 제약 조건을 적용한 경우에만 이 필드가 나타납니다.	해당 없음	해당 없음	해당 없음

악성코드 이벤트 유형

라이센스: 악성코드 또는 모두

지원되는 디바이스: 기능에 따라 다름

지원되는 Defense Center: 기능에 따라 다름

네트워크 기반 악성코드 이벤트의 경우 이벤트 유형은 다음 중 하나일 수 있습니다.

- Threat Detected in Network File Transfer
- Threat Detected in Network File Transfer(retrospective)

엔드포인트 기반 악성코드 이벤트는 다음 유형 중 하나일 수 있습니다.

- Blocked Execution
- Cloud Recall Quarantine
- Cloud Recall Quarantine Attempt Failed
- Cloud Recall Quarantine Started
- Cloud Recall Restore from Quarantine
- Cloud Recall Restore from Quarantine Failed
- Cloud Recall Restore from Quarantine Started
- FireAMP IOC
- Quarantine Failure
- Quarantined Item Restored
- Quarantine Restore Failed

- Quarantine Restore Started
- Scan Completed, No Detections
- Scan Completed With Detections
- Scan Failed
- Scan Started
- Threat Detected
- Threat Detected in Exclusion
- Threat Quarantined

파일의 전파 흔적 맵에 악성코드 이벤트가 포함된 경우 이벤트 유형은 Threat Detected in Network File Transfer, Threat Detected in Network File Transfer (retrospective), Threat Detected, Threat Detected in Exclusion 및 Threat Quarantined 중 하나입니다. 자세한 내용은 40-36페이지의 네트워크 파일 전파 흔적 작업을/를 참조하십시오.

Series 2 디바이스, Cisco NGIPS for Blue Coat X-Series 및 DC500 방어 센터는 네트워크 기반 악성코드 차단을 지원하지 않으며, 이는 표시되는 데이터에 영향을 미칠 수 있습니다. Series 2 디바이스만 관리하는 Series 3 방어 센터는 엔드포인트 기반 악성코드 이벤트만 표시할 수 있습니다.

악성코드 이벤트 검색

라이센스: 악성코드 또는 모두

방어 센터의 Search 페이지를 사용하면 특정 악성코드 이벤트를 검색하고, 이벤트 뷰어에 결과를 표시하고, 나중에 다시 사용할 수 있도록 검색 기준을 저장할 수 있습니다. Custom Analysis 대시보드 위젯, 보고서 템플릿, 사용자 지정 사용자 역할도 저장된 검색을 사용할 수 있습니다.

시스템에 제공된 검색은 Saved Searches 목록에 (`Cisco`)라는 레이블로 표시되며, 예시 역할을 수행합니다.

검색 결과는 검색 중인 이벤트에서 사용할 수 있는 데이터에 따라 달라집니다. 다시 말하면, 사용 가능한 데이터에 따라 검색 제한이 적용되지 않을 수 있습니다. 엔드포인트 기반 악성코드 이벤트는 관리되는 디바이스에서 네트워크 트래픽을 검사한 결과로 생성되지 않으므로 연결 정보(포트, 애플리케이션 프로토콜 등)를 포함하지 않습니다.

일반 검색 구문

각 검색 필드 옆에는 유효한 구문의 예가 표시됩니다. 검색 기준을 입력할 경우, 다음 사항에 유의해야 합니다.

- 모든 필드에 부정(`!`)을 사용할 수 있습니다.
- 모든 필드에 쉼표로 구분된 검색 값의 목록을 사용할 수 있습니다. 지정된 필드에 나열된 값 중 하나를 포함하는 레코드는 검색 기준과 일치합니다.
- 모든 필드에 따옴표로 감싸고 쉼표로 구분한 목록을 검색 값으로 사용할 수 있습니다.
  - 단일 값만을 포함할 수 있는 필드의 경우, 따옴표 내에 지정된 정확한 문자열을 포함하는 지정된 필드의 레코드가 검색 기준과 일치합니다. 예를 들어 `A, B, "C, D, E"`에 대한 검색은 지정된 필드에 `"A"` 또는 `"B"` 또는 `"C, D, E"`가 포함된 레코드와 일치합니다. 따라서 가능한 값으로 쉼표를 포함하는 필드에서 일치를 확인할 수 있습니다.
  - 여러 값을 동시에 포함할 수 있는 필드의 경우, 따옴표로 감싸고 쉼표로 구분한 모든 값을 포함하는 지정된 필드의 레코드가 해당 검색 기준과 일치합니다.

  - 여러 값을 동시에 포함할 수 있는 필드의 경우, 검색 기준에 단일 값은 물론 따옴표로 감싸고 쉼표로 구분한 목록도 포함할 수 있습니다. 예를 들어 하나 이상의 이러한 문자를 포함할 수 있는 필드에서 `A, B, "C, D, E"`에 대한 검색은 지정된 필드에 `A` 또는 `B`, 또는 `C`, `D`, `E` 모두가 포함된 레코드와 일치합니다.

- 검색 결과에는 모든 필드에 지정된 검색 기준과 매칭되는 레코드만 반환됩니다.
- 많은 필드에서 와일드카드로 하나 이상의 별표(*)를 사용할 수 있습니다.
- 해당 필드에 대해 사용할 수 있는 정보가 없는 이벤트를 식별하려면 필드에 `n/a`를 지정합니다. 해당 필드가 채워지는 이벤트를 식별하려면 `!n/a`를 사용합니다.
- 특정 디바이스 및 그룹, 스택 또는 클러스터의 디바이스를 검색하려면 디바이스 필드를 사용합니다. FireSIGHT 시스템에서 검색 시 디바이스 필드를 취급하는 방법에 대한 자세한 내용은 60-7페이지의 검색에서 디바이스 지정을/를 참조하십시오.
- 검색 기준으로 객체를 사용하려면 검색 필드 옆에 나타나는 객체 추가 아이콘(+)을 클릭합니다.

검색에서 객체를 사용하는 방법을 포함하여 검색 구문에 대한 자세한 내용은 60-1페이지의 이벤트 검색을/를 참조하십시오.

악성코드 이벤트용 특수 검색 구문

위에 나열된 일반 검색 구문을 보완하기 위해 다음 목록에서는 악성코드 이벤트용 특수 검색 구문 몇 가지에 대해 설명합니다.

Sending/Receiving IP

시스템은 **Sending IP** 또는 **Receiving IP**가 사용자가 지정한 IP 주소와 일치하는 모든 이벤트를 반환합니다.

이벤트 유형

특정 악성코드 이벤트 유형의 이벤트를 검색할 때에는(40-25페이지의 악성코드 이벤트 유형 참조) `"Scan Completed With Detection"`과 같이 이벤트 유형을 따옴표로 감싸십시오. 그렇게 하지 않으면 시스템이 부분 일치 확인을 수행합니다. 즉, 따옴표 없이 동일한 문자열을 사용하여 검색하면 시스템은 다음과 같은 유형의 이벤트를 반환합니다.

- `Scan Completed, No Detections`
- `Scan Completed With Detection`

Initiator/Responder Continent

시스템은 **Initiator Continent** 또는 **Responder Continent**가 사용자가 지정한 대륙과 일치하는 모든 이벤트를 반환합니다.

Initiator/Responder 국가

시스템은 **Initiator Country** 또는 **Responder Country**가 사용자가 지정한 국가와 일치하는 모든 이벤트를 반환합니다.

URI 또는 메시지

시스템에서는 부분 매칭을 수행하므로, 별표를 사용하지 않고도 필드 내용의 전체 또는 부분을 검색할 수 있습니다.

수행한 SSL Actual Action

시스템이 지정된 작업을 적용한 암호화 트래픽에 대한 악성코드 이벤트를 보려면 다음 키워드 중 하나를 입력하십시오.

- `Do Not Decrypt` - 시스템이 해독하지 못한 연결을 나타냅니다.
- `Block` 및 `Block with Reset` - 차단된 암호화 연결을 나타냅니다.
- `Decrypt (Known Key)` - 알려진 개인 키를 사용하여 해독된 수신 연결을 나타냅니다.
- `Decrypt (Replace Key)` - 대체된 공개 키가 있는 자체 서명된 서버 인증서를 사용하여 해독된 발신 연결을 나타냅니다.
- `Decrypt (Resign)` - 다시 서명된 서버 인증서를 사용하여 해독된 발신 연결을 나타냅니다.

이 열은 악성코드 이벤트 테이블 보기에 나타나지 않습니다.

SSL Failure Reason

지정된 이유로 시스템이 해독에 실패한 암호화 트래픽에 대한 악성코드 이벤트를 보려면 다음 키워드 중 하나를 입력하십시오.

- `Unknown`
- `No Match`
- `Success`
- `Uncached Session`
- `Unknown Cipher Suite`
- `Unsupported Cipher Suite`
- `Unsupported SSL Version`
- `SSL Compression Used`
- `Session Undecryptable in Passive Mode`
- `Handshake Error`
- `Decryption Error`
- `Pending Server Name Category Lookup`
- `Pending Common Name Category Lookup`
- `Internal Error`
- `Network Parameters Unavailable`
- `Invalid Server Certificate Handle`
- `Server Certificate Fingerprint Unavailable`
- `Cannot Cache Subject DN`
- `Cannot Cache Issuer DN`
- `Unknown SSL Version`
- `External Certificate List Unavailable`
- `External Certificate Fingerprint Unavailable`
- `Internal Certificate List Invalid`
- `Internal Certificate List Unavailable`
- `Internal Certificate Unavailable`
- `Internal Certificate Fingerprint Unavailable`
- `Server Certificate Validation Unavailable`
- `Server Certificate Validation Failure`
- `Invalid Action`

이 열은 악성코드 이벤트 테이블 보기에 나타나지 않습니다.

SSL Subject Country

인증서 주체의 국가와 연결된 암호화 트래픽에 대한 악성코드 이벤트를 보려면 두 글자의 ISO 3166-1 alpha-2 국가 코드를 입력하십시오.

이 열은 악성코드 이벤트 테이블 보기에 나타나지 않습니다.

SSL Issuer Country

인증서 발급자의 국가와 연결된 암호화 트래픽을 보려면 두 글자의 ISO 3166-1 alpha-2 국가 코드를 입력하십시오.

이 열은 악성코드 이벤트 테이블 보기에 나타나지 않습니다.

SSL Certificate Fingerprint

인증서를 인증하고 해당 인증서와 연결된 트래픽을 보는 데 사용된 SHA 해시 값을 입력하거나 붙여넣습니다.

이 열은 악성코드 이벤트 테이블 보기에 나타나지 않습니다.

SSL Public Key Fingerprint

공개 키를 인증하고 해당 인증서와 연결된 트래픽을 보는 데 사용된 SHA 해시 값을 입력하거나 붙여넣습니다.

이 열은 악성코드 이벤트 테이블 보기에 나타나지 않습니다.

악성코드 이벤트를 검색하려면

액세스: Admin/Any Security Analyst

1단계 **Analysis > Search**를 선택합니다.

Search 페이지가 나타납니다.

2단계 테이블 드롭다운 목록에서 **Malware Events**를 선택합니다.

해당 제약 조건으로 페이지가 업데이트됩니다.

3단계 다음 절의 설명에 따라 해당 필드에 검색 기준을 입력합니다.

- 악성코드 이벤트 테이블에 있는 필드에 대한 자세한 내용은 악성코드 이벤트 필드 표를 참조하십시오.
- 악성코드 이벤트용 특수 검색 구문은 40-27페이지의 악성코드 이벤트용 특수 검색 구문을/를 참조하십시오.
- 공개 키 인증서와 관련된 필드는 39-32페이지의 암호화된 연결과 관련된 인증서 보기을/를 참조하십시오.

4단계 선택적으로, 검색을 저장하려면 **Private** 확인란을 선택하여 자신만 액세스할 수 있는 비공개로 검색을 저장할 수 있습니다. 또는 모든 사용자가 사용할 수 있도록 검색을 저장하려면 확인란을 선택하지 않습니다.

팁 사용자 지정 사용자 역할에 대한 데이터 제한으로서 검색을 사용하려면 **반드시** 비공개 검색으로 저장해야 합니다.

5단계 선택적으로, 나중에 다시 사용할 수 있도록 검색을 저장할 수 있습니다. 다음 옵션을 이용할 수 있습니다.

- 검색 기준을 저장하려면 **Save**를 클릭합니다.

  새 검색인 경우 검색 이름을 입력하도록 대화 상자가 나타납니다. 고유한 검색 이름을 입력하고 **Save**를 클릭합니다. 이미 존재하는 검색에 대한 새 조건을 저장하는 경우 프롬프트가 나타나지 않습니다. 나중에 실행할 수 있도록 검색이 저장됩니다(**Private**을 선택한 경우 자신만 볼 수 있음).

- 새 검색을 저장하거나, 저장된 기존 검색을 변경하여 만든 검색에 새 이름을 할당하려면 **Save As New**를 클릭합니다.

  검색 이름을 입력하도록 대화 상자가 나타납니다. 고유한 검색 이름을 입력하고 **Save**를 클릭합니다. 나중에 실행할 수 있도록 검색이 저장됩니다(**Private**을 선택한 경우 자신만 볼 수 있음).

6단계 검색을 시작하려면 **Search**를 클릭합니다.

검색 결과는 현재의 시간 범위로 제한되어 기본 악성코드 이벤트 워크플로에 나타납니다.

캡처된 파일 작업

라이센스: 악성코드

지원되는 디바이스: Series 2 또는 X-Series를 제외한 모두

지원되는 Defense Center: DC500을 제외한 모든 방어 센터

현재 적용된 파일 정책의 규칙에 따라, 시스템은 관리되는 디바이스가 네트워크 트래픽에서 탐지된 파일을 캡처하는 시간을 기록합니다. 이벤트 뷰어에서 SHA-256 값과 연결된 최근 파일 이름, 파일 성향과 위협 점수, 파일 스토리지 상태, 아카이브 검사 상태, 파일이 동적 분석을 위해 수동으로 제출되었는지 여부 등 캡처된 파일과 관련된 정보를 볼 수 있습니다.

참고 악성코드는 탐지된 후 캡처되므로, 악성코드를 포함하는 디바이스에 의해 캡처된 파일은 파일 이벤트와 악성코드 이벤트를 모두 생성합니다. 자세한 내용은 40-8페이지의 파일 이벤트 작업 및 40-17페이지의 악성코드 이벤트 작업을/를 참조하십시오.

방어 센터의 이벤트 뷰어를 사용하면 캡처된 파일을 보고 검색하는 것은 물론, 동적 분석을 위해 제출할 수도 있습니다. 또한 Files Dashboard에서는 네트워크에서 탐지된 파일에 대한 자세한 정보를 차트 및 그래프를 통해 한눈에 볼 수 있습니다.

자세한 내용은 다음 링크를 참고하십시오.

- 40-31페이지의 캡처된 파일 보기
- 40-32페이지의 캡처된 파일 테이블 이해
- 40-33페이지의 캡처된 파일 검색

캡처된 파일 보기

라이센스: 악성코드

FireSIGHT 시스템의 이벤트 뷰어를 사용하면 테이블에서 캡처된 파일을 보는 것은 물론, 분석과 관련된 정보에 따라 이벤트 보기를 조작할 수도 있습니다.

캡처된 파일에 액세스할 때 볼 수 있는 페이지는, 넓은 보기에서 좀 더 집중된 보기로 이동하여 이벤트를 평가하는 데 사용할 수 있는 일련의 페이지인 워크플로에 따라 달라집니다. 시스템은 캡처된 파일에 대한 다음과 같은 사전 정의 워크플로와 함께 제공됩니다.

- *Captured File Summary*(기본값) - 유형, 카테고리, 위협 점수를 기준으로 캡처 파일의 분석을 제공합니다.
- *Dynamic Analysis Status* - 캡처 파일이 동적 분석을 위해 제출되었는지 여부에 따라 그 카운트를 제공합니다.

특정 요구와 일치하는 정보만 표시하는 사용자 지정 워크플로를 생성할 수도 있습니다. 사용자 지정 워크플로를 비롯한 서로 다른 기본 워크플로 지정에 대한 자세한 내용은 71-3페이지의 이벤트 보기 설정 구성을/를 참조하십시오.

FireSIGHT 시스템은 이벤트 뷰어, 이벤트 검색, 대시보드, Context Explorer를 비롯한 웹 인터페이스의 모든 영역에서 유니코드(UTF-8) 파일 이름의 표시와 입력을 지원합니다. 그러나 PDF 형식으로 생성하는 보고서는 유니코드를 지원하지 않습니다. 유니코드 파일 이름은 PDF 보고서에 음역 형태로 나타납니다. 자세한 내용은 57-26페이지의 보고서 생성 및 보기을/를 참조하십시오.

이벤트 뷰어를 사용할 경우 다음을 수행할 수 있습니다.

- 이벤트 검색, 정렬 및 제한은 물론 표시된 이벤트에 대한 시간 범위를 변경할 수 있습니다.
- 나타나는 열을 지정할 수 있습니다(테이블 보기 전용).
- 동일한 워크플로 내에서 서로 다른 워크플로 페이지를 사용하여 이벤트를 볼 수 있습니다.
- 다른 워크플로를 사용하는 여러 이벤트를 함께 볼 수 있습니다.
- 특정 값으로 제한하여 워크플로 내에서 페이지 간에 드릴다운할 수 있습니다.
- 나중에 동일한 데이터(데이터가 그대로 있을 경우)로 돌아올 수 있도록 현재 페이지 및 제약 조건을 북마크 처리할 수 있습니다.
- 파일의 전파 흔적을 볼 수 있습니다.
- 아카이브 파일의 내용 및 검사 상태를 볼 수 있습니다.
- 파일 목록에 파일을 추가하고, 파일을 다운로드하고, 동적 분석을 위해 파일을 제출하고, 파일의 SHA-256 값의 전체 텍스트를 볼 수 있습니다.
- 사용 가능한 경우 파일의 Dynamic Analysis Summary 보고서를 볼 수 있습니다.
- 동적 분석을 위해 동시에 최대 25개 파일을 제출할 수 있습니다.
- 현재 제약 조건을 사용하여 보고서 템플릿을 생성할 수 있습니다.

Series 2 디바이스, Cisco NGIPS for Blue Coat X-Series 및 DC500 방어 센터는 네트워크 기반 악성코드 차단 또는 아카이브 파일 검사를 지원하지 않으며, 이는 표시되는 데이터에 영향을 미칠 수 있습니다. 예를 들어 Series 2 디바이스만을 관리하는 Series 3 방어 센터는 캡처된 파일을 표시할 수 없습니다.

사용자 지정 워크플로 생성을 포함하여 이벤트 뷰어 사용에 대한 자세한 내용은 58-1페이지의 워크플로의 이해 및 사용을/를 참조하십시오.

파일 이벤트를 보려면

액세스: Admin/Any Security Analyst

1단계 **Analysis > Files > Captured Files**를 선택합니다.

기본 파일 이벤트 워크플로의 첫 번째 페이지가 나타납니다. 나타나는 열에 대한 자세한 내용은 40-32페이지의 캡처된 파일 테이블 이해을/를 참조하십시오.

캡처된 파일 테이블 이해

라이센스: 악성코드

적용된 파일 정책의 설정에 따라, 방어 센터는 관리되는 디바이스가 모니터링되는 네트워크 트래픽에서 전송되는 파일을 캡처하는 시간을 기록합니다.

사전 정의된 캡처된 파일 워크플로의 마지막 페이지이며 사용자 지정 워크플로에 추가할 수 있는 캡처된 파일의 테이블 보기에는 캡처된 파일 테이블의 각 필드에 대한 열이 포함됩니다. 캡처된 파일의 테이블 보기에서 일부 필드는 기본적으로 비활성화되어 있습니다. 세션 중에 필드를 활성화하려면 확장 화살표( )를 클릭하여 검색 제약 조건을 확장한 다음 **Disabled Columns** 아래에서 열 이름을 클릭합니다. 다음 표에서는 캡처된 파일 필드에 대해 설명합니다.

표 40-4 캡처된 파일 필드

필드	설명
Last Changed	이 파일과 관련된 정보가 마지막으로 업데이트된 시간.
File Name	파일의 SHA-256 해시 값과 연결된, 최근에 탐지된 파일 이름
Disposition	다음 파일 성향 중 하나: • `Malware` - 클라우드가 파일을 악성코드로 분류했으며 파일의 위협 점수가 파일 정책에 정의된 악성코드 임계값을 초과했음을 나타냅니다. • `Clean` - 클라우드가 파일을 정상으로 분류했거나, 사용자가 파일을 정상 목록에 추가했음을 나타냅니다. • `Unknown` - 클라우드가 성향을 할당하기 전에 악성코드 클라우드 조회가 발생했음을 나타냅니다. 파일이 분류되지 않습니다. • `Custom Detection` - 사용자가 파일을 사용자 지정 탐지 목록에 추가했음을 나타냅니다. • `Unavailable` - 방어 센터에서 악성코드 클라우드 조회를 수행할 수 없음을 나타냅니다. 이 성향의 이벤트는 비율이 낮을 수 있는데, 이는 정상적인 상황입니다. • `N/A` - Detect Files 또는 Block Files 규칙이 파일을 처리했으며 방어 센터에서 악성코드 클라우드 조회를 수행하지 않았음을 나타냅니다.
SHA256	파일의 SHA-256 해시 값, 그리고 최근에 탐지된 파일 이벤트 및 파일 성향을 나타내는 네트워크 파일 전파 흔적 아이콘. 네트워크 파일 전파 흔적을 보려면 전파 흔적 아이콘을 클릭합니다. 자세한 내용은 40-38페이지의 네트워크 파일 전파 흔적 분석을/를 참조하십시오.

표 40-4 캡처된 파일 필드(계속)

필드	설명
Threat Score	이 파일과 가장 최근에 연결된 위협 점수. • Low(●○○○) • Medium(●●○○) • High(●●●○) • Very High(●●●●) Dynamic Analysis Summary 보고서를 보려면 위협 점수 아이콘을 클릭합니다.
Type	HTML 또는 MSEXE 등의 파일 형식.
Category	다음과 같은 파일 형식의 일반 카테고리: Office Documents, Archive, Multimedia, Executables, PDF files, Encoded, Graphics 또는 System Files.
Storage Status	파일이 관리되는 디바이스에 저장되는지 여부.
Archive Inspection Status	아카이브 파일의 경우 아카이브 검사의 상태: • Pending - 시스템이 아카이브 파일 및 내용을 여전히 검사 중임을 나타냅니다. 파일이 시스템을 다시 통과하면 완전한 정보를 이용할 수 있게 됩니다. • Extracted - 시스템이 아카이브의 내용을 추출 및 검사할 수 있게 되었음을 나타냅니다. • Failed - 매우 드물지만, 시스템이 확장을 처리할 수 없는 경우 나타날 수 있습니다. • Depth Exceeded - 아카이브에 허용되는 최대 깊이를 초과하여 중첩된 아카이브 파일이 포함되어 있음을 나타냅니다. • Encrypted - 아카이브 파일의 내용이 암호화되어 검사할 수 없음을 나타냅니다. • Not Inspectable - 시스템이 아카이브의 내용을 확장 및 검사할 수 없음을 나타냅니다. 이 상태의 세 가지 주요 원인은 정책 규칙 작업, 정책 컨피그레이션 및 손상된 파일입니다. 아카이브 파일의 내용을 보려면 이벤트 뷰어 행을 마우스 오른쪽 버튼으로 클릭하여 컨텍스트 메뉴를 열고 **View Archive Contents**를 선택합니다. 자세한 내용은 37-20페이지의 아카이브 파일 검사 옵션 구성을/를 참조하십시오.
Analysis Status	동적 분석을 위해 파일이 제출되었는지 여부.
Last Sent	동적 분석을 위해 파일이 최근에 클라우드에 제출된 시간.

캡처된 파일 검색

라이센스: 악성코드

방어 센터의 Search 페이지를 사용하면 특정 캡처된 파일을 검색하고, 이벤트 뷰어에 결과를 표시하고, 나중에 다시 사용할 수 있도록 검색 기준을 저장할 수 있습니다. Custom Analysis 대시보드 위젯, 보고서 템플릿, 사용자 지정 사용자 역할도 저장된 검색을 사용할 수 있습니다.

검색 결과는 검색 중인 이벤트에서 사용할 수 있는 데이터에 따라 달라집니다. 다시 말하면, 사용 가능한 데이터에 따라 검색 제한이 적용되지 않을 수 있습니다. 예를 들어 동적 분석을 위해 제출된 적이 없는 파일에는 연결된 위협 점수가 없을 수 있습니다.

일반 검색 구문

각 검색 필드 옆에는 유효한 구문의 예가 표시됩니다. 검색 기준을 입력할 경우, 다음 사항에 유의해야 합니다.

- 모든 필드에 부정(!)을 사용할 수 있습니다.

- 모든 필드에 쉼표로 구분된 검색 값의 목록을 사용할 수 있습니다. 지정된 필드에 나열된 값 중 하나를 포함하는 레코드는 검색 기준과 일치합니다.
- 모든 필드에 따옴표로 감싸고 쉼표로 구분한 목록을 검색 값으로 사용할 수 있습니다.
  - 단일 값만을 포함할 수 있는 필드의 경우, 따옴표 내에 지정된 정확한 문자열을 포함하는 지정된 필드의 레코드가 검색 기준과 일치합니다. 예를 들어 `A, B, "C, D, E"`에 대한 검색은 지정된 필드에 `"A"` 또는 `"B"` 또는 `"C, D, E"`가 포함된 레코드와 일치합니다. 따라서 가능한 값으로 쉼표를 포함하는 필드에서 일치를 확인할 수 있습니다.
  - 여러 값을 동시에 포함할 수 있는 필드의 경우, 따옴표로 감싸고 쉼표로 구분한 모든 값을 포함하는 지정된 필드의 레코드가 해당 검색 기준과 일치합니다.
  - 여러 값을 동시에 포함할 수 있는 필드의 경우, 검색 기준에 단일 값은 물론 따옴표로 감싸고 쉼표로 구분한 목록도 포함할 수 있습니다. 예를 들어 하나 이상의 이러한 문자를 포함할 수 있는 필드에서 `A, B, "C, D, E"`에 대한 검색은 지정된 필드에 `A` 또는 `B`, 또는 `C`, `D`, `E` 모두가 포함된 레코드와 일치합니다.
- 검색 결과에는 모든 필드에 지정된 검색 기준과 매칭되는 레코드만 반환됩니다.
- 많은 필드에서 와일드카드로 하나 이상의 별표(*)를 사용할 수 있습니다.
- 해당 필드에 대해 사용할 수 있는 정보가 없는 이벤트를 식별하려면 필드에 `n/a`를 지정합니다. 해당 필드가 채워지는 이벤트를 식별하려면 `!n/a`를 사용합니다.
- 검색 기준으로 객체를 사용하려면 검색 필드 옆에 나타나는 객체 추가 아이콘(+)을 클릭합니다.

검색에서 객체를 사용하는 방법을 포함하여 검색 구문에 대한 자세한 내용은 60-1페이지의 이벤트 검색을/를 참조하십시오.

캡처된 파일용 특수 검색 구문

위에 나열된 일반 검색 구문을 보완하기 위해 다음 목록에서는 캡처된 파일용 특수 검색 구문 몇 가지에 대해 설명합니다.

표 40-5 캡처된 파일 특수 검색 구문

검색 기준	특수 구문
Storage Status	다음 중 하나 이상을 지정하십시오. • `File Stored` - 디바이스에 저장된 모든 캡처된 파일을 반환합니다. • `Unable to Store File` - 디바이스에 저장되지 않은 모든 캡처된 파일을 반환합니다.
Dynamic Analysis Status	다음 중 하나 이상을 지정하십시오. • `Sent for Analysis` - 동적 분석을 위해 대기열에 추가된 모든 캡처된 파일을 반환합니다. • `Not Sent for Analysis` - 동적 분석을 위해 제출되지 않은 모든 캡처된 파일을 반환합니다. • `Analysis Complete` - 위협 점수 및 동적 분석 요약 보고서를 받은, 동적 분석을 위해 제출된 모든 캡처된 파일을 반환합니다. • `Previously Analyzed` - 사용자가 동적 분석을 위해 다시 제출하려고 시도한, 캐시된 위협 점수가 있는 모든 파일을 반환합니다. • `Failure (Analysis Timeout)` - 클라우드가 결과를 반환해야 하는, 동적 분석을 위해 제출된 모든 캡처된 파일을 반환합니다. • `Failure (Network Issue)` - 네트워크 연결 실패 때문에 동적 분석을 위해 제출되지 않은 모든 파일을 반환합니다. • `Failure (Cannot Run File)` - 클라우드가 테스트 환경에서 실행하지 못한, 동적 분석을 위해 제출된 모든 파일을 반환합니다.

캡처된 파일을 검색하려면

액세스: Admin/Any Security Analyst

1단계 **Analysis > Search**를 선택합니다.

Search 페이지가 나타납니다.

2단계 테이블 드롭다운 목록에서 **Captured Files**를 선택합니다.

해당 제약 조건으로 페이지가 업데이트됩니다.

3단계 해당 필드에 검색 기준을 입력합니다.

캡처된 파일 테이블에 있는 필드에 대한 자세한 내용은 캡처된 파일 필드 표를 참조하십시오.

4단계 선택적으로, 검색을 저장하려면 **Private** 확인란을 선택하여 자신만 액세스할 수 있는 비공개로 검색을 저장할 수 있습니다. 또는 모든 사용자가 사용할 수 있도록 검색을 저장하려면 확인란을 선택하지 않습니다.

팁 사용자 지정 사용자 역할에 대한 데이터 제한으로서 검색을 사용하려면 **반드시** 비공개 검색으로 저장해야 합니다.

5단계 선택적으로, 나중에 다시 사용할 수 있도록 검색을 저장할 수 있습니다. 다음 옵션을 이용할 수 있습니다.

- 검색 기준을 저장하려면 **Save**를 클릭합니다.

  새 검색인 경우 검색 이름을 입력하도록 대화 상자가 나타납니다. 고유한 검색 이름을 입력하고 **Save**를 클릭합니다. 이미 존재하는 검색에 대한 새 조건을 저장하는 경우 프롬프트가 나타나지 않습니다. 나중에 실행할 수 있도록 검색이 저장됩니다(**Private**을 선택한 경우 자신만 볼 수 있음).

- 새 검색을 저장하거나, 저장된 기존 검색을 변경하여 만든 검색에 새 이름을 할당하려면 **Save As New**를 클릭합니다.

  검색 이름을 입력하도록 대화 상자가 나타납니다. 고유한 검색 이름을 입력하고 **Save**를 클릭합니다. 나중에 실행할 수 있도록 검색이 저장됩니다(**Private**을 선택한 경우 자신만 볼 수 있음).

6단계 검색을 시작하려면 **Search**를 클릭합니다.

검색 결과는 현재의 시간 범위로 제한되어 기본 캡처된 파일 워크플로에 나타납니다.

네트워크 파일 전파 흔적 작업

라이센스: 악성코드 또는 모두

지원되는 디바이스: 기능에 따라 다름

지원되는 Defense Center: 기능에 따라 다름

네트워크 파일 전파 흔적 기능은 호스트가 파일(악성코드 파일 포함)을 전송한 방법을 네트워크 전체에 매핑합니다. 이 맵을 사용하여 어떤 호스트가 악성코드를 전송했는지, 어떤 호스트가 위험한지를 확인하고 파일 전송 추세를 관찰할 수 있습니다.

전파 흔적 맵은 파일 전송 데이터, 파일의 성향, 파일 전송의 차단 여부 또는 파일의 격리 여부를 차트로 표시합니다. 맵 작성에 사용되는 데이터는 네트워크 기반 악성코드 이벤트(시스템이 악성코드 클라우드 조회를 수행하고 악성코드 성향을 반환한 파일 이벤트)와 악성코드의 탐지 및 차단과 관련된 특정 엔드포인트 기반 악성코드 이벤트(Threat Detected 또는 Threat Quarantined 이벤트 유형)에서 올 수 있습니다. 데이터 포인트 간 세로 줄은 호스트 간 파일 전송을 나타냅니다. 데이터 포인트를 연결하는 가로 줄은 시간에 따른 호스트의 파일 활동을 보여줍니다.

시스템이 악성코드 클라우드 조회를 수행할 수 있는 파일 형식의 전송을 추적할 수 있습니다. 파일의 전파 흔적에 직접 액세스하려면 Network File Trajectory List 페이지(**Analysis > Files > Network File Trajectory**)를 사용하고 특정 파일을 찾을 수 있습니다. 또한 침입을 분석하고 관련 파일의 전파 흔적을 검토하려면 Context Explorer나 대시보드, 또는 연결, 파일, 악성코드 이벤트의 이벤트 보기에서 파일의 전파 흔적에 액세스할 수 있습니다.

단일 전파 흔적 맵이 표시하는 데이터는 어플라이언스에 적용된 라이센스에 따라 다릅니다. 다음 표는 서로 다른 유형의 파일 전파 흔적을 추적하는 데 필요한 라이센스를 보여줍니다.

표 40-6 네트워크 파일 전파 흔적용 라이센스 요구 사항

보려는 내용	필요한 라이센스
네트워크 기반 파일 및 악성코드 전파 흔적	악성코드
엔드포인트 기반 위협 및 격리 추적	임의(FireAMP 서브스크립션 필요)

자세한 내용은 37-2페이지의 악성코드 차단 및 파일 제어 이해을/를 참조하십시오.

악성코드 라이센스를 DC500에서 사용할 수 없고 악성코드 라이센스를 Series 2 디바이스 또는 Cisco NGIPS for Blue Coat X-Series에서 활성화할 수 없으므로 개별 파일을 캡처, 저장, 차단하거나, 동적 분석을 위해 파일을 제출하거나, 아카이브 파일의 내용을 보거나, 악성코드 클라우드 조회를 수행할 파일의 전파 흔적을 보는 데 이러한 어플라이언스를 사용할 수 없습니다. 그러나 여전히 엔드포인트 기반 위협 및 격리 추적을 위해 파일 전파 흔적을 볼 수 있습니다.

자세한 내용은 다음 절을 참조하십시오.

- 40-37페이지의 네트워크 파일 전파 흔적 검토
- 40-38페이지의 네트워크 파일 전파 흔적 분석

네트워크 파일 전파 흔적 검토

라이센스: 악성코드 또는 모두

지원되는 디바이스: 기능에 따라 다름

지원되는 Defense Center: 기능에 따라 다름

캡처된 파일, 파일 이벤트 및 악성코드 이벤트를 검토할 때 Context Explorer, 적절히 구성된 대시보드 위젯, 각종 이벤트 보기에서 파일의 전파 흔적 맵을 볼 수 있습니다. Network File Trajectory List 페이지에서도 최근에 본 네트워크 파일 전파 흔적 및 최근에 탐지된 악성코드를 검토할 수 있습니다.

자세한 내용은 다음 절을 참조하십시오.

- 56-26페이지의 Top File Names 그래프 보기
- 56-39페이지의 Context Explorer 데이터에 대해 드릴다운
- 55-11페이지의 Custom Analysis 위젯 이해
- 37-20페이지의 아카이브 파일 검사 옵션 구성
- 40-10페이지의 파일 이벤트 테이블 이해
- 40-21페이지의 악성코드 이벤트 테이블 이해
- 40-32페이지의 캡처된 파일 테이블 이해
- 39-11페이지의 연결 및 보안 인텔리전스 이벤트에서 제공되는 정보
- 40-37페이지의 네트워크 파일 전파 흔적에 액세스

네트워크 파일 전파 흔적에 액세스

라이센스: 악성코드 또는 모두

지원되는 디바이스: 기능에 따라 다름

지원되는 Defense Center: 기능에 따라 다름

Network File Trajectory List 페이지에서는 SHA-256 해시 값이 있는 파일을 찾거나, 최근에 탐지된 악성코드를 분석하거나, 특정 위협을 추적할 수 있습니다.

이 페이지에는 네트워크에서 최근에 탐지한 악성코드는 물론 최근에 전파 흔적 맵을 살펴본 파일도 표시됩니다. 네트워크에서 최근에 파일을 본 시간, 파일의 SHA-256 해시 값, 이름, 형식, 현재 파일 성향, 내용(아카이브 파일의 경우), 파일과 관련된 이벤트 수 등을 이러한 목록에서 확인할 수 있습니다. 필드에 대한 자세한 내용은 40-10페이지의 파일 이벤트 테이블 이해을/를 참조하십시오.

이 페이지에는 SHA-256 해시 값이나 파일 이름을 기반으로, 또는 파일을 전송하거나 수신한 호스트의 IP 주소별로 파일을 찾을 수 있는 검색 상자도 포함되어 있습니다. 파일을 찾은 후 **File SHA256** 값을 클릭하여 자세한 전파 흔적 맵을 볼 수 있습니다. 자세한 내용은 40-38페이지의 네트워크 파일 전파 흔적 분석을/를 참조하십시오.

FireSIGHT 시스템은 이벤트 뷰어, 이벤트 검색, 대시보드, Context Explorer를 비롯한 웹 인터페이스의 모든 영역에서 유니코드(UTF-8) 파일 이름의 표시와 입력을 지원합니다. 그러나 PDF 형식으로 생성하는 보고서는 유니코드를 지원하지 않습니다. 유니코드 파일 이름은 PDF 보고서에 음역 형태로 나타납니다. 자세한 내용은 57-26페이지의 보고서 생성 및 보기을/를 참조하십시오.

악성코드 라이센스를 DC500에서 사용할 수 없고 악성코드 라이센스를 Series 2 디바이스 또는 Cisco NGIPS for Blue Coat X-Series에서 활성화할 수 없으므로 악성코드 클라우드 조회를 수행할 파일의 전파 흔적을 보는 데 이러한 어플라이언스를 사용할 수 없습니다.

Network File Trajectory List 페이지에서 파일을 찾으려면

액세스: Any

1단계 **Analysis > Files > Network File Trajectory**를 선택합니다.

최근에 본 파일 및 최근 악성코드가 표시된 Network File Trajectory List 페이지가 나타납니다.

2단계 선택적으로, 전체 SHA-256 해시 값, 호스트 IP 주소 또는 추적할 파일의 파일 이름을 검색 필드에 입력하고 Enter 키를 누를 수 있습니다.

검색과 일치하는 모든 파일이 나열된 Query Results 페이지가 나타납니다. 일치하는 결과가 하나뿐이면 해당 파일의 Network File Trajectory 페이지가 나타납니다.

네트워크 파일 전파 흔적 분석

라이센스: 악성코드 또는 모두

지원되는 디바이스: 기능에 따라 다름

지원되는 Defense Center: 기능에 따라 다름

자세한 네트워크 파일 전파 흔적을 살펴봄으로써 네트워크를 통해 파일을 추적할 수 있습니다. 파일의 전파 흔적은 파일에 대한 요약 정보를 보여주고, 시간에 따른 데이터 포인트를 차트화한 맵을 표시하며, 테이블의 데이터 포인트와 연결된 이벤트 데이터를 나열합니다. 테이블과 맵을 사용하면 특정 파일 이벤트, 이 파일을 전송하거나 수신한 네트워크의 호스트, 맵의 관련 이벤트, 선택한 값으로 제한된 테이블의 기타 관련 이벤트를 정확히 확인할 수 있습니다.

악성코드 라이센스를 DC500에서 사용할 수 없고 악성코드 라이센스를 Series 2 디바이스 또는 Cisco NGIPS for Blue Coat X-Series에서 활성화할 수 없으므로 악성코드 클라우드 조회를 수행할 파일의 전파 흔적을 보는 데 이러한 어플라이언스를 사용할 수 없습니다.

자세한 내용은 다음 절을 참조하십시오.

- 40-38페이지의 요약 정보
- 40-41페이지의 전파 흔적 맵
- 40-43페이지의 이벤트 테이블

요약 정보

라이센스: 악성코드 또는 모두

지원되는 디바이스: 기능에 따라 다름

지원되는 Defense Center: 기능에 따라 다름

파일의 전파 흔적 페이지에는 파일 식별 정보, 파일을 처음 본 시간과 네트워크에서 최근에 본 시간, 파일과 관련된 이벤트와 호스트의 수, 파일의 현재 성향을 비롯한 파일에 대한 기본 정보가 표시됩니다. 관리되는 디바이스가 파일을 저장한 경우 이 섹션에서 로컬로 다운로드하거나, 동적 분석을 위해 파일을 제출하거나, 파일 목록에 파일을 추가할 수 있습니다.

팁 관련 파일 이벤트를 보려면 필드 값 링크를 클릭하십시오. File Events 기본 워크플로의 첫 번째 페이지가 새 창에서 열리고, 선택한 값도 포함하는 모든 파일 이벤트가 표시됩니다.

다음 표에서는 요약 정보 필드에 대해 설명합니다.

표 40-7 네트워크 파일 전파 흔적 요약 정보 필드

이름	설명
File SHA256	파일의 SHA-256 해시 값. 해시는 기본적으로 압축된 형식으로 표시됩니다. 전체 해시 값을 보려면 포인터를 값 위로 이동합니다. 파일 이름 하나에 여러 SHA-256 해시 값이 연결되어 있는 경우 모든 해시 값을 보려면 포인터를 링크 위로 이동합니다. 파일을 로컬 컴퓨터로 다운로드하려면 파일 다운로드 아이콘( )을 클릭합니다. 프롬프트가 표시되면 파일 다운로드를 확인합니다. 파일을 저장하려면 브라우저의 프롬프트를 따릅니다. 파일을 다운로드할 수 없는 경우 이 아이콘이 회색으로 표시됩니다. **주의** Cisco 사용자는 유해한 결과로 이어질 수 있는 악성코드를 다운로드해서는 **안 됩니다**. 어떤 파일을 다운로드할 때 악성코드를 포함했을 수도 있으므로 각별히 주의하십시오. 파일을 다운로드하기 전에 다운로드할 위치를 보호하기 위해 필요한 모든 예방 조치를 취해야 합니다.
File Names	이벤트와 연결된, 네트워크에서 표시되는 파일의 이름. 여러 파일 이름이 하나의 SHA-256 해시 값에 연결되어 있으면 최근에 탐지된 파일 이름이 나열됩니다. 나머지 파일 이름을 보려면 more를 클릭하여 확장할 수 있습니다.
File Type	파일의 파일 형식(예: HTML 또는 MSEXE).
File Category	파일 형식의 일반 카테고리(예: Office Documents 또는 System Files).
Parent Application	탐지가 발생했을 때 악성코드 파일에 액세스하는 클라이언트 애플리케이션. 이러한 애플리케이션은 네트워크 검색 또는 애플리케이션 제어에 연결되지 **않습니다**. 이 필드는 엔드포인트 기반 악성코드 이벤트에 대해서만 나타납니다.
First Seen	관리되는 디바이스 또는 FireAMP Connector가 파일을 처음 탐지한 시간, 파일을 처음 업로드한 호스트의 IP 주소.
Last Seen	관리되는 디바이스 또는 FireAMP Connector가 파일을 최근에 탐지한 시간, 그리고 파일을 마지막으로 다운로드한 호스트의 IP 주소.
Event Count	네트워크에 표시되는 파일과 관련된 이벤트의 수, 그리고 탐지된 이벤트가 250개가 넘는 경우 맵에 표시되는 이벤트의 수.
Seen On	파일을 전송했거나 수신한 호스트의 수. 한 호스트가 다른 시간에 파일을 업로드 및 다운로드할 수 있으므로 총 호스트 수는 Seen On Breakdown 필드에 지정된 총 전송자 수와 총 수신자 수의 합과 일치하지 않을 수 있습니다.
Seen On Breakdown	파일을 보낸 호스트의 수와 파일을 받은 호스트의 수.

표 40-7 네트워크 파일 전파 흔적 요약 정보 필드(계속)

이름	설명
Current Disposition	다음 파일 성향 중 하나: • Malware - 클라우드가 파일을 악성코드로 분류했으며 파일의 위협 점수가 파일 정책에 정의된 악성코드 임계값을 초과했음을 나타냅니다. • Clean - 클라우드가 파일을 정상으로 분류했거나, 사용자가 파일을 정상 목록에 추가했음을 나타냅니다. • Unknown - 클라우드가 성향을 할당하기 전에 악성코드 클라우드 조회가 발생했음을 나타냅니다. 파일이 분류되지 않습니다. • Custom Detection - 사용자가 파일을 사용자 지정 탐지 목록에 추가했음을 나타냅니다. • Unavailable - 방어 센터에서 악성코드 클라우드 조회를 수행할 수 없음을 나타냅니다. 이 성향의 이벤트는 비율이 낮을 수 있는데, 이는 정상적인 상황입니다. • N/A - Detect Files 또는 Block Files 규칙이 파일을 처리했으며 방어 센터에서 악성코드 클라우드 조회를 수행하지 않았음을 나타냅니다. 정상 목록 또는 사용자 지정 탐지 목록에 파일을 추가하거나 목록에서 파일을 제거하려면 수정 아이콘( )을 클릭합니다. 이 필드는 네트워크 기반 악성코드 이벤트에 대해서만 나타납니다.
Archive Contents	검사한 아카이브 파일의 경우 아카이브에 포함된 파일의 수. Archive Contents 창에서 파일 내용에 대한 정보를 보려면 보기 아이콘( )을 클릭합니다. 아카이브 파일 검사에 대한 자세한 내용은 37-20페이지의 아카이브 파일 검사 옵션 구성을/를 참조하십시오.
Threat Name	파일과 연결된 악성코드 위협의 이름. 이 필드는 엔드포인트 기반 악성코드 이벤트에 대해서만 나타납니다.
Threat Score	파일의 위협 점수 • Low( ) • Medium( ) • High( ) • Very High( ) Dynamic Analysis Summary 보고서를 보려면 위협 점수 아이콘을 클릭합니다. 모든 캡처된 파일을 해당 위협 점수와 함께 보려면 위협 점수 링크를 클릭합니다. 동적 분석을 위해 클라우드에 파일을 제출하려면 클라우드 아이콘( )을 클릭합니다. 파일을 제출할 수 없거나 클라우드에 연결할 수 없는 경우 이 아이콘이 회색으로 표시됩니다.

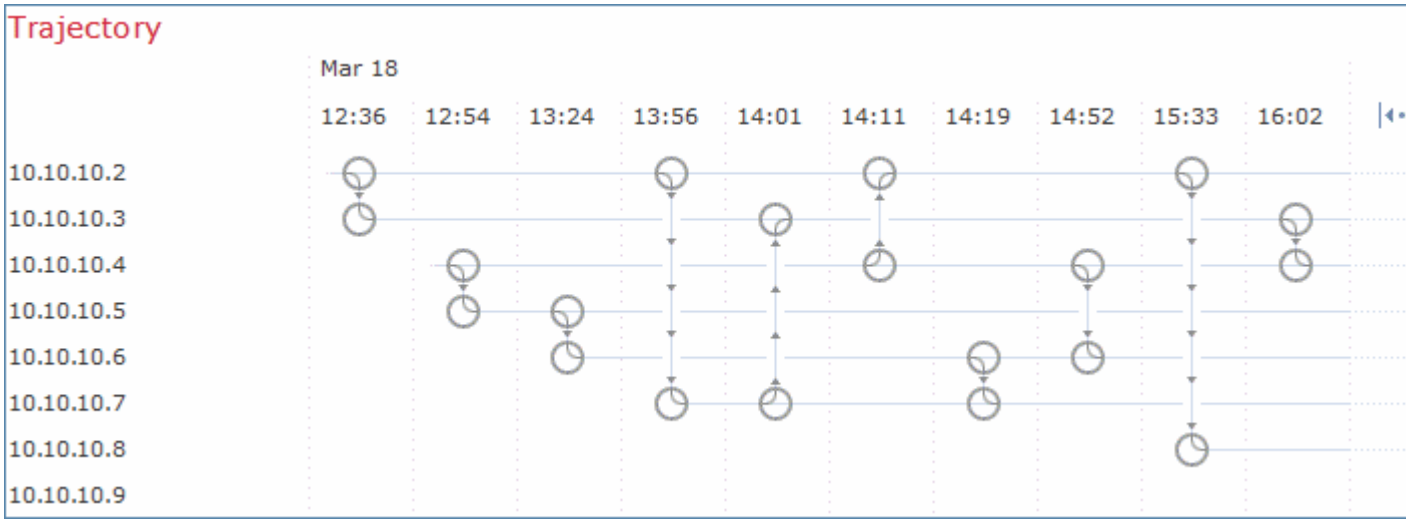
전파 흔적 맵

라이센스: 악성코드 또는 모두

지원되는 디바이스: 기능에 따라 다름

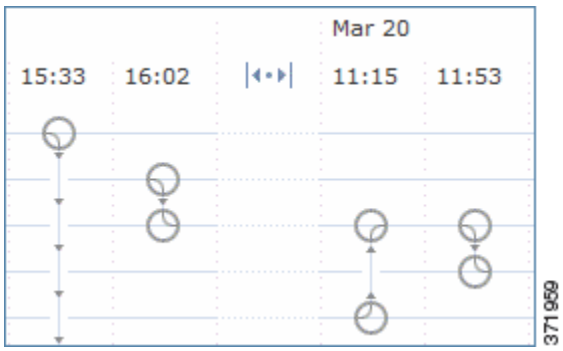
지원되는 Defense Center: 기능에 따라 다름

파일의 전파 흔적 맵은 네트워크에서의 첫 번째 탐지에서 최근까지 파일을 시각적으로 추적합니다. 맵에는 호스트가 파일을 전송하거나 수신한 시간, 파일 전송 빈도, 파일이 차단되거나 격리된 시간이 표시됩니다. 또한 파일에 대해 파일 이벤트가 발생한 빈도 및 시스템이 성향 또는 소급 성향을 할당한 시간도 표시됩니다. 맵에서 데이터 포인트를 선택하고 호스트가 파일을 처음 전송한 시점으로 역추적하는 경로를 강조 표시할 수 있습니다. 이 경로는 또한 파일의 전송자 또는 수신자로서 호스트가 개입한 모든 시점과 교차합니다. 다음 그림에서는 전파 흔적 맵의 예를 보여줍니다.



맵의 y축에는 파일과 상호작용한 모든 호스트 IP 주소의 목록이 포함됩니다. IP 주소는 시스템이 해당 호스트에서 파일을 처음 탐지한 시점을 기반으로 내림차순으로 나열됩니다. 각 행에는 단일 파일 이벤트, 파일 전송 또는 소급 이벤트 등 해당 IP 주소와 관련된 모든 이벤트가 포함됩니다. X축에는 시스템이 각 이벤트를 탐지한 날짜와 시간이 포함됩니다. 타임스탬프는 시간순으로 나열됩니다. 1분 내에 여러 이벤트가 발생한 경우 모두가 동일한 열에 나열됩니다. 추가 이벤트 및 IP 주소를 보려면 맵을 가로와 세로로 스크롤할 수 있습니다.

맵에는 파일 SHA-256 해시와 관련된 최대 250개의 이벤트가 표시됩니다. 이벤트가 250개가 넘으면 처음 10개가 표시되고 추가 이벤트는 화살표 아이콘(|◂•▸|)과 함께 생략됩니다. 그런 다음 나머지 이벤트 240개가 표시됩니다. 다음 그림에서는 화살표 아이콘과 함께 생략된 이벤트를 보여줍니다.

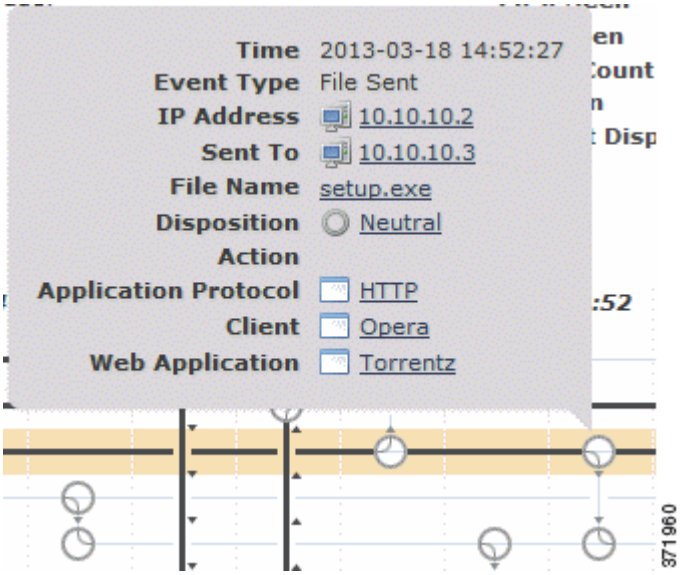


화살표 아이콘(|◂▸|)을 클릭하면 File Summary 이벤트 보기에 표시되지 않은 모든 이벤트를 볼 수 있습니다. File Events 기본 워크플로의 첫 번째 페이지는 파일 형식을 기반으로 제한된 모든 추가 이벤트와 함께 새 창에 나타납니다. 엔드포인트 기반 악성코드 이벤트가 표시되지 않으면 악성코드 이벤트 테이블로 전환하여 이러한 이벤트를 표시해야 합니다.

각 데이터 포인트는 맵 아래의 범례에 설명된 대로 이벤트 및 파일 성향을 나타냅니다. 예를 들어 Malware Block 이벤트 아이콘은 Malicious Disposition 아이콘과 Block Event 아이콘을 결합합니다.

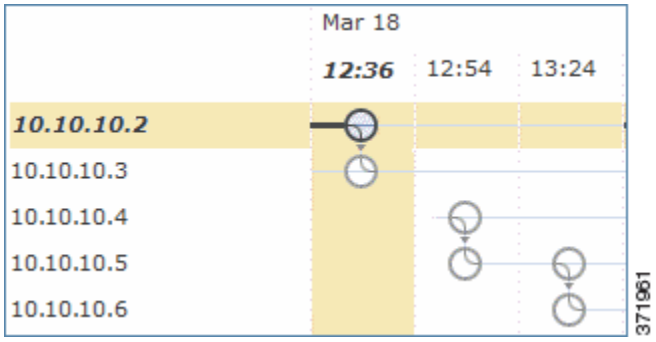
엔드포인트 기반 악성코드 이벤트는 아이콘 하나를 포함합니다. 소급 이벤트는 파일이 탐지된 각 호스트에 대한 열에 아이콘을 표시합니다. 파일 전송 이벤트에는 항상 두 개의 아이콘, 즉 파일 보내기 아이콘과 파일 받기 아이콘이 포함되며, 이 둘은 세로 선으로 연결됩니다. 화살표는 전송자에서 수신자로의 파일 전송 방향을 나타냅니다.

포인터를 이벤트 아이콘( ) 위로 이동하면 이벤트 아이콘에서 요약 정보를 볼 수 있습니다. 표시된 요약 정보는 이벤트 테이블에 표시된 정보와 일치합니다. 다음 그림에서는 이벤트 아이콘의 요약 정보를 보여줍니다.



이벤트 요약 정보 링크를 클릭하면 파일 형식을 기반으로 제약된 모든 추가 이벤트와 함께 File Events 기본 워크플로의 첫 번째 페이지가 새 창에 나타나고, File Summary 이벤트 보기가 새 창에서 열리며 사용자가 클릭한 기준 값과 일치하는 모든 파일 이벤트가 표시됩니다.

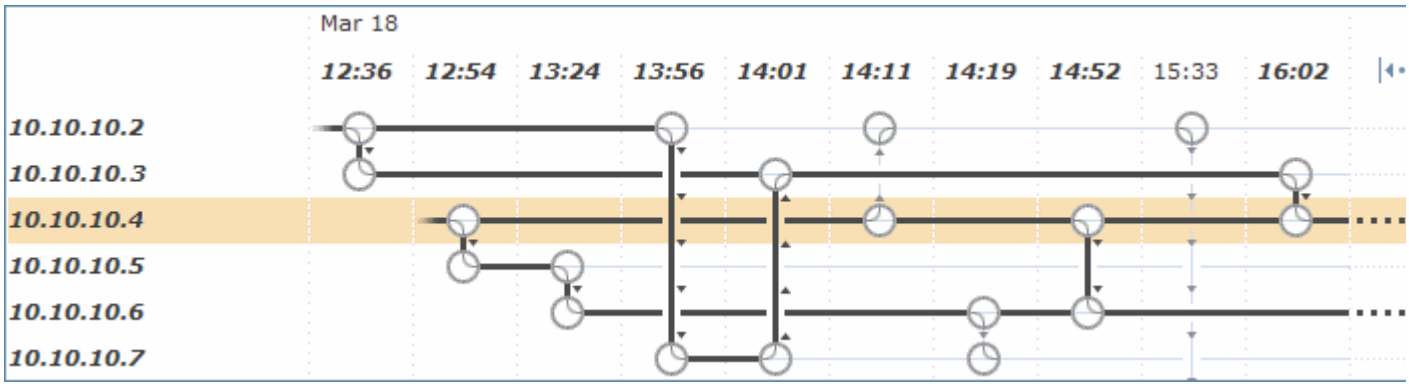
IP 주소와 관련하여 파일 이벤트가 처음 발생한 시점을 찾으려면 주소를 클릭합니다. 그러면 해당 데이터 포인트에 대한 경로는 물론 첫 번째 파일 이벤트와 관련된 중간 파일 이벤트 및 IP 주소도 강조 표시됩니다. 이벤트 테이블의 해당 이벤트도 강조 표시됩니다. 현재 보이지 않으면 해당 데이터 포인트로 맵이 스크롤됩니다. 다음 그림에서는 IP 주소를 클릭한 후 강조 표시되는 경로를 보여줍니다.



네트워크에서 파일의 진행 상황을 추적하려면, 원하는 데이터 포인트를 클릭하여 이와 연결된 모든 데이터 포인트를 포함하는 경로를 강조 표시할 수 있습니다. 여기에는 다음 이벤트 유형과 관련된 데이터 포인트가 포함됩니다.

- 연결된 IP 주소가 전송자 또는 수신자인 파일 전송
- 연결된 IP 주소와 관련된 엔드포인트 기반 악성코드 이벤트
- 또 다른 IP 주소가 관련된 경우, 연결된 해당 IP 주소가 전송자 또는 수신자인 모든 파일 전송
- 또 다른 IP 주소가 관련된 경우, 다른 IP 주소가 관련된 엔드포인트 기반 악성코드 이벤트

다음 그림에서는 이벤트 아이콘을 클릭한 후 강조 표시되는 경로를 보여줍니다.



강조 표시된 데이터 포인트와 연결된 모든 IP 주소 및 타임스탬프도 강조 표시됩니다. 이벤트 테이블의 해당 이벤트도 강조 표시됩니다. 경로에 생략된 이벤트가 포함된 경우 경로 자체는 점선으로 강조 표시됩니다. 생략된 이벤트는 경로와 교차할 수도 있지만 맵에는 표시되지 않습니다.

이벤트 테이블

라이센스: 악성코드 또는 모두

지원되는 디바이스: 기능에 따라 다름

지원되는 Defense Center: 기능에 따라 다름

이벤트 테이블에는 맵의 각 데이터 이벤트에 대한 이벤트 정보가 나열됩니다. 열 제목을 클릭하여 오름차순 또는 내림차순으로 이벤트를 정렬할 수 있습니다. 테이블 행을 선택하여 맵에서 데이터 포인트를 강조 표시할 수 있습니다. 선택한 파일 이벤트가 현재 보이지 않는 경우 해당 이벤트를 표시하도록 맵이 스크롤됩니다. 필드에 대한 자세한 내용은 40-10페이지의 파일 이벤트 테이블 이해을/를 참조하십시오.

41장

침입 이벤트 작업

FireSIGHT 시스템을 사용하면 네트워크에서 호스트와 호스트 데이터의 가용성, 무결성 및 신뢰성에 영향을 줄 수 있는 트래픽을 모니터링할 수 있습니다. 주요 네트워크 세그먼트에 관리되는 디바이스를 배치함으로써 악의적인 활동을 위해 네트워크에서 이동하는 패킷을 검토할 수 있습니다. 시스템에는 공격자들이 개발한 광범위한 익스플로잇을 찾기 위해 사용되는 몇 가지 메커니즘에 있습니다.

시스템은 침입 가능성을 식별하면 날짜, 시간, 익스플로잇 유형, 그리고 공격 소스와 대상에 대한 컨텍스트 정보의 레코드인 *침입 이벤트*를 생성합니다. 패킷 기반 이벤트의 경우 이벤트를 트리거한 패킷의 사본도 기록됩니다. 관리되는 디바이스는 방어 센터에 이벤트를 전송합니다. 여기에서 집계된 데이터를 보고 네트워크 자산에 대한 공격을 더 잘 이해할 수 있습니다.

또한 관리되는 디바이스를 인라인, 스위치드 또는 라우티드 침입 시스템으로 구축할 수 있으며, 이를 통해 해로운 것으로 알려진 패킷을 삭제 또는 교체하도록 디바이스를 구성할 수 있습니다.

FireSIGHT 시스템은 또한 침입 이벤트를 검토하고, 이러한 이벤트가 네트워크 환경 및 보안 정책의 컨텍스트에서 중요한지를 평가하기 위해 필요한 툴을 제공합니다. 이러한 툴에는 다음이 포함됩니다.

- 관리되는 디바이스에서 현재 활동을 검토할 수 있는 이벤트 요약 페이지
- 선택한 기간에 대해 생성할 수 있는 텍스트 기반 보고서와 그래프 보고서. 사용자는 자신의 보고서를 설계하고 예약된 간격으로 실행되도록 구성할 수 있습니다.
- 공격과 관련된 이벤트 데이터를 수집하기 위해 사용할 수 있는 인시던트 처리 툴. 조사와 응답을 추적하는 데 도움이 되도록 메모를 추가할 수도 있습니다.
- SNMP, 이메일 및 syslog를 위해 구성할 수 있는 자동화된 알림
- 특정 침입 이벤트에 대한 응답과 교정에 사용할 수 있는 자동화된 상관관계 정책
- 더 자세히 조사할 이벤트를 식별하기 위해 데이터에서 드릴다운할 수 있는 사전 정의 및 사용자 지정 워크플로

자세한 내용은 다음 절을 참조하십시오.

- 41-2페이지의 침입 이벤트 통계 보기 — 어플라이언스 상태의 개요 및 네트워크에 대한 상위 위협의 요약을 제공하는 Intrusion Event Statistics 페이지에 대해 설명합니다.
- 41-5페이지의 침입 이벤트 성능 보기 — 침입 이벤트 성능 통계의 그래프를 생성하는 방법에 대해 설명합니다.
- 41-8페이지의 침입 이벤트 그래프 보기 — 시간에 따른 이벤트 추세를 보여주는 차트를 생성하는 방법에 대해 설명합니다.
- 41-9페이지의 침입 이벤트 보기 — 침입 이벤트를 보고 조사하기 위한 웹 인터페이스의 사용 방법에 대해 설명합니다.

- 41-17페이지의 침입 이벤트에 대한 워크플로 페이지 이해 — 침입 이벤트 워크플로에서 사용할 수 있는 다양한 페이지 및 이러한 페이지를 사용하여 침입 이벤트를 분석하는 방법에 대해 설명합니다.
- 41-19페이지의 드릴다운 및 테이블 보기 페이지 사용 — 침입 이벤트 워크플로에서 두 가지 페이지 유형의 기능에 대해 설명합니다.
- 41-22페이지의 패킷 보기 사용 — 침입 이벤트의 패킷 보기 사용 방법에 대해 설명합니다.
- 41-38페이지의 이벤트를 평가하기 위한 영향 레벨 사용 — 영향 수준을 사용하여 침입 이벤트를 평가하는 방법에 대해 설명합니다.
- 41-39페이지의 프리프로세서 이벤트 읽기 — 프리프로세서 규칙에 의해 생성되는 이벤트를 읽는 방법에 대해 설명합니다.
- 41-42페이지의 침입 이벤트 검색 — 검색 기능을 사용하여 침입 이벤트의 목록을 특정 기준으로 제한하는 방법에 대해 설명합니다.
- 41-50페이지의 클립보드 사용 — 나중에 인시던트에 추가할 수 있도록 침입 이벤트를 클립보드라는 보관 영역에 추가하는 방법에 대해 설명합니다. 이 절에서는 또한 클립보드의 내용을 기반으로 이벤트 보고서를 생성하는 방법에 대해 설명합니다.

다음도 참조하십시오.

- 42-1페이지의 인시던트 처리 — 인시던트 처리 방법 및 인시던트를 사용하여 이벤트 분석의 진행 상황을 추적하는 방법에 대해 설명합니다.
- 44-1페이지의 침입 규칙에 대한 외부 알림 구성 — 자동화된 알림에 대해 설명합니다.
- 57-1페이지의 보고서 작업 — 침입 이벤트 보고서에 대해 설명합니다.
- 58-20페이지의 지오로케이션 사용 — 침입 이벤트의 지오로케이션 정보에 대해 설명합니다.

침입 이벤트 통계 보기

라이센스: 보호

Intrusion Event Statistics 페이지에서는 어플라이언스의 현재 상태 및 네트워크에 대해 생성된 침입 이벤트에 대한 빠른 요약을 제공합니다.

Intrusion Event Statistics 페이지에는 세 가지 주요 영역이 있습니다.

- 41-3페이지의 호스트 통계 — 어플라이언스 및 관리되는 디바이스(방어 센터의 경우)에 대한 정보를 제공하는 Host Statistics 섹션에 대해 설명합니다.
- 41-4페이지의 이벤트 개요 — 이벤트 데이터베이스에서 정보의 개요를 제공하는 Event Overview에 대해 설명합니다.
- 41-4페이지의 이벤트 통계 — 이벤트 데이터베이스의 정보에 대한 구체적인 세부사항(예: 상위 10개 이벤트 유형)을 제공하는 Event Statistics에 대해 설명합니다.

페이지에 있는 각 IP 주소, 포트, 프로토콜, 이벤트 메시지 등은 링크입니다. 관련 이벤트 정보를 보려면 링크를 클릭하십시오. 예를 들어 상위 10개 목적지 포트 중 하나가 `80 (http)/tcp`인 경우 해당 링크를 클릭하면 기본 침입 이벤트 워크플로의 첫 번째 페이지가 표시되고, 해당 포트를 대상으로 하는 이벤트가 나열됩니다. 현재 시간 범위의 이벤트(그리고 이벤트를 생성하는 관리되는 디바이스)만 나타납니다. 또한 검토한 것으로 표시한 침입 이벤트는 통계에 계속 나타납니다. 예를 들어 현재의 시간 범위가 과거 시간이지만 첫 번째 이벤트가 5시간 전에 생성된 경우 **First Event** 링크를 클릭하면, 시간 범위를 변경하기 전에는 결과 이벤트 페이지에 이벤트가 표시되지 않습니다.

침입 이벤트 통계를 보려면

액세스: Admin/Intrusion Admin

1단계 **Overview > Summary > Intrusion Event Statistics**를 선택합니다.

Intrusion Event Statistics 페이지가 나타납니다.

2단계 페이지 상단에 있는 두 개의 선택 상자에서 통계를 보려는 영역 및 디바이스를 선택합니다. 침입 이벤트를 수집하는 모든 디바이스에 대한 통계를 보려면 **All Security Zones** 및 **All Devices**를 선택합니다.

3단계 **Get Statistics**를 클릭합니다.

Intrusion Event Statistics 페이지가 선택한 디바이스의 데이터로 새로 고쳐집니다.

팁 사용자 지정 시간 범위의 데이터를 보려면 오른쪽 위 페이지 영역의 링크를 클릭하고 58-22페이지의 이벤트 시간 제약 조건 설정의 지침을 따르십시오.

4단계 Intrusion Event Statistics 페이지에 나타나는 통계에 대한 자세한 내용은 다음 절을 참조하십시오.

- 41-3페이지의 호스트 통계
- 41-4페이지의 이벤트 개요
- 41-4페이지의 이벤트 통계

호스트 통계

라이센스: 보호

Intrusion Event Statistics 페이지의 Host Statistics 절에서는 어플라이언스 자체에 대한 정보를 제공합니다. 방어 센터의 경우 이 섹션에서는 관리되는 디바이스에 대한 정보도 제공합니다.

이 정보에는 다음 항목이 포함됩니다.

- **Time** — 어플라이언스의 현재 시간을 표시합니다.
- **Uptime** — 어플라이언스 자체를 다시 시작한 이후의 일수, 시간 및 분을 표시합니다. 방어 센터의 경우 각 관리되는 디바이스가 마지막으로 재부팅된 시간, 로그인한 사용자의 수 및 로드 평균도 표시됩니다.
- **Disk Usage** — 사용되고 있는 디스크의 비율을 표시합니다.
- **Memory Usage** — 사용되고 있는 시스템 메모리의 비율을 표시합니다.
- **Load Average** — 지난 1분, 5분 및 15분 동안 CPU 대기열의 평균 프로세스 수를 표시합니다.

이벤트 개요

라이센스: 보호

Intrusion Event Statistics 페이지의 Event Overview 섹션에서는 침입 이벤트 데이터베이스의 정보 개요를 제공합니다.

이러한 통계는 다음과 같습니다.

- **Events** — 침입 이벤트 데이터베이스의 이벤트 수를 표시합니다.
- **Events in Time Range** — 현재 선택된 시간 범위는 물론 시간 범위에 속하는 데이터베이스의 이벤트 수와 비율도 표시합니다.
- **First Event** — 이벤트 데이터베이스의 첫 번째 이벤트에 대한 이벤트 메시지를 표시합니다.
- **Last Event** — 이벤트 데이터베이스의 마지막 이벤트에 대한 이벤트 메시지를 표시합니다.

참고 방어 센터의 경우 관리되는 디바이스를 선택했다면 해당 디바이스의 Event Overview 섹션이 대신 나타납니다.

이벤트 통계

라이센스: 보호

Intrusion Event Statistics 페이지의 Event Statistics 섹션에서는 침입 이벤트 데이터베이스의 정보에 대한 좀 더 구체적인 정보를 제공합니다.

이 정보에는 다음에 대한 세부사항이 포함됩니다.

- 상위 10개 이벤트 유형
- 상위 10개 소스 IP 주소
- 상위 10개 목적지 IP 주소
- 상위 10개 목적지 포트
- 이벤트 수가 가장 많은 프로토콜, 인그레스와 이그레스 보안 영역, 디바이스

침입 이벤트 성능 보기

라이센스: 보호

침입 이벤트 성능 페이지에서는 특정 기간 동안 침입 이벤트의 성능 통계를 보여주는 그래프를 생성할 수 있습니다. 초당 침입 이벤트의 수, 초당 메가비트의 수, 패킷당 평균 바이트 수, Snort에서 검사하지 않은 패킷의 비율, TCP 표준화의 결과 차단된 패킷의 수를 보여주는 그래프를 생성할 수 있습니다. 이러한 그래프는 운영의 마지막 시간, 마지막 날, 마지막 주 또는 마지막 달에 대한 통계를 보여줄 수 있습니다.

자세한 내용은 41-5페이지의 침입 이벤트 성능 통계 그래프 생성을/를 참조하십시오.

침입 이벤트 성능 통계를 보려면

액세스: Admin/Maint

1단계 **Overview > Summary > Intrusion Event Performance**를 선택합니다.

Intrusion Event Performance 페이지가 나타납니다.

침입 이벤트 성능 통계 그래프 생성

라이센스: 보호

초당 이벤트 수, 초당 메가비트, 패킷당 평균 바이트, Snort에서 검사하지 않은 패킷의 비율, TCP 표준화의 결과 차단된 패킷의 수를 기반으로 방어 센터 또는 관리되는 디바이스에 대한 성능 통계를 보여주는 그래프를 생성할 수 있습니다.

참고 새 데이터는 통계 그래프를 위해 5분마다 누적됩니다. 따라서 그래프를 빠르게 다시 로드하는 경우 다음 5분 증가분이 발생하기까지 데이터가 변경되지 않을 수 있습니다.

다음 표에는 사용 가능한 그래프 유형이 나열되어 있습니다. 네트워크 분석 정책 **Inline Mode** 설정의 영향을 받는 데이터로 채워지는 경우 그래프 유형이 다르게 표시됩니다. **Inline Mode**가 비활성화되어 있으면 웹 인터페이스에서 별표(*)로 표시된 그래프 유형(아래의 열에서 `yes`로 표시된 행)은, **Inline Mode**가 활성화되었다면 시스템에서 수정 또는 삭제했을 트래픽에 대한 데이터로 채워집니다. **인라인 모드** 설정에 대한 자세한 내용은 26-5페이지의 인라인 구축에서 프리프로세서가 트래픽에 영향을 미치도록 허용을/를 참조하십시오.

필수 옵션 및 설정에 대한 자세한 내용은 29-7페이지의 인라인 트래픽 표준화, 26-5페이지의 인라인 구축에서 프리프로세서가 트래픽에 영향을 미치도록 허용 및 31-6페이지의 인라인 구축에서 삭제 동작 설정을/를 참조하십시오.

표 41-1 침입 이벤트 성능 그래프 유형

데이터를 생성할 항목	수행해야 할 작업	나타내는 내용	Inline Mode의 영향을 받는지 여부
Avg Bytes/Packet	해당 없음	각 패킷에 포함된 평균 바이트 수	아니요
ECN Flags Normalized in TCP Traffic/Packet	**Explicit Congestion Notification**을 활성화하고 **Packet** 선택	협상과 상관없이 패킷 단위로 ECN 플래그가 지워진 패킷의 수	예

표 41-1 침입 이벤트 성능 그래프 유형(계속)

데이터를 생성할 항목	수행해야 할 작업	나타내는 내용	Inline Mode의 영향을 받는지 여부
ECN Flags Normalized in TCP Traffic/Session	**Explicit Congestion Notification**을 활성화하고 **Stream** 선택	ECN 사용이 협상되지 않은 경우 스트림 단위로 ECN 플래그가 지워진 횟수	예
Events/Sec	해당 없음	디바이스에서 생성되는 초당 이벤트의 수	아니요
ICMPv4 Echo Normalizations	**Normalize ICMPv4** 활성화	Echo(Request) 또는 Echo Reply 메시지의 8비트 Code 필드가 지워진 ICMPv4 패킷의 수	예
ICMPv6 Echo Normalizations	**Normalize ICMPv6** 활성화	Echo(Request) 또는 Echo Reply 메시지의 8비트 Code 필드가 지워진 ICMPv6 패킷의 수	예
IPv4 DF Flag Normalizations	**Normalize IPv4** 및 **Normalize Don't Fragment Bit** 활성화	IPv4 Flags 헤더의 단일 비트 Don't Fragment 하위 필드가 지워진 IPv4 패킷의 수	예
IPv4 Options Normalizations	**Normalize IPv4** 활성화	옵션 옥텟이 1(No Operation)로 설정된 IPv4 패킷의 수	예
IPv4 Reserved Flag Normalizations	**Normalize IPv4** 및 **Normalize Reserved Bit** 활성화	IPv4 Flags 헤더의 단일 비트 Reserved 하위 필드가 지워진 IPv4 패킷의 수	예
IPv4 Resize Normalizations	**Normalize IPv4** 활성화	IP 헤더에 지정된 데이터그램 길이로 잘린, 과도한 길이의 페이로드가 있는 IPv4 패킷의 수	예
IPv4 TOS Normalizations	**Normalize IPv4** 및 **Normalize TOS Bit** 활성화	1바이트 Differentiated Services(DS) 필드(이전의 Type of Service(TOS) 필드)가 지워진 IPv4 패킷의 수	예
IPv4 TTL Normalizations	**Normalize IPv4**, **Maximum TTL** 및 **Reset TTL** 활성화	IPv4 Time to Live 표준화의 수	예
IPv6 Options Normalizations	**Normalize IPv6** 활성화	Hop-by-Hop Options 또는 Destination Options 확장 헤더의 Option Type 필드가 00(건너뛰고 계속 처리)으로 설정된 IPv6 패킷의 수	예
IPv6 TTL Normalizations	**Normalize IPv6**, **Minimum TTL** 및 **Reset TTL** 활성화	IPv6 Hop Limit(TTL) 표준화의 수	예
Mbits/Sec	해당 없음	디바이스를 통해 전달되는 트래픽의 초당 메가바이트 수	아니요
Packet Resized to Fit MSS Normalizations	**Trim Data to MSS** 활성화	페이로드가 TCP Data 필드보다 길어서 Maximum Segment Size로 잘리는 패킷의 수	예
Packet Resized to Fit TCP Window Normalizations	**Trim Data to Window** 활성화	TCP Data 필드가 수신 호스트의 TCP 창에 맞게 잘리는 패킷의 수	예
Percent Packets Dropped	해당 없음	선택한 모든 디바이스에서 검사하지 않은 패킷의 평균 비율. 예를 들어 디바이스를 2개 선택하고 평균이 50%이면, 한 디바이스는 삭제율이 90%이고 나머지는 삭제율이 10%임을 나타낼 수 있습니다. 또는 두 디바이스 모두 삭제율이 50%임을 나타낼 수도 있습니다. 그래프는 단일 디바이스를 선택할 경우의 총 삭제 %만 나타냅니다.	아니요

표 41-1 침입 이벤트 성능 그래프 유형(계속)

데이터를 생성할 항목	수행해야 할 작업	나타내는 내용	Inline Mode의 영향을 받는지 여부
RST Packets With Data Stripped Normalizations	**Remove Data on RST** 활성화	TCP 재설정(RST) 패킷에서 데이터가 삭제된 패킷의 수	예
SYN Packets With Data Stripped Normalizations	**Remove Data on SYN** 활성화	TCP 운영 체제가 Mac OS가 아닐 때 SYN 패킷에서 제거된 패킷의 수	예
TCP Header Padding Normalizations	**Normalize/Clear Option Padding Bytes** 활성화	옵션 패킷 바이트가 0으로 설정되었을 때 TCP 패킷의 수	예
TCP No Option Normalizations	**Allow These TCP Options**를 활성화하고 `any` 이외의 옵션으로 설정	Time Stamp 옵션이 제거된 패킷의 수	예
TCP NS Flag Normalizations	**Explicit Congestion Notification**을 활성화하고 **Packet** 선택	ECN Nonce Sum(NS) 옵션 표준화의 수	예
TCP Options Normalizations	**Allow These TCP Options**를 활성화하고 `any` 이외의 옵션으로 설정	옵션 필드가 No Operation(TCP Option 1)으로 설정된 옵션의 수(MSS, Window Scale, Time Stamp 및 명시적으로 허용된 옵션 제외)	예
TCP Packets Blocked By Normalizations	**Normalize TCP Payload** 활성화(세그먼트 리어셈블리가 실패함)	TCP 세그먼트를 제대로 리어셈블할 수 없기 때문에 삭제된 패킷의 수	예
TCP Reserved Flags Normalizations	**Normalize/Clear Reserved Bits** 활성화	Reserved 비트가 지워진 TCP 패킷의 수	예
TCP Segment Reassembly Normalizations	**Normalize TCP Payload** 활성화(세그먼트 리어셈블리가 성공함)	재전송된 데이터의 일관성을 보장하기 위해 TCP Data 필드가 표준화된 패킷의 수(제대로 리어셈블할 수 없는 세그먼트는 삭제됨)	예
TCP SYN Option Normalizations	**Allow These TCP Options**를 활성화하고 `any` 이외의 옵션으로 설정	SYN 제어 비트가 설정되지 않아서 Maximum Segment Size or Window Scale 옵션이 No Operation(TCP Option 1)으로 설정된 옵션의 수	예
TCP Timestamp ECR Normalizations	**Allow These TCP Options**를 활성화하고 `any` 이외의 옵션으로 설정	Acknowledgment(ACK) 제어 비트가 설정되지 않았기 때문에 Time Stamp Echo Reply(TSecr) 옵션 필드가 지워진 패킷의 수	예
TCP Urgent Pointer Normalizations	**Normalize Urgent Pointer** 활성화	2바이트 TCP 헤더 Urgent Pointer 필드가 페이로드 길이보다 긴 패킷 및 페이로드 길이로 설정된 패킷의 수	예
Total Blocked Packets	**Inline Mode** 또는 **Drop when Inline** 구성	규칙, 디코더 및 프리프로세서 삭제를 비롯한 삭제된 패킷의 총수	아니요
Total Injected Packets	**Inline Mode** 구성	재전송되기 전에 크기가 조정된 패킷의 수	아니요
Total TCP Filtered Packets	TCP Stream Preprocessing 구성	TCP 포트 필터링 때문에 스트림에서 건너뛴 패킷의 수	아니요
Total UDP Filtered Packets	UDP Stream Preprocessing 구성	UDP 포트 필터링 때문에 스트림에서 건너뛴 패킷의 수	아니요

표 41-1 침입 이벤트 성능 그래프 유형(계속)

데이터를 생성할 항목	수행해야 할 작업	나타내는 내용	Inline Mode의 영향을 받는지 여부
Urgent Flag Cleared Normalizations	**Clear URG if Urgent Pointer is Not Set** 활성화	Urgent Pointer가 설정되지 않아서 TCP 헤더 URG 제어 비트가 지워진 패킷의 수	예
Urgent Pointer and Urgent Flag Cleared Normalizations	**Clear Urgent Pointer/URG on Empty Payload** 활성화	페이로드가 없기 때문에 TCP 헤더 Urgent Pointer 필드 및 URG 제어 비트가 지워진 패킷의 수	예
Urgent Pointer Cleared Normalizations	**Clear Urgent Pointer if URG=0** 활성화	Urgent(URG) 제어 비트가 설정되지 않았기 때문에 16비트 TCP 헤더 Urgent Pointer 필드가 지워진 패킷의 수	예

침입 이벤트 성능 그래프를 생성하려면

액세스: Admin/Maint

1단계 **Overview > Summary > Intrusion Event Performance**를 선택합니다.

Intrusion Event Performance 페이지가 나타납니다.

2단계 데이터를 보려는 디바이스를 **Select Device** 목록에서 선택합니다.

3단계 생성할 그래프 유형을 **Select Graph(s)** 목록에서 선택합니다.

4단계 그래프에 사용할 시간 범위를 **Select Time Range** 목록에서 선택합니다.

마지막 시간, 마지막 날, 마지막 주 또는 마지막 달 중에서 선택할 수 있습니다.

5단계 **Graph**를 클릭합니다.

지정한 정보를 보여주는 그래프가 나타납니다.

6단계 그래프를 저장하려면 마우스 오른쪽 버튼으로 그래프를 클릭한 후 이미지 저장에 대한 브라우저의 지침을 따릅니다.

침입 이벤트 그래프 보기

라이센스: 보호

FireSIGHT 시스템은 시간에 따른 침입 이벤트 추세를 보여주는 그래프를 제공합니다. 마지막 시간에서 마지막 달까지 다음에 대해 시간에 따른 침입 이벤트 그래프를 생성할 수 있습니다.

- 하나 또는 모든 관리되는 디바이스
- 상위 10개 목적지 포트
- 상위 10개 소스 IP 주소
- 상위 10개 이벤트 메시지

이벤트 그래프를 생성하려면

액세스: Admin/Intrusion Admin

1단계 **Overview > Summary > Intrusion Event Graphs**를 선택합니다.

Intrusion Event Graphs 페이지가 나타납니다. 페이지 상단에 있는 세 개의 선택 상자가 어떤 그래프를 생성할지를 제어합니다.

2단계 **Select Device** 아래에서 **all**을 선택하여 모든 디바이스를 포함하거나, 그래프에 포함하려는 특정 디바이스를 선택합니다.

3단계 생성할 그래프 유형을 **Select Graph(s)**에서 선택합니다.

4단계 그래프의 시간 범위를 **Select Time Range**에서 선택합니다.

5단계 **Graph**를 클릭합니다.

그래프가 생성됩니다.

침입 이벤트 보기

라이센스: 보호

시스템은 악의적일 가능성이 있는 패킷을 인식하면 침입 이벤트를 생성하고 데이터베이스에 추가합니다.

초기 침입 이벤트는 페이지에 액세스하는 데 사용하는 워크플로에 따라 다릅니다. 하나 이상의 드릴다운 페이지, 침입 이벤트의 테이블 보기, 종료 패킷 보기 등 사전 정의 워크플로 중 하나를 사용할 수도 있고, 고유한 워크플로를 생성할 수도 있습니다. 침입 이벤트가 포함되어 있을 수 있는 사용자 지정 테이블을 기반으로 하는 워크플로를 볼 수도 있습니다. 많은 IP 주소가 포함되었는데 **Resolve IP Addresses** 이벤트 보기 설정을 활성화한 경우 이벤트 보기를 표시하는 속도가 느려질 수 있습니다. 자세한 내용은 71-3페이지의 이벤트 보기 설정 구성을/를 참조하십시오.

네트워크 보안에 위협이 있는지를 판단하려면 침입 이벤트를 확인합니다. 침입 이벤트가 악의적이지 않다고 확신하면 이벤트를 검토한 것으로 표시할 수 있습니다. 그러면 자신의 이름이 Reviewer로 나타나며, 검토된 이벤트는 기본 침입 이벤트 보기에 더 이상 나열되지 않습니다. 이벤트를 검토하지 않은 것으로 표시함으로써 검토된 이벤트를 기본 침입 이벤트 보기로 되돌릴 수 있습니다.

검토한 것으로 표시한 침입 이벤트를 볼 수 있습니다. 검토된 이벤트는 이벤트 데이터베이스에 저장되며 이벤트 요약 통계에 포함되지만, 기본 이벤트 페이지에는 더 이상 나타나지 않습니다. 자세한 내용은 41-16페이지의 침입 이벤트 검토을/를 참조하십시오.

백업을 수행한 후 검토한 침입 이벤트를 삭제하면, 백업의 복원은 삭제된 침입 이벤트를 복원하지만 검토된 상태는 복원하지 않습니다. 복원된 침입 이벤트는 Reviewed Events가 아니라 Intrusion Events에서 볼 수 있습니다.

하나 이상의 침입 이벤트와 관련된 연결 이벤트를 빠르게 보려면 이벤트 뷰어의 확인란을 사용하여 침입 이벤트를 선택한 다음 **Jump to** 드롭다운 목록에서 **Connections**를 선택합니다. 이벤트의 테이블 보기 간에 탐색할 때에는 이 방법이 가장 유용합니다. 특별한 연결과 관련된 침입도 유사한 방법으로 볼 수 있습니다.

자세한 내용은 다음 절을 참조하십시오.

- 41-10페이지의 침입 이벤트 이해
- 58-38페이지의 사용자 지정 워크플로 생성
- 41-19페이지의 드릴다운 및 테이블 보기 페이지 사용
- 41-22페이지의 패킷 보기 사용
- 41-15페이지의 침입 이벤트와 관련된 연결 데이터 보기
- 41-16페이지의 침입 이벤트 검토
- 59-9페이지의 사용자 지정 테이블을 기반으로 워크플로 보기

침입 이벤트를 보려면

액세스: Admin/Intrusion Admin

1단계 **Analysis > Intrusions > Events**를 선택합니다.

기본 침입 이벤트 워크플로의 첫 번째 페이지가 나타납니다. 다른 기본 워크플로 지정에 대한 자세한 내용은 71-3페이지의 이벤트 보기 설정 구성을/를 참조하십시오. 이벤트가 표시되지 않을 경우 시간 범위를 조정해야 할 수 있습니다. 58-22페이지의 이벤트 시간 제약 조건 설정을/를 참조하십시오.

팁 침입 이벤트의 테이블 보기가 포함되지 않은 사용자 지정 워크플로를 사용하는 경우, 워크플로 제목 옆에 있는 **(switch workflow)**를 클릭하여 어플라이언스와 함께 제공되는 사전 정의 워크플로 중 하나를 선택하십시오.

침입 이벤트 보기에 나타나는 이벤트에 대한 자세한 내용은 41-10페이지의 침입 이벤트 이해을/를 참조하십시오. 분석에 중요한 침입 이벤트로 보기를 좁히는 방식에 대한 자세한 내용은 41-17페이지의 침입 이벤트에 대한 워크플로 페이지 이해을/를 참조하십시오.

침입 이벤트 이해

라이센스: 보호

시스템은 패킷에서 호스트와 호스트 데이터의 가용성, 무결성 및 신뢰성에 영향을 줄 수 있는, 네트워크를 이동하는 악의적인 활동을 검토합니다. 시스템은 침입 가능성을 식별하면 날짜, 시간, 익스플로잇 유형, 그리고 공격 소스와 대상에 대한 컨텍스트 정보의 레코드인 *침입 이벤트*를 생성합니다. 패킷 기반 이벤트의 경우 이벤트를 트리거한 패킷의 사본도 기록됩니다. 모든 개별 침입 이벤트에 대해 사용 가능한 정보는 라이센스를 비롯한 여러 요소에 따라 달라집니다. 자세한 내용은 65-2페이지의 라이센스 유형 및 제한 사항을/를 참조하십시오.

다음 목록에서는 침입 이벤트에 포함된 정보에 대해 설명합니다. 침입 이벤트의 테이블 보기에서 일부 필드는 기본적으로 비활성화되어 있습니다. 세션 중에 필드를 활성화하려면 확장 화살표( )를 클릭하여 검색 제약 조건을 확장한 다음 **Disabled Columns** 아래에서 열 이름을 클릭합니다.

Time

이벤트의 날짜 및 시간

Priority

Cisco VRT에 의해 결정된 이벤트 우선순위

Impact

이 필드의 영향 수준은 침입 데이터, 네트워크 검색 데이터 및 취약성 정보 사이의 상관관계를 나타냅니다. 자세한 내용은 41-38페이지의 이벤트를 평가하기 위한 영향 레벨 사용을/를 참조하십시오.

NetFlow 데이터를 기반으로 네트워크 맵에 추가된 호스트에 대해 사용할 수 있는 운영 체제 정보가 없으므로, 호스트 입력 기능을 사용하여 호스트 운영 체제 ID를 수동으로 설정하지 않는 한 방어 센터에서는 그러한 호스트와 관련된 침입 이벤트에 대해 Vulnerable (impact 1: red) 영향 레벨을 할당할 수 없습니다.

Inline Result

다음 중 하나:

- 검은색 아래쪽 화살표 — 시스템이 규칙을 트리거한 패킷을 삭제했음을 나타냄
- 회색 아래쪽 화살표 — **Drop when Inline** 침입 정책 옵션을 활성화했다면(인라인 구축에서) 또는 시스템이 정리되는 동안 Drop and Generate 규칙이 이벤트를 생성했다면 IPS가 패킷을 삭제했을 것임을 나타냅니다.
- 비어 있음 — 트리거된 규칙이 Drop 및 Generate 이벤트로 설정되지 않았음을 나타냄

침입 정책의 규칙 상태 또는 인라인 삭제 동작과 상관없이, 인라인 인터페이스가 탭 모드인 경우를 포함하여 패시브 구축에서는 시스템이 패킷을 삭제하지 않습니다.

Source IP

전송 호스트에서 사용하는 IP 주소

Source Country

전송 호스트의 국가

Destination IP

수신 호스트에서 사용하는 IP 주소

Destination Country

수신 호스트의 국가

Original Client IP

XFF(X-Forwarded-For), True-Client-IP 또는 사용자 정의 HTTP 헤더에서 추출된 원래 클라이언트 IP 주소. 이 필드의 값을 표시하려면 네트워크 분석 정책에서 HTTP 프리프로세서 **Extract Original Client IP Address** 옵션을 활성화해야 합니다. 선택적으로, 네트워크 분석 정책의 동일한 영역에서 최대 6개의 사용자 지정 클라이언트 IP 헤더를 지정할 수 있으며, 시스템이 Original Client IP 이벤트 필드에 대한 값을 선택하는 우선순위 순서를 설정할 수 있습니다. 자세한 내용은 27-32페이지의 서버 레벨 HTTP 표준화 옵션 선택을/를 참조하십시오.

이 필드는 기본적으로 활성화되어 있습니다.

Source Port / ICMP Type

전송 호스트의 포트 번호. ICMP 트래픽의 경우 포트 번호가 없으면 시스템은 ICMP 유형을 표시합니다.

Destination Port / ICMP Code

트래픽을 수신하는 호스트의 포트 번호. ICMP 트래픽의 경우 포트 번호가 없으면 시스템은 ICMP 코드를 표시합니다.

SSL Status

SSL 규칙, 기본 작업 또는 암호화된 연결을 로깅한 해독 불가능한 트래픽 작업과 관련된 작업입니다.

- `Block` 및 `Block with reset` — 차단된 암호화 연결을 나타냅니다.
- `Decrypt (Resign)` — 다시 서명된 서버 인증서를 사용하여 해독된 발신 연결을 나타냅니다.
- `Decrypt (Replace Key)` — 대체된 공개 키가 있는 자체 서명된 서버 인증서를 사용하여 해독된 발신 연결을 나타냅니다.
- `Decrypt (Known Key)` — 알려진 개인 키를 사용하여 해독된 수신 연결을 나타냅니다.
- `Do not Decrypt` — 시스템이 해독하지 못한 연결을 나타냅니다.

시스템이 암호화된 연결을 해독하지 못할 경우, 해독 불가능한 트래픽 작업이 실행되었다는 내용과 함께 실패 사유가 표시됩니다. 시스템이 알려지지 않은 암호 그룹으로 암호화 트래픽을 탐지한 후 추가 검사 없이 허용한 경우 이 필드에는 `Do Not Decrypt (Unknown Cipher Suite)`가 표시됩니다.

인증서 세부사항을 보려면 잠금 아이콘( )을 클릭합니다. 자세한 내용은 39-32페이지의 암호화된 연결과 관련된 인증서 보기을/를 참조하십시오.

VLAN ID

침입 이벤트를 트리거한 패킷과 관련된 가장 안쪽 VLAN ID

MPLS Label

이 침입 이벤트를 트리거한 패킷과 관련된 Multiprotocol Label Switching 레이블

이 필드는 기본적으로 비활성화되어 있습니다.

Message

이벤트에 대한 설명 텍스트. 규칙 기반 침입 이벤트의 경우 규칙에서 이벤트 메시지가 나옵니다. 디코더 및 프리프로세서 기반 이벤트의 경우 이벤트 메시지는 하드 코딩됩니다.

Classification

이벤트를 생성한 규칙이 속하는 분류. 규칙 분류 이름과 번호의 목록은 규칙 분류 테이블을/를 참조하십시오.

Generator

이벤트를 생성한 구성 요소. 침입 이벤트 Generator ID의 목록은 41-40 페이지의 표 41-7을/를 참조하십시오.

Source User

소스 호스트에 로그인한 알려진 사용자의 User ID

Destination User

목적지 호스트에 로그인한 알려진 사용자의 User ID

Application Protocol

침입 이벤트를 트리거한 트래픽에서 탐지된, 호스트 간의 통신을 나타내는 애플리케이션 프로토콜(사용 가능한 경우). 시스템이 방어 센터 웹 인터페이스에서 탐지된 애플리케이션 프로토콜을 식별하는 방법에 대한 자세한 내용은 45-13 페이지의 표 45-3을/를 참조하십시오.

Client

침입 이벤트를 트리거한 트래픽에서 탐지된 모니터링되는 호스트에서 실행 중인 소프트웨어를 나타내는 클라이언트 애플리케이션(사용 가능한 경우).

Web Application

침입 이벤트를 트리거한 트래픽에서 탐지된 HTTP 트래픽의 요청된 URL 또는 내용을 나타내는 웹 애플리케이션.

HTTP의 애플리케이션 프로토콜은 탐지하지만 특정 웹 애플리케이션은 탐지하지 못하는 경우 시스템은 여기에서 일반 웹 브라우징 지정을 제공합니다.

IOC

침입 이벤트를 트리거한 트래픽이 연결과 관련된 호스트에 대해 IOC(indication of compromise)도 트리거했는지 여부. IOC에 대한 자세한 내용은 45-20페이지의 IOC 이해을/를 참조하십시오.

Category, Tag(Application Protocol, Client, Web Application)

애플리케이션 기능 이해에 도움이 되도록 애플리케이션의 특성을 부여하는 기준. 45-11 페이지의 표 45-2을/를 참조하십시오.

Application Risk

침입 이벤트를 트리거한 트래픽에서 탐지된 애플리케이션과 관련된 위험. 연결에서 탐지된 각 애플리케이션 유형에는 관련된 위험이 있습니다. 이 필드에는 그중 가장 높은 위험이 표시됩니다. 자세한 내용은 45-11 페이지의 표 45-2을/를 참조하십시오.

Business Relevance

침입 이벤트를 트리거한 트래픽에서 탐지된 애플리케이션과 관련된 비즈니스 연관성. 연결에서 탐지된 각 애플리케이션 유형에는 관련된 비즈니스 연관성이 있습니다. 이 필드에는 그중 가장 낮은 값(가장 연관성이 적음)이 표시됩니다. 자세한 내용은 45-11 페이지의 표 45-2을/를 참조하십시오.

Ingress Security Zone

이벤트를 트리거한 패킷의 인그레스 보안 영역. 패시브 구축에서는 이 보안 영역 필드만 채워집니다. 3-38페이지의 보안 영역 작업을/를 참조하십시오.

Egress Security Zone

인라인 구축의 경우 이벤트를 트리거한 패킷의 이그레스 보안 영역. 패시브 구축에서는 이 보안 영역 필드가 채워지지 않습니다. 3-38페이지의 보안 영역 작업을/를 참조하십시오.

Device

액세스 제어 정책이 적용된 관리되는 디바이스. 4-1페이지의 디바이스 관리을/를 참조하십시오.

Ingress Interface

트래픽이 통과된 가상 방화벽 그룹을 식별하는 메타데이터입니다. 이 필드는 다중 컨텍스트 모드의 ASA FirePOWER 디바이스에 대해서만 채워집니다.

Ingress Interface

이벤트를 트리거한 패킷의 인그레스 인터페이스. 패시브 인터페이스에 대해서는 이 인터페이스 열만 채워집니다. 4-60페이지의 센싱 인터페이스 구성을/를 참조하십시오.

Egress Interface

인라인 집합의 경우 이벤트를 트리거한 패킷의 이그레스 인터페이스. 패시브 인터페이스에 대해서는 이 인터페이스 열이 채워지지 않습니다. 4-60페이지의 센싱 인터페이스 구성을/를 참조하십시오.

Intrusion Policy

이벤트를 생성한 침입, 프리프로세서 또는 디코더 규칙이 활성화된 침입 정책. 액세스 제어 정책에 대한 기본 작업으로 침입 정책을 선택할 수 있습니다. 또는 침입 정책을 액세스 제어 규칙과 연결할 수 있습니다. 12-6페이지의 네트워크 트래픽의 기본 처리 및 검사 설정 및 18-7페이지의 액세스 제어 규칙을 구성하여 침입 방지 수행을/를 참조하십시오.

Access Control Policy

이벤트를 생성한 침입, 프리프로세서 또는 디코더 규칙이 활성화된 침입 정책을 포함하는 액세스 제어 정책. 12-10페이지의 액세스 제어 정책 관리을/를 참조하십시오.

Access Control Rule

이벤트를 생성한 침입 정책을 호출한 액세스 제어 규칙. 18-7페이지의 액세스 제어 규칙을 구성하여 침입 방지 수행을/를 참조하십시오. `Default Action`은 규칙이 활성화된 침입 정책이 특정 액세스 제어 규칙과 연결되지 않았지만, 대신 액세스 제어 정책의 기본 작업으로 구성되었음을 나타냅니다. 12-6페이지의 네트워크 트래픽의 기본 처리 및 검사 설정을/를 참조하십시오.

침입 검사가 액세스 제어 규칙 및 기본 작업과 모두 연결되지 않은 경우(예: 패킷이 기본 침입 정책에 의해 검토된 경우) 이 필드는 비어 있습니다. 자세한 내용은 25-1페이지의 액세스 제어에 대한 기본 침입 정책 설정을/를 참조하십시오.

Network Analysis Policy

이벤트의 생성과 연결된 NAP(network analysis policy)(있는 경우). 26-1페이지의 네트워크 분석 정책 시작하기을/를 참조하십시오.

HTTP Hostname

HTTP 요청 Host 헤더에서 추출된 호스트 이름(있는 경우). 요청 패킷에 항상 호스트 이름이 포함되는 것은 아닙니다.

호스트 이름을 표시하려면 HTTP Inspect 프리프로세서 **Log Hostname** 옵션을 활성화해야 합니다. 자세한 내용은 27-32페이지의 서버 레벨 HTTP 표준화 옵션 선택을/를 참조하십시오.

이 열에는 추출된 호스트 이름의 처음 50자가 표시됩니다. 약식 호스트 이름의 표시된 부분 위로 마우스 포인터를 이동하여 최대 256바이트까지 전체 이름을 표시할 수 있습니다. 패킷 보기에서도 최대 256바이트까지 전체 호스트 이름을 표시할 수 있습니다. 자세한 내용은 41-24페이지의 이벤트 정보 보기을/를 참조하십시오.

이 필드는 기본적으로 비활성화되어 있습니다.

HTTP URI

침입 이벤트를 트리거한 HTTP 요청 패킷과 연결된 원시 URI(있는 경우). 요청 패킷에 항상 URI가 포함되는 것은 아닙니다.

확장된 URI를 표시하려면 HTTP Inspect 프리프로세서 **Log URI** 옵션을 활성화해야 합니다. 자세한 내용은 27-32페이지의 서버 레벨 HTTP 표준화 옵션 선택을/를 참조하십시오.

HTTP 응답에 의해 트리거된 침입 이벤트에서 연결된 HTTP URI를 보려면 **Perform Stream Reassembly on Both Ports** 옵션에서 HTTP 서버를 구성해야 합니다. 그러나 이렇게 하면 트래픽 리어셈블리를 위한 리소스 수요가 증가합니다. 29-27페이지의 스트림 리어셈블리 옵션 선택을/를 참조하십시오.

이 열에는 추출된 URI의 처음 50자가 표시됩니다. 약식 URI의 표시된 부분 위로 마우스 포인터를 이동하여 최대 2048바이트까지 전체 URI를 표시할 수 있습니다. 패킷 보기에서도 최대 2048바이트까지 전체 URI를 표시할 수 있습니다. 자세한 내용은 41-24페이지의 이벤트 정보 보기을/를 참조하십시오.

이 필드는 기본적으로 비활성화되어 있습니다.

Email Sender

SMTP MAIL FROM 명령에서 추출된 이메일 전송자의 주소. 이 필드의 값을 표시하려면 SMTP 프리프로세서 **Log From Address** 옵션을 활성화해야 합니다. 여러 전송자 주소가 지원됩니다. 자세한 내용은 27-58페이지의 SMTP 디코딩 이해을/를 참조하십시오.

이 필드는 기본적으로 비활성화되어 있습니다.

Email Recipient

SMTP RCPT TO 명령에서 추출된 이메일 수신자의 주소. 이 필드의 값을 표시하려면 SMTP 프리프로세서 **Log To Addresses** 옵션을 활성화해야 합니다. 여러 수신자 주소가 지원됩니다. 자세한 내용은 27-58페이지의 SMTP 디코딩 이해을/를 참조하십시오.

이 필드는 기본적으로 비활성화되어 있습니다.

Email Attachments

MIME Content-Disposition 헤더에서 추출된 MIME 첨부 파일 이름. 첨부 파일 이름을 표시하려면 SMTP 프리프로세서 **Log MIME Attachment Names** 옵션을 활성화해야 합니다. 여러 첨부 파일 이름이 지원됩니다. 자세한 내용은 27-58페이지의 SMTP 디코딩 이해을/를 참조하십시오.

이 필드는 기본적으로 비활성화되어 있습니다.

Reviewed By

이벤트를 검토한 사용자의 이름. 41-16페이지의 침입 이벤트 검토을/를 참조하십시오.

Count

각 행에 표시되는 정보와 매칭되는 이벤트의 수. 둘 이상의 동일한 행을 생성하는 제약 조건을 적용한 경우에만 Count 필드가 나타납니다.

침입 이벤트와 관련된 연결 데이터 보기

라이센스: 보호

시스템은 침입 이벤트가 탐지된 연결을 로깅할 수 있습니다. 이 로깅은 액세스 제어 규칙과 연결된 침입 정책에 대해 자동으로 수행되지만, 기본 작업에 대한 관련 연결 데이터를 보려면 연결 로깅을 수동으로 활성화해야 합니다. 38-15페이지의 액세스 제어 처리 기반 연결 로깅을/를 참조하십시오.

참고 개별 연결 또는 보안 인텔리전스 이벤트에 대해 사용 가능한 정보는 라이센스 및 어플라이언스 모델을 비롯한 여러 요소에 따라 달라집니다. 자세한 내용은 38-9페이지의 연결 로깅의 라이센스 및 모델 요구 사항을/를 참조하십시오.

하나 이상의 침입 이벤트와 관련된 연결 데이터를 보려면

액세스: Admin

1단계 **Analysis > Intrusions > Events**를 선택합니다.

기본 침입 이벤트 워크플로의 첫 번째 페이지가 나타납니다.

이벤트의 테이블 보기 간에 탐색할 때에는 관련된 데이터를 보는 것이 가장 유용합니다. 분석에 중요한 침입 이벤트로 보기를 좁히는 방식에 대한 자세한 내용은 41-17페이지의 침입 이벤트에 대한 워크플로 페이지 이해을/를 참조하십시오.

2단계 이벤트 뷰어의 확인란을 사용하여 침입 이벤트를 선택한 다음 **Jump to** 드롭다운 목록에서 **Connections**를 선택합니다.

특별한 연결과 관련된 침입 이벤트도 유사한 방법으로 볼 수 있습니다. 자세한 내용은 58-35페이지의 워크플로 간 이동을/를 참조하십시오.

사용자가 관련 이벤트를 볼 때 방어 센터는 기본 연결 데이터 워크플로를 사용합니다. 연결 데이터에 대한 자세한 내용은 39-1페이지의 연결 및 보안 인텔리전스 데이터 작업을/를 참조하십시오.

팁 침입 이벤트의 테이블 보기가 포함되지 않은 사용자 지정 워크플로를 사용하는 경우, 워크플로 제목 옆에 있는 **(switch workflow)**를 클릭하여 어플라이언스와 함께 제공되는 사전 정의 워크플로 중 하나를 선택하십시오.

침입 이벤트 검토

라이센스: 보호

침입 이벤트를 검토한 결과 네트워크 보안에 위협이 되지 않을 것으로 확신하는 경우(예: 네트워크의 호스트 중 어떤 것도 탐지된 익스플로잇에 취약하지 않음을 알고 있음) 해당 이벤트를 검토한 것으로 표시할 수 있습니다. 그러면 자신의 이름이 Reviewer로 나타나며, 검토된 이벤트는 기본 침입 이벤트 보기에 더 이상 나열되지 않습니다. 검토한 것으로 표시한 이벤트는 이벤트 데이터베이스에 남아 있지만 더 이상 침입 이벤트 보기에 나타나지 않습니다.

침입 이벤트를 검토한 것으로 표시하려면

액세스: Admin/Intrusion Admin

1단계 침입 이벤트를 보여주는 페이지에는 두 가지 옵션이 있습니다.

- 이벤트 목록에서 하나 이상의 침입 이벤트를 검토한 것으로 표시하려면 이벤트 옆에 있는 확인란을 선택하고 **Review**를 클릭합니다.
- 이벤트 목록에서 모든 침입 이벤트를 표시하려면 **Review All**을 클릭합니다.

성공 메시지가 나타나고 검토된 이벤트의 목록이 업데이트됩니다.

침입 이벤트 보기에 나타나는 이벤트에 대한 자세한 내용은 41-10페이지의 침입 이벤트 이해을/를 참조하십시오. 분석에 중요한 침입 이벤트로 보기를 좁히는 방식에 대한 자세한 내용은 41-17페이지의 침입 이벤트에 대한 워크플로 페이지 이해을/를 참조하십시오.

참고 검토된 이벤트는 침입 이벤트 관련 워크플로 페이지에는 나타나지 않지만 이벤트 요약 통계에는 포함됩니다.

전에 검토된 것으로 표시된 이벤트를 보려면

액세스: Admin/Intrusion Admin

1단계 **Analysis > Intrusions > Reviewed Events**를 선택합니다.

기본 검토된 침입 이벤트 워크플로의 첫 번째 페이지가 나타납니다. 다른 기본 워크플로 지정에 대한 자세한 내용은 71-3페이지의 이벤트 보기 설정 구성을/를 참조하십시오. 이벤트가 표시되지 않을 경우 시간 범위를 조정해야 할 수 있습니다. 58-22페이지의 이벤트 시간 제약 조건 설정을/를 참조하십시오.

팁 침입 이벤트의 테이블 보기가 포함되지 않은 사용자 지정 워크플로를 사용하는 경우, 워크플로 제목 옆에 있는 **(switch workflow)**를 클릭하여 어플라이언스와 함께 제공되는 사전 정의 워크플로 중 하나를 선택하십시오.

검토된 침입 이벤트 보기에 나타나는 이벤트에 대한 자세한 내용은 41-10페이지의 침입 이벤트 이해을/를 참조하십시오. 분석에 중요한 침입 이벤트로 보기를 좁히는 방식에 대한 자세한 내용은 41-17페이지의 침입 이벤트에 대한 워크플로 페이지 이해을/를 참조하십시오.

검토된 이벤트를 검토되지 않은 것으로 표시하려면

액세스: Admin/Intrusion Admin

1단계 검토된 이벤트를 표시하는 페이지에는 두 가지 옵션이 있습니다.

- 검토된 이벤트의 목록에서 개별 침입 이벤트를 제거하려면 이벤트 옆에 있는 확인란을 선택하고 **Unreview**를 클릭합니다.
- 검토된 이벤트의 목록에서 모든 침입 이벤트를 제거하려면 **Unreview All**을 클릭합니다.

성공 메시지가 나타나고 검토된 이벤트의 목록이 업데이트됩니다.

침입 이벤트에 대한 워크플로 페이지 이해

라이센스: 보호

현재 침입 정책에서 활성화된 프리프로세서, 디코더 및 침입 규칙은 모니터링하는 트래픽이 정책을 위반할 때마다 침입 이벤트를 생성합니다.

FireSIGHT 시스템은 이벤트 데이터로 채워진, 침입 이벤트를 보고 분석할 수 있는 사전 정의 워크플로 집합을 제공합니다. 이러한 각 워크플로는 평가하고자 하는 침입 이벤트를 정확히 찾아낼 수 있도록 일련의 페이지로 사용자를 안내합니다.

사전 정의된 침입 이벤트 워크플로에는 세 가지 서로 다른 페이지 유형 또는 이벤트 보기가 포함되어 있습니다.

- 하나 이상의 드릴다운 페이지
- 침입 이벤트의 테이블 보기
- 패킷 보기

*드릴다운 페이지*에는 일반적으로 한 테이블(일부 드릴다운 보기의 경우 둘 이상의 테이블)에 하나의 특정 정보 유형을 볼 수 있는 둘 이상의 열이 포함되어 있습니다.

하나 이상의 목적지 포트에 대한 추가 정보를 찾기 위해 "드릴다운"할 때 자동으로 이러한 이벤트를 선택하게 되며, 워크플로의 다음 페이지가 나타납니다. 이런 식으로, 드릴다운 테이블을 사용하면 매번 분석하는 이벤트 수를 줄일 수 있습니다.

침입 이벤트의 초기 *테이블 보기*에서는 각 침입 이벤트가 고유한 행에 나열됩니다. 테이블의 열에는 시간, 소스 IP 주소와 포트, 목적지 IP 주소와 포트, 이벤트 우선순위, 이벤트 메시지 등의 정보가 나열됩니다.

워크플로에서 이벤트를 선택하고 다음 페이지를 표시하는 대신, 테이블 보기에서 이벤트를 선택하면 *제약 조건*이라는 것을 추가하게 됩니다. 제약 조건이란 분석할 이벤트 유형에 대해 가하는 제한입니다.

예를 들어 임의의 열에서 열 닫기 아이콘(✖)을 클릭하고 드롭다운 목록에서 **Time**을 지우면, 열 중에 하나인 Time을 제거할 수 있습니다. 분석에서 이벤트 목록을 좁히려면 테이블 보기의 행 중 하나에서 값에 대한 링크를 클릭할 수 있습니다. 예를 들어 소스 IP 주소 중 하나(잠재적인 공격자)에서 생성되는 이벤트로 분석을 제한하려면 **Source IP Address** 열에서 해당 IP 주소를 클릭합니다.

테이블 보기에서 하나 이상의 행을 선택하고 **View**를 클릭하면 패킷 보기가 나타납니다. *패킷 보기*는 규칙을 트리거한 패킷 또는 이벤트를 생성한 프리프로세서에 대한 정보를 제공합니다. 패킷 보기의 각 섹션에는 패킷의 특정 레이어에 대한 정보가 포함되어 있습니다. 더 많은 정보를 보려면 축소된 섹션을 확장할 수 있습니다.

참고 각 포트스캔 이벤트는 여러 패킷에 의해 트리거되므로, 포트스캔 이벤트는 패킷 보기의 특수 버전을 사용합니다. 자세한 내용은 34-3페이지의 포트스캔 탐지을/를 참조하십시오.

사전 정의 워크플로가 특정 요구에 맞지 않으면 관심 있는 정보만 표시하는 사용자 지정 워크플로를 생성할 수 있습니다. 사용자 지정 침입 이벤트 워크플로에는 드릴다운 페이지, 이벤트의 테이블 보기 또는 둘 모두를 포함할 수 있습니다. 시스템은 자동으로 패킷 보기를 마지막 페이지로 포함합니다. 이벤트를 조사하려는 방법에 따라, 사전 정의 워크플로와 사용자 지정 워크플로 간에 손쉽게 전환할 수 있습니다.

팁 58-1페이지의 워크플로의 이해 및 사용에서는 워크플로 사용 방법 및 모든 워크플로 페이지에 공통된 기능에 대해 설명합니다. 사용자 지정 침입 이벤트 워크플로를 생성하고 사용하는 방법에 대해서도 설명합니다.

자세한 내용은 다음 링크를 참고하십시오.

- 41-19페이지의 드릴다운 및 테이블 보기 페이지 사용 — 많은 공통된 기능이 있는 드릴다운 페이지 및 이벤트의 테이블 보기를 사용하는 방법에 대해 설명합니다.
- 41-22페이지의 패킷 보기 사용 — 패킷 보기에서 기능을 사용하는 방법에 대해 설명합니다.
- 41-42페이지의 침입 이벤트 검색 — 특정 침입 이벤트에 대한 이벤트 데이터베이스를 검색하는 방법에 대해 설명합니다.

드릴다운 및 테이블 보기 페이지 사용

라이센스: 보호

침입 이벤트를 조사하기 위해 사용할 수 있는 워크플로는 세 가지 서로 다른 페이지 유형을 활용할 수 있습니다.

- 드릴다운 페이지
- 침입 이벤트의 테이블 보기
- 패킷 보기

이러한 각 페이지에 대해서는 41-17페이지의 침입 이벤트에 대한 워크플로 페이지 이해에서 설명합니다.

이벤트의 드릴다운 보기 및 테이블 보기에는 몇 가지 공통된 기능이 있습니다. 이러한 기능을 사용하면 이벤트 목록의 범위를 좁히고 관련 이벤트의 그룹으로 분석을 집중할 수 있습니다. 다음 표에서는 이러한 기능에 대해 설명합니다.

표 41-2 침입 이벤트 공통 기능

목적	가능한 작업
나타나는 열에 대해 자세히 알아보기	41-10페이지의 침입 이벤트 이해에서 자세히 알아보십시오.
호스트의 프로필 보기	호스트 IP 주소 옆에 나타나는 호스트 프로필 아이콘()을 클릭합니다.
지오로케이션 세부사항 보기	Source Country or Destination Country 열에 나타나는 플래그 아이콘 클릭
표시된 이벤트에 대한 시간 및 날짜 범위 수정	58-22페이지의 이벤트 시간 제약 조건 설정에서 자세히 알아보십시오. 어플라이언스의 구성된 시간 창(전역이든 이벤트 전용이든)을 벗어나 생성된 이벤트는 시간 기준으로 이벤트 보기를 제한할 경우 이벤트 보기에 나타날 수 있습니다. 이는 어플라이언스에 대한 슬라이딩 시간 창을 구성한 경우에도 발생할 수 있습니다.
현재 워크플로 페이지에서 이벤트를 정렬 및 제한	다음에서 자세히 알아보기: • 58-34페이지의 드릴다운 워크플로 페이지 정렬 • 드릴다운 페이지에서 이벤트 제한 표 • 이벤트의 테이블 보기에서 이벤트 제한 표
현재 워크플로 페이지 내에서 이동	58-35페이지의 워크플로의 다른 페이지로 이동에서 자세히 알아보십시오. **팁** 서로 다른 워크플로 페이지에 동일한 침입 이벤트가 표시되지 않도록, 시간 범위는 다른 이벤트 페이지를 표시하기 위해 페이지 아래쪽에서 링크를 클릭할 때 일시 중지되고, 후속 페이지에서 다른 작업을 수행하기 위해 클릭할 때 다시 시작됩니다. 자세한 내용은 58-22페이지의 이벤트 시간 제약 조건 설정을/를 참조하십시오.
현재의 제약 조건을 유지한 채 현재 워크플로에서 페이지 간 이동	워크플로 페이지의 왼쪽 위에서 적절한 페이지 링크를 클릭합니다. 자세한 내용은 58-18페이지의 워크플로 페이지 사용을/를 참조하십시오.

표 41-2 침입 이벤트 공통 기능(계속)

목적	가능한 작업
나중에 인시던트에 전송할 수 있도록 이벤트를 클립보드에 추가	다음 방법 중 하나를 사용합니다. • 워크플로 페이지의 여러 침입 이벤트를 클립보드로 복사하려면 복사하려는 이벤트 옆에 있는 확인란을 선택하고 **Copy**를 클릭합니다. • 현재 제한된 보기의 모든 침입 이벤트를 클립보드로 복사하려면 **Copy All**을 클릭합니다. 클립보드에는 사용자당 25,000개의 이벤트가 저장됩니다. 자세한 내용은 41-50페이지의 클립보드 사용을/를 참조하십시오.
이벤트 데이터베이스에서 이벤트 삭제	다음 방법 중 하나를 사용합니다. • 선택한 침입 이벤트를 삭제하려면 삭제할 이벤트 옆에 있는 확인란을 선택하고 **Delete**를 클릭합니다. • 현재 제한된 보기에서 모든 침입 이벤트를 삭제하려면 **Delete All**을 클릭하고 모든 이벤트를 삭제할 것인지를 확인합니다.
이벤트를 검토된 것으로 표시하여 침입 이벤트 페이지에서는 제거하되 이벤트 데이터베이스에서는 제거하지 않음	다음 방법 중 하나를 사용합니다. • 선택한 침입 이벤트를 검토하려면 검토할 이벤트 옆에 있는 확인란을 선택하고 **Review**를 클릭합니다. • 현재 제한된 보기의 모든 침입 이벤트를 검토하려면 **Review All**을 클릭합니다. 자세한 내용은 41-16페이지의 침입 이벤트 검토을/를 참조하십시오.
선택한 각 이벤트를 트리거한 패킷(libpcap 형식의 패킷 캡처 파일)의 로컬 복사본 다운로드	다음 방법 중 하나를 사용합니다. • 선택한 침입 이벤트를 트리거한 패킷을 다운로드하려면, 다운로드하려는 패킷에 의해 트리거된 이벤트의 옆에 있는 확인란을 선택하고 **Download Packets**를 클릭합니다. • 현재 제한된 보기의 침입 이벤트를 트리거한 모든 패킷을 다운로드하려면 **Download All Packets**를 클릭합니다. 캡처된 패킷은 libpcap 형식으로 저장됩니다. 이 형식은 여러 인기 있는 프로토콜 분석기에서 사용됩니다.
관련 이벤트를 보기 위해 다른 이벤트 보기로 이동	58-35페이지의 워크플로 간 이동에서 자세히 알아보십시오.
일시적으로 다른 워크플로 사용	**(switch workflow)**를 클릭합니다. 자세한 내용은 58-16페이지의 워크플로 선택을/를 참조하십시오.
신속하게 다시 돌아올 수 있도록 현재 페이지 북마크 지정	**Bookmark This Page**를 클릭합니다. 자세한 내용은 58-36페이지의 북마크 사용을/를 참조하십시오.
Summary Dashboard의 Intrusion Events 섹션 보기	**Dashboards**를 클릭합니다. 자세한 내용은 55-35페이지의 대시보드 작업을/를 참조하십시오.
북마크 관리 페이지로 이동	**View Bookmarks**를 클릭합니다. 자세한 내용은 58-36페이지의 북마크 사용을/를 참조하십시오.
현재 보기의 데이터를 기반으로 보고서 생성	**Report Designer**를 클릭합니다. 자세한 내용은 57-9페이지의 이벤트 보기에서 보고서 템플릿 생성을/를 참조하십시오.

이벤트 보기에 나타나는 침입 이벤트의 수는 다음에 따라 매우 클 수 있습니다.

- 선택한 시간 범위
- 네트워크의 트래픽 양
- 적용한 침입 정책

침입 이벤트를 더 쉽게 분석하려면 이벤트 페이지를 제한할 수 있습니다. 제한 프로세스는 침입 이벤트의 드릴다운 보기와 테이블 보기에서 약간 다릅니다.

팁 다른 페이지로 이동하기 위해 침입 이벤트 워크플로 페이지 아래쪽에 있는 링크 중 하나를 클릭할 때 시간 범위가 일시 중지하고, 후속 페이지에서 다른 작업을 수행하기 위해 클릭할 때 시간 범위가 다시 시작됩니다. 따라서 더 많은 이벤트를 보기 위해 워크플로에서 다른 페이지로 이동할 때 동일한 페이지가 표시될 가능성이 줄어듭니다. 자세한 내용은 58-22페이지의 이벤트 시간 제약 조건 설정 및 58-35페이지의 워크플로의 다른 페이지로 이동을/를 참조하십시오.

다음 표에서는 드릴다운 페이지를 사용하는 방법에 대해 설명합니다.

표 41-3 드릴다운 페이지에서 이벤트 제한

목적	가능한 작업
다음 워크플로 페이지로 드릴다운하여 특정 값으로 제한	값을 클릭합니다. 예를 들어 Destination Port 워크플로에서, 목적지 포트 80으로 이벤트를 제한하려면 **DST Port/ICMP Code** 열에서 **80/tcp**를 클릭합니다. 워크플로의 다음 페이지인 Events가 나타나고, 포트 80/tcp 이벤트로 범위가 제한됩니다.
다음 워크플로 페이지로 드릴다운하여 선택한 이벤트로 제한	다음 워크플로 페이지에서 보려는 이벤트 옆에 있는 확인란을 선택하고 **View**를 클릭합니다. 예를 들어 Destination Port 워크플로에서 목적지 포트 20/tcp 및 21/tcp로 이벤트를 제한하려면 해당 포트에 대한 행 옆에 있는 확인란을 선택하고 **View**를 클릭합니다. 워크플로의 다음 페이지인 Events가 나타나고, 포트 20/tcp 및 21/tcp 이벤트로 범위가 제한됩니다. **참고** 여러 행으로 제한하려는 경우 테이블에 열이 두 개 이상이면(Count 열은 포함하지 않음) 복합 제약 조건을 구축해야 합니다. 복합 제약 조건은 의도한 것보다 더 많은 이벤트가 제약 조건에 포함되지 않도록 보장합니다. 예를 들어 Event and Destination 워크플로를 사용하는 경우 첫 번째 드릴다운 페이지에서 선택하는 각 행은 복합 제약 조건을 생성합니다. 복합 제약 조건을 사용하는 경우 목적지 IP 주소 10.10.10.100으로 이벤트 1:100을 선택하고 목적지 IP 주소 192.168.10.100으로 이벤트 1:200을 선택하면, 1:100의 이벤트를 이벤트 유형으로 그리고 192.168.10.100을 목적지 IP 주소로 선택하거나 이벤트 1:200을 이벤트 유형으로 그리고 10.10.10.100을 목적지 IP 주소로 선택하게 되지 않습니다.
현재의 제약 조건을 유지한 채 다음 워크플로 페이지로 드릴다운	**View All**을 클릭합니다.

다음 표에서는 테이블 보기를 사용하는 방법에 대해 설명합니다.

표 41-4 이벤트의 테이블 보기에서 이벤트 제한

목적	가능한 작업
이벤트에 대한 보기를 단일 특성으로 제한	특성을 클릭합니다. 예를 들어 목적지 포트 80의 이벤트로 보기를 제한하려면 **DST Port/ICMP Code** 열에서 **80/tcp**를 클릭합니다.
테이블에서 열 제거	숨기려는 열 머리글에서 닫기 아이콘(✖)을 클릭합니다. 표시되는 팝업 창에서 **Apply**를 클릭합니다. **팁** 다른 열을 숨기거나 표시하려면 **Apply**를 클릭하기 전에 해당 확인란을 선택하거나 선택 취소합니다. 비활성화된 열을 다시 보기에 추가하려면 확장 화살표(▶)를 클릭하여 검색 제약 조건을 확장한 다음 **Disabled Columns** 아래에서 열 이름을 클릭합니다.
하나 이상의 이벤트와 관련된 패킷 보기	다음 중 하나: • 패킷을 보려는 이벤트 옆에 있는 아래쪽 화살표 아이콘(⬇)을 클릭합니다. • 패킷을 보려는 하나 이상의 이벤트를 선택하고 페이지 아래쪽에서 **View**를 클릭합니다. • 페이지 아래쪽에서, 현재 제약 조건과 일치하는 모든 이벤트에 대한 패킷을 보려면 **View All**을 클릭합니다.

팁 프로세스의 어떤 지점에서든 제약 조건을 검색 기준 집합으로 저장할 수 있습니다. 예를 들어 지난 며칠 동안 공격자가 단일 IP 주소로 네트워크를 프로브한 것을 발견한 경우, 조사 중에 제약 조건을 저장한 다음 나중에 다시 사용할 수 있습니다. 그러나 복합 제약 조건을 검색 기준 집합으로 저장할 수는 없습니다. 자세한 내용은 60-1페이지의 검색 수행 및 저장을/를 참조하십시오.

팁 이벤트 보기에 침입 이벤트가 나타나지 않는 경우 선택 기간을 조정하면 결과가 반환될 수 있습니다. 좀 더 오래된 시간 범위를 선택하면 해당 시간 범위의 이벤트가 삭제되었을 수 있습니다. 규칙 임계값 지정 컨피그레이션을 조정하면 이벤트가 생성됩니다.

패킷 보기 사용

라이센스: 보호

패킷 보기는 침입 이벤트를 생성한 규칙을 트리거한 패킷에 대한 정보를 제공합니다.

팁 이벤트를 탐지한 디바이스에 대해 **Transfer Packet** 옵션이 비활성화된 경우 방어 센터의 패킷 보기에는 패킷 정보가 포함되지 않습니다.

패킷 보기는 패킷이 트리거한 침입 이벤트에 대한 정보를 제공함으로써 특정 패킷이 캡처된 이유를 나타냅니다. 그러한 정보에는 이벤트의 타임스탬프, 메시지, 분류, 우선순위가 포함되며 이벤트가 표준 텍스트 규칙에 의해 생성된 경우 이벤트를 생성한 규칙도 포함됩니다. 패킷 보기는 또한 크기를 비롯한 패킷에 대한 일반 정보도 제공합니다.

패킷 보기에는 데이터 링크, 네트워크, 전송 등 패킷의 각 레이어에 대해 설명하는 섹션은 물론, 패킷을 구성하는 바이트에 대해 설명하는 섹션도 있습니다. 시스템이 패킷을 해독하면 해독된 바이트를 볼 수 있습니다. 자세한 정보를 보려면 축소된 섹션을 확장할 수 있습니다.

참고 각 포트스캔 이벤트는 여러 패킷에 의해 트리거되므로, 포트스캔 이벤트는 패킷 보기의 특수 버전을 사용합니다. 자세한 내용은 34-3페이지의 포트스캔 탐지을/를 참조하십시오.

다음 표에서는 패킷 보기에서 할 수 있는 작업에 대해 설명합니다.

표 41-5 패킷 보기 작업

목적	가능한 작업
패킷 보기의 날짜 및 시간 범위 수정	58-22페이지의 이벤트 시간 제약 조건 설정에서 자세히 알아보십시오.
패킷 보기에 표시되는 정보에 대해 자세히 알아보기	다음에서 자세히 알아보기: • 41-24페이지의 이벤트 정보 보기 • 41-31페이지의 프레임 정보 보기 • 41-32페이지의 데이터 링크 레이어 정보 보기 • 41-32페이지의 네트워크 레이어 정보 보기 • 41-35페이지의 전송 레이어 정보 보기 • 41-37페이지의 패킷 바이트 정보 보기
나중에 인시던트에 전송할 수 있도록 이벤트를 클립보드에 추가	다음 중 하나: • 패킷을 보고 있는 이벤트를 복사하려면 **Copy** 클릭 • 전에 패킷을 선택한 모든 이벤트를 복사하려면 **Copy All** 클릭 클립보드에는 사용자당 25,000개의 이벤트가 저장됩니다. 클립보드에 대한 자세한 내용은 41-50페이지의 클립보드 사용을/를 참조하십시오.
이벤트데이터베이스에서 이벤트 삭제	다음 중 하나: • 패킷을 보고 있는 이벤트를 삭제하려면 **Delete** 클릭 • 전에 패킷을 선택한 모든 이벤트를 삭제하려면 **Delete All** 클릭
이벤트를 검토된 것으로 표시하여 이벤트 보기에서는 제거하되 이벤트 데이터베이스에서는 제거하지 않음	다음 중 하나: • 패킷을 보고 있는 이벤트를 검토하려면 **Review** 클릭 • 전에 패킷을 선택한 모든 이벤트를 검토하려면 **Review All** 클릭 자세한 내용은 41-16페이지의 침입 이벤트 검토을/를 참조하십시오. 검토된 이벤트는 Intrusion Event Statistics 페이지의 이벤트 통계에 계속 포함됩니다.

표 41-5 패킷 보기 작업(계속)

목적	가능한 작업
이벤트를 트리거한 패킷(libpcap 형식의 패킷 캡처 파일)의 로컬 복사본 다운로드	다음 중 하나: • 보고 있는 이벤트에 대한 캡처된 패킷의 복사본을 저장하려면 **Download Packet** 클릭 • 전에 패킷을 선택한 모든 이벤트에 대한 캡처된 패킷의 복사본을 저장하려면 **Download All Packets** 클릭 캡처된 패킷은 libpcap 형식으로 저장됩니다. 이 형식은 여러 인기 있는 프로토콜 분석기에서 사용됩니다. 단일 포트스캔 이벤트는 여러 패킷을 기반으로 하기 때문에 포트스캔 패킷을 다운로드할 수 없습니다. 그러나 포트스캔 보기는 사용할 만한 모든 패킷 정보를 제공합니다. 자세한 내용은 34-7페이지의 포트스캔 이벤트 이해을/를 참조하십시오. 다운로드하려면 사용 가능한 디스크 공간이 15% 이상 남아 있어야 합니다.
페이지 섹션 확장 또는 축소	섹션 옆에 있는 화살표를 클릭합니다.

패킷 보기를 표시하려면

액세스: Admin/Intrusion Admin

1단계 침입 이벤트의 테이블 보기에서 보려는 패킷을 선택합니다. 자세한 내용은 이벤트의 테이블 보기에서 이벤트 제한 표를 참조하십시오.

패킷 보기가 나타납니다. 둘 이상의 이벤트를 선택한 경우 페이지 아래쪽에 있는 페이지 번호를 사용하여 각 페이지에서 패킷을 살펴볼 수 있습니다.

이벤트 정보 보기

라이센스: 보호

패킷 보기에서는 Event Information 섹션에서 패킷에 대한 정보를 볼 수 있습니다.

이벤트

이벤트 메시지. 규칙 기반 이벤트의 경우 규칙 메시지에 해당합니다. 다른 이벤트의 경우 디코더 또는 프리프로세서에 의해 결정됩니다.

이벤트의 ID는 *(GID:SID:Rev)* 형식으로 메시지에 추가됩니다. *GID*는 이벤트를 생성한 규칙 엔진, 디코더 또는 프리프로세서의 Generator ID입니다. *SID*는 규칙, 디코더 메시지 또는 프리프로세서 메시지에 대한 식별자입니다. *Rev*는 규칙의 개정 번호입니다. 추가 정보는 41-40페이지의 프리프로세서 Generator ID 읽기을/를 참조하십시오.

타임스탬프

패킷이 캡처된 시간

분류

이벤트 분류. 규칙 기반 이벤트의 경우 규칙 분류에 해당합니다. 다른 이벤트의 경우 디코더 또는 프리프로세서에 의해 결정됩니다.

Priority(우선순위)

이벤트 우선순위. 규칙 기반 이벤트의 경우 `priority` 키워드의 값 또는 `classtype` 키워드의 값에 해당합니다. 다른 이벤트의 경우 디코더 또는 프리프로세서에 의해 결정됩니다.

Ingress Security Zone

이벤트를 트리거한 패킷의 인그레스 보안 영역. 패시브 구축에서는 이 보안 영역 필드만 채워집니다. 3-38페이지의 보안 영역 작업을/를 참조하십시오.

Egress Security Zone

인라인 구축의 경우 이벤트를 트리거한 패킷의 이그레스 보안 영역. 3-38페이지의 보안 영역 작업을/를 참조하십시오.

디바이스

액세스 제어 정책이 적용된 관리되는 디바이스. 4-1페이지의 디바이스 관리을/를 참조하십시오.

보안 상황

트래픽이 통과된 가상 방화벽 그룹을 식별하는 메타데이터입니다. 이 필드는 다중 컨텍스트 모드의 ASA FirePOWER 디바이스에 대해서만 채워집니다.

Ingress Interface

이벤트를 트리거한 패킷의 인그레스 인터페이스. 패시브 인터페이스에 대해서는 이 인터페이스 열만 채워집니다. 4-60페이지의 센싱 인터페이스 구성을/를 참조하십시오.

Egress Interface

인라인 집합의 경우 이벤트를 트리거한 패킷의 이그레스 인터페이스. 4-60페이지의 센싱 인터페이스 구성을/를 참조하십시오.

Source/Destination IP

이벤트(소스)를 트리거한 패킷이 시작된 호스트 IP 주소 또는 도메인 이름, 또는 이벤트를 트리거한 트래픽의 대상(목적지) 호스트.

도메인 이름을 표시하려면 IP 주소 확인을 활성화해야 합니다. 자세한 내용은 71-3페이지의 이벤트 보기 설정 구성을/를 참조하십시오.

주소 또는 도메인 이름을 클릭하여 컨텍스트 메뉴를 표시한 다음, 호스트에서 whois 검색을 수행하려면 **Whois**를, 호스트 정보를 보려면 **View Host Profile**을, 전역 블랙리스트나 화이트리스트에 주소를 추가하려면 **Blacklist Now** 또는 **Whitelist Now**를 선택합니다. 49-1페이지의 호스트 프로필 사용 및 3-7페이지의 전역 화이트리스트 및 블랙리스트 작업을/를 참조하십시오.

Source Port/ICMP Type

이벤트를 트리거한 패킷의 소스 포트. ICMP 트래픽의 경우 포트 번호가 없으면 시스템은 ICMP 유형을 표시합니다.

Destination Port/ICMP Code

트래픽을 수신하는 호스트의 포트 번호. ICMP 트래픽의 경우 포트 번호가 없으면 시스템은 ICMP 코드를 표시합니다.

Email Headers

이메일 헤더에서 추출된 데이터. 이메일 헤더는 침입 이벤트의 테이블 보기에 나타나지 않지만, 이메일 헤더를 검색 기준으로 사용할 수 있습니다.

이메일 헤더를 SMTP 트래픽용 침입 이벤트와 연결하려면 SMTP 프리프로세서 **Log Headers** 옵션을 활성화해야 합니다. 자세한 내용은 27-58페이지의 SMTP 디코딩 이해을/를 참조하십시오. 규칙 기반 이벤트의 경우 이메일 데이터가 추출될 때 이 행이 나타납니다.

HTTP Hostname

HTTP 요청 Host 헤더에서 추출된 호스트 이름(있는 경우). 이 행은 최대 256바이트까지 전체 호스트 이름을 표시합니다. 단일 행보다 긴 경우 전체 호스트 이름을 표시하려면 확장 아이콘 ( )을 클릭합니다.

호스트 이름을 표시하려면 HTTP Inspect 프리프로세서 **Log Hostname** 옵션을 활성화해야 합니다. 자세한 내용은 27-32페이지의 서버 레벨 HTTP 표준화 옵션 선택을/를 참조하십시오.

HTTP 요청 패킷에 항상 호스트 이름이 포함되는 것은 아닙니다. 규칙 기반 이벤트의 경우 이 행은 패킷에 HTTP 호스트 이름 또는 HTTP URI가 포함된 경우 나타납니다.

HTTP URI

침입 이벤트를 트리거한 HTTP 요청 패킷과 연결된 원시 URI(있는 경우). 이 행은 최대 2048바이트까지 전체 URI를 표시합니다. 단일 행보다 긴 경우 전체 URI를 표시하려면 확장 아이콘 ( )을 클릭합니다.

URI를 표시하려면 HTTP Inspect 프리프로세서 **Log URI** 옵션을 활성화해야 합니다. 자세한 내용은 27-32페이지의 서버 레벨 HTTP 표준화 옵션 선택을/를 참조하십시오.

HTTP 요청 패킷에 항상 URI가 포함되는 것은 아닙니다. 규칙 기반 이벤트의 경우 이 행은 패킷에 HTTP 호스트 이름 또는 HTTP URI가 포함된 경우 나타납니다.

HTTP 응답에 의해 트리거된 침입 이벤트에서 연결된 HTTP URI를 보려면 **Perform Stream Reassembly on Both Ports** 옵션에서 HTTP 서버를 구성해야 합니다. 그러나 이렇게 하면 트래픽 리어셈블리를 위한 리소스 수요가 증가합니다. 29-27페이지의 스트림 리어셈블리 옵션 선택을/를 참조하십시오.

침입 정책

침입 이벤트를 생성한 침입, 프리프로세서 또는 디코더 규칙이 활성화된 침입 정책(있는 경우). 액세스 제어 정책에 대한 기본 작업으로 침입 정책을 선택하거나, 침입 정책을 액세스 제어 규칙과 연결할 수 있습니다. 12-6페이지의 네트워크 트래픽의 기본 처리 및 검사 설정 및 18-7페이지의 액세스 제어 규칙을 구성하여 침입 방지 수행을/를 참조하십시오.

액세스 제어 정책

이벤트를 생성한 침입, 프리프로세서 또는 디코더 규칙이 활성화된 침입 정책을 포함하는 액세스 제어 정책. 12-10페이지의 액세스 제어 정책 관리을/를 참조하십시오.

Access Control Rule

이벤트를 생성한 침입 규칙과 관련된 액세스 제어 규칙. 18-7페이지의 액세스 제어 규칙을 구성하여 침입 방지 수행을/를 참조하십시오. `Default Action`은 규칙이 활성화된 침입 정책이 액세스 제어 규칙과 연결되지 않았지만, 대신 액세스 제어 정책의 기본 작업으로 구성되었음을 나타냅니다. 12-6페이지의 네트워크 트래픽의 기본 처리 및 검사 설정을/를 참조하십시오.

규칙

표준 텍스트 규칙 이벤트의 경우 이벤트를 생성한 규칙.

이벤트가 공유 객체 규칙, 디코더 또는 프리프로세서를 기반으로 하는 경우에는 규칙을 사용할 수 없습니다.

규칙 데이터에는 네트워크에 대한 민감한 정보가 포함될 수 있으므로 관리자는 사용자 역할 편집기의 View Local Rules 권한을 사용하여 패킷 보기에서 규칙 정보를 보는 사용자의 기능을 전환할 수 있습니다. 자세한 내용은 61-54페이지의 사용자 권한 및 옵션 수정을/를 참조하십시오.

조치

표준 텍스트 규칙 이벤트의 경우, 이벤트를 트리거한 규칙에 대해 다음 작업을 수행하려면 **Actions**를 확장합니다.

- 규칙 수정
- 규칙의 개정에 대한 문서 보기
- 규칙에 코멘트 추가
- 규칙의 상태 변경
- 규칙에 대한 임계값 설정
- 규칙 억제

자세한 내용은 41-27페이지의 패킷 보기 작업 사용, 41-29페이지의 패킷 보기 내에서 임계값 옵션 설정 및 41-30페이지의 패킷 보기 내에서 억제 옵션 설정을/를 참조하십시오.

이벤트가 공유 객체 규칙, 디코더 또는 프리프로세서를 기반으로 하는 경우에는 규칙을 사용할 수 없습니다.

패킷 보기 작업 사용

라이센스: 보호

패킷 보기의 Event Information 섹션에서, 이벤트를 트리거한 규칙에 대해 몇 가지 작업을 수행할 수 있습니다. 이벤트가 공유 객체 규칙, 디코더 또는 프리프로세서를 기반으로 하는 경우에는 규칙을 사용할 수 없습니다. 규칙 작업을 표시하려면 **Actions**를 확장해야 합니다.

Edit

표준 텍스트 규칙 이벤트의 경우 이벤트를 생성한 규칙을 수정하려면 **Edit**를 클릭합니다.

이벤트가 공유 객체 규칙, 디코더 또는 프리프로세서를 기반으로 하는 경우에는 규칙을 사용할 수 없습니다.

참고 Cisco에서 제공한 규칙을 수정하려면(사용자 지정 표준 텍스트 규칙과 반대) 실제로 새 로컬 규칙을 생성해야 합니다. 이벤트를 생성하도록 로컬 규칙을 설정하고, 현재 침입 정책에서 원래 규칙을 비활성화해야 합니다. 그러나 기본 정책의 로컬 규칙은 활성화할 수 **없습니다**. 자세한 내용은 36-104페이지의 기존 규칙 수정을/를 참조하십시오.

View Documentation

표준 텍스트 규칙 이벤트의 경우, 이벤트를 생성한 규칙 개정에 대해 자세히 알아보려면 **View Documentation**을 클릭합니다.

Rule Comment

표준 텍스트 규칙 이벤트의 경우, 이벤트를 생성한 규칙에 텍스트 코멘트를 추가하려면 **Rule Comment**를 클릭합니다.

그러면 규칙과 익스플로잇 또는 식별하는 정책 위반에 대한 추가 컨텍스트와 정보를 제공할 수 있습니다. 또한 규칙 편집기에서 규칙 코멘트를 추가하고 볼 수 있습니다. 자세한 내용은 36-106페이지의 규칙에 코멘트 추가을/를 참조하십시오.

Disable this rule

이 이벤트가 표준 텍스트 규칙에 의해 생성된 경우 필요 시 규칙을 비활성화할 수 있습니다. 로컬로 수정할 수 있는 모든 정책에서 규칙을 설정할 수 있습니다. 또는 현재 정책을 로컬로 수정할 수 있는 경우 현재 정책(즉, 이벤트를 생성한 정책)에서만 규칙을 설정할 수 있습니다.

자세한 내용은 32-20페이지의 규칙 상태 설정을/를 참조하십시오.

현재 정책 옵션은 현재 정책을 수정할 수 있는 경우에만 나타납니다. 예를 들어, 사용자 지정 정책은 수정할 수 있지만 Cisco에서 제공한 기본 정책은 수정할 수 없습니다.

참고 패킷 보기에서 공유 객체 규칙을 비활성화할 수 **없으며**, 기본 정책에서도 규칙을 비활성화할 수 없습니다.

Set this rule to generate events

이 이벤트가 표준 텍스트 규칙에 의해 생성된 경우, 로컬에서 수정할 수 있는 모든 정책에서 이 이벤트를 생성하도록 규칙을 설정할 수 있습니다. 또는 현재 정책을 로컬로 수정할 수 있는 경우 현재 정책(즉, 이벤트를 생성한 정책)에서만 규칙을 설정할 수 있습니다.

자세한 내용은 32-20페이지의 규칙 상태 설정을/를 참조하십시오.

현재 정책 옵션은 현재 정책을 수정할 수 있는 경우에만 나타납니다. 예를 들어, 사용자 지정 정책은 수정할 수 있지만 Cisco에서 제공한 기본 정책은 수정할 수 없습니다.

참고 패킷 보기에서 공유 객체 규칙을 설정할 수 **없으며**, 기본 정책에서도 규칙을 비활성화할 수 없습니다.

Set this rule to drop

관리되는 디바이스가 네트워크에서 인라인으로 구축된 경우, 이벤트를 트리거한 규칙이 로컬로 수정할 수 있는 모든 정책에서 규칙을 트리거하는 패킷을 삭제하도록 설정할 수 있습니다. 또는 현재 정책을 로컬로 수정할 수 있는 경우 현재 정책(즉, 이벤트를 생성한 정책)에서만 규칙을 설정할 수 있습니다.

현재 정책 옵션은 현재 정책을 수정할 수 있는 경우에만 나타납니다. 예를 들어, 사용자 지정 정책은 수정할 수 있지만 Cisco에서 제공한 기본 정책은 수정할 수 없습니다. 또한 이 옵션은 **Drop when Inline**이 현재 정책에서 활성화된 경우에만 나타납니다. 자세한 내용은 31-6페이지의 인라인 구축에서 삭제 동작 설정을/를 참조하십시오.

Set Thresholding Options

이 옵션을 사용하면 로컬로 수정할 수 있는 모든 정책에서 이 이벤트를 트리거한 규칙에 대해 임계값을 생성할 수 있습니다. 또는 현재 정책을 로컬로 수정할 수 있는 경우 현재 정책(즉, 이벤트를 생성한 정책)에 대해서만 임계값을 생성할 수 있습니다.

임계값 옵션에 대해서는 41-29페이지의 패킷 보기 내에서 임계값 옵션 설정에 설명되어 있습니다.

현재 정책 옵션은 현재 정책을 수정할 수 있는 경우에만 나타납니다. 예를 들어, 사용자 지정 정책은 수정할 수 있지만 Cisco에서 제공한 기본 침입 정책은 수정할 수 없습니다.

Set Suppression Options

이 옵션을 사용하면 로컬로 수정할 수 있는 모든 정책에서 이 이벤트를 트리거한 규칙을 억제할 수 있습니다. 또는 현재 정책을 로컬로 수정할 수 있는 경우 현재 정책(즉, 이벤트를 생성한 정책)에서만 규칙을 억제할 수 있습니다.

억제 옵션에 대해서는 41-30페이지의 패킷 보기 내에서 억제 옵션 설정에 설명되어 있습니다.

현재 정책 옵션은 현재 정책을 수정할 수 있는 경우에만 나타납니다. 예를 들어, 사용자 지정 정책은 수정할 수 있지만 Cisco에서 제공한 기본 정책은 수정할 수 없습니다.

패킷 보기 내에서 임계값 옵션 설정

라이센스: 보호

침입 이벤트의 패킷 보기에서 임계값 옵션을 설정하여 시간에 따라 규칙당 생성되는 이벤트의 수를 제어할 수 있습니다. 로컬로 수정할 수 있는 모든 정책에서 또는 로컬로 수정할 수 있는 경우 현재 정책(즉, 이벤트 생성을 일으킨 정책)에서만 임계값 옵션을 설정할 수 있습니다.

패킷 보기 내에서 임계값 옵션을 설정하려면

액세스: Admin/Intrusion Admin

1단계 침입 규칙에 의해 생성된 침입 이벤트의 패킷 보기 내에서 Event Information 섹션의 **Actions**를 확장합니다. **Set Thresholding Options**를 확장하고 두 가지 가능한 옵션 중 하나를 선택합니다.

- **in the current policy**
- **in all locally created policies**

현재 정책 옵션은 현재 정책을 수정할 수 있는 경우에만 나타납니다. 예를 들어, 사용자 지정 정책은 수정할 수 있지만 Cisco에서 제공한 기본 정책은 수정할 수 없습니다.

임계값 옵션이 나타납니다.

2단계 설정할 임계값 유형을 선택합니다.

- 기간당 지정된 이벤트 인스턴스의 수로 알림을 제한하려면 **limit**를 선택합니다.
- 기간당 지정된 각 이벤트 인스턴스의 수에 대해 알림을 제공하려면 **threshold**를 선택합니다.
- 지정된 이벤트 인스턴스의 수 이후 기간당 한 번 알림을 제공하려면 **both**를 선택합니다.

3단계 이벤트 인스턴스를 **Source** IP 주소로 추적할지 **Destination** IP 주소로 추적할지를 나타내려면 해당 라디오 버튼을 선택합니다.

4단계 임계값으로 사용할 이벤트 인스턴스의 수를 **Count** 필드에 입력합니다.

5단계 이벤트 인스턴스를 추적할 기간을 지정하는 1~86400의 숫자를 **Seconds** 필드에 입력합니다.

6단계 기존 침입 정책에서 이 규칙에 대한 현재 임계값을 재정의하려면 **Override any existing settings for this rule**을 선택합니다.

7단계 **Save Thresholding**을 클릭합니다.

시스템에서 임계값을 추가하고, 성공적으로 추가했음을 알리는 메시지를 표시합니다. 기존 설정을 재정의하지 않도록 선택한 경우 충돌이 있으면 이를 알리는 메시지가 나타납니다.

패킷 보기 내에서 억제 옵션 설정

라이센스: 보호

침입 이벤트를 완전히 억제하거나 소스 또는 목적지 IP 주소를 기반으로 억제하도록 억제 옵션을 사용할 수 있습니다. 로컬로 수정할 수 있는 모든 정책에서 억제 옵션을 설정할 수 있습니다. 또는 현재 정책을 로컬로 수정할 수 있는 경우 현재 정책(즉, 이벤트를 생성한 정책)에서만 억제 옵션을 설정할 수 있습니다.

패킷 보기 내에서 침입 이벤트를 억제하려면

액세스: Admin/Intrusion Admin

1단계 침입 규칙에 의해 생성된 침입 이벤트의 패킷 보기 내에서 Event Information 섹션의 **Actions**를 확장합니다. **Set Suppression Options**를 확장하고 두 가지 가능한 옵션 중 하나를 클릭합니다.

- **in the current policy**
- **in all locally created policies**

현재 정책 옵션은 현재 정책을 수정할 수 있는 경우에만 나타납니다. 예를 들어, 사용자 지정 정책은 수정할 수 있지만 Cisco에서 제공한 기본 정책은 수정할 수 없습니다.

억제 옵션이 나타납니다.

2단계 다음 **Track By** 옵션 중 하나를 선택합니다.

- 이 이벤트를 트리거한 규칙에 대한 이벤트를 완전히 억제하려면 **Rule**을 선택합니다.
- 지정된 소스 IP 주소에서 나온 패킷에 의해 생성된 이벤트를 억제하려면 **Source**를 선택합니다.
- 지정된 목적지 IP 주소로 이동하는 패킷에 의해 생성된 이벤트를 억제하려면 **Destination**을 선택합니다.

3단계 소스 또는 목적지 IP 주소로 지정하려는 IP 주소 또는 CIDR 블록/접두사 길이를 **IP address or CIDR block** 필드에 입력합니다.

FireSIGHT 시스템에서 CIDR 표기법 및 접두사 길이를 사용하는 방법에 대한 자세한 내용은 1-19 페이지의 IP 주소 표기 규칙을/를 참조하십시오.

4단계 **Save Suppression**을 클릭합니다.

침입 정책 내 억제 옵션이 사양에 따라 수정됩니다. 기존 설정을 재정의하지 않도록 선택한 경우 충돌이 있으면 이를 알리는 메시지가 나타납니다.

프레임 정보 보기

라이센스: 보호

패킷 보기에서 캡처된 프레임에 대한 정보를 볼 **Frame** 옆에 있는 화살표를 클릭합니다. 패킷 보기에 단일 프레임 또는 다중 프레임이 표시될 수 있습니다. 각 프레임은 개별 네트워크 패킷에 대한 정보를 제공합니다. 예를 들면 태그가 지정된 패킷에서 또는 리어셈블된 TCP 스트림의 패킷에서 여러 프레임을 보게 될 수 있습니다. 태그가 지정된 패킷에 대한 자세한 내용은 36-90페이지의 공격 이후 트래픽 평가을/를 참조하십시오. 리어셈블된 TCP 스트림에 대한 자세한 내용은 29-27페이지의 TCP 스트림 리어셈블을/를 참조하십시오.

Frame n

캡처된 프레임. 여기서 *n*은 단일 프레임 패킷의 경우 1이고 다중 프레임 패킷의 경우 증분 프레임 수입니다. 프레임에서 캡처된 바이트의 수가 프레임 수에 추가됩니다.

Arrival Time

프레임이 캡처된 날짜와 시간.

Time delta from previous captured frame

다중 프레임 패킷의 경우 이전 프레임이 캡처된 이후 경과한 시간.

Time delta from previous displayed frame

다중 프레임 패킷의 경우 이전 프레임이 표시된 이후 경과한 시간.

Time since reference or first frame

다중 프레임 패킷의 경우 첫 번째 프레임이 캡처된 이후 경과한 시간.

Frame Number

증분 프레임 수.

Frame Length

바이트 단위의 프레임 길이.

Capture Length

바이트 단위의 캡처된 프레임 길이.

Frame is marked

프레임이 표시되었는지 여부(true 또는 false).

Protocols in frame

프레임에 포함된 프로토콜.

데이터 링크 레이어 정보 보기

라이센스: 보호

패킷 보기에서 데이터 링크 레이어 프로토콜(예: **Ethernet II**) 옆에 있는 화살표를 클릭하여, 소스 및 목적지 호스트에 대한 48비트 MAC(media access control) 주소가 포함된 패킷에 대한 데이터 링크 레이어 정보를 봅니다. 하드웨어 프로토콜에 따라, 패킷에 대한 기타 정보도 표시될 수 있습니다.

참고 이 예에서는 이더넷 링크 레이어 정보에 대해 설명합니다. 다른 프로토콜도 나타날 수 있습니다.

패킷 보기는 데이터 링크 레이어에 사용된 프로토콜을 반영합니다. 다음 목록에서는 Ethernet II 또는 IEEE 802.3 Ethernet 패킷에 대해 패킷 보기에 표시될 수 있는 정보에 대해 설명합니다.

대상

목적지 호스트의 MAC 주소.

참고 이더넷은 멀티캐스트 및 브로드캐스트 주소를 목적지 주소로 사용할 수도 있습니다.

소스

소스 호스트의 MAC 주소.

유형

Ethernet II 패킷의 경우 이더넷 프레임으로 캡슐화된 패킷의 유형(예: IPv6 또는 ARP 데이터그램). 이 항목은 Ethernet II 패킷에 대해서만 나타납니다.

길이

IEEE 802.3 Ethernet 패킷의 경우 체크섬을 제외한 패킷의 전체 길이(바이트 단위). 이 항목은 IEEE 802.3 Ethernet 패킷에 대해서만 나타납니다.

네트워크 레이어 정보 보기

라이센스: 보호

패킷과 관련된 네트워크 레이어 정보에 대해 자세히 알아보려면, 패킷 보기에서 네트워크 레이어 프로토콜(예: **Internet Protocol**) 옆에 있는 화살표를 클릭합니다.

참고 이 예에서는 IP 패킷에 대해 설명합니다. 다른 프로토콜도 나타날 수 있습니다.

자세한 내용은 다음 절을 참조하십시오.

- 41-33페이지의 IPv4 네트워크 레이어 정보 보기
- 41-34페이지의 IPv6 네트워크 레이어 정보 보기

IPv4 네트워크 레이어 정보 보기

라이센스: 보호

다음 목록에서는 IPv4 패킷에 나타날 수 있는 프로토콜 관련 정보에 대해 설명합니다.

버전

Internet Protocol 버전 번호.

헤더 길이

헤더의 바이트 수(IP 옵션 포함). 옵션이 없는 IP 헤더의 길이는 20바이트입니다.

Differentiated Services Field

전송 호스트가 ECN(Explicit Congestion Notification)을 지원하는 방법을 나타내는 차별화된 서비스에 대한 값.

- `0x0` — ECT(ECN-Capable Transport)를 지원하지 않음
- `0x1` 및 `0x2` — ECT를 지원함
- `0x3` — CE(Congestion Experienced)

Total Length

IP 패킷에서 IP 헤더를 뺀 길이(바이트 단위)

식별

소스 호스트가 전송한 IP 데이터그램을 고유하게 식별하는 값. 이 값은 동일한 데이터그램의 프래그먼트를 추적하는 데 사용됩니다.

플래그

IP 프래그먼트화를 제어하는 값.

Last Fragment 플래그의 값은 데이터그램과 관련된 프래그먼트가 더 있는지 여부를 나타냅니다.

- `0` — 데이터그램과 관련된 프래그먼트가 없음
- `1` — 데이터그램과 관련된 프래그먼트가 있음

Don't Fragment 플래그의 값은 데이터그램을 프래그먼트화할 수 있는지 여부를 나타냅니다.

- `0` — 데이터그램을 프래그먼트화할 수 있음
- `1` — 데이터그램을 프래그먼트화해서는 **안 됨**

프래그먼트 옵셋

데이터그램 시작을 기준으로 프래그먼트 옵셋의 값.

Time to Live (ttl)

데이터그램이 만료되기 전 데이터그램이 라우터 간에 만들 수 있는 나머지 홉(hop)의 수.

프로토콜

IP 데이터그램에서 캡슐화되는 전송 프로토콜(예: ICMP, IGMP, TCP 또는 UDP).

헤더 체크섬

IP 체크섬이 유효한지를 나타내는 지표. 체크섬이 유효하지 않으면, 데이터그램이 전송 중에 손상되었거나 침입 회피 시도에 사용 중일 수 있습니다.

Source/Destination

소스(또는 목적지) 호스트의 IP 주소나 도메인 이름.

도메인 이름을 표시하려면 IP 주소 확인을 활성화해야 합니다. 자세한 내용은 71-3페이지의 이벤트 보기 설정 구성을/를 참조하십시오.

주소 또는 도메인 이름을 클릭하여 컨텍스트 메뉴를 표시한 다음, 호스트에서 whois 검색을 수행하려면 **Whois**를, 호스트 정보를 보려면 **View Host Profile**을, 전역 블랙리스트나 화이트리스트에 주소를 추가하려면 **Blacklist Now** 또는 **Whitelist Now**를 선택합니다. 49-1페이지의 호스트 프로필 사용 및 3-7페이지의 전역 화이트리스트 및 블랙리스트 작업을/를 참조하십시오.

IPv6 네트워크 레이어 정보 보기

라이센스: 보호

다음 목록에서는 IPv6 패킷에 나타날 수 있는 프로토콜 관련 정보에 대해 설명합니다.

Traffic Class

IPv4에 대해 제공되는 차별화된 서비스 기능과 유사한 IPv6 패킷 클래스 또는 우선순위를 식별하기 위한 IPv6 헤더의 실험적인 8비트 필드. 사용되지 않는 경우 이 필드는 0으로 설정됩니다.

Flow Label

기본이 아닌 서비스 품질 또는 실시간 서비스 등의 특수 플로우를 식별하는 선택적인 20비트 IPv6 16진수 값 1~FFFFF. 사용되지 않는 경우 이 필드는 0으로 설정됩니다.

Payload Length

IPv6 페이로드에서 옥텟 수를 식별하는 16비트 필드로, IPv6 헤더 뒤에 나오는 모든 패킷(확장 헤더 포함)으로 구성됨.

Next Header

IPv6 헤더 바로 뒤에 나오는 헤더 유형을 식별하는 8비트 필드로, IPv4 Protocol 필드와 같은 값 사용.

Hop Limit

패킷을 전달하는 각 노드가 1씩 감소하는 8비트 10진수 정수. 감소한 값이 0에 도달하면 패킷이 취소됩니다.

소스

소스 호스트에 대한 128비트 IPv6 주소.

대상

목적지 호스트에 대한 128비트 IPv6 주소.

전송 레이어 정보 보기

라이센스: 보호

패킷에 대해 자세히 알아보려면, 패킷 보기에서 전송 레이어 프로토콜(예: **TCP**, **UDP** 또는 **ICMP**) 옆에 있는 화살표를 클릭합니다.

팁 패킷 보기의 Packet Information 섹션에서 바로 위에 있는 프로토콜에 대한 페이로드의 처음 24바이트를 보도록 제공되면 **Data**를 클릭하십시오.

다음의 각 프로토콜에 대한 전송 레이어의 내용은 아래에서 설명합니다.

- 41-35페이지의 TCP 패킷 보기
- 41-36페이지의 UDP 패킷 보기
- 41-37페이지의 ICMP 패킷 보기

참고 이러한 예에서는 TCP, UDP 및 ICMP 패킷에 대해 설명합니다. 다른 프로토콜도 나타날 수 있습니다.

TCP 패킷 보기

라이센스: 보호

이 절에서는 TCP 패킷의 프로토콜 관련 정보에 대해 설명합니다.

Source port

시작 애플리케이션 프로토콜을 식별하는 번호.

Destination port

수신 애플리케이션 프로토콜을 식별하는 번호.

시퀀스 번호

현재 TCP 세그먼트의 첫 번째 바이트에 대한 값으로, TCP 스트림에서 초기 시퀀스 번호로 키가 지정됨.

Next sequence number

응답 패킷에서, 전송할 다음 패킷의 시퀀스 번호.

Acknowledgement number

전에 허용된 데이터의 시퀀스 번호로 키가 지정되는 TCP 승인.

헤더 길이

헤더의 바이트 수.

플래그

TCP 세그먼트의 전송 상태를 나타내는 6개 비트.

- U — Urgent Pointer가 유효함
- A — 승인 번호가 유효함
- P — 수신자가 데이터를 푸시해야 함
- R — 연결 재설정
- S — 새 연결을 시작하도록 시퀀스 번호 동기화
- F — 전송자가 데이터 전송을 완료함

Window size

수신 호스트가 허용하는, 승인되지 않은 데이터의 양(바이트 단위)

Checksum

TCP 체크섬이 유효한지를 나타내는 지표. 체크섬이 유효하지 않으면, 데이터그램이 전송 중에 손상되었거나 회피 시도에 사용 중일 수 있습니다.

긴급 포인터

긴급 데이터가 종료되는 TCP 세그먼트의 위치(있는 경우). U 플래그와 함께 사용됨.

옵션

TCP 옵션의 값(있는 경우)

UDP 패킷 보기

라이센스: 보호

이 절에서는 UDP 패킷의 프로토콜 관련 정보에 대해 설명합니다.

Source port

시작 애플리케이션 프로토콜을 식별하는 번호.

Destination port

수신 애플리케이션 프로토콜을 식별하는 번호.

길이

UDP 헤더 및 데이터를 결합한 길이.

Checksum

UDP 체크섬이 유효한지를 나타내는 지표. 체크섬이 유효하지 않으면 전송 중 데이터그램이 손상되었을 수 있습니다.

ICMP 패킷 보기

라이센스: 보호

이 절에서는 ICMP 패킷의 프로토콜 관련 정보에 대해 설명합니다.

유형

ICMP 메시지의 유형:

- 0 — 에코 응답
- 3 — 목적지 도달 불가
- 4 — 소스 끄기
- 5 — 리디렉션
- 8 — 에코 요청
- 9 — 라우터 광고
- 10 — 라우터 제안
- 11 — 시간 초과됨
- 12 — 매개 변수 문제
- 13 — 타임스탬프 요청
- 14 — 타임스탬프 응답
- 15 — 정보 요청(사용되지 않음)
- 16 — 정보 응답(사용되지 않음)
- 17 — 주소 마스크 요청
- 18 — 주소 마스크 응답

코드

ICMP 메시지 유형에 대한 동반 코드. ICMP 메시지 유형 3, 5, 11 및 12에는 RFC 792에 설명된 응답 코드가 있습니다.

Checksum

ICMP 체크섬이 유효한지를 나타내는 지표. 체크섬이 유효하지 않으면 전송 중 데이터그램이 손상되었을 수 있습니다.

패킷 바이트 정보 보기

라이센스: 보호

패킷을 구성하는 바이트의 16진수 및 ASCII 버전을 보려면 패킷 보기에서 **Packet Bytes** 옆에 있는 화살표를 클릭합니다. 시스템이 트래픽을 해독하면 해독된 패킷 바이트를 볼 수 있습니다.

이벤트를 평가하기 위한 영향 레벨 사용

라이센스: 보호

이벤트가 네트워크에 미치는 영향을 평가할 수 있도록 방어 센터는 침입 이벤트의 테이블 보기에 영향 레벨을 표시합니다. 각 이벤트에 대해 방어 센터는 침입 데이터, 네트워크 검색 데이터 및 취약성 정보 사이의 상관관계를 색으로 나타내는 영향 레벨 아이콘을 추가합니다.

참고 NetFlow 데이터를 기반으로 네트워크 맵에 추가된 호스트에 대해 사용할 수 있는 운영 체제 정보가 없으므로, 호스트 입력 기능을 사용하여 호스트 운영 체제 ID를 수동으로 설정하지 않는 한 방어 센터에서는 그러한 호스트와 관련된 침입 이벤트에 대해 Vulnerable (impact level 1: red) 영향 레벨을 할당할 수 없습니다.

다음 표에서는 영향 레벨의 가능한 값에 대해 설명합니다.

표 41-6 영향 레벨

영향 레벨	취약성	색상	설명
0	Unknown	회색	소스 호스트와 목적지 호스트 모두 네트워크 검색에 의해 모니터링되는 네트워크에 없습니다.
1	Vulnerable	빨간색	다음 중 하나: • 소스 또는 목적지 호스트가 네트워크 맵에 있으며, 취약성이 호스트에 매핑됨 • 소스 또는 목적지 호스트가 바이러스, 트로이 목마 또는 기타 악의적인 소프트웨어로 구성되었을 수 있음. 자세한 내용은 36-45페이지의 영향 레벨 1 설정 참조
2	Potentially Vulnerable	주황색	소스 또는 목적지 호스트가 네트워크 맵에 있으며, 다음 중 하나가 참임: • 포트로 향하는 트래픽의 경우 포트가 서버 애플리케이션 프로토콜을 실행함 • 포트로 향하는 트래픽이 아닌 경우 호스트가 프로토콜을 사용함
3	Currently Not Vulnerable	노란색	소스 또는 목적지 호스트가 네트워크 맵에 있으며, 다음 중 하나가 참임: • 포트로 향하는 트래픽의 경우(예: TCP 또는 UDP), 포트가 열려 있지 않음 • 포트로 향하는 트래픽이 아닌 경우(예: ICMP), 호스트가 프로토콜을 사용하지 않음
4	Unknown Target	파란색	소스 호스트 또는 목적지 호스트가 모니터링되는 호스트에 있지만, 네트워크 맵에는 호스트에 대한 항목이 없음.

테이블 보기에서 영향 레벨을 사용하여 이벤트를 평가하려면

액세스: Admin/Intrusion Admin

1단계 **Analysis > Intrusions > Events**를 선택합니다.

기본 침입 이벤트 워크플로의 첫 번째 페이지가 나타납니다. 다른 기본 워크플로 지정에 대한 자세한 내용은 71-3페이지의 이벤트 보기 설정 구성을/를 참조하십시오. 이벤트가 표시되지 않을 경우 시간 범위를 조정해야 할 수 있습니다. 58-22페이지의 이벤트 시간 제약 조건 설정을/를 참조하십시오.

2단계 평가할 이벤트만 표시되도록 이벤트 보기를 제한합니다.

자세한 내용은 41-19페이지의 드릴다운 및 테이블 보기 페이지 사용을/를 참조하십시오.

3단계 페이지 상단에서 **Table View of Events**를 클릭합니다.

이벤트의 테이블 보기가 나타납니다. **Impact**의 값은 영향 레벨 표에 설명된 값 중 하나일 수 있습니다.

4단계 영향 수준으로 테이블을 정렬하려면 **Impact**를 클릭합니다.

이벤트가 영향 레벨 기준으로 정렬됩니다.

팁 정렬 순서를 반대로 하려면 **Impact**를 다시 클릭합니다.

프리프로세서 이벤트 읽기

라이센스: 보호

프리프로세서는 두 가지 기능을 제공합니다. 하나는 패킷에서 지정된 작업을 수행하는 것(예: HTTP 트래픽의 디코딩 및 표준화)이고, 다른 하나는 패킷이 지정된 프리프로세서 옵션을 트리거하고 관련 프리프로세서 규칙이 활성화될 때마다 이벤트를 생성함으로써 해당 프리프로세서 옵션의 실행을 보고하는 것입니다. 예를 들어 프리프로세서가 IIS 이중 인코딩 트래픽을 발견할 때 이벤트를 생성하도록 하려면 `Double Encoding` HTTP Inspect 옵션 그리고 HTTP Inspect GID(Generator ID) 119 및 SID(Snort ID) 2와 관련된 프리프로세서 규칙을 활성화할 수 있습니다. 프리프로세서의 실행을 보고하는 이벤트를 생성하면 비정상적인 프로토콜 익스플로잇을 탐지하는 데 도움이 됩니다. 예를 들어 공격자는 중복 IP 프래그먼트를 조작하여 호스트에서 DoS 공격을 일으킬 수 있습니다. IP 디프래그먼트화 프리프로세서는 이 유형의 공격을 탐지하고 이에 대한 침입 이벤트를 생성할 수 있습니다.

자세한 내용은 다음 절을 참조하십시오.

- 41-40페이지의 프리프로세서 이벤트 패킷 표시 이해 — 프리프로세서 생성 이벤트에 포함된 정보에 대해 설명합니다.
- 41-40페이지의 프리프로세서 Generator ID 읽기 — 프리프로세서 generator ID가 제공하는 정보에 대해 자세히 설명합니다.

프리프로세서 이벤트 패킷 표시 이해

라이센스: 보호

패킷 표시에 이벤트에 대한 자세한 규칙 설명이 포함되지 않는다는 점에서 프리프로세서 이벤트는 규칙 이벤트와 다릅니다. 대신 패킷 표시에는 이벤트 메시지, generator ID, Snort ID, 패킷 헤더 데이터 및 패킷 페이로드가 나타납니다. 이를 통해 패킷의 헤더 정보를 분석하고, 헤더 옵션이 사용 중인지와 시스템을 악용할 수 있는지를 파악하고, 패킷 페이로드를 검사할 수 있습니다. 프리프로세서가 각 패킷을 분석하면 규칙 엔진은 콘텐츠 수준 위협을 더 깊이 분석하고 보고할 수 있도록 이에 대해 적절한 규칙을 실행합니다(프리프로세서가 이를 디프래그먼트하고 유효한 세션의 일부로 설정할 수 있는 경우).

프리프로세서 **Generator ID** 읽기

라이센스: 보호

각 프리프로세서에는 어떤 프리프로세서가 패킷에 의해 트리거되었는지를 나타내는 자체 GID(Generator ID)가 있습니다. 일부 프리프로세서에는 또한 잠재적 공격을 분류하는 ID 번호인 관련 SID도 있습니다. 이를 통해, 규칙의 SID(Snort ID)가 규칙을 트리거하는 패킷에 대한 컨텍스트를 제공하는 것과 유사한 방식으로 이벤트의 유형을 카테고리화하여 이벤트를 훨씬 효과적으로 분석할 수 있습니다. 침입 정책 Rules 페이지의 Preprocessors 필터 그룹에 프리프로세서별로 프리프로세서 규칙을 나열할 수 있습니다. 또한 Category 필터 그룹의 프리프로세서 및 패킷 디코더 하위 그룹에 프리프로세서 규칙을 나열할 수도 있습니다. 자세한 내용은 32-1페이지의 규칙을 사용하여 침입 정책 조정 및 32-2 페이지의 표 32-1을/를 참조하십시오.

참고 표준 텍스트 규칙에 의해 생성된 이벤트의 generator ID는 1입니다. 이벤트의 SID는 어떤 특정 규칙이 트리거되었는지를 나타냅니다. 공유 객체 규칙의 경우 이벤트에는 특정 규칙이 트리거되었음을 나타내는 generator ID 3 및 SID가 있습니다.

다음 표에서는 각 GID를 생성하는 이벤트 유형에 대해 설명합니다.

표 41-7 Generator ID

ID	구성 요소	설명	참조 섹션
1	Standard Text Rule	패킷이 표준 텍스트 규칙을 트리거하여 이벤트가 생성되었습니다.	32-2 페이지의 표 32-1
2	Tagged Packets	Tag 생성기에 의해 이벤트가 생성되었으며, 이에 따라 태그가 지정된 세션에서 패킷이 생성됩니다. 이는 `tag` 규칙 옵션이 사용될 때 발생합니다.	36-90페이지의 공격 이후 트래픽 평가
3	Shared Object Rule	패킷이 공유 객체 규칙을 트리거하여 이벤트가 생성되었습니다.	32-2 페이지의 표 32-1
102	HTTP Decoder	디코더 엔진이 패킷 내에서 HTTP 데이터를 디코딩했습니다.	27-30페이지의 HTTP 트래픽 디코딩
105	Back Orifice Detector	Back Orifice Detector가 패킷과 관련된 Back Orifice 공격을 식별했습니다.	34-1페이지의 Back Orifice 탐지
106	RPC Decoder	RPC 디코더가 패킷을 디코딩했습니다.	27-45페이지의 Sun RPC 프리프로세서 사용
116	Packet Decoder	패킷 디코더에 의해 이벤트가 생성되었습니다.	29-17페이지의 패킷 디코딩 이해

표 41-7 Generator ID(계속)

ID	구성 요소	설명	참조 섹션
119, 120	HTTP Inspect Preprocessor	HTTP Inspect 프리프로세서에 의해 이벤트가 생성되었습니다. GID 120 규칙은 서버별 HTTP 트래픽과 관련이 있습니다.	27-30페이지의 HTTP 트래픽 디코딩
122	Portscan Detector	포트스캔 플로우 디코더에 의해 이벤트가 생성되었습니다. 자세한 내용은 다음을 참조하십시오.	34-3페이지의 포트스캔 탐지
123	IP Defragmentor	프래그먼트된 IP 데이터그램을 제대로 리어셈블할 수 없어서 이벤트가 생성되었습니다.	29-12페이지의 IP 패킷 디프래그먼트
124	SMTP Decoder	SMTP 프리프로세서가 SMTP 동사에서 익스플로잇을 탐지하여 이벤트가 생성되었습니다.	27-58페이지의 SMTP 디코딩 이해
125	FTP Decoder	FTP/Telnet 디코더가 FTP 트래픽 내에서 익스플로잇을 탐지하여 이벤트가 생성되었습니다.	27-22페이지의 서버 레벨 FTP 옵션 이해 27-27페이지의 클라이언트 레벨 FTP 옵션 이해
126	Telnet Decoder	FTP/Telnet 디코더가 텔넷 트래픽 내에서 익스플로잇을 탐지하여 이벤트가 생성되었습니다.	27-18페이지의 FTP 및 텔넷 트래픽 디코딩
128	SSH Preprocessor	SSH 프리프로세서가 SSH 트래픽 내에서 익스플로잇을 탐지하여 이벤트가 생성되었습니다.	27-66페이지의 SSH 프리프로세서를 사용하여 익스플로잇 탐지
129	Stream Preprocessor	스트림 프리프로세서에 의한 스트림 전처리 중에 이벤트가 생성되었습니다.	29-21페이지의 TCP 스트림 전처리 사용
131	DNS Preprocessor	DNS 프리프로세서에 의해 이벤트가 생성되었습니다.	27-14페이지의 DNS 이름 서버 응답에서 익스플로잇 탐지
133	DCE/RPC Preprocessor	DCE/RPC 프리프로세서에 의해 이벤트가 생성되었습니다.	27-2페이지의 DCE/RPC 트래픽 디코딩
134	Rule Latency Packet Latency	규칙 레이턴시가 침입 규칙의 그룹을 일시 중지(134:1) 또는 다시 활성화(134:2)하여, 또는 패킷 레이턴시 임계값이 초과되었기 때문에 시스템이 패킷 검사를 중지하여(134:3) 이벤트가 생성되었습니다.	18-12페이지의 패킷 및 침입 규칙 레이턴시 임계값 구성
135	Rate-Based Attack Detector	속도 기반 공격 탐지기가 네트워크의 호스트에 대한 과도한 연결을 식별하여 이벤트가 생성되었습니다.	34-9페이지의 속도 기반 공격 방지
138, 139	Sensitive Data Preprocessor	민감한 데이터 프리프로세서에 의해 이벤트가 생성되었습니다.	34-18페이지의 민감한 데이터 탐지
140	SIP Preprocessor	SIP 프리프로세서에 의해 이벤트가 생성되었습니다.	27-46페이지의 SIP(Session Initiation Protocol) 디코딩
141	IMAP Preprocessor	IMAP 프리프로세서에 의해 이벤트가 생성되었습니다.	27-52페이지의 IMAP 트래픽 디코딩
142	POP Preprocessor	POP 프리프로세서에 의해 이벤트가 생성되었습니다.	27-55페이지의 POP 트래픽 디코딩
143	GTP Preprocessor	GTP 프리프로세서에 의해 이벤트가 생성되었습니다.	27-51페이지의 GTP 명령 채널 구성

표 41-7 Generator ID(계속)

ID	구성 요소	설명	참조 섹션
144	Modbus Preprocessor	Modbus SCADA 프리프로세서에 의해 이벤트가 생성되었습니다.	28-1페이지의 Modbus 프리프로세서 구성
145	DNP3 Preprocessor	DNP3 SCADA 프리프로세서에 의해 이벤트가 생성되었습니다.	28-3페이지의 DNP3 프리프로세서 구성

침입 이벤트 검색

라이센스: 보호

FireSIGHT 시스템으로 제공된 사전 정의 검색을 사용하거나 자체 검색 기준을 생성하여 특정 침입 이벤트를 검색할 수 있습니다.

사전 정의된 검색은 예제 역할을 하며, 이를 통해 네트워크에 대한 정보에 빠르게 액세스할 수 있습니다. 네트워크 환경에 맞게 맞춤화하기 위해 기본 검색 내에서 특정 필드를 수정한 다음, 나중에 사용할 수 있도록 저장할 수 있습니다. 검색 결과는 검색 중인 이벤트에서 사용할 수 있는 데이터에 따라 달라집니다. 다시 말하면, 사용 가능한 데이터에 따라 검색 제한이 적용되지 않을 수 있습니다. 예를 들면 해독된 트래픽에 대해 트리거된 침입 이벤트에만 SSL 정보가 포함됩니다.

팁 침입 이벤트 검색에서 IP 주소 및 포트를 지정하기 위한 구문에 대한 자세한 내용은 60-6페이지의 검색에서 IP 주소 지정 및 60-7페이지의 검색에서 포트 지정을/를 참조하십시오.

저장된 검색을 로드 및 삭제하는 방법을 포함하여 검색에 대한 자세한 내용은 60-1페이지의 이벤트 검색을/를 참조하십시오.

사용할 수 있는 검색 기준은 다음 목록에 설명되어 있습니다.

Priority

보려는 이벤트의 우선순위를 지정합니다. 우선순위는 `priority` 키워드의 값 또는 `classtype` 키워드의 값에 해당합니다. 기타 침입 이벤트의 경우 우선순위는 디코더 또는 프리프로세서에 의해 결정됩니다. 유효한 값은 `high`, `medium` 및 `low`입니다.

Impact

침입 데이터와 네트워크 검색 데이터 간 상관관계를 기반으로 상관관계 이벤트에 할당되는 영향 레벨을 지정합니다. 유효한 값(대/소문자를 구분하지 않음): `Impact 0`, `Impact Level 0`, `Impact 1`, `Impact Level 1`, `Impact 2`, `Impact Level 2`, `Impact 3`, `Impact Level 3`, `Impact 4` 및 `Impact Level 4`.

영향 아이콘 색상 또는 부분 문자열(예: `blue`, `level 1` 또는 `0`)을 사용하지 마십시오.

자세한 내용은 41-38페이지의 이벤트를 평가하기 위한 영향 레벨 사용을/를 참조하십시오.

Inline Result

다음 중 하나 입력:

- `dropped` — 패킷이 인라인 구축에서 삭제되는지 여부를 지정
- `would have dropped` — 인라인 구축에서 패킷을 삭제하도록 침입 정책을 설정했다면 패킷이 삭제되었을 것인지를 지정

침입 정책의 규칙 상태 또는 인라인 삭제 동작과 상관없이, 인라인 인터페이스가 탭 모드인 경우를 포함하여 패시브 구축에서는 시스템이 패킷을 삭제하지 않습니다.

Source IP

침입 이벤트와 관련된 소스 호스트에 의해 사용되는 IP 주소를 지정합니다.

Destination IP

침입 이벤트와 관련된 목적지 호스트에 의해 사용되는 IP 주소를 지정합니다.

Source/Destination IP

침입 이벤트를 보려는 호스트에 의해 사용되는 소스 또는 목적지 IP 주소를 지정합니다.

Source Country

침입 이벤트와 관련된 소스 호스트의 국가를 지정합니다.

Destination Country

침입 이벤트와 관련된 목적지 호스트의 국가를 지정합니다.

Source/Destination Country

보려는 침입 이벤트와 관련된 소스 또는 목적지 호스트의 국가를 지정합니다.

Source Continent

침입 이벤트와 관련된 소스 호스트의 대륙을 지정합니다.

Destination Continent

침입 이벤트와 관련된 목적지 호스트의 대륙을 지정합니다.

Source/Destination Continent

보려는 침입 이벤트와 관련된 소스 또는 목적지 호스트의 대륙을 지정합니다.

Original Client IP

XFF(X-Forwarded-For), True-Client-IP 또는 사용자 정의 HTTP 헤더에서 추출된 원래 클라이언트 IP 주소를 지정합니다. 침입 이벤트에서 이 필드의 값을 추출하려면 HTTP 프리프로세서 **Extract Original Client IP Address** 옵션을 활성화해야 합니다. 선택적으로, 네트워크 분석 정책의 동일한 영역에서 최대 6개의 사용자 지정 클라이언트 IP 헤더를 지정할 수 있으며, 시스템이 Original Client IP 이벤트 필드에 대한 값을 선택하는 우선순위 순서를 설정할 수 있습니다. 자세한 내용은 27-32페이지의 서버 레벨 HTTP 표준화 옵션 선택을/를 참조하십시오.

Protocol

연결에 사용된 전송 프로토콜의 이름이나 번호를 http://www.iana.org/assignments/protocol-numbers에 표시된 대로 입력합니다.

침입 이벤트 테이블 보기에는 Protocol 열이 없습니다. 이것은 소스 및 목적지 포트/ICMP 열과 관련된 프로토콜입니다.

Source Port / ICMP Type

침입 이벤트와 관련된 소스 포트를 지정합니다.

팁 포트를 대상으로 하지 않는 ICMP 트래픽의 경우 특정 ICMP 유형의 이벤트를 검색하는 데 이 필드를 사용할 수 있습니다.

Destination Port / ICMP Code

침입 이벤트와 관련된 목적지 포트를 지정합니다.

팁 포트를 대상으로 하지 않는 ICMP 트래픽의 경우 특정 ICMP 코드의 이벤트를 검색하는 데 이 필드를 사용할 수 있습니다.

VLAN ID

침입 이벤트를 트리거한 패킷과 관련된 가장 안쪽 VLAN ID를 지정합니다.

MPLS Label

침입 이벤트를 트리거한 패킷과 관련된 패킷의 Multiprotocol Label Switching 레이블을 지정합니다.

Message

보려는 이벤트에 대한 이벤트 메시지의 전체 또는 일부를 지정합니다.

Classification

분류 번호, 또는 보려는 이벤트를 생성한 규칙에 대한 분류 이름이나 설명의 전체 또는 일부를 입력합니다. 쉼표로 구분된 숫자, 이름 또는 설명의 목록을 입력할 수도 있습니다. 마지막으로, 사용자 지정 분류를 추가하는 경우 이름이나 설명의 전체 또는 일부를 사용하여 검색할 수도 있습니다. 분류 번호, 이름 또는 설명의 목록은 규칙 분류 표를 참조하십시오.

Generator

보려는 이벤트를 생성한, 41-40 페이지의 표 41-7에 나열된 구성 요소를 지정합니다.

Snort ID

이벤트를 생성한 규칙의 SID(Snort ID)를 지정합니다. 또는 선택적으로, 규칙의 GID(generator ID)와 SID 조합을 지정합니다. 여기서 GID와 SID는 GID:SID 형식으로 콜론(:)으로 구분됩니다. 다음 표의 값을 지정할 수 있습니다.

표 41-8 Snort ID 검색 값

가치	예
단일 SID	10000
SID 범위	10000-11000
SID보다 큼	>10000
SID보다 크거나 같음	>=10000
SID보다 작음	<10000
SID보다 작거나 같음	<=10000

표 41-8 Snort ID 검색 값(계속)

가치	예
쉼표로 구분된 SID 목록	10000,11000,12000
단일 GID:SID 조합	1:10000
쉼표로 구분된 GID:SID 조합의 목록	1:10000,1:11000,1:12000
쉼표로 구분된 SID 및 GID:SID 조합의 목록	10000,1:11000,12000

자세한 내용은 41-40페이지의 프리프로세서 Generator ID 읽기을/를 참조하십시오.

Snort ID 열은 검색 결과에 나타나지 않습니다. 보고 있는 이벤트의 SID는 Message 열에 나열됩니다.

Source User

소스 호스트에 로그인한 사용자의 User ID를 지정합니다.

Destination User

목적지 호스트에 로그인한 사용자의 User ID를 지정합니다.

Source/Destination User

소스 또는 목적지 호스트에 로그인한 사용자의 User ID를 지정합니다.

Application Protocol

침입 이벤트를 트리거한 트래픽에서 탐지된, 호스트 간의 통신을 나타내는 애플리케이션 프로토콜의 이름을 입력합니다.

Client

침입 이벤트를 트리거한 트래픽에서 탐지된 모니터링되는 호스트에서 실행 중인 소프트웨어를 나타내는 클라이언트 애플리케이션의 이름을 입력합니다.

Web Application

침입 이벤트를 트리거한 트래픽에서 탐지된 HTTP 트래픽의 요청된 URL 또는 내용을 나타내는 웹 애플리케이션의 이름을 입력합니다.

Category, Tag(Application Protocol, Client, Web Application)

세션에서 탐지된 애플리케이션과 관련된 카테고리 또는 태그를 입력합니다. 여러 카테고리나 태그를 구분하려면 쉼표를 사용합니다. 이러한 필드는 대/소문자를 구분합니다.

Application Risk

세션에서 탐지된 애플리케이션과 관련된 최고 위험을 입력합니다. 유효한 기준은 `Very High`, `High`, `Medium`, `Low` 및 `Very Low`입니다. 이러한 필드는 대/소문자를 구분합니다.

Business Relevance

세션에서 탐지된 애플리케이션과 관련된 가장 낮은 비즈니스 연관성을 입력합니다. 유효한 기준은 `Very High`, `High`, `Medium`, `Low` 및 `Very Low`입니다. 이러한 필드는 대/소문자를 구분합니다.

Security Zone (Ingress, Egress, Ingress/Egress)

이벤트를 트리거한 패킷과 관련된 보안 영역의 이름을 입력합니다. 이러한 필드는 대/소문자를 구분합니다. 3-38페이지의 보안 영역 작업을/를 참조하십시오.

Device

액세스 제어 정책이 적용된 특정 디바이스로 검색을 제한하려면 디바이스 이름이나 IP 주소, 디바이스 그룹, 스택 또는 클러스터 이름을 입력합니다. FireSIGHT 시스템에서 검색 시 디바이스 필드를 처리하는 방법에 대한 자세한 내용은 60-7페이지의 검색에서 디바이스 지정을/를 참조하십시오.

스태킹된 컨피그레이션의 기본 및 보조 디바이스는 침입 이벤트를 별도로 보고합니다. 자세한 내용은 4-43페이지의 스태킹된 디바이스 관리을/를 참조하십시오.

Security Context

트래픽이 통과한 가상 방화벽 그룹을 식별하는 보안 컨텍스트의 이름을 입력합니다. 이 필드는 다중 컨텍스트 모드의 ASA FirePOWER 디바이스에 대해서만 채워집니다.

Interface (Ingress, Egress)

이벤트를 트리거한 패킷과 관련된 인터페이스의 이름을 입력합니다. 4-60페이지의 센싱 인터페이스 구성을/를 참조하십시오.

Intrusion Policy

이벤트와 관련된 침입 정책의 이름을 입력합니다. 31-3페이지의 침입 정책 관리을/를 참조하십시오.

Access Control Policy

이벤트와 관련된 액세스 제어 정책의 이름을 입력합니다. 12-10페이지의 액세스 제어 정책 관리을/를 참조하십시오.

Access Control Rule

이벤트와 관련된 액세스 제어 규칙의 이름을 입력합니다. 14-1페이지의 액세스 제어 규칙을 사용하여 트래픽 플로우 조정을/를 참조하십시오.

HTTP Hostname

HTTP 요청 Host 헤더에서 추출된 단일 호스트 이름을 지정합니다.

호스트 이름을 HTTP 클라이언트 트래픽에 대한 침입 이벤트와 연결하려면 HTTP Inspect 프리프로세서 **Log Hostname** 옵션을 활성화해야 합니다. 자세한 내용은 27-32페이지의 서버 레벨 HTTP 표준화 옵션 선택을/를 참조하십시오.

HTTP URI

침입 이벤트를 트리거한 HTTP 요청 패킷과 관련된 단일 URI를 지정합니다.

URI를 HTTP 트래픽에 대한 침입 이벤트와 연결하려면 HTTP Inspect 프리프로세서 **Log URI** 옵션을 활성화해야 합니다. 자세한 내용은 27-32페이지의 서버 레벨 HTTP 표준화 옵션 선택을/를 참조하십시오.

Email Sender

SMTP MAIL FROM 명령에서 추출된 이메일 전송자의 주소를 지정합니다. 쉼표로 구분된 목록을 입력하면 지정된 모든 주소와 관련된 이벤트를 검색할 수도 있습니다. 자세한 내용은 41-10페이지의 침입 이벤트 이해을/를 참조하십시오.

Email Recipient

SMTP RCPT TO 명령에서 추출된 이메일 수신자의 주소를 지정합니다. 쉼표로 구분된 목록을 입력하면 지정된 모든 주소와 관련된 이벤트를 검색할 수도 있습니다. 자세한 내용은 41-10페이지의 침입 이벤트 이해을/를 참조하십시오.

Email Attachments

MIME Content-Disposition 헤더에서 추출된 MIME 첨부 파일 이름을 지정합니다. 목록에서 모든 첨부 파일 이름과 관련된 이벤트를 검색하려면 쉼표로 구분된 목록을 입력합니다. 자세한 내용은 41-10페이지의 침입 이벤트 이해을/를 참조하십시오.

Email Headers

이메일 헤더에서 추출된 데이터를 지정합니다. 이메일 헤더는 침입 이벤트의 테이블 보기에 나타나지 않지만, 이메일 헤더를 검색 기준으로 사용할 수 있습니다.

이메일 헤더를 SMTP 트래픽용 침입 이벤트와 연결하려면 SMTP 프리프로세서 **Log Headers** 옵션을 활성화해야 합니다. 자세한 내용은 27-58페이지의 SMTP 디코딩 이해을/를 참조하십시오.

Reviewed By

이벤트를 검토한 사용자의 이름을 지정합니다. 41-16페이지의 침입 이벤트 검토을/를 참조하십시오.

팁 검토되지 않은 이벤트를 검색하려면 `unreviewed`를 입력할 수 있습니다.

침입 이벤트용 특수 검색 구문

위에 나열된 일반 검색 구문을 보완하기 위해 다음 목록에서는 침입 이벤트용 특수 검색 구문 몇 가지에 대해 설명합니다.

수행한 SSL Actual Action

시스템이 지정된 작업을 적용한 암호화 트래픽에 대한 침입 이벤트를 보려면 다음 키워드 중 하나를 입력하십시오.

- `Do Not Decrypt` — 시스템이 해독하지 못한 연결을 나타냅니다.
- `Block` 및 `Block with Reset` — 차단된 암호화 연결을 나타냅니다.
- `Decrypt (Known Key)` — 알려진 개인 키를 사용하여 해독된 수신 연결을 나타냅니다.
- `Decrypt (Replace Key)` — 대체된 공개 키가 있는 자체 서명된 서버 인증서를 사용하여 해독된 발신 연결을 나타냅니다.
- `Decrypt (Resign)` — 다시 서명된 서버 인증서를 사용하여 해독된 발신 연결을 나타냅니다.

이 열은 침입 이벤트 테이블 보기에 나타나지 않습니다.

SSL Failure Reason

지정된 이유로 시스템이 해독에 실패한 암호화 트래픽에 대한 침입 이벤트를 보려면 다음 키워드 중 하나를 입력하십시오.

- `Unknown`
- `No Match`
- `Success`
- `Uncached Session`
- `Unknown Cipher Suite`
- `Unsupported Cipher Suite`
- `Unsupported SSL Version`
- `SSL Compression Used`
- `Session Undecryptable in Passive Mode`

- Handshake Error
- Decryption Error
- Pending Server Name Category Lookup
- Pending Common Name Category Lookup
- Internal Error
- Network Parameters Unavailable
- Invalid Server Certificate Handle
- Server Certificate Fingerprint Unavailable
- Cannot Cache Subject DN
- Cannot Cache Issuer DN
- Unknown SSL Version
- External Certificate List Unavailable
- External Certificate Fingerprint Unavailable
- Internal Certificate List Invalid
- Internal Certificate List Unavailable
- Internal Certificate Unavailable
- Internal Certificate Fingerprint Unavailable
- Server Certificate Validation Unavailable
- Server Certificate Validation Failure
- Invalid Action

이 열은 침입 이벤트 테이블 보기에 나타나지 않습니다.

SSL Subject Country

인증서 주체의 국가와 연결된 암호화 트래픽에 대한 침입 이벤트를 보려면 두 글자의 ISO 3166-1 alpha-2 국가 코드를 입력하십시오.

이 열은 침입 이벤트 테이블 보기에 나타나지 않습니다.

SSL Issuer Country

인증서 발행자의 국가와 연결된 암호화 트래픽에 대한 침입 이벤트를 보려면 두 글자의 ISO 3166-1 alpha-2 국가 코드를 입력하십시오.

이 열은 침입 이벤트 테이블 보기에 나타나지 않습니다.

SSL Certificate Fingerprint

인증서와 연결된 트래픽에 대한 침입 이벤트를 보려면 해당 인증서의 인증에 사용된 SHA 해시 값을 입력하거나 붙여넣으십시오.

이 열은 침입 이벤트 테이블 보기에 나타나지 않습니다.

SSL Public Key Fingerprint

인증서와 연결된 트래픽에 대한 침입 이벤트를 보려면 해당 인증서 내에 포함된 공개 키의 인증에 사용된 SHA 해시 값을 입력하거나 붙여넣으십시오.

이 열은 침입 이벤트 테이블 보기에 나타나지 않습니다.

침입 이벤트를 검색하려면

액세스: Admin/Intrusion Admin

1단계 **Analysis > Search**를 선택합니다.

Intrusion Events search 페이지가 나타납니다.

침입 이벤트 목록을 보는 동안 **Search**를 클릭할 수도 있습니다(**Analysis > Intrusions > Events**).

2단계 절차 위의 목록에 설명된 대로 해당 필드에 검색 기준을 입력합니다.

- 검색에서 객체를 사용하는 방법을 포함하여 검색 구문에 대한 자세한 내용은 60-1페이지의 이벤트 검색을/를 참조하십시오.
- 공개 키 인증서와 관련된 필드는 39-32페이지의 암호화된 연결과 관련된 인증서 보기을/를 참조하십시오.
- 침입 이벤트용 특수 검색 구문은 41-47페이지의 침입 이벤트용 특수 검색 구문을/를 참조하십시오.

3단계 선택적으로, 검색을 저장하려면 **Private** 확인란을 선택하여 자신만 액세스할 수 있는 비공개로 검색을 저장할 수 있습니다. 또는 모든 사용자가 사용할 수 있도록 검색을 저장하려면 확인란을 선택하지 않습니다.

팁 사용자 지정 사용자 역할에 대한 데이터 제한으로서 검색을 사용하려면 **반드시** 비공개 검색으로 저장해야 합니다.

4단계 선택적으로, 나중에 다시 사용할 수 있도록 검색을 저장할 수 있습니다. 다음 옵션을 이용할 수 있습니다.

- 검색 기준을 저장하려면 **Save**를 클릭합니다.

  새 검색인 경우 검색 이름을 입력하도록 대화 상자가 나타납니다. 고유한 검색 이름을 입력하고 **Save**를 클릭합니다. 이미 존재하는 검색에 대한 새 조건을 저장하는 경우 프롬프트가 나타나지 않습니다. 나중에 실행할 수 있도록 검색이 저장됩니다(**Private**을 선택한 경우 자신만 볼 수 있음).

- 새 검색을 저장하거나, 저장된 기존 검색을 변경하여 만든 검색에 새 이름을 할당하려면 **Save As New**를 클릭합니다.

  검색 이름을 입력하도록 대화 상자가 나타납니다. 고유한 검색 이름을 입력하고 **Save**를 클릭합니다. 나중에 실행할 수 있도록 검색이 저장됩니다(**Private**을 선택한 경우 자신만 볼 수 있음).

5단계 검색을 시작하려면 **Search**를 클릭합니다.

검색 결과는 현재의 시간 범위로 제한되어 기본 침입 이벤트 워크플로에 나타납니다. 다른 기본 워크플로 지정에 대한 자세한 내용은 71-3페이지의 이벤트 보기 설정 구성을/를 참조하십시오.

클립보드 사용

라이센스: 보호

클립보드는 침입 이벤트 보기에서 침입 이벤트를 복사할 수 있는 보관 영역입니다. 이벤트를 클립보드에 추가하는 방법에 대한 자세한 내용은 41-19페이지의 드릴다운 및 테이블 보기 페이지 사용 및 41-22페이지의 패킷 보기 사용을/를 참조하십시오.

클립보드의 내용은 이벤트가 생성된 날짜 및 시간별로 정렬됩니다. 침입 이벤트를 클립보드에 추가한 후, 클립보드에서 삭제할 수도 있고 클립보드의 내용에 대해 보고서를 생성할 수도 있습니다.

보안 정책의 위반과 관련이 있는 것으로 의심하는 이벤트의 모음인 인시던트에 클립보드의 침입 이벤트를 추가할 수도 있습니다. 클립보드의 이벤트를 인시던트에 추가하는 방법에 대한 자세한 내용은 42-5페이지의 인시던트 생성을/를 참조하십시오.

자세한 내용은 다음 절을 참조하십시오.

- 41-50페이지의 클립보드 보고서 생성
- 41-51페이지의 클립보드에서 이벤트 삭제

클립보드 보고서 생성

라이센스: 보호

다른 이벤트 보기에서 하는 것처럼 클립보드의 이벤트에 대한 보고서를 생성할 수 있습니다.

클립보드에서 침입 이벤트에 대한 보고서를 생성하려면

액세스: Admin/Intrusion Admin

1단계 하나 이상의 이벤트를 클립보드에 추가합니다.

- 드릴다운 페이지 또는 이벤트의 테이블 보기에서 클립보드로 이벤트를 추가하는 방법에 대한 자세한 내용은 41-19페이지의 드릴다운 및 테이블 보기 페이지 사용을/를 참조하십시오.
- 패킷 보기에서 클립보드로 이벤트를 추가하는 방법에 대한 자세한 내용은 41-22페이지의 패킷 보기 사용을/를 참조하십시오.

2단계 **Analysis > Intrusions > Clipboard**를 선택합니다.

클립보드가 나타납니다.

3단계 다음 옵션을 이용할 수 있습니다.

- 클립보드의 페이지에 있는 특정 이벤트를 포함하려면 해당 페이지로 이동하고, 이벤트 옆의 확인란을 선택하고, **Generate Report**를 클릭합니다.
- 클립보드의 모든 이벤트를 포함하려면 **Generate Report All**을 클릭합니다.

어느 경우든 Report Templates 페이지가 나타납니다.

4단계 보고서의 모양을 지정한 후 **Generate**를 클릭합니다.

Generate Report 팝업 대화 상자가 나타납니다.

5단계 하나 이상의 출력 형식(HTML, PDF, CSV)을 선택하고, 선택적으로 다른 설정을 수정합니다.

팁 Report Designer 사용에 대한 자세한 내용은 57-1페이지의 보고서 작업을/를 참조하십시오.

6단계 **Generate**와 **Yes**를 차례로 클릭합니다.

Report Generation Complete 팝업 창이 보고서를 볼 수 있는 링크와 함께 나타납니다.

7단계 다음 중 하나를 클릭합니다.

- 보고서 링크 — 선택한 보고서를 표시할 새 창이 열립니다.
- **OK** — 보고서 디자인을 수정할 수 있는 Report Templates 페이지로 돌아갑니다.

클립보드에서 이벤트 삭제

라이센스: 보호

클립보드의 이벤트 중 인시던트에 추가하지 않으려는 이벤트가 있으면 해당 이벤트를 삭제할 수 있습니다.

참고 이벤트를 클립보드에서 삭제해도 이벤트 데이터베이스에서 삭제되지는 **않습니다**. 그러나 이벤트 데이터베이스에서 이벤트를 삭제하면 클립보드에서도 해당 이벤트가 삭제됩니다.

클립보드에서 이벤트를 삭제하려면

액세스: Admin/Intrusion Admin

1단계 **Analysis > Intrusions > Clipboard**를 선택합니다.

클립보드가 나타납니다.

2단계 다음 옵션을 이용할 수 있습니다.

- 클립보드의 페이지에 있는 특정 침입 이벤트를 삭제하려면 해당 페이지로 이동하고, 이벤트 옆의 확인란을 선택하고, **Delete**를 클릭합니다.

  이벤트가 삭제됩니다.

- 클립보드에서 모든 침입 이벤트를 삭제하려면 **Delete All**을 클릭합니다.

  클립보드에서 모든 이벤트가 삭제됩니다. Event Preferences에서 **Confirm 'All' Actions** 옵션을 선택하면 모든 이벤트를 삭제할 것인지 확인하는 메시지가 표시됩니다.

42장

인시던트 처리

인시던트 처리란 보안 정책 위반이 의심될 때 조직에서 취하는 대응을 가리킵니다. FireSIGHT 시스템에는 인시던트의 조사와 관련된 정보의 수집 및 처리를 지원하는 기능이 포함되어 있습니다. 이러한 기능을 통해 인시던트와 관련이 있을 수 있는 침입 이벤트와 패킷을 수집할 수 있습니다. 공격의 효과를 완화하기 위해 FireSIGHT 시스템의 외부에서 수행하는 활동에 대한 메모의 저장소로 인시던트를 사용할 수도 있습니다. 예를 들어 감염된 호스트를 네트워크에서 격리하도록 보안 정책에서 요구하는 경우 인시던트에 그 내용을 메모할 수 있습니다.

또한 FireSIGHT 시스템은 인시던트 라이프사이클을 지원하며, 따라서 공격에 대한 대응을 진행할 때 인시던트의 상태를 변경할 수 있습니다. 인시던트를 종료할 때 학습 내용의 결과로서 보안 정책에 대해 변경한 내용을 메모할 수 있습니다.

FireSIGHT 시스템에서 인시던트를 처리하는 방법에 대한 자세한 내용은 다음 절을 참조하십시오.

인시던트 처리 기본

라이센스: 보호

각 조직은 보안 정책 위반의 검색, 정의 및 대응에 대한 자체 프로세스를 가지고 있을 것입니다. 다음 절에서는 인시던트 처리의 몇 가지 기본 사항 및 인시던트 대응 계획에 FireSIGHT 시스템을 통합하는 방법에 대해 설명합니다.

인시던트 정의

라이센스: 보호

일반적으로 *인시던트*는 보안 정책 위반과 관련이 있을 것으로 의심되는 하나 이상의 침입 이벤트로 정의됩니다. Cisco에서는 인시던트에 대한 대응을 추적하기 위해 FireSIGHT 시스템에서 사용하는 기능을 설명하는 데에도 이 용어를 사용합니다.

41-1페이지의 침입 이벤트 작업에서 설명했듯이, 일부 침입 이벤트는 네트워크 자산의 가용성, 기밀성 및 무결성에서 다른 이벤트보다 더 중요합니다. 예를 들어 FireSIGHT 시스템에서 제공하는 포트 스캔 탐지 기능은 네트워크에서의 포트 스캐닝 활동을 지속적으로 알려줄 수 있습니다. 그러나 보안 정책에서는 포트 스캐닝을 명시적으로 금지하지 않거나 우선순위가 높은 위협으로 간주하지 않을 수 있으며, 따라서 직접적인 조치를 취하기보다는 향후 포렌식 연구를 위해 포트 스캐닝의 로그를 보존하고자 할 수 있습니다.

반면, 네트워크 내 호스트가 감염되었으며 DDoS(Distributed Denial-of-Service)에 참여하고 있음을 나타내는 이벤트가 생성되면, 이 활동은 명백한 보안 정책 위반이 될 수 있으므로 해당 이벤트의 조사를 추적하는 데 도움이 되도록 FireSIGHT 시스템에서 인시던트를 생성해야 합니다.

일반 인시던트 처리 프로세스

라이센스: 보호

각 조직은 보안 인시던트 처리를 위한 자체 프로세스를 정의할 수 있습니다. 대부분의 방법론에는 다음 단계의 일부 또는 전체가 포함됩니다.

- 42-2페이지의 준비
- 42-3페이지의 탐지 및 알림
- 42-3페이지의 조사 및 자격
- 42-3페이지의 의사소통
- 42-4페이지의 봉쇄 및 복구
- 42-4페이지의 습득한 교훈

이러한 각 단계에 대해서는 다음 절에서 설명합니다. 각 단계에서 FireSIGHT 시스템을 적절히 활용하는 방법에 대해서도 설명합니다.

준비

두 가지 방법으로 인시던트를 준비할 수 있습니다.

- 분명하고 포괄적인 보안 정책과 더불어 이를 적용할 하드웨어 및 소프트웨어 리소스를 지정합니다.
- 확실하게 정의된 인시던트 대응 계획을 세우고, 계획을 구현할 수 있도록 적절하게 팀을 훈련합니다.

인시던트 처리의 중요한 부분은 네트워크의 어떤 부분이 가장 위험한가를 파악하는 것입니다. 그러한 네트워크 세그먼트에 FireSIGHT 시스템 구성 요소를 구축하면 인시던트가 언제 어떻게 발생하는지를 더 잘 인지할 수 있습니다. 또한 각각의 관리되는 디바이스에 대해 침입 정책을 세부적으로 조정하면, 최고의 품질로 이벤트가 생성되도록 보장할 수 있습니다.

탐지 및 알림

인시던트를 탐지하지 못하면 인시던트에 대응할 수 없습니다. 인시던트 처리 프로세스에는 탐지할 수 있는 보안 관련 이벤트의 종류와 탐지에 사용되는 메커니즘(소프트웨어와 하드웨어 모두)을 명시해야 합니다. 또한 보안 정책의 위반을 어디서 탐지할 수 있는지도 명시해야 합니다. 네트워크에 능동적으로 또는 수동적으로 모니터링되지 않는 세그먼트가 포함되어 있으면 그러한 내용도 명시해야 합니다.

네트워크에 구축한 관리되는 디바이스는 각각 설치된 세그먼트에서 트래픽을 분석하여 침입을 탐지하고 이를 설명하는 이벤트를 생성해야 합니다. 관리되는 디바이스 각각에 적용하는 액세스 제어 정책은 탐지할 활동의 종류 및 우선순위 지정 방법을 결정합니다. 인시던트 팀이 수백 개의 인시던트를 엄밀히 조사하지 않아도 되도록 특정 침입 이벤트 유형에 대한 알림 옵션을 설정할 수 있습니다. 특정 레벨의 우선순위, 특정 레벨의 심각도 이벤트가 탐지될 때 자동으로 알림을 전송하도록 지정할 수 있습니다.

조사 및 자격

인시던트 처리 프로세스에는 보안 인시던트가 탐지된 이후 조사를 수행하는 방법을 지정해야 합니다. 일부 조직에서는 팀의 신입 멤버가 모든 인시던트를 분류하고 덜 심각하거나 우선순위가 낮은 사례를 직접 처리합니다. 심각도와 우선순위가 높은 인시던트는 팀의 선임 멤버가 처리합니다. 각 팀 멤버가 인시던트의 중요도를 결정하는 기준을 이해할 수 있도록 에스컬레이션 프로세스를 신중하게 정리해두어야 합니다.

에스컬레이션 프로세스의 일부는 탐지된 이벤트가 네트워크 자산의 보안에 어떤 영향을 미칠 수 있는지를 파악하는 것과 연결됩니다. 예를 들어 Microsoft SQL Server를 실행하는 호스트에 대한 공격은 다른 데이터베이스 서버를 사용하는 조직에서 우선순위가 높지 않습니다. 마찬가지로, 이 공격은 네트워크에서 SQL Server를 사용하는 경우에도 덜 중요하지만, 모든 서버가 패치되었고 공격에 취약하지 않은지를 확인해야 합니다. 그러나 누군가가 최근에 취약한 소프트웨어 버전을 설치했다면(예: 테스트 목적으로), 피상적인 조사에서 제시하는 것보다 문제가 더 클 수 있습니다.

FireSIGHT 시스템은 조사 및 자격 프로세스의 지원에서 특별히 뛰어납니다. 사용자는 고유한 이벤트 분류를 생성한 다음 네트워크 취약성에 가장 적합하게 적용할 수 있습니다. 네트워크의 트래픽이 이벤트를 트리거하면 특수 지표를 통해 해당 이벤트에 대한 우선순위와 자격이 자동으로 지정되어, 어떤 공격이 취약한 것으로 알려진 호스트로 향하는지를 알 수 있습니다.

또한 FireSIGHT 시스템의 인시던트 추적 기능에는 어떤 인시던트가 에스컬레이션되었는지를 표시하기 위해 변경할 수 있는 상태 지표도 포함됩니다.

의사소통

모든 인시던트 처리 프로세스에는 인시던트 처리 팀과 내부 및 외부 담당자 간 인시던트의 커뮤니케이션 방법을 지정해야 합니다. 예를 들면, 관리 개입이 필요한 인시던트 종류 및 해당 레벨을 고려해야 합니다. 외부 조직과의 커뮤니케이션 방법 및 시기에 대해서도 프로세스에 명시해야 합니다. 일부 인시던트의 경우 법 집행 기관에 알려야 합니까? 호스트가 원격 사이트에 대한 DDoS(distributed denial of service)에 참여하고 있는 경우 해당 사이트에 알려야 합니까? CERT/CC(CERT Coordination Center) 또는 FIRST 등의 조직과 정보를 공유하고자 합니까?

FireSIGHT 시스템에는 타인과 손쉽게 공유할 수 있도록 침입 데이터를 HTML, PDF, CSV(comma-separated values) 등의 표준 형식으로 수집할 수 있는 기능이 있습니다.

예를 들어 CERT/CC는 웹사이트의 보안 인시던트에 대한 표준 정보를 수집합니다. CERT/CC는 FireSIGHT 시스템에서 손쉽게 추출할 수 있는 다음과 같은 유형의 정보를 찾습니다.

- 영향을 받는 시스템에 대한 다음과 같은 정보:
- 호스트 이름 및 IP
- 표준 시간대
- 호스트의 목적 또는 기능
- 공격 소스에 대한 다음과 같은 정보:

- 호스트 이름 및 IP
- 표준 시간대
- 공격자와 접촉이 있었는지 여부
- 인시던트 처리 예상 비용
- 인시던트에 대한 다음과 같은 설명:
- 날짜
- 침입 방법
- 관련된 침입자 툴
- 소프트웨어 버전 및 패치 레벨
- 침입자 툴 출력
- 악용된 취약성 세부사항
- 공격의 소스
- 기타 관련 정보

인시던트의 코멘트 섹션을 사용하여 문제에 대해 누구와 언제 커뮤니케이션했는지를 기록할 수 있습니다.

봉쇄 및 복구

인시던트 처리 프로세스에는 호스트 또는 다른 네트워크 구성 요소가 손상될 때 어떤 단계를 따라야 하는지를 분명히 명시해야 합니다. 봉쇄 및 복구 옵션의 범위는 취약한 호스트에 패치를 적용하는 것부터 대상을 종료하고 네트워크에서 제거하는 것까지 다양합니다. 또한 공격의 본질과 심각도에 따라, 형사 고발로 이어질 경우에 대비하여 증거 보존의 중요도를 고려해야 합니다.

인시던트의 봉쇄 및 복구 단계 중에 취한 작업의 레코드를 유지 관리하려면 FireSIGHT 시스템의 인시던트 기능을 사용할 수 있습니다.

습득한 교훈

성공적인 공격이든 아니든, 각 보안 인시던트는 보안 정책을 검토할 수 있는 기회입니다. 방화벽 규칙을 업데이트해야 합니까? 패치 관리에 대해 좀 더 구조적인 접근 방식이 필요합니까? 무단 무선 액세스 포인트가 새로운 보안 문제입니까? 각각의 습득한 교훈을 보안 정책에 반영하여 다음 인시던트에 더 잘 대비해야 합니다.

FireSIGHT 시스템의 인시던트 유형

라이센스: 보호

생성하는 각 인시던트에 인시던트 유형을 할당할 수 있습니다. 기본적으로 FireSIGHT 시스템에서는 다음 유형이 지원됩니다.

- 침입
- 서비스 거부
- 무단 관리자 액세스
- 웹사이트 파손
- 시스템 무결성 손상
- 날조
- 도난

- 손상
- 알 수 없음

또한 42-8페이지의 사용자 지정 인시던트 유형 생성에 설명된 대로 고유한 인시던트 유형을 생성할 수 있습니다.

인시던트 생성

라이센스: 보호

이 절에서는 인시던트 생성 방법에 대해 설명합니다.

인시던트를 생성하려면

액세스: Admin/Intrusion Admin

1단계 **Analysis > Intrusions > Incidents**를 선택합니다.

Incidents 페이지가 나타납니다.

2단계 **Create Incident**를 클릭합니다.

Create Incident 페이지가 나타납니다.

전에 침입 이벤트를 클립보드에 복사한 경우 페이지 하단에 나타납니다. 클립보드 사용에 대한 자세한 내용은 41-50페이지의 클립보드 사용을/를 참조하십시오.

3단계 **Type** 드롭다운 메뉴에서 인시던트를 가장 잘 설명하는 옵션을 선택합니다.

4단계 인시던트에 사용한 시간을 #d #h #m #s 형식으로 **Time Spent** 필드에 입력합니다. #은 일수, 시간, 분 또는 초를 나타냅니다.

5단계 인시던트에 대한 짧은 설명을 **Summary** 텍스트 상자에 입력합니다(최대 255자의 영숫자 문자, 공백 및 기호).

6단계 인시던트에 대한 좀 더 완전한 설명을 **Add Comment** 텍스트 상자에 입력합니다(최대 8191자의 영숫자 문자, 공백 및 기호).

7단계 이 인시던트에 이벤트를 추가하시겠습니까?

- 대답이 **예**인 경우 클립보드에서 이벤트를 선택하고 **Add to Incident**를 클릭합니다.

  Add All to Incident를 클릭하면 클립보드의 모든 이벤트를 추가할 수 있습니다.
- 대답이 **아니요**인 경우 **Save**를 클릭합니다.

어떤 경우든, 입력한 정보와 함께 인시던트가 저장됩니다.

참고 둘 이상의 클립보드 페이지에서 개별 이벤트를 추가하려는 경우, 먼저 한 페이지의 이벤트를 추가한 후 다른 페이지의 이벤트를 별도로 추가해야 합니다.

인시던트 입력

라이센스: 보호

더 많은 정보를 수집함에 따라 인시던트를 업데이트할 수 있습니다. 조사를 진행하면서 인시던트에서 이벤트를 추가 또는 삭제할 수도 있습니다.

인시던트를 수정하려면

액세스: Admin/Intrusion Admin

1단계 **Analysis > Intrusions > Incidents**를 선택합니다.

Incidents 페이지가 나타납니다.

2단계 수정할 인시던트 옆에 있는 수정 아이콘( )을 클릭합니다.

3단계 인시던트의 다음과 같은 부분을 수정할 수 있습니다.

- 상태 변경
- 유형 변경
- 클립보드에서 이벤트 추가
- 이벤트 삭제

4단계 인시던트에 사용한 추가 시간을 **Time Spent** 필드에 입력합니다.

5단계 인시던트에 대한 변경 사항의 설명을 **Add Comment** 텍스트 상자에 입력합니다(최대 8191자의 영숫자 문자, 공백 및 기호).

6단계 선택적으로, 인시던트에서 이벤트를 추가 또는 삭제할 수 있습니다.

- 클립보드의 이벤트를 추가하려면 클립보드에서 원하는 이벤트를 선택하고 **Add to Incident**를 클릭합니다.
- 클립보드의 모든 이벤트를 추가하려면 **Add All to Incident**를 클릭합니다.
- 인시던트에서 특정 이벤트를 삭제하려면 이벤트를 선택하고 **Delete**를 클릭합니다.
- 인시던트에서 모든 이벤트를 삭제하려면 **Delete All**을 클릭합니다.
- 이벤트를 추가 또는 삭제하지 않고 인시던트를 업데이트하려면 **Save**를 클릭합니다.

인시던트에 대한 변경 사항이 저장됩니다.

인시던트 보고서 생성

라이센스: 보호

FireSIGHT 시스템을 사용하면 인시던트에 추가한 이벤트의 정보와 함께 인시던트 요약, 인시던트 상태 및 코멘트를 포함할 수 있는 인시던트 보고서를 생성할 수 있습니다. 또한 보고서에 이벤트 요약 정보를 포함할지 여부를 지정할 수 있습니다.

인시던트 보고서를 생성하려면

액세스: Admin/Intrusion Admin

1단계 **Analysis > Intrusions > Incidents**를 선택합니다.

Incidents 페이지가 나타납니다.

2단계 보고서에 포함할 인시던트 옆에 있는 수정 아이콘()을 클릭합니다.

3단계 다음 2가지 옵션을 사용할 수 있습니다.

- 인시던트의 모든 이벤트를 보고서에 포함하려면 **Generate Report All**을 클릭합니다.
- 인시던트의 특정 이벤트를 보고서에 포함하려면 원하는 이벤트 옆의 확인란을 선택하고 **Generate Report**를 클릭합니다.

어떤 경우든, 인시던트 보고서에 대한 옵션이 있는 Generate Report 페이지가 나타납니다.

4단계 보고서의 이름을 입력합니다. 영숫자, 마침표 및 공백을 사용할 수 있습니다.

5단계 **Incident Report Sections**에서, 보고서에 포함할 인시던트의 부분에 대한 확인란(**status**, **summary**, 및 **comments**)을 선택합니다.

6단계 보고서에 이벤트 정보를 포함하려면 사용하려는 워크플로를 선택하고, **Report Sections**에서 이벤트 요약 정보의 포함 여부를 지정합니다.

7단계 보고서에 포함할 워크플로 페이지 옆에 있는 확인란을 선택합니다.

8단계 보고서에 대해 사용할 출력 형식(**PDF**, **HTML** 및 **CSV**) 옆에 있는 확인란을 선택합니다.

참고 CSV 기반 인시던트 보고서에는 이벤트 정보만 포함됩니다. 인시던트의 상태, 요약 또는 코멘트는 포함되지 **않습니다**.

9단계 **Generate Report**를 클릭하고 보고서 프로필 업데이트를 확인합니다.

보고서가 생성됩니다.

사용자 지정 인시던트 유형 생성

라이센스: 보호

FireSIGHT 시스템에서는 인시던트 분류에 사용할 수 있는 다음과 같은 인시던트 유형을 제공합니다.

- 시스템 무결성 손상
- 손상
- 서비스 거부
- 날조
- 침입
- 도난
- 무단 관리자 액세스
- 알 수 없음
- 웹사이트 파손

이러한 인시던트 유형이 요구에 맞지 않으면 자신의 유형을 추가할 수 있습니다. 사용자 지정 인시던트 유형은 삭제할 수 없습니다.

새 인시던트 유형을 생성하려면

액세스: Admin/Intrusion Admin

1단계 **Analysis > Intrusions > Incidents**를 선택합니다.

Incident 페이지가 나타납니다.

2단계 **Create Incident**를 클릭합니다.

Create Incident 페이지가 나타납니다.

3단계 **Type** 영역에서 **Types**를 클릭합니다.

Incident Management Types 페이지가 나타납니다. 기본 인시던트 유형이 페이지 하단에 나열됩니다.

4단계 **Incident Type Name** 필드에 새 인시던트 유형의 이름을 입력합니다.

영숫자와 공백을 사용할 수 있습니다.

5단계 **Add**를 클릭합니다.

새 인시던트 유형이 추가됩니다.

6단계 **Done**을 클릭하여 팝업 창을 닫고 Incidents 페이지로 돌아갑니다.

다음에 인시던트를 생성하거나 수정할 때 새 인시던트 유형을 사용할 수 있습니다.

43장

외부 알림 구성

FireSIGHT 시스템에서는 웹 인터페이스 내 다양한 이벤트 보기를 제공하며, 사용자는 중요한 시스템을 지속적으로 모니터링할 수 있도록 외부 이벤트 알림을 구성할 수 있습니다. 다음 중 하나가 발생하는 경우 이메일, SNMP 트랩 또는 syslog를 통해 전달하는 알림을 생성하도록 FireSIGHT 시스템을 구성할 수 있습니다.

- 특정 영향 플래그가 있는 침입 이벤트
- 특정 검색 이벤트 유형
- 네트워크 기반 악성코드 이벤트 또는 소급 악성코드 이벤트
- 특정 상관관계 정책 위반에 의해 트리거된 상관관계 이벤트
- 특정 액세스 제어 규칙에 의해 트리거된 연결 이벤트
- 상태 정책의 모듈에 대한 특정 상태 변경

시스템에서 이러한 알림을 전송하도록 하려면 먼저 FireSIGHT 시스템 및 알림을 전송할 외부 시스템의 상호 작용을 허용하는 컨피그레이션 집합인 *알림 응답*을 생성해야 합니다. 그러한 컨피그레이션에서는 예를 들면 이메일 릴레이 호스트, SNMP 알림 매개 변수 또는 syslog 기능과 우선순위를 지정할 수 있습니다.

알림 응답을 생성한 후에는 알림을 트리거하는 데 사용할 이벤트와 연결합니다. 알림 응답을 이벤트와 연결하는 프로세스는 이벤트 유형에 따라 다릅니다.

- 각각의 컨피그레이션 페이지를 사용하여 알림 응답을 영향 플래그, 검색 이벤트 및 악성코드 이벤트와 연결합니다.
- 상관관계 정책에서 상관관계 이벤트를 알림 응답(및 교정 응답, 54-1페이지의 교정 생성 참조)과 연결합니다.
- 액세스 제어 규칙과 정책을 사용하여 SNMP 및 syslog 알림 응답을 로깅된 연결과 연결합니다. 로깅된 연결에는 이메일 알림이 지원되지 않습니다.
- 상태 모니터링을 사용하여 알림 응답을 상태 모듈 상태 변경과 연결합니다.

FireSIGHT 시스템에서 수행할 수 있는 또 다른 알림 유형이 있습니다. 즉, 영향 플래그와 상관없이 개별 침입 이벤트에 대해 이메일, SNMP 및 syslog 침입 이벤트 알림을 구성하는 것입니다. 이러한 알림은 침입 정책에서 구성합니다. 44-1페이지의 침입 규칙에 대한 외부 알림 구성 및 32-33페이지의 SNMP 알림 추가을/를 참조하십시오. 다음 표에서는 알림을 생성하기 위해 보유해야 하는 라이센스에 대해 설명합니다.

표 43-1 알림 생성을 위한 라이센스 요건

다음을 기반으로 알림 생성	필요한 라이센스
특정 영향 플래그가 있는 침입 이벤트	FireSIGHT + 보호
특정 검색 이벤트 유형	FireSIGHT
네트워크 기반 악성코드 이벤트	악성코드
상관관계 정책 위반	정책 위반 트리거에 필요한 라이센스
연결 이벤트	연결 로깅에 필요한 라이센스
상태 모듈 상태 변경	모두

자세한 내용은 다음 링크를 참고하십시오.

- 43-2페이지의 알림 응답 작업
- 43-8페이지의 영향 플래그 알림 구성
- 43-9페이지의 검색 이벤트 알림 구성
- 43-9페이지의 AMP 알림 구성
- 51-48페이지의 규칙 및 화이트리스트에 응답 추가
- 38-1페이지의 네트워크 트래픽의 연결 로깅
- 68-38페이지의 상태 모니터 알림 구성

알림 응답 작업

라이센스: 모두

외부 알림을 구성하는 첫 단계는, 알림을 전송할 외부 시스템과 FireSIGHT 시스템의 상호 작용을 허용하는 컨피그레이션 집합인 알림 응답을 생성하는 것입니다. 이메일, SNMP(Simple Network Management Protocol) 트랩 또는 syslog(시스템 로그)를 통해 알림을 전송하려면 알림 응답을 생성할 수 있습니다.

알림을 통해 수신하는 정보는 알림을 트리거한 이벤트 유형에 따라 달라집니다. 예를 들어, 영향 플래그 알림에는 타임스탬프, 침입 규칙, 영향 플래그 및 이벤트 설명 정보가 포함됩니다. 또 다른 예로 검색 이벤트 알림에는 타임스탬프와 설명 정보, 그리고 검색 이벤트 유형 정보가 포함됩니다.

상관관계 정책에서 알림 응답을 사용 중인 경우 알림의 정보는 상관관계 정책 위반을 트리거한 이벤트 유형에 따라 달라집니다.

참고 연결 추적을 포함하는 상관관계 규칙에 대한 응답으로서 알림을 구성하는 경우, 상관관계 규칙 자체가 다른 종류의 이벤트를 기반으로 하더라도 사용자가 수신하는 알림 정보는 트래픽 프로필 변경에 대한 알림의 정보와 동일합니다.

알림 응답은 생성과 동시에 자동으로 활성화됩니다. 활성화된 알림 응답만이 알림을 생성할 수 있습니다. 알림의 생성을 중지하려면 컨피그레이션을 삭제하기보다 알림 응답을 일시적으로 비활성화할 수 있습니다.

Alerts 페이지에서 알림 응답을 관리합니다(**Policies > Actions > Alerts**). 각 알림 응답 옆의 슬라이더는 활성 여부를 나타냅니다. 활성화된 알림 응답만 알림을 생성할 수 있습니다. 이 페이지에서는 또한 알림 응답이 컨피그레이션에서 사용되고 있는지도 알 수 있습니다(예: 액세스 제어 규칙에서 연결을 기록하기 위해). 해당 열 제목을 클릭하여 이름, 유형, 사용 상태 및 활성화/비활성화 상태 기준으로 알림 응답을 정렬할 수 있습니다. 열 제목을 다시 클릭하면 역순으로 정렬됩니다.

자세한 내용은 다음 링크를 참고하십시오.

이메일 알림 응답 생성

라이센스: 모두

액세스 제어 정책의 로깅된 연결에서는 이메일 알림을 수행할 수 **없습니다**.

이메일 알림 응답을 생성하려면 먼저 방어 센터에서 자체 IP 주소를 역해석할 수 있는지 확인해야 합니다. 또한 63-18페이지의 메일 릴레이 호스트 및 알림 주소 구성에 설명된 대로 메일 릴레이 호스트를 구성해야 합니다.

이메일 알림 응답을 생성하려면

액세스: Admin

1단계 **Policies > Actions > Alerts**를 선택합니다.

Alerts 페이지가 나타납니다.

2단계 **Create Alert** 드롭다운 메뉴에서 **Create Email Alert**를 선택합니다.

Create Email Alert Configuration 팝업 창이 나타납니다.

3단계 알림 응답을 식별하는 데 사용할 이름을 **Name** 필드에 입력합니다.

4단계 알림을 전송할 이메일 주소를 **To** 필드에 입력합니다.

이메일 주소가 여러 개인 경우 쉼표로 구분하십시오.

5단계 알림 전송자로 표시할 이메일 주소를 **From** 필드에 입력합니다.

6단계 **Relay Host** 옆에서, 나열된 메일 서버가 알림을 전송하는 데 사용하려는 서버인지 확인합니다.

서버를 변경하려면, 또는 릴레이 호스트를 아직 구성하지 않은 경우, 수정 아이콘( )을 클릭하여 팝업 창에 System Policy 페이지를 표시한 다음 63-18페이지의 메일 릴레이 호스트 및 알림 주소 구성의 지침을 따르십시오. 시스템 정책을 수정한 후 적용해야만 변경 사항이 반영됩니다.

7단계 **Save**를 클릭합니다.

알림 응답이 저장되고 자동으로 활성화됩니다.

SNMP 알림 응답 생성

라이센스: 모두

SNMPv1, SNMPv2 또는 SNMPv3을 사용하여 SNMP 알림 응답을 생성할 수 있습니다.

참고 64비트 값을 SNMP로 모니터링하려면 SNMPv2 또는 SNMPv3을 사용해야 합니다. SNMPv1에서는 64비트 모니터링을 지원하지 않습니다.

네트워크 관리 시스템에 방어 센터의 MIB(Management Information Base) 파일이 필요한 경우 `/etc/sf/DCEALERT.MIB`에서 가져올 수 있습니다.

SNMP 알림 응답을 생성하려면

액세스: Admin

1단계 **Policies > Actions > Alerts**를 선택합니다.

Alerts 페이지가 나타납니다.

2단계 **Create Alert** 드롭다운 메뉴에서 **Create SNMP Alert**를 선택합니다.

Create SNMP Alert Configuration 팝업 창이 나타납니다.

3단계 SNMP 응답을 식별하는 데 사용할 이름을 **Name** 필드에 입력합니다.

4단계 SNMP 트랩 서버의 호스트 이름 또는 IP 주소를 영숫자 문자를 사용하여 **Trap Server** 필드에 입력합니다.

이 필드에 잘못된 IPv4 주소(예: 192.169.1.456)를 입력해도 시스템에서 경고를 표시하지 **않습니다**. 대신, 잘못된 주소는 호스트 이름으로 처리됩니다.

5단계 사용할 SNMP 버전을 **Version** 드롭다운 목록에서 선택합니다.

SNMP v3이 기본값입니다. SNMP v1 또는 SNMP v2를 선택하면 다른 옵션이 나타납니다.

6단계 어떤 SNMP 버전을 선택하셨습니까?

- SNMP v1 또는 SNMP v2의 경우, 영숫자 문자나 특수 문자 * 또는 $를 사용하여 **Community String** 필드에 SNMP 커뮤니티 이름을 입력하고 12단계로 건너뜁니다.
- SNMP v3의 경우, SNMP 서버로 인증할 사용자의 이름을 **User Name** 필드에 입력하고 다음 단계로 계속 진행합니다.

7단계 **Authentication Protocol** 드롭다운 목록에서 인증에 사용할 프로토콜을 선택합니다.

8단계 SNMP 서버와의 인증에 필요한 비밀번호를 **Authentication Password** 필드에 입력합니다.

9단계 **Privacy Protocol** 목록에서, 비공개 프로토콜을 사용하지 않으려면 **None**을 선택하고 Data Encryption Standard를 비공개 프로토콜로 사용하려면 **DES**를 선택합니다.

10단계 SNMP 서버에 필요한 비공개 비밀번호를 **Privacy Password** 필드에 입력합니다.

11단계 짝수를 사용하여 SNMP 엔진의 ID를 16진수 표기법으로 **Engine ID** 필드에 입력합니다.

SNMPv3을 사용하는 경우 시스템에서는 메시지 암호화에 Engine ID 값을 사용합니다. SNMP 서버에서 메시지를 암호 해독하려면 이 값이 필요합니다.

Cisco에서는 방어 센터 IP 주소의 16진수 버전을 사용할 것을 권장합니다. 예를 들어 방어 센터의 IP 주소가 `10.1.1.77`이면 `0a01014D0`을 사용합니다.

12단계 **Save**를 클릭합니다.

알림 응답이 저장되고 자동으로 활성화됩니다.

Syslog 알림 응답 생성

라이센스: 모두

Syslog 알림 응답을 구성할 때에는 syslog 서버에서 적절히 처리되도록, syslog 메시지와 연결된 심각도 및 기능을 지정할 수 있습니다. 기능은 메시지를 생성하는 하위 시스템을 나타내며, 심각도는 메시지의 심각도를 정의합니다. 기능과 심각도는 syslog에 나타나는 실제 메시지에는 표시되지 않지만, syslog 메시지를 수신하는 시스템에 카테고리화 방법을 알려주는 데 사용됩니다.

팁 Syslog 작동 방식 및 구성 방법에 대한 자세한 내용은 시스템의 설명서를 참조하십시오. UNIX 시스템에서는 `syslog` 및 `syslog.conf`의 `man` 페이지에서 개념 정보 및 컨피그레이션 지침을 제공합니다.

Syslog 알림 응답을 생성할 때에는 어떤 유형의 기능이든 선택할 수 있지만, 모든 기능을 지원하는 모든 syslog 서버가 아니라 현재의 syslog 서버를 기반으로 합리적인 하나의 기능을 선택해야 합니다. UNIX syslog 서버의 경우 `syslog.conf` 파일은 어떤 기능이 서버의 어떤 로그 파일에 저장되는지를 나타냅니다.

다음 표에는 선택 가능한 syslog 기능이 나열되어 있습니다.

표 43-2 사용 가능한 Syslog 기능

설비	설명
ALERT	알림 메시지
AUDIT	감사 하위 시스템에 의해 생성된 메시지
AUTH	보안 및 인증과 관련된 메시지
AUTHPRIV	보안 및 인증과 관련된 제한적인 액세스 메시지. 많은 시스템에서 이러한 메시지는 보안 파일로 전달됩니다
CLOCK	클록 디먼에 의해 생성된 메시지 Windows 운영 체제를 실행하는 syslog 서버는 `CLOCK` 기능을 사용합니다.
CRON	클록 디먼에 의해 생성된 메시지 Linux 운영 체제를 실행하는 syslog 서버는 `CRON` 기능을 사용합니다.
DAEMON	시스템 디먼에 의해 생성된 메시지
FTP	FTP 디먼에 의해 생성된 메시지
KERN	커널에 의해 생성된 메시지. 많은 시스템에서 이러한 메시지는 콘솔에 인쇄되어 나타납니다
LOCAL0-LOCAL7	내부 프로세스에 의해 생성된 메시지
LPR	인쇄 하위 시스템에 의해 생성된 메시지
MAIL	메일 시스템에 의해 생성된 메시지
NEWS	네트워크 뉴스 하위 시스템에 의해 생성된 메시지
NTP	NTP 디먼에 의해 생성된 메시지
SYSLOG	Syslog 디먼에 의해 생성된 메시지
USER	사용자 레벨 프로세스에 의해 생성된 메시지
UUCP	UUCP 하위 시스템에 의해 생성된 메시지

다음 표에는 선택 가능한 표준 syslog 심각도가 나열되어 있습니다.

표 43-3 Syslog 심각도

수준	설명
ALERT	즉시 해결해야 하는 상태
CRIT	심각한 상태
DEBUG	디버깅 정보가 포함된 메시지
EMERG	모든 사용자에게 위험 상태 알림
ERR	오류 상태
INFO	정보 메시지
NOTICE	오류 상태는 아니지만 주의가 필요한 상태
WARNING	경고 메시지

Syslog 알림 전송을 시작하기 전에, syslog 서버가 원격 메시지를 허용할 수 있는지 확인해야 합니다.

Syslog 알림을 생성하려면

액세스: Admin

1단계 **Policies > Actions > Alerts**를 선택합니다.

Alerts 페이지가 나타납니다. **Create Alert** 드롭다운 메뉴에서 **Create Syslog Alert**를 선택합니다.

Create Syslog Alert Configuration 팝업 창이 나타납니다.

2단계 저장된 응답을 식별하는 데 사용할 이름을 **Name** 필드에 입력합니다.

3단계 Syslog 서버의 호스트 이름또는 IP주소를 **Host** 필드에입력합니다.

이 필드에 잘못된 IPv4 주소(예: 192.168.1.456)를 입력해도 시스템에서 경고를 표시하지 **않습니다**. 대신, 잘못된 주소는 호스트 이름으로 처리됩니다.

4단계 서버가 syslog 메시지에 사용할 포트를 **Port** 필드에 입력합니다.

기본적으로 이 값은 514입니다.

5단계 **Facility** 목록에서 기능을 선택합니다.

사용 가능한 기능 목록은 사용 가능한 Syslog 기능 표를 참조하십시오.

6단계 **Severity** 목록에서 심각도를 선택합니다.

사용 가능한 심각도 목록은 Syslog 심각도 표를 참조하십시오.

7단계 Syslog 메시지에 표시할 태그 이름을 **Tag** 필드에 입력합니다.

태그 이름에는 영숫자 문자만 사용해야 합니다. 공백이나 밑줄은 사용할 수 **없습니다**.

예를 들어, syslog로 전송되는 모든 메시지 앞에 `FromDC`가 오도록 하려면 필드에 `FromDC`를 입력합니다.

8단계 **Save**를 클릭합니다.

알림 응답이 저장되고 자동으로 활성화됩니다.

알림 응답 수정

라이센스: 모두

대부분의 알림 유형에서, 알림 응답이 활성화되었고 사용 중인 경우 알림 응답에 대한 변경 사항은 즉시 반영됩니다. 그러나 연결 이벤트 기록을 위해 액세스 제어 규칙에서 사용되는 알림 응답의 경우, 액세스 제어 정책을 다시 적용하기까지 변경 사항이 반영되지 않습니다.

알림 응답을 수정하려면

액세스: Admin

1단계 **Policies > Actions > Alerts**를 선택합니다.

Alerts 페이지가 나타납니다.

2단계 수정하려는 알림 응답 옆에 있는 수정 아이콘( )을 클릭합니다.

해당 알림 응답에 대한 컨피그레이션 팝업 창이 나타납니다.

3단계 필요에 따라 변경합니다.

4단계 **Save**를 클릭합니다.

알림 응답이 저장됩니다.

알림 응답 삭제

라이센스: 모두

사용하지 않는 알림 응답을 삭제할 수 있습니다.

알림 응답을 삭제하려면

액세스: Admin

1단계 **Policies > Actions > Alerts**를 선택합니다.

Alerts 페이지가 나타납니다.

2단계 삭제하려는 알림 응답 옆에 있는 수정 아이콘( )을 클릭합니다.

3단계 알림 응답을 삭제할 것임을 확인합니다.

알림 응답이 삭제됩니다.

알림 응답 활성화 및 비활성화

라이센스: 모두

활성화된 알림 응답만이 알림을 생성할 수 있습니다. 알림의 생성을 중지하려면 컨피그레이션을 삭제하기보다 알림 응답을 일시적으로 비활성화할 수 있습니다. 알림이 사용 중일 때 비활성화하면, 비활성화된 후에도 여전히 사용 중인 것으로 간주됩니다.

알림 응답을 활성화 또는 비활성화하려면

액세스: Admin

1단계 **Policies > Actions > Alerts**를 선택합니다.

Alerts 페이지가 나타납니다.

2단계 활성화 또는 비활성화할 알림 응답 옆에 있는 활성화/비활성화 슬라이더를 클릭합니다.

알림 응답이 활성화되었던 경우에는 비활성화되고, 비활성화되었던 경우에는 활성화됩니다.

영향 플래그 알림 구성

라이센스: 보호

특정 영향 플래그의 침입 이벤트가 발생할 때마다 알림을 전송하도록 시스템을 구성할 수 있습니다. 영향 플래그는 침입 데이터, 네트워크 검색 데이터 및 취약성 정보를 상호 연결하여, 침입이 네트워크에 미치는 영향을 평가하는 데 도움이 됩니다. 자세한 내용은 41-38페이지의 이벤트를 평가하기 위한 영향 레벨 사용을/를 참조하십시오.

영향 플래그 알림을 구성하려면

액세스: Admin

1단계 **Policies > Actions > Alerts**를 선택한 다음 **Impact Flag Alerts** 탭을 선택합니다.

Impact Flag Alerts 페이지가 나타납니다.

2단계 Alerts 섹션에서 각 알림 유형에 사용할 알림 응답을 선택합니다.

새 알림 응답을 생성하려면 드롭다운 목록에서 **New**를 선택합니다. 자세한 내용은 43-2페이지의 알림 응답 작업을/를 참조하십시오.

3단계 Impact Configuration 섹션에서 각 영향 플래그에 대해 수신하고자 하는 알림에 해당하는 확인란을 선택합니다.

4단계 **Save**를 클릭합니다.

영향 플래그 알림 설정이 저장됩니다.

검색 이벤트 알림 구성

라이센스: FireSIGHT

특정 유형의 검색 이벤트가 발생할 때마다 알리도록 시스템을 구성할 수 있습니다. 서로 다른 이벤트 유형에 대한 자세한 내용은 50-9페이지의 검색 이벤트 유형 이해 및 50-13페이지의 호스트 입력 이벤트 유형 이해을/를 참조하십시오.

검색 이벤트 유형을 기반으로 알림을 생성하려면 해당 이벤트 유형을 기록하도록 네트워크 검색 정책을 구성해야 합니다. 45-37페이지의 검색 이벤트 로깅 구성을/를 참조하십시오. 기본적으로 로깅은 모든 이벤트 유형에 대해 활성화됩니다.

검색 이벤트 알림을 구성하려면

액세스: Admin

1단계 **Policies > Actions > Alerts**를 선택한 다음 **Discovery Event Alerts** 탭을 선택합니다.

Discovery Event Alerts 페이지가 나타납니다.

2단계 **Alerts** 섹션에서 각 알림 유형에 사용할 알림 응답을 선택합니다.

새 알림 응답을 생성하려면 드롭다운 목록에서 **New**를 선택합니다. 자세한 내용은 43-2페이지의 알림 응답 작업을/를 참조하십시오.

3단계 **Events Configuration** 섹션에서 각 검색 이벤트 유형에 대해 수신하고자 하는 알림에 해당하는 확인란을 선택합니다.

4단계 **Save**를 클릭합니다.

검색 이벤트 알림 설정이 저장됩니다.

AMP 알림 구성

라이센스: 악성코드

지원되는 디바이스: Series 3 또는 가상

지원되는 Defense Center: DC500을 제외한 모두

소급 이벤트를 비롯한 네트워크 기반 악성코드 이벤트가 생성될 때마다 알림을 보내도록 시스템을 구성할 수 있습니다. 그러나 엔드포인트 기반(FireAMP) 악성코드 이벤트에 대해서는 알림을 보낼 수 없습니다. 악성코드 이벤트에 대한 자세한 내용은 40-17페이지의 악성코드 이벤트 작업을/를 참조하십시오.

악성코드 이벤트를 기반으로 알림을 생성하려면 악성코드 클라우드 조회를 수행하는 파일 정책을 생성한 다음, 해당 정책을 액세스 제어 규칙과 연결해야 합니다. 자세한 내용은 18-1페이지의 침입 정책 및 파일 정책을 사용하여 트래픽 제어을/를 참조하십시오.

악성코드 이벤트 알림을 구성하려면

액세스: Admin

1단계 **Policies > Actions > Alerts**를 선택한 다음 **Advanced Malware Protections Alerts** 탭을 선택합니다.

Advanced Malware Protection Alerts 페이지가 나타납니다.

2단계 **Alerts** 섹션에서 각 알림 유형에 사용할 알림 응답을 선택합니다.

새 알림 응답을 생성하려면 드롭다운 목록에서 **New**를 선택합니다. 자세한 내용은 43-2페이지의 알림 응답 작업을/를 참조하십시오.

3단계 **Event Configuration** 섹션에서 각 악성코드 이벤트 유형에 대해 수신하고자 하는 알림에 해당하는 확인란을 선택합니다.

All network-based malware events에는 **Retrospective Events**가 포함된다는 점에 유의해야 합니다.

4단계 **Save**를 클릭합니다.

악성코드 이벤트 알림 설정이 저장됩니다.

44장 침입 규칙에 대한 외부 알림 구성

FireSIGHT 시스템에서는 웹 인터페이스 내 다양한 침입 이벤트 보기를 제공하지만, 일부 기업은 중요한 시스템을 지속적으로 모니터링할 수 있도록 외부 침입 이벤트 알림을 직접 정의하는 방식을 선호합니다. 중요한 이벤트를 특정 담당자에게 즉시 알리려면 이를 위한 이메일 알림을 설정할 수 있습니다. 또는 syslog에 대한 로깅 기능을 활성화하거나 이벤트 데이터를 SNMP 트랩 서버로 전송할 수 있습니다.

각 침입 정책 내에서 침입 이벤트 알림 제한을 지정하고, 외부 로깅 장소에 대한 침입 이벤트 알림을 설정하고, 침입 이벤트에 대한 외부 응답을 구성할 수 있습니다.

팁 일부 분석가는 동일한 침입 이벤트에 대해 여러 알림을 수신하는 것보다 특정 침입 이벤트 발생에 대한 알림의 횟수를 제어하는 방식을 더 좋아합니다. 자세한 내용은 32-22페이지의 정책당 침입 이벤트 알림 필터링을/를 참조하십시오.

침입 정책 외부, FireSIGHT 시스템에서 수행할 수 있는 또 다른 알림 유형이 있습니다. 특정 영향 플래그가 있는 침입 이벤트 또는 특정 액세스 제어 규칙에 의해 로깅된 연결 이벤트 등 다른 이벤트 유형에 대해 이메일, SNMP 및 syslog 알림 응답을 구성할 수 있습니다. 자세한 내용은 43-1페이지의 외부 알림 구성을/를 참조하십시오.

외부 침입 이벤트 알림에 대한 자세한 내용은 다음 절을 참조하십시오.

- 44-1페이지의 SNMP 응답 사용 - 이벤트 데이터를 지정된 SNMP 트랩 서버로 전송하도록 구성할 수 있는 옵션에 대해 설명하고, SNMP 알림 옵션을 지정하기 위한 절차를 제공합니다.
- 44-4페이지의 Syslog 응답 사용 - 이벤트 데이터를 외부 syslog로 전송하도록 구성할 수 있는 옵션에 대해 설명하고, syslog 알림 옵션을 지정하기 위한 절차를 제공합니다.
- 44-7페이지의 이메일 알림 이해 - 침입 이벤트의 알림을 이메일로 전송하도록 구성할 수 있는 옵션에 대해 설명합니다.

SNMP 응답 사용

라이센스: 보호

*SNMP 트랩*은 네트워크 관리 알림입니다. 침입 이벤트 알림을 SNMP 트랩(*SNMP 알림*이라고도 함)으로 전송하도록 디바이스를 구성할 수 있습니다. 각 SNMP 알림에는 다음이 포함되어 있습니다.

- 트랩을 생성하는 서버의 이름
- 알림을 탐지한 디바이스의 IP 주소
- 알림을 탐지한 디바이스의 이름
- 이벤트 데이터

다양한 SNMP 알림 매개 변수를 설정할 수 있습니다. 사용 가능한 매개 변수는 SNMP 버전에 따라 다릅니다. SNMP 알림의 활성화 및 비활성화에 대한 자세한 내용은 31-7페이지의 침입 정책에서 고급 설정 구성을/를 참조하십시오.

팁 네트워크 관리 시스템에 방어 센터의 MIB(Management Information Base) 파일이 필요한 경우 `/etc/sf/DCEALERT.MIB`에서 가져올 수 있습니다.

SNMP v2 옵션

SNMP v2의 경우 다음 표에 설명된 옵션을 지정할 수 있습니다.

표 44-1 SNMP v2 옵션

옵션	설명
Trap Type	알림에 나타나는 IP 주소에 사용할 트랩 유형. 네트워크 관리 시스템이 INET_IPV4 주소 유형을 올바르게 표현하는 경우 **as Binary**를 선택할 수 있습니다. 그렇지 않으면 **as String**을 선택합니다. 예를 들면 HP Openview에는 문자열 유형이 필요합니다.
Trap Server	SNMP 트랩 알림을 수신할 서버. 단일 IP 주소 또는 호스트 이름을 지정할 수 있습니다.
Community String	커뮤니티 이름.

SNMP v3 옵션

SNMP v3의 경우 다음 표에 설명된 옵션을 지정할 수 있습니다.

참고 SNMP v3을 사용하는 경우 어플라이언스에서는 메시지 암호화에 Engine ID 값을 사용합니다. SNMP 서버에서 메시지를 암호 해독하려면 이 값이 필요합니다. 현재 이 Engine ID 값은 항상 문자열이 `01`로 끝나는 어플라이언스 IP 주소의 16진수 버전이 됩니다. 예를 들어 SNMP 알림을 전송하는 어플라이언스의 IP 주소가 `172.16.1.50`이면 Engine ID는 `0xAC10013201`이며, 어플라이언스의 IP 주소가 `10.1.1.77`이면 `0x0a01014D01`이 Engine ID로 사용됩니다.

표 44-2 SNMP v3 옵션

옵션	설명
Trap Type	알림에 나타나는 IP 주소에 사용할 트랩 유형. 네트워크 관리 시스템이 INET_IPV4 주소 유형을 올바르게 표현하는 경우 **as Binary**를 선택할 수 있습니다. 그렇지 않으면 **as String**을 선택합니다. 예를 들면 HP Openview에는 문자열 유형이 필요합니다.
Trap Server	SNMP 트랩 알림을 수신할 서버. 단일 IP 주소 또는 호스트 이름을 지정할 수 있습니다.
Authentication Password	인증에 필요한 비밀번호. SNMP v3은 컨피그레이션에 따라 MD5(Message Digest 5) 해시 함수 또는 SHA(Secure Hash Algorithm) 해시 함수를 사용하여 이 비밀번호를 암호화합니다. 인증 암호를 지정하면 인증이 활성화됩니다.

표 44-2 SNMP v3 옵션(계속)

옵션	설명
Private Password	프라이버시를 위한 SNMP. SNMP v3은 DES(Data Encryption Standard) 블록 암호를 사용하여 이 비밀번호를 암호화합니다. 비공개 비밀번호를 지정하면 프라이버시가 활성화됩니다. 개인 비밀번호를 지정하는 경우 인증 비밀번호도 지정해야 합니다.
User Name	SNMP 사용자 이름.

SNMP 알림 구성에 대한 자세한 내용은 44-3페이지의 SNMP 응답 구성을/를 참조하십시오.

SNMP 응답 구성

라이센스: 보호

침입 정책에서 SNMP 알림을 구성할 수 있습니다. 액세스 제어 정책의 일부로서 정책을 적용하면 시스템은 SNMP 트랩을 통해 탐지하는 침입 이벤트를 사용자에게 알립니다. SNMP 알림에 대한 자세한 내용은 44-1페이지의 SNMP 응답 사용을/를 참조하십시오.

SNMP 알림 옵션을 구성하려면

액세스: Admin/Intrusion Admin

1단계 **Policies > Intrusion > Intrusion Policy**를 선택합니다.

Intrusion Policy 페이지가 나타납니다.

2단계 수정할 정책 옆에 있는 수정 아이콘( )을 클릭합니다.

다른 정책에 저장하지 않은 변경 사항이 있는 경우 변경 사항을 취소하고 계속 진행하려면 **OK**를 클릭합니다. 저장하지 않은 변경 사항을 다른 정책에 저장하는 방법에 대한 자세한 내용은 23-15페이지의 충돌 해결 및 정책 변경 사항 커밋을/를 참조하십시오.

Policy Information 페이지가 나타납니다.

3단계 왼쪽의 탐색 패널에서 **Advanced Settings**를 클릭합니다.

Advanced Settings 페이지가 나타납니다.

4단계 External Responses 아래에서 **SNMP Alerting**이 활성화되었는지 여부에 따라 두 가지 선택 사항이 있습니다.

- 컨피그레이션이 활성화되어 있으면 **Edit**를 클릭합니다.
- 컨피그레이션이 비활성화되어 있으면 **Enabled**를 클릭한 다음 **Edit**를 클릭합니다.

SNMP Alerting 페이지가 나타납니다.

페이지 하단에 있는 메시지는 컨피그레이션이 포함된 침입 정책 레이어를 식별합니다. 자세한 내용은 24-1페이지의 네트워크 분석 또는 침입 정책에서 레이어 사용을/를 참조하십시오.

5단계 알림에 나타나는 IP 주소에 사용할 트랩 유형 형식을 **as Binary** 또는 **as String**으로 지정합니다.

참고 네트워크 관리 시스템이 INET_IPV4 주소 유형을 올바르게 표현하는 경우 **as Binary**를 사용할 수 있습니다. 그렇지 않으면 **as String** 옵션을 사용합니다. 예를 들면 HP OpenView에는 **as String** 옵션이 필요합니다.

6단계 SNMP v2 또는 SNMP v3을 선택합니다.

- SNMP v2를 구성하려면 사용할 트랩 서버의 IP 주소와 커뮤니티 이름을 해당 필드에 입력합니다. 44-2페이지의 SNMP v2 옵션을/를 참조하십시오.
- SNMP v3을 구성하려면 사용할 트랩 서버의 IP 주소, 인증 비밀번호, 개인 비밀번호 및 사용자 이름을 해당 필드에 입력합니다. 자세한 내용은 44-2페이지의 SNMP v3 옵션을/를 참조하십시오.

참고 SNMP v2 **또는** SNMP v3을 선택해야 합니다.

참고 SNMP v3 비밀번호를 입력하면, 초기 컨피그레이션에서는 일반 텍스트로 표시되지만 저장 시 암호화된 형식으로 바뀝니다.

7단계 정책을 저장하거나, 계속 수정하거나, 변경 사항을 취소하거나, 기반 정책의 기본 컨피그레이션 설정으로 돌아가거나, 시스템 캐시에 변경 사항이 남아 있는 상태로 종료합니다. 자세한 내용은 23-15 페이지의 충돌 해결 및 정책 변경 사항 커밋을/를 참조하십시오.

Syslog 응답 사용

라이센스: 보호

시스템 로그(*syslog*)는 네트워크 이벤트 로깅을 위한 표준 로깅 메커니즘입니다. 침입 이벤트 알림인 *syslog 알림*을 어플라이언스의 syslog로 전송할 수 있습니다. Syslog에서는 우선순위와 기능별로 정보를 카테고리화할 수 있습니다. *우선순위(priority)*는 알림의 심각도를 반영하고 *기능(facility)*은 알림을 생성한 하위 시스템을 나타냅니다. 기능과 우선순위는 syslog에 나타나는 실제 메시지에는 표시되지 않지만, syslog 메시지를 수신하는 시스템에 카테고리화 방법을 알려주는 데 사용됩니다.

Syslog 알림에는 다음 정보가 포함됩니다.

- 알림 생성 날짜 및 시간
- 이벤트 메시지
- 이벤트 데이터
- 트리거링 이벤트의 generator ID
- 트리거링 이벤트의 Snort ID
- 개정

침입 정책에서 syslog 알림을 설정하고, syslog의 침입 이벤트 알림과 관련된 syslog 우선순위 및 기능을 지정할 수 있습니다. 액세스 제어 정책의 일부로 침입 이벤트를 적용하면 시스템은 탐지하는 침입 이벤트에 대한 syslog 알림을 로컬 호스트 또는 정책에 지정된 로깅 호스트의 syslog 기능으로 전송합니다. 알림을 받은 호스트는 알림을 카테고리화하기 위해 syslog 알림을 구성할 때 사용자가 설정한 기능 및 우선순위 정보를 사용합니다.

다음 표에는 syslog 알림을 구성할 때 선택할 수 있는 기능이 나열되어 있습니다. 사용하는 원격 syslog 서버의 컨피그레이션을 기반으로 합리적인 기능을 구성해야 합니다. 원격 시스템에 있는 `syslog.conf` 파일(syslog 메시지를 UNIX 또는 Linux 기반 시스템에 로깅하는 경우)은 어떤 기능이 서버의 어떤 로그 파일에 저장되는지를 나타냅니다.

표 44-3 사용 가능한 Syslog 기능

설비	설명
AUTH	보안 및 인증과 관련된 메시지
AUTHPRIV	보안 및 인증과 관련된 제한적인 액세스 메시지. 많은 시스템에서 이러한 메시지는 보안 파일로 전달됩니다
CRON	클록 디먼에 의해 생성된 메시지
DAEMON	시스템 디먼에 의해 생성된 메시지
FTP	FTP 디먼에 의해 생성된 메시지
KERN	커널에 의해 생성된 메시지. 많은 시스템에서 이러한 메시지는 콘솔에 인쇄되어 나타납니다
LOCAL0-LOCAL7	내부 프로세스에 의해 생성된 메시지
LPR	인쇄 하위 시스템에 의해 생성된 메시지
MAIL	메일 시스템에 의해 생성된 메시지
NEWS	네트워크 뉴스 하위 시스템에 의해 생성된 메시지
SYSLOG	Syslog 디먼에 의해 생성된 메시지
USER	사용자 레벨 프로세스에 의해 생성된 메시지
UUCP	UUCP 하위 시스템에 의해 생성된 메시지

생성되는 모든 알림에 대해 표시할 표준 syslog 우선순위 레벨을 다음 중에서 선택하십시오.

표 44-4 Syslog 우선순위 레벨

수준	설명
EMERG	모든 사용자에게 위험 상태 알림
ALERT	즉시 해결해야 하는 상태
CRIT	심각한 상태
ERR	오류 상태
WARNING	경고 메시지
NOTICE	오류 상태는 아니지만 주의가 필요한 상태
INFO	정보 메시지
DEBUG	디버그 정보가 포함된 메시지

Syslog 작동 방식 및 구성 방법에 대한 자세한 내용은 시스템과 함께 제공된 설명서를 참조하십시오. UNIX 또는 Linux 기반 시스템의 syslog에 로깅하는 경우 `syslog.conf` man 파일(명령줄에서 `man syslog.conf` 입력) 및 syslog man 파일(명령줄에서 `man syslog` 입력)은 syslog의 작동 방식 및 구성 방법에 대한 정보를 제공합니다.

Syslog 응답 구성

라이센스: 보호

침입 정책에서 Syslog 알림을 구성할 수 있습니다. 액세스 제어 정책의 일부로서 정책을 적용하면 시스템은 Syslog를 통해 탐지하는 침입 이벤트를 사용자에게 알립니다. Syslog 알림에 대한 자세한 내용은 44-4페이지의 Syslog 응답 사용을/를 참조하십시오.

Syslog 알림 옵션을 구성하려면

액세스: Admin/Intrusion Admin

1단계 **Policies > Intrusion > Intrusion Policy**를 선택합니다.

Intrusion Policy 페이지가 나타납니다.

2단계 수정할 정책 옆에 있는 수정 아이콘( )을 클릭합니다.

다른 정책에 저장하지 않은 변경 사항이 있는 경우 변경 사항을 취소하고 계속 진행하려면 **OK**를 클릭합니다. 저장하지 않은 변경 사항을 다른 정책에 저장하는 방법에 대한 자세한 내용은 23-15페이지의 충돌 해결 및 정책 변경 사항 커밋을/를 참조하십시오.

Policy Information 페이지가 나타납니다.

3단계 왼쪽의 탐색 패널에서 **Advanced Settings**를 클릭합니다.

Advanced Settings 페이지가 나타납니다.

4단계 External Responses 아래에서 **Syslog Alerting**이 활성화되었는지 여부에 따라 두 가지 선택 사항이 있습니다.

- 컨피그레이션이 활성화되어 있으면 **Edit**를 클릭합니다.
- 컨피그레이션이 비활성화되어 있으면 **Enabled**를 클릭한 다음 **Edit**를 클릭합니다.

Syslog Alerting 페이지가 나타납니다.

페이지 하단에 있는 메시지는 컨피그레이션이 포함된 침입 정책 레이어를 식별합니다. 자세한 내용은 24-1페이지의 네트워크 분석 또는 침입 정책에서 레이어 사용을/를 참조하십시오.

5단계 선택적으로, 로깅 호스트로서 지정할 원격 액세스 IP 주소를 **Logging Hosts** 필드에 입력합니다. 호스트가 여러 개인 경우 쉼표로 구분하십시오.

6단계 드롭다운 목록에서 기능 및 우선순위 레벨을 선택합니다.

기능 및 우선순위 옵션에 대한 자세한 내용은 44-4페이지의 Syslog 응답 사용을/를 참조하십시오.

7단계 정책을 저장하거나, 계속 수정하거나, 변경 사항을 취소하거나, 기반 정책의 기본 컨피그레이션 설정으로 돌아가거나, 시스템 캐시에 변경 사항이 남아 있는 상태로 종료합니다. 자세한 내용은 23-15페이지의 충돌 해결 및 정책 변경 사항 커밋을/를 참조하십시오.

이메일 알림 이해

라이센스: 보호

*이메일 알림*이란 이메일로 침입 이벤트를 알리는 것입니다. 이메일 알림에는 다음 정보가 포함됩니다.

- 데이터베이스에 있는 총 알림 수
- 마지막 이메일 시간(시스템이 마지막 이메일 보고서를 생성한 시간)
- 현재 시간(시스템이 현재 이메일 보고서를 생성한 시간)
- 새로운 알림 총수
- 지정된 이메일 필터와 일치하는 이벤트 수(이벤트가 특정 규칙에 대해 구성된 경우)
- 각 이벤트에 대한(Summary Output이 해제된 경우) 타임스탬프, 프로토콜, 이벤트 메시지 및 세션 정보(트래픽 방향과 함께 소스 및 목적지 IP와 포트)

참고 여러 침입 이벤트가 동일한 소스 IP에서 오는 경우 추가 이벤트의 수를 표시하는 메모가 이벤트 아래에 나타납니다.

- 목적지 포트당 이벤트 수
- 소스 IP당 이벤트 수

각 규칙 또는 규칙 그룹에서 침입 이벤트에 대한 이메일 알림을 활성화 또는 비활성화할 수 있습니다. 액세스 제어 정책의 일부로서 어떤 침입 정책을 디바이스에 적용하는지와 상관없이 이메일 알림 설정이 사용됩니다.

다음은 이메일 알림에 대해 설정할 수 있는 매개 변수를 설명하는 목록입니다.

On/Off

이메일 알림을 활성화 또는 비활성화합니다.

From Address

시스템이 침입 이벤트를 전송하는 소스 이메일 주소를 지정합니다.

To Address

시스템이 침입 이벤트를 전송하는 대상 이메일 주소를 지정합니다. 여러 수신자에게 이메일을 전송하려면 이메일 주소를 쉼표로 구분합니다. 예를 들면 다음과 같습니다.

```
user1@example.com, user2@example.com
```

Max Alerts

Frequency (seconds)로 지정한 기간에 시스템이 이메일을 통해 전송하는 최대 침입 이벤트 수를 지정합니다.

Frequency (seconds)

시스템이 침입 이벤트를 전송하는 빈도를 지정합니다. Frequency 설정은 또한 이메일 설정이 저장되는 빈도도 지정합니다.

최소 빈도: 300초
최대 빈도: 40억 초

Coalesce Alerts

동일한 소스 IP에 대해 생성된 여러 동일한 침입 이벤트가 페이지에서 하나의 이벤트로만 표시되도록 소스 IP 및 이벤트에 의한 침입 이벤트의 그룹화를 활성화 또는 비활성화합니다.

알림 합체(그룹화)는 이벤트가 필터링된 후 발생합니다. 따라서 특정 규칙에 대해 이메일 알림을 구성하면 Mail Alerting Configuration에서 지정한 규칙과 일치하는 이벤트 목록만 수신하게 됩니다.

Summary Output

호출기 같이 텍스트가 제한된 디바이스에 적합한 간단한 이메일 알림을 활성화 또는 비활성화합니다. 간단한 이메일 알림에는 다음이 포함됩니다.

- 이벤트 타임스탬프
- 방어 센터의 경우 이벤트를 생성한 디바이스의 IP 주소
- 이벤트 프로토콜
- 소스 IP 및 포트
- 목적지 IP 및 포트
- 이벤트 메시지
- 동일한 소스 IP에 대해 생성되는 침입 이벤트의 수

예를 들면 다음과 같습니다.

```
2011-05-18 10:35:10 10.1.1.100 icmp 10.10.10.1:8 -> 10.2.1.3:0
snort_decoder: Unknown Datagram decoding problem! (116:108)
```

Email Alerting on Specific Rules Configuration

지정한 이메일 주소로 이벤트를 전송하고자 하는 규칙 또는 규칙 그룹을 지정합니다.

이메일 알림 구성에 대한 자세한 내용은 44-8페이지의 이메일 알림 구성을/를 참조하십시오.

이메일 알림 구성

라이센스: 보호

특정 규칙 또는 규칙 그룹에 대해 침입 이벤트가 발생할 때마다 어플라이언스에서 알려주도록 이메일 알림을 구성할 수 있습니다.

이메일 알림을 받으려면 먼저 다음이 **필요합니다**.

- 이메일 알림을 받을 메일 호스트 구성(63-18페이지의 메일 릴레이 호스트 및 알림 주소 구성 참조)
- 관리되는 디바이스와 방어 센터가 모두 자체 IP 주소를 역으로 확인할 수 있어야 함

이메일 알림 옵션을 구성하려면

액세스: Admin/Intrusion Admin

1단계 **Policies > Intrusion > Email**을 선택합니다.

Email Alerting 페이지가 나타납니다.

2단계 **State** 옆에서 **on**을 선택하여 이메일 알림을 활성화합니다.

3단계 이메일 알림의 From 필드에 표시할 주소를 **From Address** 필드에 입력합니다.

4단계 이메일 알림을 수신할 주소를 **To Address** 필드에 입력합니다.

5단계 단일 이메일에 포함할 최대 이벤트 수를 **Max Alerts** 필드에 입력합니다.

6단계 이메일 알림을 받을 최소 빈도의 기간(초)을 **Min Frequency** 필드에 입력합니다.

7단계 이벤트를 IP 주소별로 그룹화하려면 **Coalesce Alerts** 옆에서 **on**을 선택합니다.

8단계 간단한 이메일 알림을 전송하려면 **Summary Output** 옆에서 **on**을 선택합니다.

팁 **Summary Output**을 활성화할 경우 생성되는 알림 수를 줄이려면 **Coalesce Alerts**를 활성화할 수 있습니다. 또한 디바이스 문자 메시지 버퍼의 오버플로를 피하려면 **Max Alerts**를 1로 설정할 수 있습니다.

9단계 **Time Zone** 필드의 드롭다운 목록에서 표준 시간대를 선택합니다.

10단계 규칙당 이메일 알림을 활성화하려면 **Email Alerting per Rule Configuration**을 클릭합니다.

규칙 그룹이 나타납니다.

팁 모든 카테고리의 모든 규칙에 대해 이메일 알림을 수신하려면 **Select All**을 선택합니다.

11단계 다음 중 하나 또는 둘 다를 수행합니다.

- 카테고리에 속하는 모든 규칙에 대해 이메일 알림을 수신하려면 규칙 카테고리 옆에 있는 **All**을 클릭합니다.
- 카테고리의 개별 규칙에 대한 이메일 알림을 지정할 해당 카테고리 폴더를 클릭한 다음, 이메일 알림을 수신할 규칙을 활성화합니다.

12단계 **Save**를 클릭합니다.

이메일 알림 컨피그레이션이 저장됩니다. 해당 침입 이벤트가 발생하면 이메일 알림이 전송됩니다.

45장

네트워크 검색 소개

FireSIGHT 시스템에서는 *네트워크 검색*이라는 기능을 사용하여 네트워크의 트래픽을 미러링하고 네트워크 자산의 포괄적인 맵을 작성합니다.

시스템은 지정된 네트워크 세그먼트에서 관리되는 디바이스가 트래픽을 수동적으로 관찰할 때 특정 패킷 헤더 값과 기타 네트워크 트래픽의 고유한 데이터를 설정된 정의(*핑거프린트*라고 함)와 비교하여, 네트워크에 있는 호스트(네트워크 디바이스 포함)의 수와 유형은 물론 이러한 호스트의 운영 체제, 활성 애플리케이션 및 열린 포트도 확인합니다.

또한 FireSIGHT 시스템가 관리하는 디바이스를 구성하여 네트워크의 사용자 활동을 모니터링하면 정책 위반, 공격 또는 네트워크 취약성을 식별할 수 있습니다.

시스템에 의해 수집된 데이터를 보완하려면 NetFlow 지원 디바이스, Nmap 활성 스캔, 호스트 입력 기능, 그리고 Microsoft Active Directory 서버에 상주하며 LDAP 인증을 보고하는 User Agents에 의해 생성된 레코드를 가져올 수 있습니다. FireSIGHT 시스템은 이러한 레코드를 관리되는 디바이스에 의한 직접 네트워크 트래픽 관찰을 통해 수집한 정보와 통합합니다.

네트워크의 호스트에서 발생하는 특정 유형의 침입, 악성코드 및 기타 이벤트를 서로 연결하여 호스트의 보안이 침해될 가능성이 있는 경우를 확인하고, 이러한 호스트에 IOC(*indications of compromise*) 태그를 추가할 수 있습니다. IOC 데이터는 모니터링되는 네트워크의 위협(호스트와 관련될 때)에 대한 분명하고 직접적인 상황을 시각적으로 제공할 수 있습니다.

시스템에서는 이러한 모든 정보를 사용하여 포렌식 분석, 동작 프로파일링, 액세스 제어, 조직에 영향을 줄 수 있는 취약점과 익스플로잇의 완화 및 대응을 지원합니다.

자세한 내용은 다음 링크를 참고하십시오.

- 45-1페이지의 검색 데이터 수집 이해
- 45-16페이지의 NetFlow 이해
- 45-20페이지의 IOC 이해
- 45-23페이지의 네트워크 검색 정책 생성

검색 데이터 수집 이해

라이센스: FireSIGHT

검색 데이터에는 네트워크의 호스트와 운영 체제, 활성 애플리케이션, 호스트에서의 사용자 활동 등에 대한 정보가 포함됩니다.

검색 데이터 수집을 시작하려면 먼저 액세스 제어 정책을 적용해야 합니다. 액세스 제어 정책은 사용자가 허용하는 트래픽, 즉 네트워크 검색으로 모니터링할 수 있는 트래픽을 정의합니다. 따라서 액세스 제어를 사용하여 특정 트래픽을 차단하면 시스템은 해당 트래픽에서 호스트, 사용자 또는 애플리케이션 활동을 검토할 수 없습니다. 예를 들어, 소셜 네트워킹 애플리케이션에 대한 액세스를 차단하면 시스템은 소셜 네트워크 애플리케이션에 대한 검색 데이터를 제공하지 않습니다.

액세스 제어 정책을 적용한 후에는 관리되는 디바이스로 모니터링할 네트워크 세그먼트와 포트 그리고 수집할 데이터 종류를 지정하는 네트워크 검색 정책을 구성하고 적용해야 합니다. 네트워크 검색 정책을 적용하면 시스템에서는 검색 데이터 생성을 시작합니다. 그러면 방어 센터 웹 인터페이스를 사용하여 데이터를 보고 분석할 수 있습니다.

시스템은 네트워크 검색 데이터를 방어 센터 데이터베이스에 저장합니다. 스토리지 제한에 대한 자세한 내용은 63-15페이지의 데이터베이스 이벤트 제한 구성을/를 참조하십시오. 데이터베이스 제한 외에도, 방어 센터가 저장할 수 있는 탐지된 총 호스트 및 사용자 수는 FireSIGHT 라이센스에 따라 달라질 수 있습니다.

시스템은 라이센스 사용자 제한에 도달하면 대부분의 경우 데이터베이스에 대한 새 사용자 추가를 중지합니다. 새 사용자를 추가하려면 데이터베이스에서 오래된 사용자 또는 비활성 사용자를 수동으로 삭제하거나 모든 사용자를 삭제해야 합니다. 한편, 라이센스 호스트 제한에 도달할 경우 시스템에서 데이터베이스에 새 호스트 추가를 중지하도록 하거나 가장 오랫동안 비활성 상태를 유지해온 호스트를 대체하도록 구성할 수 있습니다.

시스템에 의해 수집된 데이터를 보완하려면 NetFlow 지원 디바이스, Nmap 활성 스캔, 호스트 입력 기능, 그리고 Microsoft Active Directory 서버에 상주하며 LDAP 인증을 보고하는 User Agents에 의해 생성된 레코드를 가져올 수 있습니다. FireSIGHT 시스템은 이러한 레코드를 관리되는 디바이스에 의한 직접 네트워크 트래픽 관찰을 통해 수집한 정보와 통합합니다.

자세한 내용은 다음 링크를 참고하십시오.

- 45-2페이지의 호스트 데이터 수집 이해
- 45-3페이지의 사용자 데이터 수집 이해
- 45-10페이지의 애플리케이션 탐지 이해
- 45-20페이지의 IOC 이해
- 45-15페이지의 서드파티 검색 데이터 가져오기
- 45-16페이지의 검색 데이터 용도

호스트 데이터 수집 이해

라이센스: FireSIGHT

시스템에서는 네트워크를 이동하는 트래픽을 수동으로 모니터링할 때 특정 패킷 헤더 값과 기타 네트워크 트래픽의 고유한 데이터를 설정된 정의(*핑거프린트*라고 함)와 비교하여 네트워크의 호스트에 대한 다음과 같은 정보를 확인합니다.

- 호스트의 수 및 유형(브리지, 라우터, 로드 밸런서 및 NAT 디바이스 등의 네트워크 디바이스 포함)
- 네트워크의 검색 지점에서 호스트로의 홉(hop) 수를 비롯한 기본 네트워크 토폴로지 데이터
- 호스트에서 실행 중인 운영 체제
- 호스트의 애플리케이션 및 이러한 애플리케이션과 연결된 사용자

시스템이 호스트의 운영 체제를 식별할 수 없는 경우, 사용자 지정 핑거프린트 기능을 사용하여 사용자 지정 클라이언트 또는 서버 핑거프린트를 생성할 수 있습니다. 시스템은 이러한 핑거프린트를 사용하여 새 호스트를 식별합니다. 핑거프린트를 VDB(취약성 데이터베이스)의 시스템에 매핑하면 사용자 지정 핑거프린트를 사용하여 호스트가 식별될 때마다 적절한 취약성 정보를 표시할

수 있습니다. 자세한 내용은 46-7페이지의 사용자 지정 핑거프린트 사용을/를 참조하십시오.

호스트 입력 기능을 통해 호스트 및 운영 체제 데이터를 추가 또는 업데이트할 수도 있습니다. 또한 호스트 탐지를 활성화하여 NetFlow 지원 검색 규칙을 생성하면 NetFlow 데이터로부터 호스트를 네트워크 맵에 추가할 수 있습니다.

시스템에서 탐지한 호스트를 보려면 방어 센터 웹 인터페이스를 사용할 수 있습니다.

- 이벤트 뷰어를 사용하여 호스트를 보고 검색하는 방법에 대한 자세한 내용은 50-19페이지의 호스트 작업을/를 참조하십시오.
- 네트워크 자산 및 토폴로지를 자세히 보여주는 네트워크 맵 보기에 대한 자세한 내용은 48-1페이지의 네트워크 맵 사용을/를 참조하십시오.
- 탐지된 호스트에 사용할 수 있는 모든 정보를 완전하게 보여주는 호스트 프로필 보기에 대한 자세한 내용은 49-1페이지의 호스트 프로필 사용을/를 참조하십시오.

사용자 데이터 수집 이해

라이센스: FireSIGHT

네트워크에서 사용자 활동을 모니터링하는 데에는 위협, 엔드포인트 및 네트워크 인텔리전스를 사용자 ID 정보와 연결하는 FireSIGHT 시스템을 사용할 수 있습니다. 시스템에서 네트워크 동작, 트래픽 및 이벤트를 개별 사용자와 직접 연결하므로 정책 위반, 공격 또는 네트워크 취약성의 소스를 손쉽게 식별할 수 있습니다. 다시 말해, 시스템은 사용자에게 "무엇" 뒤에 "누가" 있는지를 알려줄 수 있습니다. 예를 들면 다음을 확인할 수 있습니다.

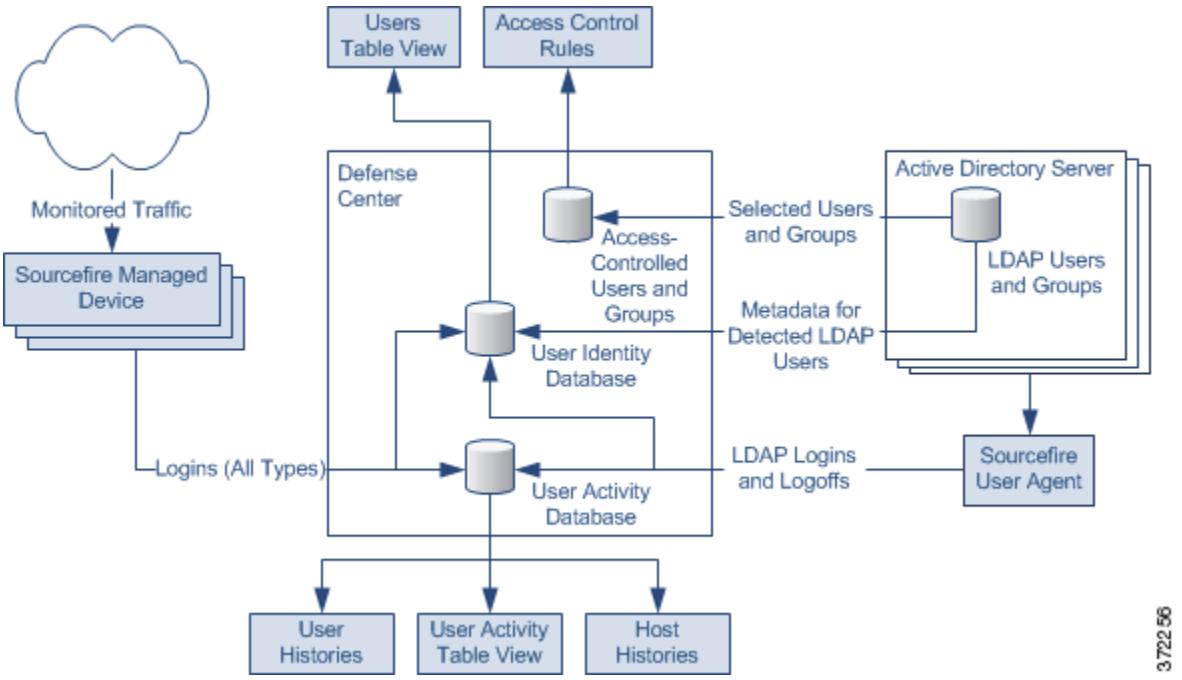
- 영향 레벨이 Vulnerable (level 1: red)인 침입 이벤트의 대상이 된 호스트를 소유한 사용자
- 내부 공격 또는 포트 스캔을 시작한 사용자
- 호스트 중요도가 높은 서버에 무단 액세스를 시도하는 사용자
- 대역폭을 너무 많이 사용하는 사용자
- 중요한 운영 체제 업데이트를 적용하지 않은 사용자
- 회사 IT 정책을 위반하며 인스턴트 메시징 소프트웨어나 피어 투 피어 파일 공유 애플리케이션을 사용하는 사용자

이러한 정보로 무장하면 표적 접근 방식을 통해 위험을 완화하고, 사용자 또는 사용자 활동을 차단하고, 다른 곳의 중단을 방지하기 위한 조치를 취할 수 있습니다. 또한 이러한 기능을 통해 감사 제어 효과를 크게 높이고 규정 준수를 강화할 수 있습니다.

LDAP 연결의 사용자 인식 설정을 기반으로 시스템은 Microsoft Active Directory LDAP 서버에서 액세스 제어 정책에 사용된 사용자를 다운로드합니다. 그러면 User Agent는 이러한 사용자에 대한 로그인 데이터를 제공하며, 사용자는 사용자 데이터베이스에 추가됩니다. 이러한 사용자를 *액세스 제어된 사용자*라고 부릅니다. 사용자 조건이 포함된 액세스 제어 정책을 작성할 때 액세스 제어된 사용자에 대해 그러한 조건을 작성합니다. 자세한 내용은 17-3페이지의 액세스 제어 규칙에 사용자 조건 추가을/를 참조하십시오.

시스템이 사용자 로그인, User Agent, 트래픽에서 탐지된 애플리케이션 데이터에서 또는 POP3, SMTP, IMAP 등을 통한 이메일 로그인에서 사용자 데이터를 탐지하면, 로그인하는 사용자가 사용자 목록을 기준으로 점검됩니다. 로그인 사용자가 에이전트에서 보고한 기존 사용자와 일치하면 로그인의 데이터가 사용자에게 할당됩니다. 로그인이 기존 사용자와 일치하지 않으면 SMTP 트래픽의 로그인이 아닌 경우 새 사용자가 생성됩니다. SMTP 트래픽의 일치하지 않는 로그인은 삭제됩니다.

다음 다이어그램은 FireSIGHT 시스템이 사용자 데이터를 수집 및 저장하는 방법을 보여줍니다.



다이어그램에서 볼 수 있듯이, 사용자 데이터에 대한 소스 3개와 데이터가 저장되는 장소 3개가 있습니다. 사용자 데이터 수집에 대한 자세한 내용은 다음을 참조하십시오.

- 45-4페이지의 관리되는 디바이스
- 45-5페이지의 User Agents
- 45-7페이지의 방어 센터-LDAP 서버 연결
- 45-7페이지의 사용자 데이터베이스
- 45-8페이지의 사용자 활동 데이터베이스
- 45-8페이지의 액세스 제어된 사용자 데이터베이스
- 45-9페이지의 사용자 데이터 수집 제한 사항

관리되는 디바이스

라이센스: FireSIGHT

지정한 네트워크에서 LDAP, AIM, POP3, IMAP, Oracle, SIP(VoIP), FTP, HTTP, MDNS 및 SMTP 로그인을 수동적으로 탐지하는 관리되는 디바이스를 구성하려면 네트워크 검색 정책을 사용합니다. 네트워크 검색 규칙에서 사용자 검색을 활성화하면 호스트 검색도 자동으로 활성화됩니다.

참고 관리되는 디바이스는 LDAP에 대한 Kerberos 로그인만 LDAP 인증으로 해석합니다. 관리되는 디바이스는 SSL이나 TLS 등의 프로토콜을 사용하는 암호화된 LDAP 인증을 탐지할 수 없습니다.

디바이스는 로그인을 탐지하면 다음 정보를 방어 센터로 전송하여 사용자 활동으로 기록합니다.

- 로그인에서 확인된 사용자 이름
- 로그인 시간
- 로그인과 관련된 IP 주소. 사용자 호스트(LDAP, POP3, IMAP 및 AIM 로그인), 서버(HTTP, MDNS, FTP, SMTP 및 Oracle 로그인) 또는 세션 시작 주체(SIP 로그인)의 IP 주소일 수 있습니다.
- 사용자의 이메일 주소(POP3, IMAP, SMTP 로그인용)
- 로그인을 탐지한 디바이스의 이름

사용자가 이전에 탐지된 적이 있는 경우, 방어 센터에서는 해당 사용자의 로그인 기록을 업데이트합니다. 방어 센터는 POP3 및 IMAP 로그인의 이메일 주소를 사용하여 LDAP 사용자와의 상관관계를 분석합니다. 예를 들어, 방어 센터에서 새로운 IMAP 로그인을 탐지하고 IMAP 로그인의 이메일 주소가 기존 LDAP 사용자와 일치할 경우, IMAP 로그인에서는 신규 사용자를 생성하지 않고 해당 LDAP 사용자의 기록을 업데이트합니다.

사용자가 이전에 탐지된 적이 없는 경우, 방어 센터에서는 해당 사용자를 사용자 데이터베이스에 추가합니다. 이러한 로그인 이벤트에는 방어 센터에서 다른 로그인 유형과의 상관관계를 분석할 수 있는 데이터가 없으므로, 고유한 AIM, SIP, Oracle 로그인에서는 항상 새로운 사용자 레코드를 생성합니다.

방어 센터에서는 다음과 같은 경우 사용자 활동 또는 사용자 신원을 기록하지 **않습니다**.

- 해당 로그인 유형을 무시하도록 네트워크 검색 정책을 구성한 경우(45-30페이지의 사용자 로깅 제한의 설명 참조)
- 관리되는 디바이스에서 SMTP 로그인을 탐지했지만 사용자 데이터베이스에 일치하는 이메일 주소를 보유한 이전에 탐지된 LDAP, POP3 또는 IMAP 사용자가 없는 경우

User Agents

라이센스: FireSIGHT

Microsoft Active Directory LDAP 서버를 사용하는 조직의 경우, Cisco에서는 Active Directory 서버를 통해 사용자 활동을 모니터링하려면 User Agents를 설치할 것을 권장합니다. 사용자 제어를 수행하려면 **반드시** User Agents를 설치하고 사용해야 합니다. 이 에이전트는 사용자를 IP 주소와 연결하며, 이에 따라 사용자 조건이 있는 액세스 제어 규칙이 트리거될 수 있습니다. 에이전트 하나를 사용하면 최대 5개의 Active Directory 서버에서 사용자 활동을 모니터링할 수 있습니다.

에이전트를 사용하려면 에이전트에 연결된 각 방어 센터와 모니터링되는 LDAP 서버 간에 연결을 구성해야 합니다. 이러한 연결을 활용하면 User Agents에서 로그인 및 로그오프가 탐지된 사용자의 메타데이터를 검색할 수 있을 뿐만 아니라, 액세스 제어 규칙을 사용할 사용자 및 그룹을 지정할 수도 있습니다. 사용자 검색을 위해 LDAP 서버를 구성하는 방법에 대한 자세한 내용은 17-4페이지의 액세스 제어 대상 사용자 및 LDAP 사용자 메타데이터 검색을/를 참조하십시오.

각 에이전트는 정기적으로 예약된 폴링 또는 실시간 모니터링을 사용해 암호화된 트래픽을 사용하여 로그인을 모니터링할 수 있습니다. 워크스테이션에서 또는 원격 데스크톱 로그인을 통해 사용자가 컴퓨터에 로그인하면 Active Directory 서버에 의해 로그인이 생성됩니다.

에이전트에서는 사용자 로그오프도 모니터링 및 보고할 수 있습니다. 사용자가 호스트 IP 주소에서 로그아웃할 때 에이전트 자체에 의해 로그오프가 생성됩니다. 호스트에 로그인한 사용자가 변경된 것을 에이전트에서 탐지하는 경우에도(Active Directory 서버에서 그러한 변경 사항을 보고하기 전에) 로그오프가 생성됩니다. 로그오프 데이터를 로그인 데이터와 결합하면 사용자의 네트워크 로그인에 대한 좀 더 완전한 상황을 파악할 수 있습니다.

Active Directory 서버 폴링을 통해 에이전트는 정의된 폴링 간격으로 일련의 사용자 활동 데이터를 검색할 수 있습니다. Active Directory 서버가 데이터를 받자마자 실시간 모니터링이 사용자 활동 데이터를 에이전트로 전송합니다.

특정 사용자 이름 또는 IP 주소와 연결된 로그인 또는 로그오프는 보고에서 제외하도록 에이전트를 구성할 수 있습니다. 파일 공유와 인쇄 서버 등 공유 서버에 대한 반복적인 로그인 및 문제 해결 목적으로 컴퓨터에 로그인하는 사용자는 제외하는 것이 좋습니다.

에이전트는 제외된 사용자 이름 또는 IP 주소 외의 모든 탐지된 로그인 및 로그오프의 레코드를 방어 센터로 전송합니다. 그러면 해당 레코드는 이곳에서 사용자 활동으로 보고됩니다. 에이전트는 방어 센터 버전을 탐지하고, 적절한 데이터 형식으로 로그인 레코드를 전송합니다. 이는 관리되는 디바이스에 의해 직접 탐지되는 사용자 활동을 보완합니다. User Agents에 의해 보고된 로그인은 사용자를 IP 주소와 연결하며, 이에 따라 사용자 조건이 있는 액세스 제어 규칙이 트리거될 수 있습니다.

User Agents는 사용자가 네트워크에 로그인할 때 또는 기타 이유로 Active Directory 자격 증명에 대해 계정을 인증할 때 사용자를 모니터링합니다. User Agent의 버전 2.1은 호스트에 대한 인터랙티브 사용자 로그인, 원격 데스크톱 로그인, 파일 공유 인증, 컴퓨터 계정 로그인은 물론 사용자 로그오프, 로그오프 시 원격 데스크톱 세션도 탐지합니다.

탐지된 로그인 유형에 따라 에이전트가 로그인을 보고하는 방법 및 호스트 프로필에 로그인이 표시되는 방법이 결정됩니다. 호스트에 대한 *권한 있는 사용자 로그인*의 경우 새 로그인의 사용자로 변경되도록 현재 사용자가 호스트 IP 주소에 매핑됩니다. 호스트의 기존 사용자가 호스트에 대해 권한 있는 사용자 로그인을 가지고 있지 않으면, 다른 로그인은 현재 사용자를 변경하지 않거나 호스트에 대한 현재 사용자만 변경합니다. 이러한 경우 예상 사용자가 더 이상 로그인하지 않으면 에이전트는 해당 사용자에 대해 로그오프를 생성합니다. 호스트의 기존 사용자가 호스트에 대해 권한 있는 사용자 로그인을 가지고 있지 않으면, 네트워크 검색에 의해 탐지된 사용자 로그인은 호스트에 대한 현재 사용자만 변경합니다. 에이전트에서 탐지한 로그인은 네트워크 맵에 다음과 같은 영향을 미칩니다.

- 사용자 또는 원격 데스크톱 로그인의 호스트에 대한 인터랙티브 로그인을 탐지하면 에이전트는 호스트에 대해 권한 있는 사용자 로그인을 보고하고 호스트의 현재 사용자를 새 사용자로 변경합니다.
- 파일 공유 인증을 위한 로그인을 탐지하면 에이전트는 호스트에 대한 사용자 로그인을 보고하되, 호스트의 현재 사용자를 변경하지 않습니다.
- 호스트에 대한 컴퓨터 계정 로그인을 탐지하면 에이전트는 NetBIOS Name Change 검색 이벤트를 생성하며 호스트 프로필은 NetBIOS 이름에 대한 변경 사항을 반영합니다.
- 제외된 사용자 이름의 로그인을 탐지하면 에이전트는 방어 센터에 로그인을 보고하지 않습니다.

로그인 또는 기타 인증이 발생하면 에이전트는 다음 정보를 방어 센터에 전송합니다.

- 사용자의 LDAP 사용자 이름
- 로그인 및 기타 인증 시간
- 사용자 호스트의 IP 주소 및 링크 로컬 주소(에이전트가 컴퓨터 계정 로그인에 대해 IPv6 주소를 보고하는 경우)

방어 센터는 로그인 및 로그오프 정보를 사용자 활동으로 기록합니다. User Agent가 사용자 로그인 또는 로그오프에서 사용자 데이터를 보고하면, 보고된 사용자가 사용자 목록을 기준으로 점검됩니다. 보고된 사용자가 에이전트에서 보고한 기존 사용자와 일치하면 보고된 데이터가 사용자에게 할당됩니다. 보고된 사용자가 기존 사용자와 일치하지 않으면 새 사용자가 생성됩니다.

제외된 사용자 이름과 연결된 사용자 활동이 보고되지 않더라도 관련 사용자 활동은 계속 보고될 수 있습니다. 컴퓨터에 대한 첫 번째 로그인에 이어 두 번째 로그인이 탐지된 상태에서 두 번째 사용자 로그인과 연결된 사용자 이름을 보고에서 제외한 경우, 에이전트는 원래 사용자에 대한 로그오프를 보고합니다. 그러나 두 번째 사용자에 대한 로그인은 보고되지 않습니다. 그 결과, 제외된 사용자가 호스트에 로그인한 경우에도 사용자가 IP 주소에 매핑되지 않습니다.

에이전트에서 탐지한 사용자 이름에 대한 다음 제한 사항을 참고하십시오.

- 방어 센터에 보고된, 달러 기호 문자($)로 끝나는 사용자 이름은 네트워크 맵을 업데이트하지만 사용자 로그인으로 표시되지는 않습니다.
- 방어 센터에서 유니코드 문자가 포함된 사용자 이름을 표시하는 데에는 제한 사항이 있을 수 있습니다.

방어 센터가 저장할 수 있는 탐지된 총 사용자 수는 FireSIGHT 라이센스에 따라 다릅니다. 라이센스 사용자 제한에 도달하면 대부분의 경우 시스템은 데이터베이스에 대한 새 사용자 추가를 중지합니다. 새 사용자를 추가하려면 데이터베이스에서 오래된 사용자 또는 비활성 사용자를 수동으로 삭제하거나 모든 사용자를 삭제해야 합니다.

방어 센터-LDAP 서버 연결

라이센스: FireSIGHT

방어 센터-LDAP 서버 연결을 사용하면 특정 탐지된 사용자에 대한 메타데이터를 검색할 수 있습니다. 해당 로그인이 관리되는 디바이스에 의해 탐지되었든 User Agent에 의해 탐지되었든, LDAP 사용자에 대한 메타데이터를 검색할 수 있습니다. 그러한 사용자가 LDAP 사용자와 동일한 이메일 주소를 가지고 있는 경우 POP3 및 IMAP 사용자에 대한 메타데이터도 검색할 수 있습니다.

조직에서 Microsoft Active Directory 서버를 사용하는 경우, 연결을 통해 액세스 제어 규칙에서 사용할 LDAP 사용자 및 그룹을 지정할 수 있습니다. 사용자 제어를 수행하려면 방어 센터와 Active Directory 서버 간 연결을 **반드시** 구성해야 합니다. 조직에서 Active Directory를 사용하지 않는 경우에도 관리되는 디바이스를 통해 사용자 로그인을 탐지할 수 있으며, Oracle 또는 OpenLDAP 서버의 일부 사용자에 대한 메타데이터도 가져올 수 있습니다. 그러나 그러한 사용자 또는 사용자 활동을 기반으로 사용자 제어를 수행할 수는 없습니다.

방어 센터는 각 사용자에 대한 다음과 같은 정보 및 메타데이터를 LDAP 서버에서 가져옵니다.

- LDAP 사용자 이름
- 이름 및 성
- email address
- 부서
- 전화 번호

사용자 데이터베이스

라이센스: FireSIGHT

사용자 데이터베이스에는 관리되는 디바이스 또는 User Agents에 의해 탐지된 각 사용자에 대한 레코드가 포함되어 있습니다. 방어 센터가 저장할 수 있는 탐지된 총 사용자 수는 FireSIGHT 라이센스에 따라 다릅니다. 라이센스 제한에 도달하면 대부분의 경우 시스템은 데이터베이스에 대한 새 사용자 추가를 중지합니다. 새 사용자를 추가하려면 데이터베이스에서 오래된 사용자 또는 비활성 사용자를 수동으로 삭제하거나 모든 사용자를 삭제해야 합니다.

그러나 시스템은 권한 있는 사용자 로그인을 선호합니다. 제한에 도달한 상태에서 시스템이 전에 탐지하지 못한 권한 있는 사용자의 로그인을 탐지하면, 오랫동안 비활성 상태를 유지한 권한 없는 사용자를 삭제하고 새로운 사용자를 대신 추가합니다.

사용자 데이터베이스의 내용은 방어 센터 웹 인터페이스를 통해 볼 수 있습니다. 탐지된 사용자를 보고 검색하고 삭제하는 방법에 대한 자세한 내용은 50-59페이지의 사용자 작업을/를 참조하십시오.

사용자 활동 데이터베이스

라이센스: FireSIGHT

사용자 활동 데이터베이스에는 Sourcefire User Agent로 모니터링되는 Active Directory LDAP 서버에 대한 연결을 통한 또는 네트워크 검색을 통한 네트워크상의 사용자 활동 레코드가 포함됩니다. 시스템에서는 다음과 같은 상황에서 이벤트를 기록합니다.

- 개별 로그인 또는 로그오프를 탐지한 경우
- 새 사용자를 탐지한 경우
- 수동으로 사용자를 삭제한 경우
- 데이터베이스에 없는 사용자를 탐지했으나 FireSIGHT 라이센스 제한 때문에 사용자를 추가할 수 없는 경우

시스템에서 탐지한 사용자 활동을 보려면 방어 센터 웹 인터페이스를 사용할 수 있습니다. 탐지된 사용자 활동을 보고 검색하고 삭제하는 방법에 대한 자세한 내용은 50-65페이지의 사용자 활동 작업을/를 참조하십시오. User Agent의 버전 2.1을 사용하여 LDAP 로그인 데이터를 방어 센터에 전송하려는 경우, 에이전트가 연결할 각 방어 센터에서 각 에이전트에 대한 연결을 구성해야 합니다. 이렇게 하면 에이전트는 방어 센터와 안전한 연결을 설정하여 로그인 데이터를 전송할 수 있습니다. 특정 사용자 이름을 제외하도록 에이전트를 구성한 경우 해당 사용자 이름의 로그인 데이터는 방어 센터에 보고되지 않습니다.

또한 사용자 액세스 제어를 구현하려는 경우, 데이터를 수집할 각 Microsoft Active Directory 서버에 대해 사용자 인식 매개 변수를 구성하여 연결을 설정해야 합니다.

가능한 경우마다 FireSIGHT 시스템은 사용자 활동을 다른 이벤트 유형과 상호 연결합니다. 예를 들어, 침입 이벤트는 이벤트 발생 시점에 소스 및 대상 호스트에 로그인한 사용자를 알려줄 수 있습니다.

시스템은 또한 사용자 활동을 사용하여, 각 사용자가 로그인한 호스트를 추적하는 *호스트 기록* 및 각 개별 호스트에 로그인한 사용자를 추적하는 *사용자 기록*을 생성합니다. 시스템은 마지막 24시간의 각 사용자 활동 및 각 호스트에 대한 마지막 24시간의 로그인에 대한 그래픽 화면을 제공합니다. 자세한 내용은 50-63페이지의 사용자 세부사항 및 호스트 기록 이해 및 49-22페이지의 호스트 프로필에서 사용자 기록 작업을/를 참조하십시오.

액세스 제어된 사용자 데이터베이스

라이센스: 제어

액세스 제어된 사용자 데이터베이스에는 액세스 제어 규칙에 사용할 수 있는 사용자 및 그룹이 포함되므로, FireSIGHT 시스템을 통한 사용자 제어를 수행할 수 있습니다. 이러한 사용자는 다음의 두 유형 중 하나일 수 있습니다.

- *액세스 제어된 사용자* - 사용자 제어를 수행하기 위해 액세스 제어 규칙에 추가할 수 있는 사용자. 방어 센터-LDAP 서버 연결을 구성할 때 액세스 제어된 사용자가 소속될 그룹을 지정합니다.
- *액세스 제어되지 않은 사용자* - 기타 탐지된 사용자.

방어 센터-LDAP 서버 연결을 구성할 때 액세스 제어된 사용자가 소속될 그룹을 지정합니다(17-4페이지의 액세스 제어 대상 사용자 및 LDAP 사용자 메타데이터 검색의 설명 참조).

User Agent의 버전 2.1을 사용하여 LDAP 로그인 및 로그오프 데이터를 버전 5.x 방어 센터에 전송하려는 경우, 에이전트가 연결할 각 방어 센터에서 각 에이전트에 대한 연결을 구성해야 합니다. 이렇게 하면 에이전트는 방어 센터와 안전한 연결을 설정하여 사용자 활동 데이터를 전송할 수 있습니다.

특정 사용자 이름을 제외하도록 에이전트를 구성한 경우 해당 사용자 이름의 사용자 활동 데이터는 방어 센터에 보고되지 않습니다. 이러한 제외된 사용자 이름은 데이터베이스에 남아 있지만 IP 주소와는 연결되지 않습니다.

또한 사용자 액세스 제어를 구현하려는 경우, 데이터를 수집할 각 Microsoft Active Directory 서버에 대해 사용자 인식 매개 변수를 구성하여 연결을 설정해야 합니다.

액세스 제어에 사용할 수 있는 최대 사용자 수는 FireSIGHT 라이센스에 따라 다릅니다. 방어 센터-LDAP 서버 연결을 구성할 때에는 포함하는 총 사용자 수가 FireSIGHT 사용자 라이센스를 넘지 않도록 해야 합니다. 자세한 내용은 65-8페이지의 FireSIGHT 호스트 및 사용자 라이센스 제한 이해을/를 참조하십시오.

사용자 데이터 수집 제한 사항

라이센스: FireSIGHT

다음 표에서는 사용자 데이터 수집의 제한 사항에 대해 설명합니다.

표 45-1 사용자 인식 제한 사항

제한 사항	설명
사용자 제어	사용자 제어를 수행하려면 조직에서 **반드시** Microsoft Active Directory LDAP 서버를 사용해야 합니다. 시스템은 액세스 제어 규칙에 사용할 수 있는 사용자 및 그룹을 Active Directory에서 가져오며, Active Directory 서버에 설치된 User Agents에서 보고하는 로그인 및 로그오프로 사용자를 IP 주소에 연결합니다.
LDAP 연결에 대한 비 Kerberos 로그인	관리되는 디바이스는 LDAP에 대한 Kerberos 로그인만 LDAP 인증으로 해석합니다. 관리되는 디바이스는 SSL이나 TLS 등의 기타 프로토콜을 사용하는 암호화된 LDAP 인증을 탐지할 수 없습니다. 반면 Active Directory 서버에서 보안 로그를 사용하여 사용자 로그인 데이터를 수집하는 User Agents에는 그러한 제한 사항이 적용되지 않습니다.
로그인 탐지	Active Directory 서버에 대한 로그인을 탐지하려는 경우 Active Directory 서버 연결을 서버 IP 주소로 구성해야 합니다. 자세한 내용은 *User Agent Configuration Guide*를 참조하십시오. 여러 사용자가 원격 세션을 사용해서 한 호스트에 로그인하는 경우 에이전트는 해당 호스트의 로그인을 제대로 탐지하지 못할 수 있습니다. 이 문제를 방지하는 방법에 대한 자세한 내용은 *User Agent Configuration Guide*를 참조하십시오.
로그오프 탐지	로그오프는 즉시 탐지되지 않을 수 있습니다. 로그오프와 연결된 타임스탬프는, 사용자가 더 이상 호스트 IP 주소에 매핑되지 않음을 에이전트가 탐지한 시간을 반영합니다. 이는 사용자가 호스트에서 로그오프한 실제 시간과 일치하지 않을 수 있습니다. 사용자가 호스트 IP 주소에서 로그아웃할 때 에이전트 자체에 의해 로그오프가 생성됩니다. 호스트에 로그인한 사용자가 변경된 것을 에이전트에서 탐지하는 경우에도(Active Directory 서버에서 그러한 변경 사항을 보고하기 전에) 로그오프가 생성됩니다.
실시간 데이터 검색	Active Directory 서버는 Windows Server 2008 또는 Windows Server 2012를 실행해야 합니다.

표 45-1 사용자 인식 제한 사항 (계속)

제한 사항	설명
서로 다른 사용자가 동일한 호스트에 다중 로그인	시스템은 특정 시점에 어느 한 호스트에 한 사용자만 로그인하며 호스트의 현재 사용자가 마지막 권한 있는 사용자 로그인이라고 가정합니다. 권한 없는 로그인만 호스트에 로그인한 경우 마지막 권한 없는 로그인이 현재 사용자로 간주됩니다. 원격 세션을 통해 여러 사용자가 로그인한 경우 Active Directory 서버에서 보고한 마지막 사용자가 방어 센터에 보고된 사용자입니다.
동일한 사용자가 동일한 호스트에 다중 로그인	시스템은 특정 호스트에 대한 사용자의 첫 번째 로그인만 기록하고 이후의 로그인은 무시합니다. 개별 사용자가 특정 호스트에 로그인하는 유일한 사람인 경우, 시스템에서는 원래 로그인만 기록합니다. 그러나 또 다른 사용자가 해당 호스트에 로그인하면 시스템에서는 새 로그인을 기록합니다. 그런 다음 원래 사용자가 다시 로그인하면 새 로그인이 기록됩니다.
유니코드 문자	유니코드 문자의 사용자 이름은 사용자 인터페이스에 정확하게 표시되지 않을 수 있습니다.
사용자 데이터베이스의 LDAP 사용자 계정	LDAP 서버에서 LDAP 사용자를 제거 또는 비활성화하거나 방어 센터에 대한 보고에서 사용자 이름을 제외하는 경우, 방어 센터는 해당 사용자를 사용자 데이터베이스에서 제거하지 않으며 해당 사용자는 데이터베이스에 나열된 사용자의 라이센스 제한에서 계속 계산됩니다. 사용자를 데이터베이스에서 직접 삭제해야 합니다. 사용자 라이센스 제한은 액세스 제어된 사용자에 대해 병렬로 적용됩니다. 액세스 제어된 사용자에 대한 사용자 카운트는 LDAP 컨피그레이션에 의해 검색되는 사용자 수에 의존합니다.
AIM(AOL Instant Messenger) 로그인 탐지	관리되는 디바이스는 OSCAR 프로토콜만을 사용하여 AIM 로그인을 탐지할 수 있습니다. 대부분의 AIM 클라이언트는 OSCAR을 사용하지만 일부는 TOC2를 사용합니다.

애플리케이션 탐지 이해

라이센스: FireSIGHT

FireSIGHT 시스템은 IP 트래픽을 분석할 때 네트워크에서 자주 사용되는 애플리케이션을 확인하려고 시도합니다. 애플리케이션 인식은 애플리케이션 기반 액세스 제어를 수행하기 위한 중요한 요소입니다.

시스템에서는 세 가지 유형의 애플리케이션을 탐지합니다.

- *Application Protocols* - 호스트 간 통신을 나타냄(예: HTTP 및 SSH)
- *Clients* - 호스트에서 실행 중인 소프트웨어를 나타냄(예: 웹 브라우저 및 이메일 클라이언트)
- *Web Applications* - HTTP 트래픽의 요청 URL 또는 콘텐츠를 나타냄(예: MPEG 비디오 및 Facebook)

시스템에서는 패킷 헤더의 ASCII 또는 16진수 패턴 또는 트래픽에서 사용되는 포트를 사용하여 네트워크 트래픽에서 애플리케이션을 확인합니다. 일부 애플리케이션 탐지기에서는 포트 및 패턴 탐지를 모두 사용하여 특정 애플리케이션의 트래픽을 올바르게 확인할 수 있는 확률을 높입니다. 또한 SSL(Secure Socket Layers) 프로토콜 탐지기는 보안 세션의 정보를 사용하여 세션에서 애플리케이션을 식별합니다. FireSIGHT 시스템에는 두 가지 소스의 애플리케이션 탐지기가 있습니다.

- *Cisco 제공 탐지기* - 웹 애플리케이션, 클라이언트, 애플리케이션 프로토콜 탐지

  Cisco에서 제공하는 애플리케이션(및 운영 체제, 45-2페이지의 호스트 데이터 수집 이해 참조) 탐지기 가용성은 FireSIGHT 시스템의 버전 및 설치한 VDB 버전에 따라 다릅니다. 릴리스 정보 및 권고문에는 새 탐지기 및 업데이트된 탐지기에 대한 정보가 포함되어 있습니다. Professional Services에서 작성한 개별 탐지기를 가져올 수도 있습니다. 탐지된 애플리케이션의 전체 목록은 지원 사이트를 참조하십시오.

- *사용자 정의 애플리케이션 프로토콜 탐지기* - 시스템의 애플리케이션 프로토콜 탐지 기능을 강화하기 위해 생성된 탐지기

애플리케이션 프로토콜은 *내장된 애플리케이션 프로토콜 탐지*를 통해서도 탐지할 수 있으며, 이는 클라이언트의 탐지를 기반으로 애플리케이션 프로토콜의 존재를 암시합니다.

시스템은 다음 표에 설명된 기준을 사용하여, 탐지된 애플리케이션 각각에 특성을 부여합니다. 시스템은 이러한 특성을 사용하여 애플리케이션 필터 또는 애플리케이션 그룹을 생성합니다. 이러한 필터 및 액세스 제어를 수행하기 위해, 그리고 검색, 보고서 및 대시보드 위젯을 제한하기 위해 생성하는 필터를 사용할 수 있습니다. 자세한 내용은 3-15페이지의 애플리케이션 필터 작업을/를 참조하십시오.

표 45-2 애플리케이션 특성

특성	설명	예
유형	애플리케이션 유형: • **Application Protocols** - 호스트 간 통신을 나타냅니다. • **Client** - 호스트에서 실행 중인 소프트웨어를 나타냅니다. • **Web Applications** - HTTP 트래픽에 대한 콘텐츠 또는 요청 URL을 나타냅니다.	HTTP 및 SSH는 애플리케이션 프로토콜입니다. 웹 브라우저 및 이메일 클라이언트는 클라이언트입니다. MPEG 비디오 및 Facebook은 웹 애플리케이션입니다.
위험	조직의 보안 정책을 거스를 수 있는 용도로 애플리케이션이 사용될 가능성. 애플리케이션 위험의 범위는 **Very Low**에서 **Very High**까지입니다.	피어 투 피어 애플리케이션의 위험은 주로 Very High입니다.
비즈니스 연관성	조직의 비즈니스 운영(레크리에이션과 반대) 컨텍스트 내에서 애플리케이션이 사용될 가능성. 애플리케이션 비즈니스 연관성의 범위는 **Very Low**에서 **Very High**까지입니다.	게임 애플리케이션의 비즈니스 연관성은 주로 Very Low입니다.
카테고리	가장 중요한 기능을 설명하는 일반 애플리케이션 분류. 각 애플리케이션은 적어도 하나의 카테고리에 속합니다.	Facebook의 카테고리는 **social networking**입니다.
태그	애플리케이션에 대한 추가 정보. 애플리케이션에는 0부터 원하는 수만큼의 태그를 포함할 수 있습니다.	비디오 스트리밍 웹 애플리케이션은 종종 **high bandwidth** 및 **displays ads**로 태그가 지정됩니다.

시스템에 의해 수집된 애플리케이션 데이터를 보완하려면 NetFlow 지원 디바이스, Nmap 활성 스캔, 호스트 입력 기능에 의해 생성된 레코드를 사용할 수 있습니다.

자세한 내용은 다음 링크를 참고하십시오.

- 45-12페이지의 애플리케이션 프로토콜 탐지 프로세스 이해
- 45-13페이지의 클라이언트 탐지로부터의 암시된 애플리케이션 프로토콜 탐지
- 45-14페이지의 애플리케이션 프로토콜 탐지를 위한 특별 고려 사항: Squid
- 45-14페이지의 특별 고려 사항: SSL 애플리케이션 탐지
- 45-15페이지의 특별 고려 사항: 참조된 웹 애플리케이션
- 46-17페이지의 애플리케이션 탐지기 작업
- 45-15페이지의 서드파티 검색 데이터 가져오기

- 45-16페이지의 NetFlow 이해

애플리케이션 프로토콜 탐지 프로세스 이해

라이센스: FireSIGHT

시스템은 애플리케이션 트래픽을 탐지하면, 특정 포트를 유일한 탐지 기준으로서 사용하는 탐지기가 식별한 포트에서 애플리케이션 프로토콜이 실행 중인지를 우선 확인합니다. 그러한 포트 중 하나에서 애플리케이션 프로토콜이 실행 중이면 시스템은 잘 알려진 포트 탐지기를 사용하여 애플리케이션을 긍정적으로 식별합니다.

참고 Cisco 제공 탐지기에 의해 사용되는 포트에서 사용자 정의 포트 기반 애플리케이션 프로토콜 탐지기를 만들고 활성화할 수 있으므로, Cisco의 탐지 기능을 재정의하는 것이 가능합니다. 예를 들어, 사용자 정의 탐지기가 포트 22에서 모든 애플리케이션 프로토콜 트래픽을 `myapplication` 애플리케이션 프로토콜로 식별하면, 포트 22의 SSH 트래픽이 `myapplication` 트래픽으로 잘못 식별됩니다.

애플리케이션 프로토콜이 이러한 포트 중 하나에서 실행되고 있지 않으면 시스템은 포트 및 패턴 일치를 기반으로 식별하는 좀 더 강력한 방법을 사용합니다. 두 탐지기가 모두 트래픽을 긍정적으로 식별하면, 더 긴 패턴 일치를 사용하는 탐지기가 우선권을 갖습니다. 마찬가지로, 다중 패턴 일치가 있는 탐지기가 단일 패턴 일치가 있는 탐지기보다 우선권을 갖습니다.

네트워크 검색 정책에 정의된 대로 시스템은 모니터링되는 네트워크의 호스트에서 실행되는 애플리케이션 프로토콜만 식별합니다. 예를 들어, 모니터링 중인 원격 사이트의 FTP 서버에 내부 호스트가 액세스하는 경우 시스템은 애플리케이션 프로토콜을 FTP로 식별하지 못합니다. 반면, 모니터링 중인 FTP 서버에 원격 또는 내부 호스트가 액세스하면 시스템은 애플리케이션 프로토콜을 긍정적으로 식별할 수 있습니다.

시스템이 모니터링되지 않는 서버에 액세스하는 모니터링되는 호스트 간 연결에 사용되는 클라이언트를 식별할 수 있는 경우 예외가 발생합니다. 이런 경우 시스템은 연결의 클라이언트에 해당하는 적절한 애플리케이션 프로토콜을 긍정적으로 식별하지만, 네트워크 맵에 애플리케이션 프로토콜을 추가하지는 않습니다. 자세한 내용은 45-13페이지의 클라이언트 탐지로부터의 암시된 애플리케이션 프로토콜 탐지을/를 참조하십시오. 애플리케이션 탐지가 발생하려면 클라이언트 세션에 서버의 응답이 포함되어야 합니다.

다음 표에서는 FireSIGHT 시스템이 방어 센터 웹 인터페이스에서 탐지된 애플리케이션 프로토콜을 식별하는 방법을 간단하게 보여줍니다. 여기에는 네트워크 맵, 호스트 프로필, 이벤트 보기 등이 포함됩니다.

표 45-3 FireSIGHT 시스템의 애플리케이션 프로토콜 식별

애플리케이션	설명
애플리케이션 프로토콜 이름	다음과 같은 경우 방어 센터는 애플리케이션 프로토콜을 이름으로 식별합니다. • 애플리케이션 프로토콜이 시스템에 의해 긍정적으로 식별된 경우 • 애플리케이션 프로토콜이 NetFlow 데이터를 통해 식별되었으며 /etc/sf/services에 포트 애플리케이션 프로토콜 상관관계가 있는 경우 • 애플리케이션 프로토콜이 호스트 입력 기능을 통해 수동으로 식별된 경우 • 애플리케이션 프로토콜이 Nmap 또는 다른 활성 소스에 의해 식별된 경우
pending	시스템이 애플리케이션을 긍정적으로도 부정적으로도 식별할 수 없는 경우 방어 센터는 애플리케이션 프로토콜을 pending으로 식별합니다. 대부분의 경우 시스템이 보류 중인 애플리케이션을 식별하려면 더 많은 연결 데이터(애플리케이션이 식별된)를 수집 및 분석해야 합니다. Application Details 및 Servers 테이블과 호스트 프로필에서 pending 상태는 특정 애플리케이션 프로토콜 트래픽이 탐지된 애플리케이션 프로토콜(탐지된 클라이언트 또는 웹 애플리케이션 트래픽에 의해 암시된 것이 아니라)에 대해서만 나타납니다.
unknown	다음과 같은 경우 방어 센터는 애플리케이션 프로토콜을 unknown으로 식별합니다. • 애플리케이션이 시스템의 탐지기 중 하나와 일치하지 않는 경우 • 애플리케이션 프로토콜이 NetFlow 데이터를 통해 식별되었지만 /etc/sf/services에 포트 애플리케이션 프로토콜 상관관계가 없는 경우
공백	사용 가능한 모든 탐지된 데이터가 검토되었지만 애플리케이션 프로토콜이 식별되지 않았습니다. Application Details 및 Servers 테이블과 호스트 프로필에서, 탐지된 애플리케이션 프로토콜이 없는 비 HTTP 일반 클라이언트 트래픽에 대해 애플리케이션 프로토콜은 비어 있게 됩니다.

클라이언트 탐지로부터의 암시된 애플리케이션 프로토콜 탐지

라이센스: FireSIGHT

모니터링되지 않는 서버에 액세스하는 모니터링되는 호스트 간 연결에 사용되는 클라이언트를 시스템이 식별할 수 있는 경우 방어 센터는 클라이언트와 상응하는 애플리케이션 프로토콜이 연결에 사용되고 있다고 추론합니다. 시스템은 모니터링되는 네트워크에서만 애플리케이션을 추적하므로, 일반적으로 연결 로그에는 모니터링되는 호스트가 모니터링되지 않는 서버에 액세스하는 연결에 대한 애플리케이션 프로토콜 정보가 포함되지 않습니다.

클라이언트 탐지에서 오는 애플리케이션 프로토콜의 암시된 탐지에 따른 몇 가지 결과가 있습니다.

- 시스템은 이러한 서버에 대해 New TCP Port 또는 New UDP Port 이벤트를 생성하지 않으므로 Servers 테이블에 서버가 나타나지 않습니다. 또한 이러한 애플리케이션 프로토콜의 탐지를 기준으로 사용하여 검색 이벤트 알림 또는 상관관계 규칙을 트리거할 수 없습니다.
- 애플리케이션 프로토콜은 호스트와 연결되지 않으므로 호스트 프로필의 세부사항을 볼 수 없거나, 서버 ID를 설정할 수 없거나, 트래픽 프로필 또는 상관관계 규칙에 대한 호스트 프로필 자격에서 해당 정보를 사용할 수 없습니다. 또한 시스템은 이러한 유형의 탐지를 기반으로 취약성을 호스트와 연결하지 않습니다.

그러나 연결에서 애플리케이션 프로토콜 정보에 대한 상관관계 이벤트를 트리거할 수 있습니다. 또한 연결 로그에서 애플리케이션 프로토콜 정보를 사용하여 연결 추적기 및 트래픽 프로필을 생성할 수 있습니다.

호스트 제한 및 검색 이벤트 로깅

라이센스: FireSIGHT

시스템은 클라이언트, 서버 또는 웹 애플리케이션을 탐지하면, 연결된 호스트가 이미 최대 클라이언트, 서버 또는 웹 애플리케이션 수에 도달하지 않은 경우 검색 이벤트를 생성합니다.

호스트 프로필은 호스트당 클라이언트 최대 16개, 서버 100개, 웹 애플리케이션 100개를 표시합니다. 자세한 내용은 49-15페이지의 호스트 프로필에서 서버 작업 및 49-20페이지의 호스트 프로필에서 애플리케이션 보기을/를 참조하십시오.

클라이언트, 서버 또는 웹 애플리케이션의 탐지에 의존하는 작업은 이 제한의 영향을 받지 않습니다. 예를 들어, 서버를 트리거하도록 구성된 액세스 제어 규칙은 여전히 연결 이벤트를 기록합니다.

애플리케이션 프로토콜 탐지를 위한 특별 고려 사항: Squid

라이센스: FireSIGHT

다음과 같은 경우 시스템은 Squid 서버 트래픽을 긍정적으로 식별합니다.

- 시스템이 모니터링되는 네트워크의 호스트에서 프록시 인증이 활성화된 Squid 서버로의 연결을 탐지하는 경우 또는
- 시스템이 모니터링되는 네트워크의 Squid 프록시 서버에서 대상 시스템(즉, 클라이언트가 정보 또는 다른 리소스를 요청하는 대상 서버)으로의 연결을 탐지하는 경우

그러나 다음과 같은 경우 시스템은 Squid 서비스를 식별할 수 없습니다.

- 모니터링되는 네트워크의 호스트가 프록시 인증이 비활성화된 Squid 서버에 연결된 경우
- HTTP 응답에서 Via: 헤더 필드를 제거하도록 Squid 프록시 서버가 구성된 경우

특별 고려 사항: SSL 애플리케이션 탐지

라이센스: FireSIGHT

FireSIGHT 시스템에서는 애플리케이션 프로토콜, 클라이언트 애플리케이션 또는 세션의 웹 애플리케이션을 확인할 수 있도록 SSL(Secure Socket Layers) 세션에서 세션 정보를 사용할 수 있는 탐지기를 제공합니다.

시스템에서 암호화 연결을 탐지할 경우, 해당 연결은 일반 HTTPS 연결 또는 좀 더 구체적인 보안 프로토콜(예: SMTPS)로 표시됩니다(해당되는 경우). 시스템에서 SSL 세션을 탐지할 경우, 세션에 대한 연결 이벤트의 **Client** 필드에 `SSL client`가 추가됩니다. 세션에 대한 웹 애플리케이션이 확인될 경우, 시스템에서는 트래픽에 대한 검색 이벤트를 생성합니다.

SSL 애플리케이션 트래픽의 경우, 관리되는 디바이스에서는 서버 인증서의 CN을 탐지하고, 이를 SSL 호스트 패턴의 클라이언트 또는 웹 애플리케이션과 일치하는지 확인할 수 있습니다. 시스템에서 특정 클라이언트를 식별한 경우, `SSL 클라이언트`가 해당 클라이언트의 이름으로 변경됩니다.

SSL 애플리케이션 트래픽이 암호화되므로, 시스템에서는 암호화된 스트림 내에 있는 애플리케이션 데이터가 아닌 인증서의 정보만을 식별에 사용할 수 있습니다. 이러한 이유로, SSL 호스트 패턴은 애플리케이션을 만든 회사만 식별할 수 있는 경우가 간혹 있으므로, 같은 회사에서 제작한 SSL 애플리케이션의 경우 식별 과정이 동일할 수 있습니다.

HTTPS 세션이 HTTP 세션 내에서 실행되는 등의 일부 경우에는 관리되는 디바이스가 클라이언트 측 패킷의 클라이언트 인증서에서 서버 이름을 탐지합니다.

SSL 애플리케이션 식별을 활성화하려면 responder 트래픽을 모니터링하는 액세스 제어 규칙을 생성해야 합니다. 그러한 규칙에는 SSL 애플리케이션에 대한 애플리케이션 조건 또는 SSL 인증서의 URL을 사용하는 URL 조건이 있어야 합니다. 네트워크 검색의 경우 responder IP 주소는 네트워크 검색 정책에서 모니터링할 네트워크에 있어야 할 필요가 없습니다. 액세스 제어 정책 컨피그레이션이 트래픽의 식별 여부를 결정합니다. SSL 애플리케이션에 대해 탐지기를 식별하려면, 애플리케이션 탐지기 목록에서 또는 액세스 제어 규칙에서 애플리케이션 조건을 추가할 때 `SSL protocol` 태그별로 필터링할 수 있습니다.

특별 고려 사항: 참조된 웹 애플리케이션

웹 서버는 더러 다른 웹사이트에 대한 트래픽(종종 광고 서버)을 참조합니다. 네트워크에서 발생하는 참조된 트래픽의 컨텍스트를 더 잘 이해할 수 있도록, 시스템은 참조된 세션에 대한 이벤트의 Web Application 필드에 트래픽을 참조한 웹 애플리케이션을 나열합니다. VDB에는 알려진 참조된 사이트의 목록이 포함되어 있습니다. 시스템이 그러한 사이트 중 하나의 트래픽을 탐지하면 해당 트래픽에 대한 이벤트와 함께 참조하는 사이트가 저장됩니다. 예를 들어, Facebook을 통해 액세스하는 광고가 실제로 Advertising.com에 호스트되면, 탐지된 Advertising.com 트래픽은 Facebook 웹 애플리케이션과 연결됩니다. 시스템은 또한 HTTP 트래픽에서 참조하는 URL을 탐지할 수 있습니다(예: 웹사이트가 또 다른 사이트에 단순 링크를 제공할 때). 이 경우 참조하는 URL이 HTTP Referrer 이벤트 필드에 나타납니다.

참조하는 애플리케이션이 존재하는 경우 트래픽에 대한 웹 애플리케이션으로 나열되는 반면, URL은 참조된 사이트에 대한 것입니다. 위의 예에서 해당 트래픽에 대한 연결 이벤트의 웹 애플리케이션은 Facebook일 수 있지만, URL은 Advertising.com일 수 있습니다. 참조하는 웹 애플리케이션이 탐지되지 않거나 호스트가 스스로를 참조하거나 추천의 체인이 있는 경우, 참조된 애플리케이션이 이벤트에 웹 애플리케이션으로 나타날 수 있습니다. 대시보드에서 웹 애플리케이션의 연결 및 바이트 카운트에는 웹 애플리케이션이 스스로 참조한 트래픽과 연결된 세션이 포함됩니다.

참조된 트래픽에 대해 특별히 작동하는 규칙을 생성하는 경우 참조하는 애플리케이션보다는 참조된 애플리케이션에 대한 조건을 추가해야 합니다. 예를 들어, Facebook에서 참조되는 Advertising.com 트래픽을 차단하려면 Advertising.com 애플리케이션에 대한 액세스 제어 규칙에 애플리케이션 조건을 추가하십시오.

서드파티 검색 데이터 가져오기

라이센스: FireSIGHT

운영 체제, 애플리케이션, 취약성, 시스템에서 수집한 데이터 보완 등에 대한 정보를 추가하려면 Nmap 활성 스캔을 사용할 수 있습니다. Nmap 스캐닝 및 스캔 결과에 대한 자세한 내용은 47-1페이지의 Nmap 스캔 이해을/를 참조하십시오.

시스템이 네트워크 트래픽 모니터링에서 수집한 정보를 보완하려면, 서드파티 애플리케이션이 API를 통해 FireSIGHT 시스템과 상호 작용하도록 구성하거나 수동으로 데이터를 추가하여 호스트 입력 기능을 사용할 수 있습니다. 서드파티 데이터를 Cisco 정의에 매핑하기 위해 제품, 취약성 및 수정 매핑을 생성하여 운영 체제 및 서버에 대한 영향 상관관계를 활성화할 수 있습니다. 호스트 입력 기능 및 서드파티 데이터 매핑에 대한 자세한 내용은 *FireSIGHT 시스템 Host Input API Guide* 및 46-29페이지의 호스트 입력 데이터 가져오기을/를 참조하십시오.

시스템은 운영 체제 및 서버 ID에 대해 수집한 데이터를 조정하여 핑거프린트 소스 우선순위 값, ID 충돌 해결 설정 및 수집 시간을 기반으로 각 ID를 결정합니다.

네트워크 맵 및 이벤트 테이블을 개선하려면 NetFlow 지원 디바이스의 데이터를 사용하여 네트워크 맵을 구성할 수도 있습니다. 자세한 내용은 45-16페이지의 NetFlow 이해을/를 참조하십시오.

검색 데이터 용도

라이센스: FireSIGHT

검색 데이터를 기록하면 다음을 비롯하여 FireSIGHT 시스템의 많은 기능을 활용할 수 있습니다.

- 네트워크 맵 보기 - 호스트와 네트워크 디바이스, 호스트 특성, 애플리케이션 프로토콜 또는 취약성을 그룹화하여 네트워크 자산 및 토폴로지를 자세히 볼 수 있습니다. 48-1페이지의 네트워크 맵 사용을/를 참조하십시오.
- 호스트 프로필 보기 - 탐지된 호스트에 사용할 수 있는 모든 정보를 완전하게 보여줍니다. 49-1페이지의 호스트 프로필 사용을/를 참조하십시오.
- 대시보드 보기 - 무엇보다, 네트워크 자산과 사용자 활동을 한눈에 볼 수 있는 기능을 제공합니다. 55-1페이지의 대시보드 사용을/를 참조하십시오.
- 시스템이 기록한 검색 이벤트 및 사용자 활동에 대한 자세한 정보 보기. 50-1페이지의 검색 이벤트 작업을/를 참조하십시오.
- 검색 데이터를 기반으로 보고서 생성. 57-1페이지의 보고서 작업을/를 참조하십시오.
- 애플리케이션 및 사용자 제어 수행 - 애플리케이션 및 사용자 조건을 사용하여 액세스 제어 규칙을 작성합니다. 16-2페이지의 애플리케이션 트래픽 제어 및 17-3페이지의 액세스 제어 규칙에 사용자 조건 추가을/를 참조하십시오.
- 호스트와 서버 또는 여기에서 실행 중인 클라이언트를 영향받기 쉬운 익스플로잇과 연결 - 네트워크 자산을 최대한 보호할 수 있도록 취약성을 식별 및 완화하고, 침입 이벤트가 네트워크에 미치는 영향을 평가하며, 침입 규칙 상태를 조정할 수 있습니다. 49-26페이지의 호스트 프로필에서 취약성 작업, 41-38페이지의 이벤트를 평가하기 위한 영향 레벨 사용, 45-20페이지의 IOC 이해 및 33-1페이지의 네트워크 자산에 대한 침입 방지 맞춤화을/를 참조하십시오.
- 시스템이 특정 영향 플래그와 함께 침입 이벤트를 생성하거나 특정 검색 이벤트를 생성할 경우 이메일, SNMP 트랩 또는 syslog를 통해 알림. 43-1페이지의 외부 알림 구성을/를 참조하십시오.
- 허용되는 운영 체제, 클라이언트, 애플리케이션 프로토콜 및 프로토콜의 화이트리스트로 조직의 규정준수 모니터링. 52-1페이지의 규정준수 툴로 FireSIGHT 시스템 사용을/를 참조하십시오.
- 시스템이 검색 이벤트를 생성하거나 사용자 활동을 탐지할 때 상관관계 이벤트를 트리거 및 생성하는 규칙으로 상관관계 정책 생성. 51-1페이지의 상관관계 정책 및 규칙 구성을/를 참조하십시오.
- 해당 연결 데이터를 사용하여 NetFlow 연결을 기록하는 경우. 38-5페이지의 방어 센터 또는 외부 서버와의 연결 로깅을/를 참조하십시오.

NetFlow 이해

라이센스: FireSIGHT

NetFlow는 네트워크 운영의 특징을 결정짓는 Cisco IOS Software에 포함된 기능입니다. RFC 프로세스를 통해 표준화된 NetFlow는 Cisco 네트워킹 디바이스에서 이용할 수 있는 것은 물론 Juniper, FreeBSD 및 OpenBSD 디바이스에 포함할 수도 있습니다.

NetFlow 지원 디바이스는 이러한 디바이스를 통과하는 트래픽에 대한 데이터를 캡처하고 내보내기 위해 광범위하게 사용됩니다. NetFlow 지원 디바이스에는 디바이스를 통과하는 플로우의 레코드를 저장하는 NetFlow 캐시라는 데이터베이스가 있습니다. 플로우(FireSIGHT 시스템에서 *연결*이라고도 함)는 특정 포트, 프로토콜 및 애플리케이션 프로토콜을 사용하여 소스와 대상 호스트 간 세션을 나타내는 연속된 패킷입니다.

지정된 네트워크에서 FireSIGHT 시스템가 관리하는 디바이스는 NetFlow 지원 디바이스에서 내보낸 레코드를 탐지하고, 그러한 레코드의 데이터를 기반으로 연결 이벤트를 생성하며, 마지막으로 그러한 이벤트를 방어 센터로 전송하여 데이터베이스에 기록합니다. NetFlow 연결의 정보를 기반으로 호스트 및 애플리케이션 프로토콜 정보를 데이터베이스에 추가하도록 시스템을 구성할 수도 있습니다.

관리되는 디바이스에 의해 직접 수집된 데이터를 보완하기 위해 이 검색 및 연결 데이터를 사용할 수 있습니다. 이는 NetFlow 지원 디바이스가 관리되는 디바이스에서 모니터링할 수 없는 네트워크에 구축된 경우 특히 유용합니다.

네트워크 검색 정책의 규칙을 사용하여 연결 로깅을 비롯한 NetFlow 데이터 수집을 구성합니다. 이것을 FireSIGHT 시스템 관리되는 디바이스에서 탐지한 연결에 대한 로깅(38-15페이지의 액세스 제어 처리 기반 연결 로깅에서 설명한 대로 액세스 제어 규칙 단위로 구성)과 비교합니다. NetFlow 데이터 수집은 액세스 제어 규칙보다는 네트워크에 연결되므로 기록하려는 연결을 매우 세부적으로 제어할 수는 없습니다. 또한 시스템은 모든 NetFlow 기반 연결 이벤트를 방어 센터 연결 이벤트 데이터베이스에 저장합니다. 사용자는 이러한 데이터를 SNMP 트랩 서버로 전송할 수 없습니다.

자세한 내용은 다음 링크를 참고하십시오.

- 45-17페이지의 NetFlow 및 FireSIGHT 데이터 간 차이점
- 45-19페이지의 NetFlow 데이터 분석 준비
- 45-16페이지의 검색 데이터 용도
- 38-5페이지의 방어 센터 또는 외부 서버와의 연결 로깅

NetFlow 및 FireSIGHT 데이터 간 차이점

라이센스: FireSIGHT

한 가지(TCP 플래그)를 제외하면, NetFlow 레코드에서 사용 가능한 정보는 관리되는 디바이스를 사용하여 네트워크 트래픽을 모니터링함으로써 생성되는 정보보다 좀 더 제한적입니다. 시스템은 NetFlow 데이터에 의해 표시되는 트래픽을 직접 분석할 수 없으므로, NetFlow 레코드를 처리할 때 해당 데이터를 연결 로그로 변환하고, 호스트 및 애플리케이션 프로토콜 레코드로 변환하기 위해 다양한 방법을 사용합니다.

변환된 NetFlow 데이터와 관리되는 디바이스에서 직접 수집한 검색 및 연결 데이터 사이에는 몇 가지 차이점이 있습니다. 필요한 분석을 수행할 경우 이러한 차이점에 유의해야 합니다.

- 탐지된 연결 수에 대한 통계
- 운영 체제 및 기타 호스트 관련 정보(취약성 포함)
- 클라이언트 정보, 웹 애플리케이션 정보, 공급업체 및 버전 서버 정보를 비롯한 애플리케이션 데이터
- 연결에서 어떤 호스트가 initiator이고 어떤 호스트가 responder인지 파악

팁 연결 이벤트의 각 필드에 대해 39-12 페이지의 표 39-1에서는, 연결이 FireSIGHT 시스템 관리되는 디바이스에 의해 직접 탐지되었는지 또는 연결 이벤트가 NetFlow 데이터를 기반으로 하는지에 따라 사용 가능한 데이터를 나타냅니다.

모니터링되는 세션마다 생성되는 연결 이벤트의 수

관리되는 디바이스에서 직접 탐지하는 연결의 경우, 액세스 제어 규칙 작업에 따라 연결의 시작이나 끝에, 또는 모두에 양방향 연결 이벤트를 기록할 수 있습니다.

그러나 NetFlow 지원 디바이스는 단방향 연결 데이터를 내보내므로 시스템은 디바이스 구성 방법에 따라 NetFlow 지원 디바이스에서 탐지하는 각 연결에 대해 항상 최소 2개의 연결 이벤트를 생성합니다. 이는 또한 NetFlow 데이터 기반의 각 연결에 대해 요약의 연결 카운트가 2씩 증가하므로, 네트워크에서 실제로 발생하는 연결 수보다 많은 결과가 제공됩니다.

연결이 끝날 때만 레코드를 출력하도록 NetFlow 지원 디바이스를 구성하면 시스템은 해당 세션에 대해 2개의 연결 이벤트를 생성합니다. 반면, 연결이 계속 유지되고 있더라도 고정된 간격으로 레코드를 출력하도록 NetFlow 지원 디바이스를 구성하면 시스템은 디바이스에서 내보낸 각 레코드에 대해 연결 이벤트를 생성합니다. 예를 들어, 오래 실행되는 연결에 대해 5분마다 레코드를 출력하도록 NetFlow 지원 디바이스를 구성하고 특정 연결이 12분간 지속되면, 시스템은 해당 세션에 대해 6개의 연결 이벤트를 생성합니다.

- 첫 번째 5분 동안 이벤트 쌍 하나
- 두 번째 5분 동안 이벤트 쌍 하나
- 연결이 종료될 때 마지막 쌍

이러한 이유 때문에 Cisco에서는 모니터링되는 세션이 끝날 때에만 레코드를 출력하도록 NetFlow 지원 디바이스를 구성할 것을 **적극** 권장합니다.

호스트 및 운영 체제 데이터

NetFlow 레코드를 기반으로 호스트를 네트워크 맵에 추가하도록 네트워크 검색 정책을 구성할 수 있지만 호스트 프로필은 연결에서 관련된 호스트에 대해 운영 체제 또는 NetBIOS 데이터를 포함하지 않으며, 시스템은 호스트가 네트워크 디바이스(브리지, 라우터, NAT 디바이스 또는 로드 밸런서)인지를 식별할 수도 없습니다. 그러나 호스트 입력 기능을 사용하여 호스트의 운영 체제를 수동으로 설정할 수 있습니다.

응용프로그램 데이터

관리되는 디바이스에서 직접 탐지하는 연결의 경우, 시스템은 연결의 패킷을 검토하여 애플리케이션 프로토콜, 클라이언트 및 웹 애플리케이션을 식별할 수 있습니다.

시스템은 NetFlow 레코드를 처리할 때 애플리케이션 프로토콜 ID를 추정하기 위해 `/etc/sf/services`의 포트 상관관계를 사용합니다. 그러나 그러한 애플리케이션 프로토콜에 대한 공급업체 또는 버전 정보가 없으며, 연결 로그에는 세션에서 사용된 클라이언트 또는 웹 애플리케이션에 대한 정보가 포함되지 않습니다. 그러나 호스트 입력 기능을 사용해 이러한 정보를 수동으로 제공할 수 있습니다.

단순한 포트 상관관계는, 비표준 포트에서 실행 중인 애플리케이션 프로토콜이 식별되지 않거나 잘못 식별될 수 있음을 의미합니다. 또한 상관관계가 존재하지 않는 경우 시스템은 연결 로그에서 애플리케이션 프로토콜을 `unknown`으로 표시합니다.

취약성 매핑

호스트 입력 기능을 사용하여 호스트의 운영 체제 ID 또는 애플리케이션 프로토콜 ID를 수동으로 설정하지 않는 한, FireSIGHT 시스템은 어떤 취약성이 NetFlow 레코드를 기반으로 네트워크 맵에 추가된 호스트에 영향을 미칠지 확인할 수 없습니다. NetFlow 연결에는 클라이언트 정보가 없으므로 클라이언트 취약성을 NetFlow 호스트와 연결할 수 없습니다.

연결의 Initiator 및 Responder 정보

관리되는 디바이스에서 직접 탐지하는 연결의 경우, 시스템은 어떤 호스트가 initiator(또는 소스)인지, 그리고 어떤 호스트가 responder(또는 대상)인지를 식별할 수 있습니다. 그러나 NetFlow 데이터에는 initiator 또는 responder 정보가 포함되어 있지 않습니다.

시스템에서 NetFlow 레코드를 처리할 때 각 호스트에서 사용하는 포트를 기반으로 이 정보를 확인하고 이 포트가 잘 알려진 것인지 확인하기 위해 알고리즘을 사용합니다.

- 사용 중인 두 포트 모두 잘 알려진 포트이거나 둘 다 잘 알려진 포트가 아닌 경우 시스템은 낮은 번호의 포트를 사용하는 호스트를 responder로 간주합니다.
- 호스트 중 하나만 잘 알려진 포트인 경우 시스템은 이 호스트를 responder로 간주합니다.

따라서 잘 알려진 포트는 1~1023 범위의 포트이거나 관리되는 디바이스에서 `/etc/sf/services`에 애플리케이션 프로토콜 정보를 포함하는 포트입니다.

NetFlow 데이터 분석 준비

라이센스: FireSIGHT

NetFlow 데이터 분석을 위해 FireSIGHT 시스템을 구성하기 전에, 사용하려는 라우터 또는 기타 NetFlow 지원 디바이스에서 NetFlow 기능을 활성화하고, 관리되는 디바이스의 센싱 인터페이스가 연결된 대상 네트워크로 NetFlow 버전 5 데이터를 내보내도록 디바이스를 구성해야 합니다.

시스템은 NetFlow 버전 5 및 NetFlow 버전 9 레코드를 모두 구문 분석할 수 있습니다. FireSIGHT 시스템 구축에서 NetFlow 지원 디바이스를 사용하려면, 해당 디바이스에서 이러한 버전 중 하나를 **반드시** 사용해야 합니다. 또한 시스템은 특정 필드를 템플릿에 포함할 것을 요구하며 NetFlow 지원 디바이스가 브로드캐스트하는 내용을 기록합니다. NetFlow 지원 디바이스에서 버전 9(사용자 지정 가능)를 사용 중인 경우, 디바이스에서 브로드캐스트하는 템플릿과 레코드에 다음 필드가 포함되어 있는지 **반드시** 확인해야 합니다(순서는 상관없음).

- IN_BYTES (1)
- IN_PKTS (2)
- PROTOCOL (4)
- TCP_FLAGS (6)
- L4_SRC_PORT (7)
- IPV4_SRC_ADDR (8)
- L4_DST_PORT (11)
- IPV4_DST_ADDR (12)
- LAST_SWITCHED (21)
- FIRST_SWITCHED (22)
- IPV6_SRC_ADDR (27)
- IPV6_DST_ADDR (28)

FireSIGHT 시스템은 관리되는 디바이스를 NetFlow 데이터 분석에 사용하므로, NetFlow 지원 디바이스를 모니터링할 수 있는 하나 이상의 관리되는 디바이스를 구축에 포함해야 합니다. 해당 관리되는 디바이스에 있는 하나 이상의 센싱 인터페이스를 NetFlow 지원 디바이스가 내보내는 데이터를 수집할 수 있는 네트워크에 연결해야 합니다. 관리되는 디바이스의 센싱 인터페이스에는 일반적으로 IP 주소가 없기 때문에 시스템은 NetFlow 레코드의 직접 수집을 지원하지 않습니다.

또한 Cisco에서는 모니터링되는 세션이 끝날 때에만 레코드를 출력하도록 NetFlow 지원 디바이스를 구성할 것을 **적극** 권장합니다. 고정된 간격으로 레코드를 출력하도록 NetFlow 지원 디바이스를 구성하는 경우 NetFlow 레코드에서 파생된 연결 데이터 분석이 좀 더 복잡해질 수 있습니다. 45-17페이지의 모니터링되는 세션마다 생성되는 연결 이벤트의 수을/를 참조하십시오.

끝으로, 일부 NetFlow 지원 디바이스에서 사용 가능한 Sampled NetFlow 기능은 디바이스를 통과하는 패킷의 하위 집합에 대해서만 NetFlow 통계를 수집합니다. 이 기능을 활성화하면 NetFlow 지원 디바이스에서 CPU 사용률이 향상될 수 있지만, 시스템에 의한 분석을 위해 수집하는 데이터에 영향을 줄 수 있습니다.

IOC 이해

라이센스: FireSIGHT

네트워크 검색의 일부로서, FireSIGHT 시스템의 Data Correlator는 다양한 유형의 데이터(침입 이벤트, 보안 인텔리전스, 연결 이벤트 또는 악성코드 이벤트)를 호스트와 연결하여, 모니터링되는 네트워크의 호스트가 악의적인 수단에 감염되었는지를 확인합니다. 이러한 상관관계를 IOC(indications of compromise)라고 합니다. 이 기능을 활성화하려면 검색 정책 편집기에서 이 기능 및 Cisco에서 사전 정의한 *IOC 규칙* 중 하나를 활성화합니다. 이 기능이 활성화되면 해당 호스트의 호스트 프로필에서 개별 호스트에 대한 규칙 상태도 수정할 수 있습니다. 각 IOC 규칙은 하나의 특정 *IOC 태그*에 해당하며, 이러한 태그는 호스트와 연결됩니다.

Data Correlator 외에도, Cisco의 엔드포인트 기반 종합 보안 인텔리전스 클라우드 데이터는 또한 IOC 규칙에서 IOC 태그를 생성할 수 있습니다. 이 데이터는 호스트 자체에 대한 활동(예: 개별 프로그램에 의해 또는 개별 프로그램에서 수행되는 작업)을 검토하므로, 네트워크 전용 데이터에서는 할 수 없는 위협 가능성에 대한 통찰력을 제공할 수 있습니다.엔드포인트의 FireAMP IOC 데이터는 Cisco 클라우드 연결을 통해 전송됩니다.

활성 IOC 태그의 호스트는 일반 호스트 아이콘( ) 대신 감염된 호스트 아이콘( )과 함께 이벤트 보기의 IP Address 열에 나타납니다. IOC 태그를 트리거할 수 있는 이벤트에 대한 이벤트 보기는 이벤트가 IOC를 트리거했는지 여부를 나타냅니다.

IOC 유형 이해

라이센스: FireSIGHT

다수의 IOC(indications of compromise) 규칙 및 태그 유형이 있습니다. 모두가 Cisco에서 사전 정의한 것이며, 한 IOC 규칙이 한 IOC 태그에 해당합니다. IOC 규칙은 FireSIGHT 시스템의 다른 기능(일부 이벤트의 경우 Cisco 클라우드)에서 제공된 데이터를 기반으로 트리거되므로 IOC 태그를 설정하려면 그러한 기능이 사용 가능해야 하며 IOC 규칙에 대해 활성 상태여야 합니다. Cisco에서 새로운 엔드포인트 기반 악성코드 이벤트 IOC 유형을 개발하면 시스템은 클라우드를 통해 이를 자동으로 다운로드하고 사용하기 시작합니다. 다음 목록에서는 IOC 규칙 유형, 관련된 기능 및 기타 추가 라이센싱 요구 사항(네트워크 검색에 필요한 FireSIGHT 라이센스 이상)에 대해 자세히 설명합니다.

- 45-20페이지의 엔드포인트 기반 악성코드 이벤트 IOC 유형
- 45-21페이지의 침입 이벤트 IOC 유형
- 45-22페이지의 보안 인텔리전스 이벤트 IOC 유형

엔드포인트 기반 악성코드 이벤트 IOC 유형

라이센스: FireSIGHT

다음 목록에는 Cisco 클라우드에 대한 서브스크립션이 필요한, 엔드포인트 기반 악성코드 이벤트와 연결된 IOC 유형의 예가 포함되어 있습니다. 아래에 나열된 IOC 유형 외에도 Cisco는 주기적으로 새 유형을 개발합니다. 시스템은 클라우드에 대한 연결을 통해 이러한 유형을 자동으로 다운로드 및 구현합니다.

엔드포인트 기반 악성코드 차단 구성에 대한 자세한 내용은 37-24페이지의 FireAMP를 위한 클라우드 연결 작업 및 37-8페이지의 네트워크 기반 AMP와 엔드포인트 기반 FireAMP 비교을/를 참조하십시오.

- Adobe Reader Compromise - Adobe Reader 실행 셸
- Adobe Reader Compromise - FireAMP에서 탐지된 PDF 손상
- CnC Connected - FireAMP에서 탐지된 의심스러운 봇넷
- Dropper Infection - FireAMP에서 탐지된 드로퍼 감염
- Excel Compromise - FireAMP에서 탐지된 Excel 손상
- Excel Compromise - Excel 실행 셸
- FireAMP에서 탐지된 일반 IOC
- Java Compromise - FireAMP에서 탐지된 Java 손상
- Java Compromise - Java 실행 셸
- Malware Detected - FireAMP에서 탐지된 위협 - 실행되지 않음
- Malware Detected - 파일 전송에서 탐지된 위협
- Malware Executed - FireAMP에서 탐지된 위협 - 실행됨
- Microsoft Calculator Compromise - FireAMP에서 탐지된 Microsoft 계산기 손상
- Microsoft Notepad Compromise - FireAMP에서 탐지된 Microsoft 메모장 손상
- PowerPoint Compromise - FireAMP에서 탐지된 PowerPoint 손상
- PowerPoint Compromise - PowerPoint 실행 셸
- QuickTime Compromise - FireAMP에서 탐지된 QuickTime 손상
- QuickTime Compromise - QuickTime 실행 셸
- Word Compromise - FireAMP에서 탐지된 Word 손상
- Word Compromise - Word 실행 셸

침입 이벤트 IOC 유형

라이센스: FireSIGHT+보호

다음 IOC 유형은 보호 라이센스가 필요한 침입 이벤트와 연결되어 있습니다. 침입 이벤트를 보고 침입 탐지 및 방지를 구성하는 방법에 대한 자세한 내용은 18-1페이지의 침입 정책 및 파일 정책을 사용하여 트래픽 제어 및 41-9페이지의 침입 이벤트 보기을/를 참조하십시오.

- CnC Connected - Intrusion Event - malware-backdoor
- CnC Connected - Intrusion Event - malware-cnc
- Exploit Kit - Intrusion Event - exploit-kit
- Impact 1 Attack - Impact 1 Intrusion Event - attempted-admin
- Impact 1 Attack - Impact 1 Intrusion Event - attempted-user
- Impact 1 Attack - Impact 1 Intrusion Event - successful-admin
- Impact 1 Attack - Impact 1 Intrusion Event - successful-user
- Impact 1 Attack - Impact 1 Intrusion Event - web-application-attack
- Impact 2 Attack - Impact 2 Intrusion Event - attempted-admin

- Impact 2 Attack - Impact 2 Intrusion Event - attempted-user
- Impact 2 Attack - Impact 2 Intrusion Event - successful-admin
- Impact 2 Attack - Impact 2 Intrusion Event - successful-user
- Impact 2 Attack - Impact 2 Intrusion Event - web-application-attack

보안 인텔리전스 이벤트 IOC 유형

라이센스: FireSIGHT+보호

지원되는 디바이스: Series 2를 제외한 모두

지원되는 Defense Center: DC500을 제외한 모든 방어 센터

CnC Connected - Security Intelligence Event - CnC 유형과 은 연결 이벤트 유형인 보안 인텔리전스 이벤트와 연결되어 있습니다. 보안 인텔리전스 기능에는 보호 라이센스가 필요합니다. 보안 인텔리전스를 구성하고 보안 인텔리전스 이벤트를 보는 방법에 대한 자세한 내용은 13-1페이지의 보안 인텔리전스 IP 주소 평판 블랙리스트에 추가 및 39-14페이지의 연결 및 보안 인텔리전스 데이터 보기을/를 참조하십시오.

IOC 데이터 보기 및 수정

라이센스: FireSIGHT

네트워크 검색 정책 자체 외에 FireSIGHT 시스템 웹 인터페이스의 기타 여러 부분에서 IOC(indications of compromise) 데이터를 보고 수정할 수 있습니다

- 대시보드에서는 Summary Dashboard의 Threats 탭에 시간이 지남에 따라 트리거되는 호스트 및 새 IOC 규칙별로 IOC 태그가 기본적으로 표시됩니다. Custom Analysis 위젯은 IOC 데이터를 기반으로 하는 사전 설정을 제공합니다. 자세한 내용은 55-1페이지의 대시보드 사용 및 55-15페이지의 Custom Analysis 위젯 구성을/를 참조하십시오.
- Context Explorer의 Indications of Compromise 섹션에는 IOC 카테고리별 호스트의 그래프 및 호스트별 IOC 카테고리의 그래프가 표시됩니다. 자세한 내용은 56-4페이지의 Indications of Compromise 섹션 이해을/를 참조하십시오.
- 검색(IOC), 연결, 보안 인텔리전스, 침입 및 악성코드 이벤트에 대한 이벤트 보기에서는 이벤트가 IOC 규칙을 트리거했는지 여부를 표시합니다(IOC 열에). IOC 규칙을 트리거하는 엔드포인트 기반 악성코드 이벤트는 이벤트 유형 FireAMP IOC를 포함하고 있으며, 감염을 지정하는 이벤트 하위 유형과 함께 나타납니다. 이벤트 뷰어에 나타나는 모든 IOC 데이터에 대해 규정 준수 규칙을 작성할 수 있습니다. 자세한 내용은 다음 절을 참조하십시오.
- 39-14페이지의 연결 및 보안 인텔리전스 데이터 보기
- 41-9페이지의 침입 이벤트 보기
- 40-17페이지의 악성코드 이벤트 작업
- 50-32페이지의 IOC 작업
- 51-1페이지의 상관관계 정책 및 규칙 구성
- 네트워크 맵의 Indications of Compromise 탭에는 모니터링되는 네트워크의 호스트가 IOC 태그로 그룹화되어 나열됩니다. 자세한 내용은 48-5페이지의 IOC 네트워크 맵 작업을/를 참조하십시오.
- 감염 가능성이 있는 호스트에 대한 호스트 프로필 보기에서는 해당 호스트와 연결된 모든 IOC 태그를 보고, IOC 태그의 일부 또는 전부를 확인하고, IOC 규칙 상태를 구성할 수 있습니다. 자세한 내용은 49-8페이지의 호스트 프로필에서 IOC 작업을/를 참조하십시오.

네트워크 검색 정책 생성

라이센스: FireSIGHT

방어 센터의 네트워크 검색 정책에서는 시스템이 조직의 네트워크 자산에서 데이터를 수집하는 방법과 모니터링해야 할 네트워크 세그먼트 및 포트를 제어합니다.

정책 내 검색 규칙은 FireSIGHT 시스템에서 트래픽의 네트워크 데이터를 기반으로 검색 데이터를 생성하기 위해 모니터링해야 할 네트워크 및 포트를 지정하며, 정책을 적용할 영역을 지정합니다. 규칙 내에서는 호스트, 애플리케이션 및 사용자의 검색 여부를 구성할 수 있습니다. 검색에서 네트워크와 영역을 제외하는 규칙을 생성할 수 있습니다. NetFlow 디바이스에서 검색할 규칙을 생성할 경우 연결만 기록하도록 선택할 수 있습니다.

네트워크 검색 정책에는 0.0.0.0/0 네트워크의 모든 IPv4 트래픽에서 애플리케이션을 검색하도록 구성된 단일 기본 규칙이 있습니다. 네트워크 검색 정책을 적용하려면 먼저 대상 디바이스에 액세스 제어 정책을 적용해야 합니다. 규칙에서 네트워크, 영역 또는 포트가 제외되지 않으며, 호스트와 사용자 검색 및 NetFlow 디바이스는 구성되지 않습니다. 관리되는 디바이스가 방어 센터에 등록되면 정책이 기본적으로 해당 디바이스에 적용됩니다. 호스트 또는 데이터 수집을 시작하려면, 검색 규칙을 추가 또는 수정하고 디바이스에 정책을 다시 적용해야 합니다.

액세스 제어 정책은 사용자가 허용하는 트래픽, 즉 네트워크 검색으로 모니터링할 수 있는 트래픽을 정의합니다. 따라서 액세스 제어를 사용하여 특정 트래픽을 차단하면 시스템은 해당 트래픽에서 호스트, 사용자 또는 애플리케이션 활동을 검토할 수 없습니다. 예를 들어, 액세스 제어 정책에서 소셜 네트워킹 애플리케이션에 대한 액세스를 차단하면 시스템에서 해당 애플리케이션에 대한 검색 데이터가 제공되지 않습니다.

네트워크 검색의 범위를 조정하려면 추가 검색 규칙을 생성하고 기본 규칙을 수정 또는 제거할 수 있습니다. NetFlow 디바이스에서 데이터 검색을 구성하고 네트워크에서 사용자 데이터가 검색되는 트래픽에 대한 프로토콜을 제한할 수 있습니다.

침입 탐지 및 방지를 수행하기 위해 FireSIGHT 시스템을 사용하되 검색 데이터를 활용할 필요가 없는 경우 새 검색을 비활성화하여 성능을 최적화할 수 있습니다. 먼저, 적용된 액세스 제어 정책에 사용자, 애플리케이션 또는 URL 조건의 규칙이 포함되어 있지 않은지 확인합니다. 그런 다음 네트워크 검색 정책에서 모든 규칙을 제거하고 관리되는 디바이스에 정책을 다시 적용합니다. 액세스 제어 규칙 구성에 대한 자세한 내용은 14-1페이지의 액세스 제어 규칙을 사용하여 트래픽 플로우 조정을/를 참조하십시오.

검색 규칙에서 사용자 검색을 활성화한 경우 애플리케이션 프로토콜 집합의 트래픽에서 사용자 로그인 활동을 통해 사용자를 탐지할 수 있습니다. 필요한 경우 모든 규칙에서 특정 프로토콜에서의 검색을 비활성화할 수 있습니다. 일부 프로토콜을 비활성화하면 FireSIGHT 라이센스와 연결된 사용자 제한에 도달하는 것을 방지하여, 다른 프로토콜의 사용자에 대해 사용할 수 있는 사용자 카운트를 확보할 수 있습니다.

고급 네트워크 검색 설정을 사용하면 어떤 데이터를 기록할지, 검색 데이터를 어떻게 저장할지, 어떤 IOC(indications of compromise) 규칙을 활성화할지, 영향 평가에 어떤 취약성 매핑을 사용할지, 소스에서 충돌하는 검색 데이터를 제공할 경우 어떤 일이 발생할지를 관리할 수 있습니다. 호스트 입력을 위해 NetFlow 디바이스 및 소스를 추가할 수도 있습니다.

자세한 내용은 다음 링크를 참고하십시오.

- 45-24페이지의 검색 규칙 작업
- 45-30페이지의 사용자 로깅 제한
- 45-31페이지의 고급 네트워크 검색 옵션 구성
- 45-38페이지의 네트워크 검색 정책 적용

검색 규칙 작업

라이센스: FireSIGHT

검색 규칙을 사용하면 원하는 특정 데이터만 포함하도록 네트워크 맵에 대해 검색되는 정보를 맞춤화할 수 있습니다. 네트워크 검색 정책의 규칙은 차례로 평가됩니다. 모니터링 기준을 중첩하여 규칙을 생성할 수 있지만 그렇게 하면 시스템 성능에 영향이 미칠 수 있습니다.

호스트 또는 네트워크를 모니터링에서 제외하면 해당 호스트 또는 네트워크는 네트워크 맵에 나타나지 않으며 그에 대한 이벤트도 보고되지 않습니다. Cisco에서는 로드 밸런서(또는 로드 밸런서의 특정 포트) 및 NAT 디바이스를 모니터링에서 제외할 것을 권장합니다. 이러한 디바이스는 잘못된 이벤트를 과도하게 생성하여 데이터베이스를 채우고 방어 센터에 과부하를 가져올 수 있습니다. 예를 들어, 모니터링되는 NAT 디바이스는 단기간에 운영 체제의 여러 업데이트를 표시할 수 있습니다. 로드 밸런서 및 NAT 디바이스의 IP 주소를 알고 있으면 모니터링에서 이들을 제외할 수 있습니다.

팁 시스템은 네트워크 트래픽을 검토하여 다수의 로드 밸런서 및 NAT 디바이스를 식별할 수 있습니다. 네트워크의 어떤 호스트가 로드 밸런서 및 NAT 디바이스인지 확인하려면 네트워크 검색 정책을 적용하고, 시스템이 네트워크 맵을 채울 때까지 기다린 다음, 호스트 유형을 제한하여 호스트 검색을 수행합니다.

또한 사용자 지정 서버 핑거프린트를 생성해야 할 경우, 핑거프린트 생성 중인 호스트와 통신하는 데 사용하는 IP 주소를 모니터링에서 일시적으로 제외해야 합니다. 그렇게 하지 않으면 네트워크 맵 및 검색 이벤트 보기가 해당 IP 주소로 표시되는 호스트에 대한 부정확한 정보와 뒤섞이게 됩니다. 핑거프린트를 생성한 후에는 IP 주소를 다시 모니터링하도록 정책을 구성할 수 있습니다. 자세한 내용은 46-11페이지의 서버 핑거프린트을/를 참조하십시오.

Cisco에서는 또한 NetFlow 지원 디바이스 및 FireSIGHT 시스템 관리되는 디바이스와 동일한 네트워크 세그먼트를 모니터링하지 **않을** 것을 권장합니다. 중첩되지 않는 규칙으로 네트워크 검색 정책을 구성하는 것이 이상적이지만, 시스템은 관리되는 디바이스에 의해 생성된 중복 연결 로그를 삭제합니다. 관리되는 디바이스 및 NetFlow 지원 디바이스 모두에서 탐지된 연결에 대한 중복 연결 로그는 삭제할 수 **없습니다**.

자세한 내용은 다음 절을 참조하십시오.

- 45-25페이지의 디바이스 선택 이해
- 45-25페이지의 작업 및 검색된 자산 이해
- 45-26페이지의 모니터링되는 네트워크 이해
- 45-26페이지의 네트워크 검색 정책의 영역 이해
- 45-26페이지의 포트 제외 이해
- 45-27페이지의 검색 규칙 추가
- 45-28페이지의 네트워크 객체 생성
- 45-29페이지의 포트 객체 생성

디바이스 선택 이해

라이센스: FireSIGHT

검색 규칙에서 NetFlow 디바이스를 선택하면, 지정된 네트워크에 대한 NetFlow 데이터의 검색으로 규칙이 제한됩니다. 규칙 동작의 다른 부분을 구성하기 전에 NetFlow 디바이스를 선택하십시오. NetFlow 디바이스를 선택하면 사용 가능한 규칙 작업이 변경되기 때문입니다. 또한 NetFlow 트래픽에 대해 포트 제외를 구성할 수 없습니다.

네트워크 검색 규칙에서 NetFlow 디바이스를 선택하려면 먼저 네트워크 검색 고급 설정에서 NetFlow 디바이스에 대한 연결을 구성해야 합니다. 자세한 내용은 45-35페이지의 NetFlow 지원 디바이스 추가을/를 참조하십시오.

작업 및 검색된 자산 이해

라이센스: FireSIGHT

검색 규칙을 구성할 때에는 규칙에 대한 작업을 선택해야 합니다. 작업은 시스템이 규칙을 처리할 때 검색 또는 제외할 자산을 결정합니다. 그러나 규칙 작업의 영향은 관리되는 디바이스 또는 NetFlow 지원 디바이스에서 데이터를 검색하는 데 규칙을 사용하는지 여부에 따라 달라집니다.

호스트 또는 사용자를 검색하는 규칙 없이 네트워크 검색 정책을 생성하는 경우, 정책을 적용하면 어플라이언스에 대해 새 검색이 비활성화됩니다. 침입 방지를 위해 관리되는 디바이스만을 사용하는 경우 성능을 최적화하려면, 정책에서 모든 검색 규칙을 제거한 다음 활성 디바이스에 정책을 다시 적용하십시오.

다음 표에서는 이러한 두 시나리오에서 지정된 작업 설정과 함께 규칙에 의해 어떤 자산이 검색되는지에 대해 설명합니다.

표 45-4 검색 규칙 작업

작업	관리되는 디바이스	NetFlow
제외	지정된 네트워크를 모니터링에서 제외합니다. 연결의 소스 또는 대상 호스트가 검색에서 제외되면 연결이 기록되기는 하지만 제외된 호스트에 대해 검색 이벤트가 생성되지 않습니다.	
검색: 호스트	검색 이벤트를 기반으로 호스트를 네트워크 맵에 추가합니다 (선택 사항, 사용자 검색이 활성화된 경우 필수.).	NetFlow 레코드를 기반으로 호스트를 네트워크 맵에 추가합니다. (필수)
검색: 애플리케이션	애플리케이션 탐지기를 기반으로 애플리케이션을 네트워크 맵에 추가합니다. 애플리케이션 검색 없이는 규칙에서 호스트 또는 사용자를 검색할 수 없습니다 (필수).	NetFlow 레코드 및 포트 애플리케이션 프로토콜 상관관계(`/etc/sf/services`)를 기반으로 애플리케이션 프로토콜을 네트워크 맵에 추가합니다. (선택 사항)
검색: 사용자	사용자를 사용자 테이블에 추가하고, 네트워크 검색 정책에 구성된 사용자 프로토콜과 일치하는 트래픽에서 탐지된 활동을 기반으로 사용자 활동을 기록합니다 (선택 사항).	해당 없음
NetFlow 연결 기록	해당 없음	NetFlow 연결만 기록합니다. 호스트나 애플리케이션은 검색하지 않습니다.

모니터링되는 네트워크 이해

라이센스: FireSIGHT

검색 규칙을 사용하면 지정된 네트워크의 호스트에서 나가고 들어오는 트래픽에서만 모니터링되는 자산의 검색이 이루어집니다. 검색 규칙에서는 모니터링할 네트워크 내 IP 주소에 대해서만 생성되는 이벤트와 함께, 지정된 네트워크 내에 하나 이상의 IP 주소를 가지고 있는 연결에 대해 검색이 이루어집니다. 기본 검색 규칙은 `0.0.0.0/0` 및 `::/0` 네트워크에서만 애플리케이션을 검색합니다.

지정된 NetFlow 디바이스 및 **Log Network Connections** 옵션이 활성화된 규칙의 경우, 지정된 네트워크의 IP 주소와의 연결도 기록됩니다. 네트워크 검색 규칙이 NetFlow 네트워크 연결을 기록하기 위한 유일한 방법입니다.

모니터링할 네트워크를 지정하기 위해 네트워크 객체 또는 객체 그룹을 사용할 수도 있습니다. 네트워크 검색 정책에서 사용되는 네트워크 객체를 수정하는 경우 검색에 변경 사항을 적용하려면 정책을 다시 적용해야 합니다.

네트워크 검색 정책의 영역 이해

라이센스: FireSIGHT

성능상의 이유로, 규칙의 영역이 규칙에서 모니터링할 네트워크에 물리적으로 연결된 관리되는 디바이스에 센싱 인터페이스를 포함하도록 각 검색 규칙을 구성해야 합니다.

그러나 네트워크 컨피그레이션 변경 사항에 대해 항상 지속적으로 알림을 받지는 못할 수도 있습니다. 네트워크 관리자는 별도의 알림 없이 라우팅 또는 호스트 변경을 통해 네트워크 컨피그레이션을 수정할 수 있으며, 이 경우 적절한 네트워크 검색 정책 컨피그레이션의 최신 상태를 유지하기가 어려울 수 있습니다. 관리되는 디바이스의 센싱 인터페이스가 네트워크에 어떻게 물리적으로 연결되어 있는지를 모르는 경우, 구축의 모든 영역에 검색 규칙을 적용하는 기본값으로 영역 컨피그레이션을 유지하십시오. (제외되는 영역이 없으면 검색 정책이 모든 영역에 적용됩니다.)

포트 제외 이해

라이센스: FireSIGHT

호스트를 모니터링에서 제외할 수 있는 것처럼(45-25페이지의 작업 및 검색된 자산 이해 참조), 특정 포트도 모니터링에서 제외할 수 있습니다.

예를 들면, 로드 밸런서는 짧은 기간에 동일한 포트에서 여러 애플리케이션을 보고할 수 있습니다. 포트를 모니터링에서 제외하도록 네트워크 검색 정책을 구성할 수 있습니다(예: 웹 팜을 처리하는 로드 밸런서의 포트 80 제외).

또 다른 시나리오로, 조직에서는 특정 포트 범위를 사용하는 사용자 지정 클라이언트를 사용할 수 있습니다. 이 클라이언트의 트래픽이 잘못된 이벤트를 과도하게 생성하면 해당 포트를 모니터링에서 제외할 수 있습니다. 마찬가지로, DNS 트래픽을 모니터링하지 않도록 결정할 수도 있습니다. 이 경우 포트 53을 모니터링하지 않도록 정책을 구성할 수 있습니다.

제외할 포트를 추가할 때 Available Ports 목록에서 재사용 가능한 포트 객체의 사용 여부를 결정하거나, 포트를 소스 또는 대상 제외 목록에 직접 추가하거나, 재사용 가능한 새 포트를 만든 다음 제외 목록으로 이동할 수 있습니다.

NetFlow 지원 디바이스의 경우 디바이스를 모니터링에서 제외하도록 구성할 수 없습니다.

검색 규칙 추가

라이센스: FireSIGHT

호스트 및 애플리케이션 데이터의 검색을 요구에 맞춤화하도록 검색 규칙을 구성할 수 있습니다. 규칙에서 참조되는 객체를 수정할 경우, 변경 사항을 적용하려면 네트워크 검색 정책을 다시 적용해야 합니다.

검색 규칙을 추가하려면

액세스: Admin/Discovery Admin

1단계 액세스 제어 정책을 점검하여, 네트워크 데이터를 검색하고자 하는 트래픽에 대해 필요에 따라 연결이 기록되고 있는지 확인합니다.

자세한 내용은 38-15페이지의 액세스 제어 처리 기반 연결 로깅을/를 참조하십시오. 대부분의 데이터를 검색하려면, 검색할 트래픽에 대한 연결의 끝에서 기록하십시오.

2단계 **Policies > Network Discovery**를 선택합니다.

Network Discovery Policy 페이지가 나타납니다.

3단계 **Add Rule**을 클릭합니다.

Add Rule 팝업 창이 나타납니다.

4단계 다음 2가지 옵션을 사용할 수 있습니다.

- NetFlow 트래픽을 모니터링하기 위한 규칙을 사용하려면 Add Rule 팝업 창에서 **NetFlow Device**를 클릭합니다.

  NetFlow Device 페이지가 나타납니다.

  NetFlow 디바이스를 검색 정책에 추가한 경우에만 NetFlow 디바이스를 이용할 수 있습니다. 자세한 내용은 45-35페이지의 NetFlow 지원 디바이스 추가을/를 참조하십시오.
- 관리되는 디바이스를 모니터링하는 규칙을 사용하려면 6단계로 건너뛰십시오.

자세한 내용은 45-17페이지의 NetFlow 및 FireSIGHT 데이터 간 차이점 및 45-25페이지의 디바이스 선택 이해을/를 참조하십시오.

5단계 사용할 NetFlow 디바이스의 IP 주소를 드롭다운 목록에서 선택합니다.

6단계 규칙에 대한 작업을 설정합니다.

- 규칙과 일치하는 모든 트래픽을 네트워크 검색에서 제외하려면 **Exclude**를 선택합니다. 이 규칙 작업을 선택하면 Port Exclusions 탭이 비활성화됩니다.
- 규칙과 일치하는 트래픽에서 선택한 데이터 유형을 검색하려면 **Discovery**를 선택한 다음 해당 데이터 유형 확인란을 선택하거나 선택 취소합니다.

  관리되는 디바이스 트래픽을 모니터링하는 경우 애플리케이션 로깅이 필요합니다. 사용자를 모니터링하는 경우 호스트 로깅이 필요합니다. NetFlow 트래픽을 모니터링하는 경우, 사용자 로깅은 이용할 수 없으며 애플리케이션 로깅은 선택 사항입니다.
- NetFlow 트래픽을 모니터링하는 경우 규칙을 사용하여 NetFlow 트래픽의 연결을 기록하려면 **Log NetFlow Connections**를 선택합니다. 규칙에서 NetFlow 디바이스를 선택해야만 이 옵션이 나타납니다.

참고 시스템은 네트워크 검색 정책 설정을 기반으로 NetFlow 트래픽에서 연결을 탐지합니다. 관리되는 디바이스 트래픽의 연결 로깅은 액세스 제어 정책에서 구성됩니다. 자세한 내용은 38-1페이지의 네트워크 트래픽의 연결 로깅을/를 참조하십시오.

규칙 작업 및 자산 검색에 대한 자세한 내용은 45-25페이지의 작업 및 검색된 자산 이해을/를 참조하십시오.

7단계 모든 검색 규칙에는 하나 이상의 네트워크를 포함해야 합니다. 선택적으로, 규칙 작업을 특정 네트워크로 제한하려면 **Networks** 탭을 클릭하고, **Available Networks** 목록에서 네트워크를 선택하고, **Add**를 클릭하거나, Networks 목록 아래에 네트워크를 입력하고 **Add**를 클릭합니다.

네트워크 모니터링에 대한 자세한 내용은 45-26페이지의 모니터링되는 네트워크 이해을/를 참조하십시오. Available Networks 목록에 네트워크 객체를 추가하는 방법에 대한 자세한 내용은 45-28페이지의 네트워크 객체 생성을/를 참조하십시오. 네트워크 검색 정책에서 사용되는 네트워크 객체를 수정하는 경우 검색에 변경 사항을 적용하려면 정책을 다시 적용해야 합니다.

8단계 선택적으로, 규칙 작업을 특정 영역의 트래픽으로 제한하려면 **Zones**를 클릭하고 **Available Zones** 목록에서 영역을 선택한 다음 **Add**를 클릭합니다.

모니터링할 영역 선택에 대한 자세한 내용은 45-26페이지의 네트워크 검색 정책의 영역 이해을/를 참조하십시오.

9단계 포트를 모니터링에서 제외하려면 **Port Exclusions**를 클릭합니다.

Port Exclusions 페이지가 나타납니다.

10단계 특정 소스 포트를 모니터링에서 제외하려면 두 가지 옵션을 이용할 수 있습니다.

- **Available Ports** 목록에서 포트를 선택하고 **Add to Source**를 클릭합니다.
- 포트 객체를 추가하지 않은 채 특정 소스 포트에서 트래픽을 제외하려면, **Selected Source Ports** 목록 아래 **Protocol** 드롭다운 목록에서 적절한 프로토콜을 선택하고, **Port** 필드에 1~65535의 포트 번호를 입력한 다음 **Add**를 클릭합니다.

  모니터링할 포트를 제외하는 방법에 대한 자세한 내용은 45-26페이지의 포트 제외 이해을/를 참조하십시오. Available Ports 목록에 포트 객체를 추가하는 방법에 대한 자세한 내용은 45-29페이지의 포트 객체 생성을/를 참조하십시오. 네트워크 검색 정책에서 사용되는 포트 객체를 수정하는 경우 검색에 변경 사항을 적용하려면 정책을 다시 적용해야 합니다.

11단계 특정 목적지 포트를 모니터링에서 제외하려면 두 가지 옵션을 이용할 수 있습니다.

- **Available Ports** 목록에서 포트를 선택하고 **Add to Destination**을 클릭합니다.
- 포트 객체를 추가하지 않은 채 특정 목적지 포트에서 트래픽을 제외하려면, **Selected Destination Ports** 목록 아래 **Protocol** 드롭다운 목록에서 적절한 프로토콜을 선택하고, **Port** 필드에 1~65535의 포트 번호를 입력한 다음 **Add**를 클릭합니다.

12단계 규칙 수정을 완료하면 **Save**를 클릭하여 검색 정책 규칙 목록으로 돌아갑니다.

변경 사항을 적용하려면 네트워크 검색 정책을 적용해야 합니다. 자세한 내용은 45-38페이지의 네트워크 검색 정책 적용을/를 참조하십시오.

네트워크 객체 생성

라이센스: FireSIGHT

검색 규칙에 나타나는 사용 가능한 네트워크의 목록에는 FireSIGHT 시스템의 어디서나 사용할 수 있는 재사용 가능한 네트워크 객체 및 그룹이 포함됩니다. 새 네트워크 객체를 목록에 추가할 수 있습니다. 규칙에서 참조되는 객체를 수정할 경우, 변경 사항을 적용하려면 네트워크 검색 정책을 다시 적용해야 합니다.

새 네트워크 객체를 생성하려면

Admin/Discovery Admin

1단계 **Policies > Network Discovery**를 선택합니다.

Network Discovery Policy 페이지가 나타납니다.

2단계 **Add Rule**을 클릭합니다.

Add Rule 팝업 창이 나타납니다.

3단계 Networks 페이지에서 추가 아이콘( )을 클릭합니다.

Network Objects 팝업 창이 나타납니다.

4단계 네트워크 객체의 **Name**을 입력합니다. 파이프(|) 또는 중괄호({})를 제외한 인쇄 가능한 표준 ASCII 문자를 사용할 수 있습니다.

5단계 네트워크 객체에 추가하고자 하는 각 IP 주소, CIDR 블록 및 접두사 길이에 대해 값을 입력하고 **Add**를 클릭합니다.

6단계 **Save**를 클릭하여 네트워크 객체를 Available Networks 목록에 추가합니다.

팁 네트워크가 목록에 즉시 나타나지 않으면 새로 고침 아이콘( )을 클릭하십시오.

포트 객체 생성

라이센스: FireSIGHT

검색 규칙에 나타나는 사용 가능한 포트의 목록에는 FireSIGHT 시스템의 어디서나 사용할 수 있는 재사용 가능한 포트 객체 및 그룹이 포함됩니다. 새 포트 객체를 목록에 추가할 수 있습니다. 규칙에서 참조되는 객체를 수정할 경우, 변경 사항을 적용하려면 네트워크 검색 정책을 다시 적용해야 합니다.

새 포트 객체를 생성하려면

Admin/Discovery Admin

1단계 **Port Exclusions**를 클릭합니다.

Port Exclusions 페이지가 나타납니다.

2단계 Available Ports 목록에 포트를 추가하려면 객체 추가 아이콘( )을 클릭합니다.

Port Objects 팝업 창이 나타납니다.

3단계 포트 객체의 **Name**을 입력합니다. 파이프(|) 또는 중괄호({})를 제외한 인쇄 가능한 표준 ASCII 문자를 사용할 수 있습니다.

4단계 제외할 트래픽의 프로토콜을 **Protocol** 필드에 지정합니다.

TCP, **UDP** 또는 **Other**를 선택하고, 드롭다운 목록에서 프로토콜 하나 또는 **All**을 선택합니다.

5단계 모니터링에서 제외할 포트를 **Port(s)** 필드에 입력합니다.

단일 포트를 지정할 수도 있고, 대시(-)를 사용하여 포트 범위를 지정하거나, 쉼표로 구분된 포트 목록 및 포트 범위를 지정할 수도 있습니다. 허용되는 값의 범위는 1~65535입니다.

6단계 **Save**를 클릭하여 포트를 Available Ports 목록에 추가합니다.

팁 포트가 목록에 즉시 나타나지 않으면 새로 고침 아이콘( )을 클릭하십시오.

사용자 로깅 제한

라이센스: FireSIGHT

사용자를 검색하는 규칙과 함께 네트워크 검색 정책을 적용하면 AIM, IMAP, LDAP, Oracle, POP3, SMTP, FTP, HTTP, MDNS 및 SIP 프로토콜을 사용하는 트래픽에서 사용자가 검색됩니다. 이러한 사용자는 Analysis 메뉴에서 액세스할 수 있는 사용자 테이블에 추가됩니다. 가장 완전한 사용자 정보를 제공할 수 있을 것 같은 사용자들에게 집중할 수 있도록 사용자 활동을 검색하는 프로토콜을 제한하여 탐지되는 총 사용자 수를 줄일 수 있습니다.

방어 센터가 저장할 수 있는 탐지된 총 사용자 수는 FireSIGHT 라이센스에 따라 다릅니다. 라이센스 제한에 도달하면 대부분의 경우 시스템은 데이터베이스에 대한 새 사용자 추가를 중지합니다. 새 사용자를 추가하려면 데이터베이스에서 오래된 사용자 또는 비활성 사용자를 수동으로 삭제하거나 모든 사용자를 삭제해야 합니다. 프로토콜 탐지를 제한하면 사용자 이름 혼란을 최소화하고 FireSIGHT 사용자 라이센스를 보존하는 데 도움이 됩니다.

예를 들어 AIM, POP3, IMAP 등의 프로토콜을 통해 사용자 이름을 가져오는 경우 계약직원, 방문자, 기타 손님 등의 네트워크 액세스 때문에 조직과 관련이 없는 사용자 이름이 포함될 수 있습니다.

또 다른 예로 AIM, Oracle 및 SIP 로그인은 외부 사용자 레코드를 생성할 수 있습니다. 이러한 로그인 유형은 LDAP 서버에서 시스템이 가져오는 사용자 메타데이터와도 연결되지 않고, 관리되는 디바이스에서 탐지하는 기타 로그인 유형에 포함된 정보와도 연결되지 않으므로 이 문제가 발생합니다. 따라서 방어 센터는 이러한 사용자를 다른 사용자 유형과 상호 연결할 수 없습니다.

관리되는 디바이스만이 비 LDAP 사용자 로그인을 탐지할 수 있다는 점에 유의하십시오. 사용자 활동을 탐지하는 데 Microsoft Active Directory 서버에 설치된 User Agents만 사용하는 경우 비 LDAP 로그인 제한은 효과가 없습니다. 또한 SMTP 로깅도 제한할 수 없습니다. 이는 사용자가 SMTP 로그인을 기반으로 데이터베이스에 추가되지 않기 때문입니다. 시스템이 SMTP 로그인을 탐지하더라도 데이터베이스에 일치하는 이메일 주소의 사용자가 이미 있지 않으면 로그인이 기록되지 않습니다.

LDAP, POP3, FTP 또는 IMAP 트래픽에서 탐지된 실패한 사용자 로그인에 대한 실패한 로그인 시도를 기록하도록 선택할 수 있습니다. 실패한 로그인 시도는 데이터베이스의 사용자 목록에 새 사용자를 추가하지 않습니다. User Agent는 실패한 로그인 활동을 보고하지 않습니다. 탐지된 실패한 활동에 대한 사용자 활동 유형은 Failed User Login입니다.

시스템은 실패한 HTTP 로그인과 성공한 HTTP 로그인을 구분할 수 없습니다. HTTP 사용자 정보를 보려면 **Capture Failed Login Attempts**를 활성화해야 합니다.

사용자 로그인이 탐지되는 프로토콜을 제한하려면

Admin/Discovery Admin

1단계 **Policies > Network Discovery**를 선택합니다.

Network Discovery Policy 페이지가 나타납니다.

2단계 **User**를 클릭합니다.

User 페이지가 나타납니다.

3단계 로그인을 탐지하려는 프로토콜에 대한 확인란을 선택하거나, 로그인을 탐지하지 않으려는 프로토콜에 대한 확인란을 선택 취소합니다.

4단계 선택적으로, LDAP, POP3, FTP 또는 IMAP 트래픽에서 탐지되는 실패한 로그인 시도를 기록하거나 HTTP 로그인에 대한 사용자 정보를 캡처하려면 **Capture Failed Login Attempts**를 활성화합니다.

5단계 **Save**를 클릭하여 네트워크 정책을 저장합니다.

변경 사항을 적용하려면 네트워크 검색 정책을 적용해야 합니다. 자세한 내용은 45-38페이지의 네트워크 검색 정책 적용을/를 참조하십시오.

고급 네트워크 검색 옵션 구성

라이센스: FireSIGHT

네트워크 검색 정책의 Advanced 탭에서는 어떤 이벤트를 탐지할지, 검색 데이터를 얼마 동안 보존하고 얼마나 자주 업데이트할지, 영향 상관관계에 어떤 취약성 매핑을 사용할지, 운영 체제 및 서버 ID 충돌을 어떻게 해결할지 등 정책 전반의 설정을 구성할 수 있습니다. 또한 다른 소스에서 데이터를 가져올 수 있도록 호스트 입력 소스 및 NetFlow 지원 디바이스를 추가할 수 있습니다.

검색 및 사용자 활동 이벤트에 대한 데이터베이스 이벤트 제한은 시스템 정책에서 설정합니다. 자세한 내용은 63-15페이지의 데이터베이스 이벤트 제한 구성을/를 참조하십시오.

고급 설정을 구성하려면

Admin/Discovery Admin

1단계 **Policies > Network Discovery**를 선택합니다.

Network Discovery Policy 페이지가 나타납니다.

2단계 **Advanced**를 클릭합니다.

Advanced 페이지가 나타납니다.

3단계 필요에 맞게 고급 설정을 수정합니다.

- 45-32페이지의 일반 설정 구성
- 45-32페이지의 ID 충돌 해결 구성
- 45-33페이지의 취약성 영향 평가 매핑 활성화
- 45-34페이지의 IOC 규칙 설정
- 45-35페이지의 NetFlow 지원 디바이스 추가
- 45-35페이지의 데이터 스토리지 구성
- 45-37페이지의 검색 이벤트 로깅 구성
- 45-37페이지의 ID 소스 추가

4단계 설정 구성을 완료하면 **Save**를 클릭하여 정책을 저장합니다.

5단계 정책이 완료 및 저장되면, 업데이트된 설정이 적용되도록 정책을 적용합니다. 자세한 내용은 45-38페이지의 네트워크 검색 정책 적용을/를 참조하십시오.

일반 설정 구성

라이센스: FireSIGHT

일반 설정은 네트워크 맵에서 시스템이 정보를 업데이트하는 빈도 및 검색 중 서버 배너의 캡처 여부를 제어합니다.

배너 캡처

시스템이 서버 공급업체 및 버전("배너")을 광고하는 네트워크 트래픽에서 헤더 정보를 저장하도록 하려면 이 확인란을 선택합니다. 이 정보는 수집하는 정보에 추가 컨텍스트를 제공할 수 있습니다. 서버 세부사항에 액세스하여 호스트에 대해 수집된 서버 배너에 액세스할 수 있습니다.

업데이트 간격

호스트의 IP 주소 중 하나가 마지막으로 표시된 시간, 애플리케이션이 사용된 시간 또는 애플리케이션의 히트 수 등의 정보를 시스템이 업데이트하는 간격. 기본 설정은 3600초(1시간)입니다.

업데이트 시간 초과의 간격을 더 낮게 설정하면 호스트 표시에 더 정확한 정보가 제공되지만, 네트워크 이벤트가 더 많이 생성됩니다.

일반 설정을 업데이트하려면

Admin/Discovery Admin

1단계 **General Settings** 옆의 수정 아이콘( )을 클릭합니다.

General Settings 팝업 창이 나타납니다.

2단계 필요에 맞게 설정을 수정합니다.

3단계 **Save**를 클릭하여 일반 설정을 저장하고 네트워크 검색 정책의 Advanced 탭으로 돌아갑니다.

변경 사항을 적용하려면 네트워크 검색 정책을 적용해야 합니다. 자세한 내용은 45-38페이지의 네트워크 검색 정책 적용을/를 참조하십시오.

ID 충돌 해결 구성

라이센스: FireSIGHT

시스템은 트래픽의 패턴을 기준으로 운영 체제 및 서버의 핑거프린트가 일치하는지를 검토하여, 특정 호스트에서 어떤 운영 체제와 애플리케이션이 실행 중인지 확인합니다. 가장 신뢰할 수 있는 운영 체제 및 서버 ID 정보를 제공하기 위해 시스템은 여러 소스에서 온 핑거프린트 정보를 맞춰봅니다.

시스템은 운영 체제 ID를 도출하고 신뢰도 값을 할당하기 위해 모든 수동 데이터를 사용합니다. 현재 ID 및 시스템이 현재 ID를 선택하는 방법에 대한 자세한 내용은 46-4페이지의 네트워크 맵 향상을/를 참조하십시오.

기본적으로 ID 충돌이 없으면, 스캐너 또는 서드파티 애플리케이션에 의해 추가된 ID 데이터가 FireSIGHT 시스템에 의해 탐지된 ID 데이터를 재정의합니다. 우선순위별로 스캐너 및 서드파티 애플리케이션 핑거프린트 소스의 순위를 매기려면 Identity Sources 설정을 사용할 수 있습니다. 시스템은 각 소스에 대해 하나의 ID를 보유하지만, 우선순위가 가장 높은 서드파티 애플리케이션 또는 스캐너 소스의 데이터만 현재 ID로 사용됩니다. 그러나 우선순위와 상관없이 사용자 입력 데이터가 스캐너 및 서드파티 애플리케이션 데이터를 재정의한다는 점에 유의하십시오.

시스템이 Identity Sources 설정에 나열된 활성 스캐너나 서드파티 애플리케이션 소스 또는 FireSIGHT 시스템 사용자에게서 온 기존 ID와 충돌하는 ID를 탐지하면 ID 충돌이 발생합니다. 기본적으로 ID 충돌은 자동으로 해결되지 않으므로, 호스트 프로필을 통해 또는 호스트를 다시 스캔하거나 새 ID 데이터를 다시 추가하여 수동 ID를 재정의함으로써 충돌을 해결해야 합니다. 그러나 항상 수동 ID를 유지하여 충돌을 자동으로 해결하거나, 항상 능동 ID를 유지하여 해결하도록 시스템을 설정할 수 있습니다.

Generate Identity Conflict Event

네트워크 맵의 호스트에서 ID 충돌이 발생할 때 이벤트를 생성하도록 하려면 이 옵션을 활성화합니다.

Automatically Resolve Conflicts

다음 옵션을 이용할 수 있습니다.

- ID 충돌을 수동으로 해결하려면 **Automatically Resolve Conflicts** 드롭다운 목록에서 **Disabled**를 선택합니다.
- ID 충돌이 발생할 때 수동 핑거프린트를 사용하려면 **Automatically Resolve Conflicts** 드롭다운 목록에서 **Identity**를 선택합니다.
- ID 충돌이 발생할 경우 우선순위가 가장 높은 활성 소스의 현재 ID를 사용하려면 **Automatically Resolve Conflicts** 드롭다운 목록에서 **Keep Active**를 선택합니다.

ID 충돌 해결 설정을 업데이트하려면

Admin/Discovery Admin

1단계 **Identity Conflict Settings** 옆의 수정 아이콘( )을 클릭합니다.

Edit Identity Conflict Settings 팝업 창이 나타납니다.

2단계 필요에 맞게 설정을 수정합니다.

3단계 **Save**를 클릭하여 ID 충돌 설정을 저장하고 네트워크 검색 정책의 **Advanced** 탭으로 돌아갑니다.

변경 사항을 적용하려면 네트워크 검색 정책을 적용해야 합니다. 자세한 내용은 45-38페이지의 네트워크 검색 정책 적용을/를 참조하십시오.

취약성 영향 평가 매핑 활성화

라이센스: FireSIGHT

FireSIGHT 시스템에서 침입 이벤트로 영향 상관관계를 수행하는 방법을 구성할 수 있습니다. 다음 옵션을 사용할 수 있습니다.

- 시스템 기반 취약성 정보를 사용하여 영향 상관관계를 수행하려면 **Use Network Discovery Vulnerability Mappings**를 선택합니다.
- 서드파티 취약성 참조를 사용하여 영향 상관관계를 수행하려면 **Use Third-Party Vulnerability Mappings**를 선택합니다. 자세한 내용은 46-33페이지의 서드파티 취약성 매핑 또는 *FireSIGHT 시스템 Host Input API Guide*를 참조하십시오.

확인란 중 하나를 선택할 수도 있고 둘을 모두 선택할 수도 있습니다. 시스템이 침입 이벤트를 생성하며 선택한 취약성 매핑 집합의 취약성과 함께 이벤트 관련 호스트에 서버나 운영 체제가 있는 경우, 침입 이벤트는 Vulnerable (level 1: red) 영향 아이콘으로 표시됩니다. 공급업체 또는 버전 정보가 없는 서버의 경우 시스템 정책에서 취약성 매핑을 구성해야 합니다. 자세한 내용은 63-30페이지의 서버에 대한 취약성 매핑을/를 참조하십시오.

두 확인란을 모두 선택 취소한 경우 침입 이벤트는 Vulnerable (level 1: red) 영향 아이콘으로 표시되지 **않습니다**. 자세한 내용은 41-38페이지의 이벤트를 평가하기 위한 영향 레벨 사용을/를 참조하십시오.

취약성 설정을 업데이트하려면

Admin/Discovery Admin

1단계 **Vulnerabilities to use for Impact Assessment** 옆의 수정 아이콘()을 클릭합니다.

Edit Vulnerability Settings 팝업 창이 나타납니다.

2단계 필요에 맞게 설정을 수정합니다.

3단계 **Save**를 클릭하여 취약성 설정을 저장하고 네트워크 검색 정책의 Advanced 탭으로 돌아갑니다.

변경 사항을 적용하려면 네트워크 검색 정책을 적용해야 합니다. 자세한 내용은 45-38페이지의 네트워크 검색 정책 적용을/를 참조하십시오.

IOC 규칙 설정

라이센스: FireSIGHT

시스템에서 IOC(indications of compromise)를 탐지하고 태그하도록 하려면 먼저 검색 정책에서 하나 이상의 IOC 규칙을 활성화해야 합니다. 각 IOC 규칙은 한 유형의 IOC 태그에 해당하며 모든 IOC 규칙은 Cisco에서 사전 정의합니다. 원래 규칙은 사용자가 생성할 수 없습니다. 네트워크 및 조직의 필요에 따라 규칙의 일부 또는 전체를 활성화할 수 있습니다. 예를 들어, Microsoft Excel과 같은 소프트웨어를 사용하는 호스트가 모니터링되는 네트워크에 나타나지 않으면 Excel 기반 위협에 해당하는 IOC 태그를 활성화하지 않을 수 있습니다. IOC 기능에 대한 자세한 내용은 45-20페이지의 IOC 이해을/를 참조하십시오.

활성화한 IOC 규칙과 연결된 FireSIGHT 시스템 기능(예: 침입 및 악성코드 차단)을 활성화해야 합니다. 규칙과 연결된 기능을 활성화하지 않으면 관련 데이터가 수집되지 않으며 규칙을 트리거할 수 없습니다. IOC 규칙 유형 및 관련 기능에 대한 자세한 내용은 45-20페이지의 IOC 유형 이해을/를 참조하십시오.

검색 정책에서 IOC 규칙을 설정하려면

Admin/Discovery Admin

1단계 **Indications of Compromise Settings** 옆에 있는 수정 아이콘()을 클릭합니다.

Edit Indications of Compromise Settings 팝업 창이 나타납니다.

2단계 전체 IOC 기능을 설정 또는 해제하려면 **Enable IOC** 옆에 있는 슬라이더를 클릭합니다.

3단계 개별 IOC 규칙을 활성화 또는 비활성화하려면 규칙의 **Enabled** 열에 있는 슬라이더를 클릭합니다.

4단계 **Save**를 클릭하여 IOC 규칙 설정을 저장하고 검색 정책의 Advanced 탭으로 돌아갑니다.

변경 내용이 저장되었습니다.

변경 사항을 적용하려면 네트워크 검색 정책을 적용해야 합니다. 자세한 내용은 45-38페이지의 네트워크 검색 정책 적용을/를 참조하십시오.

NetFlow 지원 디바이스 추가

라이센스: FireSIGHT

NetFlow 지원 디바이스에서 NetFlow 기능을 활성화한 경우, 이러한 디바이스에서 내보낸 연결 데이터를 사용하여 Cisco 디바이스에서 수집한 연결 데이터를 보완할 수 있습니다.

검색 규칙에서 이러한 데이터를 사용할 수 있으려면 먼저 사용하고자 하는 NetFlow 지원 디바이스를 구성한 다음(45-19페이지의 NetFlow 데이터 분석 준비 참조) 네트워크 검색 정책에 추가해야 합니다.

FireSIGHT 시스템에서 NetFlow 데이터를 사용하는 방법 및 추가 전제 조건에 대한 자세한 내용은 45-16페이지의 NetFlow 이해을/를 참조하십시오.

연결 데이터 수집을 위해 NetFlow 지원 디바이스를 추가하려면

Admin/Discovery Admin

1단계 **Policies > Network Discovery**를 선택합니다.

Network Discovery Policy 페이지가 나타납니다.

2단계 **Advanced**를 클릭합니다.

Advanced 페이지가 나타납니다.

3단계 NetFlow Devices 옆의 추가 아이콘( )을 클릭합니다.

Add NetFlow Device 팝업 창이 나타납니다.

4단계 연결 데이터를 수집하는 데 사용할 NetFlow 지원 디바이스의 IP 주소를 **IP Address** 필드에 입력합니다.

5단계 NetFlow 지원 디바이스를 더 추가하려면 3단계와 4단계를 반복합니다.

팁 NetFlow 지원 디바이스를 제거하려면 제거하려는 디바이스 옆의 삭제 아이콘( )을 클릭합니다. 검색 규칙에서 NetFlow 지원 디바이스를 사용하는 경우, Advanced 페이지에서 디바이스를 삭제하려면 먼저 규칙을 삭제해야 합니다. 자세한 내용은 45-24페이지의 검색 규칙 작업을/를 참조하십시오.

6단계 **Save**를 클릭합니다.

디바이스가 NetFlow 지원 디바이스의 목록에 나타납니다.

변경 사항을 적용하려면 네트워크 검색 정책을 적용해야 합니다. 자세한 내용은 45-38페이지의 네트워크 검색 정책 적용을/를 참조하십시오.

데이터 스토리지 구성

라이센스: FireSIGHT

데이터 스토리지 설정은 데이터베이스에 저장되는 데이터의 종류를 제어하며, 따라서 FireSIGHT 시스템이 사용할 수 있는 데이터를 결정합니다. 이러한 설정은 네트워크 맵에 데이터를 보유하는 기간도 제어합니다.

다음 옵션은 네트워크 검색 데이터 스토리지 설정을 구성합니다.

When Host Limit Reached

방어 센터가 호스트 제한에 도달할 때(FireSIGHT 라이센스에 의해 결정됨) 그리고 네트워크 맵이 가득 찰 때 호스트가 처리되는 방법을 제어할 수 있습니다. 이 옵션은 스푸핑된 호스트가 네트워크 맵에서 유효한 호스트를 대신하지 않도록 하려는 경우 특히 유용합니다. 오래된 호스트를 삭제하려면 **When Host Limit Reached** 드롭다운 목록에서 **Drop hosts**를 선택합니다. 새 호스트를 삭제하려면 **When Host Limit Reached** 드롭다운 목록에서 **Don't insert new hosts**를 선택합니다. 자세한 내용은 65-8페이지의 FireSIGHT 호스트 및 사용자 라이센스 제한 이해을/를 참조하십시오.

Host Timeout

시스템이 비활성화 상태의 호스트를 네트워크 맵에서 삭제하기까지의 경과 시간(분 단위). 기본 설정은 10080분(7일)입니다. 개별 호스트 IP 주소 및 MAC 주소는 개별적으로 시간 초과될 수 있지만, 관련된 모든 주소가 시간 초과되기 전에는 호스트가 네트워크 맵에서 사라지지 않습니다.

호스트의 조기 시간 초과를 방지하려면 호스트 시간 초과 값이 네트워크 검색 정책의 업데이트 간격보다 긴지 확인하십시오. 업데이트 간격에 대한 자세한 내용은 45-32페이지의 일반 설정 구성을/를 참조하십시오.

Server Timeout

시스템이 비활성화 상태의 서버를 네트워크 맵에서 삭제하기까지의 경과 시간(분 단위). 기본 설정은 10080분(7일)입니다.

서버의 조기 시간 초과를 방지하려면 서비스 시간 초과 값이 네트워크 검색 정책의 업데이트 간격보다 긴지 확인하십시오. 자세한 내용은 45-32페이지의 일반 설정 구성을/를 참조하십시오.

Client Application Timeout

시스템이 비활성화 상태의 클라이언트를 네트워크 맵에서 삭제하기까지의 경과 시간(분 단위). 기본 설정은 10080분(7일)입니다.

클라이언트 시간 초과 값이 네트워크 검색 정책의 업데이트 간격보다 긴지 확인하십시오. 자세한 내용은 45-32페이지의 일반 설정 구성을/를 참조하십시오.

데이터 스토리지 설정을 업데이트하려면

Admin/Discovery Admin

1단계 **Data Storage Settings** 옆의 수정 아이콘( )을 클릭합니다.

Data Storage Settings 팝업 창이 나타납니다.

2단계 필요에 맞게 설정을 수정합니다.

3단계 **Save**를 클릭하여 데이터 스토리지 설정을 저장하고 네트워크 검색 정책의 Advanced 탭으로 돌아갑니다.

변경 사항을 적용하려면 네트워크 검색 정책을 적용해야 합니다. 자세한 내용은 45-38페이지의 네트워크 검색 정책 적용을/를 참조하십시오.

검색 이벤트 로깅 구성

라이센스: FireSIGHT

Event Logging Settings는 검색 및 호스트 입력 이벤트의 로깅 여부를 제어합니다. 이벤트를 기록하지 않으면 이벤트 보기에서 검색할 수 없거나, 상관관계 규칙을 트리거하는 데 사용할 수 없습니다.

이벤트 로깅 설정을 구성하려면

Admin/Discovery Admin

1단계 **Event Logging Settings** 옆의 수정 아이콘()을 클릭합니다.

Event Logging Settings 팝업 창이 나타납니다.

2단계 데이터베이스에 기록할 검색 및 호스트 입력 이벤트 유형 옆에 있는 확인란을 선택하거나 선택 취소합니다. 각 이벤트 유형에 대해 자세히 알아보려면 50-9페이지의 검색 이벤트 유형 이해 및 50-13페이지의 호스트 입력 이벤트 유형 이해을/를 참조하십시오.

3단계 **Save**를 클릭하여 이벤트 로깅 설정을 저장하고 네트워크 검색 정책의 Advanced 탭으로 돌아갑니다.

변경 사항을 적용하려면 네트워크 검색 정책을 적용해야 합니다. 자세한 내용은 45-38페이지의 네트워크 검색 정책 적용을/를 참조하십시오.

ID 소스 추가

라이센스: FireSIGHT

이 페이지를 통해 새 활성 소스를 추가하거나, 기존 소스에 대한 우선순위 또는 시간 초과 설정을 변경할 수 있습니다. 이 페이지에 스캐너를 추가한다고 해서 Nmap 스캐너에 대해 존재하는 모든 통합 기능이 추가되지는 않지만, 가져온 서드파티 애플리케이션 또는 스캔 결과를 통합하는 것은 가능합니다. 서드파티 애플리케이션 또는 스캐너에서 데이터를 가져오는 경우 소스의 취약성을 네트워크 맵의 취약성에 매핑해야 합니다. 자세한 내용은 46-33페이지의 서드파티 취약성 매핑을/를 참조하십시오.

ID 소스를 추가하려면

Admin/Discovery Admin

1단계 **OS and Server Identity Sources** 옆의 수정 아이콘()을 클릭합니다.

Edit OS and Server Identity Sources 팝업 창이 나타납니다.

2단계 새 소스를 추가하려면 **Add Source**를 클릭합니다.

Add Identity Source 팝업 창이 나타납니다.

3단계 소스의 **Name**을 입력합니다.

4단계 **Type** 드롭다운 목록에서 입력 소스 유형을 선택합니다.

- AddScanResult 기능을 사용하여 스캔 결과를 가져오려면 **Scanner**를 선택합니다.
- 스캔 결과를 가져오지 않으려는 경우 **Application**을 선택합니다.

5단계 이 소스가 네트워크 맵에 ID가 추가되는 시간과 해당 ID가 삭제되는 시간 사이의 간격을 지정하려면 **Timeout** 드롭다운 목록에서 **Hours**, **Days** 또는 **Weeks**를 선택하고 적절한 기간을 입력합니다.

팁 추가한 소스를 삭제하려면 소스 옆의 삭제 아이콘( )을 클릭합니다.

6단계 선택적으로, 특정 소스를 승격하여 운영 체제 및 애플리케이션 ID가 목록에서 그 아래에 있는 소스에 사용되도록 하려면, 해당 소스를 선택하고 위쪽 화살표를 클릭합니다.

7단계 선택적으로, 특정 소스를 강등하여 목록에서 그 위에 있는 소스가 제공하는 ID가 없는 경우에만 운영 체제 및 애플리케이션 ID가 사용되도록 하려면, 해당 소스를 선택하고 아래쪽 화살표를 클릭합니다.

8단계 **Save**를 클릭하여 ID 소스 설정을 저장하고 네트워크 검색 정책의 Advanced 탭으로 돌아갑니다.

변경 사항을 적용하려면 네트워크 검색 정책을 적용해야 합니다. 자세한 내용은 45-38페이지의 네트워크 검색 정책 적용을/를 참조하십시오.

네트워크 검색 정책 적용

라이센스: FireSIGHT

기본적으로 네트워크 검색 정책은 관리되는 디바이스(방어 센터로 등록된 경우)의 대상 영역에 적용됩니다. 네트워크 검색 정책을 적용하면 시스템은 사양에 따라 네트워크 모니터링을 시작할 수 있습니다. 네트워크 검색 정책을 변경하는 경우 변경 사항을 적용하려면 정책을 다시 적용해야 합니다.

네트워크 검색 정책을 다시 적용하면

- 시스템은 모니터링되는 네트워크의 호스트에 대한 네트워크 맵에서 MAC 주소, TTL 및 홉 정보를 삭제한 후 다시 검색합니다.
- 영향받는 관리되는 디바이스는 아직 방어 센터로 전송되지 않은 검색 데이터를 삭제합니다.

네트워크 검색 정책을 적용할 때에는 방어 센터에서 관리하는 모든 디바이스에 액세스 제어 정책을 이미 적용했는지 확인하십시오. 액세스 제어 정책을 각 디바이스에 적용하지 않은 경우 네트워크 검색 정책 적용이 실패합니다. FireSIGHT 라이센스가 설치되지 않은 방어 센터에서는 네트워크 검색 정책을 적용할 수 없습니다.

네트워크 검색 정책에서 사용되는 네트워크 또는 포트 객체를 수정하는 경우 검색에 변경 사항을 적용하려면 정책을 다시 적용해야 합니다.

FireSIGHT 시스템의 서로 다른 버전을 실행하는(예: 디바이스 중 하나에 대한 업그레이드가 실패한 경우) 스태킹된 디바이스에는 네트워크 검색 정책을 적용할 수 없습니다.

네트워크 검색 정책을 적용하려면

Admin/Security Approver

1단계 **Policies > Network Discovery**를 선택합니다.

Network Discovery Policy 페이지가 나타납니다.

2단계 **Apply**을 클릭합니다.

방어 센터에서 액세스 제어 정책의 대상이 되는 모든 영역에 정책을 적용할 것인지 확인하는 메시지가 나타납니다.

3단계 정책을 적용하려면 **Yes**를 클릭합니다.

46장

네트워크 검색 향상

FireSIGHT 시스템에서 수집하는 네트워크 트래픽에 대한 정보는 시스템이 이 정보를 연계하여 가장 소중하고 가장 중요한 네트워크의 호스트를 식별할 때 가장 가치 있게 사용됩니다.

예를 들어 SuSE Linux의 사용자 지정 버전을 실행하는 디바이스가 네트워크에 여러 개 있는 경우 시스템은 해당 운영 체제를 식별할 수 없으므로 호스트에 취약성을 매핑할 수 없습니다. 그러나 시스템에 SuSE Linux에 대한 취약성 목록이 있음을 알고 있다면, 호스트 중 하나에 대한 사용자 지정 핑거프린트를 생성한 다음 동일한 운영 체제를 실행하는 다른 호스트의 식별에 이를 사용할 수 있습니다. 핑거프린트에 SuSE Linux에 대한 취약성 목록의 매핑을 포함하여, 해당 목록을 핑거프린트와 일치하는 각 호스트와 연결할 수 있습니다.

호스트 입력 기능을 사용하여 서드파티 시스템의 호스트 데이터를 네트워크 맵에 직접 입력할 수도 있습니다. 그러나 서드파티 운영 체제나 애플리케이션 데이터는 취약성 정보에 자동으로 매핑되지 않습니다. 서드파티 운영 체제, 서버 및 애플리케이션 프로토콜 데이터를 사용하여 호스트에 대한 취약성을 보고 영향 상관관계를 수행하려면, 서드파티 시스템의 공급업체 및 버전 정보를 VDB(취약성 데이터베이스)에 나열된 공급업체 및 버전에 매핑해야 합니다. 호스트 입력 데이터를 지속적으로 유지 관리할 수도 있습니다. 애플리케이션 데이터를 FireSIGHT 시스템 공급업체 및 버전 정의에 매핑해도, 가져온 서드파티 취약성은 클라이언트 또는 웹 애플리케이션에 대한 영향 평가에 사용되지 않습니다.

시스템이 네트워크의 호스트에서 실행되는 애플리케이션 프로토콜을 식별할 수 없는 경우, 포트나 패턴을 기반으로 시스템이 애플리케이션을 식별하도록 하는 사용자 정의 애플리케이션 프로토콜 탐지기를 생성할 수 있습니다. 특정 애플리케이션 탐지기를 가져오고 활성화 및 비활성화하여 FireSIGHT 시스템의 애플리케이션 탐지 기능을 한층 더 맞춤화할 수 있습니다.

Nmap 활성 스캐너의 스캔 결과를 사용하여 운영 체제 및 애플리케이션 데이터의 탐지를 교체하거나 취약성 목록을 서드파티 취약성으로 보강할 수도 있습니다. 시스템에서는 애플리케이션의 ID를 확인하기 위해 여러 소스의 데이터를 조정할 수 있습니다. 시스템에서 이를 수행하는 방법에 대한 자세한 내용은 46-5페이지의 현재 ID 이해을/를 참조하십시오. 활성 스캐닝에 대한 자세한 내용은 47-1페이지의 활성 스캐닝 구성을/를 참조하십시오.

자세한 내용은 다음 절을 참조하십시오.

탐지 전략 평가

라이센스: FireSIGHT

시스템의 기본 탐지 기능을 변경하려면 먼저 어떤 호스트가 올바르게 식별되지 않는지, 그 이유가 무엇인지를 분석해야 합니다. 그래야만 어떤 해결책을 구현할지 결정할 수 있습니다. 결정을 내리기 위한 지침으로 다음을 사용하십시오.

관리되는 디바이스의 배치가 올바릅니까?

라이센스: FireSIGHT

로드 밸런서, 프록시 서버 또는 NAT 디바이스 같은 네트워크 디바이스가 관리되는 디바이스 및 식별되지 않는/잘못 식별된 호스트 사이에 상주하는 경우, 사용자 지정 핑거프린트를 사용하기보다는 관리되는 디바이스를 잘못 식별된 호스트에 더 가까이 두십시오. Cisco에서는 이 시나리오에서 사용자 지정 핑거프린트의 사용을 권장하지 않습니다.

식별되지 않은 운영 체제에 고유한 TCP 스택이 있습니까?

라이센스: FireSIGHT

시스템에서 호스트를 잘못 식별하면 호스트가 잘못 식별된 이유를 조사하여, 사용자 지정 핑거프린트를 생성 및 활성화할지 아니면 검색 데이터 대신 Nmap 또는 호스트 입력 데이터를 사용할지를 결정해야 합니다.

주의 잘못 식별된 호스트를 발견하면 사용자 지정 핑거프린트를 생성하기 전에 먼저 지원 부서에 문의하십시오.

기본적으로 호스트가 시스템에서 탐지되지 않는 운영 체제를 실행 중이며 TCP 스택 특성 파악 내용을 기존의 탐지된 운영 체제와 공유하지 않는 경우에는 사용자 지정 핑거프린트를 생성해야 합니다.

예를 들어 시스템이 식별할 수 없는 고유한 TCP 스택의 사용자 지정된 Linux 버전을 가지고 있는 경우 사용자 지정 핑거프린트를 생성하면 도움이 될 수 있습니다. 이렇게 하면 시스템은 스캔 결과나 서드파티 데이터를 사용하는 대신 호스트를 식별하고 지속적으로 모니터링할 수 있습니다. 이 경우 사용자가 직접 지속적, 능동적으로 데이터를 업데이트해야 합니다.

많은 오픈 소스 Linux 배포에서 동일한 커널이 사용되며, 시스템은 Linux 커널 이름을 사용하여 이들을 식별합니다. Red Hat Linux 시스템에 대해 사용자 핑거프린트를 생성하는 경우, 동일한 핑거프린트가 여러 Linux 배포 제품과 일치하기 때문에 다른 운영 체제(예: Debian Linux, Mandrake Linux, Knoppix 등)도 Red Hat Linux로 표시될 수 있습니다.

모든 상황에 핑거프린트를 사용해서는 안 됩니다. 예를 들어 호스트의 TCP 스택이 다른 운영 체제와 유사하거나 동일하게 수정되었을 수 있습니다. 예를 들어 Apple Mac OS X 호스트가 변경되어 해당 핑거프린트가 Linux 2.4 호스트와 동일해지면 시스템은 Mac OS X을 Linux 2.4로 식별하게 됩니다. Mac OS X 호스트용 사용자 지정 핑거프린트를 생성하는 경우 올바른 모든 Linux 2.4 호스트가 Mac OS X 호스트로 잘못 식별될 수 있습니다. 이 경우 Nmap이 호스트를 올바르게 식별하면 해당 호스트에 대해 주기적인 Nmap 스캔을 예약할 수 있습니다.

호스트 입력을 사용하여 서드파티 시스템의 데이터를 가져오는 경우, 서드파티가 서버 및 애플리케이션 프로토콜을 설명하는 데 사용하는 공급업체, 제품 및 버전 문자열을 해당 제품의 Cisco 정의에 매핑해야 합니다. 자세한 내용은 46-30페이지의 서드파티 제품 매핑 관리을/를 참조하십시오. 애플리케이션 데이터를 FireSIGHT 시스템 공급업체 및 버전 정의에 매핑해도, 가져온 서드파티 취약성은 클라이언트 또는 웹 애플리케이션에 대한 영향 평가에 사용되지 않습니다.

시스템에서는 운영 체제 또는 애플리케이션의 현재 ID를 확인하기 위해 여러 소스의 데이터를 조정할 수 있습니다. 시스템에서 이를 수행하는 방법에 대한 자세한 내용은 46-5페이지의 현재 ID 이해을/를 참조하십시오.

Nmap 데이터의 경우 정기적인 Nmap 스캔을 예약할 수 있습니다. 호스트 입력 데이터의 경우 가져오기 또는 명령줄 유틸리티에 대해 Perl 스크립트를 정기적으로 실행할 수 있습니다. 그러나 활성 스캔 데이터 및 호스트 입력 데이터는 검색 데이터의 빈도로 업데이트되지 않을 수 있습니다.

FireSIGHT 시스템이 모든 애플리케이션을 식별할 수 있습니까?

라이센스: FireSIGHT

호스트가 시스템에서 올바르게 식별되지만 미확인 애플리케이션을 포함하고 있는 경우, 애플리케이션 식별에 도움이 되도록 사용자 정의 탐지기를 생성하여 시스템에 포트 및 패턴 매칭 정보를 제공할 수 있습니다. 자세한 내용은 46-19페이지의 사용자 정의 애플리케이션 프로토콜 탐지기 생성을/를 참조하십시오.

취약성을 수정하는 패치를 적용했습니까?

라이센스: FireSIGHT

시스템이 호스트를 올바르게 식별하지만 적용된 수정을 반영하지 않는 경우 호스트 입력 기능을 사용하여 패치 정보를 가져올 수 있습니다. 패치 정보를 가져오면 수정 이름을 데이터베이스의 수정에 매핑해야 합니다. 자세한 내용은 46-32페이지의 서드파티 제품 수정 매핑을/를 참조하십시오.

서드파티 취약성을 추적하고자 합니까?

라이센스: FireSIGHT

영향 상관관계에 사용하고자 하는 서드파티 시스템의 취약성 정보를 가지고 있는 경우, 서버 및 애플리케이션 프로토콜에 대한 서드파티 취약성 식별자를 Cisco 데이터베이스의 취약성 식별자에 매핑한 다음 호스트 입력 기능을 사용하여 취약성을 가져올 수 있습니다. 호스트 입력 기능 사용에 대한 자세한 내용은 *FireSIGHT 시스템 Host Input API Guide*를 참조하십시오. 서드파티 취약성 매핑에 대한 자세한 내용은 46-33페이지의 서드파티 취약성 매핑을/를 참조하십시오. 애플리케이션 데이터를 FireSIGHT 시스템 공급업체 및 버전 정의에 매핑해도, 가져온 서드파티 취약성은 클라이언트 또는 웹 애플리케이션에 대한 영향 평가에 사용되지 않습니다.

네트워크 맵 향상

라이센스: FireSIGHT

FireSIGHT 시스템은 수동적으로 트래픽을 분석하여 탐지한 데이터를 사용하여 네트워크 맵을 작성합니다. 또한 호스트 입력 기능 및 Nmap 스캐너 같은 활성 소스를 통해 추가된 데이터를 사용합니다. 시스템이 애플리케이션이나 운영 체제 ID에 사용할 데이터를 결정하는 방법을 이해하면 활성 입력 소스로 시스템의 수동 탐지 기능을 최대한 확대하는 방법을 파악하는 데 도움이 됩니다.

자세한 내용은 다음 항목을 참조하십시오.

수동 탐지 이해

라이센스: FireSIGHT

*수동 탐지*는 시스템에서 수동적으로 수집하는 트래픽의 분석을 통해 호스트 운영 체제, 클라이언트, 애플리케이션 정보를 탐지하는 것입니다. 시스템은 네트워크 자산을 식별하는 데 VDB의 정보를 사용합니다.

시스템이 호스트에서 운영 체제를 식별할 수 없으면 사용자는 이를 직접 확인하고, 시스템이 유사한 운영 체제 특성을 갖는 다른 호스트에서 해당 운영 체제를 인식할 수 있도록 사용자 지정 서버 또는 클라이언트 핑거프린트를 생성할 수 있습니다.

시스템은 호스트 운영 체제에 대해 수집된 모든 수동 핑거프린트를 사용하여 *파생 핑거프린트*를 생성합니다. 시스템은 수집된 각 핑거프린트의 신뢰 가치 및 ID 간 확증 핑거프린트 데이터의 양을 사용하여 가장 근접한 ID를 계산하는 공식을 적용하여 파생 핑거프린트를 생성합니다. ID 간 공통된 요소가 식별됩니다.

네트워크에서 사용자 정의 애플리케이션 탐지기를 사용하는 경우, 애플리케이션 식별에 필요한 정보를 시스템에 제공하는 사용자 지정 탐지기를 생성하여 시스템의 애플리케이션 탐지 기능을 보강할 수 있습니다. NetFlow도 수동 탐지 애플리케이션 정보를 네트워크 맵에 추가할 수 있습니다.

시스템은 *unknown*으로 분류한 애플리케이션 프로토콜 및 운영 체제 데이터를 사용하지 않습니다. 그러한 데이터를 해석할 수 없기 때문입니다. 관리되는 디바이스는 방어 센터에 ID를 `unknown`으로 보고하며, ID 데이터는 핑거프린트 파생에 사용되지 않습니다.

능동 탐지 이해

라이센스: FireSIGHT

*능동 탐지*는 호스트 운영 체제 및 애플리케이션 정보 등 활성 소스로 수집한 데이터를 네트워크 맵에 추가하는 것입니다. 예를 들어 네트워크에서 대상으로 삼은 호스트를 능동적으로 스캔하려면 Nmap 스캐너를 사용할 수 있습니다. Nmap은 호스트에서 운영 체제 및 애플리케이션을 검색합니다.

또한 호스트 입력 기능을 사용하면 *호스트 입력 데이터*를 네트워크 맵에 능동적으로 추가할 수 있습니다. 호스트 입력 데이터의 두 가지 카테고리가 있습니다.

- FireSIGHT 시스템 사용자 인터페이스를 통해 호스트의 운영 체제 또는 애플리케이션 ID를 수정할 수 있습니다. 이 인터페이스를 통해 추가되는 데이터가 *사용자 입력 데이터*입니다.

- 명령줄 유틸리티를 사용하여 데이터를 가져올 수도 있습니다. 가져온 데이터는 *호스트 가져오기 입력 데이터*입니다.

시스템은 각 활성 소스에 대해 하나의 ID를 유지합니다. 예를 들어 Nmap 스캔 인스턴스를 실행하면 이전 스캔 결과가 새 스캔 결과로 교체됩니다. 그러나 Nmap 스캔을 실행한 다음 그 결과를 명령줄을 통해 가져온 클라이언트의 데이터로 교체하면, 시스템은 Nmap 결과의 ID와 가져오기 클라이언트의 ID를 모두 유지합니다. 그런 다음 시스템은 시스템 정책에 설정된 우선순위를 사용하여 어떤 능동 ID를 현재 ID로 사용할 것인지를 결정합니다.

사용자 입력은 서로 다른 사용자에게서 온 것이더라도 하나의 소스로 간주됩니다. 예를 들어 UserA가 호스트 프로필을 통해 운영 체제를 설정한 다음 UserB가 호스트 프로필을 통해 정의를 변경하면, UserB가 설정한 정의가 유지되고 UserA가 설정한 정의는 폐기됩니다. 또한 사용자 입력은 다른 모든 활성 소스를 재정의하며, 존재하는 경우 현재 ID로써 사용됩니다.

현재 ID 이해

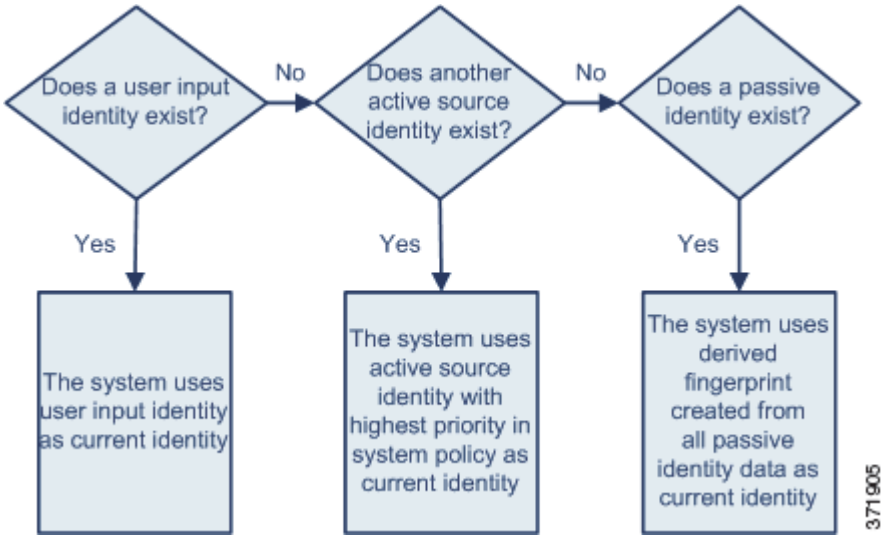
라이센스: FireSIGHT

호스트에 있는 애플리케이션 또는 운영 체제의 *현재 ID*는 시스템이 가장 정확할 것이라고 판단하는 ID입니다.

시스템은 다음과 같은 용도로 운영 체제 또는 애플리케이션에 대한 현재 ID를 사용합니다.

- 호스트에 취약성 할당
- 영향 평가
- 운영 체제 식별, 호스트 프로필 자격 및 규정 준수 화이트리스트에 대해 작성한 상관관계 규칙 평가
- 워크플로의 Hosts 및 Servers 테이블 보기에서 표시
- 호스트 프로필에서 표시
- Discovery Statistics 페이지에서 운영 체제 및 애플리케이션 통계 계산

시스템은 어떤 능동 ID를 애플리케이션 또는 운영 체제에 대한 현재 ID로 사용할지를 결정하는 데 소스 우선순위를 사용합니다.



예를 들어 사용자가 호스트에서 운영 체제를 Windows 2003 Server로 설정하면 Windows 2003 Server가 현재 ID가 됩니다. 해당 호스트의 Windows 2003 Server 취약성에 대한 공격에는 더 높은 영향이 지정되고, 호스트 프로필의 해당 호스트에 대해 나열된 취약성에는 Windows 2003 Server 취약성이 포함됩니다.

데이터베이스에는 호스트의 특정 운영 체제 또는 특정 애플리케이션에 대한 여러 소스의 정보가 포함되어 있을 수 있습니다.

시스템은 데이터에 대한 소스가 가장 높은 소스 우선순위를 가지고 있을 때 운영 체제 또는 애플리케이션 ID를 현재 ID로 취급합니다. 가능한 소스의 우선순위 순서는 다음과 같습니다.

1. 사용자
2. 스캐너 및 애플리케이션(네트워크 검색 정책에 설정됨)
3. 관리되는 디바이스
4. NetFlow

우선순위가 더 높은 새 애플리케이션 ID는 현재 ID보다 세부사항이 부족하면 현재 애플리케이션 ID를 재정의하지 않습니다.

또한 ID 충돌이 발생하는 경우 충돌의 해결은 네트워크 검색 정책의 설정 또는 수동 해결에 의존하게 됩니다(46-6페이지의 ID 충돌 이해 참조).

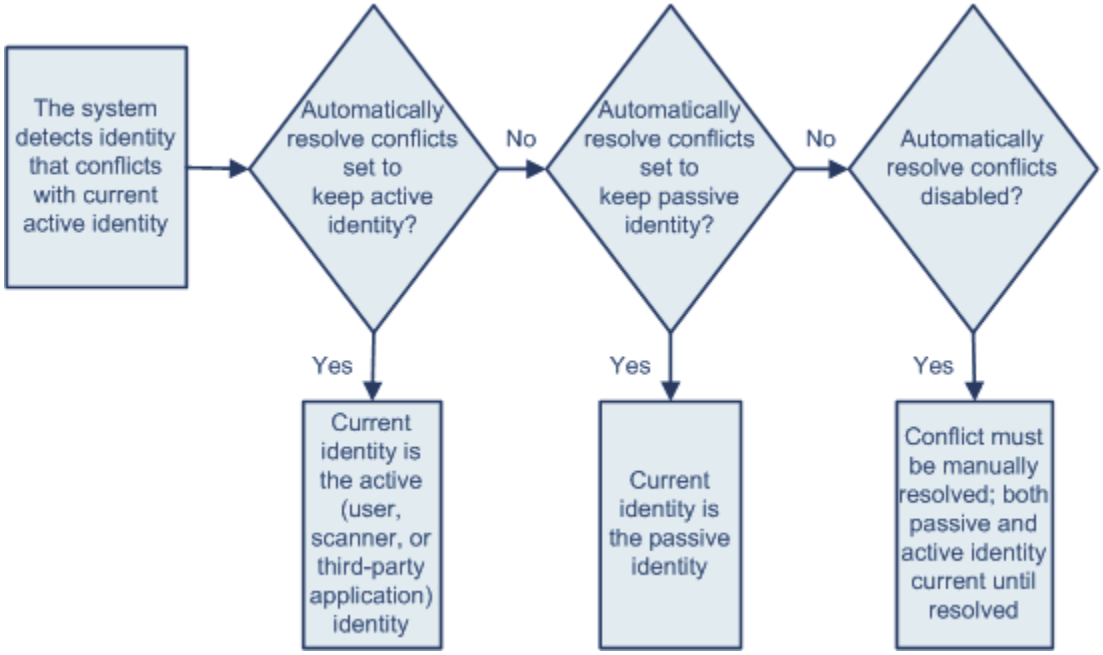
ID 충돌 이해

라이센스: FireSIGHT

시스템이 현재 능동 ID와 충돌하며 전에는 수동 ID로 보고되었던 새로운 수동 ID를 보고하면 *ID 충돌*이 발생합니다. 예를 들어, 운영 체제에 대한 이전의 수동 ID가 Windows 2000으로 보고된 이후 Windows XP의 능동 ID가 현재 ID가 됩니다. 다음에 시스템은 Ubuntu Linux 8.04.1의 새로운 수동 ID를 탐지합니다. 그러면 Windows XP와 Ubuntu Linux ID가 충돌하게 됩니다.

호스트의 운영 체제 또는 호스트의 애플리케이션에서 ID 충돌이 발생하면 시스템은 충돌이 해결될 때까지 충돌하는 두 ID를 모두 현재 ID로 나열하고 영향 평가에 둘을 모두 사용합니다.

관리자 권한이 있는 사용자는 항상 수동 ID를 사용하거나 항상 능동 ID를 사용하도록 선택하여 ID 충돌을 자동으로 해결할 수 있습니다. ID 충돌의 자동 해결을 비활성화하지 않는 한 ID 충돌은 항상 자동으로 해결됩니다.



관리자 권한이 있는 사용자는 ID 충돌이 발생할 경우 이벤트를 생성하도록 시스템을 구성할 수도 있습니다. 그러면 해당 사용자는 Nmap 스캔을 상관관계 응답으로써 사용하는 상관관계 규칙으로 상관관계 정책을 설정할 수 있습니다. 이벤트가 발생하면 Nmap은 호스트를 스캔하여 업데이트된 호스트 운영 체제 및 애플리케이션 데이터를 가져옵니다.

사용자 지정 핑거프린트 사용

라이센스: FireSIGHT

FireSIGHT 시스템에는 시스템이 탐지하는 각 호스트에서 운영 체제를 식별하는 데 사용하는 운영 체제 *핑거프린트*가 포함되어 있습니다. 그러나 운영 체제와 일치하는 핑거프린트가 없기 때문에 때때로 시스템은 호스트 운영 체제를 식별할 수 없거나 잘못 식별합니다. 이 문제를 바로잡으려면 알 수 없거나 잘못 식별된 운영 체제에 고유한 운영 체제 특성 패턴을 제공하는 *사용자 지정 핑거프린트*를 생성하여, 식별 목적으로 운영 체제의 이름을 제공할 수 있습니다.

시스템이 호스트의 운영 체제를 확인할 수 없으면 호스트에 대한 취약성도 식별할 수 없습니다. 시스템은 각 호스트에 대한 취약성 목록을 운영 체제 핑거프린트에서 가져오기 때문입니다. 예를 들어 Microsoft Windows를 실행하는 호스트를 탐지하는 경우 시스템은 탐지된 Windows 운영 체제를 기반으로 해당 호스트에 대한 호스트 프로필을 추가하는 저장된 Microsoft Windows 취약성 목록을 가지고 있습니다.

예를 들어 Microsoft Windows의 새 베타 버전을 실행하는 디바이스가 네트워크에 여러 개 있는 경우 시스템은 해당 운영 체제를 식별할 수 없으므로 호스트에 취약성을 매핑할 수 없습니다. 그러나 시스템에 Microsoft Windows에 대한 취약성 목록이 있음을 알고 있다면, 호스트 중 하나에 대한 사용자 지정 핑거프린트를 생성한 다음 동일한 운영 체제를 실행하는 다른 호스트의 식별에 이를 사용할 수 있습니다. 핑거프린트에 Microsoft Windows에 대한 취약성 목록의 매핑을 포함하여, 해당 목록을 핑거프린트와 일치하는 각 호스트와 연결할 수 있습니다.

사용자 지정 핑거프린트를 생성하면 운영 체제 정보의 사용자 지정 표시를 추가할 수 있으며, 시스템이 핑거프린트에 대한 취약성 목록의 모델로 사용해야 할 운영 체제에 대한 공급업체, 제품 이름 및 제품 버전을 선택할 수 있습니다. 방어 센터는 동일한 운영 체제를 실행하는 호스트의 해당 핑거프린트와 관련된 취약성 집합을 나열합니다. 생성한 사용자 지정 핑거프린트에 취약성이 매핑되어 있지 않으면, 시스템은 핑거프린트를 사용하여 사용자가 핑거프린트에서 제공하는 사용자 지정 운영 체제 정보를 할당합니다. 이미 탐지되었으며 현재 네트워크 맵에 상주하는 호스트에서 새 트래픽을 탐지하면 시스템은 새 핑거프린트 정보로 호스트를 업데이트합니다. 시스템은 또한 새 호스트 및 이들이 처음 탐지된 운영 체제를 식별하는 데에도 새 핑거프린트를 사용합니다.

호스트의 핑거프린트 처리를 시도하기 전에, 호스트가 올바르게 식별되지 않는 이유를 파악하여 사용자 지정 핑거프린트가 실용적인 해결책인지 결정해야 합니다. 자세한 내용은 46-2페이지의 탐지 전략 평가을/를 참조하십시오.

시스템에서 두 가지 유형의 핑거프린트를 생성할 수 있습니다.

- 클라이언트 핑거프린트 - 호스트가 네트워크의 다른 호스트에서 실행 중인 TCP 애플리케이션에 연결될 때 전송하는 SYN 패킷을 기반으로 운영 체제를 식별합니다.

  호스트에 대한 클라이언트 핑거프린트를 가져오는 방법에 대한 자세한 내용은 46-8페이지의 클라이언트 핑거프린트을/를 참조하십시오.

- 서버 핑거프린트 - 실행 중인 TCP 애플리케이션에 대한 수신 연결에 응답하기 위해 호스트가 사용하는 SYN-ACK 패킷을 기반으로 운영 체제를 식별합니다.

  호스트에 대한 서버 핑거프린트를 가져오는 방법에 대한 자세한 내용은 46-11페이지의 서버 핑거프린트을/를 참조하십시오.

핑거프린트를 생성한 후에는 활성화해야만 시스템이 해당 핑거프린트를 호스트와 연결할 수 있습니다. 자세한 내용은 46-13페이지의 핑거프린트 관리을/를 참조하십시오.

참고 클라이언트 및 서버 핑거프린트가 동일한 호스트와 일치하면 클라이언트 핑거프린트가 사용됩니다.

클라이언트 핑거프린트

라이센스: FireSIGHT

클라이언트 핑거프린트는 호스트가 네트워크의 다른 호스트에서 실행 중인 TCP 애플리케이션에 연결될 때 전송하는 SYN 패킷을 기반으로 운영 체제를 식별합니다.

방어 센터가 모니터링되는 호스트와 직접 연결되지 않은 경우, 방어 센터에 의해 관리되며 클라이언트 핑거프린트 속성을 지정할 때 핑거프린트 처리할 호스트와 가장 가까운 디바이스를 지정할 수 있습니다.

핑거프린트 처리를 시작하기 전에 핑거프린트 처리할 호스트에 대한 다음 정보를 확인하십시오.

- 호스트와 방어 센터 또는 핑거프린트를 가져오기 위해 사용할 디바이스 간 네트워크 홉의 수 (Cisco에서는 방어 센터 또는 디바이스를 호스트가 연결된 것과 동일한 서브넷에 연결할 것을 적극 권장합니다.)
- 호스트가 상주하는 네트워크에 연결된 네트워크 인터페이스(방어 센터 또는 디바이스)
- 호스트의 실제 운영 체제 공급업체, 제품 및 버전
- 클라이언트 트래픽을 생성하기 위해 호스트에 액세스

호스트에 대한 클라이언트 핑거프린트를 가져오려면

액세스: Admin/Discovery Admin

1단계 **Policies** > **Network Discovery**를 선택하고 **Custom Operating Systems**를 선택합니다.

Custom Fingerprint 페이지가 나타납니다.

2단계 **Create Custom Fingerprint**를 클릭합니다.

Create Custom Fingerprint 페이지가 나타납니다.

3단계 **Device** 드롭다운 목록에서 핑거프린트 수집에 사용할 디바이스 또는 방어 센터를 선택합니다.

4단계 **Fingerprint Name** 필드에 핑거프린트의 식별 이름을 입력합니다.

5단계 **Fingerprint Description** 필드에 핑거프린트에 대한 설명을 입력합니다.

6단계 **Fingerprint Type** 목록에서 **Client**를 선택합니다.

7단계 **Target IP Address** 필드에 핑거프린트 처리할 호스트의 IP 주소를 입력합니다. 핑거프린트는 사용자가 지정하는 호스트 IP 주소(호스트의 다른 IP 주소가 아닌)를 통과하는 트래픽만을 기반으로 합니다.

주의 관리되는 디바이스 및 방어 센터에서 IPv6을 활성화하는 방법에 대한 자세한 내용은 64-8페이지의 관리 인터페이스 구성을/를 참조하십시오.

8단계 핑거프린트를 수집하기 위해 3단계에서 선택한 디바이스와 호스트 간 네트워크 홉의 수를 **Target Distance** 필드에 입력합니다.

주의 이 값은 호스트에 대한 물리적 네트워크 홉의 실제 숫자여야 하며, 시스템에 의해 탐지된 홉의 수와 같을 수도 있고 다를 수도 있습니다.

9단계 호스트가 상주하는 네트워크 세그먼트에 연결된 네트워크 인터페이스를 **Interface** 목록에서 선택합니다.

주의 Cisco에서는 여러 가지 이유로, 관리되는 디바이스의 센싱 인터페이스를 핑거프린트에 사용하지 **않을** 것을 권장합니다. 첫째, 센싱 인터페이스가 span 포트에 있으면 핑거프린트가 작동하지 않습니다. 또한 디바이스에서 센싱 인터페이스를 사용하면 디바이스는 핑거프린트를 수집하는 데 걸리는 시간 동안 네트워크의 모니터링을 중지합니다. 그러나 핑거프린트 수집을 수행하는 데 관리 인터페이스 또는 기타 사용 가능한 네트워크 인터페이스를 사용할 수 있습니다. 디바이스에서 어떤 인터페이스가 센싱 인터페이스인지 모르는 경우, 핑거프린트 처리에 사용 중인 특정 모델의 *Installation Guide*를 참조하십시오.

10단계 핑거프린트 처리된 호스트에 대한 호스트 프로필에 사용자 지정 정보를 표시하려면(또는 핑거프린트 처리할 호스트가 OS Vulnerability Mappings 섹션에 상주하지 않는 경우), Custom OS Display 섹션에서 **Use Custom OS Display**를 선택하고 다음에 대해 호스트 프로필에 표시할 값을 제공합니다.

- **Vendor String** 필드에 운영 체제의 공급업체 이름을 입력합니다. 예를 들어 Microsoft Windows의 공급업체는 Microsoft입니다.
- **Product String** 필드에 운영 체제의 제품 이름을 입력합니다. 예를 들어 Microsoft Windows 2000의 제품 이름은 Windows입니다.
- **Version String** 필드에 운영 체제의 버전 번호를 입력합니다. 예를 들어 Microsoft Windows 2000의 버전 번호는 2000입니다.

11단계 OS Vulnerability Mappings 섹션에서 취약성 매핑에 사용할 운영 체제, 제품 및 버전을 선택합니다.

예를 들어 사용자 지정 핑거프린트를 통해 Redhat Linux 9의 취약성 목록을 매칭 호스트에 할당하려면 공급업체로 **Redhat, Inc.**, 제품으로 **Redhat Linux**, 주요 버전으로 **9**를 선택합니다.

팁 핑거프린트를 생성할 때 핑거프린트에 대한 단일 가용성 매핑을 할당하십시오. 핑거프린트가 생성 및 활성화되면 운영 체제의 다른 버전에 대해 취약성 매핑을 더 추가할 수 있습니다. 자세한 내용은 46-16페이지의 활성 핑거프린트 수정을/를 참조하십시오.

핑거프린트를 사용하여 매칭 호스트에 대한 취약성을 식별하려는 경우 또는 사용자 지정 운영 체제 표시 정보를 할당하지 않은 경우 이 섹션에서 Vendor and Product 이름을 지정해야 합니다. 운영 체제의 모든 버전에 대해 취약성을 매핑하려면 공급업체 및 제품 이름만 지정하십시오. 예를 들어 Palm OS의 모든 버전을 추가하려면 **Vendor** 목록에서 **PalmSource, Inc.**, **Product** 목록에서 **Palm OS**를 선택하고 다른 모든 목록은 기본 설정으로 두십시오.

참고 선택한 운영 체제에 **Major Version**, **Minor Version**, **Revision Version**, **Build**, **Patch** 및 **Extension** 드롭다운 목록의 모든 옵션이 적용되지는 않을 수도 있습니다. 또한 핑거프린트 처리하려는 운영 체제와 일치하는 정의가 목록에 나타나지 않으면 해당 값을 비워 둘 수 있습니다. 핑거프린트에서 OS 취약성 매핑을 생성하지 않으면 시스템은 핑거프린트에 의해 식별되는 호스트가 포함된 취약성 목록을 할당하는 데 핑거프린트를 사용할 수 없습니다.

12단계 **Create**를 클릭합니다.

Custom Fingerprint 상태 페이지가 다시 나타납니다. 문제의 호스트에서 데이터를 수신할 때까지 10초마다 상태 페이지가 새로 고쳐집니다.

팁 **Create**를 클릭하면 짧게 `New`가 표시된 다음 상태가 `Pending`으로 전환됩니다. 여기서 핑거프린트에 대한 트래픽이 표시될 때까지 유지되다가 상태가 `Ready`로 전환됩니다.

13단계 대상 IP 주소로 지정된 IP 주소를 사용하여, 핑거프린트 처리하려는 호스트에 액세스하고 어플라이언스에 대한 TCP 연결을 시작합니다.

예를 들면, 핑거프린트 처리할 호스트에서 방어 센터의 웹 인터페이스에 액세스하거나 호스트에서 방어 센터의 SSH에 액세스합니다. SSH에서 다음 명령을 사용합니다.

```
ssh -b localIPv6address DCmanagementIPv6address
```

여기서 *`localIPv6address`*는 7단계에서 지정되었고 현재 호스트에 할당된 IPv6 주소이며, *`DCmanagementIPv6address`*는 방어 센터의 관리 IPv6 주소입니다.

Custom Fingerprint 페이지가 "Ready" 상태로 다시 로드됩니다.

참고 정확한 핑거프린트를 생성하려면 핑거프린트를 수집하는 어플라이언스에 트래픽이 **표시되어야** 합니다. 스위치를 통해 연결된 경우 어플라이언스 외의 시스템에 대한 트래픽은 시스템에 표시되지 않을 수 있습니다.

14단계 핑거프린트를 생성한 후 활성화해야만 방어 센터에서 이를 사용하여 호스트를 식별할 수 있습니다. 자세한 내용은 46-13페이지의 핑거프린트 관리을/를 참조하십시오.

서버 핑거프린트

라이센스: FireSIGHT

서버 핑거프린트는 실행 중인 TCP 애플리케이션에 대한 수신 연결에 응답하기 위해 호스트가 사용하는 SYN-ACK 패킷을 기반으로 운영 체제를 식별합니다. 시작하기 전에 핑거프린트 처리할 호스트에 대한 다음 정보를 확인하십시오.

- 호스트와 핑거프린트를 가져오기 위해 사용할 어플라이언스 간 네트워크 홉의 수. Cisco에서는 어플라이언스의 미사용 인터페이스를 호스트가 연결된 것과 동일한 서브넷에 연결할 것을 적극 권장합니다.
- 호스트가 상주하는 네트워크에 연결된 네트워크 인터페이스(어플라이언스)
- 호스트의 실제 운영 체제 공급업체, 제품 및 버전
- 현재 사용되고 있지 않으며 호스트가 있는 네트워크에서 인증된 IP 주소

팁 방어 센터가 모니터링되는 호스트와 직접 연결되지 않은 경우 서버 핑거프린트 속성을 지정할 때 핑거프린트 처리할 호스트와 가장 가까운 관리되는 디바이스를 지정할 수 있습니다.

호스트에 대한 서버 핑거프린트를 가져오려면

액세스: Admin/Discovery Admin

1단계 **Policies** > **Network Discovery**를 선택하고 **Custom Operating Systems**를 선택합니다.

Custom Fingerprint 페이지가 나타납니다.

2단계 **Create Custom Fingerprint**를 클릭합니다.

Create Custom Fingerprint 페이지가 나타납니다.

3단계 **Device** 목록에서 핑거프린트 수집에 사용할 관리되는 디바이스 또는 방어 센터를 선택합니다.

4단계 **Fingerprint Name** 필드에 핑거프린트의 식별 이름을 입력합니다.

5단계 **Fingerprint Description** 필드에 핑거프린트에 대한 설명을 입력합니다.

6단계 **Fingerprint Type** 목록에서 **Server**를 선택합니다.

서버 핑거프린트 옵션이 나타납니다.

7단계 **Target IP Address** 필드에 핑거프린트 처리할 호스트의 IP 주소를 입력합니다. 핑거프린트는 사용자가 지정하는 호스트 IP 주소(호스트의 다른 IP 주소가 아닌)를 통과하는 트래픽만을 기반으로 합니다.

주의 FireSIGHT 시스템의 버전 5.2 이상을 실행하는 어플라이언스에서만 IPv6 핑거프린트를 캡처할 수 있습니다.

8단계 핑거프린트를 수집하기 위해 3단계에서 선택한 디바이스와 호스트 간 네트워크 홉의 수를 **Target Distance** 필드에 입력합니다.

주의 이 값은 호스트에 대한 물리적 네트워크 홉의 실제 숫자여야 하며, 시스템에 의해 탐지된 홉의 수와 같을 수도 있고 다를 수도 있습니다.

9단계 호스트가 상주하는 네트워크 세그먼트에 연결된 네트워크 인터페이스를 **Interface** 목록에서 선택합니다.

주의 Cisco에서는 여러 가지 이유로, 관리되는 디바이스의 센싱 인터페이스를 핑거프린트에 사용하지 **않을** 것을 권장합니다. 첫째, 센싱 인터페이스가 span 포트에 있으면 핑거프린트가 작동하지 않습니다. 또한 디바이스에서 센싱 인터페이스를 사용하면 디바이스는 핑거프린트를 수집하는 데 걸리는 시간 동안 네트워크의 모니터링을 중지합니다. 그러나 핑거프린트 수집을 수행하는 데 관리 인터페이스 또는 기타 사용 가능한 네트워크 인터페이스를 사용할 수 있습니다. 디바이스에서 어떤 인터페이스가 센싱 인터페이스인지 모르는 경우, 핑거프린트 처리에 사용 중인 특정 모델의 *Installation Guide*를 참조하십시오.

10단계 **Get Active Ports**를 클릭합니다.

시스템이 호스트에서 열린 포트를 탐지하면 드롭다운 목록에 그러한 포트가 나타납니다.

11단계 핑거프린트를 수집하기 위해 선택한 디바이스가 연결을 시작하도록 할 포트를 **Server Port** 필드에 입력하거나, **Get Active Ports** 드롭다운 목록에서 포트를 선택합니다.

호스트에 열려 있음을 알고 있는 서버 포트를 아무거나 사용할 수 있습니다(예: 호스트가 웹 서버를 실행 중인 경우 80).

12단계 호스트와의 통신을 시도하기 위해 사용해야 할 IP 주소를 **Source IP Address** 필드에 입력합니다.

네트워크에서 사용하도록 인증되었지만 현재 사용되고 있지 않은 소스 IP 주소(예: 현재 사용되고 있지 않은 DHCP 풀 주소)를 사용해야 합니다. 이렇게 하면 핑거프린트를 생성하는 동안 일시적으로 다른 호스트를 오프라인으로 탐색하지 않아도 됩니다.

또한 핑거프린트를 생성하는 동안에는 네트워크 검색 정책에서 해당 IP 주소의 모니터링을 제외해야 합니다. 그렇게 하지 않으면 네트워크 맵 및 검색 이벤트 보기가 해당 IP 주소로 표시되는 호스트에 대한 부정확한 정보와 뒤섞이게 됩니다. 자세한 내용은 45-1페이지의 검색 데이터 수집 이해을/를 참조하십시오.

13단계 **Source Subnet Mask** 필드에 사용 중인 IP 주소의 서브넷 마스크를 입력합니다.

14단계 **Source Gateway** 필드가 나타나면 호스트에 대한 경로를 설정하기 위해 사용해야 할 기본 게이트웨이 IP 주소를 입력합니다.

대상 거리(홉의 수)가 1 이상이며 호스트가 상주하는 네트워크에 연결하기 위해 관리 인터페이스 이외의 인터페이스를 사용 중인 경우 **Source Gateway** 필드가 나타납니다.

15단계 핑거프린트 처리된 호스트에 대한 호스트 프로필에 사용자 지정 정보를 표시하려면 또는 사용하려는 핑거프린트 이름이 OS Definition 섹션에 없으면 Custom OS Display 섹션에서 **Use Custom OS Display**를 선택합니다.

호스트 프로필에 표시할 다음에 대한 값을 제공합니다.

- **Vendor String** 필드에 운영 체제의 공급업체 이름을 입력합니다. 예를 들어 Microsoft Windows의 공급업체는 Microsoft입니다.
- **Product String** 필드에 운영 체제의 제품 이름을 입력합니다. 예를 들어 Microsoft Windows 2000의 제품 이름은 Windows입니다.
- **Version String** 필드에 운영 체제의 버전 번호를 입력합니다. 예를 들어 Microsoft Windows 2000의 버전 번호는 2000입니다.

16단계 OS Vulnerability Mappings 섹션에서 취약성 매핑에 사용할 운영 체제, 제품 및 버전을 선택합니다. 예를 들어 사용자 지정 핑거프린트를 통해 Redhat Linux 9의 취약성 목록을 매칭 호스트에 할당하려면 공급업체로 **Redhat, Inc.**, 제품으로 **Redhat Linux**, 버전으로 **9**를 선택합니다.

팁 핑거프린트를 생성할 때 핑거프린트에 대한 단일 가용성 매핑을 할당하십시오. 핑거프린트가 생성 및 활성화되면 운영 체제의 다른 버전에 대해 취약성 매핑을 더 추가할 수 있습니다. 자세한 내용은 46-16페이지의 활성 핑거프린트 수정을/를 참조하십시오.

핑거프린트를 사용하여 매칭 호스트에 대한 취약성을 식별하려는 경우 또는 사용자 지정 운영 체제 표시 정보를 할당하지 않은 경우 이 섹션에서 Vendor and Product 이름을 지정해야 합니다. 운영 체제의 모든 버전에 대해 취약성을 매핑하려면 공급업체 및 제품 이름만 지정하십시오. 예를 들어 Palm OS의 모든 버전을 추가하려면 **Vendor** 목록에서 **PalmSource, Inc.**, **Product** 목록에서 **Palm OS**를 선택하고 다른 모든 목록은 기본 설정으로 두십시오.

참고 선택한 운영 체제에 **Major Version**, **Minor Version**, **Revision Version**, **Build**, **Patch** 및 **Extension** 드롭다운 목록의 모든 옵션이 적용되지는 않을 수도 있습니다. 또한 핑거프린트 처리하려는 운영 체제와 일치하는 정의가 목록에 나타나지 않으면 해당 값을 비워 둘 수 있습니다. 핑거프린트에서 OS 취약성 매핑을 생성하지 않으면 시스템은 핑거프린트에 의해 식별되는 호스트가 포함된 취약성 목록을 할당하는 데 핑거프린트를 사용할 수 없습니다.

17단계 **Create**를 클릭합니다.

18단계 Custom Fingerprint 상태 페이지가 나타납니다. 이 페이지는 10초마다 다시 로드되며, 상태는 "Ready"여야 합니다.

참고 핑거프린트 처리 중에 대상 시스템이 응답을 중지하면 상태에 `ERROR: No Response` 메시지가 나타납니다. 이 메시지가 표시되면 핑거프린트를 다시 제출하십시오. 3~5분 정도 기다렸다가(시간은 대상 시스템에 따라 달라질 수 있음) 수정 아이콘( )을 클릭하여 Custom Fingerprint 페이지에 액세스한 다음 **Create**를 클릭합니다.

19단계 핑거프린트가 생성된 후 활성화하고, 선택적으로 취약성 매핑을 추가합니다. 자세한 내용은 46-13페이지의 핑거프린트 관리을/를 참조하십시오.

핑거프린트 관리

라이센스: FireSIGHT

사용자 지정 핑거프린트를 활성화, 비활성화, 삭제, 보기 및 수정할 수 있습니다. 핑거프린트를 생성할 때 핑거프린트에 대한 단일 가용성 매핑을 할당하십시오. 핑거프린트 생성에 대한 자세한 내용은 46-8페이지의 클라이언트 핑거프린트 및 46-11페이지의 서버 핑거프린트을/를 참조하십시오. 핑거프린트를 생성 및 활성화한 후에는 원하는 대로 내용을 수정하거나 취약성 매핑을 추가할 수 있습니다.

Custom Fingerprints 페이지에 액세스하려면

액세스: Admin/Discovery Admin

1단계 **Policies** > **Network Discovery**를 선택하고 **Custom Operating Systems**를 선택합니다.

Custom Fingerprint 페이지가 나타납니다.

핑거프린트 생성을 위해 데이터를 기다리고 있는 시스템은 핑거프린트가 생성될 때까지 10초마다 페이지를 자동으로 새로 고칩니다.

자세한 내용은 다음 절을 참조하십시오.

- 46-14페이지의 핑거프린트 활성화
- 46-14페이지의 핑거프린트 비활성화
- 46-15페이지의 핑거프린트 삭제
- 46-15페이지의 핑거프린트 수정

핑거프린트 활성화

라이센스: FireSIGHT

사용자 지정 핑거프린트를 생성한 후 활성화해야만 시스템에서 이를 사용하여 호스트를 식별할 수 있습니다. 새 핑거프린트가 활성화되면 시스템에서는 이를 사용하여 전에 검색된 호스트를 다시 식별하고 새 호스트를 검색합니다.

핑거프린트를 활성화하려면

액세스: Admin/Discovery Admin

1단계 **Policies** > **Network Discovery**를 선택하고 **Custom Operating Systems**를 선택합니다.

Custom Fingerprint 페이지가 나타납니다.

2단계 활성화할 핑거프린트 옆에 있는 슬라이더를 클릭합니다.

참고 생성한 핑거프린트가 유효한 경우에만 활성화 옵션을 사용할 수 있습니다. 슬라이더를 사용할 수 없는 경우 핑거프린트를 다시 생성해 보십시오.

방어 센터는 핑거프린트를 활성화하고 이를 모든 관리되는 디바이스에 전파합니다. 핑거프린트 이름 옆에 있는 아이콘이 변경되어, 핑거프린트가 활성 상태임을 나타냅니다.

핑거프린트 비활성화

라이센스: FireSIGHT

핑거프린트 사용을 중지하려면 비활성화할 수 있습니다. 핑거프린트를 비활성화하면 더 이상 사용되지 않지만, 시스템에 그대로 둘 수 있습니다. 핑거프린트를 비활성화하면 운영 체제는 핑거프린트를 사용하는 호스트에 대해 Unknown으로 표시됩니다. 호스트가 다시 탐지되고 다른 활성 핑거프린트와 일치하면 해당 활성 핑거프린트로 식별됩니다.

핑거프린트를 삭제하면 시스템에서 완전히 제거됩니다. 핑거프린트를 비활성화한 후에 삭제할 수 있습니다.

활성 핑거프린트를 비활성화하려면

액세스: Admin/Discovery Admin

1단계 **Policies** > **Network Discovery**를 선택하고 **Custom Operating Systems**를 선택합니다.

Custom Fingerprint 페이지가 나타납니다.

2단계 비활성화할 활성 핑거프린트 옆에 있는 슬라이더를 클릭합니다.

방어 센터는 핑거프린트를 비활성화하고 이를 모든 관리되는 디바이스에 전파합니다.

핑거프린트 삭제

라이센스: FireSIGHT

핑거프린트를 더 이상 사용하지 않는 경우 시스템에서 삭제할 수 있습니다. 핑거프린트를 먼저 비활성화한 후에 삭제해야 합니다.

핑거프린트를 삭제하려면

액세스: Admin/Discovery Admin

1단계 **Policies** > **Network Discovery**를 선택하고 **Custom Operating Systems**를 선택합니다.

Custom Fingerprint 페이지가 나타납니다.

2단계 삭제하려는 핑거프린트가 활성 상태이면 각 핑거프린트 옆에 있는 슬라이더 아이콘을 클릭하여 비활성화합니다.

3단계 삭제할 핑거프린트 옆에 있는 삭제 아이콘( )을 클릭합니다.

4단계 **OK**를 클릭하여 핑거프린트를 삭제할 것임을 확인합니다.

핑거프린트가 삭제됩니다.

핑거프린트 수정

라이센스: FireSIGHT

핑거프린트를 만든 후에는 보거나 수정할 수 있습니다. 핑거프린트를 수정하여 다시 제출하거나 핑거프린트에 취약성 매핑을 추가할 수 있습니다. 활성 상태이든 비활성 상태이든 핑거프린트를 수정할 수 있지만, 핑거프린트의 상태에 따라 수정 가능한 내용이 다릅니다.

핑거프린트가 *비활성 상태*이면 핑거프린트의 모든 요소를 수정한 후 방어 센터에 다시 제출할 수 있습니다. 여기에는 핑거프린트 유형, 대상 IP 주소와 포트, 취약성 매핑 등 핑거프린트 생성 시 지정한 모든 속성이 포함됩니다. 비활성 핑거프린트를 수정하고 다시 제출하면 시스템에 다시 제출되며, 클라이언트 핑거프린트인 경우 활성화하기 전에 어플라이언스에 트래픽을 다시 전송해야 합니다. 비활성 핑거프린트에 대해서는 단일 취약성 매핑만 선택할 수 있습니다. 핑거프린트를 활성화한 후 추가 운영 체제 및 버전을 취약성 목록에 매핑할 수 있습니다.

핑거프린트가 *활성 상태*이면 핑거프린트 이름, 설명, 사용자 지정 운영 체제 표시 등을 수정하고 추가 취약성을 매핑할 수 있습니다.

자세한 내용은 다음 절을 참조하십시오.

- 46-16페이지의 비활성 핑거프린트 수정
- 46-16페이지의 활성 핑거프린트 수정

비활성 핑거프린트 수정

라이센스: FireSIGHT

핑거프린트가 비활성 상태이면 핑거프린트의 속성을 수정한 후 시스템에 다시 제출할 수 있습니다. 변경할 수 있는 속성에는 사용할 핑거프린트의 유형, 핑거프린트 처리할 대상 시스템 등이 포함됩니다.

비활성 핑거프린트를 수정하려면

액세스: Admin/Discovery Admin

1단계 **Policies** > **Network Discovery**를 선택하고 **Custom Operating Systems**를 선택합니다.

Custom Fingerprint 페이지가 나타납니다.

2단계 수정할 핑거프린트 옆에 있는 수정 아이콘( )을 클릭합니다.

Edit Custom Fingerprint 페이지가 나타납니다.

3단계 필요한 대로 핑거프린트를 수정합니다.

- 클라이언트 핑거프린트를 수정하는 경우 구성 가능한 옵션에 대한 자세한 내용은 46-8페이지의 클라이언트 핑거프린트을/를 참조하십시오.
- 서버 핑거프린트를 수정하는 경우 구성 가능한 옵션에 대한 자세한 내용은 46-11페이지의 서버 핑거프린트을/를 참조하십시오.

4단계 핑거프린트를 다시 제출하려면 **Save**를 클릭합니다.

참고 클라이언트 핑거프린트를 수정한 경우 호스트에서 어플라이언스(핑거프린트를 수집하는)로 트래픽을 전송해야 합니다.

활성 핑거프린트 수정

라이센스: FireSIGHT

핑거프린트가 활성 상태이면 이름, 설명 및 표시 레이블을 변경할 수 있습니다. 또한 취약성 매핑의 추가와 삭제를 포함하여, 취약성 매핑을 관리할 수 있습니다.

활성 핑거프린트를 수정하려면

액세스: Admin/Discovery Admin

1단계 **Policies** > **Network Discovery**를 선택하고 **Custom Operating Systems**를 선택합니다.

Custom Fingerprint 페이지가 나타납니다.

2단계 수정할 핑거프린트 옆에 있는 수정 아이콘( )을 클릭합니다.

Edit Custom Fingerprint Product Mappings 페이지가 나타납니다.

3단계 핑거프린트 이름, 설명 및 사용자 지정 OS 표시를 필요에 따라 수정합니다.

4단계 취약성 매핑을 삭제하려면 페이지의 Pre-Defined OS Product Maps 섹션에서 매핑 옆에 있는 **Delete**를 클릭합니다.

5단계 취약성 매핑에 대한 운영 체제를 더 추가하려면 **Product**를 선택하고, 해당되는 경우 **Major Version**, **Minor Version**, **Revision Version**, **Build**, **Patch** 및 **Extension**을 선택한 다음 **Add OS Definition**을 클릭합니다.

취약성 매핑이 Pre-Defined OS Product Maps 목록에 추가됩니다.

6단계 변경 사항을 저장하려면 **Save**를 클릭합니다.

애플리케이션 탐지기 작업

라이센스: FireSIGHT

FireSIGHT 시스템은 IP 트래픽을 분석할 때 네트워크에서 자주 사용되는 애플리케이션을 확인하기 위해 탐지기를 사용합니다. Detectors 페이지(**Policies > Application Detectors**)를 사용하면 FireSIGHT 시스템의 탐지 기능을 사용자 지정할 수 있습니다.

이 페이지는 각 탐지기에 대한 다음과 같은 정보를 제공합니다.

- 탐지기의 이름
- 탐지기가 검사하는 트래픽의 프로토콜(TCP, UDP 또는 둘 다)
- 탐지기의 유형(애플리케이션 프로토콜, 클라이언트, 웹 애플리케이션 또는 내부 탐지기)
- 포트 기반 애플리케이션 탐지기의 경우 애플리케이션 트래픽에 사용되는 포트
- 탐지된 애플리케이션의 세부사항(이름, 설명, 위험, 비즈니스 연관성, 태그, 탐지기가 탐지한 애플리케이션과 관련된 카테고리)
- 탐지기의 상태(활성 또는 비활성)

시스템은 애플리케이션 트래픽을 분석하는 데 활성 탐지기만 사용합니다.

나열된 탐지기의 속성이 서로 다른 것을 알 수 있을 것입니다. 예를 들면 일부 탐지기에 대해서만 설정이 보이고 나머지에 대해서는 보이지 않습니다. 마찬가지로, 일부 탐지기만 삭제할 수 있고 나머지는 삭제할 수 없습니다. 이는 Cisco 제공 탐지기에 몇 가지 서로 다른 유형이 있기 때문입니다. 자세한 내용은 다음 절에서 설명합니다.

Cisco 제공 내부 탐지기

*내부 탐지기*는 FireSIGHT 시스템에 대한 업데이트와만 제공되는 애플리케이션 탐지기입니다. 내부 탐지기는 탐지기 유형에 따라 클라이언트, 웹 애플리케이션 또는 애플리케이션 프로토콜 트래픽을 탐지하지만, 내장된 탐지기이고 비활성화할 수 없으므로 다른 유형보다는 내부 탐지기로 분류됩니다.

내부 탐지기는 항상 켜져 있으며, 비활성화하거나 삭제하거나 다른 방법으로 구성할 수 없습니다. 내부 탐지기의 예로는 Built-in Amazon 탐지기 및 Built-in AppleTalk 탐지기가 있습니다.

Cisco 제공 클라이언트 탐지기

Cisco 제공 *클라이언트 탐지기*는 클라이언트 트래픽을 탐지하며 VDB 업데이트를 통해 제공되지만, FireSIGHT 시스템에 대한 업데이트와 함께 제공될 수도 있습니다. 이러한 탐지기는 Cisco Professional Services에 의해 중요한 탐지기로써 제공될 수도 있습니다.

조직의 필요에 따라 클라이언트 탐지기를 활성화 및 비활성화할 수 있습니다. VDB 업데이트는 클라이언트 탐지기를 활성화 또는 비활성화할 수도 있습니다. 클라이언트 탐지기는 가져온 경우에만 내보낼 수 있습니다.

Google Earth 및 Immunet 탐지기가 클라이언트 탐지기의 예입니다.

Cisco 제공 웹 애플리케이션 탐지기

Cisco 제공 *웹 애플리케이션 탐지기*는 HTTP 트래픽에서 웹 애플리케이션을 탐지하며 VDB 업데이트를 통해 제공되지만, FireSIGHT 시스템에 대한 업데이트와 함께 제공될 수도 있습니다.

조직의 필요에 따라 웹 애플리케이션 탐지기를 활성화 및 비활성화할 수 있습니다. VDB 업데이트는 웹 애플리케이션 탐지기를 활성화 또는 비활성화할 수 있습니다. 웹 애플리케이션 탐지기의 예로는 Blackboard 및 LiveJournal 탐지기가 있습니다.

Cisco 제공 애플리케이션 프로토콜(포트) 탐지기

*포트 기반 애플리케이션 프로토콜 탐지기*는 Cisco에서 제공하며, 잘 알려진 포트의 네트워크 트래픽 탐지를 기반으로 합니다. 이러한 탐지기는 VDB 업데이트를 통해 제공되지만, FireSIGHT 시스템에 대한 업데이트와 함께 제공되거나 Cisco에 의해 중요한 탐지기로써 제공될 수도 있습니다.

조직의 필요에 따라 애플리케이션 프로토콜 탐지기를 활성화 및 비활성화할 수 있습니다. 사용자 지정 탐지기에 대한 기반으로 사용하기 위해 탐지기 정의를 볼 수도 있습니다. VDB 업데이트는 애플리케이션 프로토콜 탐지기를 활성화 또는 비활성화할 수 있습니다.

Chargen 및 Finger 탐지기가 포트 탐지기의 예입니다.

Cisco 제공 애플리케이션 프로토콜(FireSIGHT) 탐지기

FireSIGHT 기반 애플리케이션 프로토콜 탐지기는 Cisco에서 제공하며, FireSIGHT 애플리케이션 핑거프린트를 사용하는 네트워크 트래픽 탐지를 기반으로 합니다. 이러한 탐지기는 VDB 업데이트를 통해 제공되지만, FireSIGHT 시스템에 대한 업데이트와 함께 제공될 수도 있습니다.

조직의 필요에 따라 애플리케이션 프로토콜 탐지기를 활성화 및 비활성화할 수 있습니다. VDB 업데이트는 Cisco 제공 애플리케이션 프로토콜 탐지기를 활성화 또는 비활성화할 수 있습니다. FireSIGHT 기반 애플리케이션 프로토콜 탐지기의 예로는 Jabber 및 Steam 탐지기가 있습니다.

애플리케이션 프로토콜(패턴) 탐지기

*패턴 기반 애플리케이션 탐지기*는 네트워크 트래픽에서 오는 패킷의 패턴 탐지를 기반으로 합니다. 이러한 탐지기는 Cisco Professional Services에 의해 중요한 탐지기로써 제공될 수도 있고 사용자가 생성할 수도 있습니다. 이러한 탐지기를 사용하면 FireSIGHT 시스템을 전체적으로 업데이트하지 않고도 새로운 패턴 기반 탐지기로 시스템의 탐지 기능을 향상할 수 있습니다.

조직의 필요에 따라 애플리케이션 프로토콜 탐지기를 활성화 및 비활성화할 수 있습니다.

가져온 사용자 정의 탐지기는 완전히 제어할 수 있으며 활성화, 비활성화, 수정, 가져오기, 내보내기 및 삭제할 수 있습니다. 패턴 기반 탐지기의 예는 사용자 지정 애플리케이션에 대한 트래픽을 탐지하기 위해 패킷 헤더의 패턴을 사용하는 사용자 정의 탐지기입니다.

FireSIGHT 시스템의 버전 및 설치한 VDB에 따라, 가져왔거나 생성한 개별 탐지기에 따라 탐지기 목록이 변경될 수 있습니다. 각 FireSIGHT 시스템 업데이트에 대한 릴리스 정보는 물론 업데이트된 탐지기 정보의 각 VDB 업데이트에 대한 자문 내용도 주의 깊게 읽어야 합니다.

자세한 내용은 다음 링크를 참고하십시오.

- 45-10페이지의 애플리케이션 탐지 이해
- 46-19페이지의 사용자 정의 애플리케이션 프로토콜 탐지기 생성
- 46-24페이지의 탐지기 관리

사용자 정의 애플리케이션 프로토콜 탐지기 생성

라이센스: FireSIGHT

네트워크에서 사용자 지정 애플리케이션을 사용하는 경우, 애플리케이션 식별에 필요한 정보를 시스템에 제공하는 사용자 정의 애플리케이션 프로토콜 탐지기를 사용할 수 있습니다. 애플리케이션 트래픽에서 사용하는 포트, 트래픽 내 패턴 또는 포트와 패턴 모두에 애플리케이션 프로토콜 탐지의 기반을 둘 수 있습니다.

예를 들어, 사용자 지정 애플리케이션 프로토콜에 대한 트래픽이 포트 1180을 사용할 것으로 예상하는 경우 해당 포트에서 트래픽을 탐지하는 애플리케이션 프로토콜 탐지기를 생성할 수 있습니다. 또 다른 예로, 애플리케이션 프로토콜 트래픽을 포함하는 패킷의 헤더에 `ApplicationName` 문자열이 있음을 알고 있는 경우 `ApplicationName`의 ASCII 문자열을 매칭할 패턴으로 등록하는 탐지기를 생성할 수 있습니다.

사용자 정의 애플리케이션 탐지기는 애플리케이션 프로토콜에 **대해서만** 생성할 수 있고, 클라이언트 또는 웹 애플리케이션에 대해서는 생성할 수 **없습니다**. 각각에 대한 설명은 45-10페이지의 애플리케이션 탐지 이해을/를 참조하십시오. 서버 트래픽에서 애플리케이션 프로토콜의 탐지 및 식별을 시작하려면, 클라이언트 세션에 시스템에 대한 서버의 Responder 패킷이 포함되어야 합니다. UDP 트래픽의 경우 시스템은 Responder 패킷의 소스를 서버로 지정합니다.

주의 새 애플리케이션 탐지기를 생성 및 활성화하면 트래픽 플로우가 잠시 중지되고 관리되는 디바이스에서 프로세싱이 발생할 수 있는데, 이 경우 일부 패킷이 검사 없이 통과될 수 있습니다.

사용자 정의 애플리케이션 프로토콜 탐지기는 포트 또는 패턴 매치를 사용해야 합니다. 기존 탐지기를 기반으로 하더라도, 둘 모두 사용하지 않는 탐지기는 생성할 수 없습니다. 두 기준을 모두 사용하는 탐지기를 생성할 수도 있습니다. 그러면 해당 애플리케이션 프로토콜에 대한 트래픽을 올바르게 식별할 가능성이 높아집니다.

팁 또 다른 방어 센터에서 이미 탐지기를 생성한 경우 이를 내보낸 다음 이 방어 센터로 가져올 수 있습니다. 그런 다음 가져온 탐지기를 필요에 맞게 수정할 수 있습니다. 사용자 정의 탐지기는 물론 Cisco Professional Services에서 제공한 탐지기도 내보내고 가져올 수 있습니다. 그러나 다른 유형의 Cisco 제공 탐지기는 내보내거나 가져올 수 **없습니다**. 자세한 내용은 A-1페이지의 컨피그레이션 가져오기 및 내보내기을/를 참조하십시오.

사용자 정의 애플리케이션 프로토콜 탐지기를 생성하려면

액세스: Admin/Discovery Admin

1단계 **Policies > Application Detectors**를 선택합니다.

Detectors 페이지가 나타납니다.

2단계 **Create Detector**를 클릭합니다.

Create Detector 페이지가 나타납니다.

3단계 탐지기 이름 및 설명 등 기본 탐지기 정보를 제공합니다.

46-20페이지의 기본 애플리케이션 프로토콜 탐지기 정보 제공을/를 참조하십시오.

4단계 선택적으로, 탐지기용 사용자 정의 애플리케이션을 생성합니다.

46-21페이지의 사용자 정의 애플리케이션 작성을/를 참조하십시오.

5단계 탐지기가 검사해야 할 트래픽의 프로토콜 및 트래픽이 사용하는 포트를 비롯한 탐지 기준을 제공합니다.

46-21페이지의 애플리케이션 프로토콜 탐지기에 대한 탐지 기준 지정을/를 참조하십시오.

6단계 선택적으로, 해당 애플리케이션 프로토콜에 대해 트래픽에서 발생하는 하나 이상의 패턴과 일치하는 트래픽을 검사하도록 탐지기를 구성합니다.

46-22페이지의 애플리케이션 프로토콜 탐지기에 탐지 패턴 추가을/를 참조하십시오.

7단계 선택적으로, 하나 이상의 PCAP 파일의 내용을 기준으로 새 탐지기를 테스트합니다.

46-23페이지의 패킷 캡처를 기준으로 애플리케이션 프로토콜 탐지기 테스트을/를 참조하십시오.

8단계 **Save**를 클릭합니다.

애플리케이션 프로토콜 탐지기가 저장됩니다.

참고 시스템이 애플리케이션 프로토콜 트래픽 분석에 사용할 수 있으려면 탐지기를 먼저 활성화해야 합니다. 자세한 내용은 46-27페이지의 탐지기 활성화 및 비활성화을/를 참조하십시오. 애플리케이션을 액세스 제어 규칙에 포함하면 탐지기가 자동으로 활성화되며, 사용 중인 동안에는 비활성화할 수 없습니다.

기본 애플리케이션 프로토콜 탐지기 정보 제공

라이센스: FireSIGHT

각 사용자 정의 애플리케이션 프로토콜 탐지기에 이름을 지정하는 것은 물론, 탐지할 애플리케이션 프로토콜을 식별해야 합니다. 선택적으로, 탐지기에 대한 간단한 설명을 제공할 수 있습니다.

사용자가 제공하는 정보 외에도 방어 센터는 탐지기가 활성 상태인지 비활성 상태인지, 탐지기가 포트 탐지기인지 패턴 탐지기인지를 나타냅니다. 탐지기가 애플리케이션 프로토콜 트래픽을 포트 및 패턴으로 식별하면 FireSIGHT 시스템에서는 이를 패턴 탐지기로 간주합니다.

기존 탐지기를 수정하는 경우 방어 센터에서는 탐지기의 작성자도 표시합니다. 사용자 정의 애플리케이션 프로토콜 탐지기의 경우 생성한 사용자가 작성자입니다. 탐지기를 가져온 사용자 또는 수정하여 저장한 사용자도 작성자입니다.

기본 애플리케이션 프로토콜 탐지기 정보를 제공하려면

액세스: Admin/Discovery Admin

1단계 Create Detector 페이지의 **Please enter a name** 필드에 탐지기의 이름을 입력합니다.

탐지기 이름은 검사 중인 트래픽에 대한 프로토콜 내에서 고유해야 합니다. 즉, TCP 탐지기와 UDP 탐지기는 동일한 이름으로 생성할 수 있지만 두 개의 TCP 탐지기는 동일한 이름으로 생성할 수 없습니다.

2단계 탐지할 애플리케이션 프로토콜을 식별합니다. 다음 옵션을 이용할 수 있습니다.

- 기존 애플리케이션 프로토콜에 대한 탐지기를 생성하는 경우(예: 비표준 포트에서 특정 애플리케이션 프로토콜을 탐지하려는 경우), **Application Protocol** 드롭다운 목록에서 애플리케이션 프로토콜을 선택합니다. 46-21페이지의 애플리케이션 프로토콜 탐지기에 대한 탐지 기준 지정에서 절차를 계속 진행합니다.

- 사용자 지정 애플리케이션에 대한 탐지기를 생성하는 경우 다음 절, 사용자 정의 애플리케이션 작성에서 절차를 계속 진행합니다.

사용자 정의 애플리케이션 작성

라이센스: FireSIGHT

네트워크에서 사용자 지정 애플리케이션을 식별하려면 사용자 정의 애플리케이션을 생성할 수 있습니다. 애플리케이션을 설명하기 위한 사용자 지정 카테고리 및 사용자 지정 태그도 생성할 수 있습니다. 여기서 생성하는 애플리케이션, 카테고리 및 태그는 액세스 제어 규칙과 애플리케이션 필터 객체 관리자에서도 사용할 수 있습니다.

애플리케이션 프로토콜과 카테고리, 태그, 위험 레벨, 이들의 설명에 사용되는 비즈니스 연관성의 설명을 비롯한 애플리케이션 탐지에 대한 자세한 내용은 45-10페이지의 애플리케이션 탐지 이해을/를 참조하십시오.

사용자 정의 애플리케이션을 생성하려면

액세스: Admin/Discovery Admin

1단계 Create Detector 페이지에서 **Add**를 클릭합니다.

Application Editor 팝업 창이 나타납니다.

2단계 사용자 지정 애플리케이션의 **Name**을 입력합니다.

3단계 사용자 지정 애플리케이션의 **Description**을 입력합니다.

4단계 **Business Relevance**를 선택합니다.

5단계 **Risk**를 선택합니다.

6단계 카테고리를 추가하려면 Categories 옆에 있는 **Add**를 클릭하고, 새 카테고리 이름을 입력하거나 **Categories** 드롭다운 목록에서 기존 카테고리를 선택합니다.

7단계 선택적으로, 태그를 추가하려면 Tags 옆에 있는 **Add**를 클릭하고, 새 태그 이름을 입력하거나 **Tags** 드롭다운 목록에서 기존 태그를 선택합니다.

OK를 클릭하여 Create Detector 페이지로 돌아갑니다.

8단계 다음 절, 애플리케이션 프로토콜 탐지기에 대한 탐지 기준 지정에서 절차를 계속 진행합니다.

애플리케이션 프로토콜 탐지기에 대한 탐지 기준 지정

라이센스: FireSIGHT

사용자 정의 애플리케이션 프로토콜 탐지기를 생성할 때에는 탐지기가 검사해야 할 트래픽의 프로토콜(TCP, UDP 또는 둘 다)을 지정해야 합니다. 선택적으로, 트래픽이 사용하는 포트를 지정할 수 있습니다.

포트를 지정하지 않는 경우 하나 이상의 패턴과 일치하는 트래픽을 검사하도록 탐지기를 구성해야 합니다(46-22페이지의 애플리케이션 프로토콜 탐지기에 탐지 패턴 추가 참조).

애플리케이션 프로토콜 탐지기에 대한 탐지 기준을 지정하려면

액세스: Admin/Discovery Admin

1단계 Create Detector 페이지의 **Protocol** 드롭다운 목록에서 탐지기가 검사해야 할 트래픽에 대한 프로토콜을 선택합니다.

탐지기는 TCP나 UDP, 또는 TCP 및 UDP 트래픽을 검사할 수 있습니다.

2단계 사용하는 포트를 기준으로 애플리케이션 프로토콜 트래픽을 식별하려면 **Port(s)** 필드에 1~65535 범위의 포트를 입력합니다. 여러 포트를 사용하려면 쉼표로 구분합니다.

3단계 다음 옵션을 이용할 수 있습니다.

- 애플리케이션 프로토콜에 대한 트래픽에서 발생하는 하나 이상의 패턴과 일치하는 트래픽을 검사하도록 애플리케이션 프로토콜 탐지기를 구성하려는 경우 다음 절, 애플리케이션 프로토콜 탐지기에 탐지 패턴 추가에서 절차를 계속 진행합니다.
- 하나 이상의 PCAP 파일의 내용을 기준으로 새 탐지기를 테스트하려면 46-23페이지의 패킷 캡처를 기준으로 애플리케이션 프로토콜 탐지기 테스트로 건너뜁니다.
- 탐지기 생성을 완료하면 **Save**를 클릭합니다.

  애플리케이션 프로토콜 탐지기가 저장됩니다.

시스템이 애플리케이션 프로토콜 트래픽 분석에 사용할 수 있으려면 탐지기를 먼저 활성화해야 합니다. 자세한 내용은 46-27페이지의 탐지기 활성화 및 비활성화을/를 참조하십시오.

애플리케이션 프로토콜 탐지기에 탐지 패턴 추가

라이센스: FireSIGHT

애플리케이션 프로토콜 트래픽이 포함된 패킷의 헤더에 특정 패턴 문자열이 있음을 알고 있는 경우, 해당 패턴을 검색하도록 사용자 정의 애플리케이션 프로토콜 탐지기를 구성할 수 있습니다.

애플리케이션 프로토콜 탐지기는 ASCII 또는 16진수 패턴을 검색할 수 있습니다(임의의 오프셋 사용). 여러 패턴을 검색하도록 탐지기를 구성할 수도 있습니다. 이 경우 애플리케이션 프로토콜을 긍정적으로 식별하려면 애플리케이션 프로토콜 트래픽은 탐지기에 대한 모든 패턴을 매칭해야 합니다.

패턴을 지정하지 않는 경우 하나 이상의 포트를 사용하는 트래픽을 검사하도록 탐지기를 구성해야 합니다(46-21페이지의 애플리케이션 프로토콜 탐지기에 대한 탐지 기준 지정 참조).

애플리케이션 프로토콜 탐지기에 탐지 패턴을 추가하려면

액세스: Admin/Discovery Admin

1단계 Create Detector 페이지의 Detection Patterns 섹션에서 **Add**를 클릭합니다.

Add Pattern 팝업 창이 나타납니다.

2단계 탐지할 패턴 유형(**Ascii** 또는 **Hex**)을 지정합니다.

3단계 **Pattern String** 필드에서 지정한 유형의 문자열을 입력합니다.

4단계 선택적으로, 시스템이 패킷의 어디에서 패턴 검색을 시작해야 하는지를 지정합니다. 이를 오프셋이라고 합니다.

Offset 필드에 오프셋을 입력합니다(패킷 페이로드 시작 부분으로부터 바이트 단위로).

패킷 페이로드는 바이트 0에서 시작되므로, 패킷 페이로드의 시작 부분부터 진행할 바이트의 수에서 1을 뺀 값으로 오프셋을 계산합니다. 예를 들어 패킷의 5번째 비트에서 패턴을 검색하려면 **Offset** 필드에 4를 입력합니다.

5단계 선택적으로, 1~4단계를 반복하여 패턴을 추가합니다.

팁 패턴을 삭제하려면 삭제할 패턴 옆에 있는 삭제 아이콘( )을 클릭합니다.

6단계 다음 옵션을 이용할 수 있습니다.

- 하나 이상의 PCAP 파일의 내용을 기준으로 새 탐지기를 테스트하려면 다음 절, 패킷 캡처를 기준으로 애플리케이션 프로토콜 탐지기 테스트에서 절차를 계속 진행합니다.
- 탐지기 생성을 완료하면 **Save**를 클릭합니다.

  애플리케이션 프로토콜 탐지기가 저장됩니다.

참고 시스템이 애플리케이션 프로토콜 트래픽 분석에 사용할 수 있으려면 탐지기를 먼저 활성화해야 합니다. 자세한 내용은 46-27페이지의 탐지기 활성화 및 비활성화을/를 참조하십시오.

패킷 캡처를 기준으로 애플리케이션 프로토콜 탐지기 테스트

라이센스: FireSIGHT

탐지하려는 애플리케이션 프로토콜에서 온 트래픽의 패킷을 포함하는 PCAP(패킷 캡처) 파일이 있는 경우 PCAP 파일을 기준으로 사용자 정의 애플리케이션 프로토콜 탐지기를 테스트할 수 있습니다. PCAP 파일은 32KB 이하여야 합니다. 더 큰 PCAP 파일을 기준으로 탐지기를 테스트하려고 시도하면 방어 센터에서 자동으로 파일을 자릅니다.

PCAP 파일을 기준으로 애플리케이션 프로토콜 탐지기를 테스트하려면

액세스: Admin/Discovery Admin

1단계 Create Detector 페이지의 Packet Captures 섹션에서 **Add**를 클릭합니다.

팝업 창이 나타납니다.

2단계 PCAP 파일을 찾은 다음 **OK**를 클릭합니다.

Packet Captures 파일 목록에 PCAP 파일이 나타납니다.

3단계 PCAP 파일의 내용을 기준으로 탐지기를 테스트하려면 PCAP 파일 옆에 있는 평가 아이콘을 클릭합니다.

테스트 성공 여부를 알려주는 메시지가 나타납니다.

4단계 선택적으로, 추가 PCAP 파일을 기준으로 탐지기를 테스트하려면 1~3단계를 반복합니다.

팁 PCAP 파일을 삭제하려면 삭제할 파일 옆에 있는 삭제 아이콘( )을 클릭합니다.

5단계 탐지기를 저장하려면 **Save**를 클릭합니다.

참고 시스템이 애플리케이션 프로토콜 트래픽 분석에 사용할 수 있으려면 탐지기를 먼저 활성화해야 합니다. 자세한 내용은 46-27페이지의 탐지기 활성화 및 비활성화을/를 참조하십시오.

탐지기 관리

라이센스: FireSIGHT

Detectors 페이지에서 탐지기를 보고 관리합니다.

Detectors 페이지에서 다음을 수행할 수 있습니다.

- 탐지기가 식별하는 애플리케이션에 대한 세부사항 보기
- 탐지기 목록 정렬, 필터링 및 찾아보기
- Cisco 제공 내부 탐지기의 목록 보기
- Cisco 제공 애플리케이션 프로토콜 포트 탐지기의 속성 보기 및 선택적으로, 수정할 수 있는 새로운 사용자 정의 탐지기로 저장하기
- 사용자 정의 애플리케이션 프로토콜 탐지기 생성, 수정, 삭제 및 내보내기
- 개별적으로 가져온 애플리케이션 프로토콜 탐지기 삭제 및 내보내기
- 사용자 정의 탐지기, 가져온 탐지기, Cisco 제공 웹 애플리케이션 탐지기, 클라이언트 탐지기, 애플리케이션 프로토콜 탐지기 활성화 및 비활성화

내부 또는 Cisco 제공 애플리케이션 프로토콜 탐지기, 클라이언트 탐지기, 웹 애플리케이션 탐지기는 수정 또는 삭제할 수 없으며 내부 탐지기는 비활성화할 수 없습니다.

자세한 내용은 다음 링크를 참고하십시오.

- 46-24페이지의 탐지기 세부사항 보기
- 46-25페이지의 탐지기 목록 정렬
- 46-25페이지의 탐지기 목록 필터링
- 46-27페이지의 다른 탐지기 페이지로 이동
- 46-27페이지의 탐지기 활성화 및 비활성화
- 46-28페이지의 애플리케이션 탐지기 수정
- 46-29페이지의 탐지기 삭제

탐지기 세부사항 보기

라이센스: FireSIGHT

애플리케이션 탐지기 목록에서 탐지기에 대한 세부사항을 볼 수 있습니다.

애플리케이션 탐지기 세부사항을 보려면

액세스: Admin/Discovery Admin

1단계 Details 열에서 정보 아이콘( )을 클릭합니다.

탐지기의 정보 팝업 창이 나타납니다.

위험, 비즈니스 연관성, 태그 및 카테고리에 대한 자세한 내용은 45-10페이지의 애플리케이션 탐지 이해을/를 참조하십시오.

탐지기 목록 정렬

라이센스: FireSIGHT

기본적으로 Detectors 페이지에는 탐지기가 이름별 알파벳순으로 나열됩니다. 열 머리글 옆의 위로 (▲) 또는 아래로 화살표는 해당 열이 그 방향으로 정렬됨을 나타냅니다.

탐지기를 정렬하려면

액세스: Admin/Discovery Admin

1단계 Detectors 페이지에서 원하는 열 머리글을 클릭합니다.

열 머리글에 나타나는 화살표의 방향으로 탐지기가 정렬됩니다. 반대 방향으로 정렬하려면 머리글을 다시 클릭합니다.

탐지기 목록 필터링

라이센스: FireSIGHT

Detectors 페이지에 표시된 탐지기를 단일 기준 또는 여러 기준의 조합으로 필터링할 수 있습니다. 구성한 필터는 페이지 위에 나타납니다. 탐지기 목록을 필터링하는 데 여러 필터 그룹을 별도로 사용할 수도 있고 함께 사용할 수도 있습니다.

Name

입력한 문자열이 들어 있는 이름이나 설명의 탐지기를 찾습니다. 문자열에는 영숫자나 특수 문자를 포함할 수 있습니다.

Custom Filter

객체 관리 페이지에서 생성된 사용자 지정 애플리케이션 필터와 일치하는 탐지기를 찾습니다. 자세한 내용은 3-15페이지의 애플리케이션 필터 작업을/를 참조하십시오.

Author

탐지기를 생성한 사용자에 따라 탐지기를 찾습니다. 탐지기를 다음 기준으로 필터링할 수 있습니다.

- 탐지기를 생성하거나 가져온 개별 사용자
- **Cisco** - 모든 Cisco 제공 탐지기를 나타냅니다. *단*, 개별적으로 가져온 애드온 탐지기는 예외입니다. 탐지기를 가져온 사용자는 탐지기의 작성자가 됩니다.
- **Any User** - Cisco에서 제공하지 않은 모든 탐지기를 나타냅니다.

State

상태(즉, **Active** 또는 **Inactive**)에 따라 탐지기를 찾습니다. 자세한 내용은 46-27페이지의 탐지기 활성화 및 비활성화을/를 참조하십시오.

Type

탐지기 유형(**Application Protocol**, **Web Application**, **Client**, 또는 **Internal Detector**)에 따라 탐지기를 찾습니다.

애플리케이션 프로토콜 탐지기에는 탐지기를 추가로 필터링하는 데 사용할 수 있는 세 가지 하위 유형이 있습니다.

- **Port** 애플리케이션 프로토콜 탐지기에는 Cisco에서 제공하는 잘 알려진 포트 탐지기 및 포트 기반 사용자 정의 애플리케이션 탐지기가 포함됩니다.
- **Pattern** 애플리케이션 프로토콜 탐지기에는 패턴 기반 또는 포트 및 패턴 기반 사용자 정의 애플리케이션 탐지기가 포함됩니다.
- **FireSIGHT** 애플리케이션 프로토콜 탐지기는 활성화 및 비활성화할 수 있는, Cisco에서 제공하는 애플리케이션 프로토콜 핑거프린트 탐지기입니다.

탐지기 유형에 대한 자세한 내용은 46-17페이지의 애플리케이션 탐지기 작업을/를 참조하십시오.

Protocol

탐지기가 검사하는 트래픽 프로토콜에 따라 탐지기를 찾습니다. 탐지기는 TCP나 UDP, 또는 TCP 및 UDP 트래픽을 검사할 수 있습니다.

Category

탐지하는 애플리케이션에 할당된 카테고리에 따라 탐지기를 찾습니다.

Tag

탐지하는 애플리케이션에 할당된 태그에 따라 탐지기를 찾습니다.

Risk

탐지하는 애플리케이션에 할당된 위험(**Very High**, **High**, **Medium**, **Low** 및 **Very Low**)에 따라 탐지기를 찾습니다.

Business Relevance

탐지하는 애플리케이션에 할당된 비즈니스 연관성(**Very High**, **High**, **Medium**, **Low** 및 **Very Low**)에 따라 탐지기를 찾습니다.

필터를 적용하려면

Admin/Discovery Admin

1단계 Detectors 페이지에서 탐지기 필터링에 사용할 필터 그룹을 확장합니다.

2단계 사용할 필터의 이름을 입력하거나 특정 필터를 선택합니다. 그룹의 모든 필터를 선택하려면 그룹 이름을 마우스 오른쪽 버튼으로 클릭하고 **Check All**을 선택합니다.

3단계 선택적으로, 사용 중인 필터에 하위 필터가 있는 경우 탐지기를 추가로 필터링하려면 하위 필터를 선택합니다.

필터를 제거하려면

액세스: Admin/Discovery Admin

1단계 **Filters** 필드의 필터 이름에서 제거 아이콘(✖)을 클릭하거나 필터 목록에서 필터를 비활성화합니다. 그룹의 모든 필터를 제거하려면 그룹 이름을 마우스 오른쪽 버튼으로 클릭하고 **Uncheck All**을 선택합니다.

필터가 제거되고 결과가 업데이트됩니다.

모든 필터를 제거하려면

액세스: Admin/Discovery Admin

1단계 탐지기에 적용된 필터 목록 옆에 있는 **Clear all**을 클릭합니다.

다른 탐지기 페이지로 이동

라이센스: FireSIGHT

Detectors 페이지에는 동시에 25개의 탐지기가 표시됩니다. 다음 표에서는 페이지의 하단에 있는 탐색 링크를 사용하여 탐지기의 추가 페이지를 보는 방법에 대해 설명합니다.

액세스: Admin/Discovery Admin

표 46-1 탐지기 페이지 탐색

목적	가능한 작업
다음 페이지 보기	오른쪽 화살표 아이콘( )을 클릭합니다.
이전 페이지 보기	왼쪽 화살표 아이콘( )을 클릭합니다.
다른 페이지 보기	페이지 번호를 입력하고 Enter 키를 누릅니다.
마지막 페이지로 바로 이동	오른쪽 끝 화살표 아이콘( )을 클릭합니다.
첫 페이지로 바로 이동	왼쪽 끝 화살표 아이콘( )을 클릭합니다.

탐지기 활성화 및 비활성화

라이센스: FireSIGHT

네트워크 트래픽 분석에 사용할 수 있으려면 탐지기를 먼저 활성화해야 합니다. 기본적으로 모든 Cisco 제공 탐지기는 활성화되어 있습니다.

시스템의 탐지 기능을 보완하기 위해 각 포트에 대해 여러 애플리케이션 탐지기를 활성화할 수 있습니다.

정책의 액세스 제어 규칙에 애플리케이션이 포함되어 있고 정책이 적용될 때 해당 애플리케이션에 대한 활성 탐지기가 없으면 하나 이상의 탐지기가 자동으로 활성화됩니다. 마찬가지로, 적용된 정책에서 애플리케이션이 사용 중일 때 탐지기를 비활성화하여 해당 애플리케이션에 대한 활성 탐지기가 없어지면 탐지기를 비활성화할 수 없습니다.

주의 기존 탐지기를 활성화 또는 비활성화하면 트래픽 플로우가 잠시 중지되고 관리되는 디바이스에서 프로세싱이 발생할 수 있는데, 이 경우 일부 패킷이 검사 없이 통과될 수 있습니다.

팁 성능을 높이려면 관심이 없는 애플리케이션 프로토콜, 클라이언트 또는 웹 애플리케이션 탐지기를 비활성화하십시오.

탐지기를 활성화 또는 비활성화하려면

액세스: Admin/Discovery Admin

1단계 **Policies > Application Detectors**를 선택합니다.

Detectors 페이지가 나타납니다.

2단계 활성화 또는 비활성화할 탐지기를 찾습니다.

활성화 또는 비활성화할 탐지기가 첫 번째 페이지에 없으면 탐지기 목록에서 이동하거나 하나 이상의 필터를 적용하여 찾을 수 있습니다. 자세한 내용은 46-24페이지의 탐지기 관리을/를 참조하십시오.

3단계 다음 옵션을 이용할 수 있습니다.

- 시스템이 네트워크 트래픽 분석에 사용하도록 탐지기를 **활성화**하려면 탐지기 옆에 있는 비활성 슬라이더()를 클릭합니다.
- 시스템이 네트워크 트래픽 분석에 사용하지 않도록 탐지기를 **비활성화**하려면 탐지기 옆에 있는 활성 슬라이더()를 클릭합니다.

일부 애플리케이션 탐지기는 다른 탐지기에 필요합니다. 이러한 탐지기 중 하나를 비활성화하면, 여기에 의존하는 탐지기도 비활성화됨을 알리는 경고가 나타납니다.

애플리케이션 탐지기 수정

라이센스: FireSIGHT

사용자 정의 애플리케이션 탐지기를 수정하려면 다음 절차를 사용하십시오.

애플리케이션 탐지기를 수정하려면

액세스: Admin/Discovery Admin

1단계 **Policies > Applications**를 선택합니다.

Detectors 페이지가 나타납니다.

2단계 수정할 탐지기를 찾습니다.

수정할 탐지기가 첫 번째 페이지에 없으면 탐지기 목록에서 이동하거나 하나 이상의 필터를 적용하여 찾을 수 있습니다. 자세한 내용은 46-24페이지의 탐지기 관리을/를 참조하십시오.

3단계 사용자 정의 탐지기를 수정하려면 수정할 탐지기 옆에 있는 **Edit**를 클릭합니다.

Edit Application Detector 페이지가 나타납니다.

4단계 탐지기를 수정합니다.

변경할 수 있는 각종 컨피그레이션에 대한 자세한 내용은 46-19페이지의 사용자 정의 애플리케이션 프로토콜 탐지기 생성을/를 참조하십시오.

5단계 다음 옵션을 이용할 수 있습니다.

- 비활성 상태의 사용자 정의 탐지기를 수정하는 경우 변경 사항을 저장하려면 **Save**를 클릭하고, 탐지기를 비활성 상태의 새로운 사용자 정의 탐지기로 저장하려면 **Save as New**를 클릭합니다.
- 활성 상태의 사용자 정의 탐지기를 수정하는 경우 변경 사항을 저장하고 수정된 탐지기를 즉시 시작하려면 **Save and Reactivate**를 클릭하고, 탐지기를 비활성 상태의 새로운 사용자 정의 탐지기로 저장하려면 **Save as New**를 클릭합니다.

참고 시스템은 애플리케이션 트래픽을 분석하는 데 활성 탐지기의 애플리케이션만 사용합니다. 자세한 내용은 46-27페이지의 탐지기 활성화 및 비활성화을/를 참조하십시오.

탐지기 삭제

라이센스: FireSIGHT

탐지기를 삭제하려면 다음 절차를 사용하십시오. 사용자 정의 탐지기는 물론 Cisco Professional Services에서 제공한, 개별적으로 가져온 애드온 탐지기도 삭제할 수 있습니다. 그러나 다른 Cisco 제공 탐지기는 삭제할 수 없습니다(이들 중 다수는 비활성화 가능).

참고 적용된 정책에서 탐지기가 사용 중인 동안에는 탐지기를 비활성화하거나 삭제할 수 없습니다.

탐지기를 삭제하려면

액세스: Admin/Discovery Admin

1단계 **Policies > Application Detectors**를 선택합니다.

Detectors 페이지가 나타납니다.

2단계 삭제할 탐지기 옆에 있는 확인란을 선택한 다음 **Delete**를 클릭합니다.

삭제할 탐지기가 첫 번째 페이지에 없으면 탐지기 목록에서 이동하거나 하나 이상의 필터를 적용하여 찾을 수 있습니다. 자세한 내용은 46-24페이지의 탐지기 관리을/를 참조하십시오.

3단계 **OK**를 클릭하여 탐지기를 삭제할 것임을 확인합니다.

탐지기가 삭제됩니다.

호스트 입력 데이터 가져오기

라이센스: FireSIGHT

조직이 서드파티의 네트워크 맵 데이터를 가져오기 위해 스크립트를 작성하거나 명령줄 가져오기 파일을 생성할 수 있는 경우, 네트워크 맵의 정보를 보강하기 위해 데이터를 가져올 수 있습니다. 또한 운영 체제나 애플리케이션 ID를 수정하여 또는 애플리케이션 프로토콜, 프로토콜, 호스트 특성, 웹 인터페이스를 사용하는 클라이언트 등을 삭제하여 호스트 입력 기능을 사용할 수 있습니다.

시스템에서는 운영 체제 또는 애플리케이션의 현재 ID를 확인하기 위해 여러 소스의 데이터를 조정할 수 있습니다. 시스템에서 이를 수행하는 방법에 대한 자세한 내용은 46-5페이지의 현재 ID 이해을/를 참조하십시오.

영향받는 호스트가 네트워크 맵에서 제거되면 서드파티 취약성을 제외한 모든 데이터가 폐기됩니다. 스크립트 설정 또는 파일 가져오기에 대한 자세한 내용은 *FireSIGHT 시스템 Host Input API Guide*를 참조하십시오.

가져온 데이터를 영향 상관관계에 포함하려면 데이터를 데이터베이스의 운영 체제 및 애플리케이션 정의에 매핑해야 합니다. 자세한 내용은 다음 절을 참조하십시오.

서드파티 데이터 사용 활성화

라이센스: FireSIGHT

네트워크의 서드파티 시스템에서 네트워크 맵 데이터를 가져올 수 있습니다. 그러나 침입 및 검색 데이터가 함께 사용되는 기능(예: FireSIGHT 권장 사항, 적응형 프로필, 영향 평가 등)을 활성화하려면 가능한 한 많은 요소를 해당 정의에 매핑해야 합니다. 서드파티 데이터 사용을 위한 다음과 같은 요구 사항을 고려해 보십시오.

- 네트워크 자산에 대한 특정 데이터가 포함된 서드파티 시스템이 있는 경우 호스트 입력 기능을 사용하여 해당 데이터를 가져올 수 있습니다. 그러나 서드파티에서 제품 이름을 다르게 지정할 수 있으므로 서드파티 공급업체, 제품 및 버전을 해당 Cisco 제품 정의에 매핑해야 합니다. 제품을 매핑한 후에는 영향 상관관계를 허용하기 위해 시스템 정책에서 영향 평가를 위한 취약성 매핑을 활성화해야 합니다. 버전 또는 공급업체가 없는 애플리케이션 프로토콜의 경우 시스템 정책에서 애플리케이션 프로토콜에 대한 취약성을 매핑해야 합니다. 자세한 내용은 46-31페이지의 서드파티 제품 매핑을/를 참조하십시오.
- 서드파티에서 패치 정보를 가져오고 해당 패치에 의해 수정된 모든 취약성을 무효 상태로 표시하려면 서드파티 수정 이름을 데이터베이스의 수정 정의에 매핑해야 합니다. 그러면 수정에 의해 해결된 모든 취약성이 해당 수정을 추가한 호스트에서 제거됩니다. 자세한 내용은 46-32페이지의 서드파티 제품 수정 매핑을/를 참조하십시오.
- 서드파티에서 운영 체제 및 애플리케이션 프로토콜 취약성을 가져와서 영향 상관관계에 사용하려면 서드파티 취약성 식별 문자열을 데이터베이스의 취약성에 매핑해야 합니다. 관련된 취약성이 있는 클라이언트가 많고 영향 평가에 클라이언트가 사용되지만, 서드파티 클라이언트 취약성을 가져와서 매핑할 수는 없습니다. 취약성을 매핑한 후에는 시스템 정책에서 영향 평가를 위한 서드파티 취약성 매핑을 활성화해야 합니다. 자세한 내용은 46-33페이지의 서드파티 취약성 매핑을/를 참조하십시오. 공급업체 또는 버전 정보가 없는 애플리케이션 프로토콜을 취약성에 매핑하려면 관리 사용자는 시스템 정책에서 애플리케이션에 대한 취약성을 매핑해야 합니다. 자세한 내용은 63-30페이지의 서버에 대한 취약성 매핑을/를 참조하십시오.
- 애플리케이션 데이터를 가져와 영향 상관관계에 사용하려는 경우 각 애플리케이션 프로토콜에 대한 공급업체 문자열을 해당 Cisco 애플리케이션 프로토콜 정의에 매핑해야 합니다. 자세한 내용은 46-34페이지의 사용자 지정 제품 매핑 관리을/를 참조하십시오.

서드파티 제품 매핑 관리

라이센스: FireSIGHT

사용자 입력 기능을 통해 서드파티의 데이터를 네트워크 맵에 추가할 때에는 서드파티에서 사용하는 공급업체, 제품 및 버전 이름을 Cisco 제품 정의에 매핑해야 합니다. 제품을 Cisco 정의에 매핑하면 정의를 기반으로 취약성이 할당됩니다.

마찬가지로, 서드파티에서 패치 정보(예: 패치 관리 제품)를 가져오는 경우 수정의 이름을 데이터베이스의 적절한 공급업체와 제품 그리고 해당 수정에 매핑해야 합니다.

자세한 내용은 다음 절을 참조하십시오.

- 46-31페이지의 서드파티 제품 매핑
- 46-32페이지의 서드파티 제품 수정 매핑

서드파티 제품 매핑

라이센스: FireSIGHT

서드파티의 데이터를 가져오는 경우 취약성을 할당하고 해당 데이터로 영향 상관관계를 수행하려면 Cisco 제품을 서드파티 이름에 매핑해야 합니다. 제품을 매핑하면 Cisco 취약성 정보가 서드파티 제품 이름과 연결되며, 이를 통해 시스템에서는 해당 데이터를 사용해 영향 상관관계를 수행할 수 있습니다.

호스트 입력 가져오기 기능을 사용하여 데이터를 가져올 경우 AddScanResult 기능을 사용하여 가져오는 동안 서드파티 제품을 운영 체제 및 애플리케이션 취약성에 매핑해야 합니다.

예를 들어 애플리케이션 이름이 Apache Tomcat으로 나열되고 제품 버전이 6인 서드파티 데이터를 가져오는 경우 **Vendor Name**이 `Apache`, **Product Name**이 `Tomcat`으로 설정된 서드파티 맵을 추가할 수 있습니다. **Vendor** 드롭다운 목록에서 **Apache**, **Product** 드롭다운 목록에서 **Tomcat**, **Version** 드롭다운 목록에서 **6**을 선택합니다. 이렇게 매핑하면 Apache Tomcat 6에 대한 취약성이 Apache Tomcat에 대한 애플리케이션 목록과 함께 호스트에 할당됩니다.

버전 또는 공급업체가 없는 애플리케이션의 경우 시스템 정책에서 애플리케이션 유형에 대한 취약성을 매핑해야 합니다. 자세한 내용은 63-30페이지의 서버에 대한 취약성 매핑을/를 참조하십시오. 관련된 취약성이 있는 클라이언트가 많고 영향 평가에 클라이언트가 사용되지만, 서드파티 클라이언트 취약성을 가져와서 매핑할 수는 없습니다.

팁 또 다른 방어 센터에서 이미 서드파티 매핑을 생성한 경우 이를 내보낸 다음 이 방어 센터로 가져올 수 있습니다. 그런 다음 가져온 매핑을 필요에 맞게 수정할 수 있습니다. 자세한 내용은 A-1페이지의 컨피그레이션 가져오기 및 내보내기을/를 참조하십시오.

서드파티 제품을 Cisco 제품 정의에 매핑하려면

액세스: Admin

1단계 **Policies > Application Detectors**를 선택하고 **User Third-Party Mappings**를 클릭합니다.

User Third-Party Mappings 페이지가 나타납니다.

2단계 2가지 옵션이 있습니다.

- 기존 맵 집합을 수정하려면 맵 집합 옆에 있는 **Edit**를 클릭합니다.
- 새로운 맵 집합을 생성하려면 **Create Product Map Set**를 클릭합니다.

Edit Third-Party Product Mappings 페이지가 나타납니다.

3단계 **Mapping Set Name** 필드에 매핑 집합의 이름을 입력합니다.

4단계 **Description** 필드에 설명을 입력합니다.

5단계 2가지 옵션이 있습니다.

- 서드파티 제품을 매핑하려면 **Add Product Map** 을 클릭합니다.
- 기존 서드파티 제품 맵을 수정하려면 맵 집합 옆에 있는 **Edit**를 클릭합니다.

Add Product Map 페이지가 나타납니다.

6단계 서드파티 제품에서 사용되는 공급업체 문자열을 **Vendor String** 필드에 입력합니다.

7단계 서드파티 제품에서 사용되는 제품 문자열을 **Product String** 필드에 입력합니다.

8단계 서드파티 제품에서 사용되는 버전 문자열을 **Version String** 필드에 입력합니다.

9단계 Product Mappings 섹션에서 취약성 매핑에 사용할 운영 체제, 제품 및 버전을 다음 목록에서 선택합니다(해당되는 경우).

- **벤더**
- **제품**
- **주요 버전**
- **일반 버전**
- **개정 버전**
- **구축**
- **패치**
- **확장**

예를 들어 서드파티 문자열로 이름이 구성된 제품을 실행 중인 호스트에서 Redhat Linux 9의 취약성을 사용하도록 하려면 공급업체로 **Redhat, Inc.**, 제품으로 **Redhat Linux**, 버전으로 **9**를 선택합니다.

10단계 **Save**를 클릭합니다.

서드파티 제품 수정 매핑

라이센스: FireSIGHT

수정 이름을 데이터베이스에 있는 특별한 수정 집합에 매핑하면, 서드파티 패치 관리 애플리케이션에서 데이터를 가져와 호스트 집합에 수정을 적용할 수 있습니다. 수정 이름을 호스트로 가져오면 시스템은 해당 수정으로 해결된 모든 취약성을 해당 호스트에 대해 무효 상태로 표시합니다.

서드파티 수정을 Cisco 수정 정의에 매핑하려면

액세스: Admin/

1단계 **Policies > Application Detectors**를 선택하고 **User Third-Party Mappings**를 클릭합니다.

User Third-Party Mappings 페이지가 나타납니다.

2단계 2가지 옵션이 있습니다.

- 기존 맵 집합을 수정하려면 맵 집합 옆에 있는 **Edit**를 클릭합니다.
- 새로운 맵 집합을 생성하려면 **Create Product Map Set**를 클릭합니다.

Edit Third-Party Product Mappings 페이지가 나타납니다.

3단계 **Mapping Set Name** 필드에 매핑 집합의 이름을 입력합니다.

4단계 **Description** 필드에 설명을 입력합니다.

5단계 2가지 옵션이 있습니다.

- 서드파티 제품을 매핑하려면 **Add Fix Map** 을 클릭합니다.
- 기존 서드파티 제품 맵을 수정하려면 옆에 있는 **Edit**를 클릭합니다.

Add Fix Map 페이지가 나타납니다.

6단계 매핑할 수정의 이름을 **Third-Party Fix Name** 필드에 입력합니다.

7단계 Product Mappings 섹션에서 수정 매핑에 사용할 운영 체제, 제품 및 버전을 다음 목록에서 선택합니다(해당되는 경우).

- **벤더**
- **제품**
- **주요 버전**
- **일반 버전**
- **개정 버전**
- **구축**
- **패치**
- **확장**

예를 들어 매핑을 통해 Redhat Linux 9의 선택한 수정을 패치가 적용되는 호스트에 할당하려면 공급업체로 **Redhat, Inc.**, 제품으로 **Redhat Linux**, 버전으로 **9**를 선택합니다.

8단계 **Save**를 클릭하여 수정 맵을 저장합니다.

서드파티 취약성 매핑

라이센스: FireSIGHT

서드파티의 취약성 정보를 VDB에 추가하려면 가져온 각 취약성에 대한 서드파티 식별 문자열을 기존의 Cisco, Bugtraq 또는 Snort ID에 매핑해야 합니다. 취약성에 대한 매핑을 생성하면 네트워크 맵에서 호스트로 가져온 모든 취약성에 대해 매핑이 제대로 작동하며, 그러한 취약성에 대해 영향 상관관계를 수행할 수 있게 됩니다.

상관관계가 발생하도록 하려면 서드파티 취약성에 대한 영향 상관관계를 활성화해야 합니다. 자세한 내용은 45-33페이지의 취약성 영향 평가 매핑 활성화을/를 참조하십시오. 버전 또는 공급업체가 없는 애플리케이션의 경우 시스템 정책에서 애플리케이션 유형에 대한 취약성을 매핑해야 합니다. 자세한 내용은 63-30페이지의 서버에 대한 취약성 매핑을/를 참조하십시오.

관련된 취약성이 있는 클라이언트가 많고 영향 분석에 클라이언트가 사용되지만, 영향 평가에는 서드파티 클라이언트 취약성을 사용할 수 없습니다.

팁 또 다른 방어 센터에서 이미 서드파티 매핑을 생성한 경우 이를 내보낸 다음 이 방어 센터로 가져올 수 있습니다. 그런 다음 가져온 매핑을 필요에 맞게 수정할 수 있습니다. 자세한 내용은 A-1페이지의 컨피그레이션 가져오기 및 내보내기을/를 참조하십시오.

서드파티 취약성을 기존 취약성에 매핑하려면

액세스: Admin

1단계 **Policies > Application Detectors**를 선택하고 **User Third-Party Mappings**를 클릭합니다.

User Third-Party Mappings 페이지가 나타납니다.

2단계 2가지 옵션이 있습니다.

- 기존 취약성 집합을 수정하려면 취약성 집합 옆에 있는 **Edit**를 클릭합니다.
- 새로운 취약성 집합을 생성하려면 **Create Vulnerability Map Set**를 클릭합니다.

Edit Third-Party Vulnerability Mappings 페이지가 나타납니다.

3단계 **Add Vulnerability Map**을 클릭합니다.

Add Vulnerability Map 팝업 창이 나타납니다.

4단계 **Vulnerability ID** 필드에 취약성에 대한 서드파티 ID를 입력합니다.

5단계 **Vulnerability Description** 필드에 설명을 입력합니다.

6단계 선택적으로, **Snort Vulnerability ID Mappings** 필드에 Signature ID를 입력합니다.

7단계 선택적으로, **Cisco Vulnerability ID Mappings** 필드에 Cisco 취약성 ID를 입력합니다.

8단계 선택적으로, **Bugtraq Vulnerability ID Mappings** 필드에 Bugtraq 식별 번호를 입력합니다.

9단계 **Add**를 클릭합니다.

사용자 지정 제품 매핑 관리

라이센스: FireSIGHT

서드파티에 의한 서버 입력이 적절한 Cisco 정의와 연결되었는지 확인하려면 제품 매핑을 사용할 수 있습니다. 제품 매핑을 정의 및 활성화하면, 매핑된 공급업체 문자열이 있는 네트워크 맵 호스트의 모든 서버 또는 클라이언트는 사용자 지정 제품 매핑을 사용합니다. 따라서 서버의 공급업체, 제품 및 버전을 명시적으로 설정하는 대신 특정 공급업체 문자열로 네트워크 맵에 있는 모든 서버에 대해 취약성을 매핑할 수도 있습니다.

자세한 내용은 다음을 참조하십시오.

- 46-34페이지의 사용자 지정 제품 매핑 생성
- 46-35페이지의 사용자 지정 제품 매핑 목록 수정
- 46-36페이지의 사용자 지정 제품 매핑 활성화 상태 관리

사용자 지정 제품 매핑 생성

라이센스: FireSIGHT

시스템이 네트워크 맵의 서버를 VDB의 공급업체 및 제품에 매핑할 수 없는 경우, 서버를 식별할 때 사용할 서버용 매핑을 직접 생성할 수 있습니다. 사용자 지정 제품 매핑을 활성화하면 시스템은 선택한 공급업체 및 제품에 대한 취약성을, 해당 공급업체 문자열이 발생하는 네트워크 맵의 모든 서버에 매핑합니다.

참고 사용자 지정 제품 매핑은 애플리케이션 데이터의 소스(예: Nmap, 호스트 입력 기능 또는 FireSIGHT 시스템 자체)와 상관없이 애플리케이션 프로토콜의 모든 경우에 적용됩니다. 그러나 호스트 입력 기능을 사용하여 가져온 데이터에 대한 서드파티 취약성 매핑이 사용자 지정 제품 매핑을 통해 설정한 매핑과 충돌하면, 서드파티 취약성 매핑은 사용자 지정 제품 매핑을 재정의하며 입력이 발생할 경우 서드파티 취약성 매핑 설정을 사용합니다. 자세한 내용은 46-33페이지의 서드파티 취약성 매핑을/를 참조하십시오.

제품 매핑의 목록을 생성한 다음, 각 목록을 활성화 또는 비활성화하여 여러 매핑의 사용을 동시에 활성화 또는 비활성화할 수 있습니다. 매핑할 공급업체를 선택하면 시스템은 해당 공급업체의 제품만 포함하도록 제품 목록을 업데이트합니다.

사용자 지정 제품 매핑을 생성한 후에는 사용자 지정 제품 매핑 목록을 활성화해야 합니다. 사용자 지정 제품 매핑의 목록을 활성화하면, 시스템은 지정된 공급업체 문자열이 발생할 때 모든 서버를 업데이트합니다. 호스트 입력 기능을 통해 가져온 데이터의 경우, 이 서버에 대해 제품 매핑을 이미 명시적으로 설정하지 않았다면 취약성이 업데이트됩니다.

예를 들어, 회사에서 Apache Tomcat 웹 서버에 대한 배너를 `Internal Web Server`로 수정하면 공급업체 문자열 `Internal Web Server`를 공급업체 **Apache** 및 제품 **Tomcat**에 매핑한 다음 해당 매핑이 포함된 목록을 활성화할 수 있습니다. `Internal Web Server`라는 레이블의 서버가 나타나는 모든 호스트는 데이터베이스에 Apache Tomcat에 대한 취약성을 포함합니다.

팁 이 기능을 사용하면 규칙에 대한 SID를 또 다른 취약성에 매핑하여 취약성을 로컬 침입 규칙에 매핑할 수 있습니다.

사용자 지정 제품 매핑을 생성하려면

액세스: Admin

1단계 **Policies > Application Detectors**를 선택하고 **Custom Product Mappings**를 클릭합니다.

Custom Product Mappings 페이지가 나타납니다.

2단계 **Create Custom Product Mapping List**를 클릭합니다.

Edit Custom Product Mappings List 페이지가 나타납니다.

3단계 **Custom Product Mapping List Name** 필드에 이름을 입력합니다.

4단계 **Add Vendor String**을 클릭합니다.

Add Vendor String 팝업 창이 나타납니다.

5단계 선택한 공급업체 및 제품 값에 매핑해야 할 애플리케이션을 식별하는 공급업체 문자열을 **Vendor String** 필드에 입력합니다.

6단계 매핑하고자 하는 공급업체를 **Vendor** 드롭다운 목록에서 선택합니다.

7단계 매핑하고자 하는 제품을 **Product** 드롭다운 목록에서 선택합니다.

8단계 **Add**를 클릭하여 매핑된 공급업체 문자열을 목록에 추가합니다.

9단계 선택적으로, 공급업체 문자열 매핑을 목록에 더 추가하려면 필요에 따라 4~9단계를 반복합니다.

10단계 완료하면 **Save**를 클릭합니다.

추가한 목록과 함께 Custom Product Mappings 페이지가 다시 나타납니다.

사용자 지정 제품 매핑 목록 수정

라이센스: FireSIGHT

공급업체 문자열을 추가 또는 제거하거나 목록 이름을 변경하여 기존의 사용자 지정 제품 매핑 목록을 수정할 수 있습니다.

사용자 지정 제품 매핑을 수정하려면

액세스: Admin

1단계 **Policies > Application Detectors**를 선택하고 **Custom Product Mappings**를 클릭합니다.

Custom Product Mappings 페이지가 나타납니다.

2단계 수정할 제품 매핑 목록 옆에 있는 수정 아이콘( )을 클릭합니다.

Edit Custom Product Mappings List 페이지가 나타납니다.

3단계 필요한 대로 목록을 수정합니다. 자세한 내용은 46-34페이지의 사용자 지정 제품 매핑 생성을/를 참조하십시오.

4단계 완료하면 **Save**를 클릭합니다.

업데이트한 목록과 함께 Custom Product Mappings 페이지가 나타납니다.

사용자 지정 제품 매핑 활성화 상태 관리

라이센스: FireSIGHT

사용자 지정 제품 매핑의 전체 목록 사용을 동시에 활성화 또는 비활성화할 수 있습니다. 사용자 지정 제품 매핑 목록을 활성화하면, 관리되는 디바이스에 의해 탐지되었든 호스트 입력 기능을 통해 가져왔든, 해당 목록의 각 매핑이 지정된 공급업체 문자열이 있는 네트워크 맵 호스트의 모든 애플리케이션에 적용됩니다.

사용자 지정 제품 매핑을 활성화 또는 비활성화하려면

액세스: Admin

1단계 **Policies > Application Detectors**를 선택하고 **Custom Product Mappings**를 클릭합니다.

Custom Product Mappings 페이지가 나타납니다.

2단계 사용자 지정 제품 매핑 목록의 상태를 수정합니다.

- 사용자 지정 제품 매핑 목록의 사용을 활성화하려면 **Activate**를 클릭합니다.
- 사용자 지정 제품 매핑 목록의 사용을 비활성화하려면 **Deactivate**를 클릭합니다.

47장

활성 스캐닝 구성

FireSIGHT 시스템은 네트워크에서 트래픽의 패시브 분석을 통해 네트워크 맵을 작성합니다. 그러나 때때로 호스트에 대한 정보를 확인하려면 호스트를 능동적으로 스캔해야 할 수 있습니다. 예를 들어 호스트의 공개 포트에서 서버가 실행 중이지만 시스템이 네트워크를 모니터링하는 동안 서버가 트래픽을 받거나 보내지 않은 경우, 시스템은 해당 서버에 대한 정보를 네트워크 맵에 추가하지 않습니다. 그러나 활성 스캐너를 사용하여 해당 호스트를 직접 스캔하는 경우 서버 존재를 탐지할 수 있습니다.

호스트를 능동적으로 스캔할 경우 호스트에 대한 정보를 얻기 위한 시도로 패킷을 전송합니다. FireSIGHT 시스템에는 호스트에서 실행 중인 운영 체제와 서버를 탐지하기 위해 사용할 수 있는 네트워크 탐색과 보안 감사를 위한 오픈 소스 활성 스캐너인 Nmap™ 6.01이 통합되어 있습니다. Nmap 스캔 시 호스트에서 실행 중인 운영 체제와 서버에 대한 자세한 정보를 확인하고, 그러한 호스트를 기반으로 시스템의 취약성 보고를 개선할 수 있습니다.

참고 일부 스캐닝 옵션(예: 포트스캔)은 저대역폭 네트워크에 상당한 부담을 줄 수 있습니다. 이러한 스캔은 항상 네트워크 사용량이 적을 때 실행해야 합니다.

자세한 내용은 다음 절을 참조하십시오.

Nmap 스캔 이해

라이센스: FireSIGHT

Nmap은 네트워크의 호스트에서 능동적으로 포트를 스캔하여 호스트의 운영 체제와 서버 데이터를 결정하는데, 이를 통해 네트워크 맵을 개선하고 스캔된 호스트에 매핑된 취약성의 정확성을 더욱 정밀하게 조정할 수 있습니다. 호스트가 네트워크 맵에 있어야만 Nmap이 결과를 호스트 프로필에 추가할 수 있습니다. 결과 파일에서 스캔 결과를 볼 수도 있습니다.

Nmap을 사용하여 호스트를 스캔할 경우, 전에 탐지되지 않은 열린 포트에 있는 서버가 해당 호스트에 대한 호스트 프로필의 Servers 목록에 추가됩니다. 호스트 프로필은 필터링된/닫힌 TCP 포트 또는 UDP 포트에서 탐지된 서버를 Scan Results 섹션에 나열합니다. 기본적으로 Nmap은 1660개가 넘는 TCP 포트를 스캔합니다.

Nmap은 스캔 결과를 1500개가 넘는 알려진 운영 체제 핑거프린트와 비교하여 운영 체제를 확인하고 각각에 점수를 할당합니다. 호스트에 할당된 운영 체제는 최고 점수의 운영 체제 핑거프린트입니다.

시스템이 Nmap 스캔에서 식별된 서버를 인식하고 해당 서버 정의를 가지고 있는 경우, 해당 서버에 대한 취약성이 호스트에 매핑됩니다. 시스템은 Nmap이 서버에 대해 사용하는 이름을 해당 Cisco 서버 정의에 매핑한 다음 시스템의 각 서버에 매핑된 취약성을 사용합니다. 마찬가지로 시스템은 Nmap 운영 체제 이름을 Cisco 운영 체제 정의에 매핑합니다. Nmap이 호스트의 운영 체제를 탐지하면 시스템은 해당 Cisco 운영 체제 정의의 취약성을 호스트에 할당합니다.

스캔에 사용되는 기반 Nmap 기술에 대한 자세한 내용은 http://insecure.org에서 제공하는 Nmap 설명서를 참조하십시오.

사용 중인 Cisco 어플라이언스의 Nmap에 대한 자세한 내용은 다음 항목을 참조하십시오.

- 47-2페이지의 Nmap 교정 이해
- 47-5페이지의 Nmap 스캐닝 전략 생성
- 47-6페이지의 샘플 Nmap 스캐닝 프로필

Nmap 교정 이해

라이센스: FireSIGHT

Nmap 교정을 생성하여 Nmap 스캔에 대한 설정을 정의할 수 있습니다. Nmap 교정은 상관관계 정책에서 응답으로 사용하거나, 온디맨드 방식으로 실행하거나, 특정 시간에 실행되도록 예약할 수 있습니다. Nmap 스캔의 결과가 네트워크 맵에 나타나도록 하려면 스캔된 호스트가 이미 네트워크 맵에 있어야 합니다.

Nmap 제공 서버 및 운영 체제 데이터는 또 다른 Nmap 스캔을 실행할 때까지 고정 상태로 유지됩니다. Nmap을 사용하여 호스트에서 운영 체제 및 서버 데이터를 스캔하려는 경우 Nmap 제공 운영 체제 및 서버 데이터를 최신 상태로 유지하기 위해 정기적인 예약 스캔을 설정할 수 있습니다. 자세한 내용은 62-5페이지의 Nmap 스캔 자동화을/를 참조하십시오. 또한 네트워크 맵에서 호스트가 삭제되면 해당 호스트에 대한 모든 Nmap 스캔 결과가 삭제됩니다.

Nmap 기능에 대한 자세한 내용은 http://insecure.org에서 제공하는 Nmap 설명서를 참조하십시오. 다음 표에서는 FireSIGHT 시스템의 Nmap 교정에서 구성할 수 있는 옵션에 대해 설명합니다.

표 47-1 Nmap 교정 옵션

옵션	설명	해당 Nmap 옵션
Scan Which Address(es) From Event?	상관관계 규칙에 대한 응답으로 Nmap 스캔을 사용할 때 이벤트의 어떤 주소를 스캔할 것인지, 소스 호스트 주소인지 목적지 호스트 주소인지 아니면 둘 다인지를 제어하기 위한 옵션을 선택합니다.	해당 없음
Scan Types	Nmap이 포트를 스캔하는 방법을 선택합니다. • **TCP Syn** 스캔은 완전한 TCP 핸드셰이크를 사용하지 않은 채 수천 개의 포트에 빠르게 연결합니다. 이 옵션을 사용하면 TCP 연결을 시작하기만 하고 완료하지 않음으로써, `admin` 계정이 원시 패킷 액세스 권한을 가지고 있거나 IPv6이 실행되지 않고 있는 호스트의 스텔스(stealth) 모드에서 빠르게 스캔할 수 있습니다. 호스트가 TCP Syn 스캔에서 전송된 Syn 패킷을 인식하면 Nmap은 연결을 재설정합니다. • **TCP Connect** 스캔은 `connect()` 시스템 호출을 사용하여 호스트의 운영 체제를 통한 연결을 엽니다. 방어 센터 또는 관리되는 디바이스의 `admin` 사용자가 호스트에 대한 원시 패킷 권한을 가지고 있지 않거나 현재 IPv6 네트워크를 스캔 중인 경우 TCP Connect 스캔을 사용할 수 있습니다. 다시 말하면, TCP Syn 스캔을 사용할 수 없는 상황에서는 이 옵션을 사용합니다. • **TCP ACK** 스캔은 ACK 패킷을 전송하여 포트의 필터링 여부를 확인합니다. • **TCP Window** 스캔은 TCP ACK 스캔과 동일한 방식으로 작동하지만, 포트가 열렸는지 또는 닫혔는지도 확인할 수 있습니다. • **TCP Maimon** 스캔은 FIN/ACK 프로브를 사용하여 BSD에서 파생된 시스템을 식별합니다.	**TCP Syn**: `-sS` **TCP Connect**: `-sT` **TCP ACK**: `-sA` **TCP Window**: `-sW` **TCP Maimon**: `-sM`
Scan for UDP ports	TCP 포트 외에 UDP 포트 스캔도 활성화합니다. UDP 포트 스캐닝에는 시간이 많이 걸릴 수 있으므로 빠르게 스캔하려는 경우 이 옵션을 사용하지 마십시오.	`Su`
Use Port From Event	상관관계 정책에서 교정을 응답으로서 사용하려는 경우, 교정이 상관관계 응답을 트리거하는 이벤트에 지정된 포트만 스캔하도록 설정합니다. **팁** 또한 Nmap이 운영 체제 정보 및 서버 정보를 수집할지 여부도 제어할 수 있습니다. 새 서버와 관련된 포트를 스캔하려면 **Use Port From Event** 옵션을 활성화하십시오.	해당 없음
Scan from reporting detection engine	호스트를 보고한 탐지 엔진이 상주하는 어플라이언스에서 호스트를 스캔하도록 설정합니다.	해당 없음
Fast Port Scan	스캐닝을 수행하는 디바이스의 `/var/sf/nmap/share/nmap/nmap-services` 디렉토리에 있는 `nmap-services` 파일에 나열된 TCP 포트만 스캔하고 다른 포트 설정은 무시하도록 설정합니다. 이 옵션은 **Port Ranges and Scan Order** 옵션과 함께 사용할 수 없습니다.	`F.`
Port Ranges and Scan Order	Nmap 포트 사양 구문을 사용하여 스캔할 특정 포트를 설정하고 스캔 순서를 지정합니다. 이 옵션은 **Fast Port Scan** 옵션과 함께 사용할 수 없습니다.	`-p`
Probe open ports for vendor and version information	서버 공급업체 및 버전 정보의 탐지를 활성화합니다. 열린 포트에서 서버 공급업체 및 버전 정보를 조사하면 Nmap은 서버 식별에 사용하는 서버 데이터를 얻게 됩니다. 그런 다음 해당 서버에 대한 Cisco 서버 데이터를 교체합니다.	`-sV`

표 47-1 Nmap 교정 옵션 (계속)

옵션	설명	해당 Nmap 옵션
Service Version Intensity	서비스 버전에 대한 Nmap 프로브의 강도를 선택합니다. 서비스 강도 번호가 높으면 더 많은 프로브가 사용되고 그 결과 정확성이 높아지는 반면, 강도가 낮으면 프로브 속도는 빨라지지만 얻는 정보가 적어집니다.	`--version-intensity <intensity>`
Detect Operating System	호스트에 대한 운영 체제 정보의 탐지를 활성화합니다. 호스트에 대한 운영 체제의 탐지를 구성하면 Nmap은 호스트를 스캔하고 그 결과를 사용하여 각 운영 체제에 대한 점수를 생성합니다. 이 점수는 운영 체제가 호스트에서 실행되고 있을 가능성을 반영합니다. Nmap 식별 ID 데이터가 네트워크 맵에 나타나는 시기와 방법에 대한 자세한 내용은 46-5페이지의 현재 ID 이해을/를 참조하십시오.	`-O`
Treat All Hosts As Online	호스트 검색 프로세스를 건너뛰고 대상 범위의 모든 호스트에서 포트 스캔을 실행하도록 설정합니다. 이 옵션을 활성화하면 Nmap은 **Host Discovery Method** 및 **Host Discovery Port List**에 대한 설정을 무시합니다.	`-PN`
Host Discovery Method	대상 범위의 모든 호스트에 대해 **Host Discovery Port List**에 나열된 포트에서(포트가 나열되지 않은 경우 해당 호스트 검색 방법에 대한 기본 포트에서) 호스트 검색을 수행하려면 선택합니다. 그러나 **Treat All Hosts As Online**도 활성화한 경우 **Host Discovery Method** 옵션은 효과가 없으며 호스트 검색이 수행되지 않습니다. 호스트가 있으며 사용 가능한지를 알아보기 위해 Nmap으로 테스트할 때 사용할 방법을 선택합니다. • **TCP SYN** 옵션은 SYN 플래그가 설정된 빈 TCP 패킷을 전송하고 응답을 받으면 호스트가 사용 가능한 상태인 것으로 인식합니다. TCP SYN은 기본적으로 포트 80을 스캔합니다. 스테이트풀 방화벽 규칙이 있는 방화벽에서는 TCP SYN 스캔을 차단할 가능성이 적습니다. • **TCP ACK** 옵션은 ACK 플래그가 설정된 빈 TCP 패킷을 전송하고 응답을 받을 경우 호스트가 사용 가능한 상태인 것으로 인식합니다. TCP ACK도 기본적으로 포트 80을 스캔합니다. 스테이트리스 방화벽 규칙이 있는 방화벽에서는 TCP ACK 스캔을 차단할 가능성이 희박합니다. • **UDP** 옵션은 UDP 패킷을 전송하고, 닫힌 포트에서 포트 도달 불가 응답이 돌아오면 호스트가 사용 가능한 상태인 것으로 간주합니다. UDP는 기본적으로 포트 40125를 스캔합니다.	**TCP SYN**: `-PS` **TCP ACK**: `-PA` **UDP**: `-PU`
Host Discovery Port List	호스트 검색을 수행할 때 스캔할 포트의 사용자 지정 목록을 쉼표로 구분하여 지정합니다.	호스트 검색 방법에 대한 포트 목록
Default NSE Scripts	호스트 검색 및 서버/운영 체제/취약성 탐지에 대한 Nmap 스크립트의 기본 설정 실행을 활성화합니다. 기본 스크립트 목록은 http://nmap.org/nsedoc/categories/default.html을/를 참조하십시오.	`-sC`
Timing Template	스캔 프로세스의 타이밍을 선택합니다. 높은 숫자를 선택할수록 스캔의 범위가 줄고 속도가 빨라집니다.	**0**: `T0` (paranoid) **1**: `T1` (sneaky) **2**: `T2` (polite) **3**: `T3` (normal) **4**: `T4` (aggressive) **5**: `T5` (insane)

Nmap 스캐닝 전략 생성

라이센스: FireSIGHT

활성 스캐닝을 통해 귀중한 정보를 얻을 수 있지만 Nmap 등의 툴을 과용하면 네트워크 리소스에 과부하가 발생하거나 중요한 호스트가 충돌할 수도 있습니다. 활성 스캐너를 사용하는 동안에는 반드시 필요한 호스트와 포트만 스캔할 수 있도록 스캐닝 전략을 세워야 합니다.

자세한 내용은 다음 절을 참조하십시오.

- 47-5페이지의 적절한 스캔 대상 선택
- 47-6페이지의 스캔할 적절한 포트 선택
- 47-6페이지의 호스트 검색 옵션 설정

적절한 스캔 대상 선택

라이센스: FireSIGHT

Nmap을 구성할 때 스캔할 호스트를 식별하는 스캔 대상을 생성할 수 있습니다. 스캔 대상에는 스캔할 단일 IP 주소, CIDR 블록 또는 IP 주소의 옥텟 범위, IP 주소 범위, IP 주소의 목록이나 범위는 물론 호스트의 포트도 포함됩니다.

다음과 같은 방법으로 대상을 지정할 수 있습니다.

- IPv6 호스트의 경우
  - 정확한 IP 주소(예: `192.168.1.101`)
- IPv4 호스트의 경우
  - 정확한 IP 주소(예: `192.168.1.101`) 또는 쉼표나 공백으로 구분한 IP 주소의 목록
  - CIDR 표기법을 사용한 IP 주소 블록(예를 들어 `192.168.1.0/24`는 192.168.1.1과 192.168.1.254(포함) 사이의 254개 호스트를 스캔함)

    FireSIGHT 시스템에서 CIDR 표기법을 사용하는 방법에 대한 자세한 내용은 1-19페이지의 IP 주소 표기 규칙을/를 참조하십시오.
  - 옥텟 범위 주소 지정을 사용한 IP 주소 범위(예를 들어 `192.168.0-255.1-254`는 .0 또는 .255로 끝나는 주소를 제외한 192.168.x.x 범위의 모든 주소를 스캔함)
  - 하이픈을 사용한 IP 주소 범위(예를 들어 `192.168.1.1 - 192.168.1.5`는 192.168.1.1과 192.168.1.5(포함) 사이의 6개 호스트를 스캔함)
  - 쉼표나 공백으로 구분한 주소 목록 또는 범위(예를 들어 `192.168.1.0/24, 194.168.1.0/24`는 192.168.1.1과 192.168.1.254(포함) 사이의 254개 호스트 및 194.168.1.1과 194.168.1.254(포함) 사이의 254개 호스트를 스캔함)

Nmap 스캔을 위한 이상적인 스캔 대상에는 시스템이 식별할 수 없는 운영 체제의 호스트, 식별되지 않은 서버의 호스트 또는 네트워크에서 최근에 탐지되지 않은 호스트가 포함됩니다. 네트워크 맵에 존재하지 않는 호스트에 대한 네트워크 맵에는 Nmap 결과를 추가할 수 없습니다.

주의 Nmap 제공 서버 및 운영 체제 데이터는 또 다른 Nmap 스캔을 실행할 때까지 고정 상태로 유지됩니다. Nmap을 사용하여 호스트를 스캔하려는 경우 Nmap 제공 운영 체제 및 서버 데이터를 최신 상태로 유지하기 위해 정기적인 예약 스캔을 설정할 수 있습니다. 자세한 내용은 62-5페이지의 Nmap 스캔 자동화을/를 참조하십시오. 또한 네트워크 맵에서 호스트가 삭제되면 모든 Nmap 스캔 결과가 삭제됩니다. 사용자는 대상을 스캔할 권한이 있어야 합니다. 자신 또는 자신의 회사에 속하지 않은 호스트를 스캔하기 위해 Nmap을 사용하는 것은 불법일 수 있습니다.

스캔할 적절한 포트 선택

라이센스: FireSIGHT

구성하는 각 스캔 대상에 대해 스캔할 포트를 선택할 수 있습니다. 각 대상에서 스캔해야 할 정확한 포트 집합을 식별하려면 개별 포트 번호, 포트 범위 또는 포트 번호와 포트 범위의 시리즈를 지정할 수 있습니다.

기본적으로 Nmap은 1~1024의 TCP 포트를 스캔합니다. 상관관계 정책에서 교정을 응답으로서 사용하려는 경우, 교정이 상관관계 응답을 트리거하는 이벤트에 지정된 포트만 스캔하도록 할 수 있습니다. 온디맨드 방식으로 또는 예약된 작업으로 교정을 실행하는 경우 또는 이벤트에서 포트를 사용하지 않는 경우 다른 포트 옵션을 사용하여 어떤 포트를 스캔할지를 결정할 수 있습니다. `nmap-services` 파일에 나열된 TCP 포트만 스캔하고 다른 포트 설정은 무시하도록 선택할 수 있습니다. 또한 TCP 포트 외에 UDP 포트도 스캔할 수 있습니다. UDP 포트 스캐닝에는 시간이 많이 걸릴 수 있으므로 빠르게 스캔하려는 경우 이 옵션을 사용하지 마십시오. 스캔할 특정 포트 또는 포트 범위를 선택하려면 포트를 식별하기 위한 Nmap 포트 사양 구문을 사용하십시오.

호스트 검색 옵션 설정

라이센스: FireSIGHT

호스트에 대한 포트 스캔을 시작하기 전에 호스트 검색 수행 여부를 결정할 수 있습니다. 또는 스캔하려는 모든 호스트가 온라인 상태라고 가정할 수 있습니다. 모든 호스트를 온라인 상태로 취급하지 않으려는 경우 원하는 호스트 검색 방법을 선택할 수 있으며, 필요에 따라 호스트 검색 중 스캔할 포트 목록을 사용자 지정할 수 있습니다. 호스트 검색은 나열된 포트에서 운영 체제 또는 서버 정보를 조사하지 않습니다. 특정 포트에 대한 응답을 사용하여 호스트가 활성 상태이며 사용 가능한지만 확인합니다. 호스트 검색을 수행했는데 호스트가 사용 가능하지 않으면 Nmap은 해당 호스트에서 포트를 스캔하지 않습니다.

샘플 Nmap 스캐닝 프로필

라이센스: FireSIGHT

다음 시나리오는 네트워크에서 Nmap이 사용되는 예를 제공합니다.

- 47-6페이지의 예: 알 수 없는 운영 체제 해결
- 47-7페이지의 예: 새 호스트에 응답

예: 알 수 없는 운영 체제 해결

라이센스: FireSIGHT

시스템이 네트워크에 있는 호스트의 운영 체제를 확인할 수 없으면 Nmap을 사용하여 호스트를 능동적으로 스캔할 수 있습니다. Nmap은 스캔에서 얻은 정보를 사용하여 가능한 운영 체제를 평가합니다. 그런 다음 호스트 운영 체제 식별의 점수가 가장 높은 운영 체제를 사용합니다.

Nmap을 사용하여 새 호스트에서 운영 체제와 서버 정보를 확인하면 시스템은 스캔된 호스트에서 해당 정보를 모니터링하지 않습니다. Nmap을 사용하여 호스트를 검색하고 시스템에서 알 수 없는 운영 체제가 포함된 것으로 표시한 호스트의 서버 운영 체제를 검색하는 경우 유사한 호스트 그룹을 식별할 수 있습니다. 그런 다음 이들 중 하나를 기반으로 사용자 지정 핑거프린트를 생성하여, Nmap 스캔을 기반으로 호스트에서 실행 중임을 알고 있는 운영 체제의 핑거프린트와 연결할 수 있습니다. 가능하면 Nmap과 같은 서드파티 소스를 통해 고정 데이터를 입력하기보다 사용자 지정 핑거프린트를 사용하십시오. 사용자 지정 핑거프린트를 사용하면 시스템은 계속해서 호스트 운영 체제를 모니터링하고 필요 시 업데이트할 수 있기 때문입니다.

Nmap으로 운영 체제를 검색하려면

액세스: Admin/Discovery Admin

1단계 Nmap 모듈에 대한 스캔 인스턴스를 구성합니다.

자세한 내용은 47-9페이지의 Nmap 스캔 인스턴스 생성을/를 참조하십시오.

2단계 다음 설정을 사용하여 Nmap 교정을 생성합니다.

- 새 서버와 관련된 포트를 스캔하려면 **Use Port From Event**를 활성화합니다.
- 호스트에 대한 운영 체제 정보를 탐지하려면 **Detect Operating System**을 활성화합니다.
- 서버 공급업체 및 버전 정보를 탐지하려면 **Probe open ports for vendor and version information**을 활성화합니다.
- 호스트가 존재하는 것을 아는 경우 **Treat All Hosts as Online**을 활성화합니다.

Nmap 교정 생성에 대한 자세한 내용은 47-11페이지의 Nmap 교정 생성을/를 참조하십시오.

3단계 시스템이 알려지지 않은 운영 체제의 호스트를 탐지할 때 트리거되는 상관관계 규칙을 생성합니다.

이 규칙은 **검색 이벤트가 발생할 때** 및 **호스트의 OS 정보가 변경될 때** 그리고 **OS 이름을 알 수 없음** 조건을 충족할 때 트리거됩니다.

상관관계 규칙 생성에 대한 자세한 내용은 51-3페이지의 상관관계 정책에 대한 규칙 생성을/를 참조하십시오.

4단계 상관관계 규칙이 포함된 상관관계 정책을 생성합니다.

상관관계 정책 생성에 대한 자세한 내용은 51-45페이지의 상관관계 정책 생성을/를 참조하십시오.

5단계 상관관계 정책에서, 2단계에서 생성한 Nmap 교정을 3단계에서 생성한 규칙에 추가합니다.

6단계 상관관계 정책을 활성화합니다.

7단계 네트워크 검색이 다시 시작되고 네트워크 맵이 재작성되도록 네트워크 맵의 호스트를 삭제합니다.

8단계 하루나 이틀 후 상관관계 정책에 의해 생성된 이벤트를 검색합니다. 호스트에서 탐지된 운영 체제에 대한 Nmap 결과를 분석하여 네트워크에 시스템이 인식하지 못한 특별한 호스트 컨피그레이션에 있는지 알아봅니다.

Nmap 결과 분석에 대한 자세한 내용은 47-21페이지의 스캔 결과 분석을/를 참조하십시오.

9단계 Nmap 결과가 동일한 알 수 없는 운영 체제의 호스트를 찾으면 그러한 호스트 중 하나에 대해 사용자 지정 핑거프린트를 생성하고 향후 유사한 호스트를 식별하는 데 사용합니다.

자세한 내용은 46-8페이지의 클라이언트 핑거프린트을/를 참조하십시오.

예: 새 호스트에 응답

라이센스: FireSIGHT

침입 가능성이 있는 서브넷에서 시스템이 새 호스트를 탐지하면, 이에 대한 정확한 취약성 정보가 있는지 확인하기 위해 해당 호스트를 스캔할 수 있습니다.

그렇게 하려면 이 서브넷에 새 호스트가 나타날 때 이를 탐지하고 호스트에서 Nmap 스캔을 수행하는 교정을 실행하는 상관관계 정책을 생성 및 활성화하면 됩니다.

정책을 활성화한 후 주기적으로 교정 상태 보기를 점검하여(**Policy & Response > Responses > Remediations > Status**) 언제 교정이 실행되었는지를 알아볼 수 있습니다. 교정의 동적 스캔 대상에는 서버 탐지의 결과로서 스캔한 호스트의 IP 주소를 포함해야 합니다. Nmap에서 탐지한 운영 체제와 서버를 기반으로, 그러한 호스트의 호스트 프로필을 검토하여 호스트에 대해 해결해야 할 취약성이 있는지 알아보십시오.

주의 대규모 동적 네트워크가 있는 경우 새 호스트 탐지가 너무 빈번하여 스캔 사용에 응답하지 못할 수 있습니다. 리소스 과부하를 피하려면 자주 발생하는 이벤트에 대한 응답으로 Nmap 스캔을 사용하지 마십시오. 또한 Nmap을 사용하여 새 호스트에서 운영 체제와 서버 정보를 확인하면 Cisco는 스캔된 호스트에서 해당 정보를 모니터링하지 않습니다.

나타나는 새 호스트에 응답하여 스캔하려면

액세스: Admin/Discovery Admin

1단계 Nmap 모듈에 대한 스캔 인스턴스를 구성합니다.

자세한 내용은 47-9페이지의 Nmap 스캔 인스턴스 생성을/를 참조하십시오.

2단계 다음 설정을 사용하여 Nmap 교정을 생성합니다.

- 새 서버와 관련된 포트를 스캔하려면 **Use Port From Event**를 활성화합니다.
- 호스트에 대한 운영 체제 정보를 탐지하려면 **Detect Operating System**을 활성화합니다.
- 서버 공급업체 및 버전 정보를 탐지하려면 **Probe open ports for vendor and version information**을 활성화합니다.
- 호스트가 존재하는 것을 아는 경우 **Treat All Hosts as Online**을 활성화합니다.

Nmap 교정 생성에 대한 자세한 내용은 47-11페이지의 Nmap 교정 생성을/를 참조하십시오.

3단계 시스템이 특정 서브넷에서 새 호스트를 탐지할 때 트리거되는 상관관계 규칙을 생성합니다.

규칙은 **검색 이벤트가 발생할 때** 및 **새 호스트가 탐지될 때** 트리거되어야 합니다.

상관관계 규칙 생성에 대한 자세한 내용은 51-3페이지의 상관관계 정책에 대한 규칙 생성을/를 참조하십시오.

4단계 상관관계 규칙이 포함된 상관관계 정책을 생성합니다.

상관관계 정책 생성에 대한 자세한 내용은 51-45페이지의 상관관계 정책 생성을/를 참조하십시오.

5단계 상관관계 정책에서, 2단계에서 생성한 Nmap 교정을 3단계에서 생성한 규칙에 추가합니다.

6단계 상관관계 정책을 활성화합니다.

7단계 새 호스트에 대한 알림이 제공되면 해당 호스트 프로필에서 Nmap 스캔의 결과를 확인하고 호스트에 적용되는 취약성을 해결합니다.

Nmap 스캔 설정

라이센스: FireSIGHT

Nmap을 사용하여 스캔하려면 먼저 스캔 인스턴스 및 스캔 교정을 구성해야 합니다. Nmap 스캔을 예약하려면 스캔 대상도 정의해야 합니다.

자세한 내용은 다음 절을 참조하십시오.

- 47-9페이지의 Nmap 스캔 인스턴스 생성
- 47-10페이지의 Nmap 스캔 대상 생성
- 47-11페이지의 Nmap 교정 생성

Nmap 스캔 인스턴스 생성

라이센스: FireSIGHT

네트워크에서 취약성을 스캔하기 위해 사용할 각 Nmap 모듈에 대해 별도의 스캔 인스턴스를 설정할 수 있습니다. 방어 센터의 로컬 Nmap 모듈 및 원격으로 스캔을 실행하기 위해 사용할 디바이스에 대해 스캔 인스턴스를 설정할 수 있습니다. 원격 디바이스에서 스캔을 실행하는 경우에도, 각 스캔의 결과는 스캔을 구성하는 방어 센터에 항상 저장됩니다. 미션 크리티컬 호스트에 대한 악의적인 스캔 또는 실수로 이루어지는 스캔을 방지하려면, 인스턴스로 스캔해서는 안 되는 호스트를 나타내기 위해 인스턴스에 대한 블랙리스트를 생성할 수 있습니다.

기존 스캔 인스턴스와 동일한 이름의 스캔 인스턴스를 추가할 수 없습니다.

스캔 인스턴스를 생성하려면

액세스: Admin/Discovery Admin

1단계 **Policies > Actions > Scanners**를 선택합니다.

Scanners 페이지가 나타납니다.

2단계 **Add Nmap Instance**를 클릭합니다.

Instance Detail 페이지가 나타납니다.

3단계 1~63자의 영숫자로 된 이름을 **Instance Name** 필드에 입력합니다. 밑줄(_)과 대시(-) 이외의 특수 문자 및 공백은 사용할 수 없습니다.

4단계 공백과 특수 문자를 포함하여 0~255자의 영숫자로 된 설명을 **Description** 필드에 지정합니다.

5단계 선택적으로, 다음 구문을 사용하여 이 스캔 인스턴스로 스캔해서는 *안 되는* 호스트 또는 네트워크를 **Black Listed Scan hosts** 필드에 지정합니다.

- IPv6 호스트의 경우 정확한 IP 주소(예: `2001:DB8::fedd:eeff`)
- IPv4 호스트의 경우 정확한 IP 주소(예: `192.168.1.101`) 또는 CIDR 표기법을 사용하는 IP 주소 블록(예: `192.168.1.0/24`는 `192.168.1.1`과 `192.168.1.254` 사이(포함)의 254개 호스트를 스캔함)
- 주소 값을 부정하기 위해 느낌표(!)를 사용할 수 없습니다.

스캔 대상을 블랙리스트에 추가된 네트워크에 있는 호스트로 구체적으로 지정하는 경우 해당 스캔은 실행되지 않습니다.

6단계 선택적으로, 방어 센터 대신 원격 디바이스에서 스캔을 실행하려면 방어 센터 웹 인터페이스에서 디바이스의 Information 페이지 **Remote Device Name** 필드에 나타나는 디바이스의 IP 주소 또는 이름을 지정합니다.

7단계 **Create**를 클릭합니다.

스캔 인스턴스가 생성됩니다.

Nmap 스캔 대상 생성

라이센스: FireSIGHT

특정 호스트 및 포트를 식별하는 스캔 대상을 생성 및 저장할 수 있습니다. 그런 다음 온디맨드 스캔을 수행하거나 스캔을 예약할 때 저장된 스캔 대상 중 하나를 사용할 수 있습니다.

IPv4 주소의 대상을 스캔하려면 IP 주소, IP 주소의 목록, CIDR 표기법 또는 Nmap 스캔 옥텟을 사용하여 스캔할 호스트를 선택할 수 있습니다. 하이픈을 사용하여 주소 범위를 지정할 수도 있습니다. 목록의 주소 및 범위는 쉼표나 공백을 사용하여 구분합니다.

IPv6 주소를 스캔하려면 IP 주소를 사용해야 합니다. 범위는 지원되지 않습니다.

Nmap 제공 서버 및 운영 체제 데이터는 또 다른 Nmap 스캔을 실행할 때까지 고정 상태로 유지됩니다. Nmap을 사용하여 호스트를 스캔하려는 경우 Nmap 제공 운영 체제 및 서버 데이터를 최신 상태로 유지하기 위해 정기적인 예약 스캔을 설정할 수 있습니다. 자세한 내용은 62-5페이지의 Nmap 스캔 자동화을/를 참조하십시오. 또한 네트워크 맵에서 호스트가 삭제되면 해당 호스트에 대한 모든 Nmap 스캔 결과가 삭제됩니다.

스캔 대상을 생성하려면

액세스: Admin/Discovery Admin

1단계 **Policies > Actions > Scanners**를 선택합니다.

Scanners 페이지가 나타납니다.

2단계 툴바에서 **Targets**를 클릭합니다.

Scan Target List 페이지가 나타납니다.

3단계 **Create Scan Target**을 클릭합니다.

Scan Target 페이지가 나타납니다.

4단계 이 스캔 대상에 사용할 이름을 **Name** 필드에 입력합니다.

5단계 다음 구문을 사용하여 스캔할 호스트를 **IP Range** 텍스트 상자에 지정합니다.

- IPv6 호스트의 경우 정확한 IP 주소(예: `2001:DB8::fedd:eeff`)
- IPv4 호스트의 경우 정확한 IP 주소(예: `192.168.1.101`) 또는 쉼표로 구분된 IP 주소의 목록
- IPv4 호스트의 경우 CIDR 표기법을 사용한 IP 주소 블록(예를 들어 `192.168.1.0/24`는 192.168.1.1과 192.168.1.254(포함) 사이의 254개 호스트를 스캔함)

  FireSIGHT 시스템에서 CIDR 표기법을 사용하는 방법에 대한 자세한 내용은 1-19페이지의 IP 주소 표기 규칙을/를 참조하십시오.
- IPv4 호스트의 경우 옥텟 범위 주소 지정을 사용한 IP 주소 범위(예를 들어 `192.168.0-255.1-254`는 .0 또는 .255로 끝나는 주소를 제외한 `192.168.x.x` 범위의 모든 주소를 스캔함)
- IPv4 호스트의 경우 하이픈을 사용한 IP 주소 범위(예를 들어 `192.168.1.1 - 192.168.1.5`는 192.168.1.1과 192.168.1.5(포함) 사이의 6개 호스트를 스캔함)

- IPv4 호스트의 경우 쉼표나 공백으로 구분한 주소 목록 또는 범위(예를 들어 `192.168.1.0/24, 194.168.1.0/24`는 192.168.1.1과 192.168.1.254(포함) 사이의 254개 호스트 및 194.168.1.1과 194.168.1.254(포함) 사이의 254개 호스트를 스캔함)

참고 **IP Range** 텍스트 상자에는 최대 255개 문자를 입력할 수 있습니다. 또한 스캔 대상에서 IP 주소나 범위의 목록에 쉼표를 사용하는 경우, 대상을 저장할 때 쉼표는 공백으로 변환됩니다.

6단계 스캔할 포트를 **Ports** 필드에 지정합니다.

1~65535의 값을 사용하여 다음 중 하나를 입력할 수 있습니다.

- 포트 번호
- 쉼표로 구분된 포트 목록
- 대시로 구분된 포트 번호의 범위
- 대시로 구분된, 쉼표로 구분된 포트 번호의 범위

7단계 **Save**를 클릭합니다.

스캔 대상이 생성됩니다.

Nmap 교정 생성

라이센스: FireSIGHT

Nmap 교정을 생성하여 Nmap 스캔에 대한 설정을 정의할 수 있습니다. Nmap 교정은 상관관계 정책에서 응답으로 사용하거나, 온디맨드 방식으로 실행하거나, 특정 시간에 실행되도록 예약할 수 있습니다. Nmap 스캔의 결과가 네트워크 맵에 나타나도록 하려면 스캔된 호스트가 이미 네트워크 맵에 있어야 합니다.

Nmap 교정의 특정 설정에 대한 자세한 내용은 47-2페이지의 Nmap 교정 이해을/를 참조하십시오.

Nmap 제공 서버 및 운영 체제 데이터는 또 다른 Nmap 스캔을 실행할 때까지 고정 상태로 유지됩니다. Nmap을 사용하여 호스트에서 운영 체제 및 서버 데이터를 스캔하려는 경우 Nmap 제공 운영 체제 및 서버 데이터를 최신 상태로 유지하기 위해 정기적인 예약 스캔을 설정할 수 있습니다. 자세한 내용은 62-5페이지의 Nmap 스캔 자동화을/를 참조하십시오. 또한 네트워크 맵에서 호스트가 삭제되면 해당 호스트에 대한 모든 Nmap 스캔 결과가 삭제됩니다.

Nmap 기능에 대한 자세한 내용은 http://insecure.org에서 제공하는 Nmap 설명서를 참조하십시오.

Nmap 교정을 생성하려면

액세스: Admin/Discovery Admin

1단계 **Policies > Actions > Scanners**를 선택합니다.

Scanners 페이지가 나타납니다.

2단계 교정을 추가하려는 스캔 인스턴스 옆에 있는 **Add Remediation**을 클릭합니다.

Edit Remediation 페이지가 나타납니다.

3단계 1~63자의 영숫자로 된 교정 이름을 **Remediation Name** 필드에 입력합니다. 밑줄(_)과 대시(-) 이외의 특수 문자 및 공백은 사용할 수 없습니다.

4단계 공백과 특수 문자를 포함하여 0~255자의 영숫자로 된 교정 설명을 **Description** 필드에 입력합니다.

5단계 침입 이벤트, 연결 이벤트 또는 사용자 이벤트를 트리거하는 상관관계 규칙에 대한 응답으로 이 교정을 사용하려는 경우 **Scan Which Address(es) From Event?** 옵션을 구성합니다.

- 이벤트에서 소스 IP 주소 및 목적지 IP 주소로 표시되는 호스트를 스캔하려면 **Scan Source and Destination Addresses**를 선택합니다.
- 이벤트의 소스 IP 주소로 표시되는 호스트를 스캔하려면 **Scan Source Address Only**를 선택합니다.
- 이벤트의 목적지 IP 주소로 표시되는 호스트를 스캔하려면 **Scan Destination Address Only**를 선택합니다.

검색 이벤트 또는 호스트 입력 이벤트에서 트리거되는 상관관계 규칙에 대한 응답으로 이 교정을 사용하려는 경우, 기본적으로 교정은 이벤트와 관련된 호스트의 IP 주소를 스캔합니다. 이 옵션을 구성할 필요가 없습니다.

참고 트래픽 프로필 변경을 트리거하는 상관관계 규칙에는 Nmap 교정을 응답으로서 할당하지 **마십시오**.

6단계 **Scan Type** 옵션을 구성합니다.

- TCP 연결을 시작하기만 하고 완료하지 않음으로써, `admin` 계정이 원시 패킷 액세스 권한을 가지고 있거나 IPv6이 실행되지 않고 있는 호스트의 스텔스(stealth) 모드에서 빠르게 스캔하려면 **TCP Syn Scan**을 선택합니다.
- 방어 센터의 `admin` 계정이 원시 패킷 액세스 권한을 가지고 있지 않거나 IPv6이 실행되고 있는 호스트에서 사용할 수 있는 시스템 `connect()` 호출을 사용하여 스캔하려면 **TCP Connect Scan**을 선택합니다.
- 포트의 필터링 여부를 확인하기 위해 ACK 패킷을 전송하려면 **TCP ACK Scan**을 선택합니다.
- 포트의 필터링 여부를 확인하는 것은 물론 포트가 열려 있는지 여부를 확인하기 위해 ACK 패킷을 전송하려면 **TCP Window Scan**을 선택합니다.
- FIN/ACK 프로브를 사용하여 BSD 파생 시스템을 식별하려면 **TCP Maimon Scan**을 선택합니다.

7단계 선택적으로, TCP 포트 외에 UDP 포트도 스캔하려면 **Scan for UDP ports** 옵션에 대해 **On**을 선택합니다.

팁 UDP 포트스캔이 TCP 포트스캔보다 시간이 더 걸립니다. 스캔 속도를 높이려면 이 옵션을 비활성화하십시오.

8단계 상관관계 정책 위반에 대한 응답으로 이 교정을 사용하려는 경우 **Use Port From Event** 옵션을 구성합니다.

- 11단계에서 지정한 포트 대신 상관관계 이벤트의 포트를 스캔하려면 **On**을 선택합니다.

  상관관계 이벤트의 포트를 스캔하는 경우 교정은 5단계에서 지정한 IP 주소의 포트를 스캔한다는 점에 유의하십시오. 또한 이러한 포트는 교정의 동적 스캔 대상에 추가됩니다.
- 11단계에서 지정하는 포트만 스캔하려면 **Off**를 선택합니다.

9단계 상관관계 정책 위반에 대한 응답으로 이 교정을 사용하고 이벤트를 탐지한 탐지 엔진을 실행하는 어플라이언스를 사용하여 스캔을 실행하려는 경우 **Scan from reporting detection engine** 옵션을 구성합니다.

- 보고 탐지 엔진을 실행하는 어플라이언스에서 스캔하려면 **On**을 선택합니다.
- 교정에서 구성된 어플라이언스에서 스캔하려면 **Off**를 선택합니다.

10단계 **Fast Port Scan** 옵션을 구성합니다.

- 스캐닝을 수행하는 디바이스의 `/var/sf/nmap/share/nmap/nmap-services` 디렉토리에 있는 `nmap-services` 파일에 나열된 포트만 스캔하고 다른 포트 설정은 무시하려면 **On**을 선택합니다.

- 모든 TCP 포트를 스캔하려면 **Off**를 선택합니다.

11단계 Nmap 구문을 사용하여 기본적으로 스캔할 포트를 원하는 스캔 순서대로 **Port Ranges and Scan Order** 필드에 입력합니다.

1~65535의 값을 지정합니다. 쉼표나 공백을 사용하여 포트를 구분합니다. 하이픈을 사용하여 포트 범위를 지정할 수도 있습니다. TCP 및 UDP 포트를 모두 스캔하는 경우, 스캔할 TCP 포트의 목록 앞에는 T를 추가하고 UDP 포트의 목록 앞에는 U를 추가합니다. 예를 들어 UDP 트래픽에 대해 포트 53 및 111을 스캔하고 TCP 트래픽에 대해 포트 21-25를 스캔하려면 `U:53,111,T:21-25`를 입력합니다.

8단계에 설명된 대로, 상관관계 정책 위반에 대한 응답으로 교정이 실행되는 경우 **Use Port From Event** 옵션은 이 설정을 재정의합니다.

12단계 열린 포트에서 서버 공급업체 및 버전 정보를 조사하려면 **Probe open ports for vendor and version information:**을 구성합니다.

- 호스트의 열린 포트에서 서버 정보를 스캔하여 서버 공급업체 및 버전을 식별하려면 **On**을 선택합니다.
- 호스트에 대한 Cisco 서버 정보를 계속해서 사용하려면 **Off**를 선택합니다.

13단계 열린 포트를 조사하려는 경우 **Service Version Intensity** 드롭다운 목록에서 숫자를 선택하여 사용되는 프로브의 수를 설정합니다.

- 더 오래 걸리지만 더 정확한 스캔을 위해 더 많은 프로브를 사용하려면 더 높은 숫자를 선택합니다.
- 덜 정확하지만 더 빠른 스캔을 위해 더 적은 프로브를 사용하려면 더 낮은 숫자를 선택합니다.

14단계 운영 체제 정보를 스캔하려면 **Detect Operating System** 설정을 구성합니다.

- 호스트에서 운영 체제를 식별하기 위한 정보를 스캔하려면 **On**을 선택합니다.
- 호스트에 대한 Cisco 운영 체제 정보를 계속해서 사용하려면 **Off**를 선택합니다.

15단계 호스트 검색 발생 여부 및 포트 스캔을 사용 가능한 호스트에 대해서만 실행할지 여부를 결정하려면 **Treat All Hosts As Online:**을 구성합니다.

- 호스트 검색 프로세스를 건너뛰고 대상 범위의 모든 호스트에서 포트 스캔을 실행하려면 **On**을 선택합니다.
- **Host Discovery Method** 및 **Host Discovery Port List**에 대한 설정을 사용하여 호스트 검색을 수행하고 사용할 수 없는 호스트에 대한 포트 스캔은 건너뛰려면 **Off**를 선택합니다.

16단계 호스트 가용성을 테스트할 때 Nmap이 사용할 방법을 선택합니다.

- SYN 플래그 세트와 함께 빈 TCP 패킷을 전송하고 닫힌 포트에서 RST 응답을 유도하거나 호스트에서 사용 가능한 열린 포트에서 SYN/ACK 응답을 유도하려면 **TCP SYN**을 선택합니다.

  이 옵션은 기본적으로 포트 80을 스캔하며, TCP SYN 스캔은 스테이트풀 방화벽 규칙이 있는 방화벽에 의해 차단될 가능성이 희박하다는 점에 유의해야 합니다.
- ACK 플래그 세트와 함께 빈 TCP 패킷을 전송하고 사용 가능한 호스트에서 RST 응답을 유도하려면 **TCP ACK** 를 선택합니다.

  이 옵션은 기본적으로 포트 80을 스캔하며, TCP ACK 스캔은 스테이트리스 방화벽 규칙이 있는 방화벽에 의해 차단될 가능성이 희박하다는 점에 유의해야 합니다.
- 사용 가능한 호스트의 닫힌 포트에서 포트 도달 불가 응답을 유도하기 위해 UDP 패킷을 전송하려면 **UDP**를 선택합니다. 이 옵션은 기본적으로 포트 40125를 스캔합니다.

17단계 호스트 검색 중 사용자 지정 포트 목록을 스캔하려면 선택한 호스트 검색 방법에 적절한 포트 목록을 쉼표로 구분하여 **Host Discovery Port List** 필드에 입력합니다.

18단계 호스트 검색 및 서버, 운영 체제, 취약성 검색에 대해 기본 Nmap 스크립트 세트를 사용할지 여부를 제어하려면 **Default NSE Scripts** 옵션을 구성합니다.

- 기본 Nmap 스크립트 세트를 실행하려면 **On**을 선택합니다.
- 기본 Nmap 스크립트 세트를 건너뛰려면 **Off**를 선택합니다.

기본 스크립트 목록은 http://nmap.org/nsedoc/categories/default.html을/를 참조하십시오.

19단계 스캔 프로세스의 타이밍을 설정하려면 타이밍 템플릿 번호를 선택합니다. 번호가 높으면 스캔이 더 빠르고 덜 포괄적이며, 번호가 낮으면 더 느리고 좀 더 포괄적입니다.

20단계 **Save**를 클릭한 후 **Done**을 클릭합니다.

교정이 생성됩니다.

Nmap 스캔 관리

라이센스: FireSIGHT

필요에 따라 Nmap 스캔 인스턴스 및 교정을 수정 또는 삭제할 수 있습니다. 온디맨드 Nmap 스캔을 실행할 수도 있습니다. 이전 스캔에 대한 Nmap 결과를 보거나 다운로드할 수도 있습니다. 자세한 내용은 다음 절을 참조하십시오.

- 47-14페이지의 Nmap 스캔 인스턴스 관리
- 47-15페이지의 Nmap 교정 관리
- 47-16페이지의 온디맨드 Nmap 스캔 실행

Nmap 스캔 인스턴스 관리

라이센스: FireSIGHT

Nmap 스캔 인스턴스를 수정 또는 삭제할 수 있습니다. 자세한 내용은 다음 절을 참조하십시오.

- 47-14페이지의 Nmap 스캔 인스턴스 수정
- 47-15페이지의 Nmap 스캔 인스턴스 삭제

Nmap 스캔 인스턴스 수정

라이센스: FireSIGHT

스캔 인스턴스를 수정하려면 다음 절차를 사용하십시오. 수정 시 인스턴스와 관련된 교정을 보고 추가하고 삭제할 수 있습니다.

스캔 인스턴스를 수정하려면

액세스: Admin/Discovery Admin

1단계 **Policies > Actions > Scanners**를 선택합니다.

Scanners 페이지가 나타납니다.

2단계 수정하려는 인스턴스 옆에 있는 **View**를 클릭합니다.

Instance Detail 페이지가 나타납니다.

3단계 선택적으로, 보거나 수정할 교정 옆에 있는 **View**를 클릭합니다.

교정 수정에 대한 자세한 내용은 47-15페이지의 Nmap 교정 수정을/를 참조하십시오.

4단계 선택적으로, 삭제할 교정 옆에 있는 **Delete**를 클릭합니다.

교정 삭제에 대한 자세한 내용은 47-16페이지의 Nmap 교정 삭제을/를 참조하십시오.

5단계 선택적으로, 이 스캔 인스턴스에 새 교정을 추가하려면 **Add**를 클릭합니다.

새 교정 생성에 대한 자세한 내용은 47-15페이지의 Nmap 교정 관리을/를 참조하십시오.

6단계 선택적으로, 스캔 인스턴스 설정을 변경하고 **Save**를 클릭합니다.

7단계 **Done**을 클릭합니다.

스캔 인스턴스가 수정됩니다.

Nmap 스캔 인스턴스 삭제

라이센스: FireSIGHT

인스턴스에 있는 Nmap 모듈을 더 이상 사용하지 않으려는 경우 Nmap 스캔 인스턴스를 삭제할 수 있습니다. 스캔 인스턴스를 삭제할 때 해당 인스턴스를 사용하는 교정도 삭제할 수 있습니다.

스캔 인스턴스를 삭제하려면

액세스: Admin/Discovery Admin

1단계 **Policies > Actions > Scanners**를 클릭합니다.

Scanners 페이지가 나타납니다.

2단계 삭제할 스캔 인스턴스 옆에 있는 **Delete**를 클릭합니다.

인스턴스가 삭제됩니다.

Nmap 교정 관리

라이센스: FireSIGHT

Nmap 교정을 수정 또는 삭제할 수 있습니다. 자세한 내용은 다음 절을 참조하십시오.

- 47-15페이지의 Nmap 교정 수정
- 47-16페이지의 Nmap 교정 삭제

Nmap 교정 수정

라이센스: FireSIGHT

Nmap 교정에 대한 수정은 진행 중인 스캔에 영향을 미치지 않습니다. 새 설정은 다음 스캔이 시작될 때 적용됩니다.

Nmap 교정을 수정하려면

액세스: Admin/Discovery Admin

1단계 **Policies > Actions > Scanners**를 선택합니다.

Scanners 페이지가 나타납니다.

2단계 수정할 교정 옆에 있는 **View**를 클릭합니다.

Remediation Edit 페이지가 나타납니다.

3단계 필요한 대로 수정합니다.

변경할 수 있는 설정에 대한 자세한 내용은 47-11페이지의 Nmap 교정 생성을/를 참조하십시오.

4단계 **Save**를 클릭한 후 **Done**을 클릭합니다.

교정이 수정됩니다.

Nmap 교정 삭제

라이센스: FireSIGHT

더 이상 필요하지 않은 Nmap 교정은 삭제할 수 있습니다.

Nmap 교정을 삭제하려면

액세스: Admin/Discovery Admin

1단계 **Policies > Actions > Scanners**를 선택합니다.

Scanners 페이지가 나타납니다.

2단계 삭제할 교정 옆에 있는 **Delete**를 클릭합니다.

3단계 교정을 삭제할 것임을 확인합니다.

교정이 삭제됩니다.

온디맨드 Nmap 스캔 실행

라이센스: FireSIGHT

필요할 때마다 온디맨드 Nmap 스캔을 실행할 수 있습니다. 스캔할 IP 주소와 포트를 입력하거나 기존 스캔 대상을 선택하여 온디맨드 스캔을 위한 대상을 지정할 수 있습니다.

Nmap 제공 서버 및 운영 체제 데이터는 또 다른 Nmap 스캔을 실행할 때까지 고정 상태로 유지됩니다. Nmap을 사용하여 호스트를 스캔하려는 경우 Nmap 제공 운영 체제 및 서버 데이터를 최신 상태로 유지하기 위해 정기적인 예약 스캔을 설정할 수 있습니다. 자세한 내용은 62-5페이지의 Nmap 스캔 자동화을/를 참조하십시오. 또한 네트워크 맵에서 호스트가 삭제되면 모든 Nmap 스캔 결과가 삭제됩니다.

온디맨드 Nmap 스캔을 실행하려면

액세스: Admin/Discovery Admin

1단계 **Policies > Actions > Scanners**를 선택합니다.

Scanners 페이지가 나타납니다.

2단계 스캔을 수행할 Nmap 교정 옆에 있는 **Scan**을 클릭합니다.

Nmap Scan Target 대화 상자가 나타납니다.

3단계 선택적으로, 저장된 스캔 대상을 사용하여 스캔하려면 **Saved Targets** 드롭다운 목록에서 대상을 선택하고 **Load**를 클릭합니다.

스캔 대상과 연결된 IP 주소 및 포트가 **IP Range(s)** 및 **Ports** 필드를 채웁니다.

팁 스캔 대상을 생성하려면 **Edit/Add Targets**를 클릭합니다. 자세한 내용은 47-10페이지의 Nmap 스캔 대상 생성을/를 참조하십시오.

4단계 **IP Range(s)** 필드에서 최대 255자로 스캔할 호스트의 IP 주소를 지정하거나 로드된 목록을 수정합니다.

IPv4 주소의 호스트에 대해서는 여러 IP 주소를 쉼표로 구분하여 지정하거나 CIDR 표기법을 사용할 수 있습니다. 또한 앞에 느낌표(!)를 사용하여 IP 주소를 부정할 수 있습니다. FireSIGHT 시스템에서 CIDR 표기법을 사용하는 방법에 대한 자세한 내용은 1-19페이지의 IP 주소 표기 규칙을/를 참조하십시오.

IPv6 주소의 호스트에 대해서는 정확한 IP 주소를 사용해야 합니다. 범위는 지원되지 않습니다.

5단계 **Ports** 필드에서 스캔할 포트를 지정하거나 로드된 목록을 수정합니다.

포트 번호, 쉼표로 구분된 포트 목록 또는 대시로 구분된 포트 번호 범위를 입력할 수 있습니다. 포트 입력에 대한 자세한 내용은 60-7페이지의 검색에서 포트 지정을/를 참조하십시오.

6단계 **Scan Now**를 클릭합니다.

Nmap 서버는 스캔을 수행합니다.

Nmap은 IP 주소 범위를 검증하고 범위가 잘못된 경우 오류 메시지를 표시합니다. 이 경우 유효한 IP 주소 범위를 표시하도록 **IP Range(s)** 필드의 내용을 수정하십시오.

스캔 대상 관리

라이센스: FireSIGHT

Nmap 모듈을 구성할 때 온디맨드 또는 예약된 스캔을 수행할 호스트와 포트를 식별하는 스캔 대상을 생성 및 저장할 수 있습니다. 그러면 매번 새로운 스캔 대상을 작성할 필요가 없습니다. 스캔 대상에는 스캔할 단일 IP 주소 또는 IP 주소 블록은 물론 호스트의 포트도 포함됩니다. Nmap 대상에 대해 Nmap 옥텟 범위 주소 지정 또는 IP 주소 범위를 사용할 수도 있습니다. Nmap 옥텟 범위 주소 지정에 대한 자세한 내용은 http://insecure.org에서 제공하는 Nmap 설명서를 참조하십시오.

다수의 호스트가 포함된 스캔 대상을 스캔하는 데에는 많은 시간이 소요될 수 있습니다. 해결책은 한 번에 더 적은 수의 호스트를 스캔하는 것입니다.

스캔 대상을 생성한 후 수정 또는 삭제할 수 있습니다.

자세한 내용은 다음 절을 참조하십시오.

- 47-10페이지의 Nmap 스캔 대상 생성
- 47-18페이지의 스캔 대상 수정
- 47-18페이지의 스캔 대상 삭제

스캔 대상 수정

라이센스: FireSIGHT

생성한 스캔 대상을 수정할 수 있습니다.

팁 특정 IP 주소를 스캔하기 위해 교정을 사용하고자 하지만 호스트가 교정을 실행한 상관관계 정책 위반과 관련되어 있기 때문에 IP 주소가 대상에 추가된 경우 교정의 동적 스캔 대상을 수정할 수 있습니다.

기존 스캔 대상을 수정하려면

액세스: Admin/Discovery Admin

1단계 **Policies > Actions > Scanners**를 선택합니다.

Scanners 페이지가 나타납니다.

2단계 툴바에서 **Targets**를 클릭합니다.

Scan Target List 페이지가 나타납니다.

3단계 수정할 스캔 대상 옆에 있는 **Edit**를 클릭합니다.

Scan Target 페이지가 나타납니다.

4단계 필요한 대로 수정하고 **Save**를 클릭합니다.

스캔 대상이 업데이트됩니다.

스캔 대상 삭제

라이센스: FireSIGHT

나열된 호스트를 더 이상 스캔하지 않으려면 스캔 대상을 삭제하십시오.

스캔 대상을 삭제하려면

액세스: Admin/Discovery Admin

1단계 **Policies > Actions > Scanners**를 선택합니다.

Scanners 페이지가 나타납니다.

2단계 툴바에서 **Targets**를 클릭합니다.

Scan Target List 페이지가 나타납니다.

3단계 삭제할 스캔 대상 옆에 있는 **Delete**를 클릭합니다.

스캔 대상이 삭제됩니다.

활성 스캔 결과 작업

라이센스: FireSIGHT

진행 중인 Nmap 스캔을 모니터링하고, 전에 FireSIGHT 시스템을 통해 수행한 스캔의 결과 또는 FireSIGHT 시스템 외부에서 수행한 결과를 가져오고, 스캔 결과를 보고 분석하는 방법에 대한 자세한 내용은 다음 절을 참조하십시오.

스캔 결과 보기

라이센스: FireSIGHT

스캔 결과의 테이블을 본 후, 찾고 있는 정보에 따라 이벤트 보기를 조작할 수 있습니다.

스캔 결과에 액세스할 때 표시되는 페이지는 사용하는 워크플로에 따라 달라집니다. 스캔 결과 테이블 보기를 포함하는 사전 정의 워크플로를 사용할 수 있습니다.

특정 요구와 일치하는 정보만 표시하는 사용자 지정 워크플로를 생성할 수도 있습니다. 사용자 지정 워크플로 생성에 대한 자세한 내용은 58-38페이지의 사용자 지정 워크플로 생성을/를 참조하십시오.

다음 표에서는 스캔 결과 워크플로 페이지에서 수행할 수 있는 몇 가지 특정 작업에 대해 설명합니다.

표 47-2 스캔 결과 기능 표

목적	가능한 작업
테이블에서 열의 내용에 대해 자세히 알아보기	47-21페이지의 스캔 결과 테이블 이해에서 자세히 알아보십시오.
스캔 결과에 대한 시간 및 날짜 범위 수정	시간 범위 링크를 클릭합니다. 자세한 내용은 58-22페이지의 이벤트 시간 제약 조건 설정을/를 참조하십시오.
스캔 결과 정렬	열 제목을 클릭합니다. 정렬 순서를 반대로 하려면 열 제목을 다시 클릭합니다.

표 47-2 스캔 결과 기능 표 (계속)

목적	가능한 작업
나타나는 열 제한	숨기려는 열 머리글에서 닫기 아이콘(✖)을 클릭합니다. 표시되는 팝업 창에서 **Apply**를 클릭합니다. **팁** 다른 열을 숨기거나 표시하려면 **Apply**를 클릭하기 전에 해당 확인란을 선택하거나 선택 취소합니다. 비활성화된 열을 다시 보기에 추가하려면 확장 화살표( )를 클릭하여 검색 제약 조건을 확장한 다음 **Disabled Columns** 아래에 있는 열 이름을 클릭합니다.
워크플로의 다음 페이지로 드릴다운하여 특정 값으로 제한	다음 방법 중 하나를 사용합니다. • 사용자 지정 워크플로에서 생성한 드릴다운 페이지에서 행 내의 값을 클릭합니다. 테이블 보기의 행 내에서 값을 클릭하면 테이블 보기가 제한되며 다음 페이지로 드릴다운되지 **않습니다**. • 일부 사용자로 제한하여 다음 워크플로 페이지로 드릴다운하려면, 다음 워크플로 페이지에서 볼 사용자의 옆에 있는 확인란을 선택하고 **View**를 클릭합니다. • 현재의 제약 조건을 유지한 채 다음 워크플로 페이지로 드릴다운하려면 **View All**을 클릭합니다. **팁** 테이블 보기의 페이지 이름에는 항상 "Table View"가 포함됩니다. 자세한 내용은 58-30페이지의 이벤트 제한을/를 참조하십시오.
스캔 인스턴스 및 교정 구성	툴바에서 **Scanners**를 클릭합니다. 자세한 내용은 47-9페이지의 Nmap 스캔 설정을/를 참조하십시오.
워크플로 페이지 내부 및 페이지 간 이동	58-18페이지의 워크플로 페이지 사용에서 자세히 알아보십시오.
관련 이벤트를 보기 위해 다른 이벤트 보기로 이동	**Jump to** 드롭다운 목록에서 보려는 이벤트 보기의 이름 자세한 내용은 58-35페이지의 워크플로 간 이동을/를 참조하십시오.
스캔 결과 검색	**Search**를 클릭합니다. 자세한 내용은 47-22페이지의 스캔 결과 검색을/를 참조하십시오.

검색 결과를 보려면

액세스: Admin/Discovery Admin

1단계 **Policies > Actions > Scanners**를 선택합니다.

2단계 **Scan Results**를 클릭합니다.

기본 스캔 결과 워크플로의 첫 번째 페이지가 나타납니다. 사용자 지정 워크플로를 비롯한 다른 워크플로를 사용하려면 워크플로 제목 옆의 **(switch workflows)**를 클릭합니다. 다른 기본 워크플로 지정에 대한 자세한 내용은 71-3페이지의 이벤트 보기 설정 구성을/를 참조하십시오.

스캔 결과 테이블 이해

라이센스: FireSIGHT

Nmap 스캔을 실행할 때 방어 센터는 데이터베이스에서 스캔 결과를 수집합니다. 다음 표에서는 검색 결과 테이블의 필드에 대해 설명합니다.

표 47-3 검색 결과 필드

필드	설명
Start Time	결과를 생성한 스캔이 시작된 날짜와 시간
End Time	결과를 생성한 스캔이 종료된 날짜와 시간
Scan Target	결과를 생성한 스캔에 대한 스캔 대상의 IP 주소(또는 호스트 이름, DNS 확인이 활성화된 경우)
Scan Type	결과를 생성한 스캔의 유형을 나타내기 위한 서드파티 스캐너의 이름 또는 `Nmap`
Scan Mode	결과를 생성한 스캔의 모드 • `On Demand` - 온디맨드 방식으로 실행된 스캔의 결과 • `Imported` - 다른 시스템에서 실행하고 방어 센터로 가져온 스캔의 결과 • `Scheduled` - 예약 작업으로서 실행한 스캔의 결과

스캔 결과 분석

라이센스: FireSIGHT

로컬 Nmap 모듈을 사용하여 생성한 스캔 결과를 팝업 창에서 렌더링된 페이지로서 볼 수 있습니다. Nmap 결과 파일을 원시 XML 형식으로 다운로드할 수도 있습니다.

또한 호스트 프로필 및 네트워크 맵에서 Nmap으로 탐지한 운영 체제 및 서버 정보를 볼 수 있습니다. 호스트의 스캔이 필터링된 포트 또는 닫힌 포트에서 서버에 대한 서버 정보를 생성하는 경우 또는 스캔에서 운영 체제 정보나 서버 섹션에 포함할 수 없는 정보를 수집하는 경우 호스트 프로필의 Nmap Scan Results 섹션에 그러한 결과가 포함됩니다. 자세한 내용은 49-5페이지의 호스트 프로필 보기을/를 참조하십시오.

스캔 모니터링

라이센스: FireSIGHT

Nmap 스캔의 진행 상황을 확인하고 현재 진행 중인 스캔 작업을 취소할 수 있습니다. 스캔 결과는 각 스캔의 시작 시간 및 종료 시간을 제공합니다. 또한 스캔이 완료된 후 스캔 결과를 팝업 창에서 렌더링된 페이지로서 볼 수 있습니다. Nmap 버전 1.01 DTD(http://insecure.org에서 다운로드 가능)를 사용하여 Nmap 결과를 다운로드하고 볼 수 있습니다. 스캔 결과를 지울 수도 있습니다.

스캔을 모니터링하려면

액세스: Admin/Discovery Admin

1단계 **Policies > Actions > Scanners** 를 선택합니다.

2단계 **Scan Results**를 클릭합니다.

기본 스캔 결과 워크플로의 첫 번째 페이지가 나타납니다. 사용자 지정 워크플로를 비롯한 다른 워크플로를 사용하려면 워크플로 제목 옆의 **(switch workflows)**를 클릭합니다. 다른 기본 워크플로 지정에 대한 자세한 내용은 71-3페이지의 이벤트 보기 설정 구성을/를 참조하십시오.

팁 스캔 결과의 테이블 보기가 포함되지 않은 사용자 지정 워크플로를 사용 중인 경우 워크플로 옆에 있는 **(switch workflows)**를 클릭하고 **Scan Results**를 선택합니다.

3단계 다음과 같은 동작을 수행할 수 있습니다.

- 스캔 결과를 팝업 창에서 렌더링된 페이지로서 보려면 스캔 작업 옆에 있는 **View**를 클릭합니다.
- 텍스트 편집기에서 원시 XML 코드를 볼 수 있도록 스캔 결과 파일의 복사본을 저장하려면 스캔 작업 옆에 있는 **Download**를 클릭합니다.

스캔 결과 가져오기

라이센스: FireSIGHT

FireSIGHT 시스템 외부에서 수행된 Nmap 스캔에 의해 생성된 XML 결과 파일을 가져올 수 있습니다. FireSIGHT 시스템에서 전에 다운로드한 XML 결과 파일을 가져올 수도 있습니다. Nmap 스캔 결과를 가져오려면 결과 파일은 XML 형식이어야 하며 Nmap 버전 1.01 DTD를 준수해야 합니다. Nmap 결과 생성 및 Nmap DTD에 대한 자세한 내용은 http://insecure.org에서 제공하는 Nmap 설명서를 참조하십시오. FireSIGHT 시스템에서 XML 결과를 다운로드하는 방법에 대한 자세한 내용은 47-21페이지의 스캔 모니터링을/를 참조하십시오.

호스트가 네트워크 맵에 있어야만 Nmap이 결과를 호스트 프로필에 추가할 수 있습니다.

결과를 가져오려면

액세스: Admin/Discovery Admin

1단계 **Policies > Actions > Scanners**를 선택합니다.

Scan Instances 페이지가 나타납니다.

2단계 툴바에서 **Import Results**를 클릭합니다.

Import Results 페이지가 나타납니다.

3단계 결과 파일을 찾아보려면 **Browse**를 클릭합니다.

4단계 Import Results 페이지로 돌아온 후 **Import**를 클릭하여 결과를 가져옵니다.

결과 파일 가져오기가 수행됩니다.

스캔 결과 검색

라이센스: FireSIGHT

FireSIGHT 시스템의 어플라이언스 또는 관리되는 어플라이언스에서 실행된 스캔에 대한 Nmap 또는 서드파티 스캔 결과를 검색할 수 있습니다.

표 47-4 스캔 결과 검색 기준

필드	검색 기준 규칙
Start Time	결과를 생성한 스캔이 시작된 날짜와 시간을 입력합니다. 시간 입력을 위한 구문은 60-5페이지의 검색에서 시간 제약 조건 지정을/를 참조하십시오.
End Time	결과를 생성한 스캔이 종료된 날짜와 시간을 입력합니다. 시간 입력을 위한 구문은 60-5페이지의 검색에서 시간 제약 조건 지정을/를 참조하십시오.
Scan Target	결과를 생성한 스캔에 대한 스캔 대상의 IP 주소(또는 호스트 이름, DNS 확인이 활성화된 경우)를 입력합니다. 특정 IP 주소 또는 CIDR 표기법을 사용하여 IP 주소의 범위를 지정합니다. IP 주소에 허용되는 구문에 대한 전체 설명은 60-6페이지의 검색에서 IP 주소 지정을/를 참조하십시오.
Scan Type	결과를 생성한 스캔의 유형을 나타내기 위한 `Nmap` 또는 서드파티 스캐너 ID를 입력합니다.
Scan Mode	결과를 생성한 스캔의 모드를 입력합니다. • 온디맨드 방식으로 실행된 스캔의 결과를 검색하려면 `On Demand`를 입력합니다. • 다른 시스템에서 실행하고 방어 센터로 가져온 스캔의 결과를 검색하려면 `Imported`를 입력합니다. • 예약 작업으로서 실행한 스캔의 결과를 검색하려면 `Scheduled`를 입력합니다.

저장된 검색을 로드 및 삭제하는 방법을 포함하여 검색에 대한 자세한 내용은 60-1페이지의 이벤트 검색을/를 참조하십시오.

스캔 결과를 검색하려면

액세스: Admin/Discovery Admin

1단계 **Analysis > Search**를 선택한 다음 테이블 드롭다운 목록에서 **Scan Results**를 선택합니다.

Scan Results 검색 페이지가 나타납니다.

팁 데이터베이스에서 서로 다른 종류의 이벤트를 검색하려면 테이블 드롭다운 목록에서 선택합니다.

2단계 스캔 결과 검색 기준 표에 설명된 대로 해당 필드에 검색 기준을 입력합니다.

여러 필드에 대한 조건을 입력하는 경우 모든 필드에 대해 지정한 검색 기준과 일치하는 레코드만 반환됩니다.

3단계 선택적으로, 검색을 저장하려면 **Private** 확인란을 선택하여 자신만 액세스할 수 있는 비공개로 검색을 저장할 수 있습니다. 또는 모든 사용자가 사용할 수 있도록 검색을 저장하려면 확인란을 선택하지 않습니다.

팁 제한된 권한과 함께 사용자 지정 사용자 역할에 대한 제한으로서 검색을 저장하려면 **반드시** 비공개 검색으로 저장해야 합니다.

4단계 선택적으로, 나중에 다시 사용할 수 있도록 검색을 저장할 수 있습니다. 다음 옵션을 이용할 수 있습니다.

- 검색 기준을 저장하려면 **Save**를 클릭합니다.

  새 검색인 경우 검색 이름을 입력하도록 대화 상자가 나타납니다. 고유한 검색 이름을 입력하고 **Save**를 클릭합니다. 이미 존재하는 검색에 대한 새 조건을 저장하는 경우 프롬프트가 나타나지 않습니다. 나중에 실행할 수 있도록 검색이 저장됩니다(**Private**을 선택한 경우 자신만 볼 수 있음).

- 새 검색을 저장하거나, 저장된 기존 검색을 변경하여 만든 검색에 새 이름을 할당하려면 **Save As New**를 클릭합니다.

  검색 이름을 입력하도록 대화 상자가 나타납니다. 고유한 검색 이름을 입력하고 **Save**를 클릭합니다. 나중에 실행할 수 있도록 검색이 저장됩니다(**Private**을 선택한 경우 자신만 볼 수 있음).

5단계 검색을 시작하려면 **Search**를 클릭합니다.

검색 결과가 나타납니다.

48장

네트워크 맵 사용

FireSIGHT 시스템은 네트워크를 통과하는 트래픽을 수동적으로 수집하고, 데이터를 디코딩하고, 이를 설정된 운영 체제 및 핑거프린트와 비교합니다. 시스템은 이 정보에서 네트워크를 자세히 표현하는 *네트워크 맵*을 작성합니다.

네트워크 맵을 사용하면 호스트 및 네트워크 디바이스(브리지, 라우터, NAT 디바이스 및 로드 밸런서) 관점에서 방어 센터를 볼 수 있습니다. 네트워크 맵은 네트워크를 전체적으로 빠르게 볼 수 있는 유용한 툴입니다. 또한 네트워크를 사용하면 관련된 호스트 특성, 애플리케이션, 클라이언트, IOC 호스트 및 취약성으로 드릴다운할 수 있습니다. 다시 말하면, 수행하는 분석에 맞게 네트워크 맵의 서로 다른 보기를 선택할 수 있습니다.

호스트 입력 기능을 사용하여 서드파티 애플리케이션의 호스트 특성 정보, 운영 체제, 애플리케이션, 클라이언트 또는 프로토콜을 추가함으로써 시스템이 수집하는 정보를 보강할 수 있습니다. Nmap을 사용하여 네트워크 맵에서 호스트를 능동적으로 스캔하고, 스캔 결과를 네트워크 맵에 추가할 수도 있습니다.

사용자 지정 토폴로지 기능을 사용하면 네트워크 맵의 보기에서 서브넷을 구성 및 식별하는 데 도움이 될 수 있습니다. 예를 들어 조직의 각 부서에서 서로 다른 서브넷을 사용하는 경우 사용자 지정 토폴로지 기능을 사용하여 친숙한 레이블을 서브넷에 할당할 수 있습니다.

자세한 내용은 다음 절을 참조하십시오.

네트워크 맵 이해

라이센스: FireSIGHT

네트워크 맵의 각 보기는 확장 가능한 카테고리 및 하위 카테고리가 있는 계층적 트리의 동일한 형식을 가지고 있습니다. 카테고리를 클릭하면 그 아래의 하위 카테고리가 표시되도록 카테고리가 확장됩니다. 수행하는 분석의 종류에 따라 네트워크 맵의 서로 다른 보기를 선택할 수 있습니다.

방어 센터는 검색 정책이 적용되는 모든 보안 영역(NetFlow 지원 디바이스의 데이터를 처리하는 영역 포함)에서 데이터를 수집합니다. 여러 디바이스가 동일한 네트워크 자산을 탐지하면 방어 센터는 하나의 복합 자산 표현으로 정보를 결합합니다.

NetFlow 지원 디바이스에서 내보낸 데이터를 추가하도록 네트워크 검색 정책을 구성할 수 있지만, 이러한 호스트에 대해 사용할 수 있는 정보는 제한적입니다. 예를 들어, 호스트 입력 기능을 사용하여 제공하지 않는 한 이러한 호스트에 대해 사용할 수 있는 운영 체제 데이터가 없습니다. 자세한 내용은 45-17페이지의 NetFlow 및 FireSIGHT 데이터 간 차이점을/를 참조하십시오.

네트워크 맵에서 호스트의 *호스트 프로필*을 볼 수 있습니다. 호스트 프로필은 해당 호스트에 대해 시스템에서 수집한 모든 정보의 완전한 보기를 제공합니다. 호스트 프로필에는 호스트 이름, 운영 체제, 연결된 모든 IP 주소와 같은 일반 정보는 물론 탐지된 프로토콜, 애플리케이션, IOC, 호스트에서 실행되는 클라이언트와 같은 좀 더 구체적인 정보도 포함됩니다. 또한 호스트 및 탐지된 자산과 연결된 취약성에 대한 정보도 포함됩니다. 호스트 프로필에 대한 자세한 내용은 49-1페이지의 호스트 프로필 사용을/를 참조하십시오.

더 이상 조사할 필요가 없는 항목은 네트워크 맵에서 삭제할 수 있습니다. 네트워크 맵에서 호스트와 애플리케이션을 삭제할 수 있으며, 취약성을 삭제하거나 비활성화할 수도 있습니다. 삭제된 호스트와 관련된 활동이 탐지되면 해당 호스트는 네트워크 맵에 다시 추가됩니다. 마찬가지로, 시스템에서 애플리케이션의 변경 사항(예: Apache 웹 서버가 새 버전으로 업그레이드됨)을 탐지하면 삭제된 애플리케이션이 애플리케이션 네트워크 맵에 다시 추가됩니다. 호스트를 취약하게 만드는 변경 사항이 탐지되면 특정 호스트에서 취약성이 다시 활성화됩니다.

네트워크 맵을 사용하여 네트워크 전체에서 취약성을 비활성화할 수도 있습니다. 즉, 시스템에서는 취약하다고 판단했지만 특정 공격 또는 익스플로잇으로부터 이러한 호스트가 안전하다고 간주하는 것입니다.

팁 네트워크 맵에서 호스트 또는 서브넷을 영구적으로 제외하려면 네트워크 검색 정책을 수정하십시오. 로드 밸런서 및 NAT 디바이스를 모니터링에서 제외할 수 있습니다. 이러한 디바이스는 잘못된 이벤트를 과도하게 생성하여 데이터베이스를 채우고 방어 센터에 과부하를 가져올 수 있습니다. 자세한 내용은 45-2페이지의 호스트 데이터 수집 이해을/를 참조하십시오.

호스트 네트워크 맵 작업

라이센스: FireSIGHT

호스트 네트워크 맵을 사용하면 계층적 트리에 서브넷으로 구성된 네트워크의 호스트를 볼 수 있으며, 특정 호스트에 대한 호스트 프로필로 드릴다운할 수도 있습니다. 이 네트워크 맵 보기는 시스템에서 탐지한 모든 고유한 호스트의 카운트를 제공합니다(IP가 하나이든 여러 개이든).

NetFlow 지원 디바이스에서 내보낸 데이터를 기반으로 네트워크 맵에 호스트를 추가하도록 네트워크 검색 정책을 구성할 수 있지만, 이러한 호스트에 대해 사용할 수 있는 정보는 제한적입니다. 예를 들어 NetFlow 데이터를 사용하여 네트워크 맵에 추가된 호스트에 대해 사용 가능한 운영 체제 데이터는 호스트 입력 기능을 사용하여 제공해야 합니다.

네트워크에 대한 사용자 지정 토폴로지를 생성하면, 부서 이름과 같은 의미 있는 레이블(예: 부서 이름)을 서브넷에 할당할 수 있으며, 이는 호스트 네트워크 맵에 나타납니다.

또한 사용자 지정 토폴로지에서 지정한 조직에 따라 호스트 네트워크 맵을 볼 수 있습니다. 48-10페이지의 사용자 지정 네트워크 토폴로지 작업을/를 참조하십시오.

호스트 네트워크 맵에서 전체 네트워크, 서브넷 또는 개별 호스트를 삭제할 수 있습니다. 특정 호스트가 네트워크에 더 이상 연결되어 있지 않음을 알고 있다면 분석을 간소화하기 위해 해당 호스트를 네트워크 맵에서 삭제할 수 있습니다. 삭제된 호스트와 관련된 활동이 이후에 탐지되면 해당 호스트는 네트워크 맵에 다시 추가됩니다. 네트워크 맵에서 호스트 또는 서브넷을 영구적으로 제외하려면 네트워크 검색 정책을 수정하십시오. 자세한 내용은 45-23페이지의 네트워크 검색 정책 생성을/를 참조하십시오.

참고 Cisco에서는 네트워크 디바이스를 네트워크 맵에서 삭제하지 **않을** 것을 **적극** 권장합니다. 시스템에서 이들의 위치를 사용하여 네트워크 토폴로지를 결정하기 때문입니다(모니터링되는 호스트에 대한 네트워크 홉 및 TTL 값 생성 포함). 네트워크 디바이스 네트워크 맵에서는 네트워크 디바이스를 삭제할 수 없지만, 호스트 네트워크 맵에서 이들을 삭제하지 않도록 하십시오.

호스트 네트워크 맵을 보려면

액세스: Admin/Any Security Analyst

1단계 **Analysis > Hosts > Network Map**을 선택하고 **Hosts** 탭을 선택합니다.

호스트 네트워크 맵이 나타나며 호스트 IP 주소 및 MAC 주소의 목록과 호스트 카운트가 표시됩니다. 각 주소 및 부분 주소는 다음 레벨에 대한 링크입니다.

2단계 조사하려는 호스트의 특정 IP 주소 또는 MAC 주소로 드릴다운합니다.

예를 들어 IP 주소 192.168.40.11을 보려면 **192**, **192.168**, **192.168.40**, **192.168.40.11**을 차례로 클릭합니다. **192.168.40.11**을 클릭하면 호스트 프로필이 나타납니다. 호스트 프로필에 대한 자세한 내용은 49-1페이지의 호스트 프로필 사용을/를 참조하십시오.

IP 또는 MAC 주소를 기준으로 필터링하려면 검색 필드에 주소를 입력합니다. 검색을 지우려면 지우기 아이콘(✖)을 클릭합니다.

3단계 선택적으로, 서브넷 IP 주소 또는 MAC 주소를 삭제하려면 삭제할 요소 옆에 있는 삭제 아이콘( )을 클릭한 다음 호스트 또는 서브넷을 삭제할 것임을 확인합니다.

호스트가 삭제됩니다. 호스트가 다시 검색되면 해당 호스트는 네트워크 맵에 다시 추가됩니다.

4단계 선택적으로, 호스트 네트워크 맵의 호스트 보기와 토폴로지 보기 간에 전환합니다.

- 호스트 보기에서 사용자 지정 토폴로지에 의해 구성된 호스트 네트워크 맵의 보기(기본값)로 전환하려면 네트워크 맵의 상단에서 **(topology)**를 클릭합니다.
- 서브넷에 의해 구성된 호스트 네트워크 맵의 보기로 전환하려면 네트워크 맵의 상단에서 **(hosts)**를 클릭합니다.

사용자 지정 토폴로지 구성에 대한 자세한 내용은 48-10페이지의 사용자 지정 네트워크 토폴로지 작업을/를 참조하십시오.

네트워크 디바이스 네트워크 맵 작업

라이센스: FireSIGHT

네트워크의 한 세그먼트를 다른 세그먼트에 연결하는 네트워크 디바이스(브리지, 라우터, NAT 디바이스 및 로드 밸런서)를 보고 그러한 네트워크 디바이스의 호스트 프로필로 드릴다운하려면 네트워크 디바이스 네트워크 맵을 사용할 수 있습니다. 네트워크 디바이스 네트워크 맵은 IP와 MAC의 두 섹션으로 구분됩니다. IP 섹션에는 IP 주소로 식별되는 네트워크 디바이스가 나열되고, MAC 섹션에는 MAC 주소로 식별되는 네트워크 디바이스가 나열됩니다. 이 네트워크 맵 보기는 시스템에서 탐지한 모든 고유한 네트워크 디바이스의 카운트를 제공합니다(IP가 하나이든 여러 개이든).

네트워크에 대해 사용자 지정 토폴로지를 생성하면, 서브넷에 할당하는 레이블이 네트워크 디바이스 네트워크 맵에 나타납니다.

시스템이 네트워크 디바이스를 구분하기 위해 사용하는 방법은 다음과 같습니다.

- CDP(Cisco Discovery Protocol) 메시지의 분석 - 네트워크 디바이스 및 유형을 식별할 수 있습니다(Cisco 디바이스만 해당).
- STP(Spanning Tree Protocol)의 탐지 - 디바이스를 스위치 또는 브리지로 식별합니다.
- 동일한 MAC 주소를 사용하는 여러 호스트 탐지 - MAC 주소를 라우터에 속한 것으로 식별합니다.
- 클라이언트 측에서 TTL 값 변경 탐지 또는 일반적인 부팅시간보다 더 자주 변경되는 TTL 값 - NAT 디바이스 및 로드 밸런서를 탐지합니다.

네트워크 디바이스가 CDP를 사용하여 통신하는 경우 IP 주소가 하나 이상일 수 있습니다. STP를 사용하여 통신하는 경우 MAC 주소가 하나뿐일 수 있습니다.

네트워크 디바이스를 네트워크 맵에서 삭제할 수 없습니다. 시스템에서 이들의 위치를 사용하여 네트워크 토폴로지를 결정하기 때문입니다(모니터링되는 호스트에 대한 네트워크 홉 및 TTL 값 생성 포함).

네트워크 디바이스의 호스트 프로필에는 Operating Systems 섹션이 아닌 Systems 섹션이 있습니다. 여기에는 네트워크 디바이스 뒤에서 탐지되는 모바일 디바이스에 대한 하드웨어 플랫폼을 반영하는 Hardware 열이 포함됩니다. Systems 아래에 하드웨어 플랫폼에 대한 값이 나열되면 해당 시스템은 네트워크 디바이스 뒤에서 탐지된 하나 이상의 모바일 디바이스를 나타냅니다. 모바일 디바이스에는 하드웨어 플랫폼 정보가 있을 수도 있고 없을 수도 있지만, 모바일 디바이스가 아닌 시스템에 대해서는 하드웨어 플랫폼 정보가 탐지되지 않습니다.

네트워크 디바이스 네트워크 맵을 보려면

액세스: Admin/Any Security Analyst

1단계 **Analysis > Hosts > Network Map > Network Devices**를 선택합니다.

네트워크 디바이스 네트워크 맵이 나타나서 고유한 네트워크 디바이스의 카운트 및 네트워크 디바이스 IP 주소와 MAC 주소의 목록을 표시합니다. 각 주소 및 부분 주소는 개별 호스트의 다음 주소 레벨 또는 호스트 프로필에 대한 링크입니다.

2단계 조사하려는 네트워크 디바이스의 특정 IP 주소 또는 MAC 주소로 드릴다운합니다.

네트워크 디바이스의 호스트 프로필이 나타납니다. 호스트 프로필에 대한 자세한 내용은 49-1페이지의 호스트 프로필 사용을/를 참조하십시오.

3단계 선택적으로, IP 또는 MAC 주소를 기준으로 필터링하려면 검색 필드에 주소를 입력합니다. 검색을 지우려면 지우기 아이콘(✖)을 클릭합니다.

IOC 네트워크 맵 작업

라이센스: FireSIGHT

IOC(indications of compromise) 카테고리로 구성된, 네트워크의 손상된 호스트를 보려면 IOC 네트워크 맵을 사용할 수 있습니다. 영향받는 호스트는 각 카테고리 아래에 나열됩니다.

침입 이벤트, 보안 인텔리전스, FireAMP 등 호스트의 손상된 상태를 확인하기 위해 시스템은 여러 소스의 데이터를 사용합니다.

IOC 네트워크 맵에서는 특정 방법으로 손상된 것으로 판단된 각 호스트의 호스트 프로필을 볼 수 있습니다. 특정 IOC 카테고리 또는 특정 호스트를 삭제(또는 해결된 것으로 표시)할 수 있는데, 그렇게 하면 관련 호스트에서 IOC 태그가 제거됩니다. 예를 들면, 문제가 해결되어 재발하지 않을 것으로 판단한 경우 네트워크 맵에서 IOC 카테고리를 삭제할 수 있습니다.

네트워크 맵에서 호스트 또는 IOC 카테고리를 해결된 것으로 표시하더라도 네트워크에서 제거되지 않습니다. 해당 IOC를 트리거하는 정보가 새로 탐지되면 네트워크 맵에 해결된 호스트 또는 IOC 카테고리가 다시 나타납니다.

IOC 네트워크 맵을 보려면

액세스: Admin/Any Security Analyst

1단계 **Analysis > Hosts > Network Map > Indications of Compromise**를 선택합니다.

IOC 네트워크 맵이 나타납니다.

2단계 조사하려는 특정 IOC 카테고리를 클릭합니다.

예를 들어 악성코드가 탐지된 호스트를 보려면 **Malware Detected**를 클릭합니다.

IP 또는 MAC 주소를 기준으로 필터링하려면 검색 필드에 주소를 입력합니다. 검색을 지우려면 지우기 아이콘( )을 클릭합니다.

3단계 선택한 IOC 카테고리 아래의 특정 IP 주소로 드릴다운합니다. 각 주소 및 부분 주소는 다음 레벨에 대한 링크입니다.

IOC 섹션이 확장되면서 손상된 호스트의 호스트 프로필이 나타납니다. 호스트 프로필의 IOC 섹션에 대한 자세한 내용은 49-8페이지의 호스트 프로필에서 IOC 작업을/를 참조하십시오.

4단계 선택적으로, IOC 카테고리, 손상된 호스트 또는 손상된 호스트 그룹을 해결된 것으로 표시하려면 원하는 요소 옆에 있는 삭제 아이콘( )을 클릭한 다음 해결된 것으로 표시할 것임을 확인합니다.

카테고리 또는 호스트가 해결됩니다(IOC 태그가 제거됨). IOC가 다시 트리거되면 해당 IOC는 네트워크 맵에 다시 추가됩니다.

모바일 디바이스 네트워크 맵 작업

라이센스: FireSIGHT

네트워크에 연결된 모바일 디바이스를 보고 해당 디바이스에 대한 호스트 프로필로 드릴다운하려면 모바일 디바이스 네트워크 맵을 사용할 수 있습니다. 이 네트워크 맵 보기는 시스템에서 탐지한 모든 고유한 모바일 디바이스의 카운트를 제공합니다(IP가 하나이든 여러 개이든).

시스템이 모바일 디바이스를 구분하기 위해 사용하는 방법은 다음과 같습니다.

- 모바일 디바이스의 모바일 브라우저에서 HTTP 트래픽의 사용자 에이전트 문자열 분석
- 특정 모바일 애플리케이션의 HTTP 트래픽 모니터링

네트워크에 대해 사용자 지정 토폴로지를 생성하면, 서브넷에 할당하는 레이블이 모바일 디바이스 네트워크 맵에 나타납니다.

모바일 디바이스 네트워크 맵을 보려면

액세스: Admin/Any Security Analyst

1단계 **Analysis > Hosts > Network Map**을 선택하고 **Mobile Devices** 탭을 선택합니다.

모바일 디바이스 네트워크 맵이 나타나서 고유한 모바일 디바이스의 카운트 및 모바일 디바이스 IP 주소 목록을 표시합니다. 각 주소 및 부분 주소는 다음 레벨에 대한 링크입니다.

2단계 조사하려는 모바일 디바이스의 특정 IP 주소로 드릴다운합니다.

예를 들어 IP 주소 10.11.40.11을 보려면 **10**, **10.11**, **10.11.40**, **10.11.40.11**을 차례로 클릭합니다. **10.11.40.11**을 클릭하면 호스트 프로필이 나타납니다. 호스트 프로필에 대한 자세한 내용은 49-1페이지의 호스트 프로필 사용을/를 참조하십시오.

IP 또는 MAC 주소를 기준으로 필터링하려면 검색 필드에 주소를 입력합니다. 검색을 지우려면 지우기 아이콘( )을 클릭합니다.

3단계 선택적으로, 서브넷 IP 주소를 삭제하려면 삭제할 요소 옆에 있는 삭제 아이콘( )을 클릭한 다음 디바이스 또는 서브넷을 삭제할 것임을 확인합니다.

디바이스가 삭제됩니다. 디바이스가 다시 검색되면 해당 디바이스는 네트워크 맵에 다시 추가됩니다.

애플리케이션 네트워크 맵 작업

라이센스: FireSIGHT

애플리케이션 이름, 공급업체, 버전별로, 그리고 마지막으로 각 애플리케이션을 실행하는 호스트별로 계층형 트리에 구성되어 있는 네트워크의 애플리케이션을 보려면 애플리케이션 네트워크 맵을 사용할 수 있습니다.

시스템 소프트웨어와 VDB가 업데이트되는 경우, 그리고 애드온 탐지기를 가져오는 경우 시스템에서 탐지하는 애플리케이션이 변경될 수 있습니다. 각 시스템 또는 VDB 업데이트에 대한 릴리스 정보나 자문 텍스트에는 새 탐지기 및 업데이트된 탐지기에 대한 정보가 포함되어 있습니다. 포괄적인 최신 탐지기 목록을 보려면 다음 지원 사이트를 참조하십시오.

- **Sourcefire:** (https://support.sourcefire.com/)
- **Cisco:** (http://www.cisco.com/cisco/web/support/index.html)

애플리케이션 네트워크 맵에서는 특정 애플리케이션을 실행하는 각 호스트의 호스트 프로필을 볼 수도 있고 애플리케이션 카테고리, 모든 호스트에서 실행되는 애플리케이션 또는 특정 호스트에서 실행되는 애플리케이션을 삭제할 수도 있습니다. 예를 들어, 애플리케이션이 호스트에서 비활성화된 것을 알고 있으며 시스템이 영향 레벨 자격에 애플리케이션을 사용하지 않도록 하려면 네트워크 맵에서 해당 애플리케이션을 삭제할 수 있습니다.

네트워크 맵에서 애플리케이션을 삭제해도 네트워크에서 제거되지는 않습니다. 시스템에서 애플리케이션의 변경 사항(예: Apache 웹 서버가 새 버전으로 업그레이드됨)을 탐지하거나 시스템의 검색 기능을 다시 시작하는 경우 삭제된 애플리케이션이 네트워크 맵에 다시 나타납니다.

삭제한 내용에 따라 동작이 달라집니다.

- 애플리케이션 카테고리를 삭제하면 해당 애플리케이션 카테고리가 네트워크 맵에서 제거됩니다. 카테고리에 속하는 모든 애플리케이션이 해당 호스트 프로필에서 제거됩니다.

  예를 들어 **http**를 삭제하면 **http**로 식별되는 모든 애플리케이션이 모든 호스트 프로필에서 제거되며, 네트워크 맵의 애플리케이션 보기에 **http**가 더 이상 나타나지 않습니다.

- 특정 애플리케이션, 공급업체 또는 버전을 삭제하면 영향받는 애플리케이션이 네트워크 맵 및 해당 호스트 프로필에서 제거됩니다.

  예를 들어 **http** 카테고리를 확장하고 **Apache**를 삭제하면, Apache 아래에 나열된 버전과 상관없이 Apache로서 나열된 모든 애플리케이션이 해당 호스트 프로필에서 제거됩니다. 마찬가지로, **Apache**를 삭제하는 대신 특정 버전(예: **1.3.17**)을 삭제하면 선택한 버전만이 영향받는 호스트 프로필에서 삭제됩니다.

- 특정 IP 주소를 삭제하면 애플리케이션 목록에서 해당 IP 주소가 제거되며, 선택한 IP 주소의 호스트 프로필에서 애플리케이션 자체도 제거됩니다.

  예를 들어 **http**, **Apache**, **1.3.17(Win32)**을 확장한 다음 **172.16.1.50:80/tcp**를 삭제하면 Apache 1.3.17(Win32) 애플리케이션이 IP 주소 172.16.1.50의 호스트 프로필에서 삭제됩니다.

애플리케이션 네트워크 맵을 보려면

액세스: Admin/Any Security Analyst

1단계 **Analysis > Hosts > Network Map > Applications**를 선택합니다.

애플리케이션 네트워크 맵이 나타납니다.

2단계 조사하려는 특정 애플리케이션으로 드릴다운합니다.

예를 들어 Apache 같은 특정 웹 서버 유형을 보려면 **http**를 클릭하고 **Apache**를 클릭한 다음, 보려는 Apache 웹 서버의 버전을 클릭합니다.

IP 또는 MAC 주소를 기준으로 필터링하려면 검색 필드에 주소를 입력합니다. 검색을 지우려면 지우기 아이콘(✖)을 클릭합니다.

3단계 선택한 애플리케이션 아래에서 특정 IP 주소를 클릭합니다.

애플리케이션을 실행하는 호스트의 호스트 프로필이 확장된 애플리케이션 섹션과 함께 나타납니다. 호스트 프로필의 애플리케이션 섹션에 대한 자세한 내용은 49-15페이지의 호스트 프로필에서 서버 작업을/를 참조하십시오.

4단계 선택적으로, 애플리케이션 카테고리, 모든 호스트에서 실행되는 애플리케이션 또는 특정 호스트에서 실행되는 애플리케이션을 삭제하려면 삭제할 요소 옆에 있는 삭제 아이콘( )을 클릭하고 삭제할 것임을 확인합니다.

애플리케이션이 삭제됩니다. 애플리케이션이 다시 검색되면 해당 애플리케이션은 네트워크 맵에 다시 추가됩니다.

취약성 네트워크 맵 작업

라이센스: FireSIGHT

시스템이 네트워크에서 탐지한, 레거시 취약성 ID(SVID), Bugtraq ID, CVE ID 또는 Snort ID로 구성된 취약성을 보려면 취약성 네트워크 맵을 사용할 수 있습니다. 취약성은 식별 번호로 정돈되며, 각 취약성 아래에 영향받는 호스트가 나열됩니다.

취약성 네트워크 맵에서 특정 취약성의 세부사항을 볼 수 있으며, 특정 취약성의 영향을 받기 쉬운 호스트의 호스트 프로필도 볼 수 있습니다. 이렇게 하면 해당 취약성이 영향받는 특정 호스트에 미치는 위협을 평가하는 데 도움이 될 수 있습니다.

특정 취약성이 네트워크의 호스트에 영향을 미치지 않을 것으로 생각되면(예: 패치를 적용함) 해당 취약성을 비활성화할 수 있습니다. 비활성화된 취약성은 여전히 네트워크 맵에 나타나지만 영향받는 이전 호스트의 IP 주소는 회색의 기울임꼴로 나타납니다. 그러한 호스트의 호스트 프로필은 비활성화된 취약성을 무효 상태로 표시합니다(개별 호스트에 대해 수동으로 취약성을 유효 상태로 표시할 수 있음). 자세한 내용은 49-30페이지의 개별 호스트에 대해 취약성 설정을/를 참조하십시오.

호스트에서 애플리케이션이나 운영 체제의 ID 충돌이 있는 경우 시스템은 잠재적인 두 ID에 대한 취약성을 나열합니다. ID 충돌이 해결되면 취약성과 현재 ID의 연결 상태가 유지됩니다. 자세한 내용은 46-5페이지의 현재 ID 이해 및 46-6페이지의 ID 충돌 이해을/를 참조하십시오.

기본적으로, 패킷에 애플리케이션의 공급업체 및 버전이 포함된 경우에만 취약성 네트워크 맵에 탐지된 애플리케이션의 취약성이 표시됩니다. 그러나 시스템 정책에서 애플리케이션에 대한 취약성 매핑 설정을 활성화함으로써, 공급업체 및 버전 데이터가 없는 애플리케이션에 대한 취약성을 나열하도록 시스템을 구성할 수 있습니다. 애플리케이션에 대한 취약성 매핑을 설정하는 방법에 대한 자세한 내용은 63-30페이지의 서버에 대한 취약성 매핑을/를 참조하십시오.

취약성 ID(또는 취약성 ID의 범위) 옆에 있는 숫자는 두 개의 카운트를 나타냅니다.

- 첫 번째 숫자는 취약성의 영향을 받는 고유하지 않은 호스트의 카운트입니다. 하나의 호스트가 둘 이상의 취약성에 의해 영향을 받으면 여러 번으로 계산됩니다. 따라서 카운트가 네트워크에 있는 호스트의 수보다 클 수 있습니다. 취약성을 비활성화하면 해당 취약성의 영향을 받을 가능성이 있는 호스트의 수만큼 이 카운트가 줄어듭니다. 취약성 또는 취약성 범위의 영향을 받을 가능성이 있는 호스트에 대해 취약성을 비활성화하지 않은 경우 이 카운트가 표시되지 않습니다.
- 두 번째 숫자는 시스템이 취약성의 영향을 받을 *가능성*이 있는 것으로 판단한, 고유하지 않은 총 호스트의 유사 카운트입니다.

취약성을 비활성화하면 지정한 호스트에 대해서만 비활성이 적용됩니다. 취약한 것으로 판단한 모든 호스트에 대해 또는 취약한 개별 지정 호스트에 대해 취약성을 비활성화할 수 있습니다. 그 후 비활성화되지 않은 호스트에서 취약성이 탐지되면(예: 네트워크 맵의 새 호스트) 시스템은 해당 호스트에 대해 취약성을 활성화합니다. 새로 검색된 취약성은 명시적으로 비활성화해야 합니다. 또한 호스트에 대해 운영 체제 또는 애플리케이션 변경이 탐지되면 시스템은 비활성화된 관련 취약성을 다시 활성화할 수 있습니다.

취약성 네트워크 맵을 보려면

액세스: Admin/Any Security Analyst

1단계 **Analysis > Hosts > Network Map > Vulnerabilities**를 선택합니다.

취약성 네트워크 맵이 나타납니다.

2단계 **Type** 드롭다운 목록에서 보려는 취약성 클래스를 선택합니다. 기본적으로 취약성은 레거시 취약성 ID(SVID)에 의해 표시됩니다.

3단계 조사하려는 특정 취약성으로 드릴다운합니다.

IP 또는 MAC 주소를 기준으로 필터링하려면 검색 필드에 주소를 입력합니다. 검색을 지우려면 지우기 아이콘( )을 클릭합니다.

취약성 세부사항이 나타납니다. 제공된 정보에 대한 자세한 내용은 49-27페이지의 취약성 세부사항 보기을/를 참조하십시오.

또한 네트워크 맵에서 방어 센터는 영향받는 호스트의 IP 주소를 표시합니다. 해당 호스트에 대한 호스트 프로필을 표시하려면 IP 주소를 클릭할 수 있습니다.

4단계 선택적으로, 취약성을 비활성화합니다.

- 취약성의 영향을 받는 모든 호스트에 대해 취약성을 비활성화하려면 취약성 번호 옆에 있는 삭제 아이콘( )을 클릭합니다.
- 개별 호스트에 대해 취약성을 비활성화하려면 호스트 IP 주소 옆에 있는 삭제 아이콘( )을 클릭합니다.

취약성이 비활성화됩니다. 적용되는 호스트의 IP 주소는 네트워크 맵에서 회색의 기울임꼴로 나타납니다. 또한 그러한 호스트의 호스트 프로필에는 비활성화된 취약성이 무효 상태로 표시됩니다.

팁 취약성을 다시 활성화하는 방법에 대한 자세한 내용은 49-30페이지의 개별 호스트에 대해 취약성 설정을/를 참조하십시오.

호스트 특성 네트워크 맵 작업

라이센스: FireSIGHT

호스트 특성으로 구성된 네트워크의 호스트를 보려면 호스트 특성 네트워크 맵을 사용할 수 있습니다. 호스트를 구성하는 데 사용할 호스트 특성을 선택하면 방어 센터는 네트워크 맵에서 해당 특성에 대해 사용할 수 있는 값을 나열하고 할당된 값을 기반으로 호스트를 그룹화합니다. 또한 특정 호스트 특성 값이 할당된 호스트의 호스트 프로필을 볼 수도 있습니다.

호스트 특성 네트워크 맵은 사용자 정의 호스트 특성을 기반으로 호스트를 구성할 수 있습니다. 이러한 특성에 대해 네트워크 맵은 Unassigned로 할당된 값이 없는 호스트를 표시합니다.

자세한 내용은 49-31페이지의 사용자 정의 호스트 특성 작업을/를 참조하십시오.

또한 호스트 특성 네트워크 맵은 사용자가 생성한 규정 준수 화이트리스트에 해당하는 호스트 특성을 기반으로 호스트를 구성할 수 있습니다. 자동으로 생성되는 각 규정 준수 화이트리스트는 화이트리스트와 동일한 이름으로 호스트 특성을 생성합니다.

가능한 화이트리스트 호스트 특성 값은 다음과 같습니다.

- `Compliant` - 화이트리스트를 준수하는 호스트
- `Non-Compliant` - 화이트리스트를 위반하는 호스트
- `Not Evaluated` - 화이트리스트의 유효하지 않은 대상인 호스트 또는 어떤 이유로든 평가되지 않은 호스트

규정준수 화이트리스트에 대한 자세한 내용은 52-1페이지의 규정준수 툴로 FireSIGHT 시스템 사용을/를 참조하십시오.

참고 호스트 특성 네트워크 맵에서는 사전 정의 호스트 특성(예: 호스트 중요도)을 사용하여 호스트를 구성할 수 없습니다.

호스트 특성 네트워크 맵을 보려면

액세스: Admin/Any Security Analyst

1단계 **Analysis > Hosts > Network Map > Host Attributes**를 선택합니다.

호스트 특성 네트워크 맵이 나타납니다.

2단계 **Attribute** 드롭다운 목록에서 호스트 특성을 선택합니다.

방어 센터는 호스트 특성의 값을 나열하며 해당 값이 할당된 호스트의 수를 괄호로 표시합니다.

IP 또는 MAC 주소를 기준으로 필터링하려면 검색 필드에 주소를 입력합니다. 검색을 지우려면 지우기 아이콘(✖)을 클릭합니다.

3단계 값이 할당된 호스트를 보려면 호스트 특성 값을 클릭합니다.

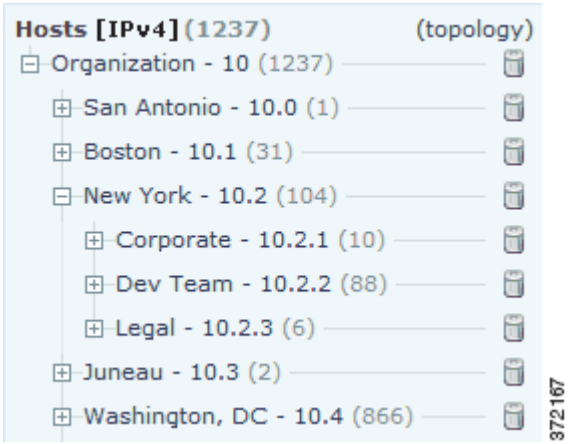
4단계 해당 호스트에 대한 호스트 프로필을 보려면 호스트 IP 주소를 클릭합니다.

사용자 지정 네트워크 토폴로지 작업

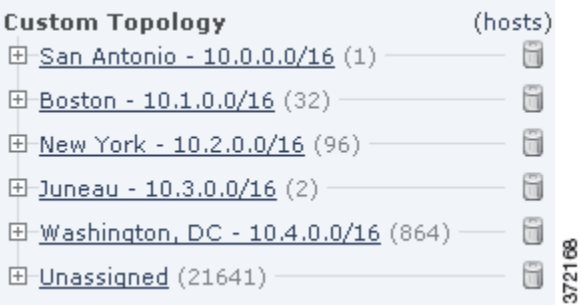
라이센스: FireSIGHT

사용자 지정 토폴로지 기능을 사용하면 호스트 및 네트워크 디바이스 네트워크 맵에서 서브넷을 구성 및 식별하는 데 도움이 될 수 있습니다.

예를 들어 조직의 각 부서에서 서로 다른 서브넷을 사용하는 경우 사용자 지정 토폴로지 기능을 사용하여 서브넷에 레이블을 지정할 수 있습니다. 그런 다음 호스트 또는 네트워크 디바이스 네트워크 맵을 보면, 다음 그림과 같이 서브넷에 할당한 레이블이 나타납니다.



또한 사용자 지정 토폴로지에서 지정한 조직에 따라 호스트 네트워크 맵을 볼 수 있습니다.



호스트 및 네트워크 디바이스 네트워크 맵에 대한 자세한 내용은 48-2페이지의 호스트 네트워크 맵 작업 및 48-4페이지의 네트워크 디바이스 네트워크 맵 작업을/를 참조하십시오.

자세한 내용은 다음 절을 참조하십시오.

- 48-11페이지의 사용자 지정 토폴로지 생성
- 48-15페이지의 사용자 지정 토폴로지 관리

사용자 지정 토폴로지 생성

라이센스: FireSIGHT

사용자 지정 토폴로지를 생성하려면 네트워크를 지정해야 합니다. 다음 세 카테고리 중 하나를 사용하여 지정할 수 있습니다.

- Cisco 검색 토폴로지 가져오기 - 시스템이 탐지한 호스트 및 네트워크 디바이스를 기반으로 네트워크가 구축된 방법을 "가장 잘 추측"하여 네트워크를 추가합니다.
- 네트워크 검색 정책에서 네트워크 가져오기 - FireSIGHT 시스템이 네트워크 검색 정책에서 모니터링하도록 구성한 네트워크를 추가합니다.
- 네트워크를 토폴로지에 수동으로 추가 - 위의 두 방법으로 구축이 부정확하게 또는 불완전하게 표시되는 경우 이 방법을 사용합니다.

토폴로지를 네트워크 맵과 함께 사용하려면 먼저 저장 및 활성화해야 합니다.

사용자 지정 토폴로지를 생성하려면

액세스: Admin/Discovery Admin

1단계 **Policies > Network Discovery**를 선택하고 **Custom Topology**를 클릭합니다.

Custom Topology 페이지가 나타납니다.

2단계 **Create Topology**를 클릭합니다.

Create Topology 페이지가 나타납니다.

3단계 토폴로지 이름 및 설명 등 기본 토폴로지 정보를 제공합니다.

48-12페이지의 기본 토폴로지 정보 제공을/를 참조하십시오.

4단계 네트워크를 토폴로지에 추가합니다. 다음의 전략 중 하나 또는 모두를 사용할 수 있습니다.

- Cisco 검색 토폴로지를 가져와서 네트워크를 토폴로지에 추가하려면 48-12페이지의 검색된 토폴로지 가져오기의 절차를 수행합니다.

- 네트워크 검색 정책에서 네트워크를 가져와 토폴로지에 추가하려면 48-13페이지의 네트워크 검색 정책에서 네트워크 가져오기의 절차를 수행합니다.
- 네트워크를 토폴로지에 수동으로 추가하려면 48-14페이지의 사용자 지정 토폴로지에 네트워크를 수동으로 추가의 절차를 수행합니다.

5단계 토폴로지를 정리하려면

- 사용자 지정 토폴로지에서 네트워크를 제거하려면 제거할 네트워크 옆에 있는 **Delete**를 클릭합니다.
- 네트워크의 이름을 변경하려면 네트워크 옆에 있는 **Rename**을 클릭합니다. 나타나는 팝업 창에서 **Name** 필드에 새 이름을 입력하고 **Rename**을 클릭합니다. 이 이름이 네트워크 맵에서 네트워크의 레이블이 됩니다.

6단계 **Save**를 클릭합니다.

토폴로지가 저장됩니다.

참고 토폴로지를 네트워크 맵과 함께 사용하려면 먼저 활성화해야 합니다. 자세한 내용은 48-15페이지의 사용자 지정 토폴로지 관리을/를 참조하십시오.

기본 토폴로지 정보 제공

라이센스: FireSIGHT

각 사용자 지정 토폴로지에 이름을 지정해야 하며, 선택적으로 짧은 설명을 지정할 수 있습니다.

기본 토폴로지 정보를 제공하려면

액세스: Admin

1단계 Edit Topology 페이지의 **Name** 필드에 토폴로지의 이름을 입력합니다.

2단계 선택적으로, 토폴로지에 대한 설명을 **Description** 필드에 입력합니다.

3단계 선택적으로, 원하는 사용자 지정 토폴로지 작성 방법에 따라 다음 절의 절차를 계속 진행합니다.

- 48-12페이지의 검색된 토폴로지 가져오기
- 48-13페이지의 네트워크 검색 정책에서 네트워크 가져오기
- 48-14페이지의 사용자 지정 토폴로지에 네트워크를 수동으로 추가

검색된 토폴로지 가져오기

라이센스: FireSIGHT

네트워크를 사용자 지정 토폴로지에 추가할 수 있는 한 가지 방법은 FireSIGHT 시스템에 의해 검색된 토폴로지를 가져오는 것입니다. 이 검색된 토폴로지는, 탐색한 호스트 및 네트워크 디바이스를 기반으로 네트워크가 어떻게 구축되었는지를 시스템이 "가장 잘 추측"한 것입니다.

검색된 토폴로지를 가져오려면

액세스: Admin

1단계 Edit Topology 페이지에서 **Import Discovered Topology**를 클릭합니다.

2단계 검색된 네트워크가 페이지에 채워집니다.

3단계 선택적으로, 원하는 사용자 지정 토폴로지 작성 방법에 따라 다음 절의 절차를 계속 진행합니다.

- 48-12페이지의 검색된 토폴로지 가져오기
- 48-13페이지의 네트워크 검색 정책에서 네트워크 가져오기
- 48-14페이지의 사용자 지정 토폴로지에 네트워크를 수동으로 추가

네트워크 검색 정책에서 네트워크 가져오기

라이센스: FireSIGHT

네트워크를 사용자 지정 토폴로지에 추가할 수 있는 한 가지 방법은 FireSIGHT 시스템이 네트워크 검색 정책에서 모니터링하도록 구성한 네트워크를 가져오는 것입니다. 45-23페이지의 네트워크 검색 정책 생성을/를 참조하십시오.

네트워크 검색 정책에서 네트워크를 가져오려면

액세스: Admin

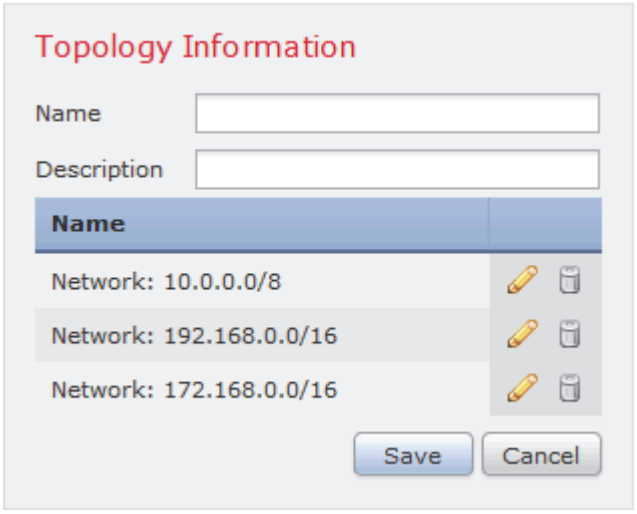
1단계 Edit Topology 페이지에서 **Import Policy Networks**를 클릭합니다.

팝업 창이 나타납니다.

2단계 드롭다운 목록에서 사용할 네트워크 검색 정책을 선택하고 **Load**를 클릭합니다.

3단계 네트워크 검색 정책의 모니터링되는 네트워크가 페이지에 채워집니다.

예를 들어 10.0.0.0/8, 192.168.0.0/16 및 172.12.0.0/16 네트워크를 모니터링하도록 네트워크 검색 정책을 구성한 경우 페이지에 해당 네트워크가 나타납니다.



4단계 다른 네트워크 검색 정책에서 네트워크를 추가하려면 1단계와 2단계를 반복합니다.

5단계 선택적으로, 원하는 사용자 지정 토폴로지 작성 방법에 따라 다음 절의 절차를 수행합니다.

- 48-12페이지의 검색된 토폴로지 가져오기
- 48-14페이지의 사용자 지정 토폴로지에 네트워크를 수동으로 추가

사용자 지정 토폴로지에 네트워크를 수동으로 추가

라이센스: FireSIGHT

Cisco 검색 토폴로지를 가져오고 네트워크 검색 정책에서 네트워크를 가져온 결과 네트워크 구축이 부정확하게 또는 불완전하게 표시되는 경우, 사용자 지정 토폴로지에 네트워크를 수동으로 추가할 수 있습니다.

사용자 지정 토폴로지에 네트워크를 수동으로 추가하려면

액세스: Admin

1단계 Edit Topology 페이지에서 **Add Network**를 클릭합니다.

팝업 창이 나타납니다.

2단계 선택적으로, **Name** 필드에 이름을 입력하여 네트워크 이름을 지정합니다.

토폴로지를 활성화한 후 이 이름은 호스트 및 네트워크 디바이스 네트워크 맵에서 네트워크의 레이블이 됩니다.

자세한 내용은 48-2페이지의 호스트 네트워크 맵 작업 및 48-4페이지의 네트워크 디바이스 네트워크 맵 작업을/를 참조하십시오.

3단계 토폴로지에 추가하려는 네트워크를 나타내는 IP 주소 및 네트워크 마스크(CIDR 표기법)를 **IP Address** 및 **Netmask** 필드에 입력합니다.

FireSIGHT 시스템에서 CIDR 표기법을 사용하는 방법에 대한 자세한 내용은 1-19페이지의 IP 주소 표기 규칙을/를 참조하십시오.

4단계 **Add**를 클릭합니다.

네트워크가 토폴로지에 추가됩니다.

5단계 토폴로지에 네트워크를 더 추가하려면 1~4단계를 반복합니다.

팁 토폴로지에서 네트워크를 삭제하려면 삭제할 네트워크 옆에 있는 **Delete**를 클릭하고, 네트워크 및 네트워크에 대한 모든 링크를 삭제할 것임을 확인합니다.

6단계 선택적으로, 원하는 사용자 지정 토폴로지 작성 방법에 따라 다음 절의 절차를 수행합니다.

- 48-12페이지의 검색된 토폴로지 가져오기
- 48-13페이지의 네트워크 검색 정책에서 네트워크 가져오기

사용자 지정 토폴로지 관리

라이센스: FireSIGHT

사용자 지정 토폴로지를 관리하려면 Custom Topology 페이지를 사용할 수 있습니다. 토폴로지를 생성, 수정 및 삭제할 수 있습니다.

토폴로지의 상태가 이름과 함께 나타납니다. 정책 이름 옆에 있는 전구 아이콘이 밝게 표시되면 토폴로지가 활성 상태이며 네트워크 맵에 영향을 미치게 됩니다. 어두우면 토폴로지가 비활성 상태입니다. 언제든 하나의 사용자 지정 토폴로지만 활성 상태를 유지할 수 있습니다. 여러 토폴로지를 생성한 경우 하나를 활성화하면 현재 활성 상태인 토폴로지는 자동으로 비활성화됩니다.

사용자 지정 토폴로지를 활성화/비활성화하거나 수정하거나 삭제하려면 다음 절차를 따르십시오.

활성 토폴로지를 삭제하면 변경 사항이 즉시 영향을 미칩니다. 즉, 네트워크 맵에 사용자 지정 토폴로지가 더 이상 표시되지 않습니다.

사용자 지정 토폴로지를 활성화 또는 비활성화하려면

액세스: Admin

1단계 **Policies > Network Discovery > Custom Topology**를 선택합니다.

Custom Topology 페이지가 나타납니다.

2단계 다음 2가지 옵션을 사용할 수 있습니다.

- 토폴로지를 **활성화**하려면 정책 옆에 있는 **Activate**를 클릭합니다.
- 토폴로지를 **비활성화**하려면 정책 옆에 있는 **Deactivate**를 클릭합니다.

사용자 지정 토폴로지를 수정하려면

액세스: Admin

1단계 **Policies > Network Discovery > Custom Topology**를 선택합니다.

Custom Topology 페이지가 나타납니다.

2단계 수정할 토폴로지 옆에 있는 수정 아이콘( )을 클릭합니다.

Edit Topology 페이지가 나타납니다. 변경할 수 있는 각종 컨피그레이션에 대한 자세한 내용은 48-11페이지의 사용자 지정 토폴로지 생성을/를 참조하십시오.

3단계 필요한 대로 변경하고 **Save**를 클릭합니다.

토폴로지가 변경됩니다. 토폴로지가 활성 상태인 경우 변경한 내용이 네트워크 맵에서 즉시 적용됩니다.

사용자 지정 토폴로지를 삭제하려면

액세스: Admin

1단계 **Policies > Network Discovery > Custom Topology**를 선택합니다.

Custom Topology 페이지가 나타납니다.

2단계 삭제할 토폴로지 옆에 있는 **Delete**를 클릭합니다. 토폴로지가 활성 상태이면 삭제할 것임을 확인합니다.

토폴로지가 삭제됩니다.

49장

호스트 프로필 사용

호스트 프로필은 시스템이 단일 호스트에 대해 수집한 모든 정보를 완벽하게 보여줍니다. 프로필을 통해 호스트 이름과 운영 체제 등 일반적인 호스트 정보에 액세스할 수 있습니다. 예를 들어, 호스트에 대한 MAC 주소를 빠르게 찾아야 하는 경우 호스트 프로필에서 찾아볼 수 있습니다.

해당 호스트에 대한 *호스트 특성*도 프로필에 나열됩니다. 호스트 특성은 호스트에 적용할 수 있는 사용자 정의 설명입니다. 예를 들면 호스트의 정확한 위치를 나타내는 호스트 특성을 할당할 수 있습니다. 호스트 프로필에서 해당 호스트에 적용된 기존 호스트 속성을 보고 호스트 특성 값을 수정할 수 있습니다. 또 다른 예로, *호스트 중요도* 특성은 특정 호스트의 비즈니스 중요도를 할당하고 호스트 중요도를 기반으로 상관관계 정책 및 알림을 맞춤화하는 데 사용할 수 있습니다.

호스트 프로필은 특정 호스트에서 실행 중인 서버, 클라이언트, 호스트 프로토콜에 대한 정보를 제공하며 여기에는 규정 준수 화이트리스트의 준수 여부도 포함됩니다. 서버 목록에서 서버를 제거하고 해당 서버에 대한 세부사항을 볼 수 있습니다. 또한 서버의 *연결 이벤트*를 보고, 서버 트래픽이 탐지된 세션에 대한 정보를 로깅할 수 있습니다. 클라이언트에 대한 세부사항 및 연결 이벤트를 보고 호스트 프로필에서 서버, 클라이언트 또는 호스트 프로토콜을 삭제할 수 있습니다.

FireSIGHT 시스템 구축에 FireSIGHT 라이센스가 포함된 경우 호스트 프로필에서 IOC(*indications of compromise*)를 볼 수 있습니다. 이러한 IOC는 다양한 유형의 데이터(침입 이벤트, 보안 인텔리전스, 연결 이벤트, 파일 또는 악성코드 이벤트)를 호스트와 연결하여, 모니터링되는 네트워크의 호스트가 악의적인 수단에 의해 손상될 가능성이 있는지를 확인합니다. 호스트 프로필에서 호스트 IOC 태그의 개요를 보고, IOC와 연결된 이벤트를 보고, IOC 태그를 확인된 것으로 표시하고, 검색 정책에서 IOC 규칙 상태를 수정할 수 있습니다.

구축에 보호 라이센스가 포함된 경우 호스트의 운영 체제 유형과 호스트가 실행 중인 서버 및 클라이언트에 가장 알맞게 시스템의 트래픽 처리 방법을 맞춤화할 수 있습니다. 자세한 내용은 30-1페이지의 수동 구축 시 전처리 튜닝을/를 참조하십시오.

시스템에서 추적하도록 구성한 경우 호스트에 대한 사용자 기록 정보를 볼 수 있습니다. 그러면 사용자 활동의 마지막 24시간을 그래프로 볼 수 있습니다.

호스트 프로필에서 호스트에 대한 취약성 목록을 수정할 수 있습니다. 이 기능을 사용하면 어떤 취약성이 호스트에 대해 해결되었는지를 추적할 수 있습니다. 또한 취약성에 대한 수정을 적용하고, 수정으로 해결된 모든 취약성을 자동으로 유효하지 않은 것으로 표시할 수 있습니다.

Cisco 시스템에서 생성한 취약성 정보로 작업하고 서드파티 스캐너로 탐지된 취약성에 대한 정보도 사용할 수 있으며, 호스트 입력 기능을 사용하여 이를 방어 센터로 가져올 수 있습니다.

선택적으로, 호스트 프로필에서 Nmap 스캔을 수행하여 호스트 프로필의 서버 및 운영 체제 정보를 강화할 수 있습니다. Nmap 스캐너는 호스트를 적극적으로 조사하여 호스트에서 실행 중인 운영 체제와 서버에 대한 정보를 가져옵니다. 스캔 결과는 호스트에 대한 운영 체제 및 서버 ID의 목록에 추가됩니다.

네트워크의 모든 호스트에 대해 호스트 프로필을 이용할 수 있는 것은 아닙니다. 가능한 이유는 다음과 같습니다.

- 시간 초과되어 호스트가 네트워크 맵에서 삭제됨
- FireSIGHT 호스트 라이센스 제한에 도달함
- 호스트가 네트워크 검색 정책에서 모니터링하지 않는 네트워크 세그먼트에 상주함

호스트 프로필에 표시되는 정보는 호스트 유형 및 호스트에 대해 사용 가능한 정보에 따라 달라질 수 있습니다. 예를 들어 시스템에서 비 IP 기반 프로토콜(예: STP, SNAP, IPX)을 탐지한 경우, 호스트는 네트워크 맵에 MAC 호스트로 추가되는데 이 경우 IP 호스트에 비해 사용 가능한 정보가 훨씬 적습니다.

또 다른 예로, NetFlow 지원 디바이스에서 내보낸 데이터를 기반으로 네트워크 맵에 호스트와 서버 및 클라이언트를 추가하도록 네트워크 검색 정책을 구성할 수 있지만, 이러한 호스트와 서버 및 클라이언트에 대해 사용할 수 있는 정보는 제한적입니다. 예를 들어 이 호스트에 사용 가능한 운영 체제 데이터는 스캐너 또는 호스트 입력 기능을 사용하여 제공해야 합니다. 자세한 내용은 45-17페이지의 NetFlow 및 FireSIGHT 데이터 간 차이점을/를 참조하십시오.

다음 그림에서는 호스트 프로필의 예를 보여줍니다.

Host Profile

Scan Host | Generate White List Profile

IP Addresses	**192.168.1.4**
NetBIOS Name	
Device (Hops)	sampledevice (9)
MAC Addresses (TTL)	00:00:00:00:00:00 (Dell Inc.) (64)
Host Type	Host
Last Seen	2013-11-22 23:18:55
Current User	
View	Context Explorer | Connection Events | Intrusion Events | File Events | Malware Events

Indications of Compromise (3)

Edit Rule States | Mark All Resolved

Category	Event Type	Description	First Seen	Last Seen
Malware Executed	Threat Detected by FireAMP - Executed	The host has executed malware	2013-11-20 14:23:30	2013-12-03 10:35:07
Malware Detected	Threat Detected by FireAMP - Not Executed	The host has encountered malware	2013-11-20 15:26:50	2013-12-03 09:40:20
Dropper Infection	Dropper Infection Detected by FireAMP	The host may be infected with Dropper	2013-11-21 02:43:56	2013-12-02 03:44:29

Operating System (pending)

Edit Operating System

Users (no user history available)

Attributes

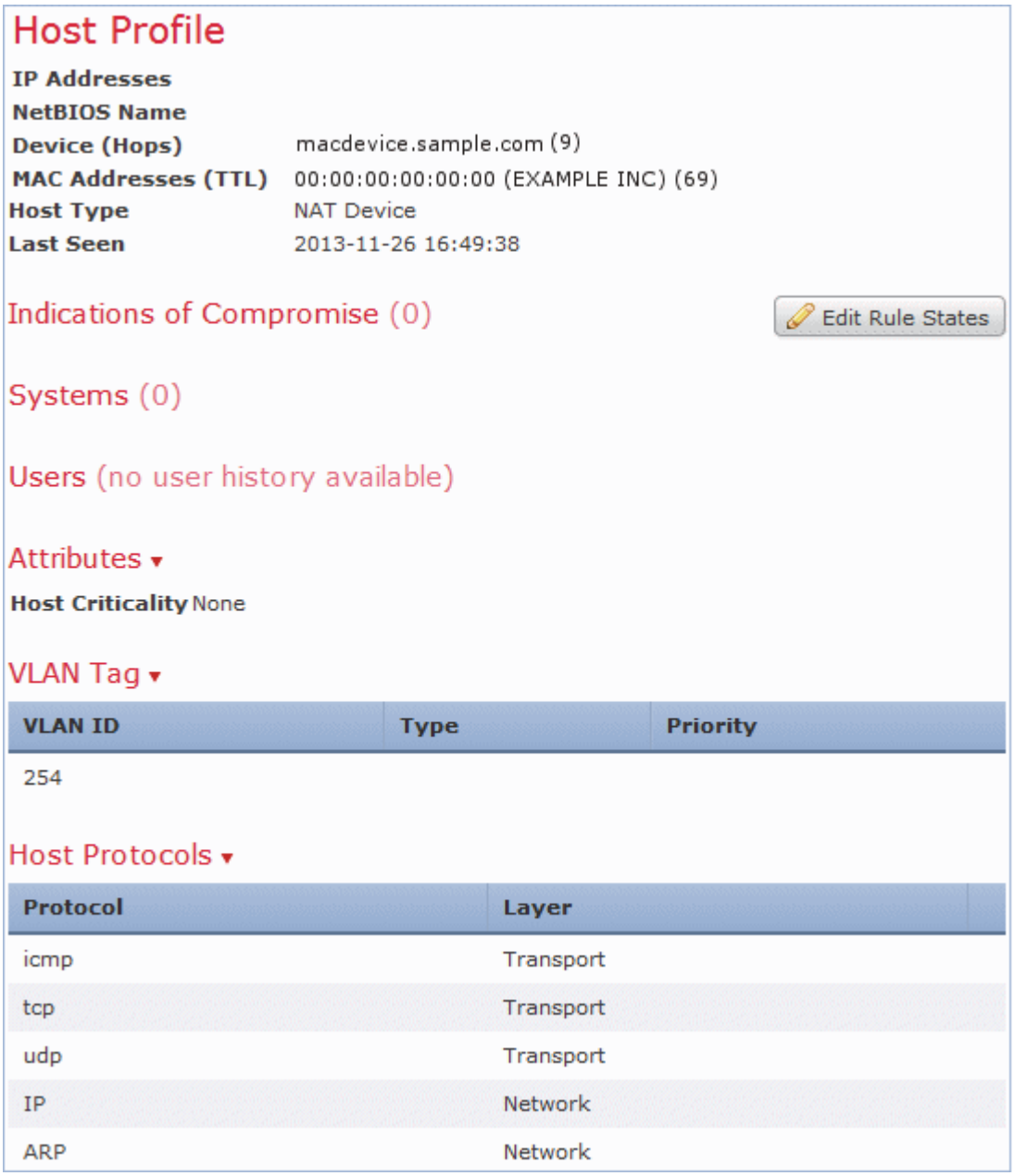
Edit Attributes

Host Criticality None

Host Protocols

Protocol	Layer
icmp	Transport
tcp	Transport
udp	Transport
IP	Network
ARP	Network

다음 그림에서는 MAC 호스트에 대한 호스트 프로필의 예를 보여줍니다.



호스트 프로필의 각 섹션에 대한 자세한 내용은 다음을 참조하십시오.

- 49-5페이지의 호스트 프로필 보기 - 호스트 프로필에 액세스하는 방법에 대해 설명합니다.
- 49-6페이지의 호스트 프로필에서 기본 호스트 정보 작업 - 호스트 프로필의 Host 섹션에서 제공하는 정보에 대해 설명합니다.
- 49-8페이지의 호스트 프로필에서 IP 주소 작업 - 호스트 프로필의 IP Addresses 섹션에서 제공하는 정보에 대해 설명합니다.
- 49-8페이지의 호스트 프로필에서 IOC 작업 - 호스트 프로필의 Indications of Compromise 섹션에서 제공하는 정보에 대해 설명합니다.

- 49-10페이지의 호스트 프로필에서 운영 체제 작업 - 호스트 프로필의 Operating System 또는 Operating System Conflicts 섹션에서 제공하는 정보에 대해 설명하고, 운영 체제를 수정하거나 운영 체제 충돌을 해결하는 방법에 대해 설명합니다.
- 49-15페이지의 호스트 프로필에서 서버 작업 - 호스트 프로필의 Servers, Server Detail 및 Server Banner 섹션에서 제공하는 정보에 대해 설명합니다.
- 49-19페이지의 호스트 프로필에서 애플리케이션 작업 - 호스트 프로필의 Clients 섹션에서 제공하는 정보에 대해 설명합니다.
- 49-21페이지의 호스트 프로필에서 VLAN 태그 작업 - 호스트 프로필의 VLAN Tag 섹션에서 제공하는 정보에 대해 설명합니다.
- 49-22페이지의 호스트 프로필에서 사용자 기록 작업 - 호스트 프로필의 User History 섹션에서 제공하는 정보에 대해 설명합니다.
- 49-22페이지의 호스트 프로필에서 호스트 특성 작업 - 호스트 프로필의 Attributes 섹션에서 제공하는 정보에 대해 설명합니다.
- 49-30페이지의 사전 정의 호스트 특성 작업 - 호스트 중요도 특성을 설정하는 방법 및 호스트 프로필에 메모를 추가하는 방법에 대해 설명합니다.
- 49-31페이지의 사용자 정의 호스트 특성 작업 - 사용자 정의 호스트 특성의 생성 및 사용에 대한 정보를 제공합니다.
- 49-23페이지의 호스트 프로필에서 호스트 프로토콜 작업 - 호스트 프로필의 Host Protocols 섹션에서 제공하는 정보에 대해 설명합니다.
- 49-24페이지의 호스트 프로필에서 화이트리스트 위반 작업 - 호스트 프로필의 White List Violations 섹션에서 제공하는 정보에 대해 설명합니다.
- 49-25페이지의 호스트 프로필에서 악성코드 탐지 작업 - 호스트 프로필의 Most Recent Malware Detections 섹션에서 제공하는 정보에 대해 설명합니다.
- 49-26페이지의 호스트 프로필에서 취약성 작업 - 호스트 프로필의 Vulnerabilities 및 Vulnerability Detail 섹션에서 제공하는 정보에 대해 설명합니다.

호스트 프로필 보기

라이센스: FireSIGHT

모니터링되는 네트워크에 있는 호스트의 IP 주소를 포함하는 이벤트 보기 또는 네트워크 맵에서 호스트 프로필에 액세스할 수 있습니다. 예를 들어, 검색 이벤트의 테이블 보기에는 IP Address 열의 모든 항목 옆에 있는 호스트 프로필에 대한 링크가 포함되어 있습니다. IOC(Indication of Compromise) 규칙을 활성화하면, 손상 가능성이 있는 호스트는 다른 호스트 프로필 아이콘으로 표시됩니다.

이벤트 보기에서 호스트 프로필을 보려면

액세스: Admin/Any Security Analyst

1단계 이벤트 보기에서, 프로필을 보려는 호스트의 IP 주소 옆에 있는 호스트 프로필 아이콘( ) 또는 손상된 호스트 아이콘( )을 클릭합니다.

호스트 프로필이 팝업 창에 나타납니다.

네트워크 맵에서 호스트 프로필을 보려면

액세스: Admin/Any Security Analyst

1단계 네트워크 맵에서, 프로필을 보려는 호스트의 IP 주소로 드릴다운합니다.

호스트 프로필이 나타납니다. 네트워크 맵에서 호스트 프로필에 액세스하는 방법의 예는 48-2페이지의 호스트 네트워크 맵 작업을/를 참조하십시오.

호스트 프로필에서 기본 호스트 정보 작업

라이센스: FireSIGHT

각 호스트 프로필은 탐지된 호스트 또는 기타 디바이스에 대한 기본 정보를 제공합니다.

다음은 각각의 기본 호스트 프로필 필드에 대한 설명입니다.

IP Addresses

호스트와 연결된 모든 IP 주소(IPv4 및 IPv6 모두). IPv6 호스트에는 종종 4개의 IPv6 주소(로컬 전용 및 전역 라우팅 가능)가 있으며 IPv4 주소도 있을 수 있습니다. IPv4 전용 호스트에는 여러 개의 IPv4 주소가 있을 수 있습니다. 사용 가능한 경우, 라우팅 가능한 호스트 IP 주소에는 관련 지오로케이션 데이터를 나타내는 국가 코드 및 플래그 아이콘도 포함할 수 있습니다. 이것과 기타 지오로케이션 기능에 대한 자세한 내용은 58-20페이지의 지오로케이션 사용을/를 참조하십시오.

Hostname

알려진 경우 호스트의 정규화된 도메인 이름

NetBIOS Name

사용 가능한 경우 호스트의 NetBIOS 이름. Microsoft Windows 호스트는 물론 Macintosh, Linux 또는 NetBIOS를 사용하도록 구성된 기타 플랫폼은 NetBIOS 이름을 가질 수 있습니다. 예를 들어 Samba 서버로 구성된 Linux 호스트는 NetBIOS 이름을 가질 수 있습니다.

Device (Hops)

다음 중 하나:

- 네트워크 검색 정책에 정의된 대로, 호스트가 상주하는 네트워크에 대한 보고 디바이스 또는
- 호스트를 네트워크 맵에 추가한 NetFlow 데이터를 처리한 디바이스
- 디바이스 이름 뒤에 호스트를 탐지한 디바이스와 호스트 자체 간 네트워크 홉의 수가 괄호로 표시됩니다. 여러 디바이스가 호스트를 볼 수 있는 경우 보고 디바이스는 굵은 글꼴로 표시됩니다.
- 이 필드가 비어 있는 경우는 다음 중 하나입니다.
- 네트워크 검색 정책에 정의된 대로, 호스트 상주 네트워크를 명시적으로 모니터링하지 않는 디바이스에 의해 호스트가 네트워크 맵에 추가되었습니다.
- 호스트가 호스트 입력 기능으로 추가되었으며 FireSIGHT 시스템에 의해 탐지되지 않았습니다.

MAC Addresses (TTL)

호스트의 탐지된 MAC 주소 및 관련 NIC 공급업체. NIC의 하드웨어 공급업체와 TTL(time-to-live) 값은 괄호로 표시됩니다. 굵은 글꼴로 표시되는 MAC 주소는 ARP 및 DHCP 트래픽을 통해 시스템에 의해 탐지된 호스트의 실제 MAC 주소입니다. 여러 디바이스가 호스트를 탐지한 경우 이를 보고한 디바이스와 상관없이, 방어 센터에서는 호스트와 관련된 모든 MAC 주소 및 TTL 값을 표시합니다.

동일한 MAC 주소와 함께 호스트의 목록을 보려면 MAC 주소를 클릭할 수 있습니다. 라우터 호스트 프로필은 일반적으로 이 목록에서 라우팅하는 네트워크 세그먼트의 호스트(IP 주소)를 보여줍니다. 모니터링되는 라우터의 IP 주소는 종종 모니터링되는 워크스테이션 및 서버에 대해 이 목록에 나타납니다. MAC 주소의 실제 IP 주소는 굵은 글꼴로 표시됩니다.

Host Type

호스트, 모바일 디바이스, 탈옥 모바일 디바이스, 라우터, 브리지, NAT 디바이스 또는 로드 밸런서 등 시스템이 탐지한 디바이스의 유형.

시스템이 네트워크 디바이스를 구분하기 위해 사용하는 방법은 다음과 같습니다.

- CDP(Cisco Discovery Protocol) 메시지의 분석 - 네트워크 디바이스 및 유형을 식별할 수 있습니다(Cisco 디바이스만 해당).
- STP(Spanning Tree Protocol)의 탐지 - 디바이스를 스위치 또는 브리지로 식별합니다.
- 동일한 MAC 주소를 사용하는 여러 호스트 탐지 - MAC 주소를 라우터에 속한 것으로 식별합니다.
- 클라이언트 측에서 TTL 값 변경 탐지 또는 일반적인 부팅시간보다 더 자주 변경되는 TTL 값 - NAT 디바이스 및 로드 밸런서를 탐지합니다.
- 시스템이 모바일 디바이스를 구분하기 위해 사용하는 방법은 다음과 같습니다.
- 모바일 디바이스의 모바일 브라우저에서 HTTP 트래픽의 사용자 에이전트 문자열 분석
- 특정 모바일 애플리케이션의 HTTP 트래픽 모니터링

네트워크 디바이스 또는 모바일 디바이스로 식별되지 않는 디바이스는 호스트로 분류됩니다.

Last Seen

마지막으로 탐지한 호스트 IP 주소 중 하나의 날짜 및 시간

Current User

가장 최근에 이 호스트에 로그인한 사용자

기존의 현재 사용자가 권한 있는 사용자가 아닌 경우, 호스트에 로그인한 권한 없는 사용자는 호스트에서 현재 사용자로만 등록됩니다. 자세한 내용은 45-7페이지의 사용자 데이터베이스을/를 참조하십시오.

View

이벤트 데이터의 보기에 대한 링크. 해당 이벤트 유형에 대해 기본 워크플로를 사용하며 호스트와 관련된 이벤트를 표시하도록 제한됩니다. 가능한 경우 이러한 이벤트에는 호스트와 연결된 모든 IP 주소가 포함됩니다. 자세한 내용은 다음 절을 참조하십시오.

- 목차 탐색 - 자세한 내용은 56-1페이지의 Context Explorer 사용 참조
- 연결 이벤트 - 자세한 내용은 39-2페이지의 연결 및 보안 인텔리전스 데이터 이해 참조
- 검색 이벤트 - 자세한 내용은 50-1페이지의 검색 이벤트 작업 참조
- 악성코드 이벤트 - 자세한 내용은 40-17페이지의 악성코드 이벤트 작업 참조
- 소스별 침입 이벤트 - 자세한 내용은 41-1페이지의 침입 이벤트 작업 참조
- 대상별 침입 이벤트 - 자세한 내용은 41-1페이지의 침입 이벤트 작업 참조

호스트 프로필에서 IP 주소 작업

라이센스: FireSIGHT

시스템은 호스트와 연결된 IP 주소를 탐지하며, 지원되는 경우 동일한 호스트에 의해 사용되는 여러 IP 주소를 그룹화합니다. IPv6 호스트에는 대개 최소 2개의 IPv6 주소(로컬 전용 및 전역 라우팅 가능)가 있습니다. 하나 이상의 할당된 IPv4 주소도 있을 수 있습니다. IPv4 전용 호스트에는 여러 개의 IPv4 주소가 있을 수 있습니다.

호스트 프로필에는 해당 호스트와 연결된 모든 탐지된 IP 주소가 나열됩니다. 사용 가능한 경우, IP 주소는 작은 플래그 아이콘 및 관련 국가를 나타내는 ISO 국가 코드와 함께 나타납니다. 지오로케이션 세부사항을 보려면 플래그 아이콘 또는 국가 코드를 클릭할 수 있습니다. 자세한 내용은 58-20페이지의 지오로케이션 사용을/를 참조하십시오.

기본적으로 처음 3개 주소만 표시됩니다. 호스트의 모든 주소를 표시하려면 **show all**을 클릭하십시오.

호스트 프로필에서 IOC 작업

라이센스: FireSIGHT

FireSIGHT 시스템은 다양한 유형의 데이터(침입 이벤트, 보안 인텔리전스, 연결 이벤트, 파일 또는 악성코드 이벤트)를 호스트와 연결하여, 모니터링되는 네트워크의 호스트가 악의적인 수단에 의해 손상될 가능성이 있는지를 확인합니다. 이벤트 데이터의 특정 조합 및 빈도는 영향받는 호스트에서 IOC(indications of compromise) 태그를 트리거합니다. 호스트 프로필의 Indications of Compromise 섹션에는 호스트에 대한 모든 IOC 태그가 표시됩니다. 이 섹션에서는 호스트에서 직면한 위협의 세부사항을 보고, IOC 태그를 트리거한 이벤트로 이동하고 IOC 규칙 상태를 수정하고, 더 이상 관련이 없는 IOC 태그를 해제할 수 있습니다.

IOC 기능을 사용하려면 이 기능과 함께 검색 정책에서 적어도 하나의 IOC 규칙을 활성화해야 합니다. 또한 해당 호스트의 호스트 프로필 페이지에서 개별 호스트에 대한 규칙 상태도 수정할 수 있습니다. 각 IOC 규칙은 하나의 IOC 태그 유형에 해당합니다. 조직의 요구에 따라 일부 또는 전체 규칙을 활성화할 수 있습니다. 검색 정책 및 전반적인 IOC에 대한 자세한 내용은 45-20페이지의 IOC 이해을/를 참조하십시오.

호스트 프로필의 내용 외에도, 이벤트 뷰어에서 IOC 데이터를 분석할 수 있습니다. 자세한 내용은 50-32페이지의 IOC 작업을/를 참조하십시오.

다음은 호스트 프로필에 표시되는 IOC 정보 필드에 대한 설명입니다.

IP Address

IOC를 트리거한 호스트와 연결된 IP 주소

Category

표시된 감염 유형에 대한 짧은 설명(예: `Malware Executed` 또는 `Impact 1 Attack`)

Event Type

특정 IOC(Indication of Compromise)와 관련된 식별자로, 이를 트리거한 이벤트를 가리킴

Description

감염 가능성이 있는 호스트를 위협하는 것에 대한 설명(예: `This host may be under remote control` 또는 `Malware has been executed on this host`)

First/Last Seen

호스트의 IOC를 트리거하는 이벤트가 발생한 최초의(또는 가장 최근의) 날짜 및 시간

호스트 프로필에서 IOC 데이터로 작업하는 방법에 대한 자세한 내용은 다음 절을 참조하십시오.

- 49-9페이지의 단일 호스트에 대한 IOC 규칙 상태 수정
- 49-9페이지의 IOC에 대한 소스 이벤트 보기
- 49-10페이지의 IOC 해결

단일 호스트에 대한 IOC 규칙 상태 수정

라이센스: FireSIGHT

시스템에서 IOC(indications of compromise)를 탐지하고 태깅하도록 하려면 먼저 검색 정책에서 IOC 기능을 활성화하고 적어도 하나의 IOC 규칙(정책 전체 또는 개별 호스트)을 활성화해야 합니다. 호스트 프로필에서 해당 개별 호스트에 적용되는 IOC 규칙 상태를 설정할 수 있습니다. 검색 정책에서 IOC를 구성하고 정책 전체 IOC 규칙 상태를 설정하는 방법에 대한 자세한 내용은 45-34페이지의 IOC 규칙 설정을/를 참조하십시오.

호스트 프로필의 Indications of Compromise 섹션에서 **Edit Rule States** 링크를 이용해 IOC 규칙 목록에 액세스하고 내용을 수정할 수 있습니다. 네트워크 및 조직의 필요에 따라 규칙의 일부 또는 전체를 활성화할 수 있습니다. 예를 들어, Microsoft Excel과 같은 소프트웨어를 사용하는 호스트가 모니터링되는 네트워크에 나타나지 않으면 Excel 기반 위협에 해당하는 IOC 태그를 활성화하지 않을 수 있습니다.

모든 IOC 규칙은 Cisco에서 사전 정의합니다. 트리거된 IOC 태그에 대해 규정 준수 규칙을 작성할 수는 있지만 원래 규칙을 생성할 수는 없습니다. 자세한 내용은 51-1페이지의 상관관계 정책 및 규칙 구성을/를 참조하십시오. 각 IOC 규칙은 한 가지 이벤트 유형(예: 악성코드 또는 침입)에 의해 트리거되며 하나의 특정 IOC 태그에 해당합니다. 손쉬운 대응을 위해 규칙과 태그에 모두 동일한 Category, Event Type 및 Description 데이터가 있습니다. IOC 규칙 상태의 Edit 페이지에는 또한 각 규칙에 대한 이벤트 데이터 Source가 나열되어, 규칙 트리거에 필요한 시스템 기능이 무엇인지를 분명하게 보여줍니다.

호스트에 대한 IOC 규칙 상태를 수정하려면

액세스: Admin/Any Security Analyst

1단계 호스트 프로필의 **Indications of Compromise** 섹션에서 **Edit Rule States**를 클릭합니다.

Edit Indication of Compromise Rule States 페이지가 새 창에 나타납니다.

2단계 규칙의 **Enabled** 열에서 슬라이더를 클릭하여 규칙을 활성화 또는 비활성화합니다.

3단계 **Save**를 클릭합니다.

변경 내용이 저장되었습니다.

IOC에 대한 소스 이벤트 보기

라이센스: FireSIGHT

호스트에서 IOC 태그를 트리거한 이벤트로 빠르게 이동하려면 Indications of Compromise 섹션을 사용할 수 있습니다. 이러한 이벤트를 분석하면 손상 가능성이 있는 호스트에 대한 위협을 해결하기 위해 어떤 조치가 필요한지(및 필요한지 여부)를 결정하기 위해 필요한 정보를 얻을 수 있습니다.

IOC 태그의 타임스탬프 옆에 있는 보기 아이콘( )을 클릭하면 IOC 태그를 트리거한 이벤트만 표시하도록 제한된, 관련 이벤트 유형에 대한 이벤트의 테이블 보기로 이동합니다.

IOC 태그를 트리거한 이벤트와 기능의 유형에 대한 자세한 내용은 다음을 참조하십시오.

- 39-1페이지의 연결 및 보안 인텔리전스 데이터 작업
- 41-1페이지의 침입 이벤트 작업
- 37-2페이지의 악성코드 차단 및 파일 제어 이해

IOC 태그에 대한 소스 이벤트를 보려면

액세스: Admin/Any Security Analyst

1단계 호스트 프로필의 **Indications of Compromise** 섹션에서, 조사할 IOC 태그에 대한 **First Seen** 또는 **Last Seen** 열에 있는 보기 아이콘( )을 클릭합니다.

IOC를 트리거한 해당 이벤트에 대한 이벤트의 테이블 보기가 나타나며, 트리거링 이벤트만 표시하도록 제한됩니다. 호스트 프로필 페이지가 별도의 창에 나타나는 경우 이벤트 보기는 주 창에 나타납니다.

IOC 해결

라이센스: FireSIGHT

IOC 태그에 의해 표시된 위협을 분석 및 해결했거나 IOC 태그가 오탐인 것으로 확인되는 경우, 태그를 해결된 것으로 표시할 수 있습니다. 해결된 것으로 표시된 IOC 태그는 호스트 프로필에서 제거됩니다. 호스트의 모든 활성 IOC 태그가 해결되면 해당 호스트에는 감염된 호스트 아이콘( )이 더 이상 표시되지 않습니다. 해결된 IOC에 대해 여전히 IOC 트리거링 이벤트가 표시될 수 있습니다.

호스트의 IOC 태그를 트리거한 이벤트가 반복되면 태그가 다시 설정됩니다. 호스트에서 개별 IOC 태그를 해결할 수도 있고, 호스트의 태그를 모두 해결된 것으로 표시할 수도 있습니다.

IOC 태그를 해결하려면

액세스: Admin/Any Security Analyst

1단계 호스트 프로필의 **Indications of Compromise** 섹션에는 두 가지 옵션이 있습니다.

- 개별 IOC 태그를 해결된 것으로 표시하려면 원하는 태그의 오른쪽에 있는 해결 아이콘( )을 클릭합니다.
- 호스트의 모든 IOC 태그를 해결된 것으로 표시하려면 **Mark All Resolved**를 클릭합니다.

변경 사항이 저장되고 선택한 IOC 태그가 제거됩니다.

호스트 프로필에서 운영 체제 작업

라이센스: FireSIGHT

시스템은 호스트에 의해 생성되는 트래픽에서 네트워크 및 애플리케이션 스택을 분석하거나 User Agent에 의해 보고된 호스트 데이터를 분석하여, 호스트에서 실행되는 운영 체제의 ID를 수동적으로 탐지합니다. 시스템은 또한 Nmap 스캐너 또는 호스트 입력 기능을 통해 가져온 애플리케이션 데이터 등의 다른 소스에서 운영 체제 정보를 취합합니다. 사용할 ID를 결정할 때 시스템은 각 ID 소스에 할당된 우선순위를 고려합니다. 기본적으로 사용자 입력의 우선순위가 가장 높고, 그다음은 애플리케이션 또는 스캐너 소스, 그다음은 Cisco에서 검색한 ID입니다.

트래픽 및 기타 ID 소스는 좀 더 구체적인 ID에 대해 충분한 정보를 제공하지 않으므로 때때로 시스템은 일반(특정이 아닌) 운영 체제 정의를 제공합니다. 시스템은 가능한 한 가장 자세한 정의를 사용하기 위해 여러 소스의 정보를 취합합니다.

다음은 호스트 프로필에 표시되는 운영 체제 정보 필드에 대한 설명입니다.

Hardware

모바일 디바이스용 하드웨어 플랫폼

OS Vendor/Vendor

운영 체제 공급업체

OS Product/Product

모든 소스에서 수집된 ID 데이터를 기반으로, 호스트에서 실행되는 것으로 확인될 가능성이 높은 운영 체제

운영 체제가 `Pending`이면 시스템에서 아직 운영 체제를 식별하지 못한 것이며, 사용 가능한 다른 ID 데이터가 없는 것입니다. 운영 체제가 `unknown`이면 시스템에서 운영 체제를 식별할 수 없는 것이며, 운영 체제에 대해 사용 가능한 다른 ID 데이터가 없는 것입니다.

호스트의 운영 체제가 시스템이 탐지할 수 없는 운영 체제인 경우 다음 전략 중 하나를 사용할 수 있습니다.

- 46-7페이지의 사용자 지정 핑거프린트 사용에서 설명한 대로 호스트에 대한 사용자 지정 핑거프린트 생성
- 49-35페이지의 호스트 프로필에서 호스트 스캐닝에서 설명한 대로 호스트에 대해 Nmap 스캔 실행
- *FireSIGHT 시스템 Host Input API Guide*에서 설명한 대로 호스트 입력 기능을 사용하여 네트워크 맵으로 데이터 가져오기
- 49-10페이지의 호스트 프로필에서 운영 체제 작업에서 설명한 대로 수동으로 운영 체제 정보 입력

OS Version/Version

운영 체제 버전. 호스트가 탈옥 모바일 디바이스인 경우, 버전 뒤에 괄호로 `Jailbroken`이 표시됩니다.

Source

다음 값 중 하나:

- 사용자: *`user_name`*
- 애플리케이션: *`app_name`*
- 스캐너: *`scanner_type`*(시스템 정책을 통해 추가된 Nmap 또는 스캐너)
- FireSIGHT

시스템에서는 운영 체제의 ID를 확인하기 위해 여러 소스의 데이터를 조정할 수 있습니다. 46-5페이지의 현재 ID 이해을/를 참조하십시오.

호스트에 대한 취약성 목록 및 호스트를 대상으로 하는 이벤트에 대한 이벤트 영향 상관관계는 운영 체제에 따라 다르기 때문에 좀 더 구체적인 운영 체제 정보를 수동으로 제공할 수 있습니다. 또한 운영 체제에 수정(예: 서비스 팩 및 업데이트)이 적용되었음을 나타낼 수 있고, 수정에 의해 해결된 취약성을 무효화할 수 있습니다.

예를 들어, 시스템에서 호스트의 운영 체제를 Microsoft Windows 2003으로 식별했지만 실제로 호스트에서는 Microsoft Windows XP Professional 서비스 팩 2가 실행되고 있음을 알고 있는 경우, 운영 체제 ID를 올바르게 설정할 수 있습니다. 운영 체제 ID를 좀 더 구체적으로 설정하면 호스트에 대한 취약성 목록이 세부적으로 조정되므로, 해당 호스트에 대한 영향 상관관계의 집중력과 정확성이 향상됩니다.

시스템이 호스트에 대한 운영 체제 정보를 탐지했는데 그 정보가 활성 소스에 의해 제공된 현재 운영 체제 ID와 충돌하는 경우 ID 충돌이 발생합니다. ID 충돌이 발생하면 시스템에서는 취약성과 영향 상관관계에 두 ID를 모두 사용합니다.

NetFlow 지원 디바이스에서 내보낸 데이터를 기반으로 네트워크 맵에 호스트를 추가하도록 네트워크 검색 정책을 구성할 수는 있지만, 운영 체제 ID를 설정하지 않는 한 이러한 호스트에 대해 사용할 수 있는 운영 체제 데이터가 없습니다. 자세한 내용은 45-17페이지의 NetFlow 및 FireSIGHT 데이터 간 차이점을/를 참조하십시오.

활성화된 네트워크 검색 정책의 규정 준수 화이트리스트를 위반하는 운영 체제가 호스트에서 실행되고 있는 경우 방어 센터에서는 해당 운영 체제 정보를 화이트리스트 위반 아이콘( )으로 표시합니다. 또한 탈옥 모바일 디바이스가 활성 화이트리스트를 위반하면 디바이스에 대한 운영 체제 옆에 아이콘이 나타납니다.

호스트의 운영 체제 ID에 대해 사용자 지정 표시 문자열을 설정할 수 있습니다. 그러면 해당 표시 문자열이 호스트 프로필에 사용됩니다.

참고 호스트에 대한 운영 체제 정보를 변경하면 규정 준수 화이트리스트에 대한 규정 준수 여부도 변경될 수 있습니다.

네트워크 디바이스에 대한 호스트 프로필에서, Operating Systems 섹션에 대한 레이블이 Systems로 변경되며 추가 Hardware 열이 나타납니다. Systems 아래에 하드웨어 플랫폼에 대한 값이 나열되면 해당 시스템은 네트워크 디바이스 뒤에서 탐지된 하나 이상의 모바일 디바이스를 나타냅니다. 모바일 디바이스에는 하드웨어 플랫폼 정보가 있을 수도 있고 없을 수도 있지만, 모바일 디바이스가 아닌 시스템에 대해서는 하드웨어 플랫폼 정보가 탐지되지 않습니다.

운영 체제 ID 보기

라이센스: FireSIGHT

호스트에 대해 추가되거나 검색된 특정 운영 체제 ID를 볼 수 있습니다. 시스템은 호스트에 대한 현재 ID를 확인하기 위해 소스 우선순위를 사용합니다. ID 목록에서 현재 ID는 굵은 글꼴로 강조 표시됩니다.

각 운영 체제 ID에서 호스트 프로필에는 49-10페이지의 호스트 프로필에서 운영 체제 작업에서 설명한 정보가 포함되어 있을 수 있습니다.

View 버튼은 호스트에 대해 여러 운영 체제 ID가 존재하는 경우에만 사용할 수 있습니다.

호스트에 대한 운영 체제 ID 목록을 보려면

액세스: Admin/Any Security Analyst

1단계 호스트 프로필의 **Operating System** 또는 **Operating System Conflicts** 섹션에서 **View**를 클릭합니다.

Operating System Identity Information 팝업 창이 나타납니다.

팁 Operating System Identity Information 팝업 창에서 ID를 제거하고, 해당되는 경우 호스트 프로필에서 운영 체제에 대한 현재 ID를 업데이트하려면 운영 체제 ID 옆에 있는 삭제 아이콘( )을 클릭하십시오. Cisco에서 탐지한 운영 체제 ID는 삭제할 수 없습니다.

운영 체제 수정

라이센스: FireSIGHT

FireSIGHT 시스템 웹 인터페이스를 사용하여 호스트에 대한 현재 운영 체제 ID를 설정할 수 있습니다. 웹 인터페이스를 통해 ID를 설정하면 취약성 평가 및 영향 상관관계에 ID가 사용될 수 있도록 다른 모든 ID 소스가 재정의됩니다. 그러나 사용자가 운영 체제를 수정한 후 시스템에서 호스트에 대해 충돌하는 운영 체제 ID를 탐지하면 운영 체제 충돌이 발생합니다.

이 경우 사용자가 충돌을 해결할 때까지 두 운영 체제 모두 현재 운영 체제로 간주됩니다. 자세한 내용은 49-14페이지의 운영 체제 ID 충돌 해결을/를 참조하십시오.

운영 체제 ID를 변경하려면

액세스: Admin/Any Security Analyst

1단계 호스트 프로필의 **Operating System** 섹션에서 **Edit**를 클릭합니다.

운영 체제 ID를 설정할 수 있는 팝업 창이 나타납니다.

2단계 여러 옵션이 있습니다.

- 호스트 입력을 통해 현재 운영 체제 ID를 확인하려면 **OS Definition** 드롭다운 목록에서 **Current Definition**을 선택하고 6단계로 건너뜁니다.
- **OS Definition** 드롭다운 목록에서 현재 운영 체제 ID에 대한 변형을 선택하고 6단계로 건너뜁니다.
- **OS Definition** 드롭다운 목록에서 **User-Defined**를 선택하고 3단계를 계속 진행합니다.

3단계 선택적으로, **Use Custom Display String**을 선택하고 **Vendor String**, **Product String** 및 **Version String** 필드에 표시할 사용자 지정 문자열을 수정합니다.

4단계 선택적으로, 다른 공급업체의 운영 체제로 변경하려면 **Vendor** 및 **Product** 드롭다운 목록에서 공급업체 및 기타 운영 체제 세부사항을 선택합니다.

5단계 선택적으로, 운영 체제 제품 릴리스 레벨을 구성하려면 **Major**, **Minor**, **Revision**, **Build**, **Patch** 및 **Extension** 드롭다운 목록에서 해당 항목을 선택합니다.

6단계 선택적으로, 운영 체제에 대한 수정이 적용되었음을 나타내려면 **Configure Fixes**를 클릭합니다.

사용 가능한 패키지 수정 목록이 표시됩니다.

7단계 드롭다운 목록에서 해당 수정을 선택하고 **Add**를 클릭합니다.

8단계 선택적으로, **Patch** 및 **Extension** 드롭다운 목록을 사용하여 관련 패치 및 확장을 추가합니다.

9단계 운영 체제 ID 컨피그레이션을 완료하려면 **Finish**를 클릭합니다.

운영 체제 ID 충돌 해결

라이센스: FireSIGHT

현재 ID가 스캐너, 애플리케이션, 사용자 등의 활성 소스에 의해 제공된 경우, 시스템이 탐지한 새 ID가 현재 ID와 충돌하면 운영 체제 ID 충돌이 발생합니다.

충돌을 일으키는 운영 체제 ID 목록이 호스트 프로필에서 굵은 글꼴로 표시됩니다.

시스템 웹 인터페이스를 통해 ID 충돌을 해결하고 호스트에 대한 현재 운영 체제 ID를 설정할 수 있습니다. 웹 인터페이스를 통해 ID를 설정하면 취약성 평가 및 영향 상관관계에 ID가 사용될 수 있도록 다른 모든 ID 소스가 재정의됩니다.

충돌하는 ID 중 하나를 현재 ID로 설정하려면

액세스: Admin/Any Security Analyst

1단계 다음 2가지 옵션을 사용할 수 있습니다.

- 호스트에 대한 운영 체제로 설정할 운영 체제 ID 옆에 있는 **Make Current**를 클릭합니다.
- 현재 ID로 지정하지 *않으려는* ID가 활성 소스에서 온 것이면 원하지 않는 ID를 삭제합니다.

운영 체제 ID 충돌을 해결하려면

액세스: Admin/Any Security Analyst

1단계 호스트 프로필의 **Operating System Conflicts** 섹션에서 **Resolve**를 클릭합니다.

현재 운영 체제 ID를 설정할 수 있는 팝업 창이 나타납니다.

2단계 여러 옵션이 있습니다.

- 호스트 입력을 통해 현재 운영 체제 ID를 확인하려면 **OS Definition** 드롭다운 목록에서 **Current Definition**을 선택하고 6단계로 건너뜁니다.
- **OS Definition** 드롭다운 목록에서 충돌하는 운영 체제 ID 중 하나에 대한 변형을 선택하고 6단계로 건너뜁니다.
- **OS Definition** 드롭다운 목록에서 **User-Defined**를 선택하고 3단계를 계속 진행합니다.

3단계 선택적으로, **Use Custom Display String**을 선택하고 **Vendor String**, **Product String** 및 **Version String** 필드에 표시할 사용자 지정 문자열을 입력합니다.

4단계 선택적으로, 다른 공급업체의 운영 체제로 변경하려면 공급업체 및 기타 운영 체제 세부사항을 선택합니다.

5단계 선택적으로, 운영 체제 제품 릴리스 레벨을 구성하려면 **Major**, **Minor**, **Revision**, **Build, Patch** 및 **Extension** 드롭다운 목록에서 해당 항목을 선택합니다.

6단계 선택적으로, 운영 체제에 대한 수정이 적용되었음을 나타내려면 **Configure Fixes**를 클릭합니다.

7단계 적용한 수정을 수정 목록에 추가합니다.

8단계 운영 체제 ID 컨피그레이션을 완료하고 호스트 프로필로 돌아가려면 **Finish**를 클릭합니다.

호스트 프로필에서 서버 작업

라이센스: FireSIGHT

모니터링되는 네트워크의 호스트에서 실행 중인 서버를 시스템이 탐지하거나, 호스트 입력 기능 또는 스캐너나 기타 활성 소스를 통해 서버가 추가되면 방어 센터는 호스트 프로필의 Servers 섹션에 해당 서버를 나열합니다.

방어 센터는 호스트당 최대 100개의 서버를 나열합니다. 이 제한에 도달하면, 호스트에서 서버를 삭제하거나 서버가 시간 초과될 때까지 소스의 새 서버 정보(능동이든 수동이든)가 폐기됩니다. 자세한 내용은 45-14페이지의 호스트 제한 및 검색 이벤트 로깅을/를 참조하십시오.

Nmap을 사용하여 호스트를 스캔하면, Nmap은 열린 TCP 포트에서 실행되는, 전에 탐지되지 않은 서버의 결과를 Servers 목록에 추가합니다. 호스트에서 Nmap 스캔을 수행하거나 Nmap 결과를 가져오는 경우 호스트 프로필에 Scan Results 섹션이 나타나며, 여기에 Nmap 스캔에 의해 호스트에서 탐지된 서버 정보가 나열됩니다. 자세한 내용은 49-35페이지의 호스트 프로필에서 스캔 결과 작업 및 47-9페이지의 Nmap 스캔 설정을/를 참조하십시오. 또한 네트워크 맵에서 호스트가 삭제되면 호스트에 대한 해당 서버의 Nmap 스캔 결과가 삭제됩니다.

참고 NetFlow 지원 디바이스에서 내보낸 데이터를 기반으로 네트워크 맵에 서버 및 클라이언트를 추가하도록 네트워크 검색 정책을 구성할 수 있지만, 이러한 애플리케이션에 대해 사용할 수 있는 정보는 제한적입니다. 자세한 내용은 45-17페이지의 NetFlow 및 FireSIGHT 데이터 간 차이점을/를 참조하십시오.

호스트 프로필의 서버 작업 프로세스는 프로필에 액세스한 방법에 따라 달라집니다.

- Servers 네트워크 맵을 통해 드릴다운하여 호스트 프로필에 액세스한 경우 굵은 글꼴로 표시된 서버 이름과 함께 해당 서버에 대한 세부사항이 나타납니다. 호스트의 다른 서버에 대한 세부사항을 보려면 해당 서버 이름 옆에 있는 보기 아이콘( )을 클릭합니다.
- 다른 방법으로 호스트 프로필에 액세스한 경우 Servers 섹션을 확장하고 세부사항을 보려는 서버 옆에 있는 보기 아이콘( )을 클릭합니다.

다음과 같은 동작을 수행할 수도 있습니다.

- 호스트의 특정 서버와 관련된 연결 이벤트를 분석하려면 서버 옆에 있는 이벤트 아이콘을 클릭합니다.

  연결 이벤트에 대한 기본 설정 워크플로의 첫 번째 페이지가 나타나서, 서버의 포트와 프로토콜에 의해 제한되는 연결 이벤트 및 호스트의 IP 주소를 보여줍니다. 연결 이벤트에 대한 기본 설정 워크플로가 없는 경우 선택해야 합니다. 연결 데이터에 대한 자세한 내용은 39-1페이지의 연결 및 보안 인텔리전스 데이터 작업을/를 참조하십시오.
- 호스트 프로필에서 서버를 삭제하려면 서버 옆에 있는 삭제 아이콘( )을 클릭합니다.

  서버가 호스트 프로필에서 삭제되지만, 시스템이 해당 서버에서 트래픽을 다시 탐지하면 서버가 다시 나타납니다. 호스트에서 서버를 삭제하면 해당 호스트는 화이트리스트의 규정 준수 상태로 전환될 수 있습니다.
- 서버 ID 충돌을 해결하려면 서버 옆에 있는 해결 아이콘을 클릭합니다.

  충돌하는 ID 중 하나를 선택하거나, 그러한 ID 중 하나의 변형을 선택하거나, 새로운 사용자 정의 ID를 설정할 수 있습니다.
- 서버 ID를 수정하려면 서버 옆에 있는 수정 아이콘( )을 클릭합니다.

  현재 ID를 선택하거나, 해당 ID의 변형을 선택하거나, 새로운 사용자 정의 ID를 설정할 수 있습니다.

다음은 Servers 목록의 열에 대한 설명입니다.

Protocol

서버가 사용하는 프로토콜의 이름

Port

서버가 실행 중인 포트

Application Protocol

다음 중 하나:

- 애플리케이션 프로토콜의 이름
- `pending` - 여러 이유 중 하나 때문에 시스템이 애플리케이션 프로토콜을 긍정적으로 또는 부정적으로 식별할 수 없는 경우
- `unknown` - 알려진 애플리케이션 프로토콜 핑거프린트를 기반으로 시스템이 애플리케이션 프로토콜을 식별할 수 없는 경우, 또는 해당 서버는 추가하지 않은 채 포트 정보의 취약성을 추가함으로써 호스트 입력을 통해 서버를 추가한 경우

마우스를 애플리케이션 프로토콜 이름 위로 이동하면 태그가 표시됩니다. 태그에 대한 자세한 내용은 45-10페이지의 애플리케이션 탐지 이해을/를 참조하십시오.

Vendor and Version

FireSIGHT 시스템, Nmap 또는 다른 활성 소스에 의해 식별되었거나 호스트 입력 기능을 통해 수집된 공급업체 및 버전. 사용 가능한 소스 중 ID를 제공한 소스가 없으면 필드는 비어 있게 됩니다.

활성화된 상관관계 정책의 규정 준수 화이트리스트를 위반하는 서버가 호스트에서 실행되고 있는 경우 방어 센터에서는 규정을 준수하지 않는 서버를 화이트리스트 위반 아이콘()으로 표시합니다.

자세한 내용은 다음 절을 참조하십시오.

- 49-16페이지의 서버 세부사항
- 49-18페이지의 서버 ID 수정
- 49-19페이지의 서버 ID 충돌 해결

서버 세부사항

라이센스: FireSIGHT

방어 센터는 서버당 최대 16개의 수동 탐지(Cisco 또는 NetFlow 탐지) ID를 나열합니다. 시스템이 서버에 대해 여러 공급업체 또는 버전을 탐지하는 경우 해당 서버는 여러 수동 ID를 가질 수 있습니다. 예를 들어 웹 서버가 서버 소프트웨어와 동일한 버전을 실행하지 않는 경우, 관리되는 디바이스와 웹 서버 팜 간 로드 밸런서를 사용하면 시스템은 HTTP에 대해 여러 수동 ID를 식별하게 될 수 있습니다. 방어 센터는 사용자 입력, 소스 또는 기타 애플리케이션 등 활성 소스에서 오는 서버 ID의 수를 제한하지 않습니다.

현재 ID는 방어 센터에서 굵은 글꼴로 표시됩니다. 시스템은 호스트에 취약성을 할당하고, 영향 평가를 수행하고, 호스트 프로필 자격 및 규정 준수 화이트리스트에 대해 작성된 상관관계 규칙을 평가하는 등 여러 용도에 서버의 현재 ID를 사용합니다.

팁 서버 ID를 변경하고 서버 세부사항에서 ID 충돌을 해결하는 방법에 대한 자세한 내용은 49-18페이지의 서버 ID 수정 및 49-19페이지의 서버 ID 충돌 해결을/를 참조하십시오.

서버 세부사항에는 선택한 서버에 대해 알려진 업데이트된 하위 서버 정보도 표시될 수 있습니다. 마지막으로, 서버 세부사항에는 서버 배너가 표시될 수 있습니다. 이 배너는 호스트 프로필에서 서버를 볼 때 서버 세부사항 아래에 표시됩니다.

서버 배너는 서버 식별에 도움이 될 수 있는, 서버에 대한 추가 정보를 제공합니다. 공격자가 고의로 서버 배너 문자열을 변경하면 시스템이 서버를 식별하지 못하거나 잘못된 서버를 탐지할 수 있습니다. 서버 배너에는 서버에 대해 탐지된 첫 번째 패킷의 처음 256바이트가 표시됩니다. 이러한 정보는 시스템에서 서버를 처음 탐지할 때 한 번만 수집됩니다. 배너 내용은 왼쪽에는 16진수로, 오른쪽에는 ASCII로 표시되어 두 열에 나타납니다.

참고 서버 배너를 보려면 네트워크 검색 정책에서 **Capture Banners** 확인란을 활성화해야 합니다. 이 옵션은 기본적으로 비활성화되어 있습니다.

다음은 서버 세부사항에서 제공하는 정보에 대한 설명입니다.

Protocol

서버가 사용하는 프로토콜의 이름

Port

서버가 실행 중인 포트

Hits

Cisco 관리되는 디바이스 또는 Nmap에 의해 서버가 탐지된 횟수. 호스트 입력을 통해 가져온 서버에 대한 트래픽을 시스템에서 탐지하지 못하면 해당 서버의 히트 수는 0입니다.

Last Used

서버가 마지막으로 탐지된 시간 및 날짜. 시스템이 서버에 대해 새 트래픽을 탐지하지 못하면 호스트 입력 데이터의 마지막 사용 시간은 초기 데이터 가져오기 시간을 반영합니다. 호스트 입력 기능을 통해 가져온 스캐너 및 애플리케이션 데이터는 시스템 정책의 설정에 따라 시간 초과되지만, 방어 센터 웹 인터페이스를 통한 사용자 입력은 시간 초과되지 않습니다.

Application Protocol

알려진 경우, 서버에서 사용하는 애플리케이션 프로토콜의 이름

Vendor

서버 공급업체. 공급업체가 알려지지 않은 경우 이 필드는 나타나지 않습니다.

Version

서버 버전. 버전이 알려지지 않은 경우 이 필드는 나타나지 않습니다.

Source

다음 값 중 하나:

- 사용자: *user_name*
- 애플리케이션: *app_name*
- 스캐너: *scanner_type*(시스템 정책을 통해 추가된 Nmap 또는 스캐너)
- `FireSIGHT`, `FireSIGHT Port Match` 또는 `FireSIGHT Pattern Match` - Cisco 탐지 애플리케이션의 경우
- `NetFlow` - NetFlow 데이터 기반의 네트워크 맵에 추가된 서버의 경우

시스템에서는 서버의 ID를 확인하기 위해 여러 소스의 데이터를 조정할 수 있습니다. 46-5페이지의 현재 ID 이해을/를 참조하십시오.

서버에 대한 서버 세부사항을 보려면

액세스: Admin/Any Security Analyst

1단계 호스트 프로필의 **Servers** 섹션 옆에 있는 보기 아이콘()을 클릭합니다.

Server Detail 팝업 창이 나타납니다.

서버 ID 수정

라이센스: FireSIGHT

호스트의 서버에 대한 ID 설정을 수동으로 업데이트하고, 수정으로 해결된 취약성을 제거하도록 호스트에 적용한 수정을 구성할 수 있습니다. 서버 ID를 삭제할 수도 있습니다.

ID를 삭제해도(유일한 ID인 경우에도) 서버는 삭제되지 않습니다. ID를 삭제하면 Server Detail 팝업 창에서 ID가 제거되며, 해당되는 경우 호스트 프로필에서 서버에 대한 현재 ID가 업데이트됩니다.

Cisco 관리되는 디바이스에 의해 추가된 서버 ID는 수정 또는 삭제할 수 없습니다.

서버 ID를 수정하려면

액세스: Admin/Any Security Analyst

1단계 호스트 프로필의 **Servers** 섹션에서 **View**를 클릭하여 Server Detail 팝업 창을 엽니다.

2단계 다음 2가지 옵션을 사용할 수 있습니다.

- 서버 ID를 삭제하려면 제거할 서버 ID 옆에 있는 삭제 아이콘()을 클릭합니다.
- 서버 ID를 수정하려면 서버 목록에서 서버 옆에 있는 수정 아이콘()을 클릭합니다.

  Server Identity 팝업 창이 나타납니다.

3단계 다음 2가지 옵션을 사용할 수 있습니다.

- **Select Server Type** 드롭다운 목록에서 현재 정의를 선택합니다.
- **Select Server Type** 드롭다운 목록에서 서버 유형을 선택합니다.

4단계 선택적으로, 해당 서버 유형에 대한 공급업체와 제품만 나열하려면 **Restrict by Server Type** 확인란을 선택합니다.

5단계 선택적으로, 서버의 이름과 버전을 사용자 지정하려면 **Use Custom Display String**을 선택하고 **Vendor String** 및 **Version String**을 입력합니다.

6단계 **Product Mappings** 섹션에서 사용할 운영 체제, 제품 및 버전을 선택합니다.

예를 들어 서버를 Red Hat Linux 9에 매핑하려면 공급업체로 **Redhat, Inc.**, 제품으로 **Redhat Linux**, 버전으로 **9**를 선택합니다.

7단계 서버에 대한 수정이 적용되었음을 나타내려면 **Configure Fixes**를 클릭합니다. 그렇지 않을 경우 9단계로 건너뜁니다.

Available Package Fixes 페이지가 나타납니다.

8단계 해당 서버에 대해 적용할 패치를 수정 목록에 추가합니다.

9단계 서버 ID 컨피그레이션을 완료하려면 **Finish**를 클릭합니다.

서버 ID 충돌 해결

라이센스: FireSIGHT

애플리케이션이나 스캐너 같은 활성 소스가 서버에 대한 ID 데이터를 호스트에 추가할 때 시스템이 해당 포트에 대해 서버 ID가 충돌함을 나타내는 트래픽을 탐지하면 서버 ID 충돌이 발생합니다.

서버 ID 충돌을 해결하려면

액세스: Admin/Any Security Analyst

1단계 **Servers** 목록에서 서버 옆에 있는 해결 아이콘을 클릭합니다.

Server Identity 팝업 창이 나타납니다.

2단계 **Select Server Type** 드롭다운 목록에서 서버 유형을 선택합니다.

3단계 선택적으로, 해당 서버 유형에 대한 공급업체와 제품만 나열하려면 **Restrict by Server Type** 확인란을 선택합니다.

4단계 선택적으로, 서버의 이름과 버전을 사용자 지정하려면 **Use Custom Display String**을 선택하고 **Vendor String** 및 **Version String**을 입력합니다.

5단계 **Product Mappings** 섹션에서 사용할 운영 체제, 제품 및 버전을 선택합니다.

예를 들어 서버를 Red Hat Linux 9에 매핑하려면 공급업체로 **Redhat, Inc.**, 제품으로 **Redhat Linux**, 버전으로 **9**를 선택합니다.

6단계 서버에 대한 수정이 적용되었음을 나타내려면 **Configure Fixes**를 클릭합니다. 그렇지 않을 경우 9단계로 건너뜁니다.

Available Package Fixes 페이지가 나타납니다.

7단계 해당 서버에 대해 적용할 패치를 수정 목록에 추가합니다.

8단계 서버 ID 컨피그레이션을 완료하고 호스트 프로필로 돌아가려면 **Finish**를 클릭합니다.

호스트 프로필에서 애플리케이션 작업

라이센스: FireSIGHT

호스트에서 실행 중인 애플리케이션을 호스트 프로필에서 볼 수 있습니다. 호스트 프로필에서 애플리케이션을 제거하려면 해당 애플리케이션을 삭제할 수 있습니다.

호스트 프로필에서 애플리케이션을 관리하는 방법에 대한 자세한 내용은 다음을 참조하십시오.

- 49-20페이지의 호스트 프로필에서 애플리케이션 보기
- 49-21페이지의 호스트 프로필에서 애플리케이션 삭제

호스트 프로필에서 애플리케이션 보기

라이센스: FireSIGHT

시스템은 네트워크의 호스트에서 실행 중인 다양한 클라이언트 및 웹 애플리케이션을 탐지할 수 있습니다.

참고 시스템이 모니터링되는 네트워크의 호스트에서 애플리케이션을 탐지하도록 하려면 네트워크 검색 정책에 있는 NetFlow 디바이스에 대한 검색 규칙에서 **Applications** 확인란을 선택해야 합니다. 이 옵션은 NetFlow 규칙에서 기본적으로 활성화되며, 관리되는 디바이스를 통한 검색에 사용되는 규칙에 대해 비활성화할 수 없습니다.

호스트 프로필은 호스트에서 탐지되는 애플리케이션의 제품 및 버전, 사용 가능한 클라이언트 또는 웹 애플리케이션 정보, 그리고 애플리케이션 사용이 마지막으로 탐지된 시간을 표시합니다.

방어 센터는 호스트에서 실행 중인 클라이언트를 최대 16개 나열합니다. 이 한계에 도달하면, 호스트에서 클라이언트 애플리케이션을 삭제하거나 비활성화 때문에(클라이언트 시간 초과) 시스템이 호스트 프로필에서 클라이언트를 삭제할 때까지, 소스의 새 클라이언트 정보(능동이든 수동이든)가 삭제됩니다.

또한 탐지된 각 웹 브라우저에 대해 호스트 프로필은 액세스된 처음 100개의 웹 애플리케이션을 표시합니다. 이 한계에 도달하면 다음과 같이 될 때까지 소스의 해당 브라우저와 관련된 새 웹 애플리케이션(능동이든 수동이든)이 삭제됩니다.

- 웹 브라우저 클라이언트 애플리케이션이 시간 초과됨, 또는
- 호스트 프로필에서 웹 애플리케이션과 관련된 애플리케이션 정보 삭제

다음은 호스트 프로필에 나타나는 애플리케이션 정보에 대한 설명입니다.

Application Protocol

애플리케이션(HTTP 브라우저, DNS 클라이언트 등)이 사용하는 애플리케이션 프로토콜을 표시합니다.

Client

FireSIGHT 시스템에 의해 식별되거나 Nmap 또는 다른 활성 소스에 의해 캡처되거나 호스트 입력 기능을 통해 수집된 경우, 페이로드에서 파생된 클라이언트 정보. 사용 가능한 소스 중 ID를 제공한 소스가 없으면 필드는 비어 있게 됩니다.

Version

클라이언트의 버전을 표시합니다.

Web Application

웹 브라우저의 경우 시스템이 http 트래픽에서 탐지한 콘텐츠. 웹 애플리케이션 정보는 FireSIGHT 시스템에 의해 식별되고, Nmap 또는 다른 활성 소스에 의해 캡처되고, 호스트 입력 기능을 통해 수집된 특정 콘텐츠 유형(예: WMV 또는 QuickTime)을 나타냅니다. 사용 가능한 소스 중 ID를 제공한 소스가 없으면 필드는 비어 있게 됩니다.

활성화된 상관관계 정책의 규정 준수 화이트리스트를 위반하는 애플리케이션이 호스트에서 실행되고 있는 경우 방어 센터에서는 규정을 준수하지 않는 애플리케이션을 화이트리스트 위반 아이콘()으로 표시합니다.

호스트의 특정 애플리케이션과 관련된 연결 이벤트를 분석하려면 애플리케이션 옆에 있는 이벤트 아이콘( )을 클릭합니다. 연결 이벤트에 대한 기본 설정 워크플로의 첫 번째 페이지가 나타나서 애플리케이션의 유형, 제품 및 버전에 의해 제한되는 연결 이벤트 및 호스트의 IP 주소를 보여줍니다. 연결 이벤트에 대한 기본 설정 워크플로가 없는 경우 선택해야 합니다. 연결 데이터에 대한 자세한 내용은 39-1페이지의 연결 및 보안 인텔리전스 데이터 작업을/를 참조하십시오.

호스트 프로필에서 애플리케이션 삭제

라이센스: FireSIGHT

호스트에서 실행되고 있지 않음을 알고 있는 애플리케이션을 제거하려면 호스트 프로필에서 해당 애플리케이션을 삭제할 수 있습니다. 호스트에서 애플리케이션을 삭제하면 해당 호스트는 화이트리스트의 규정 준수 상태로 전환될 수 있습니다.

참고 해당 애플리케이션이 다시 탐지되면 네트워크 맵 및 호스트 프로필에 다시 추가됩니다.

호스트 프로필에서 애플리케이션을 삭제하려면

액세스: Admin/Any Security Analyst

1단계 호스트 프로필의 **Applications** 섹션에서 삭제할 애플리케이션 옆에 있는 삭제 아이콘( )을 클릭합니다.

해당 호스트에 대한 애플리케이션이 삭제됩니다.

호스트 프로필에서 **VLAN** 태그 작업

라이센스: FireSIGHT

호스트가 VLAN(Virtual LAN)의 멤버인 경우 호스트 프로필의 VLAN Tag 섹션이 나타납니다.

물리적 네트워크 장비는 종종 VLAN을 사용하여 서로 다른 네트워크 블록에서 논리적 네트워크 세그먼트를 생성합니다. 시스템은 802.1q VLAN 태그를 탐지하고 각각에 대해 다음과 같은 정보를 표시합니다.

- **VLAN ID** - 호스트가 멤버로 있는 VLAN을 식별합니다. 802.1q VLAN의 경우 0~4095 사이의 정수일 수 있습니다.
- **Type** - VLAN 태그를 포함하는 캡슐화된 패킷을 식별하며, 이더넷 또는 토큰 링일 수 있습니다.
- **Priority** - VLAN 태그의 우선순위를 식별하며, 범위는 0~7의 정수이고 7이 가장 높은 우선순위입니다.

VLAN 태그가 패킷 내에 중첩된 경우 시스템은 가장 안쪽의 VLAN 태그를 처리하고 방어 센터는 이를 표시합니다. ARP 및 DHCP 트래픽을 통해 식별하는 MAC 주소에 대해서만 시스템은 VLAN 태그 정보를 수집하고 방어 센터는 이를 표시합니다.

예를 들면 VLAN이 프린터로만 구성되어 있고 시스템이 해당 VLAN에서 Microsoft Windows 2000 운영 체제를 탐지하는 경우에는 VLAN 태그 정보가 유용할 수 있습니다. VLAN 정보는 또한 시스템이 좀 더 정확한 네트워크 맵을 생성하는 데에도 도움이 됩니다.

호스트 프로필에서 사용자 기록 작업

라이센스: FireSIGHT

호스트 프로필의 사용자 기록 부분은 사용자 활동의 마지막 24시간을 그래프로 보여줍니다. 일반적인 사용자는 저녁에 로그오프하고 호스트 리소스를 다른 사용자와 공유할 것입니다. 정기적인 로그인 요청(예: 이메일 확인을 위해)은 짧은 일반 막대로 표시할 수 있습니다. 사용자 ID의 목록은 사용자 로그인이 탐지된 시점을 나타내기 위해 막대 그래프로 제공됩니다. 권한 없는 로그인의 경우에는 막대 그래프가 회색입니다.

시스템은 권한 없는 사용자의 호스트 로그인을 해당 호스트의 IP 주소와 연결하여, 사용자가 호스트의 사용자 기록에 나타나도록 합니다. 그러나 동일한 호스트에서 권한 있는 사용자 로그인이 탐지되면 권한 있는 사용자 로그인과 연결된 사용자가 호스트 IP 주소의 연결 관계를 인수하며, 권한 없는 새 사용자 로그인은 호스트 IP 주소와 사용자의 연결 관계를 중단하지 않습니다. 사용자 유형에 대한 자세한 내용은 45-7페이지의 사용자 데이터베이스을/를 참조하십시오. 네트워크 검색 정책에서 실패한 로그인의 캡처를 구성하는 경우 목록에는 호스트 로그인에 실패한 사용자가 포함됩니다.

호스트 프로필에서 호스트 특성 작업

라이센스: FireSIGHT

네트워크 환경에서 중요한 방법으로 호스트를 분류하려면 *호스트 특성*을 사용할 수 있습니다. 호스트 특성 값은 양의 정수, 문자열 또는 URL일 수 있습니다. 사용자는 문자열 값의 목록을 생성하고 호스트 IP 주소를 기반으로 자동으로 할당할 수 있습니다. 사용자 정의 호스트 특성의 생성 및 관리에 대한 자세한 내용은 49-31페이지의 사용자 정의 호스트 특성 작업을/를 참조하십시오.

FireSIGHT 시스템에는 두 개의 사전 정의 호스트 특성(Host Criticality 및 Notes)이 포함되어 있습니다. 이러한 사전 정의 호스트 특성 작업에 대한 자세한 내용은 49-30페이지의 사전 정의 호스트 특성 작업을/를 참조하십시오.

또한 자동으로 생성되는 각 규정 준수 화이트리스트는 화이트리스트와 동일한 이름으로 호스트 특성을 생성합니다. 가능한 값은 Compliant(화이트리스트를 준수하는 호스트), Non-Compliant(화이트리스트를 위반하는 호스트) 또는 Not Evaluated(화이트리스트의 유효한 대상이 아니거나 어떤 이유로든 평가되지 않은 호스트)입니다. 화이트리스트 호스트 특성의 값은 수동으로 변경할 수 **없습니다**. 화이트리스트에 대한 자세한 내용은 52-1페이지의 규정준수 툴로 FireSIGHT 시스템 사용을/를 참조하십시오.

호스트 특성 값 할당

라이센스: FireSIGHT

기존 호스트 특성의 값으로 양의 정수, 문자열 또는 URL을 지정할 수 있습니다.

팁 호스트에 호스트 특성을 신속하게 할당하려면 호스트 프로필 페이지의 **Attributes** 섹션에서 **Edit** 링크를 클릭할 수 있습니다. 그러면 모든 호스트 특성에 대한 필드가 포함된 팝업 창이 나타납니다.

호스트 특성 값을 할당하려면

액세스: Admin/Any Security Analyst

1단계 호스트 프로필을 엽니다.

2단계 값을 할당하려는 호스트 특성의 이름을 **Attributes** 아래에서 클릭합니다.

팝업 창이 나타납니다.

3단계 특성에 대한 값을 입력하거나 드롭다운 목록에서 값을 선택합니다.

4단계 **Save**를 클릭합니다.

호스트 특성 값이 저장됩니다.

호스트 프로필에서 호스트 프로토콜 작업

라이센스: FireSIGHT

호스트에서 실행 중인 프로토콜을 호스트 프로필을 통해 볼 수 있습니다. 필요한 경우 프로필에서 특정 호스트에 대한 호스트 프로토콜을 삭제할 수도 있습니다.

각 호스트 프로필에는 호스트와 연결된 네트워크 트래픽에서 탐지된 프로토콜에 대한 정보가 포함되어 있습니다.

다음은 프로토콜 및 네트워크 레이어 정보에 대한 설명입니다.

Protocol

호스트에서 사용하는 프로토콜의 이름입니다.

Layer

프로토콜이 실행되는 네트워크의 레이어입니다(`Network` 또는 `Transport`).

활성화된 상관관계 정책의 규정 준수 화이트리스트를 위반하는 프로토콜이 호스트에서 실행되고 있는 경우 방어 센터에서는 규정을 준수하지 않는 프로토콜을 화이트리스트 위반 아이콘(방어 센터)으로 표시합니다.방어 센터

호스트에서 실행되고 있지 않음을 알고 있는 프로토콜을 제거하려면 호스트 프로필에서 해당 프로토콜을 삭제할 수 있습니다. 호스트에서 프로토콜을 삭제하면 해당 호스트는 규정 준수 화이트리스트를 다시 준수하게 될 수 있습니다.

참고 시스템은 해당 프로토콜을 다시 탐지하면 네트워크 맵 및 호스트 프로필에 다시 추가합니다.

호스트 프로필에서 프로토콜을 삭제하려면

액세스: Admin/Any Security Analyst

1단계 호스트 프로필의 **Protocols** 섹션에서 삭제할 프로토콜 옆에 있는 삭제 아이콘( )을 클릭합니다.

해당 호스트에 대한 프로토콜이 삭제됩니다.

호스트 프로필에서 화이트리스트 위반 작업

라이센스: FireSIGHT

규정 준수 화이트리스트(또는 *화이트리스트*)는 특정 서브넷에서 실행 가능한 운영 체제, 애플리케이션 프로토콜, 클라이언트, 웹 애플리케이션 및 프로토콜을 지정할 수 있는 기준 집합입니다.

활성 상관관계 정책에 화이트리스트를 추가한 경우 시스템이 호스트에서 화이트리스트 위반을 탐지하면, 방어 센터는 화이트리스트 이벤트(특정 상관관계 이벤트 유형)를 데이터베이스에 로깅합니다. 이러한 각 화이트리스트 이벤트는 특정 호스트가 어떻게, 왜 화이트리스트를 위반했는지를 나타내는 *화이트리스트 위반*과 연결됩니다. 호스트가 하나 이상의 화이트리스트를 위반하면 호스트 프로필에서 두 가지 방법으로 이러한 위반을 볼 수 있습니다.

첫째, 호스트 프로필은 호스트와 관련된 모든 개별 화이트리스트 위반을 나열합니다.

다음은 호스트 프로필에 표시되는 화이트리스트 위반 정보에 대한 설명입니다.

Type

위반의 유형, 즉 위반이 발생한 원인(규정을 준수하지 않는 운영 체제, 애플리케이션, 서버 또는 프로토콜)

Reason

위반의 특정 이유. 예를 들어 Microsoft Windows 호스트만 허용하는 화이트리스트가 있는 경우, 호스트 프로필에는 호스트에서 실행 중인 현재 운영 체제(예: `Linux 2.4, 2.6`)가 표시됩니다.

White List

위반과 연결된 화이트리스트의 이름

둘째, 운영 체제, 애플리케이션, 프로토콜 및 서버와 관련된 섹션에서 방어 센터는 규정을 준수하지 않는 요소를 화이트리스트 위반 아이콘( )으로 표시합니다. 예를 들어 Microsoft Windows 호스트만 허용하는 화이트리스트의 경우, 호스트 프로필은 해당 호스트의 운영 체제 정보 옆에 화이트리스트 위반 아이콘을 표시합니다.

규정 준수 화이트리스트에 대한 공유 호스트 프로필을 생성하려면 호스트의 프로필을 사용할 수 있습니다. 자세한 내용은 다음 절, 호스트 프로필에서 화이트리스트 호스트 프로필 생성을/를 참조하십시오.

호스트 프로필에서 화이트리스트 호스트 프로필 생성

라이센스: FireSIGHT

규정 준수 화이트리스트용 공유 호스트 프로필은 여러 화이트리스트 전체에 대해 대상 호스트에서 실행 가능한 운영 체제, 애플리케이션 프로토콜, 클라이언트, 웹 애플리케이션 및 프로토콜을 지정합니다. 즉, 여러 개의 화이트리스트를 생성하지만 동일한 호스트 프로필을 사용하여 화이트리스트 전반에 걸쳐 특정 운영 체제를 실행하는 호스트를 평가하려는 경우, 공유 호스트 프로필을 사용합니다.

규정 준수 화이트리스트가 사용할 수 있는 공유 호스트 프로필을 생성하려면 알려진 IP 주소가 있는 호스트의 호스트 프로필을 사용할 수 있습니다. 그러나 시스템이 호스트의 운영 체제를 아직 식별하지 못한 경우에는 개별 호스트의 호스트 프로필을 기반으로 공유 호스트 프로필을 생성할 수 없습니다.

호스트 프로필을 기반으로 규정 준수 화이트리스트에 대한 공유 호스트 프로필을 생성하려면

액세스: Admin

1단계 네트워크 맵 또는 이벤트 보기에서 호스트 프로필에 액세스합니다.

자세한 내용은 49-5페이지의 호스트 프로필 보기을/를 참조하십시오.

2단계 **Generate White List Profile**을 클릭합니다.

Edit Shared Profiles 페이지가 나타납니다. 액세스한 호스트 프로필의 정보를 기반으로 페이지의 필드가 미리 채워집니다.

3단계 특정 요구에 맞게 공유 호스트 프로필을 수정 및 저장합니다.

규정준수 화이트리스트용 공유 호스트 프로필 생성에 대한 자세한 내용은 52-25페이지의 공유 호스트 프로필 작업을/를 참조하십시오.

호스트 프로필에서 악성코드 탐지 작업

라이센스: FireSIGHT 및 악성코드

Most Recent Malware Detections 섹션에는 호스트가 악성코드 파일을 주고받은 가장 최근의 악성코드 이벤트가 최대 100개까지 나열됩니다. 호스트 프로필은 네트워크 기반 및 엔드포인트 기반 악성코드 이벤트를 모두 나열합니다.

파일이 악성코드로 소급 식별된 파일 이벤트에 호스트가 관련된 경우, 악성코드 식별이 발생한 후 파일이 전송된 원래 이벤트가 악성코드 탐지 목록에 나타납니다. 악성코드로 식별된 파일이 악성코드가 아닌 것으로 소급 결정되면 해당 파일과 연결된 악성코드 이벤트가 더 이상 목록에 나타나지 않습니다. 예를 들어 파일에 `Malware` 성향이 있는데 해당 성향이 `Clean`으로 변경되면, 해당 파일의 이벤트는 호스트 프로필의 악성코드 탐지 목록에서 제거됩니다. 악성코드 이벤트에 대한 자세한 내용은 40-17페이지의 악성코드 이벤트 작업을/를 참조하십시오.

다음은 호스트 프로필의 Most Recent Malware Detections 섹션에 있는 열에 대한 설명입니다.

Time

이벤트가 생성된 날짜 및 시간

파일이 악성코드로 소급 식별된 이벤트의 경우, 악성코드가 식별된 시간이 아니라 원래 이벤트의 시간을 나타냅니다.

Host Role

탐지된 악성코드 전송에서 호스트의 역할(sender 또는 receiver). 엔드포인트 기반 악성코드 이벤트의 경우 호스트는 항상 receiver입니다.

Threat Name

탐지된 악성코드의 이름

File Name

악성코드 파일의 이름

File Type

`PDF` 또는 `MSEXE` 등의 파일 형식

호스트 프로필에서 악성코드 탐지를 볼 때 이벤트 뷰어에서는 해당 호스트의 악성코드 이벤트를 볼 수 있습니다. 이벤트를 보려면 악성코드 아이콘( )을 클릭합니다.

호스트 프로필에서 취약성 작업

라이센스: FireSIGHT

호스트 프로필의 Vulnerabilities 섹션에는 해당 호스트에 영향을 미치는 취약성이 나열됩니다.

Sourcefire Vulnerabilities 섹션에는 시스템이 호스트에서 탐지한 운영 체제, 서버 및 애플리케이션 기반의 취약성이 나열됩니다.

호스트의 운영 체제 또는 호스트의 애플리케이션 프로토콜에서 ID 충돌이 발생하면 시스템은 충돌이 해결될 때까지 두 ID에 대한 취약성을 나열합니다.

NetFlow 데이터를 기반으로 네트워크 맵에 추가된 호스트에 대해 사용할 수 있는 운영 체제 정보가 없으므로, 호스트 입력 기능을 사용하여 호스트 운영 체제 ID를 수동으로 설정하지 않는 한 방어 센터에서는 그러한 호스트에 어떤 취약성이 영향을 미칠지를 파악할 수 없습니다.

서버 공급업체 및 버전 정보는 종종 트래픽에 포함되지 않습니다. 기본적으로 시스템은 트래픽을 보내고 받는 호스트에 대해 관련 취약성을 매핑하지 않습니다. 그러나 시스템 정책을 사용하면 공급업체 또는 버전 정보가 없는 특정 애플리케이션 프로토콜에 대한 취약성을 매핑하도록 시스템을 구성할 수 있습니다. 자세한 내용은 63-30페이지의 서버에 대한 취약성 매핑을/를 참조하십시오.

호스트 입력 기능을 사용하여 네트워크의 호스트에 대한 서드파티 취약성 정보를 추가하는 경우 추가적인 Vulnerabilities 섹션이 나타납니다. 예를 들어 QualysGuard Scanner에서 취약성을 가져오면 호스트 프로필에 QualysGuard Vulnerabilities 섹션이 포함됩니다.

서드파티 취약성을 운영 체제 및 애플리케이션 프로토콜과 연결할 수 있지만 클라이언트와는 연결할 수 없습니다. 서드파티 취약성 가져오기에 대한 자세한 내용은 *FireSIGHT 시스템 Host Input API Guide*를 참조하십시오.

다음은 호스트 프로필의 Vulnerabilities 섹션에 있는 열에 대한 설명입니다.

Name

취약성의 이름

Remote

취약성이 원격으로 악용될 수 있는지를 나타냅니다. 이 열이 비어 있으면 취약성 정의에 이 정보가 포함되지 않은 것입니다.

Component

취약성과 관련된 운영 체제, 애플리케이션 프로토콜 또는 클라이언트의 이름

Port

취약성이 지정된 포트에서 실행 중인 애플리케이션 프로토콜과 연결된 경우 포트 번호

서드파티 취약성의 경우 호스트 프로필의 해당 Vulnerabilities 섹션에 표시되는 정보는 호스트 입력 기능을 사용하여 취약성 데이터를 가져올 때 제공한 정보로 제한됩니다.

호스트 프로필에서 취약성을 볼 때 수행할 수 있는 일은 다음과 같습니다.

- 열 머리글을 클릭하여 **Vulnerabilities** 섹션의 열을 정렬합니다. 정렬 순서를 반대로 하려면 다시 클릭합니다.

- 취약성의 이름을 클릭하여 취약성에 대한 기술적 세부사항을 봅니다(알려진 해결책 포함). 자세한 내용은 49-27페이지의 취약성 세부사항 보기을/를 참조하십시오. 취약성 이벤트 보기 또는 Vulnerabilities 네트워크 맵에서도 취약성 세부사항에 액세스할 수 있습니다.
- 영향 상관관계 평가에 취약성이 사용되는 것을 방지합니다. 자세한 내용은 49-28페이지의 취약성 영향 자격 설정을/를 참조하십시오.
- 네트워크의 호스트에서 검색된 취약성을 완화하기 위한 패치를 다운로드합니다. 자세한 내용은 49-29페이지의 취약성용 패치 다운로드을/를 참조하십시오.
- 호스트가 패치되었음을 알고 있는 경우 개별 취약성에 대해 호스트가 취약하지 않은 것으로 표시합니다. 자세한 내용은 49-30페이지의 개별 호스트에 대해 취약성 설정을/를 참조하십시오.

취약성 세부사항 보기

라이센스: FireSIGHT

취약성 세부사항에는 취약성 및 알려진 해결책에 대한 기술적 설명이 포함됩니다.

특정 취약성의 취약성 세부사항에 액세스하려면 **Analysis > Vulnerabilities** 또는 **Analysis > Third-Party Vulnerabilities**를 선택하고 SVID 옆에 있는 보기 아이콘( )을 클릭합니다. 네트워크 맵 및 호스트 프로필에서도 취약성 세부사항에 액세스할 수 있습니다.

다음은 Vulnerability Detail 페이지의 필드에 대한 설명입니다.

Cisco Vulnerability ID

시스템이 취약성 추적에 사용하는 식별 번호(SVID)

Snort ID

SID(Snort ID) 데이터베이스의 취약성과 연결된 식별 번호. 즉, 침입 규칙이 특정 취약성을 악용하는 네트워크 트래픽을 탐지할 수 있으면 해당 취약성은 침입 규칙의 SID와 연결됩니다.

취약성을 둘 이상의 SID와 연결할 수 있습니다(SID와 연결하지 않을 수도 있음). 취약성에 관련 SID가 없으면 이 필드는 나타나지 않습니다.

BugTraq ID

Bugtraq 데이터베이스의 취약성과 연결된 식별 번호(http://www.securityfocus.com/bid)

CVE ID

MITRE CVE(Common Vulnerabilities and Exposures) 데이터베이스(http://www.cve.mitre.org/)의 취약성과 연결된 식별 번호

Title

취약성의 제목

Impact Qualification

드롭다운 목록을 사용하여 취약성을 활성화 또는 비활성화합니다. 방어 센터는 영향 상관관계에서 비활성화된 취약성을 무시합니다.

지정한 설정은 시스템 전체에서 취약성의 취급 방법을 결정하며, 값을 선택한 호스트 프로필로 제한되지 않습니다. 이 기능을 사용하여 취약성을 활성화 및 비활성화하는 방법에 대한 자세한 내용은 49-28페이지의 취약성 영향 자격 설정을/를 참조하십시오.

Date Published

취약성이 게시된 날짜

Vulnerability Impact

Bugtraq 데이터베이스에서 취약성에 할당된 심각도로, 범위는 1~10이며 10이 가장 높은 값입니다. 취약성 영향은 SANS CVA(Critical Vulnerability Analysis) 기준을 참조하여 스스로 내리는 최선의 판단으로 취약성을 결정하는 Bugtraq 항목 작성자에 의해 결정됩니다.

Remote

취약성이 원격으로 악용될 수 있는지를 나타냅니다.

Available Exploits

취약성에 대한 알려진 익스플로잇이 있는지 여부를 나타냅니다.

Description

취약성에 대한 요약 설명

Technical Description

취약성에 대한 자세한 기술적 설명

Solution

취약성 해결에 대한 정보

Additional Information

알려진 익스플로잇과 가용성, 익스플로잇 시나리오, 완화 전략 등 취약성에 대한 추가 정보(사용 가능한 경우)를 보려면 화살표를 클릭합니다.

Fixes

선택한 취약성에 대해 다운로드할 수 있는 패치에 대한 링크를 제공합니다.

팁 수정 또는 패치 다운로드에 대한 직접 링크가 표시되면 해당 링크를 마우스 오른쪽 버튼으로 클릭하고 파일을 로컬 컴퓨터에 저장합니다.

취약성 영향 자격 설정

라이센스: FireSIGHT

시스템이 네트워크에 해당되지 않는 취약성을 보고하면, 해당 취약성이 영향 플래그 상관관계 평가에 사용되는 것을 차단할 수 있습니다. 호스트 프로필에서 취약성을 비활성화하면 해당 취약성은 네트워크의 모든 호스트에서 비활성화됩니다. 그러나 언제든 다시 활성화할 수 있습니다.

호스트의 운영 체제 또는 호스트의 애플리케이션에서 ID 충돌이 발생하면 시스템은 충돌이 해결될 때까지 충돌하는 두 ID에 대한 취약성을 모두 나열합니다. 자세한 내용은 46-6페이지의 ID 충돌 이해 및 49-14페이지의 운영 체제 ID 충돌 해결을/를 참조하십시오.

시스템은 Impact Qualification 기능을 사용하여 비활성화한 취약성을 기반으로 하는 침입 규칙에 대해 규칙 상태를 권장하지 않습니다. 자세한 내용은 33-1페이지의 네트워크 자산에 대한 침입 방지 맞춤화을/를 참조하십시오.

팁 네트워크 맵 및 취약성 이벤트 보기에서도 취약성을 비활성화할 수 있습니다. 자세한 내용은 48-8페이지의 취약성 네트워크 맵 작업 및 50-53페이지의 취약성 비활성화을/를 참조하십시오.

시스템 전체에서 취약성 사용을 변경하려면

액세스: Admin/Any Security Analyst

1단계 비활성화할 취약성의 영향을 받는 호스트의 프로필에 액세스합니다.

2단계 **Vulnerabilities** 섹션을 확장합니다.

3단계 활성화 또는 비활성화할 취약성의 이름을 클릭합니다.

취약성 세부사항이 포함된 팝업 창이 나타납니다. 자세한 내용은 49-27페이지의 취약성 세부사항 보기을/를 참조하십시오.

4단계 취약성이 사용되는 방법을 지정하려면 **Impact Qualification** 드롭다운 목록에서 **Disabled** 또는 **Enabled**를 선택합니다.

5단계 네트워크 맵의 모든 호스트에 대해 Impact Qualification을 변경할 것인지 확인합니다.

취약성이 활성화 또는 비활성화됩니다.

6단계 취약성 세부사항 팝업 창을 닫으려면 **Done**을 클릭합니다.

취약성용 패치 다운로드

라이센스: FireSIGHT

사용 가능한 경우, 네트워크의 호스트에서 검색된 취약성을 완화하기 위한 패치를 다운로드합니다.

취약성용 패치를 다운로드하려면

액세스: Admin/Any Security Analyst

1단계 패치를 다운로드할 호스트의 호스트 프로필에 액세스합니다.

2단계 **Vulnerabilities** 섹션을 확장합니다.

3단계 패치를 적용할 취약성의 이름을 클릭합니다.

Vulnerability Detail 페이지가 나타납니다.

4단계 **Fixes** 섹션을 확장합니다.

취약성에 대해 다운로드 가능한 패치의 목록이 나타납니다.

5단계 다운로드할 패치 옆에 있는 **Download**를 클릭합니다.

패치 공급업체가 제공하는 다운로드 페이지가 나타납니다.

6단계 패치를 다운로드하고 영향받는 시스템에 적용합니다.

개별 호스트에 대해 취약성 설정

라이센스: FireSIGHT

호스트 기반으로 취약성을 활성화 또는 비활성화하려면 호스트 취약성 편집기를 사용할 수 있습니다. 호스트에 대한 취약성을 비활성화할 경우 해당 호스트에 대한 영향 상관관계에는 여전히 사용되지만 영향 레벨은 자동으로 한 단계 줄어듭니다.

단일 호스트에 대해 취약성을 활성화 또는 비활성화하려면

액세스: Admin/Security Analyst

1단계 호스트 프로필을 엽니다.

2단계 **Vulnerabilities** 옆에 있는 **Edit**를 클릭합니다.

Host Vulnerabilities 편집기 페이지가 나타납니다.

팁 취약성에 대한 세부사항을 보려면 해당 취약성을 선택하고 **View**를 클릭합니다. 자세한 내용은 49-27페이지의 취약성 세부사항 보기을/를 참조하십시오.

3단계 다음 2가지 옵션을 사용할 수 있습니다.

- 취약성을 비활성화하려면 **Valid Vulnerabilities** 목록에서 선택한 다음 아래쪽 화살표를 클릭합니다.
- 취약성을 활성화하려면 **Invalid Vulnerabilities** 목록에서 선택한 다음 위쪽 화살표를 클릭합니다.

팁 여러 취약성을 선택하려면 Ctrl 또는 Shift 키를 누른 채 클릭합니다. 클릭하고 끌어 다수의 인접 취약성을 선택할 수 있습니다. 또한 취약성을 목록 간에 이동하려면 두 번 클릭할 수 있습니다.

4단계 **Save**를 클릭합니다.

변경 내용이 저장되었습니다.

사전 정의 호스트 특성 작업

라이센스: FireSIGHT

각 호스트에 할당할 수 있는 두 가지 사전 정의 호스트 특성, 즉 호스트 중요도 및 호스트 전용 메모가 있습니다. 호스트 중요도 특성은 특정 호스트의 비즈니스 중요도를 할당하고 호스트 중요도를 기반으로 상관관계 정책 및 알림을 맞춤화하는 데 사용할 수 있습니다. 예를 들어, 조직의 메일 서버가 일반적인 사용자 워크스테이션보다 비즈니스에 더 중요하다고 생각한다면 메일 서버에는 High, 다른 주요 비즈니스 디바이스에는 Medium, 기타 호스트에는 Low 값을 할당할 수 있습니다. 그런 다음 영향받는 호스트의 중요도를 기반으로 서로 다른 알림을 생성하는 상관관계 정책을 생성할 수 있습니다.

다른 분석가에게 보여줄 호스트에 대한 정보를 기록하려면 Notes 기능을 사용합니다. 예를 들어, 운영 체제의 패치되지 않은 이전 버전이 있는 테스트용 컴퓨터가 네트워크에 있는 경우, Notes 기능을 사용하여 시스템을 의도적으로 패치하지 않았음을 표시할 수 있습니다.

호스트 프로필에서 사전 정의 호스트 특성을 설정하려면

액세스: Admin/Security Analyst

1단계 비즈니스 중요도를 설정할 호스트에 대한 호스트 프로필을 엽니다.

2단계 **Attributes** 옆의 연필 아이콘( )을 클릭합니다.

Host Attributes 팝업 창이 나타납니다.

3단계 **Host Criticality** 드롭다운 목록에서 적용할 값(**None**, **Low**, **Medium** 또는 **High**)을 선택합니다.

4단계 **Save**를 클릭합니다.

선택한 내용이 저장됩니다.

사용자 정의 호스트 특성 작업

라이센스: FireSIGHT

FireSIGHT 시스템에는 네트워크에서 호스트의 비즈니스 중요도를 나타내기 위해 사용할 수 있는 두 가지 사전 정의 호스트 특성, 즉 호스트 중요도 및 호스트 메모가 있습니다. 호스트 식별에 사용할 다른 기준이 있는 경우 사용자 정의 호스트 특성을 생성할 수 있습니다.

사용자 정의 호스트 특성은 호스트 프로필 페이지에 나타나며, 여기서 호스트 단위로 값을 할당할 수 있습니다. 상관관계 정책 및 검색에서 그러한 특성을 사용할 수 있습니다. 호스트 특성 테이블 보기에서 특성을 볼 수 있으며, 이를 기반으로 보고서를 생성할 수 있습니다.

참고 호스트 특성은 정책 단위라기보다는 전역적으로 정의됩니다. 호스트 특성을 생성하면, 적용된 정책과 상관없이 사용 가능합니다.

사용자 정의 호스트 특성의 예는 다음과 같습니다.

- 호스트에 물리적 위치 식별자 할당(예: 시설 코드, 도시 또는 방 번호).
- 특정 호스트의 담당 시스템 관리자가 누구인지를 나타내는 Responsible Party Identifier. 호스트와 관련된 문제가 탐지될 때 올바른 시스템 관리자에게 알림을 전송하도록 상관관계 규칙 및 정책을 구성할 수 있습니다.

호스트 특성은 텍스트 또는 숫자 범위의 사전 정의된 목록에서 선택한 텍스트 문자열 또는 값일 수 있습니다. 호스트의 IP 주소를 기반으로 사전 정의된 목록에서 호스트로 값을 자동으로 할당할 수도 있습니다. 이 기능을 사용하면 네트워크에 처음 나타나는 새 호스트에 값을 자동으로 할당할 수 있습니다.

호스트 특성은 다음 중 하나일 수 있습니다.

텍스트

호스트에 최대 255자의 텍스트 문자열을 수동으로 할당할 수 있습니다.

정수

양의 정수 범위의 첫 번째와 마지막 숫자를 지정한 다음 이러한 숫자 중 하나를 호스트에 수동으로 할당할 수 있습니다.

목록

문자열 값의 목록을 생성한 다음 이러한 값 중 하나를 호스트에 수동으로 할당할 수 있습니다. 호스트의 IP 주소를 기반으로 호스트에 값을 자동으로 할당할 수도 있습니다.

참고 여러 IP 주소가 있는 호스트에서 한 IP 주소를 기반으로 값을 자동 할당하면, 그 호스트와 연결된 모든 주소에 해당 값이 적용됩니다. Host Attributes 테이블을 볼 때에는 이러한 점에 유의해야 합니다.

URL

URL 값을 호스트에 수동으로 할당할 수 있습니다.

자동으로 생성되는 각 규정 준수 화이트리스트는 화이트리스트와 동일한 이름으로 호스트 특성을 생성합니다. 가능한 값은 `Compliant`(화이트리스트를 준수하는 호스트), `Non-Compliant`(화이트리스트를 위반하는 호스트) 및 `Not Evaluated`(화이트리스트의 유효한 대상이 아니거나 어떤 이유로든 평가되지 않은 호스트)입니다. 화이트리스트 호스트 특성의 값은 수동으로 변경할 수 **없습니다**. 화이트리스트에 대한 자세한 내용은 52-1페이지의 규정준수 툴로 FireSIGHT 시스템 사용을/를 참조하십시오.

자세한 내용은 다음 절을 참조하십시오.

- 49-32페이지의 사용자 정의 호스트 특성 생성
- 49-34페이지의 사용자 정의 호스트 특성 수정
- 49-34페이지의 사용자 정의 호스트 특성 삭제

사용자 정의 호스트 특성 생성

라이센스: FireSIGHT

다음 절차는 사용자 정의 호스트 특성의 생성 방법에 대해 설명합니다.

참고 호스트 특성은 정책 단위라기보다는 전역적으로 정의됩니다. 호스트 특성을 생성하면, 적용된 정책과 상관없이 사용 가능합니다.

새 호스트 특성을 생성하려면

액세스: Admin/Discovery Admin

1단계 **Analysis > Hosts > Host Attributes**를 선택합니다.

Host Attributes 페이지가 나타납니다.

2단계 **Host Attribute Management**를 클릭합니다.

Host Attribute Management 페이지가 나타납니다.

3단계 **Create Attribute**를 클릭합니다.

Create Attribute 페이지가 나타납니다.

4단계 영숫자 문자 및 공백을 사용하여 **Name** 필드에 호스트 특성의 이름을 입력합니다.

5단계 49-22페이지의 호스트 프로필에서 호스트 특성 작업에 설명된 대로, 생성할 특성 유형을 **Type** 드롭다운 목록에서 선택합니다.

- **Text** 또는 **URL** 호스트 특성을 생성하는 경우 6단계단계를 계속 진행합니다.
- **Integer** 호스트 특성을 생성 중인 경우 49-33페이지의 정수 호스트 특성 생성을/를 참조하십시오.

- **List** 호스트 특성을 생성 중인 경우 49-33페이지의 목록 호스트 특성 생성을/를 참조하십시오.

6단계 **Save**를 클릭합니다.

새 사용자 정의 호스트 특성이 저장됩니다.

정수 호스트 특성 생성

라이센스: FireSIGHT

정수 기반 호스트 특성을 정의할 때에는 호스트가 허용하는 숫자 범위를 지정해야 합니다.

정수 기반 호스트 특성을 생성하려면

액세스: Admin/Discovery Admin

1단계 호스트에 할당할 수 있는 최소 정수 값을 **Min** 필드에 입력합니다.

2단계 호스트에 할당할 수 있는 최대 정수 값을 **Max** 필드에 입력합니다.

3단계 **Save**를 클릭합니다.

새 정수 기반 호스트 특성이 저장됩니다.

목록 호스트 특성 생성

라이센스: FireSIGHT

목록 기반 호스트 특성을 정의할 때에는 목록의 각 값을 제공해야 합니다. 이러한 값에는 영숫자 문자, 공백 및 기호를 포함할 수 있습니다.

새 호스트가 검색되면 호스트 특성에 대한 값이 자동으로 할당되도록, 호스트 특성의 값을 생성할 때 IP 주소 블록에 값을 자동 할당할 수도 있습니다.

목록 기반 호스트 특성을 생성하려면

액세스: Admin/Discovery Admin

1단계 목록에 값을 추가하려면 **Add Value**를 클릭합니다.

List Values 섹션이 확장됩니다.

2단계 영숫자 문자, 공백 및 기호를 사용하여, 추가할 첫 번째 값을 **Name** 필드에 입력합니다.

3단계 선택적으로, 방금 추가한 특성 값을 호스트에 자동 할당하려면 **Add Networks**를 클릭합니다.

Auto-Assign Networks 섹션이 확장됩니다.

4단계 추가한 값을 **Value** 드롭다운 목록에서 선택합니다.

5단계 이 값을 자동 할당하려는 IP 주소 블록을 나타내는 IP 주소 및 네트워크 마스크(CIDR 표기법)를 **IP Address** 및 **Netmask** 필드에 입력합니다.

FireSIGHT 시스템에서 CIDR 표기법을 사용하는 방법에 대한 자세한 내용은 1-19페이지의 IP 주소 표기 규칙을/를 참조하십시오.

6단계 목록에 값을 더 추가하여 IP 주소 블록에 속하는 새 호스트에 자동으로 할당하려면 1~5단계를 반복합니다.

팁 특정 IP 블록에서 호스트에 목록 값을 자동 할당하지 않으려면 49-30페이지의 사전 정의 호스트 특성 작업에 설명된 대로 수동으로 값을 할당할 수 있습니다.

사용자 정의 호스트 특성 수정

라이센스: FireSIGHT

기존의 사용자 정의 호스트 특성을 수정할 경우 값의 정의는 변경할 수 있지만 특성 유형(텍스트, 목록, 정수, URL)은 변경할 수 없습니다. 또한 규정 준수 화이트리스트 호스트 특성도 수정할 수 **없습니다**.

기존의 사용자 정의 호스트 특성을 수정하려면

액세스: Admin/Discovery Admin

1단계 **Analysis > Hosts > Host Attributes**를 선택합니다.

Host Attributes 페이지가 나타납니다.

2단계 **Host Attribute Management**를 클릭합니다.

Host Attribute Management 페이지가 나타납니다.

3단계 수정하려는 호스트 특성 옆의 수정 아이콘( )을 클릭합니다.

선택한 특성 설정과 함께 호스트 특성 페이지가 나타납니다.

4단계 원하는 대로 설정을 수정하고 **Save**를 클릭합니다.

수정할 수 있는 특성 유형 및 그러한 특성에 포함할 수 있는 값에 대한 자세한 내용은 49-32페이지의 사용자 정의 호스트 특성 생성을/를 참조하십시오.

사용자 정의 호스트 특성 삭제

라이센스: FireSIGHT

모든 호스트 프로필에서 사용자 정의 호스트 특성을 제거하려면 해당 특성을 삭제할 수 있습니다. 규정 준수 화이트리스트 호스트 특성은 삭제할 수 **없습니다**.

호스트 특성을 삭제하려면

액세스: Admin/Discovery Admin

1단계 **Analysis > Hosts > Host Attributes**를 선택합니다.

Host Attributes 페이지가 나타납니다.

2단계 **Host Attribute Management**를 클릭합니다.

Host Attribute Management 페이지가 나타납니다.

3단계 삭제할 호스트 특성 옆에 있는 삭제 아이콘( )을 클릭합니다.

선택한 호스트 특성이 시스템에서 제거됩니다.

호스트 프로필에서 스캔 결과 작업

라이센스: FireSIGHT

Nmap을 사용하여 호스트를 스캔하거나 Nmap 스캔에서 결과를 가져오면 그러한 결과는 스캔에 포함된 호스트에 대한 호스트 프로필에 나타납니다.

필터링되지 않은 열린 포트에서 실행되는 호스트 운영 체제 및 서버에 대해 Nmap이 수집하는 정보는 각각 호스트 프로필의 Operating System 및 Servers 섹션에 직접 추가됩니다. 또한 Nmap은 해당 호스트에 대한 스캔 결과의 목록을 Scan Results 섹션에 추가합니다.

각 결과는 정보의 소스, 스캔된 포트의 번호와 유형, 포트에서 실행되는 서버의 이름, Nmap에서 탐지한 추가 정보(예: 포트의 상태 또는 서버의 공급업체 이름) 등을 나타냅니다. UDP 포트를 스캔하면 해당 포트에서 탐지된 서버는 Scan Results 섹션에만 나타납니다.

호스트 프로필에서 Nmap 스캔을 수행할 수 있습니다. 자세한 내용은 다음 절, 호스트 프로필에서 호스트 스캐닝을/를 참조하십시오.

호스트 프로필에서 호스트 스캐닝

라이센스: FireSIGHT

호스트 프로필에서 호스트에 대해 Nmap 스캔을 수행할 수 있습니다. 스캔이 완료되면 해당 호스트에 대한 서버 및 운영 체제 정보가 호스트 프로필에서 업데이트됩니다. 호스트 프로필의 Scan Results 섹션에 스캔 결과가 추가됩니다.

주의 또 다른 Nmap 스캔을 실행하거나 우선순위가 더 높은 호스트 입력으로 재정의할 때까지 Nmap 제공 서버 및 운영 체제 데이터는 고정 상태로 유지됩니다. Nmap을 사용하여 호스트를 스캔하려는 경우 Nmap 제공 운영 체제 및 서버 데이터를 최신 상태로 유지하기 위해 정기적인 예약 스캔을 설정할 수 있습니다. 자세한 내용은 62-5페이지의 Nmap 스캔 자동화을/를 참조하십시오.

호스트 프로필에서 호스트를 스캔하려면

액세스: Admin

1단계 호스트 프로필에서 **Scan Host**를 클릭합니다.

Scan Host 팝업 창이 나타납니다.

2단계 호스트 스캔에 사용할 스캔 교정 옆에 있는 **Scan**을 클릭합니다.

호스트가 스캔되고 호스트 프로필에 결과가 추가됩니다.

50장

검색 이벤트 작업

검색 이벤트는 네트워크에서의 활동에 대해 알려주며 적절히 대응해야 할 정보를 제공합니다. 검색 이벤트는 관리되는 디바이스가 모니터링되는 네트워크 세그먼트에서 탐지하는 변경 사항에 의해 트리거됩니다. *네트워크 검색 정책*에서는 시스템이 수집하는 데이터의 종류, 모니터링되는 네트워크 세그먼트, 시스템이 트래픽 모니터링에 사용하는 특정 하드웨어 인터페이스 등을 지정합니다. 네트워크 검색에 대한 자세한 내용은 45-1페이지의 검색 데이터 수집 이해을/를 참조하십시오.

검색 이벤트의 간단한 예로, 방문 직원들이 네트워크에 접속하는 회의실 또는 여분의 업무 공간이 있을 수 있습니다. 이러한 세그먼트에서 생성되는 새 호스트 이벤트를 정기적으로 관찰하고자 할 수 있으며, 악의적인 의도를 의심하지는 않을 것입니다. 그러나 잠겨 있는 네트워크 세그먼트에서 새 호스트 이벤트가 발견되면 그에 따라 응답을 에스컬레이션할 수 있습니다.

사용자 검색 이벤트는 네트워크의 호스트에 로그인하는 사용자에 대한 정보를 제공합니다. 네트워크에서 사용자 활동을 분류하는 이벤트를 확인하고, 특정 사용자에 대한 정보를 보기 위해 드릴다운할 수 있습니다. 예를 들어 어떤 사용자가 새 호스트와 연결되었는지 확인하려면, 호스트 프로필을 점검하여 호스트를 드나드는 트래픽에서 어떤 사용자가 탐지되었는지를 찾아낼 수 있습니다.

검색 이벤트는 네트워크에서의 활동에 대한 훨씬 심층적인 통찰력을 제공하며 이 간단한 예에서 보여주는 것보다 훨씬 더 세분화된 정보를 제공합니다. 각 모니터링되는 호스트에 대해 관련 애플리케이션 프로토콜, 네트워크 프로토콜, 클라이언트, 사용자 및 잠재적 취약성을 탐지하도록 시스템을 구성할 수 있습니다. 시스템은 또한 서드파티 스캐너에 의해 탐지된 취약성 정보를 제공할 수 있으며, 이러한 정보는 호스트 입력 기능을 사용해 방어 센터로 가져올 수 있습니다. IOC(indication of compromise)는 침입, 악성코드 및 기타 데이터를 사용해 보안이 손상될 수 있는 호스트를 식별합니다. 또한 사용자 인터페이스를 통해 사용자가 입력하는 호스트 중요도, 호스트 특성 또는 취약성 설정에 대한 변경 사항을 추적할 수도 있습니다.

시스템에서 생성하는 검색 이벤트를 분석하는 데 사용할 수 있는 사전 정의 워크플로 집합이 제공됩니다. 또한 특정 요구와 일치하는 정보만 표시하는 사용자 지정 워크플로를 생성할 수도 있습니다.

분석할 네트워크 검색 데이터를 수집 및 저장하려면, Cisco가 관리하는 디바이스 및 NetFlow 지원 디바이스가 트래픽을 모니터링하는 네트워크 및 영역에서 적절한 데이터를 검색하도록 네트워크 검색 정책이 구성되어 있는지 확인합니다. 검색에서 모니터링되는 영역을 제외하려면 네트워크 검색 정책에서 구성합니다. 네트워크 검색 정책을 적용하려면 먼저 관리되는 디바이스에 액세스 제어 정책을 적용해야 합니다. 자세한 내용은 45-23페이지의 네트워크 검색 정책 생성을/를 참조하십시오.

자세한 내용은 다음 링크를 참고하십시오.

검색 이벤트 통계 보기

라이센스: FireSIGHT

Discovery Statistics 페이지에는 시스템에서 탐지한 호스트, 이벤트, 프로토콜, 애플리케이션 프로토콜 및 운영 체제의 요약이 표시됩니다.

- 통계 요약은 총 이벤트, 애플리케이션 프로토콜, 호스트, 네트워크 디바이스 및 호스트 제한 사용량 정보에 대한 일반적인 통계를 제공합니다. 50-3페이지의 통계 요약을/를 참조하십시오.
- 이벤트 분류는 시스템에서 발생하는 이벤트 유형에 대한 통계를 제공합니다. 50-4페이지의 Event Breakdown을/를 참조하십시오.
- 프로토콜 분류는 탐지된 호스트에서 사용하는 프로토콜에 대한 통계를 제공합니다. 50-4페이지의 Protocol Breakdown을/를 참조하십시오.
- 애플리케이션 프로토콜 분류는 네트워크에서 실행 중인 애플리케이션 프로토콜에 대한 통계를 제공합니다. 50-4페이지의 Application Protocol Breakdown을/를 참조하십시오.
- 운영 체제 분류는 네트워크에서 실행 중인 운영 체제 및 각 운영 체제를 사용 중인 호스트의 수를 나열합니다. 50-5페이지의 OS Breakdown을/를 참조하십시오.

이 페이지에는 마지막 시간에 대한 통계 및 총 누적 통계가 나열됩니다. 특정 디바이스 또는 모든 디바이스에 대한 통계를 선택할 수 있습니다. 요약 내에 나열된 이벤트, 서버, 운영 체제 또는 운영 체제 공급업체를 클릭하여 페이지의 항목과 일치하는 이벤트를 볼 수도 있습니다.

검색 통계 요약을 보려면

액세스: Admin/Any Security Analyst

1단계 **Overview > Summary > Discovery Statistics**를 선택합니다.

통계 요약 페이지가 나타납니다.

2단계 통계를 보려는 디바이스를 **Select Device** 목록에서 선택합니다. 방어 센터에 의해 관리되는 모든 디바이스의 통계를 보려면 **All**을 선택합니다.

통계 요약

라이센스: FireSIGHT

통계 요약은 총 이벤트, 애플리케이션 프로토콜, 호스트, 네트워크 디바이스 및 호스트 제한 사용량 정보에 대한 일반적인 통계를 제공합니다.

다음은 Statistics Summary 섹션의 행에 대한 설명입니다.

Total Events

방어 센터에 저장된 총 검색 이벤트 수

Total Events Last Hour

마지막 시간에 생성된 총 검색 이벤트 수

Total Events Last Day

마지막 날에 생성된 총 검색 이벤트 수

Total Application Protocols

탐지된 호스트에서 실행 중인 서버의 총 애플리케이션 프로토콜 수

Total IP Hosts

고유한 IP 주소로 식별된 총 탐지된 호스트 수

Total MAC Hosts

IP 주소로 식별되지 않은 총 탐지된 호스트 수

모든 디바이스에 대한 검색 통계를 보든 특정 디바이스에 대한 검색 통계를 보든, Total MAC Hosts 통계는 동일합니다. 관리되는 디바이스는 IP 주소를 기반으로 호스트를 검색하기 때문입니다. 이 통계는 다른 수단에 의해 식별되는 총 호스트 수를 제공하며 특정 관리되는 디바이스와는 독립적입니다.

Total Routers

라우터로서 식별된 총 탐지된 노드 수

Total Bridges

브리지로서 식별된 총 탐지된 노드 수

Host Limit Usage

현재 사용 중인 호스트 제한의 총 비율. 호스트 제한은 FireSIGHT 라이센스에 의해 정의됩니다. 모든 관리되는 디바이스에 대한 통계를 보는 경우에만 Host Limit Usage가 나타납니다. 호스트 사용량 모니터링에 대한 자세한 내용은 68-16페이지의 Host FireSIGHTUsage 모니터링 구성을/를 참조하십시오.

참고 호스트 제한에 도달해서 특정 호스트가 삭제되면, 해당 호스트는 검색을 수행하도록 구성된 모든 관리되는 디바이스에서 네트워크 검색을 다시 시작할 때까지 네트워크 맵에 다시 나타나지 않습니다.

Last Event Received

가장 최근 검색 이벤트가 발생한 날짜 및 시간

Last Connection Received

가장 최근 연결이 완료된 날짜 및 시간

Event Breakdown

라이센스: FireSIGHT

Event Breakdown 섹션에는 마지막 시간 내에 발생한 네트워크 검색 및 호스트 입력 이벤트의 각 유형별 카운트는 물론 데이터베이스에 저장된 각 이벤트 유형의 총계 카운트도 나열됩니다. 각 이벤트 유형에 대한 완전한 설명은 50-9페이지의 검색 이벤트 유형 이해 및 50-13페이지의 호스트 입력 이벤트 유형 이해을/를 참조하십시오.

검색 및 호스트 입력 이벤트에 대한 세부사항을 보는 데에도 Event Breakdown 섹션을 사용할 수 있습니다.

유형별 네트워크 검색 및 호스트 입력 이벤트를 보려면

액세스: Admin/Any Security Analyst

1단계 보려는 이벤트의 유형을 클릭합니다.

선택한 이벤트 유형에 의해 제한된 상태로, 기본 검색 이벤트 워크플로의 첫 번째 페이지가 나타납니다. 사용자 지정 워크플로를 비롯한 다른 워크플로를 사용하려면 워크플로 제목 옆의 **(switch workflow)**를 클릭합니다. 다른 기본 워크플로 지정에 대한 자세한 내용은 71-3페이지의 이벤트 보기 설정 구성을/를 참조하십시오. 이벤트가 표시되지 않을 경우 시간 범위를 조정해야 할 수 있습니다. 58-22페이지의 이벤트 시간 제약 조건 설정을/를 참조하십시오.

검색 이벤트 작업에 대한 자세한 내용은 50-8페이지의 검색 및 호스트 입력 이벤트 작업을/를 참조하십시오.

Protocol Breakdown

라이센스: FireSIGHT

Protocol Breakdown 섹션에는 탐지된 호스트에서 현재 사용 중인 프로토콜이 나열됩니다. 탐지된 각 프로토콜 이름, 프로토콜 스택에서의 "레이어", 프로토콜을 사용하여 통신하는 총 호스트 수가 표시됩니다.

Application Protocol Breakdown

라이센스: FireSIGHT

Application Protocol Breakdown 섹션에는 탐지된 호스트에서 현재 사용 중인 애플리케이션 프로토콜이 나열됩니다. 프로토콜 이름, 지난 시간 동안 애플리케이션 프로토콜을 실행하던 총 호스트 수, 특정 시점에 프로토콜을 실행하던 것으로 탐지된 총 호스트 수가 나열됩니다.

탐지된 프로토콜을 사용하는 서버에 대한 세부사항을 보는 데에도 Application Protocol Breakdown 섹션을 사용할 수 있습니다.

나열된 애플리케이션 프로토콜을 사용하는 서버를 보려면

액세스: Admin/Any Security Analyst

1단계 보려는 애플리케이션 프로토콜의 이름을 클릭합니다.

선택한 애플리케이션 프로토콜에 의해 제한된 상태로, 기본 서버 워크플로의 첫 번째 페이지가 나타납니다. 사용자 지정 워크플로를 비롯한 다른 워크플로를 사용하려면 워크플로 제목 옆의 **(switch workflow)**를 클릭합니다. 다른 기본 워크플로 지정에 대한 자세한 내용은 71-3페이지의 이벤트 보기 설정 구성을/를 참조하십시오.

서버 작업에 대한 자세한 내용은 50-36페이지의 서버 작업을/를 참조하십시오.

OS Breakdown

라이센스: FireSIGHT

OS Breakdown 섹션에는 모니터링되는 네트워크에서 현재 실행 중인 운영 체제와 더불어 해당 공급업체 및 각 운영 체제를 실행 중인 총 호스트 수가 나열됩니다.

운영 체제 이름 및 버전에 사용되는 `unknown` 값은 해당 운영 체제 및 버전이 시스템의 핑거프린트와 일치하지 않음을 의미합니다. `pending` 값은 시스템이 운영 체제 및 버전을 식별하는 데 필요한 정보를 아직 충분히 수집하지 못했음을 의미합니다.

탐지된 운영 체제에 대한 세부사항을 보는 데에도 OS Breakdown 섹션을 사용할 수 있습니다.

운영 체제 또는 공급업체별로 호스트를 보려면

액세스: Admin/Any Security Analyst

1단계 다음 2가지 옵션을 사용할 수 있습니다.

- 특정 운영 체제를 실행 중인 모든 호스트를 보려면 **OS Name** 아래에서 운영 체제 이름을 클릭합니다.
- 특정 공급업체의 운영 체제를 실행 중인 모든 호스트를 보려면 **OS Vendor** 아래에서 공급업체 이름을 클릭합니다.

선택한 운영 체제 또는 공급업체에 의해 제한된 상태로, 기본 호스트 워크플로의 첫 번째 페이지가 나타납니다. 사용자 지정 워크플로를 비롯한 다른 워크플로를 사용하려면 워크플로 제목 옆의 **(switch workflow)**를 클릭합니다. 다른 기본 워크플로 지정에 대한 자세한 내용은 71-3페이지의 이벤트 보기 설정 구성을/를 참조하십시오.

호스트 작업에 대한 자세한 내용은 50-19페이지의 호스트 작업을/를 참조하십시오.

검색 성능 그래프 보기

라이센스: FireSIGHT

검색 이벤트와 함께 관리되는 디바이스에 대한 성능 통계를 표시하는 그래프를 생성할 수 있습니다.

참고 새 데이터는 통계 그래프를 위해 5분마다 누적됩니다. 따라서 그래프를 빠르게 다시 로드하는 경우 다음 5분 증가분이 발생하기까지 데이터가 변경되지 않을 수 있습니다.

다음은 사용 가능한 그래프 유형에 대한 설명입니다.

Processed Events/Sec

Data Correlator가 초당 처리하는 이벤트 수를 나타내는 그래프를 표시합니다.

Processed Connections/Sec

Data Correlator가 초당 처리하는 연결 수를 나타내는 그래프를 표시합니다.

Generated Events/Sec

시스템이 초당 생성하는 이벤트 수를 나타내는 그래프를 표시합니다.

Mbits/Sec

초당 검색 프로세스에 의해 분석되는 트래픽의 메가비트 수를 나타내는 그래프를 표시합니다.

Avg Bytes/Packet

검색 프로세스에 의해 분석되는 각 패킷에 포함된 평균 바이트 수를 나타내는 그래프를 표시합니다.

K Packets/Sec

초당 검색 프로세스에 의해 분석되는 패킷 수를 나타내는 그래프를 표시합니다(1,000 단위).

검색 성능 그래프를 생성하려면

액세스: Admin/Maint

1단계 **Overview > Summary > Discovery Performance**를 선택합니다.

Discovery Performance 페이지가 나타납니다.

2단계 포함할 방어 센터 또는 관리되는 디바이스를 **Select Device** 목록에서 선택합니다.

선택하는 어플라이언스에 따라 **Select Graph(s)** 목록에 표시되는 사용 가능한 그래프가 조정됩니다.

3단계 생성할 그래프 유형을 **Select Graph(s)** 목록에서 선택합니다.

팁 Ctrl 또는 Shift 키를 누른 상태에서 그래프 유형을 클릭하여 여러 그래프를 선택할 수 있습니다.

4단계 그래프에 사용할 시간 범위를 **Select Time Range** 목록에서 선택합니다. 마지막 시간, 마지막 날, 마지막 주 또는 마지막 달 중에서 선택할 수 있습니다.

5단계 선택한 통계를 그래프로 표시하려면 **Graph**를 클릭합니다.

선택한 그래프가 나타납니다.

검색 이벤트 워크플로 이해

라이센스: FireSIGHT

방어 센터에서는 네트워크에 대해 생성되는 검색 이벤트 분석에 사용할 수 있는 워크플로 집합을 제공합니다. 워크플로는 네트워크 맵과 더불어 네트워크 자산에 대한 핵심 정보 소스입니다. 이러한 워크플로에는 시스템에서 생성하는 검색 데이터로 채워지는 테이블이 포함되어 있습니다.

네트워크 검색 워크플로는 **Analysis > Hosts** 메뉴에서 액세스합니다. 방어 센터에서는 검색 이벤트에 대한 사전 정의 워크플로는 물론 탐지된 호스트와 호스트 특성, 서버, 애플리케이션, 애플리케이션 세부사항, 취약성, 사용자 활동, 사용자 등에 대한 사전 정의 워크플로도 제공합니다. 사용자 지정 워크플로를 생성할 수도 있습니다. 워크플로에 대한 자세한 내용은 58-1페이지의 워크플로의 이해 및 사용을/를 참조하십시오.

팁 사용자 지정 테이블을 기반으로 워크플로에 액세스하려면 **Analysis > Custom > Custom Tables**를 선택합니다.

네트워크 검색 워크플로를 사용 중인 경우 이벤트 유형이 무엇이든 공통 작업을 수행할 수 있습니다. 이러한 공통 기능은 공통 검색 이벤트 작업 표에 설명되어 있습니다.

표 50-1 공통 검색 이벤트 작업

목적	가능한 작업
IP 주소에 대한 호스트 프로필 보기	호스트 프로필 아이콘( )을 클릭하거나, 활성 IOC(indication of compromise) 태그가 있는 호스트의 경우 IP 주소 옆에 나타나는 감염된 호스트 아이콘( )을 클릭합니다. IOC에 대한 자세한 내용은 50-32페이지의 IOC 작업을/를 참조하십시오.
사용자 프로필 정보 보기	사용자 ID 옆에 나타나는 사용자 아이콘( )을 클릭합니다. 자세한 내용은 50-63페이지의 사용자 세부사항 및 호스트 기록 이해을/를 참조하십시오.
데이터 정렬	열 제목을 클릭합니다. 정렬 순서를 반대로 하려면 열 제목을 다시 클릭합니다.
워크플로의 다음 페이지로 드릴다운	다음 방법 중 하나를 사용합니다. • 특정 값으로 제한하여 다음 워크플로 페이지로 드릴다운하려면 행 내의 값을 클릭합니다. 이 방법은 드릴다운 페이지에만 해당됩니다. 테이블 보기의 행 내에서 값을 클릭하면 테이블 보기가 제한될 뿐이고 다음 페이지로 드릴다운되지 않습니다. • 일부 이벤트로 제한하여 다음 워크플로 페이지로 드릴다운하려면, 다음 워크플로 페이지에서 볼 이벤트의 옆에 있는 확인란을 선택하고 **View**를 클릭합니다. • 현재의 제약 조건을 유지한 채 다음 워크플로 페이지로 드릴다운하려면 **View All**을 클릭합니다. **팁** 테이블 보기의 페이지 이름에는 항상 "Table View"가 포함됩니다. 자세한 내용은 58-30페이지의 이벤트 제한을/를 참조하십시오.

표 50-1 공통 검색 이벤트 작업 (계속)

목적	가능한 작업
나타나는 열 제한	숨기려는 열 머리글에서 닫기 아이콘(✖)을 클릭합니다. 표시되는 팝업 창에서 **Apply**를 클릭합니다. 팁 다른 열을 숨기거나 표시하려면 **Apply**를 클릭하기 전에 해당 확인란을 선택하거나 선택 취소합니다. 비활성화된 열을 보기에 다시 추가하려면 확장 화살표를 클릭하여 검색 제약 조건을 확장한 다음, Disabled Columns 아래에서 열 이름을 클릭합니다.
현재 워크플로 페이지 내에서 이동	58-35페이지의 워크플로의 다른 페이지로 이동에서 자세히 알아보십시오.
현재의 제약 조건을 유지한 채 현재 워크플로에서 페이지 간 이동	워크플로 페이지의 왼쪽 위에서 적절한 페이지 링크를 클릭합니다. 자세한내용은 58-18페이지의 워크플로 페이지 사용을/를 참조하십시오.
다음을 비롯한 항목을 시스템에서 삭제: • 검색 이벤트 워크플로의 검색 및 호스트 입력 이벤트 • 호스트 워크플로의 호스트 및 네트워크 디바이스 • 호스트 특성 워크플로의 호스트 특성 • 서버 워크플로의 서버 • 애플리케이션 워크플로의 애플리케이션 • 서드파티 취약성 워크플로의 서드파티 취약성 • 사용자 워크플로의 사용자	다음 방법 중 하나를 사용합니다. • 일부 항목을 삭제하려면 삭제할 항목 옆에 있는 확인란을 선택하고 **Delete**를 클릭합니다. • 현재 제한된 보기에서 모든 항목을 삭제하려면 **Delete All**을 클릭하고 모든 항목을 삭제할 것인지를 확인합니다. 이러한 항목은 시스템의 검색 기능이 다시 시작될 때까지(이 경우 다시 탐지될 수도 있음) 삭제된 상태로 유지됩니다. 팁 데이터베이스에서 모든 검색 이벤트를 삭제하는 방법 및 검색을 다시 시작하는 방법에 대한 자세한 내용은 B-1페이지의 데이터베이스에서 검색 데이터 삭제을/를 참조하십시오. Cisco(서드파티와 반대) 취약성은 삭제할 수 **없습니다**. 그러나 검토한 것으로 표시할 수는 있습니다. 자세한 내용은 50-50페이지의 취약성 작업을/를 참조하십시오.
관련 이벤트를 보기 위해 다른 이벤트 보기로 이동	58-35페이지의 워크플로 간 이동에서 자세히 알아보십시오.

검색 및 호스트 입력 이벤트 작업

라이센스: FireSIGHT

시스템에서는 모니터링되는 네트워크 세그먼트의 변경 세부사항을 전달하는 검색 이벤트를 생성합니다. 새로 검색된 네트워크 기능에 대해서는 *새* 이벤트가 생성되고, 이전에 식별된 네트워크 자산의 변경 사항에 대해서는 변경 이벤트가 생성됩니다.

초기 네트워크 검색 단계에서 시스템은 각 호스트에 대해, 그리고 각 호스트에서 실행 중인 것으로 검색된 TCP 또는 UDP 서버에 대해 새 이벤트를 생성합니다. 선택적으로, NetFlow 지원 디바이스에서 내보낸 데이터를 사용하여 이러한 새 호스트 및 서버 이벤트를 생성하도록 시스템을 구성할 수 있습니다.

또한 시스템은 검색된 각 호스트에서 실행 중인 각 애플리케이션 프로토콜, 네트워크 및 전송에 대해 새 이벤트를 생성합니다. NetFlow 지원 디바이스를 포함하도록 구성된 검색 규칙을 생성할 경우 애플리케이션 프로토콜의 탐지를 비활성화할 수 있습니다. 그러나 구성된 NetFlow 지원 디바이스를 사용하지 않는 검색 규칙에서는 애플리케이션 탐지를 비활성화할 수 없습니다. 비 NetFlow 검색 규칙에서 호스트 또는 사용자 검색을 비활성화하면 애플리케이션이 자동으로 검색됩니다.

초기 네트워크 매핑이 완료되면 시스템은 변경 이벤트를 생성하여 네트워크 변경 사항을 계속해서 기록합니다. 전에 검색한 자산의 컨피그레이션이 변경될 때마다 변경 이벤트가 생성됩니다.

생성된 검색 이벤트는 데이터베이스에 기록됩니다. 검색 이벤트를 보고 검색하고 삭제하려면 방어 센터 웹 인터페이스를 사용할 수 있습니다. 상관관계 규칙에서도 검색 이벤트를 사용할 수 있습니다. 생성된 검색 이벤트 및 지정한 다른 기준을 기반으로 상관관계 규칙을 작성할 수 있습니다. 상관관계 정책에서 사용할 경우 이러한 규칙은 네트워크 트래픽이 조건을 충족하면 교정과 syslog, SNMP, 이메일 알림 응답을 실행합니다.

호스트 입력 기능을 사용하여 네트워크 맵에 데이터를 추가할 수 있습니다. 운영 체제 정보를 추가, 수정 또는 삭제할 수 있으며, 이 경우 시스템은 해당 호스트에 대한 해당 정보의 업데이트를 중지합니다. 또한 애플리케이션 프로토콜, 클라이언트, 서버 및 호스트 특성을 수동으로 추가, 수정 또는 삭제할 수 있으며 취약성 정보를 수정할 수도 있습니다. 이렇게 하면 시스템은 호스트 입력 이벤트를 생성합니다.

자세한 내용은 다음 절을 참조하십시오.

- 50-9페이지의 검색 이벤트 유형 이해
- 50-13페이지의 호스트 입력 이벤트 유형 이해
- 50-15페이지의 검색 및 호스트 입력 이벤트 보기
- 50-15페이지의 검색 이벤트 테이블 이해
- 50-16페이지의 검색 이벤트 검색

검색 이벤트 유형 이해

라이센스: FireSIGHT

검색 이벤트에는 여러 유형이 있습니다. 예를 들어, 모니터링되는 네트워크 세그먼트에서 새 호스트를 탐지할 경우 시스템은 새 호스트 이벤트를 생성 및 기록합니다. 검색 이벤트의 테이블을 볼 경우 **Event** 열에 이벤트 유형이 나열됩니다. 자세한 내용은 50-15페이지의 검색 및 호스트 입력 이벤트 보기을/를 참조하십시오.

시스템이 모니터링되는 네트워크에서 변경 사항(예: 전에는 탐지되지 않던 호스트에서 트래픽이 탐지됨)을 탐지할 때 생성되는 검색 이벤트를 사용자가 특정 작업(예: 호스트를 수동으로 추가)을 수행할 때 생성되는 호스트 입력 이벤트와 비교해보십시오. 호스트 입력 이벤트에 대한 자세한 내용은 50-13페이지의 호스트 입력 이벤트 유형 이해을/를 참조하십시오.

네트워크 검색 정책을 수정하여, 시스템이 기록하는 검색 이벤트의 유형을 구성할 수 있습니다. 기본적으로 시스템은 모든 유형의 검색 이벤트를 기록합니다. 자세한 내용은 63-15페이지의 데이터베이스 이벤트 제한 구성을/를 참조하십시오.

서로 다른 유형의 검색 이벤트가 제공하는 정보를 이해하면 어떤 이벤트를 기록하고 알림을 전송할지, 상관관계 정책에서 이러한 알림을 어떻게 사용할지를 좀 더 효과적으로 결정할 수 있습니다. 또한 이벤트 유형의 이름을 알면 좀 더 효과적으로 이벤트를 검색할 수 있습니다. 다음은 서로 다른 유형의 검색 이벤트에 대한 설명입니다.

Additional MAC Detected for Host

시스템이 전에 검색된 호스트에 대해 새 MAC 주소를 탐지할 경우 이 이벤트가 생성됩니다.

시스템이 라우터를 통해 트래픽을 전달하는 호스트를 탐지할 경우 이 이벤트가 종종 생성됩니다. 각 호스트에는 서로 다른 IP 주소가 있지만, 모든 호스트는 라우터와 연결된 MAC 주소가 있는 것으로 표시됩니다. IP 주소와 연결된 실제 MAC 주소를 탐지할 경우 시스템은 호스트 프로필 내에 MAC 주소를 굵은 텍스트로 표시하며, 이벤트 보기의 이벤트 설명 내에 "ARP/DHCP detected" 메시지를 표시합니다.

Client Timeout

비활성화 때문에 시스템이 데이터베이스에서 클라이언트를 삭제할 경우 이 이벤트가 생성됩니다.

Client Update

시스템이 HTTP 트래픽에서 페이로드(즉, 오디오, 비디오, 웹메일 등 특정 유형의 콘텐츠)를 탐지할 경우 이 이벤트가 생성됩니다.

DHCP: IP Address Changed

DHCP 주소 할당 때문에 호스트 IP 주소가 변경된 것을 시스템이 탐지할 경우 이 이벤트가 생성됩니다.

DHCP: IP Address Reassigned

호스트가 IP 주소를 재사용할 경우, 즉 DHCP IP 주소 할당 때문에 호스트가 전에 다른 물리적 호스트에 사용되던 IP 주소를 얻는 경우 이 이벤트가 생성됩니다.

Hops Change

호스트 및 해당 호스트를 탐지하는 디바이스 간 다수의 네트워크 홉에서 시스템이 변경 사항을 탐지할 경우 이 이벤트가 생성됩니다.

이 이벤트는 디바이스가 여러 라우터를 통과하는 호스트 트래픽을 확인하고 호스트 위치에 대한 더 나은 결정을 내릴 수 있는 경우 발생할 수 있습니다. 디바이스가 호스트로부터 ARP 전송을 탐지하고 로컬 세그먼트에 호스트가 있음을 나타내는 경우에도 이 이벤트가 발생할 수 있습니다.

Host Deleted: Host Limit Reached

방어 센터에서 호스트 제한이 초과되어 방어 센터의 네트워크 맵에서 모니터링되는 호스트가 삭제될 경우 이 이벤트가 생성됩니다.

Host Dropped: Host Limit Reached

방어 센터에서 호스트 제한에 도달하여 새 호스트가 삭제될 경우 이 이벤트가 생성됩니다. 이 이벤트를, 호스트 제한에 도달할 경우 오래된 호스트가 네트워크 맵에서 삭제되는 이전 이벤트와 비교해보십시오.

호스트 제한에 도달할 경우 새 호스트를 삭제하려면 **Policies > Network Discovery > Advanced**로 이동하여 **When Host Limit Reached**를 **Drop hosts**로 설정합니다. 자세한 내용은 45-35페이지의 데이터 스토리지 구성을/를 참조하십시오.

Host IOC Set

호스트에 대해 IOC(indication of compromise)가 설정되고 알림이 생성될 경우 이 이벤트가 발생합니다.

Host Timeout

호스트가 네트워크 검색 정책에 정의된 간격 내에 트래픽을 생성하지 못했기 때문에 네트워크 맵에서 삭제될 경우 이 이벤트가 생성됩니다. 개별 호스트 IP 주소 및 MAC 주소는 개별적으로 시간 초과됩니다. 관련된 모든 주소가 시간 초과되기 전에는 호스트가 네트워크 맵에서 사라지지 않습니다. 호스트 시간 초과 값을 구성하는 방법에 대한 자세한 내용은 45-35페이지의 데이터 스토리지 구성을/를 참조하십시오.

네트워크 검색 정책에서 모니터링할 네트워크를 변경하는 경우, FireSIGHT 라이센스에서 계산되지 않도록 네트워크 맵에서 오래된 호스트를 수동으로 삭제하고자 할 수 있습니다. 자세한 내용은 48-2페이지의 호스트 네트워크 맵 작업을/를 참조하십시오.

Host Type Changed to Network Device

탐지된 호스트가 실제로 네트워크 디바이스임을 시스템에서 확인할 경우 이 이벤트가 생성됩니다.

Identity Conflict

서버 또는 운영 체제에 대한 현재의 능동 ID와 충돌하는 새 서버 또는 운영 체제 ID를 시스템이 탐지할 경우 이 이벤트가 생성됩니다.

새로운 능동 ID 데이터를 얻기 위해 호스트를 다시 스캔하여 ID 충돌을 해결하려면 Nmap 교정을 트리거하는 Identity Conflict 이벤트를 사용할 수 있습니다. 자세한 내용은 54-11페이지의 Nmap 교정 구성을/를 참조하십시오.

자세한 내용은 46-6페이지의 ID 충돌 이해 및 45-32페이지의 ID 충돌 해결 구성을/를 참조하십시오. 수동으로 충돌을 해결하는 방법에 대한 자세한 내용은 49-14페이지의 운영 체제 ID 충돌 해결 및 49-19페이지의 서버 ID 충돌 해결을/를 참조하십시오.

Identity Timeout

활성 소스를 통해 네트워크 맵에 추가된 ID 데이터가 시간 초과될 경우 이 이벤트가 생성됩니다.

새로운 능동 ID 데이터를 얻기 위해 호스트를 다시 스캔하여 ID 데이터를 새로 고치려면 Nmap 교정을 트리거하는 Identity Conflict 이벤트를 사용할 수 있습니다. 자세한 내용은 54-11페이지의 Nmap 교정 구성을/를 참조하십시오.

자세한 내용은 49-19페이지의 서버 ID 충돌 해결을/를 참조하십시오.

MAC Information Change

특정 MAC 주소 또는 TTL 값과 연결된 정보에서 시스템이 변경 사항을 탐지할 경우 이 이벤트가 생성됩니다.

시스템이 라우터를 통해 트래픽을 전달하는 호스트를 탐지할 경우 이 이벤트가 종종 발생합니다. 각 호스트에는 서로 다른 IP 주소가 있지만, 모든 호스트는 라우터와 연결된 MAC 주소가 있는 것으로 표시됩니다. IP 주소와 연결된 실제 MAC 주소를 탐지할 경우 시스템은 호스트 프로필 내에 MAC 주소를 굵은 텍스트로 표시하며, 이벤트 보기의 이벤트 설명 내에 "ARP/DHCP detected" 메시지를 표시합니다. 트래픽이 여러 라우터를 통과할 수 있으므로 TTL이 변경될 수 있습니다. 또는 시스템이 호스트의 실제 MAC 주소를 탐지하는 경우에도 TTL이 변경될 수 있습니다.

NETBIOS Name Change

시스템이 호스트 NetBIOS 이름의 변경을 탐지할 경우 이 이벤트가 생성됩니다. 이 이벤트는 NetBIOS 프로토콜을 사용하는 호스트에 대해서만 생성됩니다.

New Client

시스템이 새 클라이언트를 탐지할 경우 이 이벤트가 생성됩니다.

참고 분석용 클라이언트 데이터를 수집 및 저장하려면 네트워크 검색 정책의 검색 규칙에서 애플리케이션 탐지를 활성화하십시오. 자세한 내용은 45-10페이지의 애플리케이션 탐지 이해을/를 참조하십시오.

New Host

시스템이 네트워크에서 실행 중인 새 호스트를 탐지할 경우 이 이벤트가 생성됩니다.

NetFlow 디바이스가 선택된 네트워크 검색 규칙에서 **Discover** 옵션을 선택하고 **Hosts**를 선택한 경우, 새 호스트와 관련된 NetFlow 데이터를 디바이스에서 처리할 때에도 이 이벤트가 생성됩니다.

New Network Protocol

호스트가 새 네트워크 프로토콜(IP, ARP 등)과 통신 중임을 시스템이 탐지할 경우 이 이벤트가 생성됩니다.

New OS

시스템이 호스트에 대한 새 운영 체제를 탐지하거나 호스트 운영 체제에서 변경 사항을 탐지할 경우 이 이벤트가 생성됩니다.

New TCP Port

호스트에서 활성화된 새 TCP 서버 포트(예: SMTP 또는 웹 서비스에서 사용하는 포트)를 시스템이 탐지할 경우 이 이벤트가 생성됩니다. 이 이벤트는 애플리케이션 프로토콜 또는 이와 연결된 서버를 식별하는 데 사용되지 않습니다. 그러한 정보는 TCP Server Information Update 이벤트에서 전송됩니다.

NetFlow 데이터에 대한 네트워크 검색 규칙에서 **Discover** 옵션을 선택한 다음 **Applications**를 선택하면, 디바이스가 아직 네트워크 맵에 존재하지 않는 모니터링되는 네트워크의 서버와 관련된 NetFlow 데이터를 처리할 경우에도 이 이벤트가 생성됩니다.

New Transport Protocol

호스트가 TCP, UDP 등의 새 네트워크 프로토콜과 통신 중임을 시스템이 탐지할 경우 이 이벤트가 생성됩니다.

New UDP Port

시스템이 호스트에서 실행 중인 새 UDP 서버 포트를 탐지할 경우 이 이벤트가 생성됩니다.

NetFlow 데이터에 대한 네트워크 검색 규칙에서 **Discover** 옵션을 선택한 다음 **Applications**를 선택하면, 디바이스가 아직 네트워크 맵에 존재하지 않는 모니터링되는 네트워크의 서버와 관련된 NetFlow 데이터를 처리할 경우에도 이 이벤트가 생성됩니다.

TCP Port Closed

시스템이 호스트에서 닫힌 TCP 포트를 탐지할 경우 이 이벤트가 생성됩니다.

TCP Port Timeout

시스템이 네트워크 검색 정책에 정의된 간격 내에 TCP 포트로부터의 활동을 탐지하지 못한 경우 이 이벤트가 생성됩니다. 서버 시간 초과 값을 구성하는 방법에 대한 자세한 내용은 45-35 페이지의 데이터 스토리지 구성을/를 참조하십시오.

TCP Server Information Update

시스템이 호스트에서 실행 중인 검색된 TCP 서버에서 변경 사항을 탐지할 경우 이 이벤트가 생성됩니다.

TCP 서버가 업그레이드되는 경우에도 이 이벤트가 생성될 수 있습니다.

UDP Port Closed

시스템이 호스트에서 닫힌 UDP 포트를 탐지할 경우 이 이벤트가 생성됩니다.

UDP Port Timeout

시스템이 네트워크 검색 정책에 정의된 간격 내에 UDP 포트로부터의 활동을 탐지하지 못한 경우 이 이벤트가 생성됩니다. 서버 시간 초과 값을 구성하는 방법에 대한 자세한 내용은 45-35 페이지의 데이터 스토리지 구성을/를 참조하십시오.

UDP Server Information Update

시스템이 호스트에서 실행 중인 검색된 UDP 서버에서 변경 사항을 탐지할 경우 이 이벤트가 생성됩니다.

UDP 서버가 업그레이드되는 경우에도 이 이벤트가 생성될 수 있습니다.

VLAN Tag Information Update

시스템이 호스트에 속하는 VLAN 태그에서 변경 사항을 탐지할 경우 이 이벤트가 생성됩니다. VLAN 태그에 대한 자세한 내용은 49-21페이지의 호스트 프로필에서 VLAN 태그 작업을/를 참조하십시오.

호스트 입력 이벤트 유형 이해

라이센스: FireSIGHT

호스트 입력 이벤트에는 여러 유형이 있습니다. 예를 들어, 사용자가 호스트 가져오기 기능을 사용하여 호스트를 추가할 경우 시스템은 Add Host 이벤트를 생성하여 기록합니다. 검색 이벤트의 테이블을 볼 경우 **Event** 열에 이벤트 유형이 나열됩니다. 자세한 내용은 50-15페이지의 검색 및 호스트 입력 이벤트 보기을/를 참조하십시오.

사용자가 특정 작업(예: 수동으로 호스트 추가)을 수행할 때 생성되는 호스트 입력 이벤트를 시스템이 모니터링되는 네트워크에서 직접 변경 사항을 탐지(예: 전에 탐지되지 않던 호스트에서 트래픽 탐지)할 때 생성되는 검색 이벤트와 비교해보십시오. 호스트 입력 이벤트에 대한 자세한 내용은 50-9페이지의 검색 이벤트 유형 이해을/를 참조하십시오.

네트워크 검색 정책을 수정하여, 시스템이 기록하는 호스트 입력 이벤트의 유형을 구성할 수 있습니다. 기본적으로 시스템은 모든 유형의 호스트 입력 이벤트를 기록합니다. 자세한 내용은 63-15페이지의 데이터베이스 이벤트 제한 구성을/를 참조하십시오.

서로 다른 유형의 호스트 입력 이벤트가 제공하는 정보를 이해하면 어떤 이벤트를 기록하고 알림을 전송할지, 상관관계 정책에서 이러한 알림을 어떻게 사용할지를 좀 더 효과적으로 결정할 수 있습니다. 또한 이벤트 유형의 이름을 알면 좀 더 효과적으로 이벤트를 검색할 수 있습니다. 다음은 서로 다른 유형의 호스트 입력 이벤트에 대한 설명입니다.

Add Client

사용자가 클라이언트를 추가할 경우 이 이벤트가 생성됩니다.

Add Host

사용자가 호스트를 추가할 경우 이 이벤트가 생성됩니다.

Add Protocol

사용자가 프로토콜을 추가할 경우 이 이벤트가 생성됩니다.

Add Scan Result

시스템이 Nmap 스캔의 결과를 호스트에 추가할 경우 이 이벤트가 생성됩니다.

Add Port

사용자가 서버 포트를 추가할 경우 이 이벤트가 생성됩니다.

Delete Client

사용자가 시스템에서 클라이언트를 삭제할 경우 이 이벤트가 생성됩니다.

Delete Host/Network

사용자가 시스템에서 IP 주소 또는 서브넷을 삭제할 경우 이 이벤트가 생성됩니다.

Delete Protocol

사용자가 시스템에서 프로토콜을 삭제할 경우 이 이벤트가 생성됩니다.

Delete Port

사용자가 시스템에서 서버 포트 또는 서버 포트 그룹을 삭제할 경우 이 이벤트가 생성됩니다.

Host Attribute Add

사용자가 새 호스트 특성을 생성할 경우 이 이벤트가 생성됩니다.

Host Attribute Delete

사용자가 사용자 정의 호스트 특성을 삭제할 경우 이 이벤트가 생성됩니다.

Host Attribute Delete Value

사용자가 호스트 특성에 할당된 값을 삭제할 경우 이 이벤트가 생성됩니다.

Host Attribute Set Value

사용자가 호스트에 대한 호스트 특성 값을 설정할 경우 이 이벤트가 생성됩니다.

Host Attribute Update

사용자가 사용자 정의 호스트 특성의 정의를 변경할 경우 이 이벤트가 생성됩니다.

Set Host Criticality

사용자가 호스트에 대한 호스트 중요도 값을 설정 또는 수정할 경우 이 이벤트가 생성됩니다.

Set Operating System Definition

사용자가 호스트에 대한 운영 체제를 설정할 경우 이 이벤트가 생성됩니다.

Set Server Definition

사용자가 서버에 대한 공급업체 및 버전 정의를 설정할 경우 이 이벤트가 생성됩니다.

Set Vulnerability Impact Qualification

취약성 영향 자격이 설정될 경우 이 이벤트가 생성됩니다.

영향 자격에 대해 사용 중인 취약성이 전역 레벨에서 비활성화되거나 전역 레벨에서 취약성이 활성화될 경우 이 이벤트가 생성됩니다.

Vulnerability Set Invalid

사용자가 취약성을 무효화 또는 검토할 경우 이 이벤트가 생성됩니다.

Vulnerability Set Valid

전에 잘못된 것으로 표시되었던 취약성을 사용자가 검증할 경우 이 이벤트가 생성됩니다.

검색 및 호스트 입력 이벤트 보기

라이센스: FireSIGHT

검색 이벤트와 호스트 입력 이벤트 모두 검색 이벤트 워크플로를 사용하여 볼 수 있습니다. 검색 이벤트는 어플라이언스에 대해 구성된 네트워크 검색 정책을 기반으로 네트워크 검색 데이터의 탐지를 기록합니다. 호스트 입력 이벤트는 호스트 입력 기능을 통해 호스트 데이터의 입력을 네트워크 맵에 기록합니다. 자세한 내용은 50-9페이지의 검색 이벤트 유형 이해 및 50-13페이지의 호스트 입력 이벤트 유형 이해을/를 참조하십시오.

방어 센터를 사용하면 검색 또는 호스트 입력 이벤트의 테이블을 볼 수 있습니다. 그런 다음 찾고 있는 정보에 따라 이벤트 보기를 조작할 수 있습니다.

이벤트에 액세스할 때 표시되는 페이지는 사용하는 워크플로에 따라 달라집니다. 검색 이벤트의 테이블 보기 및 호스트 보기 종료 페이지를 포함하는 사전 정의 워크플로를 사용할 수 있습니다. 특정 요구와 일치하는 정보만 표시하는 사용자 지정 워크플로를 생성할 수도 있습니다. 사용자 지정 워크플로 생성에 대한 자세한 내용은 58-38페이지의 사용자 지정 워크플로 생성을/를 참조하십시오.

아래의 검색 이벤트 작업 표에서는 검색 이벤트 워크플로 페이지에서 수행할 수 있는 몇 가지 특정 작업에 대해 설명합니다. 공통 검색 이벤트 작업 표에 설명된 작업을 수행할 수도 있습니다.

표 50-2 검색 이벤트 작업

목적	가능한 작업
표시된 이벤트에 대한 시간 및 날짜 범위 수정	58-22페이지의 이벤트 시간 제약 조건 설정에서 자세히 알아보십시오. 어플라이언스의 구성된 시간 창(전역이든 이벤트 전용이든)을 벗어나 생성된 이벤트는 시간 기준으로 이벤트 보기를 제한할 경우 이벤트 보기에 나타날 수 있습니다. 이는 어플라이언스에 대한 슬라이딩 시간 창을 구성한 경우에도 발생할 수 있습니다.
테이블에서 열의 내용에 대해 자세히 알아보기	50-15페이지의 검색 이벤트 테이블 이해에서 자세히 알아보십시오.

검색 이벤트를 보려면

액세스: Admin/Any Security Analyst

1단계 **Analysis > Hosts > Discovery Events**를 선택합니다.

기본 검색 이벤트 워크플로의 첫 번째 페이지가 나타납니다. 사용자 지정 워크플로를 비롯한 다른 워크플로를 사용하려면 **(switch workflow)**를 클릭합니다. 다른 기본 워크플로 지정에 대한 자세한 내용은 71-3페이지의 이벤트 보기 설정 구성을/를 참조하십시오. 이벤트가 표시되지 않을 경우 시간 범위를 조정해야 할 수 있습니다. 58-22페이지의 이벤트 시간 제약 조건 설정을/를 참조하십시오.

검색 이벤트 테이블 이해

라이센스: FireSIGHT

시스템에서는 모니터링되는 네트워크 세그먼트의 변경 세부사항을 전달하는 검색 이벤트를 생성합니다. 새로 검색된 네트워크 기능에 대해서는 *새* 이벤트가 생성되고, 이전에 식별된 네트워크 자산의 변경 사항에 대해서는 변경 이벤트가 생성됩니다.

초기 네트워크 검색 단계에서 시스템은 각 호스트에 대해, 그리고 각 호스트에서 검색된 TCP 또는 UDP 서버에 대해 새 이벤트를 생성합니다. 또한 시스템은 검색된 각 호스트에서 실행 중인 각 애플리케이션 프로토콜, 네트워크 또는 전송에 대해 새 이벤트를 생성합니다. NetFlow 관련 트래픽의 경우 시스템이 호스트에서 실행 중인 애플리케이션 프로토콜을 탐지할 때 새 이벤트를 생성할지 여부를 제어할 수 있습니다. 초기 네트워크 매핑이 완료되면 시스템은 변경 이벤트를 생성하여 네트워크 변경 사항을 계속해서 기록합니다. 전에 검색한 호스트, 서버 또는 클라이언트의 컨피그레이션이 변경될 때마다 변경 이벤트가 생성됩니다.

다음은 검색 이벤트 테이블의 필드에 대한 설명입니다.

Time

시스템이 이벤트를 생성한 시간

Event

이벤트 유형. 사용 가능한 각 이벤트에 대한 설명은 50-9페이지의 검색 이벤트 유형 이해 및 50-13페이지의 호스트 입력 이벤트 유형 이해을/를 참조하십시오.

IP Address

이벤트와 관련된 호스트와 연결된 IP 주소

User

이벤트가 생성되기 전 이벤트와 관련된 호스트에 로그인한 마지막 사용자. 권한 있는 사용자 이후 권한 없는 사용자만 로그인한 경우, 권한 있는 사용자가 호스트에 대한 현재 사용자로 유지됩니다(또 다른 권한 있는 사용자가 로그인하지 않는 한).

MAC Address

검색 이벤트를 트리거한 네트워크 트래픽에 의해 사용된 NIC의 MAC 주소. 이 MAC 주소는 이벤트와 관련된 호스트의 실제 MAC 주소일 수도 있고, 트래픽이 통과한 네트워크 디바이스의 MAC 주소일 수도 있습니다.

MAC Vendor

검색 이벤트를 트리거한 네트워크 트래픽에 의해 사용된 NIC의 MAC 하드웨어 공급업체

Port

이벤트를 트리거한 트래픽에서 사용하는 포트(해당되는 경우)

Description

이벤트의 텍스트 설명

Device

이벤트를 생성한 디바이스의 이름. NetFlow 데이터를 기반으로 하는 새 호스트 및 새 서버 이벤트의 경우 이것이 NetFlow 데이터를 처리한 디바이스입니다.

검색 이벤트 검색

라이센스: FireSIGHT

특정 검색 이벤트를 검색할 수 있습니다. 네트워크 환경에 맞춤화된 검색을 생성한 다음 나중에 다시 사용할 수 있도록 저장할 수 있습니다.

일반 검색 구문

각 검색 필드 옆에는 유효한 구문의 예가 표시됩니다. 검색 기준을 입력할 경우, 다음 사항에 유의해야 합니다.

- 모든 필드에 부정(!)을 사용할 수 있습니다.
- 모든 필드에 쉼표로 구분된 검색 값의 목록을 사용할 수 있습니다. 지정된 필드에 나열된 값 중 하나를 포함하는 레코드는 검색 기준과 일치합니다.
- 모든 필드에 따옴표로 감싸고 쉼표로 구분한 목록을 검색 값으로 사용할 수 있습니다.
  - 단일 값만을 포함할 수 있는 필드의 경우, 따옴표 내에 지정된 정확한 문자열을 포함하는 지정된 필드의 레코드가 검색 기준과 일치합니다. 예를 들어 `A, B, "C, D, E"`에 대한 검색은 지정된 필드에 `"A"` 또는 `"B"` 또는 `"C, D, E"`가 포함된 레코드와 일치합니다. 따라서 가능한 값으로 쉼표를 포함하는 필드에서 일치를 확인할 수 있습니다.
  - 여러 값을 동시에 포함할 수 있는 필드의 경우, 따옴표로 감싸고 쉼표로 구분한 모든 값을 포함하는 지정된 필드의 레코드가 해당 검색 기준과 일치합니다.
  - 여러 값을 동시에 포함할 수 있는 필드의 경우, 검색 기준에 단일 값은 물론 따옴표로 감싸고 쉼표로 구분한 목록도 포함할 수 있습니다. 예를 들어 하나 이상의 이러한 문자를 포함할 수 있는 필드에서 `A, B, "C, D, E"`에 대한 검색은 지정된 필드에 `A` 또는 `B`, 또는 `C, D, E` 모두가 포함된 레코드와 일치합니다.
- 검색 결과에는 모든 필드에 지정된 검색 기준과 매칭되는 레코드만 반환됩니다.
- 많은 필드에서 와일드카드로 하나 이상의 별표(*)를 사용할 수 있습니다.
- 일부 필드의 경우, 해당 필드에 대해 사용할 수 있는 정보가 없는 이벤트를 식별하려면 필드에 `n/a` 또는 `blank`를 지정할 수 있습니다. 해당 필드가 채워지는 이벤트를 식별하려면 `!n/a` 또는 `!blank`를 사용합니다.
- 대부분의 필드에서 대/소문자를 구분합니다.
- IP 주소는 CIDR 표기법으로 지정할 수 있습니다.
- 특정 디바이스 및 그룹, 스택 또는 클러스터의 디바이스를 검색하려면 디바이스 필드를 사용합니다. FireSIGHT 시스템에서 검색 시 디바이스 필드를 취급하는 방법에 대한 자세한 내용은 60-7페이지의 검색에서 디바이스 지정을/를 참조하십시오.
- 검색 기준으로 객체를 사용하려면 검색 필드 옆에 나타나는 객체 추가 아이콘(+)을 클릭합니다.

검색에서 객체를 사용하는 방법을 포함하여 검색 구문에 대한 자세한 내용은 60-1페이지의 이벤트 검색을/를 참조하십시오.

검색 이벤트용 특수 검색 구문

다음 표에서는 특정 검색 이벤트 필드와 관련된 검색 정보에 대해 설명합니다. 검색 이벤트 필드에 대한 자세한 내용은 50-20페이지의 호스트 테이블 이해을/를 참조하십시오.

표 50-3 검색 이벤트 검색 기준 참고 사항

필드	검색 기준 참고 사항
이벤트	이벤트 이름의 범위는 50-9페이지의 검색 이벤트 유형 이해 및 50-13페이지의 호스트 입력 이벤트 유형 이해에 나열되어 있습니다.

표 50-3 검색 이벤트 검색 기준 참고 사항 (계속)

필드	검색 기준 참고 사항
MAC Vendor	가상 MAC 공급업체, 즉 가상 머신과 관련된 이벤트를 검색하려면 `virtual_mac_vendor`를 입력하십시오. 이름에 쉼표가 포함된 공급업체를 검색하려면 전체 검색어를 따옴표로 감싸십시오. 그렇게 하지 않으면 방어 센터에서는 해당 검색어를 두 가지 검색으로 취급하여 각 검색어와 일치하는 이벤트를 반환합니다.
Port	다음에 유의하십시오. • 다른 종류의 이벤트 검색에서 가능한 포트/프로토콜 조합을 입력할 수 없습니다. • 포트 번호 또는 범위를 지정할 때 공백을 사용할 수 없습니다.

검색 이벤트를 검색하려면

액세스: Admin/Any Security Analyst

1단계 **Analysis > Search**를 선택합니다.

Search 페이지가 나타납니다.

2단계 테이블 드롭다운 목록에서 **Discovery Events**를 선택합니다.

해당 제약 조건으로 페이지가 업데이트됩니다.

3단계 50-17페이지의 일반 검색 구문 및 50-17페이지의 검색 이벤트용 특수 검색 구문에 설명된 대로 해당 필드에 검색 기준을 입력합니다.

여러 필드에 대한 조건을 입력하는 경우 모든 필드에 대해 지정한 검색 기준과 일치하는 레코드만 반환됩니다. 검색 기준으로 객체를 사용하려면 검색 필드 옆에 나타나는 추가 아이콘(+)을 클릭합니다.

4단계 선택적으로, 검색을 저장하려면 **Private** 확인란을 선택하여 자신만 액세스할 수 있는 비공개로 검색을 저장할 수 있습니다. 또는 모든 사용자가 사용할 수 있도록 검색을 저장하려면 확인란을 선택하지 않습니다.

팁 사용자 지정 사용자 역할에 대한 데이터 제한으로서 검색을 사용하려면 **반드시** 비공개 검색으로 저장해야 합니다.

5단계 선택적으로, 나중에 다시 사용할 수 있도록 검색을 저장할 수 있습니다. 다음 옵션을 이용할 수 있습니다.

- 검색 기준을 저장하려면 **Save**를 클릭합니다.

  새 검색인 경우 검색 이름을 입력하도록 대화 상자가 나타납니다. 고유한 검색 이름을 입력하고 **Save**를 클릭합니다. 이미 존재하는 검색에 대한 새 조건을 저장하는 경우 프롬프트가 나타나지 않습니다. 나중에 실행할 수 있도록 검색이 저장됩니다(**Private**을 선택한 경우 자신만 볼 수 있음).

- 새 검색을 저장하거나, 저장된 기존 검색을 변경하여 만든 검색에 새 이름을 할당하려면 **Save As New**를 클릭합니다.

  검색 이름을 입력하도록 대화 상자가 나타납니다. 고유한 검색 이름을 입력하고 **Save**를 클릭합니다. 나중에 실행할 수 있도록 검색이 저장됩니다(**Private**을 선택한 경우 자신만 볼 수 있음).

6단계 검색을 시작하려면 **Search**를 클릭합니다.

검색 결과는 현재의 시간 범위로 제한되어 기본 검색 이벤트 워크플로에 나타납니다. 사용자 지정 워크플로를 비롯한 다른 워크플로를 사용하려면 **(switch workflow)**를 클릭합니다. 다른 기본 워크플로 지정에 대한 자세한 내용은 71-3페이지의 이벤트 보기 설정 구성을/를 참조하십시오.

호스트 작업

라이센스: FireSIGHT

시스템에서는 호스트를 탐지하고 관련 정보를 수집하여 호스트 프로필을 작성할 때 이벤트를 생성합니다. 호스트를 보고 검색하고 삭제하려면 방어 센터 웹 인터페이스를 사용할 수 있습니다.

호스트를 보는 동안 선택한 호스트를 기반으로 트래픽 프로필 및 규정전수 화이트리스트를 생성할 수 있습니다. 또한 호스트 중요도 값(비즈니스 중요도 지정)을 비롯한 호스트 특성을 호스트 그룹에 할당할 수 있습니다. 그런 다음 상관관계 규칙 및 정책 내에서 이러한 중요도 값, 화이트리스트 및 트래픽 프로필을 사용할 수 있습니다.

NetFlow 지원 디바이스에서 내보낸 데이터를 기반으로 네트워크 맵에 호스트를 추가하도록 네트워크 검색 정책을 구성할 수 있지만, 이러한 호스트에 대해 사용할 수 있는 정보는 제한적입니다. 예를 들어, 호스트 입력 기능을 사용하여 제공하지 않는 한 이러한 호스트에 대해 사용할 수 있는 운영 체제 데이터가 없습니다. 자세한 내용은 45-17페이지의 NetFlow 및 FireSIGHT 데이터 간 차이점을/를 참조하십시오.

자세한 내용은 다음 절을 참조하십시오.

- 50-19페이지의 호스트 보기
- 50-20페이지의 호스트 테이블 이해
- 50-23페이지의 선택한 호스트에 대해 트래픽 프로필 생성
- 50-24페이지의 선택한 호스트를 기반으로 규정준수 화이트리스트 생성
- 50-24페이지의 호스트 검색
- 50-29페이지의 선택한 호스트에 대해 호스트 특성 설정

호스트 보기

라이센스: FireSIGHT

방어 센터를 사용하면 시스템에서 탐지한 호스트의 테이블을 볼 수 있습니다. 그런 다음 찾고 있는 정보에 따라 보기를 조작할 수 있습니다.

호스트에 액세스할 때 표시되는 페이지는 사용하는 워크플로에 따라 달라집니다. 미리 정의된 두 워크플로는 사용자의 제한 사항을 충족하는 모든 호스트에 대한 호스트 프로필이 포함된 호스트 보기에서 종료됩니다. 특정 요구와 일치하는 정보만 표시하는 사용자 지정 워크플로를 생성할 수도 있습니다. 자세한 내용은 58-38페이지의 사용자 지정 워크플로 생성을/를 참조하십시오.

아래의 호스트 작업 표에서는 호스트 워크플로 페이지에서 수행할 수 있는 몇 가지 특정 작업에 대해 설명합니다. 공통 검색 이벤트 작업 표에 설명된 작업을 수행할 수도 있습니다.

표 50-4 호스트 작업

목적	가능한 작업
테이블에서 열의 내용에 대해 자세히 알아보기	50-20페이지의 호스트 테이블 이해에서 자세히 알아보십시오.
선택한 호스트에 호스트 특성 할당	50-29페이지의 선택한 호스트에 대해 호스트 특성 설정에서 자세히 알아보십시오.
선택한 호스트에 대한 트래픽 프로필 생성	50-23페이지의 선택한 호스트에 대해 트래픽 프로필 생성에서 자세히 알아보십시오.
선택한 호스트를 기반으로 규정준수 화이트리스트 생성	50-24페이지의 선택한 호스트를 기반으로 규정준수 화이트리스트 생성에서 자세히 알아보십시오.

호스트를 보려면

액세스: Admin/Any Security Analyst

1단계 **Analysis > Hosts > Hosts**를 선택합니다.

기본 호스트 워크플로의 첫 번째 페이지가 나타납니다. 사용자 지정 워크플로를 비롯한 다른 워크플로를 사용하려면 **(switch workflow)**를 클릭합니다. 다른 기본 워크플로 지정에 대한 자세한 내용은 71-3페이지의 이벤트 보기 설정 구성을/를 참조하십시오.

팁 호스트의 테이블 보기가 포함되지 않은 사용자 지정 워크플로를 사용 중인 경우 **(switch workflow)**를 클릭한 다음 **Hosts**를 선택하십시오.

호스트 테이블 이해

라이센스: FireSIGHT

시스템은 호스트를 검색하면 해당 호스트에 대한 데이터를 수집합니다. 여기에는 호스트의 IP 주소, 실행 중인 운영 체제 등이 포함될 수 있습니다. 그러한 정보 중 일부는 호스트의 테이블 보기에서 볼 수 있습니다. 시스템이 탐지된 호스트에 대해 수집하는 데이터에 대한 자세한 내용은 49-1페이지의 호스트 프로필 사용을/를 참조하십시오.

다음은 호스트 테이블의 필드에 대한 설명입니다.

NetFlow 지원 디바이스에서 내보낸 데이터를 기반으로 네트워크 맵에 호스트를 추가하도록 네트워크 검색 정책을 구성할 수 있지만, 이러한 호스트에 대해 사용할 수 있는 정보는 제한적입니다. 예를 들어, 호스트 입력 기능을 사용하여 제공하지 않는 한 이러한 호스트에 대해 사용할 수 있는 운영 체제 데이터가 없습니다. 자세한 내용은 45-17페이지의 NetFlow 및 FireSIGHT 데이터 간 차이점을/를 참조하십시오.

Last Seen

시스템에서 마지막으로 탐지한 호스트 IP 주소 중 하나의 날짜 및 시간. Last Seen 값은 적어도 네트워크 검색 정책에서 구성한 업데이트 간격만큼 그리고 호스트 IP 주소 중 하나에 대해 새 호스트 이벤트를 생성할 때 업데이트됩니다.

호스트 입력 기능을 사용하여 업데이트된 운영 체제 데이터가 있는 호스트의 경우 Last Seen 값은 데이터가 원래 추가된 날짜 및 시간을 나타냅니다.

IP Address

호스트와 연결된 IP 주소

MAC Address

호스트에서 탐지한 NIC의 MAC 주소.

MAC Address 필드는 호스트 워크플로에서 찾을 수 있는 호스트의 테이블 보기에 나타납니다. MAC Address 필드를 다음에도 추가할 수 있습니다.

- 호스트 테이블의 필드를 포함하는 사용자 지정 테이블
- 호스트 테이블 기반의 사용자 지정 워크플로에 있는 드릴다운 페이지

MAC Vendor

호스트에서 탐지한 NIC의 MAC 하드웨어 공급업체.

MAC Vendor 필드는 호스트 워크플로에서 찾을 수 있는 호스트의 테이블 보기에 나타납니다. MAC Vendor 필드를 다음에도 추가할 수 있습니다.

- 호스트 테이블의 필드를 포함하는 사용자 지정 테이블
- 호스트 테이블 기반의 사용자 지정 워크플로에 있는 드릴다운 페이지

Current User

현재 호스트에 로그인한 사용자의 사용자 ID(사용자 이름)

권한 없는 사용자가 호스트에 로그인하면 해당 로그인은 사용자 및 호스트 내역에 기록됩니다. 호스트와 연결된 권한 있는 사용자가 없는 경우, 권한 없는 사용자가 호스트의 현재 사용자가 될 수 있습니다. 그러나 권한 있는 사용자가 호스트에 로그인한 후에는 또 다른 권한 있는 사용자의 로그인에 의해서만 현재 사용자가 변경됩니다. 또한 권한 없는 사용자가 호스트의 현재 사용자인 경우, 해당 사용자를 사용자 제어에 사용할 수 없습니다.

Host Criticality

호스트에 할당된 사용자 지정 중요도 값. 이 필드에 대한 자세한 내용은 50-28페이지의 호스트 특성 테이블 이해의 Host Criticality 열에 대한 설명을/를 참조하십시오.

NetBIOS Name

호스트의 NetBIOS 이름. NetBIOS 프로토콜을 실행하는 호스트만이 NetBIOS 이름을 가질 수 있습니다.

VLAN ID

호스트에서 사용하는 VLAN ID. VLAN ID에 대한 자세한 내용은 49-21페이지의 호스트 프로필에서 VLAN 태그 작업을/를 참조하십시오.

Hops

호스트를 탐지한 디바이스에서 호스트로의 네트워크 홉 수

Host Type

호스트 유형(호스트, 모바일 디바이스, 탈옥 모바일 디바이스, 라우터, 브리지, NAT 디바이스 또는 로드 밸런서). 시스템이 네트워크 디바이스를 구분하기 위해 사용하는 방법은 다음과 같습니다.

- CDP(Cisco Discovery Protocol) 메시지의 분석 - 네트워크 디바이스 및 유형을 식별할 수 있습니다(Cisco 디바이스만 해당).
- STP(Spanning Tree Protocol)의 탐지 - 디바이스를 스위치 또는 브리지로 식별합니다.

- 동일한 MAC 주소를 사용하는 여러 호스트 탐지 - MAC 주소를 라우터에 속한 것으로 식별합니다.
- 클라이언트 측에서 TTL 값 변경 탐지 또는 일반적인 부팅시간보다 더 자주 변경되는 TTL 값 - NAT 디바이스 및 로드 밸런서를 탐지합니다.

네트워크 디바이스로 식별되지 않는 디바이스는 호스트로 분류됩니다.

Hardware

모바일 디바이스용 하드웨어 플랫폼

OS

호스트에서 실행 중인 것으로 탐지되거나 Nmap 또는 호스트 입력 기능을 사용하여 업데이트된 운영 체제(이름, 공급업체 및 버전). 대시보드의 Custom Analysis 위젯에서 호스트 이벤트 보기를 호출할 경우 이 필드가 나타납니다. 이것은 또한 호스트 테이블 기반의 사용자 지정 테이블에 있는 필드 옵션이기도 합니다.

시스템에서는 여러 ID를 식별하면 쉼표로 구분된 목록으로 표시합니다.

이 필드에서 `unknown` 값은, 운영 체제가 알려진 핑거프린트 중 어떤 것과도 일치하지 않음을 의미합니다. `pending` 값은 시스템이 운영 체제를 식별하는 데 필요한 정보를 아직 충분히 수집하지 못했음을 의미합니다.

OS Vendor

호스트에서 탐지되었거나 Nmap 또는 호스트 입력 기능을 사용하여 업데이트된 운영 체제의 공급업체.

시스템에서는 여러 공급업체를 식별하면 쉼표로 구분된 목록으로 표시합니다.

이 필드에서 `unknown` 값은, 운영 체제가 알려진 핑거프린트 중 어떤 것과도 일치하지 않음을 의미합니다. `pending` 값은 시스템이 운영 체제를 식별하는 데 필요한 정보를 아직 충분히 수집하지 못했음을 의미합니다.

OS Name

호스트에서 실행 중인 것으로 탐지되거나 Nmap 또는 호스트 입력 기능을 사용하여 업데이트된 운영 체제.

시스템에서는 여러 이름을 식별하면 쉼표로 구분된 목록으로 표시합니다.

이 필드에서 `unknown` 값은, 운영 체제가 알려진 핑거프린트 중 어떤 것과도 일치하지 않음을 의미합니다. `pending` 값은 시스템이 운영 체제를 식별하는 데 필요한 정보를 아직 충분히 수집하지 못했음을 의미합니다.

OS Version

호스트에서 탐지되었거나 Nmap 또는 호스트 입력 기능을 사용하여 업데이트된 운영 체제의 버전.

시스템에서는 여러 버전을 식별하면 쉼표로 구분된 목록으로 표시합니다.

이 필드에서 `unknown` 값은, 운영 체제가 알려진 핑거프린트 중 어떤 것과도 일치하지 않음을 의미합니다. `pending` 값은 시스템이 운영 체제를 식별하는 데 필요한 정보를 아직 충분히 수집하지 못했음을 의미합니다.

Source Type

호스트 운영 체제 ID의 소스에 대한 다음 값 중 하나:

- 사용자: *user_name*
- 애플리케이션: *app_name*
- 스캐너: *scanner_type*(네트워크 검색 컨피그레이션을 통해 추가된 Nmap 또는 스캐너)
- FireSIGHT, 시스템에서 탐지한 운영 체제

시스템에서는 운영 체제의 ID를 확인하기 위해 여러 소스의 데이터를 조정할 수 있습니다. 46-5페이지의 현재 ID 이해을/를 참조하십시오.

Confidence

다음 중 하나:

- 호스트에서 실행 중인 운영 체제의 ID에 대한 시스템의 신뢰도 비율 - 시스템에서 탐지한 호스트
- 100% - 호스트 입력 기능 또는 Nmap 스캐너 등 활성 소스에 의해 식별된 운영 체제
- unknown - 시스템이 운영 체제 ID를 확인할 수 없는 호스트 및 NetFlow 데이터를 기반으로 네트워크 맵에 추가된 호스트

Notes

Notes 호스트 특성의 사용자 정의 내용.

Device

트래픽을 탐지한 관리되는 디바이스, 또는 네트워크 맵에 호스트를 추가한 호스트 입력 데이터 또는 NetFlow를 처리한 디바이스.

이 필드가 비어 있으면 호스트가 상주하는 네트워크를 명시적으로 모니터링하지 않는 디바이스에 의해 호스트가 네트워크 맵에 추가되었거나(네트워크 검색 정책에 정의된 대로), 호스트가 호스트 입력 기능을 사용하여 추가되었지만 아직 시스템에 의해 탐지되지 않은 것입니다.

Count

각 행에 표시되는 정보와 매칭되는 이벤트의 수. 둘 이상의 동일한 행을 생성하는 제약 조건을 적용한 경우에만 Count 필드가 나타납니다.

선택한 호스트에 대해 트래픽 프로필 생성

라이센스: FireSIGHT

트래픽 프로필은 네트워크의 트래픽 프로필로, 지정한 기간에 수집된 연결 데이터를 기반으로 합니다. 트래픽 프로필을 생성한 후에는 프로필을 기준으로 새 트래픽을 평가하여, 정상적인 것처럼 보일 수 있는 비정상적인 네트워크 트래픽을 탐지할 수 있습니다.

지정한 호스트 그룹에 대한 트래픽 프로필을 생성하려면 Hosts 페이지를 사용할 수 있습니다. 트래픽 프로필은 지정한 호스트 중 하나가 호스트를 시작하는 것으로 탐지된 연결을 기반으로 합니다. 프로필을 생성하고자 하는 호스트를 격리하려면 정렬 또는 검색 기능을 사용할 수 있습니다.

선택한 호스트에 대해 트래픽 프로필을 생성하려면

액세스: Admin

1단계 호스트 워크플로의 테이블 보기에서 트래픽 프로필을 생성하려는 호스트 옆에 있는 확인란을 선택합니다.

2단계 페이지의 하단에서 **Create Traffic Profile**을 클릭합니다.

모니터링할 호스트로서 지정한 호스트의 IP 주소가 채워진 상태로 Create Profile 페이지가 나타납니다.

3단계 특정 요구에 맞게 트래픽 프로필을 수정 및 저장합니다.

트래픽 프로필 생성에 대한 자세한 내용은 53-1페이지의 트래픽 프로필 생성을/를 참조하십시오.

선택한 호스트를 기반으로 규정준수 화이트리스트 생성

라이센스: FireSIGHT

규정준수 화이트리스트를 사용하면 네트워크에서 허용할 운영 체제와 클라이언트, 그리고 네트워크, 전송 또는 애플리케이션 프로토콜을 지정할 수 있습니다.

지정한 호스트 그룹의 호스트 프로필을 기반으로 규정준수 화이트리스트를 생성하려면 Hosts 페이지를 사용할 수 있습니다. 화이트리스트를 생성하고자 하는 호스트를 격리하려면 정렬 또는 검색 기능을 사용할 수 있습니다.

선택한 호스트를 기반으로 규정준수 화이트리스트를 생성하려면

액세스: Admin

1단계 호스트 워크플로의 테이블 보기에서 화이트리스트를 생성하려는 호스트 옆에 있는 확인란을 선택합니다.

2단계 페이지의 하단에서 **Create White List**를 클릭합니다.

지정한 호스트의 호스트 프로필에 정보가 채워진 상태로 Create White List 페이지가 나타납니다.

3단계 특정 요구에 맞게 화이트리스트를 수정 및 저장합니다.

규정준수 화이트리스트 생성에 대한 자세한 내용은 52-8페이지의 규정준수 화이트리스트 생성을/를 참조하십시오.

호스트 검색

라이센스: FireSIGHT

사전 정의된 검색 중 하나를 사용하거나 자체 검색 기준을 사용하여 특정 호스트를 검색할 수 있습니다.

호스트를 검색할 때에는, NetFlow 지원 디바이스에서 내보낸 데이터를 기반으로 네트워크 맵에 호스트를 추가하도록 네트워크 검색 정책을 구성할 수 있지만 이러한 호스트에 대해 사용할 수 있는 정보는 제한적이라는 점을 염두에 두어야 합니다. 예를 들어, 호스트 입력 기능을 사용하여 제공하지 않는 한 이러한 호스트에 대해 사용할 수 있는 운영 체제 데이터가 없습니다. 자세한 내용은 45-17페이지의 NetFlow 및 FireSIGHT 데이터 간 차이점을/를 참조하십시오.

특정 검색 이벤트를 검색할 수 있습니다. 네트워크 환경에 맞춤화된 검색을 생성한 다음 나중에 다시 사용할 수 있도록 저장할 수 있습니다.

일반 검색 구문

각 검색 필드 옆에는 유효한 구문의 예가 표시됩니다. 검색 기준을 입력할 경우, 다음 사항에 유의해야 합니다.

- 모든 필드에 부정(`!`)을 사용할 수 있습니다.
- 모든 필드에 쉼표로 구분된 검색 값의 목록을 사용할 수 있습니다. 지정된 필드에 나열된 값 중 하나를 포함하는 레코드는 검색 기준과 일치합니다.
- 모든 필드에 따옴표로 감싸고 쉼표로 구분한 목록을 검색 값으로 사용할 수 있습니다.
  - 단일 값만을 포함할 수 있는 필드의 경우, 따옴표 내에 지정된 정확한 문자열을 포함하는 지정된 필드의 레코드가 검색 기준과 일치합니다. 예를 들어 `A, B, "C, D, E"`에 대한 검색은 지정된 필드에 `"A"` 또는 `"B"` 또는 `"C, D, E"`가 포함된 레코드와 일치합니다. 따라서 가능한 값으로 쉼표를 포함하는 필드에서 일치를 확인할 수 있습니다.
  - 여러 값을 동시에 포함할 수 있는 필드의 경우, 따옴표로 감싸고 쉼표로 구분한 모든 값을 포함하는 지정된 필드의 레코드가 해당 검색 기준과 일치합니다.
  - 여러 값을 동시에 포함할 수 있는 필드의 경우, 검색 기준에 단일 값은 물론 따옴표로 감싸고 쉼표로 구분한 목록도 포함할 수 있습니다. 예를 들어 하나 이상의 이러한 문자를 포함할 수 있는 필드에서 `A, B, "C, D, E"`에 대한 검색은 지정된 필드에 `A` 또는 `B`, 또는 `C, D, E` 모두가 포함된 레코드와 일치합니다.
- 검색 결과에는 모든 필드에 지정된 검색 기준과 매칭되는 레코드만 반환됩니다.
- 많은 필드에서 와일드카드로 하나 이상의 별표(`*`)를 사용할 수 있습니다.
- 일부 필드의 경우, 해당 필드에 대해 사용할 수 있는 정보가 없는 이벤트를 식별하려면 필드에 `n/a` 또는 `blank`를 지정할 수 있습니다. 해당 필드가 채워지는 이벤트를 식별하려면 `!n/a` 또는 `!blank`를 사용합니다.
- 대부분의 필드에서 대/소문자를 구분합니다.
- IP 주소는 CIDR 표기법으로 지정할 수 있습니다. FireSIGHT 시스템에서 IP 주소를 입력하는 방법에 대한 자세한 내용은 1-19페이지의 IP 주소 표기 규칙을/를 참조하십시오.

참고 IP 주소별로 호스트를 검색하면 하나 이상의 IP 주소가 검색 기준과 일치하는 모든 호스트가 결과에 포함됩니다. 즉, IPv6 주소를 검색하면 기본 주소가 IPv4인 호스트가 반환될 수 있습니다.

- 특정 디바이스 및 그룹, 스택 또는 클러스터의 디바이스를 검색하려면 디바이스 필드를 사용합니다. FireSIGHT 시스템에서 검색 시 디바이스 필드를 취급하는 방법에 대한 자세한 내용은 60-7페이지의 검색에서 디바이스 지정을/를 참조하십시오.
- 검색 기준으로 객체를 사용하려면 검색 필드 옆에 나타나는 객체 추가 아이콘(+)을 클릭합니다.

검색에서 객체를 사용하는 방법을 포함하여 검색 구문에 대한 자세한 내용은 60-1페이지의 이벤트 검색을/를 참조하십시오.

호스트용 특수 검색 구문

다음 표에서는 특정 호스트 필드와 관련된 검색 정보에 대해 설명합니다. 호스트 필드에 대한 자세한 내용은 50-20페이지의 호스트 테이블 이해을/를 참조하십시오.

표 50-5 호스트 검색 기준

필드	검색 기준 참고 사항
Host Type	모든 네트워크 디바이스를 검색하려면 `!host`를 입력합니다.
MAC Vendor	가상 MAC 공급업체, 즉 가상 머신과 관련된 이벤트를 검색하려면 `virtual_mac_vendor`를 입력하십시오. 이름에 쉼표가 포함된 공급업체를 검색하려면 전체 검색어를 따옴표로 감싸십시오. 그렇게 하지 않으면 방어 센터에서는 해당 검색어를 두 가지 검색으로 취급하여 각 검색어와 일치하는 이벤트를 반환합니다.
OS Vendor/Name/Version	운영 체제를 알 수 없는 호스트를 검색하려면 `unknown`을 입력합니다. 운영 체제가 아직 식별되지 않은 호스트를 검색하려면 `n/a`를 입력합니다.
Confidence	신뢰도 앞에 보다 큼(`>`), 보다 크거나 같음(`>=`), 보다 작음(`<`), 보다 작거나 같음(`<=`) 또는 같음(`=`) 연산자를 사용할 수 있습니다. `n/a` 검색의 일치 항목에는 NetFlow 데이터를 기반으로 네트워크 맵에 추가된 호스트가 포함됩니다.
OS Conflict	검색 결과에는 OS Conflict 열이 나타나지 않습니다. 호스트를 볼 때 운영 체제 충돌을 표시할지 여부를 결정하려면 워크플로 페이지에서 검색 제약 조건을 확장합니다. 운영 체제 충돌 해결에 대한 자세한 내용은 49-14페이지의 운영 체제 ID 충돌 해결을/를 참조하십시오.

저장된 검색을 로드 및 삭제하는 방법을 포함하여 검색에 대한 자세한 내용은 60-1페이지의 이벤트 검색을/를 참조하십시오.

호스트를 검색하려면

액세스: Admin/Any Security Analyst

1단계 **Analysis > Search**를 선택합니다.

Search 페이지가 나타납니다.

2단계 테이블 드롭다운 목록에서 **Hosts**를 선택합니다.

해당 제약 조건으로 페이지가 업데이트됩니다.

팁 데이터베이스에서 서로 다른 종류의 이벤트를 검색하려면 테이블 드롭다운 목록에서 선택합니다.

3단계 호스트 검색 기준 표에 설명된 대로 해당 필드에 검색 기준을 입력합니다.

여러 필드에 대한 조건을 입력하는 경우 방어 센터에서는 모든 필드에 대해 지정한 검색 기준과 일치하는 레코드만 반환합니다. 검색 기준으로 객체를 사용하려면 검색 필드 옆에 나타나는 추가 아이콘(+)을 클릭합니다.

4단계 선택적으로, 검색을 저장하려면 **Private** 확인란을 선택하여 자신만 액세스할 수 있는 비공개로 검색을 저장할 수 있습니다. 또는 모든 사용자가 사용할 수 있도록 검색을 저장하려면 확인란을 선택하지 않습니다.

팁 제한된 권한과 함께 사용자 지정 사용자 역할에 대한 제한으로서 검색을 저장하려면 **반드시** 비공개 검색으로 저장해야 합니다.

5단계 선택적으로, 나중에 다시 사용할 수 있도록 검색을 저장할 수 있습니다. 다음 옵션을 이용할 수 있습니다.

- 검색 기준을 저장하려면 **Save**를 클릭합니다.

  새 검색인 경우 검색 이름을 입력하도록 대화 상자가 나타납니다. 고유한 검색 이름을 입력하고 **Save**를 클릭합니다. 이미 존재하는 검색에 대한 새 조건을 저장하는 경우 프롬프트가 나타나지 않습니다. 나중에 실행할 수 있도록 검색이 저장됩니다(**Private**을 선택한 경우 자신만 볼 수 있음).

- 새 검색을 저장하거나, 저장된 기존 검색을 변경하여 만든 검색에 새 이름을 할당하려면 **Save As New**를 클릭합니다.

  검색 이름을 입력하도록 대화 상자가 나타납니다. 고유한 검색 이름을 입력하고 **Save**를 클릭합니다. 나중에 실행할 수 있도록 검색이 저장됩니다(**Private**을 선택한 경우 자신만 볼 수 있음).

6단계 검색을 시작하려면 **Search**를 클릭합니다.

검색 결과는 기본 호스트 워크플로에 나타납니다. 사용자 지정 워크플로를 비롯한 다른 워크플로를 사용하려면 **(switch workflow)**를 클릭합니다. 다른 기본 워크플로 지정에 대한 자세한 내용은 71-3페이지의 이벤트 보기 설정 구성을/를 참조하십시오.

호스트 특성 작업

라이센스: FireSIGHT

FireSIGHT 시스템은 탐지한 호스트에 대한 정보를 수집하고 이 정보를 사용하여 호스트 프로필을 작성합니다. 그러나 분석가에게 제공하고자 하는, 네트워크의 호스트에 대한 추가 정보가 있을 수 있습니다. 호스트 프로필에 메모를 추가하거나, 호스트의 비즈니스 중요도를 설정하거나, 선택한 다른 정보를 제공할 수 있습니다. 이러한 각각의 정보를 호스트 특성이라고 합니다.

호스트 프로필 자격에 호스트 특성을 사용할 수 있습니다. 이러한 특성은 트래픽 프로필 작성 중에 수집하는 데이터를 제한하며, 상관관계 규칙을 트리거할 조건을 제한할 수도 있습니다. 상관관계 규칙에 대한 응답에 특성 값을 설정할 수도 있습니다.

자세한 내용은 다음 링크를 참고하십시오.

- 50-27페이지의 호스트 특성 보기
- 50-28페이지의 호스트 특성 테이블 이해
- 50-29페이지의 선택한 호스트에 대해 호스트 특성 설정
- 50-30페이지의 호스트 특성 검색
- 54-15페이지의 Set Attribute 교정 구성

호스트 특성 보기

라이센스: FireSIGHT

방어 센터를 사용하면 시스템에서 탐지한 호스트의 테이블을 호스트 특성과 함께 볼 수 있습니다. 그런 다음 찾고 있는 정보에 따라 보기를 조작할 수 있습니다.

호스트 특성에 액세스할 때 표시되는 페이지는 사용하는 워크플로에 따라 달라집니다. 탐지된 모든 호스트 및 해당 특성을 나열하는 호스트 특성의 테이블 보기를 포함하며, 제약 조건에 맞는 모든 호스트에 대한 호스트 프로필이 포함된 호스트 보기 페이지에서 종료되는 사전 정의 워크플로를 사용할 수 있습니다.

특정 요구와 일치하는 정보만 표시하는 사용자 지정 워크플로를 생성할 수도 있습니다. 사용자 지정 워크플로 생성에 대한 자세한 내용은 58-38페이지의 사용자 지정 워크플로 생성을/를 참조하십시오.

아래의 호스트 특성 작업 표에서는 호스트 특성 워크플로 페이지에서 수행할 수 있는 몇 가지 특정 작업에 대해 설명합니다. 공통 검색 이벤트 작업 표에 설명된 작업을 수행할 수도 있습니다.

표 50-6 호스트 특성 작업

목적	가능한 작업
테이블에서 열의 내용에 대해 자세히 알아보기	50-28페이지의 호스트 특성 테이블 이해에서 자세히 알아보십시오.
선택한 호스트에 호스트 특성 할당	50-29페이지의 선택한 호스트에 대해 호스트 특성 설정에서 자세히 알아보십시오.

호스트 특성을 보려면

액세스: Admin/Any Security Analyst

1단계 **Analysis > Hosts > Host Attributes**를 선택합니다.

기본 호스트 특성 워크플로의 첫 번째 페이지가 나타납니다. 사용자 지정 워크플로를 비롯한 다른 워크플로를 사용하려면 **(switch workflow)**를 클릭합니다. 다른 기본 워크플로 지정에 대한 자세한 내용은 71-3페이지의 이벤트 보기 설정 구성을/를 참조하십시오.

팁 호스트 특성의 테이블 보기가 포함되지 않은 사용자 지정 워크플로를 사용 중인 경우 **(switch workflow)**를 클릭한 다음 **Attributes**를 선택하십시오.

호스트 특성 테이블 이해

라이센스: FireSIGHT

FireSIGHT 시스템은 탐지한 호스트에 대한 정보를 수집하고 이 정보를 사용하여 호스트 프로필을 작성합니다. 그러나 분석가에게 제공하고자 하는, 네트워크의 호스트에 대한 추가 정보가 있을 수 있습니다. 호스트 프로필에 메모를 추가하거나, 비즈니스 중요도를 설정하거나, 선택한 다른 정보를 제공할 수 있습니다. 이러한 각각의 정보를 호스트 특성이라고 합니다.

호스트 프로필 자격에 호스트 특성을 사용할 수 있습니다. 이러한 특성은 트래픽 프로필 작성 중에 수집하는 데이터를 제한하며, 상관관계 규칙을 트리거할 조건을 제한할 수도 있습니다.

MAC 주소에 의해서만 식별되는 호스트는 특성 테이블에 표시되지 않습니다.

호스트 특성에 대한 자세한 내용은 49-30페이지의 사전 정의 호스트 특성 작업 및 49-31페이지의 사용자 정의 호스트 특성 작업을/를 참조하십시오.

다음은 호스트 특성 테이블의 필드에 대한 설명입니다.

IP 주소

호스트와 연결된 IP 주소

현재 사용자

현재 호스트에 로그인한 사용자의 사용자 ID(사용자 이름)

권한 없는 사용자가 호스트에 로그인하면 해당 로그인은 사용자 및 호스트 내역에 기록됩니다. 호스트와 연결된 권한 있는 사용자가 없는 경우, 권한 없는 사용자가 호스트의 현재 사용자가 될 수 있습니다. 그러나 권한 있는 사용자가 호스트에 로그인한 후에는 또 다른 권한 있는 사용자의 로그인에 의해서만 현재 사용자가 변경됩니다. 또한 권한 없는 사용자가 호스트의 현재 사용자인 경우, 해당 사용자를 사용자 제어에 사용할 수 없습니다.

Host Criticality

엔터프라이즈에 사용자가 할당하는 호스트의 중요도. 정책 위반 및 응답을 이벤트와 관련된 호스트의 중요도에 맞추려면 상관관계 규칙 및 정책에 호스트 중요도를 사용할 수 있습니다. Low, Medium, High 또는 None의 호스트 중요도를 할당할 수 있습니다.

호스트 중요도 설정에 대한 자세한 내용은 49-30페이지의 사전 정의 호스트 특성 작업 및 50-29페이지의 선택한 호스트에 대해 호스트 특성 설정을/를 참조하십시오.

참고

다른 분석가에게 보여줄 호스트에 대한 정보. 메모 추가에 대한 자세한 내용은 49-30페이지의 사전 정의 호스트 특성 작업을/를 참조하십시오.

Any user-defined host attribute, including those for compliance white lists

사용자 정의 호스트 특성의 값.

호스트 특성 테이블에는 각 사용자 정의 호스트 특성에 대한 필드가 포함되어 있습니다. 자세한 내용은 49-31페이지의 사용자 정의 호스트 특성 작업을/를 참조하십시오.

개수

각 행에 표시되는 정보와 매칭되는 이벤트의 수. 둘 이상의 동일한 행을 생성하는 제약 조건을 적용한 경우에만 Count 필드가 나타납니다.

선택한 호스트에 대해 호스트 특성 설정

라이센스: FireSIGHT

각 호스트에 할당할 수 있는 두 가지 사전 정의 호스트 특성, 즉 호스트 중요도 및 호스트 전용 메모가 있습니다.

특정 호스트의 비즈니스 중요도를 지정하려면 호스트 중요도를 사용합니다. 호스트 중요도를 기반으로 상관관계 정책 및 알림을 맞춤 설정할 수 있습니다. 예를 들어, 조직의 메일 서버는 일반적인 사용자 워크스테이션보다 비즈니스 중요도가 높습니다. 메일 서버 및 기타 주요 비즈니스 서버에는 높은 호스트 중요도 값을 할당하고, 기타 호스트에는 중간 또는 낮은 값을 할당할 수 있습니다. 그런 다음 영향받는 호스트의 중요도를 기반으로 서로 다른 알림을 생성하는 상관관계 정책을 생성할 수 있습니다.

다른 분석가에게 보여줄 호스트에 대한 정보를 기록하려면 Notes를 사용합니다. 예를 들어, 운영 체제의 패치되지 않은 이전 버전이 있는 테스트용 컴퓨터가 네트워크에 있는 경우, Notes 기능을 사용하여 시스템을 의도적으로 패치하지 않았음을 표시할 수 있습니다.

사용자 정의 호스트 특성을 생성할 수도 있습니다. 예를 들어, 호스트에 물리적 위치 식별자(예: 시설 코드, 도시 또는 방 번호)를 할당하는 호스트 특성을 만들 수 있습니다. 사용자 정의 호스트 특성 생성에 대한 자세한 내용은 49-32페이지의 사용자 정의 호스트 특성 생성을/를 참조하십시오.

호스트 워크플로에서, 그리고 호스트 프로필 내에서 선택한 호스트의 호스트 중요도를 설정할 수 있고, 교정을 통해 설정할 수도 있습니다. 자세한 내용은 49-30페이지의 사전 정의 호스트 특성 작업 또는 54-15페이지의 Set Attribute 교정 구성을/를 참조하십시오.

선택한 호스트에 대해 호스트 특성을 설정하려면

액세스: Admin/Any Security Analyst

1단계 호스트 특성을 추가하려는 호스트의 옆에 있는 확인란을 선택합니다.

팁 정렬 및 검색 기능을 사용하여, 특정 특성을 할당할 호스트를 격리합니다.

2단계 페이지의 하단에서 **Set Attributes**를 클릭합니다.

Host Attributes 팝업 창이 나타납니다.

3단계 선택적으로, 선택한 호스트의 호스트 중요도를 설정합니다.

None, **Low**, **Medium** 또는 **High**를 선택할 수 있습니다.

4단계 선택적으로, 텍스트 상자에 최대 255자의 영숫자 문자, 특수 문자 및 공백을 입력하여 선택한 호스트의 호스트 프로필에 메모를 추가합니다.

5단계 선택적으로, 이미 구성한 사용자 정의 호스트 특성을 설정합니다.

6단계 **Save**를 클릭합니다.

선택한 호스트에 사용자가 지정한 호스트 특성이 할당됩니다.

호스트 특성 검색

라이센스: FireSIGHT

특정 호스트 특성이 있는 호스트를 검색할 수 있습니다. 예를 들어, 회사에 여러 지역 사무소가 있는 경우 어떤 호스트가 어떤 도시에 있는지를 알려주는 호스트 특성을 구성할 수 있습니다. 그런 다음 특정 지역의 호스트를 검색할 수 있습니다. 호스트 특성에 대한 자세한 내용은 49-31페이지의 사용자 정의 호스트 특성 작업을/를 참조하십시오.

네트워크 환경에 맞춤화된 검색을 생성한 다음 나중에 다시 사용할 수 있도록 저장할 수 있습니다. 호스트 특성 필드에 대한 자세한 내용은 50-28페이지의 호스트 특성 테이블 이해을/를 참조하십시오.

일반 검색 구문

각 검색 필드 옆에는 유효한 구문의 예가 표시됩니다. 검색 기준을 입력할 경우, 다음 사항에 유의해야 합니다.

- 모든 필드에 부정(!)을 사용할 수 있습니다.
- 모든 필드에 쉼표로 구분된 검색 값의 목록을 사용할 수 있습니다. 지정된 필드에 나열된 값 중 하나를 포함하는 레코드는 검색 기준과 일치합니다.
- 모든 필드에 따옴표로 감싸고 쉼표로 구분한 목록을 검색 값으로 사용할 수 있습니다.
  - 단일 값만을 포함할 수 있는 필드의 경우, 따옴표 내에 지정된 정확한 문자열을 포함하는 지정된 필드의 레코드가 검색 기준과 일치합니다. 예를 들어 `A, B, "C, D, E"`에 대한 검색은 지정된 필드에 `"A"` 또는 `"B"` 또는 `"C, D, E"`가 포함된 레코드와 일치합니다. 따라서 가능한 값으로 쉼표를 포함하는 필드에서 일치를 확인할 수 있습니다.
  - 여러 값을 동시에 포함할 수 있는 필드의 경우, 따옴표로 감싸고 쉼표로 구분한 모든 값을 포함하는 지정된 필드의 레코드가 해당 검색 기준과 일치합니다.

  - 여러 값을 동시에 포함할 수 있는 필드의 경우, 검색 기준에 단일 값은 물론 따옴표로 감싸고 쉼표로 구분한 목록도 포함할 수 있습니다. 예를 들어 하나 이상의 이러한 문자를 포함할 수 있는 필드에서 `A, B, "C, D, E"`에 대한 검색은 지정된 필드에 `A` 또는 `B`, 또는 `C, D, E` 모두가 포함된 레코드와 일치합니다.
- 검색 결과에는 모든 필드에 지정된 검색 기준과 매칭되는 레코드만 반환됩니다.
- 많은 필드에서 와일드카드로 하나 이상의 별표(*)를 사용할 수 있습니다.
- 일부 필드의 경우, 해당 필드에 대해 사용할 수 있는 정보가 없는 이벤트를 식별하려면 필드에 `n/a` 또는 `blank`를 지정할 수 있습니다. 해당 필드가 채워지는 이벤트를 식별하려면 `!n/a` 또는 `!blank`를 사용합니다.
- 대부분의 필드에서 대/소문자를 구분합니다.
- IP 주소는 CIDR 표기법으로 지정할 수 있습니다. FireSIGHT 시스템에서 IPv4 및 IPv6 주소를 입력하는 방법에 대한 자세한 내용은 1-19페이지의 IP 주소 표기 규칙을/를 참조하십시오.
- 검색 기준으로 객체를 사용하려면 검색 필드 옆에 나타나는 객체 추가 아이콘(+)을 클릭합니다.

검색에서 객체를 사용하는 방법을 포함하여 검색 구문에 대한 자세한 내용은 60-1페이지의 이벤트 검색을/를 참조하십시오.

호스트 특성을 검색하려면

액세스: Admin/Any Security Analyst

1단계 **Analysis > Search**를 선택합니다.

Search 페이지가 나타납니다.

2단계 테이블 드롭다운 목록에서 **Host Attributes**를 선택합니다.

해당 제약 조건으로 페이지가 업데이트됩니다.

팁 데이터베이스에서 서로 다른 종류의 이벤트를 검색하려면 테이블 드롭다운 목록에서 선택합니다.

3단계 호스트 특성 테이블 이해에 설명된 대로 해당 필드에 검색 기준을 입력합니다.

여러 필드에 대한 조건을 입력하는 경우 모든 필드에 대해 지정한 검색 기준과 일치하는 레코드만 반환됩니다. 검색 기준으로 객체를 사용하려면 검색 필드 옆에 나타나는 추가 아이콘(+)을 클릭합니다.

4단계 선택적으로, 검색을 저장하려면 **Private** 확인란을 선택하여 자신만 액세스할 수 있는 비공개로 검색을 저장할 수 있습니다. 또는 모든 사용자가 사용할 수 있도록 검색을 저장하려면 확인란을 선택하지 않습니다.

팁 제한된 권한과 함께 사용자 지정 사용자 역할에 대한 제한으로서 검색을 저장하려면 **반드시** 비공개 검색으로 저장해야 합니다.

5단계 선택적으로, 나중에 다시 사용할 수 있도록 검색을 저장할 수 있습니다. 다음 옵션을 이용할 수 있습니다.

- 검색 기준을 저장하려면 **Save**를 클릭합니다.

  새 검색인 경우 검색 이름을 입력하도록 대화 상자가 나타납니다. 고유한 검색 이름을 입력하고 **Save**를 클릭합니다. 이미 존재하는 검색에 대한 새 조건을 저장하는 경우 프롬프트가 나타나지 않습니다. 나중에 실행할 수 있도록 검색이 저장됩니다(**Private**을 선택한 경우 자신만 볼 수 있음).

- 새 검색을 저장하거나, 저장된 기존 검색을 변경하여 만든 검색에 새 이름을 할당하려면 **Save As New**를 클릭합니다.

  검색 이름을 입력하도록 대화 상자가 나타납니다. 고유한 검색 이름을 입력하고 **Save**를 클릭합니다. 나중에 실행할 수 있도록 검색이 저장됩니다(**Private**을 선택한 경우 자신만 볼 수 있음).

6단계 검색을 시작하려면 **Search**를 클릭합니다.

검색 결과는 기본 호스트 특성 워크플로에 나타납니다. 사용자 지정 워크플로를 비롯한 다른 워크플로를 사용하려면 **(switch workflow)**를 클릭합니다. 다른 기본 워크플로 지정에 대한 자세한 내용은 71-3페이지의 이벤트 보기 설정 구성을/를 참조하십시오.

IOC 작업

라이센스: FireSIGHT

FireSIGHT 시스템은 다양한 유형의 데이터(침입 이벤트, 보안 인텔리전스, 연결 이벤트, 파일 또는 악성코드 이벤트)를 호스트와 연결하여, 모니터링되는 네트워크의 호스트가 악의적인 수단에 감염되었는지를 확인합니다. 이벤트 데이터의 특정 조합 및 빈도는 영향받는 호스트에서 IOC(indications of compromise) 태그를 트리거합니다. IOC 태그의 호스트 IP 주소가 특수한 감염된 호스트 아이콘( )과 함께 이벤트 보기에 나타납니다. IOC 태그 호스트를 설명하는 규정준수 규칙을 작성할 수도 있습니다.

이 기능을 사용하려면 네트워크 검색 규칙에서 IOC 규칙이 활성화되어야 합니다. 감염된 호스트에서 IOC 태그를 트리거하려면 사전 정의된 규칙의 일부 또는 전체를 활성화할 수 있습니다. 자세한 내용은 45-34페이지의 IOC 규칙 설정을/를 참조하십시오.

IOC에 대한 자세한 내용은 다음 절을 참조하십시오.

- 50-32페이지의 IOC 보기
- 50-33페이지의 IOC 테이블 이해
- 50-34페이지의 IOC 검색

IOC 보기

라이센스: FireSIGHT

방어 센터를 사용하면 트리거된 IOC(Indications of Compromise)의 테이블을 볼 수 있습니다. 그런 다음 찾고 있는 정보에 따라 이벤트 보기를 조작할 수 있습니다.

IOC에 액세스할 때 표시되는 페이지는 사용하는 워크플로에 따라 달라집니다. 두 사전 정의 IOC 워크플로 모두 제약 조건을 충족하는 모든 호스트에 대한 호스트 프로필이 포함된 호스트 보기에서 종료됩니다. 특정 요구와 일치하는 정보만 표시하는 사용자 지정 워크플로를 생성할 수도 있습니다. 자세한 내용은 58-38페이지의 사용자 지정 워크플로 생성을/를 참조하십시오.

다음 표에서는 IOC 워크플로 페이지에서 수행할 수 있는 몇 가지 특정 작업에 대해 설명합니다. 공통 검색 이벤트 작업 표에 설명된 작업을 수행할 수도 있습니다.

표 50-7 감염 작업 표시

목적	가능한 작업
테이블에서 열의 내용에 대해 자세히 알아보기	50-33페이지의 IOC 테이블 이해에서 자세히 알아보십시오.
감염된 호스트에 대한 호스트 프로필 보기	**IP Address** 열에서 감염된 호스트 아이콘( )을 클릭합니다.
목록에 더 이상 나타나지 않도록 선택한 IOC 이벤트를 확인된 것으로 표시	수정할 IOC 이벤트 옆에 있는 확인란을 선택한 다음 **Mark Resolved**를 클릭합니다. 자세한 내용은 49-10페이지의 IOC 해결을/를 참조하십시오.
IOC를 트리거한 이벤트의 세부사항 보기	**First Seen** 또는 **Last Seen** 열에서 보기 아이콘( ) 클릭

IOC를 보려면

액세스: Admin/Any Security Analyst

1단계 **Analysis > Hosts > Indications of Compromise**를 선택합니다.

기본 IOC(indications of compromise) 워크플로의 첫 번째 페이지가 나타납니다. 사용자 지정 워크플로를 비롯한 다른 워크플로를 사용하려면 **(switch workflow)**를 클릭합니다. 다른 기본 워크플로 지정에 대한 자세한 내용은 71-3페이지의 이벤트 보기 설정 구성을/를 참조하십시오.

팁 IOC 테이블 보기가 포함되지 않은 사용자 지정 워크플로를 사용 중인 경우 **(switch workflow)**를 클릭한 다음 **Indications of Compromise**를 선택하십시오.

IOC 테이블 이해

라이센스: FireSIGHT

FireSIGHT 시스템은 다양한 유형의 이벤트 데이터를 호스트와 연결하여, 모니터링되는 네트워크의 호스트가 악의적인 수단에 감염되었는지를 확인합니다. 이러한 상관관계는 IOC(indications of compromise)와 같은 호스트와 연결되어 나타납니다. 호스트 IOC를 확인된 것으로 표시할 수 있습니다. 그러면 호스트에서 해당 IOC 태그가 제거됩니다. 호스트는 여러 IOC 태그를 트리거할 수 있습니다. 호스트 프로필의 Indications of Compromise 섹션에서 호스트와 연결된 모든 IOC 태그를 볼 수 있습니다. 호스트 프로필의 IOC 데이터에 대한 자세한 내용은 49-8페이지의 호스트 프로필에서 IOC 작업을/를 참조하십시오.

다음은 IOC 테이블의 필드에 대한 설명입니다.

IP 주소

IOC를 트리거한 호스트와 연결된 IP 주소.

카테고리

표시된 감염 유형에 대한 짧은 설명(예: `Malware Executed` 또는 `Impact 1 Attack`).

이벤트 유형

특정 IOC(Indication of Compromise)와 관련된 식별자로, 이를 트리거한 이벤트를 가리킴.

설명

감염 가능성이 있는 호스트에 대해 IOC가 어떤 의미인지에 대한 설명(예: `This host may be under remote control` 또는 `Malware has been executed on this host`).

First/Last Seen

호스트의 IOC를 트리거하는 이벤트가 발생한 최초의(또는 가장 최근의) 날짜 및 시간.

IOC 검색

라이센스: FireSIGHT

사전 정의된 검색 중 하나를 사용하거나 자체 검색 기준을 사용하여 모니터링되는 호스트에서 트리거된 특정 IOC(indications of compromise) 태그를 검색할 수 있습니다. 사전 정의된 검색은 예제 역할을 하며, 이를 통해 네트워크에 대한 정보에 빠르게 액세스할 수 있습니다.

네트워크 환경에 맞게 맞춤화하기 위해 기본 검색 내에서 특정 필드를 수정한 다음, 나중에 사용할 수 있도록 저장할 수 있습니다. 데이터 검색에 사용할 수 있는 필드는 50-33페이지의 IOC 테이블 이해에서 설명합니다.

일반 검색 구문

각 검색 필드 옆에는 유효한 구문의 예가 표시됩니다. 검색 기준을 입력할 경우, 다음 사항에 유의해야 합니다.

- 모든 필드에 부정(`!`)을 사용할 수 있습니다.
- 모든 필드에 쉼표로 구분된 검색 값의 목록을 사용할 수 있습니다. 지정된 필드에 나열된 값 중 하나를 포함하는 레코드는 검색 기준과 일치합니다.
- 모든 필드에 따옴표로 감싸고 쉼표로 구분한 목록을 검색 값으로 사용할 수 있습니다.
  - 단일 값만을 포함할 수 있는 필드의 경우, 따옴표 내에 지정된 정확한 문자열을 포함하는 지정된 필드의 레코드가 검색 기준과 일치합니다. 예를 들어 `A, B, "C, D, E"`에 대한 검색은 지정된 필드에 `"A"` 또는 `"B"` 또는 `"C, D, E"`가 포함된 레코드와 일치합니다. 따라서 가능한 값으로 쉼표를 포함하는 필드에서 일치를 확인할 수 있습니다.
  - 여러 값을 동시에 포함할 수 있는 필드의 경우, 따옴표로 감싸고 쉼표로 구분한 모든 값을 포함하는 지정된 필드의 레코드가 해당 검색 기준과 일치합니다.
  - 여러 값을 동시에 포함할 수 있는 필드의 경우, 검색 기준에 단일 값은 물론 따옴표로 감싸고 쉼표로 구분한 목록도 포함할 수 있습니다. 예를 들어 하나 이상의 이러한 문자를 포함할 수 있는 필드에서 `A, B, "C, D, E"`에 대한 검색은 지정된 필드에 `A` 또는 `B`, 또는 `C, D, E` 모두가 포함된 레코드와 일치합니다.
- 검색 결과에는 모든 필드에 지정된 검색 기준과 매칭되는 레코드만 반환됩니다.
- 많은 필드에서 와일드카드로 하나 이상의 별표(`*`)를 사용할 수 있습니다.
- 일부 필드의 경우, 해당 필드에 대해 사용할 수 있는 정보가 없는 이벤트를 식별하려면 필드에 `n/a` 또는 `blank`를 지정할 수 있습니다. 해당 필드가 채워지는 이벤트를 식별하려면 `!n/a` 또는 `!blank`를 사용합니다.
- 대부분의 필드에서 대/소문자를 구분합니다.
- IP 주소는 CIDR 표기법으로 지정할 수 있습니다. FireSIGHT 시스템에서 IPv4 및 IPv6 주소를 입력하는 방법에 대한 자세한 내용은 1-19페이지의 IP 주소 표기 규칙을/를 참조하십시오.

- 검색 기준으로 객체를 사용하려면 검색 필드 옆에 나타나는 객체 추가 아이콘(+)을 클릭합니다.

검색에서 객체를 사용하는 방법을 포함하여 검색 구문에 대한 자세한 내용은 60-1페이지의 이벤트 검색을/를 참조하십시오.

IOC를 검색하려면

액세스: Admin/Any Security Analyst

1단계 **Analysis > Search**를 선택합니다.

Search 페이지가 나타납니다.

2단계 테이블 드롭다운 목록에서 **Indications of Compromise**를 선택합니다.

해당 제약 조건으로 페이지가 업데이트됩니다.

팁 데이터베이스에서 서로 다른 종류의 이벤트를 검색하려면 테이블 드롭다운 목록에서 선택합니다.

3단계 50-33페이지의 IOC 테이블 이해에 설명된 대로 해당 필드에 검색 기준을 입력합니다.

여러 필드에 대한 조건을 입력하는 경우 모든 필드에 대해 지정한 검색 기준과 일치하는 레코드만 반환됩니다. 검색 기준으로 객체를 사용하려면 검색 필드 옆에 나타나는 추가 아이콘(+)을 클릭합니다.

4단계 선택적으로, 검색을 저장하려면 **Private** 확인란을 선택하여 자신만 액세스할 수 있는 비공개로 검색을 저장할 수 있습니다. 또는 모든 사용자가 사용할 수 있도록 검색을 저장하려면 확인란을 선택하지 않습니다.

팁 제한된 권한과 함께 사용자 지정 사용자 역할에 대한 제한으로서 검색을 저장하려면 **반드시** 비공개 검색으로 저장해야 합니다.

5단계 선택적으로, 나중에 다시 사용할 수 있도록 검색을 저장할 수 있습니다. 다음 옵션을 이용할 수 있습니다.

- 검색 기준을 저장하려면 **Save**를 클릭합니다.

  새 검색인 경우 검색 이름을 입력하도록 대화 상자가 나타납니다. 고유한 검색 이름을 입력하고 **Save**를 클릭합니다. 이미 존재하는 검색에 대한 새 조건을 저장하는 경우 프롬프트가 나타나지 않습니다. 나중에 실행할 수 있도록 검색이 저장됩니다(**Private**을 선택한 경우 자신만 볼 수 있음).

- 새 검색을 저장하거나, 저장된 기존 검색을 변경하여 만든 검색에 새 이름을 할당하려면 **Save As New**를 클릭합니다.

  검색 이름을 입력하도록 대화 상자가 나타납니다. 고유한 검색 이름을 입력하고 **Save**를 클릭합니다. 나중에 실행할 수 있도록 검색이 저장됩니다(**Private**을 선택한 경우 자신만 볼 수 있음).

6단계 검색을 시작하려면 **Search**를 클릭합니다.

검색 결과는 기본 IOC 워크플로에 나타납니다. 사용자 지정 워크플로를 비롯한 다른 워크플로를 사용하려면 **(switch workflow)**를 클릭합니다. 다른 기본 워크플로 지정에 대한 자세한 내용은 71-3페이지의 이벤트 보기 설정 구성을/를 참조하십시오.

서버 작업

라이센스: FireSIGHT

FireSIGHT 시스템은 모니터링되는 네트워크 세그먼트의 호스트에서 실행 중인 모든 서버에 대한 정보를 수집합니다. 시스템이 수집하는 정보에는 서버의 이름, 서버에서 사용하는 애플리케이션 및 네트워크 프로토콜, 서버의 공급업체 및 버전, 서버를 실행하는 호스트와 연결된 IP 주소, 서버와 통신하는 포트 등이 포함됩니다.

시스템은 서버를 탐지하면, 연결된 호스트가 이미 최대 서버 수에 도달하지 않은 경우 검색 이벤트를 생성합니다. 자세한 내용은 45-14페이지의 호스트 제한 및 검색 이벤트 로깅을/를 참조하십시오. 서버 이벤트를 보고 검색하고 삭제하려면 방어 센터 웹 인터페이스를 사용할 수 있습니다.

상관관계 규칙의 기반을 서버 이벤트에 둘 수도 있습니다. 예를 들어, 시스템이 호스트 중 하나에서 실행 중인 채팅 서버(예: ircd)를 검색할 경우 상관관계 규칙을 트리거할 수 있습니다.

NetFlow 지원 디바이스에서 내보낸 애플리케이션 데이터를 기반으로 네트워크 맵에 서버를 추가하도록 네트워크 검색 정책을 구성할 수 있지만, 이러한 서버에 대해 사용할 수 있는 정보는 제한적입니다. 자세한 내용은 45-17페이지의 NetFlow 및 FireSIGHT 데이터 간 차이점을/를 참조하십시오.

자세한 내용은 다음 절을 참조하십시오.

- 50-36페이지의 서버 보기
- 50-37페이지의 서버 테이블 이해
- 50-39페이지의 서버 검색
- 49-18페이지의 서버 ID 수정

서버 보기

라이센스: FireSIGHT

방어 센터를 사용하면 탐지한 서버의 테이블을 볼 수 있습니다. 그런 다음 찾고 있는 정보에 따라 이벤트 보기를 조작할 수 있습니다.

서버에 액세스할 때 표시되는 페이지는 사용하는 워크플로에 따라 달라집니다. 모든 사전 정의 워크플로는 제약 조건을 충족하는 모든 호스트에 대한 호스트 프로필이 포함된 호스트 보기에서 종료됩니다. 특정 요구와 일치하는 정보만 표시하는 사용자 지정 워크플로를 생성할 수도 있습니다. 자세한 내용은 58-38페이지의 사용자 지정 워크플로 생성을/를 참조하십시오.

아래의 서버 작업 표에서는 서버 워크플로 페이지에서 수행할 수 있는 몇 가지 특정 작업에 대해 설명합니다. 공통 검색 이벤트 작업 표에 설명된 작업을 수행할 수도 있습니다.

표 50-8 서버 작업

목적	가능한 작업
테이블에서 열의 내용에 대해 자세히 알아보기	50-37페이지의 서버 테이블 이해에서 자세히 알아보십시오.
서버 ID 수정	수정할 서버에 대한 이벤트 옆에 있는 확인란을 선택한 다음 **Set Server Identity**를 클릭합니다. 자세한 내용은 49-18페이지의 서버 ID 수정을/를 참조하십시오.

서버를 보려면

액세스: Admin/Any Security Analyst

1단계 **Analysis > Hosts > Servers**를 선택합니다.

기본 서버 워크플로의 첫 번째 페이지가 나타납니다. 사용자 지정 워크플로를 비롯한 다른 워크플로를 사용하려면 **(switch workflow)**를 클릭합니다. 다른 기본 워크플로 지정에 대한 자세한 내용은 71-3페이지의 이벤트 보기 설정 구성을/를 참조하십시오.

팁 서버의 테이블 보기가 포함되지 않은 사용자 지정 워크플로를 사용 중인 경우 **(switch workflow)**를 클릭한 다음 **Servers**를 선택하십시오.

서버 테이블 이해

라이센스: FireSIGHT

FireSIGHT 시스템은 모니터링되는 네트워크 세그먼트의 호스트에서 실행 중인 서버에 대한 정보를 수집합니다.

다음은 서버 테이블의 필드에 대한 설명입니다.

NetFlow 지원 디바이스에서 내보낸 데이터를 기반으로 네트워크 맵에 서버를 추가하도록 네트워크 검색 정책을 구성할 수 있지만, 이러한 서버에 대해 사용할 수 있는 정보는 제한적입니다. 자세한 내용은 45-17페이지의 NetFlow 및 FireSIGHT 데이터 간 차이점을/를 참조하십시오.

Last Used

네트워크에서 서버가 마지막으로 사용된 날짜 및 시간, 또는 호스트 입력 기능을 사용하여 서버가 원래 업데이트된 날짜 및 시간. Last Used 값은 적어도 네트워크 검색 정책에서 구성한 업데이트 간격만큼 그리고 시스템이 서버 정보 업데이트를 탐지할 때 업데이트됩니다. 업데이트 간격 설정에 대한 자세한 내용은 45-35페이지의 데이터 스토리지 구성을/를 참조하십시오.

IP 주소

서버를 실행하는 호스트와 연결된 IP 주소.

포트

서버가 실행 중인 포트.

프로토콜

서버에서 사용하는 네트워크 또는 전송 프로토콜.

Application Protocol

다음 중 하나로 표시되는 애플리케이션 프로토콜:

- 서버에 대한 애플리케이션 프로토콜의 이름
- `pending` - 여러 이유 중 하나 때문에 시스템이 서버를 긍정적으로 또는 부정적으로 식별할 수 없는 경우
- `unknown` - 시스템이 알려진 서버 핑거프린트를 기반으로 서버를 식별할 수 없는 경우 또는 서버가 호스트 입력을 통해 추가되었고 애플리케이션 프로토콜을 포함하지 않은 경우

Category, Tags, Risk, or Business Relevance for Application Protocols

애플리케이션 프로토콜에 할당된 카테고리, 태그, 위험 레벨 및 비즈니스 연관성. 특정 데이터 집합에 집중하려면 이러한 필터를 사용할 수 있습니다. 자세한 내용은 45-11 페이지의 표 45-2을/를 참조하십시오.

벤더

다음 중 하나:

- 시스템, Nmap, 다른 활성 소스 등에 의해 식별된 서버 공급업체 또는 호스트 입력 기능을 사용하여 지정한 서버 공급업체
- blank - 시스템이 알려진 서버 핑거프린트를 기반으로 공급업체를 식별할 수 없는 경우 또는 NetFlow 데이터를 사용하여 서버가 네트워크 맵에 추가된 경우

버전

다음 중 하나:

- 시스템, Nmap, 다른 활성 소스 등에 의해 식별된 서버 공급업체 또는 호스트 입력 기능을 사용하여 지정한 서버 버전
- blank - 시스템이 알려진 서버 핑거프린트를 기반으로 버전을 식별할 수 없는 경우 또는 NetFlow 데이터를 사용하여 서버가 네트워크 맵에 추가된 경우

웹 애플리케이션

http 트래픽에서 시스템에 의해 탐지된 페이로드 내용을 기반으로 하는 웹 애플리케이션. `HTTP`의 애플리케이션 프로토콜은 탐지하지만 특정 웹 애플리케이션은 탐지하지 못하는 경우 시스템은 일반 웹 브라우징 지정을 제공합니다.

Category, Tags, Risk, or Business Relevance for Web Applications

웹 애플리케이션에 할당된 카테고리, 태그, 위험 레벨 및 비즈니스 연관성. 특정 데이터 집합에 집중하려면 이러한 필터를 사용할 수 있습니다. 자세한 내용은 45-11 페이지의 표 45-2을/를 참조하십시오.

Hits

서버에 액세스한 횟수. 호스트 입력 기능을 사용하여 추가된 서버의 경우 이 값은 항상 0입니다.

Source Type

다음 값 중 하나:

- 사용자: *`user_name`*
- 애플리케이션: *`app_name`*
- 스캐너: *`scanner_type`*(네트워크 검색 컨피그레이션을 통해 추가된 Nmap 또는 스캐너)
- FireSIGHT, FireSIGHT Port Match 또는 FireSIGHT Pattern Match - FireSIGHT 시스템에 의해 탐지된 서버의 경우
- NetFlow - NetFlow 데이터 기반의 네트워크 맵에 추가된 서버의 경우

시스템에서는 서버의 ID를 확인하기 위해 여러 소스의 데이터를 조정할 수 있습니다. 46-5페이지의 현재 ID 이해을/를 참조하십시오.

디바이스

서버를 탐지한 디바이스, 또는 네트워크 맵에 서버를 추가한 호스트 입력 데이터나 NetFlow를 처리한 디바이스의 이름.

현재 사용자

현재 호스트에 로그인한 사용자의 사용자 ID(사용자 이름).

권한 없는 사용자가 호스트에 로그인하면 해당 로그인은 사용자 및 호스트 내역에 기록됩니다. 호스트와 연결된 권한 있는 사용자가 없는 경우, 권한 없는 사용자가 호스트의 현재 사용자가 될 수 있습니다. 그러나 권한 있는 사용자가 호스트에 로그인한 후에는 또 다른 권한 있는 사용자의 로그인에 의해서만 현재 사용자가 변경됩니다. 또한 권한 없는 사용자가 호스트의 현재 사용자인 경우, 해당 사용자를 사용자 제어에 사용할 수 없습니다.

개수

각 행에 표시되는 정보와 매칭되는 이벤트의 수. 둘 이상의 동일한 행을 생성하는 제약 조건을 적용한 경우에만 Count 필드가 나타납니다.

서버 검색

라이센스: FireSIGHT

사전 정의된 검색 중 하나를 사용하거나 자체 검색 기준을 사용하여, 모니터링되는 호스트에서 실행 중인 특정 서버를 검색할 수 있습니다. 사전 정의된 검색은 예제 역할을 하며, 이를 통해 네트워크에 대한 정보에 빠르게 액세스할 수 있습니다.

네트워크 환경에 맞게 맞춤화하기 위해 기본 검색 내에서 특정 필드를 수정한 다음, 나중에 사용할 수 있도록 저장할 수 있습니다. 데이터 검색에 사용할 수 있는 필드는 50-37페이지의 서버 테이블 이해에서 설명합니다.

서버를 검색할 때에는, NetFlow 지원 디바이스에서 내보낸 데이터를 기반으로 네트워크 맵에 애플리케이션(서버 포함)을 추가하도록 네트워크 검색 정책을 구성할 수 있지만 이러한 서버에 대해 사용할 수 있는 정보는 제한적이라는 점을 염두에 두어야 합니다. 자세한 내용은 45-17페이지의 NetFlow 및 FireSIGHT 데이터 간 차이점을/를 참조하십시오.

일반 검색 구문

각 검색 필드 옆에는 유효한 구문의 예가 표시됩니다. 검색 기준을 입력할 경우, 다음 사항에 유의해야 합니다.

- 모든 필드에 부정(!)을 사용할 수 있습니다.
- 모든 필드에 쉼표로 구분된 검색 값의 목록을 사용할 수 있습니다. 지정된 필드에 나열된 값 중 하나를 포함하는 레코드는 검색 기준과 일치합니다.
- 모든 필드에 따옴표로 감싸고 쉼표로 구분한 목록을 검색 값으로 사용할 수 있습니다.
  - 단일 값만을 포함할 수 있는 필드의 경우, 따옴표 내에 지정된 정확한 문자열을 포함하는 지정된 필드의 레코드가 검색 기준과 일치합니다. 예를 들어 `A, B, "C, D, E"`에 대한 검색은 지정된 필드에 `"A"` 또는 `"B"` 또는 `"C, D, E"`가 포함된 레코드와 일치합니다. 따라서 가능한 값으로 쉼표를 포함하는 필드에서 일치를 확인할 수 있습니다.
  - 여러 값을 동시에 포함할 수 있는 필드의 경우, 따옴표로 감싸고 쉼표로 구분한 모든 값을 포함하는 지정된 필드의 레코드가 해당 검색 기준과 일치합니다.
  - 여러 값을 동시에 포함할 수 있는 필드의 경우, 검색 기준에 단일 값은 물론 따옴표로 감싸고 쉼표로 구분한 목록도 포함할 수 있습니다. 예를 들어 하나 이상의 이러한 문자를 포함할 수 있는 필드에서 `A, B, "C, D, E"`에 대한 검색은 지정된 필드에 `A` 또는 `B`, 또는 `C, D, E` 모두가 포함된 레코드와 일치합니다.
- 검색 결과에는 모든 필드에 지정된 검색 기준과 매칭되는 레코드만 반환됩니다.
- 많은 필드에서 와일드카드로 하나 이상의 별표(*)를 사용할 수 있습니다.

- 일부 필드의 경우, 해당 필드에 대해 사용할 수 있는 정보가 없는 이벤트를 식별하려면 필드에 `n/a` 또는 `blank`를 지정할 수 있습니다. 해당 필드가 채워지는 이벤트를 식별하려면 `!n/a` 또는 `!blank`를 사용합니다.
- 대부분의 필드에서 대/소문자를 구분합니다.
- IP 주소는 CIDR 표기법으로 지정할 수 있습니다. FireSIGHT 시스템에서 IPv4 및 IPv6 주소를 입력하는 방법에 대한 자세한 내용은 1-19페이지의 IP 주소 표기 규칙을/를 참조하십시오.
- 특정 디바이스 및 그룹, 스택 또는 클러스터의 디바이스를 검색하려면 디바이스 필드를 사용합니다. FireSIGHT 시스템에서 검색 시 디바이스 필드를 취급하는 방법에 대한 자세한 내용은 60-7페이지의 검색에서 디바이스 지정을/를 참조하십시오.
- 검색 기준으로 객체를 사용하려면 검색 필드 옆에 나타나는 객체 추가 아이콘(+)을 클릭합니다.

검색에서 객체를 사용하는 방법을 포함하여 검색 구문에 대한 자세한 내용은 60-1페이지의 이벤트 검색을/를 참조하십시오.

서버를 검색하려면

액세스: Admin/Any Security Analyst

1단계 **Analysis > Search**를 선택합니다.

Search 페이지가 나타납니다.

2단계 테이블 드롭다운 목록에서 **Servers**를 선택합니다.

해당 제약 조건으로 페이지가 업데이트됩니다.

팁 데이터베이스에서 서로 다른 종류의 이벤트를 검색하려면 테이블 드롭다운 목록에서 선택합니다.

3단계 해당 필드에 검색 기준을 입력합니다.

여러 필드에 대한 조건을 입력하는 경우 모든 필드에 대해 지정한 검색 기준과 일치하는 레코드만 반환됩니다. 검색 기준으로 객체를 사용하려면 검색 필드 옆에 나타나는 추가 아이콘(+)을 클릭합니다.

4단계 선택적으로, 검색을 저장하려면 **Private** 확인란을 선택하여 자신만 액세스할 수 있는 비공개로 검색을 저장할 수 있습니다. 또는 모든 사용자가 사용할 수 있도록 검색을 저장하려면 확인란을 선택하지 않습니다.

팁 제한된 권한과 함께 사용자 지정 사용자 역할에 대한 제한으로서 검색을 저장하려면 **반드시** 비공개 검색으로 저장해야 합니다.

5단계 선택적으로, 나중에 다시 사용할 수 있도록 검색을 저장할 수 있습니다. 다음 옵션을 이용할 수 있습니다.

- 검색 기준을 저장하려면 **Save**를 클릭합니다.

  새 검색인 경우 검색 이름을 입력하도록 대화 상자가 나타납니다. 고유한 검색 이름을 입력하고 **Save**를 클릭합니다. 이미 존재하는 검색에 대한 새 조건을 저장하는 경우 프롬프트가 나타나지 않습니다. 나중에 실행할 수 있도록 검색이 저장됩니다(**Private**을 선택한 경우 자신만 볼 수 있음).
- 새 검색을 저장하거나, 저장된 기존 검색을 변경하여 만든 검색에 새 이름을 할당하려면 **Save As New**를 클릭합니다.

검색 이름을 입력하도록 대화 상자가 나타납니다. 고유한 검색 이름을 입력하고 **Save**를 클릭합니다. 나중에 실행할 수 있도록 검색이 저장됩니다(**Private**을 선택한 경우 자신만 볼 수 있음).

6단계 검색을 시작하려면 **Search**를 클릭합니다.

검색 결과는 기본 서버 워크플로에 나타납니다. 사용자 지정 워크플로를 비롯한 다른 워크플로를 사용하려면 **(switch workflow)**를 클릭합니다. 다른 기본 워크플로 지정에 대한 자세한 내용은 71-3페이지의 이벤트 보기 설정 구성을/를 참조하십시오.

애플리케이션 작업

라이센스: FireSIGHT

모니터링되는 호스트가 다른 호스트에 연결되면, 시스템은 많은 경우 어떤 애플리케이션이 사용되었는지를 확인할 수 있습니다. FireSIGHT 시스템에서는 이메일, 인스턴트 메시징, 피어 투 피어, 웹 애플리케이션 및 기타 유형의 애플리케이션 사용을 탐지합니다.

탐지된 각 애플리케이션에 대해 시스템은 애플리케이션을 사용한 IP 주소, 제품, 버전, 탐지된 사용 횟수 등을 기록합니다. 애플리케이션 이벤트를 보고 검색하고 삭제하려면 웹 인터페이스를 사용할 수 있습니다. 또한 호스트 입력 기능을 사용하여 호스트의 애플리케이션 데이터를 업데이트할 수 있습니다.

어떤 애플리케이션이 어떤 호스트에서 실행 중인지 안다면, 이를 통해 호스트 프로필 자격을 생성할 수 있습니다. 이러한 특성은 트래픽 프로필 작성 중에 수집하는 데이터를 제한하며, 상관관계 규칙을 트리거할 조건을 제한할 수도 있습니다. 상관관계 규칙의 기반을 애플리케이션 탐지에 둘 수도 있습니다. 예를 들어 직원이 특정 메일 클라이언트를 사용하도록 하려면, 호스트 중 하나에서 다른 메일 클라이언트가 실행 중임을 시스템에서 탐지할 때 상관관계 규칙을 트리거할 수 있습니다.

각 FireSIGHT 시스템 업데이트에 대한 릴리스 정보는 물론 업데이트된 탐지기 정보의 각 VDB 업데이트에 대한 자문 내용도 주의 깊게 읽어야 합니다.

분석용 애플리케이션 데이터를 수집 및 저장하려면 네트워크 검색 정책에서 애플리케이션 탐지를 활성화하십시오. 자세한 내용은 45-1페이지의 검색 데이터 수집 이해을/를 참조하십시오.

자세한 내용은 다음 절을 참조하십시오.

- 50-46페이지의 애플리케이션 세부사항 보기
- 50-46페이지의 애플리케이션 세부사항 테이블 이해
- 50-48페이지의 애플리케이션 세부사항 검색

애플리케이션 보기

라이센스: FireSIGHT

방어 센터를 사용하면 탐지한 애플리케이션의 테이블을 볼 수 있습니다. 그런 다음 찾고 있는 정보에 따라 이벤트 보기를 조작할 수 있습니다.

애플리케이션에 액세스할 때 표시되는 페이지는 사용하는 워크플로에 따라 달라집니다. 특정 요구와 일치하는 정보만 표시하는 사용자 지정 워크플로를 생성할 수도 있습니다. 자세한 내용은 58-38페이지의 사용자 지정 워크플로 생성을/를 참조하십시오.

아래의 애플리케이션 작업 표에서는 애플리케이션 워크플로 페이지에서 수행할 수 있는 몇 가지 특정 작업에 대해 설명합니다. 공통 검색 이벤트 작업 표에 설명된 작업을 수행할 수도 있습니다.

표 50-9 애플리케이션 작업

목적	가능한 작업
테이블에서 열의 내용에 대해 자세히 알아보기	50-42페이지의 애플리케이션 테이블 이해에서 자세히 알아보십시오.
특정 애플리케이션에 대한 애플리케이션 세부사항 보기 열기	클라이언트, 애플리케이션 프로토콜 또는 웹 애플리케이션 옆에 있는 애플리케이션 세부사항 보기 아이콘( )을 클릭합니다.

애플리케이션을 보려면

액세스: Admin/Any Security Analyst

1단계 **Analysis > Hosts > Application Details**를 선택합니다.

기본 애플리케이션 세부사항 워크플로의 첫 번째 페이지가 나타납니다. 사용자 지정 워크플로를 비롯한 다른 워크플로를 사용하려면 **(switch workflow)**를 클릭합니다. 다른 기본 워크플로 지정에 대한 자세한 내용은 71-3페이지의 이벤트 보기 설정 구성을/를 참조하십시오.

팁 애플리케이션 세부사항의 테이블 보기가 포함되지 않은 사용자 지정 워크플로를 사용 중인 경우 **(switch workflow)**를 클릭한 다음 **Clients**를 선택하십시오.

애플리케이션 테이블 이해

라이센스: FireSIGHT

모니터링되는 호스트가 다른 호스트에 연결되면, FireSIGHT 시스템은 많은 경우 어떤 애플리케이션이 사용되었는지를 확인할 수 있습니다. 시스템은 다양한 웹 브라우저나 서버, 이메일 클라이언트나 서버, 인스턴트 메신저, 피어 투 피어 애플리케이션 등을 탐지합니다. 알려진 클라이언트, 애플리케이션 프로토콜 또는 웹 애플리케이션에 대한 트래픽을 탐지하면 시스템은 애플리케이션 및 이를 실행하는 호스트에 대한 정보를 기록합니다.

FireSIGHT 시스템은 애플리케이션 데이터를 클라이언트, 웹 애플리케이션 및 웹 프로토콜의 세 유형으로 분류합니다. 애플리케이션 테이블은 어플라이언스에서 탐지된 세 가지 유형의 애플리케이션을 모두 결합하는 목록을 제공합니다.

다음은 애플리케이션 테이블의 필드에 대한 설명입니다.

Application

탐지된 애플리케이션의 이름

IP Address

애플리케이션을 사용하는 호스트와 연결된 IP 주소

Category

가장 중요한 기능을 설명하는 일반 애플리케이션 분류. 각 애플리케이션은 적어도 하나의 카테고리에 속합니다.

Tag

애플리케이션에 대한 추가 정보. 애플리케이션에는 0부터 원하는 수만큼의 태그를 포함할 수 있습니다.

Risk

조직의 보안 정책을 거스를 수 있는 용도로 애플리케이션이 사용될 가능성. 애플리케이션 위험의 범위는 `Very Low`에서 `Very High`까지입니다.

침입 이벤트를 트리거한 트래픽에서 탐지된 Application Protocol Risk, Client Risk, Web Application Risk의 세 가지 중 최고(사용 가능한 경우).

Business Relevance

조직의 비즈니스 운영(레크리에이션과 반대) 컨텍스트 내에서 애플리케이션이 사용될 가능성. 애플리케이션 비즈니스 연관성의 범위는 `Very Low`에서 `Very High`까지입니다.

침입 이벤트를 트리거한 트래픽에서 탐지된 Application Protocol Business Relevance, Client Business Relevance, Web Application Business Relevance의 세 가지 중 최저(사용 가능한 경우).

Current User

현재 호스트에 로그인한 사용자의 사용자 ID(사용자 이름).

권한 없는 사용자가 호스트에 로그인하면 해당 로그인은 사용자 및 호스트 내역에 기록됩니다. 호스트와 연결된 권한 있는 사용자가 없는 경우, 권한 없는 사용자가 호스트의 현재 사용자가 될 수 있습니다. 그러나 권한 있는 사용자가 호스트에 로그인한 후에는 또 다른 권한 있는 사용자의 로그인에 의해서만 현재 사용자가 변경됩니다. 또한 권한 없는 사용자가 호스트의 현재 사용자인 경우, 해당 사용자를 사용자 제어에 사용할 수 없습니다.

Type

애플리케이션 유형:

- **Application Protocols** - 호스트 간 통신을 나타냅니다.
- **Client Applications** - 호스트에서 실행 중인 소프트웨어를 나타냅니다.
- **Web Applications** - HTTP 트래픽에 대한 콘텐츠 또는 요청 URL을 나타냅니다.

Count

각 행에 표시되는 정보와 매칭되는 이벤트의 수. 둘 이상의 동일한 행을 생성하는 제약 조건을 적용한 경우에만 Count 필드가 나타납니다.

애플리케이션 검색

라이센스: FireSIGHT

특정 클라이언트, 애플리케이션 프로토콜 또는 웹 애플리케이션을 실행 중인 호스트를 검색할 수 있습니다. 네트워크 환경에 맞춤화된 검색을 생성한 다음 나중에 다시 사용할 수 있도록 저장할 수 있습니다.

일반 검색 구문

각 검색 필드 옆에는 유효한 구문의 예가 표시됩니다. 검색 기준을 입력할 경우, 다음 사항에 유의해야 합니다.

- 모든 필드에 부정(`!`)을 사용할 수 있습니다.

- 모든 필드에 쉼표로 구분된 검색 값의 목록을 사용할 수 있습니다. 지정된 필드에 나열된 값 중 하나를 포함하는 레코드는 검색 기준과 일치합니다.
- 모든 필드에 따옴표로 감싸고 쉼표로 구분한 목록을 검색 값으로 사용할 수 있습니다.
  - 단일 값만을 포함할 수 있는 필드의 경우, 따옴표 내에 지정된 정확한 문자열을 포함하는 지정된 필드의 레코드가 검색 기준과 일치합니다. 예를 들어 `A, B, "C, D, E"`에 대한 검색은 지정된 필드에 `"A"` 또는 `"B"` 또는 `"C, D, E"`가 포함된 레코드와 일치합니다. 따라서 가능한 값으로 쉼표를 포함하는 필드에서 일치를 확인할 수 있습니다.
  - 여러 값을 동시에 포함할 수 있는 필드의 경우, 따옴표로 감싸고 쉼표로 구분한 모든 값을 포함하는 지정된 필드의 레코드가 해당 검색 기준과 일치합니다.
  - 여러 값을 동시에 포함할 수 있는 필드의 경우, 검색 기준에 단일 값은 물론 따옴표로 감싸고 쉼표로 구분한 목록도 포함할 수 있습니다. 예를 들어 하나 이상의 이러한 문자를 포함할 수 있는 필드에서 `A, B, "C, D, E"`에 대한 검색은 지정된 필드에 `A` 또는 `B`, 또는 `C, D, E` 모두가 포함된 레코드와 일치합니다.
- 검색 결과에는 모든 필드에 지정된 검색 기준과 매칭되는 레코드만 반환됩니다.
- 많은 필드에서 와일드카드로 하나 이상의 별표(*)를 사용할 수 있습니다.
- 일부 필드의 경우, 해당 필드에 대해 사용할 수 있는 정보가 없는 이벤트를 식별하려면 필드에 `n/a` 또는 `blank`를 지정할 수 있습니다. 해당 필드가 채워지는 이벤트를 식별하려면 `!n/a` 또는 `!blank`를 사용합니다.
- 대부분의 필드에서 대/소문자를 구분합니다.
- IP 주소는 CIDR 표기법으로 지정할 수 있습니다. FireSIGHT 시스템에서 IPv4 및 IPv6 주소를 입력하는 방법에 대한 자세한 내용은 1-19페이지의 IP 주소 표기 규칙을/를 참조하십시오.
- 검색 기준으로 객체를 사용하려면 검색 필드 옆에 나타나는 객체 추가 아이콘(+)을 클릭합니다.

검색에서 객체를 사용하는 방법을 포함하여 검색 구문에 대한 자세한 내용은 60-1페이지의 이벤트 검색을/를 참조하십시오.

애플리케이션을 검색하려면

액세스: Admin/Any Security Analyst

1단계 **Analysis > Search**를 선택합니다.

Search 페이지가 나타납니다.

2단계 테이블 드롭다운 목록에서 **Applications**를 선택합니다.

해당 제약 조건으로 페이지가 업데이트됩니다.

3단계 해당 필드에 검색 기준을 입력합니다.

여러 필드에 대한 조건을 입력하는 경우 모든 필드에 대해 지정한 검색 기준과 일치하는 레코드만 반환됩니다. 검색 기준으로 객체를 사용하려면 검색 필드 옆에 나타나는 추가 아이콘(+)을 클릭합니다.

4단계 선택적으로, 검색을 저장하려면 **Private** 확인란을 선택하여 자신만 액세스할 수 있는 비공개로 검색을 저장할 수 있습니다. 또는 모든 사용자가 사용할 수 있도록 검색을 저장하려면 확인란을 선택하지 않습니다.

팁 제한된 권한과 함께 사용자 지정 사용자 역할에 대한 제한으로서 검색을 저장하려면 **반드시** 비공개 검색으로 저장해야 합니다.

5단계 선택적으로, 나중에 다시 사용할 수 있도록 검색을 저장할 수 있습니다. 다음 옵션을 이용할 수 있습니다.

- 검색 기준을 저장하려면 **Save**를 클릭합니다.

  새 검색인 경우 검색 이름을 입력하도록 대화 상자가 나타납니다. 고유한 검색 이름을 입력하고 **Save**를 클릭합니다. 이미 존재하는 검색에 대한 새 조건을 저장하는 경우 프롬프트가 나타나지 않습니다. 나중에 실행할 수 있도록 검색이 저장됩니다(**Private**을 선택한 경우 자신만 볼 수 있음).

- 새 검색을 저장하거나, 저장된 기존 검색을 변경하여 만든 검색에 새 이름을 할당하려면 **Save As New**를 클릭합니다.

  검색 이름을 입력하도록 대화 상자가 나타납니다. 고유한 검색 이름을 입력하고 **Save**를 클릭합니다. 나중에 실행할 수 있도록 검색이 저장됩니다(**Private**을 선택한 경우 자신만 볼 수 있음).

6단계 검색을 시작하려면 **Search**를 클릭합니다.

검색 결과는 기본 클라이언트 워크플로에 나타납니다. 사용자 지정 워크플로를 비롯한 다른 워크플로를 사용하려면 **(switch workflow)**를 클릭합니다. 다른 기본 워크플로 지정에 대한 자세한 내용은 71-3페이지의 이벤트 보기 설정 구성을/를 참조하십시오.

애플리케이션 세부사항 작업

라이센스: FireSIGHT

모니터링되는 호스트가 다른 호스트에 연결되면, 시스템은 많은 경우 어떤 애플리케이션이 사용되었는지를 확인할 수 있습니다. FireSIGHT 시스템에서는 이메일, 인스턴트 메시징, 피어 투 피어, 웹 애플리케이션 및 기타 유형의 애플리케이션 사용을 탐지합니다.

탐지된 각 애플리케이션에 대해 시스템은 애플리케이션을 사용한 IP 주소, 제품, 버전, 탐지된 사용 횟수 등을 기록합니다. 애플리케이션 이벤트를 보고 검색하고 삭제하려면 웹 인터페이스를 사용할 수 있습니다. 또한 호스트 입력 기능을 사용하여 호스트의 애플리케이션 데이터를 업데이트할 수 있습니다.

어떤 애플리케이션이 어떤 호스트에서 실행 중인지 안다면, 이를 통해 호스트 프로필 자격을 생성할 수 있습니다. 이러한 특성은 트래픽 프로필 작성 중에 수집하는 데이터를 제한하며, 상관관계 규칙을 트리거할 조건을 제한할 수도 있습니다. 상관관계 규칙의 기반을 애플리케이션 탐지에 둘 수도 있습니다. 예를 들어 직원이 특정 메일 클라이언트를 사용하도록 하려면, 호스트 중 하나에서 다른 메일 클라이언트가 실행 중임을 시스템에서 탐지할 때 상관관계 규칙을 트리거할 수 있습니다.

각 FireSIGHT 시스템 업데이트에 대한 릴리스 정보는 물론 업데이트된 탐지기 정보의 각 VDB 업데이트에 대한 자문 내용도 주의 깊게 읽어야 합니다.

분석용 애플리케이션 데이터를 수집 및 저장하려면 네트워크 검색 정책에서 애플리케이션 탐지를 활성화하십시오. 자세한 내용은 45-10페이지의 애플리케이션 탐지 이해을/를 참조하십시오.

자세한 내용은 다음 절을 참조하십시오.

- 50-46페이지의 애플리케이션 세부사항 보기
- 50-46페이지의 애플리케이션 세부사항 테이블 이해
- 50-48페이지의 애플리케이션 세부사항 검색

애플리케이션 세부사항 보기

라이센스: FireSIGHT

방어 센터를 사용하면 탐지한 애플리케이션 세부사항의 테이블을 볼 수 있습니다. 그런 다음 찾고 있는 정보에 따라 이벤트 보기를 조작할 수 있습니다.

애플리케이션 세부사항에 액세스할 때 표시되는 페이지는 사용하는 워크플로에 따라 달라집니다. 두 가지 사전 정의 워크플로가 있습니다. 특정 요구와 일치하는 정보만 표시하는 사용자 지정 워크플로를 생성할 수도 있습니다. 자세한 내용은 58-38페이지의 사용자 지정 워크플로 생성을/를 참조하십시오.

아래의 애플리케이션 세부사항 작업 표에서는 애플리케이션 세부사항 워크플로 페이지에서 수행할 수 있는 몇 가지 특정 작업에 대해 설명합니다. 공통 검색 이벤트 작업 표에 설명된 작업을 수행할 수도 있습니다.

표 50-10 애플리케이션 세부사항 작업

목적	가능한 작업
테이블에서 열의 내용에 대해 자세히 알아보기	50-46페이지의 애플리케이션 세부사항 테이블 이해에서 자세히 알아보십시오.
특정 애플리케이션에 대한 애플리케이션 세부사항 보기 열기	클라이언트 옆에 있는 애플리케이션 세부사항 보기 아이콘( )을 클릭합니다.

애플리케이션 세부사항을 보려면

액세스: Admin/Any Security Analyst

1단계 **Analysis > Hosts > Application Details**를 선택합니다.

기본 애플리케이션 세부사항 워크플로의 첫 번째 페이지가 나타납니다. 사용자 지정 워크플로를 비롯한 다른 워크플로를 사용하려면 **(switch workflow)**를 클릭합니다. 다른 기본 워크플로 지정에 대한 자세한 내용은 71-3페이지의 이벤트 보기 설정 구성을/를 참조하십시오.

팁 애플리케이션 세부사항의 테이블 보기가 포함되지 않은 사용자 지정 워크플로를 사용 중인 경우 **(switch workflow)**를 클릭한 다음 **Clients**를 선택하십시오.

애플리케이션 세부사항 테이블 이해

라이센스: FireSIGHT

모니터링되는 호스트가 다른 호스트에 연결되면, FireSIGHT 시스템은 많은 경우 어떤 애플리케이션이 사용되었는지를 확인할 수 있습니다. 시스템은 다양한 웹 브라우저, 이메일 클라이언트, 인스턴트 메신저, 피어 투 피어 애플리케이션 등을 탐지합니다

알려진 클라이언트, 애플리케이션 프로토콜 또는 웹 애플리케이션에 대한 트래픽을 탐지하면 시스템은 애플리케이션 및 이를 실행하는 호스트에 대한 정보를 기록합니다. 다음은 애플리케이션 세부사항 테이블의 필드에 대한 설명입니다.

Last Used

애플리케이션이 마지막으로 사용된 시간 또는 호스트 입력 기능을 사용하여 애플리케이션 데이터가 업데이트된 시간. Last Used 값은 적어도 네트워크 검색 정책에서 구성한 업데이트 간격만큼 그리고 시스템이 애플리케이션 정보 업데이트를 탐지할 때 업데이트됩니다. 업데이트 간격 설정에 대한 자세한 내용은 45-35페이지의 데이터 스토리지 구성을/를 참조하십시오.

IP Address

애플리케이션을 사용하는 호스트와 연결된 IP 주소

Client

애플리케이션의 이름. 시스템이 애플리케이션 프로토콜을 탐지했지만 특정 클라이언트를 탐지하지 못한 경우, 일반 이름을 제공하기 위해 애플리케이션 프로토콜 이름에 `client`가 첨부됩니다.

Version

애플리케이션의 버전

Category, Tags, Risk, or Business Relevance for Clients, Application Protocols, and Web Applications

애플리케이션에 할당된 카테고리, 태그, 위험 레벨 및 비즈니스 연관성. 특정 데이터 집합에 집중하려면 이러한 필터를 사용할 수 있습니다. 자세한 내용은 45-11 페이지의 표 45-2을/를 참조하십시오.

Application Protocol

애플리케이션에서 사용하는 애플리케이션 프로토콜. 시스템이 애플리케이션 프로토콜을 탐지했지만 특정 클라이언트를 탐지하지 못한 경우, 일반 이름을 제공하기 위해 애플리케이션 프로토콜 이름에 `client`가 첨부됩니다.

Web Application

http 트래픽에서 시스템에 의해 탐지된 페이로드 내용 또는 URL을 기반으로 하는 웹 애플리케이션. `HTTP`의 애플리케이션 프로토콜은 탐지하지만 특정 웹 애플리케이션은 탐지하지 못하는 경우 시스템은 여기에서 일반 웹 브라우징 지정을 제공합니다.

Hits

시스템이 사용 중인 애플리케이션을 탐지한 횟수. 호스트 입력 기능을 사용하여 추가된 애플리케이션의 경우 이 값은 항상 `0`입니다.

Device

애플리케이션 세부사항을 포함하는 검색 이벤트를 생성한 디바이스

Current User

현재 호스트에 로그인한 사용자의 사용자 ID(사용자 이름).

권한 없는 사용자가 호스트에 로그인하면 해당 로그인은 사용자 및 호스트 내역에 기록됩니다. 호스트와 연결된 권한 있는 사용자가 없는 경우, 권한 없는 사용자가 호스트의 현재 사용자가 될 수 있습니다. 그러나 권한 있는 사용자가 호스트에 로그인한 후에는 또 다른 권한 있는 사용자의 로그인에 의해서만 현재 사용자가 변경됩니다. 또한 권한 없는 사용자가 호스트의 현재 사용자인 경우, 해당 사용자를 사용자 제어에 사용할 수 없습니다.

Count

각 행에 표시되는 정보와 매칭되는 이벤트의 수. 둘 이상의 동일한 행을 생성하는 제약 조건을 적용한 경우에만 Count 필드가 나타납니다.

애플리케이션 세부사항 검색

라이센스: FireSIGHT

특정 클라이언트, 애플리케이션 프로토콜 또는 웹 애플리케이션을 실행 중인 호스트를 검색할 수 있습니다. 네트워크 환경에 맞춤화된 검색을 생성한 다음 나중에 다시 사용할 수 있도록 저장할 수 있습니다.

일반 검색 구문

각 검색 필드 옆에는 유효한 구문의 예가 표시됩니다. 검색 기준을 입력할 경우, 다음 사항에 유의해야 합니다.

- 모든 필드에 부정(!)을 사용할 수 있습니다.
- 모든 필드에 쉼표로 구분된 검색 값의 목록을 사용할 수 있습니다. 지정된 필드에 나열된 값 중 하나를 포함하는 레코드는 검색 기준과 일치합니다.
- 모든 필드에 따옴표로 감싸고 쉼표로 구분한 목록을 검색 값으로 사용할 수 있습니다.
  - 단일 값만을 포함할 수 있는 필드의 경우, 따옴표 내에 지정된 정확한 문자열을 포함하는 지정된 필드의 레코드가 검색 기준과 일치합니다. 예를 들어 `A, B, "C, D, E"`에 대한 검색은 지정된 필드에 `"A"` 또는 `"B"` 또는 `"C, D, E"`가 포함된 레코드와 일치합니다. 따라서 가능한 값으로 쉼표를 포함하는 필드에서 일치를 확인할 수 있습니다.
  - 여러 값을 동시에 포함할 수 있는 필드의 경우, 따옴표로 감싸고 쉼표로 구분한 모든 값을 포함하는 지정된 필드의 레코드가 해당 검색 기준과 일치합니다.
  - 여러 값을 동시에 포함할 수 있는 필드의 경우, 검색 기준에 단일 값은 물론 따옴표로 감싸고 쉼표로 구분한 목록도 포함할 수 있습니다. 예를 들어 하나 이상의 이러한 문자를 포함할 수 있는 필드에서 `A, B, "C, D, E"`에 대한 검색은 지정된 필드에 `A` 또는 `B`, 또는 `C, D, E` 모두가 포함된 레코드와 일치합니다.
- 검색 결과에는 모든 필드에 지정된 검색 기준과 매칭되는 레코드만 반환됩니다.
- 많은 필드에서 와일드카드로 하나 이상의 별표(*)를 사용할 수 있습니다.
- 일부 필드의 경우, 해당 필드에 대해 사용할 수 있는 정보가 없는 이벤트를 식별하려면 필드에 `n/a` 또는 `blank`를 지정할 수 있습니다. 해당 필드가 채워지는 이벤트를 식별하려면 `!n/a` 또는 `!blank`를 사용합니다.
- 대부분의 필드에서 대/소문자를 구분합니다.
- IP 주소는 CIDR 표기법으로 지정할 수 있습니다. FireSIGHT 시스템에서 IPv4 및 IPv6 주소를 입력하는 방법에 대한 자세한 내용은 1-19페이지의 IP 주소 표기 규칙을/를 참조하십시오.
- 특정 디바이스 및 그룹, 스택 또는 클러스터의 디바이스를 검색하려면 디바이스 필드를 사용합니다. FireSIGHT 시스템에서 검색 시 디바이스 필드를 취급하는 방법에 대한 자세한 내용은 60-7페이지의 검색에서 디바이스 지정을/를 참조하십시오.
- 검색 기준으로 객체를 사용하려면 검색 필드 옆에 나타나는 객체 추가 아이콘(✚)을 클릭합니다.

검색에서 객체를 사용하는 방법을 포함하여 검색 구문에 대한 자세한 내용은 60-1페이지의 이벤트 검색을/를 참조하십시오.

애플리케이션 세부사항을 검색하려면

액세스: Admin/Any Security Analyst

1단계 **Analysis > Search**를 선택합니다.

Search 페이지가 나타납니다.

2단계 테이블 드롭다운 목록에서 **Application Details**를 선택합니다.

해당 제약 조건으로 페이지가 업데이트됩니다.

팁 데이터베이스에서 서로 다른 종류의 이벤트를 검색하려면 테이블 드롭다운 목록에서 선택합니다.

3단계 해당 필드에 검색 기준을 입력합니다.

여러 필드에 대한 조건을 입력하는 경우 모든 필드에 대해 지정한 검색 기준과 일치하는 레코드만 반환됩니다. 검색 기준으로 객체를 사용하려면 검색 필드 옆에 나타나는 추가 아이콘(+)을 클릭합니다.

4단계 선택적으로, 검색을 저장하려면 **Private** 확인란을 선택하여 자신만 액세스할 수 있는 비공개로 검색을 저장할 수 있습니다. 또는 모든 사용자가 사용할 수 있도록 검색을 저장하려면 확인란을 선택하지 않습니다.

팁 제한된 권한과 함께 사용자 지정 사용자 역할에 대한 제한으로서 검색을 저장하려면 **반드시** 비공개 검색으로 저장해야 합니다.

5단계 선택적으로, 나중에 다시 사용할 수 있도록 검색을 저장할 수 있습니다. 다음 옵션을 이용할 수 있습니다.

- 검색 기준을 저장하려면 **Save**를 클릭합니다.

  새 검색인 경우 검색 이름을 입력하도록 대화 상자가 나타납니다. 고유한 검색 이름을 입력하고 **Save**를 클릭합니다. 이미 존재하는 검색에 대한 새 조건을 저장하는 경우 프롬프트가 나타나지 않습니다. 나중에 실행할 수 있도록 검색이 저장됩니다(**Private**을 선택한 경우 자신만 볼 수 있음).

- 새 검색을 저장하거나, 저장된 기존 검색을 변경하여 만든 검색에 새 이름을 할당하려면 **Save As New**를 클릭합니다.

  검색 이름을 입력하도록 대화 상자가 나타납니다. 고유한 검색 이름을 입력하고 **Save**를 클릭합니다. 나중에 실행할 수 있도록 검색이 저장됩니다(**Private**을 선택한 경우 자신만 볼 수 있음).

6단계 검색을 시작하려면 **Search**를 클릭합니다.

검색 결과는 기본 애플리케이션 세부사항 워크플로에 나타납니다. 사용자 지정 워크플로를 비롯한 다른 워크플로를 사용하려면 **(switch workflow)**를 클릭합니다. 다른 기본 워크플로 지정에 대한 자세한 내용은 71-3페이지의 이벤트 보기 설정 구성을/를 참조하십시오.

취약성 작업

라이센스: FireSIGHT

FireSIGHT 시스템에는 자체 취약성 추적 데이터베이스가 포함되어 있습니다. 이 데이터베이스를 시스템의 핑거프린트 인식 기능과 함께 사용하면 네트워크의 호스트와 관련된 취약성을 식별할 수 있습니다.

호스트에서 실행 중인 운영 체제, 서버 및 클라이언트에서 가지고 있는 관련 취약성 집합은 서로 다릅니다. 호스트를 패치하거나 호스트가 취약성에 대해 면역력이 있다고 판단한 후에는 취약성을 비활성화할 수 있습니다. 각 호스트에 대한 취약성을 추적 및 검토하기 위해 방어 센터를 사용할 수 있습니다.

서버에서 사용된 애플리케이션 서버가 시스템 정책에서 매핑되어 있지 않으면, 공급업체가 없는 서버 및 버전이 없는 서버의 취약성은 매핑되지 않습니다. 공급업체가 없는 클라이언트 및 버전이 없는 클라이언트의 취약성은 매핑할 수 없습니다. 자세한 내용은 63-30페이지의 서버에 대한 취약성 매핑을/를 참조하십시오.

자세한 내용은 다음 링크를 참고하십시오.

취약성 보기

라이센스: FireSIGHT

방어 센터를 사용하면 취약성의 테이블을 볼 수 있습니다. 그런 다음 찾고 있는 정보에 따라 이벤트 보기를 조작할 수 있습니다.

취약성에 액세스할 때 표시되는 페이지는 사용하는 워크플로에 따라 달라집니다. 취약성 테이블 보기를 포함하는 사전 정의 워크플로를 사용할 수 있습니다. 탐지된 호스트가 취약성을 보이는지 여부와 상관없이 테이블 보기에는 데이터베이스의 각 취약성에 대한 행이 포함되어 있습니다. 사전 정의 워크플로의 두 번째 페이지에는 네트워크에서 탐지된 호스트에 적용되는 각 취약성의 행(비활성화하지 않은)이 포함되어 있습니다. 사전 정의 워크플로는 제약 조건을 충족하는 모든 취약성에 대한 자세한 설명이 포함된 취약성 세부사항 보기에서 종료됩니다.

팁 단일 호스트 또는 호스트 집합에 적용되는 취약성을 보려면 호스트에 대한 IP 주소 또는 IP 주소의 범위를 지정하여 취약성 검색을 수행하십시오. 취약성 검색에 대한 자세한 내용은 50-53페이지의 취약성 검색을/를 참조하십시오.

특정 요구와 일치하는 정보만 표시하는 사용자 지정 워크플로를 생성할 수도 있습니다. 사용자 지정 워크플로 생성에 대한 자세한 내용은 58-38페이지의 사용자 지정 워크플로 생성을/를 참조하십시오.

다음 표에서는 취약성 워크플로 페이지에서 수행할 수 있는 몇 가지 특정 작업에 대해 설명합니다. 공통 검색 이벤트 작업 표에 설명된 작업을 수행할 수도 있습니다.

표 50-11 취약성 작업

목적	가능한 작업
테이블에서 열의 내용에 대해 자세히 알아보기	50-51페이지의 취약성 테이블 이해에서 자세히 알아보십시오.
취약성에 대한 취약성 세부사항 보기	SVID 열에서 보기 아이콘(🔍)을 클릭합니다. 또는 취약성 ID를 제한하고 취약성 세부사항 페이지로 드릴다운합니다. 자세한 내용은 49-27페이지의 취약성 세부사항 보기을/를 참조하십시오.
현재의 취약한 호스트에 대한 침입 영향 상관관계에 더 이상 사용되지 않도록 선택한 취약성 비활성화	50-53페이지의 취약성 비활성화에서 자세히 알아보십시오.
취약성 제목의 전체 텍스트 보기	제목을 마우스 오른쪽 버튼으로 클릭하고 **Show Full Text**를 선택합니다.

취약성을 보려면

액세스: Admin/Any Security Analyst

1단계 **Analysis > Vulnerabilities > Vulnerabilities**를 선택합니다.

기본 취약성 워크플로의 첫 번째 페이지가 나타납니다. 사용자 지정 워크플로를 비롯한 다른 워크플로를 사용하려면 **(switch workflow)**를 클릭합니다. 다른 기본 워크플로 지정에 대한 자세한 내용은 71-3페이지의 이벤트 보기 설정 구성을/를 참조하십시오.

팁 취약성의 테이블 보기가 포함되지 않은 사용자 지정 워크플로를 사용 중인 경우 **(switch workflow)**를 클릭한 다음 **Vulnerabilities**를 선택하십시오.

취약성 테이블 이해

라이센스: FireSIGHT

FireSIGHT 시스템에는 자체 취약성 추적 데이터베이스가 포함되어 있습니다. 이 데이터베이스를 시스템의 핑거프린트 인식 기능과 함께 사용하면 네트워크의 호스트와 관련된 취약성을 식별할 수 있습니다.

호스트에서 실행 중인 운영 체제, 서버 및 클라이언트에서 가지고 있는 관련 취약성 집합은 서로 다릅니다. 호스트를 패치하거나 호스트가 취약성에 대해 면역력이 있다고 판단한 후에는 취약성을 비활성화할 수 있습니다. 각 호스트에 대한 취약성을 추적 및 검토하기 위해 방어 센터를 사용할 수 있습니다.

취약성에 대한 자세한 내용은 48-8페이지의 취약성 네트워크 맵 작업 및 49-26페이지의 호스트 프로필에서 취약성 작업을/를 참조하십시오.

다음은 취약성 테이블의 필드에 대한 설명입니다.

SVID

시스템이 취약성 추적에 사용하는 Cisco 취약성 식별 번호.

SVID에 대한 취약성 세부사항에 액세스하려면 보기 아이콘(🔍)을 클릭합니다. 자세한 내용은 49-27페이지의 취약성 세부사항 보기을/를 참조하십시오.

Bugtraq ID

Bugtraq 데이터베이스의 취약성과 연결된 식별 번호. (http://www.securityfocus.com/bid/)

Snort ID

SID(Snort ID) 데이터베이스의 취약성과 연결된 식별 번호. 즉, 침입 규칙이 특정 취약성을 악용하는 네트워크 트래픽을 탐지할 수 있으면 해당 취약성은 침입 규칙의 SID와 연결됩니다.

취약성을 둘 이상의 SID와 연결할 수 있습니다(SID와 연결하지 않을 수도 있음). 취약성이 둘 이상의 SID와 연결되면 취약성 테이블에는 각 SID에 대한 행이 포함됩니다.

Title

취약성의 제목.

IP Address

취약성의 영향을 받는 호스트와 연결된 IP 주소.

Date Published

취약성이 게시된 날짜.

Vulnerability Impact

Bugtraq 데이터베이스에서 취약성에 할당된 심각도를 0~10 범위로 표시합니다(10이 가장 심각). 취약성 영향은 Bugtraq 항목 작성자가 SANS CVA(Critical Vulnerability Analysis) 기준을 참조하여 스스로 내리는 최선의 판단에 의해 결정됩니다.

Remote

취약성이 원격으로 악용될 수 있는지를 나타냅니다.

Available Exploits

취약성에 대한 알려진 익스플로잇이 있는지 여부를 나타냅니다.

Description

취약성에 대한 간단한 설명.

Technical Description

취약성에 대한 자세한 기술적 설명.

Solution

취약성 해결에 대한 정보.

Count

각 행에 표시되는 정보와 매칭되는 이벤트의 수. 둘 이상의 동일한 행을 생성하는 제약 조건을 적용한 경우에만 Count 필드가 나타납니다.

취약성 비활성화

라이센스: FireSIGHT

네트워크의 호스트를 패치하거나 호스트가 면역력이 있다고 판단한 후에는 취약성을 비활성화하십시오. 비활성화된 취약성은 침입 영향 상관관계에 사용되지 않습니다. 시스템이 해당 취약성의 영향을 받는 새 호스트를 검색하면, 이 취약성은 해당 호스트에 대해 유효한 것으로 간주됩니다(따라서 자동으로 비활성화되지 않음).

네트워크의 특정 호스트에 대해 취약성을 보이는 워크플로 페이지의 취약성 워크플로 **내에서만** 취약성을 비활성화할 수 있습니다. 즉,

- 기본 취약성 워크플로의 두 번째 페이지인 **Vulnerabilities on the Network** - 네트워크의 호스트에 해당되는 취약성만 표시
- 검색을 사용하여 IP 주소를 기반으로 제한한 취약성 워크플로의 임의의 페이지(사용자 지정 또는 사전 정의)

IP 주소에서 제한하지 않은 취약성 워크플로 내에서 취약성을 비활성화하면 네트워크에서 탐지된 *모든* 호스트에 대해 취약성이 비활성화됩니다. 단일 호스트에 대해 취약성을 비활성화하려면 세 가지 옵션 중 하나를 이용할 수 있습니다.

- 네트워크 맵을 사용합니다.

  자세한 내용은 48-8페이지의 취약성 네트워크 맵 작업을/를 참조하십시오.

- 호스트의 호스트 프로필을 사용합니다.

  자세한 내용은 49-30페이지의 개별 호스트에 대해 취약성 설정을/를 참조하십시오.

- 취약성을 비활성화할 호스트의 IP 주소를 기반으로 취약성 워크플로를 제한합니다. 연결된 여러 IP 주소가 있는 호스트의 경우 이 기능은 해당 호스트의 선택된 단일 IP에만 적용됩니다.

IP 주소를 기반으로 보기를 제한하려면 취약성을 비활성화할 호스트에 대해 IP 주소 또는 IP 주소의 범위를 지정하여 취약성 검색을 수행하십시오. 취약성 검색에 대한 자세한 내용은 50-53페이지의 취약성 검색을/를 참조하십시오.

취약성을 비활성화하려면

액세스: Admin/Any Security Analyst

1단계 Vulnerabilities on the Network 페이지에서 비활성화할 취약성 옆에 있는 확인란을 선택하고 **Review**를 클릭합니다.

취약성 검색

라이센스: FireSIGHT

네트워크의 호스트에 영향을 주는 취약성을 검색할 수 있습니다. 네트워크 환경에 맞춤화된 검색을 생성한 다음 나중에 다시 사용할 수 있도록 저장할 수 있습니다.

일반 검색 구문

각 검색 필드 옆에는 유효한 구문의 예가 표시됩니다. 검색 기준을 입력할 경우, 다음 사항에 유의해야 합니다.

- 모든 필드에 부정(!)을 사용할 수 있습니다.

- 모든 필드에 쉼표로 구분된 검색 값의 목록을 사용할 수 있습니다. 지정된 필드에 나열된 값 중 하나를 포함하는 레코드는 검색 기준과 일치합니다.
- 모든 필드에 따옴표로 감싸고 쉼표로 구분한 목록을 검색 값으로 사용할 수 있습니다.
  - 단일 값만을 포함할 수 있는 필드의 경우, 따옴표 내에 지정된 정확한 문자열을 포함하는 지정된 필드의 레코드가 검색 기준과 일치합니다. 예를 들어 `A, B, "C, D, E"`에 대한 검색은 지정된 필드에 `"A"` 또는 `"B"` 또는 `"C, D, E"`가 포함된 레코드와 일치합니다. 따라서 가능한 값으로 쉼표를 포함하는 필드에서 일치를 확인할 수 있습니다.
  - 여러 값을 동시에 포함할 수 있는 필드의 경우, 따옴표로 감싸고 쉼표로 구분한 모든 값을 포함하는 지정된 필드의 레코드가 해당 검색 기준과 일치합니다.
  - 여러 값을 동시에 포함할 수 있는 필드의 경우, 검색 기준에 단일 값은 물론 따옴표로 감싸고 쉼표로 구분한 목록도 포함할 수 있습니다. 예를 들어 하나 이상의 이러한 문자를 포함할 수 있는 필드에서 `A, B, "C, D, E"`에 대한 검색은 지정된 필드에 `A` 또는 `B`, 또는 `C`, `D`, `E` 모두가 포함된 레코드와 일치합니다.
- 검색 결과에는 모든 필드에 지정된 검색 기준과 매칭되는 레코드만 반환됩니다.
- 많은 필드에서 와일드카드로 하나 이상의 별표(*)를 사용할 수 있습니다.
- 일부 필드의 경우, 해당 필드에 대해 사용할 수 있는 정보가 없는 이벤트를 식별하려면 필드에 `n/a` 또는 `blank`를 지정할 수 있습니다. 해당 필드가 채워지는 이벤트를 식별하려면 `!n/a` 또는 `!blank`를 사용합니다.
- 대부분의 필드에서 대/소문자를 구분합니다.
- IP 주소는 CIDR 표기법으로 지정할 수 있습니다. FireSIGHT 시스템에서 IPv4 및 IPv6 주소를 입력하는 방법에 대한 자세한 내용은 1-19페이지의 IP 주소 표기 규칙을/를 참조하십시오.
- 검색 기준으로 객체를 사용하려면 검색 필드 옆에 나타나는 객체 추가 아이콘(+)을 클릭합니다.

검색에서 객체를 사용하는 방법을 포함하여 검색 구문에 대한 자세한 내용은 60-1페이지의 이벤트 검색을/를 참조하십시오.

취약성에 대한 특정 검색 기준

다음 정보는 취약성 검색에만 해당됩니다.

- Bugtraq ID 번호를 http://www.securityfocus.com/bid에서 찾습니다.
- 악용된 취약성을 검색하려면 `TRUE`를 입력하고, 그러한 취약성을 제외하려면 `FALSE`를 입력합니다.

취약성을 검색하려면

액세스: Admin/Any Security Analyst

1단계 **Analysis > Search**를 선택합니다.

Search 페이지가 나타납니다.

2단계 테이블 드롭다운 목록에서 **Vulnerabilities**를 선택합니다.

해당 제약 조건으로 페이지가 업데이트됩니다.

3단계 해당 필드에 검색 기준을 입력합니다.

여러 필드에 대한 조건을 입력하는 경우 모든 필드에 대해 지정한 검색 기준과 일치하는 레코드만 반환됩니다. 검색 기준으로 객체를 사용하려면 검색 필드 옆에 나타나는 추가 아이콘(+)을 클릭합니다.

4단계 선택적으로, 검색을 저장하려면 **Private** 확인란을 선택하여 자신만 액세스할 수 있는 비공개로 검색을 저장할 수 있습니다. 또는 모든 사용자가 사용할 수 있도록 검색을 저장하려면 확인란을 선택하지 않습니다.

팁 사용자 지정 사용자 역할에 대한 데이터 제한으로서 검색을 사용하려면 **반드시** 비공개 검색으로 저장해야 합니다.

5단계 선택적으로, 나중에 다시 사용할 수 있도록 검색을 저장할 수 있습니다. 다음 옵션을 이용할 수 있습니다.

- 검색 기준을 저장하려면 **Save**를 클릭합니다.

  새 검색인 경우 검색 이름을 입력하도록 대화 상자가 나타납니다. 고유한 검색 이름을 입력하고 **Save**를 클릭합니다. 이미 존재하는 검색에 대한 새 조건을 저장하는 경우 프롬프트가 나타나지 않습니다. 나중에 실행할 수 있도록 검색이 저장됩니다(**Private**을 선택한 경우 자신만 볼 수 있음).

- 새 검색을 저장하거나, 저장된 기존 검색을 변경하여 만든 검색에 새 이름을 할당하려면 **Save As New**를 클릭합니다.

  검색 이름을 입력하도록 대화 상자가 나타납니다. 고유한 검색 이름을 입력하고 **Save**를 클릭합니다. 나중에 실행할 수 있도록 검색이 저장됩니다(**Private**을 선택한 경우 자신만 볼 수 있음).

6단계 검색을 시작하려면 **Search**를 클릭합니다.

검색 결과는 기본 취약성 워크플로에 나타납니다. 사용자 지정 워크플로를 비롯한 다른 워크플로를 사용하려면 **(switch workflow)**를 클릭합니다. 다른 기본 워크플로 지정에 대한 자세한 내용은 71-3페이지의 이벤트 보기 설정 구성을/를 참조하십시오.

서드파티 취약성 작업

라이센스: FireSIGHT

FireSIGHT 시스템에는 자체 취약성 추적 데이터베이스가 포함되어 있습니다. 이 데이터베이스를 시스템의 핑거프린트 인식 기능과 함께 사용하면 네트워크의 호스트와 관련된 취약성을 식별할 수 있습니다.

조직이 서드파티 애플리케이션에서 네트워크 맵 데이터를 가져오기 위해 스크립트를 작성하거나 명령줄 가져오기 파일을 생성할 수 있는 경우, 시스템의 취약성 데이터를 보강하기 위해 서드파티 취약성 데이터를 가져올 수 있습니다. 자세한 내용은 *FireSIGHT 시스템 Host Input API Guide*를 참조하십시오.

가져온 데이터를 영향 상관관계에 포함하려면 서드파티 취약성 정보를 데이터베이스의 운영 체제 및 애플리케이션 정의에 매핑해야 합니다. 서드파티 취약성 정보를 클라이언트 정의에 매핑할 수는 없습니다.

자세한 내용은 다음 링크를 참고하십시오.

- 50-56페이지의 서드파티 취약성 보기
- 50-56페이지의 서드파티 취약성 테이블 이해
- 50-57페이지의 서드파티 취약성 검색

서드파티 취약성 보기

라이센스: FireSIGHT

호스트 입력 기능을 사용하여 서드파티 취약성 데이터를 가져왔으면 방어 센터를 사용하여 서드파티 취약성의 테이블을 볼 수 있습니다. 그런 다음 찾고 있는 정보에 따라 이벤트 보기를 조작할 수 있습니다.

서드파티 취약성에 액세스할 때 표시되는 페이지는 사용하는 워크플로에 따라 달라집니다. 두 가지 사전 정의 워크플로가 있습니다. 특정 요구와 일치하는 정보만 표시하는 사용자 지정 워크플로를 생성할 수도 있습니다. 자세한 내용은 58-38페이지의 사용자 지정 워크플로 생성을/를 참조하십시오.

다음 표에서는 서드파티 취약성 워크플로 페이지에서 수행할 수 있는 몇 가지 특정 작업에 대해 설명합니다. 공통 검색 이벤트 작업 표에 설명된 작업을 수행할 수도 있습니다.

표 50-12 서드파티 취약성 작업

목적	가능한 작업
테이블에서 열의 내용에 대해 자세히 알아보기	50-56페이지의 서드파티 취약성 테이블 이해에서 자세히 알아보십시오.
서드파티 취약성에 대한 취약성 세부사항 보기	SVID 열에서 보기 아이콘( )을 클릭합니다. 또는 취약성 ID를 제한하고 취약성 세부사항 페이지로 드릴다운합니다. 자세한 내용은 49-27페이지의 취약성 세부사항 보기을/를 참조하십시오.

서드파티 취약성을 보려면

액세스: Admin/Any Security Analyst

1단계 **Analysis > Vulnerabilities > Third-Party Vulnerabilities**를 선택합니다.

기본 서드파티 취약성 워크플로의 첫 번째 페이지가 나타납니다. 사용자 지정 워크플로를 비롯한 다른 워크플로를 사용하려면 **(switch workflow)**를 클릭합니다. 다른 기본 워크플로 지정에 대한 자세한 내용은 71-3페이지의 이벤트 보기 설정 구성을/를 참조하십시오.

팁 서드파티 취약성의 테이블 보기가 포함되지 않은 사용자 지정 워크플로를 사용 중인 경우 **(switch workflow)**를 클릭한 다음 **Vulnerabilities by Source** 또는 **Vulnerabilities by IP Address**를 선택하십시오.

서드파티 취약성 테이블 이해

라이센스: FireSIGHT

호스트 입력 기능을 사용하여 서드파티 취약성 정보를 가져오면 시스템은 해당 정보를 데이터베이스에 저장합니다. 다음 표에서는 서드파티 취약성 테이블의 필드에 대해 설명합니다.

Vulnerability Source

서드파티 취약성 소스(예: QualysGuard 또는 NeXpose).

Vulnerability ID

소스의 취약성과 연결된 ID 번호.

IP 주소

취약성의 영향을 받는 호스트와 연결된 IP 주소.

포트

취약성이 지정된 포트에서 실행 중인 서버와 연결된 경우 포트 번호.

Bugtraq ID

Bugtraq 데이터베이스의 취약성과 연결된 식별 번호. (http://www.securityfocus.com/bid/)

CVE ID

MITRE CVE(Common Vulnerabilities and Exposures) 데이터베이스(http://www.cve.mitre.org/)의 취약성과 연결된 식별 번호.

SVID

시스템이 취약성 추적에 사용하는 레거시 취약성 식별 번호.

SVID에 대한 취약성 세부사항에 액세스하려면 보기 아이콘( )을 클릭합니다. 자세한 내용은 49-27페이지의 취약성 세부사항 보기을/를 참조하십시오.

Snort ID

SID(Snort ID) 데이터베이스의 취약성과 연결된 식별 번호. 즉, 침입 규칙이 특정 취약성을 악용하는 네트워크 트래픽을 탐지할 수 있으면 해당 취약성은 침입 규칙의 SID와 연결됩니다.

취약성을 둘 이상의 SID와 연결할 수 있습니다(SID와 연결하지 않을 수도 있음). 취약성이 둘 이상의 SID와 연결되면 취약성 테이블에는 각 SID에 대한 행이 포함됩니다.

제목

취약성의 제목.

설명

취약성에 대한 간단한 설명.

개수

각 행에 표시되는 정보와 매칭되는 이벤트의 수. 둘 이상의 동일한 행을 생성하는 제약 조건을 적용한 경우에만 Count 필드가 나타납니다.

서드파티 취약성 검색

라이센스: FireSIGHT

네트워크의 호스트에 영향을 주는 서드파티 취약성을 검색할 수 있습니다. 네트워크 환경에 맞춤화된 검색을 생성한 다음 나중에 다시 사용할 수 있도록 저장할 수 있습니다.

일반 검색 구문

각 검색 필드 옆에는 유효한 구문의 예가 표시됩니다. 검색 기준을 입력할 경우, 다음 사항에 유의해야 합니다.

- 모든 필드에 부정(!)을 사용할 수 있습니다.

- 모든 필드에 쉼표로 구분된 검색 값의 목록을 사용할 수 있습니다. 지정된 필드에 나열된 값 중 하나를 포함하는 레코드는 검색 기준과 일치합니다.
- 모든 필드에 따옴표로 감싸고 쉼표로 구분한 목록을 검색 값으로 사용할 수 있습니다.
  - 단일 값만을 포함할 수 있는 필드의 경우, 따옴표 내에 지정된 정확한 문자열을 포함하는 지정된 필드의 레코드가 검색 기준과 일치합니다. 예를 들어 `A, B, "C, D, E"`에 대한 검색은 지정된 필드에 `"A"` 또는 `"B"` 또는 `"C, D, E"`가 포함된 레코드와 일치합니다. 따라서 가능한 값으로 쉼표를 포함하는 필드에서 일치를 확인할 수 있습니다.
  - 여러 값을 동시에 포함할 수 있는 필드의 경우, 따옴표로 감싸고 쉼표로 구분한 모든 값을 포함하는 지정된 필드의 레코드가 해당 검색 기준과 일치합니다.
  - 여러 값을 동시에 포함할 수 있는 필드의 경우, 검색 기준에 단일 값은 물론 따옴표로 감싸고 쉼표로 구분한 목록도 포함할 수 있습니다. 예를 들어 하나 이상의 이러한 문자를 포함할 수 있는 필드에서 `A, B, "C, D, E"`에 대한 검색은 지정된 필드에 `A` 또는 `B`, 또는 `C, D, E` 모두가 포함된 레코드와 일치합니다.
- 검색 결과에는 모든 필드에 지정된 검색 기준과 매칭되는 레코드만 반환됩니다.
- 많은 필드에서 와일드카드로 하나 이상의 별표(*)를 사용할 수 있습니다.
- 일부 필드의 경우, 해당 필드에 대해 사용할 수 있는 정보가 없는 이벤트를 식별하려면 필드에 `n/a` 또는 `blank`를 지정할 수 있습니다. 해당 필드가 채워지는 이벤트를 식별하려면 `!n/a` 또는 `!blank`를 사용합니다.
- 대부분의 필드에서 대/소문자를 구분합니다.
- IP 주소는 CIDR 표기법으로 지정할 수 있습니다. FireSIGHT 시스템에서 IPv4 및 IPv6 주소를 입력하는 방법에 대한 자세한 내용은 1-19페이지의 IP 주소 표기 규칙을/를 참조하십시오.
- 검색 기준으로 객체를 사용하려면 검색 필드 옆에 나타나는 객체 추가 아이콘(+)을 클릭합니다.

검색에서 객체를 사용하는 방법을 포함하여 검색 구문에 대한 자세한 내용은 60-1페이지의 이벤트 검색을/를 참조하십시오.

취약성에 대한 특정 검색 기준

다음 정보는 취약성 검색에만 해당됩니다.

- Bugtraq ID 번호를 http://www.securityfocus.com/bid에서 찾습니다.
- 악용된 취약성을 검색하려면 `TRUE`를 입력하고, 그러한 취약성을 제외하려면 `FALSE`를 입력합니다.

서드파티 취약성을 검색하려면

액세스: Admin/Any Security Analyst

1단계 **Analysis > Search**를 선택합니다.

Search 페이지가 나타납니다.

2단계 테이블 드롭다운 목록에서 **Third-Party Vulnerabilities**를 선택합니다.

해당 제약 조건으로 페이지가 업데이트됩니다.

3단계 해당 필드에 검색 기준을 입력합니다.

여러 필드에 대한 조건을 입력하는 경우 모든 필드에 대해 지정한 검색 기준과 일치하는 레코드만 반환됩니다. 검색 기준으로 객체를 사용하려면 검색 필드 옆에 나타나는 추가 아이콘(+)을 클릭합니다.

4단계 선택적으로, 검색을 저장하려면 **Private** 확인란을 선택하여 자신만 액세스할 수 있는 비공개로 검색을 저장할 수 있습니다. 또는 모든 사용자가 사용할 수 있도록 검색을 저장하려면 확인란을 선택하지 않습니다.

팁 사용자 지정 사용자 역할에 대한 데이터 제한으로서 검색을 사용하려면 **반드시** 비공개 검색으로 저장해야 합니다.

5단계 선택적으로, 나중에 다시 사용할 수 있도록 검색을 저장할 수 있습니다. 다음 옵션을 이용할 수 있습니다.

- 검색 기준을 저장하려면 **Save**를 클릭합니다.

  새 검색인 경우 검색 이름을 입력하도록 대화 상자가 나타납니다. 고유한 검색 이름을 입력하고 **Save**를 클릭합니다. 이미 존재하는 검색에 대한 새 조건을 저장하는 경우 프롬프트가 나타나지 않습니다. 나중에 실행할 수 있도록 검색이 저장됩니다(**Private**을 선택한 경우 자신만 볼 수 있음).

- 새 검색을 저장하거나, 저장된 기존 검색을 변경하여 만든 검색에 새 이름을 할당하려면 **Save As New**를 클릭합니다.

  검색 이름을 입력하도록 대화 상자가 나타납니다. 고유한 검색 이름을 입력하고 **Save**를 클릭합니다. 나중에 실행할 수 있도록 검색이 저장됩니다(**Private**을 선택한 경우 자신만 볼 수 있음).

6단계 검색을 시작하려면 **Search**를 클릭합니다.

검색 결과는 기본 서드파티 취약성 워크플로에 나타납니다. 사용자 지정 워크플로를 비롯한 다른 워크플로를 사용하려면 **(switch workflow)**를 클릭합니다. 다른 기본 워크플로 지정에 대한 자세한 내용은 71-3페이지의 이벤트 보기 설정 구성을/를 참조하십시오.

사용자 작업

라이센스: FireSIGHT

Active Directory Agent 또는 관리되는 디바이스가 아직 데이터베이스에 없는 사용자의 사용자 로그인을 탐지하면, 이러한 로그인 유형을 특별히 제한하지 않은 경우 해당 사용자는 데이터베이스에 추가됩니다(45-30페이지의 사용자 로깅 제한 참조).

참고 시스템에서는 SMTP 로그인을 탐지하더라도 데이터베이스에 아직 일치하는 이메일 주소의 사용자가 없으면 이를 기록하지 않습니다. SMTP 로그인을 기반으로 사용자가 데이터베이스에 추가되지는 **않습니다**.

다음 표에 설명된 대로, 시스템이 탐지한 로그인 유형은 새 사용자에 대해 저장될 정보를 결정합니다.

표 50-13 로그인 유형 및 저장되는 사용자 데이터

로그인 유형	저장되는 사용자 데이터
LDAP AIM Oracle SIP HTTP FTP MDNS	• username • 현재 IP 주소 • 로그인 유형(`aim`, `ldap`, `oracle`, `sip`, `http`, `ftp` 또는 `mdns`)
POP3 IMAP	• username • 현재 IP 주소 • email address • 로그인 유형(`pop3` 또는 `imap`)

방어 센터-LDAP 서버 연결을 구성한 경우 방어 센터는 5분마다 LDAP 서버에 쿼리하고 사용자 데이터베이스에서 새 사용자에 대한 메타데이터를 가져옵니다. 동시에 방어 센터는 방어 센터 데이터베이스에 있는 레코드가 12시간을 넘은 사용자에 대한 업데이트된 정보를 LDAP 서버에 쿼리합니다. 시스템에서 새 사용자 로그인을 탐지한 후 방어 센터 데이터베이스에서 사용자 메타데이터를 업데이트하는 데 5~10분 정도 걸릴 수 있습니다. 방어 센터는 각 사용자에 대한 다음과 같은 정보 및 메타데이터를 LDAP 서버에서 얻게 됩니다.

- LDAP 사용자 이름
- 이름 및 성
- email address
- 부서
- 전화 번호

방어 센터가 데이터베이스에 저장할 수 있는 최대 사용자 수는 FireSIGHT 라이센스에 따라 다릅니다. AIM, Oracle 및 SIP 로그인은 시스템이 LDAP 서버에서 가져오는 사용자 메타데이터와 연결되지 않으므로 중복 사용자 레코드를 생성합니다. 이러한 프로토콜에서 오는 중복된 사용자 레코드 때문에 사용자 카운트가 과용되는 상황을 방지하려면 네트워크 검색 정책에서 해당 프로토콜의 로깅을 비활성화하십시오. 자세한 내용은 45-30페이지의 사용자 로깅 제한을/를 참조하십시오.

데이터베이스에서 사용자를 검색하고 보고 삭제할 수 있습니다. 또한 데이터베이스에서 모든 사용자를 삭제할 수도 있습니다. 자세한 내용은 다음 절을 참조하십시오.

- 50-61페이지의 사용자 보기
- 50-61페이지의 사용자 테이블 이해
- 50-63페이지의 사용자 세부사항 및 호스트 기록 이해
- 50-63페이지의 사용자 검색

사용자 보기

라이센스: FireSIGHT

사용자의 테이블을 본 후, 찾고 있는 정보에 따라 이벤트 보기를 조작할 수 있습니다.

사용자에게 액세스할 때 표시되는 페이지는 사용하는 워크플로에 따라 달라집니다. 탐지된 모든 사용자를 나열하는 사용자의 테이블 보기를 포함하며 사용자 세부사항 페이지에서 종료되는 사전 정의 워크플로를 사용할 수 있습니다. 사용자 세부사항 페이지는 제약 조건을 충족하는 모든 사용자에 대한 정보를 제공합니다.

특정 요구와 일치하는 정보만 표시하는 사용자 지정 워크플로를 생성할 수도 있습니다. 사용자 지정 워크플로 생성에 대한 자세한 내용은 58-38페이지의 사용자 지정 워크플로 생성을/를 참조하십시오.

테이블에 있는 열의 내용에 대한 자세한 내용은 사용자 워크플로 페이지에서 수행할 수 있는 몇 가지 특정 작업에 대해 설명한 50-61페이지의 사용자 테이블 이해을/를 참조하십시오. 공통 검색 이벤트 작업 표에 설명된 작업을 수행할 수도 있습니다.

사용자를 보려면

액세스: Admin/Any Security Analyst

1단계 **Analysis > Users > Users**를 선택합니다.

기본 사용자 워크플로의 첫 번째 페이지가 나타납니다. 사용자 지정 워크플로를 비롯한 다른 워크플로를 사용하려면 **(switch workflow)**를 클릭합니다. 다른 기본 워크플로 지정에 대한 자세한 내용은 71-3페이지의 이벤트 보기 설정 구성을/를 참조하십시오.

팁 사용자의 테이블 보기가 포함되지 않은 사용자 지정 워크플로를 사용 중인 경우 **(switch workflow)**를 클릭한 다음 **Users**를 선택하십시오.

사용자 테이블 이해

라이센스: FireSIGHT

시스템은 사용자를 검색하면 해당 사용자에 대한 데이터를 수집하여 데이터베이스에 저장합니다. 다음은 사용자 테이블의 필드에 대한 설명입니다.

사용자

다음 중 하나:

- 이름, 성 및 사용자 이름 - 선택적인 방어 센터-LDAP 서버 연결을 통해 수집된 사용자의 경우
- 사용자 이름만 - 방어 센터-LDAP 서버 연결을 구성하지 않은 경우 또는 방어 센터가 LDAP 레코드와 상관관계를 설정할 수 없는 사용자의 경우

방어 센터는 또한 사용자를 탐지하는 데 사용된 프로토콜도 표시합니다.

실패한 AIM 로그인 시도도 기록되므로 방어 센터는 잘못된 AIM 사용자도 저장할 수 있습니다(예: 사용자 이름의 철자 오류).

현재 IP

사용자가 로그인하는 호스트와 연결된 IP 주소. 사용자 로그인 이후 권한 있는 또 다른 사용자가 동일한 IP 주소로 호스트에 로그인하는 경우, 기존 사용자가 권한 있는 사용자이고 새 사용자가 권한 없는 사용자가 아닌 한 이 필드는 비어 있습니다. (시스템에서는 로그인한 마지막 권한 있는 사용자의 IP 주소를 호스트와 연결합니다.) 권한 있는 사용자와 권한 없는 사용자에 대한 자세한 내용은 45-7페이지의 사용자 데이터베이스을/를 참조하십시오.

이름

선택적인 방어 센터-LDAP 서버 연결에서 가져오는 사용자의 이름. 다음과 같은 경우 이 필드는 비어 있습니다.

- 방어 센터-LDAP 서버 연결을 구성하지 않은 경우
- 방어 센터가 방어 센터 데이터베이스의 사용자를 LDAP 레코드와 상호 연결할 수 없는 경우(예: AIM, Oracle 또는 SIP 로그인을 통해 데이터베이스에 추가된 사용자의 경우)
- LDAP 서버의 사용자와 연결된 이름이 없는 경우

성

선택적인 방어 센터-LDAP 서버 연결에서 가져오는 사용자의 성. 다음과 같은 경우 이 필드는 비어 있습니다.

- 방어 센터-LDAP 서버 연결을 구성하지 않은 경우
- 방어 센터가 방어 센터 데이터베이스의 사용자를 LDAP 레코드와 상호 연결할 수 없는 경우(예: AIM, Oracle 또는 SIP 로그인을 통해 데이터베이스에 추가된 사용자의 경우)
- LDAP 서버의 사용자와 연결된 성이 없는 경우

이메일

사용자의 이메일 주소. 다음과 같은 경우 이 필드는 비어 있습니다.

- AIM 로그인을 통해 사용자가 데이터베이스에 추가된 경우
- LDAP 로그인을 통해 사용자가 데이터베이스에 추가되었으며 LDAP 서버의 사용자와 연결된 이메일 주소가 없는 경우

부서

선택적인 방어 센터-LDAP 서버 연결에서 가져오는 사용자의 부서. LDAP 서버의 사용자와 명시적으로 연결된 부서가 없는 경우, 부서는 서버가 할당하는 기본 그룹으로 나열됩니다. 예를 들면 Active Directory에서는 `Users (ad)`입니다. 다음과 같은 경우 이 필드는 비어 있습니다.

- 방어 센터-LDAP 서버 연결을 구성하지 않은 경우
- 방어 센터가 방어 센터 데이터베이스의 사용자를 LDAP 레코드와 상호 연결할 수 없는 경우(예: AIM, Oracle 또는 SIP 로그인을 통해 데이터베이스에 추가된 사용자의 경우)

전화

선택적인 방어 센터-LDAP 서버 연결에서 가져오는 사용자의 전화 번호. 다음과 같은 경우 이 필드는 비어 있습니다.

- 방어 센터-LDAP 서버 연결을 구성하지 않은 경우
- 방어 센터가 방어 센터 데이터베이스의 사용자를 LDAP 레코드와 상호 연결할 수 없는 경우(예: AIM, Oracle 또는 SIP 로그인을 통해 데이터베이스에 추가된 사용자의 경우)
- LDAP 서버의 사용자와 연결된 전화 번호가 없는 경우

사용자 유형

사용자를 탐지하는 데 사용된 프로토콜. 예를 들어 POP3 로그인을 탐지하면 사용자가 데이터베이스에 추가되는 경우 사용자 유형은 pop3입니다.

개수

각 열에 나타나는 정보와 일치하는 사용자의 수. 둘 이상의 동일한 행을 생성하는 제약 조건을 적용한 경우에만 Count 필드가 나타납니다.

사용자 세부사항 및 호스트 기록 이해

라이센스: FireSIGHT

특정 사용자에 대해 자세히 알아보려면 사용자 ID 데이터를 다른 이벤트 유형과 연결하는 이벤트 보기 및 사용자의 테이블 보기에서 User Identity 팝업 창을 표시할 수 있습니다. 사용자 정보는 사용자 워크플로의 종료 페이지에도 나타납니다.

여기에 표시되는 사용자 데이터는 사용자의 테이블 보기에 표시되는 데이터와 동일합니다. 자세한 내용은 50-61페이지의 사용자 테이블 이해을/를 참조하십시오.

호스트 기록은 사용자 활동의 마지막 24시간을 그래프로 보여줍니다. 사용자가 로그인 및 로그오프한 호스트의 IP 주소 목록은 막대 그래프로 로그인 및 로그아웃 시간의 근사치를 나타냅니다. 일반 사용자는 하루에 수차례 호스트에 로그인 및 로그오프할 수 있습니다. 예를 들어, 메일 서버에 대한 정기적인 자동 로그인은 여러 개의 짧은 세션으로 표시되고, 좀 더 긴 로그인(예: 근무 시간 중)은 더 긴 세션으로 표시될 수 있습니다.

권한 없는 사용자가 호스트에 로그인한 것이 탐지되면 해당 로그인은 사용자 및 호스트 내역에 기록됩니다. 호스트와 연결된 권한 있는 사용자가 없는 경우, 권한 없는 사용자가 호스트의 현재 사용자가 될 수 있습니다. 그러나 해당 호스트에서 권한 있는 사용자 로그인이 탐지되면, 또 다른 권한 있는 사용자 로그인만이 현재 사용자를 변경합니다. 또한 권한 없는 사용자가 호스트의 현재 사용자인 경우, 해당 사용자를 사용자 제어에 사용할 수 없습니다. 네트워크 검색 정책에서 실패한 로그인의 캡처를 구성하는 경우 호스트 기록에는 사용자가 로그인에 실패한 호스트도 포함됩니다.

호스트 기록을 생성하는 데 사용된 데이터는 사용자 기록 데이터베이스에 저장됩니다. 이 데이터베이스에는 기본적으로 1,000만 개의 사용자 로그인 이벤트가 저장됩니다. 특정 사용자에 대한 호스트 기록에 데이터가 없는 경우 사용자가 비활성 상태이거나, 데이터베이스 제한을 늘려야 할 수 있습니다. 자세한 내용은 63-15페이지의 데이터베이스 이벤트 제한 구성을/를 참조하십시오.

사용자 세부사항 및 호스트 기록을 보려면

액세스: Admin/Any Security Analyst

1단계 다음 2가지 옵션을 사용할 수 있습니다.

- 사용자가 나열된 이벤트 보기에서 사용자 ID 옆에 나타나는 사용자 아이콘( )을 클릭합니다.
- 사용자 워크플로에서 Users 종료 페이지를 클릭합니다.

사용자 세부사항이 나타납니다.

사용자 검색

라이센스: FireSIGHT

특정 사용자를 검색할 수 있습니다. 네트워크 환경에 맞춤화된 검색을 생성한 다음 나중에 다시 사용할 수 있도록 저장할 수 있습니다.

일반 검색 구문

각 검색 필드 옆에는 유효한 구문의 예가 표시됩니다. 검색 기준을 입력할 경우, 다음 사항에 유의해야 합니다.

- 모든 필드에 부정(!)을 사용할 수 있습니다.
- 모든 필드에 쉼표로 구분된 검색 값의 목록을 사용할 수 있습니다. 지정된 필드에 나열된 값 중 하나를 포함하는 레코드는 검색 기준과 일치합니다.
- 모든 필드에 따옴표로 감싸고 쉼표로 구분한 목록을 검색 값으로 사용할 수 있습니다.
  - 단일 값만을 포함할 수 있는 필드의 경우, 따옴표 내에 지정된 정확한 문자열을 포함하는 지정된 필드의 레코드가 검색 기준과 일치합니다. 예를 들어 `A, B, "C, D, E"`에 대한 검색은 지정된 필드에 `"A"` 또는 `"B"` 또는 `"C, D, E"`가 포함된 레코드와 일치합니다. 따라서 가능한 값으로 쉼표를 포함하는 필드에서 일치를 확인할 수 있습니다.
  - 여러 값을 동시에 포함할 수 있는 필드의 경우, 따옴표로 감싸고 쉼표로 구분한 모든 값을 포함하는 지정된 필드의 레코드가 해당 검색 기준과 일치합니다.
  - 여러 값을 동시에 포함할 수 있는 필드의 경우, 검색 기준에 단일 값은 물론 따옴표로 감싸고 쉼표로 구분한 목록도 포함할 수 있습니다. 예를 들어 하나 이상의 이러한 문자를 포함할 수 있는 필드에서 `A, B, "C, D, E"`에 대한 검색은 지정된 필드에 `A` 또는 `B`, 또는 `C, D, E` 모두가 포함된 레코드와 일치합니다.
- 검색 결과에는 모든 필드에 지정된 검색 기준과 매칭되는 레코드만 반환됩니다.
- 많은 필드에서 와일드카드로 하나 이상의 별표(*)를 사용할 수 있습니다.
- 일부 필드의 경우, 해당 필드에 대해 사용할 수 있는 정보가 없는 이벤트를 식별하려면 필드에 `n/a` 또는 `blank`를 지정할 수 있습니다. 해당 필드가 채워지는 이벤트를 식별하려면 `!n/a` 또는 `!blank`를 사용합니다.
- 대부분의 필드에서 대/소문자를 구분합니다.
- IP 주소는 CIDR 표기법으로 지정할 수 있습니다. FireSIGHT 시스템에서 IPv4 및 IPv6 주소를 입력하는 방법에 대한 자세한 내용은 1-19페이지의 IP 주소 표기 규칙을/를 참조하십시오.
- 검색 기준으로 객체를 사용하려면 검색 필드 옆에 나타나는 객체 추가 아이콘(+)을 클릭합니다.

검색에서 객체를 사용하는 방법을 포함하여 검색 구문에 대한 자세한 내용은 60-1페이지의 이벤트 검색을/를 참조하십시오.

특정 사용자 검색 기준

User Type에서 유효한 검색 기준은 `ldap`, `pop3`, `imap`, `oracle`, `sip`, `http`, `ftp`, `mdns` 및 `aim`입니다. SMTP 로그인 기반의 사용자는 데이터베이스에 추가되지 않으므로 `smtp`를 입력하면 결과가 반환되지 않습니다.

사용자를 검색하려면

액세스: Admin/Any Security Analyst

1단계 **Analysis > Search**를 선택합니다.

Search 페이지가 나타납니다.

2단계 테이블 드롭다운 목록에서 **Users**를 선택합니다.

Users 검색 페이지가 나타납니다.

팁 데이터베이스에서 서로 다른 종류의 이벤트를 검색하려면 테이블 드롭다운 목록에서 선택합니다.

3단계 해당 필드에 검색 기준을 입력합니다.

여러 필드에 대한 조건을 입력하는 경우 모든 필드에 대해 지정한 검색 기준과 일치하는 레코드만 반환됩니다.

4단계 선택적으로, 검색을 저장하려면 **Private** 확인란을 선택하여 자신만 액세스할 수 있는 비공개로 검색을 저장할 수 있습니다. 또는 모든 사용자가 사용할 수 있도록 검색을 저장하려면 확인란을 선택하지 않습니다.

팁 제한된 권한과 함께 사용자 지정 사용자 역할에 대한 제한으로서 검색을 저장하려면 **반드시** 비공개 검색으로 저장해야 합니다.

5단계 선택적으로, 나중에 다시 사용할 수 있도록 검색을 저장할 수 있습니다. 다음 옵션을 이용할 수 있습니다.

- 검색 기준을 저장하려면 **Save**를 클릭합니다.

  새 검색인 경우 검색 이름을 입력하도록 대화 상자가 나타납니다. 고유한 검색 이름을 입력하고 **Save**를 클릭합니다. 이미 존재하는 검색에 대한 새 조건을 저장하는 경우 프롬프트가 나타나지 않습니다. 나중에 실행할 수 있도록 검색이 저장됩니다(**Private**을 선택한 경우 자신만 볼 수 있음).

- 새 검색을 저장하거나, 저장된 기존 검색을 변경하여 만든 검색에 새 이름을 할당하려면 **Save As New**를 클릭합니다.

  검색 이름을 입력하도록 대화 상자가 나타납니다. 고유한 검색 이름을 입력하고 **Save**를 클릭합니다. 나중에 실행할 수 있도록 검색이 저장됩니다(**Private**을 선택한 경우 자신만 볼 수 있음).

6단계 검색을 시작하려면 **Search**를 클릭합니다.

검색 결과는 기본 사용자 워크플로에 나타납니다. 다른 워크플로를 사용하려면 **(switch workflow)**를 클릭합니다. 다른 기본 워크플로 지정에 대한 자세한 내용은 71-3페이지의 이벤트 보기 설정 구성을/를 참조하십시오.

사용자 활동 작업

라이센스: FireSIGHT

FireSIGHT 시스템은 네트워크에서 사용자 활동의 세부사항을 전달하는 이벤트를 생성합니다. 다음은 네 가지 유형의 사용자 활동에 대한 설명입니다.

New User Identity

시스템이 데이터베이스에 없는 사용자에 대한 사용자 로그인을 탐지할 경우 이 이벤트가 생성됩니다.

User Login

다음 중 하나가 발생할 경우 이 이벤트가 생성됩니다.

- Active Directory 서버에 설치한 Active Directory Agent가 LDAP 로그인 탐지
- 관리되는 디바이스가 LDAP, POP3, IMAP, SMTP, AIM, Oracle, FTP, HTTP, MDNS 또는 SIP 로그인 탐지
- 사용자 로그인 이벤트에 대해 유의해야 할 몇 가지 사항이 있습니다.

- 데이터베이스에 이미 일치하는 이메일 주소의 사용자가 있지 않은 한 SMTP 로그인은 기록되지 않습니다.
- 실패한 로그인은 LDAP, IMAP, FTP, POP3의 경우, 그리고 트래픽에서 탐지된 경우뿐입니다. 실패한 로그인의 결과 때문에 사용자가 탐지된 사용자 데이터베이스에 추가되지는 않지만, 네트워크 검색 정책의 사용자 로깅 컨피그레이션을 기반으로, 활동은 선택적으로 사용자 활동 데이터베이스에 기록됩니다.
- 로그인 유형을 특별히 제한한 경우 사용자 로그인이 기록되지 않습니다. 45-30페이지의 사용자 로깅 제한을/를 참조하십시오.

권한 없는 사용자가 호스트에 로그인하면 해당 로그인은 사용자 및 호스트 내역에 기록됩니다. 호스트와 연결된 권한 있는 사용자가 없는 경우, 권한 없는 사용자가 호스트의 현재 사용자가 될 수 있습니다. 그러나 권한 있는 사용자가 호스트에 로그인한 후에는 또 다른 권한 있는 사용자의 로그인에 의해서만 현재 사용자가 변경됩니다. 또한 권한 없는 사용자가 호스트의 현재 사용자인 경우, 해당 사용자를 사용자 제어에 사용할 수 없습니다.

Delete User Identity

데이터베이스에서 사용자를 수동으로 삭제할 경우 이 이벤트가 생성됩니다.

User Identity Dropped: User Limit Reached

시스템이 데이터베이스에 없는 사용자를 탐지했지만, FireSIGHT 라이센스 관련 데이터베이스에 추가할 수 있는 사용자 최대 수에 도달했기 때문에 해당 사용자를 추가할 수 없는 경우 이 이벤트가 생성됩니다.

방어 센터가 저장할 수 있는 탐지된 총 사용자 수는 FireSIGHT 라이센스에 따라 다릅니다. 라이센스 제한에 도달하면 대부분의 경우 시스템은 데이터베이스에 대한 새 사용자 추가를 중지합니다. 새 사용자를 추가하려면 데이터베이스에서 오래된 사용자 또는 비활성 사용자를 수동으로 삭제하거나 모든 사용자를 삭제해야 합니다.

그러나 시스템은 권한 있는 사용자를 선호합니다. 제한에 도달한 상태에서 시스템이 전에 탐지하지 못한 권한 있는 사용자의 로그인을 탐지하면, 오랫동안 비활성 상태를 유지한 권한 없는 사용자를 삭제하고 새로운 권한 있는 사용자를 대신 추가합니다.

시스템은 사용자 활동을 탐지하면 데이터베이스에 기록합니다. 사용자 활동을 보고 검색하고 삭제할 수 있습니다. 또한 데이터베이스에서 모든 사용자 활동을 삭제할 수도 있습니다.

가능한 경우마다 FireSIGHT 시스템은 사용자 활동을 다른 이벤트 유형과 상호 연결합니다. 예를 들어, 침입 이벤트는 이벤트 발생 시점에 소스 및 대상 호스트에 로그인한 사용자를 알려줄 수 있습니다. 이를 통해 공격 대상인 호스트의 소유자, 또는 내부 공격이나 포트스캔을 시작한 사용자를 알 수 있습니다.

상관관계 규칙에서 사용자 활동을 사용할 수도 있습니다. 사용자 활동 및 지정한 다른 기준을 기반으로 상관관계 규칙을 작성할 수 있습니다. 상관관계 정책에서 사용할 경우 이러한 규칙은 네트워크 트래픽이 조건을 충족하면 교정과 알림 응답을 실행합니다. 사용자 활동에 대한 자세한 내용은 45-3페이지의 사용자 데이터 수집 이해을/를 참조하십시오.

자세한 내용은 다음 절을 참조하십시오.

- 50-67페이지의 사용자 활동 이벤트 보기
- 50-67페이지의 사용자 활동 테이블 이해
- 50-68페이지의 사용자 활동 검색

사용자 활동 이벤트 보기

라이센스: FireSIGHT

사용자 활동의 테이블을 본 후, 찾고 있는 정보에 따라 이벤트 보기를 조작할 수 있습니다.

사용자 활동에 액세스할 때 표시되는 페이지는 사용하는 워크플로에 따라 달라집니다. 사용자 활동의 테이블 보기를 포함하며 사용자 세부사항 페이지(제약 조건을 충족하는 모든 사용자에 대한 사용자 세부사항 포함)에서 종료되는 사전 정의 워크플로를 사용할 수 있습니다. 특정 요구와 일치하는 정보만 표시하는 사용자 지정 워크플로를 생성할 수도 있습니다. 사용자 지정 워크플로 생성에 대한 자세한 내용은 58-38페이지의 사용자 지정 워크플로 생성을/를 참조하십시오.

테이블에 있는 열의 내용에 대한 자세한 내용은 사용자 활동 워크플로 페이지에서 수행할 수 있는 몇 가지 특정 작업에 대해 설명한 50-67페이지의 사용자 활동 테이블 이해을/를 참조하십시오. 공통 검색 이벤트 작업 표에 설명된 작업을 수행할 수도 있습니다.

사용자 활동을 보려면

액세스: Admin/Any Security Analyst

1단계 **Analysis > Users > User Activity**를 선택합니다.

기본 사용자 활동 워크플로의 첫 번째 페이지가 나타납니다. 사용자 지정 워크플로를 비롯한 다른 워크플로를 사용하려면 **(switch workflow)**를 클릭합니다. 다른 기본 워크플로 지정에 대한 자세한 내용은 71-3페이지의 이벤트 보기 설정 구성을/를 참조하십시오. 이벤트가 표시되지 않을 경우 시간 범위를 조정해야 할 수 있습니다. 58-22페이지의 이벤트 시간 제약 조건 설정을/를 참조하십시오.

팁 사용자 활동의 테이블 보기가 포함되지 않은 사용자 지정 워크플로를 사용 중인 경우 **(switch workflow)**를 클릭한 다음 **User Activity**를 선택하십시오.

사용자 활동 테이블 이해

라이센스: FireSIGHT

시스템은 사용자 활동을 탐지하면 데이터베이스에 기록합니다. 다음은 사용자 테이블의 필드에 대한 설명입니다.

Time

시스템이 사용자 활동을 탐지한 시간.

이벤트

사용자 활동 유형. 자세한 내용은 50-65페이지의 사용자 활동 작업을/를 참조하십시오.

사용자

활동과 연결된 사용자. 이 필드에는 최소한 사용자 이름 및 사용자 삭제에 사용된 프로토콜이 포함됩니다. 사용자에 대한 LDAP 메타데이터가 있는 경우 이 필드에는 사용자의 이름과 성도 포함될 수 있습니다.

사용자 유형

사용자를 탐지하는 데 사용된 프로토콜. 예를 들어 시스템에서 POP3 로그인을 탐지하면 사용자가 데이터베이스에 추가되는 경우 사용자 유형은 pop3입니다.

IP 주소

User Login 활동의 경우 로그인과 관련된 IP 주소. 사용자 호스트(LDAP, POP3, IMAP, FTP, HTTP, MDNS 및 AIM 로그인), 서버(SMTP 및 Oracle 로그인) 또는 세션 시작 주체(SIP 로그인)의 IP 주소일 수 있습니다.

IP 주소가 연결되어 있다고 해서 사용자가 해당 IP 주소의 현재 사용자라는 의미는 아닙니다. 권한 없는 사용자가 호스트에 로그인하면 해당 로그인은 사용자 및 호스트 기록에 추가됩니다. 호스트와 연결된 권한 있는 사용자가 없는 경우, 권한 없는 사용자가 호스트의 현재 사용자가 될 수 있습니다. 그러나 권한 있는 사용자가 호스트에 로그인한 후에는 또 다른 권한 있는 사용자의 로그인에 의해서만 현재 사용자가 변경됩니다.

다른 사용자 활동의 경우 이 필드는 비어 있습니다.

설명

Delete User Identity 및 User Identity Dropped 활동의 경우, 데이터베이스에서 삭제되었거나 데이터베이스에 추가되지 못한 사용자의 사용자 이름. 네트워크 리소스에 대한 로그인의 경우 network login이 표시됩니다. 다른 사용자 활동의 경우 이 필드는 비어 있습니다.

디바이스

관리되는 디바이스에 의해 탐지된 사용자 활동의 경우, 디바이스의 이름. 다른 사용자 활동 유형의 경우, 관리하는 방어 센터.

개수

각 행에 표시되는 정보와 매칭되는 이벤트의 수. 둘 이상의 동일한 행을 생성하는 제약 조건을 적용한 경우에만 Count 필드가 나타납니다.

사용자 활동 검색

라이센스: FireSIGHT

특정 사용자 활동을 검색할 수 있습니다. 네트워크 환경에 맞춤화된 검색을 생성한 다음 나중에 다시 사용할 수 있도록 저장할 수 있습니다.

일반 검색 구문

각 검색 필드 옆에는 유효한 구문의 예가 표시됩니다. 검색 기준을 입력할 경우, 다음 사항에 유의해야 합니다.

- 모든 필드에 부정(!)을 사용할 수 있습니다.
- 모든 필드에 쉼표로 구분된 검색 값의 목록을 사용할 수 있습니다. 지정된 필드에 나열된 값 중 하나를 포함하는 레코드는 검색 기준과 일치합니다.
- 모든 필드에 따옴표로 감싸고 쉼표로 구분한 목록을 검색 값으로 사용할 수 있습니다.
  - 단일 값만을 포함할 수 있는 필드의 경우, 따옴표 내에 지정된 정확한 문자열을 포함하는 지정된 필드의 레코드가 검색 기준과 일치합니다. 예를 들어 A, B, "C, D, E"에 대한 검색은 지정된 필드에 "A" 또는 "B" 또는 "C, D, E"가 포함된 레코드와 일치합니다. 따라서 가능한 값으로 쉼표를 포함하는 필드에서 일치를 확인할 수 있습니다.
  - 여러 값을 동시에 포함할 수 있는 필드의 경우, 따옴표로 감싸고 쉼표로 구분한 모든 값을 포함하는 지정된 필드의 레코드가 해당 검색 기준과 일치합니다.

  - 여러 값을 동시에 포함할 수 있는 필드의 경우, 검색 기준에 단일 값은 물론 따옴표로 감싸고 쉼표로 구분한 목록도 포함할 수 있습니다. 예를 들어 하나 이상의 이러한 문자를 포함할 수 있는 필드에서 `A, B, "C, D, E"`에 대한 검색은 지정된 필드에 `A` 또는 `B`, 또는 `C, D, E` 모두가 포함된 레코드와 일치합니다.
- 검색 결과에는 모든 필드에 지정된 검색 기준과 매칭되는 레코드만 반환됩니다.
- 많은 필드에서 와일드카드로 하나 이상의 별표(*)를 사용할 수 있습니다.
- 일부 필드의 경우, 해당 필드에 대해 사용할 수 있는 정보가 없는 이벤트를 식별하려면 필드에 `n/a` 또는 `blank`를 지정할 수 있습니다. 해당 필드가 채워지는 이벤트를 식별하려면 `!n/a` 또는 `!blank`를 사용합니다.
- 대부분의 필드에서 대/소문자를 구분합니다.
- IP 주소는 CIDR 표기법으로 지정할 수 있습니다. FireSIGHT 시스템에서 IPv4 및 IPv6 주소를 입력하는 방법에 대한 자세한 내용은 1-19페이지의 IP 주소 표기 규칙을/를 참조하십시오.
- 특정 디바이스 및 그룹, 스택 또는 클러스터의 디바이스를 검색하려면 디바이스 필드를 사용합니다. FireSIGHT 시스템에서 검색 시 디바이스 필드를 취급하는 방법에 대한 자세한 내용은 60-7페이지의 검색에서 디바이스 지정을/를 참조하십시오.
- 검색 기준으로 객체를 사용하려면 검색 필드 옆에 나타나는 객체 추가 아이콘(+)을 클릭합니다.

검색에서 객체를 사용하는 방법을 포함하여 검색 구문에 대한 자세한 내용은 60-1페이지의 이벤트 검색을/를 참조하십시오.

사용자 활동을 검색하려면

액세스: Admin/Any Security Analyst

1단계 **Analysis > Search**를 선택합니다.

Search 페이지가 나타납니다.

2단계 테이블 드롭다운 목록에서 **User Activity**를 선택합니다.

User Activity 검색 페이지가 나타납니다.

팁 데이터베이스에서 서로 다른 종류의 이벤트를 검색하려면 테이블 드롭다운 목록에서 선택합니다.

3단계 해당 필드에 검색 기준을 입력합니다.

여러 필드에 대한 조건을 입력하는 경우 모든 필드에 대해 지정한 검색 기준과 일치하는 레코드만 반환됩니다. 검색 기준으로 객체를 사용하려면 검색 필드 옆에 나타나는 추가 아이콘(+)을 클릭합니다.

4단계 선택적으로, 검색을 저장하려면 **Private** 확인란을 선택하여 자신만 액세스할 수 있는 비공개로 검색을 저장할 수 있습니다. 또는 모든 사용자가 사용할 수 있도록 검색을 저장하려면 확인란을 선택하지 않습니다.

팁 제한된 권한과 함께 사용자 지정 사용자 역할에 대한 제한으로서 검색을 저장하려면 **반드시** 비공개 검색으로 저장해야 합니다.

5단계 선택적으로, 나중에 다시 사용할 수 있도록 검색을 저장할 수 있습니다. 다음 옵션을 이용할 수 있습니다.

- 검색 기준을 저장하려면 **Save**를 클릭합니다.

새 검색인 경우 검색 이름을 입력하도록 대화 상자가 나타납니다. 고유한 검색 이름을 입력하고 **Save**를 클릭합니다. 이미 존재하는 검색에 대한 새 조건을 저장하는 경우 프롬프트가 나타나지 않습니다. 나중에 실행할 수 있도록 검색이 저장됩니다(**Private**을 선택한 경우 자신만 볼 수 있음).

- 새 검색을 저장하거나, 저장된 기존 검색을 변경하여 만든 검색에 새 이름을 할당하려면 **Save As New**를 클릭합니다.

  검색 이름을 입력하도록 대화 상자가 나타납니다. 고유한 검색 이름을 입력하고 **Save**를 클릭합니다. 나중에 실행할 수 있도록 검색이 저장됩니다(**Private**을 선택한 경우 자신만 볼 수 있음).

6단계 검색을 시작하려면 **Search**를 클릭합니다.

검색 결과는 현재의 시간 범위로 제한되어 사용자 활동 워크플로에 나타납니다. 사용자 지정 워크플로를 비롯한 다른 워크플로를 사용하려면 **(switch workflow)**를 클릭합니다. 다른 기본 워크플로 지정에 대한 자세한 내용은 71-3페이지의 이벤트 보기 설정 구성을/를 참조하십시오.

51장 상관관계 정책 및 규칙 구성

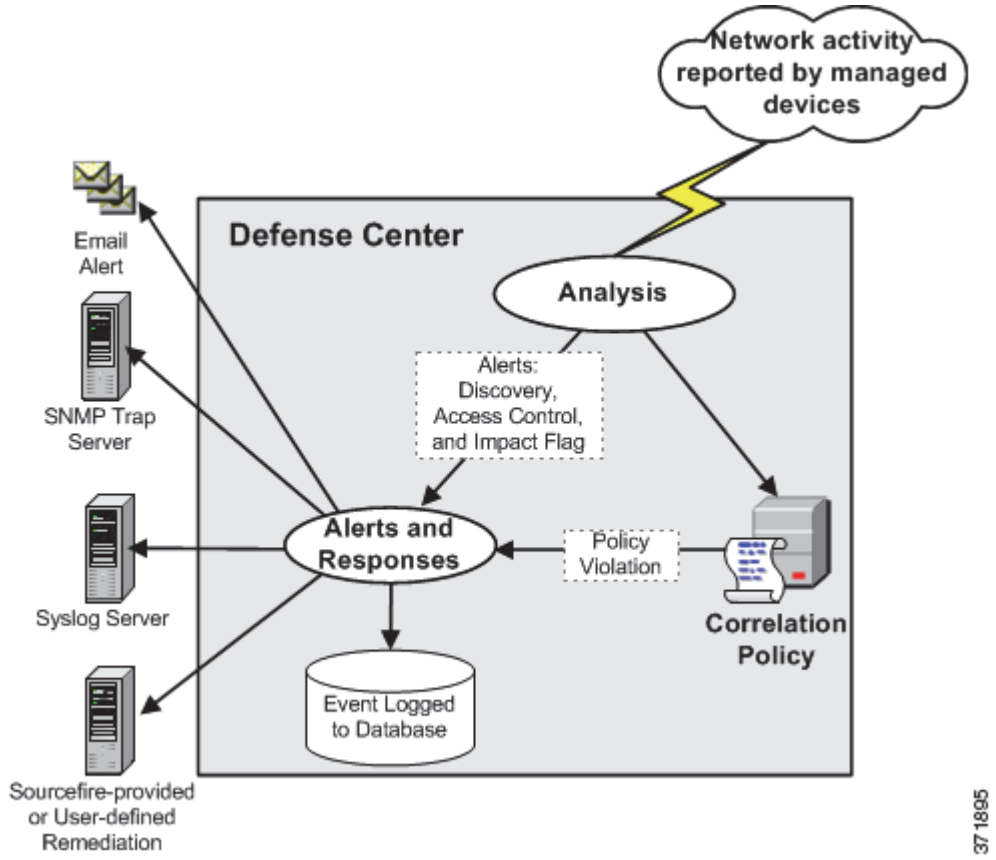
FireSIGHT 시스템의 *상관관계* 기능을 사용하면 *상관관계 규칙* 및 *규정준수 화이트리스트*로 채워지며 네트워크에 대한 위협에 실시간으로 응답할 수 있는 *상관관계 정책*을 작성할 수 있습니다. 네트워크의 활동이 상관관계 규칙 또는 화이트리스트를 트리거할 때 상관관계 *정책 위반*이 발생합니다.

상관관계 규칙은 FireSIGHT 시스템에 의해 생성된 특정 이벤트가 지정된 기준을 충족하거나 네트워크 트래픽이 기존 트래픽 프로필에 기술된 정상적인 네트워크 트래픽 패턴에서 벗어날 때 트리거됩니다.

반면 규정준수 화이트리스트는 네트워크의 호스트가 금지된 운영 체제, 클라이언트 애플리케이션(또는 클라이언트), 애플리케이션 프로토콜 또는 프로토콜에서 실행 중이라고 시스템에서 판단할 경우 트리거됩니다.

정책 위반에 대한 응답을 시작하도록 FireSIGHT 시스템을 구성할 수 있습니다. 응답에는 간단한 알림은 물론 각종 교정(예: 호스트 스캐닝)도 포함됩니다. 각 정책 위반에 대해 시스템에서 여러 응답을 실행하도록 응답을 그룹화할 수 있습니다.

다음 그림에서는 이벤트 알림 및 상관관계 프로세스를 보여줍니다.



이 장에서는 상관관계 규칙을 생성하고, 정책에서 그러한 규칙을 사용하고, 응답과 응답 그룹을 그러한 규칙과 연결하고, 상관관계 이벤트를 분석하는 방법에 대해 설명합니다. 자세한 내용은 다음 링크를 참고하십시오.

- 51-3페이지의 상관관계 정책에 대한 규칙 생성
- 51-41페이지의 상관관계 정책에 대한 규칙 관리
- 51-43페이지의 상관관계 응답 그룹화
- 51-45페이지의 상관관계 정책 생성
- 51-49페이지의 상관관계 정책 관리
- 51-51페이지의 상관관계 이벤트 작업

규정준수 화이트리스트 및 상관관계 응답(알림 및 교정) 생성에 대한 자세한 내용은 다음을 참조하십시오.

- 52-1페이지의 규정준수 툴로 FireSIGHT 시스템 사용
- 43-2페이지의 알림 응답 작업
- 51-1페이지의 상관관계 정책 및 규칙 구성

상관관계 정책에 대한 규칙 생성

라이센스: FireSIGHT, 보호, URL 필터링 또는 악성코드

지원되는 디바이스: 기능에 따라 다름

지원되는 Defense Center: 기능에 따라 다름

상관관계 정책을 생성하려면 먼저 이를 채우기 위한 상관관계 규칙 또는 규정준수 화이트리스트(또는 둘 다)를 생성해야 합니다.

참고 이 절에서는 상관관계 규칙을 생성하는 방법에 대해 설명합니다. 규정준수 화이트리스트 생성에 대한 자세한 내용은 52-8페이지의 규정준수 화이트리스트 생성을/를 참조하십시오.

네트워크 트래픽이 지정된 기준을 충족하면 상관관계 규칙이 트리거됩니다(그리고 상관관계 이벤트가 생성됩니다). 상관관계 규칙을 생성할 때에는 간단한 조건을 사용할 수도 있고, 조건과 제약 조건을 결합하고 중첩하여 좀 더 정교한 구조를 생성할 수도 있습니다.

다음과 같은 방법으로 상관관계 규칙에 기능을 추가할 수 있습니다.

- 트리거링 이벤트와 관련된 호스트의 호스트 프로필에서 정보를 사용하여 규칙을 제한하려면 *호스트 프로필 자격*을 추가합니다.
- 규칙의 초기 기준이 충족된 후 시스템이 특정 연결 추적을 시작할 수 있도록 하려면 상관관계 규칙에 *연결 추적기*를 추가합니다. 그러면 추적된 연결이 추가 조건을 충족하는 경우에만 상관관계 이벤트가 생성됩니다.
- 특정 사용자 또는 사용자 그룹을 추적하려면 상관관계 규칙에 *사용자 자격*을 추가합니다. 예를 들어 소스 또는 대상 사용자의 ID가 특정 사용자(예: 마케팅 부서 사용자)인 경우에만 트리거되도록 상관관계 규칙을 제한할 수 있습니다.
- *유휴 기간* 및 *비활성 기간*을 추가합니다. 상관관계 규칙이 한 번 트리거되면, 유휴 기간은 지정된 기간 동안(규칙 위반이 다시 발생해도) 규칙이 다시 트리거되지 않도록 합니다. 유휴 기간이 경과하면 규칙을 다시 트리거할 수 있습니다(그리고 새 유휴 기간을 시작할 수 있습니다). 비활성 기간 중에는 상관관계 규칙이 트리거되지 않습니다.

주의 자주 발생하는 이벤트에 대해 트리거되는 복잡한 상관관계 규칙을 평가하면 방어 센터 성능이 저하될 수 있습니다. 예를 들어, 시스템에 의해 로깅된 모든 연결에 대해 방어 센터에서 반드시 평가해야 하는 다중 조건 규칙은 리소스 과부하를 일으킬 수 있습니다.

다음 표에서는 효율적인 상관관계 규칙을 작성하기 위해 필요한 라이센스에 대해 설명합니다. 적절한 라이센스가 없는 경우, 라이센스가 없는 FireSIGHT 시스템을 사용하는 상관관계 규칙은 트리거되지 않습니다. 특정 라이센스에 대한 자세한 내용은 65-2페이지의 라이센스 유형 및 제한 사항을/를 참조하십시오.

표 51-1 상관관계 규칙 작성을 위한 라이센스 요구 사항

목적	필요한 라이센스
침입 이벤트 또는 보안 인텔리전스 이벤트에 대해 상관관계 규칙 트리거	보호
검색 이벤트, 호스트 입력 이벤트, 지오로케이션 데이터 또는 사용자 활동에 대해 상관관계 규칙을 트리거하거나, 호스트 프로필 또는 사용자 자격을 상관관계 규칙에 추가	FireSIGHT
연결 이벤트나 엔드포인트 기반 악성코드 이벤트에 대해 상관관계 규칙을 트리거하거나, 연결 추적기를 규칙에 추가	모두

표 51-1 상관관계 규칙 작성을 위한 라이센스 요구 사항 (계속)

목적	필요한 라이센스
URL 데이터가 있는 연결 이벤트에 대해 상관관계 규칙을 트리거하거나, URL 데이터를 사용하여 연결 추적기 작성 Series 2 디바이스와 DC500 방어 센터는 카테고리 또는 평판 기준 URL 필터링을 지원하지 않으며, Series 2 디바이스는 리터럴 URL 또는 URL 그룹 기준 URL 필터링을 지원하지 않습니다.	URL 필터링
네트워크 기반 악성코드 데이터 또는 소급 네트워크 기반 악성코드 데이터 기반의 악성코드 이벤트에 대해 상관관계 규칙 트리거 Series 2 및 Cisco NGIPS for Blue Coat X-Series 디바이스와 DC500 방어 센터는 네트워크 기반 악성코드 차단을 지원하지 않습니다.	악성코드

상관관계 규칙 트리거 기준, 호스트 프로필 자격, 사용자 자격 또는 연결 추적기를 생성할 때 구문은 각기 다르지만 원리는 동일합니다. 자세한 내용은 51-34페이지의 규칙 작성 원리 이해을/를 참조하십시오.

상관관계 규칙을 생성하려면

액세스: Admin/Discovery Admin

1단계 **Policies > Correlation**을 선택한 다음 **Rule Management** 탭을 선택합니다.

Rule Management 페이지가 나타납니다.

2단계 **Create Rule**을 클릭합니다.

Create Rule 페이지가 나타납니다.

3단계 규칙 이름, 설명 및 그룹 등 기본 규칙 정보를 제공합니다.

51-5페이지의 기본 규칙 정보 제공을/를 참조하십시오.

4단계 규칙을 트리거할 기본 기준을 지정합니다.

51-5페이지의 상관관계 규칙 트리거 기준 지정을/를 참조하십시오.

5단계 선택적으로, 호스트 프로필 자격을 규칙에 추가합니다.

51-18페이지의 호스트 프로필 자격 추가을/를 참조하십시오.

6단계 선택적으로, 연결 추적기를 규칙에 추가합니다.

51-22페이지의 시간별 연결 데이터를 사용하여 상관관계 규칙 제한을/를 참조하십시오.

7단계 선택적으로, 사용자 자격을 규칙에 추가합니다.

51-31페이지의 사용자 자격 추가을/를 참조하십시오.

8단계 선택적으로, 비활성 기간 또는 유휴 기간(또는 둘 모두)을 규칙에 추가합니다.

51-32페이지의 유휴 기간 및 비활성 기간 추가을/를 참조하십시오.

9단계 **Save Rule**을 클릭합니다.

규칙이 저장됩니다. 이제 상관관계 정책 내에서 또는 동일한 이벤트 유형에 대해 트리거되는 다른 상관관계 규칙 내에서 규칙을 사용할 수 있습니다.

기본 규칙 정보 제공

라이센스: 모두

각 상관관계 규칙에 이름을 지정해야 하며, 선택적으로 짧은 설명을 지정할 수 있습니다. 규칙을 규칙 그룹에 둘 수도 있습니다.

기본 규칙 정보를 제공하려면

액세스: Admin/Discovery Admin

1단계 **Policies > Correlation**을 선택한 다음 **Rule Management** 탭을 선택합니다.

Rule Management 페이지가 나타납니다.

2단계 **Create Rule**을 클릭합니다.

Create Rule 페이지가 나타납니다.

3단계 Create Rule 페이지의 **Rule Name** 필드에 규칙의 이름을 입력합니다.

4단계 **Rule Description** 필드에 규칙에 대한 설명을 입력합니다.

5단계 선택적으로, **Rule Group** 드롭다운 목록에서 규칙에 대한 그룹을 선택합니다.

규칙 그룹에 대한 자세한 내용은 51-41페이지의 상관관계 정책에 대한 규칙 관리를 참고하십시오.

6단계 다음 절, 상관관계 규칙 트리거 기준 지정에서 절차를 계속 진행합니다.

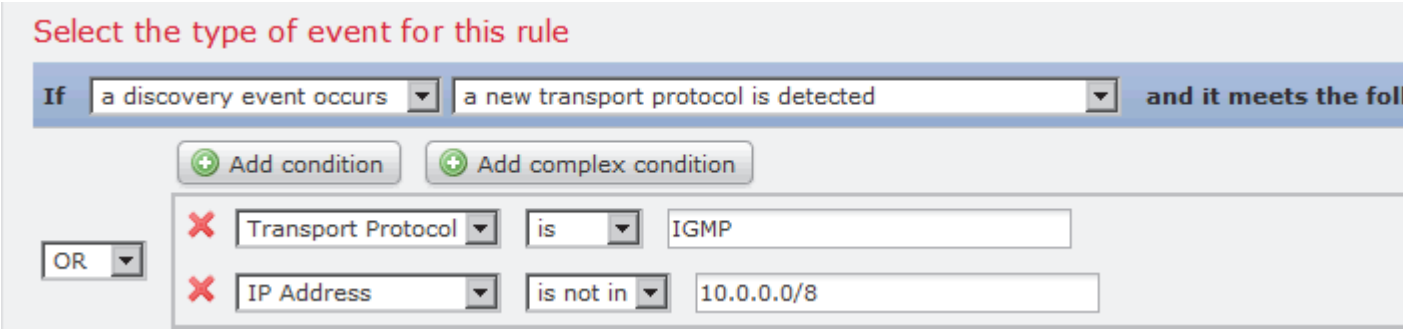
상관관계 규칙 트리거 기준 지정

라이센스: 기능에 따라 다름

지원되는 디바이스: 기능에 따라 다름

지원되는 Defense Center: 기능에 따라 다름

간단한 상관관계 규칙의 경우 특정 유형의 이벤트가 발생하기만 하면 됩니다. 더 구체적인 조건을 제공할 필요가 없습니다. 예를 들어 트래픽 프로필 변경 기반의 상관관계 규칙에는 조건이 전혀 필요하지 않습니다. 이와 달리 여러 개의 중첩된 조건을 포함하는 복합 상관관계 규칙도 있습니다. 예를 들어 다음 그림에 보이는 규칙에는 10.x.x.x 서브넷에 없는 IP 주소가 IGMP 메시지를 전송할 경우 규칙을 트리거하는 기준이 포함되어 있습니다.



참고 이벤트를 기준으로 조건을 작성할 경우에는, 디바이스가 조건에 필요한 정보를 수집할 수 있고 방어 센터가 해당 정보를 관리할 수 있을 때에만 상관관계 규칙 트리거 기준을 추가할 수 있습니다. 예를 들어 Series 2 디바이스와 DC500 방어 센터는 SSL 검사, 카테고리 또는 평판 기준 URL 필터링 또는 보안 인텔리전스를 지원하지 않으므로 이러한 기능을 기반으로 해당 어플라이언스에서 이벤트 조건을 구성할 수 없습니다. 자세한 내용은 51-3페이지의 상관관계 정책에 대한 규칙 생성을/를 참조하십시오.

상관관계 규칙 트리거 기준을 지정하려면

액세스: Admin/Discovery Admin

1단계 규칙의 기반으로 사용할 이벤트 유형을 선택합니다.

상관관계 규칙을 작성할 때에는 먼저 규칙의 기반으로 사용할 이벤트의 유형을 선택해야 합니다. **Select the type of event for this rule** 아래에 몇 가지 옵션이 있습니다.

- 특정 침입 이벤트가 발생할 때 규칙을 트리거하려면 **an intrusion event occurs**를 선택합니다.
- 특정 악성코드 이벤트가 발생할 때 규칙을 트리거하려면 **a Malware event occurs**를 선택합니다.
- 특정 검색 이벤트가 발생할 때 규칙을 트리거하려면 **a discovery event occurs**를 선택합니다. 검색 이벤트에 대해 상관관계 규칙을 트리거할 때에는 사용할 이벤트 유형도 선택해야 합니다. 50-9페이지의 검색 이벤트 유형 이해에 설명된 검색 이벤트의 하위 집합 중에서 선택할 수 있습니다. 예를 들어 홉(hop)의 변경에 대해서는 상관관계 규칙을 트리거할 수는 없습니다. 그러나 유형과 상관없이 검색 이벤트가 발생할 때 규칙을 트리거하려면 **there is any type of event**를 선택합니다.
- 새 사용자가 탐지되거나 사용자가 호스트에 로그인할 때 규칙을 트리거하려면 **user activity is detected**를 선택합니다.
- 특정 입력 이벤트가 발생할 때 규칙을 트리거하려면 **a host input event occurs**를 선택합니다. 호스트 입력 이벤트에 대해 상관관계 규칙을 트리거할 때에는 사용할 이벤트 유형도 선택해야 합니다. 50-13페이지의 호스트 입력 이벤트 유형 이해에 설명된 이벤트의 하위 집합 중에서 선택할 수 있습니다.
- 연결 데이터가 특정 기준을 충족할 때 규칙을 트리거하려면 **a connection event occurs**를 선택합니다. 연결 이벤트에 대해 상관관계 규칙을 트리거할 때에는 연결의 시작이나 끝을 나타내는 연결 이벤트를 사용할지 여부를 선택해야 합니다.
- 네트워크 트래픽이 기존 트래픽 프로필에 기술된 정상적인 네트워크 트래픽 패턴에서 벗어날 때 상관관계 규칙을 트리거하려면 **a traffic profile changes**를 선택합니다.

2단계 규칙의 조건을 지정합니다.

상관관계 규칙 트리거 기준 조건 내에 사용할 수 있는 구문은 1단계에서 선택한 기본 이벤트에 따라 각기 다르지만 원리는 동일합니다. 자세한 내용은 51-34페이지의 규칙 작성 원리 이해을/를 참조하십시오.

조건 작성 시 사용할 수 있는 구문에 대해서는 다음 절에서 자세히 설명합니다.

- 51-7페이지의 침입 이벤트 구문
- 51-9페이지의 악성코드 이벤트 구문
- 51-11페이지의 검색 이벤트 구문
- 51-13페이지의 사용자 활동 이벤트 구문
- 51-13페이지의 호스트 입력 이벤트 구문
- 51-14페이지의 연결 이벤트 구문
- 51-17페이지의 트래픽 프로필 변경 구문

팁 1단계에서 지정한 기본 이벤트 유형을 공유하는 규칙을 중첩할 수 있습니다. 예를 들어 열린 TCP 포트의 탐지를 기반으로 새 규칙을 생성하는 경우 새 규칙에 대한 트리거 기준에 **rule "MyDoom Worm" is true** 및 **rule "Kazaa (TCP) P2P" is true**를 포함할 수 있습니다.

3단계 선택적으로, 다음 절의 절차를 계속 진행합니다.

- 51-18페이지의 호스트 프로필 자격 추가
- 51-22페이지의 시간별 연결 데이터를 사용하여 상관관계 규칙 제한
- 51-31페이지의 사용자 자격 추가
- 51-32페이지의 유휴 기간 및 비활성 기간 추가

상관관계 규칙 작성을 완료했으면 51-3페이지의 상관관계 정책에 대한 규칙 생성의 절차 중 9단계를 수행하여 규칙을 저장하십시오.

침입 이벤트 구문

라이센스: 보호

다음 표에서는 기본 이벤트로 침입 이벤트를 선택할 경우 상관관계 규칙 조건을 작성하는 방법에 대해 설명합니다.

규칙 조건을 작성할 때에는 네트워크 트래픽이 규칙을 트리거할 수 있는지 확인해야 합니다. 개별 침입 이벤트에 대해 사용 가능한 정보는 탐지 방법과 로깅 방법을 비롯한 여러 요소에 따라 달라집니다. 자세한 내용은 41-10페이지의 침입 이벤트 이해을/를 참조하십시오.

표 51-2 침입 이벤트 구문

지정할 항목	연산자 선택 후 수행할 작업
액세스 제어 정책	침입 이벤트를 생성한 침입 정책을 사용하는 액세스 제어 정책을 하나 이상 선택합니다.
Access Control Rule Name	침입 이벤트를 생성한 침입 정책을 사용하는 액세스 제어 규칙의 이름 전체 또는 일부를 입력합니다.
Application Protocol	침입 이벤트와 관련된 애플리케이션 프로토콜을 하나 이상 선택합니다.
Application Protocol Category	애플리케이션 프로토콜 카테고리를 하나 이상 선택합니다.
분류	분류를 하나 이상 선택합니다.
클라이언트	침입 이벤트와 관련된 클라이언트를 하나 이상 선택합니다.
Client Category	클라이언트 카테고리를 하나 이상 선택합니다.
Destination Country 또는 Source Country	침입 이벤트에서 소스 또는 목적지 IP 주소와 관련된 국가를 하나 이상 선택합니다.
Destination IP, Source IP 또는 Source/Destination IP	단일 IP 주소 또는 주소 블록을 지정합니다. FireSIGHT 시스템에서 IP 주소 표기법 및 접두사 길이를 사용하는 방법에 대한 자세한 내용은 1-19페이지의 IP 주소 표기 규칙을/를 참조하십시오.
Destination Port/ICMP Code 또는 Source Port/ICMP Type	소스 트래픽의 포트 번호나 ICMP 유형 또는 대상 트래픽의 포트 번호나 ICMP 유형을 입력합니다.
디바이스	이벤트를 생성했을 것 같은 디바이스를 하나 이상 선택합니다.
Egress Interface 또는 Ingress Interface	인터페이스를 하나 이상 선택합니다.

표 51-2 침입 이벤트 구문 (계속)

지정할 항목	연산자 선택 후 수행할 작업
Egress Security Zone 또는 Ingress Security Zone	보안 영역을 하나 이상 선택합니다.
Generator ID	프리프로세서를 하나 이상 선택합니다. 사용 가능한 프리프로세서에 대한 자세한 내용은 26-6페이지의 네트워크 분석 정책에서 프리프로세서 구성을/를 참조하십시오.
Impact Flag	침입 이벤트에 할당된 영향 레벨을 선택합니다. `is`, `is not`, `is greater than` 등을 지정하는 연산자와 함께 다음 중 하나를 선택합니다. • 0 - 회색(Unknown) • 1 - 빨간색(Vulnerable) • 2 - 주황색(Potentially Vulnerable) • 3 - 노란색(Currently Not Vulnerable) • 4 - 파란색(Unknown Target) **참고** NetFlow 데이터를 기반으로 네트워크 맵에 추가된 호스트에 대해 사용할 수 있는 운영 체제 정보가 없으므로, 호스트 입력 기능을 사용하여 호스트 운영 체제 ID를 수동으로 설정하지 않는 한 방어 센터에서는 그러한 호스트와 관련된 침입 이벤트에 대해 Vulnerable (level 1: red) 영향 레벨을 할당할 수 없습니다. 자세한 내용은 41-38페이지의 이벤트를 평가하기 위한 영향 레벨 사용을/를 참조하십시오.
Inline Result	다음 중 하나를 선택합니다. • **dropped** - 패킷이 인라인, 스위치드 또는 라우티드 구축에서 삭제되었는지 여부를 지정 • **would have dropped** - 인라인, 스위치드 또는 라우티드 구축에서 패킷을 삭제하도록 침입 정책을 설정했다면 패킷이 삭제되었을 것인지를 지정 침입 정책의 규칙 상태 또는 삭제 동작과 상관없이, 인라인 집합이 탭 모드인 경우를 포함하여 패시브 구축에서는 시스템이 패킷을 삭제하지 않습니다.
침입 정책	침입 이벤트를 생성한 침입 정책을 하나 이상 선택합니다.
IOC 태그	침입 이벤트의 결과로 IOC 태그의 설정(`is` 또는 `is not`)을 선택합니다.
Priority(우선순위)	규칙 우선순위(**low**, **medium** 또는 **high**)를 선택합니다. 규칙 기반 침입 이벤트의 경우 우선순위는 `priority` 키워드의 값 또는 `classtype` 키워드의 값에 해당합니다. 기타 침입 이벤트의 경우 우선순위는 디코더 또는 프리프로세서에 의해 결정됩니다.
프로토콜	전송 프로토콜의 이름이나 번호를 http://www.iana.org/assignments/protocol-numbers 에 표시된 대로 입력합니다.
Rule Message	규칙 메시지의 전체 또는 일부를 입력합니다.
규칙 SID	단일 SID(Snort ID number)를 입력하거나, 여러 SID를 쉼표로 구분하여 입력합니다. **참고** 연산자로 **is in** 또는 **is not in**을 선택하는 경우 다중 선택 팝업 창을 사용할 수 없습니다. 쉼표로 구분된 SID 목록을 입력해야 합니다.
규칙 유형	규칙이 로컬인지 여부를 지정합니다. 로컬 규칙에는 사용자 지정 표준 텍스트 침입 규칙, 수정된 표준 텍스트 규칙, 수정된 헤더 정보와 함께 규칙을 저장했을 때 생성된 공유 객체 규칙이 포함됩니다. 자세한 내용은 36-104페이지의 기존 규칙 수정을/를 참조하십시오.

표 51-2 침입 이벤트 구문 (계속)

지정할 항목	연산자 선택 후 수행할 작업
SSL Actual Action	시스템이 암호화된 연결을 처리한 방법을 나타내는 SSL 규칙 작업을 선택합니다.
SSL Certificate Fingerprint	트래픽을 암호화하는 데 사용된 인증서의 핑거프린트를 입력하거나, 핑거프린트와 연결된 주체 CN을 선택합니다.
SSL Certificate Subject Common Name (CN)	세션 암호화에 사용된 인증서의 주체 CN 전체 또는 일부를 입력합니다.
SSL Certificate Subject Country (C)	세션 암호화에 사용된 인증서의 주체 국가 코드를 하나 이상 선택합니다.
SSL Certificate Subject Organization (O)	세션 암호화에 사용된 인증서의 주체 조직 이름 전체 또는 일부를 입력합니다.
SSL Certificate Subject Organizational Unit (OU)	세션 암호화에 사용된 인증서의 주체 OU 전체 또는 일부를 입력합니다.
SSL Flow Status	트래픽을 해독하려는 시스템의 결과를 기반으로 상태를 하나 이상 선택합니다.
아이디	침입 이벤트의 소스 호스트에 로그인한 사용자의 사용자 이름을 입력합니다.
VLAN ID	침입 이벤트를 트리거한 패킷과 관련된 가장 안쪽 VLAN ID를 입력합니다.
Web Application	침입 이벤트와 관련된 웹 애플리케이션을 하나 이상 선택합니다.
Web Application Category	웹 애플리케이션 카테고리를 하나 이상 선택합니다.

악성코드 이벤트 구문

라이센스: 모두 또는 악성코드

지원되는 디바이스: 기능에 따라 다름

지원되는 Defense Center: 기능에 따라 다름

악성코드 이벤트 기반 상관관계 규칙 조건의 구문은 이벤트가 엔드포인트 기반 악성코드 에이전트에 의해 보고되었는지, 관리되는 디바이스에 의해 탐지되었는지, 관리되는 디바이스에 의해 탐지되고 악성코드로 소급 식별되었는지 여부에 따라 달라집니다.

Series 2 및 Cisco NGIPS for Blue Coat X-Series 디바이스와 DC500 방어 센터는 네트워크 기반 악성코드 차단을 지원하지 않으므로, 이러한 어플라이언스에서는 네트워크 기반 악성코드 데이터 또는 소급 네트워크 기반 악성코드 데이터 기반의 악성코드 이벤트에 대한 상관관계 규칙의 트리거가 지원되지 않습니다.

규칙 조건을 작성할 때에는 네트워크 트래픽이 규칙을 트리거할 수 있는지 확인해야 합니다. 개별 연결 또는 연결 요약 이벤트에 사용 가능한 정보는 탐지 방법, 로깅 방법, 이벤트 유형 등 여러 요인에 따라 달라집니다. 자세한 내용은 40-21페이지의 악성코드 이벤트 테이블 이해을/를 참조하십시오.

다음 표에서는 기본 이벤트로 악성코드 이벤트를 선택할 경우 상관관계 규칙 조건을 작성하는 방법에 대해 설명합니다.

표 51-3 악성코드 이벤트 구문

지정할 항목	연산자 선택 후 수행할 작업
Application Protocol	악성코드 이벤트와 관련된 애플리케이션 프로토콜을 하나 이상 선택합니다.
Application Protocol Category	애플리케이션 프로토콜 카테고리를 하나 이상 선택합니다.
클라이언트	악성코드 이벤트와 관련된 클라이언트를 하나 이상 선택합니다.

표 51-3 악성코드 이벤트 구문 (계속)

지정할 항목	연산자 선택 후 수행할 작업
Client Category	클라이언트 카테고리를 하나 이상 선택합니다.
Destination Country 또는 Source Country	악성코드 이벤트에서 소스 또는 목적지 IP 주소와 관련된 국가를 하나 이상 선택합니다.
Destination IP, Host IP 또는 Source IP	단일 IP 주소 또는 주소 블록을 지정합니다. FireSIGHT 시스템에서 IP 주소 표기법을 사용하는 방법에 대한 자세한 내용은 1-19페이지의 IP 주소 표기 규칙을/를 참조하십시오.
Destination Port/ICMP Code	대상 트래픽의 포트 번호 또는 ICMP 코드를 입력합니다.
구성	`Malware` 또는 `Custom Detection` 중 하나 또는 둘 모두를 선택합니다.
이벤트 유형	악성코드 이벤트와 관련된 엔드포인트 기반 이벤트 유형을 하나 이상 선택합니다. 자세한 내용은 40-25페이지의 악성코드 이벤트 유형을/를 참조하십시오.
파일 이름	파일의 이름을 입력합니다.
파일 유형	파일의 형식(예: `PDF` 또는 `MSEXE`)을 선택합니다.
File Type Category	파일 형식 카테고리(예: `Office Documents` 또는 `Executables`)를 하나 이상 선택합니다.
IOC 태그	악성코드 이벤트의 결과로 IOC 태그의 설정(`is` 또는 `is not`)을 선택합니다.
SHA-256	파일의 SHA-256 해시 값을 입력하거나 붙여넣습니다.
SSL Actual Action	시스템이 암호화된 연결을 처리한 방법을 나타내는 SSL 규칙 작업을 선택합니다.
SSL Certificate Fingerprint	트래픽을 암호화하는 데 사용된 인증서의 핑거프린트를 입력하거나, 핑거프린트와 연결된 주체 CN을 선택합니다.
SSL Certificate Subject Common Name (CN)	세션 암호화에 사용된 인증서의 주체 CN 전체 또는 일부를 입력합니다.
SSL Certificate Subject Country (C)	세션 암호화에 사용된 인증서의 주체 국가 코드를 하나 이상 선택합니다.
SSL Certificate Subject Organization (O)	세션 암호화에 사용된 인증서의 주체 조직 이름 전체 또는 일부를 입력합니다.
SSL Certificate Subject Organizational Unit (OU)	세션 암호화에 사용된 인증서의 주체 OU 전체 또는 일부를 입력합니다.
SSL Flow Status	트래픽을 해독하려는 시스템의 결과를 기반으로 상태를 하나 이상 선택합니다.
Source Port/ICMP Type	소스 트래픽의 포트 번호 또는 ICMP 유형을 입력합니다.
Web Application	악성코드 이벤트와 관련된 웹 애플리케이션을 하나 이상 선택합니다.
Web Application Category	웹 애플리케이션 카테고리를 하나 이상 선택합니다.

검색 이벤트 구문

라이센스: FireSIGHT

상관관계 규칙이 검색 이벤트를 기반으로 하는 경우, 우선 드롭다운 목록에서 사용하고자 하는 이벤트 유형을 선택해야 합니다. 다음 표에는 트리거 기준으로 드롭다운 목록에서 선택할 수 있는 이벤트 및 해당 이벤트 유형의 상호 참조가 나열되어 있습니다. 검색 이벤트 유형에 대한 자세한 내용은 50-9페이지의 검색 이벤트 유형 이해을/를 참조하십시오.

표 51-4 상관관계 규칙 트리거 기준 대 검색 이벤트 유형

선택 옵션	규칙을 트리거할 이벤트 유형
a client has changed	Client Update
a client timed out	Client Timeout
a host IP address is reused	DHCP: IP Address Reassigned
a host is deleted because the host limit was reached	Host Deleted: Host Limit Reached
a host is identified as a network device	Host Type Changed to Network Device
a host timed out	Host Timeout
a host's IP address has changed	DHCP: IP Address Changed
a NETBIOS name change is detected	NETBIOS Name Change
a new client is detected	New Client
a new IP host is detected	New Host
a new MAC address is detected	Additional MAC Detected for Host
a new MAC host is detected	New Host
a new network protocol is detected	New Network Protocol
a new transport protocol is detected	New Transport Protocol
a TCP port closed	TCP Port Closed
a TCP port timed out	TCP Port Timeout
a UDP port closed	UDP Port Closed
a UDP port timed out	UDP Port Timeout
a VLAN tag was updated	VLAN Tag Information Update
an IOC was set	Indication of Compromise
an open TCP port is detected	New TCP Port
an open UDP port is detected	New UDP Port
the OS information for a host has changed	최신 OS
the OS or server identity for a host has a conflict	Identity Conflict
the OS or server identity for a host has timed out	Identity Timeout
there is any kind of event	any event type
there is new information about a MAC address	MAC Information Change
there is new information about a TCP server	TCP Server Information Update
there is new information about a UDP server	UDP Server Information Update

홉이 변경되는 경우 또는 라이센스가 있는 호스트 제한에 도달하여 시스템이 새 호스트를 삭제하는 경우 상관관계 규칙을 트리거할 수 없습니다. 그러나 유형과 상관없이 검색 이벤트가 발생할 때 규칙을 트리거하려면 **there is any type of event**를 선택합니다.

검색 이벤트 유형을 선택했으면 아래 표에 설명된 대로 상관관계 규칙 조건을 작성할 수 있습니다. 선택하는 이벤트 유형에 따라, 다음 표에 나와 있는 기준의 하위 집합을 사용하여 조건을 작성할 수 있습니다. 예를 들어 새 클라이언트가 탐지될 때 상관관계 규칙을 트리거하려면 호스트의 IP 또는 MAC 주소, 클라이언트 이름, 유형, 버전, 그리고 이벤트를 탐지한 디바이스를 기반으로 조건을 작성할 수 있습니다.

표 51-5 검색 이벤트 구문

지정할 항목	연산자 선택 후 수행할 작업
Application Protocol	애플리케이션 프로토콜을 하나 이상 선택합니다.
Application Protocol Category	애플리케이션 프로토콜 카테고리를 하나 이상 선택합니다.
애플리케이션 포트	애플리케이션 프로토콜 포트 번호를 입력합니다.
Client	클라이언트를 하나 이상 선택합니다.
Client Category	클라이언트 카테고리를 하나 이상 선택합니다.
Client Version	클라이언트의 버전 번호를 입력합니다.
디바이스	검색 이벤트를 생성했을 것 같은 디바이스를 하나 이상 선택합니다.
하드웨어	모바일 디바이스의 하드웨어 모델을 입력합니다. 예를 들어 일치하는 모든 Apple iPhone을 찾으려면 `iPhone`을 입력합니다.
Host Type	드롭다운 목록에서 호스트 유형을 하나 이상 선택합니다. 호스트를 선택하거나 여러 네트워크 디바이스 유형 중 하나를 선택할 수 있습니다.
IP Address 또는 New IP Address	단일 IP 주소 또는 주소 블록을 입력합니다. FireSIGHT 시스템에서 IP 주소 표기법을 사용하는 방법에 대한 자세한 내용은 1-19페이지의 IP 주소 표기 규칙을/를 참조하십시오.
Jailbroken	이벤트의 호스트가 탈옥 모바일 디바이스이면 **Yes**, 아니면 **No**를 선택합니다.
MAC 주소	호스트의 MAC 주소 전체 또는 일부를 입력합니다. 예를 들어 특정 하드웨어 제조업체 디바이스의 MAC 주소가 0A:12:34로 시작하는 것을 알고 있다면 연산자로 **begins with**를 선택하고 값으로 `0A:12:34`를 입력할 수 있습니다.
MAC 유형	MAC 주소가 **ARP/DHCP Detected**인지 여부를 선택합니다. 즉 시스템에서 MAC 주소를 호스트에 속한 것(**ARP/DHCP Detected**)으로 확실하게 식별했는지, 또는 관리되는 디바이스와 호스트 간에 라우터가 있다는 등의 이유로 여러 호스트가 해당 MAC 주소를 갖는지(**is not ARP/DHCP Detected**) 여부를 선택합니다.
MAC Vendor	검색 이벤트를 트리거한 네트워크 트래픽에 의해 사용된 NIC의 MAC 하드웨어 공급업체 이름 전체 또는 일부를 입력합니다.
모바일	이벤트의 호스트가 모바일 디바이스이면 **Yes**, 아니면 **No**를 선택합니다.
NETBIOS 이름	호스트의 NetBIOS 이름을 입력합니다.
Network Protocol	네트워크 프로토콜 번호를 http://www.iana.org/assignments/ethernet-numbers에 표시된 대로 입력합니다.
OS 이름	운영 체제 이름을 하나 이상 선택합니다.
OS Vendor	운영 체제 공급업체를 하나 이상 선택합니다.
OS 버전	운영 체제 버전을 하나 이상 선택합니다.

표 51-5 검색 이벤트 구문 (계속)

지정할 항목	연산자 선택 후 수행할 작업
Protocol 또는 Transport Protocol	전송 프로토콜의 이름이나 번호를 http://www.iana.org/assignments/protocol-numbers 에 표시된 대로 입력합니다.
소스	호스트 입력 데이터의 소스를 선택합니다(운영 체제와 서버 ID의 변경 및 시간 초과에 대해).
소스 유형	호스트 입력 데이터의 소스 유형을 선택합니다(운영 체제와 서버 ID의 변경 및 시간 초과에 대해).
VLAN ID	이벤트와 관련된 호스트 VLAN ID를 입력합니다.
Web Application	웹 애플리케이션을 선택합니다.

사용자 활동 이벤트 구문

라이센스: FireSIGHT

상관관계 규칙이 사용자 활동을 기반으로 하는 경우, 우선 드롭다운 목록에서 사용하고자 하는 사용자 활동을 선택해야 합니다.

- 사용자가 호스트에 로그인함, 또는
- 새 사용자 ID가 탐지됨

사용자 활동 유형을 선택했으면 아래 표에 설명된 대로 상관관계 규칙 조건을 작성할 수 있습니다. 선택하는 사용자 활동 유형에 따라 다음 표에 나와 있는 기준의 하위 집합을 사용하는 조건을 작성할 수 있습니다. 새 사용자 ID에 대해 트리거되는 상관관계 규칙의 경우 IP 주소를 지정할 수 없습니다.

표 51-6 사용자 활동 구문

지정할 항목	연산자 선택 후 수행할 작업
디바이스	사용자 활동을 탐색했을 것 같은 디바이스를 하나 이상 선택합니다.
IP 주소	단일 IP 주소 또는 주소 블록을 입력합니다. FireSIGHT 시스템에서 IP 주소 표기법을 사용하는 방법에 대한 자세한 내용은 1-19페이지의 IP 주소 표기 규칙을/를 참조하십시오.
아이디	사용자 이름을 입력합니다.

호스트 입력 이벤트 구문

라이센스: FireSIGHT

상관관계 규칙이 호스트 입력 이벤트를 기반으로 하는 경우, 우선 드롭다운 목록에서 사용하고자 하는 호스트 입력 이벤트 유형을 선택해야 합니다. 다음 표에는 트리거 기준으로 드롭다운 목록에서 선택할 수 있는 이벤트 및 해당 호스트 입력 이벤트 유형의 상호 참조가 나열되어 있습니다. 호스트 입력 이벤트 유형에 대한 자세한 내용은 50-13페이지의 호스트 입력 이벤트 유형 이해을/를 참조하십시오.

표 51-7 상관관계 규칙 트리거 기준 대 호스트 입력 이벤트 유형

선택 옵션	규칙을 트리거할 이벤트 유형
a client is added	Add Client
a client is deleted	Delete Client
a host is added	Add Host

표 51-7 상관관계 규칙 트리거 기준 대 호스트 입력 이벤트 유형 (계속)

선택 옵션	규칙을 트리거할 이벤트 유형
a protocol is added	Add Protocol
a protocol is deleted	Delete Protocol
a scan result is added	Add Scan Result
a server definition is set	Set Server Definition
a server is added	Add Port
a server is deleted	Delete Port
a vulnerability is marked invalid	Vulnerability Set Invalid
a vulnerability is marked valid	Vulnerability Set Valid
an address is deleted	Delete Host/Network
an attribute value is deleted	Host Attribute Delete Value
an attribute value is set	Host Attribute Set Value
an OS definition is set	Set Operating System Definition
host criticality is set	Set Host Criticality

사용자 정의 호스트 특성의 정의를 추가, 삭제 또는 변경할 때나 취약성 영향 자격을 설정할 때는 상관관계 규칙을 트리거할 수 없습니다.

호스트 입력 이벤트 유형을 선택했으면 아래 표에 설명된 대로 상관관계 규칙 조건을 작성할 수 있습니다. 선택하는 호스트 입력 이벤트 유형에 따라, 다음 표에 나와 있는 기준의 하위 집합을 사용하여 조건을 작성할 수 있습니다. 예를 들어 클라이언트가 삭제될 때 상관관계 규칙을 트리거하려면 이벤트, 삭제의 소스 유형(수동, 서드파티 애플리케이션 또는 스캐너) 및 소스 자체(특정 스캐너 유형 또는 사용자)와 관련된 호스트의 IP 주소를 기반으로 조건을 작성할 수 있습니다

표 51-8 호스트 입력 이벤트 구문

지정할 항목	연산자 선택 후 수행할 작업
IP 주소	단일 IP 주소 또는 주소 블록을 입력합니다. FireSIGHT 시스템에서 IP 주소 표기법을 사용하는 방법에 대한 자세한 내용은 1-19페이지의 IP 주소 표기 규칙을/를 참조하십시오.
소스	호스트 입력 데이터의 소스를 선택합니다.
소스 유형	호스트 입력 데이터의 소스 유형을 선택합니다.

연결 이벤트 구문

라이센스: 모두

상관관계 규칙이 연결 이벤트를 기반으로 하는 경우, 우선 연결의 시작이나 끝을 나타내는 연결 이벤트를 사용할지 여부를 선택해야 합니다. 연결 이벤트 유형을 선택했으면 연결 이벤트 구문 표에 설명된 대로 상관관계 규칙 조건을 작성할 수 있습니다.

규칙 조건을 작성할 때에는 네트워크 트래픽이 규칙을 트리거할 수 있는지 확인해야 합니다. 개별 연결 또는 연결 요약 이벤트에 사용 가능한 정보는 탐지 방법, 로깅 방법, 이벤트 유형 등 여러 요인에 따라 달라집니다. 자세한 내용은 39-11페이지의 연결 및 보안 인텔리전스 이벤트에서 제공되는 정보을/를 참조하십시오.

표 51-9 연결 이벤트 구문

지정할 항목	연산자 선택 후 수행할 작업
액세스 제어 정책	연결을 로깅한 액세스 제어 정책을 하나 이상 선택합니다.
Access Control Rule Action	연결을 로깅한 액세스 제어 규칙과 관련된 작업을 하나 이상 선택합니다. **참고** 나중에 연결을 처리하는 기본 작업 또는 규칙과 상관없이, 네트워크 트래픽이 Monitor 규칙의 조건과 일치할 때 상관관계 이벤트를 트리거하려면 **Monitor**를 선택합니다.
Access Control Rule Name	연결을 로깅한 액세스 제어 규칙의 이름 전체 또는 일부를 입력합니다. **참고** 나중에 연결을 처리하는 기본 작업 또는 규칙과 상관없이, 연결 기준으로 조건이 일치한 Monitor 규칙의 이름을 입력할 수 있습니다.
Application Protocol	연결과 관련된 애플리케이션 프로토콜을 하나 이상 선택합니다.
Application Protocol Category	애플리케이션 프로토콜 카테고리를 하나 이상 선택합니다.
Client	클라이언트를 하나 이상 선택합니다.
Client Category	클라이언트 카테고리를 하나 이상 선택합니다.
Client Version	클라이언트의 버전 번호를 입력합니다.
Connection Duration	연결 이벤트의 기간을 초 단위로 입력합니다.
연결 유형	상관관계 규칙의 트리거를 Cisco 관리되는 디바이스(**FireSIGHT**)에서 연결을 탐지했는지를 기반으로 할지, NetFlow 지원 디바이스(**NetFlow**)에서 연결을 내보냈는지를 기반으로 할지를 선택합니다.
Destination Country 또는 Source Country	연결 이벤트에서 소스 또는 목적지 IP 주소와 관련된 국가를 하나 이상 선택합니다.
디바이스	연결을 탐지한 디바이스 또는 연결을 처리한 디바이스(NetFlow 지원 디바이스에서 내보낸 연결 데이터에 대해)를 하나 이상 선택합니다.
Egress Interface 또는 Ingress Interface	인터페이스를 하나 이상 선택합니다.
Egress Security Zone 또는 Ingress Security Zone	보안 영역을 하나 이상 선택합니다.
Initiator Bytes, Responder Bytes 또는 Total Bytes	다음 중 하나 입력: • 전송된 바이트 수(**Initiator Bytes**) • 수신된 바이트 수(**Responder Bytes**) • 전송 및 수신된 바이트 수(**Total Bytes**)
Initiator IP, Responder IP 또는 Initiator/Responder IP	단일 IP 주소 또는 주소 블록을 지정합니다. FireSIGHT 시스템에서 IP 주소 표기법 및 접두사 길이를 사용하는 방법에 대한 자세한 내용은 1-19페이지의 IP 주소 표기 규칙을/를 참조하십시오.
Initiator Packets, Responder Packets 또는 Total Packets	다음 중 하나 입력: • 전송된 패킷 수(**Initiator Packets**) • 수신된 패킷 수(**Responder Packets**) • 전송 및 수신된 패킷 수(**Total Packets**)

표 51-9 연결 이벤트 구문 (계속)

지정할 항목	연산자 선택 후 수행할 작업
Initiator Port/ICMP Type 또는 Responder Port/ICMP Code	Initiator 트래픽의 포트 번호나 ICMP 유형 또는 responder 트래픽의 포트 번호나 ICMP 코드를 입력합니다.
IOC 태그	연결 이벤트의 결과로 IOC 태그의 설정(`is` 또는 `is not`)을 선택합니다.
NETBIOS 이름	연결에서 모니터링된 호스트의 NetBIOS 이름을 입력합니다.
NetFlow 장치	상관관계 규칙을 트리거하기 위해 사용하려는 연결 데이터를 내보낸 NetFlow 지원 디바이스의 IP 주소를 선택합니다. 구축에 어떤 NetFlow 지원 디바이스도 추가하지 않은 경우 NetFlow Device 드롭다운 목록은 비어 있습니다.
사유	연결 이벤트와 관련된 이유를 하나 이상 선택합니다.
Security Intelligence Category	연결 이벤트와 관련된 보안 인텔리전스 카테고리를 하나 이상 선택합니다. **참고** 연결 끝 이벤트의 조건으로 보안 인텔리전스 카테고리를 사용하려면 액세스 제어 정책의 보안 인텔리전스 섹션에서 **Block** 대신 **Monitor** 조건을 설정해야 합니다. 자세한 내용은 13-3페이지의 보안 인텔리전스 화이트리스트 및 블랙리스트 작성을/를 참조하십시오.
SSL Actual Action	시스템이 암호화된 연결을 처리한 방법을 나타내는 SSL 규칙 작업을 선택합니다.
SSL Certificate Fingerprint	트래픽을 암호화하는 데 사용된 인증서의 핑거프린트를 입력하거나, 핑거프린트와 연결된 주체 CN을 선택합니다.
SSL Certificate Status	세션 암호화에 사용된 인증서와 관련된 상태를 하나 이상 선택합니다.
SSL Certificate Subject Common Name (CN)	세션 암호화에 사용된 인증서의 주체 CN 전체 또는 일부를 입력합니다.
SSL Certificate Subject Country (C)	세션 암호화에 사용된 인증서의 주체 국가 코드를 하나 이상 선택합니다.
SSL Certificate Subject Organization (O)	세션 암호화에 사용된 인증서의 주체 조직 이름 전체 또는 일부를 입력합니다.
SSL Certificate Subject Organizational Unit (OU)	세션 암호화에 사용된 인증서의 주체 OU 전체 또는 일부를 입력합니다.
SSL Cipher Suite	세션 암호화에 사용된 암호 그룹을 하나 이상 선택합니다.
SSL Encrypted Session	**Successfully Decrypted**를 선택합니다.
SSL Flow Status	트래픽을 해독하려는 시스템의 결과를 기반으로 상태를 하나 이상 선택합니다.
SSL Policy	암호화된 연결을 로깅한 SSL 정책을 하나 이상 선택합니다.
SSL Rule Name	암호화된 연결을 로깅한 SSL 규칙의 이름 전체 또는 일부를 입력합니다.
SSL Server Name	클라이언트가 암호화된 연결을 설정한 서버의 이름 전체 또는 일부를 입력합니다.
SSL URL Category	암호화된 연결에서 방문한 URL의 URL 카테고리를 하나 이상 선택합니다.
SSL 버전	세션 암호화에 사용된 SSL 또는 TLS 버전을 하나 이상 선택합니다.
TCP Flags	상관관계 규칙을 트리거하기 위해 연결 이벤트에 포함해야 할 TCP 플래그를 선택합니다. **참고** NetFlow 지원 디바이스에서 내보낸 연결 데이터만 TCP 플래그를 포함합니다.
Transport Protocol	연결에 사용된 전송 프로토콜(`TCP` 또는 `UDP`)을 입력합니다.
URL	연결에서 방문한 URL 전체 또는 일부를 입력합니다.
URL 카테고리	연결에서 방문한 URL의 URL 카테고리를 하나 이상 선택합니다.
URL 평판	연결에서 방문한 URL의 URL 평판 값을 하나 이상 선택합니다.

표 51-9 연결 이벤트 구문 (계속)

지정할 항목	연산자 선택 후 수행할 작업
아이디	연결의 두 호스트 중 하나에 로그인한 사용자의 사용자 이름을 입력합니다.
Web Application	연결과 관련된 웹 애플리케이션을 하나 이상 선택합니다.
Web Application Category	웹 애플리케이션 카테고리를 하나 이상 선택합니다.

트래픽 프로필 변경 구문

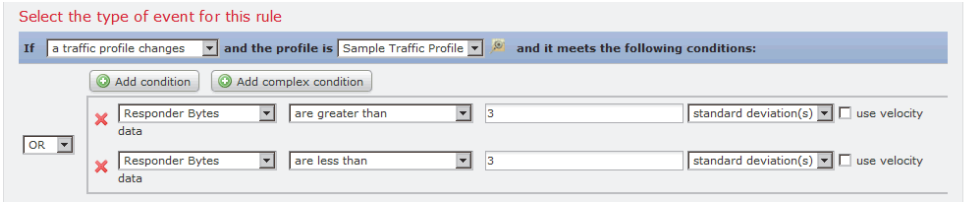
라이센스: 모두

상관관계 규칙이 트래픽 프로필 변경을 기반으로 하는 경우 네트워크 트래픽이 기존 트래픽 프로필에 기술된 정상적인 네트워크 트래픽 패턴에서 벗어날 때 규칙이 트리거됩니다. 트래픽 프로필 작성에 대한 자세한 내용은 53-1페이지의 트래픽 프로필 생성을/를 참조하십시오.

원시 데이터 또는 데이터에서 계산된 통계를 기반으로 규칙을 트리거할 수 있습니다. 예를 들어 네트워크를 통과하는 데이터의 양(바이트 단위로 측정됨)이 급증할 때(공격이나 기타 보안 정책 위반의 징후일 수 있음) 트리거되는 규칙을 작성할 수 있습니다. 다음의 경우 규칙이 트리거되도록 지정할 수 있습니다.

- 네트워크를 통과하는 바이트 수가 평균 트래픽 양의 위 또는 아래에서 표준 편차의 특정 수치 위로 급증하는 경우

  네트워크를 통과하는 바이트의 수가 표준 편차의 특정 수치(위 또는 아래)를 벗어날 때 트리거되는 규칙을 생성하려면 다음 그림에 보이는 것처럼 상한 또는 하한을 지정해야 합니다.



  통과하는 바이트 수가 평균 **위에서** 표준 편차의 특정 수보다 클 때 트리거되는 규칙을 생성하려면 그림에 보이는 첫 번째 조건만 사용하십시오.

  통과하는 바이트 수가 평균 **아래에서** 표준 편차의 특정 수보다 클 때 트리거되는 규칙을 생성하려면 두 번째 조건만 사용하십시오.

- 네트워크를 통과하는 바이트 수가 특정 바이트 수 위로 급증하는 경우

데이터 포인트 간 변경 속도를 기반으로 상관관계 규칙을 트리거하려면 **use velocity data** 확인란(39-18페이지의 그래프 유형 변경 참조)을 선택할 수 있습니다. 위의 예에서 속도 데이터를 사용한다면 다음과 같은 경우 규칙이 트리거되도록 지정할 수 있습니다.

- 네트워크를 통과하는 바이트의 양이 평균 변경 속도 위에서 표준 편차의 특정 수치 위 또는 아래로 급증하는 경우
- 네트워크를 통과하는 바이트 수의 변경이 특정 바이트 수 위로 급증하는 경우

다음 표에서는 기본 이벤트로 트래픽 프로필 변경을 선택할 경우 상관관계 규칙에서 조건을 작성하는 방법에 대해 설명합니다. 트래픽 프로필이 NetFlow 지원 디바이스에서 내보낸 연결 데이터를 사용하는 경우, 탐지 방법이 트래픽 프로필 생성에 사용되는 데이터에 어떤 영향을 미치는지에 대해 자세히 알아보려면 45-17페이지의 NetFlow 및 FireSIGHT 데이터 간 차이점을/를 참조하십시오.

표 51-10 트래픽 프로필 변경 구문

지정할 항목	연산자 선택 후 입력	다음 중 하나 선택
연결 수	탐지된 총 연결 수 **또는** 규칙을 트리거하기 위해 탐지된 연결 수가 속해야 하는 평균 위 또는 아래 표준 편차의 수	connections standard deviation(s)
Total Bytes, Initiator Bytes 또는 Responder Bytes	다음 중 하나: • 전송된 총 바이트(**Total Bytes**) • 전송된 바이트 수(**Initiator Bytes**) • 수신된 바이트 수(**Responder Bytes**) **또는** 규칙을 트리거하기 위해 위 기준 중 하나가 속해야 하는 평균 위 또는 아래 표준 편차의 수	bytes standard deviation(s)
Total Packets, Initiator Packets 또는 Responder Packets	다음 중 하나: • 전송된 총 패킷(**Total Packets**) • 전송된 패킷 수(**Initiator Packets**) • 수신된 패킷 수(**Responder Packets**) **또는** 규칙을 트리거하기 위해 위 기준 중 하나가 속해야 하는 평균 위 또는 아래 표준 편차의 수	packets standard deviation(s)
Unique Initiators	세션을 시작한 고유한 호스트의 수 **또는** 규칙을 트리거하기 위해 탐지된 고유한 initiator 수가 속해야 하는 평균 위 또는 아래 표준 편차의 수	initiators standard deviation(s)
Unique Responders	세션에 응답한 고유한 호스트의 수 **또는** 규칙을 트리거하기 위해 탐지된 고유한 responder 수가 속해야 하는 평균 위 또는 아래 표준 편차의 수	responders standard deviation(s)

호스트 프로필 자격 추가

라이센스: FireSIGHT

연결, 침입, 검색, 사용자 활동 또는 호스트 입력 이벤트를 사용하여 상관관계 규칙을 트리거하는 경우, 이벤트와 관련된 호스트의 호스트 프로필을 기반으로 규칙을 제한할 수 있습니다. 이러한 제약을 *호스트 프로필 자격(host profile qualification)*이라고 합니다.

참고 악성코드 이벤트, 트래픽 프로필 변경 또는 새 IP 호스트 탐색에 대해 트리거되는 상관관계 규칙에 호스트 프로필 자격을 추가할 수 **없습니다**.

예를 들어, Microsoft Windows 컴퓨터만이 규칙을 작성한 취약성에 취약하기 때문에 Microsoft Windows 호스트가 문제가 되는 트래픽의 대상인 경우에만 트리거되도록 상관관계 규칙을 제한할 수 있습니다. 또 다른 예로, 호스트가 화이트리스트의 규정준수를 벗어나는 경우에만 트리거되도록 상관관계 규칙을 제한할 수 있습니다.

암시된 클라이언트 또는 일반 클라이언트에 매칭하려면 클라이언트에 응답하는 서버에서 사용하는 애플리케이션 프로토콜에 따라 호스트 프로필 자격을 생성합니다. 연결의 initiator 또는 소스가 되는 호스트의 클라이언트 목록에서 어떤 애플리케이션 프로토콜 이름 다음에 **클라이언트**가 올 경우 그 클라이언트는 암시된 클라이언트일 수 있습니다. 즉 시스템은 탐지된 클라이언트 트래픽이 아니라 해당 클라이언트에 대해 애플리케이션 프로토콜을 사용하는 서버 응답 트래픽을 기반으로 클라이언트를 보고합니다.

예를 들어 시스템에서 호스트의 클라이언트로 **HTTPS 클라이언트**를 보고할 경우 **Responder Host** 또는 **Destination Host**에 대한 호스트 프로필 자격을 생성하며 여기서 **Application Protocol**은 **HTTPS**로 설정됩니다. Responder 또는 목적지 호스트에서 보낸 HTTPS 서버 응답 트래픽에 따라 **HTTPS 클라이언트**가 일반 클라이언트로 보고되기 때문입니다.

호스트 프로필 자격을 사용하려면 호스트가 네트워크 맵에 있고 자격으로 사용하려는 호스트 프로필 속성이 이미 호스트 프로필에 포함된 상태여야 합니다. 예를 들어 Windows를 실행하는 호스트에서 침입 이벤트가 생성될 때 트리거할 상관관계 규칙을 구성할 경우, 침입 이벤트 생성 시점에 이미 호스트가 Windows로 식별된 상태여야 규칙이 트리거됩니다.

호스트 프로필 자격을 추가하려면

액세스: Admin/Discovery Admin

1단계 **Policies > Correlation**을 선택한 다음 Rule Management 탭을 선택합니다.

Rule Management 페이지가 나타납니다.

2단계 **Create Rule**을 클릭합니다.

Create Rule 페이지가 나타납니다.

3단계 Create Rule 페이지에서 **Add Host Profile Qualification**을 클릭합니다.

Host Profile Qualification 섹션이 나타납니다.

팁 호스트 프로필 자격을 제거하려면 **Remove Host Profile Qualification**을 클릭합니다.

4단계 호스트 프로필 자격의 조건을 작성합니다.

하나의 단순한 조건을 생성할 수도 있고, 여러 조건을 연결하고 중첩하여 더 정교한 구성으로 만들 수도 있습니다. 웹 인터페이스를 사용하여 조건을 작성하는 방법에 대한 자세한 내용은 51-34페이지의 규칙 작성 원리 이해을/를 참조하십시오.

조건 작성 시 사용할 수 있는 구문에 대해서는 51-20페이지의 호스트 프로필 자격 구문에서 자세히 설명합니다.

5단계 선택적으로, 다음 절의 절차를 계속 진행합니다.

- 51-22페이지의 시간별 연결 데이터를 사용하여 상관관계 규칙 제한
- 51-31페이지의 사용자 자격 추가
- 51-32페이지의 유휴 기간 및 비활성 기간 추가

상관관계 규칙 작성을 완료했으면 51-3페이지의 상관관계 정책에 대한 규칙 생성의 절차 중 9단계를 수행하여 규칙을 저장하십시오.

호스트 프로필 자격 구문

라이센스: FireSIGHT

호스트 프로필 자격 조건을 작성할 때 먼저 상관관계 규칙을 제한하는 데 사용할 호스트를 선택해야 합니다. 선택할 수 있는 호스트는 다음과 같이 규칙을 트리거하기 위해 사용하는 이벤트 유형에 따라 다릅니다.

- 연결 이벤트를 사용하는 경우 **Responder Host** 또는 **Initiator Host**를 선택합니다.
- 침입 이벤트를 사용하는 경우 **Destination Host** 또는 **Source Host**를 선택합니다.
- 검색 이벤트, 호스트 입력 이벤트 또는 사용자 활동을 사용하는 경우 **Host**를 선택합니다.

호스트 유형을 선택했으면 다음 표에 설명된 대로 호스트 프로필 자격 조건의 작성을 계속합니다.

NetFlow 지원 디바이스에서 내보낸 데이터를 기반으로 네트워크 맵에 호스트를 추가하도록 네트워크 검색 정책을 구성할 수 있지만, 이러한 호스트에 대해 사용할 수 있는 정보는 제한적입니다. 예를 들어, 호스트 입력 기능을 사용하여 제공하지 않는 한 이러한 호스트에 대해 사용할 수 있는 운영 체제 데이터가 없습니다. 또한 NetFlow 지원 디바이스에서 내보낸 연결 데이터를 사용할 경우 NetFlow 레코드는 어떤 호스트가 initiator이고 어떤 호스트가 responder인가에 대한 정보를 포함하지 않는다는 점에 유의해야 합니다. 시스템에서 NetFlow 레코드를 처리할 때 각 호스트에서 사용하는 포트를 기반으로 이 정보를 확인하고 이 포트가 잘 알려진 것인지 확인하는 데 알고리즘을 사용합니다. 자세한 내용은 45-17페이지의 NetFlow 및 FireSIGHT 데이터 간 차이점을/를 참조하십시오.

표 51-11 호스트 프로필 자격 구문

지정할 항목	연산자 선택 후 수행할 작업
Host Type	호스트 유형을 하나 이상 선택합니다. 호스트를 선택하거나 여러 네트워크 디바이스 유형 중 하나를 선택할 수 있습니다.
NETBIOS 이름	호스트의 NetBIOS 이름을 입력합니다.
Operating System > OS Name	운영 체제 이름을 하나 이상 선택합니다.
Operating System > OS Vendor	운영 체제 공급업체 이름을 하나 이상 선택합니다.
Operating System > OS Version	운영 체제 버전을 하나 이상 선택합니다.
하드웨어	모바일 디바이스의 하드웨어 모델을 입력합니다. 예를 들어 일치하는 모든 Apple iPhone을 찾으려면 `iPhone`을 입력합니다.
IOC 태그	IOC 태그를 하나 이상 선택합니다. IOC 태그 유형에 대한 자세한 내용은 45-20페이지의 IOC 유형 이해을/를 참조하십시오.
Jailbroken	이벤트의 호스트가 탈옥 모바일 디바이스이면 **Yes**, 아니면 **No**를 선택합니다.
모바일	이벤트의 호스트가 모바일 디바이스이면 **Yes**, 아니면 **No**를 선택합니다.
Network Protocol	네트워크 프로토콜 번호를 http://www.iana.org/assignments/ethernet-numbers에 표시된 대로 입력합니다.
Transport Protocol	전송 프로토콜의 이름이나 번호를 http://www.iana.org/assignments/protocol-numbers에 표시된 대로 입력합니다.
Host Criticality	호스트 중요도를 선택합니다(**None**, **Low**, **Medium** 또는 **High**). 호스트 중요도에 대한 자세한 내용은 49-30페이지의 사전 정의 호스트 특성 작업을/를 참조하십시오.

표 51-11 호스트 프로필 자격 구문 (계속)

지정할 항목	연산자 선택 후 수행할 작업
VLAN ID	호스트와 연결된 VLAN ID 번호를 입력합니다.
Application Protocol > Application Protocol	애플리케이션 프로토콜을 하나 이상 선택합니다.
Application Protocol > 애플리케이션 포트	애플리케이션 프로토콜 포트 번호를 입력합니다. 상관관계 규칙을 트리거하는 데 침입 이벤트를 사용하는 경우, 호스트 프로필 자격에 대해 선택한 호스트에 따라 이 필드에 `dst_port`(**Destination Host**의 경우) 또는 `src_port`(**Source Host**의 경우)와 같이 이벤트의 포트가 미리 채워집니다.
Application Protocol > 프로토콜	프로토콜을 하나 이상 선택합니다.
Application Protocol Category	카테고리를 선택합니다.
Client > Client	클라이언트를 하나 이상 선택합니다.
Client > Client Version	클라이언트 버전을 입력합니다.
Client Category	카테고리를 선택합니다.
Web Application	웹 애플리케이션을 선택합니다.
Web Application Category	카테고리를 선택합니다.
MAC Address > MAC Address	호스트의 MAC 주소 전체 또는 일부를 입력합니다. 예를 들어 특정 하드웨어 디바이스의 MAC 주소가 0A:12:34로 시작하는 것을 알고 있다면 연산자로 **begins with**를 선택하고 값으로 `0A:12:34`를 입력할 수 있습니다.
MAC Address > MAC Type	MAC 유형이 **ARP/DHCP Detected**인지 여부를 선택합니다. 즉 시스템에서 MAC 주소를 호스트에 속한 것(**ARP/DHCP Detected**)으로 확실하게 식별했는지, 관리되는 디바이스와 호스트 간에 라우터가 있다는 등의 이유로 여러 호스트가 해당 MAC 주소를 갖는지(**is not ARP/DHCP Detected**) 또는 MAC 유형이 상관없는지(**is any**) 여부를 선택합니다.
MAC Vendor > MAC Vendor	호스트의 MAC 하드웨어 공급업체의 이름 전체 또는 일부를 입력합니다.
사용 가능한 모든 호스트 특성(기본 규정준수 화이트리스트 호스트 특성 포함)	선택하는 호스트 특성의 유형에 따라 알맞은 값을 지정합니다. • 호스트 특성 유형이 `Integer`일 경우 그 특성에 대해 정의된 범위의 정수 값을 입력합니다. • 호스트 특성 유형이 `Text`일 경우 텍스트 값을 입력합니다. • 호스트 특성 유형이 `List`일 경우 유효한 목록 문자열을 선택합니다. • 호스트 특성 유형이 `URL`일 경우 URL 값을 입력합니다. 호스트 특성에 대한 자세한 내용은 49-31페이지의 사용자 정의 호스트 특성 작업을/를 참조하십시오.

호스트 프로필 자격을 구성할 때 종종 이벤트 데이터를 사용할 수 있습니다. 예를 들어, 모리터링되는 호스트 중 하나에서 Internet Explorer를 사용하는 것을 시스템이 탐지할 때 상관관계 규칙이 트리거된다고 가정해보겠습니다. 나아가, 이러한 사용을 탐지할 때 브라우저 버전이 최신 버전이 아니면(이 예의 경우 최신 버전은 9.0) 이벤트를 생성하고자 한다고 가정해보겠습니다.

Client가 **Event Client**(즉, Internet Explorer)이지만 **Client Version**이 `9.0`이 아닐 경우에만 규칙이 트리거되도록 호스트 프로필 자격을 이 상관관계 규칙에 추가할 수 있습니다.

시간별 연결 데이터를 사용하여 상관관계 규칙 제한

라이센스: FireSIGHT

규칙의 초기 기준이 충족되면(호스트 프로필 및 사용자 자격 포함) 시스템이 특정 연결 추적을 시작할 수 있도록 *연결 추적기*는 상관관계 규칙을 제한합니다. 추적된 연결이 지정 기간 동안 수집된 추가 기준을 충족할 경우 방어 센터는 규칙에 대해 상관관계 이벤트를 생성합니다.

연결, 침입, 검색, 사용자 활동 또는 호스트 입력 이벤트를 사용하여 상관관계 규칙을 트리거하는 경우 연결 추적기를 규칙에 추가할 수 있습니다. 악성코드 이벤트 또는 트래픽 프로필 변경에 대해 트리거되는 규칙에는 연결 추적기를 추가할 수 없습니다.

팁 연결 추적기는 일반적으로 매우 구체적인 트래픽을 모니터링하며, 트리거될 경우 지정된 기간에만 실행됩니다. 일반적으로 폭넓은 네트워크 트래픽을 모니터링하고 영구적으로 실행되는 트래픽 프로필을 연결 추적기와 비교해보십시오. 자세한 내용은 53-1페이지의 트래픽 프로필 생성을/를 참조하십시오.

추적기의 구성 방법에 따라, 연결 추적기가 이벤트를 생성할 수 있는 두 가지 방법이 있습니다.

조건이 충족될 때 즉시 실행되는 연결 추적기

네트워크 트래픽이 추적기의 조건을 충족하자마자 상관관계 규칙이 실행되도록 연결 추적기를 구성할 수 있습니다. 이러한 상황이 발생하면 시스템은 시간 초과 기간이 만료되지 않았더라도 이 연결 추적기 인스턴스에 대한 연결 추적을 중지합니다. 상관관계 규칙을 트리거한 동일한 정책 위반 유형이 다시 발생하면 시스템은 새 연결 추적기를 생성합니다.

반면, 네트워크 트래픽이 연결 추적기의 조건을 충족하기 전에 시간이 만료되면 방어 센터는 상관관계 이벤트를 생성하지 않으며, 동시에 해당 규칙 인스턴스에 대한 연결 추적을 중지합니다.

예를 들어 연결 추적기는 특정 유형의 연결이 지정된 기간 내에 지정된 횟수보다 더 많이 발생하는 경우에만 상관관계 이벤트를 생성함으로써 일종의 이벤트 임계값 역할을 할 수 있습니다. 또는 초기 연결 이후 시스템에서 과도한 데이터 전송을 탐지하는 경우에만 상관관계 이벤트를 생성할 수 있습니다.

시간 초과 기간 끝에 실행되는 연결 추적기

전체 시간 초과 기간에 수집된 데이터에 의존하도록, 따라서 시간 초과 기간이 끝날 때까지 실행될 수 없도록 연결 추적기를 구성할 수 있습니다.

예를 들어 일정 기간 동안 특정 바이트 수 미만이 탐지될 때 실행되도록 연결 추적기를 구성하는 경우, 시스템은 기간이 지날 때까지 기다렸다가 네트워크 트래픽이 해당 조건을 충족하면 이벤트를 생성합니다.

자세한 내용은 다음 절을 참조하십시오.

- 51-23페이지의 연결 추적기 추가
- 51-24페이지의 연결 추적기 구문
- 51-26페이지의 연결 추적기 이벤트 구문
- 51-26페이지의 예: 외부 호스트로부터의 과도한 연결
- 51-28페이지의 예: 과도한 BitTorrent 데이터 전송

연결 추적기 추가

라이센스: FireSIGHT

규칙의 초기 기준이 충족되면(호스트 프로필 및 사용자 자격 포함) 시스템이 특정 연결 추적을 시작할 수 있도록 연결 추적기는 상관관계 규칙을 제한합니다. 추적된 연결이 지정 기간 동안 수집된 추가 기준을 충족할 경우 방어 센터는 규칙에 대해 상관관계 이벤트를 생성합니다.

연결 추적기를 구성할 때 다음을 지정해야 합니다.

- 추적하고자 하는 연결
- 상관관계 이벤트를 생성하기 위해, 추적 중인 연결이 방어 센터에 대해 충족해야 할 조건
- 연결 추적기의 최대 기간, 즉 상관관계 이벤트를 생성하기 위해 지정 조건을 충족해야 하는 기간

팁 연결, 침입, 검색, 사용자 ID 또는 호스트 입력 이벤트가 발생하기만 하면 되는 간단한 상관관계 규칙에 연결 추적기를 추가할 수 있습니다.

연결 추적기를 추가하려면

액세스: Admin/Discovery Admin

1단계 Create Rule 페이지에서 **Add Connection Tracker**를 클릭합니다.

Connection Tracker 섹션이 나타납니다.

팁 연결 추적기를 제거하려면 **Remove Connection Tracker**를 클릭합니다.

2단계 연결 추적기 기준을 설정하여 추적할 연결을 지정합니다.

하나의 단순한 조건을 생성하여 연결 추적기 기준을 설정할 수도 있고, 여러 조건을 연결하고 중첩하여 더 정교한 구성을 만들 수도 있습니다.

웹 인터페이스를 사용하여 조건을 작성하는 방법에 대한 자세한 내용은 51-34페이지의 규칙 작성 원리 이해을/를 참조하십시오. 연결 추적기 조건 작성 시 사용할 수 있는 구문에 대해서는 51-24페이지의 연결 추적기 구문에서 자세히 설명합니다.

3단계 2단계에서 추적하기로 한 연결을 기반으로, 상관관계 이벤트를 생성하고자 하는 시기를 설명합니다.

이벤트를 생성할 시기를 설명하는 하나의 단순한 조건을 생성할 수도 있고, 여러 조건을 연결하고 중첩하여 더 정교한 구성을 만들 수도 있습니다.

상관관계 이벤트를 생성하기 위해 지정 조건을 충족해야 하는 기간(초, 분 또는 시간 단위)도 지정해야 합니다.

웹 인터페이스를 사용하여 조건을 작성하는 방법에 대한 자세한 내용은 51-34페이지의 규칙 작성 원리 이해을/를 참조하십시오. 연결 추적기 조건 작성 시 사용할 수 있는 구문에 대해서는 51-26페이지의 연결 추적기 이벤트 구문에서 자세히 설명합니다.

4단계 선택적으로, 다음 절의 절차를 계속 진행합니다.

- 51-31페이지의 사용자 자격 추가
- 51-32페이지의 유휴 기간 및 비활성 기간 추가

상관관계 규칙 작성을 완료했으면 51-3페이지의 상관관계 정책에 대한 규칙 생성의 절차 중 9단계 단계를 수행하여 규칙을 저장하십시오.

연결 추적기 구문

라이센스: 모두

다음 표에서는 추적하고자 하는 연결의 종류를 지정하는 연결 추적기 조건을 작성하는 방법에 대해 설명합니다.

Cisco 관리되는 디바이스에 의해 탐지된 연결 및 NetFlow 지원 디바이스에서 내보낸 연결 데이터는 서로 다른 정보를 포함하고 있다는 점에 유의해야 합니다. 예를 들어 관리되는 디바이스에 의해 탐지된 연결에는 TCP 플래그 정보가 없습니다. 따라서 연결 이벤트에 상관관계 규칙을 트리거하는 특정 TCP 플래그가 있음을 지정하고자 하는 경우, 관리되는 디바이스에 의해 탐지된 연결 중 어떤 것도 규칙을 트리거하지 않습니다.

또 다른 예로, NetFlow 레코드는 연결의 어떤 호스트가 initiator이고 어떤 호스트가 responder인가에 대한 정보를 포함하지 않습니다. 시스템에서 NetFlow 레코드를 처리할 때 각 호스트에서 사용하는 포트를 기반으로 이 정보를 확인하고 이 포트가 잘 알려진 것인지 확인하는 데 알고리즘을 사용합니다. 자세한 내용은 45-17페이지의 NetFlow 및 FireSIGHT 데이터 간 차이점을/를 참조하십시오.

표 51-12 연결 추적기 구문

지정할 항목	연산자 선택 후 수행할 작업
액세스 제어 정책	추적하고자 하는 연결을 로깅한 액세스 제어 정책을 하나 이상 선택합니다.
Access Control Rule Action	추적하고자 하는 연결을 로깅한 액세스 제어 규칙과 관련된 액세스 제어 규칙 작업을 하나 이상 선택합니다. **참고** 나중에 연결을 처리하는 기본 작업 또는 규칙과 상관없이, Monitor 규칙의 조건과 일치하는 연결을 추적하려면 **Monitor**를 선택합니다.
Access Control Rule Name	추적하고자 하는 연결을 로깅한 액세스 제어 규칙의 이름 전체 또는 일부를 입력합니다. **참고** Monitor 규칙과 일치하는 연결을 추적하려면 Monitor 규칙의 이름을 입력하십시오. 나중에 연결을 처리하는 기본 작업 또는 규칙과 상관없이 시스템은 연결을 추적합니다.
Application Protocol	애플리케이션 프로토콜을 하나 이상 선택합니다.
Application Protocol Category	애플리케이션 프로토콜 카테고리를 하나 이상 선택합니다.
클라이언트	클라이언트를 하나 이상 선택합니다.
Client Category	클라이언트 카테고리를 하나 이상 선택합니다.
Client Version	클라이언트의 버전을 입력합니다.
Connection Duration	연결 기간을 초 단위로 입력합니다.
연결 유형	연결을 Cisco 관리되는 디바이스(**FireSIGHT**)에서 탐지된 방법으로 추적할지, NetFlow 지원 디바이스(**NetFlow**)에서 내보낸 방법으로 추적할지를 선택합니다.
Destination Country 또는 Source Country	국가를 하나 이상 선택합니다.
디바이스	탐지된 연결을 추적하려는 디바이스를 하나 이상 선택합니다. NetFlow 연결을 추적하려면 NetFlow 지원 디바이스에서 내보낸 연결 데이터를 처리하는 디바이스를 선택합니다.
Ingress Interface 또는 Egress Interface	인터페이스를 하나 이상 선택합니다.
Ingress Security Zone 또는 Egress Security Zone	보안 영역을 하나 이상 선택합니다.

표 51-12 연결 추적기 구문 (계속)

지정할 항목	연산자 선택 후 수행할 작업
Initiator IP, Responder IP 또는 Initiator/Responder IP	단일 IP 주소 또는 주소 블록을 입력합니다. FireSIGHT 시스템에서 IP 주소 표기법을 사용하는 방법에 대한 자세한 내용은 1-19페이지의 IP 주소 표기 규칙을/를 참조하십시오.
Initiator Bytes, Responder Bytes 또는 Total Bytes	다음 중 하나 입력: • 전송된 바이트 수(**Initiator Bytes**) • 수신된 바이트 수(**Responder Bytes**) • 전송 및 수신된 바이트 수(**Total Bytes**)
Initiator Packets, Responder Packets 또는 Total Packets	다음 중 하나 입력: • 전송된 패킷 수(**Initiator Packets**) • 수신된 패킷 수(**Responder Packets**) • 전송 및 수신된 패킷 수(**Total Packets**)
Initiator Port/ICMP Type 또는 Responder Port/ICMP Code	Initiator 트래픽의 포트 번호나 ICMP 유형 또는 responder 트래픽의 포트 번호나 ICMP 코드를 입력합니다.
IOC 태그	IOC 태그의 설정(`is` 또는 `is not`)을 선택합니다.
NETBIOS 이름	연결에서 모니터링된 호스트의 NetBIOS 이름을 입력합니다.
NetFlow 장치	추적하고자 하는 연결을 내보낸 NetFlow 지원 디바이스의 IP 주소를 선택합니다. 구축에 어떤 NetFlow 지원 디바이스도 추가하지 않은 경우 NetFlow Device 드롭다운 목록은 비어 있습니다.
사유	추적하고자 하는 연결과 관련된 이유를 하나 이상 선택합니다.
Security Intelligence Category	추적하고자 하는 연결과 관련된 보안 인텔리전스 카테고리를 하나 이상 선택합니다.
TCP Flags	추적을 위해 연결에 반드시 포함해야 하는 TCP 플래그를 선택합니다. **참고** NetFlow 지원 디바이스에서 내보낸 연결만 TCP 플래그 데이터를 포함합니다.
Transport Protocol	연결에 사용된 전송 프로토콜(`TCP` 또는 `UDP`)을 입력합니다.
URL	추적하고자 하는 연결에서 방문한 URL 전체 또는 일부를 입력합니다.
URL 카테고리	추적하고자 하는 연결에서 방문한 URL의 URL 카테고리를 하나 이상 선택합니다.
URL 평판	추적하고자 하는 연결에서 방문한 URL의 URL 평판 값을 하나 이상 선택합니다.
아이디	추적하고자 하는 연결의 두 호스트 중 하나에 로그인한 사용자의 사용자 이름을 입력합니다.
Web Application	웹 애플리케이션을 하나 이상 선택합니다.
Web Application Category	웹 애플리케이션 카테고리를 하나 이상 선택합니다.

연결 추적기를 구성할 때 종종 이벤트 데이터를 사용할 수 있습니다. 예를 들어, 시스템이 모니터링되는 호스트 중 하나에서 새 클라이언트를 탐지할 때 상관관계 규칙이 트리거된다고 가정해보겠습니다. 즉, 기본 이벤트 유형이 **a new client is detected**인 시스템 이벤트가 생성될 때 규칙이 트리거되는 것입니다.

나아가, 이 새 클라이언트를 탐지할 때 전에 탐지된 호스트에서 새 클라이언트와 관련된 연결을 추적하고자 한다고 가정해보겠습니다. 시스템은 호스트의 IP 주소와 클라이언트 이름을 알고 있으므로 이러한 연결을 추적하는 간단한 연결 추적기를 작성할 수 있습니다.

실제로, 이 상관관계 규칙 유형에 연결 추적기를 추가하면 연결 추적기가 기본 제약 조건으로 채워집니다. 즉, **Initiator/Responder IP**는 **Event IP Address**로 설정되고 **Client**는 **Event Client**로 설정됩니다.

팁 연결 추적기가 특정 IP 주소 또는 IP 주소 블록의 연결을 추적하도록 지정하려면 **switch to manual entry**를 클릭하여 IP를 수동으로 지정하십시오. 이벤트의 IP 주소를 사용하는 방식으로 돌아가려면 **switch to event fields**를 클릭합니다.

연결 추적기 이벤트 구문

라이센스: 모두

다음 표에서는 추적 중인 연결을 기반으로 상관관계 이벤트를 생성하고자 하는 시기를 지정하는 연결 추적기 조건의 작성 방법에 대해 설명합니다.

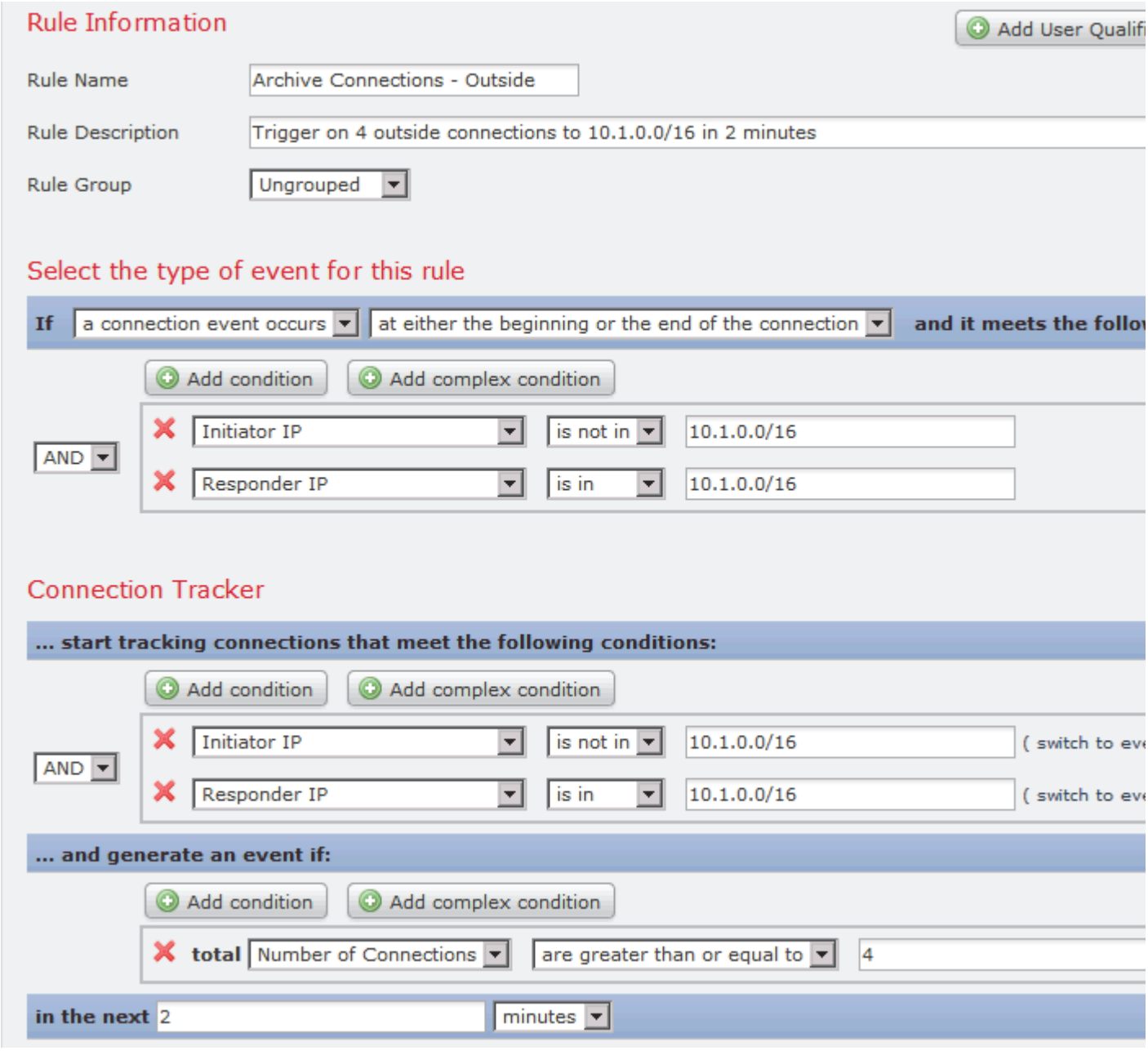
표 51-13 연결 추적기 이벤트 구문

지정할 항목	연산자 선택 후 수행할 작업
연결 수	탐지된 총 연결 수를 입력합니다.
Number of SSL Encrypted Sessions	탐지된 총 SSL 또는 TLS 암호화 세션의 수를 입력합니다.
Total Bytes, Initiator Bytes 또는 Responder Bytes	다음 중 하나 입력: • 전송된 총 바이트(**Total Bytes**) • 전송된 바이트 수(**Initiator Bytes**) • 수신된 바이트 수(**Responder Bytes**)
Total Packets, Initiator Packets 또는 Responder Packets	다음 중 하나 입력: • 전송된 총 패킷(**Total Packets**) • 전송된 패킷 수(**Initiator Packets**) • 수신된 패킷 수(**Responder Packets**)
Unique Initiators 또는 Unique Responders	다음 중 하나 입력: • 탐지된 세션을 시작한 고유한 호스트의 수(**Unique Initiators**) • 탐지된 연결에 응답한 고유한 호스트의 수(**Unique Responders**)

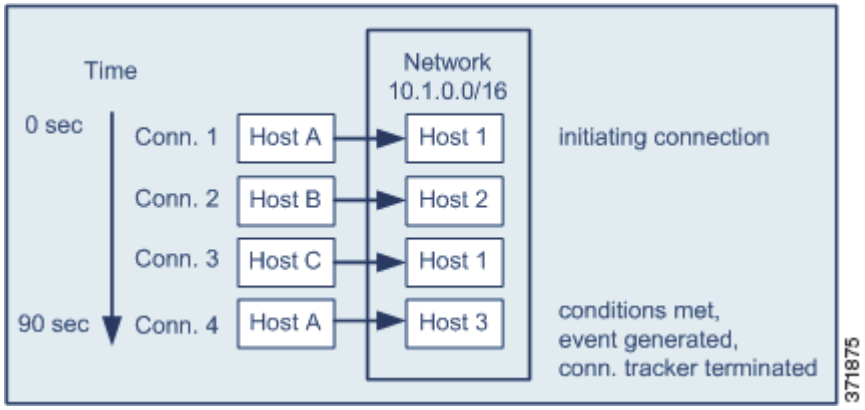
예: 외부 호스트로부터의 과도한 연결

네트워크 10.1.0.0/16에 중요한 파일을 보관하며, 이 네트워크 외부의 호스트는 일반적으로 네트워크 내부의 호스트에 대해 연결을 시작하지 않는 시나리오를 고려해 보십시오. 네트워크 외부에서 더러 연결이 시작되었지만, 2분 내에 4개 이상의 연결이 시작되면 문제가 있는 것으로 판단했습니다.

다음 그림의 규칙에서는, 10.1.0.0/16 네트워크 외부에서 네트워크 내부로 연결이 시작될 때 시스템이 해당 조건을 충족하는 연결의 추적을 시작하는 것을 알 수 있습니다. 이제 시스템이 해당 서명과 일치하는 4개의 연결(원래 연결 포함)을 2분 내에 탐지할 경우 방어 센터는 상관관계 이벤트를 생성합니다.



다음 다이어그램은 네트워크 트래픽이 위의 상관관계 규칙을 트리거하는 방법을 보여줍니다.



이 예에서 시스템은 상관관계 규칙의 기본 조건을 충족한 연결, 즉 10.1.0.0/16 네트워크 외부 호스트에서 네트워크 내부 호스트로의 연결을 탐지했습니다. 여기에서 연결 추적기가 생성됩니다.

연결 추적기는 다음과 같이 처리됩니다.

1단계 시스템은 네트워크 외부 Host A에서 네트워크 내부 Host 1로의 연결을 탐지하면 연결 추적을 시작합니다.

2단계 시스템은 연결 추적기 서명과 일치하는 연결을 2개 더 탐지합니다(Host B에서 Host 2, Host C에서 Host 1).

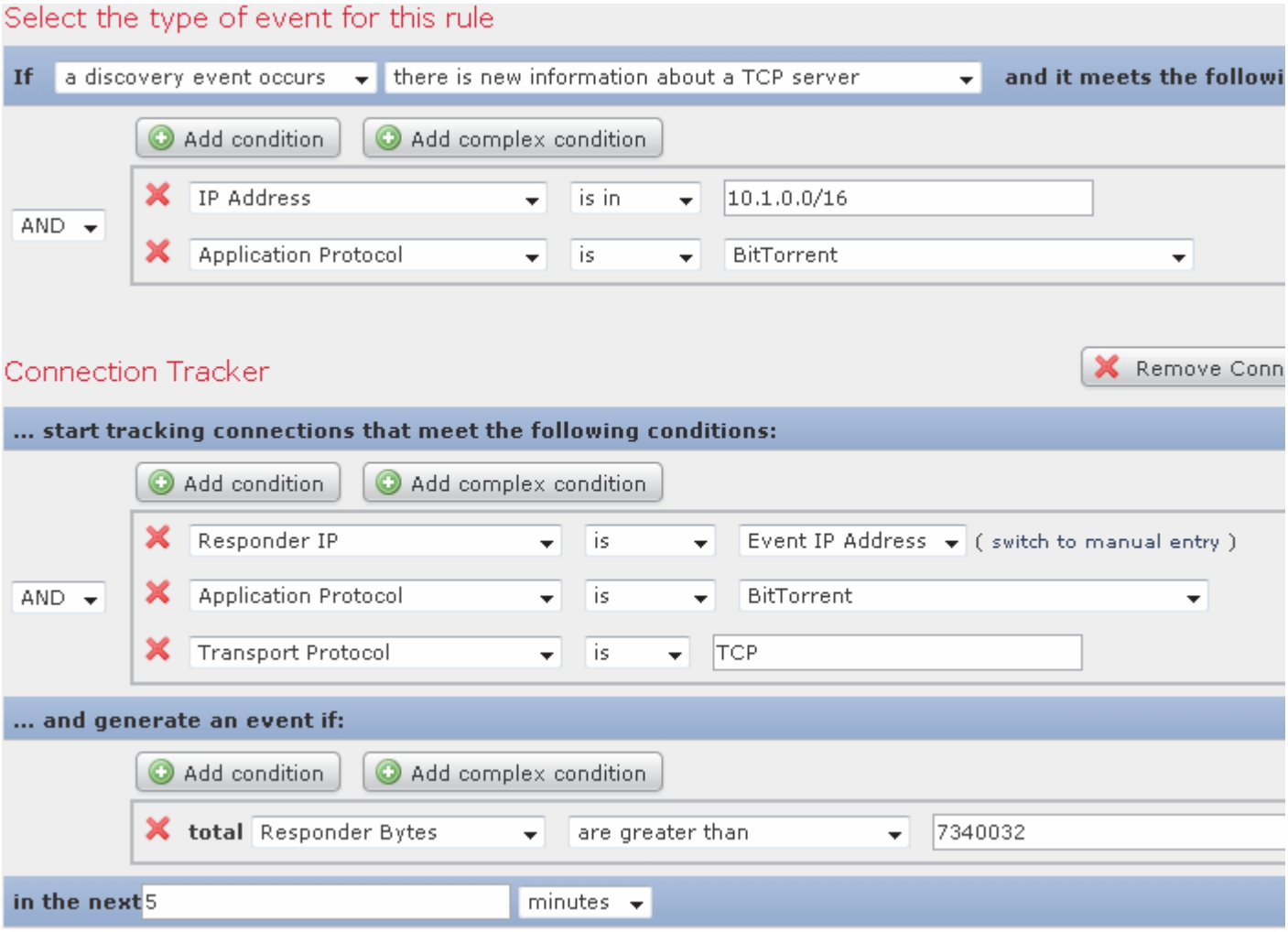
3단계 2분 시간 제한 내에 Host A가 Host 3에 연결되면 시스템은 4번째 해당 연결을 탐지하게 됩니다. 규칙 조건이 충족됩니다.

4단계 방어 센터는 상관관계 이벤트를 생성하며 시스템은 연결 추적을 중지합니다.

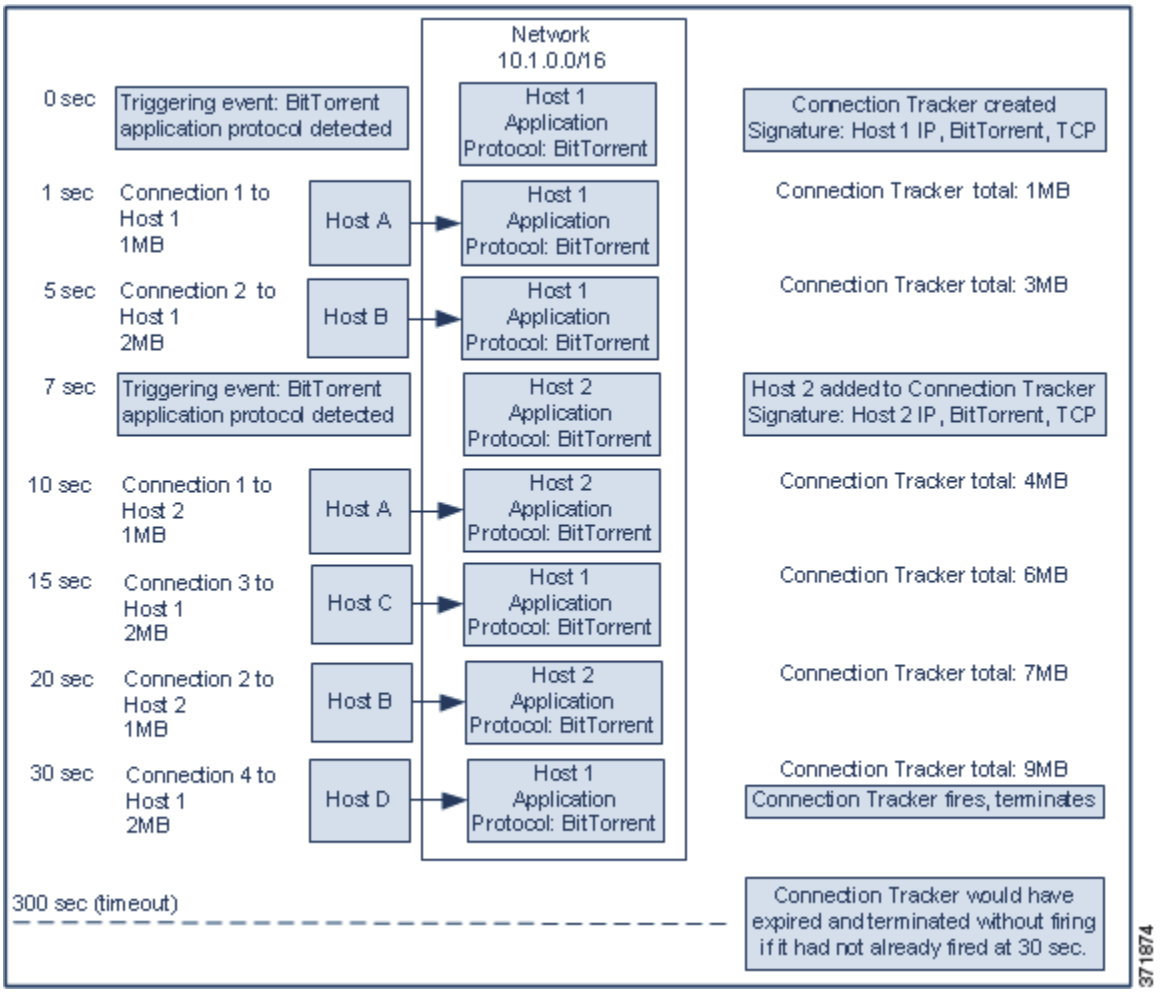
예: 과도한 BitTorrent 데이터 전송

모니터링되는 네트워크의 호스트에 대한 초기 연결 이후 시스템이 과도한 BitTorrent 데이터 전송을 탐지하는 경우 상관관계 이벤트를 생성하고자 하는 시나리오를 고려해보십시오.

다음 그림에서는 시스템이 모니터링되는 네트워크에서 BitTorrent 애플리케이션 프로토콜을 탐지할 때 트리거되는 상관관계 규칙을 보여줍니다. 이 규칙에는 모니터링되는 네트워크의 호스트(이 경우 10.1.0.0/16)가 초기 정책 위반 이후 5분 동안 BitTorrent를 통해 총 7MB(7340032바이트)가 넘는 데이터를 전송하는 경우 규칙이 트리거되도록 규칙을 제한하는 연결 추적기가 있습니다.



다음 다이어그램은 네트워크 트래픽이 위의 상관관계 규칙을 트리거하는 방법을 보여줍니다.



이 예에서 시스템은 두 호스트, 즉 Host 1과 Host 2에서 BitTorrent TCP 애플리케이션 프로토콜을 탐지했습니다. 이러한 두 호스트는 BitTorrent를 통해 4개의 다른 호스트(Host A, Host B, Host C, Host D)로 데이터를 전송합니다.

이 연결 추적기는 다음과 같이 처리됩니다.

1단계 시스템은 Host 1에서 BitTorrent 애플리케이션 프로토콜을 탐지하면 0초 마커에서 연결 추적을 시작합니다.

시스템이 5분 내에(300초 마커까지) 7MB의 BitTorrent TCP 데이터가 전송되는 것을 탐지하지 못하면 연결 추적기가 만료됩니다.

2단계 5초에 Host 1이 서명과 일치하는 3MB의 데이터를 전송했습니다.

- 1초 마커에 Host 1에서 Host A로 1MB(연결 추적기를 충족하기 위해 계산된 총 BitTorrent 트래픽 1MB)
- 5초 마커에 Host 1에서 Host B로 2MB(총 3MB)

3단계 7초에 시스템은 Host 2에서 BitTorrent 애플리케이션 프로토콜을 탐지하고 해당 호스트에 대해서도 BitTorrent 연결 추적을 시작합니다.

4단계 20초에 시스템은 서명과 일치하는 추가 데이터가 Host 1과 Host2 모두에서 전송되는 것을 탐지했습니다.

- 10초 마커에 Host 2에서 Host A로 1MB(총 4MB)
- 15초 마커에 Host 1에서 Host C로 2MB(총 6MB)
- 20초 마커에 Host 2에서 Host B로 1MB(총 7MB)

Host 1과 Host 2에서 이제 총 7MB의 BitTorrent 데이터를 전송했지만, 전송된 총 바이트 수가 7MB(**Responder Bytes are greater than 7340032**)보다 **커야** 하므로 규칙이 트리거되지 않습니다.

이 시점에 시스템이 추적기의 시간 초과 기간에 나머지 280초 동안 추가 BitTorrent 전송을 탐지하지 못하면, 추적기가 만료되고 방어 센터는 상관관계 이벤트를 생성하지 않습니다.

5단계 그러나 30초에 시스템은 추가 BitTorrent 전송을 탐지합니다.

- 30초 마커에 Host 1에서 Host D로 2MB(총 9MB)

규칙 조건이 충족됩니다.

6단계 방어 센터는 상관관계 이벤트를 생성합니다.

5분 기간이 만료되지 않았어도 방어 센터는 이 연결 추적기 인스턴스에 대한 연결 추적도 중지합니다. 이 시점에 BitTorrent TCP 애플리케이션 프로토콜을 사용하는 새 연결을 탐지하면 시스템은 새 연결 추적기를 생성합니다.

방어 센터는 세션이 끝날 때까지 연결 데이터를 집계하지 않으므로, Host 1이 총 2MB를 Host D로 전송한 *후* 상관관계 이벤트를 생성합니다.

사용자 자격 추가

라이센스: FireSIGHT

연결, 침입, 검색 또는 호스트 입력 이벤트를 사용하여 상관관계 규칙을 트리거하는 경우, 이벤트와 관련된 사용자의 ID를 기반으로 규칙을 제한할 수 있습니다. 이러한 제약을 *사용자 자격(user qualification)*이라고 합니다. 트래픽 프로필 변경 또는 사용자 활동 탐색에 대해 트리거되는 상관관계 규칙에 사용자 자격을 추가할 수 **없습니다**.

예를 들어 소스 또는 대상 사용자의 ID가 영업 부서 사용자인 경우에만 트리거되도록 상관관계 규칙을 제한할 수 있습니다.

사용자 ID 자격을 추가하려면

액세스: Admin/Discovery Admin

1단계 Create Rule 페이지에서 **Add User Qualification**을 클릭합니다.

User Identity Qualification 섹션이 나타납니다.

팁 사용자 자격을 제거하려면 **Remove User Qualification**을 클릭합니다.

2단계 사용자 자격 자격의 조건을 작성합니다.

하나의 단순한 조건을 생성할 수도 있고, 여러 조건을 연결하고 중첩하여 더 정교한 구성으로 만들 수도 있습니다. 웹 인터페이스를 사용하여 조건을 작성하는 방법에 대한 자세한 내용은 51-34페이지의 규칙 작성 원리 이해을/를 참조하십시오.

조건 작성 시 사용할 수 있는 구문에 대해서는 51-32페이지의 사용자 자격 구문에서 자세히 설명합니다.

3단계 선택적으로 51-32페이지의 유휴 기간 및 비활성 기간 추가를 계속 진행합니다.

상관관계 규칙 작성을 완료했으면 51-3페이지의 상관관계 정책에 대한 규칙 생성의 절차 중 9단계 단계를 수행하여 규칙을 저장하십시오.

사용자 자격 구문

라이센스: FireSIGHT

사용자 자격 조건을 작성할 때 먼저 상관관계 규칙을 제한하는 데 사용할 ID를 선택해야 합니다. 선택할 수 있는 ID는 다음과 같이 규칙을 트리거하기 위해 사용하는 이벤트 유형에 따라 다릅니다.

- 연결 이벤트를 사용 중인 경우 **Identity on Initiator** 또는 **Identity on Responder**를 선택합니다.
- 침입 이벤트를 사용 중인 경우 **Identity on Destination** 또는 **Identity on Source**를 선택합니다.
- 검색 이벤트를 사용 중인 경우 **Identity on Host**를 선택합니다.
- 호스트 입력 이벤트를 사용 중인 경우 **Identity on Host**를 선택합니다.

사용자 유형을 선택했으면 다음 표에 설명된 대로 사용자 자격 조건의 작성을 계속합니다.

방어 센터는 선택적인 방어 센터-LDAP 서버 연결에서 성과 이름, 부서, 전화 번호, 이메일 주소 등 사용자에 대한 특정 정보를 가져옵니다. 17-9페이지의 User Agents를 사용하여 Active Directory 로그인 보고을/를 참조하십시오. 데이터베이스의 일부 사용자에 대해서는 이 정보를 이용하지 못할 수 있습니다.

표 51-14 사용자 자격 구문

지정할 항목	연산자 선택 후 수행할 작업
아이디	상관관계 규칙을 제한하기 위해 사용하고자 하는 사용자의 사용자 이름을 입력합니다.
인증 프로토콜	인증 프로토콜(또는 사용자 유형 프로토콜)을 선택합니다. 이 프로토콜은 사용자를 탐지하는 데 사용된 프로토콜입니다.
이름	상관관계 규칙을 제한하기 위해 사용하고자 하는 사용자의 이름을 입력합니다.
성	상관관계 규칙을 제한하기 위해 사용하고자 하는 사용자의 성을 입력합니다.
부서	상관관계 규칙을 제한하기 위해 사용하고자 하는 사용자의 부서를 입력합니다.
전화	상관관계 규칙을 제한하기 위해 사용하고자 하는 사용자의 전화 번호를 입력합니다.
이메일	상관관계 규칙을 제한하기 위해 사용하고자 하는 사용자의 이메일 주소를 입력합니다.

유휴 기간 및 비활성 기간 추가

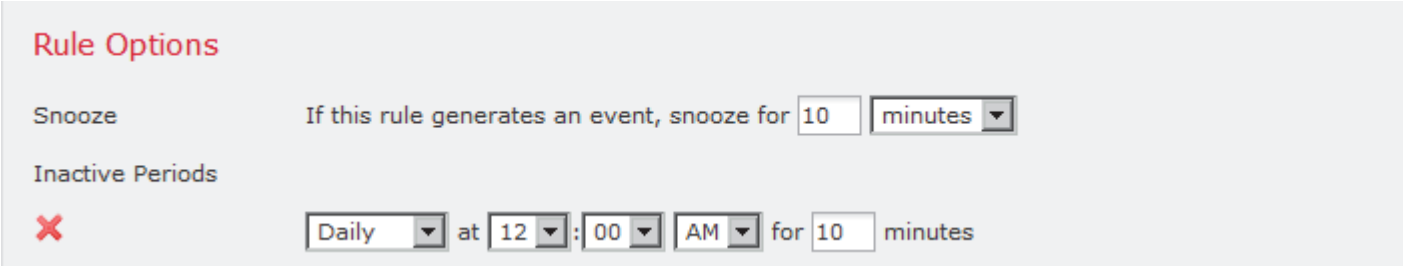
라이센스: 모두

상관관계 규칙에서 *유휴 기간*을 구성할 수 있습니다. 상관관계 규칙이 트리거되면, 유휴 기간은 지정된 기간 동안(규칙 위반이 다시 발생해도) 규칙의 실행을 중지하도록 방어 센터에 지시합니다. 유휴 기간이 경과하면 규칙을 다시 트리거할 수 있습니다(그리고 새 유휴 기간을 시작할 수 있습니다).

예를 들면 트래픽을 생성해서는 안 되는 호스트가 네트워크에 있을 수 있습니다. 시스템이 해당 호스트와 관련된 연결을 탐지할 때마다 트리거되는 간단한 상관관계 규칙은 호스트를 통과하는 네트워크 트래픽에 따라 짧은 기간에 여러 상관관계 이벤트를 생성할 수 있습니다. 정책 위반을 알리는 상관관계 이벤트의 수를 제한하려면 방어 센터가 해당 호스트와 관련하여 시스템이 탐지하는 첫 번째 연결(지정한 기간 내에)에 대해서만 상관관계 이벤트를 생성하도록 유휴 기간을 추가할 수 있습니다.

상관관계 규칙에서 비활성 시간도 설정할 수 있습니다. 비활성 기간 중에는 상관관계 규칙이 트리거되지 않습니다. 비활성 기간이 매일, 매주 또는 매월 반복되도록 설정할 수 있습니다. 예를 들어 호스트 운영 체제 변경 사항을 찾기 위해 내부 네트워크에서 야간 Nmap 스캔을 수행할 수 있습니다. 이 경우 규칙이 잘못 트리거되지 않도록 스캔 시간 및 기간에 영향받는 상관관계 규칙에 대해 일일 비활성 기간을 설정할 수 있습니다.

다음 그림에서는 유휴 기간 및 비활성 기간으로 구성된 상관관계 규칙의 일부를 보여줍니다.



유휴 기간을 추가하려면

액세스: Admin/Discovery Admin

1단계 Create Profile 페이지의 **Rule Options**에서, 규칙이 트리거된 이후 방어 센터가 규칙을 다시 트리거하기까지 대기해야 하는 기간을 지정합니다.

팁 유휴 기간을 제거하려면 간격을 0으로 지정합니다(초, 분 또는 시간).

비활성 기간을 추가하려면

액세스: Admin/Discovery Admin

1단계 Create Profile 페이지의 **Rule Options**에서 **Add Inactive Period**를 클릭합니다.

2단계 드롭다운 목록과 텍스트 필드를 사용하여, 방어 센터가 상관관계 규칙에 대한 네트워크 트래픽 평가를 억제하도록 할 시기와 빈도를 지정합니다.

팁 비활성 기간을 삭제하려면 삭제할 비활성 기간 옆에 있는 삭제 아이콘( )을 클릭합니다.

유휴 기간 및 비활성 기간의 추가를 완료했으면, 51-3페이지의 상관관계 정책에 대한 규칙 생성에 있는 절차의 9단계를 계속 진행하여 규칙을 저장합니다.

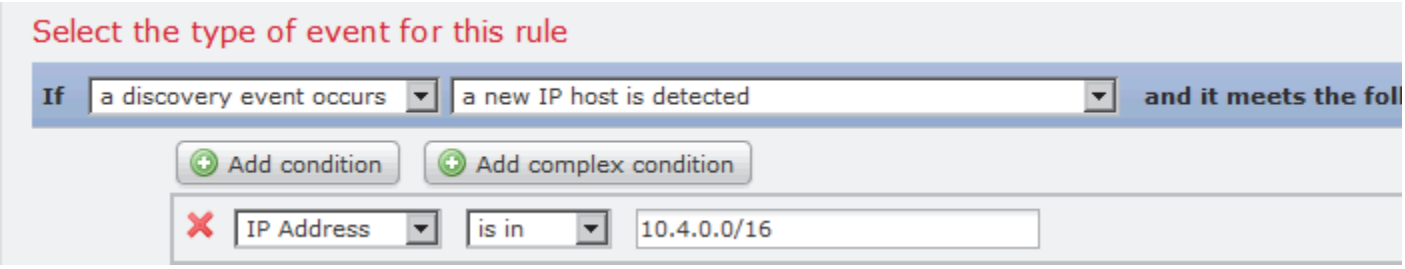
규칙 작성 원리 이해

라이센스: 모두

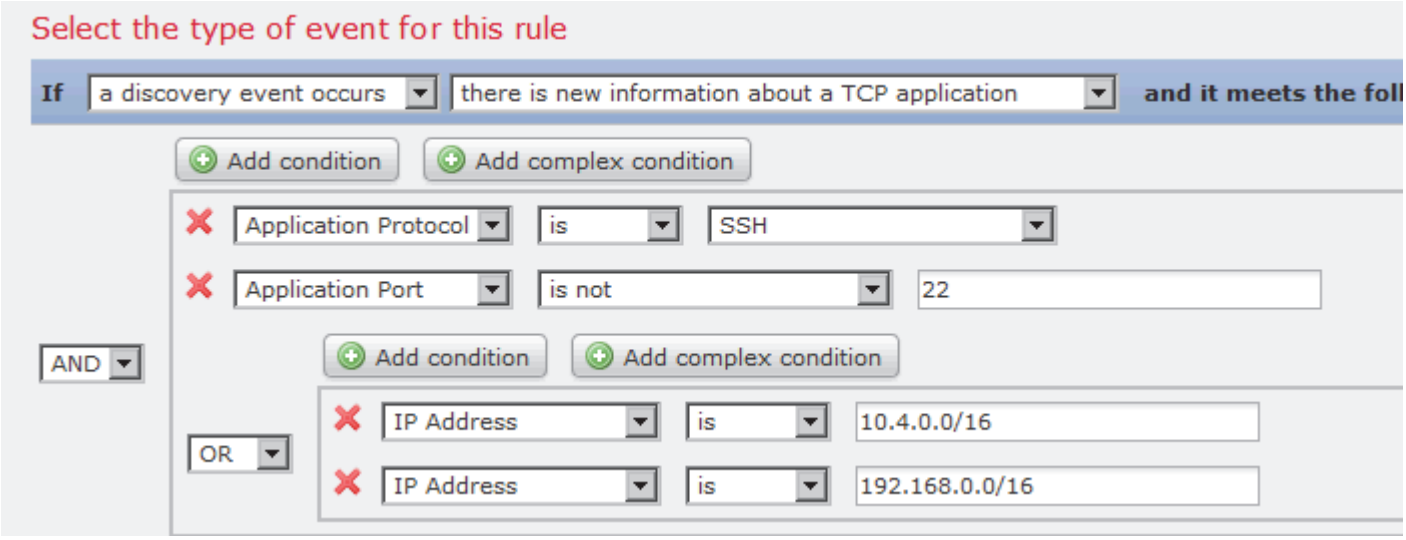
상관관계 규칙, 연결 추적기, 사용자 자격 및 호스트 프로필 자격은 각각이 트리거될 조건을 지정함으로써 작성할 수 있습니다. 단순한 조건을 생성할 수도 있고, 여러 조건을 연결하고 중첩하여 더 정교한 구성으로 만들 수도 있습니다.

예를 들어 새 호스트가 탐지될 때마다 상관관계 이벤트를 생성하려면, 다음 그림에 보이는 것처럼 조건 없이 매우 단순한 규칙을 생성할 수 있습니다.

규칙을 더 제한하여 10.4.x.x 네트워크에서 새 호스트가 탐지되는 경우에만 이벤트를 생성하려는 경우 다음 그림과 같이 단일 조건을 추가할 수 있습니다.



그러나 10.4.x.x 네트워크 및 192.168.x.x 네트워크의 비표준 포트에서 SSH 활동을 탐지하는 다음 규칙에는 4개의 조건이 있으며, 그중 마지막 2개는 복합 조건입니다.



조건 내에서 사용할 수 있는 구문은 생성하는 요소에 따라 달라지지만, 그 원리는 동일합니다.

주의 자주 발생하는 이벤트에 대해 트리거되는 복잡한 상관관계 규칙을 평가하면 방어 센터 성능이 저하될 수 있습니다. 예를 들어, 시스템에 의해 로깅된 모든 연결에 대해 방어 센터에서 반드시 평가해야 하는 다중 조건 규칙은 리소스 과부하를 일으킬 수 있습니다.

조건 작성에 대한 자세한 내용은 다음을 참조하십시오.

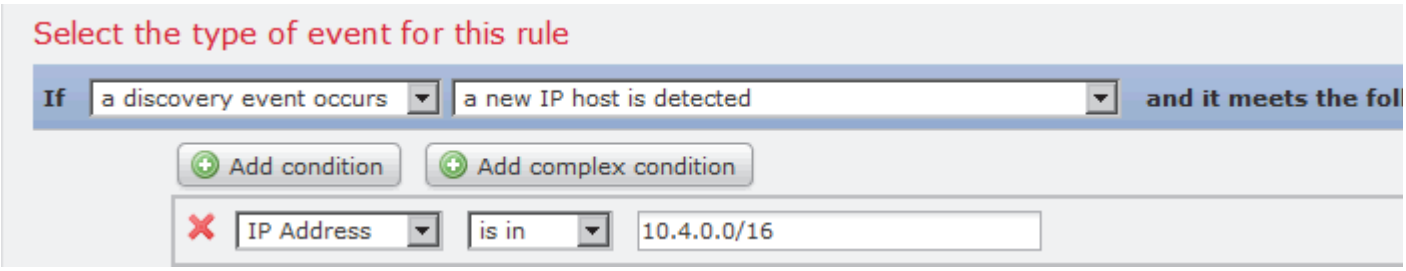
- 51-35페이지의 단일 조건 작성
- 51-37페이지의 조건 추가 및 연결
- 51-40페이지의 하나의 조건에서 여러 값 사용

단일 조건 작성

라이센스: 모두

대부분의 조건은 *category*, *operator*, *value*의 세 부분으로 구성되어 있습니다. 일부 조건은 좀 더 복잡하고 여러 카테고리를 포함하지만, 각각에는 고유한 연산자와 값이 있을 수 있습니다.

예를 들어 10.4.x.x 네트워크에서 새 호스트가 탐지되면 다음 상관관계 규칙이 트리거됩니다. 이 조건의 카테고리는 **IP Address**, 연산자는 **is in**, 값은 `10.4.0.0/16`입니다.



위의 예에서 상관관계 규칙 트리거 기준을 작성하려면

액세스: Admin/Discovery Admin

1단계 상관관계 규칙 작성을 시작합니다.

자세한 내용은 51-3페이지의 상관관계 정책에 대한 규칙 생성을/를 참조하십시오.

2단계 Create Rule 페이지의 **Select the type of event for this rule**에서 **a discovery event occurs**를 선택한 다음 드롭다운 목록에서 **a new IP host is detected**를 선택합니다.

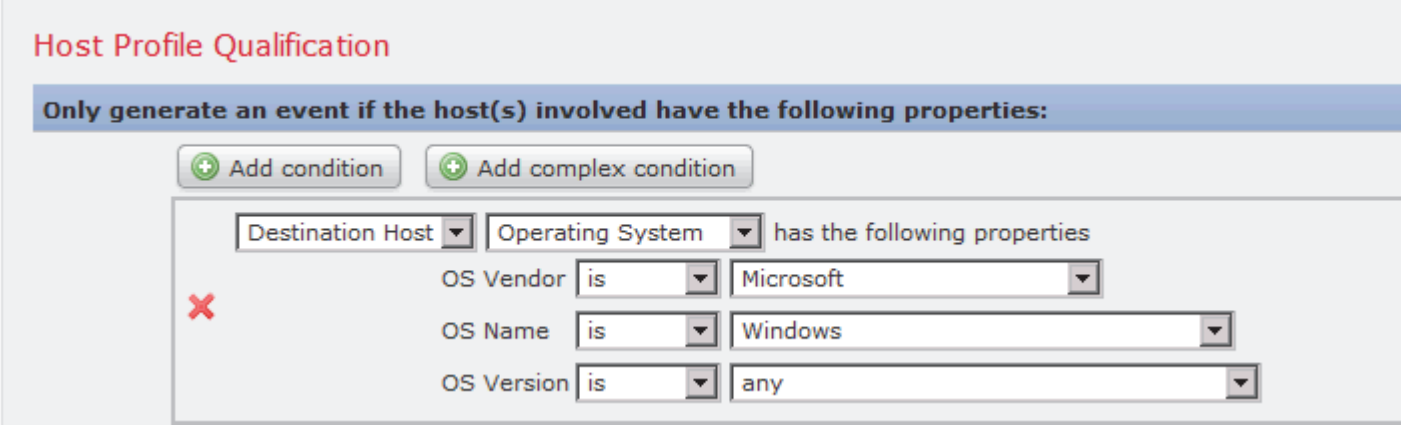
3단계 첫 번째(또는 *category*) 드롭다운 목록에서 **IP Address**를 선택하여 규칙의 단일 조건 작성을 시작합니다.

4단계 나타나는 연산자 드롭다운 목록에서 **is in**을 선택합니다.

팁 카테고리가 IP 주소를 나타낼 때 **is in** 또는 **is not in**을 연산자로 선택하면, IP 주소가 CIDR 등의 특수 표기법으로 표현된 IP 주소 블록에서 *is in* 상태인지 *is not in* 상태인지를 지정할 수 있습니다. FireSIGHT 시스템에서 IP 주소 표기법을 사용하는 방법에 대한 자세한 내용은 1-19페이지의 IP 주소 표기 규칙을/를 참조하십시오.

5단계 텍스트 필드에 `10.4.0.0/16`을 입력합니다.

이와는 달리 다음 호스트 프로필 자격은 좀 더 복잡하여, 규칙의 기반이 되는 검색 이벤트와 관련된 호스트가 Microsoft Windows 버전을 실행하는 경우에만 규칙이 트리거되는 방식으로 상관관계 규칙을 제한합니다.



위의 예에서 호스트 프로필 자격을 작성하려면

액세스: Admin/Discovery Admin

1단계 검색 이벤트에 대해 트리거되는 상관관계 규칙을 작성합니다.

자세한 내용은 51-3페이지의 상관관계 정책에 대한 규칙 생성을/를 참조하십시오.

2단계 Create Rule 페이지에서 **Add Host Profile Qualification**을 클릭합니다.

Host Profile Qualification 섹션이 나타납니다.

3단계 **Host Profile Qualification**의 첫 번째 조건에서, 상관관계 규칙을 제한하는 데 사용할 호스트 프로필이 있는 호스트를 지정합니다.

이 호스트 프로필 자격은 검색 이벤트를 기반으로 하는 상관관계 규칙의 일부이므로 사용 가능한 유일한 카테고리는 **Host**입니다.

4단계 **Operating System** 카테고리를 선택하여 호스트 운영 체제의 세부사항 지정을 시작합니다.

OS Vendor, **OS Name**, **OS Version**의 3가지 하위 카테고리가 나타납니다.

5단계 호스트에서 어떤 버전의 Microsoft Windows도 실행할 수 있도록 지정하려면 세 하위 카테고리 모두에 동일한 연산자 **is**를 사용합니다.

6단계 마지막으로 하위 카테고리에 대한 값을 지정합니다.

Microsoft를 **OS Vendor**로, **Windows**를 **OS Name**의 값으로 선택하고 **OS Version**의 값으로는 **any**를 유지합니다.

선택 가능한 카테고리는 상관관계 규칙 트리거, 호스트 프로필 자격, 연결 추적기 또는 사용자 자격 중 어떤 것을 작성 중인지에 따라 달라집니다. 상관관계 규칙 트리거 내에서는 상관관계 규칙의 기반이 되는 이벤트가 어떤 유형인가에 따라 카테고리가 좀 더 세분화됩니다.

또한 조건에서 사용 가능한 연산자는 선택하는 카테고리에 따라 달라집니다. 마지막으로, 조건의 값을 지정하는 데 사용 가능한 구문은 카테고리와 연산자에 따라 달라집니다. 텍스트 필드에 값을 입력해야 하는 경우가 있습니다. 그렇지 않으면 드롭다운 목록에서 값을 선택할 수 있습니다.

참고 조건 구문에서 드롭다운 목록의 값 선택을 허용할 경우 대개는 목록에서 여러 값을 사용할 수 있습니다. 자세한 내용은 51-40페이지의 하나의 조건에서 여러 값 사용을/를 참조하십시오.

상관관계 규칙 트리거 기준 작성용 구문에 대한 자세한 내용은 다음을 참조하십시오.

- 51-7페이지의 침입 이벤트 구문
- 51-9페이지의 악성코드 이벤트 구문
- 51-11페이지의 검색 이벤트 구문
- 51-13페이지의 사용자 활동 이벤트 구문
- 51-13페이지의 호스트 입력 이벤트 구문
- 51-14페이지의 연결 이벤트 구문
- 51-17페이지의 트래픽 프로필 변경 구문

호스트 프로필 자격, 사용자 자격 및 연결 추적기 작성용 구문에 대한 자세한 내용은 다음을 참조하십시오.

- 51-20페이지의 호스트 프로필 자격 구문
- 51-24페이지의 연결 추적기 구문
- 51-26페이지의 연결 추적기 이벤트 구문
- 51-32페이지의 사용자 자격 구문

조건 추가 및 연결

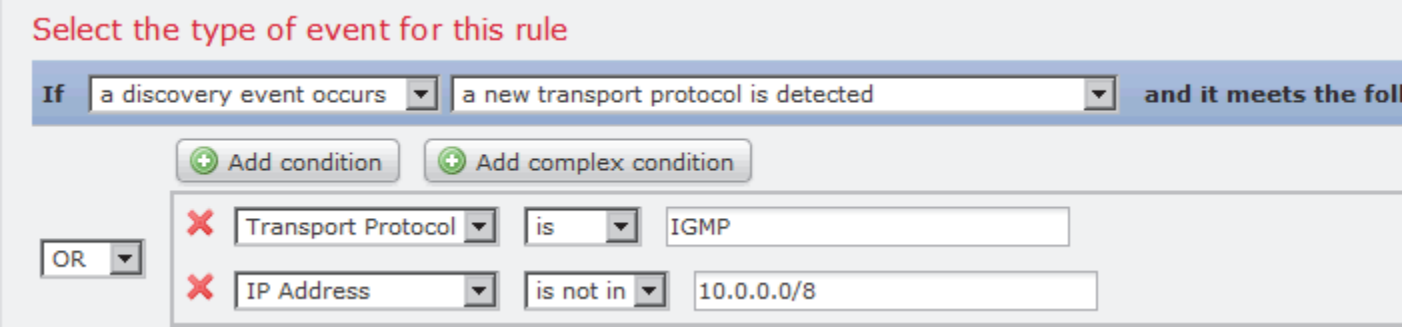
라이센스: 모두

단순한 상관관계 규칙 트리거, 연결 추적기, 호스트 프로필 자격 및 사용자 자격을 생성할 수도 있고, 조건을 연결하고 중첩하는 방법으로 더 정교하게 구성할 수도 있습니다.

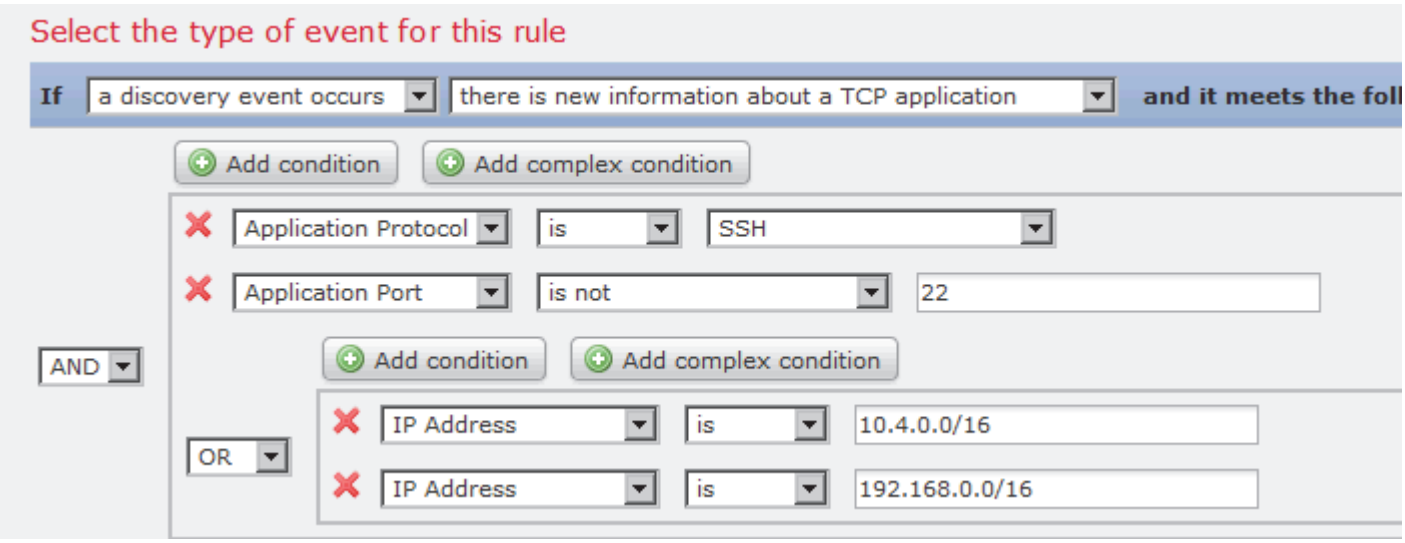
여러 개의 조건을 포함할 경우 **AND** 또는 **OR** 연산자로 연결해야 합니다. 동일한 레벨의 조건은 함께 평가됩니다.

- **AND** 연산자를 사용하면 이 연산자가 제어하는 레벨의 모든 조건을 충족해야 합니다.
- **OR** 연산자를 사용하면 이 연산자가 제어하는 레벨의 조건 중 하나 이상을 충족해야 합니다.

예를 들어 다음 상관관계 규칙 트리거 기준에서는 2개의 조건이 **OR**로 연결되어 있습니다. 이는 두 조건 중 하나가 참이면, 즉 IP 주소의 호스트가 10.x.x.x 서브넷에 없거나 호스트가 IGMP 메시지를 전송하는 경우 규칙이 트리거된다는 뜻입니다.



이와는 달리, 10.4.x.x 네트워크 및 192.168.x.x 네트워크의 비표준 포트에서 SSH 활동을 탐지하는 다음 규칙에는 4개의 조건이 있으며, 그중 마지막 2개는 복합 조건입니다.



이 규칙은 SSH가 비표준 포트에서 탐지되는 경우 트리거됩니다. 처음 두 조건의 요구 사항은 애플리케이션 프로토콜 이름이 SSH이고 포트는 22가 아닙니다. 이 규칙에서는 또한 이벤트와 관련된 호스트의 IP 주소가 10.4.x.x 네트워크 또는 192.168.x.x 네트워크에 있어야 한다고 요구합니다.

논리적으로 이 규칙은 다음과 같이 평가됩니다.

```
(A and B and (C or D))
```

표 51-15 규칙 평가

항목	조건의 내용
A	애플리케이션 프로토콜이 SSH임
B	애플리케이션 포트가 22가 아님
C	IP 주소가 10.4.0.0/8에 있음
D	IP 주소가 196.168.0.0/16에 있음

단일 조건을 추가하려면

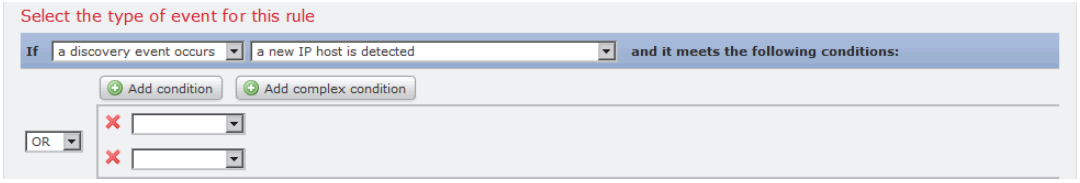
액세스: Admin/Discovery Admin

1단계 단일 조건을 추가하려면 현재 조건 위에서 **Add condition**을 클릭합니다.

새 조건이 현재의 조건 세트 아래에, 현재의 조건 세트와 동일한 레벨에 추가됩니다. 기본적으로 **OR** 연산자를 사용하여 동일한 레벨의 조건에 연결되지만, 연산자를 **AND**로 변경할 수 있습니다.

예를 들어 다음 규칙에 단순 조건을 추가할 경우

결과는 다음과 같습니다.



복합 조건을 추가하려면

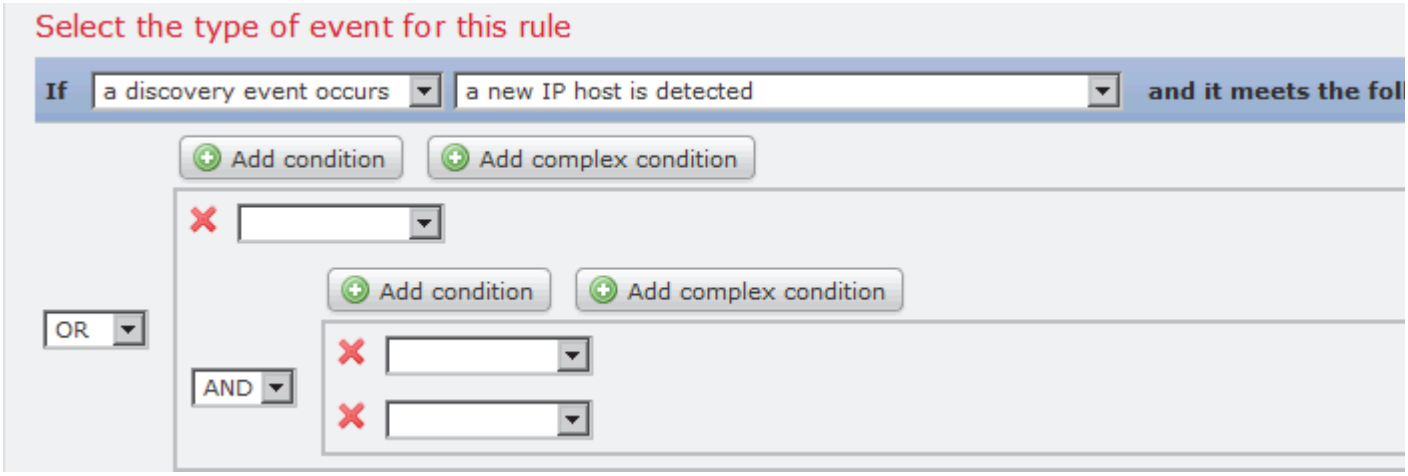
액세스: Admin/Discovery Admin

1단계 현재 조건 위에서 **Add complex condition**을 클릭합니다.

현재 조건 세트의 아래에 복합 조건이 추가됩니다. 복합 조건은 2개의 하위 조건으로 구성되며, 이들은 그 상위 레벨의 조건을 연결하는 데 쓰인 것과 상반되는 연산자로 연결됩니다.

예를 들어 다음 규칙에 복합 조건을 추가할 경우

결과는 다음과 같습니다.



조건을 연결하려면

액세스: Admin/Discovery Admin

1단계 조건 세트의 왼쪽에 있는 드롭다운 목록을 사용합니다.

- **AND** 연산자를 사용하면 이 연산자가 제어하는 레벨의 모든 조건을 충족해야 합니다.
- **OR** 연산자를 사용하면 이 연산자가 제어하는 레벨의 조건 중 하나만 충족해야 합니다.

하나의 조건에서 여러 값 사용

라이센스: 모두

조건을 작성할 때 조건 구문상 드롭다운 목록의 값 선택이 가능할 경우 대개는 목록에서 여러 값을 사용할 수 있습니다. 예를 들어 호스트에서 어떤 버전의 UNIX를 실행해야 하는 규칙에 호스트 프로필 자격을 추가하려는 경우, 여러 조건을 OR 연산자로 연결하지 않고 다음 절차를 사용합니다.

하나의 조건에 여러 값을 포함하려면

액세스: Admin/Discovery Admin

1단계 조건을 작성하면서 **is in** 또는 **is not in**을 연산자로 선택합니다.

드롭다운 목록이 텍스트 필드로 바뀝니다.

2단계 텍스트 필드의 아무 곳이나 클릭하거나 **Edit** 링크를 클릭합니다.

팝업 창이 나타납니다.

3단계 **Available**에서 Ctrl 키 또는 Shift 키를 누른 채로 클릭하여 여러 값을 선택합니다. 또는 클릭하고 드래그하여 인접한 여러 값을 선택할 수 있습니다.

4단계 오른쪽 화살표(>)를 클릭하여 선택한 항목을 **Selected**로 이동합니다.

5단계 **OK**를 클릭합니다.

Create Rule 페이지가 다시 나타납니다. 선택한 내용이 조건의 값 필드에 나타납니다.

상관관계 정책에 대한 규칙 관리

라이센스: 모두

상관관계 정책 내에서 사용되는 상관관계 규칙을 관리하려면 Rule Management 페이지를 사용하십시오. 규칙을 생성, 수정 및 삭제할 수 있습니다. 상관관계 규칙을 구성하는 데 도움이 되는 규칙 그룹을 생성할 수도 있습니다. 규칙 수정, 규칙 삭제, 규칙 그룹 생성에 대한 자세한 내용은 다음을 참조하십시오.

- 51-41페이지의 규칙 수정
- 51-42페이지의 규칙 삭제
- 51-42페이지의 규칙 그룹 생성

규칙 생성에 대한 자세한 내용은 51-3페이지의 상관관계 정책에 대한 규칙 생성을/를 참조하십시오.

규칙 수정

라이센스: 모두

기존 상관관계 규칙을 수정하려면 다음 절차를 사용하십시오.

기존 규칙을 수정하려면

액세스: Admin/Discovery Admin

1단계 **Policies > Correlation**을 선택한 다음 **Rule Management** 탭을 선택합니다.

Rule Management 페이지가 나타납니다.

2단계 규칙이 규칙 그룹에 있으면 그룹 이름을 클릭하여 그룹을 확장합니다.

3단계 수정하려는 규칙 옆에 있는 수정 아이콘( )을 클릭합니다.

Create Rule 페이지가 나타납니다.

4단계 필요한 대로 수정하고 **Save**를 클릭합니다.

규칙이 업데이트됩니다.

규칙 삭제

라이센스: 모두

하나 이상의 상관관계 정책에서 사용 중인 상관관계 규칙은 삭제할 수 없습니다. 먼저 규칙이 포함된 모든 정책에서 해당 규칙을 삭제해야 합니다. 정책에서 규칙을 삭제하는 방법에 대한 자세한 내용은 51-50페이지의 상관관계 정책 수정을/를 참조하십시오.

기존 규칙을 삭제하려면

액세스: Admin/Discovery Admin

1단계 **Policies > Correlation**을 선택한 다음 **Rule Management** 탭을 선택합니다.

Rule Management 페이지가 나타납니다.

2단계 규칙이 규칙 그룹에 있으면 그룹 이름을 클릭하여 그룹을 확장합니다.

3단계 삭제하려는 규칙 옆에 있는 삭제 아이콘( )을 클릭합니다.

4단계 규칙을 삭제할 것임을 확인합니다.

규칙이 삭제됩니다.

규칙 그룹 생성

라이센스: 모두

상관관계 규칙을 구성하는 데 도움이 되는 규칙 그룹을 생성합니다. FireSIGHT 시스템에는 기능별로 그룹화할 수 있는 많은 기본 규칙이 제공됩니다. 예를 들어 Worms 규칙 그룹은 공통된 웜 기준으로 활동을 탐지하는 규칙으로 구성되어 있습니다. 규칙 그룹의 목적은 오로지 상관관계 규칙을 편리하게 구성하는 것입니다. 규칙의 그룹을 상관관계 정책에 할당할 수 없습니다. 대신 각 규칙을 개별적으로 추가해야 합니다.

규칙을 생성하면 기존 그룹에 추가할 수 있습니다. 또한 그룹에 추가하기 위해 기존 규칙을 수정할 수도 있습니다. 자세한 내용은 다음 절을 참조하십시오.

- 51-3페이지의 상관관계 정책에 대한 규칙 생성
- 51-41페이지의 규칙 수정

팁 규칙 그룹을 삭제하려면 삭제할 그룹 옆에 있는 삭제 아이콘( )을 클릭합니다. 규칙 그룹을 삭제해도 그룹에 있던 규칙은 삭제되지 **않습니다**. 단지 그룹이 해제될 뿐입니다.

규칙 그룹을 생성하려면

액세스: Admin/Discovery Admin

1단계 **Policies > Correlation**을 선택한 다음 **Rule Management** 탭을 선택합니다.

Rule Management 페이지가 나타납니다.

2단계 **Create Group**을 클릭합니다.

Create Group 페이지가 나타납니다.

3단계 **Group Name** 필드에 그룹의 이름을 입력합니다.

4단계 **Add Group**을 클릭합니다.

그룹이 추가됩니다.

상관관계 응답 그룹화

라이센스: 모두

알림 응답과 교정을 생성했으면(43-2페이지의 알림 응답 작업 및 54-1페이지의 교정 생성 참조), 정책 위반이 그룹 내 모든 응답을 트리거하도록 이들을 그룹화할 수 있습니다. 응답 그룹을 상관관계 규칙에 할당하려면 먼저 Groups 페이지에서 그룹을 만들어야 합니다.

그룹 옆의 슬라이더는 그룹이 활성 상태인지를 나타냅니다. 상관관계 정책 내 규칙에 응답 그룹을 할당하려면 먼저 활성화해야 합니다. **Sort by** 드롭다운 목록을 사용하여 응답 그룹을 상태순으로(활성/비활성) 또는 이름 알파벳순으로 정렬할 수 있습니다.

자세한 내용은 다음 절을 참조하십시오.

- 51-43페이지의 응답 그룹 생성
- 51-44페이지의 응답 그룹 수정
- 51-44페이지의 응답 그룹 삭제
- 51-45페이지의 응답 그룹 활성화 및 비활성화

응답 그룹 생성

라이센스: 모두

개별 알림과 교정을 응답 그룹에 둘 수 있으며, 정책 위반이 발생할 때 알림 및 교정의 그룹이 실행될 수 있도록 상관관계 정책 내 규칙에 이를 할당할 수 있습니다. 활성 정책의 규칙에 그룹이 할당되면, 그룹에 대한 변경 사항 및 그룹 내 알림 또는 교정에 대한 변경 사항이 활성 정책에 자동으로 적용됩니다.

응답 그룹을 생성하려면

액세스: Admin

1단계 **Policies > Correlation**을 선택한 다음 **Groups**를 클릭합니다.

Groups 페이지가 나타납니다.

2단계 **Create Group**을 클릭합니다.

Response Group 페이지가 나타납니다.

3단계 **Name** 필드에 새 그룹의 이름을 입력합니다.

4단계 상관관계 정책 위반에 대한 응답에서 사용할 수 있도록 그룹을 활성화하려면 **Active**를 선택합니다.

5단계 그룹에 포함할 알림과 교정을 **Available Responses** 목록에서 선택합니다.

팁 여러 응답을 선택하려면 Ctrl 키를 누른 상태에서 클릭하십시오.

6단계 알림과 교정을 그룹으로 이동하려면 **>** 화살표를 클릭합니다.

반대로, **Responses in Group** 목록에서 알림과 교정을 선택하고 **<** 화살표를 클릭하면 응답 그룹 밖으로 이동할 수 있습니다.

7단계 **Save**를 클릭합니다.

그룹이 생성됩니다.

응답 그룹 수정

라이센스: 모두

응답 그룹을 수정하려면 다음 절차를 사용하십시오.

응답 그룹을 수정하려면

액세스: Admin

1단계 **Policies > Correlation**을 선택한 다음 **Groups**를 클릭합니다.

Groups 페이지가 나타납니다.

2단계 수정할 그룹 옆의 수정 아이콘( )을 클릭합니다.

Response Group 페이지가 나타납니다.

3단계 필요한 대로 변경하고 **Save**를 클릭합니다.

그룹이 활성 상태이고 사용 중이면 변경한 내용이 즉시 적용됩니다.

응답 그룹 삭제

라이센스: 모두

상관관계 정책에서 사용되고 있지 않다면 응답 그룹을 삭제할 수 있습니다. 응답 그룹을 삭제하는 경우 그룹 내 응답이 삭제되는 것이 **아니라** 서로의 관계가 해제되는 것입니다.

응답 그룹을 삭제하려면

액세스: Admin

1단계 **Policies > Correlation**을 선택한 다음 **Groups**를 클릭합니다.

Groups 페이지가 나타납니다.

2단계 삭제할 그룹 옆에 있는 삭제 아이콘( )을 클릭합니다.

3단계 그룹을 삭제할 것임을 확인합니다.

그룹이 삭제됩니다.

응답 그룹 활성화 및 비활성화

라이센스: 모두

응답 그룹을 삭제하지 않은 채 일시적으로 비활성화할 수 있습니다. 이 경우 시스템에 그룹은 그대로 남아 있지만, 그룹이 할당되어 있는 정책의 위반이 발생할 경우 해당 그룹이 실행되지 않습니다. 응답 그룹을 상관관계 정책에서 사용하는 경우 이를 비활성화하면, 비활성화되었더라도 여전히 사용 중인 것으로 간주됩니다. 사용 중인 응답 그룹은 삭제할 수 없습니다.

응답 그룹을 활성화 또는 비활성화하려면

액세스: Admin

1단계 **Policies > Correlation**을 선택한 다음 **Groups**를 클릭합니다.

Groups 페이지가 나타납니다.

2단계 활성화 또는 비활성화할 응답 그룹 옆에 있는 슬라이더를 클릭합니다.

그룹이 활성화되었던 경우 비활성화되고, 비활성화되었던 경우 활성화됩니다.

상관관계 정책 생성

라이센스: 모두

상관관계 규칙이나 규정준수 화이트리스트(또는 둘 다), 그리고 선택적으로 알림 응답과 교정을 생성했으면 이들을 사용해 상관관계 정책을 작성할 수 있습니다.

네트워크 트래픽이 상관관계 규칙 또는 정책의 화이트리스트에 지정된 기준을 충족하면 방어 센터는 상관관계 이벤트 또는 화이트리스트 이벤트를 생성합니다. 또한 규칙 또는 화이트리스트에 할당한 응답도 실행합니다. 각 규칙이나 화이트리스트를 단일 응답 또는 응답의 그룹에 매핑할 수 있습니다. 네트워크 트래픽이 여러 규칙 또는 화이트리스트를 트리거하는 경우 방어 센터는 각 규칙 및 화이트리스트와 연결된 모든 응답을 실행합니다.

상관관계 정책 작성에 사용할 수 있는 응답, 상관관계 규칙 및 규정 준수 화이트리스트의 생성에 대한 자세한 내용은 다음 절을 참조하십시오.

- 51-3페이지의 상관관계 정책에 대한 규칙 생성
- 52-8페이지의 규정준수 화이트리스트 생성

- 43-1페이지의 외부 알림 구성
- 54-1페이지의 교정 구성

팁 선택적으로, 정책 윤곽을 생성하고 나중에 이를 수정하여 규칙과 응답을 추가할 수 있습니다.

상관관계 정책을 생성하려면

액세스: Admin/Discovery Admin

1단계 **Policies > Correlation**을 선택합니다.

Policy Management 페이지가 나타납니다.

2단계 **Create Policy**를 클릭합니다.

Create Policy 페이지가 나타납니다.

3단계 이름 및 설명 등 기본 정책 정보를 제공합니다.

51-46페이지의 기본 정책 정보 제공을/를 참조하십시오.

4단계 상관관계 정책에 하나 이상의 규칙 또는 화이트리스트를 추가합니다.

51-47페이지의 상관관계 정책에 규칙 및 화이트리스트 추가을/를 참조하십시오.

5단계 선택적으로, 규칙 및 화이트리스트 우선순위를 설정합니다.

51-48페이지의 규칙 및 화이트리스트 우선순위 설정을/를 참조하십시오.

6단계 선택적으로, 추가한 규칙 또는 화이트리스트에 응답을 추가합니다.

51-48페이지의 규칙 및 화이트리스트에 응답 추가을/를 참조하십시오.

7단계 **Save**를 클릭합니다.

정책이 저장됩니다.

참고 상관관계 및 화이트리스트 이벤트를 생성하고 정책 위반에 대해 응답을 실행하려면 먼저 정책을 활성화해야 합니다. 자세한 내용은 51-49페이지의 상관관계 정책 관리을/를 참조하십시오.

기본 정책 정보 제공

라이센스: 모두

각 정책에 식별 이름을 제공해야 합니다. 선택적으로, 정책에 짧은 설명을 추가할 수 있습니다.

정책에 사용자 정의 우선순위를 할당할 수도 있습니다. 상관관계 정책 위반이 발생할 경우 그 결과로 생성되는 상관관계 이벤트에는 사용자가 정책에 할당한 우선순위 값이 표시됩니다(트리거된 규칙에 자체 우선순위가 없는 경우).

참고 규칙 및 화이트리스트 우선순위는 정책 우선순위를 재정의합니다. 자세한 내용은 51-47페이지의 상관관계 정책에 규칙 및 화이트리스트 추가을/를 참조하십시오.

기본 정책 정보를 제공하려면

액세스: Admin/Discovery Admin

1단계 Create Policy 페이지의 **Policy Name** 필드에 정책의 이름을 입력합니다.

2단계 **Policy Description** 필드에 정책에 대한 설명을 입력합니다.

3단계 **Default Priority** 드롭다운 목록에서 정책의 우선순위를 선택합니다.

1~5의 우선순위 값을 선택할 수 있습니다. 1은 가장 높은 값이고 5는 가장 낮은 값입니다. 또는 특정 규칙에 할당된 우선순위만을 사용하려면 **None**을 선택할 수 있습니다.

4단계 다음 절, 51-47페이지의 상관관계 정책에 규칙 및 화이트리스트 추가에서 절차를 계속 진행합니다.

상관관계 정책에 규칙 및 화이트리스트 추가

라이센스: 모두

상관관계 정책에는 하나 이상의 상관관계 규칙 또는 화이트리스트가 포함되어 있습니다. 정책의 규칙 또는 화이트리스트 위반이 발생하면 시스템은 데이터베이스에 이벤트를 로깅합니다. 규칙 또는 화이트리스트에 하나 이상의 응답을 할당한 경우 해당 응답이 실행됩니다.

다음 그림에서는 규정 준수 화이트리스트 및 상관관계 규칙의 집합을 포함하며 다양한 응답으로 구성된 상관관계 정책을 보여줍니다.

Policy Rules

Rule	Responses
Bugbear Worm Detects the Bugbear HTTP server backdoor	Sample Email Alert Response (Email
Default White List	Sample SNMP Alert Response (SNMP
Lovgate Worm Detects activity by the Lovgate worm backdoor component	Sample Syslog Alert Response (Sysl
MyDoom Worm Detects activity by the backdoor component of MyDoom	Sample Syslog Alert Response (Sysl Sample SNMP Alert Response (SNMP Sample Email Alert Response (Email
NetSky.S Detects the backdoor component of the NetSky.S worm.	This rule does not have any respons

상관관계 정책에 규칙 또는 화이트리스트를 추가하려면

액세스: Admin/Discovery Admin

1단계 Create Policy 페이지에서 **Add Rules**를 클릭합니다.

Available Rules 팝업 창이 나타납니다.

2단계 해당 폴더 이름을 클릭하여 확장합니다.

3단계 정책에서 사용할 규칙 및 화이트리스트를 선택하고 **Add**를 클릭합니다.

Create Policy 페이지가 다시 나타납니다. 선택한 규칙 및 화이트리스트가 정책을 채웁니다.

4단계 다음 절, 51-48페이지의 규칙 및 화이트리스트 우선순위 설정에서 절차를 계속 진행합니다.

규칙 및 화이트리스트 우선순위 설정

라이센스: 모두

상관관계 정책의 각 상관관계 규칙 또는 규정준수 화이트리스트에 사용자 정의 우선순위를 할당할 수 있습니다. 규칙 또는 화이트리스트가 트리거되면 규칙이나 화이트리스트에 할당한 우선순위가 그 결과로 생성되는 이벤트에 표시됩니다. 반면, 우선순위 값을 할당하지 않은 상태에서 규칙 또는 화이트리스트가 트리거되면 그 결과로 생성되는 이벤트에 정책의 우선순위 값이 표시됩니다.

예를 들어 정책 자체의 우선순위는 1이고 해당 규칙 또는 화이트리스트는 기본 우선순위로 설정된(우선순위 3으로 설정된 규칙 하나 제외) 정책이 있다고 가정해보겠습니다. 우선순위 3 규칙이 트리거되면 그 결과로 실행되는 상관관계 이벤트의 우선순위 값은 3으로 표시됩니다. 정책의 다른 규칙 또는 화이트리스트가 트리거되면 그 결과로 생성되는 이벤트의 우선순위 값은 2로 표시되어 정책의 우선순위를 그대로 유지합니다.

규칙 또는 화이트리스트 우선순위를 설정하려면

액세스: Admin/Discovery Admin

1단계 Create Policy 페이지에서 각 규칙 또는 화이트리스트에 대한 **Priority** 목록에서 기본 우선순위를 선택합니다. 다음을 선택할 수 있습니다.

- 1~5의 우선순위 값 - 1은 가장 높은 값이고 5는 가장 낮은 값
- **None**
- **Default** - 정책의 기본 우선순위 사용

2단계 다음 절, 51-48페이지의 규칙 및 화이트리스트에 응답 추가에서 절차를 계속 진행합니다.

규칙 및 화이트리스트에 응답 추가

라이센스: 모두

상관관계 정책 내에서 각 규칙이나 화이트리스트를 단일 응답 또는 응답의 그룹에 매핑할 수 있습니다. 정책의 규칙 또는 화이트리스트 중 하나가 위반되면 시스템은 관련 이벤트를 데이터베이스에 로깅하고, 해당 규칙 또는 화이트리스트에 할당된 응답을 실행합니다. 정책 내 여러 규칙 또는 화이트리스트가 트리거되면 방어 센터는 각 규칙 또는 화이트리스트와 관련된 응답을 실행합니다.

응답 및 응답 그룹 생성에 대한 자세한 내용은 다음을 참조하십시오.

- 43-1페이지의 외부 알림 구성
- 54-1페이지의 교정 구성
- 51-43페이지의 상관관계 응답 그룹화

참고 트래픽 프로필 변경을 트리거하는 상관관계 규칙에는 Nmap 교정을 응답으로서 할당하지 **마십시오**. 교정이 실행되지 않습니다.

다음 그림에서는 규정 준수 화이트리스트 및 상관관계 규칙의 집합을 포함하며 다양한 응답으로 구성된 상관관계 정책을 보여줍니다.

Policy Rules

Rule	Responses
Bugbear Worm Detects the Bugbear HTTP server backdoor	Sample Email Alert Response (Email
Default White List	Sample SNMP Alert Response (SNMP
Lovgate Worm Detects activity by the Lovgate worm backdoor component	Sample Syslog Alert Response (Sysl
MyDoom Worm Detects activity by the backdoor component of MyDoom	Sample Syslog Alert Response (Sysl Sample SNMP Alert Response (SNMP Sample Email Alert Response (Email
NetSky.S Detects the backdoor component of the NetSky.S worm.	This rule does not have any respons

규칙 및 화이트리스트에 응답을 추가하려면

액세스: Admin/Discovery Admin

1단계 Create Policy 페이지에서, 응답을 추가하려는 규칙 또는 화이트리스트 옆에 있는 응답 아이콘( )을 클릭합니다.

팝업 창이 나타납니다.

2단계 **Unassigned Responses** 아래에서 규칙 또는 화이트리스트가 트리거될 때 실행할 응답, 여러 응답 또는 응답 그룹을 선택하고 위쪽 화살표를 클릭합니다.

팁 여러 응답을 선택하려면 Ctrl 키를 누른 상태에서 클릭하십시오.

3단계 **Update**를 클릭합니다.

Create Policy 페이지가 다시 나타납니다. 지정한 응답이 규칙 또는 화이트리스트에 추가됩니다.

상관관계 정책 관리

라이센스: 모두

Policy Management 페이지에서 상관관계 정책을 관리합니다. 정책을 생성, 수정, 정렬, 활성화, 비활성화 및 삭제할 수 있습니다.

정책 옆의 슬라이더는 그룹이 활성 상태인지를 나타냅니다. 정책이 상관관계 이벤트 및 화이트리스트 이벤트를 생성하도록 하려면 먼저 정책을 활성화해야 합니다. **Sort by** 드롭다운 목록을 사용하여 정책을 상태순으로(활성/비활성) 또는 이름 알파벳순으로 정렬할 수 있습니다.

활성 상관관계 정책에 규정준수 화이트리스트가 포함되어 있는 경우 다음 작업을 수행하면 화이트리스트와 관련된 호스트 특성이 삭제되지 **않으며** 호스트 특성의 값이 변경되지도 않습니다.

- 정책 비활성화
- 정책을 수정하여 화이트리스트 제거
- 정책 삭제

즉, 작업 수행 시 규정을 준수한 호스트는 호스트 특성 네트워크 맵에 여전히 규정을 준수하는 것으로 나타나는 식입니다. 호스트 특성을 삭제하려면 해당 화이트리스트를 삭제해야 합니다.

네트워크에서 호스트의 화이트리스트 규정준수를 업데이트하려면 상관관계 정책을 다시 활성화하거나(비활성화한 경우) 화이트리스트를 또 다른 활성 상관관계 정책에 추가해야 합니다(상관관계 정책에서 화이트리스트를 삭제했거나 정책 자체를 삭제한 경우). 이 작업을 수행할 때 발생하는 화이트리스트를 재평가할 경우 화이트리스트 이벤트가 생성되지 **않으며** 따라서 화이트리스트와 연결한 응답도 트리거되지 않습니다. 규정준수 화이트리스트에 대한 자세한 내용은 52-1페이지의 규정준수 툴로 FireSIGHT 시스템 사용을/를 참조하십시오.

상관관계 정책 관리에 대한 자세한 내용은 다음을 참조하십시오.

- 51-50페이지의 상관관계 정책 활성화 및 비활성화
- 51-50페이지의 상관관계 정책 수정
- 51-51페이지의 상관관계 정책 삭제

새 정책 생성에 대한 자세한 내용은 51-45페이지의 상관관계 정책 생성을/를 참조하십시오.

상관관계 정책 활성화 및 비활성화

라이센스: 모두

상관관계 정책을 활성화 또는 비활성화하려면 다음 절차를 사용하십시오.

정책을 활성화 또는 비활성화하려면

액세스: Admin/Discovery Admin

1단계 **Policies > Correlation**을 선택합니다.

Policy Management 페이지가 나타납니다.

2단계 활성화 또는 비활성화할 정책 옆에 있는 슬라이더를 클릭합니다.

정책이 활성화되었던 경우 비활성화되고, 비활성화되었던 경우 활성화됩니다.

상관관계 정책 수정

라이센스: 모두

상관관계 정책을 수정하려면 다음 절차를 사용하십시오.

정책을 수정하려면

액세스: Admin/Discovery Admin

1단계 **Policies > Correlation**을 선택합니다.

Policy Management 페이지가 나타납니다.

2단계 정책 옆에 있는 수정 아이콘( )을 클릭합니다.

Create Policy 페이지가 나타납니다. 변경할 수 있는 각종 컨피그레이션에 대한 자세한 내용은 51-45페이지의 상관관계 정책 생성을/를 참조하십시오. 상관관계 정책에서 규칙 또는 화이트리스트를 제거하려면, Create Policy 페이지에서 제거할 규칙 또는 화이트리스트 옆에 있는 삭제 아이콘( )을 클릭합니다.

3단계 필요한 대로 변경하고 **Save**를 클릭합니다.

정책이 변경됩니다. 정책이 활성 상태인 경우 변경한 내용이 즉시 적용됩니다.

상관관계 정책 삭제

라이센스: 모두

상관관계 정책을 삭제하려면 다음 절차를 사용하십시오.

정책을 삭제하려면

액세스: Admin/Discovery Admin

1단계 **Policies > Correlation**을 선택합니다.

Policy Management 페이지가 나타납니다.

2단계 삭제할 정책 옆에 있는 삭제 아이콘( )을 클릭합니다.

정책이 삭제됩니다.

상관관계 이벤트 작업

라이센스: 모두

활성 상관관계 정책 내 상관관계 규칙이 트리거되면 방어 센터는 상관관계 이벤트를 생성하고 이를 데이터베이스에 로깅합니다. 데이터베이스에 저장되는 상관관계 이벤트 수를 구성하는 방법에 대한 자세한 내용은 63-15페이지의 데이터베이스 이벤트 제한 구성을/를 참조하십시오.

참고 활성 상관관계 정책 내 규정준수 화이트리스트가 트리거되면 방어 센터는 화이트리스트 이벤트를 생성합니다. 자세한 내용은 52-30페이지의 화이트리스트 이벤트 작업을/를 참조하십시오.

자세한 내용은 다음 절을 참조하십시오.

- 51-52페이지의 상관관계 이벤트 보기
- 51-53페이지의 상관관계 이벤트 테이블 이해
- 51-55페이지의 상관관계 이벤트 검색

상관관계 이벤트 보기

라이센스: 모두

상관관계 이벤트의 테이블을 본 후, 찾고 있는 정보에 따라 이벤트 보기를 조작할 수 있습니다.

상관관계 이벤트에 액세스할 때 표시되는 페이지는 사용하는 워크플로에 따라 달라집니다. 상관관계 이벤트의 테이블 보기를 포함하는 사전 정의 워크플로를 사용할 수 있습니다. 특정 요구와 일치하는 정보만 표시하는 사용자 지정 워크플로를 생성할 수도 있습니다. 사용자 지정 워크플로 생성에 대한 자세한 내용은 58-38페이지의 사용자 지정 워크플로 생성을/를 참조하십시오.

다음 표에서는 상관관계 이벤트 워크플로 페이지에서 수행할 수 있는 몇 가지 특정 작업에 대해 설명합니다.

표 51-16 상관관계 이벤트 작업

목적	가능한 작업
IP 주소에 대한 호스트 프로필 보기	IP 주소 옆에 나타나는 호스트 프로필 아이콘을 클릭합니다.
사용자 프로필 정보 보기	사용자 ID 옆에 나타나는 사용자 아이콘( )을 클릭합니다. 자세한 내용은 50-63페이지의 사용자 세부사항 및 호스트 기록 이해을/를 참조하십시오.
현재 워크플로 페이지에서 이벤트를 정렬 및 제한	58-34페이지의 드릴다운 워크플로 페이지 정렬에서 자세히 알아보십시오.
현재 워크플로 페이지 내에서 이동	58-35페이지의 워크플로의 다른 페이지로 이동에서 자세히 알아보십시오.
현재의 제약 조건을 유지한 채 현재 워크플로에서 페이지 간 이동	워크플로 페이지의 왼쪽 위에서 적절한 페이지 링크를 클릭합니다. 자세한 내용은 58-18페이지의 워크플로 페이지 사용을/를 참조하십시오.
나타나는 열에 대해 자세히 알아보기	51-53페이지의 상관관계 이벤트 테이블 이해에서 자세히 알아보십시오.
표시된 이벤트에 대한 시간 및 날짜 범위 수정	58-22페이지의 이벤트 시간 제약 조건 설정에서 자세히 알아보십시오. 어플라이언스의 구성된 시간 창(전역이든 이벤트 전용이든)을 벗어나 생성된 이벤트는 시간 기준으로 이벤트 보기를 제한할 경우 이벤트 보기에 나타날 수 있습니다. 이는 어플라이언스에 대한 슬라이딩 시간 창을 구성한 경우에도 발생할 수 있습니다.
워크플로의 다음 페이지로 드릴다운하여 특정 값으로 제한	다음 방법 중 하나를 사용합니다. • 사용자 지정 워크플로에서 생성한 드릴다운 페이지에서 행 내의 값을 클릭합니다. 테이블 보기의 행 내에서 값을 클릭하면 테이블 보기가 제한되며 다음 페이지로 드릴다운되지 **않습니다**. • 일부 사용자로 제한하여 다음 워크플로 페이지로 드릴다운하려면, 다음 워크플로 페이지에서 볼 사용자의 옆에 있는 확인란을 선택하고 **View**를 클릭합니다. • 현재의 제약 조건을 유지한 채 다음 워크플로 페이지로 드릴다운하려면 **View All**을 클릭합니다. **팁** 테이블 보기의 페이지 이름에는 항상 "Table View"가 포함됩니다. 자세한 내용은 58-30페이지의 이벤트 제한을/를 참조하십시오.

표 51-16 상관관계 이벤트 작업 (계속)

목적	가능한 작업
시스템에서 상관관계 이벤트 삭제	다음 방법 중 하나를 사용합니다. • 일부 이벤트를 삭제하려면 삭제할 이벤트 옆의 확인란을 선택한 다음 **Delete**를 클릭합니다. • 현재 제한된 보기에서 모든 이벤트를 삭제하려면 **Delete All**을 클릭하고 모든 이벤트를 삭제할 것인지를 확인합니다.
관련 이벤트를 보기 위해 다른 이벤트 보기로 이동	58-35페이지의 워크플로 간 이동에서 자세히 알아보십시오.

상관관계 이벤트를 보려면

액세스: Admin/Any Security Analyst

1단계 **Analysis > Correlation > Correlation Events**를 선택합니다.

기본 상관관계 이벤트 워크플로의 첫 번째 페이지가 나타납니다. 사용자 지정 워크플로를 비롯한 다른 워크플로를 사용하려면 워크플로 제목 옆의 **(switch workflow)**를 클릭합니다. 다른 기본 워크플로 지정에 대한 자세한 내용은 71-3페이지의 이벤트 보기 설정 구성을/를 참조하십시오. 이벤트가 표시되지 않을 경우 시간 범위를 조정해야 할 수 있습니다. 58-22페이지의 이벤트 시간 제약 조건 설정을/를 참조하십시오.

팁 상관관계 이벤트의 테이블 보기가 포함되지 않은 사용자 지정 워크플로를 사용 중인 경우 **(switch workflow)**를 클릭한 다음 **Correlation Events**를 선택하십시오.

상관관계 이벤트 테이블 이해

라이센스: 모두

상관관계 규칙이 트리거되면 방어 센터는 상관관계 이벤트를 생성합니다. 다음 표에서는 상관관계 이벤트 테이블의 필드에 대해 설명합니다.

표 51-17 상관관계 이벤트 필드

필드	설명
Time	상관관계 이벤트가 생성된 날짜 및 시간.
Impact	침입 데이터, 검색 데이터 및 취약성 정보 간 상관관계를 기반으로 상관관계 이벤트에 할당되는 영향 레벨 자세한 내용은 41-38페이지의 이벤트를 평가하기 위한 영향 레벨 사용을/를 참조하십시오.

표 51-17 상관관계 이벤트 필드 (계속)

필드	설명
Inline Result	다음 중 하나: • 검은색 아래쪽 화살표 - 시스템이 침입 규칙을 트리거한 패킷을 삭제했음을 나타냄 • 회색 아래쪽 화살표 - **Drop when Inline** 침입 정책 옵션을 활성화할 경우 시스템이 인라인, 스위치드 또는 라우티드 구축에서 패킷을 삭제할 것임을 나타냄 • 비어 있음 - 트리거된 침입 규칙이 Drop 및 Generate 이벤트로 설정되지 않았음을 나타냄 침입 정책의 규칙 상태 또는 삭제 동작과 상관없이, 인라인 집합이 탭 모드인 경우를 포함하여 패시브 구축에서는 시스템이 패킷을 삭제하지 않습니다.
Source IP 또는 Destination IP	정책 위반을 트리거한 이벤트에서 소스 또는 대상 호스트의 IP 주소.
Source Country 또는 Destination Country	정책 위반을 트리거한 이벤트에서 소스 또는 목적지 IP 주소와 관련된 국가.
Security Intelligence Category	정책 위반을 트리거한 이벤트에서 블랙리스트 IP 주소를 포함하거나 나타내는 블랙리스트 객체의 이름.
Source User 또는 Destination User	정책 위반을 트리거한 이벤트에서 소스 또는 대상 호스트에 로그인한 사용자의 이름.
Source Port/ICMP Type 또는 Destination Port/ICMP Code	정책 위반을 트리거한 이벤트와 관련된 소스 트래픽의 소스 포트 또는 ICMP 유형, 또는 대상 트래픽의 목적지 포트 또는 ICMP 코드.
Description	상관관계 이벤트의 설명. 설명의 정보는 규칙이 트리거된 방식에 따라 달라집니다. 예를 들어 규칙이 운영 체제 정보 업데이트 이벤트에 의해 트리거된 경우 새 운영 체제 이름 및 신뢰도 레벨이 나타납니다.
Policy	위반된 정책의 이름.
Rule	정책 위반을 트리거한 규칙의 이름.
Priority	정책 위반을 트리거한 정책 또는 규칙에 의해 지정된 우선순위.
Source Host Criticality 또는 Destination Host Criticality	상관관계 이벤트와 관련된 소스 또는 대상 호스트의 사용자 할당 호스트 중요도: `None`, `Low`, `Medium` 또는 `High`. 검색 이벤트, 호스트 입력 이벤트 또는 연결 이벤트 기반의 규칙에 의해 생성된 상관관계 이벤트에만 소스 호스트 중요도가 포함됩니다. 호스트 중요도에 대한 자세한 내용은 49-30페이지의 사전 정의 호스트 특성 작업을/를 참조하십시오.
Ingress Security Zone 또는 Egress Security Zone	정책 위반을 트리거한 침입 또는 연결 이벤트의 인그레스 또는 이그레스 보안 영역.
Device	정책 위반을 트리거한 이벤트를 생성한 디바이스의 이름.
Ingress Interface 또는 Egress Interface	정책 위반을 트리거한 침입 또는 연결 이벤트의 인그레스 또는 이그레스 인터페이스.
Count	각 행에 표시되는 정보와 매칭되는 이벤트의 수. 둘 이상의 동일한 행을 생성하는 제약 조건을 적용한 경우에만 **Count** 필드가 나타납니다.

상관관계 이벤트 테이블 표시에 대한 자세한 내용은 다음을 참조하십시오.

- 51-52페이지의 상관관계 이벤트 보기
- 51-55페이지의 상관관계 이벤트 검색

상관관계 이벤트 검색

라이센스: 모두

특정 상관관계 이벤트를 검색할 수 있습니다. 네트워크 환경에 맞춤화된 검색을 생성한 다음 나중에 다시 사용할 수 있도록 저장할 수 있습니다. 다음 표에는 사용할 수 있는 검색 기준이 설명되어 있습니다.

표 51-18 상관관계 이벤트 검색 기준

필드	검색 기준 규칙
Policy	검색할 상관관계 정책의 이름을 입력합니다.
Rule	검색할 상관관계 규칙의 이름을 입력합니다.
Description	상관관계 이벤트 설명의 전체 또는 일부를 입력합니다. 설명의 정보는 규칙을 트리거한 이벤트에 따라 달라집니다.
Priority	트리거된 규칙 또는 위반된 상관관계 정책의 우선순위에 의해 결정되는 상관관계 이벤트의 우선순위를 지정합니다. 우선순위가 없는 경우 none을 입력합니다. 상관관계 규칙 및 정책 우선순위 설정에 대한 자세한 내용은 51-46페이지의 기본 정책 정보 제공 및 51-48페이지의 규칙 및 화이트리스트 우선순위 설정을/를 참조하십시오.
Source Country, Destination Country 또는 Source/Destination Country	정책 위반을 트리거한 이벤트에서 소스, 대상 또는 소스나 대상 호스트 IP 주소와 연결된 국가를 지정합니다.
Source Continent, Destination Continent 또는 Source/Destination Continent	정책 위반을 트리거한 이벤트에서 소스, 대상 또는 소스나 대상 호스트 IP 주소와 연결된 대륙을 지정합니다.
Security Intelligence Category	정책 위반을 트리거한 상관관계 이벤트와 관련된 보안 인텔리전스 카테고리를 지정합니다. 보안 인텔리전스 카테고리는 보안 인텔리전스 객체의 이름, 전역 블랙리스트, 사용자 지정 보안 인텔리전스 목록이나 피드이거나 인텔리전스 피드의 카테고리 중 하나일 수 있습니다. 자세한 내용은 13-1페이지의 보안 인텔리전스 IP 주소 평판 블랙리스트에 추가을/를 참조하십시오.
Source IP, Destination IP 또는 Source/Destination IP	정책 위반을 트리거한 이벤트에서 소스, 대상 또는 소스나 대상 호스트의 IP 주소를 지정합니다. 단일 IP 주소나 주소 블록 또는 쉼표로 구분된 목록을 지정할 수 있습니다(둘 중 하나 또는 모두). 또한 부정을 사용할 수 있습니다. 자세한 내용은 60-6페이지의 검색에서 IP 주소 지정을/를 참조하십시오.
Source User 또는 Destination User	정책 위반을 트리거한 이벤트에서 소스 또는 대상 호스트에 로그인한 사용자를 지정합니다.
Source Port/ICMP Type 또는 Destination Port/ICMP Code	정책 위반을 트리거한 이벤트와 관련된 소스 트래픽의 소스 포트 또는 ICMP 유형, 또는 대상 트래픽의 목적지 포트 또는 ICMP 코드를 지정합니다.
Impact	상관관계 이벤트에 할당되는 영향 레벨을 지정합니다. 유효한 값(대/소문자를 구분하지 않음): `Impact 0`, `Impact Level 0`, `Impact 1`, `Impact Level 1`, `Impact 2`, `Impact Level 2`, `Impact 3`, `Impact Level 3`, `Impact 4` 및 `Impact Level 4`. 영향 아이콘 색상 또는 부분 문자열(예: `blue`, `level 1` 또는 `0`)을 사용하지 마십시오. 자세한 내용은 41-38페이지의 이벤트를 평가하기 위한 영향 레벨 사용을/를 참조하십시오.

표 51-18 상관관계 이벤트 검색 기준 (계속)

필드	검색 기준 규칙
Inline Result	침입 이벤트에 의해 트리거된 정책 위반에 대해 다음 중 하나를 입력합니다. • `dropped` - 패킷이 인라인, 스위치드 또는 라우티드 구축에서 삭제되었는지 여부를 지정 • `would have dropped` - 인라인, 스위치드 또는 라우티드 구축에서 패킷을 삭제하도록 침입 정책을 구성했다면 패킷이 삭제되었을 것인지를 지정 침입 정책의 규칙 상태 또는 삭제 동작과 상관없이, 인라인 집합이 탭 모드인 경우를 포함하여 패시브 구축에서는 시스템이 패킷을 삭제하지 않습니다.
Source Host Criticality 또는 Destination Host Criticality	정책 위반과 관련된 소스 또는 대상 호스트의 호스트 중요도를 지정합니다(`None`, `Low`, `Medium` 또는 `High`). 검색 이벤트, 호스트 입력 이벤트 또는 연결 이벤트 기반의 규칙에 의해 생성된 상관관계 이벤트에만 소스 호스트 중요도가 포함됩니다. 호스트 중요도에 대한 자세한 내용은 49-30페이지의 사전 정의 호스트 특성 작업을/를 참조하십시오.
Ingress Security Zone, Egress Security Zone 또는 Ingress/Egress Security Zone	정책 위반을 트리거한 침입 또는 연결 이벤트에서 인그레스, 이그레스 또는 인그레스나 이그레스 보안 영역을 지정합니다.
Device	정책 위반을 트리거한 이벤트를 생성한 특정 디바이스로 검색을 제한하려면 디바이스 이름이나 IP 주소, 디바이스 그룹, 스택 또는 클러스터 이름을 입력합니다. FireSIGHT 시스템에서 검색 시 디바이스 필드를 취급하는 방법에 대한 자세한 내용은 60-7페이지의 검색에서 디바이스 지정을/를 참조하십시오.
Ingress Interface 또는 Egress Interface	정책 위반을 트리거한 침입 또는 연결 이벤트의 인그레스 또는 이그레스 인터페이스를 지정합니다.

상관관계 이벤트를 검색하려면

액세스: Admin/Any Security Analyst

1단계 **Analysis > Search**를 선택합니다.

Search 페이지가 나타납니다.

2단계 테이블 드롭다운 목록에서 **Correlation Events**를 선택합니다.

해당 제약 조건으로 페이지가 업데이트됩니다.

3단계 상관관계 이벤트 검색 기준 표에 설명된 대로 해당 필드에 검색 기준을 입력합니다.

- 모든 필드에 부정(`!`)을 사용할 수 있습니다.
- 모든 필드에 쉼표로 구분된 검색 값의 목록을 사용할 수 있습니다. 지정된 필드에 나열된 값 중 하나를 포함하는 레코드는 검색 기준과 일치합니다.
- 모든 필드에 따옴표로 감싸고 쉼표로 구분한 목록을 검색 값으로 사용할 수 있습니다.
  - 단일 값만을 포함할 수 있는 필드의 경우, 따옴표 내에 지정된 정확한 문자열을 포함하는 지정된 필드의 레코드가 검색 기준과 일치합니다. 예를 들어 `A, B, "C, D, E"`에 대한 검색은 지정된 필드에 `"A"` 또는 `"B"` 또는 `"C, D, E"`가 포함된 레코드와 일치합니다. 따라서 가능한 값으로 쉼표를 포함하는 필드에서 일치를 확인할 수 있습니다.
  - 여러 값을 동시에 포함할 수 있는 필드의 경우, 따옴표로 감싸고 쉼표로 구분한 모든 값을 포함하는 지정된 필드의 레코드가 해당 검색 기준과 일치합니다.

  - 여러 값을 동시에 포함할 수 있는 필드의 경우, 검색 기준에 단일 값은 물론 따옴표로 감싸고 쉼표로 구분한 목록도 포함할 수 있습니다. 예를 들어 하나 이상의 이러한 문자를 포함할 수 있는 필드에서 `A, B, "C, D, E"`에 대한 검색은 지정된 필드에 `A` 또는 `B`, 또는 `C`, `D`, `E` 모두가 포함된 레코드와 일치합니다.

- 검색 결과에는 모든 필드에 지정된 검색 기준과 매칭되는 레코드만 반환됩니다.
- 많은 필드에서 와일드카드로 하나 이상의 별표(*)를 사용할 수 있습니다.
- 해당 필드에 대해 사용할 수 있는 정보가 없는 이벤트를 식별하려면 필드에 `n/a`를 지정합니다. 해당 필드가 채워지는 이벤트를 식별하려면 `!n/a`를 사용합니다.
- 검색 기준으로 객체를 사용하려면 검색 필드 옆에 나타나는 객체 추가 아이콘(+)을 클릭합니다.

검색에서 객체를 사용하는 방법을 포함하여 검색 구문에 대한 자세한 내용은 60-1페이지의 이벤트 검색을/를 참조하십시오.

4단계 선택적으로, 검색을 저장하려면 **Private** 확인란을 선택하여 자신만 액세스할 수 있는 비공개로 검색을 저장할 수 있습니다. 또는 모든 사용자가 사용할 수 있도록 검색을 저장하려면 확인란을 선택하지 않습니다.

팁 사용자 지정 사용자 역할에 대한 데이터 제한으로서 검색을 사용하려면 **반드시** 비공개 검색으로 저장해야 합니다.

5단계 선택적으로, 나중에 다시 사용할 수 있도록 검색을 저장할 수 있습니다. 다음 옵션을 이용할 수 있습니다.

- 검색 기준을 저장하려면 **Save**를 클릭합니다.

  새 검색인 경우 검색 이름을 입력하도록 대화 상자가 나타납니다. 고유한 검색 이름을 입력하고 **Save**를 클릭합니다. 이미 존재하는 검색에 대한 새 조건을 저장하는 경우 프롬프트가 나타나지 않습니다. 나중에 실행할 수 있도록 검색이 저장됩니다(**Private**을 선택한 경우 자신만 볼 수 있음).

- 새 검색을 저장하거나, 저장된 기존 검색을 변경하여 만든 검색에 새 이름을 할당하려면 **Save As New**를 클릭합니다.

  검색 이름을 입력하도록 대화 상자가 나타납니다. 고유한 검색 이름을 입력하고 **Save**를 클릭합니다. 나중에 실행할 수 있도록 검색이 저장됩니다(**Private**을 선택한 경우 자신만 볼 수 있음).

6단계 검색을 시작하려면 **Search**를 클릭합니다.

검색 결과는 현재의 시간 범위로 제한되어 기본 상관관계 이벤트 워크플로에 나타납니다. 사용자 지정 워크플로를 비롯한 다른 워크플로를 사용하려면 워크플로 제목 옆의 **(switch workflow)**를 클릭합니다. 다른 기본 워크플로 지정에 대한 자세한 내용은 71-3페이지의 이벤트 보기 설정 구성을/를 참조하십시오.

52장

규정준수 툴로 FireSIGHT 시스템 사용

규정준수 화이트리스트(또는 *화이트리스트*)는 특정 서브넷에서 실행할 수 있도록 허용된 운영 체제, 애플리케이션, 프로토콜을 지정할 수 있으며, 서브넷의 호스트가 화이트리스트를 위반할 경우 이벤트가 자동으로 생성되도록 할 수 있습니다. 예를 들어, 웹 서버는 HTTP를 실행할 수 있으나 네트워크의 다른 호스트는 그렇게 할 수 없도록 하는 보안 정책이 있는 경우를 가정해보겠습니다. 이 경우 웹 팜을 제외한 전체 네트워크를 평가하는 화이트리스트를 생성하여 어떤 호스트가 HTTP를 실행 중인지 확인할 수 있습니다.

다음과 같은 경우 트리거되는 상관관계 규칙을 구성하여, 이러한 기능을 수행하는 상관관계 규칙을 생성할 수 있습니다.

- 시스템이 애플리케이션 프로토콜에 대한 새로운 정보를 발견한 경우
- 애플리케이션 프로토콜 이름이 http인 경우
- 이벤트와 관련된 호스트의 IP 주소가 웹 팜에 없는 경우

그러나 상관관계 규칙은 네트워크의 정책 위반 사항을 알리고 이에 대응할 수 있는 보다 유연한 방법을 제공하지만, 화이트리스트보다 구성하고 유지하기가 더 복잡합니다. 또한 상관관계 규칙은 범위가 더 넓으므로, 다양한 유형의 이벤트 중 하나가 지정된 기준에 부합할 경우 상관관계 이벤트를 생성할 수 있습니다. 반면 화이트리스트는 네트워크에서 실행 중인 운영 체제, 애플리케이션 프로토콜, 클라이언트, 웹 애플리케이션, 프로토콜을 평가하고 조직의 정책을 위반하는지 평가하는 데 특히 유용합니다.

조직의 특정 요구 사항에 맞는 사용자 지정 화이트리스트를 만들거나, Cisco VRT(Vulnerability Research Team)에서 만든 기본 화이트리스트를 사용할 수 있으며 여기에는 허용되는 운영 체제, 애플리케이션 프로토콜, 클라이언트, 웹 애플리케이션, 프로토콜이 포함되어 있습니다. 네트워크 환경에 적합한 기본 화이트리스트를 맞춤화할 수도 있습니다.

활성화된 상관관계 정책에 화이트리스트를 추가하면 해당 화이트리스트를 위반하는 호스트가 탐지될 경우 시스템에서는 화이트리스트 이벤트(특수한 종류의 상관관계 이벤트)를 데이터베이스에 로깅합니다. 또한 화이트리스트 위반이 탐지될 경우 응답(위협 요소 제거 및 알림)이 트리거되도록 시스템을 구성할 수 있습니다.

참고 NetFlow 지원 디바이스에서 내보낸 데이터에 기반한 네트워크 맵에 호스트 및 애플리케이션 프로토콜을 추가하도록 하는 네트워크 검색 정책을 구성할 수는 있으나, 이러한 호스트 및 애플리케이션 프로토콜에 대해 제공되는 정보는 제한적입니다. 예를 들어, 호스트 입력 기능을 사용하여 제공하지 않는 한 이러한 호스트에 대해 사용할 수 있는 운영 체제 데이터가 없습니다. 이는 규정준수 화이트리스트를 작성하는 방법에 영향을 미칠 수 있습니다. 자세한 내용은 45-17페이지의 NetFlow 및 FireSIGHT 데이터 간 차이점을/를 참조하십시오.

시스템은 사용자가 생성한 모든 화이트리스트의 준수 여부를 나타내는 호스트 속성을 각 호스트에 생성하므로, 네트워크의 규정준수 상황을 한눈에 요약하여 파악할 수 있습니다. 조직 내의 어떤 호스트가 정책을 위반한 상태로 HTTP를 실행 중인지 단 몇 초 만에 정확히 확인하고, 적절한 조치를 취할 수 있습니다.

그런 다음 상관관계 기능을 사용하면 웹 팜에 없는 호스트가 HTTP 실행을 시작할 때마다 사용자에게 알림이 전송되도록 시스템을 구성할 수 있습니다.

또한 호스트 프로필을 사용하면 개별 호스트가 사용자가 구성한 화이트리스트를 위반하는지, 그리고 어떤 경위로 화이트리스트를 위반하는지 확인할 수 있습니다. FireSIGHT 시스템에는 각각의 개별 화이트리스트 위반 사항 및 호스트당 위반 횟수를 볼 수 있는 워크플로도 포함되어 있습니다.

마지막으로, 대시보드를 사용하여 최근 시스템 전반의 규정준수 작업을 모니터링할 수 있으며 여기에는 네트워크의 전반적인 화이트리스트 규정준수에 대한 이벤트 및 요약 보기가 포함됩니다.

규정준수 화이트리스트를 생성 및 관리하고, 화이트리스트 이벤트 및 위반을 해석하는 방법에 대한 자세한 내용은 다음 절을 참조하십시오.

- 52-2페이지의 규정준수 화이트리스트 이해
- 52-8페이지의 규정준수 화이트리스트 생성
- 52-23페이지의 규정준수 화이트리스트 관리
- 52-25페이지의 공유 호스트 프로필 작업
- 52-30페이지의 화이트리스트 이벤트 작업
- 52-35페이지의 화이트리스트 위반 작업

자세한 내용은 다음 장 및 절을 참조하십시오.

- 51-45페이지의 상관관계 정책 생성에서는 규정준수 화이트리스트가 포함된 상관관계 정책을 생성 및 구성하는 방법에 대해 설명하고, 응답 및 우선순위를 화이트리스트에 할당하는 방법을 설명합니다.
- 49-1페이지의 호스트 프로필 사용에서는 호스트의 프로필을 사용하여 호스트가 화이트리스트를 위반하는지 여부를 확인하는 방법에 대해 설명합니다.
- 55-1페이지의 대시보드 사용에서는 화이트리스트 규정준수 작업을 비롯하여 현재 시스템 상태를 한눈에 볼 수 있는 보기를 참조하는 방법을 설명합니다.

규정준수 화이트리스트 이해

라이센스: FireSIGHT

*규정준수 화이트리스트*는 네트워크에서 실행할 수 있도록 허용된 운영 체제, 클라이언트, 애플리케이션 프로토콜, 웹 애플리케이션, 프로토콜을 지정하는 기준의 집합입니다. 특정 요구 사항에 맞는 사용자 지정 화이트리스트를 만들거나, VRT에서 만든 권장 설정이 포함된 기본 화이트리스트를 사용할 수 있습니다.

사용자 지정 화이트리스트의 기준은 간단하게 설정할 수 있습니다. 즉, 특정 운영 체제를 실행하는 호스트만 허용하도록 할 수 있습니다. 기준을 복잡하게 설정하는 것도 가능합니다. 모든 운영 체제를 허용하되, 특정 운영 체제를 실행하는 호스트만 특정 포트에서 특정 애플리케이션 프로토콜을 실행하도록 지정할 수 있습니다.

화이트리스트는 *대상* 및 *호스트 프로필*이라는 두 가지 부분으로 구성됩니다. 대상은 화이트리스트에서 평가된 특정 호스트이며, 호스트 프로필은 대상에서 실행할 수 있도록 허용된 운영 체제, 클라이언트, 애플리케이션 프로토콜, 웹 애플리케이션, 프로토콜입니다.

화이트리스트를 생성한 후 이를 활성화된 상관관계 정책에 추가하면, 시스템에서는 화이트리스트의 대상을 호스트 프로필과 비교 평가하여 해당 대상이 화이트리스트를 준수하는지 확인합니다. 이러한 최초 평가 후, 유효 대상이 화이트리스트를 위반하는 것으로 탐지될 경우 *화이트리스트 이벤트*가 생성됩니다.

자세한 내용은 다음 절을 참조하십시오.

- 52-3페이지의 화이트리스트 대상 이해에서는 화이트리스트가 어떤 방식을 통해 사용자가 지정한 호스트만 대상으로 지정하는지 설명합니다.
- 52-4페이지의 화이트리스트 호스트 프로필 이해에서는 네트워크에서 실행할 수 있도록 허용된 클라이언트, 애플리케이션 프로토콜, 웹 애플리케이션, 프로토콜을 설명하는 다양한 종류의 프로필에 대해 설명합니다.
- 52-6페이지의 화이트리스트 평가 이해에서는 네트워크의 호스트를 화이트리스트와 비교 평가하는 방법에 대해 설명하고, 어떤 호스트가 규정을 준수하고 어떤 호스트가 위반하는지 확인할 수 있는 방법을 설명합니다.
- 52-6페이지의 화이트리스트 위반 이해에서는 시스템이 어떤 방식으로 화이트리스트 위반을 탐지하고 이에 대한 알림을 제공하는지 설명합니다.

화이트리스트 대상 이해

라이센스: FireSIGHT

화이트리스트를 생성할 경우, 우선 이를 적용할 네트워크의 부분을 지정해야 합니다. 화이트리스트를 사용하여 모니터링되는 네트워크의 모든 호스트를 평가할 수 있으며, 화이트리스트를 제한하여 특정 네트워크 세그먼트만 평가하거나 개별 호스트까지도 평가할 수 있습니다. 화이트리스트를 추가로 제한하여 특정 호스트 속성을 보유하거나 특정 VLAN에 속한 호스트만 평가할 수 있습니다. 화이트리스트로 평가하기에 적합한 호스트를 *유효 대상*(또는 *대상*)이라고 합니다. 유효 대상은 다음과 같습니다.

- 사용자가 지정한 IP 주소 블록 중 하나에 속해야 합니다. IP 주소 블록을 제외할 수도 있습니다.
- 사용자가 지정한 호스트 속성 중 하나 이상을 보유해야 합니다.

  예를 들어, 호스트 중요도가 높은 호스트만 평가하도록 화이트리스트를 구성할 수 있습니다. 호스트 중요도를 비롯하여 호스트 속성에 대한 자세한 내용은 49-31페이지의 사용자 정의 호스트 특성 작업 및 49-30페이지의 사전 정의 호스트 특성 작업을/를 참조하십시오.
- 사용자가 지정한 VLAN 중 하나에 속해야 합니다.

호스트가 이러한 모든 기준에 부합하지 않을 경우, 호스트 프로필이 화이트리스트를 위반하는지 여부에 상관없이 해당 호스트는 화이트리스트와 비교 평가됩니다.

화이트리스트에 여러 개의 대상이 포함된 경우, 호스트는 유효한 것으로 간주되려면 여러 대상 중 하나에만 지정된 기준을 충족해야 합니다. 예를 들어, 10.10.x.x 네트워크가 포함된 대상 및 10.10.x.x 네트워크가 제외된 대상을 생성할 경우 해당 네트워크의 호스트는 유효 대상으로 간주됩니다. 화이트리스트에 대상이 포함되지 않은 경우, 네트워크의 호스트는 화이트리스트와 비교 평가되지 않습니다.

화이트리스트에 대한 대상 네트워크는 Create White List 페이지의 왼쪽에 나열됩니다. 기본 화이트리스트에서는 0.0.0.0/0 및 ::/0으로 된 대상을 사용하며, 이는 전체 모니터링되는 네트워크를 나타냅니다. 이 화이트리스트를 사용하도록 선택할 경우 대상 네트워크를 있는 그대로 유지하거나, 해당 네트워크 환경을 반영하도록 수정할 수 있습니다.

화이트리스트 대상 생성에 대한 자세한 내용은 52-11페이지의 규정준수 화이트리스트 대상 구성을/를 참조하십시오.

화이트리스트 호스트 프로필 이해

라이센스: FireSIGHT

화이트리스트에서 평가할 대상을 지정한 이후의 다음 단계는 *호스트 프로필*을 구성하는 것입니다. 화이트리스트의 호스트 프로필은 대상 호스트에서 실행할 수 있는 운영 체제, 클라이언트, 애플리케이션 프로토콜, 웹 애플리케이션, 프로토콜을 지정합니다.

화이트리스트에서는 전역 호스트 프로필, 특정 운영 체제에 대한 호스트 프로필, 공유 호스트 프로필이라는 세 가지 종류의 호스트 프로필을 구성할 수 있습니다. 각 호스트 프로필의 유형은 화이트리스트를 생성할 때 서로 다르게 표시됩니다.

다음 표에서는 각기 다른 종류의 호스트 프로필을 식별하고 액세스하는 방법에 대해 설명합니다.

표 52-1 규정준수 화이트리스트 호스트 프로필 액세스

보려는 내용	Allowed Host Profiles 아래에서 클릭할 항목
화이트리스트에 대한 전역 호스트 프로필	**모든 운영 체제**
특정 운영 체제에 대한 호스트 프로필	기울임꼴이 아닌 일반 텍스트로 나열된 호스트 프로필 이름
화이트리스트에 사용된 공유 호스트 프로필	기울임꼴로 나열된 호스트 프로필 이름

자세한 내용은 다음 절을 참조하십시오.

- 52-4페이지의 전역 호스트 프로필 이해
- 52-4페이지의 특정 운영 체제에 대한 호스트 프로필 이해
- 52-5페이지의 공유 호스트 프로필 이해

전역 호스트 프로필 이해

라이센스: FireSIGHT

호스트의 운영 체제에 상관없이, 모든 화이트리스트에는 대상 호스트에서 실행할 수 있도록 허용된 애플리케이션 프로토콜, 클라이언트, 웹 애플리케이션, 프로토콜을 지정하는 전역 호스트 프로필이 포함되어 있습니다.

예를 들어, 여러 개의 Microsoft Windows 및 Linux 호스트 프로필을 수정하는 대신 Internet Explorer를 허용하려면 탐지를 수행하는 운영 체제에 상관없이 Internet Explorer를 허용하도록 전역 호스트 프로필을 구성할 수 있습니다. ARP, IP, TCP, UDP 프로토콜은 항상 모든 호스트에서 허용되며 해당 프로토콜은 허용하지 않을 수 없습니다. 자세한 내용은 52-14페이지의 전역 호스트 프로필 구성을/를 참조하십시오.

특정 운영 체제에 대한 호스트 프로필 이해

라이센스: FireSIGHT

네트워크에서 허용하려는 각 운영 체제에 대한 하나의 호스트 프로필을 생성해야 합니다. 네트워크에서 특정 운영 체제를 허용하지 않으려면, 해당 운영 체제에 대한 호스트 프로필을 생성하지 마십시오. 예를 들어, 네트워크의 모든 호스트가 Microsoft Windows를 실행하도록 하려면, 화이트리스트에 해당 운영 체제에 대한 호스트 프로필만 포함되도록 구성하십시오.

특정 운영 체제에 대한 호스트 프로필을 생성할 경우, 특정 버전을 충족하도록 요청할 수도 있습니다. 예를 들어, 규격 호스트가 Windows 7 또는 Server 2008 R2를 실행하도록 요청할 수 있습니다.

특정 운영 체제에 대한 호스트 프로필을 생성한 후에는 해당 운영 체제를 실행하는 대상 호스트에서 실행하도록 허용되는 애플리케이션 프로토콜, 클라이언트, 웹 애플리케이션, 프로토콜을 지정할 수 있습니다. 예를 들어, SSH를 Linux 호스트의 포트 22에서 실행하도록 허용할 수 있습니다. 또한 특정 공급업체 및 버전을 OpenSSH 4.2로 제한할 수도 있습니다.

확인되지 않은 호스트는 확인될 때까지 모든 화이트리스트를 준수하는 상태로 유지됩니다. 그러나 알 수 없는 호스트에 대한 화이트리스트 호스트 프로필을 생성할 수 있습니다.

참고 확인되지 않은 호스트는 알 수 없는 호스트와 동일하지 않습니다. *Unidentified* 호스트는 시스템이 해당 호스트의 운영 체제를 식별하기 위한 충분한 정보를 아직 수집하지 못한 호스트입니다. *Unknown* 호스트는 시스템에서 트래픽을 분석했으나, 운영 체제가 모든 알려진 핑거프린트와 일치하지 않는 호스트입니다.

자세한 내용은 52-15페이지의 특정 운영 체제에 대한 호스트 프로필 생성을/를 참조하십시오.

공유 호스트 프로필 이해

라이센스: FireSIGHT

공유 호스트 프로필은 특정 운영 체제에 연결되지만, 각 공유 호스트 프로필을 여러 개의 화이트리스트에서 사용할 수 있습니다. 즉, 여러 개의 화이트리스트를 생성하지만 동일한 호스트 프로필을 사용하여 화이트리스트 전반에 걸쳐 특정 운영 체제를 실행하는 호스트를 평가하려는 경우, 공유 호스트 프로필을 사용합니다.

예를 들어, 전 세계에 지사가 있고 각 위치에 대한 별도의 화이트리스트를 생성하고자 하지만 Apple Mac OS X를 실행하는 모든 호스트에 동일한 프로필을 항상 사용하려는 경우, 해당 운영 체제에 대한 공유 프로필을 생성하고 이를 모든 화이트리스트에 사용할 수 있습니다.

기본 화이트리스트에서는 허용되는 운영 체제, 클라이언트, 애플리케이션 프로토콜, 웹 애플리케이션, 프로토콜에 권장되는 "모범 사례" 설정을 제시합니다. 이러한 화이트리스트는 *내장형 호스트 프로필*이라고 하는 특수 카테고리의 공유 호스트 프로필을 사용합니다. 내장형 호스트 프로필은 내장형 호스트 프로필 아이콘( )으로 표시됩니다.

내장형 호스트 프로필은 내장형 애플리케이션 프로토콜, 프로토콜, 클라이언트를 사용합니다. 이러한 요소는 기본 화이트리스트 및 사용자가 생성한 사용자 지정 화이트리스트에서 모두 있는 그대로 사용하거나, 요구 사항에 맞게 수정할 수 있습니다. 해당 요소는 내장형 호스트 프로필 및 이 요소를 사용하는 모든 기타 호스트 프로필 내에 기울임꼴로 표시됩니다.

모든 공유 호스트 프로필과 마찬가지로, 내장형 호스트 프로필을 수정할 경우 이를 사용하는 모든 화이트리스트에 영향을 미칩니다. 또한 내장형 애플리케이션 프로토콜, 프로토콜 또는 클라이언트를 수정할 경우에도 이를 사용하는 모든 화이트리스트에 영향을 미칩니다.

공유 호스트 프로필에 대한 자세한 내용은 52-25페이지의 공유 호스트 프로필 작업을/를 참조하십시오.

화이트리스트 평가 이해

라이센스: FireSIGHT

화이트리스트 호스트 프로필을 생성하고 화이트리스트를 저장한 후에는, 상관관계 규칙에 수행했던 것과 마찬가지로 화이트리스트를 상관관계 정책에 추가할 수 있습니다. 자세한 내용은 51-1페이지의 상관관계 정책 및 규칙 구성을/를 참조하십시오.

상관관계 정책을 활성화하면 시스템에서는 화이트리스트의 대상을 화이트리스트 기준과 비교 평가합니다. 그런 다음 호스트 속성 네트워크 맵을 사용하여 네트워크에 있는 호스트의 화이트리스트 규정준수에 대한 전반적인 보기를 얻을 수 있습니다.

네트워크의 각 호스트에는 화이트리스트와 이름이 같은 호스트 속성이 할당됩니다. 이러한 호스트 속성에는 다음 값 중 하나가 포함됩니다.

- **Compliant** - 화이트리스트를 준수하는 유효 대상
- **Non-Compliant** - 화이트리스트에 위반되는 유효 대상
- **Not Evaluated** - 어떠한 사유로 인해 아직 평가되지 않은 비유효 대상 및 호스트

네트워크가 대규모이고 시스템이 네트워크 맵의 모든 유효 대상을 화이트리스트와 비교 평가하는 프로세스를 진행 중일 경우, 아직 평가되지 않은 대상은 `Not Evaluated`로 표시됩니다. 시스템이 프로세스를 완료하면, 더 많은 호스트가 `Not Evaluated`에서 `Compliant` 또는 `Non-Compliant`로 이동합니다. 시스템은 초당 약 100개의 호스트를 평가할 수 있습니다.

또한 호스트의 화이트리스트 준수 여부를 확인할 수 있는 충분한 정보가 시스템에 없을 경우에도 호스트가 `Not Evaluated`로 표시됩니다. 예를 들어, 시스템이 새 호스트를 탐지했으나 호스트에서 실행 중인 운영 체제, 클라이언트, 애플리케이션 프로토콜, 웹 애플리케이션, 프로토콜과 관련된 정보를 아직 수집하지 못한 경우 이러한 현상이 발생할 수 있습니다.

참고 호스트에서 호스트 속성을 변경하거나 삭제한 후 이러한 변경이나 삭제로 인해 해당 호스트가 더 이상 유효 대상이 아닐 경우, 호스트가 `Compliant` 또는 `Non-Compliant`에서 `Not Evaluated`로 변경됩니다.

호스트 특성에 대한 자세한 내용은 48-9페이지의 호스트 특성 네트워크 맵 작업을/를 참조하십시오.

화이트리스트 위반 이해

라이센스: FireSIGHT

이러한 최초 화이트리스트 평가 후, 유효 대상이 화이트리스트를 위반하는 것으로 탐지될 경우 *화이트리스트 이벤트*가 생성됩니다. 화이트리스트는 특수한 종류의 상관관계 이벤트이며, 방어 센터 상관관계 이벤트 데이터베이스에 로깅됩니다. 화이트리스트 이벤트를 워크플로에서 보거나, 특정 화이트리스트 이벤트를 검색할 수 있습니다. 자세한 내용은 52-30페이지의 화이트리스트 이벤트 작업을/를 참조하십시오.

화이트리스트 위반은 규정준수에 어긋나는 호스트를 나타내는 이벤트가 생성될 때 발생합니다. 이와 유사하게, 검색 이벤트는 이전에 규정준수를 위반했던 호스트가 현재는 규정준수에 부합한다는 것을 나타낼 수 있으며, 이러한 상황이 발생했을 때 시스템이 화이트리스트를 생성하지 **않는** 경우에도 마찬가지입니다.

다음 이벤트는 호스트의 규정준수 여부를 변경할 수 있습니다.

- 시스템이 호스트의 운영 체제의 변경 사항을 탐지한 경우
- 시스템에 호스트의 운영 체제 또는 호스트에 있는 애플리케이션 프로토콜의 ID 충돌을 탐지한 경우

- 시스템이 호스트에서 새 TCP 서버 포트(예: SMTP 또는 웹 서버에서 사용된 포트)가 활성화되었거나, 호스트에서 새 UDP 서버가 실행 중인 것을 탐지한 경우
- 시스템이 호스트에서 실행 중인 것으로 검색된 TCP 또는 UDP 서버의 변경 사항을 탐지한 경우(예: 업그레이드로 인한 버전 변경)
- 시스템이 호스트에서 새 클라이언트가 실행 중인 것을 탐지한 경우
- 시스템이 비활성 상태로 인해 데이터베이스에서 클라이언트를 삭제한 경우
- 시스템이 호스트에서 새 웹 클라이언트가 실행 중인 것을 탐지한 경우
- 시스템이 비활성 상태로 인해 호스트 프로필에서 웹 애플리케이션을 삭제한 경우
- 시스템이 호스트가 새 네트워크 프로토콜(예: Novell Netware 또는 IPv6)이나 새 전송 프로토콜(예: ICMP 또는 EGP)과 통신을 수행하는 것을 탐지한 경우
- 시스템이 탈옥한 새 모바일 디바이스를 탐지한 경우
- 시스템이 시스템에서 종료되거나 시간 초과된 TCP 또는 UDP 포트를 탐지한 경우

이와 더불어, 호스트 입력 기능 또는 호스트 프로필을 사용하여 호스트의 규정준수 변경을 트리거할 수 있습니다.

- 호스트에 클라이언트, 프로토콜 또는 서버 추가
- 호스트에서 클라이언트, 프로토콜 또는 서버 삭제
- 호스트의 운영 체제 정의 설정
- 해당 호스트가 더 이상 유효 대상이 되지 않도록 호스트의 호스트 특성 변경

예를 들어, 네트워크에서 Microsoft Windows만 허용하도록 화이트리스트를 지정할 경우, 시스템에서는 호스트가 현재 Mac OS X를 실행하고 있음을 탐지하며 화이트리스트 이벤트를 생성합니다. 또한 화이트리스트 속성과 연결된 호스트 속성의 값이 해당 호스트에 대해 `Compliant`에서 `Non-Compliant`로 변경됩니다.

이 예시에 나온 호스트의 상태가 규정준수로 돌아가려면 다음 중 하나를 수행해야 합니다.

- Mac OS X 운영 체제를 허용하도록 화이트리스트 수정
- 대한 호스트의 운영 체제 정의를 Microsoft Windows로 수동으로 변경
- 운영 체제가 Microsoft Windows로 다시 변경된 사실을 시스템에서 탐지함

모든 경우, 화이트리스트 속성과 연결된 호스트 속성의 값은 해당 호스트에 대해 `Non-Compliant`에서 `Compliant`로 변경됩니다.

또 다른 예를 들자면, 규정준수 화이트리스트에서 FTP 사용이 허용되지 않고 사용자가 애플리케이션 프로토콜 네트워크 맵 또는 이벤트 보기에서 FTP를 삭제할 경우, FTP를 실행하는 호스트는 규정준수를 위반하게 됩니다. 그러나 애플리케이션 프로토콜이 다시 탐지될 경우, 시스템에서는 화이트리스트 이벤트를 생성하며 호스트는 규정준수 위반 상태가 됩니다.

시스템이 화이트리스트에 대해 충분하지 않은 정보가 포함된 이벤트를 생성할 경우, 화이트리스트가 트리거되지 않습니다. 예를 들어, 포트 21에서 TCP FTP 트래픽만 허용하는 화이트리스트를 허용하는 시나리오를 가정해보겠습니다. 이 경우 TCP 프로토콜을 사용하는 포트 21이 화이트리스트 대상 중 하나에서 활성화된 것으로 탐지되지만, 시스템에서는 해당 트래픽이 FTP인지 확인할 수 없습니다. 이 시나리오에서는 시스템이 트래픽을 FTP 트래픽이 아닌 다른 것으로 식별할 때까지, 또는 호스트 입력 기능을 사용하여 트래픽을 비 FTP 트래픽으로 식별할 때까지 화이트리스트가 트리거되지 않습니다.

참고 화이트리스트의 초기 평가 동안, 시스템은 규정준수를 위반한 호스트에 대한 화이트리스트를 생성하지 **않습니다**. 규정준수를 위반한 모든 대상에 대한 화이트리스트 이벤트를 생성하려면 방어 센터 데이터베이스를 삭제해야 합니다. 이렇게 하면 네트워크의 호스트 및 관련 클라이언트, 애플리케이션 프로토콜, 웹 애플리케이션, 프로토콜이 다시 검색되며 이로 인해 화이트리스트 이벤트가 트리거될 수 있습니다. 자세한 내용은 B-1페이지의 데이터베이스에서 검색 데이터 삭제을/를 참조하십시오.

마지막으로, 화이트리스트 위반이 탐지될 경우 응답이 트리거되도록 시스템을 구성할 수 있습니다. 응답에는 위협 요소 제거(예: Nmap 검사 실행), 알림(이메일, SNMP, syslog 알림) 또는 알림 및 위협 요소 제거를 조합한 형태가 포함될 수 있습니다. 자세한 내용은 51-48페이지의 규칙 및 화이트리스트에 응답 추가을/를 참조하십시오.

규정준수 화이트리스트 생성

라이센스: FireSIGHT

화이트리스트를 생성할 경우, 전체 네트워크 또는 특정 네트워크 세그먼트를 조사할 수 있습니다. 네트워크를 조사하면 네트워크 세그먼트에서 탐지된 각 운영 체제의 호스트 프로필로 화이트리스트가 채워집니다. 기본적으로 이러한 호스트 프로필은 해당 운영 체제에서 탐지된 모든 클라이언트, 애플리케이션 프로토콜, 웹 애플리케이션, 프로토콜을 허용합니다.

그런 다음에는 화이트리스트의 대상을 지정해야 합니다. 화이트리스트를 구성하여 모니터링되는 네트워크의 모든 호스트를 평가할 수 있으며, 화이트리스트를 제한하여 특정 네트워크 세그먼트만 평가하거나 개별 호스트까지도 평가할 수 있습니다. 화이트리스트를 추가로 제한하여 특정 호스트 속성을 보유하거나 특정 VLAN에 속한 호스트만 평가할 수 있습니다. 네트워크를 조사하면, 조사한 네트워크 세그먼트에서 화이트리스트 대상을 기본적으로 나타냅니다. 조사한 네트워크를 수정 또는 삭제하거나, 새 대상을 추가할 수 있습니다.

다음 단계는 규정준수 호스트를 나타내는 호스트 프로필을 생성하는 것입니다. 화이트리스트의 호스트 프로필은 대상 호스트에서 실행할 수 있는 운영 체제, 클라이언트, 애플리케이션 프로토콜, 웹 애플리케이션, 프로토콜을 지정합니다. 전역 호스트 프로필을 구성하고, 모든 네트워크 조사에서 생성된 호스트 프로필을 수정하는 것은 물론 새 호스트 프로필을 추가하고, 공유 호스트 프로필을 추가 및 수정할 수 있습니다.

마지막으로, 화이트리스트를 저장하고 이를 활성화된 상관관계 정책에 추가합니다. 시스템은 대상 호스트의 규정준수 여부를 평가하고, 호스트가 화이트리스트를 위반할 경우 화이트리스트를 생성하며, 화이트리스트 위반에 대해 구성된 응답을 트리거합니다. 규정준수 화이트리스트에 대한 자세한 개요는 52-2페이지의 규정준수 화이트리스트 이해을/를 참조하십시오.

팁 호스트의 테이블 보기에서 화이트리스트를 생성할 수도 있습니다. 자세한 내용은 50-24페이지의 선택한 호스트를 기반으로 규정준수 화이트리스트 생성을/를 참조하십시오.

규정준수 화이트리스트를 생성하려면

액세스: Admin

1단계 **Policies > Correlation**을 선택한 다음 **White List**를 클릭합니다.

White List 페이지가 나타납니다.

2단계 **New White List**를 클릭합니다.

Survey Network 페이지가 나타납니다.

3단계 선택에 따라, 네트워크를 조사합니다.

- 네트워크를 조사하려면 52-9페이지의 네트워크 조사을/를 참조하십시오.
- 네트워크 조사 없이 화이트리스트를 생성하려면, **Skip**을 클릭하고 다음 단계를 계속하십시오.

Create White List 페이지가 나타납니다.

4단계 **Name** 필드에 새 화이트리스트의 이름을 입력합니다.

5단계 **Description** 필드에 화이트리스트의 짧은 설명을 입력합니다.

6단계 탈옥한 디바이스를 네트워크에서 허용하려면 **Allow Jailbroken Mobile Devices**를 활성화합니다. 모든 탈옥한 디바이스를 화이트리스트로 평가하여 화이트리스트 위반을 생성하려면 이 옵션을 비활성화합니다.

7단계 화이트리스트의 대상을 지정합니다. 네트워크 조사에서 생성된 대상을 수정하거나 삭제하고 새 타겟을 추가할 수도 있습니다. 선택에 따라, 호스트 속성 또는 VLAN ID를 기준으로 대상을 추가로 제한할 수 있습니다. 자세한 내용은 52-11페이지의 규정준수 화이트리스트 대상 구성을/를 참조하십시오.

8단계 규정준수 호스트를 나타내는 호스트 프로필을 생성합니다. 전역 호스트 프로필을 구성하고, 모든 네트워크 조사에서 생성된 호스트 프로필을 수정하는 것은 물론 새 호스트 프로필을 추가하고, 공유 호스트 프로필을 추가 및 수정할 수 있습니다. 자세한 내용은 52-13페이지의 규정준수 화이트리스트 호스트 프로필 구성을/를 참조하십시오.

9단계 **Save White List**를 클릭하여 화이트리스트를 저장합니다.

화이트리스트가 저장됩니다. 이제 이를 활성화된 상관관계 정책에 추가하여 대상 호스트의 규정준수 여부를 평가하고, 호스트가 화이트리스트를 위반한 경우 화이트리스트 이벤트를 생성하며, 선택에 따라 화이트리스트 위반에 대한 응답을 트리거할 수 있습니다. 자세한 내용은 51-45페이지의 상관관계 정책 생성을/를 참조하십시오.

네트워크 조사

라이센스: FireSIGHT

규정준수 화이트리스트 생성을 시작할 경우, 전체 네트워크 또는 특정 네트워크 세그먼트를 조사할 수 있습니다.

네트워크를 조사하면 탐지된 여러 운영 체제에서 실행 중인 애플리케이션 프로토콜, 클라이언트, 웹 애플리케이션, 프로토콜에 대한 데이터가 데이터베이스에서 수집됩니다. 그런 다음, 시스템은 탐지된 각 운영 체제의 화이트리스트 내에서 호스트 프로필을 생성합니다. 기본적으로 이러한 호스트 프로필은 각 해당 운영 체제에서 탐지된 모든 클라이언트, 애플리케이션 프로토콜, 웹 애플리케이션, 프로토콜을 허용합니다.

이렇게 하면 기본 화이트리스트가 생성되므로 여러 호스트 프로필을 수동으로 생성하거나 구성할 필요가 없습니다. 네트워크를 조사한 후에는, 조사를 통해 요구 사항에 맞게 생성된 호스트 프로필을 수정하거나 삭제할 수 있습니다. 또한 필요할 가능성이 있는 다른 호스트 프로필을 추가할 수도 있습니다.

화이트리스트 생성 프로세스 동안 언제든지 네트워크를 조사할 수 있습니다. 이렇게 하면 허용된 추가 클라이언트, 애플리케이션 프로토콜, 웹 애플리케이션, 프로토콜을 기존의 호스트 프로필에 추가할 수 있으며, 처음 조사 과정에서 탐지되지 않은 운영 체제를 실행 중인 호스트가 조사에서 탐지될 경우 추가 호스트 프로필을 추가할 수 있습니다. 활성화된 상관관계 정책에서 사용된 화이트리스트 내의 네트워크를 다시 조사하고 이러한 조사로 인해 대상 또는 호스트 프로필이 변경된 경우, 화이트리스트를 저장하면 대상 호스트가 재평가됩니다. 이러한 재평가로 인해 일부 호스트의 상태가 규정준수로 바뀔 수 있으나, 화이트리스트 이벤트는 생성되지 않습니다.

네트워크를 조사하여 규정준수 화이트리스트를 생성하려면

액세스: Admin

1단계 **Policies > Correlation**을 선택한 다음 **White List**를 클릭합니다.

White List 페이지가 나타납니다.

2단계 **New White List**를 클릭합니다.

Survey Network 페이지가 나타납니다.

3단계 네트워크를 조사하시겠습니까?

- **yes**인 경우 다음 단계를 계속합니다.
- **no**인 경우 **Skip**을 클릭합니다.

  Create White List 페이지가 나타나고 빈 화이트리스트가 표시됩니다. 다음 절, 기본적인 화이트리스트 정보 제공에서 절차를 계속 진행합니다.

4단계 **IP Address** 및 **Netmask** 필드에 조사할 호스트를 나타내는 IP 주소와 네트워크 마스크(CIDR 같은 특수 표기법 형식)를 입력합니다.

시스템이 모니터링을 수행하도록 구성한 네트워크를 네트워크 검색 정책에서 지정해야 합니다. FireSIGHT 시스템에서 IP 주소 표기법을 사용하는 방법에 대한 자세한 내용은 1-19페이지의 IP 주소 표기 규칙을/를 참조하십시오.

팁 전체 모니터링된 네트워크를 조사하려면, 기본값 `0.0.0.0/0` 및 `::/0`을 사용합니다.

5단계 **OK**를 클릭합니다.

Create White List 페이지가 나타납니다.

화이트리스트는 미리 채워져 있는 상태이며, 화이트리스트의 대상은 조사한 네트워크에 있는 호스트이며, 허용된 호스트 프로필은 이러한 대상의 프로필입니다.

6단계 추가 네트워크를 조사하려면 **Target Network**를 클릭하고 조사할 각 네트워크에 4~5단계를 반복합니다.

추가 네트워크를 조사하면 허용된 추가 클라이언트, 애플리케이션 프로토콜, 웹 애플리케이션, 프로토콜을 기존의 호스트 프로필에 추가할 수 있으며, 처음 조사 과정에서 탐지되지 않은 운영 체제를 실행 중인 호스트가 조사에서 탐지될 경우 추가 호스트 프로필을 추가할 수 있습니다. 또한 추가 네트워크를 조사하면 조사한 네트워크 세그먼트의 호스트를 나타내는 화이트리스트가 타겟에 추가됩니다. 그런 다음 이러한 대상을 수정하거나 삭제할 수 있습니다.

7단계 다음 섹션, 기본적인 화이트리스트 정보 제공에서 계속합니다.

기본적인 화이트리스트 정보 제공

라이센스: FireSIGHT

각 화이트리스트에 이름을 제공해야 하며 선택에 따라 짧은 설명을 입력합니다. 이와 더불어, 탈옥한 모바일 디바이스가 있을 경우 화이트리스트 위반이 발생하도록 할지 선택할 수 있습니다.

기본적인 화이트리스트 정보를 제공하려면

액세스: Admin

1단계 **Name** 필드에 새 화이트리스트의 이름을 입력합니다.

2단계 **Description** 필드에 화이트리스트의 짧은 설명을 입력합니다.

3단계 탈옥한 디바이스를 네트워크에서 허용하려면 **Allow Jailbroken Mobile Devices**를 활성화합니다. 모든 탈옥한 디바이스를 화이트리스트로 평가하여 화이트리스트 위반을 생성하려면 이 옵션을 비활성화합니다.

4단계 다음 섹션, 규정준수 화이트리스트 대상 구성에서 계속합니다.

규정준수 화이트리스트 대상 구성

라이센스: FireSIGHT

규정준수 화이트리스트를 생성할 경우, 이를 적용할 네트워크의 부분을 지정해야 합니다. 화이트리스트를 사용하여 모니터링되는 네트워크의 모든 호스트를 평가할 수 있으며, 화이트리스트를 제한하여 특정 네트워크 세그먼트만 평가하거나 개별 호스트까지도 평가할 수 있습니다. 화이트리스트를 추가로 제한하여 특정 호스트 속성을 보유하거나 특정 VLAN에 속한 호스트만 평가할 수 있습니다. 화이트리스트로 평가하기에 적합한 호스트를 *대상*이라고 합니다. 화이트리스트에 대한 자세한 개요는 52-3페이지의 화이트리스트 대상 이해을/를 참조하십시오.

규정준수 화이트리스트의 대상을 생성하는 과정이 완료되면 52-13페이지의 규정준수 화이트리스트 호스트 프로필 구성을/를 계속합니다.

참고 호스트에서 호스트 속성을 변경하거나 삭제한 후 이러한 수정으로 인해 호스트가 더 이상 유효 대상이 아닐 경우, 해당 호스트는 화이트리스트로 평가되지 않으며 Compliant 또는 Non-Compliant로 간주되지 않습니다.

대상을 수정하거나 삭제하는 방법에 대한 자세한 내용은 다음을 참조하십시오.

- 52-13페이지의 기존 대상 수정
- 52-13페이지의 기존 대상 삭제

규정준수 화이트리스트의 대상을 생성할 경우, 화이트리스트와 비교 평가할 때 호스트가 충족해야 하는 기준을 지정합니다. 유효 대상은 다음과 같습니다.

- 사용자가 지정한 IP 주소 블록 중 하나에 속해야 합니다. IP 주소 블록을 제외할 수도 있습니다.
- 사용자가 지정한 호스트 속성 중 하나 이상을 보유해야 합니다.
- 사용자가 지정한 VLAN 중 하나에 속해야 합니다.

활성화된 상관관계 정책에서 사용되는 화이트리스트에 대상을 추가할 경우, 화이트리스트를 저장하면 새로운 대상 호스트의 규정준수 여부가 평가됩니다. 그러나 이러한 평가로 인해 화이트리스트 이벤트가 생성되지는 않습니다.

규정준수 화이트리스트 대상을 생성하려면

액세스: Admin

1단계 Create White List 페이지에서 **Target Networks** 옆의 추가 아이콘( )을 클릭합니다.

새 대상에 대한 설정이 나타납니다.

팁 네트워크 세그먼트를 조사하여 새 대상을 생성할 수도 있습니다. Create White List 페이지에서 **Target Network**를 클릭한 다음 52-9페이지의 네트워크 조사의 4단계 및 5단계를 수행합니다. 새 대상이 생성되며 지정된 IP 주소에 따라 이름이 설정됩니다. 방금 생성한 대상을 클릭하고 이 절차의 나머지 부분을 계속하여 대상의 이름을 변경하고, 추가 네트워크를 추가 또는 제외하며, 호스트 특성 또는 VLAN 제한 사항을 추가합니다.

2단계 **Name** 필드에 새 대상의 이름을 입력합니다.

3단계 **Targeted Networks** 옆의 추가 아이콘( )을 클릭하여 특정 IP 주소 집합을 대상으로 지정합니다.

4단계 **IP Address** 및 **Netmask** 필드에 대상 지정 과정에서 대상으로 지정하거나 제외할 호스트를 나타내는 IP 주소와 네트워크 마스크(CIDR 같은 특수 표기법 형식)를 입력합니다.

시스템이 모니터링을 수행하도록 구성한 네트워크를 네트워크 검색 정책에서 지정해야 합니다. FireSIGHT 시스템에서 IP 주소 표기법을 사용하는 방법에 대한 자세한 내용은 1-19페이지의 IP 주소 표기 규칙을/를 참조하십시오.

팁 전체 모니터링된 네트워크를 대상으로 지정하려면 `0.0.0.0/0` 및 `::/0`을 사용합니다.

5단계 모니터링에서 네트워크를 제외하려면 **Exclude**를 선택합니다.

6단계 추가적인 네트워크를 추가하려면 4~5단계를 반복합니다.

7단계 **Targeted Host Attributes** 옆의 **Add**를 클릭하여 특정 호스트 속성이 있는 호스트를 대상으로 지정합니다.

8단계 **Attribute** 및 **Value** 드롭다운 목록에서 호스트 속성을 지정합니다.

9단계 추가적인 호스트 속성을 추가하려면 7~8단계를 반복합니다.

화이트리스트와 비교 평가하려면 호스트에는 사용자가 지정한 최소 하나 이상의 호스트 속성이 있어야 합니다.

10단계 **Targeted VLANs** 옆의 **Add**를 클릭하여 특정 VLAN에 속한 호스트를 대상으로 지정합니다.

11단계 **VLAN ID** 필드에서 화이트리스트와 비교 평가할 호스트의 VLAN ID를 지정합니다. 이는 802.1q VLAN의 정수 0~4095 중에서 지정할 수 있습니다.

12단계 추가적인 VLAN ID를 추가하려면 10~11단계를 반복합니다.

화이트리스트와 비교 평가하려면 호스트는 사용자가 지정한 VLAN 중 하나의 구성원이어야 합니다.

팁 네트워크, 호스트 특성 제한 또는 VLAN 제한을 제거하려면 삭제할 요소 옆의 삭제 아이콘( )을 클릭합니다.

기존 대상 수정

라이센스: FireSIGHT

대상을 변경한 후에는 화이트리스트를 저장해야 변경 사항이 적용됩니다. 활성화된 상관관계 정책에서 사용되는 화이트리스트의 대상을 수정할 경우, 화이트리스트를 저장하면 새로운 대상 호스트의 규정준수 여부가 평가됩니다. 그러나 이러한 평가로 인해 화이트리스트 이벤트가 생성되지는 않습니다. 또한 이전에 유효 대상이었던 화이트리스트 호스트 속성이 `Not Evaluated`로 변경됩니다.

기존 대상을 수정하려면

액세스: Admin

1단계 Create White List 페이지의 **Targets** 아래에서 수정할 대상을 클릭합니다.

대상에 대한 설정이 나타납니다.

2단계 필요에 따라 변경합니다.

대상의 이름을 변경하고, 추가적인 네트워크를 추가 또는 제외하며, 호스트 특성 또는 VLAN 제한 사항을 추가할 수 있습니다. 자세한 내용은 52-11페이지의 규정준수 화이트리스트 대상 구성을/를 참조하십시오.

기존 대상 삭제

라이센스: FireSIGHT

대상을 삭제한 후에는 화이트리스트를 저장해야 변경 사항이 적용됩니다. 활성화된 상관관계 정책에서 사용되는 화이트리스트에서 대상을 삭제할 경우, 이전에 유효 대상이었던 화이트리스트 호스트 속성이 `Not Evaluated`로 변경됩니다.

화이트리스트 대상을 삭제하려면

액세스: Admin

1단계 삭제할 라이센스 옆의 삭제 아이콘( )을 클릭합니다.

2단계 확인 메시지가 표시되면 대상을 삭제할 것임을 확인합니다.

대상이 삭제됩니다.

규정준수 화이트리스트 호스트 프로필 구성

라이센스: FireSIGHT

규정준수 화이트리스트의 호스트 프로필은 대상 호스트에서 실행할 수 있는 운영 체제, 클라이언트, 애플리케이션 프로토콜, 웹 애플리케이션, 프로토콜을 지정합니다. 화이트리스트에서는 세 가지 종류의 호스트 프로필을 구성할 수 있습니다.

- 전역 호스트 프로필 - 호스트의 운영 체제에 상관없이 대상 호스트에서 실행할 수 있도록 허용된 애플리케이션 프로토콜, 클라이언트, 웹 애플리케이션, 프로토콜을 지정합니다.

- 특정 운영 체제에 대한 호스트 프로필 - 네트워크에서 실행할 수 있는 운영 체제뿐만 아니라, 해당 운영 체제에서 실행할 수 있는 애플리케이션 프로토콜, 클라이언트, 웹 애플리케이션, 프로토콜도 지정합니다.
- 공유 호스트 프로필 - 단일한 화이트리스트에 연결된다는 점을 제외하고는, 특정 운영 체제에 대한 호스트 프로필과 같은 기능을 수행합니다. 이를 여러 화이트리스트 전반에 걸쳐 사용할 수 있습니다.

규정준수 화이트리스트 호스트 프로필에 대한 자세한 개요는 52-4페이지의 화이트리스트 호스트 프로필 이해을/를 참조하십시오.

규정준수 화이트리스트 호스트 프로필 생성을 완료하면, 화이트리스트를 활성화된 상관관계 정책에 추가하여 대상 호스트의 규정준수 여부를 평가하고, 호스트가 화이트리스트를 위반한 경우 화이트리스트 이벤트를 생성하며, 선택에 따라 화이트리스트 위반을 기준으로 응답을 트리거할 수 있습니다.

규정준수 화이트리스트 호스트 프로필을 생성, 수정, 삭제하는 방법에 대한 자세한 내용은 다음을 참조하십시오.

- 52-14페이지의 전역 호스트 프로필 구성
- 52-15페이지의 특정 운영 체제에 대한 호스트 프로필 생성
- 52-19페이지의 공유 호스트 프로필을 규정준수 화이트리스트에 추가
- 52-20페이지의 기존 호스트 프로필 수정
- 52-23페이지의 기존 호스트 프로필 삭제

전역 호스트 프로필 구성

라이센스: FireSIGHT

호스트의 운영 체제에 상관없이, 모든 화이트리스트에는 대상 호스트에서 실행할 수 있도록 허용된 애플리케이션 프로토콜, 클라이언트, 웹 애플리케이션, 프로토콜을 지정하는 전역 호스트 프로필이 포함되어 있습니다. 전역 호스트 프로필에 대한 자세한 개요는 52-4페이지의 전역 호스트 프로필 이해을/를 참조하십시오.

전역 호스트 프로필을 구성하려면

액세스: Admin

1단계 Create White List 페이지의 **Allowed Host Profiles** 아래에서 **Any Operating System**을 클릭합니다.

전역 호스트 프로필의 설정이 표시됩니다.

2단계 허용할 애플리케이션 프로토콜을 지정하려면 52-16페이지의 애플리케이션 프로토콜을 호스트 프로필에 추가의 지침을 따릅니다.

3단계 허용할 클라이언트를 지정하려면 52-17페이지의 클라이언트를 호스트 프로필에 추가의 지침을 따릅니다.

4단계 허용할 웹 애플리케이션을 지정하려면 52-18페이지의 웹 애플리케이션을 호스트 프로필에 추가의 지침을 따릅니다.

5단계 허용할 프로토콜을 지정하려면 52-18페이지의 프로토콜을 호스트 프로필에 추가의 지침을 따릅니다.

ARP, IP, TCP, UDP는 항상 허용됩니다.

특정 운영 체제에 대한 호스트 프로필 생성

라이센스: FireSIGHT

특정 운영 체제에 대한 호스트 프로필은 네트워크에서 실행할 수 있는 운영 체제뿐만 아니라, 해당 운영 체제에서 실행할 수 있는 애플리케이션 프로토콜, 클라이언트, 웹 애플리케이션, 프로토콜을 나타냅니다. 자세한 개요는 52-4페이지의 특정 운영 체제에 대한 호스트 프로필 이해을/를 참조하십시오.

특정 운영 체제에 대한 새 규정준수 화이트리스트 호스트 프로필을 생성하려면

액세스: Admin

1단계 **Allowed Host Profiles** 옆의 추가 아이콘( )을 클릭합니다.

새 호스트 프로필의 설정이 표시됩니다.

2단계 **Name** 필드에 호스트 프로필을 설명하는 이름을 입력합니다.

3단계 **OS Vendor**, **OS Name**, **Version** 드롭다운 목록에서 호스트 프로필을 생성할 운영 체제 및 버전을 선택합니다.

4단계 허용할 애플리케이션 프로토콜을 지정합니다. 3가지 옵션이 제공됩니다.

- 모든 애플리케이션 프로토콜을 허용하려면 **Allow all Application Protocols** 확인란을 선택한 상태로 둡니다.
- 애플리케이션 프로토콜을 허용하지 않으려면 **Allow all Application Protocols** 확인란의 선택을 취소합니다.
- 특정 애플리케이션 프로토콜을 허용하려면 52-16페이지의 애플리케이션 프로토콜을 호스트 프로필에 추가의 지침을 따릅니다.

5단계 허용할 클라이언트를 지정합니다. 3가지 옵션이 제공됩니다.

- 모든 클라이언트를 허용하려면 **Allow all Clients** 확인란을 선택한 상태로 둡니다.
- 클라이언트를 허용하지 않으려면 **Allow all Clients** 확인란의 선택을 취소합니다.
- 특정 클라이언트를 허용하려면 52-17페이지의 클라이언트를 호스트 프로필에 추가의 지침을 따릅니다.

6단계 허용할 웹 애플리케이션을 지정합니다. 3가지 옵션이 제공됩니다.

- 모든 웹 애플리케이션을 허용하려면 **Allow all Web Applications** 확인란을 선택한 상태로 둡니다.
- 웹 애플리케이션을 허용하지 않으려면 **Allow all Web Applications** 확인란의 선택을 취소합니다.
- 특정 웹 애플리케이션을 허용하려면 52-18페이지의 웹 애플리케이션을 호스트 프로필에 추가의 지침을 따릅니다.

7단계 허용할 프로토콜을 지정합니다.

Allowed Protocols 옆에 프로토콜을 추가하려면 52-18페이지의 프로토콜을 호스트 프로필에 추가의 지침을 따릅니다. ARP, IP, TCP, UDP는 항상 허용됩니다.

애플리케이션 프로토콜을 호스트 프로필에 추가

라이센스: FireSIGHT

공유 호스트 프로필 또는 단일한 화이트리스트에 속한 호스트 프로필을 사용하여 규정준수 화이트리스트를 구성할 경우, 특정 애플리케이션 프로토콜을 특정 운영 체제에서 실행하도록 허용할 수 있습니다. 또한 모든 유효 대상에서 특정 애플리케이션 프로토콜을 실행할 수 있도록 화이트리스트를 구성할 수도 있으며, 이를 전역 허용 애플리케이션 프로토콜이라고 합니다.

모든 허용된 애플리케이션 프로토콜의 경우, 허용할 애플리케이션 프로토콜의 유형(애플리케이션 프로토콜 유형의 예: FTP 및 SSH)을 지정하거나, 모든 유형의 애플리케이션 프로토콜을 지정하여 사용자 지정 애플리케이션 프로토콜을 허용할 수 있습니다. 허용된 애플리케이션 프로토콜에서 사용하는 프로토콜(TCP 또는 UDP)도 지정해야 합니다. 임의의 포트에서 애플리케이션을 허용하거나, 이를 지정된 포트로 제한할 수 있습니다.

선택에 따라, 애플리케이션 프로토콜 서버가 특정 공급업체 또는 버전을 충족하도록 요청할 수 있습니다. 예를 들어, SSH를 Linux 호스트의 포트 22에서 실행하도록 허용할 수 있습니다. 또한 특정 공급업체 및 버전을 OpenSSH 4.2로 제한할 수도 있습니다.

애플리케이션 프로토콜을 규정준수 화이트리스트 호스트 프로필에 추가하려면

액세스: Admin

1단계 화이트리스트 호스트 프로필을 생성하거나 수정할 경우, **Allowed Application Protocols** 옆의(또는 모든 운영 체제 호스트 프로필을 수정할 경우 **Globally Allowed Application Protocols** 옆의 아이콘) 추가 아이콘( )을 클릭합니다.

팝업 창이 나타납니다. 다음과 같은 애플리케이션 프로토콜이 나열됩니다.

- 화이트리스트 내에서 생성된 애플리케이션 프로토콜
- 52-9페이지의 네트워크 조사에 설명된 대로 네트워크를 조사할 당시 네트워크 맵에 있던 애플리케이션 프로토콜
- 화이트리스트의 다른 호스트 프로필에 사용된 애플리케이션 프로토콜(기본 화이트리스트에 사용하기 위해 VRT에서 생성한 내장형 애플리케이션 프로토콜이 포함될 수 있음)

2단계 다음 2가지 옵션을 사용할 수 있습니다.

- 목록에 이미 있는 애플리케이션 프로토콜을 추가하려면 해당 프로토콜을 선택하고 **OK**를 클릭합니다. 여러 애플리케이션 프로토콜을 선택하려면 Ctrl 또는 Shift 키를 누른 채 클릭합니다. 또는 클릭하고 드래그하여 인접한 여러 애플리케이션 프로토콜을 선택할 수 있습니다.

  애플리케이션 프로토콜이 추가됩니다. 내장형 애플리케이션 프로토콜을 추가할 경우, 해당 이름은 기울임꼴로 표시됩니다. 절차의 나머지 단계를 건너뛸 수 있으며, 선택에 따라 애플리케이션 프로토콜의 값(예: 포트 또는 프로토콜)을 변경하려면 방금 추가한 애플리케이션 프로토콜을 클릭하여 애플리케이션 프로토콜 편집기를 표시합니다.
- 새 애플리케이션 프로토콜을 추가하려면 **<New Application Protocol>**을 선택하고 **OK**를 클릭합니다.

  애플리케이션 프로토콜 편집기가 표시됩니다.

3단계 **Type** 드롭다운 목록에서 애플리케이션 프로토콜 유형을 선택합니다. 사용자 지정 애플리케이션 프로토콜의 경우 **any**를 선택합니다.

4단계 애플리케이션 프로토콜 포트를 지정합니다. 다음 2가지 옵션을 사용할 수 있습니다.

- 모든 포트에서 애플리케이션 프로토콜을 실행할 수 있도록 허용하려면, **Any port** 확인란을 선택합니다.
- 특정 포트에서만 애플리케이션 프로토콜을 실행할 수 있도록 허용하려면, **port** 필드에 포트 번호를 입력합니다.

5단계 **Protocol** 드롭다운 목록에서 프로토콜(**TCP** 또는 **UDP**)을 선택합니다.

6단계 선택에 따라, **Vendor** 및 **Version** 필드에서 애플리케이션 프로토콜에 대한 공급업체 및 버전을 지정합니다.

공급업체 또는 버전을 지정하지 않을 경우, 화이트리스트에서는 유형 및 프로토콜이 매칭될 때까지 모든 공급업체와 버전을 허용합니다. 공급업체 및 버전을 제한할 경우, 이벤트 보기 또는 애플리케이션 프로토콜 네트워크 맵에 표시되는 항목과 동일하게 지정해야 합니다.

7단계 **OK**를 클릭합니다.

애플리케이션 프로토콜이 추가됩니다. 변경 사항을 적용하려면 화이트리스트를 저장해야 합니다.

애플리케이션 프로토콜을 활성화된 상관관계 정책에서 사용 중인 화이트리스트에 추가한 경우, 화이트리스트를 저장하면 대상 호스트가 재평가됩니다. 이러한 재평가로 인해 일부 호스트의 상태가 규정준수로 바뀔 수 있으나, 화이트리스트 이벤트는 생성되지 않습니다.

클라이언트를 호스트 프로필에 추가

라이센스: FireSIGHT

공유 호스트 프로필 또는 단일한 화이트리스트에 속한 호스트 프로필을 사용하여 규정준수 화이트리스트를 구성할 경우, 특정 클라이언트 애플리케이션을 특정 운영 체제에서 실행하도록 허용할 수 있습니다. 또한 모든 유효 대상에서 특정 클라이언트를 실행할 수 있도록 화이트리스트를 구성할 수도 있으며, 이를 전역 허용 클라이언트라고 합니다.

선택에 따라, 특정 버전의 클라이언트를 요청할 수 있습니다. 예를 들어, Microsoft Internet Explorer 8.0에서만 Microsoft Windows 호스트를 실행하도록 허용할 수 있습니다.

클라이언트를 규정준수 화이트리스트 호스트 프로필에 추가하려면

액세스: Admin

1단계 화이트리스트 호스트 프로필을 생성하거나 수정할 경우, **Allowed Clients** 옆의(또는 모든 운영 체제 호스트 프로필을 수정할 경우 **Globally Allowed Clients** 옆의 아이콘) 추가 아이콘()을 클릭합니다.

팝업 창이 나타납니다. 다음과 같은 클라이언트가 나열됩니다.

- 화이트리스트 내에서 생성된 클라이언트
- 52-9페이지의 네트워크 조사에 설명된 대로 네트워크를 조사할 당시 네트워크 맵에서 실행 중이었던 클라이언트
- 화이트리스트의 다른 호스트 프로필에 사용된 클라이언트(기본 화이트리스트에 사용하기 위해 VRT에서 생성한 내장형 클라이언트가 포함될 수 있음)

2단계 다음 2가지 옵션을 사용할 수 있습니다.

- 목록에 이미 있는 클라이언트를 추가하려면 해당 프로토콜을 선택하고 **OK**를 클릭합니다. 여러 개의 클라이언트를 선택하려면 Ctrl + Shift를 사용합니다. 끌어서 놓기를 사용하여 여러 개의 인접한 클라이언트를 선택할 수도 있습니다.

  클라이언트가 추가됩니다. 내장형 클라이언트를 추가할 경우, 해당 이름은 기울임꼴로 표시됩니다. 절차의 나머지 단계를 건너뛸 수 있으며, 선택에 따라 클라이언트의 값(예: 해당 버전)을 변경하려면 방금 추가한 클라이언트를 클릭하여 클라이언트 편집기를 표시합니다.
- 새 클라이언트를 추가하려면 **<New Client>**를 선택하고 **OK**를 클릭합니다.

  클라이언트 편집기가 나타납니다.

3단계 **Client** 드롭다운 목록에서 클라이언트를 선택합니다.

4단계 선택에 따라, **Version** 필드에서 클라이언트의 버전을 지정합니다.

버전을 지정하지 않을 경우, 화이트리스트는 이름이 매칭될 때까지 모든 버전을 허용합니다. 버전을 제한할 경우, 클라이언트의 테이블 보기에 표시되는 항목과 동일하게 지정해야 합니다.

5단계 **OK**를 클릭합니다.

클라이언트가 추가됩니다. 변경 사항을 적용하려면 화이트리스트를 저장해야 합니다.

클라이언트를 활성화된 상관관계 정책에서 사용 중인 화이트리스트에 추가한 경우, 화이트리스트를 저장하면 대상 호스트가 재평가됩니다. 이러한 재평가로 인해 일부 호스트의 상태가 규정준수로 바뀔 수 있으나, 화이트리스트 이벤트는 생성되지 않습니다.

웹 애플리케이션을 호스트 프로필에 추가

라이센스: FireSIGHT

공유 호스트 프로필 또는 단일한 화이트리스트에 속한 호스트 프로필을 사용하여 규정준수 화이트리스트를 구성할 경우, 특정 웹 애플리케이션을 특정 운영 체제에서 실행하도록 허용할 수 있습니다. 또한 모든 유효 대상에서 특정 웹 애플리케이션을 실행할 수 있도록 화이트리스트를 구성할 수도 있으며, 이를 전역 허용 웹 애플리케이션이라고 합니다.

웹 애플리케이션을 규정준수 화이트리스트 호스트 프로필에 추가하려면

액세스: Admin

1단계 화이트리스트 호스트 프로필을 생성하거나 수정할 경우, **Allowed Web Applications** 옆의(또는 모든 운영 체제 호스트 프로필을 수정할 경우 **Globally Allowed Web Applications** 옆의 아이콘) 추가 아이콘( )을 클릭합니다.

시스템에서 탐지된 모든 웹 애플리케이션이 나열된 팝업 창이 나타납니다.

2단계 웹 애플리케이션을 선택하고 **OK**를 클릭합니다. 여러 개의 웹 애플리케이션을 선택하려면 Ctrl + Shift를 사용합니다. 끌어서 놓기를 사용하여 여러 개의 인접한 웹 애플리케이션을 선택할 수도 있습니다.

웹 애플리케이션이 추가됩니다. 변경 사항을 적용하려면 화이트리스트를 저장해야 합니다.

웹 애플리케이션을 활성화된 상관관계 정책에서 사용 중인 화이트리스트에 추가한 경우, 화이트리스트를 저장하면 대상 호스트가 재평가됩니다. 이러한 재평가로 인해 일부 호스트의 상태가 규정준수로 바뀔 수 있으나, 화이트리스트 이벤트는 생성되지 않습니다.

프로토콜을 호스트 프로필에 추가

라이센스: FireSIGHT

공유 호스트 프로필 또는 단일한 화이트리스트에 속한 호스트 프로필을 사용하여 규정준수 화이트리스트를 구성할 경우, 특정 프로토콜을 특정 운영 체제에서 실행하도록 허용할 수 있습니다. 또한 모든 유효 대상에서 특정 프로토콜을 실행할 수 있도록 화이트리스트를 구성할 수도 있으며, 이를 전역 허용 프로토콜이라고 합니다. ARP, IP, TCP, UDP는 항상 모든 호스트에서 허용되며 해당 프로토콜은 허용하지 않을 수 없습니다.

모든 허용된 프로토콜은 유형(Network 또는 Transport) 및 번호를 지정해야 합니다.

프로토콜을 규정준수 화이트리스트 호스트 프로필에 추가하려면

액세스: Admin

1단계 화이트리스트 호스트 프로필을 생성하거나 수정할 경우, **Allowed Protocols** 옆의(또는 모든 운영 체제 호스트 프로필을 수정할 경우 **Globally Allowed Protocols** 옆의 아이콘) 추가 아이콘( )을 클릭합니다.

팝업 창이 나타납니다. 다음과 같은 프로토콜이 나열됩니다.

- 화이트리스트 내에서 생성된 프로토콜
- 52-9페이지의 네트워크 조사에 설명된 대로 네트워크를 조사할 당시 네트워크 맵에서 실행 중이었던 프로토콜
- 화이트리스트의 다른 호스트 프로필에 사용된 프로토콜(기본 화이트리스트에 사용하기 위해 VRT에서 생성한 내장형 프로토콜이 포함될 수 있음)

2단계 다음 2가지 옵션을 사용할 수 있습니다.

- 목록에 이미 있는 프로토콜을 추가하려면 해당 프로토콜을 선택하고 **OK**를 클릭합니다. 여러 개의 프로토콜을 선택하려면 Ctrl + Shift를 사용합니다. 끌어서 놓기를 사용하여 여러 개의 인접한 프로토콜을 선택할 수도 있습니다.

  프로토콜이 추가됩니다. 내장형 프로토콜을 추가할 경우, 해당 이름은 기울임꼴로 표시됩니다. 절차의 나머지 단계를 건너뛸 수 있으며, 선택에 따라 프로토콜의 값(예: 유형 또는 번호)을 변경하려면 방금 추가한 프로토콜을 클릭하여 프로토콜 편집기를 표시합니다.
- 새 프로토콜을 추가하려면 **<New Protocol>**을 선택하고 **OK**를 클릭합니다.

  프로토콜 편집기가 표시됩니다.

3단계 **Type** 드롭다운 목록에서 프로토콜 유형(**Network** 또는 **Transport**)을 선택합니다.

4단계 프로토콜을 지정합니다. 다음 2가지 옵션을 사용할 수 있습니다.

- 드롭다운 목록에서 프로토콜을 선택합니다.
- **Other (manual entry)**를 선택하여 목록에 없는 프로토콜을 지정합니다. 네트워크 프로토콜의 경우, http://www.iana.org/assignments/ethernet-numbers/에 나열된 적합한 번호를 입력합니다. 전송 프로토콜의 경우, http://www.iana.org/assignments/protocol-numbers/에 나열된 적합한 번호를 입력합니다.

5단계 **OK**를 클릭합니다.

프로토콜이 추가됩니다. 변경 사항을 적용하려면 화이트리스트를 저장해야 합니다.

프로토콜을 활성화된 상관관계 정책에서 사용 중인 화이트리스트에 추가한 경우, 화이트리스트를 저장하면 대상 호스트가 재평가됩니다. 이러한 재평가로 인해 일부 호스트의 상태가 규정준수로 바뀔 수 있으나, 화이트리스트 이벤트는 생성되지 않습니다.

공유 호스트 프로필을 규정준수 화이트리스트에 추가

라이센스: FireSIGHT

공유 호스트 프로필은 특정 운영 체제에 연결되지만, 화이트리스트 전반에 걸쳐 사용할 수 있습니다. 즉, 여러 개의 화이트리스트를 생성하지만 동일한 호스트 프로필을 사용하여 화이트리스트 전반에 걸쳐 특정 운영 체제를 실행하는 호스트를 평가하려는 경우, 공유 호스트 프로필을 사용합니다.

내장형 공유 호스트 프로필을 규정준수 화이트리스트에 추가하거나, 사용자가 직접 생성한 공유 호스트 프로필을 추가할 수 있습니다. 자세한 내용은 52-5페이지의 공유 호스트 프로필 이해 및 52-25페이지의 공유 호스트 프로필 생성을/를 참조하십시오.

공유 호스트 프로필을 규정준수 화이트리스트에 추가하려면

액세스: Admin

1단계 Create White List 페이지에서 **Add Shared Host Profile**을 클릭합니다.

Add Shared Host Profile 페이지가 나타납니다.

2단계 **Name** 드롭다운 목록에서, 화이트리스트에 추가할 공유 호스트 프로필을 선택하고 **OK**를 클릭합니다.

공유 호스트 프로필이 화이트리스트에 추가되며 Create White List 페이지가 다시 표시됩니다. 공유 호스트 프로필의 이름은 Allowed Host Profiles 아래에 기울임꼴로 표시됩니다.

팁 Allowed Host Profiles 아래의 프로필 이름을 클릭하여 이를 사용하는 화이트리스트 내의 공유 호스트 프로필을 수정할 수 있습니다. 자세한 내용은 52-20페이지의 기존 호스트 프로필 수정을/를 참조하십시오.

기존 호스트 프로필 수정

라이센스: FireSIGHT

규정준수 화이트리스트 내의 호스트 프로필을 수정한 후, 화이트리스트를 저장해야 변경 사항이 적용됩니다.

수정한 호스트 파일이 활성화된 상관관계 정책에 사용되는 화이트리스트에 속한 경우, 프로필을 수정하면 호스트의 상태가 규정준수 또는 규정준수 위반으로 바뀔 수 있으나 화이트리스트 이벤트가 생성되지는 **않습니다**. 또한 공유 호스트 프로필을 수정할 경우, 이를 사용하는 모든 화이트리스트에 영향을 미칩니다. 이렇게 하면 현재 작업 중인 화이트리스트뿐만 아니라 다른 화이트리스트 내의 호스트의 상태가 규정준수 또는 규정준수 위반으로 바뀔 수 있습니다.

팁 다른 공유 호스트 프로필과 마찬가지로, 기본 화이트리스트에서 사용되는 내장형 호스트 프로필을 수정할 수 있습니다. 해당 프로필의 공장 기본값을 재설정할 수도 있습니다. 자세한 내용은 52-29페이지의 내장형 호스트 프로필을 공장 기본값으로 재설정을/를 참조하십시오.

기존 호스트 프로필을 수정하려면

액세스: Admin

1단계 Create White List 페이지에서 수정할 호스트 프로필의 이름을 클릭합니다.

호스트 프로필의 설정이 표시됩니다. 공유 호스트 프로필을 수정할 경우, 호스트 프로필의 이름 옆에 **Edit** 링크가 표시됩니다. 내장형 호스트 프로필을 수정할 경우, 내장형 호스트 프로필의 옆에도 프로필 아이콘( )이 표시됩니다.

2단계 다음 2가지 옵션을 사용할 수 있습니다.

- 공유 호스트 프로필을 수정할 경우 **Edit**를 클릭합니다.

  팝업 창이 나타납니다. 아래 표에 설명된 대로 필요에 따라 변경 사항을 적용합니다. **Save All Profiles**를 클릭하여 프로필을 저장한 다음 **Done**을 클릭하여 팝업 창을 닫습니다.

  공유 호스트 프로필의 수정에 대한 자세한 내용은 52-26페이지의 공유 호스트 프로필 수정을/를 참조하십시오.

- 화이트리스트의 전역 호스트 프로필 또는 특정 운영 체제의 호스트 프로필을 수정할 경우, 아래 절차에 설명된 작업 중 하나를 수행하십시오.

호스트 프로필의 이름을 변경하려면

액세스: Admin

1단계 **Name** 필드에 새 이름을 입력합니다.

호스트 프로필에 대한 운영 체제를 변경하려면

액세스: Admin

1단계 **OS Vendor**, **OS Name**, **Version** 드롭다운 목록에서 새 운영 체제 및 버전을 선택합니다.

이러한 값을 변경할 경우, 호스트 프로필의 이름도 변경하고자 할 수 있습니다. 화이트리스트의 전역 호스트 프로필에는 이와 연결된 운영 체제가 없으므로, 이는 변경할 수 없습니다.

애플리케이션 프로토콜을 추가하려면

액세스: Admin

1단계 52-16페이지의 애플리케이션 프로토콜을 호스트 프로필에 추가의 지침을 따릅니다.

클라이언트를 추가하려면

액세스: Admin

1단계 52-17페이지의 클라이언트를 호스트 프로필에 추가의 지침을 따릅니다.

웹 애플리케이션을 추가하려면

액세스: Admin

1단계 52-18페이지의 웹 애플리케이션을 호스트 프로필에 추가의 지침을 따릅니다.

프로토콜을 추가하려면

액세스: Admin

1단계 52-18페이지의 프로토콜을 호스트 프로필에 추가의 지침을 따릅니다.

모든 애플리케이션 프로토콜을 허용하려면

액세스: Admin

1단계 **Allowed Application Protocols** 아래에서 **Allow all Application Protocols** 확인란을 선택합니다.

이전에 허용한 모든 애플리케이션 프로토콜을 삭제할 때까지 이 확인란이 표시되지 않습니다.

모든 클라이언트를 허용하려면

액세스: Admin

1단계 **Allowed Clients** 아래에서 **Allow all Clients** 확인란을 선택합니다.

이전에 허용한 모든 클라이언트를 삭제할 때까지 이 확인란이 표시되지 않습니다.

모든 웹 애플리케이션을 허용하려면

액세스: Admin

1단계 **Allowed Web Applications** 아래에서 **Allow all Web Applications** 확인란을 선택합니다.

이전에 허용한 모든 웹 애플리케이션을 삭제할 때까지 이 확인란이 표시되지 않습니다.

애플리케이션 프로토콜, 클라이언트, 웹 애플리케이션 또는 프로토콜을 수정하려면

액세스: Admin

1단계 수정할 요소를 클릭합니다.

사용자가 변경할 수 있는 속성에 대한 자세한 내용은 다음을 참조하십시오.

- 52-16페이지의 애플리케이션 프로토콜을 호스트 프로필에 추가
- 52-17페이지의 클라이언트를 호스트 프로필에 추가
- 52-18페이지의 프로토콜을 호스트 프로필에 추가

참고 애플리케이션 프로토콜, 클라이언트, 웹 애플리케이션 또는 프로토콜에 적용한 변경 사항은 해당 요소를 사용하는 모든 호스트 프로필에 반영됩니다.

애플리케이션 프로토콜, 클라이언트, 웹 애플리케이션 또는 프로토콜을 삭제하려면

액세스: Admin

1단계 삭제할 요소 옆의 삭제 아이콘( )을 클릭합니다.

네트워크를 조사하려면

액세스: Admin

1단계 **Survey Network**를 클릭합니다. 네트워크를 조사하면 허용된 추가 클라이언트, 애플리케이션 프로토콜, 프로토콜을 기존의 호스트 프로필에 추가할 수 있으며, 처음 조사 과정에서 탐지되지 않은 운영 체제를 실행 중인 호스트가 조사에서 탐지될 경우 추가 호스트 프로필을 추가할 수 있습니다. 자세한 내용은 52-9페이지의 네트워크 조사을/를 참조하십시오.

기존 호스트 프로필 삭제

라이센스: FireSIGHT

규정준수 화이트리스트에서 호스트 프로필을 삭제한 후, 화이트리스트를 저장해야 변경 사항이 적용됩니다. 공유 호스트 프로필을 삭제하면 화이트리스트에서 해당 프로필이 제거되지만, 이를 사용하는 다른 화이트리스트의 해당 프로필은 삭제 또는 제거되지 않습니다. 화이트리스트의 전역 호스트 프로필을 삭제할 수 없습니다.

삭제한 호스트 프로필이 활성화된 상관관계 정책에 사용된 하나 이상의 화이트리스트에 속한 경우, 해당 프로필을 삭제하면 호스트의 상태가 규정준수 위반으로 바뀔 수 있으나 화이트리스트 이벤트는 생성되지 **않습니다**.

규정준수 화이트리스트 호스트 프로필을 삭제하려면

액세스: Admin

1단계 Create White List 페이지에서 삭제할 호스트 프로필 옆의 삭제 아이콘( )을 클릭합니다.

2단계 확인 메시지가 표시되면 호스트 프로필을 삭제할 것임을 확인합니다.

호스트 프로필이 삭제됩니다.

규정준수 화이트리스트 관리

라이센스: FireSIGHT

White List 페이지를 사용하여 규정준수 화이트리스트를 관리합니다. 기본 화이트리스트를 비롯한 화이트리스트를 생성, 수정, 삭제할 수 있습니다. 생성한 공유 호스트 프로필 및 내장형 공유 호스트 프로필을 수정할 수 있으며, 새 공유 호스트 프로필을 추가할 수도 있습니다. 자세한 내용은 다음 링크를 참고하십시오.

- 52-8페이지의 규정준수 화이트리스트 생성
- 52-24페이지의 규정준수 화이트리스트 수정
- 52-24페이지의 규정준수 화이트리스트 삭제
- 52-25페이지의 공유 호스트 프로필 작업

규정준수 화이트리스트 수정

라이센스: FireSIGHT

활성화된 상관관계 정책에 포함된 규정준수 화이트리스트를 수정할 경우, 시스템에서는 대상 호스트를 재평가합니다. 이때 시스템에서는 화이트리스트 이벤트를 생성하지 **않으므로**, 이러한 재평가가 진행되는 동안 화이트리스트와 관련된 어떠한 응답도 트리거되지 않습니다. 이는 활성화된 상관관계 정책에 화이트리스트가 포함되어 있고, 화이트리스트 업데이트로 인해 이전에는 규정준수 상태였던 호스트의 상태가 규정준수 위반으로 바뀌는 경우에도 마찬가지입니다.

기존 규정준수 화이트리스트를 수정하려면

액세스: Admin

1단계 **Policies > Correlation**을 선택한 다음 **White List**를 클릭합니다.

White List 페이지가 나타납니다.

2단계 수정할 화이트리스트의 옆의 수정 아이콘( )을 클릭합니다.

Create White List 페이지가 나타납니다.

3단계 필요에 따라 수정 사항을 적용하고 **Save White List**를 클릭합니다.

화이트리스트가 업데이트됩니다.

규정준수 화이트리스트 삭제

라이센스: FireSIGHT

하나 이상의 상관관계 정책에서 사용 중인 규정준수 화이트리스트를 삭제할 수 없습니다. 화이트리스트가 사용된 모든 정책에서 해당 화이트리스트를 우선 삭제해야 합니다. 정책에서 화이트리스트를 삭제하는 방법에 대한 자세한 내용은 51-50페이지의 상관관계 정책 수정을/를 참조하십시오.

화이트리스트를 삭제하면 네트워크에 있는 호스트의 화이트리스트와 연결된 호스트 속성도 제거됩니다.

기존 규정준수 화이트리스트를 삭제하려면

액세스: Admin

1단계 **Policies > Correlation**을 선택한 다음 **White List**를 클릭합니다.

White List 페이지가 나타납니다.

2단계 삭제할 화이트리스트의 옆에 있는 삭제 아이콘( )을 클릭합니다.

화이트리스트가 삭제됩니다.

공유 호스트 프로필 작업

라이센스: FireSIGHT

공유 호스트 프로필은 여러 화이트리스트 전반에 걸쳐 대상 호스트에서 실행할 수 있는 운영 체제, 클라이언트, 애플리케이션 프로토콜, 웹 애플리케이션, 프로토콜을 지정합니다. 즉, 여러 개의 화이트리스트를 생성하지만 동일한 호스트 프로필을 사용하여 화이트리스트 전반에 걸쳐 특정 운영 체제를 실행하는 호스트를 평가하려는 경우, 공유 호스트 프로필을 사용합니다. 기본 화이트리스트는 *내장형 호스트 프로필*이라고 하는 특수 카테고리의 공유 호스트 프로필을 사용합니다.

공유 호스트 프로필에 대한 자세한 개요는 52-5페이지의 공유 호스트 프로필 이해을/를 참조하십시오.

공유 호스트 프로필을 생성, 수정, 삭제할 수 있습니다. 또한 내장형 공유 호스트 프로필을 수정 또는 삭제하거나, 내장형 애플리케이션 프로토콜, 프로토콜, 클라이언트를 수정 또는 삭제할 경우 해당 요소의 공장 기본값을 재설정할 수 있습니다. 자세한 내용은 다음 링크를 참고하십시오.

- 52-25페이지의 공유 호스트 프로필 생성
- 52-26페이지의 공유 호스트 프로필 수정
- 52-28페이지의 공유 호스트 프로필 삭제
- 52-29페이지의 내장형 호스트 프로필을 공장 기본값으로 재설정

공유 호스트 프로필을 생성한 후에는 이를 여러 화이트리스트에 추가할 수 있습니다. 자세한 내용은 52-19페이지의 공유 호스트 프로필을 규정준수 화이트리스트에 추가을/를 참조하십시오.

공유 호스트 프로필 생성

라이센스: FireSIGHT

여러 화이트리스트 전반에 걸쳐 특정 운영 체제를 실행 중인 호스트를 동일한 호스트 프로필을 사용하여 평가하려는 경우, 공유 호스트 프로필을 생성합니다.

팁 또한 특정 호스트의 호스트 프로필을 사용하여 규정준수 화이트리스트의 공유 호스트 프로필을 생성할 수도 있습니다. 자세한 내용은 49-24페이지의 호스트 프로필에서 화이트리스트 호스트 프로필 생성을/를 참조하십시오.

공유 호스트 프로필을 생성하려면

액세스: Admin

1단계 **Policies > Correlation**을 선택한 다음 **White List**를 클릭합니다.

White List 페이지가 나타납니다.

2단계 **Edit Shared Profiles**를 클릭합니다.

Edit Shared Profiles 페이지가 나타납니다.

3단계 선택에 따라, 네트워크를 조사합니다.

네트워크를 조사할 경우, 시스템에 축적된 네트워크에 대한 데이터를 기준으로 여러 개의 기본 공유 화이트리스트가 생성됩니다. 이렇게 하면 여러 공유 호스트 프로필을 수동으로 생성하고 구성하지 않아도 됩니다. 다음 2가지 옵션을 사용할 수 있습니다.

- 네트워크를 조사하려면 **Survey Network**를 클릭합니다. 자세한 내용은 52-9페이지의 네트워크 조사을/를 참조하십시오.

시스템에서 하나 이상의 기본 공유 호스트 프로필을 생성합니다. 52-26페이지의 공유 호스트 프로필 수정 및 52-28페이지의 공유 호스트 프로필 삭제에 설명된 대로 이러한 공유 호스트 파일을 수정하거나 삭제할 수 있습니다. 나중에 필요할 수 있는 다른 공유 호스트 프로필을 추가하려면 다음 단계를 계속합니다.

- 네트워크 조사를 건너뛰려면 다음 단계를 계속합니다.

4단계 **Shared Host Profiles** 옆의 추가 아이콘( )을 클릭합니다.

새 공유 호스트 프로필의 설정이 표시됩니다.

5단계 **Name** 필드에 공유 호스트 프로필을 설명하는 이름을 입력합니다.

6단계 **OS Vendor**, **OS Name**, **Version** 드롭다운 목록에서 공유 호스트 프로필을 생성할 운영 체제 및 버전을 선택합니다.

7단계 허용할 애플리케이션 프로토콜을 지정합니다. 3가지 옵션이 제공됩니다.

- 모든 애플리케이션 프로토콜을 허용하려면 **Allow all Application Protocols** 확인란을 선택합니다.
- 애플리케이션 프로토콜을 허용하지 않으려면 **Allow all Application Protocols** 확인란을 취소한 상태로 둡니다.
- 특정 애플리케이션 프로토콜을 허용하려면 **Allowed Application Protocols** 옆에서 52-16페이지의 애플리케이션 프로토콜을 호스트 프로필에 추가의 지침을 따릅니다.

8단계 허용할 클라이언트를 지정합니다. 3가지 옵션이 제공됩니다.

- 모든 클라이언트를 허용하려면 **Allow all Clients** 확인란을 선택합니다.
- 클라이언트를 허용하지 않으려면 **Allow all Clients** 확인란을 취소한 상태로 둡니다.
- 특정 클라이언트를 허용하려면 52-17페이지의 클라이언트를 호스트 프로필에 추가의 지침을 따릅니다.

9단계 허용할 웹 애플리케이션을 지정합니다. 3가지 옵션이 제공됩니다.

- 모든 웹 애플리케이션을 허용하려면 **Allow all Web Applications** 확인란을 선택합니다.
- 웹 애플리케이션을 허용하지 않으려면 **Allow all Web Applications** 확인란을 취소한 상태로 둡니다.
- 특정 웹 애플리케이션을 허용하려면 52-18페이지의 웹 애플리케이션을 호스트 프로필에 추가의 지침을 따릅니다.

10단계 허용할 프로토콜을 지정합니다.

Allowed Protocols 옆에 프로토콜을 추가하려면 52-18페이지의 프로토콜을 호스트 프로필에 추가의 지침을 따릅니다. ARP, IP, TCP, UDP는 항상 허용됩니다.

11단계 **Save all Profiles**를 클릭하여 변경 사항을 저장합니다.

공유 호스트 프로필이 생성됩니다. 이제 공유 호스트 프로필을 모든 규정준수 화이트리스트에 추가할 수 있습니다.

공유 호스트 프로필 수정

라이센스: FireSIGHT

공유 호스트 프로필을 수정하면 해당 프로필이 속한 모든 화이트리스트의 프로필이 변경됩니다. 공유 호스트 프로필을 사용하는 화이트리스트 및 활성화된 상관관계 정책에서 사용되는 화이트리스트의 경우, 공유 호스트 프로필을 수정하면 호스트의 상태가 규정준수 또는 규정준수 위반으로 바뀔 수 있으나, 화이트리스트 이벤트가 생성되지는 **않습니다**.

다음 표에서는 공유 호스트 프로필을 수정할 경우 수행할 수 있는 작업이 설명되어 있습니다.

표 52-2 공유 호스트 프로필 작업

목적	가능한 작업
호스트 프로필의 이름 변경	**Name** 필드에 새 이름을 입력합니다.
운영 체제 변경	**OS Vendor**, **OS Name**, **Version** 드롭다운 목록에서 새 운영 체제 및 버전을 선택합니다. 이러한 값을 변경할 경우, 호스트 프로필의 이름도 변경하고자 할 수 있습니다.
애플리케이션 프로토콜 추가	52-16페이지의 애플리케이션 프로토콜을 호스트 프로필에 추가의 지침을 따릅니다.
클라이언트 추가	52-17페이지의 클라이언트를 호스트 프로필에 추가의 지침을 따릅니다.
웹 애플리케이션 추가	52-18페이지의 웹 애플리케이션을 호스트 프로필에 추가의 지침을 따릅니다.
프로토콜 추가	52-18페이지의 프로토콜을 호스트 프로필에 추가의 지침을 따릅니다.
모든 애플리케이션 프로토콜 허용	**Allowed Application Protocols** 아래에서 **Allow all Application Protocols** 확인란을 선택합니다. 이전에 허용한 모든 애플리케이션 프로토콜을 삭제할 때까지 이 확인란이 표시되지 않습니다.
모든 클라이언트 허용	**Allowed Clients** 아래에서 **Allow all Clients** 확인란을 선택합니다. 이전에 허용한 모든 클라이언트를 삭제할 때까지 이 확인란이 표시되지 않습니다.
모든 웹 애플리케이션 허용	**Allowed Web Applications** 아래에서 **Allow all Web Applications** 확인란을 선택합니다. 이전에 허용한 모든 클라이언트를 삭제할 때까지 이 확인란이 표시되지 않습니다.
애플리케이션 프로토콜, 클라이언트, 웹 애플리케이션 또는 프로토콜 수정	수정할 요소를 클릭합니다. 사용자가 변경할 수 있는 속성에 대한 자세한 내용은 다음을 참조하십시오. • 52-16페이지의 애플리케이션 프로토콜을 호스트 프로필에 추가 • 52-17페이지의 클라이언트를 호스트 프로필에 추가 • 52-18페이지의 웹 애플리케이션을 호스트 프로필에 추가 • 52-18페이지의 프로토콜을 호스트 프로필에 추가 **참고** 애플리케이션 프로토콜, 클라이언트, 또는 프로토콜에 적용한 변경 사항은 해당 요소를 사용하는 모든 호스트 프로필에 반영됩니다.
애플리케이션 프로토콜, 클라이언트, 웹 애플리케이션 또는 프로토콜 삭제	삭제할 요소 옆의 삭제 아이콘( )을 클릭합니다.
네트워크 조사	**Survey Network**를 클릭합니다. 네트워크를 조사하면 허용된 추가 클라이언트, 애플리케이션 프로토콜, 웹 애플리케이션, 프로토콜을 기존의 호스트 프로필에 추가할 수 있으며, 처음 조사 과정에서 탐지되지 않은 운영 체제를 실행 중인 호스트가 조사에서 탐지될 경우 추가 호스트 프로필을 추가할 수 있습니다. 자세한 내용은 52-9페이지의 네트워크 조사을/를 참조하십시오.

공유 호스트 프로필을 수정하려면

액세스: Admin

1단계 **Policies > Correlation**을 선택한 다음 **White List**를 클릭합니다.

White List 페이지가 나타납니다.

2단계 **Edit Shared Profiles**를 클릭합니다.

Edit Shared Profiles 페이지가 나타납니다.

3단계 내장형 공유 호스트 프로필 중 하나를 수정하시겠습니까?

- yes인 경우, **Built-in Host Profiles**를 확장하여 해당하는 호스트 프로필을 표시합니다.
- no인 경우 다음 단계를 계속합니다.

4단계 수정할 공유 호스트 프로필의 이름을 클릭합니다.

호스트 프로필이 나타납니다.

5단계 52-27 페이지의 표 52-2에 설명된 작업 중 하나를 수행합니다.

6단계 **Save all Profiles**를 클릭하여 변경 사항을 저장합니다.

공유 호스트 프로필이 저장됩니다.

공유 호스트 프로필 삭제

라이센스: FireSIGHT

삭제한 공유 호스트 프로필이 활성화된 상관관계 정책에 사용된 하나 이상의 화이트리스트에 속한 경우, 해당 프로필을 삭제하면 호스트의 상태가 규정준수 위반으로 바뀔 수 있으나 화이트리스트 이벤트는 생성되지 **않습니다**.

팁 기본 화이트리스트에서 사용된 내장형 공유 호스트를 삭제할 경우, 내장형 프로필을 공장 기본값으로 재설정하여 해당 호스트를 복원할 수 있습니다. 자세한 내용은 52-29페이지의 내장형 호스트 프로필을 공장 기본값으로 재설정을/를 참조하십시오.

공유 호스트 프로필을 삭제하려면

액세스: Admin

1단계 **Policies > Correlation**을 선택한 다음 **White List**를 클릭합니다.

White List 페이지가 나타납니다.

2단계 **Edit Shared Profiles**를 클릭합니다.

Edit Shared Profiles 페이지가 나타납니다.

3단계 내장형 공유 호스트 프로필 중 하나를 삭제하시겠습니까?

- yes인 경우, **Built-in Host Profiles**를 확장하여 해당하는 호스트 프로필을 표시합니다.
- no인 경우 다음 단계를 계속합니다.

4단계 삭제할 공유 호스트 프로필의 옆에 있는 삭제 아이콘( )을 클릭합니다.

확인 메시지가 표시되면 공유 호스트 프로필을 삭제할 것임을 확인합니다.

5단계 **Save all Profiles**를 클릭하여 변경 사항을 저장합니다.

공유 호스트 프로필을 사용하는 모든 규정준수 화이트리스트에서 이 프로필이 삭제 및 제거됩니다.

내장형 호스트 프로필을 공장 기본값으로 재설정

라이센스: FireSIGHT

기본 화이트리스트는 *내장형 호스트 프로필*이라고 하는 특수 카테고리의 공유 호스트 프로필을 사용합니다. 내장형 호스트 프로필은 내장형 애플리케이션 프로토콜, 프로토콜, 클라이언트를 사용합니다. 이러한 요소는 기본 화이트리스트 및 사용자가 생성한 사용자 지정 화이트리스트에서 모두 있는 그대로 사용하거나, 요구 사항에 맞게 수정할 수 있습니다. 자세한 내용은 공유 호스트 프로필 이해을/를 참조하십시오.

내장형 프로필, 애플리케이션 프로토콜, 프로토콜, 웹 애플리케이션, 클라이언트에 취소해야 할 변경 사항을 적용한 경우, 공장 기본값으로 재설정할 수 있습니다. 공장 기본값으로 재설정할 경우, 다음과 같은 작업이 이루어집니다.

- 수정한 **모든** 내장형 호스트 프로필, 애플리케이션 프로토콜, 프로토콜, 클라이언트가 공장 기본값으로 재설정됩니다.
- 삭제한 **모든** 내장형 호스트 프로필, 애플리케이션 프로토콜, 프로토콜, 클라이언트가 복원됩니다.
- 활성화된 상관관계 정책에서 사용 중이고, 재설정된 내장형 호스트 프로필, 애플리케이션 프로토콜, 프로토콜, 클라이언트에서 사용 중인 **모든** 화이트리스트(기본 화이트리스트 포함)가 재평가됩니다. 이러한 재평가로 인해 일부 호스트의 상태가 규정준수로 변경될 수 있으나, 화이트리스트 이벤트는 생성되지 않습니다.

내장형 호스트 프로필, 애플리케이션 프로토콜, 프로토콜, 클라이언트를 재설정하려면

액세스: Admin

1단계 **Policies > Correlation**을 선택한 다음 **White List**를 클릭합니다.

White List 페이지가 나타납니다.

2단계 **Edit Shared Profiles**를 클릭합니다.

Edit Shared Profiles 페이지가 나타납니다.

3단계 **Built-in Host Profiles**를 클릭합니다.

Built-in Host Profiles 페이지가 나타납니다.

4단계 **Reset to Factory Defaults**를 클릭합니다.

5단계 **OK**를 클릭하여 공장 기본값으로 재설정할 것임을 확인합니다.

모든 내장형 호스트 프로필, 애플리케이션 프로토콜, 프로토콜, 클라이언트가 공장 기본값으로 재설정됩니다. 활성화된 상관관계 정책에서 사용 중이고, 재설정된 내장형 호스트 프로필, 애플리케이션 프로토콜, 프로토콜, 클라이언트에서 사용 중인 모든 화이트리스트가 재평가됩니다.

화이트리스트 이벤트 작업

라이센스: FireSIGHT

활성화된 상관관계 정책에 포함되어 있는 화이트리스트를 특정 호스트가 위반하는 것으로 나타나는 검색 이벤트가 생성될 경우, 화이트리스트 이벤트가 생성됩니다. 화이트리스트는 특수한 종류의 상관관계 이벤트이며, 상관관계 이벤트 데이터베이스에 로깅됩니다. 화이트리스트 이벤트를 검색, 보기, 삭제할 수 있습니다.

팁 데이터베이스에 저장된 이벤트 수를 구성하는 방법에 대한 자세한 내용은 63-15페이지의 데이터베이스 이벤트 제한 구성을/를 참조하십시오. 화이트리스트 이벤트는 상관관계 이벤트 데이터베이스에 저장됩니다.

자세한 내용은 다음 절을 참조하십시오.

- 52-30페이지의 화이트리스트 이벤트 보기
- 52-31페이지의 화이트리스트 이벤트 테이블 이해
- 52-33페이지의 규정준수 화이트리스트 이벤트 검색

화이트리스트 이벤트 보기

라이센스: FireSIGHT

방어 센터를 사용하여 규정준수 화이트리스트 이벤트의 테이블을 볼 수 있습니다. 그런 다음 찾고 있는 정보에 따라 이벤트 보기를 조작할 수 있습니다.

화이트리스트 이벤트에 액세스할 때 표시되는 페이지는 사용하는 워크플로에 따라 달라집니다. 화이트리스트 이벤트의 테이블 보기가 포함된 미리 정의된 워크플로를 사용할 수 있습니다. 특정 요구와 일치하는 정보만 표시하는 사용자 지정 워크플로를 생성할 수도 있습니다. 사용자 지정 워크플로 생성에 대한 자세한 내용은 58-38페이지의 사용자 지정 워크플로 생성을/를 참조하십시오.

다음 표에는 화이트리스트 이벤트 워크플로 페이지에서 수행할 수 있는 몇 가지 특정 작업이 설명되어 있습니다.

표 52-3 규정준수 화이트리스트 이벤트 작업

목적	가능한 작업
호스트에 대한 호스트 프로필 보기	IP 주소 옆에 표시되는 호스트 프로필 아이콘( )을 입력합니다.
사용자 프로필 정보 보기	사용자 ID 옆에 표시되는 사용자 아이콘( )을 클릭합니다. 자세한 내용은 50-63페이지의 사용자 세부사항 및 호스트 기록 이해을/를 참조하십시오.
현재 워크플로 페이지에서 이벤트를 정렬 및 제한	58-34페이지의 드릴다운 워크플로 페이지 정렬에서 자세히 알아보십시오.
현재 워크플로 페이지 내에서 이동	58-35페이지의 워크플로의 다른 페이지로 이동에서 자세히 알아보십시오.
현재의 제약 조건을 유지한 채 현재 워크플로에서 페이지 간 이동	워크플로 페이지의 왼쪽 위에서 적절한 페이지 링크를 클릭합니다. 자세한 내용은 58-18페이지의 워크플로 페이지 사용을/를 참조하십시오.
나타나는 열에 대해 자세히 알아보기	52-31페이지의 화이트리스트 이벤트 테이블 이해에서 자세히 알아보십시오.
표시된 이벤트에 대한 시간 및 날짜 범위 수정	58-22페이지의 이벤트 시간 제약 조건 설정에서 자세히 알아보십시오.

표 52-3 규정준수 화이트리스트 이벤트 작업 (계속)

목적	가능한 작업
워크플로의 다음 페이지로 드릴다운하여 특정 값으로 제한	다음 방법 중 하나를 사용합니다. • 사용자 지정 워크플로에서 생성한 드릴다운 페이지에서 행 내의 값을 클릭합니다. 테이블 보기의 행 내에서 값을 클릭하면 테이블 보기가 제한되며 다음 페이지로 드릴다운되지 **않습니다**. • 일부 사용자로 제한하여 다음 워크플로 페이지로 드릴다운하려면, 다음 워크플로 페이지에서 볼 사용자의 옆에 있는 확인란을 선택하고 **View**를 클릭합니다. • 현재의 제약 조건을 유지한 채 다음 워크플로 페이지로 드릴다운하려면 **View All**을 클릭합니다. **팁** 테이블 보기의 페이지 이름에는 항상 "Table View"가 포함됩니다. 자세한 내용은 58-30페이지의 이벤트 제한을/를 참조하십시오.
시스템에서 화이트리스트 이벤트 삭제	다음 방법 중 하나를 사용합니다. • 일부 이벤트를 삭제하려면 삭제할 이벤트 옆의 확인란을 선택한 다음 **Delete**를 클릭합니다. • 현재 제한된 보기에서 모든 이벤트를 삭제하려면 **Delete All**을 클릭하고 모든 이벤트를 삭제할 것인지를 확인합니다.
관련 이벤트를 보기 위해 다른 이벤트 보기로 이동	58-35페이지의 워크플로 간 이동에서 자세히 알아보십시오.

규정준수 화이트리스트 이벤트를 보려면

액세스: Admin/Any Security Analyst/Discovery Admin

1단계 **Analysis > Correlation > White List Events**를 선택합니다.

기본 화이트리스트 워크플로의 첫 번째 페이지가 나타납니다. 사용자 지정 워크플로를 비롯하여 다른 워크플로를 사용하려면 워크플로 제목을 기준으로 **(switch workflow)**를 클릭합니다. 다른 기본 워크플로 지정에 대한 자세한 내용은 71-3페이지의 이벤트 보기 설정 구성을/를 참조하십시오. 이벤트가 표시되지 않을 경우 시간 범위를 조정해야 할 수 있습니다. 58-22페이지의 이벤트 시간 제약 조건 설정을/를 참조하십시오.

화이트리스트 이벤트 테이블 이해

라이센스: FireSIGHT

상관관계 정책 기능을 사용하여 네트워크의 위협에 실시간으로 대응하는 *상관관계 정책*을 만들 수 있습니다. 상관관계 정책은 규정준수 화이트리스트 위반을 비롯하여 정책 위반을 구성하는 작업의 유형을 설명합니다. 상관관계 정책에 대한 자세한 내용은 51-1페이지의 상관관계 정책 및 규칙 구성을/를 참조하십시오.

규정준수 화이트리스트를 위반할 경우, 시스템에서 화이트리스트 이벤트가 생성됩니다. 화이트리스트 이벤트 테이블의 필드는 다음 표에 설명되어 있습니다.

표 52-4 규정준수 화이트리스트 이벤트 필드

필드	설명
Time	화이트리스트 이벤트가 생성된 시간 및 날짜입니다.
IP Address	규정준수 위반 호스트의 IP 주소입니다.
User	규정준수 위반 호스트에 로그인한 모든 알려진 사용자의 ID입니다.
Port	애플리케이션 프로토콜 화이트리스트 위반(규정준수를 위반한 애플리케이션 프로토콜로 인해 발생한 위반)을 트리거한 이벤트와 관련된 포트입니다. 다른 유형의 화이트리스트 위반의 경우, 이 필드는 빈 칸입니다.

Description	화이트리스트를 어떤 식으로 위반했는지 설명합니다. 예를 들면 다음과 같습니다.
	`Client "AOL Instant Messenger" is not allowed.`
	애플리케이션 프로토콜 이름과 버전, 그리고 해당 프로토콜이 사용 중인 포트 및 프로토콜(TCP 또는 UDP)을 나타내는 애플리케이션 프로토콜과 관련된 위반입니다. 특정 운영 체제에 대한 금지를 제한할 경우, 설명에는 운영 체제 이름이 포함됩니다. 예를 들면 다음과 같습니다.
	`Server "ssh / 22 TCP ( OpenSSH 3.6.1p2 )" is not allowed on Operating System "Linux Linux 2.4 or 2.6".`

Policy	위반된 상관관계 정책의 이름입니다. 즉, 화이트리스트가 포함된 상관관계 정책입니다.
White List	화이트리스트의 이름입니다.
Priority	정책 또는 정책 위반을 트리거한 화이트리스트에 의해 지정된 우선순위입니다. 상관관계 규칙 및 정책 우선순위 설정에 대한 자세한 내용은 51-46페이지의 기본 정책 정보 제공 및 51-48페이지의 규칙 및 화이트리스트 우선순위 설정을/를 참조하십시오.
Host Criticality	화이트리스트를 준수하지 않는 호스트에 대해 사용자가 할당하는 호스트 중요도(`None`, `Low`, `Medium`, `High`)입니다. 호스트 중요도에 대한 자세한 내용은 49-30페이지의 사전 정의 호스트 특성 작업을/를 참조하십시오.
Device	화이트리스트 위반이 탐지된 매니지드 디바이스의 이름입니다.
Count	각 행에 표시되는 정보와 매칭되는 이벤트의 수입니다. 둘 이상의 동일한 행을 생성하는 제약 조건을 적용한 경우에만 Count 필드가 나타납니다.

규정준수 화이트리스트 이벤트 검색

라이센스: FireSIGHT

특정 규정준수 화이트리스트 이벤트를 검색할 수 있습니다. 네트워크 환경에 맞춤화된 검색을 생성한 다음, 이를 저장하여 나중에 사용할 수 있습니다. 다음 표에는 사용할 수 있는 검색 기준이 설명되어 있습니다.

표 52-5 규정준수 화이트리스트 이벤트 검색 기준

필드	검색 기준 규칙
Policy	상관관계 정책에 포함된 화이트리스트 위반으로 인해 발생한 모든 이벤트를 반환하는 상관관계 정책의 이름을 입력합니다.
White List	화이트리스트 위반으로 인해 발생한 모든 이벤트를 반환하는 화이트리스트의 이름을 입력합니다.
Description	화이트리스트 이벤트 설명을 입력합니다.
Priority	화이트리스트 이벤트의 우선순위를 지정합니다. 이는 상관관계 정책에 포함된 화이트리스트의 우선순위 또는 상관관계 정책 자체의 우선순위에 의해 결정됩니다. 화이트리스트 우선순위는 해당 정책의 우선순위를 재정의합니다. 우선순위가 없는 경우 none을 입력합니다. 상관관계 규칙 및 정책 우선순위 설정에 대한 자세한 내용은 51-46페이지의 기본 정책 정보 제공 및 51-48페이지의 규칙 및 화이트리스트 우선순위 설정을/를 참조하십시오.
IP Address	화이트리스트를 준수하지 않는 위반 상태가 된 호스트의 IP 주소를 지정합니다.
User	화이트리스트를 준수하지 않는 위반 상태가 된 호스트에 로그인한 사용자의 ID를 지정합니다.
Port	애플리케이션 프로토콜 화이트리스트 위반(규정준수를 위반한 애플리케이션 프로토콜로 인해 발생한 위반)을 트리거한 검색 이벤트와 관련된 포트를 지정합니다.
Host Criticality	화이트리스트 이벤트와 관련된 소스 호스트의 호스트 중요도를 None, Low, Medium, High로 지정합니다. 호스트 중요도에 대한 자세한 내용은 49-30페이지의 사전 정의 호스트 특성 작업을/를 참조하십시오.
Device	디바이스 이름 또는 IP 주소, 디바이스 그룹, 스택, 클러스터 이름을 입력하여 화이트리스트 위반이 탐지된 특정 디바이스에 대한 검색을 제한합니다. FireSIGHT 시스템에서 검색 시 디바이스 필드를 처리하는 방법에 대한 자세한 내용은 60-7페이지의 검색에서 디바이스 지정을/를 참조하십시오.

규정준수 화이트리스트 이벤트를 검색하려면

액세스: Admin/Any Security Analyst

1단계 **Analysis > Search**를 선택합니다.

Search 페이지가 나타납니다.

2단계 테이블 드롭다운 목록에서 **White List Events**를 선택합니다.

해당 제약 조건으로 페이지가 업데이트됩니다.

3단계 52-33 페이지의 표 52-5에 설명된 해당 필드에 검색 기준을 입력하며, 다음과 같은 추가적인 주의사항을 숙지하십시오.

- 모든 필드에 부정(!)을 사용할 수 있습니다.
- 모든 필드에 쉼표로 구분된 검색 값의 목록을 사용할 수 있습니다. 지정된 필드에 나열된 값 중 하나를 포함하는 레코드는 검색 기준과 일치합니다.
- 모든 필드에 따옴표로 감싸고 쉼표로 구분한 목록을 검색 값으로 사용할 수 있습니다.
  - 단일 값만을 포함할 수 있는 필드의 경우, 따옴표 내에 지정된 정확한 문자열을 포함하는 지정된 필드의 레코드가 검색 기준과 일치합니다. 예를 들어 `A, B, "C, D, E"`에 대한 검색은 지정된 필드에 `"A"` 또는 `"B"` 또는 `"C, D, E"`가 포함된 레코드와 일치합니다. 따라서 가능한 값으로 쉼표를 포함하는 필드에서 일치를 확인할 수 있습니다.
  - 여러 값을 동시에 포함할 수 있는 필드의 경우, 따옴표로 감싸고 쉼표로 구분한 모든 값을 포함하는 지정된 필드의 레코드가 해당 검색 기준과 일치합니다.
  - 여러 값을 동시에 포함할 수 있는 필드의 경우, 검색 기준에 단일 값은 물론 따옴표로 감싸고 쉼표로 구분한 목록도 포함할 수 있습니다. 예를 들어 하나 이상의 이러한 문자를 포함할 수 있는 필드에서 `A, B, "C, D, E"`에 대한 검색은 지정된 필드에 `A` 또는 `B`, 또는 `C`, `D`, `E` 모두가 포함된 레코드와 일치합니다.
- 검색 결과에는 모든 필드에 지정된 검색 기준과 매칭되는 레코드만 반환됩니다.
- 많은 필드에서 와일드카드로 하나 이상의 별표(*)를 사용할 수 있습니다.
- 해당 필드에 대해 사용할 수 있는 정보가 없는 이벤트를 식별하려면 필드에 `n/a`를 지정합니다. 해당 필드가 채워지는 이벤트를 식별하려면 `!n/a`를 사용합니다.
- 검색 기준으로 객체를 사용하려면 검색 필드 옆에 나타나는 객체 추가 아이콘(+)을 클릭합니다.

검색에서 객체를 사용하는 방법을 포함하여 검색 구문에 대한 자세한 내용은 60-1페이지의 이벤트 검색을/를 참조하십시오.

4단계 선택적으로, 검색을 저장하려면 **Private** 확인란을 선택하여 자신만 액세스할 수 있는 비공개로 검색을 저장할 수 있습니다. 또는 모든 사용자가 사용할 수 있도록 검색을 저장하려면 확인란을 선택하지 않습니다.

팁 사용자 지정 사용자 역할에 대한 데이터 제한으로서 검색을 사용하려면 **반드시** 비공개 검색으로 저장해야 합니다.

5단계 선택적으로, 나중에 다시 사용할 수 있도록 검색을 저장할 수 있습니다. 다음 옵션을 이용할 수 있습니다.

- 검색 기준을 저장하려면 **Save**를 클릭합니다.

  새 검색인 경우 검색 이름을 입력하도록 대화 상자가 나타납니다. 고유한 검색 이름을 입력하고 **Save**를 클릭합니다. 이미 존재하는 검색에 대한 새 조건을 저장하는 경우 프롬프트가 나타나지 않습니다. 나중에 실행할 수 있도록 검색이 저장됩니다(**Private**을 선택한 경우 자신만 볼 수 있음).
- 새 검색을 저장하거나, 저장된 기존 검색을 변경하여 만든 검색에 새 이름을 할당하려면 **Save As New**를 클릭합니다.

  검색 이름을 입력하도록 대화 상자가 나타납니다. 고유한 검색 이름을 입력하고 **Save**를 클릭합니다. 나중에 실행할 수 있도록 검색이 저장됩니다(**Private**을 선택한 경우 자신만 볼 수 있음).

6단계 검색을 시작하려면 **Search**를 클릭합니다.

검색 결과가 기본 화이트리스트 이벤트 워크플로에 표시되며, 현재 시간 범위로 제한됩니다. 사용자 지정 워크플로를 비롯한 다른 워크플로를 사용하려면 워크플로 제목 옆의 **(switch workflow)**를 클릭합니다. 다른 기본 워크플로 지정에 대한 자세한 내용은 71-3페이지의 이벤트 보기 설정 구성을/를 참조하십시오.

화이트리스트 위반 작업

라이센스: FireSIGHT

시스템에서는 네트워크의 호스트가 활성화된 상관관계 정책의 규정준수 화이트리스트를 어떤 경위로 위반하는지 지속적으로 추적합니다. 이러한 레코드를 검색하고 볼 수 있습니다.

자세한 내용은 다음 절을 참조하십시오.

- 52-35페이지의 화이트리스트 위반 보기
- 52-36페이지의 화이트리스트 위반 테이블 이해
- 52-37페이지의 화이트리스트 위반 검색

화이트리스트 위반 보기

라이센스: FireSIGHT

방어 센터를 사용하여 화이트리스트 위반에 대한 테이블을 볼 수 있습니다. 그런 다음 찾고 있는 정보에 따라 이벤트 보기를 조작할 수 있습니다. 화이트리스트 위반에 액세스할 때 표시되는 페이지는 사용하는 워크플로에 따라 달라집니다. 미리 정의된 2가지 워크플로가 제공됩니다.

- Host Violation Count 워크플로는 최소 하나 이상의 화이트리스트를 위반한 모든 호스트가 나열된 페이지를 제공합니다. 첫 번째 페이지는 호스트당 위반 횟수를 기준으로 호스트를 정렬하며, 위반 횟수가 가장 많은 호스트가 목록의 맨 위에 표시됩니다. 호스트가 여러 개의 화이트리스트를 위반할 경우, 위반된 화이트리스트마다 별도의 행이 제공됩니다. 이 워크플로에는 가장 최근에 탐지된 모든 위반이 목록의 맨 위에 나열된 화이트리스트 위반의 테이블 보기도 포함되어 있습니다. 테이블의 각 행에는 탐지된 위반 사항이 하나씩 포함되어 있습니다.
- White List Violations 워크플로에는 가장 최근에 탐지된 모든 위반이 목록의 맨 위에 나열된 화이트리스트 위반의 테이블 보기가 포함되어 있습니다. 테이블의 각 행에는 탐지된 위반 사항이 하나씩 포함되어 있습니다.

미리 정의된 두 워크플로는 사용자의 제한 사항을 충족하는 모든 호스트에 대한 호스트 프로필이 포함된 호스트 보기에서 종료됩니다. 특정 요구와 일치하는 정보만 표시하는 사용자 지정 워크플로를 생성할 수도 있습니다. 자세한 내용은 58-38페이지의 사용자 지정 워크플로 생성을/를 참조하십시오.

다음 표에는 화이트리스트 위반 워크플로 페이지에서 수행할 수 있는 몇 가지 특정 작업이 설명되어 있습니다.

표 52-6 규정준수 화이트리스트 위반 작업

목적	가능한 작업
호스트에 대한 호스트 프로필 보기	IP 주소 옆에 표시되는 호스트 프로필 아이콘( )을 입력합니다.
현재 워크플로 페이지에서 이벤트를 정렬 및 제한	58-34페이지의 드릴다운 워크플로 페이지 정렬에서 자세히 알아보십시오.

표 52-6 규정준수 화이트리스트 위반 작업 (계속)

목적	가능한 작업
현재 워크플로 페이지 내에서 이동	58-35페이지의 워크플로의 다른 페이지로 이동에서 자세히 알아보십시오.
현재의 제약 조건을 유지한 채 현재 워크플로에서 페이지 간 이동	워크플로 페이지의 왼쪽 위에서 적절한 페이지 링크를 클릭합니다. 자세한 내용은 58-18페이지의 워크플로 페이지 사용을/를 참조하십시오.
나타나는 열에 대해 자세히 알아보기	52-36페이지의 화이트리스트 위반 테이블 이해에서 자세히 알아보십시오.
워크플로의 다음 페이지로 드릴다운	다음 방법 중 하나를 사용합니다. • 특정 값으로 제한하여 다음 워크플로 페이지로 드릴다운하려면 행 내의 값을 클릭합니다. 이 방법은 드릴다운 페이지에만 해당됩니다. 테이블 보기의 행 내에서 값을 클릭하면 테이블 보기가 제한되며 다음 페이지로 드릴다운되지 **않습니다**. • 일부 이벤트로 제한하여 다음 워크플로 페이지로 드릴다운하려면, 다음 워크플로 페이지에서 볼 이벤트의 옆에 있는 확인란을 선택하고 **View**를 클릭합니다. • 현재의 제약 조건을 유지한 채 다음 워크플로 페이지로 드릴다운하려면 **View All**을 클릭합니다. **팁** 테이블 보기의 페이지 이름에는 항상 "Table View"가 포함됩니다. 자세한 내용은 58-30페이지의 이벤트 제한을/를 참조하십시오.
관련 이벤트를 보기 위해 다른 이벤트 보기로 이동	58-35페이지의 워크플로 간 이동에서 자세히 알아보십시오.

규정준수 화이트리스트 위반을 보려면

액세스: Admin/Any Security Analyst/Discovery Admin

1단계 **Analysis > Correlation > White List Violations**를 선택합니다.

기본 화이트리스트 위반 워크플로의 첫 번째 페이지가 나타납니다. 사용자 지정 워크플로를 비롯한 다른 워크플로를 사용하려면 워크플로 제목 옆의 **(switch workflow)**를 클릭합니다. 다른 기본 워크플로 지정에 대한 자세한 내용은 71-3페이지의 이벤트 보기 설정 구성을/를 참조하십시오.

화이트리스트 위반 테이블 이해

라이센스: FireSIGHT

상관관계 정책 기능을 사용하여 네트워크의 위협에 실시간으로 대응하는 *상관관계 정책*을 만들 수 있습니다. 상관관계 정책은 규정준수 화이트리스트 위반을 비롯하여 정책 위반을 구성하는 작업의 유형을 설명합니다. 상관관계 정책에 대한 자세한 내용은 51-1페이지의 상관관계 정책 및 규칙 구성을/를 참조하십시오.

규정준수 화이트리스트를 위반할 경우, 시스템에서 해당 위반 사항을 기록합니다. 테이블 보기에는 네트워크의 현재 호스트 위반 사항만 표시되므로, 테이블 보기에서 이벤트 시간 제한을 설정할 수 없습니다. 화이트리스트 위반 테이블의 필드는 다음 표에 설명되어 있습니다.

표 52-7 규정준수 화이트리스트 위반 필드

필드	설명
Time	화이트리스트 위반이 감지된 시간 및 날짜입니다.
IP Address	규정준수 위반 호스트의 관련 IP 주소입니다.
Type	화이트리스트 위반의 유형입니다. 즉, 규정준수 위반으로 인해 발생한 위반인지 나타냅니다. • 운영 체제(**os**) • 애플리케이션 프로토콜(**server**) • 클라이언트(**client**) • 프로토콜(**protocol**) • 웹 애플리케이션(**web**)
Information	화이트리스트 위반과 관련하여 제공되는 모든 공급업체, 제품 또는 버전 정보입니다. 예를 들어, Microsoft Windows 호스트만 허용하는 화이트리스트를 보유한 경우 Information 필드에는 Microsoft Windows를 실행 중이 아닌 호스트의 운영 체제가 설명됩니다. 화이트리스트를 위반한 프로토콜의 경우, Information 필드에 해당 위반이 네트워크로 인한 것인지 전송 프로토콜로 인한 것인지 표시됩니다.
Port	애플리케이션 프로토콜 화이트리스트 위반(규정준수를 위반한 애플리케이션 프로토콜로 인해 발생한 위반)을 트리거한 이벤트와 관련된 포트입니다. 다른 유형의 화이트리스트 위반의 경우, 이 필드는 빈 칸입니다.
Protocol	애플리케이션 프로토콜 화이트리스트 위반(규정준수를 위반한 애플리케이션 프로토콜로 인해 발생한 위반)을 트리거한 이벤트와 관련된 프로토콜입니다. 다른 유형의 화이트리스트 위반의 경우, 이 필드는 빈 칸입니다.
White List	위반된 화이트리스트의 이름입니다.
Count	각 행에 표시되는 정보와 매칭되는 이벤트의 수입니다. 둘 이상의 동일한 행을 생성하는 제약 조건을 적용한 경우에만 Count 필드가 나타납니다.

화이트리스트 위반 검색

라이센스: FireSIGHT

특정 규정준수 화이트리스트 위반을 검색할 수 있습니다. 네트워크 환경에 맞춤화된 검색을 생성한 다음, 이를 저장하여 나중에 사용할 수 있습니다. 다음 표에는 사용할 수 있는 검색 기준이 설명되어 있습니다.

표 52-8 규정준수 화이트리스트 위반 검색 기준

필드	검색 기준 규칙
시간	화이트리스트 위반이 감지된 시간 및 날짜를 지정합니다.
IP 주소	화이트리스트를 준수하지 않는 위반 상태가 된 호스트의 IP 주소를 지정합니다.

표 52-8 규정준수 화이트리스트 위반 검색 기준 (계속)

필드	검색 기준 규칙
White List	화이트리스트의 모든 위반을 반환하는 화이트리스트의 이름을 입력합니다.
유형	화이트리스트 위반의 유형을 입력합니다. • `os`(또는 `operating system`)를 입력하여 운영 체제를 기준으로 위반을 검색합니다. • `server`를 입력하여 애플리케이션 프로토콜을 기준으로 위반을 검색합니다. • `client`를 입력하여 클라이언트를 기준으로 위반을 검색합니다. • `protocol`을 입력하여 프로토콜을 기준으로 위반을 검색합니다. • `web application`을 입력하여 웹 애플리케이션을 기준으로 위반을 검색합니다.
정보	화이트리스트 위반 정보를 입력합니다.
포트	애플리케이션 프로토콜 화이트리스트 위반(규정준수를 위반한 애플리케이션 프로토콜로 인해 발생한 위반)을 트리거한 검색 이벤트와 관련된 포트를 지정합니다.
프로토콜	애플리케이션 프로토콜 화이트리스트 위반(규정준수를 위반한 애플리케이션 프로토콜로 인해 발생한 위반)을 트리거한 검색 이벤트와 관련된 프로토콜을 지정합니다.

규정준수 화이트리스트 위반을 검색하려면

액세스: Admin/Any Security Analyst

1단계 **Analysis > Search**를 선택합니다.

Search 페이지가 나타납니다.

2단계 테이블 드롭다운 목록에서 **White List Violations**를 선택합니다.

해당 제약 조건으로 페이지가 업데이트됩니다.

3단계 규정준수 화이트리스트 이벤트 검색 기준 테이블에 설명된 해당 필드에 검색 기준을 입력하며, 다음과 같은 추가적인 주의 사항을 숙지하십시오.

- 모든 필드에 부정(`!`)을 사용할 수 있습니다.
- 모든 필드에 쉼표로 구분된 검색 값의 목록을 사용할 수 있습니다. 지정된 필드에 나열된 값 중 하나를 포함하는 레코드는 검색 기준과 일치합니다.
- 모든 필드에 따옴표로 감싸고 쉼표로 구분한 목록을 검색 값으로 사용할 수 있습니다.
  - 단일 값만을 포함할 수 있는 필드의 경우, 따옴표 내에 지정된 정확한 문자열을 포함하는 지정된 필드의 레코드가 검색 기준과 일치합니다. 예를 들어 `A, B, "C, D, E"`에 대한 검색은 지정된 필드에 `"A"` 또는 `"B"` 또는 `"C, D, E"`가 포함된 레코드와 일치합니다. 따라서 가능한 값으로 쉼표를 포함하는 필드에서 일치를 확인할 수 있습니다.
  - 여러 값을 동시에 포함할 수 있는 필드의 경우, 따옴표로 감싸고 쉼표로 구분한 모든 값을 포함하는 지정된 필드의 레코드가 해당 검색 기준과 일치합니다.
  - 여러 값을 동시에 포함할 수 있는 필드의 경우, 검색 기준에 단일 값은 물론 따옴표로 감싸고 쉼표로 구분한 목록도 포함할 수 있습니다. 예를 들어 하나 이상의 이러한 문자를 포함할 수 있는 필드에서 `A, B, "C, D, E"`에 대한 검색은 지정된 필드에 `A` 또는 `B`, 또는 `C`, `D`, `E` 모두가 포함된 레코드와 일치합니다.

- 검색 결과에는 모든 필드에 지정된 검색 기준과 매칭되는 레코드만 반환됩니다.
- 많은 필드에서 와일드카드로 하나 이상의 별표(*)를 사용할 수 있습니다.
- 해당 필드에 대해 사용할 수 있는 정보가 없는 이벤트를 식별하려면 필드에 n/a를 지정합니다. 해당 필드가 채워지는 이벤트를 식별하려면 !n/a를 사용합니다.
- 검색 기준으로 객체를 사용하려면 검색 필드 옆에 나타나는 객체 추가 아이콘(+)을 클릭합니다.

검색에서 객체를 사용하는 방법을 포함하여 검색 구문에 대한 자세한 내용은 60-1페이지의 이벤트 검색을/를 참조하십시오.

4단계 선택적으로, 검색을 저장하려면 **Private** 확인란을 선택하여 자신만 액세스할 수 있는 비공개로 검색을 저장할 수 있습니다. 또는 모든 사용자가 사용할 수 있도록 검색을 저장하려면 확인란을 선택하지 않습니다.

팁 사용자 지정 사용자 역할에 대한 데이터 제한으로서 검색을 사용하려면 **반드시** 비공개 검색으로 저장해야 합니다.

5단계 선택적으로, 나중에 다시 사용할 수 있도록 검색을 저장할 수 있습니다. 다음 옵션을 이용할 수 있습니다.

- 검색 기준을 저장하려면 **Save**를 클릭합니다.

  새 검색인 경우 검색 이름을 입력하도록 대화 상자가 나타납니다. 고유한 검색 이름을 입력하고 **Save**를 클릭합니다. 이미 존재하는 검색에 대한 새 조건을 저장하는 경우 프롬프트가 나타나지 않습니다. 나중에 실행할 수 있도록 검색이 저장됩니다(**Private**을 선택한 경우 자신만 볼 수 있음).
- 새 검색을 저장하거나, 저장된 기존 검색을 변경하여 만든 검색에 새 이름을 할당하려면 **Save As New**를 클릭합니다.

  검색 이름을 입력하도록 대화 상자가 나타납니다. 고유한 검색 이름을 입력하고 **Save**를 클릭합니다. 나중에 실행할 수 있도록 검색이 저장됩니다(**Private**을 선택한 경우 자신만 볼 수 있음).

6단계 검색을 시작하려면 **Search**를 클릭합니다.

검색 결과가 기본 화이트리스트 위반 워크플로에 표시됩니다. 사용자 지정 워크플로를 비롯한 다른 워크플로를 사용하려면 워크플로 제목 옆의 **(switch workflow)**를 클릭합니다. 다른 기본 워크플로 지정에 대한 자세한 내용은 71-3페이지의 이벤트 보기 설정 구성을/를 참조하십시오.

53장

트래픽 프로필 생성

트래픽 프로필은 사용자 지정 시간 범위에 수집된 연결 데이터를 기반으로 하는 네트워크 트래픽의 프로필입니다. 디바이스에서 수집한 연결 데이터, NetFlow 지원 디바이스에서 내보낸 연결 데이터, 또는 둘 다 사용할 수 있습니다.

트래픽 프로필을 생성한 다음, 정상적인 네트워크 트래픽을 나타내는 이 프로필과 비교하여 신규 트래픽을 평가함으로써 비정상적인 네트워크 트래픽을 탐지할 수 있습니다.

FireSIGHT 시스템에서는 연결 데이터를 사용하여 트래픽 프로필을 생성하고 트래픽 프로필 변경에 따라 상관성 규칙을 트리거합니다. 방어 센터 데이터베이스에 로깅하지 않는 연결은 트래픽 프로필에 포함할 수 없습니다. 연결 종료(end-of-connection) 데이터만을 사용하여 연결 요약을 채우며(39-3페이지의 연결 요약 이해 참조), 이는 연결 그래프 및 트래픽 프로필 생성에 사용됩니다. 따라서 트래픽 프로필을 생성하고 사용하려는 경우, 연결 종료 시 연결 이벤트를 로깅해야 합니다.

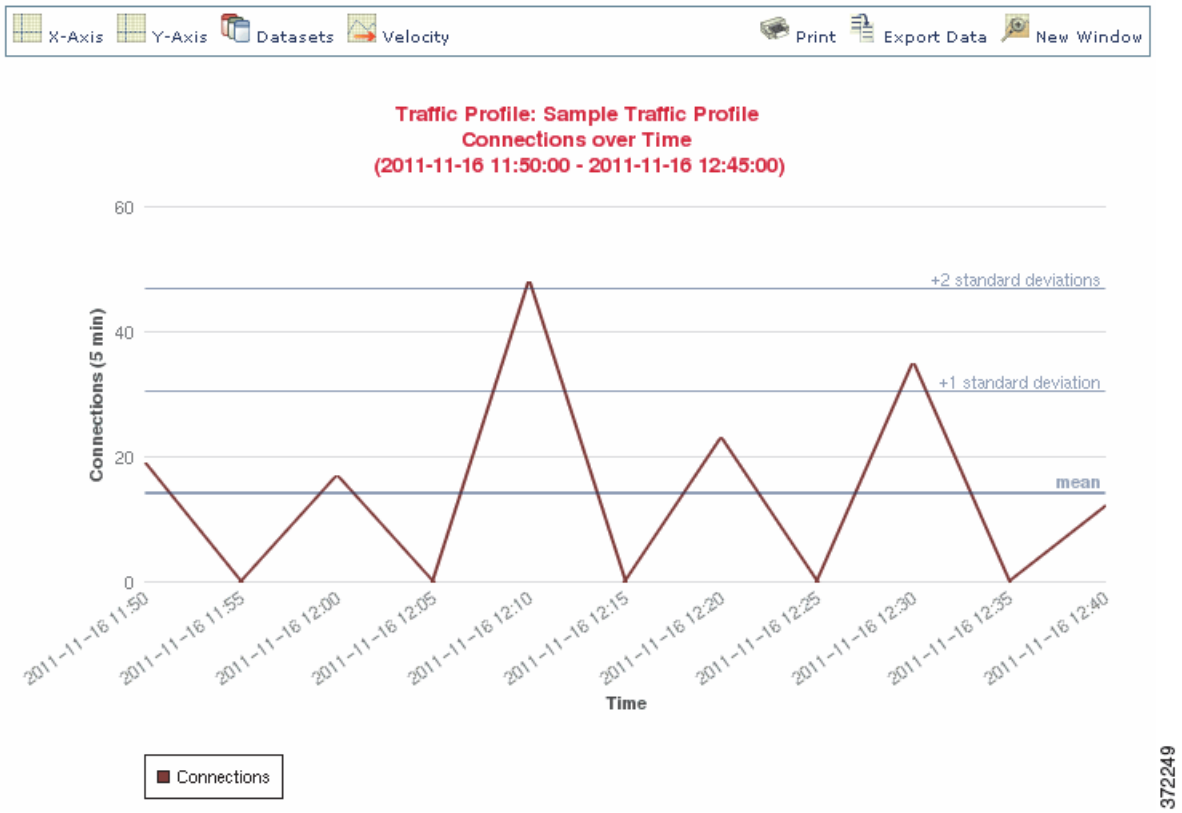
트래픽 프로필 작성을 위한 데이터 수집에 사용되는 시간 범위를 PTW(profiling time window)라고 합니다. PTW는 슬라이딩 윈도우입니다. 즉 PTW가 1주(기본값)일 경우 트래픽 프로필은 지난주에 수집한 연결 데이터를 포함합니다. PTW를 1시간으로 짧게 또는 몇 주로 길게 변경할 수도 있습니다.

트래픽 프로필을 처음 활성화하면 PTW와 동일한 시간의 학습 기간에 대해 사용자가 설정한 기준에 따라 연결 데이터를 수집하고 평가합니다. 방어 센터에서는 학습 기간이 끝날 때까지는 사용자가 작성한 규칙을 트래픽 프로필과 비교하여 평가하지 않습니다.

모니터링되는 네트워크 세그먼트의 모든 트래픽을 사용하여 프로필을 생성하거나 연결 이벤트의 데이터에 기반을 둔 기준을 사용하여 더 명확한 대상의 프로필을 생성할 수 있습니다. 이를테면 탐지된 세션에서 특정 포트, 프로토콜 또는 애플리케이션을 사용할 경우에만 트래픽 프로필에서 데이터를 수집하도록 프로필 조건을 설정할 수 있습니다. 또는 호스트 중요도가 **high**인 호스트에 대한 데이터만 수집하도록 트래픽 프로필에 호스트 프로필 자격을 추가할 수 있습니다.

트래픽 프로필을 생성할 때 비활성 기간을 지정할 수도 있습니다. 이 기간에는 연결 데이터가 프로필 통계에 영향을 주지 않고, 프로필에 대해 작성된 규칙이 트리거되지 않습니다. 트래픽 프로필을 종합하고 수집된 연결 데이터에 대한 통계를 계산하는 빈도를 변경할 수도 있습니다.

다음 그림은 PTW가 1일, 샘플링 속도가 5분인 트래픽 프로필을 보여줍니다.



트래픽 프로필을 생성하고 활성화한 다음 그 학습 기간이 끝나면 비정상적 트래픽 탐지 시 트리거되는 상관관계 규칙을 생성할 수 있습니다. 예를 들어 네트워크를 지나는 데이터의 양(패킷, KByte 또는 연결 수 단위로 측정됨)이 급증하여 트래픽 평균량보다 표준 편차의 3배만큼 많아질 때(공격이나 기타 보안 정책 위반의 징후일 수 있음) 트리거되는 규칙을 작성할 수 있습니다. 그런 다음 상관관계 정책에 그 규칙을 포함시켜 트래픽 급증을 알리거나 그에 대한 대응으로 개선 조치를 수행할 수 있습니다. 비정상적인 네트워크 트래픽을 탐지하기 위해 트래픽 프로필을 사용하는 것에 대한 자세한 내용은 51-3페이지의 상관관계 정책에 대한 규칙 생성을/를 참조하십시오.

Traffic Profiles 페이지에서 트래픽 프로필을 생성할 수 있습니다. 각 프로필 옆의 슬라이더 아이콘은 프로필의 활성 여부를 나타냅니다. 트래픽 프로필의 변경을 상관관계 규칙의 기준으로 삼으려면 프로필을 활성화해야 합니다. 슬라이더 아이콘이 파란색이고 체크 표시가 있을 경우 프로필은 활성 상태입니다. 회색이고 x 표시가 있으면 프로필은 비활성 상태입니다. 자세한 내용은 53-9페이지의 트래픽 프로필 활성화 및 비활성화을/를 참조하십시오.

진행 표시줄은 트래픽 프로필의 학습 기간 상태를 보여줍니다. 진행 표시줄이 100%에 도달하면 프로필에 대해 작성된 상관관계 규칙이 트리거됩니다.

팁

Sort by 드롭다운 목록을 사용하여 트래픽 프로필을 상태 순으로(활성/비활성) 또는 이름 알파벳순으로 정렬할 수 있습니다.

자세한 내용은 다음 링크를 참조하십시오.

- 53-3페이지의 기본 프로필 정보 제공
- 53-3페이지의 트래픽 프로필 조건 지정
- 53-5페이지의 호스트 프로필 자격 추가

기본 프로필 정보 제공

라이센스: FireSIGHT

트래픽 프로필을 생성할 때 이름을 지정하고 선택 사항으로 간단한 설명을 입력해야 합니다.

트래픽 프로필 생성을 시작하려면

액세스: Admin/Discovery Admin

1단계 **Policies > Correlation**을 선택한 다음 **Traffic Profiles**를 클릭합니다.

Traffic Profiles 페이지가 나타납니다.

2단계 **New Profile**을 클릭합니다.

Create Profile 페이지가 나타납니다.

3단계 **Profile Name** 필드에 새 트래픽 프로필의 이름을 255자 이하로 입력합니다.

4단계 **Profile Description** 필드에 새 트래픽 프로필에 대한 간단한 설명을 255자 이하로 입력합니다.

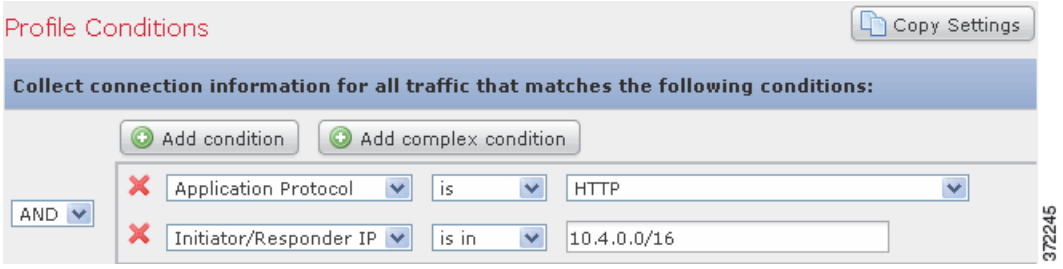
5단계 트래픽 프로필 조건 지정에서 계속하십시오.

트래픽 프로필 조건 지정

라이센스: FireSIGHT

프로필 조건은 트래픽 프로필에서 추적할 연결 데이터의 종류를 제한합니다. 모니터링되는 네트워크 세그먼트의 모든 트래픽을 대상으로 하는 단순 트래픽 프로필에는 조건이 없습니다. 이와는 달리 여러 개의 중첩된 조건을 포함하는 복합 트래픽 프로필도 있습니다.

예를 들어 다음 그림의 트래픽 프로필 조건은 10.4.x.x 서브넷의 HTTP 연결을 수집합니다.



Create Profile 페이지의 **Profile Conditions** 섹션에서 트래픽 프로필 조건을 작성합니다. 조건 작성에 대한 자세한 내용은 53-10페이지의 조건 작성 원리 이해을/를 참조하십시오. 또한 조건 작성 시 사용할 수 있는 구문에 대해 53-4페이지의 트래픽 프로필 조건의 구문에서 자세히 설명합니다.

팁 기존 트래픽 프로필의 설정을 사용하려는 경우 **Copy Settings**를 클릭하고 팝업 창에서 사용할 트래픽 프로필을 선택한 다음 **Load**를 클릭합니다.

트래픽 프로필 조건의 구문

라이센스: FireSIGHT

다음 표에서는 트래픽 프로필 조건을 작성하는 방법에 대해 설명합니다.

NetFlow 레코드는 연결의 어떤 호스트가 initiator이고 responder인가에 대한 정보를 포함하지 않습니다. 시스템에서 NetFlow 레코드를 처리할 때 각 호스트에서 사용하는 포트를 기반으로 이 정보를 확인하고, 이 포트가 잘 알려진 것인지 확인하는 데 알고리즘을 사용합니다. 자세한 내용은 45-17페이지의 NetFlow 및 FireSIGHT 데이터 간 차이점을/를 참조하십시오.

트래픽 프로필에 사용 가능한 이 정보는 탐지 방법, 로깅 방법, 이벤트 유형 등 여러 요인에 따라 달라집니다. 자세한 내용은 39-11페이지의 연결 및 보안 인텔리전스 이벤트에서 제공되는 정보을/를 참조하십시오.

표 53-1 프로필 조건의 구문

지정할 항목	연산자 선택 후 수행할 작업
Application Protocol	사용 가능 프로토콜의 드롭다운 목록에서 애플리케이션 프로토콜 이름을 선택합니다.
Application Protocol Category	사용 가능 범주의 드롭다운 목록에서 애플리케이션 프로토콜 범주 이름을 선택합니다.
Client	사용 가능 클라이언트의 드롭다운 목록에서 클라이언트 이름을 선택합니다.
Client Category	사용 가능 범주의 드롭다운 목록에서 클라이언트 범주 이름을 선택합니다.
Connection Type	Cisco 디바이스 아니면 NetFlow 지원 디바이스에서 수집한 연결 데이터를 사용할 것인지 트래픽 프로필에서 지정합니다. 연결 유형을 지정할 경우 트래픽 프로필은 둘 다 포함합니다.
Destination Country 또는 Source Country	사용 가능 국가의 드롭다운 목록에서 국가를 선택합니다. 이는 네트워크 트래픽에 식별된 소스 또는 목적지 IP 주소의 국가를 나타냅니다.
Initiator IP, Responder IP 또는 Initiator/Responder IP	특정 IP 주소 또는 CIDR 표기법을 사용하여 IP 주소의 범위를 지정합니다. IP 주소에 허용되는 구문에 대한 설명은 60-6페이지의 검색에서 IP 주소 지정을/를 참조하십시오. 그러나 모니터링하는 네트워크에 포함되거나 포함되지 않는 IP 주소를 지정하는 데 `local` 또는 `remote` 키워드를 사용할 수 **없습니다**.
NetFlow Device	어떤 NetFlow 지원 디바이스의 데이터를 트래픽 프로필 생성에 사용할지 선택합니다. (로컬 컨피그레이션을 사용하여) 구축에 어떤 NetFlow 지원 디바이스도 추가하지 않은 경우, NetFlow Device 드롭다운 목록은 비어 있습니다.
Responder Port/ICMP Code	포트 번호 또는 ICMP 코드를 입력합니다.
Security Intelligence Category	사용 가능 범주의 드롭다운 목록에서 보안 인텔리전스 범주 이름을 선택합니다. 트래픽 프로필 조건에 대한 보안 인텔리전스 범주를 사용하려면 액세스 제어 정책의 Security Intelligence 섹션에서 범주가 **Block**이 아닌 **Monitor**로 설정되어야 합니다. 자세한 내용은 13-3페이지의 보안 인텔리전스 화이트리스트 및 블랙리스트 작성을/를 참조하십시오.
SSL Encrypted Session	**Successfully Decrypted**를 선택합니다.
Transport Protocol	전송 프로토콜로 `TCP` 또는 `UDP`를 입력합니다.

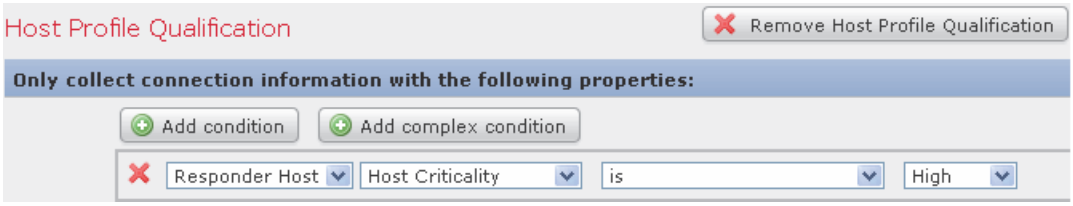
표 53-1 프로필 조건의 구문 (계속)

지정할 항목	연산자 선택 후 수행할 작업
Web Application	사용 가능 웹 애플리케이션의 드롭다운 목록에서 웹 애플리케이션 이름을 선택합니다.
Web Application Category	사용 가능 범주의 드롭다운 목록에서 웹 애플리케이션 범주 이름을 선택합니다.

호스트 프로필 자격 추가

라이센스: FireSIGHT

추적된 호스트의 호스트 프로필 정보로 어떤 트래픽 프로필도 제한할 수 있습니다. 이러한 제약을 *호스트 프로필 자격*이라고 합니다. 예를 들어 다음 그림에서 보여주는 것처럼 호스트 중요도가 **high**인 호스트의 연결 데이터만 수집할 수 있습니다.



호스트 프로필 자격을 사용하려면 호스트가 데이터베이스에 있고 자격으로 사용하려는 호스트 프로필 속성이 이미 호스트 프로필에 포함된 상태여야 합니다. 예를 들어 Windows를 실행하는 호스트에서 침입 이벤트가 생성될 때 트리거할 상관관계 정책 규칙을 구성할 경우, 침입 이벤트 생성 시점에 이미 호스트가 Windows로 식별된 상태여야 규칙이 트리거됩니다.

호스트 프로필 자격을 추가하려면

액세스: Admin/Discovery Admin

1단계 Create Profile 페이지에서 **Add Host Profile Qualification**을 클릭합니다.

Host Profile Qualification 섹션이 나타납니다.

2단계 호스트 프로필 자격의 조건을 작성합니다.

하나의 단순한 조건을 생성하거나 여러 조건을 연결하고 중첩시켜 더 정교한 구성으로 만들 수도 있습니다. 조건 작성에 대한 자세한 내용은 53-10페이지의 조건 작성 원리 이해을/를 참조하십시오.

조건 작성 시 사용할 수 있는 구문에 대해서는 53-6페이지의 호스트 프로필 자격의 구문에서 자세히 설명합니다.

팁 호스트 프로필 자격을 제거하려면 **Remove Host Profile Qualification**을 클릭합니다.

호스트 프로필 자격의 구문

라이센스: FireSIGHT

호스트 프로필 자격 조건을 작성할 때 먼저 트래픽 프로필을 제한하는 데 사용할 호스트를 선택해야 합니다. **Responder Host** 또는 **Initiator Host** 중 하나를 선택할 수 있습니다. 호스트 역할을 선택한 다음 호스트 프로필 자격의 구문 표에 설명된 대로 계속해서 호스트 프로필 자격 조건의 작성합니다.

NetFlow 지원 디바이스에서 내보낸 데이터를 기반으로 네트워크 맵에 호스트를 추가하도록 네트워크 검색 정책을 구성할 수 있으나, 이 호스트에 대해 사용 가능한 정보는 제한적입니다. 예를 들어 이 호스트에 사용 가능한 운영 체제 데이터는 호스트 입력 기능을 사용하여 제공해야 합니다. 또한 트래픽 프로필이 NetFlow 기반 디바이스에서 내보낸 연결 데이터를 사용할 경우, NetFlow 레코드는 연결의 어떤 호스트가 initiator이고 어떤 호스트가 responder인지에 대한 정보를 포함하지 않습니다. 시스템에서 NetFlow 레코드를 처리할 때 각 호스트에서 사용하는 포트를 기반으로 이 정보를 확인하고 이 포트가 잘 알려진 것인지 확인하는 데 알고리즘을 사용합니다. 자세한 내용은 45-17페이지의 NetFlow 및 FireSIGHT 데이터 간 차이점을/를 참조하십시오.

암시된 클라이언트 또는 일반 클라이언트에 매칭하려면 클라이언트에 응답하는 서버에서 사용하는 애플리케이션 프로토콜에 따라 호스트 프로필 자격을 생성합니다. 연결의 initiator 또는 소스가 되는 호스트의 클라이언트 목록에서 어떤 애플리케이션 프로토콜 이름 다음에 **클라이언트**가 올 경우 그 클라이언트는 암시된 클라이언트일 수 있습니다. 즉 시스템은 탐지된 클라이언트 트래픽이 아니라 해당 클라이언트에 대해 애플리케이션 프로토콜을 사용하는 서버 응답 트래픽을 기반으로 클라이언트를 보고합니다.

예를 들어 시스템에서 호스트의 클라이언트로 **HTTPS client**를 보고할 경우 **Responder Host**에 대한 호스트 프로필 자격을 생성하며 여기서 **Application Protocol**은 **HTTPS**로 설정됩니다. Responder 또는 목적지 호스트에서 보낸 HTTPS 서버 응답 트래픽에 따라 HTTPS 클라이언트가 일반 클라이언트로 보고되기 때문입니다.

표 53-2 호스트 프로필 자격의 구문

지정할 항목	연산자 선택 후 수행할 작업
Host Type	드롭다운 목록에서 호스트 유형을 하나 이상 선택합니다. 일반 호스트를 선택하거나 여러 네트워크 디바이스 유형 중 하나를 선택할 수 있습니다.
NETBIOS Name	호스트의 NetBIOS 이름을 입력합니다.
Operating System > OS Vendor	드롭다운 목록에서 운영 체제 공급업체 이름을 하나 이상 선택합니다.
Operating System > OS Name	드롭다운 목록에서 운영 체제 이름을 하나 이상 선택합니다.
Operating System > OS Version	드롭다운 목록에서 운영 체제 버전을 하나 이상 선택합니다.
Network Protocol	네트워크 프로토콜 번호를 http://www.iana.org/assignments/ethernet-numbers에 표시된 대로 입력합니다.
Transport Protocol	전송 프로토콜의 이름이나 번호를 http://www.iana.org/assignments/protocol-numbers에 표시된 대로 입력합니다.
Host Criticality	나타나는 목록에서 호스트 중요도를 선택합니다. **None**, **Low**, **Medium** 또는 **High**를 선택할 수 있습니다. 호스트 중요도에 대한 자세한 내용은 49-30페이지의 사전 정의 호스트 특성 작업을/를 참조하십시오.
VLAN ID	호스트의 VLAN ID 번호를 입력합니다.
Application Protocol> Application Protocol	드롭다운 목록에서 애플리케이션 프로토콜을 선택합니다.

표 53-2 호스트 프로필 자격의 구문 (계속)

지정할 항목	연산자 선택 후 수행할 작업
Application Protocol > Application Port	애플리케이션 프로토콜 포트 번호를 입력합니다.
Application Protocol > Protocol	드롭다운 목록에서 프로토콜을 선택합니다.
Client > Client	드롭다운 목록에서 클라이언트를 선택합니다.
Client > Client Version	클라이언트 버전을 입력합니다.
Web Application	드롭다운 목록에서 클라이언트를 선택합니다.
MAC Address > MAC Address	호스트의 MAC 주소 전체 또는 일부를 입력합니다.
MAC Address > MAC Type	MAC 유형이 **ARP/DHCP Detected**인지 여부를 선택합니다. 즉 시스템에서 MAC 주소를 호스트에 속한 것(**ARP/DHCP Detected**)으로 확실하게 식별했는지, 디바이스와 호스트 간에 라우터가 있는 등의 이유로 여러 호스트가 해당 MAC 주소를 갖는지(**is not ARP/DHCP Detected**) 또는 MAC 유형이 상관없는지(**is any**) 여부를 선택합니다.
MAC Vendor	호스트에서 사용하는 하드웨어의 MAC 공급업체 전체 또는 일부를 입력합니다.
사용 가능한 모든 호스트 특성(기본 규정준수 화이트리스트 호스트 특성 포함)	선택하는 호스트 특성의 유형에 따라 알맞은 값을 지정합니다. • 호스트 특성 유형이 Integer일 경우 그 특성에 대해 정의된 범위의 정수 값을 입력합니다. • 호스트 특성 유형이 Text일 경우 텍스트 값을 입력합니다. • 호스트 특성 유형이 List일 경우 드롭다운 목록에서 유효한 목록 문자열을 선택합니다. • 호스트 특성 유형이 URL일 경우 URL 값을 입력합니다. 호스트 특성에 대한 자세한 내용은 49-31페이지의 사용자 정의 호스트 특성 작업을/를 참조하십시오.

프로필 옵션 설정

라이센스: FireSIGHT

PTW(profiling time window)는 학습 기간과 동일한 길이의 슬라이딩 시간 창으로서 FireSIGHT 시스템에서는 트래픽 프로필의 통계를 계산하는 데 이를 사용합니다. 기본 PTW는 1주이지만 짧게는 1시간, 길게는 몇 주까지 변경할 수 있습니다.

또한 트래픽 프로필은 종합 연결 데이터를 기반으로 합니다. 기본적으로 트래픽 프로필은 시스템에서 발생한 연결 이벤트에 대한 통계를 5분 간격으로 생성합니다. 그러나 이 샘플링 속도를 기본값인 5분부터 1시간까지의 범위에 속하는 값으로 설정할 수 있습니다.

트래픽 프로필에는 통계적 의미가 있으므로 충분한 데이터를 포함하도록 PTW와 샘플링 속도를 설정해야 합니다. 예를 들어 PTW가 1일이고 샘플링 속도가 1시간이면 24개 데이터 지점만 포함하는데, 이는 네트워크 트래픽 패턴을 정확하게 분석하는 데 불충분할 수도 있습니다.

팁 PTW는 100개 이상의 데이터 지점을 포함해야 합니다.

트래픽 프로필에서 비활성 시간도 설정할 수 있습니다. 예를 들어 모든 워크스테이션이 매일 밤 자정에 백업되는 네트워크 인프라가 있습니다. 백업에 약 30분이 소요되고 네트워크 트래픽이 급증합니다. 이러한 경우 예정된 백업에 맞춰 트래픽 프로필에 반복적인 비활성 기간을 설정해 놓는 것이 좋을 수도 있습니다. 비활성 기간에 트래픽 프로필에서는 데이터를 수집하지만(트래픽 프로필 그래프에서 트래픽을 볼 수 있음) 프로필 통계 계산 시 그 데이터를 사용하지 않습니다. 비활성 기간이 매일, 매주 또는 매월 반복되도록 설정할 수 있습니다. 비활성 기간은 최소 5분에서 최대 1시간까지 가능합니다. 시간 추이 트래픽 프로필 그래프에서는 비활성 기간이 음영으로 나타납니다.

프로필 옵션을 설정하려면

액세스: Admin/Discovery Admin

표 53-3 Profile Options

기능	가능한 작업
프로필 작성 시간 창 변경	**Profiling Time Window** 필드에 시간, 일 또는 주 단위로 숫자를 입력합니다. 그런 다음 드롭다운 목록에서 **hour(s)**, **day(s)** 또는 **week(s)**를 선택합니다.
샘플링 속도 변경	**Sampling Rate** 드롭다운 목록에서 속도를 선택합니다.
비활성 기간 추가	**Add Inactive Period**를 클릭합니다. 그런 다음 드롭다운 목록을 사용하여 트래픽 프로필에서 데이터를 수집하지 않을 때와 빈도를 지정합니다.
비활성 기간 삭제	삭제할 비활성 기간 옆의 **Delete**를 클릭합니다.

트래픽 프로필 저장

라이센스: FireSIGHT

다음 절차에 따라 트래픽 프로필을 저장합니다.

트래픽 프로필을 저장하려면

액세스: Admin/Discovery Admin

1단계 다음 2가지 옵션을 사용할 수 있습니다.

- 프로필을 활성화하지 않고 저장하려면 **Save**를 클릭합니다.
- 프로필을 저장하고 즉시 데이터 수집을 시작하려면 **Save & Activate**를 클릭합니다.

트래픽 프로필 활성화 및 비활성화

라이센스: FireSIGHT

모니터링되는 네트워크 세그먼트의 트래픽에 대한 프로필 작성을 시작하려면 트래픽 프로필을 활성화해야 합니다.

연결 데이터 수집 및 평가를 중지하려면 프로필을 비활성화합니다. 비활성화된 트래픽 프로필에 대해 작성된 규칙은 트리거되지 않습니다. 또한 트래픽 프로필을 비활성화하면 프로필에서 수집하고 종합한 모든 데이터가 삭제됩니다. 비활성화된 트래픽 프로필을 나중에 다시 활성화할 경우, PTW의 길이만큼 기다려야 그 프로필에 대해 작성된 규칙이 트리거됩니다.

트래픽 프로필을 활성화하거나 비활성화하려면

액세스: Admin/Discovery Admin

1단계 **Policies > Correlation**을 선택한 다음 **Traffic Profiles**를 클릭합니다.

Traffic Profiles 페이지가 나타납니다.

2단계 다음 2가지 옵션을 사용할 수 있습니다.

- 비활성 트래픽 프로필을 활성화하려면 프로필 옆의 **Activate**를 클릭합니다.
- 활성 트래픽 프로필을 비활성화하려면 프로필 옆의 **Deactivate**를 클릭합니다. **OK**를 클릭하여 프로필을 비활성화할 것임을 확인합니다.

트래픽 프로필 수정

라이센스: FireSIGHT

활성 트래픽 프로필은 사실상 수정할 수 없습니다. 트래픽 프로필이 활성 상태일 경우 그 이름과 설명만 변경 가능합니다. 트래픽 프로필의 조건 옵션을 수정하려면 먼저 이 프로필을 비활성화해야 합니다. 트래픽 프로필을 비활성화하면 여기서 수집한 모든 데이터가 삭제됩니다.

트래픽 프로필 활성화 및 비활성화에 대한 자세한 내용은 53-9페이지의 트래픽 프로필 활성화 및 비활성화을/를 참조하십시오.

트래픽 프로필을 수정하려면

액세스: Admin/Discovery Admin

1단계 **Policies > Correlation**을 선택한 다음 **Traffic Profiles**를 클릭합니다.

Traffic Profiles 페이지가 나타납니다.

2단계 수정할 트래픽 프로필 옆의 **Edit**를 클릭합니다.

Create Profile 페이지가 나타납니다.

3단계 프로필을 변경하고 **Save**를 클릭합니다.

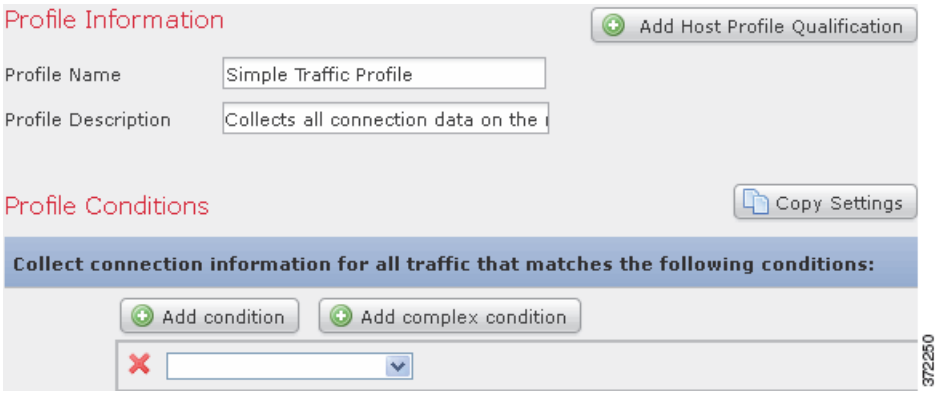
프로필이 업데이트되었습니다.

조건 작성 원리 이해

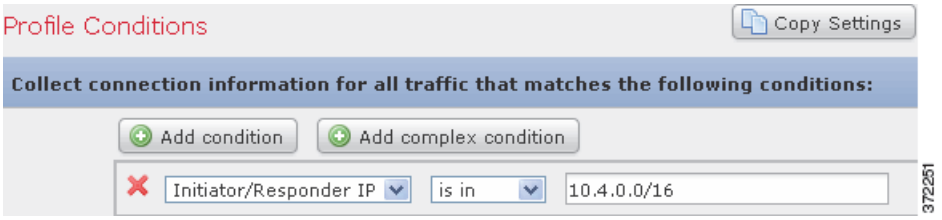
라이센스: FireSIGHT

데이터 수집에 사용할 조건을 지정하는 방법으로 트래픽 프로필을 작성합니다. 단순 조건을 만들거나 중첩된 조건으로 더욱 정교한 구조를 생성할 수 있습니다.

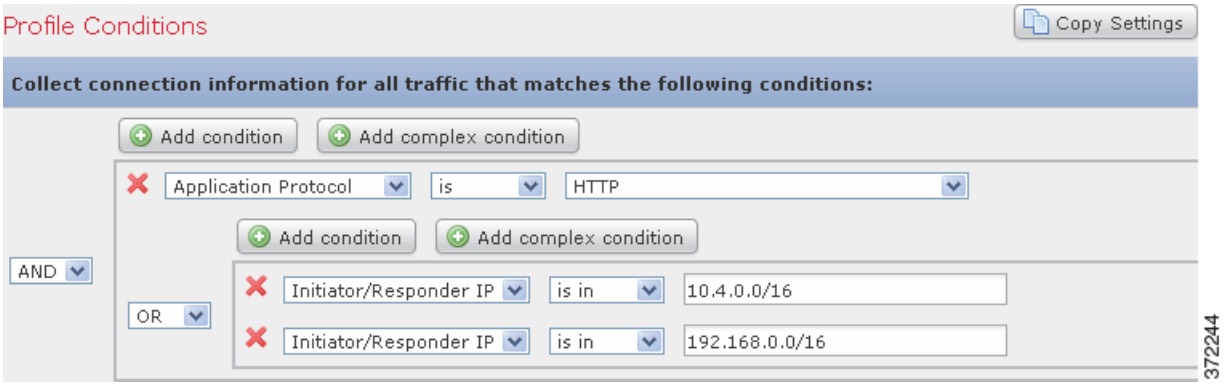
예를 들어 모니터링되는 전체 네트워크 세그먼트에 대해 데이터를 수집하는 트래픽 프로필을 생성하려는 경우 다음 그림과 같이 조건 없는 매우 단순한 프로필을 생성할 수 있습니다.



프로필을 제한하여 10.4.x.x 네트워크에 대해서만 데이터를 수집하게 하려는 경우 다음 그림과 같이 하나의 조건을 추가할 수 있습니다.



그러나 10.4.x.x 네트워크 및 192.168.x.x 네트워크에 대한 HTTP 활동을 수집하는 다음 트래픽 프로필은 3개의 조건을 가지며, 그중 마지막은 복합 조건입니다.



조건 내에서 사용할 수 있는 구문은 생성하는 요소에 따라 달라지지만, 그 원리는 동일합니다. 자세한 내용은 다음 링크를 참조하십시오.

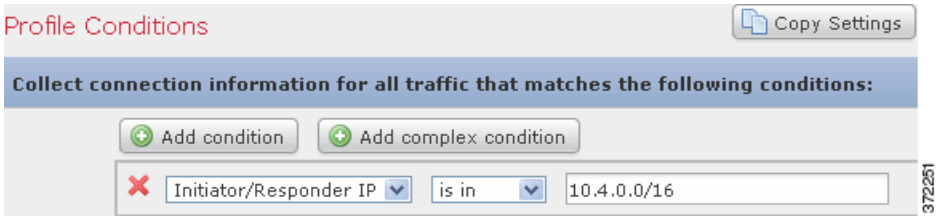
- 53-11페이지의 단일 조건 작성
- 53-13페이지의 조건 추가 및 연결
- 53-15페이지의 하나의 조건에서 여러 값 사용

단일 조건 작성

라이센스: FireSIGHT

대부분의 조건은 범주, 연산자, 값의 3개 부분으로 구성됩니다. 어떤 조건은 더 복합적이고 여러 범주를 포함하는데, 각 범주마다 고유의 연산자와 값을 가질 수도 있습니다.

예를 들어 다음 트래픽 프로필은 10.4.x.x 네트워크에 대한 정보를 수집합니다. 이 조건의 범주는 **Initiator/Responder IP**, 연산자는 **is in**, 값은 `10.4.0.0/16`입니다.



다음 단계에서는 이 트래픽 프로필 조건의 작성 방법을 설명합니다.

단일 조건을 작성하려면

액세스: Admin/Discovery Admin

1단계 **Policies > Correlation**을 선택한 다음 **Traffic Profiles**를 클릭합니다.

Traffic Profiles 페이지가 나타납니다.

2단계 **New Profile**을 클릭합니다.

Create Profile 페이지가 나타납니다.

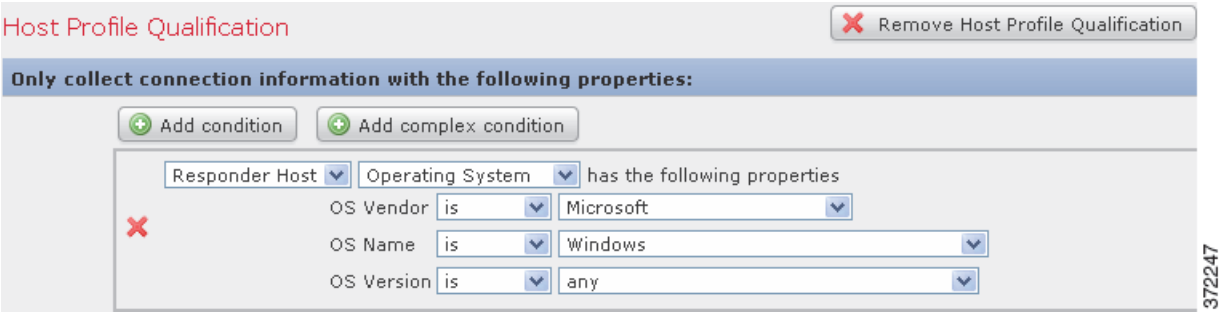
3단계 **Profile Conditions**의 첫 번째 (범주) 드롭다운 목록에서 **Initiator/Responder IP**를 선택하여 프로필의 단일 조건 작성을 시작합니다.

4단계 두 번째 (연산자) 드롭다운 목록에서 **is in**을 선택합니다.

팁 해당 범주가 IP 주소를 나타낼 때 **is in** 또는 **is not in**을 연산자로 선택하면, 해당 IP 주소가 CIDR 방식으로 표현된 IP 주소의 범위에 *속하는지 속하지 않는지*를 명시할 수 있습니다. FireSIGHT 시스템에 CIDR 표기법을 사용하는 것에 대한 자세한 내용은 1-19페이지의 IP 주소 표기 규칙을/를 참조하십시오.

5단계 텍스트 필드에 `10.4.0.0/16`을 입력합니다.

한편 다음 호스트 프로필 자격은 더 복합적입니다. 탐지된 연결의 응답 호스트가 어떤 버전의 Microsoft Windows를 실행하는 경우에만 연결 데이터를 수집하도록 트래픽 프로필을 제한합니다.



다음 단계에서는 이 호스트 프로필 자격의 작성 방법을 설명합니다.

이 호스트 프로필 자격을 작성하려면

액세스: Admin/Discovery Admin

1단계 **Policies > Correlation**을 선택한 다음 **Traffic Profiles**를 클릭합니다.

Traffic Profiles 페이지가 나타납니다.

2단계 **New Profile**을 클릭합니다.

Create Profile 페이지가 나타납니다.

3단계 **Add Host Profile Qualification**을 클릭합니다.

4단계 **Host Profile Qualification**의 첫 번째 조건에서 정보를 수집할 호스트를 지정합니다.

이 예에서는 연결의 응답 호스트에 대한 정보만 수집할 것이므로 **Responder Host**를 선택합니다.

5단계 **Operating System** 범주를 선택하여 호스트 운영 체제의 세부 사항 지정을 시작합니다.

OS Vendor, **OS Name**, **OS Version**의 3가지 하위 범주가 나타납니다.

6단계 호스트에서 어떤 버전의 Microsoft Windows도 실행할 수 있도록 지정하려면 세 하위 범주 모두에 동일한 연산자 **is**를 사용합니다.

7단계 마지막으로 하위 범주에 대한 값을 지정합니다.

Microsoft를 **OS Vendor**로, **Windows**를 **OS Name**의 값으로 선택하고 **OS Version**의 값으로는 **any**를 유지합니다.

선택 가능한 범주는 트래픽 작성의 대상이 프로필 조건인지 호스트 프로필 자격인지에 따라 달라집니다. 또한 조건에서 사용 가능한 연산자는 선택하는 범주에 따라 달라집니다. 마지막으로, 조건의 값을 지정하는 데 사용 가능한 구문은 범주와 연산자에 따라 달라집니다. 텍스트 필드에 값을 입력해야 하는 경우가 있습니다. 그렇지 않으면 드롭다운 목록에서 값을 선택할 수 있습니다.

참고 조건 구문에서 드롭다운 목록의 값 선택을 허용할 경우 대개는 목록에서 여러 값을 사용할 수 있습니다. 자세한 내용은 53-15페이지의 하나의 조건에서 여러 값 사용을/를 참조하십시오.

트래픽 프로필 조건 및 호스트 프로필 자격의 작성 구문에 대한 자세한 내용은 다음을 참조하십시오.

- 53-4페이지의 트래픽 프로필 조건의 구문
- 53-6페이지의 호스트 프로필 자격의 구문

조건 추가 및 연결

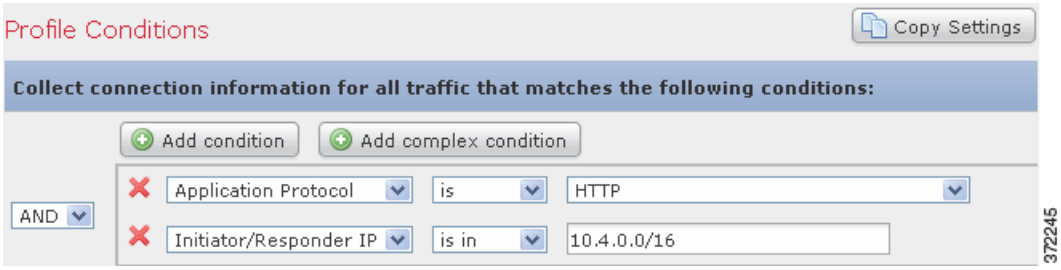
라이센스: FireSIGHT

단순한 트래픽 프로필 조건과 호스트 프로필 자격을 생성하거나 조건을 연결하고 중첩시키는 방법으로 더 정교하게 구성할 수 있습니다.

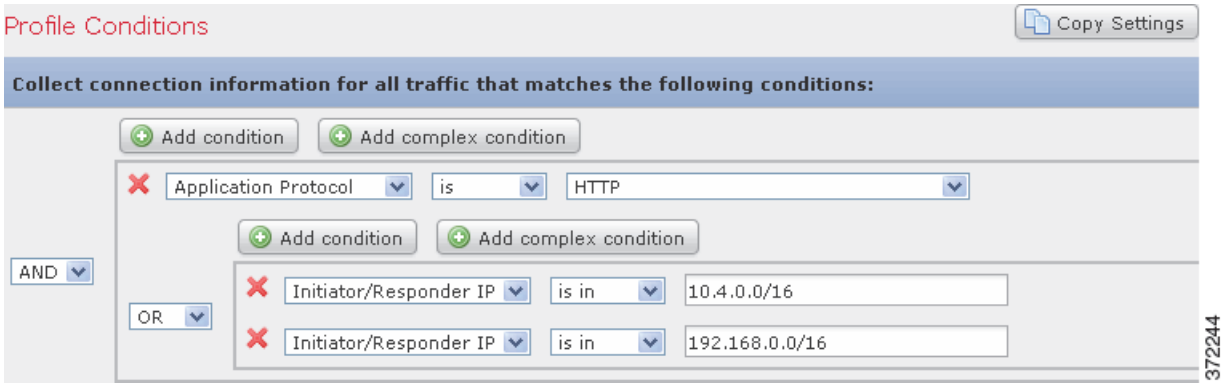
두 이상의 조건을 포함할 경우 **AND** 또는 **OR** 연산자로 연결해야 합니다. 동일한 레벨의 조건은 함께 평가됩니다.

- **AND** 연산자를 사용하면 이 연산자가 제어하는 레벨의 모든 조건을 충족해야 합니다.
- **OR** 연산자는 제어하는 레벨의 조건 중 하나 이상을 충족해야 합니다.

예를 들어 다음 트래픽 프로필에서는 2개의 조건이 **AND**로 연결되어 있습니다. 즉 이 트래픽 프로필은 두 조건이 모두 참인 경우에만 연결 데이터를 수집합니다. 이 예에서는 IP 주소가 10.4.x.x 서브넷에 있는 모든 호스트에 대해 HTTP 연결을 수집합니다.



한편 10.4.x.x 네트워크 또는 192.168.x.x 네트워크 중 하나의 HTTP 활동에 대한 연결 데이터를 수집하는 다음 트래픽 프로필은 3개의 조건을 가지며, 그중 마지막은 복합 조건입니다.



논리적으로 위 트래픽 프로필은 다음과 같이 평가됩니다.

```
(A and (B or C))
```

항목	조건의 내용
A	Application Protocol Name이 HTTP임
B	IP Address가 10.4.0.0/16에 있음
C	IP Address가 192.168.0.0/16에 있음

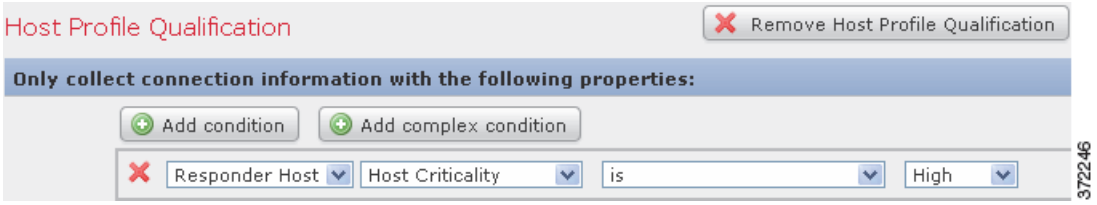
단일 조건을 추가하려면

액세스: Admin/Discovery Admin

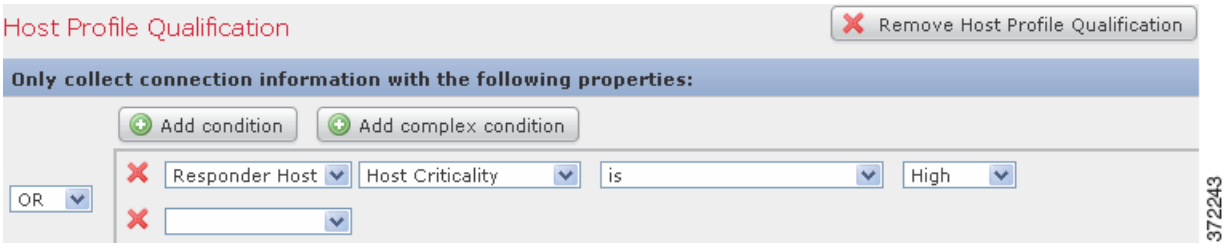
1단계 단일 조건을 추가하려면 현재 조건 위에서 **Add condition**을 클릭합니다.

현재의 조건 세트와 동일한 논리적 레벨에 새 조건이 추가됩니다. 기본적으로 **OR** 연산자를 사용하여 그 레벨의 조건에 연결되지만, 연산자를 **AND**로 변경할 수 있습니다.

예를 들어 다음 호스트 프로필 자격에 단순 조건을 추가할 경우



결과는 다음과 같습니다.



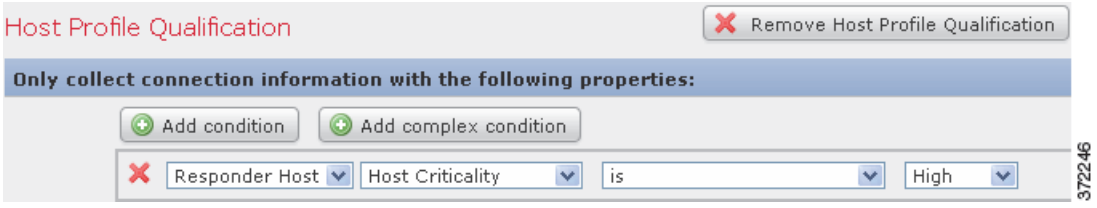
복합 조건을 추가하려면

액세스: Admin/Discovery Admin

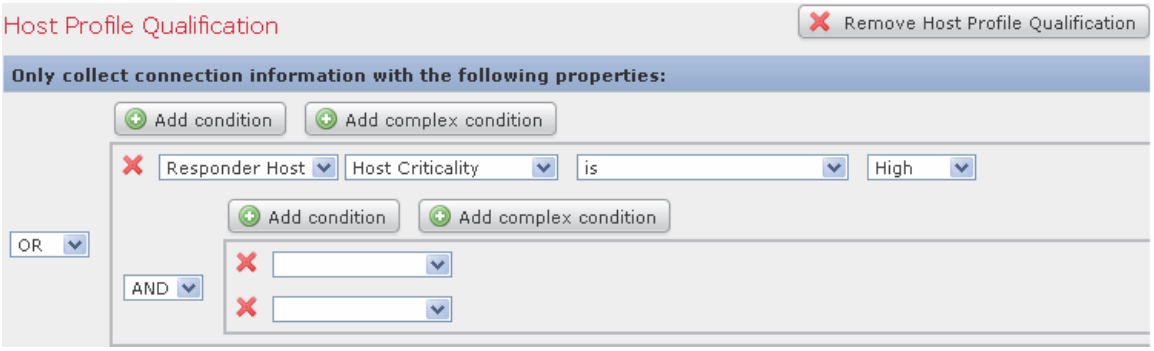
1단계 현재 조건 위에서 **Add complex condition**을 클릭합니다.

현재 조건 세트의 아래에 복합 조건이 추가됩니다. 복합 조건은 2개의 하위 조건으로 구성되며, 이들은 그 상위 레벨의 조건을 연결하는 데 쓰인 것과 상반되는 연산자로 연결됩니다.

예를 들어 다음 호스트 프로필 자격에 복합 조건을 추가할 경우



결과는 다음과 같습니다.



조건을 연결하려면

액세스: Admin/Discovery Admin

1단계 조건 세트의 왼쪽에 있는 드롭다운 목록을 사용합니다.

- 연산자가 제어하는 레벨의 모든 조건을 충족해야 하는 경우 **AND**를 선택합니다.
- 연산자가 제어하는 레벨의 조건 중 하나만 충족하면 되는 경우 **OR**를 선택합니다.

하나의 조건에서 여러 값 사용

라이센스: FireSIGHT

조건을 작성할 때 조건 구문상 드롭다운 목록의 값 선택이 가능할 경우 대개는 목록에서 여러 값을 사용할 수 있습니다. 예를 들어 호스트가 UNIX의 특정 버전을 실행해야한다는 조건을 호스트 프로필 자격으로 트래픽 프로필에 추가하려는 경우, 여러 조건을 OR 연산자로 연결하지 않고 다음 절차를 사용합니다.

하나의 조건에 여러 값을 포함하려면

액세스: Admin/Discovery Admin

1단계 B조건을 작성하면서 **is in** 또는 **is not in**을 연산자로 선택합니다.

드롭다운 목록이 텍스트 필드로 바뀝니다.

2단계 텍스트 필드의 아무 곳이나 또는 **Edit** 링크를 클릭합니다.

팝업 창이 나타납니다.

3단계 **Available**에서 Ctrl 키 또는 Shift 키를 누른 채로 클릭하여 여러 값을 선택합니다. 또는 클릭하고 드래그하여 인접한 여러 값을 선택할 수 있습니다.

4단계 오른쪽 화살표(>)를 클릭하여 선택한 항목을 **Selected**로 이동합니다.

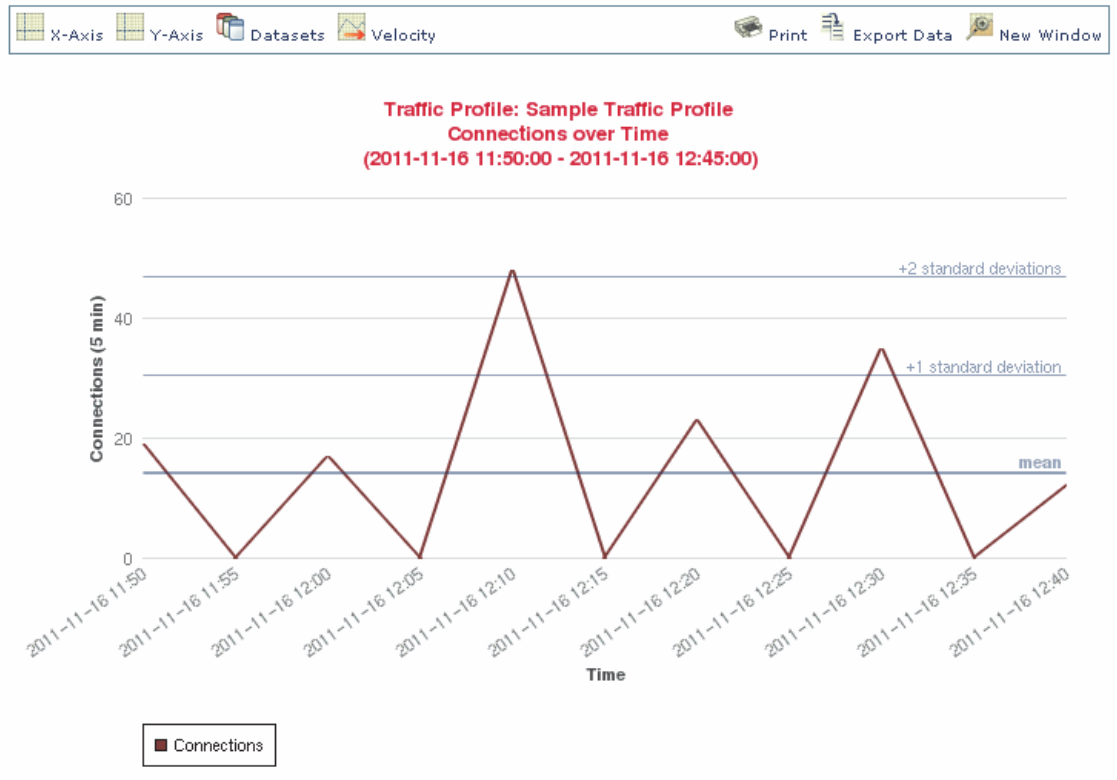
5단계 **OK**를 클릭합니다.

선택한 내용이 Create Profile 페이지의 조건 값 필드에 나타납니다.

트래픽 프로필 보기

라이센스: FireSIGHT

트래픽 프로필이 연결 데이터를 기반으로 하기 때문에 트래픽 프로필의 그래프를 볼 수 있습니다. 다음 그래프는 PTW가 1주, 샘플링 속도가 5분이고 매일 자정부터 오전 12:30까지 30분의 비활성 기간이 있는 트래픽 프로필을 보여줍니다.



연결 데이터 그래프에서 수행 가능한 거의 모든 작업을 트래픽 프로필 그래프에서도 수행할 수 있습니다. 그러나 트래픽 프로필은 종합 데이터(연결 요약)를 기반으로 하므로 그래프의 기반이 되는 개별 연결 이벤트를 조사할 수는 없습니다. 즉 트래픽 프로필 그래프에서 어떤 연결 데이터 테이블 보기로 드릴다운할 수 없습니다. 자세한 내용은 39-14페이지의 연결 및 보안 인텔리전스 데이터 보기을/를 참조하십시오. 또한 트래픽 프로필은 분리된 그래프로 나타납니다. 자세한 내용은 39-27페이지의 연결 그래프 분리을/를 참조하십시오.

그리고 시간 추이 트래픽 프로필 그래프에서는 평균 y축 값을 굵은 수평선으로 표시합니다. 또한 시간 추이 그래프에서는 네트워크 트래픽의 정규 분포를 전제로 평균값 대비 첫 4개 표준 편차의 값도 표시합니다. 기본적으로 이 통계는 PTW를 대상으로 계산되지만, 그래프의 시간 설정을 변경하면 방어 센터에서 통계를 다시 계산합니다. 그러나 트래픽 프로필 통계에 대해 작성된 규칙은 항상 PTW 통계를 기준으로 평가됩니다.

어떤 트래픽 프로필에 대한 트래픽 프로필 그래프를 보려면

액세스: Admin/Discovery Admin

1단계 **Policies > Correlation**을 선택한 다음 **Traffic Profiles**를 클릭합니다.

Traffic Profiles 페이지가 나타납니다.

2단계 그래프를 표시할 트래픽 프로필 옆의 그래프 아이콘()을 클릭합니다.

트래픽 프로필의 그래프가 별도의 브라우저 창에 나타납니다.

54장 교정 구성

상관관계 정책 위반이 발생하면 하나 또는 여러 응답을 시작하도록 FireSIGHT 시스템을 구성할 수 있으며, 여기에는 교정(예: Nmap 스캔 실행) 및 각종 알림 유형이 포함됩니다.

실행할 수 있는 가장 기본적인 종류의 응답은 알림(alert)입니다. 알림은 이메일, SNMP 트랩 서버, syslog를 통해 정책 위반을 알려줍니다. 알림 생성에 대한 자세한 내용은 43-1페이지의 외부 알림 구성을/를 참조하십시오.

실행할 수 있는 또 다른 종류의 응답은 교정(remediation)입니다. 교정은 네트워크 트래픽이 상관관계 정책을 위반할 때 방어 센터에서 실행하는 프로그램입니다. FireSIGHT 시스템에는 정책 위반 시 또는 호스트 스캔 시 방화벽이나 라우터에서 호스트를 차단하는 등의 작업을 수행하는 사전 정의된 교정이 포함되어 있습니다.

방어 센터는 교정을 실행할 때 교정 상태 이벤트를 생성합니다. 다른 이벤트와 마찬가지로 교정 상태 이벤트도 검색하고 보고 삭제할 수 있습니다.

FireSIGHT 시스템은 또한 상관관계 정책 위반에 응답하는 사용자 지정 교정 모듈을 생성하기 위해 사용할 수 있는 유연한 API를 제공합니다. 예를 들어 Linux 기반 방화벽을 실행 중인 경우 상관관계 정책을 위반하는 트래픽을 차단할 수 있도록 Linux 서버에서 `iptables` 파일을 동적으로 업데이트하는 교정 모듈을 작성하여 업로드할 수 있습니다. 자신의 고유한 교정 모듈을 작성하는 방법에 대한 자세한 내용은 *Cisco Remediation API Guide*를 참조하십시오.

참고 교정을 구성 및 사용하려면 방어 센터를 사용해야 합니다.

자세한 내용은 다음 링크를 참고하십시오.

- 54-1페이지의 교정 생성
- 54-17페이지의 교정 상태 이벤트 작업

교정 생성

라이센스: FireSIGHT

상관관계 정책 위반을 단순하게 알리는 알림 외에도 *교정*이라는 응답을 구성할 수 있습니다. 교정은 상관관계 정책이 위반될 때 방어 센터에서 실행하는 프로그램입니다. 이러한 프로그램은 특정 작업을 수행하기 위해 위반을 트리거한 이벤트에서 제공되는 정보를 사용합니다.

FireSIGHT 시스템은 사전 정의된 몇 가지 교정 모듈을 제공합니다.

- Cisco IOS Null Route 모듈 - Cisco IOS® 버전 12.0 이상을 사용하는 Cisco 라우터를 실행 중인 경우, 상관관계 정책을 위반하는 IP 주소 또는 네트워크로 전송되는 트래픽을 동적으로 차단할 수 있습니다.

  자세한 내용은 54-3페이지의 Cisco IOS 라우터에 대한 교정 구성을/를 참조하십시오.

- Cisco PIX Shun 모듈 - Cisco PIX® Firewall 버전 6.0 이상을 실행 중인 경우 상관관계 정책을 위반하는 IP 주소 또는 네트워크로부터 전송되는 트래픽을 동적으로 차단할 수 있습니다.

  자세한 내용은 54-8페이지의 Cisco PIX 방화벽에 대한 교정 구성을/를 참조하십시오.

- Nmap Scanning 모듈 - 호스트에서 실행 중인 운영 체제와 서버를 확인하기 위해 특정 대상을 능동적으로 스캔할 수 있습니다.

  자세한 내용은 54-11페이지의 Nmap 교정 구성을/를 참조하십시오.

- Set Attribute Value 모듈 - 상관관계 이벤트가 발생하는 호스트에서 호스트 특성을 설정할 수 있습니다.

  54-15페이지의 Set Attribute 교정 구성을/를 참조하십시오.

각 교정 모듈에 대해 여러 인스턴스를 생성하며, 각 인스턴스는 특정 어플라이언스에 대한 연결을 나타냅니다. 예를 들어, 교정을 전송하려는 Cisco IOS 라우터가 네 개 있는 경우 Cisco IOS 교정 모듈 인스턴스를 네 개 구성해야 합니다.

인스턴스를 생성할 때 방어 센터에서 어플라이언스와의 연결을 설정하기 위해 필요한 컨피그레이션 정보를 지정합니다. 그런 다음 구성된 각 인스턴스에 대해 정책 위반 시 어플라이언스가 수행할 작업을 설명하는 교정을 추가합니다.

구성이 완료되면 응답 그룹이라는 그룹에 교정을 추가할 수 있습니다. 또는 상관관계 정책 내 규칙에 특별히 교정을 할당할 수 있습니다. 시스템은 이러한 교정을 실행할 때 교정 이름, 교정을 트리거한 정책과 규칙, 종료 상태 메시지 등의 세부사항이 포함된 교정 상태 이벤트를 생성합니다. 이러한 이벤트에 대한 자세한 내용은 54-17페이지의 교정 상태 이벤트 작업을/를 참조하십시오.

Cisco에서 제공하는 기본 모듈 외에도 정책 위반이 트리거될 때 다른 특정 작업을 수행하는 사용자 지정 교정 모듈을 작성할 수 있습니다. 고유한 교정 모듈을 작성하여 방어 센터에 설치하는 방법에 대한 자세한 내용은 *Remediation API Guide*를 참조하십시오. 사용자 지정 모듈을 설치할 때 Modules 페이지를 사용하여 새 모듈을 설치하고 보고 삭제할 수 있습니다.

방어 센터에 새 모듈을 설치하려면

액세스: Admin/Discovery Admin

1단계 **Policies > Actions > Modules**를 선택합니다.

Modules 페이지가 나타납니다.

2단계 **Browse**를 클릭하여 사용자 지정 교정 모듈이 포함된 파일을 저장한 위치로 이동합니다(자세한 내용은 *Remediation API Guide* 참조).

3단계 **Install**을 클릭합니다.

사용자 지정 교정 모듈이 설치됩니다.

방어 센터에서 모듈을 보거나 삭제하려면

액세스: Admin/Discovery Admin

1단계 **Policies > Actions > Modules**를 선택합니다.

Modules 페이지가 나타납니다.

2단계 다음 작업 중 하나를 수행합니다.

- **View**를 클릭하여 모듈을 봅니다.

  Module Detail 페이지가 나타납니다.

- 삭제할 모듈 옆에 있는 **Delete**를 클릭합니다. Cisco에서 제공하는 기본 모듈은 삭제할 수 **없습니다**.

  교정 모듈이 삭제됩니다.

Cisco IOS 라우터에 대한 교정 구성

라이센스: FireSIGHT

Cisco에서는 상관관계 정책 위반 시 Cisco의 "null route" 명령을 사용하여 단일 IP 주소 또는 전체 주소 블록을 차단할 수 있는 Cisco IOS Null Route 교정 모듈을 제공합니다. 이 모듈은 상관관계 정책 위반이 발생할 경우 소스나 목적지 호스트로서 나열된 호스트 또는 네트워크로 전송되는 모든 트래픽을 라우터의 NULL 인터페이스로 전달하여 삭제되도록 합니다(위반하는 호스트 또는 네트워크**로부터** 전송되는 트래픽은 차단되지 않음).

Cisco IOS Null Route 교정 모듈은 Cisco IOS 12.0 이상을 실행하는 Cisco 라우터를 지원합니다. Cisco IOS 교정을 실행하려면 라우터에 대한 레벨 15 관리 액세스 권한이 있어야 합니다.

참고 목적지 기반 교정은 연결 이벤트 또는 침입 이벤트 기반의 상관관계 규칙이 트리거될 때 실행되도록 구성한 경우에만 작동합니다. 검색 이벤트는 소스 호스트를 전송하기만 합니다.

주의 Cisco IOS 교정이 활성화되는 경우 시간 초과 기간이 없습니다. 차단된 IP 주소 또는 네트워크를 라우터에서 제거하려면 라우터 자체에서 라우팅 변경 사항을 수동으로 지워야 합니다.

Cisco IOS를 실행하는 라우터에 대해 교정을 생성하려면

액세스: Admin/Discovery Admin

1단계 Cisco 라우터에서 텔넷을 활성화합니다.

텔넷 활성화에 대한 자세한 내용은 Cisco 라우터 또는 IOS 소프트웨어와 함께 제공되는 설명서를 참조하십시오.

2단계 방어 센터에서, 방어 센터와 함께 사용하려는 각 Cisco IOS 라우터에 대해 Cisco IOS Null Route 인스턴스를 추가합니다.

절차는 54-4페이지의 Cisco IOS 인스턴스 추가을/를 참조하십시오.

3단계 상관관계 정책이 위반될 때 라우터에서 이끌어낼 응답의 유형을 기반으로 각 인스턴스에 대한 특정 교정을 생성합니다.

사용 가능한 각 교정 유형에 대해서는 다음 절에서 설명합니다.

- 54-5페이지의 Cisco IOS Block Destination 교정
- 54-6페이지의 Cisco IOS Block Destination Network 교정
- 54-7페이지의 Cisco IOS Block Source 교정
- 54-7페이지의 Cisco IOS Block Source Network 교정

4단계 Cisco IOS 교정을 특정 상관관계 정책 규칙에 할당하기 시작합니다.

Cisco IOS 인스턴스 추가

라이센스: FireSIGHT

Cisco IOS 라우터에 대한 텔넷 액세스를 구성한 후(텔넷 액세스 활성화에 대한 자세한 내용은 Cisco 라우터 또는 IOS 소프트웨어와 함께 제공된 설명서 참조) 방어 센터에 인스턴스를 추가할 수 있습니다. 여러 라우터로 교정을 전송하려는 경우 각 라우터에 대해 개별 인스턴스를 생성해야 합니다.

Cisco IOS 인스턴스를 추가하려면

액세스: Admin/Discovery Admin

1단계 **Policies > Actions > Instances**를 선택합니다.

Instances 페이지가 나타납니다.

2단계 **Add a New Instance** 목록에서 **Cisco IOS Null Route (v1.0)**를 선택하고 **Add**를 클릭합니다.

Edit Instance 페이지가 나타납니다.

3단계 **Instance Name** 필드에 인스턴스의 이름을 입력합니다.

알기 쉬운 이름을 지정해야 하며 공백이나 특수 문자는 사용할 수 없습니다. 예를 들어 둘 이상의 Cisco IOS 라우터에 연결하고자 하며 여러 인스턴스를 사용하려는 경우 `IOS_01`, `IOS_02` 등의 이름을 선택할 수 있습니다.

4단계 교정에 대해 사용하려는 Cisco IOS 라우터의 IP 주소를 **Router IP** 필드에 입력합니다.

5단계 라우터에 대한 텔넷 사용자 이름을 **Username** 필드에 입력합니다. 이 사용자에게는 라우터에 대한 레벨 15 관리 액세스 권한이 있어야 합니다.

6단계 텔넷 사용자의 사용자 비밀번호를 **Connection Password** 필드에 입력합니다. 두 필드에 입력한 비밀번호가 일치해야 합니다.

7단계 텔넷 사용자의 활성 비밀번호를 **Enable Password** 필드에 입력합니다. 이 비밀번호는 라우터의 특권 모드로 들어가기 위해 사용되는 비밀번호입니다. 두 필드에 입력한 비밀번호가 일치해야 합니다.

8단계 교정에서 제외할 IP 주소를 한 줄에 하나씩 **White List** 필드에 입력합니다. CIDR 표기법 또는 특정 IP 주소를 사용할 수도 있습니다. 예를 들어 다음 화이트리스트는 시스템에서 허용됩니다.

```
10.1.1.152
172.16.1.0/24
```

이 화이트리스트는 자신이 작성한 규정 준수 화이트리스트와 연결되지 않습니다. FireSIGHT 시스템에서 CIDR 표기법을 사용하는 방법에 대한 자세한 내용은 1-19페이지의 IP 주소 표기 규칙을/를 참조하십시오.

9단계 **Create**를 클릭합니다.

인스턴스가 생성되고 페이지의 Configured Remediations 섹션에 교정이 나타납니다. 상관관계 정책에서 인스턴스를 사용하려면 특정 교정을 추가해야 합니다. 자세한 내용은 다음 절을 참조하십시오.

- 54-5페이지의 Cisco IOS Block Destination 교정
- 54-6페이지의 Cisco IOS Block Destination Network 교정
- 54-7페이지의 Cisco IOS Block Source 교정
- 54-7페이지의 Cisco IOS Block Source Network 교정

Cisco IOS Block Destination 교정

라이센스: FireSIGHT

Cisco IOS Block Destination 교정을 사용하면 라우터에서 상관관계 이벤트의 목적지 호스트로 전송되는 트래픽을 차단할 수 있습니다.

참고 검색 이벤트를 기반으로 하는 상관관계 규칙에 대한 응답으로서 이 교정을 사용하지 **마십시오**. 검색 이벤트는 소스 호스트만 전송하며 목적지 호스트는 전송하지 않습니다. 연결 이벤트 또는 침입 이벤트를 기반으로 하는 상관관계 규칙에 대한 응답으로 이 교정을 사용할 수 있습니다.

교정을 추가하려면

액세스: Admin/Discovery Admin

1단계 **Policies > Actions > Instances**를 선택합니다.

Instances 페이지가 나타납니다.

2단계 교정을 추가하려는 인스턴스 옆에 있는 보기 아이콘( )을 클릭합니다.

아직 인스턴스를 추가하지 않은 경우 54-4페이지의 Cisco IOS 인스턴스 추가을/를 참조하십시오.

Edit Instance 페이지가 나타납니다.

3단계 **Configured Remediations** 섹션에서 **Block Destination**을 선택하고 **Add**를 클릭합니다.

Edit Remediation 페이지가 나타납니다.

4단계 **Remediation Name** 필드에 교정의 이름을 입력합니다.

공백이나 특수 문자가 포함되지 않은, 알기 쉬운 이름을 지정해야 합니다. 예를 들어 여러 Cisco IOS 라우터 인스턴스 및 각 인스턴스에 대한 여러 교정이 있는 경우 `IOS_01_BlockDest`와 같은 이름을 지정할 수 있습니다.

5단계 선택적으로, 교정에 대한 설명을 **Description** 필드에 입력합니다.

6단계 **Create**를 클릭한 후 **Done**을 클릭합니다.

교정이 추가됩니다.

Cisco IOS Block Destination Network 교정

라이센스: FireSIGHT

Cisco IOS Block Destination Network 교정을 사용하면 라우터에서 상관관계 이벤트의 목적지 호스트 네트워크로 전송되는 트래픽을 차단할 수 있습니다.

참고 검색 이벤트를 기반으로 하는 상관관계 규칙에 대한 응답으로서 이 교정을 사용하지 **마십시오**. 검색 이벤트는 소스 호스트만 전송하며 목적지 호스트는 전송하지 않습니다. 연결 이벤트 또는 침입 이벤트를 기반으로 하는 상관관계 규칙에 대한 응답으로 이 교정을 사용할 수 있습니다.

교정을 추가하려면

액세스: Admin/Discovery Admin

1단계 **Policies > Actions > Instances**를 선택합니다.

Instances 페이지가 나타납니다.

2단계 교정을 추가하려는 인스턴스 옆에 있는 **View**를 클릭합니다.

아직 인스턴스를 추가하지 않은 경우 54-4페이지의 Cisco IOS 인스턴스 추가을/를 참조하십시오.

Edit Instance 페이지가 나타납니다.

3단계 **Configured Remediations** 섹션에서 **Block Destination Network**를 선택하고 **Add**를 클릭합니다.

Edit Remediation 페이지가 나타납니다.

4단계 **Remediation Name** 필드에 교정의 이름을 입력합니다.

공백이나 특수 문자가 포함되지 않은, 알기 쉬운 이름을 지정해야 합니다. 예를 들어 여러 Cisco IOS 라우터 인스턴스 및 각 인스턴스에 대한 여러 교정이 있는 경우 `IOS_01_BlockDestNet`와 같은 이름을 지정할 수 있습니다.

5단계 선택적으로, 교정에 대한 설명을 **Description** 필드에 입력합니다.

6단계 **Netmask** 필드에 서브넷 마스크를 입력하거나 CIDR 표기법을 사용하여 트래픽을 차단할 네트워크를 설명합니다.

예를 들어, 단일 호스트가 규칙을 트리거했을 때 전체 Class C 네트워크에 대한 트래픽을 차단하려면(권장 사항이 아님) 넷마스크로 `255.255.255.0` 또는 `24`를 사용합니다.

또 다른 예로, 트리거하는 IP 주소를 포함하는 30개 주소에 대한 트래픽을 차단하려면 넷마스크로 `255.255.255.224` 또는 `27`을 지정합니다. 이 경우 IP 주소 `10.1.1.15`가 교정을 트리거하면 `10.1.1.1`과 `10.1.1.30` 사이의 모든 IP 주소가 차단됩니다. 트리거하는 IP 주소만 차단하려면 필드를 비워두거나 `32`를 입력하거나 `255.255.255.255`를 입력합니다.

7단계 **Create**를 클릭한 후 **Done**을 클릭합니다.

교정이 추가됩니다.

Cisco IOS Block Source 교정

라이센스: FireSIGHT

Cisco IOS Block Source 교정을 사용하면 라우터에서 상관관계 정책을 위반하는 상관관계 이벤트에 포함된 소스 호스트로 전송되는 모든 트래픽을 차단할 수 있습니다. 소스 호스트는 상관관계 규칙의 기반이 되는 연결 이벤트 또는 침입 이벤트의 소스 IP 주소 또는 검색 이벤트의 호스트 IP 주소입니다.

교정을 추가하려면

액세스: Admin/Discovery Admin

1단계 **Policies > Actions > Instances**를 선택합니다.

Instances 페이지가 나타납니다.

2단계 교정을 추가하려는 인스턴스 옆에 있는 **View**를 클릭합니다.

아직 인스턴스를 추가하지 않은 경우 54-4페이지의 Cisco IOS 인스턴스 추가을/를 참조하십시오.

Edit Instance 페이지가 나타납니다.

3단계 **Configured Remediations** 섹션에서 **Block Source**를 선택하고 **Add**를 클릭합니다.

Edit Remediation 페이지가 나타납니다.

4단계 **Remediation Name** 필드에 교정의 이름을 입력합니다.

공백이나 특수 문자가 포함되지 않은, 알기 쉬운 이름을 지정해야 합니다. 예를 들어 여러 Cisco IOS 라우터 인스턴스 및 각 인스턴스에 대한 여러 교정이 있는 경우 `IOS_01_BlockSrc`와 같은 이름을 지정할 수 있습니다.

5단계 선택적으로, 교정에 대한 설명을 **Description** 필드에 입력합니다.

6단계 **Create**를 클릭한 후 **Done**을 클릭합니다.

교정이 추가됩니다.

Cisco IOS Block Source Network 교정

라이센스: FireSIGHT

Cisco IOS Block Source Network 교정을 사용하면 라우터에서 상관관계 이벤트의 소스 호스트 네트워크로 전송되는 트래픽을 차단할 수 있습니다. 소스 호스트는 상관관계 규칙의 기반이 되는 연결 이벤트 또는 침입 이벤트의 소스 IP 주소 또는 검색 이벤트의 호스트 IP 주소입니다.

교정을 추가하려면

액세스: Admin/Discovery Admin

1단계 **Policies > Actions > Instances**를 선택합니다.

Instances 페이지가 나타납니다.

2단계 교정을 추가하려는 인스턴스 옆에 있는 **View**를 클릭합니다.

아직 인스턴스를 추가하지 않은 경우 54-4페이지의 Cisco IOS 인스턴스 추가을/를 참조하십시오.

Edit Instance 페이지가 나타납니다.

3단계 **Configured Remediations** 섹션에서 **Block Source Network**를 선택하고 **Add**를 클릭합니다.

Edit Remediation 페이지가 나타납니다.

4단계 **Remediation Name** 필드에 교정의 이름을 입력합니다.

알기 쉬운 이름을 지정해야 하며 공백이나 특수 문자는 사용할 수 없습니다. 예를 들어 여러 Cisco IOS 라우터 인스턴스 및 각 인스턴스에 대한 여러 교정이 있는 경우 `IOS_01_BlockSourceNet`와 같은 이름을 지정할 수 있습니다.

5단계 선택적으로, 교정에 대한 설명을 **Description** 필드에 입력합니다.

6단계 **Netmask** 필드에 서브넷 마스크를 입력하거나 트래픽을 차단할 네트워크를 설명하는 CIDR 표기법을 입력합니다.

예를 들어, 단일 호스트가 규칙을 트리거했을 때 전체 Class C 네트워크에 대한 트래픽을 차단하려면(권장 사항이 아님) 넷마스크로 `255.255.255.0` 또는 `24`를 사용합니다.

또 다른 예로, 트리거하는 IP 주소를 포함하는 30개 주소에 대한 트래픽을 차단하려면 넷마스크로 `255.255.255.224` 또는 `27`을 지정합니다. 이 경우 IP 주소 `10.1.1.15`가 교정을 트리거하면 `10.1.1.1`과 `10.1.1.30` 사이의 모든 IP 주소가 차단됩니다. 트리거하는 IP 주소만 차단하려면 필드를 비워두거나 `32`를 입력하거나 `255.255.255.255`를 입력합니다.

7단계 **Create**를 클릭한 후 **Done**을 클릭합니다.

교정이 추가됩니다.

Cisco PIX 방화벽에 대한 교정 구성

라이센스: FireSIGHT

Cisco에서는 Cisco의 "shun" 명령을 사용하여 IP 주소나 네트워크를 차단할 수 있는 Cisco PIX Shun 교정 모듈을 제공합니다. 이 모듈은 상관관계 정책을 위반한 소스 또는 목적지 호스트에서 전송되는 모든 트래픽을 차단하고 모든 현재 연결을 종료합니다(방화벽을 통해 호스트*로* 전송되는 트래픽은 차단하지 않음).

Cisco PIX Shun 교정 모듈은 Cisco PIX Firewall 6.0 이상을 지원합니다. Cisco PIX 교정을 실행하려면 레벨 15 이상의 관리 액세스 권한이 있어야 합니다.

참고 목적지 기반 교정은 연결 이벤트 또는 침입 이벤트 기반의 상관관계 규칙이 트리거될 때 실행되도록 구성한 경우에만 작동합니다. 검색 이벤트는 소스 호스트를 전송하기만 합니다.

주의 Cisco PIX 교정이 활성화되는 경우 시간 초과 기간이 사용되지 않습니다. IP 주소 또는 네트워크의 차단을 해제하려면 방화벽에서 규칙을 수동으로 제거해야 합니다.

Cisco PIX 방화벽에 대한 교정을 생성하려면

액세스: Admin/Discovery Admin

1단계 방화벽에서 텔넷 또는 SSH를 활성화합니다(Cisco에서는 SSH 권장).

SSH 또는 텔넷 활성화에 대한 자세한 내용은 Cisco PIX 방화벽과 함께 제공되는 설명서를 참조하십시오.

2단계 방어 센터에서, 방어 센터와 함께 사용하려는 각 Cisco PIX 방화벽에 대해 Cisco PIX Shun 인스턴스를 추가합니다.

절차는 54-9페이지의 Cisco PIX 인스턴스 추가을/를 참조하십시오.

3단계 상관관계 정책이 위반될 때 방화벽에서 이끌어낼 응답의 유형을 기반으로 각 인스턴스에 대한 특정 교정을 생성합니다.

사용 가능한 교정 유형에 대해서는 다음 절에서 설명합니다.

- 54-10페이지의 Cisco PIX Block Destination 교정
- 54-11페이지의 Cisco PIX Block Source 교정

4단계 Cisco PIX 교정을 특정 상관관계 정책 규칙에 할당하기 시작합니다.

Cisco PIX 인스턴스 추가

라이센스: FireSIGHT

Cisco PIX 방화벽에서 SSH 또는 텔넷을 구성한 후 방어 센터에 인스턴스를 추가할 수 있습니다. 여러 방화벽으로 교정을 전송하려는 경우 각 방화벽에 대해 개별 인스턴스를 생성해야 합니다.

참고 Cisco에서는 텔넷 연결 대신 SSH 연결을 사용할 것을 권장합니다. SSH를 사용하여 전송된 데이터는 암호화되므로 텔넷보다 훨씬 안전합니다.

Cisco PIX 인스턴스를 추가하려면

액세스: Admin/Discovery Admin

1단계 **Policies > Actions > Instances**를 선택합니다.

Instances 페이지가 나타납니다.

2단계 **Add a New Instance** 목록에서 **Cisco PIX Shun**을 선택하고 **Add**를 클릭합니다.

Edit Instance 페이지가 나타납니다.

3단계 **Instance Name** 필드에 인스턴스의 이름을 입력합니다.

공백이나 특수 문자가 포함되지 않은, 알기 쉬운 이름을 지정해야 합니다. 예를 들어 둘 이상의 Cisco 방화벽에 연결하고자 하며 여러 인스턴스를 사용하려는 경우 `PIX_01`, `PIX_02` 등의 이름을 선택할 수 있습니다.

4단계 선택적으로, **Description** 필드에 인스턴스에 대한 설명을 입력합니다.

5단계 교정에 대해 사용하려는 Cisco PIX 방화벽의 IP 주소를 **PIX IP** 필드에 입력합니다.

6단계 기본값(`pix`)이 아닌 특정 사용자 이름이 필요한 경우 **Username** 필드에 입력합니다.

7단계 SSH 또는 텔넷을 사용하여 방화벽에 연결하는 데 필요한 비밀번호를 **Connection Password** 필드에 입력합니다. 두 필드에 입력한 비밀번호가 일치해야 합니다.

8단계 SSH 또는 텔넷 활성 비밀번호를 **Enable Password** 필드에 입력합니다. 이 비밀번호는 방화벽의 특권 모드로 들어가기 위해 사용되는 비밀번호입니다. 두 필드에 입력한 비밀번호가 일치해야 합니다.

9단계 교정에서 제외할 IP 주소를 한 줄에 하나씩 **White List** 필드에 입력합니다. CIDR 표기법 또는 특정 IP 주소를 사용할 수도 있습니다. 예를 들어 다음 화이트리스트는 시스템에서 허용됩니다.

```
10.1.1.152
172.16.1.0/24
```

이 화이트리스트는 자신이 작성한 규정 준수 화이트리스트와 연결되지 않습니다. FireSIGHT 시스템에서 CIDR 표기법을 사용하는 방법에 대한 자세한 내용은 1-19페이지의 IP 주소 표기 규칙을/를 참조하십시오.

10단계 방화벽에 연결하기 위해 사용할 방법을 **Protocol** 목록에서 선택합니다.

11단계 **Create**를 클릭합니다.

인스턴스가 생성되고 페이지의 Configured Remediations 섹션에 교정이 나타납니다. 상관관계 정책에서 인스턴스를 사용하려면 특정 교정을 추가해야 합니다. 자세한 내용은 다음 절을 참조하십시오.

- 54-10페이지의 Cisco PIX Block Destination 교정
- 54-11페이지의 Cisco PIX Block Source 교정

Cisco PIX Block Destination 교정

라이센스: FireSIGHT

Cisco PIX Block Destination 교정을 사용하면 상관관계 이벤트의 목적지 호스트로부터 전송되는 트래픽을 차단할 수 있습니다.

참고 검색 이벤트를 기반으로 하는 상관관계 규칙에 대한 응답으로서 이 교정을 사용하지 **마십시오**. 검색 이벤트는 소스 호스트만 전송하며 목적지 호스트는 전송하지 않습니다. 연결 이벤트 또는 침입 이벤트를 기반으로 하는 상관관계 규칙에 대한 응답으로 이 교정을 사용할 수 있습니다.

교정을 추가하려면

액세스: Admin/Discovery Admin

1단계 **Policies > Actions > Instances**를 선택합니다.

Instances 페이지가 나타납니다.

2단계 교정을 추가하려는 인스턴스 옆에 있는 **View**를 클릭합니다.

아직 인스턴스를 추가하지 않은 경우 54-9페이지의 Cisco PIX 인스턴스 추가을/를 참조하십시오.

Edit Instance 페이지가 나타납니다.

3단계 **Configured Remediations** 섹션에서 **Block Destination**을 선택하고 **Add**를 클릭합니다.

Edit Remediation 페이지가 나타납니다.

4단계 **Remediation Name** 필드에 교정의 이름을 입력합니다.

공백이나 특수 문자가 포함되지 않은, 알기 쉬운 이름을 지정해야 합니다. 예를 들어 여러 Cisco PIX 방화벽 인스턴스 및 각 인스턴스에 대한 여러 교정이 있는 경우 `PIX_01_BlockDest`와 같은 이름을 지정할 수 있습니다.

5단계 선택적으로, 교정에 대한 설명을 **Description** 필드에 입력합니다.

6단계 **Create**를 클릭한 후 **Done**을 클릭합니다.

교정이 추가됩니다.

Cisco PIX Block Source 교정

라이센스: FireSIGHT

Cisco PIX Block Source 교정을 사용하면 상관관계 정책을 위반하는 이벤트에 포함된 소스 호스트로부터 전송되는 트래픽을 차단할 수 있습니다. 소스 호스트는 상관관계 규칙의 기반이 되는 연결 이벤트 또는 침입 이벤트의 소스 IP 주소 또는 검색 이벤트의 호스트 IP 주소입니다.

교정을 추가하려면

액세스: Admin/Discovery Admin

1단계 **Policies > Actions > Instances**를 선택합니다.

Instances 페이지가 나타납니다.

2단계 교정을 추가하려는 인스턴스 옆에 있는 **View**를 클릭합니다.

아직 인스턴스를 추가하지 않은 경우 54-9페이지의 Cisco PIX 인스턴스 추가을/를 참조하십시오.

Edit Instance 페이지가 나타납니다.

3단계 **Configured Remediations** 섹션에서 **Block Source**를 선택하고 **Add**를 클릭합니다.

Edit Remediation 페이지가 나타납니다.

4단계 **Remediation Name** 필드에 교정의 이름을 입력합니다.

공백이나 특수 문자가 포함되지 않은, 알기 쉬운 이름을 지정해야 합니다. 예를 들어 여러 Cisco PIX 방화벽 인스턴스 및 각 인스턴스에 대한 여러 교정이 있는 경우 `PIX_01_BlockSrc`와 같은 이름을 지정할 수 있습니다.

5단계 선택적으로, 교정에 대한 설명을 **Description** 필드에 입력합니다.

교정이 추가됩니다.

Nmap 교정 구성

라이센스: FireSIGHT

트리거링 이벤트가 발생한 호스트를 스캔하여 상관관계 이벤트에 응답할 수 있습니다. 상관관계 이벤트를 트리거한 이벤트에서 포트만 스캔할 수도 있습니다.

상관관계 이벤트에 대한 응답에서 Nmap 스캐닝을 설정하려면 먼저 Nmap 스캔 인스턴스를 생성한 다음 Nmap 스캔 교정을 추가해야 합니다. 그런 다음 정책 내 규칙 위반에 대한 응답으로서 Nmap 스캐닝을 구성할 수 있습니다.

다음 절을 참조하십시오.

- 54-12페이지의 Nmap 스캔 인스턴스 추가
- 54-12페이지의 Nmap 스캔 교정

Nmap 스캔 인스턴스 추가

라이센스: FireSIGHT

네트워크의 호스트에서 운영 체제 및 서버 정보를 스캔하기 위해 사용할 각 Nmap 모듈에 대해 별도의 스캔 인스턴스를 설정할 수 있습니다. 방어 센터의 로컬 Nmap 모듈 및 원격으로 스캔을 실행하기 위해 사용할 관리되는 디바이스에 대해 스캔 인스턴스를 설정할 수 있습니다. 원격 관리되는 디바이스에서 스캔을 실행하는 경우에도, 각 스캔의 결과는 스캔을 구성하는 방어 센터에 항상 저장됩니다. 미션 크리티컬 호스트에 대한 악의적인 스캔 또는 실수로 이루어지는 스캔을 방지하려면, 인스턴스로 스캔해서는 안 되는 호스트를 나타내기 위해 인스턴스에 대한 블랙리스트를 생성할 수 있습니다.

기존 스캔 인스턴스와 동일한 이름의 스캔 인스턴스를 추가할 수 없습니다.

스캔 인스턴스를 생성하려면

액세스: Admin/Discovery Admin

1단계 **Policies > Actions > Instances**를 선택합니다.

Instances 페이지가 나타납니다.

2단계 **Add a module type** 드롭다운 목록에서 **Nmap Remediation (v1.0)**을 선택하고 **Add**를 클릭합니다.

Edit Instance 페이지가 나타납니다.

3단계 1~63자의 영숫자로 된 이름을 **Instance Name** 필드에 입력합니다. 밑줄(_)과 대시(-) 이외의 특수 문자 및 공백은 사용할 수 없습니다.

4단계 공백과 특수 문자를 포함하여 0~255자의 영숫자로 된 설명을 **Description** 필드에 지정합니다.

5단계 선택적으로, 다음 구문을 사용하여 이 스캔 인스턴스로 스캔해서는 *안 되는* 호스트 또는 네트워크를 **Black Listed Scan hosts** 필드에 지정합니다.

- IPv6 호스트의 경우 정확한 IP 주소(예: `2001:DB8::fedd:eeff`)
- IPv4 호스트의 경우 정확한 IP 주소(예: `192.168.1.101`) 또는 CIDR 표기법을 사용하는 IP 주소 블록(예: `192.168.1.0/24`는 `192.168.1.1`과 `192.168.1.254` 사이(포함)의 254개 호스트를 스캔함)

스캔 대상을 블랙리스트에 추가된 네트워크에 있는 호스트로 구체적으로 지정하는 경우 해당 스캔은 실행되지 않습니다. FireSIGHT 시스템에서 CIDR 표기법을 사용하는 방법에 대한 자세한 내용은 1-19페이지의 IP 주소 표기 규칙을/를 참조하십시오.

6단계 선택적으로, 방어 센터 대신 원격 관리되는 디바이스에서 스캔을 실행하려면 관리되는 디바이스의 이름 또는 IP 주소를 **Remote Device Name** 필드에 지정합니다.

7단계 **Create**를 클릭합니다.

스캔 인스턴스가 생성됩니다.

Nmap 스캔 교정

라이센스: FireSIGHT

Nmap 교정을 생성하여 Nmap 스캔에 대한 설정을 정의할 수 있습니다. Nmap 교정은 상관관계 정책에서 응답으로 사용하거나, 온디맨드 방식으로 실행하거나, 특정 시간에 실행되도록 예약할 수 있습니다. Nmap 스캔의 결과가 네트워크 맵에 나타나도록 하려면 스캔된 호스트가 이미 네트워크 맵에 있어야 합니다. NetFlow, 호스트 입력 기능 및 시스템 자체는 호스트를 네트워크 맵에 추가할 수 있습니다.

Nmap 교정의 특정 설정에 대한 자세한 내용은 47-2페이지의 Nmap 교정 이해을/를 참조하십시오.

Nmap 제공 서버 및 운영 체제 데이터는 또 다른 Nmap 스캔을 실행할 때까지 고정 상태로 유지됩니다. Nmap을 사용하여 호스트에서 운영 체제 및 서버 데이터를 스캔하려는 경우 Nmap 제공 운영 체제 및 서버 데이터를 최신 상태로 유지하기 위해 정기적인 예약 스캔을 설정할 수 있습니다. 자세한 내용은 62-5페이지의 Nmap 스캔 자동화을/를 참조하십시오. 또한 네트워크 맵에서 호스트가 삭제되면 해당 호스트에 대한 모든 Nmap 스캔 결과가 삭제됩니다.

Nmap 기능에 대한 자세한 내용은 http://insecure.org에서 제공하는 Nmap 설명서를 참조하십시오.

Nmap 교정을 생성하려면

액세스: Admin/Discovery Admin

1단계 **Policies > Actions > Scanners**를 선택합니다.

Scanners 페이지가 나타납니다.

2단계 교정을 추가하려는 스캔 인스턴스 옆에 있는 **Add Remediation**을 클릭합니다.

Edit Remediation 페이지가 나타납니다.

3단계 1~63자의 영숫자로 된 교정 이름을 **Remediation Name** 필드에 입력합니다. 밑줄(_)과 대시(-) 이외의 특수 문자 및 공백은 사용할 수 없습니다.

4단계 공백과 특수 문자를 포함하여 0~255자의 영숫자로 된 교정 설명을 **Description** 필드에 입력합니다.

5단계 침입 이벤트, 연결 이벤트 또는 사용자 이벤트를 트리거하는 상관관계 규칙에 대한 응답으로 이 교정을 사용하려는 경우 **Scan Which Address(es) From Event?** 옵션을 구성합니다.

- 이벤트에서 소스 IP 주소 및 목적지 IP 주소로 표시되는 호스트를 스캔하려면 **Scan Source and Destination Addresses**를 선택합니다.
- 이벤트의 소스 IP 주소로 표시되는 호스트를 스캔하려면 **Scan Source Address Only**를 선택합니다.
- 이벤트의 목적지 IP 주소로 표시되는 호스트를 스캔하려면 **Scan Destination Address Only**를 선택합니다.

검색 이벤트 또는 호스트 입력 이벤트에서 트리거되는 상관관계 규칙에 대한 응답으로 이 교정을 사용하려는 경우, 기본적으로 교정은 이벤트와 관련된 호스트의 IP 주소를 스캔합니다. 이 옵션을 구성할 필요가 없습니다.

참고 트래픽 프로필 변경을 트리거하는 상관관계 규칙에는 Nmap 교정을 응답으로서 할당하지 **마십시오**.

6단계 **Scan Type** 옵션을 구성합니다.

- TCP 연결을 시작하기만 하고 완료하지 않음으로써, `admin` 계정이 원시 패킷 액세스 권한을 가지고 있거나 IPv6이 실행되지 않고 있는 호스트의 스텔스(stealth) 모드에서 빠르게 스캔하려면 **TCP Syn Scan**을 선택합니다.
- 방어 센터의 `admin` 계정이 원시 패킷 액세스 권한을 가지고 있지 않거나 IPv6이 실행되고 있는 호스트에서 사용할 수 있는 시스템 `connect()` 호출을 사용하여 스캔하려면 **TCP Connect Scan**을 선택합니다.
- 포트의 필터링 여부를 확인하기 위해 ACK 패킷을 전송하려면 **TCP ACK Scan**을 선택합니다.
- 포트의 필터링 여부를 확인하는 것은 물론 포트가 열려 있는지 여부를 확인하기 위해 ACK 패킷을 전송하려면 **TCP Window Scan**을 선택합니다.
- FIN/ACK 프로브를 사용하여 BSD 파생 시스템을 식별하려면 **TCP Maimon Scan**을 선택합니다.

7단계 선택적으로, TCP 포트 외에 UDP 포트도 스캔하려면 **Scan for UDP ports** 옵션에 대해 **On**을 선택합니다.

팁 UDP 포트스캔이 TCP 포트스캔보다 시간이 더 걸립니다. 스캔 속도를 높이려면 이 옵션을 비활성화하십시오.

8단계 상관관계 정책 위반에 대한 응답으로 이 교정을 사용하려는 경우 **Use Port From Event** 옵션을 구성합니다.

- 12단계에서 지정한 포트 대신 상관관계 이벤트의 포트를 스캔하려면 **On**을 선택합니다.

  상관관계 이벤트의 포트를 스캔하는 경우 교정은 8단계에서 지정한 IP 주소의 포트를 스캔한다는 점에 유의하십시오. 또한 이러한 포트는 교정의 동적 스캔 대상에 추가됩니다.
- 12단계에서 지정하는 포트만 스캔하려면 **Off**를 선택합니다.

9단계 상관관계 정책 위반에 대한 응답으로 이 교정을 사용하고 이벤트를 탐지한 탐지 엔진을 실행하는 어플라이언스를 사용하여 스캔을 실행하려는 경우 **Scan from reporting detection engine** 옵션을 구성합니다.

- 보고 탐지 엔진을 실행하는 어플라이언스에서 스캔하려면 **On**을 선택합니다.
- 교정에서 구성된 어플라이언스에서 스캔하려면 **Off**를 선택합니다.

10단계 **Fast Port Scan** 옵션을 구성합니다.

- 스캐닝을 수행하는 관리되는 디바이스의 `/var/sf/nmap/share/nmap/nmap-services` 디렉토리에 있는 `nmap-services` 파일에 나열된 포트만 스캔하고 다른 포트 설정은 무시하려면 **On**을 선택합니다.
- 모든 TCP 포트를 스캔하려면 **Off**를 선택합니다.

11단계 Nmap 구문을 사용하여 기본적으로 스캔할 포트를 원하는 스캔 순서대로 **Port Ranges and Scan Order** 필드에 입력합니다.

1~65535의 값을 지정합니다. 쉼표나 공백을 사용하여 포트를 구분합니다. 하이픈을 사용하여 포트 범위를 지정할 수도 있습니다. TCP 및 UDP 포트를 모두 스캔하는 경우, 스캔할 TCP 포트의 목록 앞에는 T를 추가하고 UDP 포트의 목록 앞에는 U를 추가합니다. 예를 들어 UDP 트래픽에 대해 포트 53 및 111을 스캔하고 TCP 트래픽에 대해 포트 21-25를 스캔하려면 `U:53,111,T:21-25`를 입력합니다.

8단계에 설명된 대로, 상관관계 정책 위반에 대한 응답으로 교정이 실행되는 경우 **Use Port From Event** 옵션은 이 설정을 재정의합니다.

12단계 열린 포트에서 서버 공급업체 및 버전 정보를 조사하려면 **Probe open ports for vendor and version information:**을 구성합니다.

- 호스트의 열린 포트에서 서버 정보를 스캔하여 서버 공급업체 및 버전을 식별하려면 **On**을 선택합니다.
- 호스트에 대한 서버 정보를 계속해서 사용하려면 **Off**를 선택합니다.

13단계 열린 포트를 조사하려는 경우 **Service Version Intensity** 드롭다운 목록에서 숫자를 선택하여 사용되는 프로브의 수를 설정합니다.

- 더 오래 걸리지만 더 정확한 스캔을 위해 더 많은 프로브를 사용하려면 더 높은 숫자를 선택합니다.
- 덜 정확하지만 더 빠른 스캔을 위해 더 적은 프로브를 사용하려면 더 낮은 숫자를 선택합니다.

14단계 운영 체제 정보를 스캔하려면 **Detect Operating System** 설정을 구성합니다.

- 호스트에서 운영 체제를 식별하기 위한 정보를 스캔하려면 **On**을 선택합니다.
- 호스트에 대한 운영 체제 정보를 계속해서 사용하려면 **Off**를 선택합니다.

15단계 호스트 검색 발생 여부 및 포트 스캔을 사용 가능한 호스트에 대해서만 실행할지 여부를 결정하려면 **Treat All Hosts As Online**:을 구성합니다.

- 호스트 검색 프로세스를 건너뛰고 대상 범위의 모든 호스트에서 포트 스캔을 실행하려면 **On**을 선택합니다.
- **Host Discovery Method** 및 **Host Discovery Port List**에 대한 설정을 사용하여 호스트 검색을 수행하고 사용할 수 없는 호스트에 대한 포트 스캔은 건너뛰려면 **Off**를 선택합니다.

16단계 호스트가 있으며 사용 가능한지를 알아보기 위해 Nmap으로 테스트할 때 사용할 방법을 선택합니다.

- SYN 플래그 세트와 함께 빈 TCP 패킷을 전송하고 닫힌 포트에서 RST 응답을 유도하거나 호스트에서 사용 가능한 열린 포트에서 SYN/ACK 응답을 유도하려면 **TCP SYN**을 선택합니다.

  이 옵션은 기본적으로 포트 80을 스캔하며, TCP SYN 스캔은 스테이트풀 방화벽 규칙이 있는 방화벽에 의해 차단될 가능성이 희박하다는 점에 유의해야 합니다.
- ACK 플래그 세트와 함께 빈 TCP 패킷을 전송하고 사용 가능한 호스트에서 RST 응답을 유도하려면 **TCP ACK** 를 선택합니다.

  이 옵션은 기본적으로 포트 80을 스캔하며, TCP ACK 스캔은 스테이트리스 방화벽 규칙이 있는 방화벽에 의해 차단될 가능성이 희박하다는 점에 유의해야 합니다.
- 사용 가능한 호스트의 닫힌 포트에서 포트 도달 불가 응답을 유도하기 위해 UDP 패킷을 전송하려면 **UDP**를 선택합니다. 이 옵션은 기본적으로 포트 40125를 스캔합니다.

17단계 호스트 검색 중 사용자 지정 포트 목록을 스캔하려면 선택한 호스트 검색 방법에 적절한 포트 목록을 쉼표로 구분하여 **Host Discovery Port List**에 입력합니다.

18단계 호스트 검색 및 서버, 운영 체제, 취약성 검색에 대해 기본 Nmap 스크립트 세트를 사용할지 여부를 제어하려면 **Default NSE Scripts** 옵션을 구성합니다.

- 기본 Nmap 스크립트 세트를 실행하려면 **On**을 선택합니다.
- 기본 Nmap 스크립트 세트를 건너뛰려면 **Off**를 선택합니다.

기본 스크립트 목록은 http://nmap.org/nsedoc/categories/default.html 을/를 참조하십시오.

19단계 스캔 프로세스의 타이밍을 설정하려면 타이밍 템플릿 번호를 선택합니다. 번호가 높으면 스캔이 더 빠르고 덜 포괄적이며, 번호가 낮으면 더 느리고 좀 더 포괄적입니다.

20단계 **Save**를 클릭한 후 **Done**을 클릭합니다.

교정이 생성됩니다.

Set Attribute 교정 구성

라이센스: FireSIGHT

트리거링 이벤트가 발생한 호스트에서 호스트 특성 값을 설정하여 상관관계 이벤트에 응답할 수 있습니다. 텍스트 호스트 특성의 경우 이벤트의 설명을 특성 값으로 사용하도록 선택할 수 있습니다. 호스트 특성에 대한 자세한 내용은 49-30페이지의 사전 정의 호스트 특성 작업 및 49-31페이지의 사용자 정의 호스트 특성 작업을/를 참조하십시오.

상관관계 이벤트에 대한 응답에서 특성 값 설정을 구성하려면 먼저 set attribute 인스턴스를 생성한 다음 set attribute 교정을 추가해야 합니다. 그런 다음 정책 내 규칙 위반에 대한 응답으로서 특성 값 업데이트를 구성할 수 있습니다.

자세한 내용은 다음 절을 참조하십시오.

- 54-16페이지의 Set Attribute 값 인스턴스 추가
- 54-16페이지의 Set Attribute 값 교정

Set Attribute 값 인스턴스 추가

라이센스: FireSIGHT

상관관계 규칙 위반에 대한 응답에서 특성 값을 설정하도록 인스턴스를 설정할 수 있습니다.

Set attribute 인스턴스를 생성하려면

액세스: Admin/Discovery Admin

1단계 **Policies > Actions > Instances**를 선택합니다.

Instances 페이지가 나타납니다.

2단계 **Add a module type** 드롭다운 목록에서 **Set Attribute Value (v1.0)**를 선택하고 **Add**를 클릭합니다.

Edit Instance 페이지가 나타납니다.

3단계 1~63자의 영숫자로 된 이름을 **Instance Name** 필드에 입력합니다. 밑줄(_)과 대시(-) 이외의 특수 문자 및 공백은 사용할 수 없습니다.

4단계 공백과 특수 문자를 포함하여 0~255자의 영숫자로 된 설명을 **Description** 필드에 지정합니다.

5단계 **Create**를 클릭합니다.

인스턴스가 생성됩니다.

Set Attribute 값 교정

라이센스: FireSIGHT

상관관계 규칙 위반에 대한 응답에서 설정하고자 하는 각 특성 값에 대해 set attribute 값 교정을 생성할 수 있습니다. 설정하려는 특성이 텍스트 특성인 경우, 이벤트의 설명을 특성 값으로 사용하도록 교정을 설정할 수 있습니다.

Set attribute 값 교정을 생성하려면

액세스: Admin/Discovery Admin

1단계 **Policies > Actions > Instances**를 선택합니다.

Instances 페이지가 나타납니다.

2단계 교정을 추가하려는 스캔 인스턴스 옆에 있는 **View**를 클릭합니다.

Edit Instance 페이지가 나타납니다.

3단계 **Add a new remediation of type** 드롭다운 목록에서 **Set Attribute Value**를 선택합니다.

Edit Remediation 페이지가 나타납니다.

4단계 1~63자의 영숫자로 된 교정 이름을 **Remediation Name** 필드에 입력합니다. 밑줄(_)과 대시(-) 이외의 특수 문자 및 공백은 사용할 수 없습니다.

5단계 공백과 특수 문자를 포함하여 0~255자의 영숫자로 된 교정 설명을 **Description** 필드에 입력합니다.

6단계 침입 이벤트, 사용자 이벤트 또는 연결 이벤트를 트리거하는 상관관계 규칙에 대한 응답으로 이 교정을 사용하려는 경우 **Update Which Host(s) From Event** 옵션을 구성합니다.

- 이벤트의 소스 IP 주소 및 목적지 IP 주소로 표시되는 호스트에 대한 특성 값을 업데이트하려면 **Update Source and Destination Hosts**를 선택합니다.

- 이벤트의 소스 IP 주소로 표시되는 호스트에 대한 특성 값을 업데이트하려면 **Update Source Host Only**를 선택합니다.
- 이벤트의 목적지 IP 주소로 표시되는 호스트에 대한 특성 값을 업데이트하려면 **Update Destination Host Only**를 선택합니다.

검색 이벤트 또는 호스트 입력 이벤트에서 트리거되는 상관관계 규칙에 대한 응답으로 이 교정을 사용하려는 경우, 기본적으로 교정은 이벤트와 관련된 호스트의 IP 주소를 스캔합니다. 이 옵션을 구성할 필요가 없습니다.

7단계 **Use Description From Event For Attribute Value (text attributes only)** 옵션을 구성합니다.

- 이벤트의 설명을 특성 값으로 사용하려면 **On**을 선택합니다.
- 교정에 대한 Attribute Value 설정을 특성 값으로 사용하려면 **Off**를 선택합니다.

8단계 이벤트 설명을 사용하지 않으려는 경우 설정하려는 특성 값을 **Attribute Value** 필드에 입력합니다.

9단계 **Save**를 클릭한 후 **Done**을 클릭합니다.

교정이 생성됩니다.

교정 상태 이벤트 작업

라이센스: FireSIGHT

교정이 트리거되면 교정 상태 이벤트가 생성됩니다. 이러한 이벤트는 데이터베이스에 로깅되며 Remediation Status 페이지에서 볼 수 있습니다. 교정 상태 이벤트를 검색하고 보고 삭제할 수 있습니다.

자세한 내용은 다음 링크를 참고하십시오.

- 58-22페이지의 이벤트 시간 제약 조건 설정
- 54-21페이지의 교정 상태 이벤트 검색

교정 상태 이벤트 보기

라이센스: FireSIGHT

교정 상태 이벤트에 액세스할 때 표시되는 페이지는 사용하는 워크플로에 따라 달라집니다. 교정 테이블 보기를 포함하는 사전 정의 워크플로를 사용할 수 있습니다. 테이블 보기에는 각 교정 상태 이벤트의 행이 포함됩니다. 특정 요구와 일치하는 정보만 표시하는 사용자 지정 워크플로를 생성할 수도 있습니다. 사용자 지정 워크플로 생성에 대한 자세한 내용은 58-38페이지의 사용자 지정 워크플로 생성을/를 참조하십시오.

다음 표에서는 교정 상태 이벤트 워크플로 페이지에서 수행할 수 있는 몇 가지 특정 작업에 대해 설명합니다.

표 54-1 교정 상태 이벤트 보기를 위한 옵션

목적	가능한 작업
나타나는 열에 대해 자세히 알아보기	54-19페이지의 교정 상태 테이블 이해에서 자세히 알아보십시오.
표시된 이벤트에 대한 시간 및 날짜 범위 수정	58-22페이지의 이벤트 시간 제약 조건 설정을/를 참조하십시오. 어플라이언스의 구성된 시간 창(전역이든 이벤트 전용이든)을 벗어나 생성된 이벤트는 시간 기준으로 이벤트 보기를 제한할 경우 이벤트 보기에 나타날 수 있습니다. 이는 어플라이언스에 대한 슬라이딩 시간 창을 구성한 경우에도 발생할 수 있습니다.
이벤트 분류 및 제한	58-30페이지의 이벤트 제한 및 58-34페이지의 드릴다운 워크플로 페이지 정렬을/를 참조하십시오.
일시적으로 다른 워크플로 사용	워크플로 제목 옆에 있는 **(switch workflow)**를 클릭합니다. 자세한 내용은 58-16페이지의 워크플로 선택을/를 참조하십시오.
상관관계 이벤트 보기로 이동하여 관련 이벤트 보기	**Correlation Events**를 클릭합니다. 자세한 내용은 58-35페이지의 워크플로 간 이동을/를 참조하십시오.
신속하게 다시 돌아올 수 있도록 현재 페이지 북마크 지정	**Bookmark This Page**를 클릭합니다. 자세한 내용은 58-36페이지의 북마크 사용을/를 참조하십시오.
북마크 관리 페이지로 이동	**View Bookmarks**를 클릭합니다. 자세한 내용은 58-36페이지의 북마크 사용을/를 참조하십시오.
테이블 보기의 데이터를 기반으로 보고서 생성	**Report Designer**를 클릭합니다. 자세한 내용은 57-9페이지의 이벤트 보기에서 보고서 템플릿 생성을/를 참조하십시오.
워크플로의 다음 페이지로 드릴다운하여 특정 값으로 제한	다음 방법 중 하나를 사용합니다. • 사용자 지정 워크플로에서 생성한 드릴다운 페이지에서 행 내의 값을 클릭합니다. 테이블 보기의 행 내에서 값을 클릭하면 테이블 보기가 제한되며 다음 페이지로 드릴다운되지 **않습니다**. • 일부 사용자로 제한하여 다음 워크플로 페이지로 드릴다운하려면, 다음 워크플로 페이지에서 볼 사용자의 옆에 있는 확인란을 선택하고 **View**를 클릭합니다. • 현재의 제약 조건을 유지한 채 다음 워크플로 페이지로 드릴다운하려면 **View All**을 클릭합니다. **팁** 테이블 보기의 페이지 이름에는 항상 "Table View"가 포함됩니다. 자세한 내용은 58-30페이지의 이벤트 제한을/를 참조하십시오.
시스템에서 교정 상태 이벤트 삭제	다음 방법 중 하나를 사용합니다. • 일부 이벤트를 삭제하려면 삭제할 이벤트 옆에 있는 확인란을 선택하고 **Delete**를 클릭합니다. • 현재 제한된 보기에서 모든 이벤트를 삭제하려면 **Delete All**을 클릭하고 모든 이벤트를 삭제할 것인지를 확인합니다.
교정 상태 이벤트 검색	**Search**를 클릭합니다. 자세한 내용은 54-21페이지의 교정 상태 이벤트 검색을/를 참조하십시오.

교정 상태 이벤트를 보려면

액세스: Admin

1단계 **Analysis > Correlation > Status**를 선택합니다.

기본 교정 워크플로의 첫 번째 페이지가 나타납니다. 사용자 지정 워크플로를 비롯한 다른 워크플로를 사용하려면 워크플로 제목 옆의 **(switch workflow)**를 클릭합니다. 다른 기본 워크플로 지정에 대한 자세한 내용은 71-3페이지의 이벤트 보기 설정 구성을/를 참조하십시오. 이벤트가 표시되지 않을 경우 시간 범위를 조정해야 할 수 있습니다. 58-22페이지의 이벤트 시간 제약 조건 설정을/를 참조하십시오.

팁 교정의 테이블 보기가 포함되지 않은 사용자 지정 워크플로를 사용 중인 경우 워크플로 제목 옆에 있는 **(switch workflow)** 메뉴를 클릭한 다음 **Remediation Status**를 선택하십시오.

교정 상태 이벤트 작업

라이센스: FireSIGHT

이벤트 보기의 레이아웃을 변경하거나, 보기의 이벤트를 필드 값으로 제한할 수 있습니다.

열을 비활성화할 경우 (나중에 다시 추가하지 않는 한) 세션 기간 동안 비활성화됩니다. 첫 번째 열을 비활성화할 때 Count 열이 추가됩니다.

테이블 보기의 행 내에서 값을 클릭하면 테이블 보기가 제한되며 다음 페이지로 드릴다운되지 않습니다.

팁 테이블 보기의 페이지 이름에는 항상 "Table View"가 포함됩니다.

자세한 내용은 다음 항목을 참조하십시오.

- 58-30페이지의 이벤트 제한
- 58-32페이지의 복합 제약 조건 사용
- 58-34페이지의 드릴다운 워크플로 페이지 정렬
- 54-19페이지의 교정 상태 테이블 이해

교정 상태 테이블 이해

라이센스: FireSIGHT

정책 위반 및 검색 이벤트에 대한 다양한 응답을 실행하도록 방어 센터를 구성할 수 있습니다. 이러한 응답에는 정책 위반 시 방화벽이나 라우터에서 호스트를 차단하는 등의 교정이 포함됩니다. 교정이 트리거되면 교정 상태 이벤트가 생성되고 데이터베이스에 로깅됩니다. 교정에 대한 자세한 내용은 54-1페이지의 교정 구성을/를 참조하십시오.

다음 표에서는 교정 상태 테이블의 필드에 대해 설명합니다.

표 54-2 교정 상태 필드

필드	설명
Policy	위반되어 교정을 트리거한 상관관계 정책의 이름
Remediation Name	실행된 교정의 이름
Result Message	교정이 실행되었을 때 발생한 상황을 설명하는 메시지. 상태 메시지는 다음과 같습니다. • Successful completion of remediation • Error in the input provided to the remediation module • Error in the remediation module configuration • Error logging into the remote device or server • Unable to gain required privileges on remote device or server • Timeout logging into remote device or server • Timeout executing remote commands or servers • The remote device or server was unreachable • The remediation was attempted but failed • Failed to execute remediation program • Unknown/unexpected error **참고** 사용자 지정 교정 모듈이 설치된 경우 사용자 지정 모듈에 의해 구현되는 추가 상태 메시지를 볼 수 있습니다.
Rule	교정을 트리거한 규칙의 이름
Time	방어 센터가 교정을 트리거한 날짜 및 시간
Count	각 행에 표시되는 정보와 매칭되는 이벤트의 수. 둘 이상의 동일한 행을 생성하는 제약 조건을 적용한 경우에만 Count 필드가 나타납니다.

교정 상태 이벤트의 테이블 보기를 표시하려면

액세스: Admin

1단계 **Analysis > Correlation > Status**를 선택합니다.

테이블 보기가 나타납니다. 교정 상태 이벤트 작업에 대한 자세한 내용은 54-17페이지의 교정 상태 이벤트 작업을/를 참조하십시오.

팁 교정 상태 이벤트의 테이블 보기가 포함되지 않은 사용자 지정 워크플로를 사용 중인 경우 워크플로 제목 옆에 있는 **(switch workflow)**를 클릭한 다음 **Remediation Status**를 선택하십시오.

교정 상태 이벤트 검색

라이센스: FireSIGHT

특정 교정이 실행되었는지 여부 및 언제 실행되었는지를 확인하려면 교정 상태 이벤트를 검색할 수 있습니다. 네트워크 환경에 맞춤화된 검색을 생성한 다음 나중에 다시 사용할 수 있도록 저장할 수 있습니다. 사용할 수 있는 검색 기준은 다음 표에 설명되어 있습니다.

표 54-3 교정 상태 검색 기준

검색 필드	설명
Result Message	매칭할 결과 메시지(교정이 실행되었을 때 발생한 상황을 설명하는 메시지)의 **정확한** 이름을 입력합니다. 유효한 상태 메시지는 다음과 같습니다. • Successful completion of remediation • Error in the input provided to the remediation module • Error in the remediation module configuration • Error logging into the remote device or server • Unable to gain required privileges on remote device or server • Timeout logging into remote device or server • Timeout executing remote commands or servers • The remote device or server was unreachable • The remediation was attempted but failed • Failed to execute remediation program • Unknown/unexpected error **참고** 사용자 지정 교정 모듈이 설치된 경우 사용자 지정 모듈에 의해 구현된 추가 상태 메시지를 입력할 수 있습니다.
Time	방어 센터가 교정을 트리거한 날짜 및 시간을 지정합니다. 시간 입력을 위한 구문은 60-5페이지의 검색에서 시간 제약 조건 지정을/를 참조하십시오.
Remediation Name	실행된 교정의 정확한 이름을 입력합니다. 이 이름은 교정을 생성할 때 지정한 이름입니다.
Policy	교정을 트리거한 상관관계 정책의 이름을 입력합니다.
Rule	교정을 트리거한 상관관계 규칙의 이름을 입력합니다.

저장된 검색을 로드 및 삭제하는 방법을 포함하여 검색에 대한 자세한 내용은 60-1페이지의 이벤트 검색을/를 참조하십시오.

교정 상태 이벤트를 검색하려면

액세스: Admin

1단계 **Analysis > Search**를 선택합니다.

Search 페이지가 나타납니다.

2단계 테이블 드롭다운 목록에서 **Remediation Status**를 선택합니다.

팁 데이터베이스에서 서로 다른 종류의 이벤트를 검색하려면 테이블 드롭다운 목록에서 선택합니다.

3단계 교정 상태 검색 기준 표에 설명된 대로 해당 필드에 검색 기준을 입력합니다.

여러 필드에 대한 조건을 입력하는 경우 모든 필드에 대해 지정한 검색 기준과 일치하는 레코드만 반환됩니다.

4단계 선택적으로, 검색을 저장하려면 **Private** 확인란을 선택하여 자신만 액세스할 수 있는 비공개로 검색을 저장할 수 있습니다. 또는 모든 사용자가 사용할 수 있도록 검색을 저장하려면 확인란을 선택하지 않습니다.

팁 제한된 이벤트 분석가 사용자에 대한 제한으로서 검색을 저장하려면 **반드시** 비공개 검색으로 저장해야 합니다.

5단계 선택적으로, 나중에 다시 사용할 수 있도록 검색을 저장할 수 있습니다. 다음 옵션을 이용할 수 있습니다.

- 검색 기준을 저장하려면 **Save**를 클릭합니다.

  새 검색인 경우 검색 이름을 입력하도록 대화 상자가 나타납니다. 고유한 검색 이름을 입력하고 **Save**를 클릭합니다. 이미 존재하는 검색에 대한 새 조건을 저장하는 경우 프롬프트가 나타나지 않습니다. 나중에 실행할 수 있도록 검색이 저장됩니다(**Private**을 선택한 경우 자신만 볼 수 있음).

- 새 검색을 저장하거나, 저장된 기존 검색을 변경하여 만든 검색에 새 이름을 할당하려면 **Save As New**를 클릭합니다.

  검색 이름을 입력하도록 대화 상자가 나타납니다. 고유한 검색 이름을 입력하고 **Save**를 클릭합니다. 나중에 실행할 수 있도록 검색이 저장됩니다(**Private**을 선택한 경우 자신만 볼 수 있음).

6단계 검색을 시작하려면 **Search**를 클릭합니다.

검색 결과는 현재의 시간 범위로 제한되어 기본 교정 상태 워크플로에 나타납니다. 사용자 지정 워크플로를 비롯한 다른 워크플로를 사용하려면 워크플로 제목 옆의 **(switch workflow)**를 클릭합니다. 다른 기본 워크플로 지정에 대한 자세한 내용은 71-3페이지의 이벤트 보기 설정 구성을/를 참조하십시오.

55장

대시보드 사용

FireSIGHT 시스템 대시보드는 시스템에 의해 수집 및 생성된 이벤트에 대한 데이터를 비롯하여 현재 시스템 상태를 한눈에 볼 수 있는 보기를 제공합니다. 또한 구축에서 어플라이언스의 전체적인 상태에 대한 정보를 확인하는 데에도 대시보드를 사용할 수 있습니다. 특정 사용자 역할(Administrator, Maintenance User, Security Analyst, Security Analyst[Read Only], 대시보드 권한이 있는 사용자 지정 역할)만 대시보드에 액세스할 수 있습니다. 기타 역할의 경우 역할과 관련된 페이지가 기본 시작 페이지로 표시됩니다(예: Discovery Admin에게는 Network Discovery 페이지 표시).

대시보드에는 하나 이상의 탭이 있으며, 각 탭의 3단 레이아웃에 하나 이상의 위젯을 표시할 수 있습니다. 위젯이란 FireSIGHT 시스템의 서로 다른 부분에 대한 통찰력을 제공하는 자체 포함형 소형 구성 요소입니다. FireSIGHT 시스템에서는 사전 정의된 위젯을 여러 개 제공합니다. 예를 들어 Appliance Information 위젯은 어플라이언스 이름, 모델, 원격 관리자, 현재 실행 중인 FireSIGHT 시스템 소프트웨어의 버전을 알려줍니다.

대시보드에는 위젯을 제한하는 시간 범위가 있습니다. 시간 범위를 마지막 시간 단위로 짧게, 또는 마지막 연도 단위로 길게 반영하도록 구성할 수 있습니다.

대시보드는 복잡하고 사용자 지정 기능이 뛰어난 모니터링 기능입니다. 많은 유형의 시스템 데이터를 보는 또 다른 방법은, 세분화를 위한 필터와 함께(일시적으로만) 미리 설정된 시각적 컨텍스트 집합의 침입, 연결, 검색 데이터를 사용하여 정보를 제공하는 Context Explorer입니다. FireSIGHT 시스템 대시보드에서 사용할 수 있는 포괄적인 데이터와는 달리 Context Explorer에서는 모니터링되는 네트워크의 모양과 활동을 다양한 색상으로 명확하고 간결하게 보여줍니다. Context Explorer에 대한 자세한 내용은 56-1페이지의 Context Explorer 사용을/를 참조하십시오.

각 어플라이언스 유형에서는 Summary Dashboard라는 기본 대시보드를 제공합니다. 이 대시보드는 일반 FireSIGHT, 침입, 위협 탐지, 지오로케이션, FireSIGHT 시스템 구축에 대한 시스템 상태 정보 등을 일반 사용자에게 제공합니다. 일부 위젯은 특정 유형의 어플라이언스에만 유용하므로 사용자가 방어 센터 가상 방어 센터, 관리되는 디바이스 중 무엇을 사용하는지에 따라 Summary Dashboard가 달라집니다.

참고 관리되는 가상 디바이스는 웹 인터페이스가 없으며 대시보드를 지원하지 않습니다.

기본적으로 어플라이언스의 홈 페이지에는 Summary Dashboard가 표시되지만, 사용자는 고유한 기본 홈 페이지를 표시하도록 어플라이언스를 구성할 수 있습니다.

팁 홈 페이지를 변경하는 경우 **Overview > Dashboards**를 선택하여 대시보드에 액세스할 수 있습니다. 자세한 내용은 55-37페이지의 대시보드 보기을/를 참조하십시오.

표시되는 데이터는 관리되는 디바이스의 라이센스 및 구축 방법, 데이터를 제공하는 기능의 구성 여부(Series 2 어플라이언스 및 Cisco NGIPS for Blue Coat X-Series의 경우), 데이터를 제공하는 기능을 어플라이언스가 지원하는지 여부 등의 요소에 따라 달라집니다. 예를 들어 DC500 방어 센터와 Series 2 디바이스 모두 카테고리 및 평판 기준 URL 필터링을 지원하지 않으므로 DC500 방어 센터에는 이 기능에 대한 데이터가 표시되지 않으며 Series 2 디바이스에서는 이 데이터가 탐지되지 않습니다.

Summary Dashboard 외에도 방어 센터에서는 다음과 같은 사전 정의된 대시보드를 제공합니다.

- Application Statistics 대시보드 - 모니터링된 네트워크의 애플리케이션 활동과 침입 이벤트에 대한 자세한 정보를 제공합니다. 이 대시보드를 사용하면 어떤 애플리케이션이 가장 많은 트래픽, 허용 및 거부되는 연결, 침입 이벤트를 생성하는지를 추적하는 것은 물론 사용 중인 고유한 애플리케이션의 수 및 그러한 애플리케이션의 예상 위험과 비즈니스 연관성도 파악할 수 있습니다.
- Connection Summary 대시보드 - 연결 데이터를 사용해 모니터링되는 네트워크에서 활동의 테이블과 차트를 생성할 수 있습니다. 이 대시보드를 사용하면 네트워크의 연결 및 트래픽과 관련된 initiator IP와 responder IP, 포트, 애플리케이션, 연결과 트래픽의 전체 양, 지오로케이션 정보를 추적할 수 있습니다. 데이터를 생성하려면 이 대시보드에 대한 연결을 기록해야 합니다. 39-2페이지의 연결 및 보안 인텔리전스 데이터 이해을/를 참조하십시오. 이 위젯의 출력은 연결 로깅 컨피그레이션에 따라 달라집니다.

팁 이 대시보드의 위젯은 총 트래픽을 킬로바이트(KB) 단위로 나열합니다. KB 단위의 총 트래픽은 KB/s 단위의 트래픽과 선택한 시간 창에서 처리한 총 시간(초)을 곱한 값과 같습니다.

- Detailed Dashboard - 고급 사용자에게 FireSIGHT 시스템 구축에 대한 자세한 정보를 제공하며, 여기에 포함된 여러 위젯은 Cisco 뉴스 및 제품 업데이트에 대한 정보를 제공하는 것은 물론 수집된 침입 이벤트, 네트워크 검색, 규정 준수, 상관관계, 트래픽, 시스템 상태 데이터를 요약하여 보여줍니다. 이 대시보드를 사용하면 매우 광범위한 네트워크 정보를 동시에 모니터링할 수 있습니다.
- Files Dashboard - 관리되는 디바이스에 의해 네트워크에서 탐지되는 파일(악성코드 파일 포함), 디바이스에 저장되고 동적 분석을 위해 제출되는 캡처된 파일, 서브스크립션 기반 FireAMP 전략을 사용하여 탐지되는 악성코드 등에 대한 자세한 정보를 제공합니다. 네트워크 기반 악성코드 데이터를 포함하려면 악성코드 라이센스가 있어야 하며 이 대시보드용 악성코드 탐지를 활성화해야 합니다. 또한 DC500과 Series 2 디바이스 또는 Cisco NGIPS for Blue Coat X-Series 모두 AMP를 지원하지 않으므로 DC500은 이 데이터를 표시할 수 없고 Series 2 디바이스와 Cisco NGIPS for Blue Coat X-Series는 이 데이터를 탐지하지 못합니다. 자세한 내용은 37-2페이지의 악성코드 차단 및 파일 제어 이해을/를 참조하십시오.
- URL Statistics Dashboard - 모니터링되는 네트워크에서 외부 URL로의 허용 및 거부되는 트래픽에 대한 자세한 정보를 URL 카테고리 및 평판으로 정렬하여 제공합니다. URL 카테고리 및 평판 데이터를 포함하려면 URL 필터링 라이센스가 있어야 하며 이 대시보드용 URL 필터링을 활성화해야 합니다. DC500과 Series 2 디바이스 모두 평판 및 카테고리 기준 URL 필터링을 지원하지 않으므로 DC500은 이 데이터를 표시할 수 없고 Series 2 디바이스는 이 데이터를 탐지하지 못합니다. 16-10페이지의 평판 기반 URL 차단 수행을/를 참조하십시오.
- Access Controlled User Statistics Dashboard - 모니터링된 네트워크의 사용자 활동과 침입 이벤트에 대한 자세한 정보를 제공합니다. 이 대시보드를 사용하면 네트워크의 사용자와 관련된 침입 이벤트, 허용 및 거부되는 연결, 트래픽은 물론 네트워크의 고유한 사용자 수도 추적할 수 있습니다. 이 대시보드는 사용자 인식 데이터에 따라 달라지기 때문에, 이 대시보드에 의미 있는 통계를 표시하려면 User Agent 및 방어 센터-Active Directory LDAP 서버 연결을 하나 이상 구성해야 합니다. 17-9페이지의 User Agents를 사용하여 Active Directory 로그인 보고을/를 참조하십시오.

각자의 요구에 맞게 사전 정의된 대시보드를 사용하거나, 사전 정의된 대시보드를 수정하거나, 사용자 지정 대시보드를 생성할 수 있습니다. 어플라이언스의 모든 사용자와 사용자 지정 대시보드를 공유할 수도 있고, 자신의 요구에 맞게 고유한 사용자 지정 대시보드를 생성할 수도 있습니다. 사용자 지정 대시보드를 기본 대시보드로 설정할 수도 있습니다.

일부 드릴다운 페이지 및 이벤트의 테이블 보기에는 사전 정의된 관련 대시보드를 보기 위해 클릭할 수 있는 **Dashboard** 툴바 링크가 포함되어 있습니다. 다음 테이블은 어떤 이벤트 보기가 어떤 사전 정의된 대시보드에 해당하는지를 보여줍니다. 사전 정의된 대시보드나 탭을 삭제하면 관련된 대시보드 링크가 작동하지 않습니다.

표 55-1 이벤트 테이블 대시보드 링크

표	대시보드 링크
연결 이벤트 (**Analysis > Connections > Events**)	Connection Summary
보안 인텔리전스 이벤트 (**Analysis > Connections > Security Intelligence**)	Connection Summary
침입 이벤트 (**Analysis > Intrusions > Events**)	Summary (Intrusion Events tab)
악성코드 이벤트 (**Analysis > Files > Malware Events**)	Files (Malware tab)
파일 이벤트 (**Analysis > Files > File Events**)	Files (Files tab)
캡처된 파일 (**Analysis > Files > Captured Files**)	Files (File Storage tab)
애플리케이션 (**Analysis > Hosts > Applications**)	Application Statistics
신청 세부사항 (**Analysis > Hosts > Application Details**)	Application Statistics
보안 침해 지표(IoC) (**Analysis > Hosts > Indications of Compromise**)	Summary (Threats tab)
사용자 (**Analysis > Users > Users**)	Access Controlled User Statistics
사용자 활동 (**Analysis > Users > User Activity**)	Access Controlled User Statistics
상관관계 이벤트 (**Analysis > Correlation > Correlation Events**)	Detailed (Correlation tab)
쓰기 목록 이벤트 (**Analysis > Correlation > White List Events**)	Detailed (Correlation tab)

대시보드 및 대시보드 내용에 대해 자세히 알아보려면 다음 절을 참조하십시오.

- 55-4페이지의 대시보드 위젯 이해
- 55-7페이지의 사전 정의된 위젯 이해
- 55-35페이지의 대시보드 작업

대시보드 위젯 이해

라이센스: 모두

대시보드에는 하나 이상의 탭이 있으며, 각 탭의 3단 레이아웃에 하나 이상의 위젯을 표시할 수 있습니다. FireSIGHT 시스템에서는 사전 정의된 많은 위젯을 제공하며, 각 위젯은 FireSIGHT 시스템의 여러 부분에 대한 통찰력을 제공합니다. 위젯은 세 카테고리로 그룹화됩니다.

- *분석 및 보고 위젯* - FireSIGHT 시스템에 의해 수집 및 생성된 이벤트에 대한 데이터를 표시합니다.
- *기타 위젯* - 이벤트 데이터나 운영 데이터 이외의 데이터를 표시합니다. 현재 이 카테고리의 유일한 위젯은 RSS 피드를 표시합니다.
- *운영 위젯* - FireSIGHT 시스템의 전체적인 상태에 대한 정보를 표시합니다.

볼 수 있는 대시보드 위젯은 사용 중인 어플라이언스의 유형 및 사용자 역할에 따라 다릅니다. 또한 각 대시보드에는 동작을 결정하는 환경 설정 집합이 있습니다. 위젯을 최소화 및 최대화하고, 탭에서 위젯을 제거하고, 탭에 있는 위젯을 재정돈할 수 있습니다.

참고 특정 시간 범위의 이벤트 수를 표시하는 위젯의 경우, 총 이벤트 수가 이벤트 뷰어에서 사용할 수 있는 세부사항 데이터가 있는 이벤트의 수를 반영하지 않을 수 있습니다. 이는 디스크 공간 사용량을 관리하기 위해 때때로 오래된 이벤트의 세부사항을 삭제하기 때문입니다. 이벤트 세부사항이 삭제되는 경우를 최소화하기 위해 이벤트 로깅을 정밀하게 튜닝하여 구축에 가장 중요한 이벤트만 로깅하게 할 수 있습니다. 자세한 내용은 38-1페이지의 네트워크 트래픽의 연결 로깅을/를 참조하십시오.

자세한 내용은 다음 링크를 참고하십시오.

- 55-4페이지의 위젯 가용성 이해
- 55-6페이지의 위젯 환경 설정 이해
- 55-7페이지의 사전 정의된 위젯 이해
- 55-35페이지의 대시보드 작업

위젯 가용성 이해

라이센스: 모두

FireSIGHT 시스템에서는 사전 정의된 대시보드 위젯을 여러 개 제공합니다. 볼 수 있는 대시보드 위젯은 사용 중인 어플라이언스의 유형 및 사용자 역할에 따라 다릅니다.

- *잘못된* 위젯이란 잘못된 어플라이언스 유형을 사용 중이기 때문에 볼 수 없는 위젯을 말합니다.
- *무단* 위젯이란 필요한 계정 권한이 없기 때문에 볼 수 없는 위젯을 말합니다.

예를 들어 Current Sessions 위젯은 모든 어플라이언스에서 이용할 수 있지만 Administrator 계정 권한이 있는 사용자만 이용 가능한 반면, Appliance Status 위젯은 Administrator, Maintenance User, Security Analyst 또는 Security Analyst(Read Only) 계정 권한이 있는 사용자가 방어 센터에서만 이용할 수 있습니다.

무단 위젯이나 잘못된 위젯은 대시보드에 추가할 수 없지만, 다른 종류의 어플라이언스에서 생성되거나 다른 액세스 권한이 있는 사용자에 의해 생성된 대시보드를 가져오는 경우 해당 대시보드에 무단 위젯이나 잘못된 위젯이 포함되어 있을 수 있습니다. 이러한 위젯은 표시할 수 없는 이유를 설명하는 오류 메시지와 함께 비활성화됩니다.

어플라이언스가 액세스할 수 없는 데이터는 위젯에 표시할 수 없습니다. 예를 들어, 관리되는 디바이스는 상관관계 이벤트, 침입 이벤트, 검색 이벤트 등에 액세스할 수 없습니다. 이러한 데이터 유형 중 하나를 표시하도록 구성된 Custom Analysis 위젯이 포함된 관리되는 디바이스로 대시보드를 가져오는 경우, 위젯에 오류 메시지가 표시됩니다. 위젯이 시간 초과되거나 다른 문제가 발생하는 경우에도 개별 위젯에 오류 메시지가 표시됩니다.

위젯의 내용은 사용 중인 어플라이언스의 유형에 따라 달라질 수 있습니다. 예를 들어 방어 센터의 Custom Analysis 위젯은 검색 정보를 표시할 수 있지만, 관리되는 디바이스에서 Custom Analysis 위젯을 구성할 경우에는 이 기능을 이용할 수 없습니다. 테이블 열 제목을 클릭하여 테이블 형식으로 생성된 내용을 정렬할 수 있습니다.

무단 위젯이나 잘못된 위젯 또는 데이터가 표시되지 않는 위젯은 삭제하거나 최소화할 수 있습니다. 공유 대시보드에서 위젯을 수정하면 어플라이언스의 모든 사용자에 대해 수정됩니다. 자세한 내용은 55-42페이지의 위젯 최소화 및 최대화 및 55-42페이지의 위젯 삭제을/를 참조하십시오.

다음 표에는 각 어플라이언스가 표시하는 잘못된 위젯이 나열되어 있습니다.

표 55-2 FirePOWER 어플라이언스 및 대시보드 위젯 가용성

위젯	방어 센터	모든 관리되는 디바이스
Appliance Information	예	예
Appliance Status	예	아니요
Correlation Events	예	아니요
Current Interface Status	예	예
Current Sessions	예	예
Custom Analysis	예	아니요
Disk Usage	예	예
Interface Traffic	예	예
Intrusion Events	예	아니요
Network Compliance	예	아니요
Product Licensing	예	아니요
Product Updates	예	예
RSS Feed	예	예
System Load	예	예
System Time	예	예
White List Events	예	아니요

다음 표에는 각 위젯을 보기 위해 필요한 사용자 계정 권한이 나열되어 있습니다. Administrator, Maintenance User, Security Analyst 또는 Security Analyst(Read Only) 액세스 권한이 있는 사용자 계정만 대시보드를 사용할 수 있습니다.

사용자 지정 역할이 있는 사용자는 역할 권한에 따라 위젯의 조합에 액세스할 수도 있고 위젯에 전혀 액세스하지 못할 수도 있습니다.

표 55-3 사용자 역할 및 대시보드 위젯 가용성

위젯	관리자	유지 보수 사용자	보안 분석가	보안 분석가(RO)
Appliance Information	예	예	예	예
Appliance Status	예	예	예	아니요
Correlation Events	예	아니요	예	예
Current Interface Status	예	예	예	예
Current Sessions	예	아니요	아니요	아니요
Custom Analysis	예	아니요	예	예
Disk Usage	예	예	예	예
Interface Traffic	예	예	예	예
Intrusion Events	예	아니요	예	예
Network Compliance	예	아니요	예	예
Product Licensing	예	예	아니요	아니요
Product Updates	예	예	아니요	아니요
RSS Feed	예	예	예	예
System Load	예	예	예	예
System Time	예	예	예	예
White List Events	예	아니요	예	예

위젯 환경 설정 이해

라이센스: 모두

각 위젯에는 동작을 결정하는 환경 설정 집합이 있습니다.

위젯 환경 설정은 간단할 수 있습니다. 예를 들어 다음 그림에서는 내부 네트워크에서 활성화된 모든 인터페이스의 현재 상태를 표시하는 Current Interface Status 위젯의 환경 설정을 보여줍니다. 이 위젯에 대해서는 업데이트 빈도만 구성할 수 있습니다.

위젯 환경 설정은 좀 더 복잡할 수도 있습니다. 예를 들어 다음 그림에서는 FireSIGHT 시스템에 의해 수집 및 생성된 이벤트에 대한 자세한 정보를 표시할 수 있는, 사용자 지정 기능이 뛰어난 위젯인 Custom Analysis 위젯의 환경 설정을 보여줍니다.

위젯의 환경 설정을 수정하려면

액세스: Admin/Any Security Analyst/Maint

1단계 환경 설정을 변경하고자 하는 위젯의 제목 표시줄에서 환경 설정 표시 아이콘( )을 클릭합니다.

위젯의 환경 설정 섹션이 나타납니다.

2단계 필요에 따라 변경합니다.

변경 사항은 즉시 적용됩니다. 개별 위젯에 대해 지정할 수 있는 환경 설정에 대한 자세한 내용은 55-7페이지의 사전 정의된 위젯 이해을/를 참조하십시오.

3단계 환경 설정 섹션을 숨기려면 위젯의 제목 표시줄에서 환경 설정 숨기기 아이콘( )을 클릭합니다.

사전 정의된 위젯 이해

라이센스: 모두

FireSIGHT 시스템에서는 대시보드에서 사용 시 시스템에 의해 수집 및 생성된 이벤트에 대한 데이터, 구축에서 어플라이언스의 전체적인 상태에 대한 정보를 비롯하여 현재 시스템 상태를 한눈에 볼 수 있는 보기가 포함된 사전 정의된 위젯을 여러 개 제공합니다.

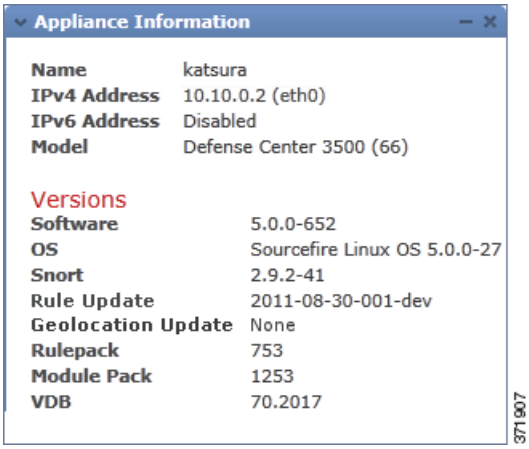
FireSIGHT 시스템과 함께 제공되는 위젯에 대한 자세한 내용은 다음 절을 참조하십시오.

참고 볼 수 있는 대시보드 위젯은 사용 중인 어플라이언스의 유형 및 사용자 역할에 따라 다릅니다. 자세한 내용은 55-4페이지의 위젯 가용성 이해을/를 참조하십시오.

Appliance Information 위젯 이해

라이센스: 모두

Appliance Information 위젯은 어플라이언스의 스냅샷을 제공하며 Detailed Dashboard 및 Summary Dashboard의 Status 탭에 기본적으로 나타납니다.



위젯에서는 다음을 제공합니다.

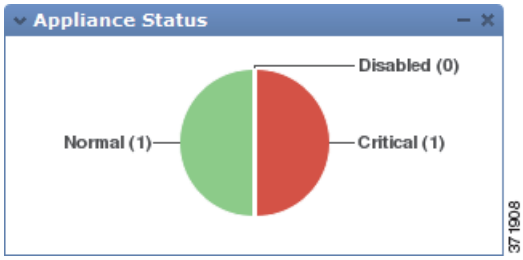
- 어플라이언스의 이름, IPv4 주소, IPv6 주소 및 모델
- 대시보드와 함께 어플라이언스에 설치된 FireSIGHT 시스템 소프트웨어의 버전, 운영 체제, Snort, 규칙 업데이트, 규칙 팩, 모듈 팩, VDB(취약성 데이터베이스) 및 지오로케이션 업데이트(가상 방어 센터 제외)
- 관리되는 어플라이언스의 경우, 관리되는 어플라이언스와의 통신 링크 상태 및 이름
- 고가용성 쌍의 방어 센터의 경우 피어 방어 센터의 FireSIGHT 시스템 소프트웨어 및 운영 체제 버전, 이름, 모델, 방어 센터에서 최근에 접속한 방법

단순한 보기 또는 고급 보기를 표시하도록 위젯 환경 설정을 수정하여 더 많은 정보 또는 더 적은 정보를 표시하도록 위젯을 구성할 수 있습니다. 환경 설정은 위젯 업데이트 빈도도 제어합니다. 자세한 내용은 55-6페이지의 위젯 환경 설정 이해을/를 참조하십시오.

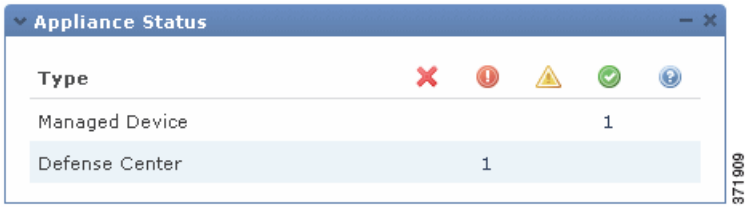
Appliance Status 위젯 이해

라이센스: 모두

Appliance Status 위젯은 어플라이언스 및 관리 중인 어플라이언스의 상태를 나타냅니다. 방어 센터는 관리되는 디바이스에 상태 정책을 자동으로 적용하지 않으므로 상태 정책을 디바이스에 수동으로 적용해야 합니다. 그렇지 않으면 상태가 `Disabled`로 표시됩니다. 이 위젯은 Detailed Dashboard 및 Summary Dashboard의 Status 탭에 기본적으로 나타납니다.



위젯 환경 설정을 수정하여 어플라이언스 상태를 원그래프 또는 테이블로 표시하도록 위젯을 구성할 수 있습니다.



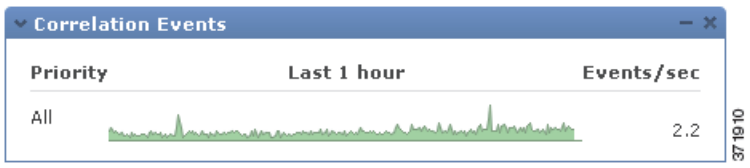
환경 설정은 또한 위젯 업데이트 빈도를 제어합니다. 자세한 내용은 55-6페이지의 위젯 환경 설정 이해을/를 참조하십시오.

원 그래프의 섹션을 클릭하거나 어플라이언스 상태 테이블의 숫자 중 하나를 클릭하여 Health Monitor 페이지로 이동한 다음 어플라이언스 및 관리 중인 어플라이언스의 컴파일된 상태를 볼 수 있습니다. 자세한 내용은 68-41페이지의 상태 모니터 사용을/를 참조하십시오.

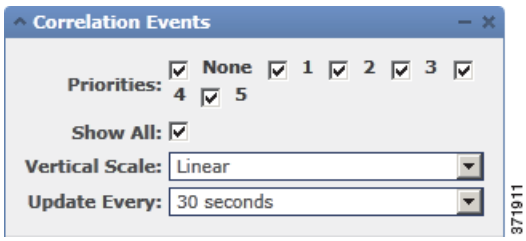
Correlation Events 위젯 이해

라이센스: FireSIGHT

Correlation Events 위젯은 대시보드 시간 범위 중 초당 상관관계 이벤트의 평균 개수를 우선순위 기준으로 보여줍니다. 이 위젯은 Detailed Dashboard의 Correlation 탭에 기본적으로 나타납니다.



위젯 환경 설정을 수정하여 서로 다른 우선순위의 상관관계 이벤트를 표시하고, linear(incremental) 또는 logarithmic(factor of ten) 비율을 선택하도록 위젯을 구성할 수 있습니다.



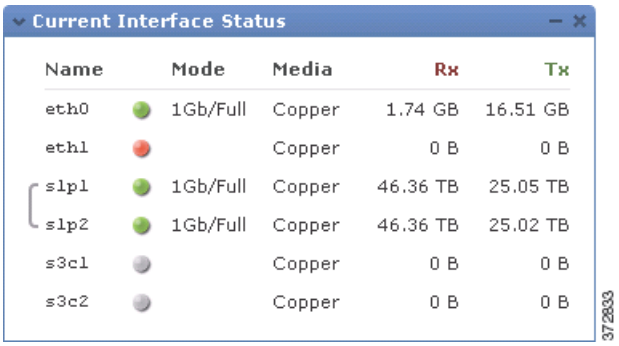
특정 우선순위의 이벤트(우선순위가 없는 이벤트 포함)에 대해 별도의 그래프를 표시하려면 하나 이상의 **Priorities** 확인란을 선택합니다. 우선순위와 상관없이 모든 상관관계 이벤트에 대해 추가 그래프를 표시하려면 **Show All**을 선택합니다. 환경 설정은 또한 위젯 업데이트 빈도를 제어합니다. 자세한 내용은 55-6페이지의 위젯 환경 설정 이해을/를 참조하십시오.

특정 우선순위의 상관관계 이벤트를 보려면 그래프 하나를 클릭하고, 모든 상관관계 이벤트를 보려면 **모든** 그래프를 클릭합니다. 어떤 경우든 이벤트는 대시보드 시간 범위에 의해 제한됩니다. 대시보드를 통해 상관관계 이벤트에 액세스하면 어플라이언스에 대한 이벤트(또는 전역) 시간 창이 변경됩니다. 상관관계 이벤트에 대한 자세한 내용은 51-52페이지의 상관관계 이벤트 보기을/를 참조하십시오.

Current Interface Status 위젯 이해

라이센스: 모두

Current Interface Status 위젯은 활성화되었든 사용되고 있지 않든, 어플라이언스에 있는 모든 인터페이스의 상태를 표시합니다. 방어 센터에서 관리(`eth0`, `eth1` 등) 인터페이스를 표시할 수 있습니다. 관리되는 디바이스에서 센싱(`s1p1` 등) 인터페이스만 표시하거나 관리 및 센싱 인터페이스를 모두 표시하도록 선택할 수 있습니다. 인터페이스는 관리, 인라인, 수동, 스위치드, 라우티드, 스태킹됨, 사용되지 않음 등의 유형별로 그룹화됩니다.



각 인터페이스에 대해 위젯은 다음을 제공합니다.

- 인터페이스의 이름
- 인터페이스의 연결 상태
- 인터페이스의 링크 모드(예: 100Mb 전이중 또는 10Mb 반이중)
- 인터페이스 유형(구리 또는 파이버)
- 인터페이스의 수신(Rx) 및 송신(Tx) 데이터 양

링크 상태를 보여주는 공의 색은 현재 상태를 다음과 같이 나타납니다.

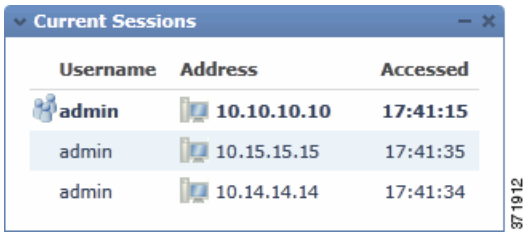
- 녹색: 링크가 전체 속도로 가동 중
- 노란색: 링크가 가동 중이지만 전체 속도가 아님
- 빨간색: 링크가 가동되지 않음
- 회색: 관리를 위해 링크가 비활성화됨
- 파란색: 링크 상태 정보를 이용할 수 없음(예: ASA)

위젯 환경 설정은 위젯 업데이트 빈도를 제어합니다. 자세한 내용은 55-6페이지의 위젯 환경 설정 이해을/를 참조하십시오.

Current Sessions 위젯 이해

라이센스: 모두

Current Sessions 위젯은 어플라이언스에 현재 로그인한 사용자, 세션이 시작된 시스템과 관련된 IP 주소, 각 사용자가 어플라이언스에서 페이지에 액세스한 마지막 시간(어플라이언스의 현지 시간 기준)을 보여줍니다. 자신을 나타내는 사용자, 즉 현재 위젯을 보고 있는 사용자는 사용자 아이콘( )과 함께 굵은 글꼴로 표시됩니다. 로그오프 또는 비활성 상태 1시간 내에 이 위젯의 데이터에서 세션이 삭제됩니다. 이 위젯은 Detailed Dashboard 및 Summary Dashboard의 Status 탭에 기본적으로 나타납니다.



Current Sessions 위젯에서 다음을 수행할 수 있습니다.

- 사용자 이름을 클릭하여 User Management 페이지에서 사용자 계정을 관리할 수 있습니다. 61-43페이지의 사용자 계정 관리을/를 참조하십시오.
- IP 주소 옆에 있는 호스트 아이콘( ) 또는 감염된 호스트 아이콘( )을 클릭하여 관련 시스템의 호스트 프로필을 볼 수 있습니다. 49-1페이지의 호스트 프로필 사용(방어 센터 및 네트워크 검색 전용)을/를 참조하십시오.
- IP 주소나 액세스 시간을 클릭하여 해당 IP 주소에 의해, 그리고 웹 IP 주소와 연결된 사용자가 웹 인터페이스에 로그온한 시간에 의해 제한되는 감사 로그를 볼 수 있습니다. 69-2페이지의 감사 레코드 보기을/를 참조하십시오.

위젯 환경 설정은 위젯 업데이트 빈도를 제어합니다. 자세한 내용은 55-6페이지의 위젯 환경 설정 이해을/를 참조하십시오.

Custom Analysis 위젯 이해

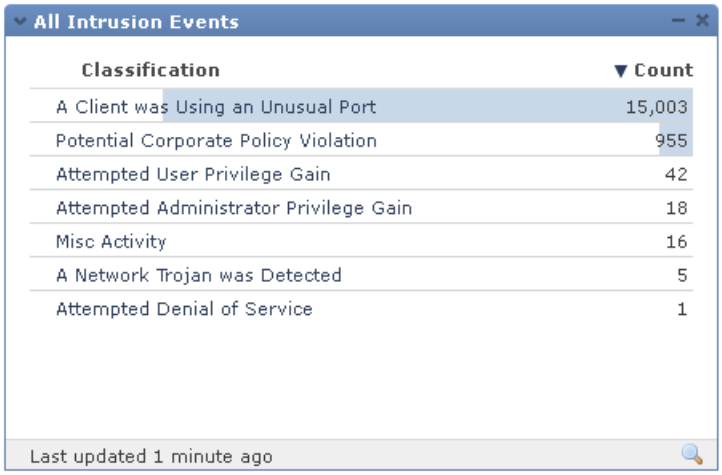
라이센스: 모두

사용자 지정 기능이 뛰어난 위젯인 Custom Analysis 위젯을 사용하면 FireSIGHT 시스템에 의해 수집 및 생성된 이벤트에 대한 자세한 정보를 표시할 수 있습니다.

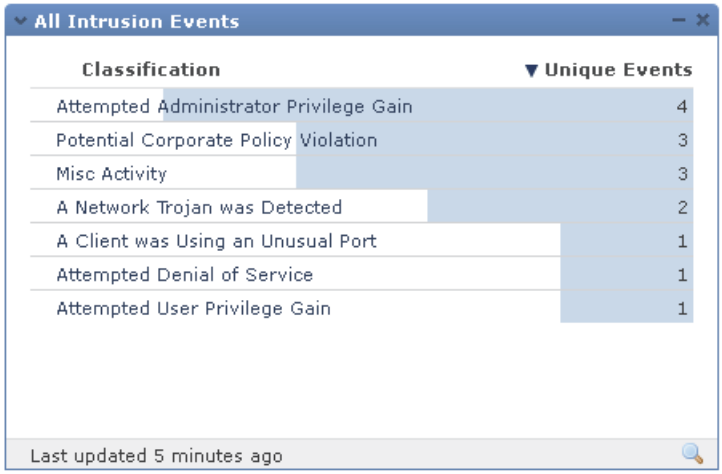
Custom Analysis 위젯은 Cisco에서 사전 정의한 컨피그레이션 그룹인 다양한 위젯 프리셋과 함께 제공됩니다. 프리셋은 예제 역할을 하며, 이를 통해 구축에 대한 정보에 빠르게 액세스할 수 있습니다. 이러한 프리셋을 사용할 수도 있고 사용자 지정 컨피그레이션을 생성할 수도 있습니다.

위젯 환경 설정을 구성할 때, 표시하고자 하는 테이블 및 개별 필드를 선택해야 하며 표시할 데이터를 위젯에서 어떻게 그룹화할지를 구성하는 어그리게이션 방법도 선택해야 합니다.

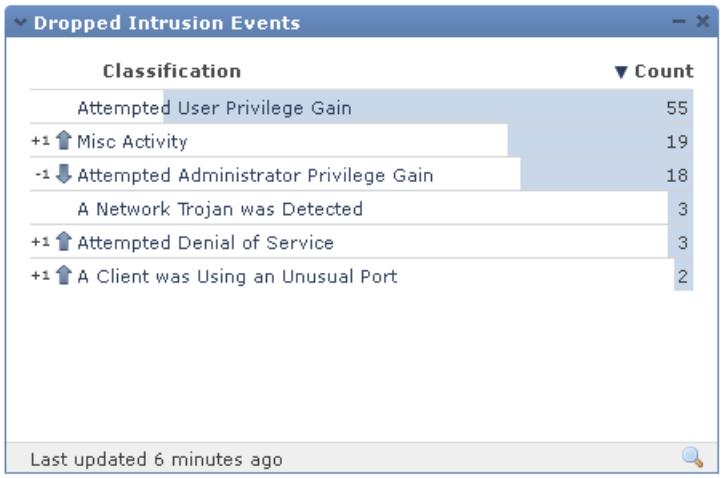
예를 들면 **Intrusion Events** 테이블의 데이터를 표시하도록 위젯을 구성하여, 최신 침입 이벤트 목록을 표시하도록 Custom Analysis 위젯을 구성할 수 있습니다. **Classification** 필드를 선택하고 **Count** 단위로 이 데이터를 결합하면 각 이벤트 유형이 생성된 방법을 파악할 수 있습니다. 카운트에는 침입 이벤트에 대한 검토된 이벤트가 포함됩니다. 이벤트 뷰어에서 카운트를 보면 검토된 이벤트가 포함되지 않습니다.



반면, **Unique Events** 단위로 결합하면 각 유형의 고유한 침입 이벤트가 발생한 횟수(예: 네트워크 트로이 목마, 회사 정책의 잠재적 위반, 서비스 거부 공격 시도 등의 탐지 횟수)를 파악할 수 있습니다.



선택적으로, 저장된 검색(어플라이언스와 함께 제공된 사전 정의된 검색 중 하나 또는 자신이 생성한 사용자 지정 검색)을 사용하여 위젯을 더 제한할 수 있습니다. 예를 들어 **Dropped Events** 검색으로 첫 번째 예제(**Classification** 필드를 사용하고 **Count**로 결합한 침입 이벤트)를 제한하면 각 유형의 침입 이벤트가 얼마나 삭제되었는지를 알 수 있습니다.



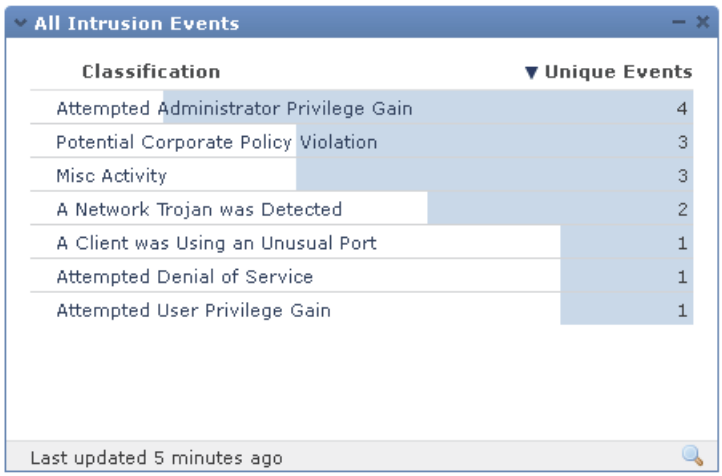
위젯 배경의 색상 막대는 각 이벤트 발생의 상대 횟수를 보여줍니다. 오른쪽에서 왼쪽으로 막대를 읽어야 합니다. 막대의 색은 물론 위젯이 표시하는 행 수도 변경할 수 있습니다. 가장 자주 발생하는 이벤트 또는 가장 적게 발생하는 이벤트를 표시하도록 위젯을 구성할 수도 있습니다.

방향 아이콘(▼)은 표시의 정렬 순서를 나타내고 제어합니다. 아래로 향하는 아이콘은 내림차순, 위로 향하는 아이콘은 오름차순을 나타냅니다. 정렬 순서를 바꾸려면 아이콘을 클릭합니다.

각 이벤트 옆에는 최신 결과에서 변경된 내용을 나타내는 세 가지 아이콘 중 하나가 표시됩니다.

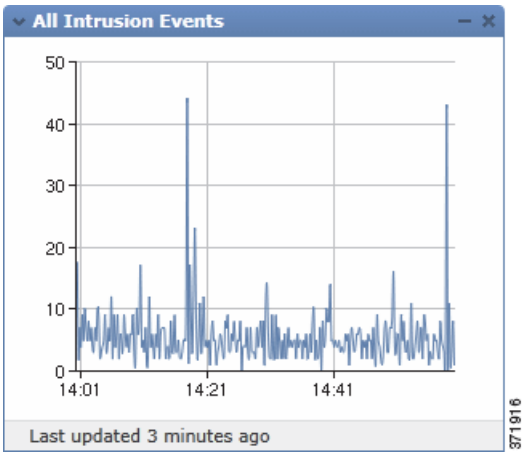
- 새 이벤트 아이콘( ) - 이벤트가 결과에 새로 추가되었음을 나타냅니다.
- 위쪽 화살표 아이콘( ) - 위젯이 마지막으로 업데이트된 이후 이벤트 순위가 위로 이동했음을 나타냅니다. 이벤트가 몇 단계 올라갔는지 알려주는 숫자가 아이콘 옆에 나타납니다.
- 아래쪽 화살표 아이콘( ) - 위젯이 마지막으로 업데이트된 이후 이벤트 순위가 아래로 이동했음을 나타냅니다. 이벤트가 몇 단계 내려갔는지 알려주는 숫자가 아이콘 옆에 나타납니다.

위젯은 어플라이언스의 현지 시간을 기준으로 마지막 업데이트 시간을 표시합니다. 위젯은 대시보드 시간 범위에 따른 빈도로 업데이트됩니다. 예를 들어 대시보드 시간 범위를 시로 설정하면 위젯은 5분마다 업데이트됩니다. 반면, 대시보드 시간 범위를 연도로 설정하면 위젯은 일주일에 한 번 업데이트됩니다. 대시보드의 다음번 업데이트 시기를 확인하려면 위젯의 왼쪽 아래에 있는 **Last updated** 알림으로 포인터를 이동합니다.



참고 저장된 검색을 사용하여 Custom Analysis 위젯을 제한한 다음 검색을 수정하면, 다음 업데이트 시간까지 위젯에 변경 사항이 반영되지 않습니다.

시간에 따라 발생한 이벤트 또는 기타 수집된 데이터에 대한 정보(예: 구축에서 시간에 따라 생성된 침입 이벤트의 총수)를 보려면 선 그래프를 표시하도록 Custom Analysis 위젯을 구성할 수 있습니다. 시간 추이 그래프의 경우 선의 색은 물론 위젯에서 사용하는 표준 시간대도 선택할 수 있습니다.



마지막으로, 위젯의 사용자 지정 제목을 선택할 수 있습니다.

Custom Analysis 위젯에서, 위젯에 표시되는 이벤트에 대한 자세한 정보를 제공하는 이벤트 보기(즉, 워크플로)를 호출할 수 있습니다. 그렇게 하려면 추가 정보를 원하는 이벤트를 클릭합니다.

또한 사용자 지정 분석 위젯에서 IP 주소를 마우스 오른쪽 버튼으로 클릭하면 나타나는 컨텍스트 메뉴에서 관련 호스트에 대한 자세한 정보를 얻을 수 있으며, 보안 인텔리전스 필터링을 위해 해당 호스트를 전역 블랙리스트 또는 화이트리스트에 추가할 수도 있습니다.

참고 구성 방법에 따라 Custom Analysis 위젯에 어플라이언스 리소스의 유출 상태를 표시할 수 있습니다. 빨간색 음영의 Custom Analysis 위젯은 해당 사용으로 인해 시스템 성능이 저하됨을 나타냅니다. 위젯이 계속해서 빨간색으로 표시되면 해당 위젯을 제거해야 합니다.

자세한 내용은 다음 절을 참조하십시오.

- 55-15페이지의 Custom Analysis 위젯 구성
- 55-24페이지의 Custom Analysis 위젯에서 관련 이벤트 보기
- 55-25페이지의 사용자 지정 Analysis Widget 제한 사항
- 2-5페이지의 컨텍스트 메뉴 사용

Custom Analysis 위젯 구성

라이센스: 모두

모든 위젯이 그렇듯이 Custom Analysis 위젯에는 동작을 결정하는 환경 설정이 있습니다. Custom Analysis 위젯을 구성하려면 55-6페이지의 위젯 환경 설정 이해에서 설명한 대로 환경 설정을 표시하십시오.

이벤트의 상대적인 발생을 표시하도록 위젯을 구성하는지(즉, 막대 그래프), 시간 추이 그래프를 표시하도록 위젯을 구성하는지(즉, 선 그래프)에 따라 다른 환경 설정 집합이 나타납니다.

막대 그래프를 표시하도록 위젯을 구성하려면 **Field** 드롭다운 필드에서 **Time** 이외의 값을 선택합니다.

선 그래프를 표시하도록 위젯을 구성하려면 **Field** 드롭다운 필드에서 **Time**을 선택합니다.

다음 표는 Custom Analysis 위젯에서 설정할 수 있는 다양한 환경 설정에 대해 설명합니다.

표 55-4 사용자 지정 Analysis Widget 환경 설정

사용할 환경 설정	제어할 내용
제목	위젯의 제목. 제목을 지정하지 않으면 어플라이언스는 구성된 이벤트 유형을 위젯 제목으로 사용합니다.
프리셋	위젯의 프리셋. Custom Analysis 위젯은 Cisco에서 사전 정의한 위젯 컨피그레이션인 다양한 프리셋과 함께 제공됩니다. 프리셋은 예제 역할을 하며, 이를 통해 구축에 대한 정보에 빠르게 액세스할 수 있습니다. 이러한 프리셋을 사용할 수도 있고 사용자 지정 컨피그레이션을 생성할 수도 있습니다. 프리셋에 대한 자세한 내용은 사용자 지정 Analysis Widget 프리셋 표를 참조하십시오.
표	위젯에 표시할 이벤트 데이터를 포함하는 이벤트의 테이블.
필드	표시할 이벤트 유형의 특정 필드. **팁** 시간 추이 그래프를 표시하려면 **Time**을 선택합니다.
집계	위젯의 어그리게이션 방법. 어그리게이션 방법은 위젯이 표시하는 데이터를 그룹화하는 방법을 구성합니다. 대부분의 이벤트 유형에서 기본 어그리게이션 기준은 **Count**입니다.
필터	위젯이 표시하는 데이터를 추가로 제한하기 위해 사용할 사용자 정의 애플리케이션 필터. Application Statistics 또는 Intrusion Event Statistics by Application 테이블에서 데이터를 표시하는 경우 애플리케이션 필터만 사용할 수 있습니다. 애플리케이션 필터에 대한 자세한 내용은 3-15페이지의 애플리케이션 필터 작업을/를 참조하십시오.
검색	위젯이 표시하는 데이터를 추가로 제한하기 위해 사용할 저장된 검색. 일부 프리셋에서는 사전 정의된 검색을 사용하지만, 검색을 지정해야 할 필요는 없습니다. 별표(*) 없이 필드의 데이터를 사용하는 저장된 연결 이벤트 검색을 생성하면 위젯에 잘못된 데이터가 표시됩니다. 연결 요약을 표시하는 필드만이 연결 이벤트를 기반으로 사용자 정의 분석 대시보드 위젯을 제한할 수 있습니다. 잘못된 검색은 회색으로 표시되며 선택할 수 없습니다.

표 55-4 사용자 지정 Analysis Widget 환경 설정 (계속)

사용할 환경 설정	제어할 내용
표시	가장 자주 발생하는 이벤트(**Top**)를 표시할지, 가장 적게 발생하는 이벤트(**Bottom**)를 표시할지 여부.
결과	표시할 결과 행의 수. 10~25의 결과 행을 5의 증분으로 표시할 수 있습니다.
Show Movers	최신 결과에서 변경된 내용을 나타내는 아이콘을 표시할지 여부.
표준 시간대	결과를 표시하기 위해 사용할 표준 시간대. 시간 기반 필드를 선택할 때마다 표준 시간대가 나타납니다.
색상	각 결과의 상대적 발생 수를 나타내는 위젯 배경의 막대 색상.

다음 표에서는 Custom Analysis 위젯에서 사용할 수 있는 프리셋에 대해 설명합니다. 또한 방어 센터 사전 정의된 대시보드(있는 경우)에서 각 프리셋을 사용할지 여부도 나타냅니다. 다음에 유의하십시오.

- NO MDC THIS TIME 관리되는 디바이스의 사전 정의된 대시보드에는 Custom Analysis 위젯이 포함되지 않습니다.
- 지원되지 않는 기능에 대한 데이터가 DC500 방어 센터에는 표시되지 않으며 Series 2 디바이스 및 Cisco NGIPS for Blue Coat X-Series에서는 탐지되지 않습니다.

특정 라이센스 유형에 대한 자세한 내용은 65-2페이지의 라이센스 유형 및 제한 사항을/를 참조하십시오.

표 55-5 사용자 지정 Analysis Widget 프리셋

프리셋	설명	사전 정의된 대시보드	라이센스
All Intrusion Events	대시보드 시간 범위 중에 모니터링되는 네트워크에서 발생한 총 침입 이벤트 수의 그래프를 표시합니다.	Detailed Dashboard Summary Dashboard	보호
All Intrusion Events (Not Dropped)	이벤트의 일부로서 패킷이 삭제되지 않은, 가장 자주 발생하는 침입 이벤트 유형을 분류별로 표시합니다.	Detailed Dashboard	보호
Allowed Connections by Application	모니터링되는 네트워크에서 허용된 애플리케이션 연결을 애플리케이션별로 그룹화하여 표시합니다.	Application Statistics	FireSIGHT
Allowed Connections by Application Risk	모니터링되는 네트워크에서 허용된 애플리케이션 연결을 애플리케이션 위험 수준별로 그룹화하여 표시합니다.	Application Statistics	FireSIGHT
Allowed Connections by Business Relevance	모니터링되는 네트워크에서 허용된 애플리케이션 연결을 비즈니스 활동에 대한 예측 연관성별로 그룹화하여 표시합니다.	Application Statistics	FireSIGHT
Allowed Connections by URL Category	모니터링되는 네트워크에서 허용된 애플리케이션 연결을 URL 카테고리별로 그룹화하여 표시합니다.	URL 통계	URL 필터링
Allowed Connections by URL Reputation	모니터링되는 네트워크에서 허용된 애플리케이션 연결을 URL 평판별로 그룹화하여 표시합니다.	URL 통계	URL 필터링

표 55-5 사용자 지정 Analysis Widget 프리셋 (계속)

프리셋	설명	사전 정의된 대시보드	라이센스
Allowed Connections by User	모니터링되는 네트워크에서 허용된 애플리케이션 연결을 연결 사용자별로 그룹화하여 표시합니다.	Access Controlled User Statistics	FireSIGHT
Application Protocols Introducing Malware	네트워크를 통해 전송된 악성코드 파일 수를 파일 전송에 사용된 애플리케이션 프로토콜별로 그룹화하여 표시합니다.	Files Dashboard	악성코드
Application Protocols Transferring Files	네트워크를 통해 전송된 파일 수를 파일 전송에 사용된 애플리케이션 프로토콜별로 그룹화하여 표시합니다.	Files Dashboard	보호
Client Applications Introducing Malware	FireAMP Connector에서 탐지된 악성코드에 액세스했거나 이를 생성한 애플리케이션 또는 상위 파일을 표시합니다.	Files Dashboard	FireAMP 구독
Client Applications Transferring Files	네트워크를 통해 파일을 전송한 애플리케이션 또는 상위 파일을 표시합니다.	Files Dashboard	보호
Clients	모니터링되는 네트워크의 클라이언트를 유형별로 표시합니다.	Detailed Dashboard	FireSIGHT
Connections by Application	탐지된 연결 수를 기반으로, 모니터링되는 네트워크의 애플리케이션을 표시합니다.	Connection Summary	FireSIGHT
Connections by Destination Continent	연결 수를 기반으로, 모니터링되는 네트워크에서 연결이 전송된 대륙을 표시합니다.	Connection Summary	FireSIGHT
Connections by Destination Country	연결 수를 기반으로, 모니터링되는 네트워크에서 연결이 전송된 국가를 표시합니다.	Connection Summary	FireSIGHT
Connections by Initiator IP	호스트의 IP 주소가 세션을 시작한 연결의 수를 기반으로, 모니터링되는 네트워크의 해당 호스트 IP 주소를 표시합니다.	Connection Summary	FireSIGHT
Connections by Port	탐지된 연결 수를 기반으로, 모니터링되는 네트워크의 포트를 표시합니다.	Connection Summary	FireSIGHT
Connections by Responder IP	세션의 responder가 호스트의 IP 주소인 연결의 수를 기반으로, 모니터링되는 네트워크의 해당 호스트 IP 주소를 표시합니다. 이 위젯의 출력은 연결 로깅 컨피그레이션에 따라 달라집니다.	Connection Summary	FireSIGHT
Connections by Security Intelligence Category	보안 인텔리전스 카테고리에 의해 그룹화되고, 모니터링되는 네트워크의 보안 인텔리전스에 의해 모니터링 및 차단된 모든 연결을 표시합니다.	Summary Dashboard	보호
Connections by Source Continent	각 대륙에서 시작된 연결 수를 기반으로, 모니터링되는 네트워크와 통신하는 대륙을 표시합니다.	Connection Summary	FireSIGHT
Connections by Source Country	각 국가에서 시작된 연결 수를 기반으로, 모니터링되는 네트워크와 통신하는 국가를 표시합니다.	Connection Summary	FireSIGHT

표 55-5 사용자 지정 Analysis Widget 프리셋 (계속)

프리셋	설명	사전 정의된 대시보드	라이센스
Connections by URL Category	모니터링되는 네트워크의 모든 애플리케이션 연결을 URL 카테고리별로 그룹화하여 표시합니다.	Summary Dashboard	URL 필터링
Connections by URL Reputation	모니터링되는 네트워크의 모든 애플리케이션 연결을 URL 평판별로 그룹화하여 표시합니다.	Summary Dashboard	URL 필터링
Connections over Time	대시보드 시간 범위 중에 모니터링되는 네트워크에서 발생한 총 연결 수의 그래프를 표시합니다.	Connection Summary	FireSIGHT
Denied Connections by Application	모니터링되는 네트워크에서 거부된 연결을 애플리케이션별로 그룹화하여 표시합니다.	Application Statistics	FireSIGHT
Denied Connections by URL Category	모니터링되는 네트워크에서 거부된 연결을 URL 카테고리별로 그룹화하여 표시합니다.	URL Statistics	URL 필터링
Denied Connections by URL Reputation	모니터링되는 네트워크에서 거부된 연결을 URL 평판별로 그룹화하여 표시합니다.	URL Statistics	URL 필터링
Denied Connections by User	모니터링되는 네트워크에서 거부된 연결을 연결 사용자별로 그룹화하여 표시합니다.	Access Controlled User Statistics	FireSIGHT
Dropped Events by Application	삭제된 침입 이벤트를 애플리케이션별로 그룹화하여 표시합니다.	Application Statistics	보호 + FireSIGHT
Dropped Events by User	삭제된 침입 이벤트를 사용자별로 그룹화하여 표시합니다.	Access Controlled User Statistics	보호 + FireSIGHT
Dropped Intrusion Events	패킷이 삭제된 침입 이벤트의 카운트를 분류별로 그룹화하여 표시합니다.	Detailed Dashboard Summary Dashboard	보호
Dynamic Analysis Traffic by Device	분석을 위해 종합 보안 인텔리전스 클라우드로 제출된 파일 데이터의 크기를 기반으로 가장 활동적인 디바이스를 표시합니다.	Files Dashboard	악성코드
Dynamic Analysis Traffic over Time	대시보드 시간 범위 중에 분석을 위해 클라우드로 제출된 캡처된 파일 데이터 크기를 표시합니다.	Files Dashboard	악성코드
File Actions	네트워크를 통해 전송된 파일 수를 파일 처리에 사용된 파일 규칙 작업별로 그룹화하여 표시합니다.	Files Dashboard	보호 또는 악성코드
File Categories	네트워크를 통해 전송된 파일 수를 파일 카테고리별로 그룹화하여 표시합니다.	Files Dashboard	보호
File Dispositions	Malware Cloud Lookup 파일 규칙 결과 네트워크 트래픽에서 탐지된 파일 수를 악성코드 성향별로 그룹화하여 표시합니다.	Files Dashboard	악성코드
File Names	네트워크를 통해 전송된 파일 수를 파일 이름별로 그룹화하여 표시합니다.	Files Dashboard	보호
File Storage by Device	대부분의 파일 데이터를 저장한 디바이스를 표시합니다.	Files Dashboard	악성코드

표 55-5 사용자 지정 Analysis Widget 프리셋 (계속)

프리셋	설명	사전 정의된 대시보드	라이센스
File Storage by Disposition	디바이스에 저장된 파일 데이터의 크기를 파일 성향을 기반으로 표시합니다(킬로바이트 단위).	Files Dashboard	악성코드
File Storage by Type	디바이스에 저장된 파일 데이터의 크기를 파일 형식을 기반으로 표시합니다(킬로바이트 단위).	Files Dashboard	악성코드
File Storage over Time	대시보드 시간 범위 중에 관리되는 디바이스에 저장된 파일 데이터의 킬로바이트 단위 그래프를 표시합니다.	Files Dashboard	악성코드
File Transfers over Time	대시보드 시간 범위 중에 네트워크 트래픽에서 시스템이 탐지한 총 파일 전송 수의 그래프를 표시합니다.	Files Dashboard	보호
File Types	네트워크를 통해 전송된 파일 수를 파일 형식별로 그룹화하여 표시합니다.	Files Dashboard	보호
File Types Infected with Malware	네트워크 트래픽에서 시스템 또는 FireAMP Connector가 탐지한 악성코드의 수를 파일 형식별로 그룹화하여 표시합니다.	Files Dashboard	악성코드
Files Sent for Dynamic Analysis over Time	대시보드 시간 범위 중에 동적 분석을 위해 제출된 총 파일 수의 그래프를 표시합니다.	Files Dashboard	악성코드
Files Stored over Time	대시보드 시간 범위 중에 관리되는 디바이스에 저장된 총 파일 수의 그래프를 표시합니다.	Files Dashboard	악성코드
Hosts Receiving Files	네트워크의 호스트 IP 주소에서 수신한(다운로드한) 파일 수를 IP 주소별로 그룹화하여 표시합니다.	Files Dashboard	보호
Hosts Receiving Malware	네트워크의 호스트 IP 주소에서 수신한 악성코드 파일 수를 IP 주소별로 그룹화하여 표시합니다.	Files Dashboard	악성코드 라이센스 또는 FireAMP 서브스크립션
Hosts Sending Files	네트워크의 호스트 IP 주소에서 전송한(업로드한) 파일 수를 IP 주소별로 그룹화하여 표시합니다.	Files Dashboard	보호
Hosts Sending Malware	네트워크의 호스트 IP 주소에서 전송한 악성코드 파일 수를 IP 주소별로 그룹화하여 표시합니다.	Files Dashboard	악성코드
Impact x Events by Application	예상 영향 수준 x(x는 0~4의 숫자)의 이벤트 수를 애플리케이션별로 그룹화하여 표시합니다.	Application Statistics	보호 + FireSIGHT
Impact Level x Events by Application Protocol	예상 영향 수준 x(x는 0~4의 숫자)의 이벤트 수를 애플리케이션 프로토콜별로 그룹화하여 표시합니다.	Summary Dashboard	보호 + FireSIGHT
Impact Level x Events by User	예상 영향 수준 x(x는 0~4의 숫자)의 이벤트 수를 사용자별로 그룹화하여 표시합니다.	Access Controlled User Statistics	보호 + FireSIGHT
Indications of Compromise by Host	트리거된 IOC의 수를 연결된 호스트 IP 주소별로 그룹화하여 표시합니다.	Summary Dashboard	FireSIGHT

표 55-5 사용자 지정 Analysis Widget 프리셋 (계속)

프리셋	설명	사전 정의된 대시보드	라이센스
Intrusion Events Requiring Analysis	이벤트 분류를 기반으로, 분석이 필요한 침입 이벤트의 수를 표시합니다.	Detailed Dashboard	보호 + FireSIGHT
Intrusion Events by Destination Continent	각 대륙과 연결된 이벤트 수를 기반으로, 침입 이벤트의 대상 대륙을 표시합니다.	Summary Dashboard	FireSIGHT
Intrusion Events by Destination Country	각 국가와 연결된 이벤트 수를 기반으로, 침입 이벤트의 대상 국가를 표시합니다.	Summary Dashboard	FireSIGHT
Intrusion Events by Source Continent	각 대륙에서 시작된 이벤트 수를 기반으로, 침입 이벤트가 시작된 대륙을 표시합니다.	Summary Dashboard	FireSIGHT
Intrusion Events by Source Country	각 국가에서 시작된 이벤트 수를 기반으로, 침입 이벤트가 시작된 국가를 표시합니다.	Summary Dashboard	FireSIGHT
Intrusion Events to High Criticality Hosts	중요도가 높은 호스트에서 발생한 침입 이벤트의 수를 기반으로 침입 이벤트를 표시합니다.	Detailed Dashboard	보호 + FireSIGHT
Malware Intrusions	악성코드를 전송하는 연결에서 발생한 침입 이벤트의 수를 기반으로 침입 이벤트를 표시합니다.	Files Dashboard	악성코드
Malware Intrusions	네트워크 트래픽에서 시스템 또는 FireAMP Connector가 탐지한 악성코드 위협의 수를 위협 이름별로 그룹화하여 표시합니다.	Files Dashboard	악성코드 라이센스 또는 FireAMP 서브스크립션
New Indications of Compromise over Time	대시보드 시간 범위 중에 탐지된 IOC의 그래프를 표시합니다.	Summary Dashboard	FireSIGHT
Operating Systems	네트워크 내에서 각 운영 체제를 실행하는 호스트의 수를 기반으로 운영 체제를 표시합니다.	Detailed Dashboard	FireSIGHT
Possible Zero-Day Malware	파일이 표시된 횟수를 기반으로, Unknown과 `High` 또는 `Very High` 위협 점수의 파일 성향과 함께 캡처된 파일(대부분 제로 데이 악성코드일 가능성이 큼)을 표시합니다.	Files Dashboard	악성코드
Processes Introducing Malware	FireAMP Connector에서 탐지한 악성코드에 액세스했거나 이를 생성한 시스템 프로세스를 표시합니다.	Files Dashboard	악성코드 라이센스 또는 FireAMP 서브스크립션
Risky Applications with Low Business Relevance	애플리케이션 위험 레벨은 높고 예상 비즈니스 연관성은 낮은, 관리되는 네트워크의 모든 애플리케이션 연결을 표시합니다.	Summary Dashboard	FireSIGHT
Servers	호스트 수 기준으로 서버를 표시합니다.	Detailed Dashboard	FireSIGHT
SSL Actions	빈도를 기반으로, 암호화된 트래픽에서 가져온 SSL 규칙 작업의 카운트를 표시합니다.	Connection Summary	모두
SSL Certificate Status	빈도를 기반으로, SSL 암호화 세션에 시스템이 탐지한 인증서 상태의 카운트를 표시합니다.	Connection Summary	모두

표 55-5 사용자 지정 Analysis Widget 프리셋 (계속)

프리셋	설명	사전 정의된 대시보드	라이센스
SSL Decryption Failure Reasons	빈도를 기반으로, 시스템이 SSL 암호화 세션을 부적절하게 해독한 이유의 카운트를 표시합니다.	Connection Summary	모두
SSL Sessions Decrypted over Time	대시보드 시간 범위 중에 시스템이 해독한 SSL 암호화 세션 수의 그래프를 표시합니다.	Connection Summary	모두
SSL Sessions Not Decrypted over Time	대시보드 시간 범위 중에 시스템이 해독하지 않은 SSL 암호화 세션 수의 그래프를 표시합니다.	Connection Summary	모두
SSL Sessions with Errors over Time	대시보드 시간 범위 중에 내부 오류를 포함한 것으로 시스템이 탐지한 SSL 암호화 세션 수의 그래프를 표시합니다.	Connection Summary	모두
Threat Detections over Time	대시보드 시간 범위 중에 네트워크 트래픽에서 시스템 또는 FireAMP Connector가 탐지한 총 악성코드 위협 수의 그래프를 표시합니다.	Files Dashboard	악성코드 라이센스 또는 FireAMP 서브스크립션
Top Attackers	나열된 IP 주소가 이벤트를 일으킨 연결에서 공격자였던 침입 이벤트의 수를 기반으로, 모니터링되는 네트워크의 공격 호스트 IP 주소를 표시합니다.	Summary Dashboard	보호
Top Client Applications Seen	클라이언트 애플리케이션이 전송한 데이터의 총 킬로바이트를 기반으로, 모니터링되는 네트워크의 클라이언트 애플리케이션을 표시합니다.	Summary Dashboard	FireSIGHT
Top Operating Systems Seen	운영 체제가 있는 네트워크 호스트의 수를 기반으로, 모니터링되는 네트워크의 운영 체제를 표시합니다.	Summary Dashboard	FireSIGHT
Top Server Applications Seen	서비스를 실행하는 호스트의 수를 기반으로, 모니터링되는 네트워크의 서버 애플리케이션을 표시합니다.	Summary Dashboard	FireSIGHT
Top Targets	주소가 이벤트를 일으킨 연결에서 공격 대상이었던 침입 이벤트의 수를 기반으로, 모니터링되는 네트워크의 호스트 IP 주소를 표시합니다.	Summary Dashboard	보호
Top Threats	위협 점수와 함께 저장된 파일의 수를 기반으로, 해당 위협 점수의 분포를 표시합니다.	Files Dashboard	악성코드
Top Web Applications Seen	클라이언트 애플리케이션이 전송한 데이터의 총 킬로바이트를 기반으로, 모니터링되는 네트워크의 웹 애플리케이션을 표시합니다.	Summary Dashboard	FireSIGHT
Total Events by Application	애플리케이션에 의해 생성된 침입 이벤트의 수를 기반으로, 모니터링되는 네트워크의 애플리케이션을 표시합니다.	Application Statistics	보호 + FireSIGHT
Total Events by Application Protocol	애플리케이션 프로토콜과 관련된 침입 이벤트의 수를 기반으로, 모니터링되는 네트워크의 애플리케이션 프로토콜을 표시합니다.	Summary Dashboard	보호 + FireSIGHT

표 55-5 사용자 지정 Analysis Widget 프리셋 (계속)

프리셋	설명	사전 정의된 대시보드	라이센스
Total Events by User	각 사용자 활동에 의해 생성된 침입 이벤트의 수를 기반으로, 모니터링되는 네트워크의 사용자를 표시합니다.	Summary Dashboard Access Controlled User Statistics	보호 + FireSIGHT
Traffic by Application	대시보드 시간 범위 중에 모니터링되는 네트워크에서 애플리케이션이 전송한 데이터의 총 킬로바이트를 기반으로, 모니터링되는 네트워크의 애플리케이션을 표시합니다.	Application Statistics Connection Summary Detailed Dashboard	FireSIGHT
Traffic by Application Category	대시보드 시간 범위 중에 모니터링되는 네트워크에서 각 카테고리의 애플리케이션이 전송한 데이터의 총 킬로바이트를 기반으로, 모니터링되는 네트워크의 애플리케이션 카테고리를 표시합니다.	Application Statistics Summary Dashboard	FireSIGHT
Traffic by Application Risk	대시보드 시간 범위 중에 모니터링되는 네트워크에서 각 레벨의 애플리케이션이 전송한 데이터의 총 킬로바이트를 기반으로, 모니터링되는 네트워크의 애플리케이션 예상 위험 레벨을 표시합니다.	Summary Dashboard	FireSIGHT
Traffic by Business Relevance	대시보드 시간 범위 중에 모니터링되는 네트워크에서 각 레벨의 애플리케이션이 전송한 데이터의 총 킬로바이트를 기반으로, 모니터링되는 네트워크의 애플리케이션 예상 비즈니스 연관성 레벨을 표시합니다.	Summary Dashboard	FireSIGHT
Traffic by Destination Continent	대시보드 시간 범위 중에 모니터링되는 네트워크에서 각 대륙으로 전송된 데이터의 총 킬로바이트를 기반으로, 모니터링되는 네트워크로부터 접속한 대륙을 표시합니다.	Connection Summary	FireSIGHT
Traffic by Destination Country	대시보드 시간 범위 중에 모니터링되는 네트워크에서 각 국가로 전송된 데이터의 총 킬로바이트를 기반으로, 모니터링되는 네트워크로부터 접속한 국가를 표시합니다.	Connection Summary	FireSIGHT
Traffic by Initiator IP	대시보드 시간 범위 중에 모니터링되는 네트워크에서 IP 주소로부터 전송된 데이터의 총 킬로바이트를 기반으로, 모니터링되는 네트워크의 호스트 IP 주소를 표시합니다.	Connection Summary Detailed Dashboard	FireSIGHT
Traffic by Initiator User	사용자가 로그인한 호스트에서 수신된 데이터의 총 킬로바이트를 기반으로, 모니터링되는 네트워크의 사용자를 표시합니다.	Detailed Dashboard Summary Dashboard	FireSIGHT
Traffic by Port	대시보드 시간 범위 중에 모니터링되는 네트워크에서 각 포트를 통해 전송된 데이터의 총 킬로바이트를 기반으로, 모니터링되는 네트워크로의 responder 포트를 표시합니다. 이 위젯의 출력은 연결 로깅 컨피그레이션에 따라 달라집니다.	Connection Summary	FireSIGHT

표 55-5 사용자 지정 Analysis Widget 프리셋 (계속)

프리셋	설명	사전 정의된 대시보드	라이센스
Traffic by Responder IP	대시보드 시간 범위 중에 모니터링되는 네트워크에서 호스트의 IP 주소가 수신한 데이터의 총 킬로바이트를 기반으로, 모니터링되는 네트워크의 IP 주소를 표시합니다. 이 위젯의 출력은 연결 로깅 컨피그레이션에 따라 달라집니다.	Connection Summary Detailed Dashboard	FireSIGHT
Traffic by Security Intelligence Category	대시보드 시간 범위 중에 각 카테고리의 연결을 통해 전송된 데이터의 총 킬로바이트를 기반으로, 모니터링되는 네트워크의 보안 인텔리전스 카테고리를 표시합니다.	Summary Dashboard	보호
Traffic by Source Continent	대시보드 시간 범위 중에 모니터링되는 네트워크에서 각 대륙으로부터 전송된 데이터의 총 킬로바이트를 기반으로, 모니터링되는 네트워크로 데이터를 전송한 대륙을 표시합니다.	Connection Summary	FireSIGHT
Traffic by Source Country	대시보드 시간 범위 중에 모니터링되는 네트워크에서 각 국가로부터 전송된 데이터의 총 킬로바이트를 기반으로, 모니터링되는 네트워크로 데이터를 전송한 국가를 표시합니다.	Connection Summary	FireSIGHT
Traffic by URL Category	대시보드 시간 범위 중에 각 카테고리의 URL과 교환된 데이터의 총 킬로바이트를 기반으로, 모니터링되는 네트워크의 애플리케이션 URL 카테고리를 표시합니다.	URL Statistics	URL 필터링
Traffic by URL Reputation	대시보드 시간 범위 중에 각 평판의 URL과 교환된 데이터의 총 킬로바이트를 기반으로, 모니터링되는 네트워크의 애플리케이션 URL 평판 유형을 표시합니다.	URL Statistics	URL 필터링
Traffic by User	대시보드 시간 범위 중에 각 사용자와 교환된 데이터의 총 킬로바이트를 기반으로, 모니터링되는 네트워크의 사용자를 표시합니다.	없음	FireSIGHT
Traffic over Time	대시보드 시간 범위 중에 모니터링되는 네트워크에서 전송한 총 데이터 킬로바이트의 그래프를 표시합니다.	Connection Summary Detailed Dashboard	FireSIGHT
Unique Applications over Time	대시보드 시간 범위 중에 모니터링되는 네트워크에서 탐지한 총 고유 애플리케이션의 그래프를 표시합니다.	Application Statistics Summary Dashboard	FireSIGHT
Unique Users over Time	대시보드 시간 범위 중에 모니터링되는 네트워크에서 탐지한 총 고유 사용자의 그래프를 표시합니다.	Access Controlled User Statistics	FireSIGHT
Users Affected by Malware	네트워크 트래픽에서 시스템 또는 FireAMP Connector가 탐지한 위협의 수를 사용자별로 그룹화하여 표시합니다.	Files Dashboard	악성코드 + FireSIGHT 또는 FireAMP 서브스크립션
Users Transferring Files	네트워크를 통해 전송된 파일 수를 전송자별로 그룹화하여 표시합니다.	Files Dashboard	악성코드 + FireSIGHT

표 55-5 사용자 지정 Analysis Widget 프리셋 (계속)

프리셋	설명	사전 정의된 대시보드	라이센스
Web Applications Introducing Malware	FireAMP Connector에서 탐지한 악성코드에 액세스했거나 이를 생성한 모니터링되는 네트워크의 웹 애플리케이션을 표시합니다.	Files Dashboard	악성코드 라이센스 또는 FireAMP 서브스크립션
Web Applications Transferring Files	네트워크를 통해 전송된 파일 수를 파일 전송에 사용된 웹 애플리케이션별로 그룹화하여 표시합니다.	Files Dashboard	악성코드 라이센스 또는 FireAMP 서브스크립션
White List Violations	화이트리스트 위반의 호스트를 위반 카운트 단위로 표시합니다.	Detailed Dashboard	FireSIGHT

Custom Analysis 위젯에서 관련 이벤트 보기

라이센스: 모두

Custom Analysis 위젯에 표시하도록 구성된 데이터의 종류에 따라, 위젯에 표시되는 이벤트에 대한 자세한 정보를 제공하는 이벤트 보기(즉, 워크플로)를 호출할 수 있습니다.

대시보드에서 이벤트 보기를 호출하면 대시보드 시간 범위에 의해 제한되어, 해당 유형에 대한 기본 워크플로에 이벤트가 나타납니다. 구성한 시간 창의 개수 및 보고자 하는 이벤트의 유형에 따라, 어플라이언스에 대한 적절한 시간 창도 변경됩니다.

예를 들어 방어 센터에서 여러 시간 창을 구성한 다음 Custom Analysis 위젯에서 상태 이벤트에 액세스하면, 이벤트는 기본 상태 이벤트 워크플로에 나타나고 상태 모니터링 시간 창은 대시보드 시간 범위로 변경됩니다.

또 다른 예로, 단일 시간 창을 구성한 다음 Custom Analysis 위젯에서 임의의 이벤트 유형에 액세스하면 그 이벤트는 해당 이벤트 유형의 기본 워크플로에 나타나고 전역 시간 창은 대시보드 시간 범위로 변경됩니다.

시간 창에 대한 자세한 내용은 71-5페이지의 기본 시간 창 및 60-5페이지의 검색에서 시간 제약 조건 지정을/를 참조하십시오.

Custom Analysis 위젯에서 관련 이벤트를 보려면

액세스: Admin/Any Security Analyst/Maint

1단계 위젯을 구성한 방법에 따라 두 가지 옵션이 제공됩니다.

- 이벤트의 관련 항목을 표시하도록 구성된 위젯(즉, 막대 그래프)에서 아무 이벤트나 클릭하여 환경 설정 및 해당 이벤트에 의해 제한되는 관련 이벤트를 봅니다. 위젯 환경 설정에 의해 제한되는 관련된 모든 이벤트를 보려면 위젯의 오른쪽 아래에 있는 모두 보기 아이콘( )을 클릭할 수도 있습니다.
- 시간에 따른 연결 데이터를 표시하도록 구성된 위젯에서, 위젯 환경 설정에 의해 제한되는 관련된 모든 이벤트를 보려면 위젯의 오른쪽 아래에 있는 모두 보기 아이콘을 클릭합니다.

특정 이벤트 유형 작업에 대한 자세한 내용은 다음 절을 참조하십시오.

- 3-4페이지의 보안 인텔리전스 목록 및 피드 작업
- 69-2페이지의 감사 레코드 보기
- 41-9페이지의 침입 이벤트 보기
- 50-15페이지의 검색 및 호스트 입력 이벤트 보기

- 40-8페이지의 파일 이벤트 보기
- 40-19페이지의 악성코드 이벤트 보기
- 40-31페이지의 캡처된 파일 보기
- 50-19페이지의 호스트 보기
- 50-27페이지의 호스트 특성 보기
- 50-32페이지의 IOC 보기
- 50-36페이지의 서버 보기
- 50-46페이지의 애플리케이션 세부사항 보기
- 50-50페이지의 취약성 보기
- 50-56페이지의 서드파티 취약성 보기
- 39-14페이지의 연결 및 보안 인텔리전스 데이터 보기
- 50-61페이지의 사용자 보기
- 50-67페이지의 사용자 활동 이벤트 보기
- 51-52페이지의 상관관계 이벤트 보기
- 52-30페이지의 화이트리스트 이벤트 보기
- 52-35페이지의 화이트리스트 위반 보기
- 68-48페이지의 상태 이벤트 보기
- 66-21페이지의 Rule Update Log 보기
- 47-19페이지의 활성 스캔 결과 작업
- 58-20페이지의 지오로케이션 사용
- 59-1페이지의 사용자 지정 테이블 이해

사용자 지정 Analysis Widget 제한 사항

라이센스: 모두

Custom Analysis 위젯을 사용할 때 유의해야 할 몇 가지 중요한 사항이 있습니다.

공유 대시보드에서 위젯을 구성 중인 경우, 사용자 계정 권한에 따라 일부 사용자에게는 일부 이벤트 유형의 데이터가 표시되지 않을 수 있습니다. 예를 들어 Maintenance User는 검색 이벤트를 볼 수 없습니다.

마찬가지로, 다른 어플라이언스에서 가져온 대시보드를 사용 중인 경우에도 일부 어플라이언스는 일부 이벤트 유형의 데이터에 액세스할 수는 없다는 점에 유의해야 합니다. 예를 들어 관리되는 디바이스는 상관관계 데이터를 저장하지 않습니다. 사용자가 볼 수 없는 데이터를 표시하는 Custom Analysis 위젯이 대시보드에 포함된 경우, 해당 사용자는 위젯의 데이터를 볼 수 있는 권한이 없는 것입니다. 그러나 사용자(대시보드를 공유하는 모든 사용자)는 자신이 볼 수 있는 데이터를 표시하도록 위젯의 환경 설정을 수정할 수 있으며 위젯을 삭제할 수도 있습니다. 이런 일이 발생하지 않도록 하려면 대시보드를 비공개로 저장하십시오.

비공개로 저장한 검색에는 저장한 당사자만 액세스할 수 있습니다. 공유 대시보드에서 위젯을 구성하고 비공개 검색을 사용하도록 해당 이벤트를 제한하면, 다른 사용자가 로그인할 때 검색을 사용할 수 없도록 위젯이 재설정됩니다. 이렇게 하면 위젯의 보기에도 영향이 미칩니다. 이런 일이 발생하지 않도록 하려면 대시보드를 비공개로 저장하십시오.

시스템 정책의 Dashboard 설정에서 Custom Analysis 위젯을 활성화 또는 비활성화할 수 있습니다. 자세한 내용은 63-14페이지의 대시보드 설정 구성을/를 참조하십시오.

Disk Usage 위젯 이해

라이센스: 모두

Disk Usage 위젯은 디스크 사용량 카테고리를 기반으로 하드 드라이브에서 사용된 공간의 비율을 표시합니다. 또한 어플라이언스의 하드 드라이브에서 각 파티션의 용량 및 사용된 공간의 비율도 표시합니다. 디바이스에 악성코드 스토리지 팩이 설치되어 있거나 방어 센터가 악성코드 스토리지 팩이 포함된 디바이스를 관리하는 경우, Disk Usage 위젯은 악성코드 스토리지 팩에 대해서도 동일한 정보를 표시합니다. 이 위젯은 Default Dashboard 및 Summary Dashboard의 Status 탭에 기본적으로 나타납니다.

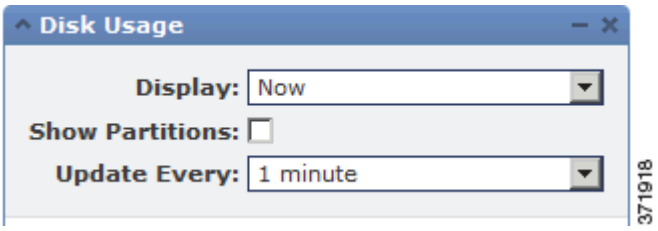
By Category 누적 막대에는 총 가용 디스크 공간 중 사용된 비율로 각 디스크 사용량 카테고리가 표시됩니다. 다음 표에서는 사용 가능한 카테고리에 대해 설명합니다.

표 55-6 디스크 사용량 카테고리

디스크 사용량 카테고리	설명
이벤트	시스템에 로깅된 모든 이벤트
파일	시스템에 저장된 모든 파일
백업	모든 백업 파일
업데이트	규칙 업데이트와 시스템 업데이트 등 업데이트와 관련된 모든 파일
기타	시스템 문제 해결 파일 및 기타 파일
무료	어플라이언스에 남아 있는 빈 공간

By Category 누적 막대에서 디스크 사용량 카테고리 위로 포인터를 이동하면 해당 카테고리에 사용된 가용 디스크 공간의 비율, 디스크의 실제 저장 공간 및 해당 카테고리의 총 가용 디스크 공간을 볼 수 있습니다. 악성코드 스토리지 팩이 설치되어 있으면, Files 카테고리에 대한 총 가용 디스크 공간은 악성코드 스토리지 팩의 가용 디스크 공간입니다. 자세한 내용은 40-3페이지의 캡처된 파일 스토리지 이해을/를 참조하십시오.

위젯 환경 설정을 수정하여 By Category 누적 막대만 표시하거나, 누적 막대 더하기 admin(/), `/Volume` 및 `/boot` 파티션 사용량을 표시하거나, `/var/storage` 파티션도 표시하도록(악성코드 스토리지 팩이 설치된 경우) 위젯을 구성할 수 있습니다.



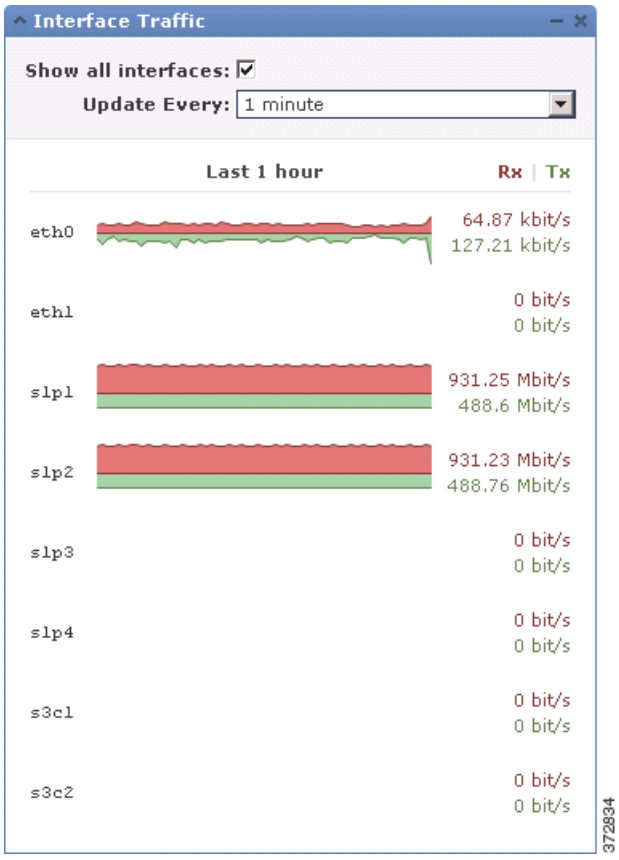
위젯 환경 설정에서는 또한 위젯 업데이트 빈도를 제어하며, 현재 디스크 사용량을 표시할지 대시보드 시간 범위 중에 수집된 디스크 사용량 통계를 표시할지도 제어합니다. 자세한 내용은 55-6페이지의 위젯 환경 설정 이해을/를 참조하십시오.

Interface Traffic 위젯 이해

라이센스: 모두

Interface Traffic 위젯은 대시보드 시간 범위 중에 어플라이언스의 관리(`eth0` 등) 및 센싱(`s1p1` 등) 인터페이스에서 트래픽의 수신(Rx) 및 송신(Tx) 속도를 보여줍니다. 이 위젯은 기본적으로 사전 정의된 대시보드에 나타나지 않습니다.

아웃바운드(전송됨) 트래픽은 플로우 제어 패킷을 포함합니다. 따라서 어플라이언스의 패시브 인터페이스는 전송된 트래픽을 표시하고 이벤트를 생성할 수 있는데, 이는 자연스러운 동작입니다. 동적 분석을 구성하지 않은 경우에도, 활성화된 악성코드 라이센스가 있는 디바이스는 Cisco 클라우드에 대한 연결을 주기적으로 시도합니다. 따라서 이러한 디바이스는 전송된 트래픽을 표시하는데, 이것 역시 자연스러운 동작입니다.

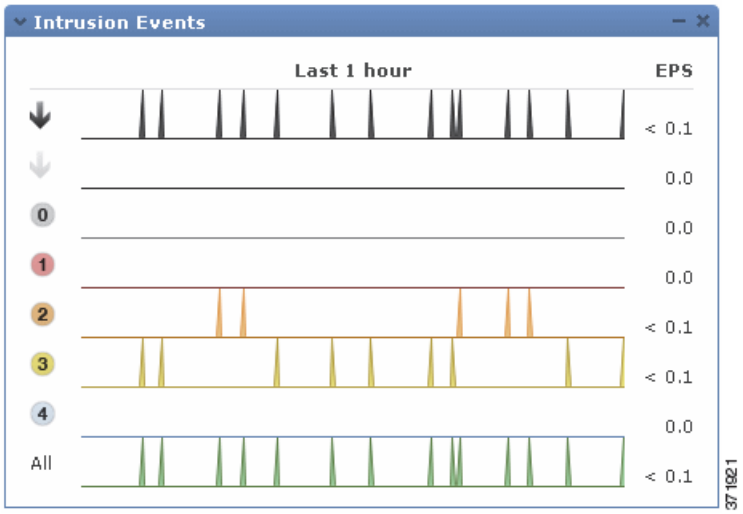


위젯 환경 설정은 위젯 업데이트 빈도를 제어합니다. 관리되는 디바이스의 환경 설정에서는 사용되지 않은 인터페이스에 대한 트래픽 속도의 표시 여부도 제어할 수 있습니다(기본적으로 위젯에는 활성 인터페이스의 트래픽 속도만 표시됨). 자세한 내용은 55-6페이지의 위젯 환경 설정 이해을/를 참조하십시오.

Intrusion Events 위젯 이해

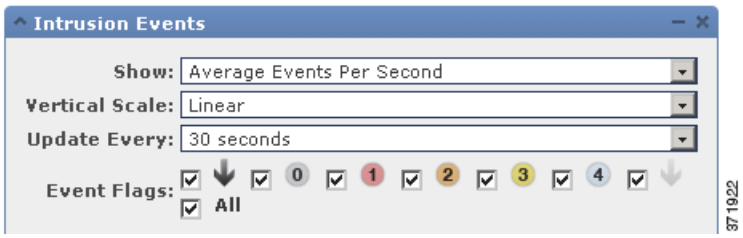
라이센스: 보호

Intrusion Events 위젯은 대시보드 시간 범위 중에 발생한 침입 이벤트를 우선순위별로 구성하여 보여줍니다. 여기에는 삭제된 패킷 및 서로 다른 영향과 함께 침입 이벤트에 대한 통계도 포함됩니다. 이 위젯은 Summary Dashboard의 Intrusion Events 탭에 기본적으로 나타납니다.



관리되는 디바이스에서 이 위젯은 삭제된(또는 수동으로 구축된 디바이스의 경우 삭제되었을) 침입 이벤트, 모든 침입 이벤트 또는 둘 모두에 대한 통계를 표시할 수 있습니다. 로컬 이벤트 스토리지를 활성화해야 하며, 그렇지 않을 경우 위젯에서 데이터를 표시할 수 없습니다. **All**로 표시되는 전체 비율에는 삭제된 이벤트 비율이 포함되지 않습니다.

에서는(관리되는 디바이스 제외) 위젯 환경 설정을 수정하여, 삭제된(dropped)/삭제되었을(would have dropped) 패킷 및 서로 다른 영향과 함께 침입 이벤트를 표시하도록 위젯을 구성할 수 있습니다. 방어 센터NO MDC THIS TIME 및 디바이스에서는 삭제된 이벤트 및 삭제되었을 이벤트를 표시할 수 있습니다. 다음 그림에서는 위젯 환경 설정의 방어 센터 버전을 보여줍니다.



위젯 환경 설정에서 다음을 수행할 수 있습니다.

- 에서하나 이상의 **Event Flags** 확인란을 선택하여 삭제된 패킷, 삭제되었을 패킷 또는 특정 영향이 포함된 이벤트에 대한 별도의 그래프를 표시할 수 있습니다. 영향 또는 규칙 상태와 상관없이 모든 침입 이벤트에 대한 추가 그래프를 표시하려면 **All**을 선택합니다. 자세한 내용은 41-38페이지의 이벤트를 평가하기 위한 영향 레벨 사용을/를 참조하십시오.
- **Show**를 선택한 후 **Average Events Per Second** 또는 **Total Events**를 선택할 수 있습니다.
- **Vertical Scale**을 선택한 후 **Linear**(incremental) 또는 **Logarithmic**(factor of ten) 비율을 선택할 수 있습니다.

환경 설정은 또한 위젯 업데이트 빈도를 제어합니다. 자세한 내용은 55-6페이지의 위젯 환경 설정 이해을/를 참조하십시오.

Intrusion Events 위젯에서 다음을 수행할 수 있습니다.

- 에서 삭제된 패킷, 삭제되었을 패킷 또는 특정 영향에 해당하는 그래프를 클릭하여 해당 유형의 침입 이벤트를 볼 수 있습니다.
- 삭제된 이벤트에 해당하는 그래프를 클릭하여 삭제된 이벤트를 볼 수 있습니다.
- 삭제되었을 이벤트에 해당하는 그래프를 클릭하여 삭제되었을 이벤트를 볼 수 있습니다.
- **모든** 그래프를 클릭하여 모든 침입 이벤트를 볼 수 있습니다.

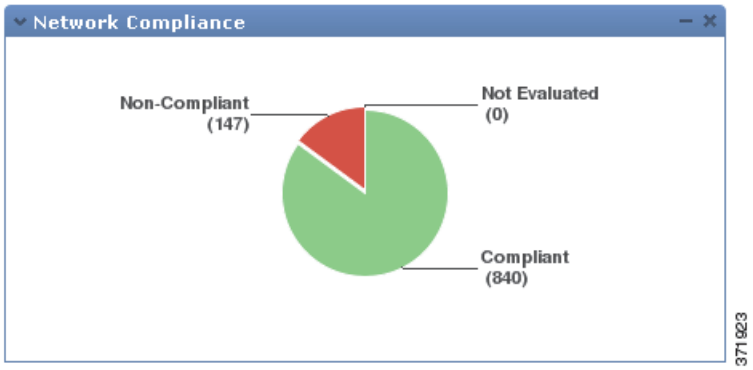
결과 이벤트 보기는 대시보드 시간 범위에 의해 제한됩니다. 대시보드를 통해 침입 이벤트에 액세스하면 어플라이언스에 대한 이벤트(또는 전역) 시간 창이 변경됩니다. 침입 이벤트에 대한 자세한 내용은 41-9페이지의 침입 이벤트 보기을/를 참조하십시오.

또한 침입 정책의 인라인 삭제 동작 또는 규칙 상태와 상관없이, 패시브 구축의 패킷은 삭제되지 않는다는 점에 유의하십시오.

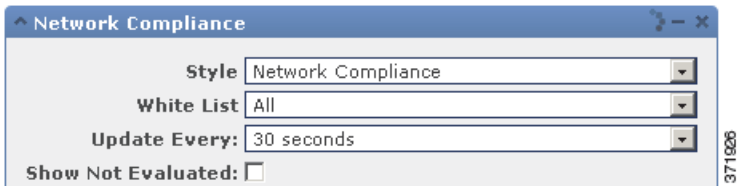
Network Compliance 위젯 이해

라이센스: FireSIGHT

Network Compliance 위젯은 사용자가 구성한 화이트리스트에 대한 호스트의 규정준수를 요약하여 보여줍니다(52-1페이지의 규정준수 툴로 FireSIGHT 시스템 사용 참조). 기본적으로 이 위젯은 활성 상관관계 정책에 있는 모든 규정준수 화이트리스트에 대해 규정을 준수하는 호스트, 규정을 준수하지 않는 호스트, 평가되지 않은 호스트의 수를 보여주는 원 그래프를 표시합니다. 이 위젯은 Detailed Dashboard의 Correlation 탭에 기본적으로 나타납니다.



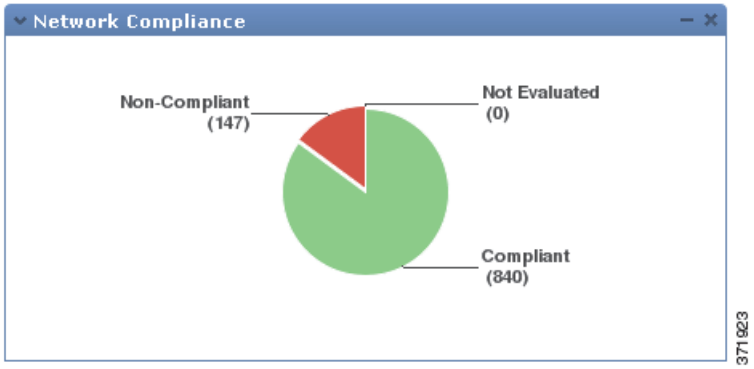
위젯 환경 설정을 수정하여 모든 화이트리스트 또는 특정 화이트리스트에 대한 네트워크 규정준수를 표시하도록 위젯을 구성할 수 있습니다.



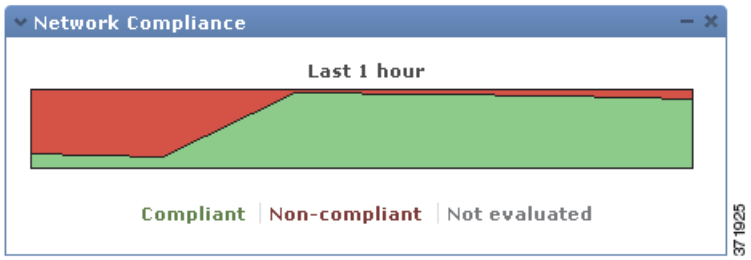
모든 화이트리스트에 대한 네트워크 규정 준수를 표시하도록 선택하는 경우, 호스트가 활성 상관관계 정책에서 임의의 화이트리스트를 따르지 않으면 위젯은 해당 호스트를 규정을 준수하지 않는 호스트로 간주합니다.

또한 위젯 환경 설정을 사용하여 네트워크 규정준수를 표시하기 위해 사용할 세 가지 서로 다른 스타일 중 하나를 지정할 수 있습니다.

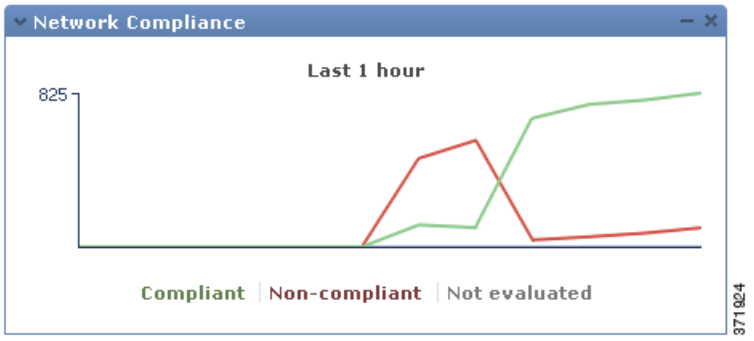
Network Compliance 스타일(기본값)은 규정을 준수하는 호스트, 규정을 준수하지 않는 호스트, 평가되지 않은 호스트의 수를 보여주는 원 그래프를 표시합니다. 호스트 위반 카운트를 보려면 원 그래프를 클릭할 수 있습니다. 그러면 하나 이상의 화이트리스트를 위반하는 호스트가 나열됩니다. 자세한 내용은 52-35페이지의 화이트리스트 위반 보기을/를 참조하십시오.



Network Compliance over Time (%) 스타일은 대시보드 시간 범위 중에 규정을 준수하는 호스트, 규정을 준수하지 않는 호스트, 평가되지 않은 호스트의 상대 비율을 보여주는 누적 영역 그래프를 표시합니다.



Network Compliance over Time 스타일은 대시보드 시간 범위 중에 규정을 준수하는 호스트, 규정을 준수하지 않는 호스트, 평가되지 않은 호스트의 수를 보여주는 선 그래프를 표시합니다.

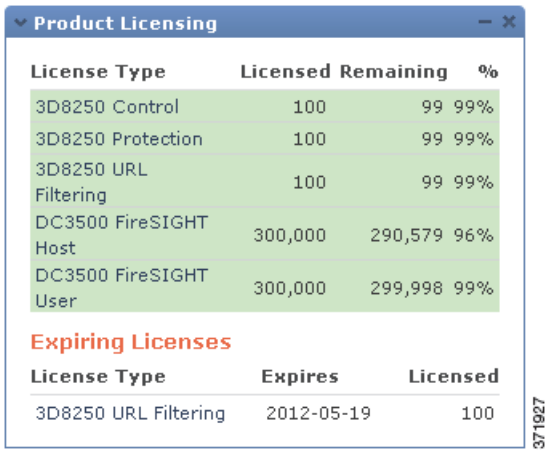


환경 설정은 위젯 업데이트 빈도를 제어합니다. 평가되지 않은 이벤트를 숨기려면 **Show Not Evaluated** 확인란을 선택할 수 있습니다. 자세한 내용은 55-6페이지의 위젯 환경 설정 이해을/를 참조하십시오.

Product Licensing 위젯 이해

라이센스: 모두

Product Licensing 위젯은 현재 방어 센터에 설치된 디바이스 및 기능 라이센스를 보여줍니다. 또한 라이센스된 항목(예: 호스트 또는 사용자) 수와 허용되는 나머지 라이센스된 항목의 수도 표시합니다. 이 위젯은 기본적으로 사전 정의된 대시보드에 나타나지 않습니다.



위젯의 위 섹션에는 방어 센터에 설치된 모든 디바이스 및 기능 라이센스(임시 라이센스 포함)가 표시되고, Expiring Licenses 섹션에는 임시 및 만료된 라이센스만 표시됩니다. 예를 들어 FireSIGHT Hosts에 대해 두 개의 기능 라이센스가 있어서 하나는 영구 라이센스로서 호스트 750개를 허용하며 다른 하나는 임시 라이센스로서 추가 호스트 750개를 허용하는 경우, 위젯의 위 섹션에는 FireSIGHT Hosts 기능 라이센스 및 1500개의 라이센스된 호스트가 표시되고 Expiring Licenses 섹션에는 FireSIGHT Hosts 기능 라이센스와 750개의 호스트가 표시됩니다.

위젯 배경의 막대는 사용되고 있는 각 라이센스 유형의 비율을 보여줍니다. 오른쪽에서 왼쪽으로 막대를 읽어야 합니다. 만료된 라이센스는 취소선으로 표시됩니다.

위젯 환경 설정을 수정하여 현재 라이센스된 기능을 표시하거나 라이센스할 수 있는 모든 기능을 표시하도록 위젯을 구성할 수 있습니다. 환경 설정은 또한 위젯 업데이트 빈도를 제어합니다. 자세한 내용은 55-6페이지의 위젯 환경 설정 이해을/를 참조하십시오.

라이센스 유형 중 하나를 클릭하여 로컬 컨피그레이션의 License 페이지로 이동해서 기능 라이센스를 추가 또는 삭제할 수 있습니다. 자세한 내용은 65-1페이지의 FireSIGHT 시스템 라이센싱을/를 참조하십시오.

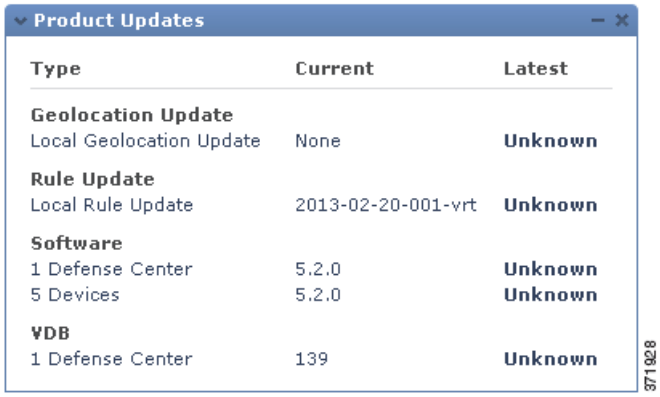
Product Updates 위젯 이해

라이센스: 모두

Product Updates 위젯은 어플라이언스에 현재 설치된 소프트웨어(FireSIGHT 시스템 소프트웨어 및 규칙 업데이트)의 요약과 함께, 다운로드했지만 아직 설치하지 않은 해당 소프트웨어에 대해 사용 가능한 업데이트에 대한 정보도 표시합니다. 이 위젯은 Detailed Dashboard 및 Summary Dashboard의 Status 탭에 기본적으로 나타납니다.

소프트웨어 업데이트를 다운로드, 푸시 또는 설치할 예약 작업을 구성하지 않은 경우 최신 소프트웨어 버전은 Unknown으로 표시됩니다. 위젯은 예약 작업을 사용하여 최신 버전을 확인합니다. 자세한 내용은 62-1페이지의 작업 예약을/를 참조하십시오.

이 위젯은 소프트웨어를 업데이트할 수 있는 페이지에 대한 링크도 제공합니다. 위젯의 방어 센터 버전은 관리되는 디바이스에서 소프트웨어를 업데이트할 수 있도록 유사한 링크를 제공합니다.



위젯 환경 설정을 수정하여 최신 버전을 숨기도록 위젯을 구성할 수 있습니다. 환경 설정은 또한 위젯 업데이트 빈도를 제어합니다. 자세한 내용은 55-6페이지의 위젯 환경 설정 이해을/를 참조하십시오.

Product Updates 위젯에서 다음을 수행할 수 있습니다.

- FireSIGHT 시스템 소프트웨어, 규칙 업데이트, 지오로케이션 업데이트 또는 VDB의 현재 버전을 클릭하여 어플라이언스를 수동으로 업데이트할 수 있습니다.
- 시스템 소프트웨어, 지오로케이션 데이터베이스 또는 VDB를 업데이트할 수 있습니다. 66-1페이지의 시스템 소프트웨어 업데이트을/를 참조하십시오.
- 최신 규칙 업데이트를 가져올 수 있습니다. 66-14페이지의 규칙 업데이트 및 로컬 규칙 파일 가져오기을/를 참조하십시오.
- 최신 버전을 클릭하거나 Latest 열의 **Unknown** 링크를 클릭하여 FireSIGHT 시스템 소프트웨어, 규칙 업데이트 또는 VDB의 최신 버전을 다운로드하기 위한 예약 작업을 생성할 수 있습니다. 62-1페이지의 작업 예약을/를 참조하십시오.

RSS Feed 위젯 이해

라이센스: 모두

RSS Feed 위젯은 RSS 피드를 대시보드에 추가합니다. 기본적으로 이 위젯은 Cisco 보안 뉴스의 피드를 보여줍니다. Detailed Dashboard 및 Summary Dashboard의 Status 탭에 기본적으로 나타납니다.

회사 뉴스, Snort.org 블로그 또는 VRT(Vulnerability Research Team) 블로그의 사전 구성된 피드를 표시하도록 위젯을 구성할 수도 있고, 위젯 환경 설정에서 URL을 지정하여 다른 RSS 피드에 대한 사용자 지정 연결을 생성할 수도 있습니다.

피드는 24시간마다 업데이트되며(수동으로 업데이트 가능), 위젯은 어플라이언스의 현지 시간을 기반으로 피드가 업데이트된 마지막 시간을 표시합니다. 어플라이언스는 웹사이트(사전 구성된 두 피드의 경우) 또는 구성한 사용자 지정 피드에 액세스할 수 있어야 합니다.

위젯을 구성할 때에는 또한 위젯에 표시할 피드의 스토리 수는 물론 헤드라인과 함께 스토리의 설명을 표시할지 여부도 선택할 수 있습니다. 모든 RSS 피드가 설명을 사용하는 것은 아닙니다.

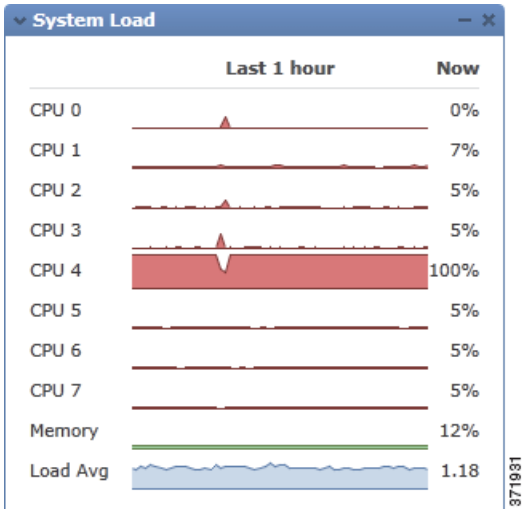
RSS Feed 위젯에서 다음을 수행할 수 있습니다.

- 스토리를 보려는 피드에서 스토리 중 하나를 클릭할 수 있습니다.
- **more** 링크를 클릭하여 피드의 웹사이트로 이동할 수 있습니다.
- 업데이트 아이콘( )을 클릭하여 피드를 수동으로 업데이트할 수 있습니다.

System Load 위젯 이해

라이센스: 모두

System Load 위젯은 현재 및 대시보드 시간 범위 모두에 대해 어플라이언스의 CPU 사용량(각 CPU), 메모리(RAM) 사용량 및 시스템 로드(실행을 기다리는 프로세스의 수로 측정한 로드 평균이라고도 함)를 보여줍니다. Detailed Dashboard 및 Summary Dashboard의 Status 탭에 기본적으로 나타납니다.

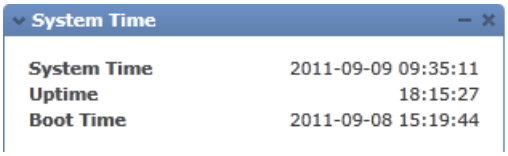


위젯 환경 설정을 수정하여 로드 평균을 표시하거나 숨기도록 위젯을 구성할 수 있습니다. 환경 설정은 또한 위젯 업데이트 빈도를 제어합니다. 자세한 내용은 55-6페이지의 위젯 환경 설정 이해을/를 참조하십시오.

System Time 위젯 이해

라이센스: 모두

System Time 위젯은 어플라이언스의 로컬 시스템 시간, 가동 시간 및 부팅시간을 보여줍니다. Detailed Dashboard 및 Summary Dashboard의 Status 탭에 기본적으로 나타납니다.

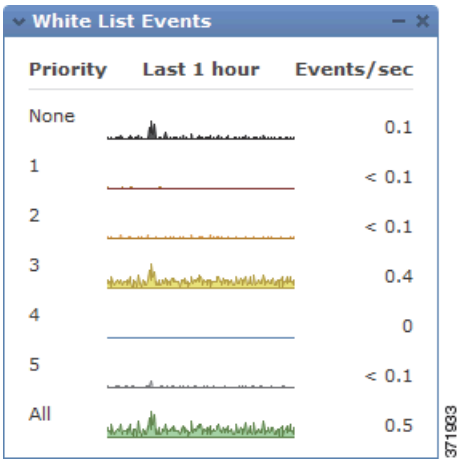


위젯 환경 설정을 수정하여 부팅시간을 숨기도록 위젯을 구성할 수 있습니다. 환경 설정은 또한 위젯과 어플라이언스 시계의 동기화 빈도를 제어합니다. 자세한 내용은 55-6페이지의 위젯 환경 설정 이해을/를 참조하십시오.

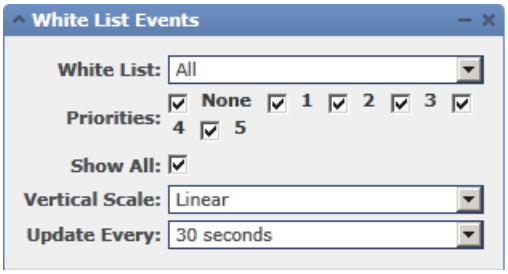
White List Events 위젯 이해

라이센스: FireSIGHT

White List Events 위젯은 대시보드 시간 범위 중에 우선순위별 초당 평균 이벤트 수를 보여줍니다. 이 위젯은 Default Dashboard의 Correlation 탭에 기본적으로 나타납니다.



위젯 환경 설정을 수정하여 서로 다른 우선순위의 화이트리스트 이벤트를 표시하도록 위젯을 구성할 수 있습니다.



위젯 환경 설정에서 다음을 수행할 수 있습니다.

- 특정 우선순위의 이벤트(우선순위가 없는 이벤트 포함)에 대해 별도의 그래프를 표시하려면 하나 이상의 **Priorities** 확인란을 선택할 수 있습니다.
- 우선순위와 상관없이 모든 상관관계 이벤트에 대해 추가 그래프를 표시하려면 **Show All**을 선택할 수 있습니다.
- **Vertical Scale**을 선택한 후 **Linear**(incremental) 또는 **Logarithmic**(factor of ten) 비율을 선택할 수 있습니다.

환경 설정은 또한 위젯 업데이트 빈도를 제어합니다. 자세한 내용은 55-6페이지의 위젯 환경 설정 이해을/를 참조하십시오.

특정 우선순위의 화이트리스트 이벤트를 보려면 그래프 하나를 클릭하고, 모든 화이트리스트 이벤트를 보려면 **모든** 그래프를 클릭합니다. 어떤 경우든 이벤트는 대시보드 시간 범위에 의해 제한됩니다. 대시보드를 통해 화이트리스트 이벤트에 액세스하면 방어 센터에 대한 이벤트(또는 전역) 시간 창이 변경됩니다. 화이트리스트 이벤트에 대한 자세한 내용은 52-30페이지의 화이트리스트 이벤트 보기을/를 참조하십시오.

대시보드 작업

라이센스: 모두

대시보드에 나타나는 위젯을 보고 수정할 수 있습니다.

대시보드는 Dashboard Management 페이지에서 관리합니다(55-37페이지의 대시보드 보기 참조). 대시보드를 생성, 보기, 수정, 내보내기 및 삭제할 수 있습니다.

각 대시보드에 대해 페이지에는 소유자(생성한 사용자) 및 대시보드의 비공개 여부가 표시됩니다. Administrator 액세스 권한이 없는 경우 자신의 비공개 대시보드만 볼 수 있으며, 다른 사용자가 생성한 비공개 대시보드는 보거나 수정할 수 없습니다.

마지막으로, 페이지에는 기본 대시보드가 표시됩니다. 사용자 환경 설정에서 기본 대시보드를 지정할 수 있습니다. 자세한 내용은 71-8페이지의 기본 대시보드 지정을/를 참조하십시오.

대시보드 작업에 대한 자세한 내용은 다음을 참조하십시오.

- 55-35페이지의 사용자 지정 대시보드 생성
- 55-37페이지의 대시보드 보기
- 55-39페이지의 대시보드 수정
- 55-43페이지의 대시보드 삭제
- A-2페이지의 컨피그레이션 내보내기

사용자 지정 대시보드 생성

라이센스: 모두

직접 생성한 것이든 Cisco의 사전 정의된 것이든, 기존 대시보드를 기반으로 새 대시보드를 생성할 수 있습니다. 이렇게 하면 기존 대시보드의 복사본이 만들어집니다. 이 복사본을 필요에 맞게 수정할 수 있습니다. 선택적으로, 기존 대시보드를 기반으로 하지 않도록 선택하여 비어 있는 새 대시보드를 생성할 수도 있습니다.

탭 변경 및 페이지 새로 고침 간격도 지정(또는 비활성화)해야 합니다. 이러한 설정은 대시보드가 해당 탭을 순환하는 빈도 및 전체 대시보드 페이지 새로 고침 빈도를 결정합니다.

전체 대시보드를 새로 고치면, 마지막 대시보드 새로 고침 이후 다른 사용자가 공유 대시보드에 대해 수행한 환경 설정 또는 레이아웃 변경 사항이나, 자신이 다른 컴퓨터에서 비공개 대시보드에 대해 수행한 변경 사항을 볼 수 있습니다. 이 기능은 예를 들면 대시보드가 늘 표시되는 NOC(network operations center)에서 유용할 수 있습니다. 대시보드를 변경하려면 로컬 컴퓨터에서 변경할 수 있습니다. 그러면 NOC의 대시보드는 지정된 간격으로 자동으로 새로 고쳐지며, NOC의 대시보드를 수동으로 새로 고치지 않아도 변경 사항이 표시됩니다. 데이터 업데이트를 보기 위해 전체 대시보드를 새로 고칠 필요는 없습니다. 개별 위젯은 환경 설정에 따라 업데이트됩니다.

마지막으로, 새 대시보드를 비공개 대시보드로 저장하여 사용자 계정과 연결하도록 선택할 수 있습니다. 대시보드를 비공개로 저장하도록 선택하지 않으면 어플라이언스의 다른 사용자들이 볼 수 있습니다.

모든 사용자 역할이 모든 대시보드 위젯에 액세스할 수 있는 것은 아니므로, 권한이 더 적은 사용자가 권한이 더 많은 사용자가 생성한 대시보드를 볼 때 대시보드의 위젯 중 일부가 표시되지 않을 수 있습니다. 무단 위젯이 대시보드에 나타날 수 있지만 비활성화된 상태로 나타납니다.

역할과 상관없이 대시보드 액세스 권한이 있는 사용자는 공유 대시보드를 수정할 수 있다는 사실을 염두에 두어야 합니다. 자신만이 특정 대시보드를 수정할 수 있도록 하려면 비공개로 저장해야 합니다.

팁 새 대시보드를 생성하지 않고 다른 어플라이언스에서 대시보드를 내보낸 다음 현재 어플라이언스로 가져올 수 있습니다. 그런 다음 가져온 대시보드를 필요에 맞게 수정할 수 있습니다. 표시되는 대시보드 위젯은 사용 중인 어플라이언스 유형 및 사용자 역할에 따라 달라집니다. 예를 들어 방어 센터에서 생성하여 관리되는 디바이스 NO MDC THIS TIME에 가져온 대시보드에는 몇몇 비활성화되고 잘못된 위젯이 표시될 수 있습니다. 자세한 내용은 A-1페이지의 컨피그레이션 가져오기 및 내보내기을/를 참조하십시오.

새 대시보드를 생성하려면

액세스: Admin/Any Security Analyst/Maint

1단계 **Overview > Dashboards > Management**를 선택합니다.

Dashboard Management 페이지가 나타납니다.

2단계 **Create Dashboard**를 클릭합니다.

Create Dashboard 페이지가 나타납니다.

3단계 **Copy Dashboard** 드롭다운 목록을 사용하여, 새 대시보드의 기반으로 삼을 대시보드를 선택합니다.

원하는 사전 정의된 대시보드 또는 사용자 정의 대시보드를 선택할 수 있습니다. 선택적으로, 빈 대시보드를 생성하려면 **None**(기본값)을 선택합니다.

4단계 대시보드의 이름과 선택적인 설명을 입력합니다.

5단계 대시보드에서 탭을 변경하는 빈도를 **Change Tabs Every** 필드에 지정합니다(분 단위).

대시보드를 일시 중지하거나 대시보드에 탭이 하나뿐인 경우가 아니면, 여기서 지정한 간격으로 보기가 다음 탭으로 이동합니다. 탭 순환을 비활성화하려면 **Change Tabs Every** 필드에 0을 입력합니다.

6단계 현재 대시보드 탭을 새 데이터로 새로 고칠 빈도를 **Refresh Page Every** 필드에 지정합니다(분 단위). 이 값은 **Change Tabs Every** 설정보다 커야 합니다.

대시보드를 일시 중지하지 않는 한, 여기서 지정한 간격으로 전체 대시보드 새로 고침이 수행됩니다. 주기적인 페이지 새로 고침을 비활성화하려면 **Refresh Page Every** 필드에 0을 입력합니다.

이 설정은 많은 개별 위젯에서 사용할 수 있는 업데이트 간격과는 별개입니다. 대시보드 페이지를 새로 고치면 개별 위젯의 업데이트 간격이 재설정되지만, **Refresh Page Every** 설정을 비활성화하더라도 위젯은 개별 환경 설정에 따라 업데이트됩니다.

7단계 선택적으로, 대시보드를 사용자 계정과 연결하여 다른 사용자가 대시보드를 보고 수정하지 못하게 하려면 **Save As Private** 확인란을 선택합니다.

8단계 **Save**를 클릭합니다.

대시보드가 생성되어 웹 인터페이스에 나타납니다. 이제 탭과 위젯을 추가하여(기존 대시보드를 기반으로 생성한 경우 위젯을 정돈 및 삭제하여) 필요에 맞게 수정할 수 있습니다. 자세한 내용은 55-39페이지의 대시보드 수정을/를 참조하십시오.

대시보드 보기

라이센스: 모두

기본적으로 어플라이언스의 홈 페이지에는 기본 대시보드가 표시됩니다. 기본 대시보드를 정의하지 않은 경우 홈 페이지에는 Dashboard Management 페이지가 표시되며, 여기에서 원하는 대시보드를 선택할 수 있습니다. 언제든 어플라이언스용으로 구성한 기본 대시보드를 보려면 **Overview > Dashboards**를 선택합니다. 사용 가능한 모든 대시보드의 세부사항을 보려면 **Overview > Dashboards > Management**를 선택합니다.

팁 대시보드 페이지가 아닌 페이지를 포함하여 다른 기본 홈 페이지를 표시하도록 어플라이언스를 구성할 수 있습니다. 기본 대시보드를 변경할 수도 있습니다. 자세한 내용은 71-2페이지의 홈 페이지 지정 및 71-8페이지의 기본 대시보드 지정을/를 참조하십시오.

각 대시보드에는 위젯을 제한하는 시간 범위가 있습니다. 시간 범위를 마지막 시간(기본값) 단위로 짧게, 또는 마지막 연도 단위로 길게 반영하도록 구성할 수 있습니다. 시간 범위를 변경하면 시간의 제한을 받을 수 있는 위젯은 새 시간 범위를 반영하여 자동으로 업데이트됩니다.

모든 위젯이 시간의 제한을 받는 것은 아닙니다. 예를 들어 어플라이언스 이름, 모델, FireSIGHT 시스템 소프트웨어의 현재 버전을 비롯한 정보를 제공하는 Appliance Information 위젯에는 대시보드 시간 범위가 영향을 미치지 않습니다.

FireSIGHT 시스템의 엔터프라이즈 구축에서 시간 범위를 긴 기간으로 변경하는 것은, 새 이벤트가 이전 이벤트를 교체하는 빈도에 따라 Custom Analysis 등의 위젯에는 유용하지 않을 수 있습니다.

대시보드를 일시 중지할 수도 있는데, 그렇게 하면 표시를 변경하고 분석을 중단하지 않아도 위젯에서 제공하는 데이터를 검토할 수 있습니다. 대시보드 일시 중지는 다음과 같은 효과가 있습니다.

- **Update Every** 위젯 환경 설정과 상관없이 개별 위젯의 업데이트가 중지됩니다.
- 대시보드 속성의 **Cycle Tabs Every** 설정과 상관없이 대시보드 탭 순환이 중지됩니다.
- 대시보드 속성의 **Refresh Page Every** 설정과 상관없이 대시보드 페이지 새로 고침이 중지됩니다.
- 시간 범위 변경이 영향을 미치지 않습니다.

분석을 마치면 대시보드의 일시 중지를 취소할 수 있습니다. 대시보드의 일시 중지를 취소하면 현재 시간 범위를 반영하여 페이지의 모든 해당 위젯이 업데이트됩니다. 또한 대시보드 속성에서 지정한 설정에 따라 대시보드 탭의 순환이 다시 시작되고, 대시보드 페이지의 새로 고침도 다시 시작됩니다.

시스템 정보를 대시보드로 보내는 플로우가 중단되는 연결 문제나 기타 문제가 발생하면, 대시보드가 자동으로 일시 중지되고 문제가 해결될 때까지 오류 알림이 나타납니다.

참고 대시보드의 일시 중지 여부와 상관없이, 비활성 상태가 1시간(또는 구성된 다른 간격 동안) 지속되면 일반적으로 세션에서 로그아웃됩니다. 대시보드를 오랫동안 수동으로 모니터링할 계획이면 세션 시간 초과에서 일부 사용자를 제외하거나 시스템 시간 초과 설정을 변경하는 방법을 고려해 보십시오. 자세한 내용은 61-47페이지의 사용자 로그인 설정 관리 및 63-29페이지의 사용자 인터페이스 설정 구성을/를 참조하십시오.

대시보드를 보려면

액세스: Admin/Any Security Analyst/Maint

1단계 **Overview > Dashboards**를 선택합니다. 기본 대시보드를 정의했는지 여부에 따라 두 가지 옵션이 제공됩니다.

- 기본 대시보드가 정의된 경우 해당 대시보드가 나타납니다. 다른 대시보드를 보려면 **Overview > Dashboards** 메뉴를 사용합니다.
- 기본 대시보드가 정의되지 않은 경우 Dashboard Management 페이지가 나타납니다. 보려는 대시보드 옆에 있는 **View**를 클릭합니다.

선택한 대시보드가 나타납니다.

대시보드 시간 범위를 변경하려면

액세스: Admin/Any Security Analyst/Maint

1단계 **Show the last** 드롭다운 목록에서 대시보드 시간 범위를 선택합니다.

대시보드가 일시 중지되지 않은 한, 새 시간 범위를 반영하여 페이지의 모든 해당 위젯이 업데이트됩니다.

대시보드를 일시 중지하려면

액세스: Admin/Any Security Analyst/Maint

1단계 시간 범위 컨트롤에서 일시 중지 아이콘()을 클릭합니다.

일시 중지를 취소할 때까지 대시보드가 일시 중지됩니다.

대시보드의 일시 중지를 취소하려면

액세스: Admin/Any Security Analyst/Maint

1단계 일시 중지된 대시보드의 시간 범위 컨트롤에서 재생 아이콘()을 클릭합니다.

대시보드의 일시 중지가 취소됩니다.

대시보드 수정

라이센스: 모두

대시보드에는 하나 이상의 탭이 있습니다. 탭을 추가, 삭제 및 이름 변경할 수 있습니다. 대시보드 탭의 순서는 변경할 수 없습니다.

각 탭의 3단 레이아웃에 하나 이상의 위젯을 표시할 수 있습니다. 위젯을 최소화 및 최대화하고, 탭에서 위젯을 제거하고, 탭에 있는 위젯을 재정돈할 수 있습니다.

기본 대시보드 속성을 변경할 수도 있습니다. 여기에는 이름과 설명, 탭 순환 및 페이지 새로 고침 간격, 대시보드를 타인과 공유할지 여부 등이 포함됩니다.

역할과 상관없이 대시보드 액세스 권한이 있는 사용자는 공유 대시보드를 수정할 수 있습니다. 특정 대시보드를 자신만 수정할 수 있도록 하려면 대시보드 속성에서 해당 대시보드를 비공개로 설정해야 합니다.

Cisco 사전 정의 대시보드에 있는 Custom Analysis 위젯의 모든 컨피그레이션은 해당 위젯의 프리셋에 해당합니다. 이러한 위젯 중 하나를 변경 또는 삭제한 경우 적절한 프리셋을 기반으로 새 Custom Analysis 위젯을 생성하여 복원할 수 있습니다. 자세한 내용은 다음을 참조하십시오.

팁 Cisco 사전 정의 대시보드에 있는 Custom Analysis 위젯의 모든 컨피그레이션은 해당 위젯의 시스템 프리셋에 해당합니다. 이러한 위젯 중 하나를 변경 또는 삭제한 경우 적절한 프리셋을 기반으로 새 Custom Analysis 위젯을 생성하여 복원할 수 있습니다. 자세한 내용은 55-15페이지의 Custom Analysis 위젯 구성을/를 참조하십시오.

자세한 내용은 다음 절을 참조하십시오.

- 55-39페이지의 대시보드 속성 변경
- 55-40페이지의 탭 추가
- 55-40페이지의 탭 삭제
- 55-41페이지의 탭 이름 변경
- 55-41페이지의 위젯 추가
- 55-42페이지의 위젯 정돈
- 55-42페이지의 위젯 최소화 및 최대화
- 55-42페이지의 위젯 삭제

대시보드 속성 변경

라이센스: 모두

이름과 설명, 탭 순환 및 페이지 새로 고침 간격, 대시보드를 타인과 공유할지 여부 등을 비롯한 기본 대시보드 속성을 변경하려면 다음 절차를 사용하십시오.

대시보드의 속성을 변경하려면

액세스: Admin/Any Security Analyst/Maint

1단계 **Overview > Dashboards > Management**를 선택합니다.

Dashboard Management 페이지가 나타납니다.

2단계 속성을 변경할 대시보드 옆에 있는 수정 아이콘( )을 클릭합니다.

Edit Dashboard 페이지가 나타납니다. 변경할 수 있는 각종 컨피그레이션에 대한 자세한 내용은 55-35페이지의 사용자 지정 대시보드 생성을/를 참조하십시오.

3단계 필요한 대로 변경하고 **Save**를 클릭합니다.

대시보드가 변경됩니다.

탭 추가

라이센스: 모두

대시보드에 탭을 추가하려면 다음 절차를 사용하십시오.

대시보드에 탭을 추가하려면

액세스: Admin/Any Security Analyst/Maint

1단계 탭을 추가하려는 대시보드를 표시합니다.

자세한 내용은 55-37페이지의 대시보드 보기을/를 참조하십시오.

2단계 기존 탭의 오른쪽에서 탭 추가 아이콘(+)을 클릭합니다.

탭의 이름을 지정할 수 있는 팝업 창이 나타납니다.

3단계 탭의 이름을 입력하고(최대 25자) **OK**를 클릭합니다. 기본 이름을 사용하려면 그냥 **OK**를 클릭합니다. 언제든지 탭의 이름을 변경할 수 있습니다. 55-41페이지의 탭 이름 변경을/를 참조하십시오.

새 탭이 추가됩니다. 이제 새 탭에 위젯을 추가할 수 있습니다. 자세한 내용은 55-41페이지의 위젯 추가을/를 참조하십시오.

탭 삭제

라이센스: 모두

대시보드 탭과 모든 해당 위젯을 삭제하려면 다음 절차를 사용하십시오. 대시보드의 마지막 탭은 삭제할 수 없습니다. 각 대시보드에는 탭이 적어도 하나는 있어야 합니다.

대시보드에서 탭을 삭제하려면

액세스: Admin/Any Security Analyst/Maint

1단계 탭을 삭제하려는 대시보드를 표시합니다.

자세한 내용은 55-37페이지의 대시보드 보기을/를 참조하십시오.

2단계 삭제하려는 탭에서 삭제 아이콘(✖)을 클릭합니다.

3단계 탭을 삭제할 것임을 확인합니다.

탭이 삭제됩니다.

탭 이름 변경

라이센스: 모두

대시보드 탭의 이름을 변경하려면 다음 절차를 사용하십시오.

탭의 이름을 변경하려면

액세스: Admin/Any Security Analyst/Maint

1단계 탭의 이름을 변경하려는 대시보드를 표시합니다.

자세한 내용은 55-37페이지의 대시보드 보기을/를 참조하십시오.

2단계 이름을 변경할 탭을 클릭합니다.

3단계 탭 제목을 클릭합니다.

탭의 이름을 변경할 수 있는 팝업 창이 나타납니다.

4단계 탭의 이름을 입력하고(최대 25자) **OK**를 클릭합니다.

탭의 이름이 변경됩니다.

위젯 추가

라이센스: 모두

대시보드에 위젯을 추가하려면 먼저 위젯을 추가할 탭을 결정해야 합니다. 탭에 위젯을 추가하면, 위젯 수가 가장 적은 열에 자동으로 추가됩니다. 모든 열의 위젯 수가 동일하면 새 위젯은 맨 왼쪽 열에 추가됩니다. 대시보드 탭 하나에 최대 15개의 위젯을 추가할 수 있습니다.

팁 위젯을 추가한 후에는 탭의 원하는 위치로 이동할 수 있습니다. 그러나 탭 간에는 위젯을 이동할 수 없습니다. 자세한 내용은 55-42페이지의 위젯 정돈을/를 참조하십시오.

대시보드에 위젯을 추가하려면

액세스: Admin/Any Security Analyst/Maint

1단계 위젯을 추가하려는 대시보드를 표시합니다.

자세한 내용은 55-37페이지의 대시보드 보기을/를 참조하십시오.

2단계 위젯을 추가하려는 탭을 선택합니다.

3단계 **Add Widgets**를 클릭합니다.

Add Widgets 페이지가 나타납니다.

추가할 수 있는 위젯은 사용 중인 어플라이언스의 유형 및 사용자 역할에 따라 다릅니다. 위젯은 기능에 따라 분석 및 보고, 기타, 운영 카테고리로 구성됩니다. 카테고리 이름을 클릭하여 각 카테고리의 위젯을 볼 수 있습니다. 모든 위젯을 보려면 **All Categories**를 클릭합니다.

4단계 추가할 위젯 옆에 있는 **Add**를 클릭합니다.

팁 동일한 유형의 여러 위젯을 추가하려면(예: 여러 RSS Feed 위젯 또는 여러 Custom Analysis 위젯 추가) **Add**를 다시 클릭합니다.

위젯이 즉시 대시보드에 추가됩니다. Add Widgets 페이지에는 방금 추가한 위젯을 포함하여, 탭에 있는 각 유형의 위젯 수가 표시됩니다.

5단계 선택적으로, 위젯 추가를 완료했으면 **Done**을 클릭하여 대시보드로 돌아갑니다.

위젯을 추가한 탭이 다시 나타나며, 변경 사항이 반영됩니다.

위젯 정돈

라이센스: 모두

탭에서 위젯의 위치를 변경할 수 있습니다. 그러나 탭 간에 위젯을 이동할 수는 없습니다. 위젯을 다른 탭에 표시하려면 기존 탭에서 삭제한 후 새 탭에 추가해야 합니다.

위젯을 이동하려면

액세스: Admin/Any Security Analyst/Maint

1단계 이동할 위젯의 제목 표시줄을 클릭하고 새 위치로 끌어다 놓습니다.

위젯 최소화 및 최대화

라이센스: 모두

보기를 간소화하기 위해 위젯을 최소화한 다음, 다시 보고자 할 때 최대화할 수 있습니다.

위젯을 최소화하려면

액세스: Admin/Any Security Analyst/Maint

1단계 위젯의 제목 표시줄에서 최소화 아이콘(−)을 클릭합니다.

위젯을 최대화하려면

액세스: Admin/Any Security Analyst/Maint

1단계 최소화된 위젯의 제목 표시줄에서 최대화 아이콘(□)을 클릭합니다.

위젯 삭제

라이센스: 모두

탭에 더 이상 표시하지 않을 위젯은 삭제할 수 있습니다.

위젯을 삭제하려면

액세스: Admin/Any Security Analyst/Maint

1단계 위젯의 제목 표시줄에서 닫기 아이콘(✖)을 클릭합니다.

2단계 위젯을 삭제할 것임을 확인합니다.

탭에서 위젯이 삭제됩니다.

대시보드 삭제

라이센스: 모두

더 이상 사용하지 않는 대시보드는 삭제할 수 있습니다.

기본 대시보드를 삭제하는 경우 새로운 기본 대시보드를 정의해야 합니다. 그렇지 않으면 대시보드를 보려고 할 때마다 사용할 대시보드를 선택하라는 메시지가 표시됩니다. 자세한 내용은 71-8페이지의 기본 대시보드 지정을/를 참조하십시오.

대시보드를 삭제하려면

액세스: Admin/Any Security Analyst/Maint

1단계 **Overview > Dashboards > Management**를 선택합니다.

Dashboard Management 페이지가 나타납니다.

2단계 삭제할 대시보드 옆에 있는 삭제 아이콘( )을 클릭합니다.

3단계 대시보드를 삭제할 것임을 확인합니다.

대시보드가 삭제됩니다.

56장

Context Explorer 사용

FireSIGHT 시스템 Context Explorer에서는 애플리케이션에 대한 데이터, 애플리케이션 통계, 연결, 지오로케이션, IOC, 침입 이벤트, 호스트, 서버, 보안 인텔리전스, 사용자, 파일(악성코드 파일 포함), 관련 URL 등 모니터링 중인 네트워크의 상태에 대한 자세한 인터랙티브 그래픽 정보를 컨텍스트에 맞게 표시합니다. 각 섹션은 선명한 선, 막대, 파이, 도넛 그래프 형식과 자세한 목록으로 이 데이터를 표시합니다.

간편하게 사용자 지정 필터를 만들고 적용하여 정밀 분석을 수행할 수 있으며 그래프 영역을 클릭하거나 커서를 올려놓기만 하면 데이터 섹션을 자세히 확인할 수 있습니다. 또한 Explorer의 시간 범위를 마지막 시간 단위로 짧게, 또는 마지막 연도 단위로 길게 반영하도록 구성할 수도 있습니다. Administrator, Security Analyst 또는 Security Analyst(Read Only) 사용자 역할이 있는 사용자만 Context Explorer에 액세스할 수 있습니다.

FireSIGHT 시스템 대시보드는 세부적으로 맞춤화 및 구획화할 수 있으며 실시간으로 업데이트됩니다. 반면, Context Explorer는 수동으로 업데이트되고, 데이터에 대한 더 넓은 범위의 컨텍스트를 제공하도록 설계되었으며, 활성 사용자 탐색에 편리하도록 일관된 단일 레이아웃을 제공합니다.

특정 요구에 맞게 네트워크 및 어플라이언스에서 실시간 활동을 모니터링하려면 대시보드를 사용합니다. 반대로, 매우 세분화되고 분명한 컨텍스트에서 사전 정의된 최신 FireSIGHT 데이터 집합을 조사하려면 Context Explorer를 사용합니다. 예를 들어 네트워크의 호스트 중 15%만 Linux를 사용하지만 거의 모든 YouTube 트래픽을 일으키는 경우 Linux 호스트, YouTube 관련 애플리케이션 데이터, 또는 둘 모두를 보기 위한 필터를 신속하게 적용할 수 있습니다. 간결하고 매우 집중적인 대시보드 위젯과는 달리 Context Explorer 섹션은 시스템 활동을 FireSIGHT 시스템의 전문가는 물론 일반 사용자도 알기 쉬운 유용한 형식으로 시각적으로 표시하도록 설계되었습니다.

표시되는 데이터는 관리되는 디바이스의 라이센스 및 구축 방법, 데이터를 제공하는 기능의 구성 여부(Series 2 어플라이언스 및 Cisco NGIPS for Blue Coat X-Series의 경우), 데이터를 제공하는 기능을 어플라이언스가 지원하는지 여부 등의 요소에 따라 달라집니다. 예를 들면 DC500 방어 센터와 Series 2 디바이스 또는 Cisco NGIPS for Blue Coat X-Series 모두 AMP를 지원하지 않으므로 DC500 방어 센터는 이 데이터를 표시할 수 없고 Series 2 디바이스와 Cisco NGIPS for Blue Coat X-Series는 이 데이터를 탐지하지 못합니다.

다음 표에는 대시보드와 Context Explorer의 주요 차이점이 요약되어 있습니다.

표 56-1 비교: 대시보드 및 Context Explorer

기능	대시보드	Context Explorer
표시 가능한 데이터	FireSIGHT 시스템에서 모니터링하는 모든 것	애플리케이션, 애플리케이션 통계, 지오로케이션, IOC, 침입 이벤트, 파일(악성코드 파일 포함), 호스트, 보안 인텔리전스 이벤트, 서버, 사용자, URL
맞춤화 가능	• 대시보드형 위젯을 선택하여 맞춤화할 수 있음 • 개별 위젯을 다양하게 맞춤화할 수 있음	• 기본 레이아웃은 변경 불가 • 적용된 필터는 Explorer URL에 나타나며 나중에 사용하도록 북마크 처리 가능
데이터 업데이트 빈도	자동(기본값): 사용자가 구성함	수동
데이터 필터링	일부 위젯에 대해 가능(위젯 환경 설정을 수정해야 함)	Explorer의 모든 부분에 대해 가능하며 다중 필터 지원
그래픽 컨텍스트	일부 위젯(특히 Custom Analysis)은 데이터를 그래픽 형식으로 표시 가능	매우 자세한 도넛 그래프를 포함하여 폭넓은 그래픽 컨텍스트로 모든 데이터 표시 가능
관련 웹 인터페이스 페이지에 대한 링크	일부 위젯에서	모든 섹션에서
표시된 데이터의 시간 범위	사용자가 구성함	사용자가 구성함

관련 FireSIGHT 시스템 대시보드 대한 자세한 내용은 55-1페이지의 대시보드 사용을/를 참조하십시오.

Context Explorer 이해

라이센스: FireSIGHT

Context Explorer는 몇 개의 섹션으로 구성되어 있으며, 이러한 섹션이 결합되어 모니터링되는 네트워크에서 FireSIGHT 데이터의 전체적인 개요를 제공합니다. 첫 번째 섹션인 시간 경과에 따른 트래픽 및 이벤트 카운트의 선 그래프는 네트워크 활동의 최신 추세를 한눈에 볼 수 있는 그림을 제공합니다.

다른 섹션은 IOC, 네트워크, 애플리케이션, 보안 인텔리전스, 침입, 파일, 지오로케이션, URL 데이터에 대한 훨씬 자세한 정보를 제공하는 인터랙티브 그래프 및 목록 집합입니다. 트래픽 및 이벤트 시간 그래프 외의 모든 섹션을 보거나 숨길 수 있습니다. 또한 모든 섹션에 나타나는 데이터를 제한하려면 필터를 적용할 수 있습니다. 자세한 내용은 56-41페이지의 Context Explorer에서 필터 작업을/를 참조하십시오.

Context Explorer 섹션의 내용과 기능에 대한 자세한 내용은 다음 항목을 참조하십시오.

- 56-3페이지의 Traffic and Intrusion Event Counts Time 그래프 이해
- 56-4페이지의 Indications of Compromise 섹션 이해
- 56-6페이지의 Network Information 섹션 이해
- 56-13페이지의 Application Information 섹션 이해
- 56-17페이지의 Security Intelligence 섹션 이해
- 56-19페이지의 Intrusion Information 섹션 이해
- 56-25페이지의 Files Information 섹션 이해

- 56-31페이지의 Geolocation Information 섹션 이해
- 56-34페이지의 URL Information 섹션 이해

Context Explorer를 전체적으로 구성하는 방법에 대한 자세한 내용은 다음 항목을 참조하십시오.

- 56-38페이지의 Context Explorer 새로 고침
- 56-38페이지의 Context Explorer 시간 범위 설정
- 56-39페이지의 Context Explorer 섹션 최소화 및 최대화
- 56-39페이지의 Context Explorer 데이터에 대해 드릴다운

Context Explorer 필터의 구성 및 사용에 대한 자세한 내용은 다음 항목을 참조하십시오.

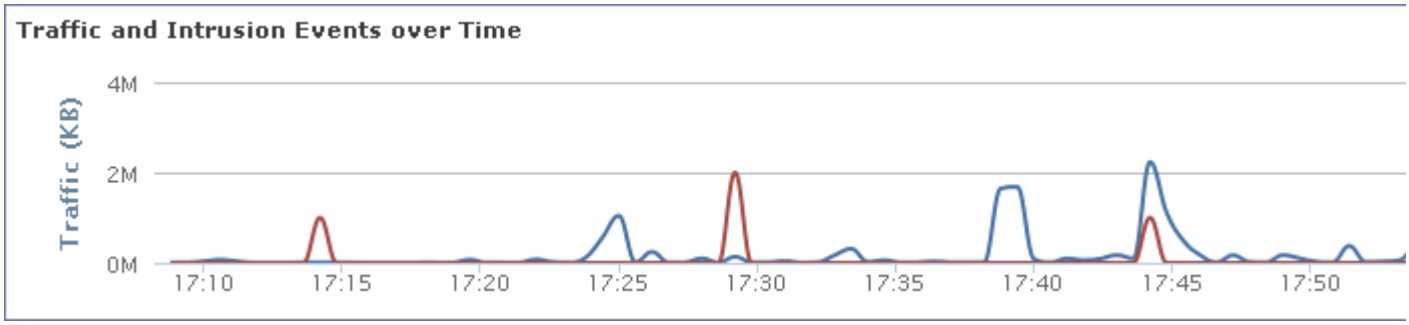
- 56-41페이지의 Context Explorer에서 필터 작업
- 56-41페이지의 필터 추가 및 적용
- 56-45페이지의 컨텍스트 메뉴로 필터 만들기
- 56-46페이지의 필터를 북마크 처리

Traffic and Intrusion Event Counts Time 그래프 이해

라이센스: FireSIGHT

Context Explorer의 상단에는 시간 경과에 따른 트래픽 및 침입 이벤트의 선 그래프가 있습니다. X축은 시간 간격을 나타냅니다(선택한 시간 창에 따라 5분에서 1개월까지). Y축은 킬로바이트 단위의 트래픽(파란색 선) 및 침입 이벤트 카운트(빨간색 선)를 나타냅니다.

X축의 최소 간격은 5분입니다. 이를 위해 시스템에서는 선택한 기간의 시작 지점과 종료 지점을 가장 가까운 5분 간격으로 반올림합니다.



기본적으로 이 섹션에는 선택한 기간의 모든 네트워크 트래픽 및 생성된 모든 침입 이벤트가 표시됩니다. 필터를 적용하면 필터에 지정된 기준과 관련이 있는 트래픽 및 침입 이벤트만 표시하도록 차트가 변경됩니다. 예를 들어 `Windows`의 **OS Name**으로 필터링하면 시간 그래프에는 Windows 운영 체제를 사용하는 호스트와 관련된 트래픽 및 이벤트만 표시됩니다.

침입 이벤트 데이터로 Context Explorer를 필터링하면(예: **Priority**가 `High`) 침입 이벤트에 더 집중할 수 있도록 파란색 트래픽 선이 숨겨집니다.

트래픽 및 이벤트 카운트에 대한 정확한 정보를 보려면 포인터를 그래프 선의 특정 지점에 올려놓을 수 있습니다. 색이 있는 선 중 하나로 포인터를 가져가면 해당 선이 그래프 앞으로 이동하므로 컨텍스트를 더 자세히 볼 수 있습니다.

이 섹션에서는 주로 Intrusion Events 및 Connection Events 테이블의 데이터를 보여줍니다.

Indications of Compromise 섹션 이해

라이센스: FireSIGHT

Context Explorer의 Indications of Compromise 섹션에는 모니터링되는 네트워크에서 감염 가능성이 있는 호스트를 전체적으로 보여주는 두 개의 인터랙티브 섹션이 있습니다. 이 둘은 각각 트리거된 가장 일반적인 IOC 유형의 비례 보기 및 트리거된 지표 수 기준의 호스트 보기입니다.

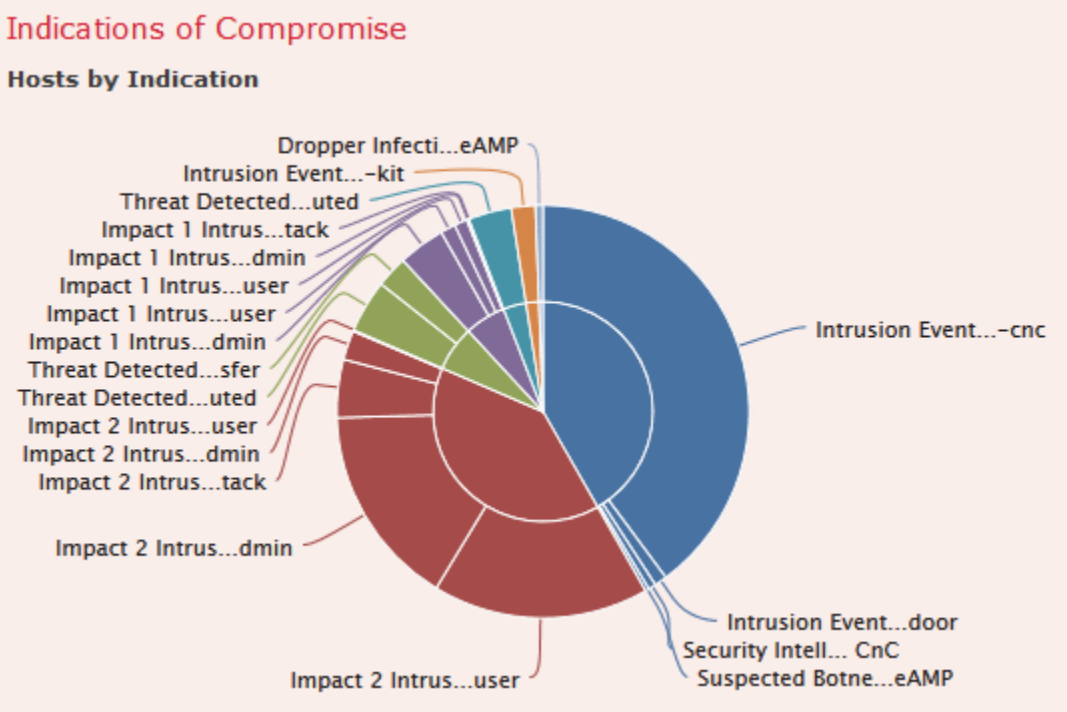
Indications of Compromise 섹션의 그래프에 대한 자세한 내용은 다음 항목을 참조하십시오.

- 56-5페이지의 Hosts by Indication 그래프 보기
- 56-5페이지의 Indications by Host 그래프 보기

Hosts by Indication 그래프 보기

라이센스: FireSIGHT

도넛 형식의 Hosts by Indication 그래프는 모니터링되는 네트워크에서 호스트별로 트리거된 IOC의 비례 보기를 제공합니다. 내부 원에는 IOC 카테고리(예: `CnC Connected` 또는 `Malware Detected`)로 구분된 내용이 표시되며, 외부 원에는 특정 이벤트 유형(예: `Impact 2 Intrusion Event – attempted-admin` 또는 `Threat Detected in File Transfer`)별로 그러한 데이터가 더 자세히 구분되어 표시됩니다.



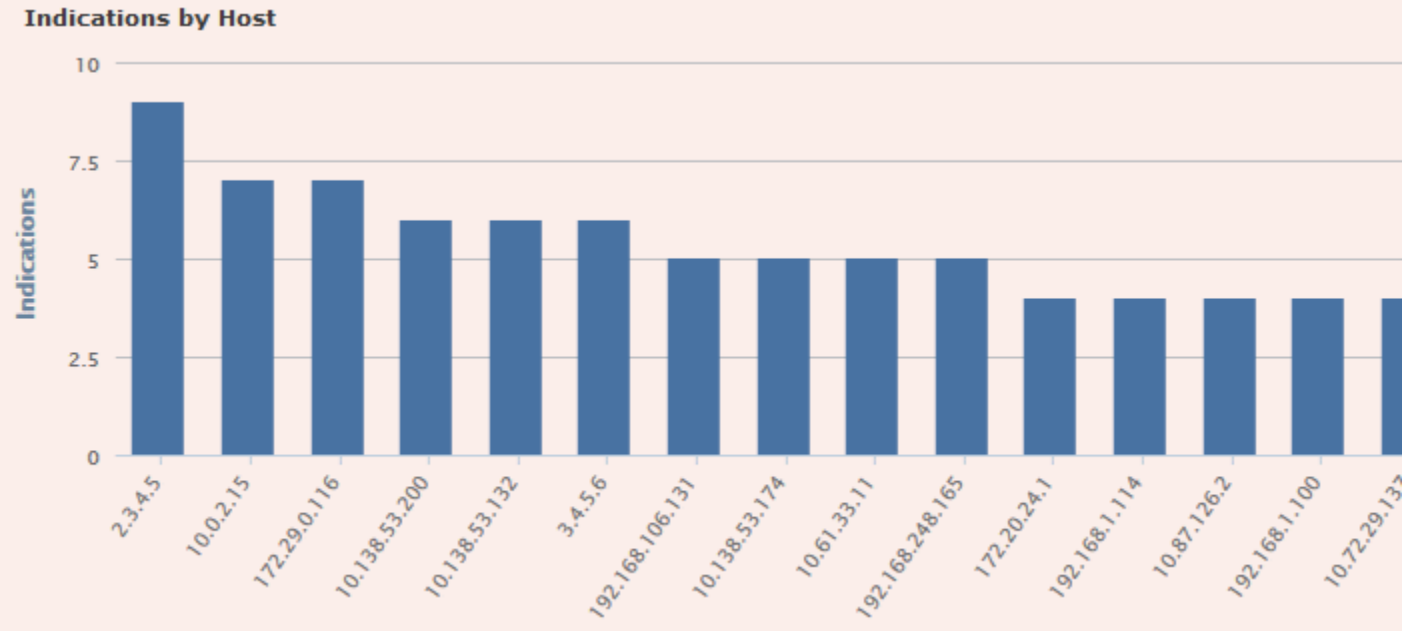
자세한 정보를 보려면 그래프의 원하는 부분으로 포인터를 이동하십시오. 그래프의 특정 부분을 클릭하면 해당 정보를 필터링하거나 드릴다운할 수 있습니다.

이 그래프에서는 Hosts 및 IOC 테이블의 데이터를 주로 보여줍니다.

Indications by Host 그래프 보기

라이센스: FireSIGHT

막대 형식의 Indications by Host 그래프는 모니터링되는 네트워크에서 IOC(Indications of Compromise)가 가장 높은 호스트 15개에 의해 트리거된 고유한 IOC의 카운트를 보여줍니다.



자세한 정보를 보려면 그래프의 원하는 부분으로 포인터를 이동하십시오. 그래프의 특정 부분을 클릭하면 해당 정보를 필터링하거나 드릴다운할 수 있습니다.

이 그래프에서는 Hosts 및 IOC 테이블의 데이터를 주로 보여줍니다.

Network Information 섹션 이해

라이센스: FireSIGHT

Context Explorer의 Network Information 섹션에는 소스, 목적지, 사용자, 트래픽과 관련된 보안 영역, 네트워크의 호스트에서 사용하는 운영 체제 구분, FireSIGHT 시스템이 네트워크에서 수행한 액세스 제어 작업의 비례 보기 등 모니터링되는 네트워크의 연결 트래픽을 전체적으로 표시하는 6개의 인터랙티브 그래프가 포함되어 있습니다.

Network Information 섹션의 그래프에 대한 자세한 내용은 다음 항목을 참조하십시오.

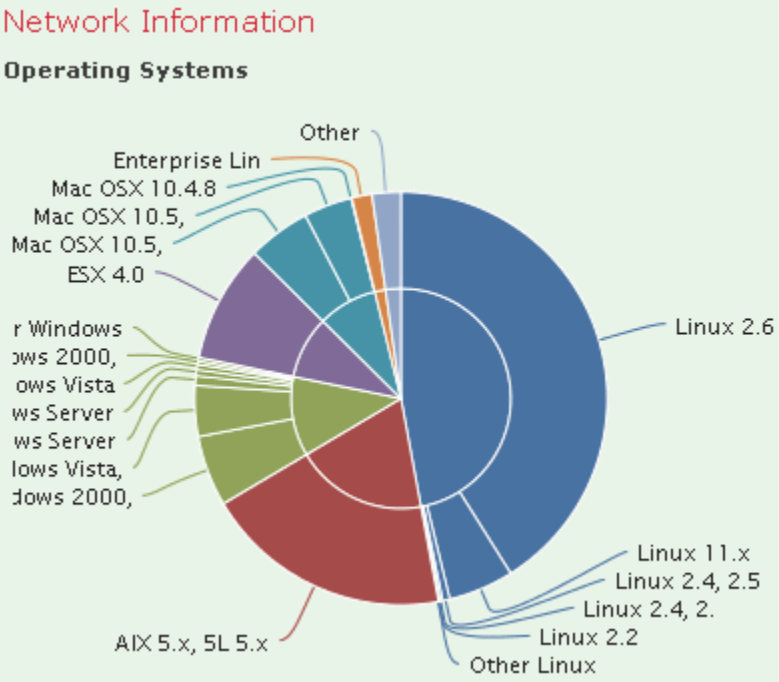
- 56-7페이지의 Operating Systems 그래프 보기
- 56-8페이지의 Traffic by Source IP 그래프 보기
- 56-9페이지의 Traffic by Source User 그래프 보기
- 56-10페이지의 Connections by Access Control Action 그래프 보기
- 56-11페이지의 Traffic by Destination IP 그래프 보기
- 56-12페이지의 Traffic by Ingress/Egress Security Zone 그래프 보기

Operating Systems 그래프 보기

라이센스: FireSIGHT

도넛 형식의 Operating Systems 그래프는 모니터링되는 네트워크의 호스트에서 탐지된 운영 체제의 비례 표시를 보여줍니다. 내부 원에는 OS 이름(예: `Windows` 또는 `Linux`)으로 구분된 내용이 표시되며, 외부 원에는 특정 운영 체제 버전(예: `Windows Server 2008` 또는 `Linux 11.x`)별 데이터가 더 자세히 구분되어 표시됩니다. 일부 긴밀하게 연결된 운영 체제(예: Windows 2000, Windows XP 및 Windows Server 2003)는 그룹화됩니다. 매우 드물거나 인식되지 않는 운영 체제는 **Other**로 그룹화됩니다.

이 그래프는 날짜 및 시간 제한 사항과 무관하게 모든 사용 가능한 데이터를 반영합니다. Explorer 시간 범위가 변경되어도 그래프는 변경되지 않습니다.



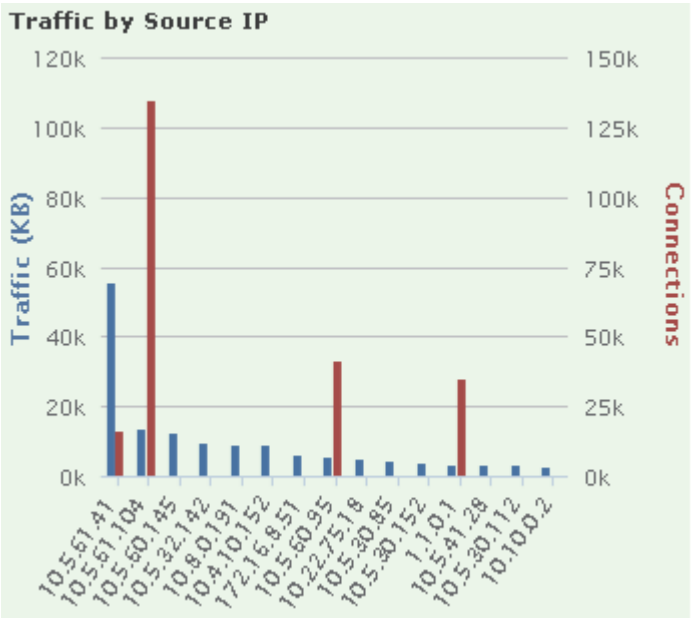
자세한 정보를 보려면 그래프의 원하는 부분으로 포인터를 이동하십시오. 그래프의 특정 부분을 클릭하면 해당 정보를 필터링하거나 드릴다운할 수 있습니다.

이 그래프에서는 Hosts 테이블의 데이터를 주로 보여줍니다.

Traffic by Source IP 그래프 보기

라이센스: FireSIGHT

막대 형식의 Traffic by Source IP 그래프는 모니터링되는 네트워크에서 가장 활발한 소스 IP 주소 15개에 대한 네트워크 트래픽(초당 킬로바이트 단위) 및 고유한 연결의 카운트를 보여줍니다. 나열된 각 소스 IP 주소에서 파란색 막대는 트래픽 데이터를, 빨간색 막대는 연결 데이터를 나타냅니다.



자세한 정보를 보려면 그래프의 원하는 부분으로 포인터를 이동하십시오. 그래프의 특정 부분을 클릭하면 해당 정보를 필터링하거나 드릴다운할 수 있습니다.

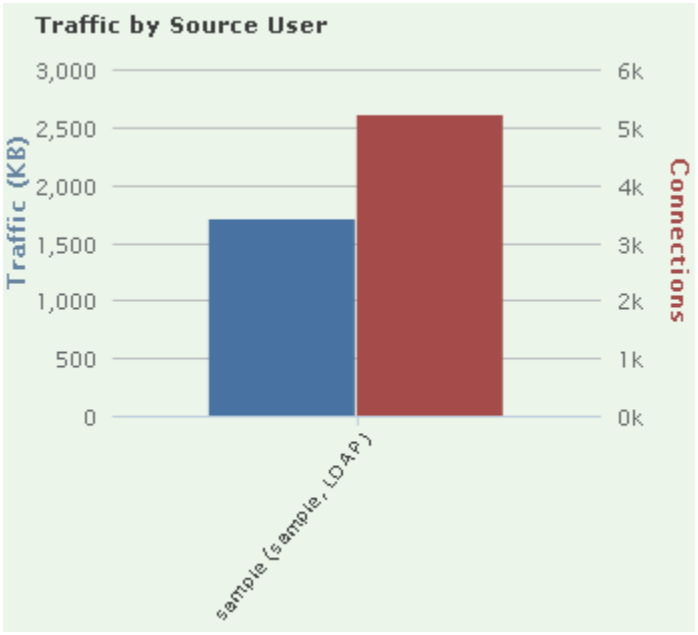
참고 침입 이벤트 정보에 대해 필터링하면 Traffic by Source IP 그래프는 숨겨집니다.

이 그래프에서는 Connection Events 테이블의 데이터를 주로 보여줍니다.

Traffic by Source User 그래프 보기

라이센스: FireSIGHT

막대 형식의 Traffic by Source User 그래프는 모니터링되는 네트워크에서 가장 활발한 소스 사용자 15명에 대한 네트워크 트래픽(초당 킬로바이트 단위) 및 고유한 연결의 카운트를 보여줍니다. 나열된 각 소스 IP 주소에서 파란색 막대는 트래픽 데이터를, 빨간색 막대는 연결 데이터를 나타냅니다.



자세한 정보를 보려면 그래프의 원하는 부분으로 포인터를 이동하십시오. 그래프의 특정 부분을 클릭하면 해당 정보를 필터링하거나 드릴다운할 수 있습니다.

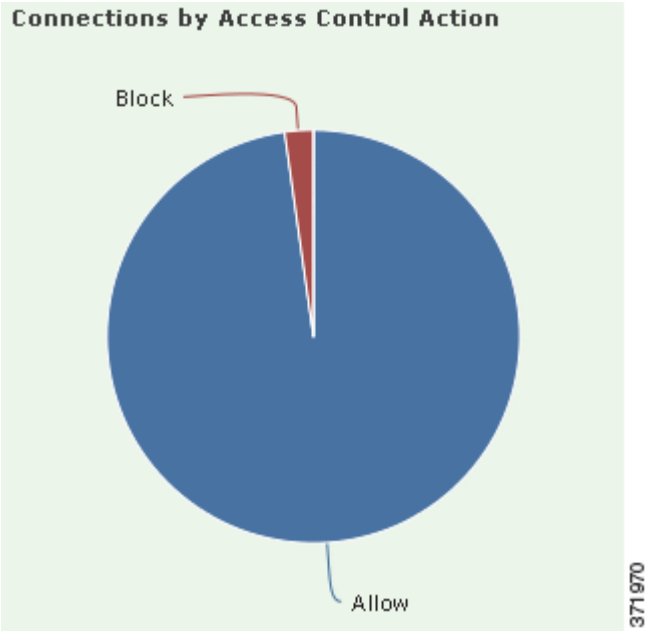
참고 침입 이벤트 정보에 대해 필터링하면 Traffic by Source User 그래프는 숨겨집니다.

이 그래프에서는 Connection Events 테이블의 데이터를 주로 보여줍니다. 여기에는 사용자 에이전트에서 보고한 사용자만 표시됩니다.

Connections by Access Control Action 그래프 보기

라이센스: FireSIGHT

원 형식의 Connections by Access Control Action 그래프는 FireSIGHT 시스템이 모니터링되는 트래픽에서 수행한 액세스 제어 작업(예: `Block` 또는 `Allow`)의 비례 보기를 제공합니다.



자세한 정보를 보려면 그래프의 원하는 부분으로 포인터를 이동하십시오. 그래프의 특정 부분을 클릭하면 해당 정보를 필터링하거나 드릴다운할 수 있습니다.

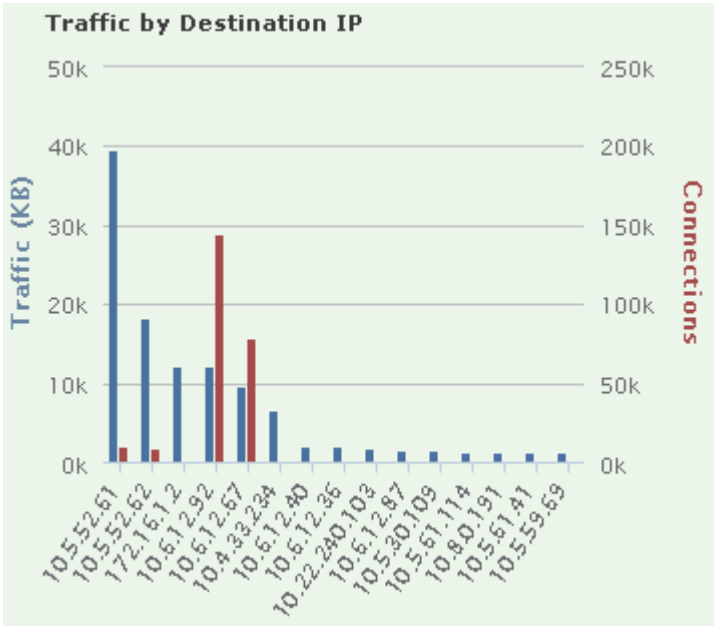
참고 침입 이벤트 정보에 대해 필터링하면 Traffic by Source User 그래프는 숨겨집니다.

이 그래프에서는 Connection Events 테이블의 데이터를 주로 보여줍니다.

Traffic by Destination IP 그래프 보기

라이센스: FireSIGHT

막대 형식의 Traffic by Destination IP 그래프는 모니터링되는 네트워크에서 가장 활발한 목적지 IP 주소 15개에 대한 네트워크 트래픽(초당 킬로바이트 단위) 및 고유한 연결의 카운트를 보여줍니다. 나열된 각 목적지 IP 주소에서 파란색 막대는 트래픽 데이터를, 빨간색 막대는 연결 데이터를 나타냅니다.



자세한 정보를 보려면 그래프의 원하는 부분으로 포인터를 이동하십시오. 그래프의 특정 부분을 클릭하면 해당 정보를 필터링하거나 드릴다운할 수 있습니다.

참고 침입 이벤트 정보에 대해 필터링하면 Traffic by Destination IP 그래프는 숨겨집니다.

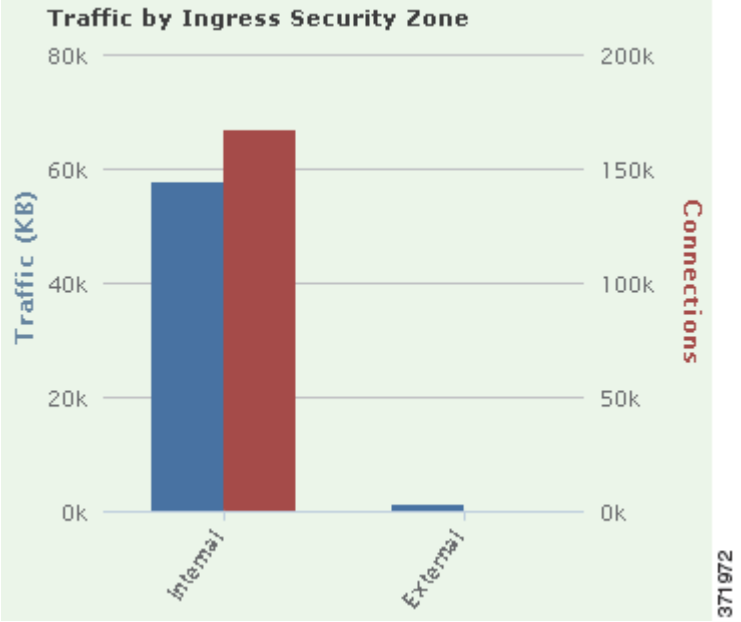
이 그래프에서는 Connection Events 테이블의 데이터를 주로 보여줍니다.

Traffic by Ingress/Egress Security Zone 그래프 보기

라이센스: FireSIGHT

막대 형식의 Traffic by Ingress/Egress Security Zone 그래프는 모니터링되는 네트워크에 구성된 각 보안 영역에 대한 들어오는 또는 나가는 네트워크 트래픽(초당 킬로바이트 단위) 및 고유한 연결의 카운트를 보여줍니다. 필요에 따라 Ingress(기본값) 또는 Egress 보안 영역 정보를 표시하도록 이 그래프를 구성할 수 있습니다.

나열된 각 보안 영역에서 파란색 막대는 트래픽 데이터를, 빨간색 막대는 연결 데이터를 나타냅니다. 보안 영역에 대한 자세한 내용은 3-38페이지의 보안 영역 작업을/를 참조하십시오.



자세한 정보를 보려면 그래프의 원하는 부분으로 포인터를 이동하십시오. 그래프의 특정 부분을 클릭하면 해당 정보를 필터링하거나 드릴다운할 수 있습니다.

팁 이그레스 보안 영역 단위 트래픽만 표시하도록 그래프를 제한하려면 포인터를 그래프 위로 이동하고 표시되는 토글 버튼에서 **Egress**를 클릭합니다. 기본 보기로 돌아가려면 **Ingress**를 클릭합니다. Context Explorer에서 빠져나가도 기본 Ingress 보기로 돌아갑니다.

참고 침입 이벤트 정보에 대해 필터링하면 Traffic by Ingress/Egress Security Zone 그래프는 숨겨집니다.

이 그래프에서는 Connection Events 테이블의 데이터를 주로 보여줍니다.

Application Information 섹션 이해

라이센스: FireSIGHT

Context Explorer의 Application Information 섹션에는 모니터링되는 네트워크에서 전반적인 애플리케이션 활동 내용을 보여주는 인터랙티브 그래프 3개 및 테이블 형식의 목록 1개가 있습니다. 트래픽, 침입 이벤트, 애플리케이션과 관련된 호스트 등은 각 애플리케이션에 할당된 비즈니스 연관성 또는 추정 위험 단위로 더 세부적으로 구성됩니다. Application Details List는 위험, 비즈니스 연관성, 카테고리 및 호스트 카운트의 인터랙티브 목록을 제공합니다.

이 섹션의 모든 "애플리케이션" 인스턴스에서 기본적으로 애플리케이션 정보 그래프 집합은 특별히 애플리케이션 프로토콜(예: DNS 또는 SSH)을 검사합니다. 특별히 클라이언트 애플리케이션(예: PuTTY 또는 Firefox) 또는 웹 애플리케이션(예: Facebook 또는 Pandora)을 검사하도록 Application Information 섹션을 구성할 수도 있습니다.

Application Information 섹션의 그래프 및 목록에 대한 자세한 내용은 다음 항목을 참조하십시오.

- 56-13페이지의 Traffic by Risk/Business Relevance and Application 그래프 보기
- 56-14페이지의 Intrusion Events by Risk/Business Relevance and Application 그래프 보기
- 56-15페이지의 Hosts by Risk/Business Relevance and Application 그래프 보기
- 56-16페이지의 Application Details List 보기

Application Information 섹션을 구성하려면 다음에 집중하십시오.

액세스: Admin/Any Security Analyst

1단계 **Analysis > Context Explorer**를 선택합니다.

Context Explorer가 나타납니다.

2단계 **Application Protocol Information** 섹션으로 포인터를 이동합니다. (동일한 Context Explorer 세션에서 전에 이 설정을 변경한 경우에는 섹션 제목이 **Client Application Information** 또는 **Web Application Information**으로 표시될 수 있습니다.)

오른쪽 위에 섹션 옵션 버튼이 나타납니다.

3단계 **Application Protocol**, **Client Application** 또는 **Web Application**을 클릭합니다.

사용자가 선택한 옵션에 따라 Application Information 섹션이 새로 고쳐집니다.

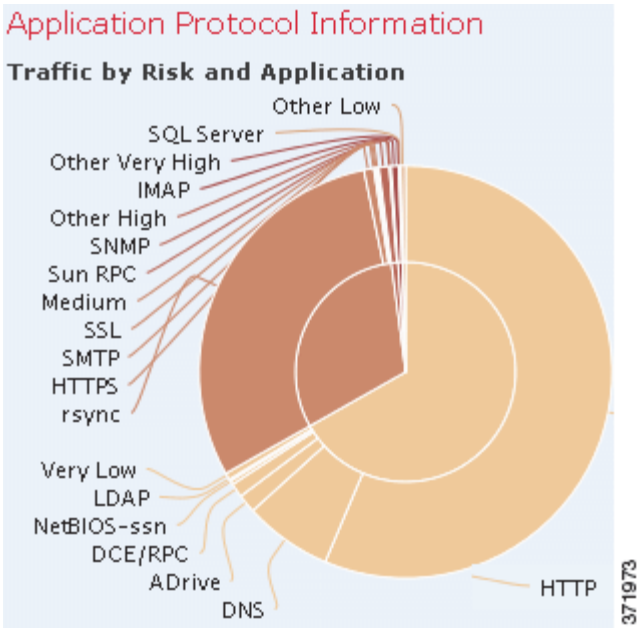
참고 Context Explorer에서 빠져나가면 이 섹션이 기본 상태(Application Protocol)로 돌아갑니다.

Traffic by Risk/Business Relevance and Application 그래프 보기

라이센스: FireSIGHT

도넛 형식의 Traffic by Risk/Business Relevance and Application 그래프는 모니터링되는 네트워크에서 탐지되는 애플리케이션 트래픽의 비례 표시를 애플리케이션의 예상 위험(기본값) 또는 예상 비즈니스 연관성 기준으로 정렬하여 보여줍니다. 내부 원에는 예상 위험/비즈니스 연관성 레벨(예: `Medium` 또는 `High`)로 구분된 내용이 표시되며, 외부 원에는 특정 애플리케이션(예: `SSH` 또는 `NetBIOS`)별 데이터가 더 자세히 구분되어 표시됩니다. 거의 검색되지 않는 애플리케이션은 **Other**로 그룹화됩니다.

이 그래프는 날짜 및 시간 제한 사항과 무관하게 모든 사용 가능한 데이터를 반영합니다. Explorer 시간 범위가 변경되어도 그래프는 변경되지 않습니다.



자세한 정보를 보려면 그래프의 원하는 부분으로 포인터를 이동하십시오. 그래프의 특정 부분을 클릭하면 해당 정보를 필터링하거나 드릴다운할 수 있습니다.

팁 비즈니스 연관성 및 애플리케이션 단위 트래픽만 표시하도록 그래프를 제한하려면 포인터를 그래프 위로 이동하고 표시되는 토글 버튼에서 **Business Relevance**를 클릭합니다. 기본 보기로 돌아가려면 **Risk**를 클릭합니다. Context Explorer에서 빠져나가도 기본 Risk 보기로 돌아갑니다.

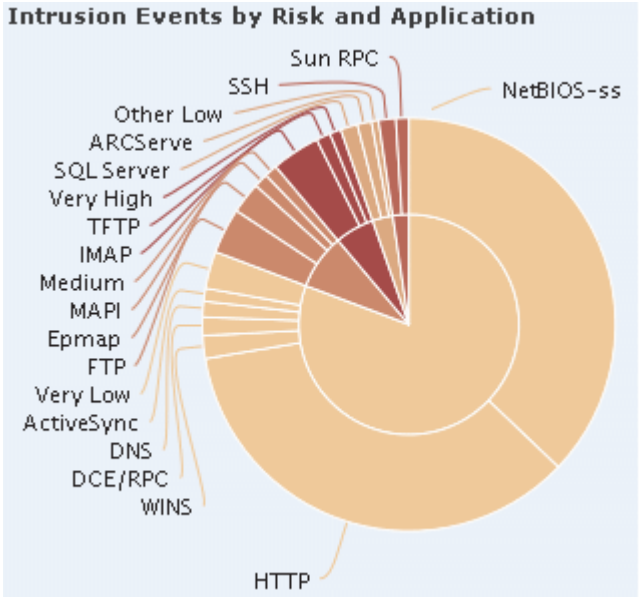
참고 침입 이벤트 정보에 대해 필터링하면 Traffic by Risk/Business Relevance and Application 그래프는 숨겨집니다.

이 그래프에서는 Connection Events 및 Application Statistics 테이블의 데이터를 주로 보여줍니다.

Intrusion Events by Risk/Business Relevance and Application 그래프 보기

라이센스: FireSIGHT

도넛 형식의 Intrusion Events by Risk/Business Relevance and Application 그래프는 모니터링되는 네트워크 및 애플리케이션에서 탐지되는 침입 이벤트의 비례 표시를 애플리케이션의 예상 위험(기본값) 또는 예상 비즈니스 연관성 기준으로 정렬하여 보여줍니다. 내부 원에는 예상 위험/비즈니스 연관성 레벨(예: `Medium` 또는 `High`)로 구분된 내용이 표시되며, 외부 원에는 특정 애플리케이션(예: `SSH` 또는 `NetBIOS`)별 데이터가 더 자세히 구분되어 표시됩니다. 거의 검색되지 않는 애플리케이션은 **Other**로 그룹화됩니다.



자세한 정보를 보려면 도넛 그래프의 원하는 부분으로 포인터를 이동하십시오. 그래프의 특정 부분을 클릭하면 해당 정보를 필터링하거나 드릴다운할 수 있습니다. 또는 해당되는 경우 애플리케이션 정보를 볼 수 있습니다.

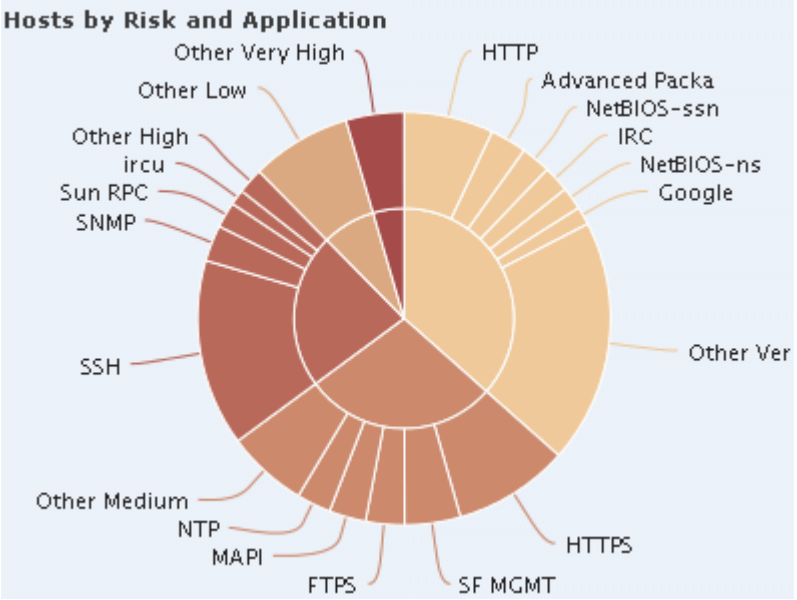
팁 비즈니스 연관성 및 애플리케이션 단위 침입 이벤트만 표시하도록 그래프를 제한하려면 포인터를 그래프 위로 이동하고 표시되는 토글 버튼에서 **Business Relevance**를 클릭합니다. 기본 보기로 돌아가려면 **Risk**를 클릭합니다. Context Explorer에서 빠져나가도 기본 Risk 보기로 돌아갑니다.

이 그래프에서는 Intrusion Events 및 Application Statistics 테이블의 데이터를 주로 보여줍니다.

Hosts by Risk/Business Relevance and Application 그래프 보기

라이센스: FireSIGHT

도넛 형식의 Hosts by Risk/Business Relevance and Application 그래프는 모니터링되는 네트워크 및 애플리케이션에서 탐지되는 호스트의 비례 표시를 애플리케이션의 예상 위험(기본값) 또는 예상 비즈니스 연관성 기준으로 정렬하여 보여줍니다. 내부 원에는 예상 위험/비즈니스 연관성 레벨(예: `Medium` 또는 `High`)로 구분된 내용이 표시되며, 외부 원에는 특정 애플리케이션(예: `SSH` 또는 `NetBIOS`)별 데이터가 더 자세히 구분되어 표시됩니다. 거의 검색되지 않는 애플리케이션은 **Other**로 그룹화됩니다.



자세한 정보를 보려면 도넛 그래프의 원하는 부분으로 포인터를 이동하십시오. 그래프의 특정 부분을 클릭하면 해당 정보를 필터링하거나 드릴다운할 수 있습니다.

팁 비즈니스 연관성 및 애플리케이션 단위 호스트만 표시하도록 그래프를 제한하려면 포인터를 그래프 위로 이동하고 표시되는 토글 버튼에서 **Business Relevance**를 클릭합니다. 기본 보기로 돌아가려면 **Risk**를 클릭합니다. Context Explorer에서 빠져나가도 기본 Risk 보기로 돌아갑니다.

이 그래프에서는 Applications 테이블의 데이터를 주로 보여줍니다.

Application Details List 보기

라이센스: FireSIGHT

Application Information 섹션 아래쪽에는 Application Details List가 있습니다. 이 목록은 모니터링되는 네트워크에서 탐지되는 각 애플리케이션에 대한 예상 위험, 예상 비즈니스 연관성, 카테고리 및 호스트 카운트 정보를 제공하는 테이블입니다. 애플리케이션은 관련 호스트 카운트의 내림차순으로 나열됩니다.

Application Details List 테이블은 정렬할 수 없지만, 원하는 테이블 항목을 클릭하면 해당 정보로 필터링 또는 드릴다운할 수 있습니다. 또는 해당되는 경우 애플리케이션 정보를 볼 수 있습니다. 이 테이블에서는 Applications 테이블의 데이터를 주로 보여줍니다.

이 목록은 날짜 및 시간 제한 사항과 무관하게 모든 사용 가능한 데이터를 반영합니다. Explorer 시간 범위가 변경되어도 목록은 변경되지 않습니다.

Security Intelligence 섹션 이해

라이센스: 보호

지원되는 디바이스: Series 2를 제외한 모두

지원되는 Defense Center: DC500을 제외한 모두

Context Explorer의 Security Intelligence 섹션에는 보안 인텔리전스에서 모니터링하거나 블랙리스트에 오른 모니터링되는 네트워크의 트래픽을 전체적으로 보여주는 세 개의 인터랙티브 막대 그래프가 있습니다. 그래프에서 그러한 트래픽은 카테고리, 소스 IP 주소, 목적지 IP 주소로 각각 정렬됩니다. 트래픽의 양(초당 킬로바이트 단위) 및 해당 연결 수가 모두 나타납니다.

Security Intelligence 섹션의 그래프에 대한 자세한 내용은 다음 항목을 참조하십시오.

- 56-17페이지의 Security Intelligence Traffic by Category 그래프 보기
- 56-18페이지의 Security Intelligence Traffic by Source IP 그래프 보기
- 56-19페이지의 Security Intelligence Traffic by Destination IP 그래프 보기

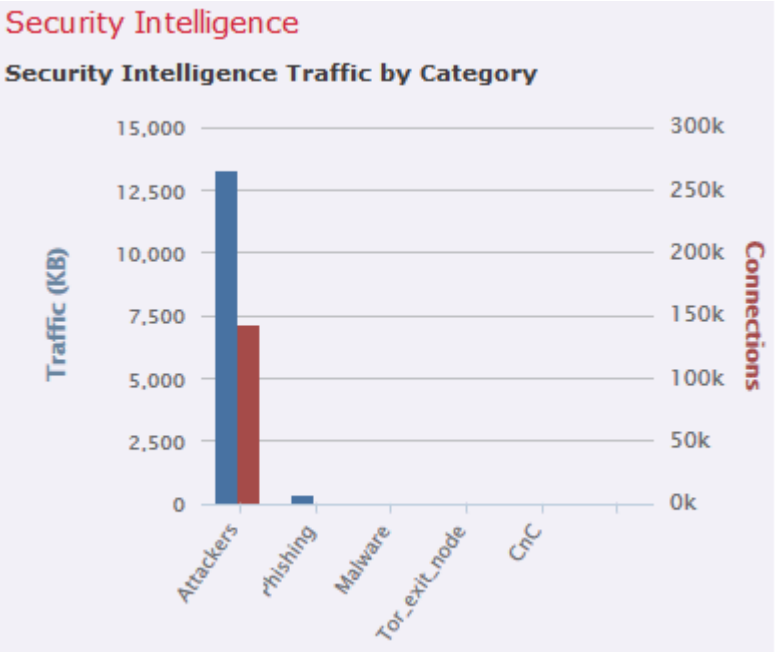
Security Intelligence Traffic by Category 그래프 보기

라이센스: 보호

지원되는 디바이스: Series 2를 제외한 모두

지원되는 Defense Center: DC500을 제외한 모두

막대 형식의 Security Intelligence Traffic by Category 그래프는 모니터링되는 네트워크에서 상위 보안 인텔리전스 카테고리에 대한 네트워크 트래픽(초당 킬로바이트 단위) 및 고유한 연결의 카운트를 보여줍니다. 나열된 각 카테고리에서 파란색 막대는 트래픽 데이터를, 빨간색 막대는 연결 데이터를 나타냅니다.



자세한 정보를 보려면 그래프의 원하는 부분으로 포인터를 이동하십시오. 그래프의 특정 부분을 클릭하면 해당 정보로 드릴다운할 수 있습니다.

참고 침입 이벤트 정보에 대해 필터링하면 Security Intelligence Traffic by Category 그래프는 숨겨집니다.

이 그래프에서는 Security Intelligence Events 테이블의 데이터를 주로 보여줍니다.

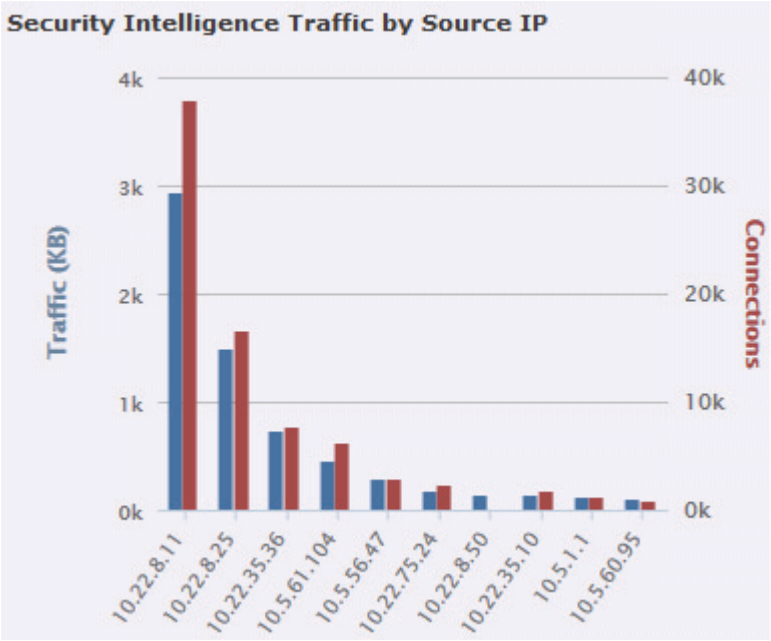
Security Intelligence Traffic by Source IP 그래프 보기

라이센스: 보호

지원되는 디바이스: Series 2를 제외한 모두

지원되는 Defense Center: DC500을 제외한 모두

막대 형식의 Security Intelligence Traffic by Source IP 그래프는 모니터링되는 네트워크에서 보안 인텔리전스로 모니터링하는 트래픽의 상위 소스 IP 주소에 대한 네트워크 트래픽(초당 킬로바이트 단위) 및 고유한 연결의 카운트를 보여줍니다. 나열된 각 카테고리에서 파란색 막대는 트래픽 데이터를, 빨간색 막대는 연결 데이터를 나타냅니다.



자세한 정보를 보려면 그래프의 원하는 부분으로 포인터를 이동하십시오. 그래프의 특정 부분을 클릭하면 해당 정보로 드릴다운할 수 있습니다.

참고 침입 이벤트 정보에 대해 필터링하면 Security Intelligence Traffic by Source IP 그래프는 숨겨집니다.

이 그래프에서는 Security Intelligence Events 테이블의 데이터를 주로 보여줍니다.

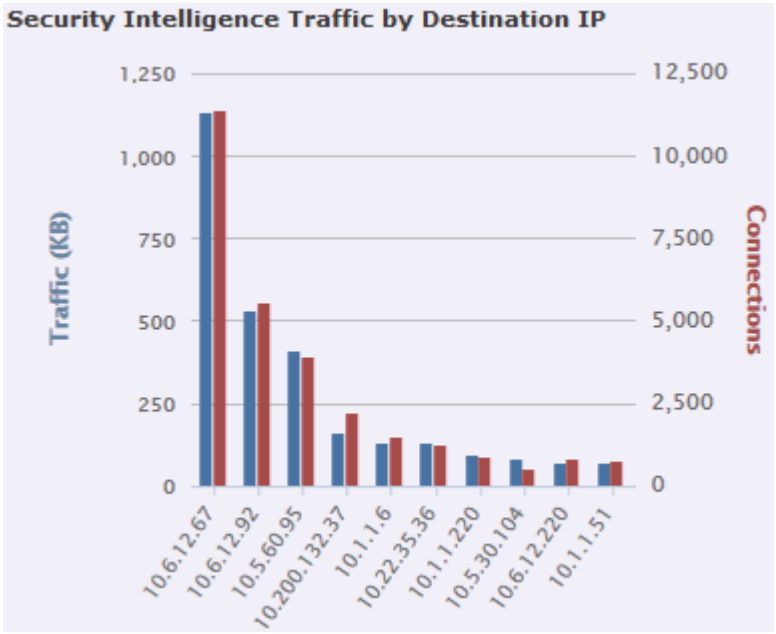
Security Intelligence Traffic by Destination IP 그래프 보기

라이센스: 보호

지원되는 디바이스: Series 2를 제외한 모두

지원되는 Defense Center: DC500을 제외한 모두

막대 형식의 Security Intelligence Traffic by Destination IP 그래프는 모니터링되는 네트워크에서 보안 인텔리전스로 모니터링하는 트래픽의 상위 목적지 IP 주소에 대한 네트워크 트래픽(초당 킬로바이트 단위) 및 고유한 연결의 카운트를 보여줍니다. 나열된 각 카테고리에서 파란색 막대는 트래픽 데이터를, 빨간색 막대는 연결 데이터를 나타냅니다.



자세한 정보를 보려면 그래프의 원하는 부분으로 포인터를 이동하십시오. 그래프의 특정 부분을 클릭하면 해당 정보로 드릴다운할 수 있습니다.

참고 침입 이벤트 정보에 대해 필터링하면 Security Intelligence Traffic by Destination IP 그래프는 숨겨집니다.

이 그래프에서는 Security Intelligence Events 테이블의 데이터를 주로 보여줍니다.

Intrusion Information 섹션 이해

라이센스: 보호

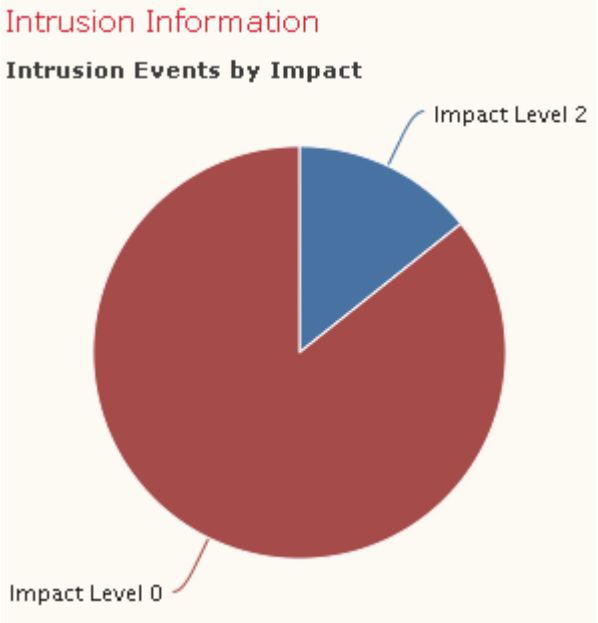
Context Explorer의 Intrusion Information 섹션에는 모니터링되는 네트워크의 침입 이벤트를 전체적으로 보여주는 인터랙티브 그래프 6개 및 테이블 형식의 목록 1개가 있습니다. 여기에는 영향 레벨, 공격 소스, 대상 목적지, 사용자, 우선순위 레벨, 침입 이벤트와 관련된 보안 영역과 더불어 침입 이벤트 분류, 우선순위 및 카운트의 자세한 목록이 포함됩니다.

Network Information 섹션의 그래프 및 목록에 대한 자세한 내용은 다음 항목을 참조하십시오.

Intrusion Events by Impact 그래프 보기

라이센스: 보호

원 형식의 Intrusion Events by Impact 그래프는 모니터링되는 네트워크에서 침입 이벤트의 비례 보기를 예상 영향 레벨(0~4)로 그룹화하여 제공합니다.



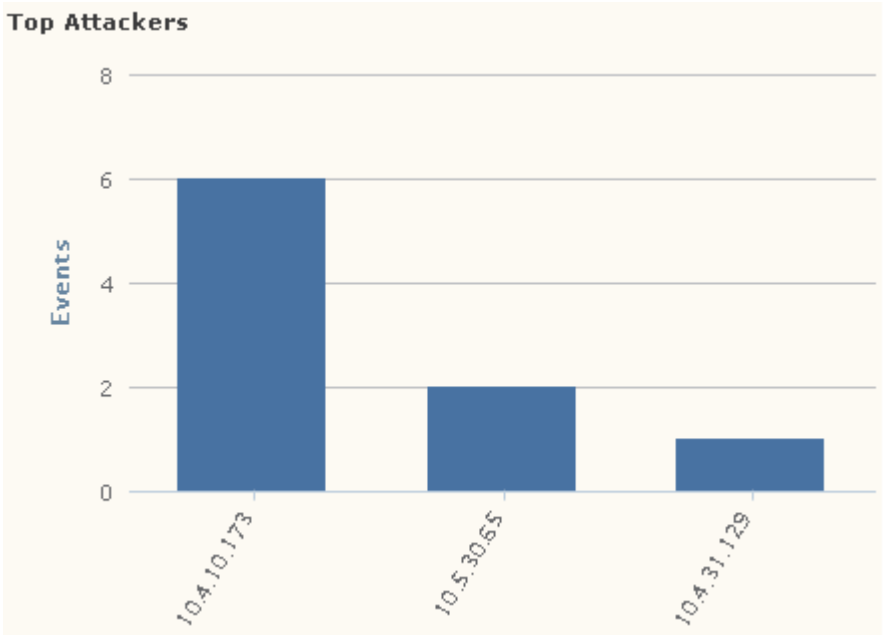
자세한 정보를 보려면 그래프의 원하는 부분으로 포인터를 이동하십시오. 그래프의 특정 부분을 클릭하면 해당 정보를 필터링하거나 드릴다운할 수 있습니다.

이 그래프에서는 IDS Statistics 및 Intrusion Events 테이블의 데이터를 주로 보여줍니다.

Top Attackers 그래프 보기

라이센스: 보호

막대 형식의 Top Attackers 그래프는 모니터링되는 네트워크에서 상위 공격 호스트 IP 주소(이벤트를 일으키는)에 대한 침입 이벤트의 카운트를 보여줍니다.



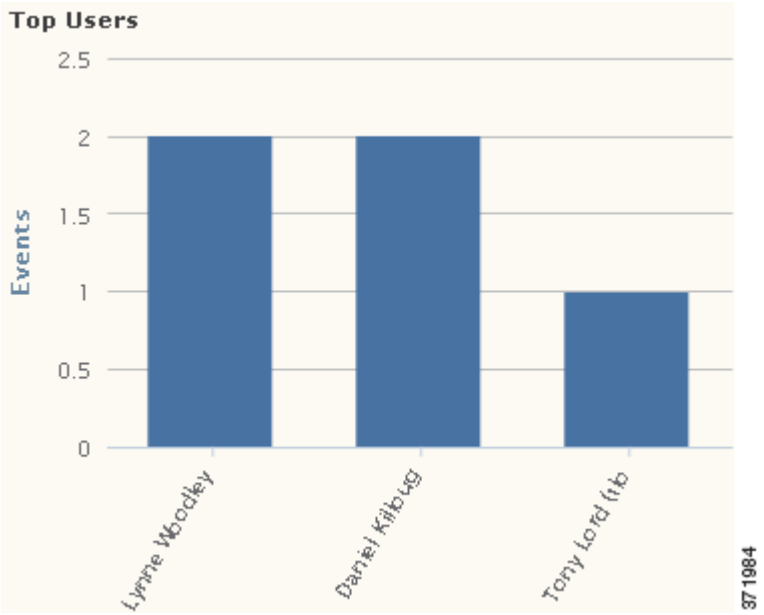
자세한 정보를 보려면 그래프의 원하는 부분으로 포인터를 이동하십시오. 그래프의 특정 부분을 클릭하면 해당 정보를 필터링하거나 드릴다운할 수 있습니다.

이 그래프에서는 Intrusion Events 테이블의 데이터를 주로 보여줍니다.

Top Users 그래프 보기

라이센스: 보호

막대 형식의 Top Users 그래프는 최고 침입 이벤트 카운트와 관련된 모니터링되는 네트워크의 사용자를 이벤트 카운트 단위로 보여줍니다.



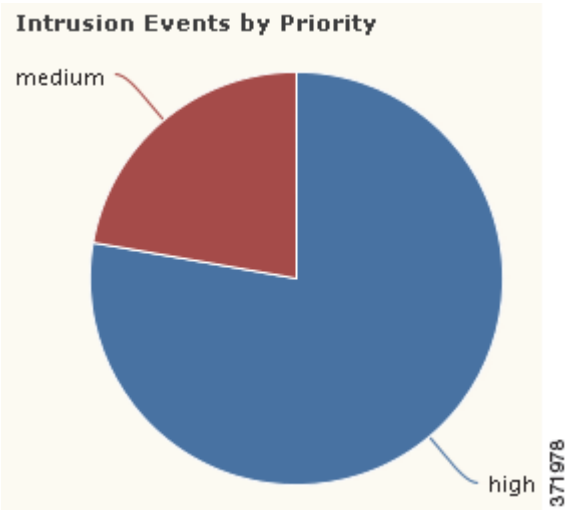
자세한 정보를 보려면 그래프의 원하는 부분으로 포인터를 이동하십시오. 그래프의 특정 부분을 클릭하면 해당 정보를 필터링하거나 드릴다운할 수 있습니다.

이 그래프에서는 IDS User Statistics 및 Intrusion Events 테이블의 데이터를 주로 보여줍니다. 여기에는 사용자 에이전트에서 보고한 사용자만 표시됩니다.

Intrusion Events by Priority 그래프 보기

라이센스: 보호

원 형식의 Intrusion Events by Priority 그래프는 모니터링되는 네트워크에서 침입 이벤트의 비례 보기를 예상 우선순위 레벨(예: `High`, `Medium` 또는 `Low`)로 그룹화하여 제공합니다.



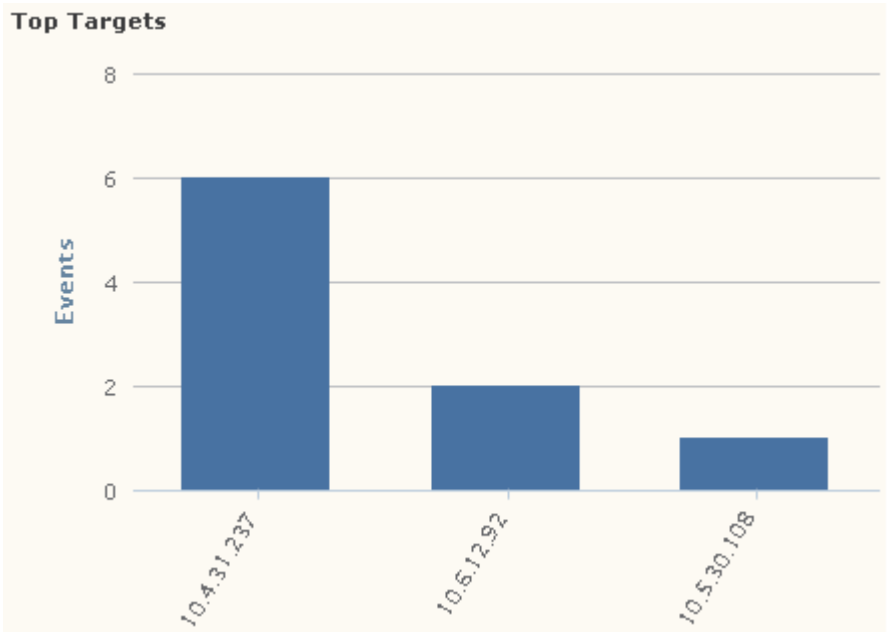
자세한 정보를 보려면 그래프의 원하는 부분으로 포인터를 이동하십시오. 그래프의 특정 부분을 클릭하면 해당 정보를 필터링하거나 드릴다운할 수 있습니다.

이 그래프에서는 Intrusion Events 테이블의 데이터를 주로 보여줍니다.

Top Targets 그래프 보기

라이센스: 보호

막대 형식의 Top Targets 그래프는 모니터링되는 네트워크에서 상위 대상 호스트 IP 주소(이벤트를 일으키는 연결의 대상)에 대한 침입 이벤트의 카운트를 보여줍니다.



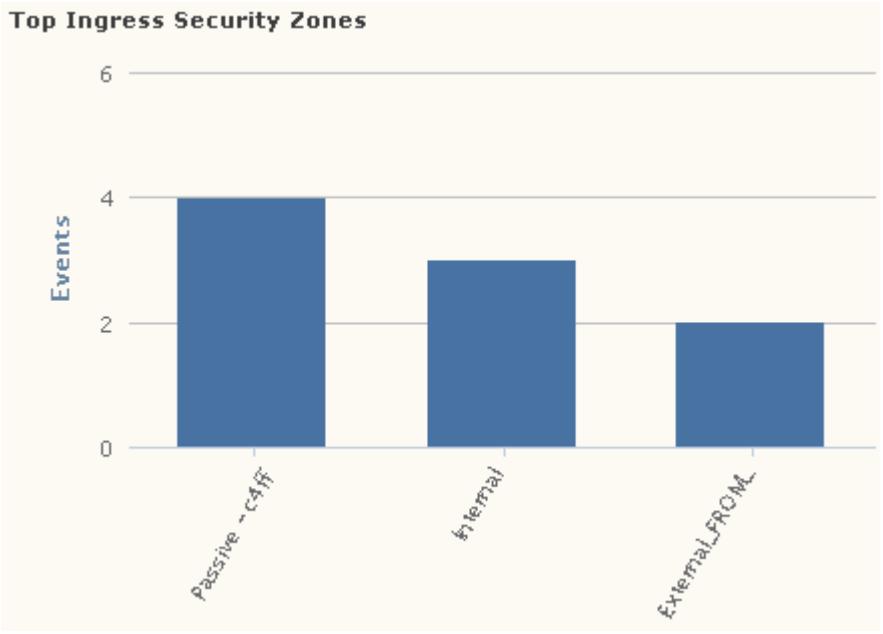
자세한 정보를 보려면 그래프의 원하는 부분으로 포인터를 이동하십시오. 그래프의 특정 부분을 클릭하면 해당 정보를 필터링하거나 드릴다운할 수 있습니다.

이 그래프에서는 Intrusion Events 테이블의 데이터를 주로 보여줍니다.

Top Ingress/Egress Security Zones 그래프 보기

라이센스: 보호

막대 형식의 Top Ingress/Egress Security Zones 그래프는 모니터링되는 네트워크에 구성된 각 보안 영역(그래프 설정에 따라 Ingress 또는 Egress)과 관련된 침입 이벤트의 카운트를 보여줍니다. 보안 영역에 대한 자세한 내용은 3-38페이지의 보안 영역 작업을/를 참조하십시오.



자세한 정보를 보려면 그래프의 원하는 부분으로 포인터를 이동하십시오. 그래프의 특정 부분을 클릭하면 해당 정보를 필터링하거나 드릴다운할 수 있습니다.

팁 이그레스 보안 영역 단위 트래픽만 표시하도록 그래프를 제한하려면 포인터를 그래프 위로 이동하고 표시되는 토글 버튼에서 **Egress**를 클릭합니다. 기본 보기로 돌아가려면 **Ingress**를 클릭합니다. Context Explorer에서 빠져나가도 기본 Ingress 보기로 돌아갑니다.

이 그래프에서는 Intrusion Events 테이블의 데이터를 주로 보여줍니다.

필요에 따라 Ingress(기본값) 또는 Egress 보안 영역 정보를 표시하도록 이 그래프를 구성할 수 있습니다.

침입 이벤트 세부사항 목록 보기

라이센스: 보호

Intrusion Information 섹션 아래쪽에는 침입 이벤트 세부사항 목록이 있습니다. 이 목록은 모니터링되는 네트워크에서 탐지되는 각 침입 이벤트에 대한 분류, 예상 우선순위 및 이벤트 카운트 정보를 제공하는 테이블입니다. 이벤트는 이벤트 카운트의 내림차순으로 나열됩니다.

침입 이벤트 세부사항 목록 테이블은 정렬할 수 없지만, 원하는 테이블 항목을 클릭하면 해당 정보로 필터링 또는 드릴다운할 수 있습니다. 이 테이블에서는 Intrusion Events 테이블의 데이터를 주로 보여줍니다.

Files Information 섹션 이해

라이센스: 보호 또는 악성코드

지원되는 디바이스: 기능에 따라 다름

지원되는 Defense Center: 기능에 따라 다름

Context Explorer의 Files Information 섹션에는 모니터링되는 네트워크의 파일 및 악성코드 이벤트를 전체적으로 표시하는 6개의 인터랙티브 그래프가 포함되어 있습니다. 그중 5개 그래프에는 네트워크 트래픽에서 탐지되는 파일의 악성코드 속성, 파일 형식, 파일 이름과 이러한 파일을 보내는(업로드) 호스트 및 받는(다운로드) 호스트가 표시됩니다. 나머지 그래프에는 네트워크에서 탐지된 악성코드 위협과 사용자가 FireAMP Connector를 설치한 엔드포인트에서 탐지되는 악성코드 위협(FireAMP 서브스크립션이 있는 경우)이 표시됩니다.

참고 침입 정보에 대해 필터링하면 전체 Files Information 섹션은 숨겨집니다.

네트워크 기반 악성코드 데이터를 포함하려면 악성코드 라이센스가 있어야 하며 파일 정보 그래프용 악성코드 탐지를 활성화해야 합니다. DC500 방어 센터와 Series 2 디바이스 및 Cisco NGIPS for Blue Coat X-Series는 AMP를 지원하지 않으므로 DC500 방어 센터는 이 데이터를 표시할 수 없고 Series 2 디바이스와 Cisco NGIPS for Blue Coat X-Series는 이 데이터를 탐지하지 못합니다. 37-2페이지의 악성코드 차단 및 파일 제어 이해을/를 참조하십시오.

Files Information 섹션의 그래프에 대한 자세한 내용은 다음 항목을 참조하십시오.

- 56-25페이지의 Top File Types 그래프 보기
- 56-26페이지의 Top File Names 그래프 보기
- 56-27페이지의 Files by Disposition 그래프 보기
- 56-28페이지의 Top Hosts Sending Files 그래프 보기
- 56-29페이지의 Top Hosts Receiving Files 그래프 보기
- 56-30페이지의 Top Malware Detections 그래프 보기

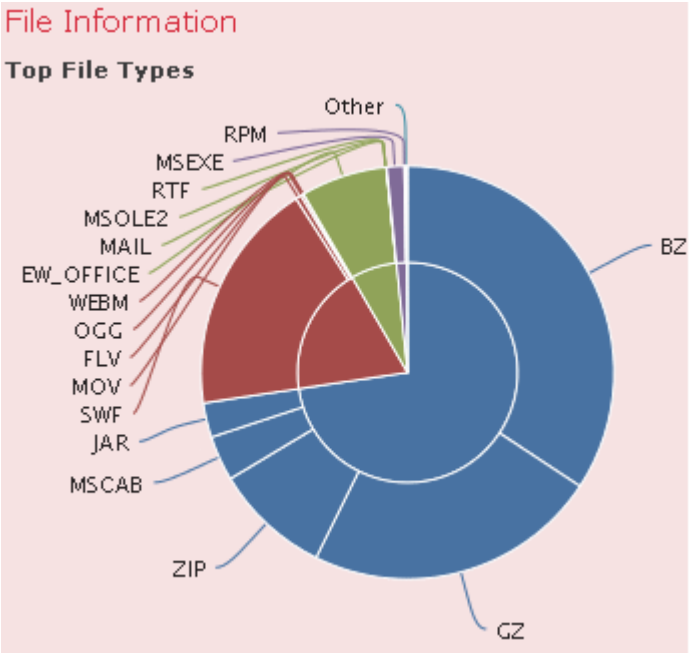
Top File Types 그래프 보기

라이센스: 보호 또는 악성코드

지원되는 디바이스: 기능에 따라 다름

지원되는 Defense Center: 기능에 따라 다름

도넛 형식의 Top File Types 그래프는 네트워크 트래픽에서 탐지되는 파일 형식(외부 원)의 비례 보기를 파일 카테고리(내부 원)로 그룹화하여 보여줍니다.



자세한 정보를 보려면 그래프의 원하는 부분으로 포인터를 이동하십시오. 그래프의 특정 부분을 클릭하면 해당 정보를 필터링하거나 드릴다운할 수 있습니다.

네트워크 기반 악성코드 데이터를 포함하려면 악성코드 라이센스가 있어야 하며 이 그래프용 악성코드 탐지를 활성화해야 합니다. DC500 방어 센터와 Series 2 디바이스 및 Cisco NGIPS for Blue Coat X-Series는 AMP를 지원하지 않으므로 DC500 방어 센터는 이 데이터를 표시할 수 없고 Series 2 디바이스와 Cisco NGIPS for Blue Coat X-Series는 이 데이터를 탐지하지 못합니다. 37-2페이지의 악성코드 차단 및 파일 제어 이해을/를 참조하십시오.

이 그래프에서는 File Events 테이블의 데이터를 주로 보여줍니다.

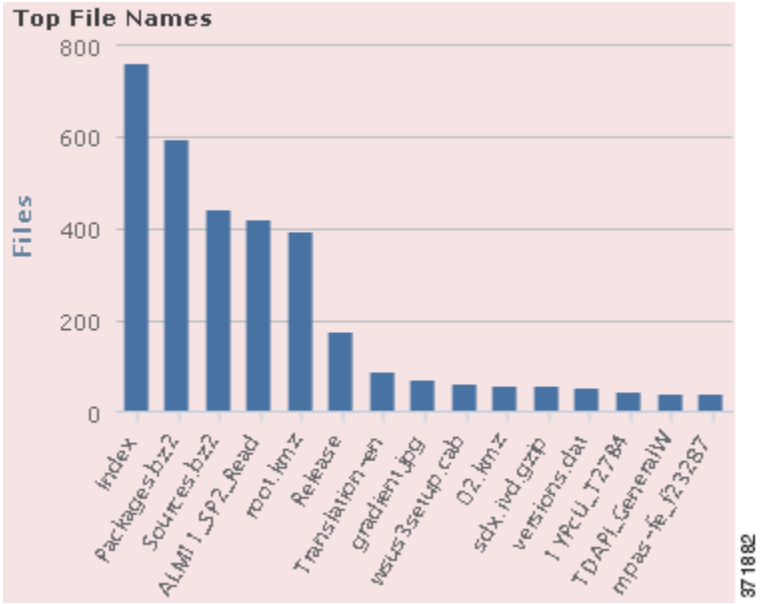
Top File Names 그래프 보기

라이센스: 보호 또는 악성코드

지원되는 디바이스: 기능에 따라 다름

지원되는 Defense Center: 기능에 따라 다름

막대 형식의 Top File Names 그래프는 네트워크 트래픽에서 탐지되는 고유한 상위 파일 이름의 카운트를 보여줍니다.



자세한 정보를 보려면 그래프의 원하는 부분으로 포인터를 이동하십시오. 그래프의 특정 부분을 클릭하면 해당 정보를 필터링하거나 드릴다운할 수 있습니다.

네트워크 기반 악성코드 데이터를 포함하려면 악성코드 라이센스가 있어야 하며 이 그래프용 악성코드 탐지를 활성화해야 합니다. DC500 방어 센터와 Series 2 디바이스 및 Cisco NGIPS for Blue Coat X-Series는 AMP를 지원하지 않으므로 DC500 방어 센터는 이 데이터를 표시할 수 없고 Series 2 디바이스와 Cisco NGIPS for Blue Coat X-Series는 이 데이터를 탐지하지 못합니다. 37-2페이지의 악성코드 차단 및 파일 제어 이해을/를 참조하십시오.

이 그래프에서는 File Events 테이블의 데이터를 주로 보여줍니다.

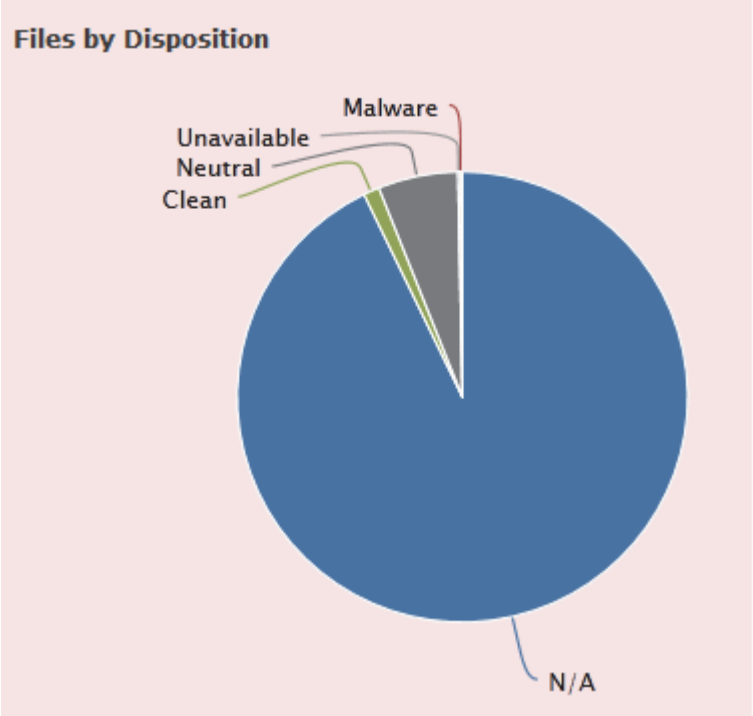
Files by Disposition 그래프 보기

라이센스: 보호 또는 악성코드

지원되는 디바이스: 기능에 따라 다름

지원되는 Defense Center: 기능에 따라 다름

원 형식의 Top File Types 그래프는 네트워크에서 탐지되는 파일에 대한 악성코드 성향의 비례 보기를 제공합니다. 방어 센터에서 종합 보안 인텔리전스 클라우드 조회를 수행한(악성코드 라이센스 필요) 대상 파일만 성향을 갖습니다. 클라우드 조회를 트리거하지 않은 파일은 `N/A` 성향을 갖습니다. `Unavailable` 성향은 방어 센터에서 악성코드 클라우드 조회를 수행할 수 없음을 나타냅니다. 기타 성향에 대한 설명은 37-2페이지의 악성코드 차단 및 파일 제어 이해을/를 참조하십시오.



자세한 정보를 보려면 그래프의 원하는 부분으로 포인터를 이동하십시오. 그래프의 특정 부분을 클릭하면 해당 정보를 필터링하거나 드릴다운할 수 있습니다.

네트워크 기반 악성코드 데이터를 포함하려면 악성코드 라이센스가 있어야 하며 이 그래프용 악성코드 탐지를 활성화해야 합니다. DC500 방어 센터와 Series 2 디바이스 및 Cisco NGIPS for Blue Coat X-Series는 AMP를 지원하지 않으므로 DC500 방어 센터는 이 데이터를 표시할 수 없고 Series 2 디바이스와 Cisco NGIPS for Blue Coat X-Series는 이 데이터를 탐지하지 못합니다. 37-2페이지의 악성코드 차단 및 파일 제어 이해을/를 참조하십시오.

이 그래프에서는 File Events 테이블의 데이터를 주로 보여줍니다.

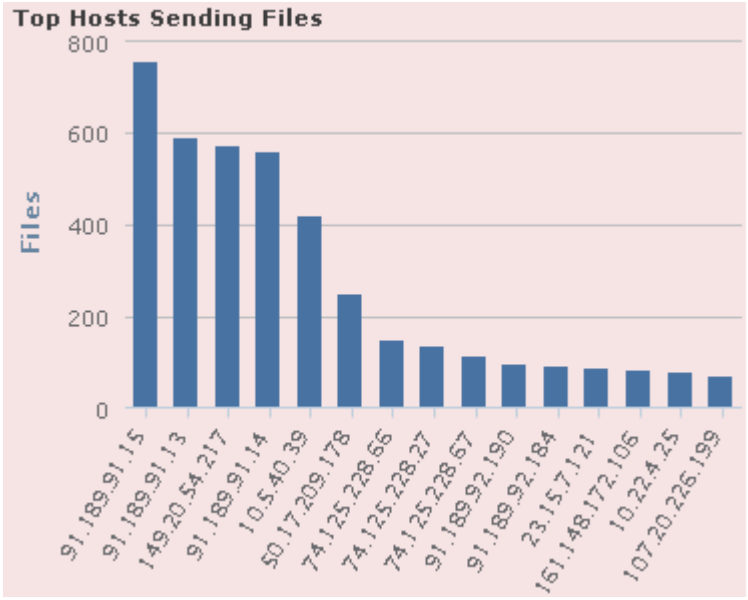
Top Hosts Sending Files 그래프 보기

라이센스: 보호 또는 악성코드

지원되는 디바이스: 기능에 따라 다름

지원되는 Defense Center: 기능에 따라 다름

막대 형식의 Top Hosts Sending Files 그래프는 상위 파일 전송 호스트 IP 주소에 대한 네트워크 트래픽에서 탐지되는 파일 수의 카운트를 제공합니다.



자세한 정보를 보려면 그래프의 원하는 부분으로 포인터를 이동하십시오. 그래프의 특정 부분을 클릭하면 해당 정보를 필터링하거나 드릴다운할 수 있습니다.

팁 악성코드 전송 호스트만 표시하도록 그래프를 제한하려면 포인터를 그래프 위로 이동하고 표시되는 토글 버튼에서 **Malware**를 클릭합니다. 기본 파일 보기로 돌아가려면 **Files**를 클릭합니다. Context Explorer에서 빠져나가도 기본 파일 보기로 돌아갑니다.

네트워크 기반 악성코드 데이터를 포함하려면 악성코드 라이센스가 있어야 하며 이 그래프용 악성코드 탐지를 활성화해야 합니다. DC500 방어 센터와 Series 2 디바이스 및 Cisco NGIPS for Blue Coat X-Series는 AMP를 지원하지 않으므로 DC500 방어 센터는 이 데이터를 표시할 수 없고 Series 2 디바이스와 Cisco NGIPS for Blue Coat X-Series는 이 데이터를 탐지하지 못합니다. 37-2페이지의 악성코드 차단 및 파일 제어 이해을/를 참조하십시오.

이 그래프에서는 File Events 테이블의 데이터를 주로 보여줍니다.

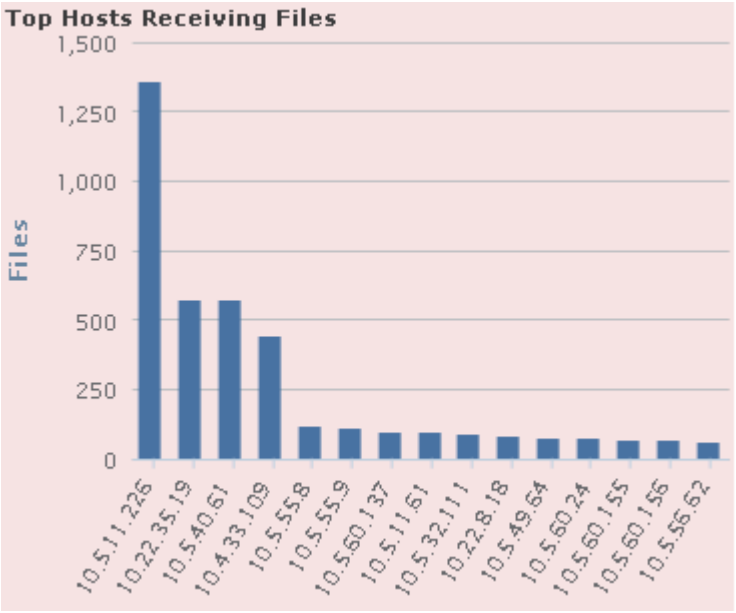
Top Hosts Receiving Files 그래프 보기

라이센스: 보호 또는 악성코드

지원되는 디바이스: 기능에 따라 다름

지원되는 Defense Center: 기능에 따라 다름

막대 형식의 Top Hosts Receiving Files 그래프는 상위 파일 수신 호스트 IP 주소에 대한 네트워크 트래픽에서 탐지되는 파일 수의 카운트를 제공합니다.



자세한 정보를 보려면 그래프의 원하는 부분으로 포인터를 이동하십시오. 그래프의 특정 부분을 클릭하면 해당 정보를 필터링하거나 드릴다운할 수 있습니다.

팁 악성코드 수신 호스트만 표시하도록 그래프를 제한하려면 포인터를 그래프 위로 이동하고 표시되는 토글 버튼에서 **Malware**를 클릭합니다. 기본 파일 보기로 돌아가려면 **Files**를 클릭합니다. Context Explorer에서 빠져나가도 기본 파일 보기로 돌아갑니다.

네트워크 기반 악성코드 데이터를 포함하려면 악성코드 라이센스가 있어야 하며 이 그래프용 악성코드 탐지를 활성화해야 합니다. DC500 방어 센터와 Series 2 디바이스 및 Cisco NGIPS for Blue Coat X-Series는 AMP를 지원하지 않으므로 DC500 방어 센터는 이 데이터를 표시할 수 없고 Series 2 디바이스와 Cisco NGIPS for Blue Coat X-Series는 이 데이터를 탐지하지 못합니다. 37-2페이지의 악성코드 차단 및 파일 제어 이해을/를 참조하십시오.

이 그래프에서는 File Events 테이블의 데이터를 주로 보여줍니다.

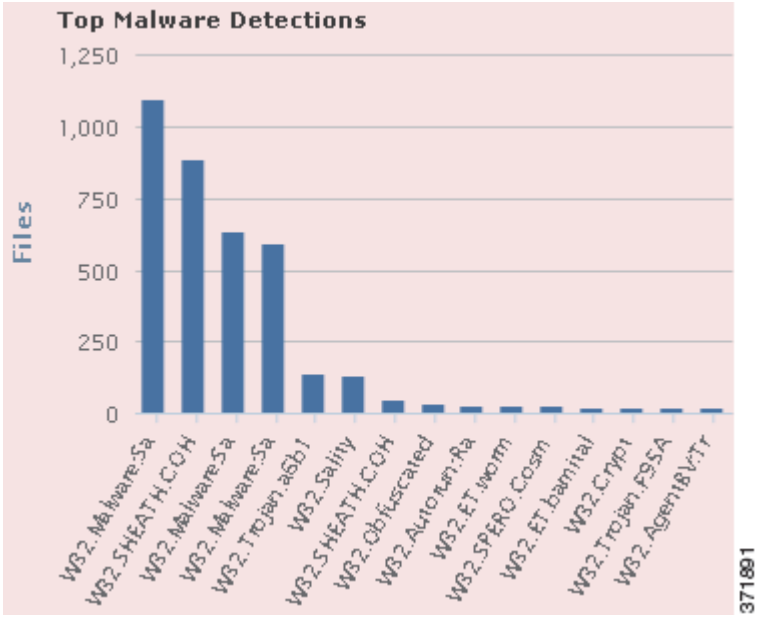
Top Malware Detections 그래프 보기

라이센스: 보호 또는 악성코드

지원되는 디바이스: 기능에 따라 다름

지원되는 Defense Center: 기능에 따라 다름

막대 형식의 Top Malware Detections 그래프는 네트워크에서, 그리고 사용자가 FireAMP Connector를 설치한 엔드포인트에서(FireAMP 서브스크립션이 있는 경우) 탐지되는 상위 악성코드 위협의 카운트를 표시합니다.



자세한 정보를 보려면 그래프의 원하는 부분으로 포인터를 이동하십시오. 그래프의 특정 부분을 클릭하면 해당 정보를 필터링하거나 드릴다운할 수 있습니다.

네트워크 기반 악성코드 데이터를 포함하려면 악성코드 라이센스가 있어야 하며 이 그래프용 악성코드 탐지를 활성화해야 합니다. DC500 방어 센터와 Series 2 디바이스 및 Cisco NGIPS for Blue Coat X-Series는 AMP를 지원하지 않으므로 DC500 방어 센터는 이 데이터를 표시할 수 없고 Series 2 디바이스와 Cisco NGIPS for Blue Coat X-Series는 이 데이터를 탐지하지 못합니다. 37-2페이지의 악성코드 차단 및 파일 제어 이해을/를 참조하십시오.

이 그래프에서는 File Events 및 Malware Events 테이블의 데이터를 주로 보여줍니다.

Geolocation Information 섹션 이해

라이센스: FireSIGHT

지원되는 Defense Center: DC500을 제외한 모두

Context Explorer의 Geolocation Information 섹션에는 모니터링되는 네트워크의 호스트가 데이터를 교환하는 국가를 전체적으로 보여주는 3개의 인터랙티브 도넛 그래프가 있습니다. 이러한 그래프는 각각 initiator 또는 responder 국가 단위의 고유한 연결, 소스 및 목적지 국가 단위의 침입 이벤트, 수신 또는 송신 국가 단위의 파일 이벤트에 대한 것입니다.

Geolocation Information 섹션의 그래프에 대한 자세한 내용은 다음 항목을 참조하십시오.

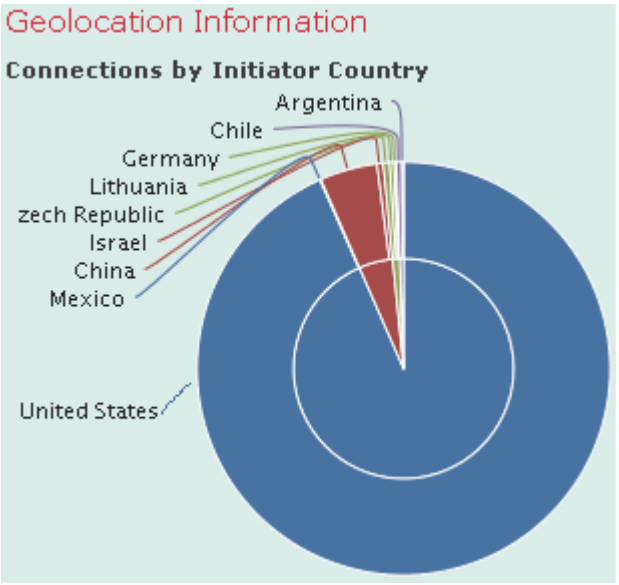
- 56-31페이지의 Connections by Initiator/Responder Country 그래프 보기
- 56-32페이지의 Intrusion Events by Source/Destination Country 그래프 보기
- 56-33페이지의 File Events by Sending/Receiving Country 그래프 보기

Connections by Initiator/Responder Country 그래프 보기

라이센스: FireSIGHT

지원되는 Defense Center: DC500을 제외한 모두

도넛 형식의 Connections by Initiator/Responder Country 그래프는 initiator(기본값) 또는 responder로서 네트워크의 연결과 관련된 국가의 비례 보기를 제공합니다. 내부 원은 이러한 국가를 대륙 단위로 그룹화합니다. 지오로케이션 정보에 대한 자세한 내용은 58-20페이지의 지오로케이션 사용을/를 참조하십시오. 연결 데이터에 대한 자세한 내용은 39-1페이지의 연결 및 보안 인텔리전스 데이터 작업을/를 참조하십시오.



자세한 정보를 보려면 그래프의 원하는 부분으로 포인터를 이동하십시오. 그래프의 특정 부분을 클릭하면 해당 정보를 필터링하거나 드릴다운할 수 있습니다.

팁 연결에서 responder 역할을 하는 국가만 표시하도록 그래프를 제한하려면 포인터를 그래프 위로 이동하고 표시되는 토글 버튼에서 **Responder**를 클릭합니다. 기본 보기로 돌아가려면 **Initiator**를 클릭합니다. Context Explorer에서 빠져나가도 기본 Initiator 보기로 돌아갑니다.

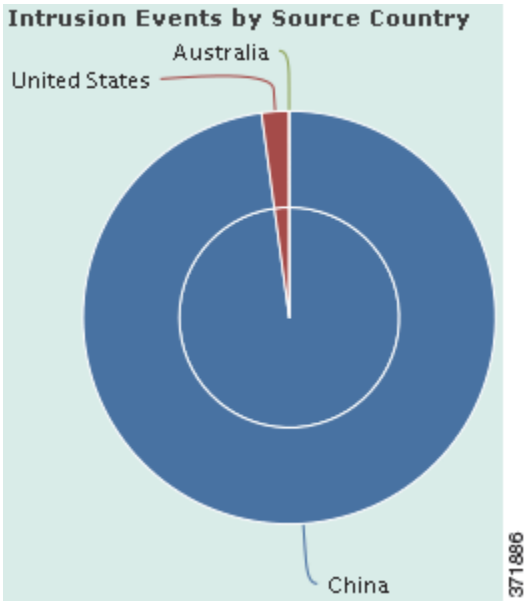
이 그래프에서는 Connection Summary Data 테이블의 데이터를 주로 보여줍니다.

Intrusion Events by Source/Destination Country 그래프 보기

라이센스: FireSIGHT

지원되는 Defense Center: DC500을 제외한 모두

도넛 형식의 Intrusion Events by Source/Destination Country 그래프는 이벤트의 소스(기본값) 또는 목적지로서 네트워크의 침입 이벤트와 관련된 국가의 비례 보기를 제공합니다. 내부 원은 이러한 국가를 대륙 단위로 그룹화합니다. 지오로케이션 정보에 대한 자세한 내용은 58-20페이지의 지오로케이션 사용을/를 참조하십시오. 침입 이벤트 데이터에 대한 자세한 내용은 41-1페이지의 침입 이벤트 작업을/를 참조하십시오.



자세한 정보를 보려면 그래프의 원하는 부분으로 포인터를 이동하십시오. 그래프의 특정 부분을 클릭하면 해당 정보를 필터링하거나 드릴다운할 수 있습니다.

팁 연결에서 침입 이벤트의 목적지 역할을 하는 국가만 표시하도록 그래프를 제한하려면 포인터를 그래프 위로 이동하고 표시되는 토글 버튼에서 **Destination**을 클릭합니다. 기본 보기로 돌아가려면 **Source**를 클릭합니다. Context Explorer에서 빠져나가도 기본 소스 보기로 돌아갑니다.

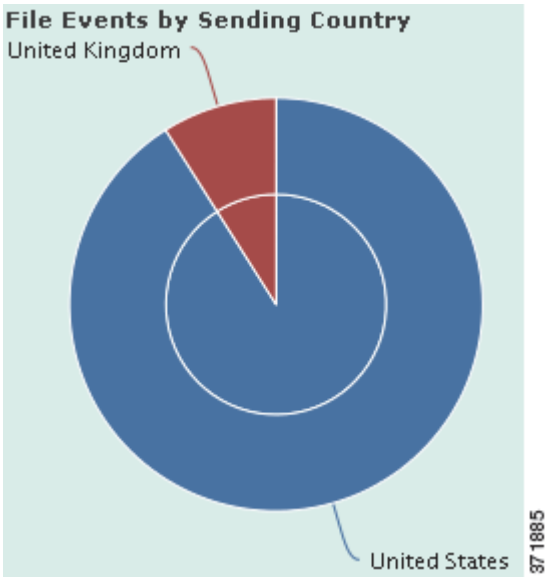
이 그래프에서는 Intrusion Events 테이블의 데이터를 주로 보여줍니다.

File Events by Sending/Receiving Country 그래프 보기

라이센스: FireSIGHT

지원되는 Defense Center: DC500을 제외한 모두

도넛 형식의 File Events by Sending/Receiving Country 그래프는 네트워크의 파일 이벤트에서 파일을 전송하거나(기본값) 수신하는 것으로 탐지되는 국가의 비례 보기를 제공합니다. 내부 원은 이러한 국가를 대륙 단위로 그룹화합니다. 지오로케이션 정보에 대한 자세한 내용은 58-20페이지의 지오로케이션 사용을/를 참조하십시오. 파일 이벤트 데이터에 대한 자세한 내용은 40-8페이지의 파일 이벤트 작업을/를 참조하십시오.



자세한 정보를 보려면 그래프의 원하는 부분으로 포인터를 이동하십시오. 그래프의 특정 부분을 클릭하면 해당 정보를 필터링하거나 드릴다운할 수 있습니다.

팁 파일 수신 국가만 표시하도록 그래프를 제한하려면 포인터를 그래프 위로 이동하고 표시되는 토글 버튼에서 **Receiver**를 클릭합니다. 기본 보기로 돌아가려면 **Sender**를 클릭합니다. Context Explorer에서 빠져나가도 기본 Sender 보기로 돌아갑니다.

이 그래프에서는 File Events 테이블의 데이터를 주로 보여줍니다.

URL Information 섹션 이해

라이센스: FireSIGHT 또는 URL 필터링

지원되는 디바이스: 기능에 따라 다름

지원되는 Defense Center: 기능에 따라 다름

Context Explorer의 URL Information 섹션에는 모니터링되는 네트워크의 호스트가 데이터를 교환하는 URL을 전체적으로 보여주는 3개의 인터랙티브 막대 그래프가 있습니다. 여기에는 URL과 연결된 트래픽 및 고유한 연결이 포함되며 개별 URL, URL 카테고리 및 URL 평판 단위로 정렬됩니다. URL 정보에 대해서는 필터링할 수 없습니다.

참고 침입 이벤트 정보에 대해 필터링하면 전체 URL Information 섹션은 숨겨집니다.

URL 카테고리 및 평판 데이터를 포함하려면 URL 필터링 라이센스가 있어야 하며 URL 필터링 그래프용 URL 필터링을 활성화해야 합니다. DC500 방어 센터와 Series 2 디바이스 모두 평판 및 카테고리 기준 URL 필터링을 지원하지 않으므로 DC500 방어 센터는 이 데이터를 표시할 수 없고 Series 2 디바이스는 이 데이터를 탐지하지 못합니다. 16-8페이지의 URL 차단을/를 참조하십시오.

URL Information 섹션의 그래프에 대한 자세한 내용은 다음 항목을 참조하십시오.

- 56-35페이지의 Traffic by URL 그래프 보기
- 56-36페이지의 Traffic by URL Category 그래프 보기
- 56-37페이지의 Traffic by URL Reputation 그래프 보기

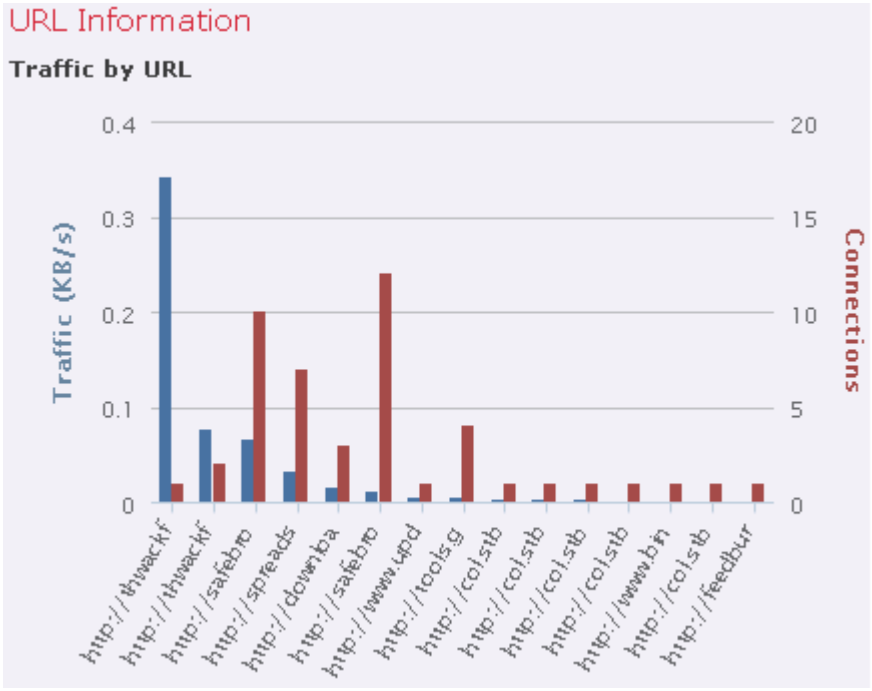
Traffic by URL 그래프 보기

라이센스: FireSIGHT 또는 URL 필터링

지원되는 디바이스: 기능에 따라 다름

지원되는 Defense Center: 기능에 따라 다름

막대 형식의 Traffic by URL 그래프는 모니터링되는 네트워크에서 가장 요청이 많은 URL 15개에 대한 네트워크 트래픽(초당 킬로바이트 단위) 및 고유한 연결의 카운트를 보여줍니다. 나열된 각 URL에서 파란색 막대는 트래픽 데이터를, 빨간색 막대는 연결 데이터를 나타냅니다.



자세한 정보를 보려면 그래프의 원하는 부분으로 포인터를 이동하십시오. 그래프의 특정 부분을 클릭하면 해당 정보로 드릴다운할 수 있습니다.

참고 침입 이벤트 정보에 대해 필터링하면 Traffic by URL 그래프는 숨겨집니다.

URL 카테고리 및 평판 데이터를 포함하려면 URL 필터링 라이센스가 있어야 하며 URL 필터링 그래프용 URL 필터링을 활성화해야 합니다. DC500 방어 센터와 Series 2 디바이스 모두 평판 및 카테고리 기준 URL 필터링을 지원하지 않으므로 DC500 방어 센터는 이 데이터를 표시할 수 없고 Series 2 디바이스는 이 데이터를 탐지하지 못합니다. 64-27페이지의 클라우드 통신 활성화을/를 참조하십시오.

이 그래프에서는 Connection Events 테이블의 데이터를 주로 보여줍니다.

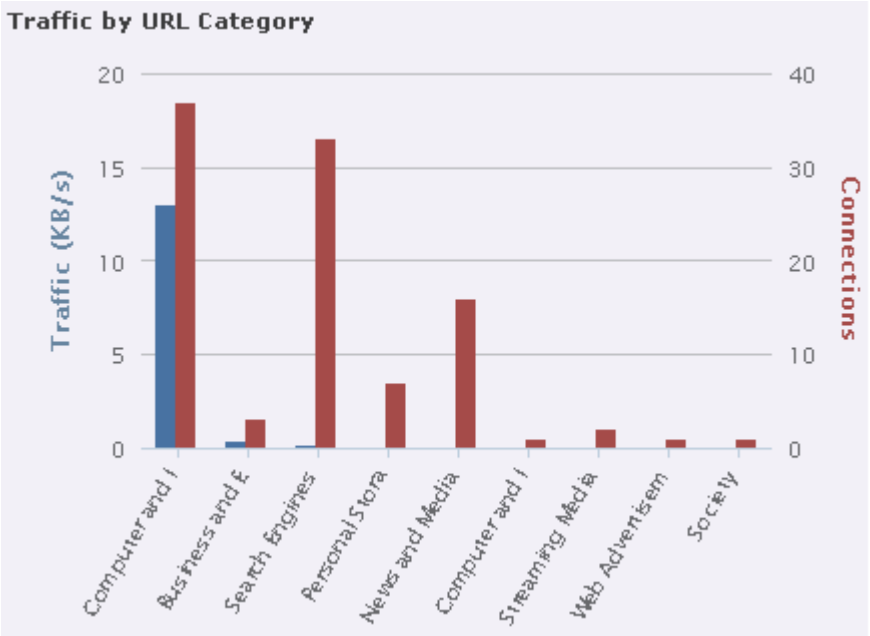
Traffic by URL Category 그래프 보기

라이센스: URL 필터링

지원되는 디바이스: 기능에 따라 다름

지원되는 Defense Center: 기능에 따라 다름

막대 형식의 Traffic by URL Category 그래프는 모니터링되는 네트워크에서 가장 요청이 많은 URL 카테고리(예: `Search Engines` 또는 `Streaming Media`)에 대한 네트워크 트래픽(초당 킬로바이트 단위) 및 고유한 연결의 카운트를 보여줍니다. 나열된 각 URL 카테고리에서 파란색 막대는 트래픽 데이터를, 빨간색 막대는 연결 데이터를 나타냅니다.



자세한 정보를 보려면 그래프의 원하는 부분으로 포인터를 이동하십시오. 그래프의 특정 부분을 클릭하면 해당 정보로 드릴다운할 수 있습니다.

참고 침입 이벤트 정보에 대해 필터링하면 Traffic by URL Category 그래프는 숨겨집니다.

URL 카테고리 및 평판 데이터를 포함하려면 URL 필터링 라이센스가 있어야 하며 URL 필터링 그래프용 URL 필터링을 활성화해야 합니다. DC500 방어 센터와 Series 2 디바이스 모두 평판 및 카테고리 기준 URL 필터링을 지원하지 않으므로 DC500 방어 센터는 이 데이터를 표시할 수 없고 Series 2 디바이스는 이 데이터를 탐지하지 못합니다. 16-10페이지의 평판 기반 URL 차단 수행을/를 참조하십시오.

이 그래프에서는 URL Statistics 및 Connection Events 테이블의 데이터를 주로 보여줍니다.

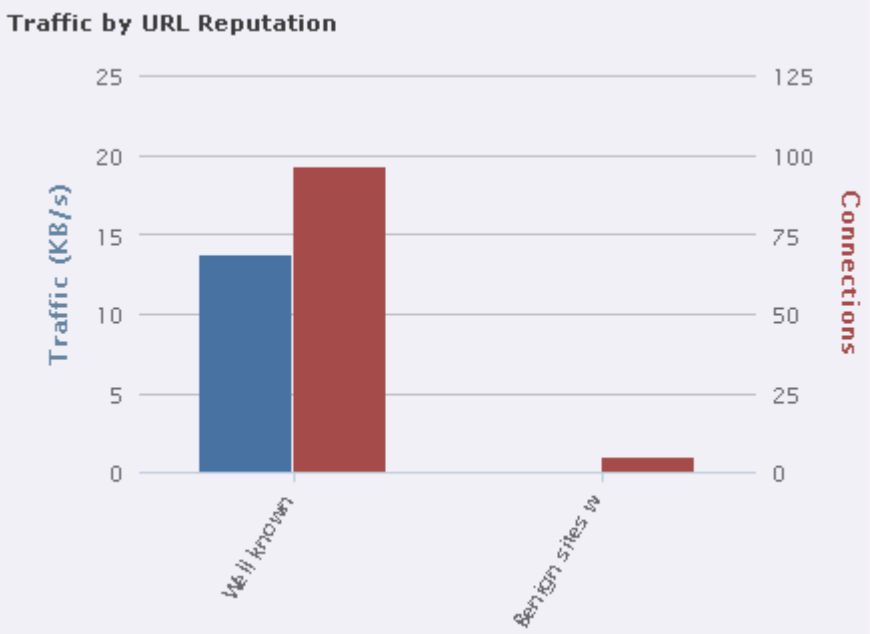
Traffic by URL Reputation 그래프 보기

라이센스: URL 필터링

지원되는 디바이스: 기능에 따라 다름

지원되는 Defense Center: 기능에 따라 다름

막대 형식의 Traffic by URL Reputation 그래프는 모니터링되는 네트워크에서 가장 요청이 많은 URL 평판 그룹(예: `Well known` 또는 `Benign sites with security risks`)에 대한 네트워크 트래픽(초당 킬로바이트 단위) 및 고유한 연결의 카운트를 보여줍니다. 나열된 각 URL 평판에서 파란색 막대는 트래픽 데이터를, 빨간색 막대는 연결 데이터를 나타냅니다.



자세한 정보를 보려면 그래프의 원하는 부분으로 포인터를 이동하십시오. 그래프의 특정 부분을 클릭하면 해당 정보로 드릴다운할 수 있습니다.

참고 침입 이벤트 정보에 대해 필터링하면 Traffic by URL Reputation 그래프는 숨겨집니다.

URL 카테고리 및 평판 데이터를 포함하려면 URL 필터링 라이센스가 있어야 하며 URL 필터링 그래프용 URL 필터링을 활성화해야 합니다. DC500 방어 센터와 Series 2 디바이스 모두 평판 및 카테고리 기준 URL 필터링을 지원하지 않으므로 DC500 방어 센터는 이 데이터를 표시할 수 없고 Series 2 디바이스는 이 데이터를 탐지하지 못합니다. 16-10페이지의 평판 기반 URL 차단 수행을/를 참조하십시오.

이 그래프에서는 URL Statistics 및 Connection Events 테이블의 데이터를 주로 보여줍니다.

Context Explorer 새로 고침

라이센스: FireSIGHT

Context Explorer는 표시되는 정보를 자동으로 업데이트하지 않습니다. 새로운 데이터를 표시하려면 Explorer를 수동으로 새로 고쳐야 합니다.

Context Explorer 자체를 다시 고치면(브라우저 프로그램을 새로 고치거나 Context Explorer에서 나간 후 다시 돌아오는 방법 사용) 표시되는 모든 정보를 새로 고칠 수 있지만, 섹션 컨피그레이션에 대해 변경한 내용(예: Ingress/Egress 그래프 및 애플리케이션 정보 섹션)이 유지되지 않으며 로딩에 지연이 발생할 수 있습니다.

Context Explorer를 새로 고치려면

액세스: Admin/Any Security Analyst

1단계 Context Explorer의 오른쪽 위에서 **Reload**를 클릭합니다.

선택한 시간 범위 내에서 최신 정보를 표시하도록 Explorer가 업데이트됩니다. 새로 고침이 완료될 때까지 **Reload** 버튼이 회색으로 표시됩니다.

Context Explorer 시간 범위 설정

라이센스: FireSIGHT

Context Explorer의 시간 범위를 마지막 시간 단위(기본값)로 짧게, 또는 마지막 연도 단위로 길게 반영하도록 구성할 수 있습니다. 시간 범위를 변경해도 변경 사항을 반영하여 Context Explorer가 자동으로 업데이트되지는 않습니다. 새로운 시간 범위를 적용하려면 Explorer를 수동으로 새로 고쳐야 합니다.

Context Explorer에서 빠져나가거나 로그인 세션을 종료해도 시간 범위에 대한 변경 사항은 유지됩니다.

Context Explorer 시간 범위를 변경하려면

액세스: Admin/Any Security Analyst

1단계 **Show the last** 드롭다운 목록에서 시간 범위를 선택합니다.

2단계 선택적으로, 새 시간 범위의 데이터를 보려면 **Reload**를 클릭합니다.

새 시간 범위를 반영하도록 Context Explorer의 모든 섹션이 업데이트됩니다.

팁 **Apply Filters**를 클릭해도 시간 범위 업데이트가 적용됩니다.

Context Explorer 섹션 최소화 및 최대화

라이센스: FireSIGHT

하나 이상의 Context Explorer 섹션을 최소화할 수 있습니다. 이는 특정 섹션에만 집중하거나 더 간단한 보기를 원하는 경우 유용합니다. Traffic and Intrusion Event Counts Time 그래프는 최소화할 수 없습니다.

페이지를 새로 고치거나 어플라이언스에서 로그아웃해도 최소화 또는 최대화 구성 상태는 Context Explorer 섹션에서 그대로 유지됩니다.

Context Explorer 섹션을 최소화하려면

액세스: Admin/Any Security Analyst

1단계 섹션의 제목 표시줄에서 최소화 아이콘(−)을 클릭합니다.

Context Explorer 섹션을 최대화하려면

액세스: Admin/Any Security Analyst

1단계 최소화된 섹션의 제목 표시줄에서 최대화 아이콘(□)을 클릭합니다.

Context Explorer 데이터에 대해 드릴다운

라이센스: 기능에 따라 다름

Context Explorer에서 허용하는 것보다 더 자세히 그래프 또는 목록 데이터를 검사하려면 관련 데이터의 테이블 보기로 드릴다운할 수 있습니다(Traffic and Intrusion Events over Time 그래프에서는 드릴다운할 수 없습니다.). 예를 들어 Traffic by Source IP 그래프에서 IP 주소로 드릴다운하면 선택한 소스 IP 주소와만 연결된 데이터를 포함하여 Connection Events 테이블의 Connections with Application Details 보기가 표시됩니다.

검사하는 데이터 유형에 따라 컨텍스트 메뉴에 추가 옵션이 표시될 수 있습니다. 특정 IP 주소와 관련된 데이터 포인트는 선택하는 IP 주소에서 호스트 또는 whois 정보를 볼 수 있는 옵션을 제공합니다. 특정 애플리케이션과 관련된 데이터 포인트는 선택하는 애플리케이션에 대한 애플리케이션 정보를 볼 수 있는 옵션을 제공합니다. 특정 사용자와 관련된 데이터 포인트는 해당 사용자의 사용자 프로필 페이지를 볼 수 있는 옵션을 제공합니다. 침입 이벤트 메시지와 관련된 데이터 포인트는 해당 이벤트와 관련된 침입 규칙에 대한 규칙 문서를 볼 수 있는 옵션을 제공하며, 특정 IP 주소와 관련된 데이터 포인트는 해당 주소를 블랙리스트 또는 화이트리스트에 추가할 수 있는 옵션을 제공합니다.

데이터에 대해 드릴다운하는 데 사용하는 컨텍스트 메뉴에는 해당 데이터를 필터링하기 위한 옵션이 포함되어 있습니다. 필터링에 대한 자세한 내용은 56-41페이지의 Context Explorer에서 필터 작업을/를 참조하십시오.

Context Explorer에서 데이터에 대해 드릴다운하려면

액세스: Admin/Any Security Analyst

1단계 **Analysis > Context Explorer**를 선택합니다.

Context Explorer가 나타납니다.

2단계 Traffic and Intrusion Events over Time을 제외한 임의의 섹션에서 조사하려는 데이터 포인트를 클릭합니다.

컨텍스트 메뉴 팝업 창이 근처에 표시됩니다.

3단계 선택한 데이터 포인트에 따라 여러 가지 옵션이 표시됩니다.

- 테이블 보기에서 이 데이터를 더 자세히 살펴보려면 **Drill into Analysis**를 선택합니다.

  선택한 데이터의 자세한 테이블 보기와 함께 새 창이 열립니다.

- 특정 IP 주소와 관련된 데이터 포인트를 선택했으며 관련 호스트에 대해 자세히 알아보려면 **View Host Information**을 선택합니다.

  선택한 IP 주소에 대한 호스트 프로필 페이지와 함께 새 창이 열립니다. 호스트 특성 및 호스트 프로필에 대한 자세한 내용은 49-1페이지의 호스트 프로필 사용을/를 참조하십시오.

- 특정 IP 주소의 데이터 포인트를 선택했으며 해당 주소에서 whois 검색을 수행하려면 **Whois**를 선택합니다.

  선택한 IP 주소에 대한 whois 쿼리 결과와 함께 새 창이 열립니다.

- 특정 애플리케이션과 관련된 데이터 포인트를 선택했으며 해당 애플리케이션에 대해 자세히 알아보려면 **View Application Information**을 선택합니다.

  선택한 애플리케이션에 대한 정보와 함께 새 창이 열립니다. 애플리케이션 특성에 관한 자세한 정보는 45-10페이지의 애플리케이션 탐지 이해을/를 참조하십시오.

- 특정 사용자와 관련된 데이터 포인트를 선택했으며 해당 사용자에 대해 자세히 알아보려면 **View User Information**을 선택합니다.

  선택한 사용자에 대한 사용자 프로필 페이지와 함께 새 창이 열립니다. 사용자 세부사항에 대해 자세히 알아보려면 50-63페이지의 사용자 세부사항 및 호스트 기록 이해을/를 참조하십시오.

- 특정 침입 이벤트 메시지와 관련된 데이터 포인트를 선택했으며 관련 침입 규칙에 대해 자세히 알아보려면 **View Rule Information**을 선택합니다.

  선택한 이벤트와 관련된 규칙 세부사항 페이지와 함께 새 창이 열립니다. 침입 규칙 세부사항에 대해 자세히 알아보려면 32-5페이지의 규칙 세부사항 보기을/를 참조하십시오.

- 특정 IP 주소와 관련된 데이터 포인트를 선택했으며 해당 IP 주소를 보안 인텔리전스 전역 블랙리스트 또는 화이트리스트에 추가하려면 해당 옵션, 즉 **Blacklist Now** 또는 **Whitelist Now**를 선택합니다. 표시되는 팝업 창에서 선택 항목을 확인합니다.

  IP 주소가 블랙리스트 또는 화이트리스트에 추가됩니다. 자세한 내용은 3-7페이지의 전역 화이트리스트 및 블랙리스트 작업을/를 참조하십시오.

  보안 인텔리전스 데이터를 지원하지 않는 DC500 방어 센터에는 이러한 옵션이 나열되지 않습니다.

Context Explorer에서 필터 작업

라이센스: FireSIGHT

Context Explorer에 처음 표시되는 기본적인 광범위한 데이터를 이용해 네트워크의 활동에 대해 좀 더 세부적인 컨텍스트를 얻기 위해 이러한 데이터를 필터링할 수 있는 옵션이 제공됩니다. 필터는 모든 유형의 FireSIGHT 데이터(URL 정보 제외)를 포괄하며, 포함과 제외를 지원하고, Context Explorer 그래프 데이터 포인트에서 클릭하여 빠르게 적용할 수 있으며, 전체 Explorer에 영향을 미칩니다. 동시에 최대 20개의 필터를 적용하여 네트워크 및 조직의 요구에 맞는 매우 구체적인 결과를 얻을 수 있습니다. 적용하는 필터는 Context Explorer URL에 반영되므로, 나중에 사용할 수 있도록 유용한 필터 집합을 브라우저 프로그램에서 북마크 처리할 수 있습니다.

Context Explorer에서 필터를 사용하는 방법에 대한 자세한 내용은 다음 항목을 참조하십시오.

- 56-41페이지의 필터 추가 및 적용
- 56-45페이지의 컨텍스트 메뉴로 필터 만들기
- 56-46페이지의 필터를 북마크 처리

필터 추가 및 적용

라이센스: 기능에 따라 다름

지원되는 디바이스: 기능에 따라 다름

지원되는 Defense Center: 기능에 따라 다름

Context Explorer 데이터에 여러 방법으로 필터를 추가할 수 있습니다.

- Add Filter 창에서
- Explorer에서 데이터 포인트를 선택한 경우 컨텍스트 메뉴 팝업 창에서
- Context Explorer 아이콘(sf) 또는 특정 세부사항 보기 페이지(Application Detail, Host Profile, Rule Detail 및 User Profile)에 나타나는 텍스트 링크에서. 이러한 링크를 클릭하면 세부사항 보기 페이지의 관련 데이터에 따라 Context Explorer가 자동으로 열리고 필터링이 수행됩니다. 예를 들어, 사용자 `jenkins`에 대한 사용자 세부사항 페이지에서 Context Explorer 링크를 클릭하면 해당 사용자와 관련된 데이터만 표시하도록 Explorer가 제한됩니다.

이 섹션에서는 Add Filter 창을 이용해 처음부터 필터를 만드는 방법에 대해 자세히 알아봅니다. Context Explorer 그래프 및 목록 데이터에서 컨텍스트 메뉴를 사용하여 빠르게 필터를 만드는 방법에 대한 자세한 내용은 56-45페이지의 컨텍스트 메뉴로 필터 만들기을/를 참조하십시오.

Context Explorer 왼쪽 위의 **Filters** 아래에 있는 더하기 아이콘(+)을 클릭하여 액세스할 수 있는 Add Filter 창에는 **Data Type** 및 **Filter**의 두 필드만 포함되어 있습니다.

Data Type 드롭다운 목록에는 Context Explorer를 제한하는 데 사용할 수 있는 많은 유형의 FireSIGHT 시스템 데이터가 포함되어 있습니다. 데이터 유형을 선택한 다음 **Filter** 필드에서 해당 유형에 대한 특정 값(예: **Continent** 유형에 대해 `Asia` 값)을 입력합니다. 사용자에게 도움이 되도록 선택 가능한 데이터 유형에 대한 몇 가지 예제 값이 Filter 필드에 회색으로 표시됩니다. (필드에 데이터를 입력하면 이러한 값이 지워집니다.)

다음 표에는 필터로 이용할 수 있는 데이터 유형과 각 유형에 대한 예제 및 간단한 정의가 나열되어 있습니다. 지원되지 않는 기능에 대한 데이터가 DC500 방어 센터에는 표시되지 않으며 Series 2 디바이스 및 Cisco NGIPS for Blue Coat X-Series에서는 탐지되지 않습니다. Series 2 디바이스 및 Cisco NGIPS for Blue Coat X-Series 기능 요약은 디바이스 모델별 지원되는 액세스 제어 기능 표를 참조하십시오.

표 56-2 필터 데이터 유형

유형	예제 값	정의
Access Control Action	`Allow`, `Block`	트래픽을 허용 또는 차단하기 위해 액세스 제어 정책에서 수행하는 작업
Application Category	`web browser`, `email`	애플리케이션의 가장 핵심적인 기능에 대한 일반 분류
Application Name	`Facebook`, `HTTP`	애플리케이션의 이름
Application Risk	`Very High`, `Medium`	애플리케이션의 예상 보안 위험
Application Tag	`encrypts communications`, `sends mail`	애플리케이션에 대한 추가 정보(애플리케이션에는 0부터 원하는 수만큼의 태그 포함 가능)
Application Type	`Client`, `Web Application`	애플리케이션 유형(application protocol, client 또는 web application)
Business Relevance	`Very Low`, `High`	비즈니스 활동에 대한 애플리케이션의 예상 연관성(레크리에이션과 반대)
Continent	`North America`, `Asia`	모니터링되는 네트워크에서 탐지되는 라우팅 가능한 IP 주소와 관련된 대륙
Country	`Canada`, `Japan`	모니터링되는 네트워크에서 탐지되는 라우팅 가능한 IP 주소와 관련된 국가
Device	`device1.example.com`, `192.168.1.3`	모니터링되는 네트워크에 있는 디바이스의 이름 또는 IP 주소
Event Classification	`Potential Corporate Policy Violation`, `Attempted Denial of Service`	침입 이벤트에 대한 설명으로, 침입 이벤트를 트리거한 규칙, 디코더 또는 프리프로세서의 분류에 의해 결정됨
Event Message	`dns response`, `P2P`	이벤트에 의해 생성되는 메시지로, 이벤트를 트리거한 규칙, 디코더 또는 프리프로세서에 의해 결정됨
File Disposition	`Malware`, `Clean`	방어 센터에서 악성코드 클라우드 조회를 수행한 파일에 대해 클라우드에서 결정하는 성향
File Name	`Packages.bz2`	네트워크 트래픽에서 탐지되는 파일의 이름
File SHA256	임의의 32비트 문자열	방어 센터에서 악성코드 클라우드 조회를 수행한 파일의 SHA-256 해시 값
File Type	`GZ`, `SWF`, `MOV`	네트워크 트래픽에서 탐지되는 파일 형식
File Type Category	`Archive`, `Multimedia`, `Executables`	네트워크 트래픽에서 탐지되는 파일 형식의 일반 카테고리
IP Address	`192.168.1.3`, `2001:0db8:85a3::0000/24`	IPv4 또는 IPv6 주소, 주소 범위 또는 주소 블록 IP 주소를 검색하면 이벤트가 반환되는데, 여기서 해당 주소는 이벤트의 소스 또는 목적지임
Impact Level	`Impact Level 1`, `Impact Level 2`	모니터링되는 네트워크에서 이벤트의 예상 영향
Inline Result	`dropped`, `would have dropped`	트래픽이 삭제되었는지, 삭제된 것으로 추정되는지 또는 시스템에 의해 작동되지 않았는지 여부
IOC Category	`High Impact Attack`, `Malware Detected`	트리거된 IOC(Indications of Compromise) 이벤트에 대한 카테고리
IOC Event Type	`exploit-kit`, `malware-backdoor`	특정 IOC(Indications of Compromise)와 관련된 식별자로, 이를 트리거한 이벤트를 가리킴

표 56-2 필터 데이터 유형 (계속)

유형	예제 값	정의
Malware Threat Name	`W32.Trojan.a6b1`	악성코드 위협의 이름
OS Name	`Windows`, `Linux`	운영 체제의 이름
OS Version	`XP`, `2.6`	운영 체제의 특정 버전
Priority	`high`, `low`	이벤트의 예상 긴급도
Security Intelligence Category	`Malware`, `Spam`	보안 인텔리전스로 확인된 위험 트래픽의 카테고리
Security Zone	`My Security Zone`, `Security Zone X`	트래픽이 분석되고 통과되는(인라인 구축의 경우) 인터페이스 집합
SSL	`yes`, `no`	SSL 또는 TLS 암호화 트래픽
User	`wsmith`, `mtwain`	모니터링되는 네트워크의 호스트에 로그인하는 사용자의 ID

Filter 필드에서, 기본적으로 이벤트 검색에서 할 수 있는 것처럼 특별한 검색 매개변수(예: `*` 및 `!`)를 입력할 수 있습니다. 제외하는 필터를 만들려면 `!` 기호를 필터 매개변수 접두사로 사용하면 됩니다. 일반적으로 FireSIGHT 시스템에서 지원되는 검색 제한 사항에 대한 자세한 내용은 60-5페이지의 검색에 와일드카드 및 기호 사용을/를 참조하십시오.

여러 필터가 활성화된 경우 동일한 데이터 유형에 대한 값은 OR 검색 기준으로 취급되므로, 적어도 하나의 값과 일치하는 모든 데이터가 표시됩니다. 서로 다른 데이터 유형에 대한 값은 AND 검색 기준으로 취급되므로, 데이터는 필터링하는 각 데이터 유형에 대해 적어도 하나의 값과 일치해야 합니다. 예를 들어 `Application: 2channel`, `Application: Reddit` 및 `User: edickinson` 필터 집합에 대해 나타나는 데이터는 사용자 `edickinson` **및(AND)** 애플리케이션 `2channel` **또는(OR)** 애플리케이션 `Reddit`과 관련이 있어야 합니다.

필터에 대한 데이터 유형과 값을 확인하면 페이지의 왼쪽 위에 필터 위젯이 나타나며, 새 필터의 데이터 유형과 값을 보여줍니다.

적용하기 전에 여러 필터를 구성하고자 할 수 있으므로, 그리고 Context Explorer의 모든 섹션을 완전히 다시 로드하는 데 시간이 좀 걸릴 수 있으므로, 추가한 필터가 자동으로 적용되지는 않습니다. 필터를 적용하려면 **Apply Filters**를 클릭해야 합니다. 구성되었지만 아직 적용되지 않은 필터는 흐리게 표시됩니다. 동시에 최대 20개의 필터를 가질 수 있으며, 필터 위젯에서 삭제 아이콘(✖)을 클릭하여 개별 필터를 삭제할 수 있습니다. 모든 필터를 동시에 삭제하려면 **Clear** 버튼을 클릭할 수 있습니다.

일부 필터 유형은 다른 유형과 호환되지 않습니다. 예를 들어 침입 이벤트(예: **Device** 및 **Inline Result**)와 관련된 필터는 연결 이벤트와 관련된 필터(예: **Access Control Action**)와 동시에 적용할 수 없습니다. 시스템에서 연결 이벤트 데이터와 침입 이벤트 데이터를 정렬할 수 없기 때문입니다. 시스템에서는 호환되지 않는 필터가 동시에 적용되는 것을 방지합니다. 한 필터 유형이 좀 더 최근에 활성화되었으면, 비호환성이 존재하는 한 호환되지 않는 유형의 필터가 숨겨집니다.

표시되는 데이터는 관리되는 디바이스의 라이센스 및 구축 방법, 데이터를 제공하는 기능의 구성 여부(Series 2 어플라이언스의 경우), 데이터를 제공하는 기능을 어플라이언스가 지원하는지 여부 등의 요소에 따라 달라집니다. 예를 들어 DC500 방어 센터와 Series 2 디바이스 모두 카테고리 및 평판 기준 URL 필터링을 지원하지 않으므로 DC500 방어 센터에는 이 기능에 대한 데이터가 표시되지 않으며 Series 2 디바이스에서는 이 데이터가 탐지되지 않습니다.

Add Filter 창에서 새 필터를 만들려면

액세스: Admin/Any Security Analyst

1단계 **Analysis > Context Explorer**를 선택합니다.

Context Explorer가 나타납니다.

2단계 오른쪽 위의 **Filters** 아래에서 더하기 아이콘(+)을 클릭합니다.

Add Filter 팝업 창이 나타납니다.

3단계 **Data Type** 드롭다운 목록에서 필터링할 데이터 유형을 선택합니다.

Filter 필드가 해당 데이터 유형의 예제 값으로 채워집니다.

4단계 **Filter** 필드에 필터링할 데이터 유형 값을 입력합니다.

5단계 **OK**를 클릭합니다.

필터가 추가됩니다. Context Explorer가 다시 나타나고 해당 필터 위젯도 나타납니다.

6단계 선택적으로, 원하는 필터 집합이 구성될 때까지 이전 단계를 반복하여 필터를 더 추가합니다. Context Explorer는 자동 새로 고침이 되지 않으므로, 필터를 추가할 때 자동으로 적용되지 않습니다.

7단계 **Apply Filters**를 클릭합니다.

필터가 적용되고, 필터링된 데이터를 반영하여 Context Explorer가 새로 고쳐집니다.

필터를 삭제하려면

액세스: Admin/Any Security Analyst

1단계 필터 위젯에서 삭제 아이콘(✖)을 클릭합니다.

필터가 삭제됩니다.

모든 필터를 지우려면

액세스: Admin/Any Security Analyst

1단계 필터 위젯 오른쪽에 나타나는 **Clear** 버튼을 클릭합니다.

모든 필터가 지워집니다.

만든 필터가 없으면 이 버튼이 나타나지 않습니다.

컨텍스트 메뉴로 필터 만들기

라이센스: FireSIGHT

Context Explorer 그래프 및 목록 데이터를 탐색할 때 데이터 포인트를 클릭한 다음 컨텍스트 메뉴를 사용하여 해당 데이터를 기반으로 빠르게 필터를 만들 수 있습니다(포함 또는 제외). 컨텍스트 메뉴를 사용하여 데이터 유형(애플리케이션, 사용자, 침입 이벤트 메시지, 개별 호스트 등)의 정보에 대해 필터링하면 필터 위젯에는 해당 데이터 유형에 대한 관련 세부사항 페이지(예: 애플리케이션 데이터의 경우 Application Detail)로 연결되는 위젯 정보 아이콘이 포함됩니다. URL 데이터에 대해서는 필터링할 수 없습니다.

특정 그래프나 목록 데이터를 좀 더 자세히 조사하려는 경우에도 컨텍스트 메뉴를 사용할 수 있습니다. 자세한 내용은 56-39페이지의 Context Explorer 데이터에 대해 드릴다운을/를 참조하십시오.

컨텍스트 메뉴에서 필터를 만들려면

액세스: Admin/Any Security Analyst

1단계 **Analysis > Context Explorer**를 선택합니다.

Context Explorer가 나타납니다.

2단계 Traffic and Intrusion Events over Time을 제외한 Explorer 섹션 또는 URL 데이터가 포함된 섹션에서 필터링할 데이터 포인트를 클릭합니다.

컨텍스트 메뉴 팝업 창이 근처에 표시됩니다.

3단계 다음 2가지 옵션을 사용할 수 있습니다.

- 이 데이터에 대한 필터를 추가하려면 **Add Filter**를 클릭합니다.

  필터가 추가되고 왼쪽 위에 위젯이 나타납니다.

- 이 데이터에 대한 필터를 제외하려면 **Add Exclude Filter**를 클릭합니다. 필터를 적용하면 제외된 값과 관련된 데이터 **외의** 모든 데이터가 표시됩니다.

  필터가 추가되고 왼쪽 위에 위젯이 나타납니다. 제외 필터는 필터 값 앞에 느낌표를 표시합니다.

필터 세부사항을 보려면

액세스: Admin/Any Security Analyst

1단계 해당 필터 위젯에서 정보 아이콘( )을 클릭합니다.

필터의 데이터 유형과 관련된 세부사항 페이지와 함께 새 창이 열립니다.

필터를 북마크 처리

라이센스: FireSIGHT

필터는 필요한 정확한 FireSIGHT 데이터 컨텍스트를 특정 시간에 얻기 위한 간단하고 민첩한 툴 역할을 합니다. 필터의 목적은 영구적인 컨피그레이션 설정이 아니며, Context Explorer에서 빠져나가거나 세션을 종료하면 필터도 사라집니다. 그러나 조직에서 특정 필터 조합을 자주 사용할 수 있습니다. 나중에 사용할 수 있도록 필터 설정을 보관하려면 원하는 필터를 적용하여 Context Explorer의 브라우저 즐겨찾기를 만들 수 있습니다. 적용된 필터는 Context Explorer 페이지 URL에 통합되므로 해당 페이지의 즐겨찾기를 로드하면 해당 필터도 로드됩니다.

57장

보고서 작업

FireSIGHT 시스템은 방어 센터에 나타나는 대시보드 또는 이벤트 보기와 함께 다중 섹션의 보고서를 빠르고 쉽게 생성할 수 있는 유연한 보고 시스템을 제공합니다. 사용자 지정 보고서를 처음부터 디자인할 수도 있습니다. 보고 기능은 방어 센터에서만 사용할 수 있습니다.

보고서는 전달할 내용이 포함된 PDF, HTML 또는 CSV 형식의 문서 파일입니다. 보고서 템플릿은 보고서 및 보고서 섹션에 대한 데이터 검색과 형식을 지정합니다. FireSIGHT 시스템에는 보고서 템플릿의 디자인을 자동화하는 강력한 보고서 디자이너가 포함되어 있습니다. 웹 인터페이스에 표시되는 이벤트 보기 테이블 또는 대시보드 그래픽의 내용을 복제할 수 있습니다.

보고서 템플릿을 필요한 만큼 작성할 수 있습니다. 각 보고서 템플릿은 보고서의 개별 섹션을 정의하며, 보고서의 내용을 생성하는 데이터베이스 검색은 물론 표시 형식(테이블, 차트, 상세 보기 등)과 시간 프레임도 지정합니다. 템플릿은 또한 커버 페이지와 목차, 문서 페이지에 머리글과 바닥글 포함(PDF 형식의 보고서에서만 사용 가능) 여부 등의 문서 특성도 지정합니다. 단일 컨피그레이션 패키지 파일로 보고서 템플릿을 내보내고, 다른 방어 센터에서 재사용하기 위해 가져올 수 있습니다.

유용성 확장을 위해 템플릿에 입력 매개 변수를 포함할 수 있습니다. 입력 매개 변수를 사용하면 동일한 보고서를 원하는 형태로 변형할 수 있습니다. 입력 매개 변수로 보고서를 생성할 경우 생성 과정 중에 각 입력 매개 변수의 값을 입력하라는 프롬프트가 표시됩니다. 입력하는 값은 1회 기반으로 보고서 내용을 제한합니다. 예를 들면, 침입 이벤트 보고서를 생성하는 검색의 목적지 IP 필드에 입력 매개 변수를 둘 수 있습니다. 보고서 생성 시 목적지 IP 주소를 입력하라는 프롬프트가 표시될 때 부서의 네트워크 세그먼트를 지정할 수 있습니다. 그러면 생성된 보고서에는 해당 특정 부서와 관련된 정보만 포함됩니다.

보고서 및 보고서 템플릿에 대한 자세한 내용은 다음 절을 참조하십시오.

보고서 템플릿 이해

라이센스: 모두

FireSIGHT 시스템의 보고 기능을 사용하면 방어 센터에서 이벤트 보기, 대시보드 또는 워크플로의 내용을 빠르게 캡처하고 보고서 형식으로 표시할 수 있습니다. 보고서 템플릿을 사용하면 각 보고서 섹션에서 데이터의 내용과 형식을 정의하는 것은 물론, 보고서 파일의 문서 특성(커버 페이지, 목차, 페이지 머리글과 바닥글)도 정의할 수 있습니다. 보고서를 생성한 후 템플릿은 삭제될 때까지 계속 재사용 가능합니다.

보고서에는 하나 이상의 정보 섹션이 포함되어 있습니다. 각 섹션의 형식(텍스트, 테이블 또는 차트)을 개별적으로 선택합니다. 한 섹션에 대해 선택한 형식은 포함 가능한 데이터를 제한할 수 있습니다. 예를 들어 원 그래프 형식을 사용하는 특정 테이블에는 시간 기반 정보를 표시할 수 없습니다. 최적의 상태로 표시하기 위해 언제든지 섹션의 형식 또는 데이터 기준을 변경할 수 있습니다.

사전 정의된 이벤트 보기를 기반으로 보고서의 초기 디자인을 작성할 수도 있고, 정의된 대시보드, 워크플로 또는 요약에서 내용을 가져와 디자인을 시작할 수도 있습니다. 빈 템플릿 셸에서 시작하여 하나씩 섹션을 추가하고 특성을 정의할 수도 있습니다.

보고서 템플릿의 모든 섹션에는 섹션의 내용과 모양을 제어하는 제목 표시줄과 다양한 특성 필드가 있습니다. 자세한 내용은 다음을 참조하십시오.

- 보고서 섹션 제목 표시줄 요소 표
- 보고서 섹션 필드 표

다음 표에서는 각 템플릿 섹션의 제목 표시줄에 있는 컨트롤에 대해 설명합니다.

표 57-1 보고서 섹션 제목 표시줄 요소

특성	정의
섹션 제목	보고서에 나타나는 섹션의 이름을 포함합니다. 변경하려면 클릭하여 새 이름을 입력할 수 있습니다. 표시 문제가 발생하지 않도록, Report Sections 페이지에서 볼 때 긴 섹션 제목 이름은 잘려서 표시됩니다.
섹션 제목 아이콘	보고서 템플릿에 중복된 섹션을 추가하려면 중복 아이콘(+)을 클릭합니다. 섹션을 최소화하려면 최소화 아이콘(−)을 클릭합니다. 섹션을 삭제하려면 확인 후 삭제 아이콘(×)을 클릭합니다.

다음 표에서는 보고서 템플릿의 각 섹션에 있는 필드를 정의합니다.

표 57-2 보고서 섹션 필드

필드 이름	정의
표	섹션 데이터가 추출된 테이블을 선택할 수 있는 드롭다운 메뉴를 표시합니다.
프리셋	사전 정의 검색의 드롭다운 메뉴를 표시합니다. 새 검색을 정의할 때 검색 기준을 시작할 적절한 프리셋을 선택할 수 있습니다.

표 57-2 보고서 섹션 필드 (계속)

필드 이름	정의
형식	섹션 데이터의 형식을 선택할 수 있는 아이콘을 표시합니다. 옵션에는 다음이 포함됩니다. 막대 그래프: 선택한 변수의 수량을 비교합니다. 선 그래프: 선택한 변수의 시간에 따른 추세/변경 사항을 표시합니다. 시간 기반 테이블에만 사용할 수 있습니다. 원 그래프: 선택한 각 변수를 전체의 비율로서 표시합니다. 수량이 0인 변수는 차트에서 삭제됩니다. 매우 소량의 항목들은 **Other**라는 카테고리로 묶입니다. 테이블 보기: 각 레코드에 대한 특성의 값을 표시합니다. 요약 또는 통계 데이터에 사용할 수 없습니다. 세부사항 보기: 패킷(침입 이벤트의 경우) 및 호스트 프로필(호스트 이벤트의 경우) 등 특정 이벤트와 관련된 복잡한 객체 데이터를 표시합니다. Format은 해당 객체와 관련된 특정 이벤트 유형에 대해서만 사용할 수 있습니다. 요청 수가 많을 경우 출력 성능이 저하될 수 있습니다.
Search 또는 Filter	검색 또는 애플리케이션 필터의 드롭다운 메뉴를 표시합니다. 대부분의 테이블에서 사전 정의 또는 저장된 **Search**를 사용하여 보고서를 제한할 수 있습니다. 또한 수정 아이콘()을 클릭하여 새 검색을 생성할 수 있습니다. 57-17페이지의 보고서 템플릿 섹션에서 검색 작업을/를 참조하십시오. Application Statistics 테이블에 대해서는 사용자 정의 애플리케이션 **Filter**를 사용하여 보고서를 제한할 수 있습니다. 필터 생성에 대한 자세한 내용은 3-15페이지의 애플리케이션 필터 작업을/를 참조하십시오.
X-Axis	선택한 차트의 X축에 대한 사용 가능한 데이터 열의 드롭다운 메뉴를 표시합니다. 차트 형식을 선택하는 경우에만 나타납니다. 선 그래프의 경우 X축 값은 항상 **Time**입니다. 막대 및 원 그래프의 경우 X축 값으로 **Time**을 선택할 수 없습니다.
Y-Axis	선택한 차트의 Y축에 대한 사용 가능한 데이터 열의 드롭다운 메뉴를 표시합니다.
Section Description	섹션의 검색 데이터 앞에 오는 설명 텍스트를 정의합니다. 텍스트 및 입력 매개변수의 조합을 입력합니다. 새 섹션의 기본값은 두 가지 입력 매개 변수인 `$<Time Window>` 및 `$<Constraints>`의 집합입니다. 입력 매개 변수에 대한 자세한 내용은 57-18페이지의 입력 매개 변수 사용을/를 참조하십시오.
Time Window	섹션에 나타나는 데이터의 시간 창을 정의합니다. 섹션에서 시간 기반 테이블을 검색하는 경우, 보고서의 전역 시간 창을 상속하는 확인란을 선택할 수 있습니다. 또는 섹션에 대한 특정 시간 창을 설정할 수 있습니다. 시간 창 설정에 대한 자세한 내용은 57-12페이지의 보고서 템플릿의 섹션 수정을/를 참조하십시오.
결과	**Top** 또는 **Bottom**을 선택하고 섹션에 포함할 최대 레코드 수를 입력합니다.
색상	섹션에서 그래프 데이터의 색을 정의합니다. 하나 이상의 색을 적절히 선택합니다.

보고서 템플릿 생성 및 수정

라이센스: 모두

다음과 같은 방법으로 새 보고서 템플릿을 작성할 수 있습니다.

- 57-4페이지의 새 보고서 템플릿 생성
- 57-6페이지의 기존 템플릿에서 보고서 템플릿 생성
- 57-9페이지의 이벤트 보기에서 보고서 템플릿 생성
- 57-11페이지의 대시보드 또는 워크플로를 가져와서 보고서 템플릿 생성

보고서 템플릿을 수정 및 사용자 지정하려면 다음 절을 참조하십시오.

- 57-12페이지의 보고서 템플릿의 섹션 수정
- 57-17페이지의 보고서 템플릿 섹션에서 검색 작업
- 57-18페이지의 입력 매개 변수 사용
- 57-22페이지의 보고서 템플릿에서 문서 특성 수정
- 57-23페이지의 커버 페이지 사용자 지정
- 57-24페이지의 로고 관리

새 보고서 템플릿 생성

라이센스: 모두

기존 보고서 템플릿을 복사하지 않으려는 경우 완전히 새로운 템플릿을 생성할 수 있습니다. 먼저 기본 템플릿 셸을 생성합니다. 그런 다음 원하는 순서대로 개별 템플릿 섹션을 디자인하고 보고서 문서의 특성을 설정합니다. 이러한 단계에 대한 자세한 내용은 다음 절을 참조하십시오.

- 57-4페이지의 템플릿 셸 생성
- 57-5페이지의 템플릿 섹션의 내용 구성
- 57-5페이지의 PDF 및 HTML 보고서 문서의 특성 설정

템플릿 셸 생성

라이센스: 모두

보고서 템플릿은 섹션의 프레임워크이며, 각각은 자체 데이터베이스 쿼리에서 독립적으로 작성됩니다. 템플릿 생성의 첫 단계는 섹션을 추가하고 형식을 지정할 수 있는 프레임워크 셸을 생성하는 것입니다.

템플릿 셸을 생성하려면

액세스: Admin/Any Security Analyst

1단계 **Overview > Reporting**을 선택합니다.

2단계 **Report Templates** 탭을 클릭합니다.

Report Templates 페이지가 나타납니다.

3단계 **Create Report Template**을 클릭합니다.

Report Sections 페이지의 **Report Title** 필드에 기본 템플릿 이름인 `New Report`가 나타납니다.

4단계 선택적으로, **Report Title** 필드에 새 템플릿의 이름을 입력하고 **Save**를 클릭합니다. 보고서 제목에는 영숫자 문자와 공백을 사용할 수 있습니다.

새 템플릿 이름의 항목이 Report Templates 페이지 목록에 나타납니다.

5단계 보고서 제목에는 입력 매개 변수를 포함할 수도 있습니다. 입력 매개 변수를 추가하려면 매개 변수의 값이 나타나야 할 제목의 위치에 커서를 두고 입력 매개 변수 삽입( ) 아이콘을 클릭합니다.

추가된 입력 매개 변수가 **Report Title** 필드에 나타납니다. 입력 매개 변수에 대한 자세한 내용은 57-18페이지의 입력 매개 변수 사용을/를 참조하십시오.

6단계 Report Sections 제목 표시줄 아래에 있는 추가 아이콘 집합을 사용하여 필요한 만큼 섹션 셀을 삽입합니다. 섹션 서식 지정에 대한 자세한 내용은 보고서 섹션 필드 표를 참조하십시오.

추가된 각 섹션은 템플릿 아래쪽에 나타납니다. 올바른 위치로 끌어옵니다.

7단계 섹션 제목 표시줄에서 섹션 제목을 클릭하고 섹션의 이름을 입력합니다(최대 120자 사용).

8단계 **Save**를 클릭하여 템플릿을 저장합니다.

템플릿이 저장됩니다.

템플릿 섹션의 내용 구성

라이센스: 모두

각 템플릿 섹션은 검색 또는 필터에 의해 생성된 데이터 집합으로 구성되며, 표시 모드를 결정하는 형식 사양(테이블, 원 그래프 등)을 가지고 있습니다. 출력에 포함하려는 데이터 레코드의 필드 및 표시할 레코드의 시간 프레임과 수를 선택하여 섹션 내용을 더 자세히 지정할 수 있습니다.

보고서 템플릿 섹션을 구성하려면

액세스: Admin/Any Security Analyst

1단계 57-12페이지의 보고서 템플릿의 섹션 수정에 설명된 대로 섹션 특성을 수정합니다.

2단계 선택적으로, 선택한 그래픽 형식 또는 열 레이아웃을 보려면 섹션 창 아래에 있는 **Preview**를 클릭합니다.

참고 원 그래프 색상 등 출력 특성과 열 선택을 확인하려면 섹션 미리 보기 유틸리티를 사용할 수 있지만, 구성한 검색의 정확성이 신뢰할 수 있는 수준으로 표시되지는 않습니다.

PDF 및 HTML 보고서 문서의 특성 설정

라이센스: 모두

템플릿에서 생성하는 보고서에는 커버 페이지, 머리글과 바닥글, 페이지 번호 지정 등 모든 섹션 및 제어 기능에 해당하는 몇 가지 문서 특성이 있습니다.

보고서 문서의 특성을 설정하려면

액세스: Admin/Any Security Analyst

1단계 **Overview > Reporting**을 선택합니다.

2단계 **Report Templates** 탭을 클릭합니다.

Report Templates 페이지가 나타납니다.

3단계 보고서 생성을 위해 사용하려는 보고서 템플릿에 대한 **Edit**를 클릭합니다.

템플릿의 Report Sections 페이지가 나타납니다.

4단계 **Advanced**를 클릭합니다.

Advanced Settings 팝업 창이 나타납니다.

5단계 PDF 또는 HTML 형식의 문서에 대해 57-22페이지의 보고서 템플릿에서 문서 특성 수정에 설명된 작업을 수행합니다.

문서 형식으로 CSV를 선택한 경우에는 설정할 문서 특성이 없습니다.

기존 템플릿에서 보고서 템플릿 생성

라이센스: 모두

기존 템플릿 중에서 좋은 모델을 찾은 경우 해당 템플릿을 복사하고 특성을 수정하여 새 보고서 템플릿을 생성할 수 있습니다. Cisco에서는 또한 사전 정의 보고서 템플릿 집합을 제공하며, 템플릿 목록의 **Reports Tab**에 표시됩니다. 특성에 대한 설명은 57-7페이지의 사전 정의 보고서 템플릿 사용을/를 참조하십시오.

기존 템플릿에서 보고서 템플릿을 생성하려면

액세스: Admin/Any Security Analyst

1단계 **Overview > Reporting**을 선택합니다.

2단계 **Report Templates** 탭을 클릭합니다.

Report Templates 페이지가 나타납니다. Cisco 제공 보고서 템플릿에 대한 자세한 내용은 57-7페이지의 사전 정의 보고서 템플릿 사용을/를 참조하십시오.

3단계 모델로서 복사할 보고서 템플릿 옆에 있는 복사 아이콘( )을 클릭합니다.

복사된 템플릿이 새 보고서 템플릿으로 나타납니다.

4단계 **Report Title** 필드에 새 보고서 템플릿의 이름을 입력합니다.

5단계 **Save**를 클릭합니다.

보고서 템플릿이 저장되고 새 보고서 템플릿에 대한 항목이 Report Templates 페이지에 나타납니다.

6단계 필요한 대로 템플릿을 변경합니다.

템플릿의 섹션 및 문서 특성 정의에 대한 자세한 내용은 다음을 참조하십시오.

- 57-12페이지의 보고서 템플릿의 섹션 수정
- 57-22페이지의 보고서 템플릿에서 문서 특성 수정

사전 정의 보고서 템플릿 사용

라이센스: 모두

다음의 사전 정의 보고서 템플릿을 있는 그대로 사용할 수도 있고 수정할 수도 있으며, 이를 기반으로 고유한 템플릿을 만들 수도 있습니다.

- Host Report: $<Host>
- User Report: $<User>
- Attack Report: Attack $<Attack SID>
- Malware Report
- FireSIGHT Report: $<Customer Name>
- Files Report

Host Report: $<Host>

Host Report: $<Host> 보고서 템플릿은 네트워크에 있는 특정 호스트에 대한 정보를 제공합니다. 이 보고서 템플릿에는 다음 섹션이 포함되어 있습니다.

- Server Applications
- Client Applications
- Intrusion Events Originating from This Host
- Intrusion Events Destined to This Host
- Connections Originating from This Host
- Connections Destined to This Host
- Users of This Host
- White List Violations by This Host

User Report: $<User>

User Report: $<User> 보고서 템플릿은 네트워크에 있는 특정 사용자에 대한 정보를 제공합니다. 이 보고서 템플릿에는 다음 섹션이 포함되어 있습니다.

- Client Applications Used by This User
- Web Applications Used by This User
- Application Protocols Used by This User
- Comprehensive List of Applications Used by This User
- Intrusion Events Originated By This User's Machines
- Intrusion Events Destined to This User's Machines
- Connections Originating from This User's Machines
- Connections Destined to This User's Machines
- Hosts for This User

Attack Report: Attack $<Attack SID>

Attack Report: Attack $<Attack SID> 보고서 템플릿은 네트워크에 있는 특정 공격에 대한 정보를 제공합니다. 이 보고서 템플릿에는 다음 섹션이 포함되어 있습니다.

- General Information About This Attack
- Number of Attacks
- Number of Machines Initiating Attack
- Number of Machines Being Attacked
- Sources of This Attack
- Destinations of This Attack
- Traffic Patterns of This Attack

Malware Report

Malware Report 보고서 템플릿은 네트워크 및 엔드포인트 기반 악성코드 이벤트에 대한 정보를 제공합니다. 이 보고서 템플릿에는 다음 섹션이 포함되어 있습니다.

- Malware Threats
- Threat Detections over Time
- Application Protocols Transferring Malware
- Hosts Receiving Malware
- Hosts Sending Malware
- Users Affected by Malware
- Malware Intrusions
- File Types Infected with Malware
- Applications Introducing Malware
- Table View of Malware Events

Series 2 디바이스 및 DC500 방어 센터는 네트워크 기반 악성코드 차단을 지원하지 않으며, 이는 탐지 및 표시되는 데이터에 영향을 미칠 수 있습니다. Series 2 디바이스만 관리하는 Series 3 방어 센터는 엔드포인트 기반 악성코드 이벤트만 표시할 수 있습니다.

FireSIGHT Report: $<Customer Name>

FireSIGHT Report: $<Customer Name> 보고서 템플릿은 조직의 네트워크에 대한 전반적인 정보를 제공합니다. 이 보고서 템플릿에는 다음 섹션이 포함되어 있습니다.

- Summary of Application Traffic by Risk
- Risky Applications with Low Business Relevance
- Users of Risky Applications
- Anonymizers and Proxies
- Typically High Bandwidth Applications
- Applications by Total Bandwidth
- Hosts Accessing Sensitive Network
- Users Accessing Sensitive Network
- Applications on Sensitive Network

- Ports and Protocols Related to Sensitive Network
- Hosts Visiting Malicious URLs
- Users Visiting Malicious URLs
- Granular Application Usage
- Web Applications
- Client Applications
- Application Protocols
- Web Browser Versions
- Operating System Versions
- Overall User Activity
- Intrusion Events by Impact
- Intrusion Events by Impact (After Blocking)
- Intrusion Events by Application
- Top Intrusion Events
- Comprehensive Application List

Files Report

Files Report 보고서 템플릿은 관리되는 디바이스가 네트워크 트래픽에서 탐지하는 파일에 대한 정보를 제공합니다. 이 보고서 템플릿에는 다음 섹션이 포함되어 있습니다.

- File Transfers over Time
- Application Protocols Used by File Transfers
- File Dispositions
- File Actions
- Hosts Receiving Files
- Hosts Sending Files
- Users Transferring Files
- File Categories
- File Types
- File Names
- Table View of File Events

이벤트 보기에서 보고서 템플릿 생성

라이센스: 모두

보고서를 생성하기 전에 보고 시스템은 요구에 맞게 수정할 수 있는 보고서 템플릿을 생성합니다. 섹션을 더 추가하고, 포함된 섹션을 자동으로 수정하고, 섹션을 삭제할 수 있습니다.

이벤트 보기에서 보고서 템플릿을 생성하려면

액세스: Admin/Any Security Analyst

1단계 보고서에서 원하는 이벤트와 함께 이벤트 보기를 채웁니다. 다음과 같은 다양한 방법으로 수행할 수 있습니다.

- 이벤트 검색을 사용하여 보려는 이벤트를 정의합니다. 이벤트 검색에 대한 자세한 내용은 60-1페이지의 이벤트 검색을/를 참조하십시오.
- 이벤트 보기에 적절한 이벤트가 표시될 때까지 워크플로에서 드릴다운합니다. 워크플로 및 워크플로 내에서 이벤트를 제한하는 방법에 대한 자세한 내용은 58-1페이지의 워크플로의 이해 및 사용을/를 참조하십시오.

2단계 이벤트 보기 페이지에서 **Report Designer**를 클릭합니다.

캡처한 워크플로의 각 보기에 대한 섹션과 함께 Report Sections 페이지가 나타납니다.

3단계 선택적으로, **Report Title** 필드에 새 이름을 입력하고 **Save**를 클릭합니다.

4단계 선택적으로, 섹션 제목 표시줄의 삭제 아이콘(✖)을 클릭하고 삭제를 확인하여 보고서에서 제외할 템플릿 섹션을 삭제합니다.

삭제된 섹션이 사라집니다.

참고 일부 워크플로의 마지막 보고서 섹션에는 워크플로에 따라 패킷, 호스트 프로필 또는 취약성을 보여주는 세부사항 보기가 포함됩니다. 보고서를 생성할 때 이러한 세부사항 보기가 있는 다수의 이벤트를 검색하면 방어 센터의 성능이 저하될 수 있습니다.

5단계 선택적으로, 보고서 섹션에서 필드의 설정을 조정합니다.

보고서 섹션의 필드 구성에 대한 자세한 내용은 57-12페이지의 보고서 템플릿의 섹션 수정을/를 참조하십시오.

팁 섹션의 현재 열 레이아웃 또는 차트 형식을 보려면 해당 섹션의 **Preview** 링크를 클릭하십시오.

6단계 선택적으로, 제목 표시줄의 섹션 제목을 클릭하여 섹션의 제목을 변경합니다.

Set Section Title 팝업 창이 나타납니다. 섹션 제목을 입력하고 **OK**를 클릭합니다.

7단계 선택적으로, 페이지 나누기를 추가합니다. 페이지 나누기 추가 아이콘()을 클릭합니다.

템플릿의 아래쪽에 새로운 페이지 나누기 객체가 나타납니다. 이 객체를 새 페이지가 시작될 섹션 앞으로 끌어옵니다. 페이지 나누기의 사용에 대한 자세한 내용은 57-12페이지의 보고서 템플릿의 섹션 수정을/를 참조하십시오.

8단계 선택적으로, 텍스트 섹션을 추가합니다. 텍스트 섹션 추가 아이콘()을 클릭합니다.

템플릿의 아래쪽에 새로운 텍스트 섹션이 나타납니다. 이것을 보고서 템플릿이 나타나야 할 위치로 끌어옵니다. 텍스트 섹션 수정에 대한 자세한 내용은 57-12페이지의 보고서 템플릿의 섹션 수정을/를 참조하십시오.

팁 풍부한 텍스트(굵게, 기울임, 가변 글꼴 크기 등)는 물론 가져온 이미지도 지원하는 텍스트 섹션은 보고서 또는 보고서 섹션에 대한 소개에 유용합니다.

9단계 선택적으로, 커버 페이지, 목차, 시작 페이지 번호 또는 머리글과 바닥글 텍스트를 추가하려면 **Advanced Settings**를 클릭합니다. 자세한 내용은 57-22페이지의 보고서 템플릿에서 문서 특성 수정을/를 참조하십시오.

10단계 보고서 템플릿이 올바르면 **Save**를 클릭합니다.

보고서 템플릿이 저장되고 보고서 템플릿에 대한 항목이 Report Templates 페이지에 나타납니다.

대시보드 또는 워크플로를 가져와서 보고서 템플릿 생성

라이센스: 모두

대시보드, 워크플로 및 통계 요약을 가져와서 새 보고서를 빠르게 생성할 수 있습니다. 가져오기를 수행하면 대시보드 및 워크플로의 각 이벤트 보기에 각 위젯 그래픽에 대한 섹션이 생성됩니다. 가장 중요한 정보에 집중할 수 있도록 불필요한 섹션을 모두 삭제할 수 있습니다. 다음 표에서는 가져오기 옵션에 대해 설명합니다.

표 57-3 Import Report Sections 창의 데이터 소스 옵션

선택 옵션	가져오기
Import Dashboard	선택한 대시보드의 사용자 지정 분석 위젯.
Import Workflow	사전 정의 또는 사용자 지정 워크플로. **팁** 선택 형식은 다음과 같습니다. `Table - Workflow name` 예를 들어 `Connection Events - Traffic by Port`는 Connection Events 테이블에서 생성된 Traffic by Port 워크플로의 보기를 가져옵니다.
Import Summary Sections	다음과 같은 일반 요약 중 하나: • Intrusion Detailed Summary • Intrusion Short Summary • Discovery Detailed Summary • Discovery Short Summary

대시보드, 워크플로 또는 통계 요약에서 보고서 템플릿을 생성하려면

액세스: Admin/Any Security Analyst

1단계 보고서에서 복제할 대시보드, 워크플로 또는 요약을 식별합니다.

2단계 **Overview > Reporting**을 선택합니다.

3단계 **Report Templates** 탭을 클릭합니다.

Report Templates 페이지가 나타납니다.

4단계 **Create Report Template**을 클릭합니다.

Report Sections 페이지가 나타납니다.

5단계 **Report Title** 필드에 새 보고서 템플릿의 이름을 입력합니다.

6단계 **Save**를 클릭하여 새 이름으로 보고서 템플릿을 저장합니다.

보고서 템플릿이 저장되고 보고서 템플릿에 대한 항목이 Report Templates 페이지에 나타납니다.

7단계 대시보드, 요약 및 워크플로에서 섹션 가져오기 아이콘()을 클릭합니다.

Import Report Sections 팝업 창이 나타납니다. Import Report Sections 창의 데이터 소스 옵션 표에 설명된 데이터 소스 중 하나를 선택할 수 있습니다.

8단계 드롭다운 메뉴에서 대시보드, 워크플로 또는 요약을 선택합니다.

9단계 추가할 데이터 소스에 대해 **Import**를 클릭합니다.

선택한 데이터 소스의 각 요소에 대한 섹션과 함께 템플릿의 Report Sections 페이지가 다시 나타납니다. 대시보드의 경우 각 위젯 그래픽이 자체 섹션을 가지며, 워크플로의 경우 각 이벤트 보기가 자체 섹션을 가집니다.

10단계 필요한 대로 섹션의 내용을 변경합니다.

보고서 템플릿 수정에 대한 자세한 내용은 57-12페이지의 보고서 템플릿의 섹션 수정을/를 참조하십시오.

참고 일부 워크플로의 마지막 보고서 섹션에는 워크플로에 따라 패킷, 호스트 프로필 또는 취약성을 보여주는 세부사항 보기가 포함됩니다. 보고서를 생성할 때 이러한 세부사항 보기가 있는 다수의 이벤트를 검색하면 방어 센터의 성능이 저하될 수 있습니다.

11단계 보고서 템플릿이 올바르면 **Save**를 클릭합니다.

보고서 템플릿이 저장되고 보고서 템플릿에 대한 항목이 Report Templates 페이지에 나타납니다.

보고서 템플릿의 섹션 수정

라이센스: 모두

다양한 보고서 섹션 특성을 수정하여, 섹션의 내용과 해당 데이터 표시 방식을 조정할 수 있습니다. 자세한 내용은 다음 절을 참조하십시오.

- 57-13페이지의 템플릿 섹션에 대한 테이블 및 데이터 형식 설정
- 57-13페이지의 템플릿 섹션에 대해 검색 또는 필터 지정
- 57-14페이지의 테이블 형식 섹션에 나타나는 검색 필드 설정
- 57-14페이지의 보고서 템플릿에 텍스트 섹션 추가
- 57-15페이지의 보고서 템플릿에 페이지 나누기 추가
- 57-15페이지의 템플릿 및 섹션에 대한 시간 창 설정
- 57-16페이지의 템플릿 섹션 이름 변경
- 57-17페이지의 템플릿 섹션 미리 보기

참고 보안 분석가는 자신이 생성한 보고서 템플릿만 수정할 수 있습니다.

템플릿 섹션에 대한 테이블 및 데이터 형식 설정

라이센스: 모두

보고서 템플릿의 각 섹션은 데이터베이스 테이블을 쿼리하여 해당 섹션의 내용을 생성합니다. 섹션의 데이터 형식을 변경할 경우 동일한 데이터 쿼리가 사용되지만, 형식 유형의 분석 목적에 따라 섹션에 나타나는 필드가 수정됩니다. 예를 들어, 침입 이벤트의 테이블 보기는 이벤트 레코드당 다수의 데이터 필드로 섹션을 채우는 반면, 원 그래프 섹션에는 개별 이벤트에 대한 세부사항 없이 선택한 각 특성이 나타내는 모든 일치하는 레코드의 일부가 표시됩니다. 막대 그래프는 특정 특성이 있는 일치하는 레코드의 총수를 비교합니다. 선 그래프는 단일 특성을 기준으로 일치하는 레코드의 시간에 따른 변경 사항을 요약합니다. 선 그래프는 시간 기반의 데이터에만 사용할 수 있으며 호스트, 사용자, 서드파티 취약성 등에 대한 정보에는 사용할 수 없습니다.

사용 가능한 여러 형식에 대한 자세한 내용은 보고서 섹션 필드 표를 참조하십시오.

템플릿 섹션에 대한 테이블 및 출력 형식을 선택하려면

액세스: Admin/Any Security Analyst

1단계 **Table** 드롭다운 메뉴를 사용하여 이 섹션에서 쿼리할 테이블을 선택합니다.

선택한 테이블에 대해 사용 가능한 출력 형식 각각에 대한 **Format** 필드에 아이콘이 나타납니다.

2단계 섹션에 해당하는 출력 형식 아이콘을 선택합니다. 이러한 형식에 대한 자세한 내용은 보고서 섹션 제목 표시줄 요소 표를 참조하십시오.

출력에 포함된 필드가 나타납니다.

3단계 검색 제약 조건을 변경하려면 **Search** 또는 **Filter** 필드 옆에 있는 수정 아이콘( )을 클릭합니다.

검색을 제한하기 위한 옵션과 함께 Search Editor 팝업 창이 나타납니다. 이 창의 사용에 대한 자세한 내용은 57-17페이지의 보고서 템플릿 섹션에서 검색 작업을/를 참조하십시오.

4단계 그래픽 출력 형식(원 그래프, 막대 그래프 등)에 대해 드롭다운 메뉴를 사용하여 **X-Axis** 및 **Y-Axis** 매개 변수를 조정합니다.

X축에 대한 값을 선택하면 호환되는 값만 Y축 드롭다운 메뉴에 나타나고, 그 반대의 경우도 마찬가지입니다.

5단계 테이블 출력에서는 열, 나타나는 순서 및 출력의 정렬 순서를 선택합니다. 자세한 내용은 57-14페이지의 테이블 형식 섹션에 나타나는 검색 필드 설정을/를 참조하십시오.

6단계 **Save**를 클릭하여 템플릿을 저장합니다.

템플릿이 저장됩니다.

템플릿 섹션에 대해 검색 또는 필터 지정

라이센스: 모두

보고서 섹션의 검색 또는 필터는 섹션 내용의 기반이 되는 데이터베이스 쿼리를 지정합니다. 대부분의 테이블에서 사전 정의 검색 또는 저장된 검색을 사용하여 보고서를 제한하거나, 즉석에서 새 검색을 생성할 수 있습니다.

- 특정 이벤트 테이블 검색을 위한 예제 역할을 하는 사전 정의 검색을 사용하면 보고서에 포함할 수 있는 네트워크에 대한 중요한 정보에 빠르게 액세스할 수 있습니다.
- 저장된 이벤트에는 자신이나 타인이 생성한 모든 공개 이벤트 검색은 물론, 자신이 저장한 모든 비공개 이벤트 검색도 포함됩니다. 저장된 이벤트 검색의 정의, 이름 지정 및 사용에 대한 자세한 내용은 60-1페이지의 이벤트 검색을/를 참조하십시오.

- 현재 보고서 템플릿에 대해 저장된 검색은 보고서 템플릿 자체에서만 액세스 가능합니다. 저장된 보고서 템플릿 검색의 검색 이름은 "Custom Search" 문자열로 끝납니다. 사용자는 보고서 디자인 중에 이러한 검색을 생성합니다.

Application Statistics 테이블에 대해서는 사용자 정의 애플리케이션 Filter를 사용하여 보고서를 제한할 수 있습니다. 필터 생성에 대한 자세한 내용은 3-15페이지의 애플리케이션 필터 작업을/를 참조하십시오.

템플릿 섹션에 대한 검색 또는 필터를 지정하려면

액세스: Admin/Any Security Analyst

1단계 쿼리할 데이터베이스 테이블을 **Table** 드롭다운 메뉴에서 선택합니다.

- 대부분의 테이블에 대해 **Search** 드롭다운 목록이 나타납니다.
- Application Statistics 테이블의 경우 **Filter** 드롭다운 목록이 나타납니다.

2단계 보고서를 제한하기 위해 사용할 검색 또는 필터를 선택합니다.

검색 기준을 볼 수도 있고 수정 아이콘을 클릭하여( ) 새 검색을 생성할 수도 있습니다. 자세한 내용은 57-17페이지의 보고서 템플릿 섹션에서 검색 작업을/를 참조하십시오.

테이블 형식 섹션에 나타나는 검색 필드 설정

라이센스: 모두

섹션에 테이블 데이터를 포함하는 경우 데이터 레코드에 어떤 필드를 표시할지를 선택할 수 있습니다. 테이블의 모든 필드를 포함하거나 제외할 수 있습니다. 보고서 목적을 달성하는 필드를 선택한 다음 적절히 순서를 지정하고 정렬합니다.

테이블 형식 섹션에서 필드를 추가 및 삭제하려면

액세스: Admin/Any Security Analyst

1단계 테이블 형식 섹션에서 **Fields** 매개 변수 옆에 있는 수정 아이콘( )을 클릭합니다.

Table Field Selector 창이 나타납니다.

2단계 선택적으로, 필드를 추가 및 삭제하고 필드 아이콘을 원하는 열 순서로 끌어옵니다.

3단계 선택적으로, 열의 정렬 순서를 변경합니다. 각 필드 아이콘의 드롭다운 목록을 사용하여 정렬 순서 및 우선순위를 설정합니다.

4단계 필드의 순서가 바르고 필드에 필요한 정렬 특성이 있으면 **OK**를 클릭합니다.

Report Sections 페이지가 나타납니다.

보고서 템플릿에 텍스트 섹션 추가

라이센스: 모두

전체 보고서 또는 개별 섹션에 대해 사용자 지정 텍스트(예: 소개)를 제공하려면 템플릿에 텍스트 섹션을 추가할 수 있습니다. 텍스트 섹션에서는 여러 글꼴 크기와 스타일(굵게, 기울임 등)의 풍부한 텍스트는 물론 입력 매개 변수와 가져온 이미지도 사용할 수 있습니다. 입력 매개 변수에 대한 자세한 내용은 57-18페이지의 입력 매개 변수 사용을/를 참조하십시오.

보고서 템플릿에 텍스트 섹션을 추가하려면

액세스: Admin/Any Security Analyst

1단계 텍스트 섹션 추가 아이콘( )을 클릭합니다.

템플릿의 아래쪽에 텍스트 섹션이 나타납니다.

2단계 보고서 템플릿의 원하는 위치로 새 텍스트 섹션을 끌어옵니다.

3단계 선택적으로, 텍스트 섹션 앞뒤에 페이지 나누기를 추가할 수 있습니다. 페이지 나누기에 대한 자세한 내용은 57-15페이지의 보고서 템플릿에 페이지 나누기 추가을/를 참조하십시오.

4단계 선택적으로, 새 이름을 입력하려면 제목 표시줄에서 텍스트 섹션의 일반 이름을 클릭합니다.

5단계 텍스트 섹션의 본문에 서식이 지정된 텍스트와 이미지를 추가합니다. 보고서를 생성할 때 동적으로 업데이트되는 입력 매개 변수를 포함할 수 있습니다.

6단계 완료 시 **Save**를 클릭합니다.

템플릿이 저장됩니다.

보고서 템플릿에 페이지 나누기 추가

라이센스: 모두

템플릿의 섹션 전후에 페이지 나누기를 추가할 수 있습니다. 이 기능은 다양한 섹션을 소개하는 텍스트 페이지가 있는 다중 섹션 보고서에서 특히 유용합니다.

페이지 나누기를 추가하려면

액세스: Admin/Any Security Analyst

1단계 페이지 나누기 추가 아이콘( )을 클릭합니다.

템플릿의 아래쪽에 페이지 나누기가 나타납니다.

2단계 페이지 나누기를 섹션 전후의 원하는 위치로 끌어옵니다.

3단계 템플릿에 추가하는 모든 페이지 나누기에 대해 이 프로세스를 반복합니다.

템플릿 및 섹션에 대한 시간 창 설정

라이센스: 모두

보고서 템플릿의 시간 창은 템플릿의 보고 기간을 정의합니다. 시간 기반 데이터(예: 침입 또는 검색 이벤트)가 포함된 보고서 템플릿에는 전역 시간 창이 있으며, 템플릿의 시간 기반 섹션은 생성될 때 기본적으로 이를 상속합니다. 전역 시간 창을 변경하면 전역 시간 창을 상속하도록 구성된 섹션에 대한 로컬 시간 창이 변경됩니다. **Inherit Time Window** 확인란의 선택을 취소하여 개별 섹션에 대해 시간 창 상속을 비활성화할 수 있습니다. 그런 다음 로컬 시간 창을 수정할 수 있습니다.

참고 전역 시간 창 상속은 시간 기반 테이블의 데이터(예: 침입 이벤트 및 검색 이벤트)와 함께 보고서 섹션에만 적용됩니다. 네트워크 자산(호스트와 디바이스) 및 관련 정보(예: 취약성)에 대해 보고하는 섹션의 경우 각 시간 창을 개별적으로 설정해야 합니다.

보고서 템플릿의 전역 시간 창을 변경하려면

액세스: Admin/Any Security Analyst

1단계 Report Templates 페이지에서 수정할 보고서 템플릿 옆에 있는 수정 아이콘( )을 클릭합니다.

Report Sections 페이지가 나타납니다.

2단계 **Generate**를 클릭합니다.

Generate Report 팝업 창이 나타납니다.

3단계 전역 시간 창을 수정하려면 시간 창 아이콘( )을 클릭합니다.

Events Time Window 페이지가 새 창에 나타납니다. 이 페이지의 사용에 대한 자세한 내용은 58-22 페이지의 이벤트 시간 제약 조건 설정을/를 참조하십시오.

4단계 완료되면 Events Time Window에서 **Apply**를 클릭합니다.

Generate Report 팝업 창이 새로운 시간 창과 함께 다시 나타납니다.

5단계 **Cancel**을 클릭하여 Report Sections 페이지로 돌아가거나 **OK**를 클릭하여 보고서를 생성합니다.

보고서에서 섹션마다 다른 시간 범위를 사용할 수 있습니다. 예를 들어 첫 번째 섹션에는 월 요약을 포함하고, 나머지 섹션에는 각 주의 세부사항을 포함할 수 있습니다. 이 경우 섹션 레벨 시간 창을 개별적으로 설정합니다.

섹션의 로컬 시간 창을 구성하려면

액세스: Admin/Any Security Analyst

1단계 템플릿의 Report Sections 페이지에서 섹션에 대한 **Inherit Time Window** 확인란(있는 경우)의 선택을 취소합니다.

로컬 섹션 시간 창 아이콘이 나타납니다.

2단계 섹션의 로컬 시간 창을 변경하려면 시간 창 아이콘( )을 클릭합니다.

Events Time Window 페이지가 나타납니다. 이 페이지의 사용에 대한 자세한 내용은 58-22페이지의 이벤트 시간 제약 조건 설정을/를 참조하십시오.

참고 통계 테이블의 데이터가 있는 섹션에는 슬라이딩 시간 창만 포함할 수 있습니다.

3단계 새 로컬 시간 창을 설정한 경우 Events Time Window에서 **Apply**를 클릭합니다.

4단계 **Save**를 클릭합니다.

더 수정할 수 있도록 Report Sections 페이지가 나타납니다.

템플릿 섹션 이름 변경

라이센스: 모두

새 템플릿을 생성할 때 사용자가 추가하는 섹션에는 일반 섹션 이름이 지정되며, 내용을 나타내려면 이름을 변경해야 합니다.

템플릿 섹션의 이름을 변경하려면

액세스: Admin/Any Security Analyst

1단계 섹션 헤더에 있는 현재 섹션 이름을 클릭합니다.

Set Section Title 팝업 창이 나타납니다.

2단계 섹션의 새 이름을 입력하고(최대 120자) **OK**를 클릭합니다.

섹션 제목 표시줄의 이름이 변경됩니다.

템플릿 섹션 미리 보기

라이센스: 모두

미리 보기 기능은 테이블 보기의 필드 레이아웃과 정렬 순서, 그리고 원 그래프 색상과 같은 그래픽의 중요한 가독성 특성을 보여줍니다.

템플릿 섹션을 미리 보려면

액세스: Admin/Any Security Analyst

1단계 섹션을 수정하는 동안 언제든지 섹션에 대한 **Preview**를 클릭합니다.

Preview 팝업 창이 나타납니다.

2단계 창 아래쪽에 있는 **OK**를 클릭하여 미리 보기를 닫습니다.

Report Sections 페이지가 나타납니다.

보고서 템플릿 섹션에서 검색 작업

라이센스: 모두

성공적인 보고서 생성의 핵심은 보고서 섹션을 채우는 검색을 정의하는 것입니다. FireSIGHT 시스템에서는 보고서 템플릿에서 사용할 수 있는 검색을 보고 새 사용자 지정 검색을 정의하기 위한 검색 편집기를 제공합니다.

팁 보고서 템플릿에서 생성하는 사용자 지정 검색은 해당 템플릿에만 적용됩니다. 이벤트 뷰어에서는 모든 보고서 템플릿에서 재사용할 수 있는 검색을 생성할 수 있습니다. 이벤트 뷰어에서 사용자 지정 검색을 저장하면 해당 검색은 모든 보고서 템플릿의 **Search** 드롭다운 메뉴에 나타납니다. 이벤트 뷰어를 사용하여 사용자 지정 검색을 생성하고 저장하는 방법에 대한 자세한 내용은 60-1페이지의 이벤트 검색을/를 참조하십시오.

사용자 지정 검색을 생성하려면

액세스: Admin/Any Security Analyst

1단계 보고서 템플릿의 관련 섹션에서 **Search** 필드 옆에 있는 수정 아이콘( )을 클릭합니다.

선택 항목을 검색할 수 있는 테이블과 함께 Search Editor 페이지가 나타납니다.

2단계 선택적으로, **Saved Searches** 드롭다운 메뉴에서 사전 정의 검색을 선택합니다.

드롭다운 메뉴에는 해당 테이블에 대해 사용할 수 있는 모든 사전 정의 검색(시스템 전체에 또는 특정 보고서에만 적용되는 검색 포함)이 나열됩니다.

3단계 해당 필드에서 검색 기준을 수정합니다. 특정 필드에서는 제약 조건으로 이벤트 검색과 동일한 연산자(<, <> 등)를 포함할 수 있습니다. 검색 기준의 구문은 60-1페이지의 이벤트 검색을/를 참조하십시오.

여러 기준을 입력하면 모든 기준과 일치하는 레코드만 반환됩니다.

4단계 선택적으로, 입력 매개 변수 아이콘( )이 나타나는 경우 제약 조건 값을 입력하는 대신 드롭다운 메뉴에서 입력 매개 변수를 삽입할 수 있습니다. 보고서 디자인에서 입력 매개 변수를 사용하는 방법에 대한 자세한 내용은 57-18페이지의 입력 매개 변수 사용을/를 참조하십시오.

일부 검색 필드의 경우 드롭다운 메뉴에 입력 매개 변수 대신 사용자 정의 관리되는 객체가 포함될 수 있습니다. 유형별로 다른 아이콘을 가지고 있는 관리되는 객체는 검색을 제한하기 위한 값으로 사용할 수 있는 시스템 컨피그레이션 변수입니다. 그러나 이러한 객체는 입력 매개 변수와 함께 발생하는 사용자 입력에 대한 생성 시간 쿼리를 만들지 않습니다. 관리되는 객체에 대한 자세한 내용은 3-1페이지의 재사용 가능 객체 관리을/를 참조하십시오.

참고 보고 검색의 제약 조건을 수정하면 시스템은 수정된 검색을 *section* `custom search` 이름으로 저장합니다. 여기서 *section*은 섹션 제목 표시줄의 이름이며, 그 뒤에 `custom search` 문자열이 옵니다. 저장된 사용자 지정 검색에 대해 의미 있는 이름을 지정하려면 수정된 검색을 저장하기 전에 섹션 이름을 변경해야 합니다. 저장된 보고 검색의 이름은 변경할 수 없습니다.

5단계 검색 편집기에서 필드 수정을 완료했으면 **OK**를 클릭합니다.

Report Sections 페이지가 다시 나타나고, 섹션의 **Search** 드롭다운 메뉴에 새로운 사전 정의 검색이 나타납니다.

입력 매개 변수 사용

라이센스: 모두

생성 시 보고서가 동적으로 업데이트할 수 있는 입력 매개 변수를 보고서 템플릿에서 사용할 수 있습니다. 입력 매개 변수 아이콘( )은 처리 가능한 필드를 나타냅니다. 두 가지 종류의 입력 매개 변수가 있습니다.

- 사전 정의 - 사전 정의 입력 매개 변수 표 참조
- 사용자 정의 - 사용자 정의 입력 매개 변수 유형 표 참조

사전 정의 입력 매개 변수

라이센스: 모두

사전 정의 입력 매개 변수는 내부 시스템 함수 또는 컨피그레이션 정보에 의해 확인됩니다. 예를 들어, 보고서 생성 시 시스템은 `$<Time>` 매개 변수를 현재 날짜 및 시간과 교체합니다. 다음 표에서는 사용 가능한 매개 변수를 정의합니다. 예를 들어, 스케줄러 컨트롤에 의해 자동으로 생성되는 월 요약 보고서의 제목에 `$<Month>`를 포함할 수 있습니다. 그러면 보고서 제목이 현재 월로 자동으로 업데이트됩니다.

표 57-4 사전 정의 입력 매개 변수

삽입할 매개 변수	템플릿에 포함할 정보
$<Logo>	선택한 업로드된 로고
$<Report Title>	보고서 제목
$<Time>	보고서가 실행된 날짜와 시간(1초 단위)
$<Month>	현재 월
$<Year>	현재 연도
$<System Name>	방어 센터의 이름
$<Model Number>	방어 센터의 모델 번호
$<Time Window>	현재 보고서 섹션에 적용된 시간 창
$<Constraints>	현재 보고서 섹션에 적용된 검색 제약 조건

다음 표에는 Report Templates 페이지의 여러 곳에서 사용할 수 있는 유효한 입력 매개 변수가 나열되어 있습니다.

표 57-5 사전 정의 입력 매개 변수 사용법

매개변수	보고서 템플릿 커버 페이지	보고서 템플릿 보고서 제목	보고서 템플릿 섹션 설명	보고서 템플릿 텍스트 섹션	보고서 파일 이름 생성	보고서 이메일 제목, 본문 생성
$<Logo>	예	아니요	아니요	아니요	아니요	아니요
$<Report Title>	예	아니요	예	예	예	예
$<Time>	예	예	예	예	예	예
$<Month>	예	예	예	예	예	예
$<Year>	예	예	예	예	예	예
$<System Name>	예	예	예	예	예	예
$<Model Number>	예	예	예	예	예	예
$<Time Window>	아니요	아니요	예	아니요	아니요	아니요
$<Constraints>	아니요	아니요	예	아니요	아니요	아니요

사용자 정의 입력 매개 변수

라이센스: 모두

섹션 검색에서 제약 조건으로 제공할 자체 입력 매개 변수를 생성할 수 있습니다. 입력 매개 변수로 검색을 제약하면 시스템은 보고서를 요청하는 사용자의 생성 시간에 값을 수집합니다. 이렇게 하면 템플릿을 변경하지 않고도 데이터의 특별한 일부를 표시하도록 생성 시 보고서를 동적으로 맞춤화할 수 있습니다. 예를 들어 보고서 섹션 검색의 **Destination IP** 필드에 입력 매개 변수를 제공할 수 있습니다. 그런 다음 보고서를 생성할 때 특정 부서의 데이터만 가져오려면 해당 부서의 IP 네트워크 세그먼트를 입력할 수 있습니다.

팁 또한 제약 조건을 무시하려면 입력 매개 변수 필드에 *를 입력할 수 있습니다.

이메일(제목이나 본문), 보고서 파일 이름, 텍스트 섹션 등 보고서의 특정 필드에 동적 텍스트를 추가하려면 문자열 유형의 입력 매개 변수를 정의할 수 있습니다. 동일한 템플릿을 사용하되 사용자 지정된 보고서 파일 이름, 이메일 주소, 이메일 메시지 등을 사용하여 부서별로 보고서를 개별 설정할 수 있습니다.

정의하는 각 입력 매개 변수에는 이름과 유형이 있습니다. 다음 표에서는 매개 변수 유형에 대해 설명합니다.

표 57-6 사용자 정의 입력 매개 변수 유형

사용할 매개 변수 유형	다음 데이터가 포함된 필드
Network/IP	CIDR 형식의 IP 주소 또는 네트워크 세그먼트
Application	애플리케이션 프로토콜, 클라이언트 애플리케이션 또는 웹 애플리케이션의 이름
Event Message	이벤트 보기 메시지
Device	3D 어플라이언스(방어 센터 또는 FireSIGHT 시스템 관리되는 디바이스)
Username	사용자 식별(예: initiator 사용자 및 responder 사용자)
Number (VLAN ID, Snort ID, Vuln ID)	VLAN ID, Snort ID 또는 취약성 ID
String	애플리케이션이나 OS 버전, 메모, 설명 등의 텍스트 필드

입력 매개 변수의 유형은 사용 가능한 검색 필드를 결정합니다. 사용자 정의 입력 매개 변수 유형 표에 설명된 대로 특정 유형은 해당 필드에서만 사용할 수 있습니다. 예를 들어 문자열 유형으로 정의하는 사용자 매개 변수는 텍스트 필드에 삽입할 수 있지만, IP 주소가 필요한 필드에는 사용할 수 없습니다.

보고서 템플릿용 사용자 정의 입력 매개 변수를 생성하려면

액세스: Admin/Any Security Analyst

1단계 **Overview > Reporting**을 선택합니다.

2단계 **Report Templates** 탭을 선택합니다.

Report Templates 페이지가 나타납니다.

3단계 수정할 템플릿의 수정 아이콘( )을 클릭합니다.

Report Sections 페이지가 나타납니다.

4단계 **Advanced**를 클릭합니다.

Advanced Settings 팝업 창이 나타납니다.

5단계 입력 매개 변수 추가 아이콘( )을 클릭합니다.

Add Input Parameter 팝업 창이 나타납니다.

6단계 **Name** 필드에 매개 변수 이름을 입력하고 **Type** 드롭다운 메뉴를 사용하여 유형을 선택한 다음 **OK**를 클릭합니다.

Input Parameters 메뉴에 새 매개 변수가 나타납니다.

7단계 필요한 매개 변수를 모두 정의할 때까지 위 단계를 반복합니다.

8단계 **OK**를 클릭합니다.

이 템플릿에 대해 새 입력 매개 변수가 저장되고 Report Sections 페이지가 다시 나타납니다.

보고서 템플릿을 재사용하는 경우 새 보고서의 목적을 더 잘 반영하도록 입력 매개 변수의 이름과 유형을 변경할 수 있습니다.

보고서 템플릿용 사용자 정의 입력 매개 변수를 수정하려면

액세스: Admin/Any Security Analyst

1단계 **Overview > Reporting**을 선택합니다.

2단계 **Report Templates** 탭을 선택합니다.

Report Templates 페이지가 나타납니다.

3단계 수정할 템플릿의 수정 아이콘( )을 클릭합니다.

Report Sections 페이지가 나타납니다.

4단계 **Advanced**를 클릭합니다.

Advanced Settings 팝업 창이 나타납니다. 보고서 템플릿에 대해 사용할 수 있는 모든 사용자 정의 매개 변수가 **Input Parameters** 섹션에 나열됩니다.

5단계 수정 아이콘( )을 클릭합니다.

Edit Input Parameter 팝업 창이 나타납니다.

6단계 **Name** 필드에서 매개 변수 이름을 변경하고 **Type** 드롭다운 메뉴를 사용하여 유형을 선택한 다음 **OK**를 클릭합니다.

Input Parameters 섹션에 변경된 매개 변수가 나타납니다.

7단계 필요한 매개 변수를 모두 정의할 때까지 위 단계를 반복합니다. **OK**를 클릭합니다.

변경 사항이 저장되며 Report Sections 페이지가 다시 나타납니다.

보고서 템플릿용 사용자 정의 입력 매개 변수를 삭제하려면

액세스: Admin/Any Security Analyst

1단계 **Overview > Reporting**을 선택합니다.

2단계 **Report Templates** 탭을 선택합니다.

Report Templates 페이지가 나타납니다.

3단계 수정할 템플릿의 수정 아이콘( )을 클릭합니다.

Report Sections 페이지가 나타납니다.

4단계 **Advanced**를 클릭합니다.

Advanced Settings 팝업 창이 나타납니다. 보고서 템플릿에 대해 사용할 수 있는 모든 사용자 정의 매개 변수가 **Input Parameters** 섹션에 나열됩니다.

5단계 입력 매개 변수 옆에 있는 삭제 아이콘( )을 클릭하고 확인합니다.

6단계 **OK**를 클릭합니다.

입력 매개 변수가 삭제되고 Report Sections 페이지가 다시 나타납니다.

입력 매개 변수를 사용하면 검색의 활용 범위를 확장할 수 있습니다. 입력 매개 변수는 보고서를 요청하는 사용자의 생성 시간에 시스템에 값을 수집하도록 지시합니다. 이렇게 하면 검색을 변경하지 않고도 데이터의 특별한 일부를 표시하도록 생성 시 보고서를 동적으로 제한할 수 있습니다. 예를 들어 부서 수준에서 보안 이벤트를 드릴다운하는 보고서 섹션의 **Destination IP** 필드에 입력 매개 변수를 제공할 수 있습니다. 보고서를 생성할 때 특정 부서의 데이터만 가져오려면 해당 부서의 IP 네트워크 세그먼트를 입력할 수 있습니다.

사용자 정의 입력 매개 변수로 보고서 템플릿에서 검색을 제한하려면

액세스: Admin/Any Security Analyst

1단계 **Overview > Reporting**을 선택합니다.

2단계 **Report Templates** 탭을 선택합니다.

Report Templates 페이지가 나타납니다.

3단계 수정할 템플릿의 수정 아이콘( )을 클릭합니다.

Report Sections 페이지가 나타납니다.

4단계 섹션 내 **Search** 필드 옆에 있는 수정 아이콘( )을 클릭합니다.

Search Editor 팝업 창이 나타납니다. 입력 매개 변수를 사용할 수 있는 필드는 입력 매개 변수 아이콘( )으로 표시됩니다.

5단계 필드 옆에 있는 입력 매개 변수 아이콘( )을 클릭한 다음 드롭다운 메뉴에서 입력 매개 변수를 선택합니다. 사용자 정의 입력 매개 변수는 아이콘( )으로 표시됩니다.

필드에 입력 매개 변수가 나타납니다.

참고 정의하는 입력 매개 변수는 해당 매개 변수 유형과 일치하는 검색 필드에서만 사용할 수 있습니다. 예를 들어 **Network/IP** 유형의 매개 변수는 IP 주소 또는 CIDR 형식의 네트워크 세그먼트가 허용되는 필드에만 사용할 수 있습니다.

6단계 필요한 모든 입력 매개 변수를 추가한 후 **OK**를 클릭합니다.

변경 사항과 함께 Report Sections 페이지가 나타납니다.

보고서 템플릿에서 문서 특성 수정

라이센스: 모두

보고서를 생성하기 전에 보고서 모양에 영향을 주는 문서 특성을 설정할 수 있습니다. 이러한 특성에는 선택적인 커버 페이지 및 목차가 포함됩니다. 일부 특성에 대한 지원은 선택한 보고서 형식(PDF, HTML 또는 CSV)에 따라 다릅니다. 다음 표에서는 형식별 특성 지원에 대한 세부사항을 제공합니다.

표 57-7 문서 특성 지원

특성	PDF 지원 여부	HTML 지원 여부	CSV 지원 여부
커버 페이지	예(로고 및 사용자 지정 모양 선택 사항)	예(로고 및 사용자 지정 모양 선택 사항)	아니요
목차	예	예	아니요

표 57-7 문서 특성 지원 (계속)

특성	PDF 지원 여부	HTML 지원 여부	CSV 지원 여부
페이지 머리글 및 바닥글	예(필드의 텍스트 또는 로고 선택 사항)	아니요	아니요
사용자 지정 시작 페이지 번호	예	아니요	아니요
첫 페이지의 번호 억제 옵션	예	아니요	아니요

PDF 및 HTML 보고서의 문서 특성을 설정하려면

액세스: Admin/Any Security Analyst

1단계 **Overview > Reporting**을 선택합니다.

2단계 **Report Templates** 탭을 선택합니다.

Report Templates 페이지가 나타납니다.

3단계 수정할 보고서 템플릿의 수정 아이콘( )을 클릭합니다.

Report Sections 페이지가 나타납니다.

4단계 **Advanced**를 클릭합니다.

Advanced Settings 팝업 창이 나타납니다.

5단계 커버 페이지를 추가하려면 **Include Cover Page**를 선택합니다.

6단계 커버 페이지 디자인을 수정하려면 **Cover Page Design** 필드 옆에 있는 수정 아이콘( )을 클릭합니다.

자세한 내용은 57-23페이지의 커버 페이지 사용자 지정을/를 참조하십시오.

7단계 목차를 추가하려면 **Include Table of Contents**를 선택합니다.

8단계 세 개의 **Header** 및 **Footer** 필드 드롭다운을 사용하여 머리글과 바닥글을 구성합니다. 드롭다운 메뉴에서 머리글 및 바닥글 내용을 선택합니다(로고, 날짜, 페이지 번호 등).

Logo를 선택하면 선택한 필드에 기본 로고 이미지가 나타납니다. 기본 로고 이미지를 변경하려면 57-24페이지의 로고 관리을/를 참조하십시오.

9단계 **Page Number Start** 필드에서 보고서 첫 페이지의 페이지 번호를 선택합니다.

커버 페이지 이후의 첫 페이지에 페이지 번호를 표시하려면 **Number First Page?**를 선택합니다. 이 경우 커버 페이지에는 번호가 표시되지 않습니다.

10단계 **OK**를 클릭합니다.

문서 특성이 저장되고 Report Sections 페이지가 다시 나타납니다.

커버 페이지 사용자 지정

라이센스: 모두

보고서 템플릿의 커버 페이지를 사용자 지정할 수 있습니다. 커버 페이지에서는 여러 글꼴 크기와 스타일(굵게, 기울임 등)의 풍부한 텍스트는 물론 입력 매개 변수와 가져온 이미지도 사용할 수 있습니다. 입력 매개 변수에 대한 자세한 내용은 57-18페이지의 입력 매개 변수 사용을/를 참조하십시오.

보고서 템플릿 커버 페이지를 사용자 지정하려면

액세스: Admin/Any Security Analyst

1단계 **Overview > Reporting**을 선택합니다.

2단계 **Report Templates** 탭을 선택합니다.

Report Templates 페이지가 나타나며 템플릿 목록이 표시됩니다.

3단계 보고서 템플릿의 수정 아이콘()을 클릭합니다.

Report Sections 페이지가 나타납니다.

4단계 **Advanced**를 클릭합니다.

Advanced Settings 팝업 창이 나타납니다.

5단계 **Cover Page Design** 옆의 수정 아이콘()을 클릭합니다.

Edit Cover Page 창이 나타나며 기본 커버 페이지 디자인이 표시됩니다.

6단계 풍부한 텍스트 편집기 내에서 커버 페이지 디자인을 수정합니다.

7단계 **OK**를 클릭합니다.

커버 페이지 디자인이 저장되고 Advanced Settings 창이 다시 나타납니다.

로고 관리

라이센스: 모두

방어 센터에 여러 로고를 저장하고 서로 다른 보고서 템플릿과 연결할 수 있습니다. 템플릿을 디자인할 때 로고 연결을 설정합니다. 템플릿을 내보내면 내보내기 패키지에 로고가 포함됩니다.

보고서에서 로고를 삽입할 수 있는 위치에 대한 자세한 내용은 57-22페이지의 보고서 템플릿에서 문서 특성 수정을/를 참조하십시오.

자세한 내용은 다음 관련 절차를 참조하십시오.

- 57-24페이지의 새 로고 추가
- 57-25페이지의 보고서 템플릿에 대한 로고 변경
- 57-26페이지의 로고 삭제

새 로고 추가

라이센스: 모두

방어 센터에 업로드된 로고는 해당 방어 센터의 모든 보고서 템플릿에서 사용할 수 있습니다. 로고 이미지는 JPG 형식이어야 합니다.

방어 센터에 로고를 추가하려면

액세스: Admin/Any Security Analyst

1단계 **Overview > Reporting**을 선택합니다.

2단계 **Report Templates** 탭을 선택합니다.

Report Templates 페이지가 나타납니다.

3단계 수정할 보고서 템플릿의 수정 아이콘( )을 클릭합니다.

Report Sections 페이지가 나타납니다.

4단계 **Advanced**를 클릭합니다.

Advanced Settings 팝업 창이 나타납니다. 현재 템플릿과 연결된 로고는 **General Settings**의 **Logo** 아래에 나타납니다.

5단계 로고의 수정 아이콘( )을 클릭합니다.

현재 업로드된 로고 이미지와 함께 Select Logo 팝업 창이 나타납니다.

6단계 **Upload Logo**를 클릭합니다.

Upload Logo 팝업 창이 나타납니다.

7단계 다음 중 하나를 수행하여 업로드할 로고 파일을 선택합니다.

- 로고 파일의 위치 입력
- **Browse** 버튼을 클릭하고 파일의 위치로 이동

8단계 **Upload**를 클릭합니다.

이미지가 방어 센터에 업로드되고 Select Logo 팝업 창에 나타납니다.

9단계 선택적으로, 새 로고를 선택하고 **OK**를 클릭하여 새 로고를 현재 템플릿과 연결합니다.

연결된 로고 이미지와 함께 Advanced Settings 창이 다시 나타납니다.

보고서 템플릿에 대한 로고 변경

라이센스: 모두

보고서의 로고를 방어 센터에 업로드된 JPG 이미지로 변경할 수 있습니다. 예를 들어 템플릿을 재사용하려면 다른 조직의 로고를 보고서와 연결할 수 있습니다.

보고서 템플릿에 대한 로고를 변경하려면

액세스: Admin/Any Security Analyst

1단계 **Overview > Reporting**을 선택합니다.

2단계 **Report Templates** 탭을 선택합니다.

Report Templates 페이지가 나타납니다.

3단계 수정할 보고서 템플릿의 수정 아이콘( )을 클릭합니다.

Report Sections 페이지가 나타납니다.

4단계 **Advanced**를 클릭합니다.

Advanced Settings 팝업 창이 나타납니다. 현재 템플릿과 연결된 로고는 **General Settings**의 **Logo** 아래에 나타납니다.

5단계 로고의 수정 아이콘( )을 클릭합니다.

현재 업로드된 로고 이미지와 함께 Select Logo 팝업 창이 나타납니다.

6단계 보고서 템플릿과 연결할 로고를 선택합니다.

선택한 로고가 강조 표시됩니다.

7단계 **OK**를 클릭합니다.

연결된 로고 이미지와 함께 Advanced Settings 창이 다시 나타납니다.

로고 삭제

라이센스: 모두

방어 센터에서 로고를 삭제할 수 있습니다. 로고를 삭제하면 사용된 모든 템플릿에서 해당 로고가 제거됩니다. 삭제는 취소할 수 없습니다.

사전 정의된 Cisco 로고는 삭제할 수 없습니다.

방어 센터에서 로고를 삭제하려면

액세스: Admin/Any Security Analyst

1단계 **Overview > Reporting**을 선택합니다.

2단계 **Report Templates** 탭을 선택합니다.

Report Templates 페이지가 나타납니다.

3단계 수정할 보고서 템플릿의 수정 아이콘( )을 클릭합니다.

Report Sections 페이지가 나타납니다.

4단계 **Advanced**를 클릭합니다.

Advanced Settings 팝업 창이 나타납니다. 현재 템플릿과 연결된 로고는 **General Settings**의 **Logo** 아래에 나타납니다.

5단계 로고의 수정 아이콘( )을 클릭합니다.

현재 업로드된 로고 이미지와 함께 Select Logo 팝업 창이 나타납니다.

6단계 삭제할 로고를 선택합니다.

선택한 로고가 강조 표시됩니다.

7단계 **Delete Logo**를 클릭합니다.

삭제된 로고가 Select Logo 팝업 창에서 사라집니다.

8단계 **OK**를 클릭합니다.

변경 사항이 저장되고 Advanced Settings 페이지가 다시 나타납니다.

보고서 생성 및 보기

라이센스: 모두

보고서 템플릿을 생성 및 사용자 지정했으면 이제 보고서 자체를 생성할 준비가 된 것입니다. 생성 프로세스에서는 보고서의 형식(HTML, PDF 또는 CSV)을 선택할 수 있습니다. 제외한 섹션 이외의 모든 섹션에 일관된 기간을 적용하는 보고서의 전역 시간 창을 조정할 수도 있습니다. 보고서 시간 창 설정에 대한 자세한 내용은 57-15페이지의 템플릿 및 섹션에 대한 시간 창 설정을/를 참조하십시오.

보고서 템플릿의 검색 사양에 사용자 입력 매개 변수가 포함된 경우 일반 프로세스에서는 값을 입력하라는 프롬프트가 표시됩니다. 이러한 값은 데이터 일부에 대한 보고서 실행을 맞춤화합니다. 입력 매개 변수에 대한 자세한 내용은 57-18페이지의 입력 매개 변수 사용을/를 참조하십시오.

Reports 탭에는 보고서 이름, 생성 날짜와 시간, 생성 사용자, 보고서가 로컬에 저장되었는지 원격에 저장되었는지 등의 정보와 함께 전에 생성된 모든 보고서가 나열됩니다. 상태 열에는 보고서가 이미 생성되었는지, 생성 대기열에 있는지(예: 예약된 작업) 또는 생성에 실패했는지(예: 디스크 공간 부족 때문에) 등이 나타납니다.

Reports 탭 페이지에는 로컬에 저장된 모든 보고서가 표시됩니다. 현재 원격 스토리지가 구성된 경우 원격으로 저장된 보고서도 표시됩니다. 로컬, NFS 및 SMB 스토리지에 대한 디스크 사용량과 함께 현재 구성된 보고서 스토리지의 위치가 페이지 아래쪽에 나타납니다. SSH를 사용하여 원격 스토리지에 액세스하는 경우 디스크 사용량 데이터를 사용할 수 없습니다. 원격 스토리지 설정에 대한 자세한 내용은 57-30페이지의 보고서에 원격 스토리지 사용을/를 참조하십시오.

참고 원격으로 저장한 후 로컬 스토리지로 전환하는 경우 원격 스토리지의 보고서가 Reports 탭 목록에 나타나지 않습니다. 마찬가지로, 원격 스토리지 위치 간에 전환하면 이전 위치의 보고서가 목록에 나타나지 않습니다.

유니코드(UTF-8) 문자를 사용한 파일 이름은 PDF 보고서에서 지원되지 않습니다. 보고서를 PDF 형식으로 생성하는 경우 특정 유니코드 파일 이름(예: 파일 또는 악성코드 이벤트에 나타나는 이름)이 포함된 보고서 섹션에는 음역 형식으로 이러한 파일 이름이 표시됩니다.

DNS 서버가 구성되어 있고 IP 주소 확인이 활성화된 경우 확인에 성공하면 보고서에 호스트 이름이 포함됩니다. 자세한 내용은 64-8페이지의 관리 인터페이스 구성 및 71-4페이지의 이벤트 환경 설정을/를 참조하십시오.

보고서를 생성하고 보려면 다음 절차를 사용하십시오. Administrator 액세스 권한이 있는 사용자는 모든 보고서를 볼 수 있습니다. 다른 사용자는 자신이 생성한 보고서만 볼 수 있습니다. 보고서 파일 관리에 대한 자세한 내용은 57-33페이지의 보고서 다운로드 및 57-34페이지의 보고서 삭제을/를 참조하십시오.

보고서 템플릿에서 보고서를 생성하려면

액세스: Admin/Any Security Analyst

1단계 **Overview > Reporting**을 선택합니다.

2단계 **Report Templates** 탭을 클릭합니다.

Report Templates 페이지가 나타납니다.

3단계 사용할 템플릿의 보고서 생성 아이콘( )을 클릭합니다.

Generate Report 팝업 대화 상자가 나타납니다.

4단계 선택적으로, **File Name** 필드에 새 이름을 입력합니다. 이렇게 하면 생성된 보고서 파일의 이름이 설정됩니다. 파일 이름에 하나 이상의 입력 매개 변수를 추가하려면 입력 매개 변수 아이콘( )을 사용할 수도 있습니다. 입력 매개 변수에 대한 자세한 내용은 57-18페이지의 입력 매개 변수 사용을/를 참조하십시오.

5단계 해당 아이콘(HTML, PDF 또는 CSV)을 클릭하여 보고서의 출력 형식을 선택합니다.

6단계 선택적으로, 시간 창 아이콘( )을 클릭하여 전역 시간 창을 변경합니다.

Events Time Window 팝업 창이 나타납니다. 이벤트 시간 창 설정에 대한 자세한 내용은 58-22페이지의 이벤트 시간 제약 조건 설정을/를 참조하십시오.

참고 개별 보고서 섹션이 전역 설정을 상속하도록 구성된 경우에만 전역 시간 창 설정이 개별 보고서 섹션의 내용에 영향을 미칩니다. 전역 시간 창의 보고서 섹션 상속에 대한 자세한 내용은 57-15페이지의 템플릿 및 섹션에 대한 시간 창 설정을/를 참조하십시오.

7단계 **Input Parameters** 섹션에 나타나는 필드의 값을 입력합니다.

팁 필드에 * 와일드카드 문자를 입력하여 사용자 매개 변수를 무시할 수 있습니다. 이 경우 검색에 대한 사용자 매개 변수의 제약 조건이 제거됩니다.

8단계 선택적으로, 시스템 정책에 이메일 릴레이 호스트가 구성된 경우 **Email**을 클릭하면 보고서 생성 시 이메일 전달이 자동화됩니다. 이메일 전달 기능에 대한 자세한 내용은 57-29페이지의 생성 시 이메일로 보고서 배포을/를 참조하십시오.

9단계 프롬프트가 표시되면 **OK**를 클릭하여 확인합니다.

Report Generation Complete 팝업 창이 보고서를 볼 수 있는 링크와 함께 나타납니다.

10단계 다음 중 하나를 클릭합니다.

- 보고서 링크 - 보고서를 표시할 새 창이 열립니다.
- **OK** - 보고서 디자인을 수정할 수 있는 Report Section 페이지로 돌아갑니다.

초기 생성 후 완료된 보고서를 검토할 수도 있습니다.

11단계 선택적으로, 보고서 파일을 관리합니다. 자세한 내용은 57-33페이지의 보고서 다운로드 및 57-34페이지의 보고서 삭제을/를 참조하십시오.

생성된 보고서를 보려면

액세스: Admin/Any Security Analyst

1단계 **Overview > Reporting**을 선택합니다.

2단계 **Reports** 탭을 클릭합니다.

Reports 페이지가 나타납니다.

3단계 보고서의 이름을 클릭합니다.

로컬 호스트의 기본 프로그램이 새 창에 보고서를 엽니다.

4단계 문서 보기를 완료했으면 브라우저를 사용하여 **Reports** 탭으로 돌아갑니다.

보고서 생성 옵션 사용

라이센스: 모두

보고서를 생성할 때 몇 가지 추가 옵션이 있습니다. 보고서 생성을 자동으로 예약하고, 이메일을 통해 보고서를 전송하고, 생성된 보고서를 원격에 저장할 수 있습니다. 자세한 내용은 다음 절을 참조하십시오.

- 57-29페이지의 스케줄러를 사용하여 보고서 생성
- 57-29페이지의 생성 시 이메일로 보고서 배포
- 57-30페이지의 보고서에 원격 스토리지 사용

스케줄러를 사용하여 보고서 생성

라이센스: 모두

FireSIGHT 시스템 스케줄러를 사용하여 보고서 생성을 자동화할 수 있습니다. 일별, 주별, 월별 등 전체 기간에 대한 일정을 사용자 지정할 수 있습니다. 자세한 내용은 62-8페이지의 보고서 생성 자동화을/를 참조하십시오.

스케줄러를 사용하여 이메일 보고서를 배포하려면 작업을 예약하기 **전에** 보고서 템플릿과 메일 릴레이를 구성해야 합니다. 자세한 내용은 57-29페이지의 생성 시 이메일로 보고서 배포 및 63-18페이지의 메일 릴레이 호스트 및 알림 주소 구성을/를 참조하십시오.

생성 시 이메일로 보고서 배포

라이센스: 모두

템플릿에서 보고서를 생성할 때 수신자 목록 전체에 보고서를 이메일 첨부 파일로 자동으로 전송하도록 선택할 수 있습니다.

참고 보고서를 이메일로 전달하려면 메일 릴레이 호스트를 적절히 구성해야 합니다. 전에 메일 호스트를 설정하지 않은 경우 63-18페이지의 메일 릴레이 호스트 및 알림 주소 구성을/를 참조하십시오.

생성 시 보고서를 이메일로 전송하려면

액세스: Admin/Any Security Analyst

1단계 **Overview > Reporting**을 선택합니다.

2단계 **Report Templates** 탭을 선택합니다.

Report Templates 페이지가 나타납니다.

3단계 생성에 사용할 템플릿의 보고서 생성 아이콘( )을 클릭합니다.

Generate Report 팝업 창이 나타납니다.

4단계 창의 **Email** 섹션을 확장합니다.

5단계 **Email Options** 필드에서 **Send Email**을 선택합니다.

6단계 **Recipient List, CC** 및 **BCC** 필드에서 쉼표로 구분된 목록에 수신자의 이메일 주소를 입력합니다.

7단계 **Subject** 필드에 이메일 제목을 입력합니다.

팁 타임스탬프나 방어 센터의 이름과 같은 정보를 이메일에서 동적으로 생성하려면 **Subject** 필드 및 메시지 본문에 입력 매개 변수를 제공할 수 있습니다. 자세한 내용은 57-18페이지의 입력 매개 변수 사용을/를 참조하십시오.

8단계 필요에 따라 이메일 본문에 설명 내용을 입력합니다. 사용 가능한 풍부한 텍스트 기능에는 광범위한 글꼴, 번호 매기기 목록과 글머리 기호 등이 포함됩니다.

9단계 Generate Report 창의 모든 필드가 올바르면 **OK**를 클릭하여 확인합니다.

시스템은 생성된 보고서를 이메일로 배포합니다. 시스템 정책에서 **Email Notification** 아래에 이메일의 From 주소를 구성할 수 있습니다. 자세한 내용은 63-1페이지의 시스템 정책 관리을/를 참조하십시오.

보고서에 원격 스토리지 사용

라이센스: 모두

새로 생성된 보고서 파일을 구성된 원격 스토리지 위치에 배치하도록 보고 시스템을 구성할 수 있습니다. 로컬에 저장된 보고서를 원격 스토리지 위치로 이동할 수도 있습니다.

참고 원격 스토리지의 보고서를 로컬 스토리지로 다시 이동할 수 없습니다.

원격 스토리지를 사용하려면 먼저 원격 스토리지 위치를 구성해야 합니다. 구성이 완료되면 보고서 목록의 아래에 원격 스토리지 위치가 나타납니다. 위치에는 NFS 및 SMB(SSH는 제외) 탑재 스토리지의 현재 디스크 사용량이 포함됩니다. 컨피그레이션 정보는 64-15페이지의 원격 스토리지 관리을/를 참조하십시오.

생성 시 보고서를 원격으로 저장하려면

액세스: Admin/Any Security Analyst

1단계 **Overview > Reporting**을 선택합니다.

2단계 **Reports** 탭을 선택합니다.

Reports 페이지가 나타납니다.

3단계 페이지 아래쪽에서 **Enable Remote Storage of Reports** 확인란을 선택합니다.

방어 센터는 새로 생성된 보고서를 페이지 아래쪽에 표시된 원격 위치에 저장합니다. 이러한 보고서의 **Location** 열 데이터는 `Remote`입니다.

배치 모드에서 또는 단독으로 로컬 스토리지의 보고서를 원격 스토리지 위치로 이동할 수 있습니다.

생성된 보고서를 로컬에서 원격 스토리지로 이동하려면

액세스: Admin/Any Security Analyst

1단계 **Overview > Reporting**을 선택합니다.

2단계 **Reports** 탭을 선택합니다.

Reports 페이지가 나타납니다.

3단계 이동할 보고서 옆에 있는 확인란을 선택하고 **Move**를 클릭합니다.

팁 페이지의 모든 보고서를 이동하려면 페이지 상단 왼쪽에 있는 확인란을 선택합니다. 보고서에 여러 페이지가 있는 경우 모든 페이지의 모든 보고서를 이동하기 위해 선택할 수 있는 두 번째 확인란이 나타납니다.

4단계 보고서를 이동할 것임을 확인합니다.

보고서가 이동됩니다.

보고서 템플릿 및 보고서 파일 관리

라이센스: 모두

템플릿의 생성 및 수정 외에도 다음과 같은 템플릿 관리 작업을 수행할 수 있습니다.

- 57-31페이지의 보고서 템플릿 내보내기 및 가져오기
- 57-33페이지의 보고서 템플릿 삭제

또한 생성된 보고서 파일에 대해 다음과 같은 관리 작업을 수행할 수 있습니다.

- 57-33페이지의 보고서 다운로드
- 57-34페이지의 보고서 삭제

보고서 템플릿 내보내기 및 가져오기

라이센스: 모두

보고서 템플릿을 내보낼 때 생성하는 파일에는 또 다른 방어 센터에 대한 동일한 보고서를 생성하기 위해 필요한 모든 데이터가 포함되어 있습니다. 독점적인 SFO 형식의 내보내기 파일에는 다음이 포함됩니다.

- 모든 섹션 디자인 요소 및 문서 특성이 포함된 보고서 템플릿
- 보고서에 사용된 모든 저장된 검색
- 보고서에 사용된 모든 이미지
- 보고서에 사용된 모든 사용자 지정 테이블

템플릿을 또 다른 방어 센터로 가져온 후 필요할 수 있는 유일한 컨피그레이션은 자동 보고서 생성 일정입니다.

참고 보고서 템플릿을 내보내고 가져오려면 두 방어 센터의 소프트웨어 버전 레벨이 동일해야 합니다.

보고서 템플릿을 내보내려면

액세스: Admin

1단계 **Overview > Reporting**을 선택합니다.

2단계 **Report Templates** 탭을 선택합니다.

Report Templates 페이지가 나타납니다.

3단계 내보내려는 템플릿에 대해 내보내기 아이콘()을 클릭합니다.

시스템은 `.sfo` 확장명의 컨피그레이션 패키지 파일을 생성하고 패키지 파일 이름을 표시하는 Opening Object 팝업 창을 엽니다.

4단계 **Save file** 및 **OK**를 선택하여 파일을 로컬 컴퓨터에 저장합니다.

5단계 편의에 따라 `.sfo` 패키지의 이름을 좀 더 설명적인 이름으로 변경할 수 있습니다. 패키지를 가져올 경우 이름과 상관없이 방어 센터는 소스 방어 센터에서 사용된 것과 동일한 이름을 템플릿에 지정합니다.

방어 센터에서 내보낸 SFO 파일에는 보고서 템플릿을 또 다른 방어 센터에 추가하기 위해 필요한 모든 요소가 포함됩니다. 따라서 가져오기 프로세스에는 패키지를 두 번째 방어 센터에 업로드하고 가져오기 프로세스를 실행하는 것만 필요합니다.

보고서 템플릿을 가져오려면

액세스: Admin

1단계 **System > Tools > Import/Export**를 선택합니다.

방어 센터에 대한 보고서 템플릿 목록이 포함된 Import/Export 페이지가 나타납니다.

2단계 **Upload Package**를 클릭합니다.

Package Name 페이지가 나타납니다.

3단계 다음 2가지 옵션을 사용할 수 있습니다.

- 업로드하려는 패키지의 경로를 입력합니다.
- **Browse**를 클릭하여 패키지를 찾습니다.

4단계 **Upload**를 클릭합니다.

컨피그레이션 목록의 **Report Template** 섹션이 나타나서 가져올 템플릿을 보여줍니다.

5단계 템플릿 옆에 있는 확인란을 선택하고 **Import**를 클릭합니다.

템플릿이 목적지 방어 센터에서 컨피그레이션 목록에 나타납니다.

보고서 템플릿 삭제

라이센스: 모두

보고서 템플릿은 삭제될 때까지 재사용할 수 있도록 Report Templates 탭에 나열됩니다. Cisco 제공 보고서 템플릿은 삭제할 수 없습니다.

참고 보안 분석가는 자신이 생성한 보고서 템플릿만 삭제할 수 있습니다.

보고서 템플릿을 삭제하려면

액세스: Admin/Any Security Analyst

1단계 **Overview > Reporting**을 선택합니다.

2단계 **Report Templates** 탭을 선택합니다.

Report Templates 페이지가 나타납니다.

3단계 삭제하려는 디바이스 옆에 있는 삭제 아이콘( )을 클릭하고 확인합니다.

목록에서 템플릿 이름이 사라집니다.

보고서 다운로드

라이센스: 모두

원하는 보고서 파일을 로컬 컴퓨터로 다운로드할 수 있습니다. 이곳에서 보고서 파일을 이메일로 전송하거나 다른 사용 가능한 수단을 통해 전자 방식으로 배포할 수 있습니다. 생성 시 이메일을 통해 보고서를 자동으로 배포하는 방법에 대한 자세한 내용은 57-29페이지의 생성 시 이메일로 보고서 배포을/를 참조하십시오.

보고서를 다운로드하려면

액세스: Admin/Any Security Analyst

1단계 **Overview > Reporting**을 선택합니다.

2단계 **Reports** 탭을 선택합니다.

Reports 페이지가 나타납니다.

3단계 다운로드할 보고서 옆에 있는 확인란을 선택하고 **Download**를 클릭합니다.

팁 페이지의 모든 보고서를 다운로드하려면 페이지 상단 왼쪽에 있는 확인란을 선택합니다. 보고서에 여러 페이지가 있는 경우 모든 페이지의 모든 보고서를 다운로드하기 위해 선택할 수 있는 두 번째 확인란이 나타납니다.

4단계 브라우저의 프롬프트에 따라 보고서를 다운로드합니다.

여러 보고서를 선택하면 단일 `.zip` 파일로 다운로드됩니다.

보고서 삭제

라이센스: 모두

언제든지 보고서 파일을 삭제할 수 있습니다. 이 절차를 수행하면 파일이 완전히 제거되며 복구할 수 없습니다. 보고서를 생성한 보고서 템플릿을 여전히 가지고 있더라도 시간 창을 확장 또는 이동한 경우 특정 보고서 파일의 재생성이 어려울 수 있습니다. 시간 창에 대한 자세한 내용은 57-12페이지의 보고서 템플릿의 섹션 수정을/를 참조하십시오. 템플릿에서 입력 매개 변수를 사용하는 경우에도 재생성이 어려울 수 있습니다. 입력 매개 변수 사용에 대한 자세한 내용은 57-18페이지의 입력 매개 변수 사용을/를 참조하십시오.

보고서를 삭제하려면

액세스: Admin/Any Security Analyst

1단계 **Overview > Reporting**을 선택합니다.

2단계 **Reports** 탭을 선택합니다.

Reports 페이지가 나타납니다.

3단계 삭제할 보고서 옆에 있는 확인란을 선택하고 **Delete**를 클릭합니다.

팁 페이지의 모든 보고서를 삭제하려면 페이지 상단 왼쪽에 있는 확인란을 선택합니다. 보고서에 여러 페이지가 있는 경우 모든 페이지의 모든 보고서를 삭제하기 위해 선택할 수 있는 두 번째 확인란이 나타납니다.

4단계 삭제를 확인합니다.

보고서가 삭제됩니다.

58장

워크플로의 이해 및 사용

워크플로는 방어 센터 웹 인터페이스에 있는 일련의 맞춤 데이터 페이지이며, 분석가는 시스템에서 생성된 이벤트를 평가하는 데 이를 사용할 수 있습니다. 방어 센터에서는 3가지 유형의 워크플로를 제공합니다.

- *사전 정의 워크플로* - 시스템에 설치된 미리 설정된 워크플로이며 수정하거나 삭제할 수 없습니다.
- *저장된 사용자 지정 워크플로* - 사전 정의된 사용자 지정 워크플로이며 수정 또는 삭제 가능합니다.
- *사용자 지정 워크플로* - 구체적인 필요에 따라 생성하고 사용자 지정하는 워크플로입니다.

예를 들어 침입 이벤트를 분석할 때 이 작업을 위해 특별히 생성된 여러 사전 정의 워크플로 중에서 선택할 수 있습니다.

워크플로에 표시된 데이터는 대개 관리되는 디바이스의 라이센스 및 구축 방식, 데이터를 제공하는 기능의 구성 여부 그리고 Series 2 어플라이언스 및 Cisco NGIPS for Blue Coat X-Series의 경우에는 어플라이언스가 데이터 제공 기능을 지원하는지 여부와 같은 요인에 따라 달라집니다. DC500 방어 센터나 Series 2 디바이스 모두 범주 및 평판 기준 URL 필터링을 지원하지 않으므로 DC500 방어 센터에서는 이 기능을 위한 데이터를 표시하지 않고 Series 2 디바이스는 이 데이터를 탐지하지 않습니다.

사전 정의 및 사용자 지정 워크플로 사용에 대한 자세한 내용은 다음 절을 참조하십시오.

- 58-1페이지의 워크플로의 구성 요소
- 58-15페이지의 워크플로 사용
- 58-38페이지의 사용자 지정 워크플로 사용

팁 사용자 지정 워크플로를 이벤트 보고서의 기반으로 사용할 수도 있습니다. 자세한 내용은 57-1페이지의 보고서 작업을/를 참조하십시오.

워크플로의 구성 요소

라이센스: 모두

워크플로는 다음 절에서 설명하는 여러 유형의 페이지를 포함할 수 있습니다.

표 보기

표 보기에는 워크플로의 기반이 되는 데이터베이스의 필드별로 하나의 열이 있습니다.

예를 들어 검색 이벤트의 표 보기는 Time, Event, IP Address, User, MAC Address, MAC Vendor, Port, Description, Device 열이 있습니다.

이와 달리 서버의 표 보기에는 Last Used, IP Address, Port, Protocol, Application Protocol, Vendor, Version, Web Application, Application Risk, Business Relevance, Hits, Source Type, Device, Current User 열이 있습니다.

드릴다운 페이지

드릴다운 페이지는 데이터베이스에서 제공하는 열의 일부를 포함합니다.

예를 들어 검색 이벤트의 드릴다운 페이지에 IP Address, MAC Address, Time 열만 포함될 수 있습니다. 한편 침입 이벤트의 드릴다운 페이지는 Priority, Impact Flag, Inline Result, Message 열이 포함될 수 있습니다.

일반적으로 드릴다운 페이지는 보기 페이지로 이동하기 전에 조사 범위를 몇몇 이벤트로 한정하는 데 사용하는 중간 단계의 페이지입니다.

그래프

연결 데이터 기반의 워크플로는 *연결 그래프*라고도 하는 그래프 페이지를 포함할 수 있습니다.

예를 들어 연결 그래프에서 시간의 경과에 따른 탐지된 연결 수를 나타내는 선 그래프가 표시될 수 있습니다. 일반적으로 연결 그래프는 드릴다운 페이지처럼 조사 범위를 한정하는 데 사용하는 중간 단계의 페이지입니다. 자세한 내용은 39-16페이지의 연결 그래프 작업을/를 참조하십시오.

최종 페이지

워크플로의 최종 페이지는 워크플로의 기반이 되는 이벤트의 유형에 따라 달라집니다.

- 호스트 보기는 애플리케이션, 애플리케이션 세부사항, 검색 이벤트, 호스트, IOC(indication of compromise), 서버 또는 임의의 취약성 유형을 기반으로 한 워크플로의 최종 페이지입니다. 이 페이지에서 호스트 프로필을 보면서 다중 주소를 갖는 호스트의 모든 IP 주소에 대한 데이터를 편리하게 볼 수 있습니다. 자세한 내용은 49-1페이지의 호스트 프로필 사용을/를 참조하십시오.
- 사용자 세부사항 보기는 사용자 및 사용자 활동을 기반으로 한 워크플로의 최종 페이지입니다. 자세한 내용은 50-63페이지의 사용자 세부사항 및 호스트 기록 이해을/를 참조하십시오.
- 취약성 세부사항 보기는 Cisco 취약성을 기반으로 하는 워크플로의 최종 페이지입니다. 자세한 내용은 49-27페이지의 취약성 세부사항 보기을/를 참조하십시오.
- 패킷 보기는 침입 이벤트를 기반으로 하는 워크플로의 최종 페이지입니다. 자세한 내용은 41-22페이지의 패킷 보기 사용을/를 참조하십시오.

다른 종류의 이벤트(예: 감사 로그 이벤트, 악성코드 이벤트)를 기반으로 하는 워크플로는 최종 페이지가 없습니다.

워크플로에 대한 자세한 내용은 다음 절을 참조하십시오.

사전 정의 및 사용자 지정 워크플로 비교

라이센스: 모두

FireSIGHT 시스템에서는 *사전 정의* 워크플로 모음(다음 절 참조)을 제공하며, 이벤트 및 수집되는 기타 데이터를 분석하는 데 이를 사용할 수 있습니다.

사용자 지정 워크플로는 조직의 고유한 필요에 맞게 생성하는 워크플로입니다. 사용자 지정 워크플로를 생성할 때 워크플로의 기반이 되는 이벤트(또는 데이터베이스 테이블)의 종류를 선택합니다. 방어 센터에서 사용자 지정 테이블을 사용자 지정 워크플로의 기반으로 선택할 수 있습니다. 또한 사용자 지정 워크플로에 포함되는 페이지를 선택할 수 있습니다. 사용자 지정 워크플로는 드릴다운, 표 보기, 호스트 또는 패킷 보기 페이지로 구성될 수 있습니다.

방어 센터에서는 여러 *저장된 사용자 지정 워크플로*가 함께 제공되며, 이는 역시 방어 센터에서 제공하는 저장된 사용자 지정 테이블을 기반으로 합니다. 사전 정의 테이블 기반 워크플로와 사용자 지정 테이블 기반 워크플로의 차이점은 다음 절, 사전 정의 및 사용자 지정 테이블의 워크플로 비교에 나와 있습니다.

사전 정의 및 사용자 지정 테이블의 워크플로 비교

라이센스: FireSIGHT

사용자 지정 테이블 기능을 사용하여 이벤트 유형 2가지 이상의 데이터를 사용하는 테이블을 생성할 수 있습니다. 이를테면 침입 이벤트 데이터를 검색 데이터와 연계하여 중요 시스템에 영향을 주는 이벤트의 단순 검색을 지원하는 테이블과 워크플로를 만들 때 유용한 기능입니다. 사용자 지정 테이블 생성에 대한 자세한 내용은 59-1페이지의 사용자 지정 테이블 사용을/를 참조하십시오.

각 사용자 지정 테이블은 기본적으로 테이블과 관련된 이벤트를 볼 때 사용할 수 있는 워크플로가 있습니다. 워크플로의 기능은 사용하는 테이블 유형에 따라 달라집니다. 예를 들어 침입 이벤트 테이블을 기반으로 하는 사용자 지정 테이블 워크플로는 항상 패킷 보기로 끝납니다. 그러나 검색 이벤트를 기반으로 하는 사용자 지정 테이블 워크플로는 호스트 보기로 끝납니다.

사전 정의 이벤트 테이블 기반의 워크플로와 달리 사용자 지정 테이블 기반의 워크플로는 다른 워크플로 유형에 대한 링크가 없습니다.

사전 정의 침입 이벤트 워크플로

라이센스: 보호

다음 표에서는 FireSIGHT 시스템에 포함된 사전 정의 침입 이벤트 워크플로에 대해 설명합니다. 이 워크플로에 액세스하는 방법에 대해서는 41-9페이지의 침입 이벤트 보기 및 41-16페이지의 침입 이벤트 검토을/를 참조하십시오.

표 58-1 사전 정의 침입 이벤트 워크플로

워크플로 이름	설명
Destination Port	대상 포트가 대개 애플리케이션과 연결되므로 이 워크플로는 알림의 양이 비정상적으로 많은 애플리케이션을 탐지하는 데 사용할 수 있습니다. Destination Port 열은 네트워크에 있어서는 안 될 애플리케이션을 식별하는 데에도 도움이 됩니다. 이 워크플로는 침입 이벤트 관련 대상 포트를 표시하는 페이지로 시작하고 그 뒤에 생성된 이벤트 유형을 표시하는 페이지가 나옵니다. 그런 다음 이벤트 정보가 표 형식으로 표시되는 이벤트 표 보기가 나타나고 이어서 각 이벤트와 관련된 패킷의 해독된 콘텐츠를 표시하는 패킷 보기가 나타납니다.
Event-Specific	이 워크플로는 두 가지의 유용한 기능을 제공합니다. 다음과 같은 이벤트가 자주 발생합니다. • 오탐 • 웜 • 잘못 구성된 네트워크 드물게 발생하는 이벤트는 표적 공격의 증거일 가능성이 높으므로 각별한 주의가 필요합니다. 이 워크플로는 생성된 이벤트 유형을 표시하는 페이지로 시작합니다. 그런 다음 2개의 표로 구성된 페이지가 나타나는데, 하나는 이벤트와 관련된 소스 IP 주소를 나열하고 다른 하나는 이벤트와 관련된 목적지 IP 주소를 표시합니다. 워크플로의 마지막 페이지는 이벤트의 표 보기와 패킷 보기입니다.
Events by Priority and Classification	이 워크플로는 이벤트와 그 유형을 이벤트 우선 순위에 따라 나열하며 각 이벤트의 발생 횟수 카운트도 표시합니다. 이 워크플로는 드릴다운 페이지로 시작하는데, 여기에는 각 나열된 이벤트의 우선 순위 레벨, 분류, 카운트가 포함되어 있습니다. 워크플로의 마지막 페이지는 이벤트의 표 보기와 패킷 보기입니다.
Events to Destinations	이 워크플로는 어떤 호스트 IP 주소가 공격받고 있으며 공격의 특성이 어떠한지 총괄적으로 보여줍니다. 가능한 경우 공격 관련 국가에 대한 정보도 볼 수 있습니다. 이 워크플로는 쌍을 이루는 이벤트 유형 및 목적지 IP 주소의 페이지로 시작하며, 어떤 유형의 이벤트가 특정 IP 주소를 목적지로 하는지 조사하는 데 이용할 수 있습니다. 워크플로의 마지막 페이지는 이벤트의 표 보기와 패킷 보기입니다.
IP-Specific	이 워크플로에서는 어떤 호스트 IP 주소가 가장 많은 알림을 생성하는지를 보여줍니다. 이벤트 수가 가장 많은 호스트는 일반에게 공개되는 수신 웜 유형 트래픽이거나(튜닝을 위한 조사 대상으로 적합), 알림의 원인을 확인하기 위해 추가 조사가 필요한 곳입니다. 카운트가 가장 낮은 호스트 역시 조사가 필요한데, 표적 공격의 주체일 가능성이 있습니다. 카운트가 낮으면 네트워크에 속하지 않는 호스트일 수도 있습니다. 이 워크플로는 2개의 표를 보여주는 페이지로 시작하는데, 각각 이벤트와 관련된 소스 IP 주소와 목적지 IP 주소를 나타냅니다. 그다음 페이지는 생성된 이벤트 유형을 표시합니다. 워크플로의 마지막 페이지는 이벤트의 표 보기와 패킷 보기입니다.

표 58-1 사전 정의 침입 이벤트 워크플로 (계속)

워크플로 이름	설명
Impact and Priority	이 워크플로에서는 영향이 큰 반복적 이벤트를 신속하게 찾을 수 있습니다. 보고된 영향 레벨은 이벤트가 발생한 횟수와 함께 표시됩니다. 이 정보를 사용하여 가장 자주 반복되고 큰 영향을 주는 이벤트를 식별할 수 있습니다. 이는 네트워크에 널리 확산된 공격의 지표일 수도 있습니다. 이 워크플로는 각 이벤트의 영향 레벨, 우선 순위, 카운트를 표시하는 페이지로 시작합니다. 그 다음에는 각 이벤트의 소스 및 목적지 IP 주소로 구성된 드릴다운 페이지가 나타납니다. 두 번째 페이지의 이벤트는 카운트 순으로 정렬됩니다. 워크플로의 마지막 페이지는 이벤트의 표 보기와 패킷 보기입니다.
Impact and Source	이 워크플로는 진행 중인 공격의 출처를 파악하는 데 도움이 될 수 있습니다. 보고된 영향 레벨은 이벤트의 소스 IP 주소와 함께 표시됩니다. 예를 들어 영향 레벨이 1인 이벤트가 동일한 IP 주소에서 반복적으로 발생하는 경우, 공격자가 취약한 시스템을 찾아내 표적으로 삼고 있음을 의미할 수 있습니다. 이 워크플로는 각 이벤트의 영향 레벨, 소스 IP 주소, 우선 순위, 카운트를 표시하는 페이지로 시작합니다. 각 이벤트 레벨 내에서 이벤트는 카운트, 그다음에는 우선 순위를 기준으로 정렬됩니다. 그다음에는 각 이벤트의 소스 및 목적지 IP 주소로 구성된 드릴다운 페이지가 나타납니다. 두 번째 페이지의 이벤트는 카운트 순으로 정렬됩니다. 워크플로의 마지막 페이지는 이벤트의 표 보기와 패킷 보기입니다.
Impact to Destination	이 워크플로를 통해 취약한 컴퓨터에서 반복적으로 발생하는 이벤트를 식별할 수 있어 시스템의 취약성을 해결하고 진행 중인 공격이 있을 경우 공격을 중지시킬 수 있습니다. 이 워크플로는 각 이벤트의 영향 레벨, 인라인 결과(패킷이 삭제되었는지 또는 삭제되었어야 했는지 여부), 목적지 IP 주소, 우선 순위, 카운트를 표시하는 이벤트로 시작합니다. 각 이벤트 레벨 내에서 이벤트는 카운트, 그다음에는 우선 순위를 기준으로 정렬됩니다. 그다음에는 각 이벤트의 소스 및 목적지 IP 주소로 구성된 드릴다운 페이지가 나타납니다. 두 번째 페이지의 이벤트는 카운트 순으로 정렬됩니다. 워크플로의 마지막 페이지는 이벤트의 표 보기와 패킷 보기입니다.
Source Port	이 워크플로는 어떤 서버에서 가장 많은 알림을 생성하는지 나타냅니다. 튜닝이 필요한 영역을 식별하고 주의가 필요한 서버를 확인하는 데 이 정보를 사용할 수 있습니다. 이 워크플로는 침입 이벤트 관련 소스 포트를 표시하는 페이지로 시작하고 생성된 이벤트 유형을 표시하는 페이지가 그 뒤를 잇습니다. 워크플로의 마지막 페이지는 이벤트의 표 보기와 패킷 보기입니다.
Source and Destination	이 워크플로는 다량의 알림을 공유하는 호스트 IP 주소를 식별합니다. 목록 맨 위의 쌍은 오탐일 가능성이 있는데, 따라서 튜닝이 필요한 영역을 나타내는 것일 수도 있습니다. 목록 맨 아래의 쌍은 표적 공격, 권한이 없는 리소스에 액세스하는 사용자, 네트워크에 속하지 않는 호스트인지의 여부에 대해 조사할 수 있습니다. 이 워크플로는 각 이벤트의 소스 및 목적지 IP 주소를 표시하는 페이지로 시작하고 이어서 생성된 이벤트 유형을 보여주는 페이지가 나타납니다. 워크플로의 마지막 페이지는 이벤트의 표 보기와 패킷 보기입니다.

사전 정의 악성 코드 워크플로

라이센스: 모두

지원되는 디바이스: 기능에 따라

지원되는 Defense Center: 기능에 따라

다음 표에서는 방어 센터에 포함된 사전 정의 악성코드 워크플로에 대해 설명합니다. 모든 사전 정의 악성코드 워크플로에서는 악성코드 이벤트의 표 보기를 사용합니다.

DC500 Series 2 방어 센터, Series 2 디바이스, Cisco NGIPS for Blue Coat X-Series에서는 AMP(advanced malware protection)를 지원하지 않으므로 DC500 방어 센터에서는 이 기능에 대한 데이터를 표시하지 않고 Series 2 디바이스 및 Cisco NGIPS for Blue Coat X-Series에서는 이 데이터를 탐지하지 않습니다.

악성코드 이벤트 액세스에 대한 자세한 내용은 40-17페이지의 악성코드 이벤트 작업을/를 참조하십시오.

표 58-2 사전 정의 악성 코드 워크플로

워크플로 이름	설명
Malware Summary	이 워크플로는 네트워크 트래픽에서 또는 엔드포인트 기반 FireAMP Connector에 의해 탐지된 악성코드를 개별 위협을 기준으로 그룹화한 목록을 제공합니다.
Malware Event Summary	이 워크플로에서는 다양한 악성 코드 이벤트 유형 및 하위 유형을 신속하게 분석할 수 있습니다.
Hosts Receiving Malware	이 워크플로는 악성코드를 수신한 호스트 IP 주소를 악성코드 파일의 관련 성향을 기준으로 그룹화한 목록을 제공합니다.
Hosts Sending Malware	이 워크플로는 악성코드를 보낸 호스트 IP 주소를 악성코드 파일의 관련 성향을 기준으로 그룹화한 목록을 제공합니다.
Applications Introducing Malware	이 워크플로는 파일을 수신한 호스트 IP 주소를 해당 파일의 관련 악성코드 성향을 기준으로 그룹화한 목록을 제공합니다.

사전 정의 파일 워크플로

라이센스: 보호

다음 표에서는 방어 센터에 포함된 사전 정의 파일 이벤트 워크플로에 대해 설명합니다. 모든 사전 정의 파일 이벤트 워크플로에서는 파일 이벤트의 표 보기를 사용합니다. 파일 이벤트 액세스에 대한 자세한 내용은 40-8페이지의 파일 이벤트 작업을/를 참조하십시오.

표 58-3 사전 정의 파일 워크플로

워크플로 이름	설명
File Summary	이 워크플로에서는 다양한 파일 이벤트 범주와 유형을 신속하게 분석할 수 있으며, 관련 악성코드 성향도 표시합니다.
Hosts Receiving Files	이 워크플로는 파일을 수신한 호스트 IP 주소를 해당 파일의 관련 악성코드 성향을 기준으로 그룹화한 목록을 제공합니다.
Hosts Sending Files	이 워크플로는 파일을 보낸 호스트 IP 주소를 해당 파일의 관련 악성코드 성향을 기준으로 그룹화한 목록을 제공합니다.

사전 정의 캡처 파일 워크플로

라이센스: 악성코드

지원되는 디바이스: 기능에 따라

지원되는 Defense Center: 기능에 따라

다음 표에서는 방어 센터에 포함된 사전 정의 캡처 파일 워크플로에 대해 설명합니다. 모든 사전 정의 캡처 파일 워크플로에서는 캡처 파일의 표 보기를 사용합니다.

DC500 Series 2 방어 센터, Series 2 디바이스, Cisco NGIPS for Blue Coat X-Series에서는 AMP를 지원하지 않으므로 DC500 방어 센터에서는 이 기능에 대한 데이터를 표시하지 않고 Series 2 디바이스 및 Cisco NGIPS for Blue Coat X-Series에서는 이 데이터를 탐지하지 않습니다.

캡처 파일 액세스에 대한 자세한 내용은 40-30페이지의 캡처된 파일 작업을/를 참조하십시오.

표 58-4 사전 정의 캡처 파일 워크플로

워크플로 이름	설명
Captured File Summary	이 워크플로에서는 유형, 범주, 위협 점수를 기준으로 캡처 파일을 분석할 수 있습니다.
Dynamic Analysis Status	이 워크플로에서는 캡처 파일이 동적 분석을 위해 제출되었는지 여부에 따라 그 카운트를 제공합니다.

사전 정의 연결 데이터 워크플로

라이센스: FireSIGHT

다음 표에서는 방어 센터에 포함된 사전 정의 연결 데이터 워크플로에 대해 설명합니다. 모든 사전 정의 연결 데이터 워크플로에서 연결 데이터의 표 보기를 사용합니다. 연결 데이터 액세스에 대한 자세한 내용은 39-14페이지의 연결 및 보안 인텔리전스 데이터 보기을/를 참조하십시오.

표 58-5 사전 정의 연결 데이터 워크플로

워크플로 이름	설명
Connection Events	이 워크플로에서는 기본 연결 및 탐지된 애플리케이션 정보에 대한 요약 보기를 제공하며, 이를 사용하여 이벤트 표 보기로 드릴다운할 수 있습니다.
Connections by Application	이 워크플로에서는 모니터링되는 네트워크 세그먼트에서 탐지된 연결 수를 기준으로 가장 활동적인 10개의 애플리케이션을 그래프로 나타냅니다.
Connections by Initiator	이 워크플로에서는 모니터링되는 네트워크 세그먼트에서 호스트가 연결 트랜잭션을 시작한 연결의 수를 기준으로 가장 활동적인 10개의 호스트 IP 주소를 그래프로 나타냅니다.
Connections by Port	이 워크플로에서는 모니터링되는 네트워크 세그먼트에서 탐지된 연결 수를 기준으로 가장 활동적인 10개의 포트를 그래프로 나타냅니다.
Connections by Responder	이 워크플로에서는 모니터링되는 네트워크 세그먼트에서 호스트 IP 주소가 연결 트랜잭션의 responder인 연결의 수를 기준으로 가장 활동적인 10개의 호스트 IP 주소를 그래프로 나타냅니다.
Connections over Time	이 워크플로에서는 모니터링되는 네트워크 세그먼트에서 시간의 경과에 따른 총 연결 수를 그래프로 나타냅니다.
Traffic by Application	이 워크플로에서는 모니터링되는 네트워크 세그먼트에서 전송된 킬로바이트 수를 기준으로 가장 활동적인 10개의 애플리케이션을 그래프로 나타냅니다.
Traffic by Initiator	이 워크플로에서는 모니터링되는 네트워크 세그먼트에서 각 주소로부터 전송된 총 킬로바이트 수를 기준으로 가장 활동적인 10개의 호스트 IP 주소를 그래프로 나타냅니다.
Traffic by Port	이 워크플로에서는 모니터링되는 네트워크 세그먼트에서 전송된 킬로바이트 수를 기준으로 가장 활동적인 10개의 포트를 그래프로 나타냅니다.
Traffic by Responder	이 워크플로에서는 모니터링되는 네트워크 세그먼트에서 각 주소가 수신한 총 킬로바이트 수를 기준으로 가장 활동적인 10개의 호스트 IP 주소를 그래프로 나타냅니다.
Traffic over Time	이 워크플로에서는 모니터링되는 네트워크 세그먼트에서 시간의 경과에 따른 총 전송 킬로바이트 수를 그래프로 나타냅니다.

표 58-5 사전 정의 연결 데이터 워크플로 (계속)

워크플로 이름	설명
Unique Initiators by Responder	이 워크플로에서는 모니터링되는 네트워크 세그먼트에서 각 주소에 연결한 고유 initiator 수를 기준으로 가장 활동적인 10개의 응답 호스트 IP 주소를 그래프로 나타냅니다.
Unique Responders by Initiator	이 워크플로에서는 모니터링되는 네트워크 세그먼트에서 각 주소가 연결한 고유 responder 수를 기준으로 가장 활동적인 10개의 발신 호스트 IP 주소를 그래프로 나타냅니다.

사전 정의 보안 인텔리전스 워크플로

라이센스: 보호

지원되는 디바이스: Series 2를 제외하고 모두

지원되는 Defense Center: DC500을 제외하고 모두

다음 표에서는 방어 센터에 포함된 사전 정의 보안 인텔리전스 워크플로에 대해 설명합니다. 모든 사전 정의 보안 인텔리전스 워크플로에서는 보안 인텔리전스 이벤트의 표 보기를 사용합니다. 보안 인텔리전스 이벤트 데이터의 액세스에 대한 자세한 내용은 39-14페이지의 연결 및 보안 인텔리전스 데이터 보기을/를 참조하십시오.

표 58-6 사전 정의 보안 인텔리전스 워크플로

워크플로 이름	설명
Security Intelligence Events	이 워크플로에서는 기본 보안 인텔리전스 및 탐지된 애플리케이션 정보에 대한 요약 보기를 제공하며, 이를 사용하여 이벤트 표 보기로 드릴다운할 수 있습니다.
Security Intelligence Summary	이 워크플로는 Security Intelligence Events 워크플로와 동일하지만 보안 인텔리전스 이벤트를 범주 및 카운트별로만 나열하는 Security Intelligence Summary 페이지로 시작합니다.

사전 정의 호스트 워크플로

라이센스: FireSIGHT

다음 표에서는 호스트 데이터와 함께 사용할 수 있는 사전 정의 워크플로에 대해 설명합니다.

표 58-7 사전 정의 호스트 워크플로

워크플로 이름	설명
Hosts	이 워크플로에서는 호스트의 표 보기에 이어 호스트 보기가 표시됩니다. 호스트 테이블 기반의 워크플로 보기에서는 어떤 호스트와 관련된 모든 IP 주소의 데이터를 편리하게 볼 수 있습니다. 자세한 내용은 50-19페이지의 호스트 보기을/를 참조하십시오.
Operating System Summary	이 워크플로를 사용하여 네트워크에서 사용 중인 운영 체제를 분석할 수 있습니다. 이 워크플로에서 제공하는 일련의 페이지는 네트워크의 운영 체제 및 운영 체제 공급업체의 목록에서 시작하여 해당 운영 체제의 각 버전을 실행하는 호스트의 수로 이어집니다. 다음 페이지에서는 중요도, IP 주소, NetBIOS 이름을 기준으로 호스트를 나열하는데, 해당 운영 체제 및 운영 체제 공급업체도 표시됩니다. 이 워크플로는 호스트의 표 보기와 호스트 보기로 끝납니다. 자세한 내용은 50-19페이지의 호스트 보기을/를 참조하십시오.

사전 정의 IOC 워크플로

라이센스: FireSIGHT

다음 표에서는 IOC 데이터와 함께 사용할 수 있는 사전 정의 워크플로에 대해 설명합니다.

표 58-8 사전 정의 IOC 워크플로

워크플로 이름	설명
Indications of Compromise	이 워크플로는 IOC 데이터를 카운트 및 범주별로 그룹화한 요약 보기로 시작합니다. 이어서 요약 데이터를 이벤트 유형별로 세분화하는 세부사항 보기가 나타납니다. 그다음은 IOC 데이터의 전체 표 보기입니다. 이 워크플로는 호스트 보기로 마무리됩니다. IOC 데이터를 보고 해석하는 것에 대한 자세한 내용은 50-32페이지의 IOC 작업을/를 참조하십시오.
Indications of Compromise by Host	이 워크플로를 사용하여 네트워크의 어떤 호스트가 공격받을 가능성이 가장 높은지 (IOC 데이터를 기반으로) 평가할 수 있습니다. 이 워크플로에서는 IOC 데이터 카운트 기준 호스트 IP 주소의 보기, IOC 데이터의 표 보기, 마지막으로 호스트 보기가 표시됩니다. IOC 데이터를 보고 해석하는 것에 대한 자세한 내용은 50-32페이지의 IOC 작업을/를 참조하십시오.

사전 정의 애플리케이션 워크플로

라이센스: FireSIGHT

다음 표에서는 애플리케이션 데이터와 함께 사용할 수 있는 사전 정의 워크플로에 대해 설명합니다.

표 58-9 사전 정의 애플리케이션 워크플로

워크플로 이름	설명
Application Business Relevance	이 워크플로를 사용하여 네트워크의 예상 비즈니스 타당성 레벨별로 실행 중인 애플리케이션을 분석함으로써 네트워크 리소스가 적절하게 사용되는지 모니터링할 수 있습니다. 이 워크플로는 각 타당성 레벨의 애플리케이션을 실행 중인 호스트의 수로 시작하여 개별 애플리케이션과 그 비즈니스 타당성 레벨 및 호스트 수가 표시되는 표, 애플리케이션 표 보기, 호스트 보기로 이어집니다. 자세한 내용은 50-41페이지의 애플리케이션 보기을/를 참조하십시오.
Application Category	이 워크플로를 사용하여 네트워크에서 범주(예: 이메일, 검색 엔진, 소셜 네트워킹)별로 실행 중인 애플리케이션을 분석함으로써 네트워크 리소스가 적절하게 사용되는지 모니터링할 수 있습니다. 이 워크플로는 각 범주의 애플리케이션을 실행 중인 호스트의 수로 시작하여 개별 애플리케이션을 실행 중인 호스트의 수, 애플리케이션의 표 보기, 호스트 보기로 이어집니다. 자세한 내용은 50-41페이지의 애플리케이션 보기을/를 참조하십시오.
Application Risk	이 워크플로를 사용하여 네트워크에서 각 예상 보안 위험 레벨의 실행 중인 애플리케이션을 분석함으로써 사용자 활동의 잠재적 리스크를 추정하고 적절한 조치를 취할 수 있습니다. 이 워크플로는 각 위험 레벨의 애플리케이션을 실행 중인 호스트의 수로 시작하여 개별 애플리케이션과 그 비즈니스 타당성 레벨 및 호스트 수가 표시되는 표, 애플리케이션 표 보기, 호스트 보기로 이어집니다. 자세한 내용은 50-41페이지의 애플리케이션 보기을/를 참조하십시오.

표 58-9 사전 정의 애플리케이션 워크플로 (계속)

워크플로 이름	설명
Application Summary	이 워크플로를 사용하여 네트워크의 애플리케이션 및 해당 호스트에 대한 세부 정보를 얻어 호스트 애플리케이션 활동을 면밀하게 조사할 수 있습니다. 이 워크플로는 애플리케이션을 실행하는 개별 호스트 IP 주소의 목록으로 시작하여 애플리케이션의 표 보기 및 호스트 보기로 이어집니다.
Applications	이 워크플로를 사용하여 네트워크에서 실행 중인 애플리케이션을 분석함으로써 네트워크가 어떻게 사용되고 있는가를 개괄적으로 파악할 수 있습니다. 이 워크플로는 개별 애플리케이션을 실행 중인 호스트 수로 시작하여 애플리케이션 표 보기 및 호스트 보기로 이어집니다. 자세한 내용은 50-41페이지의 애플리케이션 보기을/를 참조하십시오.

사전 정의 애플리케이션 세부사항 워크플로

라이센스: FireSIGHT

다음 표에서는 애플리케이션 세부사항 및 클라이언트 데이터와 함께 사용할 수 있는 사전 정의 워크플로에 대해 설명합니다.

표 58-10 사전 정의 애플리케이션 세부사항 워크플로

워크플로 이름	설명
Application Details	이 워크플로를 사용하여 네트워크의 클라이언트 애플리케이션을 더 자세히 분석할 수 있습니다. 이 워크플로를 구성하는 일련의 페이지에서는 먼저 네트워크의 클라이언트 애플리케이션 및 애플리케이션 제품의 목록으로 시작하며 각 애플리케이션을 실행하는 호스트 수도 표시합니다. 그 다음에는 해당 애플리케이션의 각 버전을 실행하는 호스트 수를 표시합니다. 그 다음 페이지에서는 특정 호스트에서 어떤 애플리케이션을 가장 자주 액세스했는지를 식별할 수 있습니다. 그런 다음 클라이언트 애플리케이션의 표 보기와 호스트 보기로 이어집니다. 자세한 내용은 50-46페이지의 애플리케이션 세부사항 보기을/를 참조하십시오.
Clients	이 워크플로에서는 클라이언트 애플리케이션의 표 보기에 이어 호스트 보기가 표시됩니다. 자세한 내용은 50-46페이지의 애플리케이션 세부사항 보기을/를 참조하십시오.

사전 정의 서버 워크플로

라이센스: FireSIGHT

다음 표에서는 서버 데이터와 함께 사용할 수 있는 사전 정의 워크플로에 대해 설명합니다.

표 58-11 사전 정의 서버 워크플로

워크플로 이름	설명
Network Applications by Count	이 워크플로를 사용하여 네트워크에서 가장 자주 사용되는 애플리케이션을 분석할 수 있습니다. 이 워크플로를 구성하는 일련의 페이지에서는 각 애플리케이션이 실행되는 호스트 수와 함께 애플리케이션을 표시한 다음 각 애플리케이션의 공급업체와 버전을 추가합니다. 그런 다음 호스트별 애플리케이션을 나열하는 표 보기와 호스트 보기로 마무리됩니다. 자세한 내용은 50-36페이지의 서버 보기을/를 참조하십시오.
Network Applications by Hit	이 워크플로를 사용하여 네트워크에서 가장 활동적인 애플리케이션을 분석할 수 있습니다. 이 워크플로를 구성하는 일련의 페이지에서는 애플리케이션을 각 애플리케이션이 액세스되는 빈도 수와 함께 표시하고 각 애플리케이션의 공급업체 및 버전 정보를 추가합니다. 그런 다음 호스트별 애플리케이션을 나열하는 표 보기와 호스트 보기가 포함된 페이지로 마무리됩니다. 자세한 내용은 50-36페이지의 서버 보기을/를 참조하십시오.
Server Details	이 워크플로를 사용하여 탐지된 서버 애플리케이션 프로토콜의 공급업체 및 버전을 더 자세히 분석할 수 있습니다. 이 워크플로에는 서버 및 해당 벤더의 목록, 서버와 공급업체 및 버전의 상관관계를 보여주는 목록, 마지막으로 서버의 표 보기 및 호스트 보기가 포함됩니다.
Servers	이 워크플로에서는 애플리케이션의 표 보기에 이어 호스트 보기가 표시됩니다. 자세한 내용은 50-36페이지의 서버 보기을/를 참조하십시오.

사전 정의 호스트 특성 워크플로

라이센스: FireSIGHT

다음 표에서는 호스트 특성 데이터와 함께 사용할 수 있는 사전 정의 워크플로에 대해 설명합니다.

표 58-12 사전 정의 호스트 특성 워크플로

워크플로 이름	설명
Attributes	이 워크플로를 사용하여 네트워크에 있는 호스트의 IP 주소 및 호스트의 상태를 모니터링할 수 있습니다. 이 워크플로는 개별 IP 주소를 현재 사용자, 호스트 중요도, 메모, 화이트리스트 준수 여부와 함께 나열하는 호스트 특성 표 보기로 시작합니다. 마지막으로 호스트 보기를 표시합니다. 자세한 내용은 50-27페이지의 호스트 특성 보기을/를 참조하십시오.

사전 정의 검색 이벤트 워크플로

라이센스: FireSIGHT

다음 표에서는 검색 이벤트 데이터와 함께 사용할 수 있는 사전 정의 워크플로에 대해 설명합니다.

표 58-13 사전 정의 검색 이벤트 워크플로

워크플로 이름	설명
Discovery Events	이 워크플로에서는 검색 이벤트의 세부 목록을 표 보기 형태로 제공하고 이어서 호스트 보기를 표시합니다. 자세한 내용은 50-15페이지의 검색 이벤트 테이블 이해을/를 참조하십시오.

사전 정의 사용자 워크플로

라이센스: FireSIGHT

다음 표에서는 방어 센터에 포함된 사전 정의 사용자 워크플로에 대해 설명합니다.

표 58-14 사전 정의 사용자 워크플로

워크플로 이름	설명
Users	이 워크플로에서는 사용자 이벤트 또는 LDAP 서버 연결로부터 수집한 사용자 정보의 목록을 제공합니다. 사용자 ID 워크플로에 대한 자세한 내용은 50-61페이지의 사용자 보기을/를 참조하십시오.

사전 정의 취약성 워크플로

라이센스: FireSIGHT

다음 표에서는 방어 센터에 포함된 사전 정의 취약성 워크플로에 대해 설명합니다.

표 58-15 사전 정의 취약성 워크플로

워크플로 이름	설명
Vulnerabilities	이 워크플로에서는 데이터베이스에 있는 모든 취약성을 표시하는 취약성 표 보기에 이어 네트워크에서 탐지된 호스트에 적용되는 활성 취약성만 표시하는 표 보기가 나타납니다. 마지막으로 제약 조건에 부합하는 모든 취약성에 대해 자세히 설명하는 취약성 세부사항 보기가 나타납니다. 자세한 내용은 50-50페이지의 취약성 보기을/를 참조하십시오.

사전 정의 서드파티 취약성 워크플로

라이센스: FireSIGHT

다음 표에서는 방어 센터에 포함된 사전 정의 서드파티 취약성 워크플로에 대해 설명합니다.

표 58-16 사전 정의 서드파티 취약성 워크플로

워크플로 이름	설명
Vulnerabilities by IP Address	이 워크플로를 사용하여 모니터링되는 네트워크의 호스트 IP 주소별로 탐지된 서드파티 취약성의 수를 신속하게 확인할 수 있습니다. 이 워크플로는 서드파티 취약성의 표 보기 및 호스트 보기로 마무리됩니다. 자세한 내용은 50-56페이지의 서드파티 취약성 보기을/를 참조하십시오.
Vulnerabilities by Source	이 워크플로를 사용하여 서드파티 취약성 소스(예: QualysGuard Scanner)별로 탐지된 서드파티 취약성의 수를 신속하게 확인할 수 있습니다. 이 워크플로에서는 중간 단계의 드릴다운 페이지에서 이 취약성에 대한 세부사항을 제공한 다음 서드파티 취약성의 표 보기 및 호스트 보기로 마무리됩니다. 자세한 내용은 50-56페이지의 서드파티 취약성 보기을/를 참조하십시오.

사전 정의 상관관계 및 화이트리스트 워크플로

라이센스: FireSIGHT

상관관계 데이터, 화이트리스트 이벤트, 화이트리스트 위반, 교정 상태 이벤트의 유형별로 사전 정의 워크플로가 있습니다.

표 58-17 사전 정의 상관관계 워크플로

워크플로 이름	설명
Correlation Events	이 워크플로는 상관관계 이벤트의 표 보기로 구성됩니다. 자세한 내용은 51-51페이지의 상관관계 이벤트 작업을/를 참조하십시오.
White List Events	이 워크플로는 화이트리스트 이벤트의 표 보기로 구성됩니다. 자세한 내용은 52-30페이지의 화이트리스트 이벤트 작업을/를 참조하십시오.
Host Violation Count	이 워크플로는 하나 이상의 화이트리스트를 위반하는 모든 호스트 IP 주소를 나열하는 일련의 페이지로 구성됩니다. 첫 페이지에서는 주소별 위반 수를 기준으로 주소를 정렬하는데, 위반 수가 가장 많은 IP 주소가 맨 위에 옵니다. 호스트 IP 주소가 둘 이상의 화이트리스트를 위반할 경우 위반된 화이트리스트별로 별도의 행이 있습니다. 이 워크플로에는 모든 위반을 나열하는 화이트리스트 위반의 표 보기도 포함되는데, 가장 최근에 탐지된 위반이 맨 위에 옵니다. 표의 각 행에는 탐지된 하나의 위반이 있습니다. 자세한 내용은 52-35페이지의 화이트리스트 위반 작업을/를 참조하십시오.
White List Violations	이 워크플로에는 모든 위반을 나열하는 화이트리스트 위반의 표 보기가 포함되는데, 가장 최근에 탐지된 위반이 맨 위에 옵니다. 표의 각 행에는 탐지된 하나의 위반이 있습니다. 자세한 내용은 52-35페이지의 화이트리스트 위반 작업을/를 참조하십시오.
Status	이 워크플로는 교정 상태의 표 보기로 구성됩니다. 여기에는 위반한 정책의 이름, 적용된 교정의 이름과 상태가 포함됩니다. 자세한 내용은 54-17페이지의 교정 상태 이벤트 작업을/를 참조하십시오.

사전 정의 시스템 워크플로

라이센스: 모두

FireSIGHT 시스템에서는 몇 가지 추가 워크플로를 제공하는데, 여기에는 감사 이벤트 및 상태 이벤트와 같은 시스템 이벤트 뿐만 아니라 규칙 업데이트 가져오기 및 활성 검사의 결과를 나열하는 워크플로도 포함됩니다.

표 58-18 추가 사전 정의 워크플로

워크플로 이름	설명
Audit Log	이 워크플로는 감사 이벤트를 나열하는 감사 로그의 표 보기로 구성됩니다. 자세한 내용은 69-2페이지의 감사 레코드 보기을/를 참조하십시오.
Health Events	이 워크플로에서는 상태 모니터링 정책에 의해 트리거되는 이벤트를 표시합니다. 자세한 내용은 68-50페이지의 Health Events 테이블 보기 작업을/를 참조하십시오.
Rule Update Import Log	이 워크플로는 성공한 규칙 업데이트 가져오기 및 실패한 규칙 업데이트 가져오기에 대한 정보를 나열하는 표 보기로 구성됩니다. 자세한 내용은 66-14페이지의 규칙 업데이트 및 로컬 규칙 파일 가져오기을/를 참조하십시오.
Scan Results	이 워크플로는 완료된 각 검사를 나열하는 표 보기로 구성됩니다. 자세한 내용은 47-19페이지의 활성 스캔 결과 작업을/를 참조하십시오.

저장된 사용자 지정 워크플로

라이센스: 보호 + FireSIGHT

수정 불가한 사전 정의 워크플로 외에도 방어 센터에는 여러 저장된 사용자 지정 워크플로가 있습니다. 이 워크플로 각각은 사용자 지정 테이블을 기반으로 하며 수정 가능합니다. 이 워크플로에 액세스하는 방법에 대해서는 59-9페이지의 사용자 지정 테이블을 기반으로 워크플로 보기을/를 참조하십시오.

표 58-19 저장된 사용자 지정 워크플로

워크플로 이름	설명
Events by Impact, Priority, and Host Criticality	이 워크플로를 사용하여 네트워크에 중요한 호스트, 현재 취약한 호스트, 현재 공격을 받고 있는 호스트를 신속하게 선별하여 집중할 수 있습니다. 기본적으로 이 워크플로는 영향 레벨, 호스트 중요도, 이벤트 발생 횟수의 순서대로 정렬되는 이벤트 요약으로 시작합니다. 워크플로의 두 번째 페이지를 사용하여 특정 이벤트가 발생한 소스 및 목적지 주소를 드릴다운 및 확인할 수 있습니다. 이 워크플로는 침입 이벤트와 목적지 중요도의 표 보기 및 패킷 보기로 마무리됩니다. 이 워크플로는 Intrusion Events with Destination Criticality 사용자 지정 테이블을 기반으로 합니다. 자세한 내용은 59-1페이지의 사용자 지정 테이블 이해을/를 참조하십시오.
Events by Priority and Classification	이 워크플로는 이벤트와 그 유형을 이벤트 우선 순위에 따라 나열하며 각 이벤트의 발생 횟수 카운트도 표시합니다. 이 워크플로는 드릴다운 페이지로 시작하는데, 여기에는 각 나열된 이벤트의 우선 순위 레벨, 분류, 카운트가 포함되어 있습니다. 워크플로의 마지막 페이지는 이벤트의 표 보기와 패킷 보기입니다. 이 워크플로는 Intrusion Events 사용자 지정 테이블을 기반으로 합니다. 자세한 내용은 59-1페이지의 사용자 지정 테이블 이해을/를 참조하십시오.
Events with Destination, Impact, and Host Criticality	이 워크플로를 사용하여 현재 취약한 상태이며 네트워크에 중요한 호스트에서 발생한 최근의 공격을 확인할 수 있습니다. 기본적으로 이 워크플로는 최근 이벤트를 영향 레벨 순으로 정렬한 목록으로 시작합니다. 이 워크플로의 다음 페이지에서는 Intrusion Events with Destination Criticality 표 보기와 패킷 보기를 제공합니다. 이 워크플로는 Intrusion Events with Destination Criticality 사용자 지정 테이블을 기반으로 합니다. 자세한 내용은 59-1페이지의 사용자 지정 테이블 이해을/를 참조하십시오.
Hosts with Servers Default Workflow	이 워크플로를 사용하여 Hosts with Servers 사용자 지정 테이블의 기본 정보를 신속하게 볼 수 있습니다. 기본적으로 이 워크플로는 호스트와 서버의 표 보기로 시작하고 호스트 보기로 이어집니다. 이 워크플로는 Hosts with Servers 사용자 지정 테이블을 기반으로 합니다. 자세한 내용은 59-1페이지의 사용자 지정 테이블 이해을/를 참조하십시오.
Intrusion Events with Destination Criticality Default Workflow	이 워크플로를 사용하여 Intrusion Events with Destination Criticality 사용자 지정 테이블의 기본 정보를 신속하게 볼 수 있습니다. 기본적으로 이 워크플로는 Intrusion Events with Destination Criticality 표 보기로 시작하고 패킷 보기로 이어집니다. 이 워크플로는 Intrusion Events with Destination Criticality 사용자 지정 테이블을 기반으로 합니다. 자세한 내용은 59-1페이지의 사용자 지정 테이블 이해을/를 참조하십시오.

표 58-19 저장된 사용자 지정 워크플로 (계속)

워크플로 이름	설명
Intrusion Events with Source Criticality Default Workflow	이 워크플로를 사용하여 Intrusion Events with Source Criticality 사용자 지정 테이블의 기본 정보를 신속하게 볼 수 있습니다. 기본적으로 이 워크플로는 Intrusion Events with Source Criticality 표 보기로 시작하고 패킷 보기로 이어집니다. 이 워크플로는 Intrusion Events with Source Criticality 사용자 지정 테이블을 기반으로 합니다. 자세한 내용은 59-1페이지의 사용자 지정 테이블 이해을/를 참조하십시오.
Server and Host Details	이 워크플로를 사용하여 네트워크에서 어떤 서버가 가장 많이 사용되었는지 그리고 어떤 호스트에서 이 서버를 실행하고 있는지를 확인할 수 있습니다. 기본적으로 이 워크플로는 서비스별 액세스 빈도를 포함한 서버의 요약으로 시작합니다. 다음 페이지에서는 운영 체제 공급업체 및 버전별로 서버를 나열합니다. 이 워크플로는 호스트와 서버의 표 보기 및 호스트 보기로 마무리됩니다. 이 워크플로는 Hosts with Servers 사용자 지정 테이블을 기반으로 합니다. 자세한 내용은 59-1페이지의 사용자 지정 테이블 이해을/를 참조하십시오.

워크플로 사용

라이센스: 모두

워크플로의 드릴다운 및 표 보기 페이지를 통해 신속하게 데이터 보기의 범위를 한정하여 분석에 중요한 이벤트에 초점을 맞출 수 있습니다. 각 워크플로 유형의 데이터가 저마다 다르지만 모든 워크플로가 공유하는 공통 기능이 있습니다. 다음 절에서는 이 기능과 그 사용 방법에 대해 설명합니다.

- 58-16페이지의 워크플로 선택에서는 워크플로 선택 페이지 및 사용할 워크플로를 선택하는 방법에 대해 설명합니다.
- 58-17페이지의 워크플로 도구 모음 이해에서는 워크플로에 제공되는 도구 모음 옵션에 대해 설명합니다.
- 58-18페이지의 워크플로 페이지 사용에서는 모든 워크플로 페이지에 나타나는 기능 및 그 사용 방법에 대해 설명합니다.
- 58-22페이지의 이벤트 시간 제약 조건 설정에서는 이벤트 기반 워크플로의 시간 범위를 설정하는 방법에 대해 설명합니다. 워크플로에는 지정된 시간 범위에서 생성된 이벤트가 포함됩니다.
- 58-30페이지의 이벤트 제한에서는 워크플로에서 워크플로 데이터 보기를 제한하거나 좁히고 워크플로 페이지를 이동하는 데 사용되는 기능에 대해 설명합니다.
- 58-32페이지의 복합 제약 조건 사용에서는 복합 제약 조건을 사용하는 방법을 예시와 함께 설명합니다.
- 58-34페이지의 드릴다운 워크플로 페이지 정렬에서는 워크플로에 표시되는 데이터를 장렬하고 표시할 표 열을 제거하고 복원하는 기능에 대해 설명합니다.
- 58-34페이지의 워크플로 페이지의 행 선택에서는 표시된 표에서 분석할 데이터 열을 선택하거나 다른 작업을 수행할 데이터 열을 선택하는 방법에 대해 설명합니다.
- 58-35페이지의 워크플로의 다른 페이지로 이동에서는 현재 워크플로에서 선택된 이벤트를 포함한 제약 조건을 사용하여 다른 워크플로를 여는 방법에 대해 설명합니다.
- 58-35페이지의 워크플로 간 이동에서는 **Jump to** 드롭다운 목록 및 이 목록을 사용하여 현재 제약 조건을 다른 워크플로에 적용하는 방법에 대해 설명합니다.
- 60-1페이지의 이벤트 검색에서는 이벤트 데이터 검색에 사용되는 기능에 대한 정보를 제공합니다.
- 58-36페이지의 북마크 사용에서는 북마크를 생성, 관리, 사용하는 방법에 대해 설명합니다.

워크플로 선택

라이센스: 모두

FireSIGHT 시스템에서는 다음 표에 나열된 데이터 유형에 대해 사전 정의 워크플로를 제공합니다.

표 58-20 워크플로를 사용하는 기능

기능	메뉴 경로	옵션
Intrusion events	Analysis > Intrusions	Events Reviewed Events Clipboard Incidents
Malware events	Analysis > Files	Malware Events
File events	Analysis > Files	File Events
Captured files	Analysis > Files	Captured Files
Connection events	Analysis > Connections	Events
Security Intelligence events	Analysis > Connections	Security Intelligence Events
Host events	Analysis > Hosts	Network Map Hosts Indications of Compromise Applications Application Details Servers Host Attributes Discovery Events
User events	Analysis > Users	User Activity Users
Vulnerability events	Analysis > Vulnerabilities	Vulnerabilities Third-Party Vulnerabilities
Correlation events	Analysis > Correlation	Correlation Events White List Events White List Violations Status
Audit events	System > Monitoring	Audit
Health events	Health > Health Events	해당 없음
Rule Update Import Log	System > Updates	해당 없음
Scan Results	Policies > Actions > Scanners	해당 없음

위 표에 있는 데이터 유형을 표시할 경우 그 데이터의 기본 워크플로 중 첫 페이지에 이벤트가 나타납니다.

또한 워크플로 액세스는 다음과 같이 사용자 역할에 따라 달라집니다(61-48페이지의 사용자 역할 구성 참조).

- 관리자 권한을 가진 사용자는 어떤 워크플로에도 액세스할 수 있으며 감사 로그, 검사 결과, 규칙 업데이트 가져오기 로그에 액세스할 수 있는 유일한 사용자입니다.
- 유지보수 권한을 가진 사용자는 상태 이벤트에 액세스할 수 있습니다.
- 보안 분석가 및 보안 분석가(읽기 전용) 권한을 가진 사용자는 침입, 악성코드, 파일, 연결, 검색, 취약성, 상관관계, 상태 워크플로에 액세스할 수 있습니다.

기본 워크플로가 아닌 워크플로를 사용하여 데이터를 보려면

액세스: Admin/Any Security Analyst

1단계 워크플로를 사용하는 기능 표에 설명된 적합한 메뉴 경로와 옵션을 선택합니다.

해당 데이터 유형의 기본 워크플로 중 첫 페이지가 나타납니다. 다른 기본 워크플로를 지정하는 것에 대한 자세한 내용은 71-3페이지의 이벤트 보기 설정 구성을/를 참조하십시오.

2단계 다른 워크플로를 선택할 수도 있습니다. 워크플로 제목 옆의 **(워크플로 전환)**을 클릭하고 사용할 워크플로를 선택합니다.

3단계 선택한 워크플로의 첫 페이지가 나타납니다.

워크플로 도구 모음 이해

라이센스: 모두

워크플로의 각 페이지에는 관련 기능에 빠르게 액세스할 수 있는 도구 모음이 있습니다. 다음 표에서는 도구 모음의 각 링크에 대해 설명합니다.

표 58-21 워크플로 도구 모음 링크

기능	설명
Bookmark This Page	현재 페이지에 북마크를 지정하여 나중에 다시 돌아올 수 있게 합니다. 북마크는 현재 보고 있는 페이지에 적용된 제약 조건을 캡처하므로 나중에 (데이터가 그대로 있을 경우) 동일한 데이터로 돌아올 수 있습니다. 북마크 생성에 대한 자세한 내용은 58-36페이지의 북마크 사용을/를 참조하십시오.
Report Designer	현재 제약 조건이 적용된 워크플로를 선택 기준으로 하는 보고서 디자인 도구를 엽니다. 보고서 생성에 대한 자세한 내용은 57-9페이지의 이벤트 보기에서 보고서 템플릿 생성을/를 참조하십시오.
Dashboard	현재 워크플로와 관련된 대시보드를 엽니다. 예를 들어 Connection Events 워크플로는 Connection Summary 대시보드와 연결됩니다. 대시보드 사용에 대한 자세한 내용은 55-1페이지의 대시보드 사용을/를 참조하십시오.
View Bookmarks	선택 가능한 저장된 북마크의 목록을 표시합니다. 북마크 생성 및 관리에 대한 자세한 내용은 58-36페이지의 북마크 사용을/를 참조하십시오.
Search	워크플로의 데이터에 대한 고급 검색을 수행할 수 있는 Search 페이지를 표시합니다. 아래쪽 화살표 아이콘을 클릭하여 저장된 검색을 선택하고 사용할 수도 있습니다. 워크플로 선택에 대한 자세한 내용은 60-1페이지의 이벤트 검색을/를 참조하십시오.

워크플로 페이지 사용

라이센스: 모두

워크플로 페이지에서 수행할 수 있는 작업은 페이지 유형에 따라 달라집니다. 표 보기 페이지 및 드릴다운 페이지에서는 표시할 이벤트 집합을 제한하거나 워크플로를 이동하는 데 사용할 수 있는 여러 기능을 제공합니다. 각 페이지 유형에서 사용 가능한 기능에 대한 자세한 내용은 다음 절을 참조하십시오.

- 58-18페이지의 공통 표 보기 또는 드릴다운 페이지 기능 사용
- 58-20페이지의 지오로케이션 사용
- 58-21페이지의 표 보기 페이지 사용
- 58-22페이지의 드릴다운 페이지 사용
- 58-22페이지의 호스트 보기, 패킷 보기 또는 취약성 세부사항 페이지 사용

공통 표 보기 또는 드릴다운 페이지 기능 사용

라이센스: 모두

표 보기 및 드릴다운 워크플로 페이지의 표 헤더 및 표 행에서는 표시된 데이터에 대한 작업을 수행하는 데 사용할 수 있는 아이콘 및 기타 기능을 제공합니다.

이 기능에 대해 다음 표에서 설명합니다.

표 58-22 표 보기 및 드릴다운 페이지 기능

기능	설명
	파란색 아래쪽 화살표 아이콘을 클릭하여 워크플로의 다음 페이지에 해당 행을 표시합니다.
 (정상)  (악성코드)  (사용자 지정 탐지)  (알 수 없음)  (사용 불가능)	파일 이름 및 SHA-256 해시 값 열에 나타나는 네트워크 파일 전파 흔적 아이콘을 클릭하여 파일의 전파 흔적 지도를 새 창에 표시합니다. 자세한 내용은 40-38페이지의 네트워크 파일 전파 흔적 분석을/를 참조하십시오. DC500 방어 센터, Series 2 디바이스, Cisco NGIPS for Blue Coat X-Series에서는 AMP를 지원하지 않으므로 이 어플라이언스에서는 네트워크 기반 악성코드 및 파일 이벤트에 대한 네트워크 파일 전파 흔적을 볼 수 없습니다.
  (침입 당했을 가능성 있음)  (블랙리스트에 등록됨)  (블랙리스트에 등록됨, 모니터링 대상으로 설정)	IP 주소 열에 나타나는 호스트 프로필 아이콘을 클릭하여 해당 IP 주소의 호스트 프로필을 팝업 창에 표시합니다. 자세한 내용은 49-1페이지의 호스트 프로필 사용을/를 참조하십시오. 트리거된 IOC 규칙에 의해 공격 가능성 태그가 지정된 호스트는 일반 아이콘이 아닌 공격 호스트 아이콘과 함께 나타납니다. IOC에 대한 자세한 내용은 45-20페이지의 IOC 이해을/를 참조하십시오. 호스트 프로필 아이콘이 회색으로 표시될 경우 호스트가 네트워크 지도에 포함될 수 없으므로(예: `0.0.0.0`) 호스트 프로필을 볼 수 없습니다. 보안 인텔리전스 데이터를 기반으로 트래픽 필터링을 수행하는 경우 연결 이벤트 보기에서 블랙리스트 및 모니터링 대상 IP 주소 옆의 호스트 아이콘이 약간 다르게 나타납니다. 그러면 연결의 어떤 호스트가 블랙리스트에 포함되었는지 쉽게 식별할 수 있습니다. DC500 방어 센터 및 Series 2 디바이스 모두 보안 인텔리전스 데이터를 지원하지 않습니다.

표 58-22 표 보기 및 드릴다운 페이지 기능 (계속)

기능	설명
●○○○ (위협 점수 낮음) ●●○○ (위협 점수 중간) ●●●○ (위협 점수 높음) ●●●● (위협 점수 매우 높음)	위협 점수 열에 나타나는 위협 점수 아이콘을 클릭하여 어떤 파일의 최고 위협 점수에 대한 Dynamic Analysis Summary 보고서를 표시합니다. DC500 방어 센터, Series 2 디바이스, Cisco NGIPS for Blue Coat X-Series에서는 AMP를 지원하지 않으므로 이 어플라이언스에서는 Dynamic Analysis Summary 보고서를 볼 수 없습니다.
	사용자 ID 열에 나타나는 사용자 아이콘을 클릭하여 사용자 프로필 정보를 봅니다. 자세한 내용은 50-63페이지의 사용자 세부사항 및 호스트 기록 이해을/를 참조하십시오. 사용자 아이콘이 회색으로 표시될 경우 사용자가 데이터베이스에 포함될 수 없으므로 (FireAMP Connector 사용자) 사용자 프로필을 볼 수 없습니다.
	서드파티 ID 열에 나타나는 취약성 아이콘을 클릭하여 서드파티 취약성에 대한 세부사항을 표시합니다. 자세한 내용은 49-27페이지의 취약성 세부사항 보기을/를 참조하십시오.
확인란	페이지에서 둘 이상 행의 확인란을 선택하여 적용 대상 행을 나타내고 페이지 맨 아래의 버튼 중 하나(예: **View** 버튼)를 클릭합니다. 행 맨 위의 확인란을 선택하여 페이지의 모든 행을 선택할 수도 있습니다.
국기 및 코드	연결 이벤트, 침입 이벤트, 파일 이벤트, 악성코드 이벤트 등 일부 워크플로 페이지에서는 라우팅 가능 IP 주소에 해당 국가에 대한 정보가 포함되어 있습니다. 이러한 *지오로케이션* 정보가 있을 경우 국기 및 ISO 코드가 해당 열(예: Source Country)에 나타납니다. 국기 위에 포인터를 두면 국가 이름이 표시됩니다. (종합이 아닌) 개별 데이터 지점을 볼 때 국기 아이콘을 클릭하여 추가 지오로케이션 정보를 표시할 수 있습니다. 자세한 내용은 58-20페이지의 지오로케이션 사용을/를 참조하십시오. DC500 방어 센터에서는 지오로케이션 데이터를 지원하지 않습니다.
검색 제약 조건	데이터 보기를 제한하는 값이 있으면 나열합니다. 확장 화살표(▶)를 클릭하여 활성 상태의 제약 조건 및 비활성화된 열 목록을 표시하거나 축소 화살표(▼)를 클릭하여 화면에서 목록을 숨깁니다. 기본적으로 이 목록은 축소되어 있습니다. 이는 제약 조건의 목록이 길어 화면의 많은 부분을 차지할 때 유용합니다. 단일 제약 조건을 제거하려면 클릭합니다. 복합 제약 조건을 제거하려면 **Compound Constraints**를 클릭합니다. **Edit Search** 또는 **Save Search**를 클릭하여 현재 단일 제약 조건이 미리 채워진 검색 페이지를 엽니다. 자세한 내용은 58-30페이지의 이벤트 제한을/를 참조하십시오. **참고** 복합 제약 조건은 카운트가 아닌 다중 값을 포함하는 행을 기반으로 생성되는 제약 조건입니다. 복합 제약 조건에 대해서는 검색을 수행하거나 검색을 저장할 수 없습니다.
시간 범위	페이지의 오른쪽 위에 있는 날짜 범위는 워크플로에 포함할 이벤트의 시간 범위를 설정합니다. 자세한 내용은 58-22페이지의 이벤트 시간 제약 조건 설정을/를 참조하십시오. 어플라이언스에 구성된 타임 윈도우(글로벌 또는 이벤트별)을 벗어나 생성되는 이벤트는 시간을 기준으로 이벤트 보기를 제한할 경우 이벤트 보기에 나타날 수 있습니다. 어플라이언스에 대해 슬라이딩 타임 윈도우를 구성한 경우에도 가능합니다.
워크플로 페이지 링크	미리 정의된 워크플로 표 보기 및 드릴다운 페이지의 왼쪽 위에서 이벤트 위, 워크플로 이름 아래에 워크플로 페이지 링크가 나타납니다. 워크플로 페이지 링크를 클릭하여 활성 제약 조건을 사용하여 해당 페이지를 표시합니다.
워크플로 이름	워크플로의 이름이 페이지의 맨 위에 나타납니다. 그 옆에 (해당되는 경우) **(워크플로 전환)** 링크가 있는데, 동일한 유형의 다른 워크플로를 선택할 때 사용할 수 있습니다.

지오로케이션 사용

라이센스: FireSIGHT

지원되는 디바이스: 기능에 따라

지원되는 Defense Center: DC500을 제외하고 모두

네트워크를 모니터링할 때 *지오로케이션* 기능은 라우팅 가능 IP 주소의 지리적 소스에 대한 추가 데이터(국가, 대륙 등)를 제공합니다. 이 데이터를 사용하여 이를테면 연결이 해당 조직과 연결되지 않은 국가에서 시작하거나 종료하는지 여부를 확인할 수 있습니다.

지오로케이션 정보는 침입 이벤트, 연결 이벤트, 파일 이벤트, 악성코드 이벤트, 호스트 프로필, 사용자 프로필에 대해 사용할 수 있습니다. 지오로케이션 정보는 Context Explorer 및 대시보드에서도 사용 가능합니다.

지오로케이션 데이터(소스 및 목적지 국가/대륙)를 액세스 제어 규칙의 조건으로 사용하거나 이 용도로 사용자 지정 지오로케이션 객체를 생성할 수도 있습니다. 소스/목적지 국가 데이터를 상관관계 규칙 및 트래픽 프로필의 조건으로 사용할 수도 있습니다. 자세한 내용은 3-52페이지의 지오로케이션 객체 작업, 15-3페이지의 네트워크 또는 지리적 위치로 트래픽 제어, 51-3페이지의 상관관계 정책에 대한 규칙 생성, 53-3페이지의 트래픽 프로필 조건 지정을/를 참조하십시오.

GeoDB(geolocation database) 업데이트를 설치하여 Geolocation Details 페이지에 IP 주소에 대한 세부 정보를 표시할 수 있습니다. 이를테면 우편 번호, 좌표, 표준 시간대, ASN(Autonomous System Number), ISP(Internet service provider), 사용 유형(가정 또는 비즈니스), 조직, 도메인 이름, 연결 유형, 프록시 정보 등입니다. 4가지 서드파티 지도 툴을 사용하여 탐지된 위치를 정확히 표시할 수도 있습니다. GeoDB 업데이트가 없으면 국기 아이콘과 국가 이름만 나타납니다. Geolocation Details 페이지는 표시할 수 없습니다. GeoDB 설치 및 업데이트에 대한 자세한 내용은 66-27페이지의 지오로케이션 데이터베이스 업데이트을/를 참조하십시오. **Help > About**을 클릭하여 GeoDB 업데이트의 현재 버전을 표시할 수 있습니다.

사용 가능 여부에 따라 다양한 필드가 Geolocation Details 페이지에 나타날 수 있습니다. 정보가 없는 필드는 표시되지 않습니다. 다음 표에서는 이 필드에 대해 설명합니다.

표 58-23 Geolocation Details 필드

필드	내용
Country	호스트의 IP 주소와 관련된 국가이며 국기가 함께 나타납니다. 대륙은 괄호로 표시됩니다. 예: `United States (North America)`, `Equatorial Guinea (Africa)`
Region	국가에서 호스트가 위치한 주, 시/도, 기타 지역입니다. 예: `VA`, `35`
City	호스트가 위치한 도시입니다. 예: `Seattle`, `Fukuoka`
Postal Code	호스트가 위치한 지역의 우편 번호입니다. 예: `361000`, `90210`
Latitude/Longitude	호스트 위치의 정확한 좌표입니다. 예: `40.0375, -76.1053`; `53.4050, -0.5484`
Maps	외부 지도 사이트와의 링크입니다(Google Maps, Yahoo Maps, Bing Maps, OpenStreetMap). 링크를 클릭하면 호스트의 대략적인 위치에 대한 컨텍스트 지도가 표시됩니다.
Timezone	호스트 위치의 시간대로서 일광 절약 시간이 표시되어 있습니다. 예: `GMT+8:00`, `GMT-4:00 (In DST)`
ASN	호스트의 IP 주소와 관련된 ASN 및 해당 ASN에 대한 추가 정보입니다. 예: `14618 (Amazon.com Inc.)`; `4837 (Cncgroup China169 Backbone)`
ISP	호스트의 IP 주소와 관련된 ISP입니다. 예: `Atlantic Broadband`; `China Unicom Ip Network`
Home/Business	호스트의 연결이 `가정` 또는 `비즈니스` 용도인지 나타냅니다.
Organization	호스트의 IP 주소와 관련된 조직입니다. 예: `Amazon.com`, `Bank of America`
Domain Name	호스트의 IP 주소와 관련된 도메인 이름입니다. 예: `amazonaws.com`, `xmcnc.net`

표 58-23 Geolocation Details 필드 (계속)

필드	내용
Connection Type	호스트의 IP 주소와 관련된 연결 유형입니다. 예: `Broadband`, `DSL`
Proxy Type	사용된 프록시의 유형입니다. 예: `Anonymous`, `Corporate`

지오로케이션 세부사항을 보려면

액세스: 모두

1단계 이벤트 보기, 호스트 프로필, 기타 지오로케이션 지원 페이지에서 개별 데이터 지점의 옆에 나타나는 작은 국기 아이콘 또는 ISO 국가 코드를 클릭합니다. Connection Summary 대시보드 등에서 국기 아이콘이 있더라도 종합 지오로케이션 정보의 세부사항을 볼 수 없습니다.

팁 이벤트 보기에서 국기 아이콘 위에 포인터를 두면 국가 이름과 함께 도구 설명이 표시됩니다.

Geolocation Details 페이지가 새 창에 나타납니다.

표 보기 페이지 사용

라이센스: 모두

표 보기에서는 데이터베이스의 각 필드에 대한 열이 (기본적으로 활성화된 경우) 표시됩니다. 표 보기에서 어떤 열을 비활성화할 경우, 그 열을 비활성화함으로써 둘 이상의 동일한 행이 생성된다면 FireSIGHT 시스템에서는 이벤트 보기에 Count 열을 추가합니다. 표 보기 페이지에서 어떤 값을 클릭하면 그 값으로 제한할 수 있습니다. 사용자 지정 워크플로를 생성할 때 **Add Table View**를 클릭하여 여기에 표 보기를 추가합니다.

표 보기 페이지는 드릴다운, 호스트 보기, 패킷 보기 또는 취약성 세부사항 페이지에 없는 추가 기능을 제공합니다. 다음 표에서는 이러한 기능에 대해 자세히 설명합니다.

표 58-24 표 보기 페이지의 추가 기능

기능	설명
✖	숨기려는 열 머리글에서 이 아이콘을 클릭합니다. 팝업 창이 나타나면 **Apply**를 클릭합니다. **팁** 다른 열을 숨기거나 표시하려면 **Apply**를 클릭하기 전에 해당 확인란을 선택하거나 선택 취소합니다.
Disabled Columns 목록	페이지에서 열을 제거하거나 열이 기본적으로 비활성화된 경우 그 열의 이름이 Disabled Columns 목록에 나타납니다. 이 목록은 표 위에 위치하며 기본적으로 숨겨져 있습니다. 비활성화된 열을 다시 이벤트 보기에 추가하려면 Search Constraints 확장 화살표 (▶)를 클릭하여 검색 제약 조건을 확장한 다음 Disabled Columns 아래에서 열 이름을 클릭합니다. 자세한 내용은 58-34페이지의 드릴다운 워크플로 페이지 정렬을/를 참조하십시오.

드릴다운 페이지 사용

라이센스: 모두

드릴다운 페이지는 데이터베이스에서 제공하는 열의 일부를 포함합니다. 사전 정의 워크플로의 드릴다운 페이지에는 항상 Count 열이 있습니다. 드릴다운 페이지에서는 표시하는 이벤트의 범위를 좁히고 워크플로에서 다음으로 진행할 수 있습니다. 이를테면 드릴다운 페이지에서 어떤 값을 클릭할 경우 그 값을 기준으로 제한하고 워크플로의 다음 페이지로 이동함으로써 선택한 값과 매칭하는 이벤트에 더 초점을 맞출 수 있습니다. 드릴다운 페이지에서 어떤 값을 클릭하더라도 그 값이 있는 열이 비활성화되지 않습니다. 진행할 페이지가 표 보기이더라도 상관없습니다. 사용자 지정 워크플로를 생성할 때 **Add Page**를 클릭하여 드릴다운 페이지를 추가합니다.

드릴다운 페이지의 기능을 사용하여 워크플로 진행 중의 이벤트 집합을 제한하는 것에 대한 자세한 내용은 58-18페이지의 공통 표 보기 또는 드릴다운 페이지 기능 사용을/를 참조하십시오.

호스트 보기, 패킷 보기 또는 취약성 세부사항 페이지 사용

라이센스: 모두

검색 이벤트, 호스트, 호스트 특성, IOC, 서버, 클라이언트 애플리케이션 또는 연결 데이터 워크플로의 마지막 페이지는 호스트 보기입니다. 취약성 워크플로의 마지막 페이지는 취약성 세부사항 페이지입니다. 침입 이벤트 워크플로는 항상 패킷 보기로 끝납니다. 워크플로의 마지막 페이지에서 세부사항 섹션을 확장하여 초점 대상인 집합의 각 객체에 대해 워크플로의 진행에 따른 구체적인 정보를 볼 수 있습니다. 웹 인터페이스에서는 워크플로의 최종 페이지에 제약 조건을 나열하지 않지만, 이미 설정된 제약 조건이 유지되어 데이터 집합에 적용됩니다.

이벤트 시간 제약 조건 설정

라이센스: 모두

각 이벤트에는 이벤트가 발생한 시점을 나타내는 타임스탬프가 있습니다. 시간 범위라고도 하는 타임 윈도우를 설정하여 일부 워크플로에 나타나는 정보를 제한할 수 있습니다.

시간에 의한 제한이 가능한 이벤트를 기반으로 하는 워크플로는 페이지 맨 위에 시간 범위 줄이 있습니다(다음 그림 참조).

기본적으로 Cisco 어플라이언스의 워크플로는 지난 시간으로 설정된 확장 타임 윈도우를 사용합니다. 예를 들어 오전 11:30에 로그인할 경우 오전 10:30부터 오전 11:30까지의 이벤트를 볼 수 있습니다. 시간이 경과하면서 타임 윈도우가 확장됩니다. 오후 12:30에는 오전 10:30부터 오후 12:30까지의 이벤트를 볼 수 있습니다.

직접 기본 타임 윈도우를 설정하여 이 동작을 변경할 수 있습니다. 그러면 3가지 속성에 적용됩니다.

- 타임 윈도우 유형(고정, 확장, 슬라이딩)
- 타임 윈도우 길이
- 타임 윈도우 개수(다중 타임 윈도우 또는 단일 글로벌 타임 윈도우)

기본 타임 윈도우에 대한 일반 정보는 71-5페이지의 기본 시간 창을/를 참조하십시오.

기본 타임 윈도우 설정과 무관하게 이벤트 분석 과정에서 페이지 맨 위의 시간 범위를 클릭하면 표시되는 Date/Time 팝업 창에서 수동으로 타임 윈도우를 변경할 수 있습니다. 구성한 타임 윈도우의 개수 및 사용 중인 어플라이언스의 유형에 따라 Date/Time 창을 사용하여 현재 보고 있는 이벤트 유형의 기본 타임 윈도우를 변경할 수도 있습니다.

또한 타임 윈도우를 일시 중지할 수도 있습니다. 그러면 타임 윈도우 없이 중요하지 않은 이벤트를 변경, 제거, 추가하면서 워크플로의 데이터를 점검할 수 있습니다. 페이지 맨 아래의 링크를 클릭하여 다른 이벤트 페이지를 표시할 때, 동일한 이벤트가 서로 다른 워크플로 페이지에 나타나지 않도록 타임 윈도우가 자동으로 일시 중지합니다. 언제라도 타임 윈도우의 일시 중지를 취소할 수 있습니다.

자세한 내용은 다음 절을 참조하십시오.

- 58-23페이지의 타임 윈도우 변경
- 58-27페이지의 이벤트 유형의 기본 타임 윈도우 변경
- 58-29페이지의 타임 윈도우 일시 중지

타임 윈도우 변경

라이센스: 모두

기본 타임 윈도우과 무관하게 이벤트 분석 과정에서 타임 윈도우를 수동으로 변경할 수 있습니다.

참고 수동 타임 윈도우 설정은 현재 세션에만 유효합니다. 로그아웃하고 다시 로그인하면 타임 윈도우는 기본 설정으로 돌아갑니다.

구성된 타임 윈도우의 수에 따라 어떤 워크플로의 타임 윈도우를 변경하면 어플라이언스의 다른 워크플로에 영향을 줄 수 있습니다. 예를 들어 단일 글로벌 타임 윈도우가 있을 경우 한 워크플로의 타임 윈도우를 변경하면 어플라이언스의 다른 워크플로에서도 변경됩니다. 이와 달리 다중 타임 윈도우를 사용하는 경우 감사 로그 또는 상태 이벤트 워크플로의 타임 윈도우를 변경하더라도 다른 타임 윈도우에 영향을 주지 않습니다. 반면에 다른 이벤트 종류의 타임 윈도우를 변경하면 (감사 이벤트 및 상태 이벤트를 제외하고) 시간의 제한을 받을 수 있는 모든 이벤트에 적용됩니다.

일부 워크플로는 시간의 제한을 받지 않을 수 있으므로 타임 윈도우 설정은 호스트, 호스트 특성, 애플리케이션, 애플리케이션 세부사항, 취약성, 사용자 또는 화이트리스트 위반을 기반으로 한 워크플로에는 적용되지 않습니다.

Date/Time 창의 Time Window 탭을 사용하여 수동으로 타임 윈도우를 구성합니다. 기본 타임 윈도우 설정에서 구성한 타임 윈도우의 수에 따라 탭의 제목은 다음 중 하나가 됩니다.

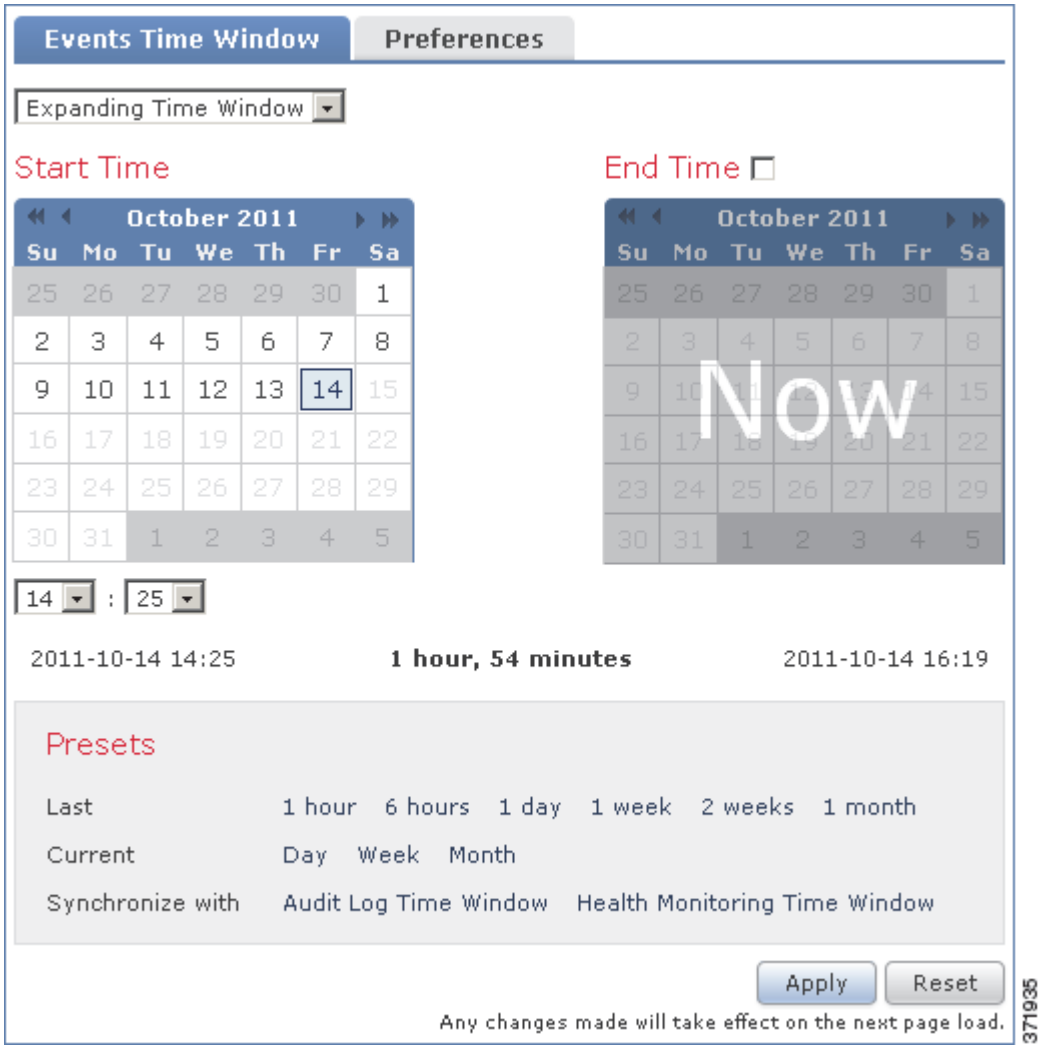
- **Events Time Window** - 다중 타임 윈도우를 구성했고 감사 로그 또는 상태 이벤트 워크플로가 아닌 워크플로의 타임 윈도우를 설정하는 경우
- **Health Monitoring Time Window** - 다중 타임 윈도우를 구성했고 상태 이벤트 워크플로의 타임 윈도우를 설정하는 경우
- **Audit Log Time Window** - 다중 타임 윈도우를 구성했고 감사 로그에 대한 타임 윈도우를 설정하는 경우
- **Global Time Window** - 단일 타임 윈도우를 구성한 경우

타임 윈도우를 구성할 때는 가장 먼저 사용할 타임 윈도우 유형을 결정해야 합니다.

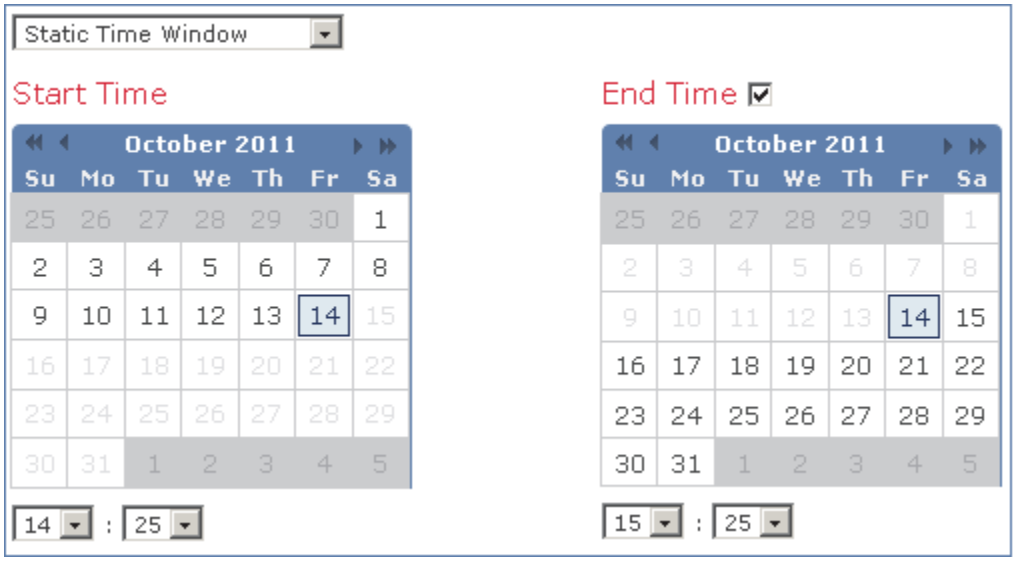
- 고정(*static*) 타임 윈도우는 특정 시작 시간부터 종료 시간까지의 모든 이벤트를 표시합니다.
- 확장(*expanding*) 타임 윈도우는 특정 시작 시간부터 현재까지 생성된 모든 이벤트를 표시합니다. 시간이 흐르면서 타임 윈도우가 확장되고 새 이벤트가 이벤트 보기에 추가됩니다.

- 슬라이딩(*sliding*) 타임 윈도우는 특정 시작 시간(예: 1주일 전)부터 현재까지 생성된 모든 이벤트를 표시합니다. 시간이 흐르면서 타임 윈도우가 "슬라이딩"하므로 구성된 범위(이 예에서는 지난주)의 이벤트만 볼 수 있습니다.

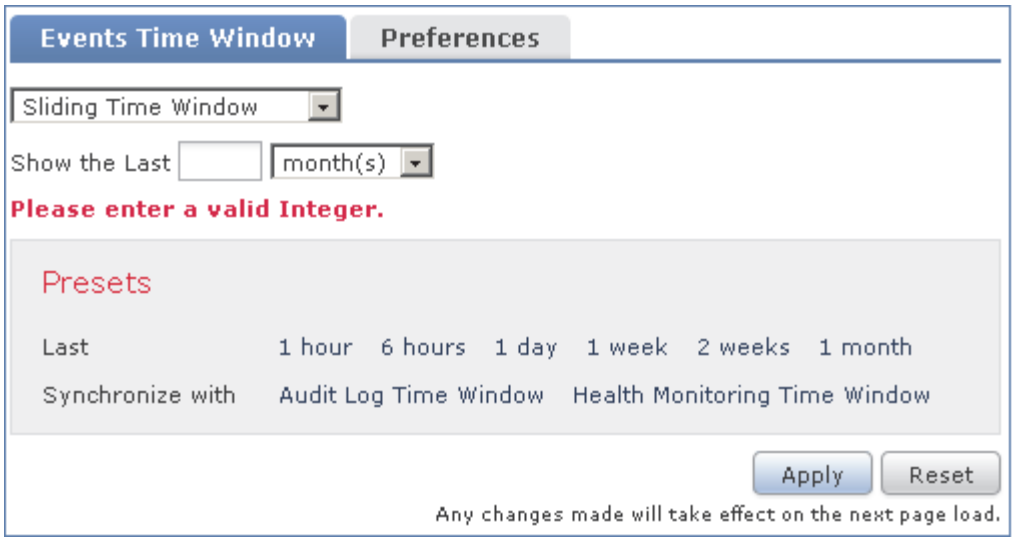
선택하는 유형에 따라 Date/Time 창이 바뀌어 각기 다른 컨피그레이션 옵션을 제공합니다. 다음 그림에서는 확장 타임 윈도우를 사용하도록 지정하는 Date/Time 창을 보여줍니다. 확장 타임 윈도우에서는 End Time 달력이 회색으로 표시되어 종료 시간이 "현재"임을 나타냅니다.



고정 타임 윈도우를 사용할 경우 종료 시간을 설정할 수 있습니다.



슬라이딩 타임 윈도우를 선택할 경우 옵션이 또 바뀝니다.



참고 FireSIGHT 시스템에서는 시간대 환경 설정에서 지정한 시간에 따라 24시간 시계를 사용합니다. 시간대 구성에 대한 자세한 내용은 71-7페이지의 기본 표준 시간대 설정을/를 참조하십시오.

다음 표에서는 Time Window 탭에서 구성할 수 있는 다양한 설정에 대해 설명합니다.

표 58-25 타임 윈도우 설정

설정	타임 윈도우 유형	설명
time window type drop-down list	해당 없음	사용할 타임 윈도우의 유형을 고정, 확장, 슬라이딩 중에서 선택합니다. 어플라이언스에 구성된 타임 윈도우(글로벌 또는 이벤트별)을 벗어나 생성되는 이벤트는 시간을 기준으로 이벤트 보기를 제한할 경우 이벤트 보기에 나타날 수 있습니다. 어플라이언스에 대해 슬라이딩 타임 윈도우를 구성한 경우에도 가능합니다.
Start Time calendar	고정, 확장	타임 윈도우의 시작 날짜와 시간을 지정합니다. 모든 타임 윈도우의 최대 시간 범위는 1970년 1월 1일 자정(UTC)부터 2038년 1월 19일 오전 03:14:07(UTC)까지입니다. **팁** 달력 대신 아래에서 설명하는 Presets 옵션을 사용할 수 있습니다.
End Time calendar	고정	타임 윈도우의 종료 날짜와 시간을 지정합니다. 모든 타임 윈도우의 최대 시간 범위는 1970년 1월 1일 자정(UTC)부터 2038년 1월 19일 오전 03:14:07(UTC)까지입니다. 확장 타임 윈도우를 사용하는 경우 End Time 달력이 회색으로 표시되어 종료 시간이 "현재"임을 나타냅니다. **팁** 달력 대신 아래에서 설명하는 Presets 옵션을 사용할 수 있습니다.
Show the Last field and drop-down list	슬라이딩	슬라이딩 타임 윈도우의 길이를 구성합니다.
Presets: Last	모두	목록에 있는 시간 범위 중 하나를 클릭하여 어플라이언스의 로컬 시간에 따라 타임 윈도우를 변경합니다. 예를 들어 **1 week**를 클릭하면 지난주를 나타내도록 타임 윈도우가 변경됩니다. 미리 설정된 값을 클릭하면 선택한 설정을 반영하여 달력이 변경됩니다.
Presets: Current	고정, 확장	목록에 있는 시간 범위 중 하나를 클릭하여 어플라이언스의 로컬 시간 및 날짜에 따라 타임 윈도우를 변경합니다. 미리 설정된 값을 클릭하면 선택한 설정을 반영하여 달력이 변경됩니다. 다음 사항에 유의하십시오. • 현재 요일은 자정에 시작합니다. • 현재 주는 일요일 자정에 시작합니다. • 현재 월은 월의 첫날 자정에 시작합니다.
Presets: Synchronize with	모두(글로벌 타임 윈도우를 사용하는 경우에는 사용 불가)	다음 중 하나를 클릭합니다. • **Events Time Window** - 현재 타임 윈도우를 이벤트 타임 윈도우dhk 동기화합니다. • **Health Monitoring Time Window** - 현재 타임 윈도우를 상태 모니터링 타임 윈도우와 동기화합니다. • **Audit Log Time Window** - 현재 타임 윈도우를 감사 로그 타임 윈도우와 동기화합니다.

이벤트 분석 과정에서 타임 윈도우를 변경하려면

액세스: Admin/Maint/Any Security Analyst

1단계 시간의 제한을 받는 워크플로에서 시간 범위 아이콘()을 클릭합니다.

Date/Time 창이 나타납니다.

2단계 **Time Window** 탭에서 타임 윈도우 설정 표에 설명된 대로 타임 윈도우를 설정합니다.

팁 **Reset**을 클릭하여 타임 윈도우를 기본 설정으로 변경합니다.

3단계 **Apply**를 클릭합니다.

창이 닫히고 이벤트 보기 페이지에서 새 시간 범위의 이벤트를 표시합니다.

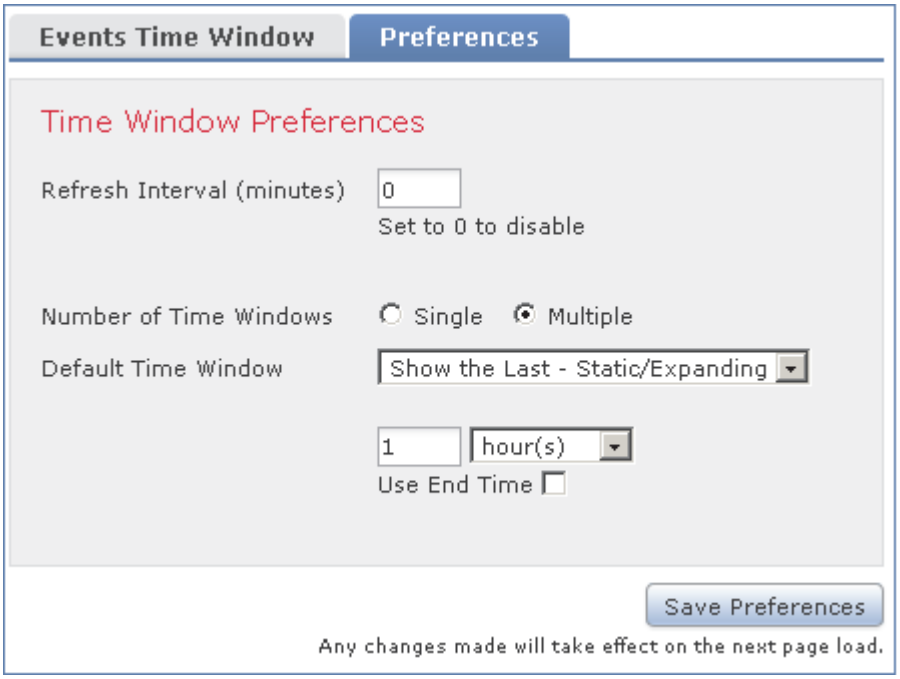
이벤트 유형의 기본 타임 윈도우 변경

라이센스: 모두

이벤트 분석 과정에서 Date/Time 창의 Preferences 탭을 사용하면 이벤트 보기 설정을 사용하지 않고도 현재 표시하는 이벤트 유형의 기본 타임 윈도우를 변경할 수 있습니다(71-5페이지의 기본 시간 창 참조).

이렇게 기본 타임 윈도우를 변경하면 현재 보고 있는 이벤트 유형의 기본 타임 윈도우만 바뀝니다. 예를 들어 다중 타임 윈도우를 구성한 경우 Preferences 탭에서 기본 타임 윈도우를 변경하면 이벤트, 상태 모니터링 또는 감사 로그 창, 즉 첫 번째 탭에 표시된 타임 윈도우의 설정이 바뀝니다. 단일 타임 윈도우를 구성한 경우 Preferences 탭에서 기본 타임 윈도우를 변경하면 모든 이벤트 유형의 기본 타임 윈도우가 바뀝니다.

다음 그림은 다중 타임 윈도우가 구성된 어플라이언스에 있는 방어 센터 버전의 Preferences 탭입니다.



다음 표에서는 Preferences 탭에서 구성할 수 있는 다양한 설정에 대해 설명합니다.

표 58-26 타임 윈도우 환경 설정

환경 설정	설명
Refresh Interval	이벤트 보기의 새로 고침 간격을 분 단위로 설정합니다. 0을 입력하면 새로 고침 옵션이 비활성화됩니다.
Number of Time Windows	사용할 타임 윈도우의 개수를 지정합니다. • 감사 로그, 상태 이벤트, 시간의 제한이 가능한 이벤트 기반 워크플로에 각각 기본 타임 윈도우를 구성하려면 **Multiple**을 선택합니다. • 모든 이벤트에 적용되는 글로벌 타임 윈도우를 사용하려면 **Single**을 선택합니다.
Default Time Window: Show the Last - Sliding	이 설정에서는 지정하는 길이의 슬라이딩 기본 타임 윈도우를 구성할 수 있습니다. 어플라이언스는 특정 시작 시간(예: 1시간 전)부터 현재까지 생성된 모든 이벤트를 표시합니다. 이벤트 보기를 변경하면 타임 윈도우가 "슬라이딩"하므로 항상 지난 1시간의 이벤트가 표시됩니다.
Default Time Window: Show the Last - Static/Expanding	이 설정에서는 지정하는 길이의 고정 또는 확장 기본 타임 윈도우를 구성할 수 있습니다. **고정** 타임 윈도우의 경우(**Use End Time** 확인란 활성화) 어플라이언스는 특정 시작 시간(예: 1시간 전)부터 처음으로 이벤트를 본 시간까지의 모든 이벤트를 표시합니다. 이벤트 보기를 변경할 때 타임 윈도우가 고정되어 있으므로 고정 타임 윈도우에 발생한 이벤트만 표시됩니다. **확장** 타임 윈도우의 경우(**Use End Time** 확인란 비활성화) 어플라이언스는 특정 시작 시간(예: 1시간 전)부터 현재까지의 모든 이벤트를 표시합니다. 이벤트 보기를 변경할 때 타임 윈도우가 현재 시간으로 확장됩니다.

표 58-26 타임 윈도우 환경 설정 (계속)

환경 설정	설명
Default Time Window: Current Day - Static/Expanding	이 설정에서는 현재 일에 대해 고정 또는 확장 기본 타임 윈도우를 구성할 수 있습니다. 현재 일은 현재 세션의 표준 시간대 설정에 따라 자정에 시작합니다. **고정** 타임 윈도우의 경우(**Use End Time** 확인란 활성화) 어플라이언스는 자정부터 처음으로 이벤트를 본 시간까지의 모든 이벤트를 표시합니다. 이벤트 보기를 변경할 때 타임 윈도우가 고정되어 있으므로 고정 타임 윈도우에 발생한 이벤트만 표시됩니다. **확장** 타임 윈도우의 경우(**Use End Time** 확인란 비활성화) 어플라이언스는 자정부터 현재까지의 모든 이벤트를 표시합니다. 이벤트 보기를 변경할 때 타임 윈도우가 현재 시간으로 확장됩니다. 로그아웃하기 전 24시간 이상 분석이 계속될 경우 이 타임 윈도우가 24시간을 초과할 수 있습니다.
Default Time Window: Current Week - Static/Expanding	이 설정에서는 현재 주에 대해 고정 또는 확장 기본 타임 윈도우를 구성할 수 있습니다. 현재 주는 현재 세션의 표준 시간대 설정에 따라 이전 일요일 자정에 시작합니다. **고정** 타임 윈도우의 경우(**Use End Time** 확인란 활성화) 어플라이언스는 자정부터 처음으로 이벤트를 본 시간까지의 모든 이벤트를 표시합니다. 이벤트 보기를 변경할 때 타임 윈도우가 고정되어 있으므로 고정 타임 윈도우에 발생한 이벤트만 표시됩니다. **확장** 타임 윈도우의 경우(**Use End Time** 확인란 비활성화) 어플라이언스는 일요일 자정부터 현재까지의 모든 이벤트를 표시합니다. 이벤트 보기를 변경할 때 타임 윈도우가 현재 시간으로 확장됩니다. 로그아웃하기 전 1주일 이상 분석이 계속될 경우 이 타임 윈도우가 1주를 초과할 수 있습니다.

이벤트 분석 과정에서 타임 윈도우 환경 설정을 변경하려면

액세스: Admin/Maint/Any Security Analyst

1단계 시간의 제한을 받는 워크플로에서 시간 범위 아이콘()을 클릭합니다.

Date/Time 창이 나타납니다.

2단계 **Preferences** 탭을 선택하고 타임 윈도우 환경 설정 표의 설명대로 환경 설정을 변경합니다.

3단계 **Save Preferences**를 클릭합니다.

환경 설정이 저장됩니다.

4단계 다음 2가지 옵션을 사용할 수 있습니다.

- 보고 있는 이벤트 보기에 새 기본 타임 윈도우 설정을 적용하려면 **Apply**를 클릭하여 Date/Time 창을 닫고 이벤트 보기를 새로 고칩니다.
- 기본 타임 윈도우 설정을 적용하지 않고 분석을 계속하려면 **Apply**를 클릭하지 않고 Date/Time 창을 닫습니다.

타임 윈도우 일시 중지

라이센스: 모두

타임 윈도우를 일시 중지할 수 있습니다. 그러면 워크플로에서 제공한 데이터의 스냅샷을 검토할 수 있습니다. 중지하지 않은 워크플로가 업데이트되면 조사할 이벤트가 제거되거나 조사 대상이 아닌 이벤트가 추가될 수 있으므로 이 기능은 유용합니다.

고정 타임 윈도우는 일시 중지할 수 없습니다. 또한 이벤트 타임 윈도우를 일시 중지하더라도 대시보드에 아무런 영향이 없으며, 또한 대시보드를 일시 중지하더라도 이벤트 타임 윈도우 일시 중지에 아무런 영향이 없습니다.

분석을 마치면 타임 윈도우의 일시 중지를 취소할 수 있습니다. 타임 윈도우 일시 중지를 취소하면 환경 설정에 따라 업데이트되며 이벤트 보기도 업데이트되어 일시 중지 취소된 타임 윈도우를 반영합니다.

데이터베이스가 단일 워크플로 페이지에 표시할 수 있는 것보다 많은 이벤트를 포함할 경우 페이지 맨 아래의 링크를 클릭하여 추가 이벤트를 표시할 수 있습니다(58-35페이지의 워크플로의 다른 페이지로 이동 참조). 그러면 동일한 데이터가 두 번 표시되지 않도록 타임 윈도우가 자동으로 일시 중지합니다. 언제라도 타임 윈도우의 일시 중지를 취소할 수 있습니다.

타임 윈도우를 일시 중지하려면

액세스: Admin/Maint/Any Security Analyst

1단계 시간 범위 컨트롤에서 일시 중지 아이콘(❚❚)을 클릭합니다.

(일시 중지를 취소할 때까지) 타임 윈도우가 일시 중지됩니다.

타임 윈도우의 일시 중지를 취소하려면

액세스: Admin/Maint/Any Security Analyst

1단계 시간 범위 컨트롤에서 재생 아이콘(▶)을 클릭합니다.

타임 윈도우의 일시 중지가 취소되고 환경 설정에 따라 타임 윈도우가 업데이트됩니다. 현재 타임 윈도우를 반영하여 이벤트 보기가 업데이트됩니다.

이벤트 제한

라이센스: 모두

워크플로 페이지에 표시되는 정보는 지정된 제약 조건에 따라 결정됩니다. 예를 들어 초기에 이벤트 워크플로를 열 때 그 정보는 이전 시간 동안 생성된 이벤트로 제한됩니다.

워크플로의 다음 페이지로 이동하고 표시되는 데이터를 특정 값으로 제한하려면 페이지에서 해당 값의 행을 선택하고 **View**를 클릭합니다. 워크플로에서 다음 페이지로 이동하되 현재 제약 조건을 유지하고 모든 이벤트를 이월하려면 **View All**을 선택합니다.

참고 카운트가 아닌 다중 값을 포함한 행을 선택하고 **View**를 클릭하면 복합 제약 조건이 생성됩니다. 복합 제약 조건에 대한 자세한 내용은 58-32페이지의 복합 제약 조건 사용을/를 참조하십시오.

워크플로에서 데이터를 제한하는 3번째 방법이 있습니다. 선택한 값의 행으로 페이지를 제한하고 선택한 값을 페이지 맨 위의 제약 조건 목록에 추가하려면 페이지에서 어떤 행의 값을 클릭합니다.

예를 들어 다음 이벤트에서 페이지의 Initiator IP 열에 있는 **10.10.60.119**를 클릭할 경우

	First Packet	Action	Initiator IP	Responder IP	Source Port / ICMP Type
	2013-03-10 23:27:34	Block	10.10.60.119	10.1.1.57	820 / tcp
	2013-03-10 23:27:34	Block	10.10.60.119	10.1.1.57	820 / tcp
	2013-03-10 22:19:28	Block	10.10.60.119	10.1.1.57	753 (rrh) / tcp
	2013-03-10 16:13:39	Block	10.10.32.124	10.10.60.165	856 / tcp

372156

...제한된 페이지는 이 IP 주소의 이벤트만 포함합니다.

▼ Search Constraints (Edit Search Save Search)

Initiator IP 10.10.60.119

Connections | Intrusion | Malware | Files | Hosts | Applications | Application Details | Server

	First Packet	Action	Initiator IP	Responder IP	Source Port / ICMP Ty
	2013-03-10 23:27:34	Block	10.10.60.119	10.1.1.57	820 / tcp
	2013-03-10 23:27:34	Block	10.10.60.119	10.1.1.57	820 / tcp
	2013-03-10 22:19:28	Block	10.10.60.119	10.1.1.57	753 (rrh) / tcp
	2013-03-09 23:21:59	Block	10.10.60.119	10.1.1.57	822 / tcp

팁 모니터 규칙 기준에 따라 연결 이벤트를 제한하는 절차는 약간 다르며 추가 단계가 필요할 수 있습니다. 또한 관련된 파일 또는 침입 정보를 기준으로 연결 이벤트를 제한할 수는 없습니다. 자세한 내용은 39-28페이지의 연결 및 보안 인텔리전스 데이터 테이블 작업을/를 참조하십시오.

검색을 사용하여 워크플로의 정보를 제한할 수도 있습니다. 검색 페이지에 입력하는 검색 기준은 페이지 맨 위에 제약 조건으로 나열되며, 그에 따라 결과 이벤트가 제한됩니다. 방어 센터에서는 현재 제약 조건이 다른 워크플로로 이동할 때에도 적용됩니다. 단, 복합 제약 조건인 경우는 제외합니다(58-35페이지의 워크플로 간 이동 참조).

검색할 때 검색 제약 조건이 검색 중인 테이블에 적용될 것인지에 대해 각별히 주의해야 합니다. 예를 들어 클라이언트 데이터는 연결 요약에서 사용할 수 없습니다. 연결에서 탐지된 클라이언트를 기반으로 연결 이벤트를 검색한 다음 그 결과를 연결 요약 이벤트 보기에 표시할 경우 방어 센터에서는 아무런 제한을 받지 않은 것처럼 연결 데이터를 표시합니다. 잘못된 제약 조건은 N/A(not applicable) 레이블이 지정되고 취소선으로 표시됩니다.

다음 표에서는 제약 조건을 적용할 때 수행 가능한 각 작업에 대해 설명합니다.

표 58-27 검색 제약 조건 기능

목적	클릭
단일 값과 매칭하는 이벤트로 보기 제한	테이블의 값을 클릭합니다. 예를 들어 로깅된 연결의 목록을 보는 중에 액세스 제어를 통해 허용된 연결로 목록을 제한하려면 **Action** 열에서 **Allow**를 클릭합니다. 또 다른 예로 침입 이벤트를 보는 중에 목적지 포트가 80인 이벤트로 제한하려는 목록을 제한하려는 경우 **DST Port/ICMP Code** 열에서 **80 (http)/tcp**를 클릭합니다.
다중 값과 매칭하는 이벤트로 목록 제한	해당 값의 이벤트 확인란을 클릭하고 **View**를 클릭합니다. 행에 카운트가 아닌 다중 값이 있을 경우 복합 제약 조건이 추가됩니다. 복합 제약 조건에 대한 자세한 내용은 58-32페이지의 복합 제약 조건 사용을/를 참조하십시오.
제약 조건 제거	Search Constraints 상자에서 제약 조건의 이름을 클릭합니다.
검색 페이지를 사용하여 제약 조건 수정	Search Constraints 상자에서 **Edit Search**를 클릭합니다. 단일 열에서 다중 값을 대상으로 제한하려면 이 기능을 사용합니다. 예를 들어 두 IP 주소와 관련된 이벤트를 보려는 경우 **Edit Search**를 클릭하고 Search 페이지에서 해당 IP 주소 필드를 수정하여 두 주소를 모두 포함하게 한 다음 **Search**를 클릭합니다.
제약 조건을 저장된 검색으로 저장	Search Constraints 상자의 **Save Search**를 클릭하고 쿼리의 이름을 지정합니다. 복합 제약 조건을 포함한 쿼리는 저장할 수 없습니다. 복합 제약 조건에 대한 자세한 내용은 58-32페이지의 복합 제약 조건 사용을/를 참조하십시오.
다른 이벤트 보기에서 동일한 제약 조건 사용	**Jump to**를 클릭하고 이벤트 보기를 선택합니다. 자세한 내용은 58-35페이지의 워크플로 간 이동을/를 참조하십시오. 다른 워크플로로 전환할 때 복합 제약 조건은 유지되지 않습니다. 복합 제약 조건에 대한 자세한 내용은 58-32페이지의 복합 제약 조건 사용을/를 참조하십시오.
제약 조건 토글 및 표시	확장 화살표(▶)를 클릭합니다. 제약 조건의 목록이 커서 화면의 대부분을 차지할 때 유용한 기능입니다.

복합 제약 조건 사용

라이센스: 모두

복합 제약 조건은 특정 이벤트에 대해 카운트가 아닌 모든 값을 기반으로 합니다. 카운트가 아닌 다중 값이 있는 행을 선택할 때 해당 페이지에서 그 행의 카운트가 아닌 모든 값과 매칭하는 이벤트만 가져오는 복합 제약 조건이 설정됩니다. 예를 들어 소스 IP 주소 `10.10.31.17`, 목적지 IP 주소 `10.10.31.15`를 포함하는 행 및 소스 IP 주소가 `172.10.10.17`, 목적지 IP 주소가 `172.10.10.15`인 행을 선택할 경우 다음 사항이 모두 검색됩니다.

- 소스 IP 주소가 10.10.31.17이고 목적지 IP 주소가 10.10.31.15인 이벤트

  또는

- 소스 IP 주소가 172.10.31.17이고 목적지 IP 주소가 172.10.31.15인 이벤트

복합 제약 조건을 단순 제약 조건과 결합할 경우 단순 제약 조건은 복합 제약 조건의 전 범위에 배포됩니다. 예를 들어 프로토콜 값이 tcp인 단순 제약 조건을 위에 소개된 복합 제약 조건에 추가한 경우 다음 사항이 모두 검색됩니다.

- 소스 IP 주소가 10.10.31.17이고 목적지 IP 주소가 10.10.31.15이며 프로토콜이 tcp인 이벤트

  또는

- 소스 IP 주소가 172.10.31.17이고 목적지 IP 주소가 172.10.31.15이며 프로토콜이 tcp인 이벤트

복합 제약 조건에 대해서는 검색을 수행하거나 검색을 저장할 수 없습니다. 또한 이벤트 보기 링크를 사용하거나 **(워크플로 전환)**을 클릭하여 다른 워크플로로 전환할 때 복합 제약 조건을 유지할 수 없습니다. 복합 제약 조건이 적용된 이벤트 보기에 북마크를 지정할 경우 제약 조건은 북마크와 함께 저장되지 않습니다.

모든 복합 제약 조건을 지우려면 **Compound Constraints**를 클릭합니다.

표 보기 페이지 정렬 및 표 보기 페이지의 레이아웃 변경

라이센스: 모두

워크플로에서 데이터를 볼 때 임의의 사용 가능 열을 기준으로 데이터를 정렬하고 표시할 열을 제거하거나 복원할 수 있습니다. 열에서 오름차순 또는 내림차순으로 데이터를 정렬할 수 있습니다.

팁 사용자 지정 워크플로를 생성할 경우 페이지에서 열의 배치를 완전히 사용자 지정하고 페이지 정렬 순서를 사전 정의할 수 있습니다. 자세한 내용은 58-38페이지의 사용자 지정 워크플로 생성을/를 참조하십시오.

표 58-28 정렬 및 레이아웃 기능

목적	클릭
열 정렬	열 제목을 클릭합니다. 정렬 순서를 반대로 하려면 열 제목을 다시 클릭합니다. **팁** 방향 아이콘(▼)은 데이터가 어떤 열을 기준으로 정렬되었는지, 그 정렬이 오름차순(위로 향하는 아이콘) 또는 내림차순(아래로 향하는 아이콘)인지 나타냅니다.
표 보기에서 열 제거	숨길 열 머리글의 닫기 아이콘(✖)을 클릭합니다. 팝업 창이 나타나면 **Apply**를 클릭합니다. 열을 비활성화할 경우 (나중에 다시 추가하지 않는 한) 세션 기간 동안 비활성화됩니다. 첫 번째 열을 비활성화할 때 Count 열이 추가됩니다. Count 열은 비활성화할 수 없습니다. **팁** 다른 열을 숨기거나 표시하려면 **Apply**를 클릭하기 전에 해당 확인란을 선택하거나 선택 취소합니다. 비활성화된 열을 다시 보기에 추가하려면 확장 화살표(▶)를 클릭하여 검색 제약 조건을 확장한 다음 Disabled Columns 아래에서 열 이름을 클릭합니다.
비활성화된 열을 다시 보기에 추가	Disabled Columns 아래의 열 제목을 클릭합니다. 기본적으로 비활성화된 열을 활성화하면 (나중에 비활성화하지 않는 한) 세션 기간 동안 활성화됩니다. 활성화한 결과 동일한 행이 없으면 Count 열은 제거됩니다.

드릴다운 워크플로 페이지 정렬

라이센스: 모두

워크플로 또는 이벤트 보기에서 데이터를 볼 때 임의의 사용 가능 열을 기준으로 데이터를 정렬하고 표시할 열을 제거하거나 복원할 수 있습니다. 열에서 오름차순 또는 내림차순으로 데이터를 정렬할 수 있습니다. 방향 아이콘(▼)은 데이터가 어떤 열을 기준으로 정렬되었는지, 그 정렬이 오름차순(위로 향하는 아이콘) 또는 내림차순(아래로 향하는 아이콘)인지 나타냅니다.

팁 사용자 지정 워크플로를 생성할 경우 페이지에서 열의 배치를 완전히 사용자 지정하고 페이지 정렬 순서를 사전 정의할 수 있습니다. 자세한 내용은 58-38페이지의 사용자 지정 워크플로 생성을/를 참조하십시오.

열을 정렬하려면

액세스: Admin/Maint/Any Security Analyst

1단계 열 제목을 클릭합니다.

정렬 순서를 반대로 하려면

액세스: Admin/Maint/Any Security Analyst

1단계 열 제목을 다시 클릭합니다.

워크플로 페이지의 행 선택

라이센스: 모두

워크플로 페이지에서 행을 선택하고 작업을 수행하는 데 여러 가지 방법이 있습니다.

- 페이지의 모든 행을 선택하려면 페이지 맨 위의 확인란을 선택합니다.

  그런 다음 페이지 맨 아래의 버튼(**View**, **Delete** 등)을 클릭하여 그 페이지의 모든 이벤트에 대해 작업을 수행할 수 있습니다.
- 개별 행을 선택하려면 해결 행의 옆에 있는 확인란을 선택합니다.

  그런 다음 페이지 맨 아래의 버튼 중 하나를 클릭하여 그 행의 이벤트에 대해서만 작업을 수행할 수 있습니다.
- 개별 행을 선택하고 그 이벤트를 워크플로의 다음 페이지에 표시하려면 화살표 아이콘( )을 클릭합니다.

참고 여러 페이지의 행을 한꺼번에 선택할 수는 없습니다.

워크플로의 다른 페이지로 이동

라이센스: 모두

데이터베이스가 단일 워크플로 페이지에 표시할 수 있는 것보다 많은 이벤트를 포함할 경우 페이지 맨 아래의 링크를 클릭하여 추가 이벤트를 표시할 수 있습니다.

이 링크 중 하나를 클릭할 때 동일한 이벤트가 두 번 표시되지 않도록 시장 창이 자동으로 일시 중지합니다. 언제라도 타임 윈도우의 일시 중지를 취소할 수 있습니다. 자세한 내용은 58-22페이지의 이벤트 시간 제약 조건 설정을/를 참조하십시오.

다음 표에서는 탐색 링크를 사용하는 방법에 대해 설명합니다.

표 58-29 탐색 페이지

목적	클릭
다른 페이지 보기	페이지 번호를 클릭하고 보려는 페이지를 입력한 다음 Enter를 누릅니다.
다음 페이지 보기	>
이전 페이지 보기	<
마지막 페이지로 바로 이동	>|
첫 페이지로 바로 이동	|<

워크플로 간 이동

라이센스: 모두

워크플로 페이지에서 **Jump to...** 드롭다운 목록의 링크를 사용하여 다른 워크플로로 이동할 수 있습니다. 드롭다운 목록을 선택하여 추가 워크플로를 표시하고 선택합니다.

새 워크플로를 선택하면 선택한 행에서 공유하는 속성 및 설정된 제약 조건이 새 워크플로에서 사용됩니다(적용 가능한 경우). 구성된 제약 조건 또는 이벤트 속성이 새 워크플로의 필드에 매핑되지 않을 경우 삭제됩니다. 또한 복합 제약 조건은 다른 워크플로로 전환할 때 유지되지 않습니다. 캡처 파일 워크플로의 제약 조건은 파일 및 악성코드 이벤트 워크플로로만 전송됩니다.

참고 어떤 시간 범위의 이벤트 수를 볼 때 총 이벤트 수가 세부사항 데이터가 있는 이벤트의 수를 반영하지 않을 수 있습니다. 이는 디스크 공간 사용량을 관리하기 위해 때때로 오래된 이벤트의 세부사항을 삭제하기 때문입니다. 이벤트 세부사항이 삭제되는 경우를 최소화하기 위해 이벤트 로깅을 정밀하게 튜닝하여 구축에 가장 중요한 이벤트만 로깅하게 할 수 있습니다. 자세한 내용은 38-1페이지의 네트워크 트래픽의 연결 로깅을/를 참조하십시오.

타임 윈도우를 일시 중지하거나 고정 타임 윈도우를 구성한 경우를 제외하고 타임 윈도우는 워크플로를 변경할 때 바뀝니다. 자세한 내용은 58-22페이지의 이벤트 시간 제약 조건 설정을/를 참조하십시오.

Jump to 드롭다운 목록에서는 다음 테이블의 워크플로에 신속하게 액세스할 수 있습니다.

- connection events
- security intelligence events
- intrusion events

- malware events
- file events
- hosts
- indications of compromise
- applications
- application details
- servers
- host attributes
- discovery events
- users
- vulnerabilities
- third-party vulnerabilities
- correlation events
- white list events

이 기능으로 의심스러운 활동을 더 효과적으로 조사할 수 있습니다. 예를 들어 연결 데이터를 보는 중에 내부 호스트가 비정상적으로 많은 양의 데이터를 외부 사이트에 보내는 것이 확인될 경우 responder IP 주소와 포트를 제약 조건으로 선택한 다음 **Applications** 워크플로로 바로 이동할 수 있습니다. 애플리케이션 워크플로는 responder IP 주소와 포트를 IP Address 및 Port 제약 조건으로 사용하면서 애플리케이션에 대한 추가 정보, 이를테면 어떤 종류의 애플리케이션인가를 표시합니다. 페이지 맨 위의 **Hosts**를 클릭하여 원격 호스트의 호스트 프로필을 볼 수도 있습니다.

애플리케이션에 대한 추가 정보를 얻은 다음 **Correlation Events**를 클릭하여 연결 데이터 워크플로로 돌아가거나 제약 조건에서 Responder IP를 제거하거나 제약 조건에 Initiator IP를 추가하거나 **Application Details**를 선택하여 시작 호스트의 사용자가 원격 호스트에 데이터를 전송할 때 사용한 클라이언트를 확인할 수 있습니다. Port 제약 조건은 Application Details 페이지에 전송되지 않습니다. 로컬 호스트를 제약 조건으로 유지하지만 다른 탐색 버튼을 사용하여 추가 정보를 찾을 수도 있습니다.

- 로컬 호스트가 어떤 정책을 위반했는지 알아보려면 IP 주소를 제약 조건으로 유지하고 **Jump to** 드롭다운 목록에서 **Correlation Events**를 선택합니다.
- 호스트에 대해 침입 규칙이 트리거되었는지(공격 지표) 확인하려면 **Jump to** 드롭다운 목록에서 **Intrusion Events**를 선택합니다.
- 로컬 호스트에 대한 호스트 프로필을 보고 호스트가 만일의 익스플로잇 취약성을 갖고 있는지 확인하려면 **Jump to** 드롭다운 목록에서 **Hosts**를 선택합니다.

북마크 사용

라이센스: 모두

이벤트 분석의 특정 위치 및 시점으로 신속하게 돌아갈 수 있게 하려면 북마크를 생성합니다. 북마크는 다음 사항에 대한 정보를 유지합니다.

- 사용 중인 워크플로
- 워크플로에서 표시하고 있는 부분
- 워크플로 내의 페이지 번호
- 모든 검색 제약 조건

- 모든 비활성 열
- 사용 중인 시간 범위

생성하는 북마크는 북마크 액세스 권한이 있는 모든 사용자 계정에서 사용할 수 있습니다. 즉 심층 분석이 필요한 이벤트 모음을 발견할 경우 편리하게 북마크를 생성한 다음 알맞은 권한을 가진 다른 사용자에게 조사를 맡길 수 있습니다.

참고 북마크에 나타난 이벤트가 삭제될 경우(사용자 직접 삭제 또는 자동 데이터베이스 정리에 의해 삭제) 북마크는 더 이상 원래의 이벤트 집합을 표시하지 않습니다.

북마크 사용에 대한 자세한 내용은 다음 절을 참조하십시오.

- 58-37페이지의 북마크 생성에서는 새 북마크를 생성하는 방법에 대해 설명합니다.
- 58-37페이지의 북마크 보기에서는 기존 북마크를 보고 사용하는 방법에 대해 설명합니다.
- 58-38페이지의 북마크 삭제에서는 북마크를 삭제하는 방법에 대해 설명합니다.

북마크 생성

라이센스: 모두

다음 절차에 따라 새 북마크를 생성합니다.

북마크를 생성하려면

액세스: Admin/Maint/Any Security Analyst

1단계 이벤트를 분석할 때 관심 이벤트가 표시된 상태에서 **Bookmark This Page**를 클릭합니다.

Create a Bookmark 페이지가 나타납니다.

2단계 **Bookmark Name** 필드에 북마크의 이름(영숫자와 공백을 포함하여 최대 80자)을 입력하고 **Save Bookmark**를 클릭합니다.

북마크가 저장되고 북마크가 지정된 이벤트 페이지가 다시 나타납니다.

북마크 보기

라이센스: 모두

다음 절차에 따라 기존 북마크를 보고 사용합니다.

북마크를 보려면

액세스: Admin/Maint/Any Security Analyst

1단계 이벤트 보기에서 **View Bookmarks**를 클릭합니다.

Bookmarks 페이지가 나타납니다.

2단계 사용할 북마크 옆의 **View**를 클릭합니다.

북마크를 지정한 페이지가 나타납니다.

참고 원래 북마크에 나타난 이벤트가 삭제될 경우(사용자 직접 삭제 또는 자동 데이터베이스 정리에 의해 삭제) 북마크는 더 이상 원래의 이벤트 집합을 표시하지 않습니다.

북마크 삭제

라이센스: 모두

다음 절차에 따라 북마크를 삭제합니다. 북마크를 삭제하더라도 그 북마크에 의해 검색되는 이벤트에는 영향을 주지 않습니다.

북마크를 삭제하려면

액세스: Admin/Maint/Any Security Analyst

1단계 이벤트 보기에서 **View Bookmarks**를 클릭합니다.

Bookmarks 페이지가 나타납니다.

2단계 제거할 북마크 옆의 **Delete**를 클릭합니다.

북마크가 삭제되었습니다.

사용자 지정 워크플로 사용

라이센스: 모두

사전 정의된 워크플로와 Cisco에서 제공하는 사용자 지정 워크플로가 필요에 부합하지 않을 경우 사용자 지정 워크플로를 생성할 수 있습니다.

자세한 내용은 다음 링크를 참조하십시오.

- 58-38페이지의 사용자 지정 워크플로 생성 - 사용자 지정 워크플로 생성 절차
- 58-40페이지의 사용자 지정 연결 데이터 워크플로 생성 - 연결 데이터를 기반으로 사용자 지정 워크플로를 생성하는 절차
- 58-42페이지의 사용자 지정 워크플로 보기 - 이벤트 및 사용자 지정 테이블을 기반으로 한 사용자 지정 워크플로를 보는 절차
- 58-43페이지의 사용자 지정 워크플로 수정 - 사용자 지정 워크플로를 수정하는 절차
- 58-44페이지의 사용자 지정 워크플로 삭제 - 사용자 지정 워크플로를 삭제하는 절차

사용자 지정 워크플로 생성

라이센스: 모두

사전 정의된 워크플로와 Cisco에서 제공하는 사용자 지정 워크플로가 필요에 부합하지 않을 경우 사용자 지정 워크플로를 생성할 수 있습니다.

팁 새 사용자 지정 워크플로를 생성하지 않고 다른 어플라이언스에서 사용자 지정 워크플로를 내보낸 다음 현재 어플라이언스로 가져올 수 있습니다. 그런 다음 가져온 워크플로를 필요에 맞게 수정할 수 있습니다. 자세한 내용은 A-1페이지의 컨피그레이션 가져오기 및 내보내기을/를 참조하십시오.

사용자 지정 워크플로를 생성할 때 다음을 수행합니다.

- 워크플로의 소스가 될 테이블 선택
- 워크플로 이름 지정
- 워크플로에 드릴다운 페이지 및 표 보기 페이지 추가

워크플로의 각 드릴다운 페이지에 대해 다음을 수행할 수 있습니다.

- 웹 인터페이스에서 페이지의 맨 위에 나타날 이름 지정
- 페이지당 최대 5개의 열 포함
- 기본 정렬 순서(오름차순 또는 내림차순) 지정

일련의 워크플로 페이지에서 임의의 위치에 표 보기 페이지를 추가할 수 있습니다. 여기에는 페이지 이름, 정렬 순서, 사용자 정의 열 위치와 같은 수정 가능한 속성이 없습니다.

사용자 지정 워크플로의 최종 페이지는 다음 표에서 설명하는 것처럼 워크플로의 기반이 되는 테이블에 따라 달라집니다. 이 최종 페이지는 워크플로 생성 시 기본적으로 추가됩니다.

표 58-30 사용자 지정 워크플로의 최종 페이지

워크플로의 기반	최종 페이지
discovery events	hosts
vulnerabilities	vulnerability detail
third-party vulnerabilities	hosts
users	users
indications of compromise	hosts
intrusion events	packets

어플라이언스에서는 다른 종류의 이벤트(예: 감사 로그, 악성 코드 이벤트)를 기반으로 한 사용자 지정 워크플로에는 최종 페이지를 추가하지 않습니다.

참고 연결 데이터 기반의 사용자 지정 워크플로를 생성하는 절차는 약간 다릅니다. 자세한 내용은 다음 절, 사용자 지정 연결 데이터 워크플로 생성을/를 참조하십시오.

사용자 지정 워크플로를 생성하려면

액세스: Admin/Any Security Analyst

1단계 **Analysis > Custom > Custom Workflows**를 선택합니다.

Custom Workflows 페이지가 나타납니다.

2단계 **Create Custom Workflow**를 클릭합니다.

Edit Custom Workflow 페이지가 나타납니다.

3단계 **Name** 필드에 워크플로의 이름을 입력합니다.

영숫자와 공백을 포함하여 최대 60자로 이름을 지정할 수 있습니다.

4단계 **Description** 필드에 워크플로에 대한 설명을 입력할 수도 있습니다.

영숫자와 공백을 포함하여 최대 80자로 입력할 수 있습니다.

5단계 **Table** 드롭다운 목록에서 추가할 표를 선택합니다.

6단계 **Add Page**를 클릭하여 워크플로에 하나 이상의 드릴다운 페이지를 추가할 수도 있습니다.

드릴다운 페이지 섹션이 나타납니다.

먼저 **Page Name** 필드에 공백 없이 최대 80자의 영숫자로 페이지의 이름을 입력합니다.

Column 1에서 정렬 우선 순위와 표 열을 선택합니다. 이 열은 페이지의 맨 왼쪽 열로 나타납니다. 예를 들어 대상이 된 목적지 포트를 표시하는 페이지를 생성하고 그 페이지를 카운트 순으로 정렬하려면 **Sort Priority** 드롭다운 목록에서 **2**를 선택하고 **Field** 드롭다운 목록에서 **DST Port/ICMP Code**를 선택합니다.

계속해서 페이지에 표시할 모든 필드가 지정될 때까지 필드를 선택하여 정렬 순서를 포함하고 설정합니다. 페이지당 최대 5개의 필드를 지정할 수 있습니다.

참고 5단계의 Table Type에서 **Vulnerabilities**를 선택한 경우 **IP Address**를 표 열로 추가하면 사용자 지정 워크플로에서 취약성을 볼 때 IP Address 열이 나타나지 않습니다. 단, 검색 기능을 사용하여 특정 IP 주소 또는 주소 영역을 표시하도록 워크플로를 제한하는 경우는 제외합니다. 취약성 검색에 대한 자세한 내용은 50-53페이지의 취약성 검색을/를 참조하십시오.

7단계 **Add Table View**를 클릭하여 표 보기 페이지를 워크플로에 추가할 수도 있습니다.

참고 하나 이상의 드릴다운 페이지 또는 이벤트 표 보기를 사용자 지정 워크플로에 추가해야 합니다.

8단계 **Save**를 클릭합니다.

새 워크플로가 저장되어 사용자 지정 워크플로 목록에 추가됩니다.

사용자 지정 연결 데이터 워크플로 생성

라이센스: FireSIGHT

연결 데이터 기반의 사용자 지정 워크플로는 다른 사용자 지정 워크플로와 비슷하지만, 드릴다운 페이지 및 표 보기 페이지뿐 아니라 연결 데이터 그래프 페이지까지 포함할 수 있습니다. 각 페이지 유형을 원하는 개수와 순서로 워크플로에 포함할 수 있습니다. 각 연결 데이터 그래프 페이지는 단일 그래프를 포함하는데, 이는 선형 그래프, 막대 그래프 또는 파이 차트가 될 수 있습니다. 선형 그래프와 막대 그래프에서는 둘 이상의 데이터 집합을 포함할 수 있습니다. 연결 요약, 연결 그래프, 데이터 집합을 포함하여 연결 데이터에 대한 자세한 내용은 39-2페이지의 연결 및 보안 인텔리전스 데이터 이해을/를 참조하십시오.

팁 새 사용자 지정 워크플로를 생성하지 않고 다른 어플라이언스에서 사용자 지정 워크플로를 내보낸 다음 현재 어플라이언스로 가져올 수 있습니다. 그런 다음 가져온 워크플로를 필요에 맞게 수정할 수 있습니다. 자세한 내용은 A-1페이지의 컨피그레이션 가져오기 및 내보내기을/를 참조하십시오.

연결 데이터를 기반으로 사용자 지정 워크플로를 생성하려면

액세스: Admin

1단계 **Analysis > Custom > Custom Workflow**를 선택합니다.

2단계 **Create Custom Workflow**를 클릭합니다.

Edit Custom Workflow 페이지가 나타납니다.

3단계 **Name** 필드에 워크플로의 이름을 입력합니다.

영숫자와 공백을 포함하여 최대 60자까지 입력할 수 있습니다.

4단계 **Description** 필드에 워크플로에 대한 설명을 입력할 수도 있습니다.

영숫자와 공백을 포함하여 최대 80자까지 입력할 수 있습니다.

5단계 **Table** 드롭다운 목록에서 **Connection Events**를 선택합니다.

6단계 하나 이상의 드릴다운 페이지를 워크플로에 추가할 수도 있습니다.

- 개별 연결의 데이터를 포함하는 드릴다운 페이지를 추가하려면 **Add Page**를 클릭합니다.
- 연결 요약 데이터를 포함하는 드릴다운 페이지를 추가하려면 **Add Summary Page**를 클릭합니다.

두 가지 경우 모두 드릴다운 페이지 섹션이 나타납니다.

먼저 **Page Name** 필드에 공백 없이 최대 80자의 영숫자로 페이지의 이름을 입력합니다.

Column 1에서 정렬 우선 순위와 표 열을 선택합니다. 이 열은 페이지의 맨 왼쪽 열로 나타납니다.

계속해서 페이지에 표시할 모든 필드가 지정될 때까지 필드를 선택하여 정렬 순서를 포함하고 설정합니다. 페이지당 최대 5개의 필드를 지정할 수 있습니다.

예를 들어 모니터링되는 네트워크를 통해 전송된 트래픽의 양을 표시하는 페이지를 생성하고 가장 많은 트래픽을 전송한 responder의 순으로 페이지를 정렬하려면 **Sort Priority** 드롭다운 목록에서 **1**을 선택하고 **Field** 드롭다운 목록에서 **Responder Bytes**를 선택합니다.

7단계 **Add Graph**를 클릭하여 워크플로에 하나 이상의 그래프 페이지를 추가할 수도 있습니다.

그래프 섹션이 나타납니다.

먼저 **Graph Name** 필드에 공백 없이 최대 80자의 영숫자로 페이지의 이름을 입력합니다.

그런 다음 페이지에 포함할 그래프의 유형(선형 그래프, 막대 그래프, 파이 차트)을 선택합니다.

그리고 그래프의 X축과 Y축을 선택하여 그래프에 표시할 데이터 종류를 지정합니다. 파이 차트에서 X축은 독립 변수를, Y축은 종속 변수를 나타냅니다.

마지막으로 그래프에 포함할 데이터 집합을 선택합니다. 파이 차트는 하나의 데이터 집합만 포함할 수 있습니다.

8단계 **Add Table View**를 클릭하여 연결 데이터의 표 보기를 추가할 수도 있습니다.

9단계 **Save**를 클릭합니다.

새 워크플로가 저장되어 사용자 지정 워크플로 목록에 추가됩니다.

사용자 지정 워크플로 보기

라이센스: 모두

워크플로를 표시하는 데 사용하는 방법은 워크플로가 사전 정의 이벤트 테이블 중 하나 또는 사용자 지정 테이블을 기반으로 하느냐에 따라 달라집니다.

사용자 지정 워크플로가 사전 정의 이벤트 테이블을 기반으로 할 경우 어플라이언스와 함께 제공되는 워크플로에 액세스하는 것과 동일한 방법으로 액세스합니다. 예를 들어 Hosts 테이블 기반의 사용자 지정 워크플로에 액세스하려면 **Analysis Hosts**를 선택합니다. 이와 달리 사용자 지정 워크플로가 사용자 지정 테이블을 기반으로 할 경우 Custom Tables 페이지에서 액세스해야 합니다.

팁 어떤 이벤트 유형에서도 사용자 지정 워크플로를 기본 워크플로로 설정할 수 없습니다. 71-3페이지의 이벤트 보기 설정 구성을/를 참조하십시오.

자세한 내용은 다음 링크를 참조하십시오.

- 58-42페이지의 사전 정의 테이블의 사용자 지정 워크플로 보기
- 58-43페이지의 사용자 지정 테이블의 사용자 지정 워크플로 보기

사전 정의 테이블의 사용자 지정 워크플로 보기

라이센스: 모두

다음 절차에 따라 사용자 지정 테이블을 기반으로 하지 **않는** 사용자 지정 워크플로를 표시합니다. 워크플로 액세스는 58-16페이지의 워크플로 선택에 설명된 대로 플랫폼 및 사용자 역할에 따라 달라집니다.

사전 정의 테이블 기반의 사용자 지정 워크플로를 표시하려면

액세스: Admin/Any Security Analyst

1단계 워크플로를 사용하는 기능 표에서 설명한 대로 사용자 지정 워크플로의 기반이 되는 테이블에 적합한 메뉴 경로와 옵션을 선택합니다.

해당 테이블의 기본 워크플로 중 첫 페이지가 나타납니다. 사용자 지정 워크플로를 비롯하여 다른 워크플로를 사용하려면 현재 워크플로 제목 옆의 **(워크플로 전환)**을 클릭합니다. 다른 기본 워크플로를 지정하는 것에 대한 자세한 내용은 71-3페이지의 이벤트 보기 설정 구성을/를 참조하십시오. 어떤 이벤트도 발생하지 않을 경우 워크플로가 시간의 제한이 가능하다면 시간 범위 조정이 필요할 수 있습니다. 58-22페이지의 이벤트 시간 제약 조건 설정을/를 참조하십시오.

사용자 지정 테이블의 사용자 지정 워크플로 보기

라이센스: FireSIGHT

다음 절차에 따라 사용자 지정 테이블을 기반으로 하는 사용자 지정 워크플로를 표시합니다.

사용자 지정 테이블 기반의 사용자 지정 워크플로를 표시하려면

액세스: Admin/Any Security Analyst

1단계 **Analysis > Custom > Custom Tables**를 선택합니다.

Custom Tables 페이지가 나타나 사용 가능 사용자 지정 테이블을 나열합니다.

2단계 표시할 사용자 지정 테이블 옆의 보기 아이콘을 클릭하거나 사용자 지정 테이블의 이름을 클릭합니다.

해당 테이블의 기본 워크플로 중 첫 페이지가 나타납니다. 사용자 지정 워크플로를 비롯하여 다른 워크플로를 사용하려면 현재 워크플로 제목 옆의 **(워크플로 전환)**을 클릭합니다. 다른 기본 워크플로를 지정하는 것에 대한 자세한 내용은 71-3페이지의 이벤트 보기 설정 구성을/를 참조하십시오. 어떤 이벤트도 발생하지 않을 경우 워크플로가 시간의 제한이 가능하다면 시간 범위 조정이 필요할 수 있습니다. 58-22페이지의 이벤트 시간 제약 조건 설정을/를 참조하십시오.

사용자 지정 워크플로 수정

라이센스: 모두

이벤트 평가 프로세스가 변경될 경우 새 필요에 맞게 사용자 지정 워크플로를 수정할 수 있습니다. 사전 정의 워크플로는 수정할 수 없습니다.

사용자 지정 워크플로를 수정하려면

액세스: Admin/Any Security Analyst

1단계 **Analysis > Custom > Custom Workflows**를 선택합니다.

Custom Workflows 페이지가 나타나 기존 사용자 지정 워크플로를 나열합니다.

2단계 수정하려는 워크플로 이름 옆의 수정 아이콘()을 클릭합니다.

Edit Workflow 페이지가 나타납니다.

3단계 워크플로를 수정하고 **Save**를 클릭합니다.

워크플로 변경사항이 저장되었습니다.

사용자 지정 워크플로 삭제

라이센스: 모두

다음 절차에서는 더 이상 필요 없는 사용자 지정 워크플로를 삭제하는 방법에 대해 설명합니다.

사용자 지정 워크플로를 삭제하려면

액세스: Admin/Any Security Analyst

1단계 **Analysis > Custom > Custom Workflows**를 선택합니다.

Custom Workflows 페이지가 나타나 사용 가능한 사용자 지정 워크플로를 나열합니다.

2단계 삭제하려는 워크플로 이름 옆의 삭제 아이콘( )을 클릭합니다.

워크플로가 삭제되었습니다.

59장 사용자 지정 테이블 사용

FireSIGHT 시스템이 네트워크에 대한 정보를 수집하면 방어 센터는 일련의 데이터베이스 테이블에 이를 저장합니다. 워크플로를 사용하여 결과 정보를 볼 경우 방어 센터는 이러한 테이블 중 하나에서 데이터를 가져옵니다. 예를 들어 Count 워크플로의 각 Network Applications 페이지에 있는 열은 Applications 테이블의 필드에서 옵니다.

서로 다른 테이블의 필드를 조합하여 네트워크에서의 활동 분석을 개선할 수 있다고 생각되는 경우 사용자 지정 테이블을 생성할 수 있습니다. 사전 정의된 Host Attributes 테이블의 호스트 중요도 정보를 사전 정의된 Connection Data 테이블의 필드와 조합한 다음 새 컨텍스트에서 연결 데이터를 검토할 수 있습니다.

사전 정의 테이블 또는 사용자 지정 테이블에 대한 사용자 지정 워크플로를 생성할 수 있습니다. 사용자 지정 워크플로 생성에 대한 자세한 내용은 58-38페이지의 사용자 지정 워크플로 생성을/를 참조하십시오.

다음 절에서는 고유한 사용자 지정 테이블을 만들고 사용하는 방법에 대해 설명합니다.

사용자 지정 테이블 이해

라이센스: FireSIGHT

사용자 지정 테이블에는 둘 이상의 사전 정의 테이블에서 오는 필드가 포함됩니다. FireSIGHT 시스템에서는 다수의 시스템 정의 사용자 지정 테이블을 제공하지만, 사용자는 특정 요구에 맞는 정보만 포함하는 사용자 지정 테이블을 추가로 생성할 수 있습니다.

예를 들어 FireSIGHT 시스템에서는 침입 이벤트 데이터를 호스트 데이터와 상호 연결하는 시스템 정의 사용자 지정 테이블을 제공하므로, 중요 시스템에 영향을 미치는 이벤트를 검색하고 하나의 워크플로에서 검색 결과를 볼 수 있습니다. 다음 표에서는 시스템에서 제공하는 사용자 지정 테이블에 대해 설명합니다.

표 59-1 시스템 정의 사용자 지정 테이블

표	설명
Hosts with Servers	Hosts 및 Servers 테이블의 필드를 포함하며, 네트워크에서 실행 중인 탐지된 애플리케이션에 대한 정보는 물론 그러한 애플리케이션을 실행하는 호스트에 대한 기본 운영 체제 정보도 제공합니다.
Intrusion Events with Destination Criticality	Intrusion Events 및 Hosts 테이블의 필드를 포함하며, 침입 이벤트에 대한 정보는 물론 각 침입 이벤트와 관련된 대상 호스트의 호스트 중요도도 제공합니다. **팁** 호스트 중요도가 높은 대상 호스트와 관련된 침입 이벤트를 검색하려면 이 테이블을 사용하십시오.
Intrusion Events with Source Criticality	Intrusion Events 및 Hosts 테이블의 필드를 포함하며, 침입 이벤트에 대한 정보 및 각 침입 이벤트와 관련된 소스 호스트의 호스트 중요도를 제공합니다. **팁** 호스트 중요도가 높은 소스 호스트와 관련된 침입 이벤트를 검색하려면 이 테이블을 사용하십시오.

가능한 테이블 조합 이해

라이센스: FireSIGHT + 보호

사용자 지정 테이블을 만들 때에는 관련 데이터가 포함된 사전 정의 테이블의 필드를 조합할 수 있습니다. 다음 표에는 새 사용자 지정 테이블 생성을 위해 조합할 수 있는 사전 정의 테이블이 나열되어 있습니다. 둘 이상의 사전 정의된 사용자 지정 테이블에서 오는 필드를 조합하는 사용자 지정 테이블을 생성할 수 있습니다.

표 59-2 사용자 지정 테이블 조합

필드 조합을 위한 소스 테이블	필드 조합을 위한 대상 테이블
애플리케이션	• Correlation Events • Intrusion Events • Connection Summary Data • Host Attributes • 신청 세부사항 • Discovery Events • Connection Events • 호스트 수 • 서버 • White List Events
Correlation Events	• 애플리케이션 • Host Attributes • 호스트 수

표 59-2 사용자 지정 테이블 조합 (계속)

필드 조합을 위한 소스 테이블	필드 조합을 위한 대상 테이블
Intrusion Events	• 애플리케이션 • Host Attributes • 호스트 수 • 서버
Connection Summary Data	• 애플리케이션 • Host Attributes • 호스트 수 • 서버
Indications of Compromise	• 애플리케이션 • 신청 세부사항 • Captured Files • Connection Events • Connection Summary Data • Correlation Events • Discovery Events • Host Attributes • 호스트 수 • Intrusion Events • Security Intelligence Events • 서버 • White List Events
Host Attributes	• 애플리케이션 • Correlation Events • Intrusion Events • Connection Summary Data • 신청 세부사항 • Discovery Events • Connection Events • 호스트 수 • 서버 • White List Events
신청 세부사항	• 애플리케이션 • Host Attributes • 호스트 수

표 59-2 사용자 지정 테이블 조합 (계속)

필드 조합을 위한 소스 테이블	필드 조합을 위한 대상 테이블
Discovery Events	• 애플리케이션 • Host Attributes • 호스트 수
Connection Events	• 애플리케이션 • Host Attributes • 호스트 수 • 서버
Security Intelligence Events	• 애플리케이션 • Host Attributes • 호스트 수 • 서버
호스트 수	• 애플리케이션 • Correlation Events • Intrusion Events • Connection Summary Data • Host Attributes • 신청 세부사항 • Discovery Events • Connection Events • 서버 • White List Events
서버	• 애플리케이션 • Intrusion Events • Connection Summary Data • Host Attributes • Connection Events • 호스트 수
White List Events	• 애플리케이션 • Host Attributes • 호스트 수

때때로 한 테이블의 한 필드가 또 다른 테이블의 둘 이상의 필드에 매핑됩니다. 예를 들어 사전 정의된 **Intrusion Events with Destination Criticality** 사용자 지정 테이블은 Events 테이블과 Hosts 테이블의 필드를 결합합니다. Intrusion Events 테이블의 각 이벤트에는 두 개의 관련 IP 주소(소스 IP 주소 및 목적지 IP 주소)가 있습니다. 그러나 Hosts 테이블의 "이벤트"는 각각 단일 호스트 IP 주소를 나타냅니다(호스트에 여러 IP 주소가 있을 수 있음). 따라서 Intrusion Events 테이블과 Hosts 테이블을 기반으로 사용자 지정 테이블을 생성할 때에는 Hosts 테이블에서 표시하는 데이터가 Intrusion Events 테이블의 호스트 소스 IP 주소 또는 호스트 목적지 IP 주소에 적용되는지 여부를 선택해야 합니다.

새 사용자 지정 테이블을 생성하면 테이블의 모든 열을 표시하는 기본 워크플로가 자동으로 생성됩니다. 또한 사전 정의 테이블과 마찬가지로, 네트워크 분석에서 사용할 데이터에 대한 사용자 지정 테이블을 검색할 수 있습니다. 사전 정의 테이블과 마찬가지로, 사용자 지정 테이블을 기반으로 보고서를 생성할 수 있습니다.

사용자 지정 테이블 생성에 대한 자세한 내용은 다음을 참조하십시오.

- 59-5페이지의 사용자 지정 테이블 생성
- 59-8페이지의 사용자 지정 테이블 수정
- 59-8페이지의 사용자 지정 테이블 삭제
- 59-9페이지의 사용자 지정 테이블을 기반으로 워크플로 보기
- 59-9페이지의 사용자 지정 테이블 검색

사용자 지정 테이블 생성

라이센스: FireSIGHT

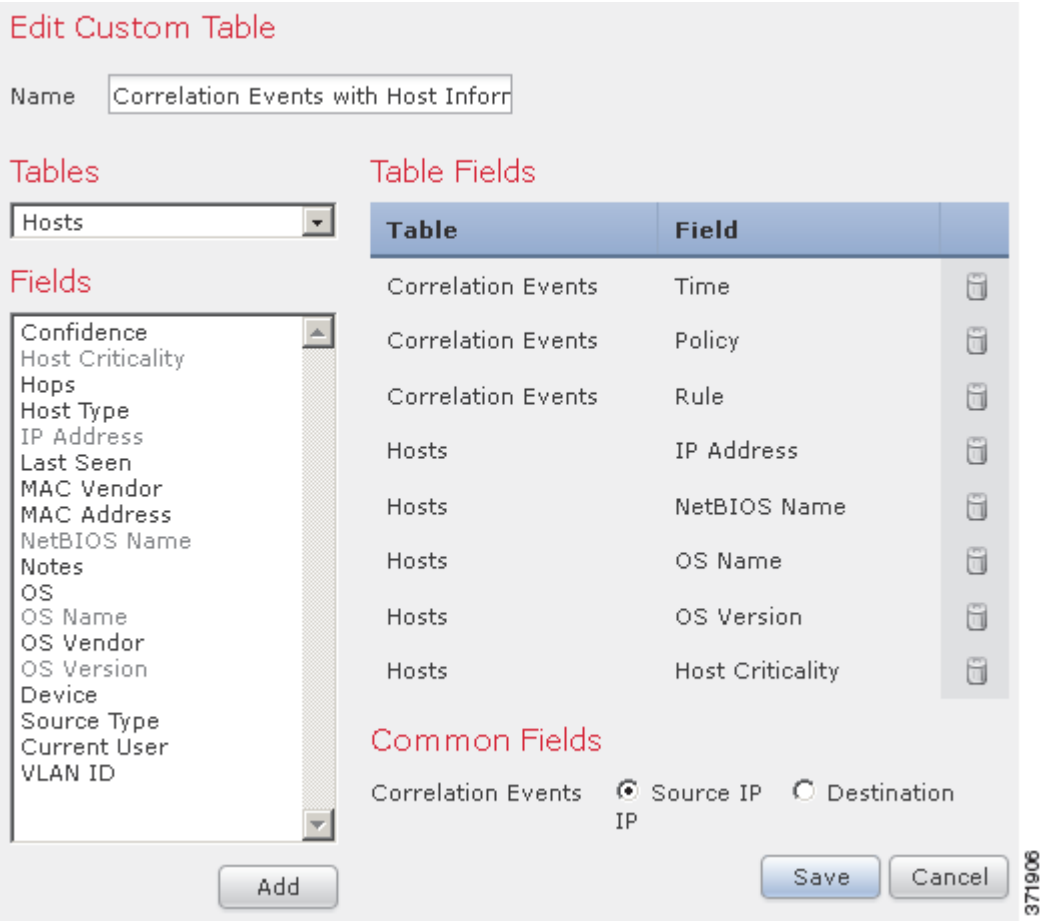
서로 다른 테이블의 필드를 조합하여 네트워크에서의 활동 분석을 개선할 수 있다고 생각되는 경우 사용자 지정 테이블을 생성할 수 있습니다.

팁 새 사용자 지정 테이블을 생성하는 대신, 다른 방어 센터에서 사용자 지정 테이블을 내보낸 다음 현재 방어 센터로 가져올 수 있습니다. 그런 다음 가져온 사용자 지정 테이블을 필요에 맞게 수정할 수 있습니다. 자세한 내용은 A-1페이지의 컨피그레이션 가져오기 및 내보내기을/를 참조하십시오.

사용자 지정 테이블을 생성하려면, FireSIGHT 시스템과 함께 제공된 사전 정의 테이블 중 어떤 것에 사용자 지정 테이블에 포함할 필드가 포함되어 있는지를 확인해야 합니다. 그런 다음, 포함하고자 하는 필드를 선택하고 필요한 경우 공통 필드에 대한 필드 매핑을 구성할 수 있습니다.

팁 Hosts 테이블과 관련된 데이터에서는 하나의 특정 IP 주소보다는 한 호스트의 모든 IP 주소와 연결된 데이터를 볼 수 있습니다.

예를 들어 Correlation Events 테이블과 Hosts 테이블의 필드를 조합하는 사용자 지정 테이블이 있다고 가정해보겠습니다. 이 사용자 지정 테이블을 사용하면 상관관계 정책의 위반과 관련된 호스트에 대한 자세한 정보를 얻을 수 있습니다. Correlation Events 테이블의 소스 IP 주소 또는 목적지 IP 주소와 일치하는 Hosts 테이블의 데이터를 표시할지 여부를 결정해야 합니다.



이 사용자 지정 테이블에 대한 이벤트를 테이블 보기로 보면 한 행에 하나씩 상관관계 이벤트가 표시됩니다. 다음 정보가 포함됩니다.

- 이벤트가 생성된 날짜 및 시간
- 위반된 상관관계 정책의 이름
- 위반을 트리거한 규칙의 이름
- 상관관계 이벤트와 관련된 소스 또는 시작 호스트와 연결된 IP 주소
- 소스 호스트의 NetBIOS 이름
- 소스 호스트가 실행 중인 운영 체제 및 버전
- 소스 호스트 중요도

팁 대상 또는 응답 호스트에 대한 동일한 정보를 표시하는 유사한 사용자 지정 테이블을 생성할 수 있습니다.

이전 예에서 사용자 지정 테이블을 작성하려면

액세스: Admin

1단계 **Analysis > Custom > Custom Tables**를 선택합니다.

Custom Tables 페이지가 나타납니다.

2단계 **Create Custom Table**을 클릭합니다.

Create Custom Table 페이지가 나타납니다.

3단계 **Name** 필드에 `Correlation Events with Host Information (Src IP)` 등 사용자 지정 테이블의 이름을 입력합니다.

4단계 **Tables** 드롭다운 목록에서 **Correlation Events**를 선택합니다.

Correlation Events 테이블의 필드가 **Fields** 목록에 나타납니다.

5단계 **Fields**에서 **Time**을 선택하고 **Add**를 클릭하여 상관관계 이벤트가 생성된 날짜와 시간을 추가합니다.

6단계 5단계를 반복하여 **Policy** 및 **Rule** 필드를 추가합니다.

팁 여러 필드를 선택하려면 Ctrl 또는 Shift 키를 누른 채 클릭할 수 있습니다. 또는 클릭하고 드래그하여 인접한 여러 값을 선택할 수 있습니다. 그러나 테이블과 연결된 이벤트의 테이블 보기에 필드가 나타나는 순서를 지정하려면 필드를 한 번에 하나씩 추가하십시오.

7단계 **Tables** 드롭다운 목록에서 **Hosts**를 선택합니다.

Hosts 테이블의 필드가 **Fields** 목록에 나타납니다. 이러한 필드에 대한 자세한 내용은 50-20페이지의 호스트 테이블 이해을/를 참조하십시오.

8단계 사용자 지정 테이블에 **IP Address**, **NetBIOS Name**, **OS Name**, **OS Version** 및 **Host Criticality** 필드를 추가합니다.

9단계 **Common Fields** 아래의 **Correlation Events** 옆에서 **Source IP**를 선택합니다.

상관관계 이벤트와 관련된 소스 또는 시작 호스트에 대해 8단계에서 선택한 호스트 정보를 표시하도록 사용자 지정 테이블이 구성됩니다.

팁 이 절차를 수행하되 **Source IP** 대신 **Destination IP**를 선택하여, 상관관계 이벤트와 관련된 대상 또는 응답 호스트에 대한 자세한 호스트 정보를 표시하는 사용자 지정 테이블을 생성할 수 있습니다.

10단계 **Save**를 클릭합니다.

사용자 지정 테이블이 저장됩니다.

사용자 지정 테이블 수정

라이센스: FireSIGHT

필요에 따라 사용자 지정 테이블에서 필드를 추가 또는 삭제할 수 있습니다.

사용자 지정 테이블을 수정하려면

액세스: Any/Admin

1단계 **Analysis > Custom > Custom Tables**를 선택합니다.

Custom Tables 페이지가 나타납니다.

2단계 수정할 테이블 옆에 있는 수정 아이콘( )을 클릭합니다.

Edit Custom Table 페이지가 나타납니다. 변경할 수 있는 각종 컨피그레이션에 대한 자세한 내용은 59-5페이지의 사용자 지정 테이블 생성을/를 참조하십시오.

3단계 선택적으로, 제거하려는 필드 옆에 있는 삭제 아이콘( )을 클릭하여 테이블에서 필드를 제거합니다.

참고 보고서에 현재 사용되고 있는 필드를 삭제하는 경우 해당 보고서에서 해당 필드를 사용하는 섹션을 제거할 것인지 묻는 메시지가 표시됩니다.

4단계 필요한 대로 나머지를 변경하고 **Save**를 클릭합니다.

사용자 지정 테이블이 업데이트됩니다.

사용자 지정 테이블 삭제

라이센스: FireSIGHT

더 이상 필요 없는 사용자 지정 테이블을 삭제할 수 있습니다. 사용자 지정 테이블을 삭제하면, 사용자 지정 테이블을 사용하는 저장된 검색도 삭제됩니다.

사용자 지정 테이블을 삭제하려면

액세스: Any/Admin

1단계 **Analysis > Custom > Custom Tables**를 선택합니다.

Custom Tables 페이지가 나타납니다.

2단계 삭제할 사용자 지정 테이블 옆에 있는 삭제 아이콘( )을 클릭합니다.

테이블이 삭제됩니다.

사용자 지정 테이블을 기반으로 워크플로 보기

라이센스: FireSIGHT

사용자 지정 테이블을 생성하면 시스템은 자동으로 이에 대한 기본 워크플로를 생성합니다. 이 워크플로의 첫 번째 페이지에는 이벤트의 테이블 보기가 표시됩니다. 사용자 지정 테이블에 침입 이벤트를 포함하면 워크플로의 두 번째 페이지는 패킷 보기 페이지가 됩니다. 그렇지 않으면 워크플로의 두 번째 페이지는 호스트 페이지가 됩니다. 사용자 지정 테이블을 기반으로 고유한 사용자 지정 워크플로를 생성할 수도 있습니다.

팁 사용자 지정 테이블을 기반으로 사용자 지정 워크플로를 생성하는 경우 이를 해당 테이블의 기본 워크플로로 지정할 수 있습니다. 자세한 내용은 71-3페이지의 이벤트 보기 설정 구성을/를 참조하십시오.

사전 정의 테이블을 기반으로 이벤트 보기에 대해 사용하는 사용자 지정 테이블에서 이벤트를 보려면 이 방법을 사용할 수 있습니다. 자세한 내용은 58-18페이지의 워크플로 페이지 사용을/를 참조하십시오.

사용자 지정 테이블을 기반으로 워크플로를 보려면

액세스: Any/Admin

1단계 **Analysis > Custom > Custom Tables**를 선택합니다.

Custom Tables 페이지가 나타납니다.

2단계 보려는 워크플로의 기반이 되는 사용자 지정 테이블 옆에 있는 보기 아이콘( )을 클릭합니다.

사용자 지정 테이블의 기본 워크플로 중 첫 페이지가 나타납니다. 다른 워크플로를 사용하려면 워크플로 제목 옆의 **(switch workflow)**를 클릭합니다. 다른 기본 워크플로 지정 방법에 대한 자세한 내용은 71-3페이지의 이벤트 보기 설정 구성을/를 참조하십시오. 어떤 이벤트도 발생하지 않을 경우 워크플로가 시간의 제한이 가능하다면 시간 범위 조정이 필요할 수 있습니다. 58-22페이지의 이벤트 시간 제약 조건 설정을/를 참조하십시오.

사용자 지정 테이블 검색

라이센스: FireSIGHT

사용자 지정 테이블에 대한 검색을 생성 및 저장할 수 있습니다. 네트워크 환경에 맞춤화된 검색을 생성한 다음 나중에 다시 사용할 수 있도록 저장할 수 있습니다. 사용자 지정 테이블을 삭제하면, 해당 사용자 지정 테이블에 대해 저장한 모든 검색도 삭제됩니다.

사용 가능한 검색 기준은 사용자 지정 테이블을 작성하기 위해 사용한 사전 정의 테이블에 대한 기준과 동일합니다. 사용 가능한 검색 기준에 대한 자세한 내용은 다음 표에 나열된 절을 참조하십시오.

표 59-3 테이블 검색 기준

검색 기준 대상	참조
Audit Events	69-8페이지의 감사 레코드 검색
Application Details	50-48페이지의 애플리케이션 세부사항 검색
Correlation Events	51-55페이지의 상관관계 이벤트 검색

표 59-3 테이블 검색 기준

검색 기준 대상	참조
Connection Data	39-32페이지의 연결 및 보안 인텔리전스 데이터 검색
Hosts	50-24페이지의 호스트 검색
Host Attributes	50-30페이지의 호스트 특성 검색
Hosts with Applications	50-24페이지의 호스트 검색 및 50-39페이지의 서버 검색
Intrusion Events	41-42페이지의 침입 이벤트 검색
Intrusion Events with Destination Criticality	41-42페이지의 침입 이벤트 검색 및 50-24페이지의 호스트 검색
Intrusion Events with Source Criticality	41-42페이지의 침입 이벤트 검색 및 50-24페이지의 호스트 검색
Status Events	54-21페이지의 교정 상태 이벤트 검색
Discovery Events	50-16페이지의 검색 이벤트 검색
User Events	50-68페이지의 사용자 활동 검색
Rule Update Import Log	66-25페이지의 Rule Update Import Log 검색
Applications	50-43페이지의 애플리케이션 검색
Security Intelligence Events	39-32페이지의 연결 및 보안 인텔리전스 데이터 검색
Users	50-63페이지의 사용자 검색
Vulnerabilities	50-53페이지의 취약성 검색
White List Events	52-33페이지의 규정준수 화이트리스트 이벤트 검색
White List Violations	52-37페이지의 화이트리스트 위반 검색

테이블 검색에서 이러한 기준을 구현하려면 다음 절차를 참조하십시오.

사용자 지정 테이블에 대한 검색을 수행하려면

액세스: Any/Admin

1단계 **Analysis > Custom > Custom Tables**를 선택합니다.

Custom Tables 페이지가 나타납니다.

2단계 검색할 사용자 지정 테이블 옆에 있는 보기 아이콘( )을 클릭합니다.

사용자 지정 테이블의 기본 워크플로 중 첫 페이지가 나타납니다. 사용자 지정 워크플로를 비롯한 다른 워크플로를 사용하려면 워크플로 제목 옆의 **(switch workflow)**를 클릭합니다. 다른 기본 워크플로 지정에 대한 자세한 내용은 71-3페이지의 이벤트 보기 설정 구성을/를 참조하십시오. 어떤 이벤트도 발생하지 않을 경우 워크플로가 시간의 제한이 가능하다면 시간 범위 조정이 필요할 수 있습니다. 58-22페이지의 이벤트 시간 제약 조건 설정을/를 참조하십시오.

3단계 **Search**를 클릭합니다.

사용자 지정 테이블의 검색 페이지가 나타납니다.

팁 데이터베이스에서 서로 다른 종류의 이벤트 또는 데이터를 검색하려면 테이블 드롭다운 목록에서 선택합니다.

4단계 해당 필드에 검색 기준을 입력합니다. 검색 기준 선택에 대한 자세한 내용은 테이블 검색 기준 표를 참조하십시오.

여러 필드에 대한 조건을 입력하는 경우 모든 필드에 대해 지정한 검색 기준과 일치하는 레코드만 반환됩니다.

팁 검색 기준으로 객체를 사용하려면 검색 필드 옆에 있는 객체 아이콘(+)을 클릭합니다. 특수 검색 구문, 검색에서 객체 사용, 검색 저장과 로드 등 검색에 대한 자세한 내용은 60-1페이지의 검색 수행 및 저장을/를 참조하십시오.

5단계 선택적으로, 검색을 저장하려면 **Private** 확인란을 선택하여 자신만 액세스할 수 있는 비공개로 검색을 저장할 수 있습니다. 또는 모든 사용자가 사용할 수 있도록 검색을 저장하려면 확인란을 선택하지 않습니다.

팁 사용자 지정 사용자 역할에 대한 데이터 제한으로서 검색을 사용하려면 **반드시** 비공개 검색으로 저장해야 합니다.

6단계 선택적으로, 나중에 다시 사용할 수 있도록 검색을 저장할 수 있습니다. 다음 옵션을 이용할 수 있습니다.

- 검색 기준을 저장하려면 **Save**를 클릭합니다.

  새 검색인 경우 검색 이름을 입력하도록 대화 상자가 나타납니다. 고유한 검색 이름을 입력하고 **Save**를 클릭합니다. 이미 존재하는 검색에 대한 새 조건을 저장하는 경우 프롬프트가 나타나지 않습니다. 나중에 실행할 수 있도록 검색이 저장됩니다(**Private**을 선택한 경우 자신만 볼 수 있음).

- 새 검색을 저장하거나, 저장된 기존 검색을 변경하여 만든 검색에 새 이름을 할당하려면 **Save As New**를 클릭합니다.

  검색 이름을 입력하도록 대화 상자가 나타납니다. 고유한 검색 이름을 입력하고 **Save**를 클릭합니다. 나중에 실행할 수 있도록 검색이 저장됩니다(**Private**을 선택한 경우 자신만 볼 수 있음).

7단계 검색을 시작하려면 **Search**를 클릭합니다.

검색 결과가 현재 시간과 범위로 제한되어(적용 가능한 경우) 사용자 지정 테이블에 대한 기본 워크플로에 나타납니다. 사용자 지정 워크플로를 비롯한 다른 워크플로를 사용하려면 워크플로 제목 옆의 **(switch workflow)**를 클릭합니다. 다른 기본 워크플로 지정에 대한 자세한 내용은 71-3페이지의 이벤트 보기 설정 구성을/를 참조하십시오.

이벤트 검색

Cisco 어플라이언스는 데이터베이스 테이블에 이벤트로 저장되는 정보를 생성합니다. 이벤트에는 어플라이언스가 이벤트를 생성하도록 만든 활동에 대해 설명하는 여러 필드가 포함되어 있습니다.

FireSIGHT 시스템은 예제 역할을 하며, 이를 통해 네트워크에 대한 중요한 정보에 빠르게 액세스하도록 도와주는 사전 정의된 검색을 제공합니다. 네트워크 환경에 대한 사전 정의된 검색 내에서 필드를 수정한 다음 나중에 다시 사용하기 위해 저장할 수 있습니다. 자신의 고유한 검색 기준을 사용할 수도 있습니다.

사용할 수 있는 검색 기준은 검색 유형에 따라 다를 수 있지만 원리는 동일합니다. 검색을 수행하는 방법 및 검색 필드에서 사용할 올바른 구문에 대한 자세한 내용은 다음 절을 참조하십시오.

검색 수행 및 저장

라이센스: 모두

서로 다른 이벤트 유형에 대한 검색을 생성하고 저장할 수 있습니다. 검색을 만들 때에는 검색의 이름을 지정하고, 검색을 자신만 사용할지 어플라이언스의 모든 사용자가 사용하도록 할지를 지정합니다. 사용자 지정 사용자 역할에 대한 데이터 제한으로서 검색을 사용하려면 **반드시** 비공개 검색으로 저장해야 합니다.

자세한 내용은 다음 절을 참조하십시오.

참고 사용자 지정 테이블을 검색하려면 약간 다른 절차를 따라야 합니다. 59-9페이지의 사용자 지정 테이블 검색을/를 참조하십시오.

검색 수행

라이센스: 모두

일부 이벤트 유형의 경우 FireSIGHT 시스템은 예제 역할을 하며, 이를 통해 네트워크에 대한 중요한 정보에 빠르게 액세스하도록 도와주는 사전 정의된 검색을 제공합니다. 네트워크 환경에 대한 사전 정의된 검색 내에서 필드를 수정한 다음 나중에 다시 사용하기 위해 저장할 수 있습니다. 자신의 고유한 검색 기준을 사용할 수도 있습니다.

검색을 수행하려면

액세스: Admin/Any Security Analyst

1단계 **Analysis > Search**를 선택합니다.

Search 페이지가 나타납니다.

2단계 테이블 드롭다운 목록에서 검색할 이벤트 또는 데이터 유형을 선택합니다.

해당 검색 제약 조건으로 페이지가 업데이트됩니다.

3단계 해당 필드에 검색 기준을 입력합니다.

- 모든 필드에 부정(!)을 사용할 수 있습니다.
- 모든 필드에 쉼표로 구분된 검색 값의 목록을 사용할 수 있습니다. 지정된 필드에 나열된 값 중 하나를 포함하는 레코드는 검색 기준과 일치합니다.
- 모든 필드에 따옴표로 감싸고 쉼표로 구분한 목록을 검색 값으로 사용할 수 있습니다.
  - 단일 값만을 포함할 수 있는 필드의 경우, 따옴표 내에 지정된 정확한 문자열을 포함하는 지정된 필드의 레코드가 검색 기준과 일치합니다. 예를 들어 `A, B, "C, D, E"`에 대한 검색은 지정된 필드에 `"A"` 또는 `"B"` 또는 `"C, D, E"`가 포함된 레코드와 일치합니다. 따라서 가능한 값으로 쉼표를 포함하는 필드에서 일치를 확인할 수 있습니다.
  - 여러 값을 동시에 포함할 수 있는 필드의 경우, 따옴표로 감싸고 쉼표로 구분한 모든 값을 포함하는 지정된 필드의 레코드가 해당 검색 기준과 일치합니다.
  - 여러 값을 동시에 포함할 수 있는 필드의 경우, 검색 기준에 단일 값은 물론 따옴표로 감싸고 쉼표로 구분한 목록도 포함할 수 있습니다. 예를 들어 하나 이상의 이러한 문자를 포함할 수 있는 필드에서 `A, B, "C, D, E"`에 대한 검색은 지정된 필드에 `A` 또는 `B`, 또는 `C`, `D`, `E` 모두가 포함된 레코드와 일치합니다.
- 검색 결과에는 모든 필드에 지정된 검색 기준과 매칭되는 레코드만 반환됩니다.
- 많은 필드에서 와일드카드로 하나 이상의 별표(*)를 사용할 수 있습니다.
- 해당 필드에 대해 사용할 수 있는 정보가 없는 이벤트를 식별하려면 필드에 `n/a`를 지정합니다. 해당 필드가 채워지는 이벤트를 식별하려면 `!n/a`를 사용합니다.
- 검색 기준으로 객체를 사용하려면 검색 필드 옆에 나타나는 객체 추가 아이콘(+)을 클릭합니다.

4단계 사용 가능한 검색 기준에 대해 자세히 알아보려면 다음 절을 참조하십시오.

- 69-8페이지의 감사 레코드 검색
- 50-43페이지의 애플리케이션 검색

- 50-48페이지의 애플리케이션 세부사항 검색
- 40-33페이지의 캡처된 파일 검색
- 52-33페이지의 규정준수 화이트리스트 이벤트 검색
- 39-32페이지의 연결 및 보안 인텔리전스 데이터 검색
- 51-55페이지의 상관관계 이벤트 검색
- 50-16페이지의 검색 이벤트 검색
- 40-13페이지의 파일 이벤트 검색
- 68-54페이지의 상태 이벤트 검색
- 50-30페이지의 호스트 특성 검색
- 50-24페이지의 호스트 검색
- 41-42페이지의 침입 이벤트 검색
- 40-26페이지의 악성코드 이벤트 검색
- 66-25페이지의 Rule Update Import Log 검색
- 54-21페이지의 교정 상태 이벤트 검색
- 47-22페이지의 스캔 결과 검색
- 50-39페이지의 서버 검색
- 50-57페이지의 서드파티 취약성 검색
- 50-63페이지의 사용자 검색
- 50-68페이지의 사용자 활동 검색
- 50-53페이지의 취약성 검색
- 52-37페이지의 화이트리스트 위반 검색

5단계 선택적으로, 검색을 저장하려면 **Private** 확인란을 선택하여 자신만 액세스할 수 있는 비공개로 검색을 저장할 수 있습니다. 또는 모든 사용자가 사용할 수 있도록 검색을 저장하려면 확인란을 선택하지 않습니다.

팁 사용자 지정 사용자 역할에 대한 데이터 제한으로서 검색을 사용하려면 **반드시** 비공개 검색으로 저장해야 합니다.

6단계 선택적으로, 나중에 다시 사용할 수 있도록 검색을 저장할 수 있습니다. 다음 옵션을 이용할 수 있습니다.

- 검색 기준을 저장하려면 **Save**를 클릭합니다.

  새 검색인 경우 검색 이름을 입력하도록 대화 상자가 나타납니다. 고유한 검색 이름을 입력하고 **Save**를 클릭합니다. 이미 존재하는 검색에 대한 새 조건을 저장하는 경우 프롬프트가 나타나지 않습니다. 나중에 실행할 수 있도록 검색이 저장됩니다(**Private**을 선택한 경우 자신만 볼 수 있음).

- 새 검색을 저장하거나, 저장된 기존 검색을 변경하여 만든 검색에 새 이름을 할당하려면 **Save As New**를 클릭합니다.

  검색 이름을 입력하도록 대화 상자가 나타납니다. 고유한 검색 이름을 입력하고 **Save**를 클릭합니다. 나중에 실행할 수 있도록 검색이 저장됩니다(**Private**을 선택한 경우 자신만 볼 수 있음).

7단계 검색을 시작하려면 **Search**를 클릭합니다.

검색 결과가 시간으로 제한되어(적용 가능한 경우) 검색 중인 테이블에 대한 기본 워크플로에 나타납니다. 사용자 지정 워크플로를 비롯한 다른 워크플로를 사용하려면 워크플로 제목 옆의 **(switch workflow)**를 클릭합니다. 다른 기본 워크플로 지정에 대한 자세한 내용은 71-3페이지의 이벤트 보기 설정 구성을/를 참조하십시오. 스캔 결과에 대해 다른 워크플로를 사용할 수 **없습니다**.

저장된 검색 로드

라이센스: 모두

전에 검색을 저장한 경우 이를 로드하고 필요한 내용을 수정한 다음 검색을 시작할 수 있습니다.

저장된 검색을 로드하려면

액세스: Admin/Any Security Analyst

1단계 다음 옵션을 이용할 수 있습니다.

- 워크플로의 원하는 페이지에서 **Search**를 클릭합니다.
- **Analysis > Search**를 선택하고, 검색할 이벤트 유형을 선택합니다.

Search 페이지가 나타납니다.

2단계 Custom Searches 목록 또는 Predefined Searches 목록에서 로드하려는 검색을 선택합니다.

저장된 검색의 설정으로 검색 제약 조건이 채워집니다.

3단계 선택적으로 검색 제약 조건을 변경합니다.

4단계 **Search**를 클릭합니다.

검색 제약 조건과 일치하는 이벤트가 나타납니다.

저장된 검색 삭제

라이센스: 모두

검색을 저장한 경우 Search 페이지에서 삭제할 수 있습니다.

저장된 검색을 삭제하려면

액세스: Admin/Any Security Analyst

1단계 다음 옵션을 이용할 수 있습니다.

- 워크플로의 원하는 페이지에서 **Search**를 클릭합니다.
- **Analysis > Search**를 선택한 다음 삭제할 검색에 대한 이벤트 유형을 선택합니다.

Search 페이지가 나타납니다.

2단계 Custom Searches 목록에서, 삭제하려는 검색을 선택하고 검색 이름 옆에 나타나는 삭제 아이콘(✖)을 클릭합니다.

검색이 삭제됩니다.

검색에 와일드카드 및 기호 사용

라이센스: 모두

문자열에서 일치하는 문자를 검색하기 위해 검색 페이지에 있는 많은 텍스트 필드에서 별표(*)를 사용할 수 있습니다. 예를 들어 `net*`는 `network`, `netware`, `netscape` 등과 일치합니다.

영숫자 외의 문자를 검색하려면(별표 문자 포함) 검색 문자열을 따옴표로 감싸십시오. 예를 들어 다음 문자열을 검색하려면

```
Find an asterisk (*)
```

다음을 입력하십시오.

```
"Find an asterisk (*)"
```

와일드카드가 허용되는 텍스트 필드에서 부분 일치 문자열을 검색하려면 **반드시** 와일드카드를 사용해야 합니다. 예를 들어 페이지 보기와 관련된 모든 감사 레코드에 대한 감사 로그를 검색하려는 경우(Page View의 메시지), `Page`를 검색하면 아무 결과도 반환되지 않습니다. 대신 `Page*`를 지정해야 합니다.

검색에서 객체 및 애플리케이션 필터 사용

라이센스: 모두

FireSIGHT 시스템에서는 네트워크 컨피그레이션의 일부로 사용할 수 있는 명명된 객체, 객체 그룹 및 애플리케이션 필터를 생성할 수 있습니다. 검색을 수행하거나 저장할 때 이러한 객체, 그룹 및 필터를 검색 기준으로 사용할 수 있습니다.

검색을 수행하면 객체, 객체 그룹 및 애플리케이션 필터가 `${object_name}`의 형식으로 나타납니다. 예를 들어 객체 이름이 `ten_ten_network`인 네트워크 객체는 검색에 `${ten_ten_network}`로 나타납니다.

검색 기준으로 객체를 사용할 수 있는 검색 필드 옆에 나타나는 객체 추가 아이콘(+)을 클릭할 수 있습니다.

검색에서 시간 제약 조건 지정

라이센스: 모두

시간 검색 제약 조건을 지정하기 위한 여러 형식을 사용할 수 있습니다. 일치를 확인할 시간을 입력할 수 있습니다. 선택적으로, 입력하는 시간 전후와 일치하는 시간을 확인하려면 보다 작음(<) 또는 보다 큼(>) 연산자를 입력할 수 있습니다.

시간 값을 입력하는 검색 기준 필드에서 허용되는 형식은 다음 표에 나와 있습니다.

표 60-1 검색 필드의 시간 사양

시간 형식	예
today [at HH:MMam|pm]	`today` `today at 12:45pm`
YYYY-MM-DD HH:MM:SS	`2006-03-22 14:22:59`

다음 연산자/키워드 중 하나를 시간 값 앞에 사용할 수 있습니다.

표 60-2 시간 사양 연산자

운영자	예	설명
<	`< 2006-03-22 14:22:59`	2006년 3월 22일 오후 2:23 이전 타임스탬프의 이벤트를 반환합니다.
>	`> today at 2:45pm`	오늘 오후 2:45 이후 타임스탬프의 이벤트를 반환합니다.

검색에서 IP 주소 지정

라이센스: 모두

검색에서 IP 주소를 지정할 때에는 개별 IP 주소, 쉼표로 구분된 주소 목록, 주소 블록, 또는 하이픈(-)으로 구분된 IP 주소 범위를 입력할 수 있습니다. 또한 부정을 사용할 수 있습니다.

IPv6을 지원하는 검색(예: 침입 이벤트, 연결 데이터, 상관관계 이벤트 검색)의 경우 IPv4 및 IPv6 주소, CIDR/접두사 길이 주소 블록을 원하는 조합으로 입력할 수 있습니다.

IP 주소 블록을 지정하기 위해 CIDR 또는 접두사 길이 표기를 사용할 경우 FireSIGHT 시스템은 마스크 또는 접두사 길이로 지정된 네트워크 IP 주소 **부분만** 사용합니다. 예를 들어 `10.1.2.3/8`을 지정하면 FireSIGHT 시스템은 `10.0.0.0/8`을 사용합니다.

다음 표에는 IP 주소를 입력하는 유효한 방법의 예가 나와 있습니다. IP 주소는 네트워크 객체로도 표현할 수 있으므로, IP 주소 검색 기준으로 네트워크 객체를 사용하려면 IP 주소 검색 필드 옆에 나타나는 네트워크 객체 추가 아이콘(✚)을 클릭할 수 있습니다. 자세한 내용은 60-5페이지의 검색에서 객체 및 애플리케이션 필터 사용을/를 참조하십시오.

표 60-3 허용되는 IP 주소 구문

지정할 주소	입력할 내용	예
단일 IP 주소	IP 주소	`192.168.1.1` `2001:db8::abcd`
목록을 사용하여 여러 IP 주소	쉼표로 구분된 IP 주소의 목록. 쉼표 전후에 공백을 추가하지 **마십시오**.	`192.168.1.1,192.168.1.2` `2001:db8::b3ff,2001:db8::0202`
CIDR 블록 또는 접두사 길이로 지정할 수 있는 IP 주소의 범위	IPv4 CIDR 또는 IPv6 접두사 길이 표기법으로 IP 주소 블록	`192.168.1.0/24` 192.168.1.0 네트워크에서 255.255.255.0(즉, 192.168.1.0~192.168.1.255)의 IP를 지정합니다. 자세한 내용은 1-19페이지의 IP 주소 표기 규칙을/를 참조하십시오.
CIDR 블록 또는 접두사로 지정할 수 없는 IP 주소의 범위	하이픈을 사용하여 IP 주소 범위. 하이픈 전후에 공백을 추가하지 **마십시오**.	`192.168.1.1-192.168.1.5` `2001:db8::0202-2001:db8::8329`

IP 주소 또는 IP 주소 범위를 지정하기 위한 기타 방법의 표기법	IP 주소, 블록 또는 범위 앞에 느낌표.	`192.168.0.0/32,!192.168.1.10`
		`!2001:db8::/32`
		`!192.168.1.10,!2001:db8::/32`

검색에서 디바이스 지정

라이센스: 모두

관리되는 디바이스를 제약 조건으로 사용하여 검색을 생성할 때 **Device** 검색 기준 필드에 다음 중 하나를 지정할 수 있습니다.

- 관리되는 디바이스 이름, IP 주소 또는 호스트 이름
- 디바이스 그룹 이름
- 디바이스 스택 이름
- 디바이스 클러스터 이름

시스템은 그룹, 클러스터 또는 스택에서 일치 항목을 찾으면 검색을 수행하기 위해 그룹, 클러스터 또는 스택 이름을 적절한 멤버 디바이스 이름과 교체합니다. 디바이스 필드에 디바이스 그룹, 클러스터 또는 스택을 사용하는 검색을 저장하면, 시스템은 디바이스 필드에 지정된 이름을 저장하고 검색이 실행될 때마다 디바이스 이름 교체를 수행합니다.

자세한 내용은 다음 절을 참조하십시오.

- 4-19페이지의 디바이스 작업
- 4-27페이지의 디바이스 그룹 관리
- 4-43페이지의 스태킹된 디바이스 관리
- 4-29페이지의 디바이스 클러스터링

검색에서 포트 지정

라이센스: 모두

FireSIGHT 시스템은 검색에서 포트 번호에 대한 특정 구문을 허용합니다. 다음을 입력할 수 있습니다.

- 단일 포트 번호
- 쉼표로 구분된 포트 번호 목록
- 대시로 구분된 두 개의 포트 번호(포트 번호의 범위를 나타냄)
- 슬래시로 구분된, 포트 번호와 프로토콜 약어(침입 이벤트를 검색하는 경우만)
- 느낌표와 포트 번호 또는 포트 번호의 범위(지정된 포트의 부정을 나타냄)

참고 포트 번호 또는 범위를 지정할 때 공백을 사용하지 **마십시오**.

다음 표에는 검색 제약 조건으로 포트를 입력하는 유효한 방법의 예가 나와 있습니다.

\

표 60-4 포트 구문 예

예	설명
`21`	TCP와 UDP 이벤트를 비롯한 포트 21의 모든 이벤트를 반환합니다.
`!23`	포트 23의 이벤트를 제외한 모든 이벤트를 반환합니다.
`25/tcp`	포트 25의 모든 TCP 관련 침입 이벤트를 반환합니다.

표 60-4 포트 구문 예 (계속)

예	설명
21/tcp,25/tcp	포트 21과 25의 모든 TCP 관련 침입 이벤트를 반환합니다.
21-25	포트 21~25의 모든 이벤트를 반환합니다.

오래 실행되는 쿼리 중지

라이센스: 모두

지원되는 디바이스: 모든 방어 센터

오래 실행되는 쿼리를 찾아서 중지하기 위해 시스템 관리자는 셸 기반 쿼리 관리 툴을 사용할 수 있습니다.

참고 웹 인터페이스에 검색 페이지를 열어 두면 쿼리가 중지되지 않습니다. 반환에 오랜 시간이 걸리는 쿼리는 쿼리 실행 중에 전체 시스템 성능에 영향을 미칩니다.

쿼리 관리 툴을 사용하면 지정된 기간(분)보다 오래 실행되는 쿼리를 찾아 중지할 수 있습니다. 쿼리를 중지하면 이벤트가 감사 로그 및 syslog에 기록됩니다.

방어 센터에 대한 셸 액세스 권한이 있는, 로컬에서 생성한 사용자만이 `admin` 사용자입니다. 셸 액세스를 허용하는 외부 인증 객체를 사용하는 경우, 셸 액세스 필터와 일치하는 사용자는 셸에도 로그인할 수 있습니다.

사용법:

```
query_manager [-v] [-l [minutes]] [-k query_id [...]]
[--kill-all minutes]
```

옵션:

`-h, --help`
간략한 도움말 메시지를 인쇄합니다.

`-l, --list [minutes]`
지정된 기간(분)보다 오래 걸린 모든 쿼리를 나열합니다. 기본적으로 1분 넘게 걸린 모든 쿼리가 표시됩니다.

`-k, --kill query_id [...]`
지정된 ID가 있는 모든 쿼리를 삭제합니다. 이 옵션에는 여러 ID가 사용될 수 있습니다.

`--kill-all minutes`
지정된 기간(분)보다 오래 걸린 모든 쿼리를 삭제합니다.

`-v, --verbose`
전체 SQL 쿼리를 포함하여 출력을 자세히 표시합니다.

주의 셸 액세스는 시스템 관리자로 제한해야 합니다.

방어 센터에서 쿼리를 중지하려면

액세스: admin 또는 셸 액세스가 허용된 기타 사용자

1단계 ssh를 통해 방어 센터에 연결합니다.

2단계 위에 설명한 구문을 사용하여 sudo 아래에서 query_manager를 실행합니다.

61장 사용자 관리

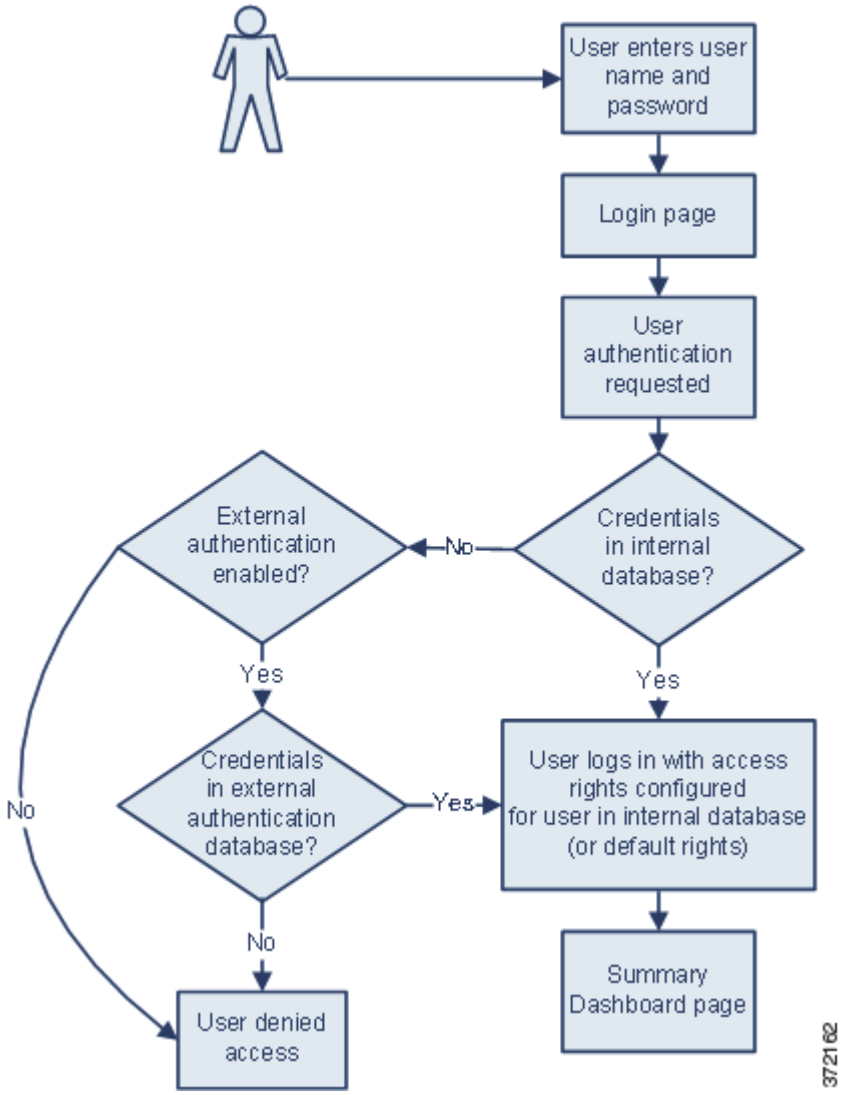
사용자 계정이 관리자 액세스 권한을 갖는 경우 방어 센터 또는 관리되는 디바이스의 웹 인터페이스에 액세스가 가능한 사용자 계정을 관리할 수 있습니다. 방어 센터에서는 내부 데이터베이스가 아닌 외부 인증 서버를 통한 사용자 인증도 설정할 수 있습니다.

자세한 내용은 다음 절을 참조하십시오.

사용자 Cisco인증 이해

라이센스: 모두

사용자가 웹 인터페이스에 로그인할 때 어플라이언스는 로컬 사용자 목록에서 매칭하는 사용자 이름과 비밀번호를 찾습니다. 이러한 프로세스를 *인증*이라고 합니다. 인증에는 내부 인증과 외부 인증의 2가지 종류가 있습니다. 사용자 계정에서 *내부 인증*을 사용할 경우 인증 프로세스는 로컬 데이터베이스에서 이 목록을 확인합니다. 계정에서 *외부 인증*을 사용할 경우 이 프로세스는 로컬 데이터베이스에서 사용자가 있는지 확인하고, 사용자가 로컬에 없으면 LDAP(Lightweight Directory Access Protocol) 디렉토리 서버, RADIUS(Remote Authentication Dial In User Service) 인증 서버와 같은 외부 서버를 쿼리하여 사용자 목록을 찾습니다.



내부 인증 사용자 또는 외부 인증 사용자의 사용자 권한을 제어할 수 있습니다. 외부 인증 사용자는 자신이 속한 그룹 또는 액세스 목록 중 하나에 대한 권한을 갖거나, 사용자 권한을 수동으로 변경하지 않는 한 서버 인증 객체나 방어 센터 관리에 대한 시스템 정책에 설정된 기본 사용자 액세스 역할을 기반으로 한 권한을 갖을 수 있습니다.

자세한 내용은 다음 절을 참조하십시오.

- 61-3페이지의 내부 인증 이해
- 61-3페이지의 외부 인증 이해
- 61-4페이지의 사용자 권한 이해

내부 인증 이해

라이센스: 모두

기본적으로 FireSIGHT 시스템에서는 사용자가 로그인할 때 내부 인증을 사용하여 사용자의 자격 증명을 확인합니다. 내부 인증은 내부 FireSIGHT 시스템 데이터베이스의 레코드와 비교하여 사용자 이름과 비밀번호를 확인하는 것입니다. 사용자 생성 시 외부 인증을 활성화하지 않으면 그 사용자 자격 증명은 내부 데이터베이스에서 관리됩니다.

각 내부 인증 사용자는 수동으로 생성하므로 사용자를 생성할 때 액세스 권한을 설정하며, 기본 설정을 둘 필요가 없습니다.

참고 외부 인증을 활성화할 경우 동일한 사용자 이름이 외부 서버의 사용자 중에 있고 그 사용자가 외부 서버에서 해당 사용자에 대해 저장된 비밀번호로 로그인한다면 내부 인증 사용자는 외부 인증으로 변환됩니다. 내부 인증 사용자가 외부 인증 사용자로 변환되면 그 사용자에 대해서는 내부 인증으로 돌아갈 수 없습니다.

외부 인증 이해

라이센스: 모두

외부 인증에서는 방어 센터 또는 관리되는 디바이스가 LDAP 디렉토리 서버, RADIUS 인증 서버와 같은 외부 저장소에서 사용자 자격 증명을 검색합니다. LDAP 인증과 RADIUS 인증은 외부 인증 유형입니다. 어떤 어플라이언스에 대해 하나의 외부 인증 유형만 사용할 수 있습니다.

외부 인증을 사용하려는 경우 사용자 정보를 요청할 외부 인증 서버 각각에 대해 *인증 객체*를 구성해야 합니다. 인증 객체에는 해당 서버에 연결하고 그로부터 사용자 데이터를 검색하기 위한 설정이 들어 있습니다. 그러면 방어 센터 관리에 대한 시스템 정책에서 그 객체를 활성화하고 어플라이언스에 정책을 적용하여 인증을 활성화할 수 있습니다. 외부 인증 사용자가 로그인할 때 웹 인터페이스는 시스템 정책에 서버가 나열된 순서대로 각 인증 서버를 검사하여 그 사용자가 등록되었는지 확인합니다.

사용자를 생성할 때 그 사용자의 내부 인증 또는 외부 인증 여부를 지정할 수 있습니다.

참고 Series 3가 관리하는 디바이스에서 외부 인증을 활성화하려면 먼저 셸 액세스 필터에 포함된 외부 인증 사용자와 동일한 사용자 이름을 갖는 내부 인증 셸 사용자를 모두 삭제해야 합니다.

관리되는 디바이스에서 외부 인증을 활성화하기 위해 이 디바이스에 시스템 정책을 푸시할 수 있으나, 디바이스의 웹 인터페이스에서 인증 객체를 제어할 수는 없습니다. 디바이스에서 외부 인증의 컨피그레이션은 새 사용자에 대한 인증 유형을 선택할 때만 이루어집니다. 관리되는 디바이스에서 외부 인증을 비활성화하려면 방어 센터 관리에 대한 시스템 정책에서 이를 비활성화하고 디바이스에 정책을 다시 적용하십시오. (관리되는 디바이스에서 생성된) 로컬 시스템 정책을 디바이스 자체에 적용할 경우 외부 인증도 비활성화됩니다.

팁 가져오기/내보내기 기능을 사용하여 시스템 정책을 내보낼 수 있습니다. 외부 인증을 활성화한 상태에서 정책을 내보낼 경우 인증 객체는 정책과 함께 내보내집니다. 그러면 다른 방어 센터에서 정책과 객체를 가져올 수 있습니다. 관리되는 디바이스에 인증 객체와 함께 정책을 가져오지 **마십시오**.

구체적인 외부 인증 유형에 대한 자세한 내용은 다음 절을 참조하십시오.

- 61-5페이지의 LDAP 인증
- 61-31페이지의 RADIUS 인증

사용자 권한 이해

라이센스: 모두

FireSIGHT 시스템에서는 사용자의 역할에 따라 사용자 권한을 할당할 수 있습니다. 예를 들어 분석가는 대개 모니터링되는 네트워크의 보안을 분석하기 위해 이벤트 데이터에 액세스해야 하지만, FireSIGHT 시스템 자체의 관리 기능에 대한 액세스 권한은 필요하지 않을 것입니다. 분석가에게는 보안 분석가, 검색 관리자와 같은 사전 정의된 역할을, FireSIGHT 시스템을 관리하는 네트워크 관리자에게는 관리자 역할을 부여할 수 있습니다. 조직의 요구 사항에 부합하는 액세스 권한을 가진 사용자 지정 사용자 역할을 만들 수도 있습니다.

방어 센터의 시스템 정책에서 모든 외부 인증 사용자에 대한 기본 액세스 역할을 설정합니다. 외부 인증 사용자가 최초로 로그인한 후 User Management 페이지에서 그 사용자에 대한 액세스 권한을 추가하거나 제거할 수 있습니다. 사용자의 권한을 수정하지 않을 경우 그 사용자는 기본적으로 부여된 권한만 갖습니다. 내부 인증 사용자는 수동으로 생성하므로 사용자 생성 시 액세스 권한을 설정합니다.

LDAP 그룹을 통해 액세스 권한 관리를 구성한 경우 사용자의 액세스 권한은 LDAP 그룹 멤버십을 기반으로 합니다. 자신이 속해 있고 액세스 레벨이 가장 높은 그룹에 대해 기본 액세스 권한을 갖습니다. 사용자가 어떤 그룹에도 속하지 않았는데 그룹 액세스가 구성된 경우 LDAP 서버의 인증 객체에 구성된 기본 사용자 액세스 권한을 갖습니다. 그룹 액세스를 구성할 경우 이 설정은 시스템 정책의 기본 액세스 설정을 재정의합니다.

또한 RADIUS 인증 객체에서 특정 사용자 역할 목록에 어떤 사용자를 지정할 경우 그 사용자는 지정된 모든 역할을 갖습니다. 단 그 역할 중 하나 이상이 서로 호환되지 않을 경우는 제외합니다. 서로 호환되지 않는 두 역할의 목록에 있는 사용자는 액세스 레벨이 가장 높은 역할을 갖습니다. 사용자가 어떤 목록에도 속하지 않으며 인증 객체에서 기본 액세스 역할이 구성된 경우 사용자는 그 역할을 갖습니다. 인증 객체에서 기본 액세스를 구성할 경우 이 설정은 시스템 정책의 기본 액세스 설정을 재정의합니다.

FireSIGHT 시스템에서는 라이센스 기능에 따라 사전 정의된 다음 사용자 역할(우선 순위 순)을 지원합니다.

- *액세스 관리자(Access Admins)*는 액세스 제어 및 파일 정책을 보고 수정할 수 있으나 그 정책 변경사항을 적용할 수는 없습니다.
- *관리자(Administrators)*는 어플라이언스의 네트워크 컨피그레이션을 설정하고 사용자 계정 및 종합 보안 인텔리전스 클라우드 연결을 관리하고 시스템 정책 및 시스템 설정을 구성할 수 있습니다. 관리자 역할의 사용자는 다른 모든 역할의 모든 권한을 (해당 권한의 더 낮고 제한된 버전은 제외하고) 갖습니다.
- *검색 관리자(Discovery Admins)*는 네트워크 검색 정책을 검토, 수정, 삭제할 수 있으나 그 정책 변경사항을 적용할 수는 없습니다.
- *외부 데이터베이스(External Database)* 사용자는 JDBC SSL 연결을 지원하는 외부 애플리케이션을 사용하여 FireSIGHT 시스템 데이터베이스를 쿼리할 수 있습니다. 해당 사용자는 웹 인터페이스에서 온라인 도움말 및 사용자 환경 설정에 액세스할 수 있습니다.
- *침입 관리자(Intrusion Admins)*는 모든 침입 정책, 침입 규칙, 네트워크 분석 정책 기능에 액세스할 수 있습니다. 침입 관리자는 **Policies** 메뉴의 침입 관련 옵션에 액세스할 수 있습니다. 침입 관리자는 액세스 제어 정책의 일부인 침입 또는 네트워크 분석 정책을 적용할 수 없습니다.

- *유지 보수 사용자(Maintenance Users)*는 모니터링 기능(예: 상태 모니터링, 호스트 통계, 성능 데이터, 시스템 로그)과 유지 보수 기능(예: 작업 예약, 시스템 백업)에 액세스할 수 있습니다.

  유지 보수 사용자는 **Policies** 메뉴의 기능에 액세스할 수 없으며 **Analysis** 메뉴에서만 대시보드에 액세스할 수 있습니다.
- *네트워크 관리자(Network Admins)*는 디바이스 컨피그레이션을 검토, 수정, 적용하고 액세스 제어 정책을 검토, 수정할 수 있습니다.
- *보안 승인자(Security Approvers)*는 컨피그레이션 및 정책 변경사항을 보고 적용할 수 있으나 생성할 수는 없습니다.
- *보안 분석가(Security Analysts)*는 침입, 검색, 사용자 활동, 연결, 상관관계, 네트워크 변경 이벤트를 검토, 분석, 삭제할 수 있습니다. 호스트, 호스트 특성, 서비스, 취약성, 클라이언트 애플리케이션을 검토, 분석하고 (해당되는 경우) 삭제할 수 있습니다. 또한 보안 분석가는 보고서를 생성할 수 있으며, 상태 이벤트를 볼 수 있지만 삭제하거나 수정할 수는 없습니다.
- *보안 분석가 읽기 전용)*는 보안 분석가와 동일한 권한을 갖지만 이벤트를 삭제할 수는 없습니다.

위와 같은 사전 정의된 역할 외에도 특별한 액세스 권한을 가진 사용자 지정 사용자 역할을 구성할 수도 있습니다. 어떤 역할도 외부 인증 사용자의 기본 액세스 역할이 될 수 있습니다.

외부 인증 사용자 계정에 사용자 역할 에스컬레이션 권한을 부여할 수 있습니다. 외부 인증 사용자의 비밀번호를 에스컬레이션 비밀번호로 사용할 수도 있습니다. 자세한 내용은 61-64페이지의 사용자 역할 에스컬레이션 관리을/를 참조하십시오.

인증 객체 관리

라이센스: 모두

인증 객체는 외부 인증 서버를 위한 서버 프로필로서 해당 서버의 연결 설정 및 인증 필터 설정을 포함합니다. 방어 센터에서 인증 객체를 생성, 구성, 삭제하고 이를 사용하여 LDAP 또는 RADIUS 서버에 대한 외부 인증을 관리할 수 있습니다. 자세한 내용은 다음 절을 참조하십시오.

- 61-5페이지의 LDAP 인증
- 61-31페이지의 RADIUS 인증
- 61-42페이지의 인증 객체 삭제

LDAP 인증

라이센스: 모두

LDAP(Lightweight Directory Access Protocol)은 중앙의 한군데서 사용자 자격 증명과 같은 객체를 체계적으로 관리하는 네트워크 디렉토리를 설정할 수 있게 합니다. 그러면 여러 애플리케이션에서 이 자격 증명 및 자격 증명의 설명에 사용된 정보에 액세스할 수 있습니다. 사용자의 자격 증명을 변경해야 할 경우 각 FireSIGHT 시스템 어플라이언스에서 변경할 필요 없이 한군데서 변경할 수 있습니다.

자세한 내용은 다음 절을 참조하십시오.

- 61-6페이지의 LDAP 인증 이해
- 61-9페이지의 CAC를 사용하는 LDAP 인증 이해
- 61-12페이지의 LDAP 인증 객체를 생성하기 위한 준비
- 61-12페이지의 기본 LDAP 인증 객체 생성
- 61-16페이지의 고급 LDAP 인증 객체 생성

- 61-26페이지의 LDAP 인증 객체의 예
- 61-31페이지의 LDAP 인증 객체 수정

LDAP 인증 이해

라이센스: 모두

LDAP 인증 객체는 방어 센터에서 생성할 수 있지만, 다른 FireSIGHT 시스템 어플라이언스에서는 불가합니다. 그러나 어떤 어플라이언스(가상 디바이스 또는 Cisco NGIPS for Blue Coat X-Series 제외)에서도 외부 인증 객체를 사용할 수 있는데, 이 객체가 해당 어플라이언스에 대해 활성화된 시스템 정책을 적용하면 됩니다. 정책을 적용할 때 그 객체가 어플라이언스에 복사됩니다.

참고 Series 3가 관리하는 디바이스에서 외부 인증을 활성화하려면 먼저 셸 액세스 필터에 포함된 외부 인증 사용자와 동일한 사용자 이름을 갖는 내부 인증 셸 사용자를 모두 삭제해야 합니다.

인증 객체에서 주소 지정과 필터 및 특성 구문에 LDAP 명명 표준을 사용할 수 있습니다. 자세한 내용은 LDAP(v3): Technical Specification, RFC 3377에 나열된 RFC를 참조하십시오. 본 절차의 전 범위에서 구문의 예가 제시됩니다. Microsoft Active Directory Server에 연결하기 위해 인증 객체를 설정할 경우, 도메인을 포함하는 사용자 이름을 참조할 때 Internet RFC 822(Standard for the Format of ARPA Internet Text Messages) 사양에 기술된 주소 지정 구문을 사용할 수 있습니다. 예를 들어 Microsoft Active Directory Server 사용 시 사용자 객체를 참조할 때 `cn=JoeSmith,ou=security,dc=example,dc=com`이라는 사용자 DN(distinguished name) 대신 `JoeSmith@security.example.com`이라고 입력하면 됩니다.

참고 현재 FireSIGHT 시스템에서는 Windows Server 2003 및 Windows Server 2008에서 Microsoft Active Directory를, Windows Server 2003 및 Windows Server 2008에서 Oracle Directory Server Enterprise Edition 7.0을 또는 Linux에서 OpenLDAP on Linux를 실행하는 LDAP 서버에 대해 LDAP 외부 인증을 지원합니다. 그러나 FireSIGHT 시스템에서는 가상 디바이스나 Cisco NGIPS for Blue Coat X-Series에 대해서는 외부 인증을 지원하지 않습니다.

자세한 내용은 다음 절을 참조하십시오.

- 61-7페이지의 기본값 이해
- 61-7페이지의 기본 DN 이해
- 61-7페이지의 기본 필터 이해
- 61-7페이지의 가장 계정 이해
- 61-7페이지의 LDAP 연결 이해
- 61-8페이지의 사용자 이름 템플릿 이해
- 61-8페이지의 연결 시간 초과 이해
- 61-8페이지의 액세스 관리를 위한 특성 이해
- 61-9페이지의 액세스 관리를 위한 그룹 멤버십 이해
- 61-9페이지의 셸 액세스 이해

기본값 이해

라이센스: 모두

연결하려는 서버 유형에 따른 기본값을 사용하여 여러 필드를 채울 수 있습니다. 서버 유형을 선택하고 기본값을 설정하면 User Name Template, UI Access Attribute, Shell Access Attribute, Group Member Attribute, Group Member URL Attribute 필드에 기본값이 전달됩니다.

기본 DN 이해

라이센스: 모두

로컬 어플라이언스에서 인증 서버의 사용자 이름을 찾기 위해 LDAP 서버를 검색할 때 그 검색의 시작점이 필요합니다. 기본 고유 이름, 즉 *기본 DN*을 제공하여 로컬 어플라이언스에서 검색할 트리를 지정할 수 있습니다.

일반적으로 기본 DN은 회사 도메인과 운영 단위를 나타내는 기본 구조를 갖습니다. 예를 들어 Example 회사의 Security 조직은 `ou=security,dc=example,dc=com`이라는 기본 DN을 가질 수 있습니다.

기본 서버를 식별한 다음 그로부터 사용 가능 기본 DN의 목록을 자동으로 가져오고 알맞은 기본 DN을 선택할 수 있습니다.

기본 필터 이해

라이센스: 모두

어떤 특성에 대해 특정 값을 설정하는 *기본 필터*(여닫는 괄호를 포함하여 최대 450자)를 추가할 수 있습니다. 기본 필터는 기본 DN에서 필터에 설정된 특성 값을 갖는 객체만 검색하는 방법으로 검색을 집중시킵니다. 기본 필터는 괄호로 묶습니다. 예를 들어 CN(common name)이 F로 시작하는 사용자만 필터링하려면 `(cn=F*)`라는 필터를 사용합니다.

테스트 사용자 이름과 비밀번호를 입력하여 더 구체적으로 기본 필터를 테스트하려면 61-37페이지의 사용자 인증 테스트을/를 참조하십시오.

가장 계정 이해

라이센스: 모두

로컬 어플라이언스에서 사용자 객체에 액세스하는 것을 허용하려면 가장 계정에 대한 사용자 자격 증명을 제공해야 합니다. *가장 계정(impersonation account)*이란 기본 DN으로 명명된 디렉토리를 탐색하고 찾고 싶은 사용자 객체를 검색하는 데 적합한 권한을 가진 사용자 계정입니다. 지정하는 사용자 DN이 서버의 트리에서 고유해야 합니다.

LDAP 연결 이해

라이센스: 모두

LDAP 연결에 대한 암호화 방식을 관리할 수 있습니다. 암호화 없음, TLS(Transport Layer Security) 또는 SSL(Secure Sockets Layer) 암호화를 선택할 수 있습니다.

TLS 또는 SSL을 통한 연결에서 인증 시 인증서를 사용하는 경우 인증서의 LDAP 서버 이름이 Host Name/IP Address 필드에 사용하는 이름과 **반드시** 매칭해야 합니다. 예를 들어 외부 인증 설정에 `10.10.10.250`을, 인증서에는 `computer1.example.com`을 입력할 경우 연결은 실패합니다. 외부 인증 설정에서 서버 이름을 `computer1.example.com`으로 변경하면 성공적으로 연결됩니다.

사용자 이름 템플릿 이해

라이센스: 모두

사용자 이름 템플릿을 선택하면 문자열 변환 문자(`%s`)를 사용자의 UI 액세스 특성 또는 셸 액세스 특성의 값에 매핑하는 방법으로 로그인 시 입력하는 사용자 이름의 형식을 지정할 수 있습니다. 사용자 이름 템플릿은 인증에 쓰이는 DN의 형식입니다. 사용자가 로그인 페이지에서 사용자 이름을 입력할 때 그 이름이 문자열 변환 문자를 대체하고 그 결과 DN이 사용자 자격 증명 검색에 사용됩니다.

예를 들어 Example 회사의 Security 조직을 위한 사용자 이름 템플릿을 설정하기 위해 `%s@security.example.com`이라고 입력할 수 있습니다. CAC 인증 및 권한 부여에 객체를 사용하려는 경우 UI 액세스 특성 값에 해당하는 사용자 이름 템플릿의 값을 **반드시** 입력해야 합니다. 자세한 내용은 61-9페이지의 CAC를 사용하는 LDAP 인증 이해을/를 참조하십시오.

연결 시간 초과 이해

라이센스: 모두

백업 인증 서버를 지정할 경우 기본 서버에 대한 연결 시도의 시간 초과를 설정할 수 있습니다. 기본 인증 서버의 응답 없이 시간 초과의 기간이 경과하면 어플라이언스는 백업 서버를 쿼리합니다. 예를 들어 기본 서버에서 LDAP이 비활성화된 경우 어플라이언스는 백업 서버를 쿼리합니다.

그러나 LDAP이 기본 LDAP 서버의 포트에서 실행 중인데 어떤 이유(잘못된 컨피그레이션 또는 기타 문제)로 요청에 대한 서비스를 거부할 경우에는 백업 서버에 대한 장애 조치가 이루어지지 않습니다.

액세스 관리를 위한 특성 이해

라이센스: 모두

각기 다른 LDAP 서버 유형은 사용자 데이터 저장에 쓰이는 특성도 저마다 다릅니다. UI 및 셸 액세스 특성에 대한 설명은 다음 절을 참조하십시오.

UI 액세스 특성

LDAP 서버에서 UI 액세스 특성 `uid`를 사용할 경우 로컬 어플라이언스는 설정된 기본 DN이 나타내는 트리에서 각 객체의 `uid` 특성 값을 확인합니다. 특정 UI 액세스 특성을 설정하지 않을 경우 로컬 어플라이언스는 LDAP 서버의 사용자 레코드별 DN이 사용자 이름과 매칭하는지 확인합니다. 객체 중 하나에 매칭하는 사용자 이름과 비밀번호가 있을 경우 사용자 로그인 요청이 인증됩니다.

다른 LDAP 특성으로 대체하여 로컬 어플라이언스에서 DN의 값 대신 그 특성과 사용자 이름을 매칭하게 할 수 있습니다. 서버 유형을 선택하고 기본값을 설정하면 해당 서버 유형에 적합한 UI 액세스 특성이 채워집니다. 객체 중 하나에 매칭하는 사용자 이름이 그리고 비 CAC 객체라면 비밀번호가 지정된 특성의 값으로 존재할 경우 사용자 로그인 요청이 인증됩니다. 그 값이 FireSIGHT 시스템 웹 인터페이스의 유효한 사용자 이름이라면 어떤 특성도 사용할 수 있습니다. 사용자 이름은 고유해야 하며 밑줄(_), 마침표(.), 하이픈(-), 영숫자를 포함할 수 있습니다. CAC 인증 및 권한 부여에 객체를 사용하려는 경우 그 사용자 이름 템플릿 값에 **해당하는** 값을 UI 액세스 특성에 입력해야 합니다. 자세한 내용은 61-9페이지의 CAC를 사용하는 LDAP 인증 이해을/를 참조하십시오.

셸 액세스 특성

LDAP 서버에서 셸 액세스 특성으로 `uid`를 사용할 경우 로컬 어플라이언스는 로그인 시 입력된 사용자 이름을 `uid` 특성 값과 비교하여 확인합니다. `uid`가 아닌 사용자 지정 셸 액세스 특성을 설정할 수도 있습니다.

서버 유형을 선택하고 기본값을 설정하면 대개 그 서버 유형에 적합한 셸 액세스 특성이 미리 채워집니다. 그 값이 유효한 셸 액세스 사용자 이름이라면 어떤 특성도 사용할 수 있습니다. 사용자 이름은 고유해야 하며 밑줄(_), 마침표(.), 하이픈(-), 영숫자를 포함할 수 있습니다.

액세스 관리를 위한 그룹 멤버십 이해

라이센스: 모두

LDAP 그룹 사용자 멤버십 기반의 기본 액세스 권한을 선호하는 경우 FireSIGHT 시스템에서 사용하는 액세스 권한별로 LDAP 서버의 기존 그룹에 대해 DN을 지정할 수 있습니다. 그러면 어떤 지정된 그룹에도 속하지 않지만 LDAP에서 탐지한 사용자에 대해 기본 액세스 설정을 구성할 수 있습니다. 사용자가 로그인할 때 FireSIGHT 시스템에서는 동적으로 LDAP 서버를 확인하고 사용자의 현재 그룹 멤버십에 따라 액세스 권한을 지정합니다.

LDAP 서버에서 인증한 사용자가 처음으로 로컬 FireSIGHT 시스템 어플라이언스에 로그인할 경우 그 사용자는 자신이 속한 그룹의 액세스 권한을 받습니다. 그룹이 구성되지 않았으면 시스템 정책에서 선택된 기본 액세스 설정이 적용됩니다.

그런 다음 이 설정을 수정할 수 있습니다. 단 그룹 멤버십을 통해 부여된 설정이 아니어야 합니다.

셸 액세스 이해

라이센스: 모두

관리되는 디바이스 또는 방어 센터에서 셸 액세스를 위한 계정을 인증하는 데 LDAP 서버를 사용할 수 있습니다. 셸 액세스 권한을 부여하려는 사용자에 대한 엔트리를 가져오는 검색 필터를 지정합니다. 시스템 정책의 첫 번째 인증 객체에 대해서만 셸 액세스를 구성할 수 있습니다. 인증 객체의 순서 관리에 대한 자세한 내용은 63-12페이지의 외부 인증 활성화을/를 참조하십시오.

관리 계정을 제외하고 셸 액세스는 오로지 사용자가 설정하는 셸 액세스 특성을 통해 제어됩니다. 셸 사용자는 어플라이언스에서 기본 사용자로 구성됩니다. 여기서 설정하는 필터는 LDAP 서버의 어떤 사용자 집합이 셸에 로그인할 수 있는가를 결정합니다.

각 셸 사용자의 홈 디렉토리가 로그인 시 생성되며, LDAP 셸 액세스 사용자 계정이 비활성화된 경우(LDAP 연결 비활성화) 디렉토리는 남지만, 사용자 셸이 `/etc/password`의 `/bin/false`로 설정되어 셸이 비활성화됩니다. 그런 다음 사용자가 다시 활성화되면 동일한 홈 디렉토리를 사용하여 셸이 재설정됩니다.

기본 DN으로 정규화된 모든 사용자가 셸 액세스 권한에 대해서도 정규화될 경우 **Same as Base Filter**를 선택하여 셸 액세스 필터가 더 효율적으로 검색하도록 구성할 수 있습니다. 일반적으로 사용자 검색을 위한 LDAP 쿼리에서는 기본 필터와 셸 액세스 필터를 결합합니다. 동일한 셸 액세스 필터를 기본 필터로 입력할 경우 동일한 쿼리가 두 번 실행되므로 불필요하게 시간이 소모됩니다.

셸 사용자는 소문자의 사용자 이름으로 로그인할 수 있습니다. 셸에 대한 로그인 인증에서는 대/소문자를 구분합니다.

주의 Series 3 방어 센터에서는 모든 셸 사용자가 `sudoers` 권한을 갖습니다. 셸 액세스 권한을 갖는 사용자의 목록을 적절하게 제한해야 합니다. Series 3 및 가상 디바이스에서는 외부 인증 사용자에게 부여되는 셸 액세스 권한이 기본적으로 명령줄 액세스의 **Configuration** 레벨이며, 여기서도 `sudoers` 권한을 부여합니다.

CAC를 사용하는 LDAP 인증 이해

라이센스: 모두

조직에서 CAC(Common Access Card)를 사용할 경우 그룹 멤버십 또는 기본 액세스 권한에 따라 웹 인터페이스에 로그인하는 사용자를 인증하고 특정 기능에 대한 액세스 권한을 부여하도록 LDAP 인증을 구성할 수 있습니다. CAC 인증 및 권한 부여가 구성된 경우 사용자는 어플라이언스에 별도의 사용자 이름과 비밀번호를 제공하지 않고 곧바로 로그인할 수 있습니다.

참고 CAC 컨피그레이션 프로세스의 일환으로 사용자 인증서를 활성화하려면 브라우저에 유효한 사용자 인증서(여기서는 CAC를 통해 브라우저에 전달된 인증서)가 **반드시** 있어야 합니다. CAC 인증 및 권한 부여를 구성하면 네트워크의 사용자는 브라우징 세션 내내 CAC 연결을 **유지해야** 합니다. 세션 중에 CAC를 제거하거나 대체할 경우 웹 브라우저는 세션을 종료하며 웹 인터페이스에서 로그아웃됩니다.

CAC 인증 및 권한 부여를 구성하고 관리하는 것에 대한 자세한 내용은 다음 절을 참조하십시오.

- 61-10페이지의 CAC 인증 및 권한 부여 구성
- 61-11페이지의 CAC 인증 및 권한 부여 관리

CAC 인증 및 권한 부여 구성

라이센스: 모두

지원되는 디바이스: 가상 또는 X-Series를 제외하고 모두

지원되는 Defense Center: 가상 또는 X-Series를 제외하고 모두

네트워크의 사용자가 CAC 자격 증명을 사용하여 로그인하려면 먼저 알맞은 권한을 가진 사용자가 CAC 인증 및 권한 부여를 위한 다단계 컨피그레이션 프로세스를 완료해야 합니다.

CAC 인증 및 권한 부여를 구성하고 활성화하려면

액세스: Admin/Network Admin

1단계 조직의 지침대로 CAC를 삽입합니다.

2단계 브라우저에서 `https://hostname/`으로 이동합니다. 여기서 *hostname*은 방어 센터의 호스트 이름입니다.

3단계 프롬프트가 나타나면 1단계에서 삽입한 CAC의 PIN을 입력합니다.

PIN이 승인됩니다.

4단계 프롬프트가 나타나면 드롭다운 목록에서 알맞은 인증서를 선택합니다.

브라우저에서 선택한 내용을 적용하고 로그인 페이지가 나타납니다.

5단계 **Username** 및 **Password** 필드에서 관리자 권한의 사용자로 로그인합니다. 사용자 이름은 대/소문자를 구별합니다.

팁 완전히 구성된 CAC 인증 및 권한 부여가 있어야 CAC 자격 증명으로 로그인할 수 **있습니다**.

기본 시작 페이지가 나타납니다.

6단계 **System > Local > User Management**로 이동하고 **External Authentication** 탭을 클릭합니다. CAC 인증 및 권한 부여 전용 LDAP 인증 객체를 생성합니다. 61-12페이지의 LDAP 인증 객체를 생성하기 위한 준비 및 61-16페이지의 고급 LDAP 인증 객체 생성의 절차를 따르십시오. 다음 항목을 구성해야 합니다.

- **LDAP-Specific Parameters** 섹션의 고급 옵션에 있는 **User Name Template**. 자세한 내용은 61-8페이지의 사용자 이름 템플릿 이해을/를 참조하십시오.
- **Attribute Mapping** 섹션의 **UI Access Attribute**. 자세한 내용은 61-8페이지의 액세스 관리를 위한 특성 이해을/를 참조하십시오.

- LDAP 그룹 멤버십을 통해 액세스 권한을 미리 구성하려는 경우, **Group Controlled Access Roles** 섹션에 있는 기존 LDAP 그룹의 DN. 자세한 내용은 61-9페이지의 액세스 관리를 위한 그룹 멤버십 이해을/를 참조하십시오.

팁 동일한 인증 객체에서 CAC 인증과 셸 액세스를 모두 구성할 수는 **없습니다**. 셸 액세스에 대한 사용자 권한 부여도 수행하려면 별도의 인증 객체를 만들고 시스템 정책에서 별도로 활성화하십시오.

7단계 **Save**를 클릭합니다.

External Authentication 페이지가 나타나며, 새 객체가 표시되어 있습니다.

8단계 **System > Local > System Policy**로 이동합니다. 63-12페이지의 외부 인증 활성화의 절차에 따라 시스템 정책에서 외부 인증과 CAC 인증을 차례로 활성화합니다.

주의 변경사항이 **적용**되려면 방어 센터 및 관리되는 디바이스에 시스템 정책을 적용해야 합니다. 자세한 내용은 63-4페이지의 시스템 정책 적용을/를 참조하십시오.

9단계 **System > Local > Configuration**으로 이동하고 **HTTPS Certificate**를 클릭합니다. 필요하다면 64-5페이지의 서버 인증서 업로드의 절차에 따라 HTTPS 서버 인증서를 가져옵니다.

참고 인증 및 권한 부여에 사용할 CAC에 대해 동일한 CA(인증 기관)에서 HTTPS 서버 인증서와 사용자 인증서를 **발급**해야 합니다.

Current HTTPS Certificate 페이지가 업데이트되어 새 인증서를 반영합니다.

10단계 **HTTPS User Certificate Settings**에서 **Enable User Certificates**를 선택합니다. 자세한 내용은 64-6페이지의 사용자 인증서 요청을/를 참조하십시오.

11단계 사용자가 처음으로 로그인한 다음 **System > Local > User Management**로 이동하여 해당 사용자에 대한 액세스 권한을 직접 추가하거나 제거할 수도 있습니다. 사용자의 권한을 수정하지 않을 경우 그 사용자는 기본적으로 부여된 권한만 갖습니다. 자세한 내용은 61-4페이지의 사용자 권한 이해및 61-54페이지의 사용자 권한 및 옵션 수정을/를 참조하십시오.

최초 로그인 후 CAC 사용자의 역할 변경에 대한 자세한 내용은 다음 61-11페이지의 CAC 인증 및 권한 부여 관리 절을 참조하십시오.

CAC 인증 및 권한 부여 관리

CAC 인증 및 권한 부여를 구성하고 활성화하면 네트워크의 사용자가 CAC 자격 증명을 사용하여 어플라이언스의 웹 인터페이스에 로그인할 수 있습니다. 자세한 내용은 2-1페이지의 어플라이언스에 로그인을/를 참조하십시오.

CAC 인증 사용자는 시스템에서 EDIPI(electronic data interchange personal identifier) 번호로 식별됩니다. 사용자가 처음으로 CAC 자격 증명을 사용하여 로그인한 다음에는 User Management 페이지에서 그 사용자에 대한 액세스 권한을 직접 추가하거나 제거할 수 있습니다. 그룹 제어 액세스 역할을 사용하여 사용자 권한을 미리 구성하지 않은 경우 사용자는 시스템 정책에서 기본적으로 부여한 권한만 갖습니다. 자세한 내용은 61-4페이지의 사용자 권한 이해, 61-9페이지의 액세스 관리를 위한 그룹 멤버십 이해, 61-54페이지의 사용자 권한 및 옵션 수정을/를 참조하십시오.

24시간 동안 아무런 작업이 없어 User Management 페이지의 CAC 인증 사용자가 삭제될 때 수동으로 구성된 액세스 권한도 삭제됩니다. 다음에 로그인할 때마다 사용자가 페이지에 복원되지만, 액세스 권한에 대한 수동 변경사항은 다시 구성해야 합니다.

LDAP 인증 객체를 생성하기 위한 준비

라이센스: 모두

LDAP 서버와의 연결을 구성하기 전에 LDAP 인증 객체를 생성하는 데 필요한 정보를 수집해야 합니다. 컨피그레이션의 특정 요소에 대한 자세한 내용은 61-6페이지의 LDAP 인증 이해을/를 참조하십시오.

인증 객체에 대해 다음 항목이 필요합니다.

- 연결할 서버의 서버 이름 또는 IP 주소
- 연결할 서버의 서버 유형
- LDAP 트리를 탐색할 권한이 있는 사용자 계정의 사용자 이름 및 비밀번호
- 어플라이언스와 LDAP 서버 간에 방화벽이 있을 경우 발신 연결을 허용하는 방화벽 엔트리
- 사용자 이름이 상주하는 서버 디렉토리의 기본 DN(가능한 경우)

서드파티 LDAP 클라이언트를 사용하여 LDAP 트리를 탐색하고 기본 DN 및 특성 설명을 볼 수 있습니다. 또한 선택된 사용자가 선택된 기본 DN을 탐색할 수 있음을 확인하는 데에도 사용 가능합니다. LDAP 관리자로부터 LDAP 서버에 대해 승인된 LDAP 클라이언트를 추천받으십시오.

LDAP 인증 객체 컨피그레이션을 어떻게 사용자 지정할 것인가에 따라 다음 표의 정보도 필요할 수 있습니다.

표 61-1 추가 LDAP 컨피그레이션 정보

목적	필요한 정보
389가 아닌 포트를 통해 연결	포트 번호
암호화 연결을 통해 연결	연결용 인증서
특성 값에 따라 어플라이언스에 액세스할 수 있는 사용자 필터링	필터링 기준이 될 특성-값 쌍
사용자 DN을 확인하지 않고 특성을 UI 액세스 특성으로 사용	특성의 이름
사용자 DN을 확인하지 않고 특성을 셸 로그인 특성으로 사용	특성의 이름
특성 값에 따라 셸을 통해 어플라이언스에 액세스할 수 있는 사용자 필터링	필터링 기준이 될 특성-값 쌍
그룹과 특정 사용자 역할 연결	각 그룹의 DN 및 그룹 멤버십 특성(정적 그룹일 경우) 또는 그룹 멤버 URL 특성(동적 그룹일 경우)
인증 및 권한 부여에 CAC 사용	CAC, CAC를 발급한 CA에서 서명한 서버 인증서, 두 인증서의 인증서 체인

기본 LDAP 인증 객체 생성

라이센스: 모두

여러 값을 사용자 지정하는 LDAP 인증 객체를 설정할 수 있습니다. 그러나 특정 디렉토리의 모든 사용자만 인증하려는 경우 해당 디렉토리의 기본 DN으로 기본 인증 객체를 생성할 수 있습니다. 해당 서버 유형의 사용자에 대해 기본값을 설정하고 서버에서 사용자 데이터를 가져오는 데 쓰인 계정에 대해 인증 자격 증명을 제공할 경우 신속하게 인증 객체를 생성할 수 있습니다. 아래의 절차를 따르십시오.

참고 인증 객체를 생성할 때 (이를테면 CAC 인증 및 권한 부여를 구성하기 위해) 각 인증 설정을 고려하고 필요하다면 사용자 지정하는 것을 선호할 경우 61-16페이지의 고급 LDAP 인증 객체 생성의 절차에 따라 객체를 생성합니다. 또한 서버와의 연결을 암호화하거나 사용자 시간 초과를 설정하거나 사용자 이름 템플릿을 사용자 지정하거나 LDAP 그룹 멤버십 기반의 FireSIGHT 시스템 사용자 역할을 지정하려는 경우에도 고급 절차를 사용해야 합니다.

LDAP 서버와의 연결을 구성하기 전에 LDAP 인증 객체를 생성하는 데 필요한 정보를 수집해야 합니다. 컨피그레이션의 특정 요소에 대한 자세한 내용은 61-6페이지의 LDAP 인증 이해을/를 참조하십시오.

기본 인증 객체를 생성하려면 다음 항목이 필요합니다.

- 연결할 서버의 서버 이름 또는 IP 주소
- 연결할 서버의 서버 유형
- LDAP 트리를 탐색할 수 있는 권한을 가진 사용자 계정의 사용자 이름 및 비밀번호. Cisco에서는 이 용도로 도메인 관리자 사용자 계정을 사용할 것을 권장합니다.

사용자 검색 범위를 더 한정하기 위해 기본 필터를 추가하여 어떤 특성의 값을 구체적으로 설정할 수도 있습니다. 기본 필터는 기본 DN에서 필터에 설정된 특성 값을 갖는 객체만 검색하는 방법으로 검색을 집중시킵니다. 기본 필터는 괄호로 묶습니다. 예를 들어 CN(common name)이 F로 시작하는 사용자만 필터링하려면 `(cn=F*)`라는 필터를 사용합니다. 인증 객체를 저장할 때 로컬 어플라이언스는 기본 필터를 사용하여 쿼리하면서 이를 테스트하고 필터가 정확한 것으로 보이는지 여부를 나타냅니다.

LDAP 인증 객체를 생성하려면

액세스: Admin

1단계 **System > Local > User Management**를 선택합니다.

User Management 페이지가 나타납니다.

2단계 **External Authentication** 탭을 클릭합니다.

External Authentication 페이지가 나타납니다.

3단계 **Create External Authentication Object**를 클릭합니다.

4단계 **Authentication Method** 드롭다운 목록에서 **LDAP**를 선택합니다.

LDAP 컨피그레이션 옵션이 나타납니다.

5단계 **Name** 및 **Description** 필드에 인증 서버의 이름과 설명을 입력합니다.

6단계 **Server Type** 드롭다운 목록에서 서버 유형을 선택하고 **Set Defaults** 버튼을 클릭하여 그 유형의 기본 설정을 구성합니다. 다음 옵션을 이용할 수 있습니다.

- Microsoft Active Directory Server에 연결하는 경우 **MS Active Directory**를 선택하고 **Set Defaults**를 클릭합니다.
- Sun Java Systems Directory Server 또는 Oracle Directory Server에 연결하는 경우 **Oracle Directory**를 선택하고 **Set Defaults**를 클릭합니다.
- OpenLDAP 서버에 연결하는 경우 **OpenLDAP**를 선택하고 **Set Defaults**를 클릭합니다.
- 그 밖의 서버에 연결하는 경우 기본 설정을 지우려면 **Other**를 선택하고 **Set Defaults**를 클릭합니다.

7단계 **Primary Server Host Name/IP Address** 필드에 인증 데이터를 가져올 기본 서버의 IP 주소 또는 호스트 이름을 입력합니다.

참고 TLS 또는 SSL을 통해 연결하는 데 인증서를 사용하는 경우 인증서의 호스트 이름이 이 필드에 사용된 호스트 이름과 매칭해야 합니다. 또한 IPv6 주소는 암호화 연결에서 지원되지 않습니다.

8단계 모든 기본 DN의 목록을 가져오려면 **Fetch DNs**를 클릭하고 드롭다운 목록에서 알맞은 기본 DN을 선택합니다.

예를 들어 Example 회사의 Security 조직에 있는 이름을 인증하려면 `ou=security,dc=example,dc=com`을 선택합니다.

9단계 기본 DN으로 지정한 디렉토리 내의 특정 객체만 가져오는 필터를 설정하려면 **Base Filter** 필드에 특성 유형, 비교 연산자, 필터로 사용할 특성 값을 괄호로 묶어 입력합니다(여닫는 괄호 포함 최대 450자).

예를 들어 트리의 사용자 객체에 physicalDeliveryOfficeName 특성이 있고 뉴욕 사무실의 사용자는 그 특성의 값이 `NewYork`인 경우, 뉴욕 사무실의 사용자만 가져오려면 `(physicalDeliveryOfficeName=NewYork)`이라고 입력합니다.

10단계 **User Name** 및 **Password** 필드에 LDAP 서버를 탐색할 수 있는 자격 증명을 가진 사용자의 DN과 비밀번호를 입력합니다.

예를 들어 OpenLDAP 서버에 연결하는 중이고 그 사용자 객체에 `uid` 특성이 있으며 Example 회사 Security 부서의 관리자 객체가 `uid` 값이 `NetworkAdmin`이라면 `uid=NetworkAdmin,ou=security,dc=example,dc=com`과 같이 입력할 수 있습니다.

주의 Microsoft Active Directory Server에 연결하는 경우 `$` 문자로 끝나는 서버 사용자 이름을 제공할 수 없습니다.

11단계 **Confirm Password** 필드에 비밀번호를 다시 입력합니다.

12단계 셸 액세스를 위한 사용자를 가져오려면 **Shell Access Attribute** 필드에 필터링할 특성 유형을 입력합니다.

예를 들어 Microsoft Active Directory Server에서 `sAMAccountName` 셸 액세스 특성을 사용하여 셸 액세스 사용자를 가져오기 위해 **Shell Access Attribute** 필드에 `sAMAccountName`이라고 입력합니다.

참고 IPv6 주소는 셸 인증에서 지원되지 않습니다.

13단계 **User Name** 및 **Password** 필드에 LDAP 서버에 대한 액세스를 검증하는 데 그 자격 증명을 사용할 사용자의 `uid` 값 또는 셸 액세스 특성 값과 비밀번호를 입력합니다. Microsoft Active Directory Server와 관련된 서버 사용자 이름은 `$` 문자로 끝날 수 없습니다.

예를 들어 Example 회사의 `JSmith` 사용자 자격 증명을 가져올 수 있는지 테스트하려면 `JSmith`라고 입력합니다.

14단계 연결을 테스트하려면 **Test**를 클릭합니다.

테스트의 성공을 알리는 메시지 또는 누락되었거나 수정해야 할 설정을 자세히 알려주는 메시지가 나타납니다. 테스트가 성공할 경우 테스트 출력이 페이지의 맨 아래에 나타나며 연결에서 검색된 사용자의 목록도 포함됩니다. 테스트 출력에 나타난 사용자의 수가 LDAP 서버에서 반환하는 사용자 레코드 수에 의해 제한될 경우 테스트 출력에서 이 사실을 알려줍니다.

15단계 다음 2가지 옵션을 사용할 수 있습니다.

- 테스트가 성공할 경우 **Save**를 클릭합니다.

  External Authentication 페이지가 나타나며, 새 객체가 표시되어 있습니다.

어플라이언스의 객체를 사용하여 LDAP 인증을 활성화하려면 그 객체가 활성화된 시스템 정책을 어플라이언스에 적용해야 합니다. 자세한 내용은 63-12페이지의 외부 인증 활성화및 63-4페이지의 시스템 정책 적용을/를 참조하십시오.

- 테스트가 실패할 경우 또는 검색된 사용자 목록을 세분화하려는 경우 다음 61-15페이지의 기본 LDAP 인증 연결 튜닝 절로 진행합니다.

기본 LDAP 인증 연결 튜닝

라이센스: 모두

LDAP 인증 객체를 생성하는 경우, 선택한 서버와의 연결에 실패하거나 원하는 사용자 목록을 가져오지 않는다면 객체의 설정을 튜닝할 수 있습니다.

연결 테스트 결과, 연결에 실패할 경우 다음 방법으로 컨피그레이션의 문제를 해결해보십시오.

- 화면 맨 위 및 테스트 출력에 표시된 메시지를 참조하여 객체의 어느 영역에서 문제를 일으키는지 확인합니다.
- 객체에 대해 사용한 사용자 이름과 비밀번호가 올바른지 확인합니다.
- 사용자가 기본 DN에 나타난 디렉토리로 이동할 권한이 있는지 확인하기 위해 서드파티 LDAP 브라우저를 사용하여 LDAP 서버에 연결해봅니다.
- 사용자 이름이 LDAP 서버의 디렉토리 정보 트리에서 고유한지 확인합니다.
- 사용자 이름이 밑줄, 마침표, 하이픈, 영숫자만 포함하는지 확인합니다.
- 테스트 출력에 LDAP 바인드 오류 49가 있을 경우 그 사용자에 대한 사용자 바인딩이 실패한 것입니다. 서드파티 애플리케이션을 통해 서버 인증을 시도하여 그 연결에서도 바인딩이 실패하는지 확인합니다.
- 서버를 정확하게 식별했는지 확인합니다.
- 서버 IP 주소 또는 호스트 이름이 정확한지 확인합니다.
- 로컬 어플라이언스에서 연결할 인증 서버까지 TCP/IP 액세스 권한이 있는지 확인합니다.
- 서버에 대한 액세스가 방화벽에 의해 차단되지 않고 객체에 구성한 포트가 열려 있는지 확인합니다.
- TLS 또는 SSL을 통해 연결하는 데 인증서를 사용하는 경우 인증서의 호스트 이름이 서버에 대해 사용된 호스트 이름과 매칭해야 합니다.
- 셸 액세스를 인증하는 경우 서버 연결에 IPv6 주소를 사용하지 않았는지 확인합니다.
- 서버 유형 기본값을 사용한 경우 정확한 서버 유형인지 확인하고 **Set Defaults**를 다시 클릭하여 기본값을 재설정합니다.

  자세한 내용은 61-17페이지의 LDAP 인증 서버 식별을/를 참조하십시오.
- 기본 DN을 입력한 경우 **Fetch DNs**를 클릭하여 서버에서 사용 가능한 모든 기본 DN을 가져오고 그 목록에서 이름을 선택합니다.
- 필터, 액세스 특성 또는 고급 설정을 사용하는 경우 각각이 올바르고 제대로 입력되었는지 확인합니다.
- 필터, 액세스 특성 또는 고급 설정을 사용하는 경우 각 설정을 제거하고 그 설정 없이 객체를 테스트해봅니다.
- 기본 필터 또는 셸 액세스 필터를 사용하는 경우 필터가 괄호로 묶여 있고 올바른 비교 연산자를 사용하고 있는지 확인합니다. 자세한 내용은 61-7페이지의 기본 필터 이해및 61-9페이지의 셸 액세스 이해을/를 참조하십시오.

- 더 제한적인 기본 필터를 테스트하려면 사용자의 기본 DN으로 설정하여 그 사용자만 검색해 봅니다.
- 암호화 연결을 사용하는 경우
- 인증서에 있는 LDAP 서버의 이름이 연결에 사용하는 호스트 이름과 매칭하는지 확인합니다.
- 암호화 서버 연결에 IPv6 주소를 사용하지 않았는지 확인합니다.
- 테스트 사용자를 사용하는 경우 사용자 이름과 비밀번호가 제대로 입력되었는지 확인합니다.
- 테스트 사용자를 사용하는 경우 사용자 자격 증명을 제거하고 객체를 테스트합니다.
- 사용 중인 쿼리를 테스트합니다. 연결에 사용할 어플라이언스의 명령줄에서 다음 구문을 사용하여 LDAP 서버에 연결합니다.

```
ldapsearch -x -b 'base_distinguished_name'
-h LDAPserver_ip_address -p port -v -D
'user_distinguished_name' -W 'base_filter'
```

예를 들어 `myrtle.example.com`의 보안 도메인에 연결하기 위해 `domainadmin@myrtle.example.com` 사용자와 (`cn=*`) 기본 필터를 사용하는 경우 다음 구문으로 연결을 테스트할 수 있습니다.

```
ldapsearch -x -b 'CN=security,DC=myrtle,DC=example,DC=com'
-h myrtle.example.com -p 389 -v -D
'domainadmin@myrtle.example.com' -W '(cn=*)'
```

연결 테스트에 성공했지만 시스템 정책을 적용한 후 인증이 되지 않을 경우, 어플라이언스에 적용되는 시스템 정책에서 인증 및 사용할 객체가 모두 활성화되었는지 확인합니다.

성공적으로 연결했지만 연결에서 검색되는 사용자 목록을 조정하려는 경우 기본 필터 또는 셸 액세스 필터를 추가하거나 변경할 수 있습니다. 또는 더 제한적이거나 덜 제한적인 기본 DN을 사용할 수 있습니다. 자세한 내용은 다음 항목을 참조하십시오.

- 61-7페이지의 기본 DN 이해
- 61-7페이지의 기본 필터 이해
- 61-18페이지의 LDAP 관련 매개 변수 구성

고급 LDAP 인증 객체 생성

라이센스: 모두

어플라이언스에 사용자 인증 서비스를 제공하기 위해 LDAP 인증 객체를 생성할 수 있습니다.

인증 객체를 생성할 때 인증 서버에 연결하기 위한 설정을 정의합니다. 서버에서 사용자 데이터를 검색하는 데 사용할 디렉토리 컨텍스트 및 검색 기준도 선택합니다. 셸 액세스 인증을 구성할 수도 있습니다.

로컬 어플라이언스에서 연결할 인증 서버까지 TCP/IP 액세스 권한이 있어야 합니다.

기본 LDAP 컨피그레이션을 신속하게 설정하기 위해 서버 유형의 기본 설정을 사용할 수 있지만, 고급 설정을 사용자 지정하여 어플라이언스와 LDAP 서버의 암호화 연결 여부, 연결의 시간 초과, 서버가 사용자 정보를 얻기 위해 확인할 특성을 제어할 수 있습니다.

LDAP 관련 매개 변수에는 LDAP 명명 표준, 필터 및 특성 구문을 사용할 수 있습니다. 자세한 내용은 LDAP(v3): Technical Specification, RFC 3377에 나열된 RFC를 참조하십시오. 본 절차의 전 범위에서 구문의 예가 제시됩니다. Microsoft Active Directory Server에 연결하기 위해 인증 객체를 설정할 경우, 도메인을 포함하는 사용자 이름을 참조할 때 Internet RFC 822(Standard for the Format of ARPA Internet Text Messages) 사양에 기술된 주소 지정 구문을 사용할 수 있습니다. 예를 들어 Microsoft Active Directory Server 사용 시 사용자 객체를 참조할 때 `cn=JoeSmith,ou=security,dc=example,dc=com`이라는 사용자 DN(distinguished name) 대신 `JoeSmith@security.example.com`이라고 입력하면 됩니다.

참고 CAC 인증과 함께 사용할 LDAP 인증 객체를 구성하는 경우 컴퓨터에 삽입된 AC를 제거해서는 **안 됩니다**. 사용자 인증서를 활성화한 다음에는 항상 CAC가 **삽입된** 상태여야 합니다. 자세한 내용은 64-6페이지의 사용자 인증서 요청및 61-9페이지의 CAC를 사용하는 LDAP 인증 이해을/를 참조하십시오.

고급 인증 객체를 생성하려면

액세스: Admin

1단계 **System > Local > User Management**를 선택합니다.

User Management 페이지가 나타납니다.

2단계 **External Authentication** 탭을 클릭합니다.

External Authentication 페이지가 나타납니다.

3단계 **Create External Authentication Object**를 클릭합니다.

Create External Authentication Object 페이지가 나타납니다.

4단계 외부 인증을 위해 사용자 데이터를 검색할 인증 서버를 식별합니다. 자세한 내용은 61-17페이지의 LDAP 인증 서버 식별을/를 참조하십시오.

5단계 인증할 사용자를 가져오는 검색 요청을 작성하도록 인증 설정을 구성합니다. 사용자가 로그인할 때 입력하는 사용자 이름의 형식을 지정하기 위해 사용자 이름 템플릿을 지정합니다. 자세한 내용은 61-18페이지의 LDAP 관련 매개 변수 구성을/를 참조하십시오.

6단계 기본 액세스 역할 지정에 기준으로 사용할 LDAP 그룹을 구성할 수도 있습니다. 자세한 내용은 61-22페이지의 그룹별 액세스 권한 구성을/를 참조하십시오.

팁 CAC 인증 및 권한 부여에 이 객체를 사용하려는 경우 Cisco에서는 액세스 역할 지정을 관리하도록 LDAP 그룹을 구성하는 것을 권장합니다. 자세한 내용은 61-11페이지의 CAC 인증 및 권한 부여 관리을/를 참조하십시오.

7단계 셸 액세스를 위한 인증 설정을 구성할 수도 있습니다. 자세한 내용은 61-24페이지의 셸 액세스 구성을/를 참조하십시오.

8단계 성공적으로 인증할 수 있는 사용자의 이름과 비밀번호를 입력하여 컨피그레이션을 테스트합니다. 자세한 내용은 61-25페이지의 사용자 인증 테스트을/를 참조하십시오.

변경 내용이 저장되었습니다. 객체가 활성화된 시스템 정책을 어플라이언스에 적용해야 해당 어플라이언스에서 인증 변경사항이 적용됩니다. 자세한 내용은 63-12페이지의 외부 인증 활성화및 63-4페이지의 시스템 정책 적용을/를 참조하십시오.

LDAP 인증 서버 식별

라이센스: 모두

인증 객체를 생성할 때 관리되는 디바이스나 방어 센터에서 인증을 위해 연결할 기본 및 백업 서버와 그 서버 포트를 먼저 지정합니다.

LDAP 인증 서버를 식별하려면

액세스: Admin

1단계 **System > Local > User Management**를 선택합니다.

User Management 페이지가 나타납니다.

2단계 **External Authentication** 탭을 클릭합니다.

External Authentication 페이지가 나타납니다.

3단계 **Create External Authentication Object**를 클릭합니다.

Create External Authentication Object 페이지가 나타납니다.

4단계 **Authentication Method** 드롭다운 목록에서 **LDAP**를 선택합니다.

LDAP 컨피그레이션 옵션이 나타납니다.

5단계 CAC 인증 및 권한 부여에 이 인증 객체를 사용하려는 경우 **CAC** 확인란을 선택할 수도 있습니다.

CAC 인증 및 권한 부여를 구성하는 것에 대한 개요는 61-9페이지의 CAC를 사용하는 LDAP 인증 이해을/를 참조하십시오.

6단계 **Name** 및 **Description** 필드에 인증 서버의 이름과 설명을 입력합니다.

7단계 **Server Type** 필드에서 연결할 LDAP 서버의 유형을 선택하고 **Set Defaults**를 클릭하여 **User Name Template**, **UI Access Attribute**, **Shell Access Attribute**, **Group Member Attribute**, **Group Member URL Attribute** 필드를 기본값으로 채울 수도 있습니다. 다음 옵션을 이용할 수 있습니다.

- Microsoft Active Directory Server에 연결하는 경우 **MS Active Directory**를 선택하고 **Set Defaults**를 클릭합니다.
- Sun Java Systems Directory Server 또는 Oracle Directory Server에 연결하는 경우 **Oracle Directory**를 선택하고 **Set Defaults**를 클릭합니다.
- OpenLDAP 서버에 연결하는 경우 **OpenLDAP**를 선택하고 **Set Defaults**를 클릭합니다.
- 그 밖의 LDAP 서버에 연결하는 경우 기본 설정을 지우려면 **Other**를 선택하고 **Set Defaults**를 클릭합니다.

8단계 **Primary Server Host Name/IP Address** 필드에 인증 데이터를 가져올 기본 서버의 IP 주소 또는 호스트 이름을 입력합니다.

참고 TLS 또는 SSL을 통해 연결하는 데 인증서를 사용하는 경우 인증서의 호스트 이름이 이 필드에 사용된 호스트 이름과 매칭해야 합니다. 또한 IPv6 주소는 암호화 연결에서 지원되지 않습니다.

9단계 **Primary Server Port** 필드에서 기본 인증 서버가 사용하는 포트를 수정할 수도 있습니다.

10단계 **Backup Server Host Name/IP Address** 필드에 인증 데이터를 가져올 백업 서버의 IP 주소 또는 호스트 이름을 입력할 수도 있습니다.

11단계 **Backup Server Port** 필드에서 기본 인증 서버가 사용하는 포트를 수정할 수도 있습니다.

61-18페이지의 LDAP 관련 매개 변수 구성에서 계속하십시오.

LDAP 관련 매개 변수 구성

라이센스: 모두

LDAP 관련 매개 변수 섹션의 설정은 어플라이언스가 사용자 이름을 검색할 LDAP 디렉토리의 영역을 결정하고 어플라이언스가 LDAP 서버와 연결하는 방식의 세부사항을 제어합니다.

이러한 설정을 구성할 때 사용자 이름은 고유해야 하며 밑줄(_), 마침표(.), 하이픈(-)을 포함할 수 있지만 그 밖에는 영숫자만 지원됩니다.

또한 대부분의 LDAP 관련 설정에서는 LDAP 명명 표준, 필터 및 특성 구문을 사용할 수 있습니다. 자세한 내용은 LDAP(v3): Technical Specification, RFC 3377에 나열된 RFC를 참조하십시오. 본 절차의 전 범위에서 구문의 예가 제시됩니다. Microsoft Active Directory Server에 연결하기 위해 인증 객체를 설정할 경우, 도메인을 포함하는 사용자 이름을 참조할 때 Internet RFC 822(Standard for the Format of ARPA Internet Text Messages) 사양에 기술된 주소 지정 구문을 사용할 수 있습니다. 예를 들어 Microsoft Active Directory Server 사용 시 사용자 객체를 참조할 때 `cn=JoeSmith,ou=security, dc=example,dc=com`이라는 사용자 DN(distinguished name) 대신 `JoeSmith@security.example.com`이라고 입력하면 됩니다.

다음 표에서는 LDAP 관련 매개 변수 각각에 대해 설명합니다.

표 61-2 LDAP 관련 매개 변수

설정	설명	예
Base DN	어플라이언스가 LDAP 서버에서 사용자 정보를 찾기 위해 검색하는 디렉토리의 기본 DN입니다. 일반적으로 기본 DN은 회사 도메인과 운영 단위를 나타내는 기본 구조를 갖습니다. 기본 서버를 식별한 다음 그 서버에서 사용 가능한 기본 DN의 목록을 자동으로 가져온 다음 알맞은 기본 DN을 선택할 수 있습니다.	예를 들어 Example 회사의 Security 조직은 `ou=security,dc=example, dc=com`이라는 기본 DN을 가질 수 있습니다.
Base Filter	기본 DN에서 필터에 설정된 특성-값 쌍을 갖는 객체만 검색하는 방법으로 검색을 집중시킵니다. 기본 필터는 괄호로 묶어야 합니다. 테스트 사용자 이름과 비밀번호를 입력하여 더 구체적으로 기본 필터를 테스트하려면 61-25페이지의 사용자 인증 테스트을/를 참조하십시오.	CN이 F로 시작하는 사용자만 필터링하려면 `(cn=F*)`라는 필터를 사용합니다.
User Name/ Password	로컬 어플라이언스에서 사용자 객체에 액세스할 수 있게 합니다. 검색하려는 인증 객체에 대해 알맞은 권한을 가진 사용자의 자격 증명을 제공합니다. 지정하는 사용자의 DN이 LDAP 서버의 디렉토리 정보 트리에서 고유해야 합니다. Microsoft Active Directory Server와 관련된 서버 사용자 이름은 `$` 문자로 끝날 수 없습니다.	Example 회사 Security 조직의 `admin` 사용자는 사용자 이름이 다음과 같을 수 있습니다. `cn=admin, ou=security, dc=example,dc=com`
Encryption	통신이 암호화되는지 여부와 그 방식을 결정합니다. 암호화 없음, TLS(Transport Layer Security) 또는 SSL(Secure Sockets Layer) 암호화를 선택할 수 있습니다. TLS 또는 SSL을 통한 연결에서 인증 시 인증서를 사용하는 경우 인증서의 LDAP 서버 이름이 연결에 사용하는 이름과 **반드시** 매칭해야 합니다. 포트를 지정한 후 암호화 방식을 변경할 경우 포트는 선택된 서버 유형의 기본값으로 재설정됩니다.	외부 인증 설정에 `10.10.10.250`을 입력하고 인증서에 `computer1. example.com`이라고 입력하면 `computer1. example.com`의 IP 주소가 `10.10.10.250`이더라도 연결은 실패합니다. 외부 인증 설정에서 서버의 이름을 `computer1. example.com`으로 변경하면 연결에 성공합니다.
SSL Certificate Upload Path	로컬 컴퓨터에서 암호화에 사용할 인증서에 대한 경로를 나타냅니다.	`c:/server.crt`

표 61-2 LDAP 관련 매개 변수 (계속)

설정	설명	예
User Name Template	로그인할 때 입력하는 사용자 이름의 형식을 지정합니다. 문자열 변환 문자(`%s`)를 해당 사용자의 셸 액세스 특성 값에 매핑합니다. 사용자 이름 템플릿은 인증에 쓰이는 DN의 형식입니다. 사용자가 로그인 페이지에서 사용자 이름을 입력할 때 어플라이언스를 그 이름으로 문자열 변환 문자를 대체하고 그 결과 DN을 사용자 자격 증명 검색에 사용합니다. CAC 인증 및 권한 부여에 이 객체를 사용하려는 경우 **UI Access Attribute** 값에 해당하는 값을 입력해야 합니다. 자세한 내용은 61-9페이지의 CAC를 사용하는 LDAP 인증 이해을/를 참조하십시오.	`%s@security.example.com`, `%s@mail.com`, `%s@mil`, `%s@smil.mil`,
Timeout	기본 서버와의 연결 시도에 대한 시간 초과를 설정하며, 이 기간이 경과하면 백업 서버에 연결을 시도합니다. 이 필드에 초 단위로 표시된 값(또는 LDAP 서버의 시간 초과)만큼 경과할 때까지 기본 인증 서버의 응답이 없으면 어플라이언스는 백업 서버에 쿼리합니다. 그러나 LDAP이 기본 LDAP 서버의 포트에서 실행 중이고 어떤 이유로 요청에 대한 서비스를 거부할 경우 백업 서버에 대한 장애 조치가 이루어지지 않습니다.	기본 서버에서 LDAP이 비활성화된 경우 어플라이언스는 백업 서버를 쿼리합니다.
UI Access Attribute	로컬 어플라이언스에 사용자 DN의 값이 아닌 특정 특성의 값을 매칭하도록 지시합니다. 그 값이 FireSIGHT 시스템 웹 인터페이스의 유효한 사용자 이름이라면 어떤 특성도 사용할 수 있습니다. 객체 중 하나에 매칭하는 사용자 이름과 비밀번호가 있을 경우 사용자 로그인 요청이 인증됩니다. 서버 유형을 선택하고 기본값을 설정하면 **UI Access Attribute**가 대개 해당 사용자 유형에 적합한 값으로 미리 채워집니다. 이 필드를 비워 둘 경우 로컬 어플라이언스는 LDAP 서버의 사용자 레코드별 사용자 DN 값을 검사하여 사용자 이름과 매칭하는지 확인합니다. CAC 인증 및 권한 부여에 이 객체를 사용하려는 경우 **User Name Template** 값에 해당하는 값을 입력해야 합니다. 자세한 내용은 61-9페이지의 CAC를 사용하는 LDAP 인증 이해을/를 참조하십시오.	`sAMAccountName`, `userPrincipalName`, `mail`
Shell Access Attribute	셸 액세스 자격 증명에 대해 특정 특성을 확인하려는 경우 이 필드가 특성과 매칭하도록 명시적으로 설정해야 합니다. 그 값이 유효한 셸 액세스 사용자 이름이라면 어떤 특성도 사용할 수 있습니다. 이 필드를 비워 둘 경우 사용자 DN이 셸 액세스 인증에 사용됩니다. 서버 유형을 선택하고 기본값을 설정하면 대개 그 서버 유형에 적합한 특성으로 이 필드가 미리 채워집니다.	`sAMAccountName`

서버에 대해 LDAP 관련 매개 변수를 구성하려면

액세스: Admin

1단계 Create External Authentication Object 페이지의 **LDAP-Specific Parameters** 섹션에서 2가지 옵션으로 기본 DN을 설정할 수 있습니다.

- 모든 사용 가능 도메인의 목록을 가져오려면 **Fetch DNs**를 클릭하고 드롭다운 목록에서 알맞은 기본 도메인 이름을 선택합니다.
- **Base DN** 필드에 액세스하려는 LDAP 디렉토리의 기본 DN을 입력합니다.

예를 들어 Example 회사의 Security 조직에 있는 이름을 인증하려면 `ou=security,dc=example,dc=com`을 입력하거나 선택합니다.

2단계 기본 DN으로 지정한 디렉토리 내의 특정 객체만 가져오는 필터를 설정하려면 **Base Filter** 필드에 특성 유형, 비교 연산자, 필터로 사용할 특성 값을 괄호로 묶어 입력합니다.

예를 들어 디렉토리 트리의 사용자 객체에 physicalDeliveryOfficeName 특성이 있고 뉴욕 사무실의 사용자는 그 특성의 값이 `NewYork`인 경우, 뉴욕 사무실의 사용자만 가져오려면 `(physicalDeliveryOfficeName=NewYork)`이라고 입력합니다.

3단계 **User Name** 및 **Password** 필드에 LDAP 디렉토리에 대한 액세스를 검증하는 데 그 자격 증명을 사용할 사용자의 DN과 비밀번호를 입력합니다.

예를 들어 OpenLDAP 서버에 연결하는 중이고 그 사용자 객체에 `uid` 특성이 있으며 Example 회사 Security 부서의 관리자 객체가 `uid` 값이 `NetworkAdmin`이라면 `uid=NetworkAdmin,ou=security,dc=example,dc=com`과 같이 입력할 수 있습니다.

주의 Microsoft Active Directory Server에 연결하는 경우 `$` 문자로 끝나는 서버 사용자 이름을 제공할 수 없습니다.

4단계 **Confirm Password** 필드에 비밀번호를 다시 입력합니다.

5단계 기본 LDAP 관련 매개 변수를 구성한 다음에는 몇 가지 옵션이 있습니다.

- 고급 옵션에 액세스하려면 **Show Advanced Options** 옆의 화살표를 클릭하고 다음 단계로 진행합니다.
- LDAP 그룹 멤버십에 따라 사용자 기본 역할을 구성하려는 경우 61-22페이지의 그룹별 액세스 권한 구성으로 진행합니다.
- 인증에 LDAP 그룹을 사용하지 않는 경우 61-24페이지의 셸 액세스 구성으로 진행합니다.

6단계 다음 암호화 모드 중 하나를 선택할 수도 있습니다.

- SSL을 사용하여 연결하려면 **SSL**을 선택합니다.
- TLS를 사용하여 연결하려면 **TLS**를 선택합니다.
- 암호화하지 않고 연결하려면 **None**을 선택합니다.

참고 포트를 지정한 다음 암호화 방식을 변경할 경우 그 방법에 대해서는 포트가 기본값으로 재설정됩니다. 없음 또는 TLS일 경우 포트는 기본값인 389를 사용합니다. SSL 암호화를 선택할 경우 포트는 기본값인 636을 사용합니다.

7단계 TLS 또는 SSL 암호화를 선택했고 인증서를 사용하여 인증하려는 경우 **Browse**를 클릭하여 유효한 TLS 또는 SSL 인증서의 위치로 이동하거나 **SSL Certificate Upload Path** 필드에 인증서의 경로를 입력합니다.

인증서 업로드에 성공했다는 메시지가 나타납니다.

참고 인증서를 업로드한 적이 있고 그 인증서를 대체하려는 경우 새 인증서를 업로드하고 시스템 정책을 어플라이언스에 다시 적용하여 새 인증서를 복사합니다.

8단계 **User Name Template** 필드에 **UI Access Attribute**에 있는 값으로 사용자 이름을 확인하는 데 쓰이는 문자열 변환 문자(`%s`)를 입력할 수도 있습니다.

예를 들어 Example 회사의 Security 조직에서 근무하는 모든 사용자를 인증하기 위해 셸 액세스 특성이 `uid`인 OpenLDAP 서버에 연결하려면 **User Name Template** 필드에 `uid=%s,ou=security,dc=example,dc=com`이라고 입력할 수 있습니다. Microsoft Active Directory Server는 `%s@security.example.com`이라고 입력할 수 있습니다.

인증 및 권한 부여에 CAC 자격 증명을 사용하려는 경우 **User Name Template** 필드에 값을 입력해야 합니다. 자세한 내용은 61-9페이지의 CAC를 사용하는 LDAP 인증 이해을/를 참조하십시오.

9단계 **Timeout** 필드에 백업 연결로 전환할 때까지 기다리는 시간(초)을 입력할 수 있습니다.

10단계 또한 기본 DN 및 기본 필터 대신 특성을 기준으로 사용자를 검색하려면 2가지 옵션이 있습니다.

- **Fetch Attrs**를 클릭하여 사용 가능 특성의 목록을 가져오고 알맞은 특성을 선택합니다.
- **UI Access Attribute** 필드에 특성을 입력합니다.

예를 들어 Microsoft Active Directory Server의 경우 Active Directory Server 사용자 객체에 `uid` 특성이 없기 때문에 UI Access Attribute를 사용하여 사용자를 검색하려는 경우도 있습니다. 그 대신 `userPrincipalName` 특성을 검색할 수 있는데, `userPrincipalName`을 **UI Access Attribute** 필드에 입력하면 됩니다.

인증 및 권한 부여에 CAC 자격 증명을 사용하려는 경우 **UI Access Attribute** 필드에 값을 입력해야 합니다. 자세한 내용은 61-9페이지의 CAC를 사용하는 LDAP 인증 이해을/를 참조하십시오.

11단계 셸 액세스를 위한 사용자를 가져오려면 **Shell Access Attribute** 필드에 필터링 기준이 될 특성을 입력합니다.

예를 들어 Microsoft Active Directory Server에서 `sAMAccountName` 셸 액세스 특성을 사용하여 셸 액세스 사용자를 가져오기 위해 **Shell Access Attribute** 필드에 `sAMAccountName`이라고 입력합니다.

참고 동일한 인증 객체에서 CAC 인증과 권한 부여 및 셸 액세스를 구성할 수는 **없습니다**. **CAC** 확인란을 선택하면 페이지에서 셸 액세스 컨피그레이션 옵션이 비활성화됩니다. 그 대신 별도의 인증 객체를 생성하고 시스템 정책에서 따로 활성화하십시오. 자세한 내용은 63-12페이지의 외부 인증 활성화을/를 참조하십시오.

12단계 다음 단계에는 3가지 옵션이 있습니다.

- LDAP 그룹 멤버십에 따라 사용자 기본 역할을 구성하려는 경우 61-22페이지의 그룹별 액세스 권한 구성으로 진행합니다.
- 인증에 LDAP 그룹을 사용하지 **않지만** 셸 액세스를 구성하려는 경우 61-24페이지의 셸 액세스 구성으로 진행합니다.
- 인증에 LDAP 그룹을 사용하지 **않는** 상태에서 셸 액세스를 구성하지 **않으려면** 61-25페이지의 사용자 인증 테스트으로 진행합니다.

그룹별 액세스 권한 구성

라이센스: 모두

LDAP 그룹 사용자 멤버십 기반의 기본 액세스 권한을 선호하는 경우 FireSIGHT 시스템에서 사용하는 액세스 권한별로 LDAP 서버의 기존 그룹에 대해 DN을 지정할 수 있습니다. 그러면 어떤 지정된 그룹에도 속하지 않지만 LDAP에서 탐지한 사용자에 대해 기본 액세스 설정을 구성할 수 있습니다. 사용자가 로그인할 때 FireSIGHT 시스템에서는 동적으로 LDAP 서버를 확인하고 사용자의 현재 그룹 멤버십에 따라 기본 액세스 권한을 지정합니다.

CAC 인증 및 권한 부여에 객체를 사용하려는 경우 Cisco에서는 CAC 인증 사용자에 대해 액세스 역할 지정을 관리하도록 LDAP 그룹을 구성하는 것을 권장합니다. 자세한 내용은 61-11페이지의 CAC 인증 및 권한 부여 관리을/를 참조하십시오.

참조하는 모든 그룹이 LDAP 서버에 있어야 합니다. 고정 LDAP 그룹 또는 동적 LDAP 그룹을 참조할 수 있습니다. 고정 LDAP 그룹은 특정 사용자를 가리키는 그룹 객체 특성에 의해 멤버십이 결정되며, 동적 LDAP 그룹에서는 사용자 객체 특성에 따라 그룹 사용자를 가져오는 LDAP 검색을 생성하여 멤버십을 결정합니다. 어떤 역할에 대한 그룹 액세스 권한은 그룹의 멤버인 사용자에게만 영향을 미칩니다.

사용자가 FireSIGHT 시스템에 로그인할 때 부여되는 액세스 권한은 LDAP 컨피그레이션에 따라 달라집니다.

- LDAP 서버에 대해 어떤 그룹 액세스 권한도 구성되지 않을 경우, 새 사용자가 로그인하면 FireSIGHT 시스템에서는 LDAP 서버를 대상으로 사용자를 인증한 다음 시스템 정책에 설정된 기본 최소 액세스 역할에 따라 사용자 권한을 부여합니다.
- 그룹 설정이 구성된 경우 지정된 그룹에 속한 새 사용자는 자신이 멤버인 그룹의 최소 액세스 설정을 상속합니다.
- 새 사용자가 지정된 어떤 그룹에도 속하지 않을 경우 인증 객체의 Group Controlled Access Roles 섹션에 지정된 기본 최소 액세스 역할이 부여됩니다.
- 사용자가 둘 이상의 구성된 그룹에 속할 경우 최소 액세스 역할에서 액세스 레벨이 가장 높은 그룹의 액세스 역할을 갖습니다.

LDAP 그룹 멤버십에 따라 액세스 역할이 지정된 사용자의 최소 액세스 권한을 제거하는 데 FireSIGHT 시스템 사용자 관리 페이지를 사용할 수 없습니다. 그러나 추가 권한을 지정할 수는 있습니다. 외부 인증 사용자에 대한 액세스 권한을 수정할 때 User Management 페이지의 Authentication Method 열은 상태가 **External - Locally Modified**입니다.

참고 동적 그룹을 사용하는 경우 LDAP 서버에 구성된 대로 LDAP 쿼리가 사용됩니다. 이런 이유로 FireSIGHT 시스템에서는 검색 반복 횟수를 4로 제한하여 검색 구문 오류로 인한 무한 루프를 방지합니다. 그 반복 과정에서 사용자의 그룹 멤버십이 설정되지 않을 경우 Group Controlled Access Roles 섹션에 정의된 기본 액세스 역할이 사용자에게 부여됩니다.

그룹 멤버십에 따라 기본 역할을 구성하려면

액세스: Admin

1단계 Create External Authentication Object 페이지에서 **Group Controlled Access Roles** 옆의 아래쪽 화살표를 클릭합니다.

섹션이 펼쳐집니다.

2단계 그룹 멤버십별로 액세스 기본값을 구성할 수도 있습니다.

FireSIGHT 시스템 사용자 역할에 해당하는 **DN** 필드에 그 역할이 부여될 사용자를 포함하는 LDAP 그룹의 DN을 입력합니다.

예를 들어 **Administrator** 필드에 다음과 같이 입력하여 `Example` 회사의 정보 기술 조직에 있는 이름을 인증할 수 있습니다.

```
cn=itgroup,ou=groups, dc=example,dc=com
```

사용자 액세스 역할에 대한 자세한 내용은 61-44페이지의 새 사용자 계정 추가을/를 참조하십시오.

3단계 **Default User Role** 목록에서 지정된 어떤 그룹에도 속하지 않는 사용자의 기본 최소 액세스 역할을 선택합니다.

팁 Ctrl 키를 누른 채로 역할 이름을 클릭하여 여러 역할을 선택할 수 있습니다.

4단계 고정 그룹을 사용한 경우 **Group Member Attribute** 필드에 고정 그룹의 멤버십을 지정하는 LDAP 특성을 입력합니다.

예를 들어 기본 보안 분석가 액세스에 참조하는 고정 그룹의 멤버십을 나타내는 데 `member` 특성을 사용할 경우 `member`라고 입력합니다.

5단계 동적 그룹을 사용한 경우 **Group Member URL Attribute** 필드에 동적 그룹의 멤버십을 확인하는 데 쓰이는 LDAP 검색 문자열이 포함된 LDAP 특성을 입력합니다.

예를 들어 `memberURL` 특성이 기본 관리자 액세스에 대해 지정한 동적 그룹의 멤버를 가져오는 LDAP 검색을 포함할 경우 `memberURL`이라고 입력합니다.

6단계 61-24페이지의 셸 액세스 구성에서 계속하십시오.

셸 액세스 구성

라이센스: 모두

관리되는 디바이스 또는 방어 센터에서 셸 액세스를 위한 계정을 인증하는 데에도 LDAP 서버를 사용할 수 있습니다. 셸 액세스 권한을 부여하려는 사용자에 대한 엔트리를 가져오는 검색 필터를 지정합니다.

동일한 인증 객체에서 CAC 인증과 권한 부여 및 셸 액세스를 구성할 수는 **없습니다**. 그 대신 별도의 인증 객체를 생성하고 시스템 정책에서 따로 활성화하십시오. 셸 액세스를 위한 인증 객체는 시스템 정책의 첫 번째 인증 객체여야 합니다. 인증 객체의 순서 관리에 대한 자세한 내용은 63-12페이지의 외부 인증 활성화을/를 참조하십시오.

참고 Cisco에서는 가상 디바이스나 Cisco NGIPS for Blue Coat X-Series에 대해서는 외부 인증을 지원하지 않습니다. 또한 IPv6는 셸 액세스 인증에서 지원되지 않습니다.

관리 계정을 제외하고 셸 액세스는 오로지 사용자가 설정하는 셸 액세스 특성을 통해 제어됩니다. 설정하는 셸 액세스 필터는 LDAP 서버의 어떤 사용자 집합이 셸에 로그인할 수 있는가를 결정합니다.

각 셸 사용자의 홈 디렉토리가 로그인 시 생성되며, LDAP 셸 액세스 사용자 계정이 비활성화된 경우(LDAP 연결 비활성화) 디렉토리는 남지만, 사용자 셸이 `/etc/password`의 `/bin/false`로 설정되어 셸이 비활성화됩니다. 그런 다음 사용자가 다시 활성화되면 동일한 홈 디렉토리를 사용하여 셸이 재설정됩니다.

Same as Base Filter 확인란은 기본 DN에서 정규화된 모든 사용자가 셸 액세스 권한에 대해서도 정규화될 경우 더 효율적으로 검색할 수 있게 합니다. 일반적으로 사용자 검색을 위한 LDAP 쿼리에서는 기본 필터와 셸 액세스 필터를 결합합니다. 셸 액세스 필터가 기본 필터와 동일할 경우 동일한 쿼리가 두 번 실행되므로 불필요하게 시간이 소모됩니다. **Same as Base Filter** 옵션을 사용하여 두 가지 목적으로 쿼리가 한 번만 실행되게 할 수 있습니다.

셸 사용자는 소문자로 된 사용자 이름으로 로그인할 수 있습니다. 셸에 대한 로그인 인증에서는 대/소문자를 구분합니다.

주의 Series 3 방어 센터에서는 모든 셸 사용자가 sudoers 권한을 갖습니다. 셸 액세스 권한을 갖는 사용자의 목록을 적절하게 제한해야 합니다. Series 3 및 가상 디바이스에서는 외부 인증 사용자에게 부여되는 셸 액세스 권한이 기본적으로 명령줄 액세스의 **Configuration** 레벨이며, 여기서도 sudoers 권한을 부여합니다.

셸 계정 인증을 구성하려면

액세스: Admin

1단계 Create External Authentication Object 페이지에서 셸 액세스 계정 필터를 설정합니다. 여러 옵션이 있습니다.

- 특성 값에 따라 관리 사용자 엔트리를 검색하려면 **Shell Access Filter** 필드에 특성 이름, 비교 연산자, 필터로 사용할 특성 값을 괄호로 묶어 입력합니다.
- 인증 설정을 구성할 때 지정한 것과 동일한 필터를 사용하려면 **Same as Base Filter**를 선택합니다.
- 셸 액세스에 대해 LDAP 인증을 하지 않으려면 이 필드를 비워 둡니다. 셸 액세스 필터를 지정하지 않으면 인증 객체를 저장할 때 경고 메시지가 나타나 필터를 비워 둘 것인지 확인합니다.

예를 들어 모든 네트워크 관리자에게 manager 특성이 있고 그 값이 shell이라면 (manager=shell)이라는 기본 필터를 설정할 수 있습니다.

2단계 61-25페이지의 사용자 인증 테스트에서 계속하십시오.

사용자 인증 테스트

라이센스: 모두

LDAP 서버 및 인증 설정을 구성한 다음 이 설정을 테스트하기 위해 어떤 인증 가능 사용자에 대한 사용자 자격 증명을 지정할 수 있습니다.

사용자 이름에는 테스트할 사용자의 uid 특성 값을 입력합니다. Microsoft Active Directory Server에 연결하는 경우 uid 대신 셸 액세스 특성을 제공했다면 그 특성의 값을 사용자 이름으로 사용합니다. 그 사용자의 정규화된 DN을 지정할 수도 있습니다.

테스트 출력에서는 유효한 사용자 이름과 유효하지 않은 사용자 이름을 나열합니다. 사용자 이름은 고유해야 하며 밑줄(_), 마침표(.), 하이픈(-)을 포함할 수 있지만 그 밖에는 영숫자만 지원됩니다. 공백과 같이 영숫자가 아닌 다른 문자를 포함하는 사용자 이름은 잘못된 것입니다.

1,000명이 넘는 사용자로 서버와의 연결을 테스트할 경우 웹 인터페이스 페이지 크기 제한 때문에 1,000명의 사용자만 반환됩니다.

팁 테스트 사용자의 이름이나 비밀번호를 잘못 입력할 경우 서버 컨피그레이션이 올바르더라도 테스트는 실패합니다. 먼저 추가 테스트 매개 변수 없이 서버 컨피그레이션을 테스트하십시오. 그 테스트가 성공하면 사용자 이름과 비밀번호를 입력하여 특정 사용자로 테스트하십시오.

사용자 인증을 테스트하려면

액세스: Admin

1단계 **User Name** 및 **Password** 필드에 LDAP 서버에 대한 액세스를 검증하는 데 그 자격 증명을 사용할 사용자의 `uid` 값 또는 셸 액세스 특성 값과 비밀번호를 입력합니다.

예를 들어 Example 회사의 `JSmith` 사용자 자격 증명을 가져올 수 있는지 테스트하려면 `JSmith`라고 입력합니다.

2단계 **Test**를 클릭합니다.

테스트의 성공을 알리는 메시지 또는 누락되었거나 수정해야 할 설정을 자세히 알려주는 메시지가 나타납니다. 다음 2가지 옵션을 사용할 수 있습니다.

- 테스트가 성공할 경우 테스트 출력이 페이지의 맨 아래에 나타납니다. **Save**를 클릭합니다. External Authentication 페이지가 나타나며, 새 객체가 표시되어 있습니다.

  어플라이언스의 객체를 사용하여 LDAP 인증을 활성화하려면 그 객체가 활성화된 시스템 정책을 어플라이언스에 적용해야 합니다. 자세한 내용은 63-12페이지의 외부 인증 활성화및 63-4페이지의 시스템 정책 적용을/를 참조하십시오.
- 테스트가 실패할 경우 61-15페이지의 기본 LDAP 인증 연결 튜닝를 참조하여 연결의 문제를 해결하십시오. 오류 메시지는 연결이 실패한 이유를 알려줍니다.

LDAP 인증 객체의 예

라이센스: 모두

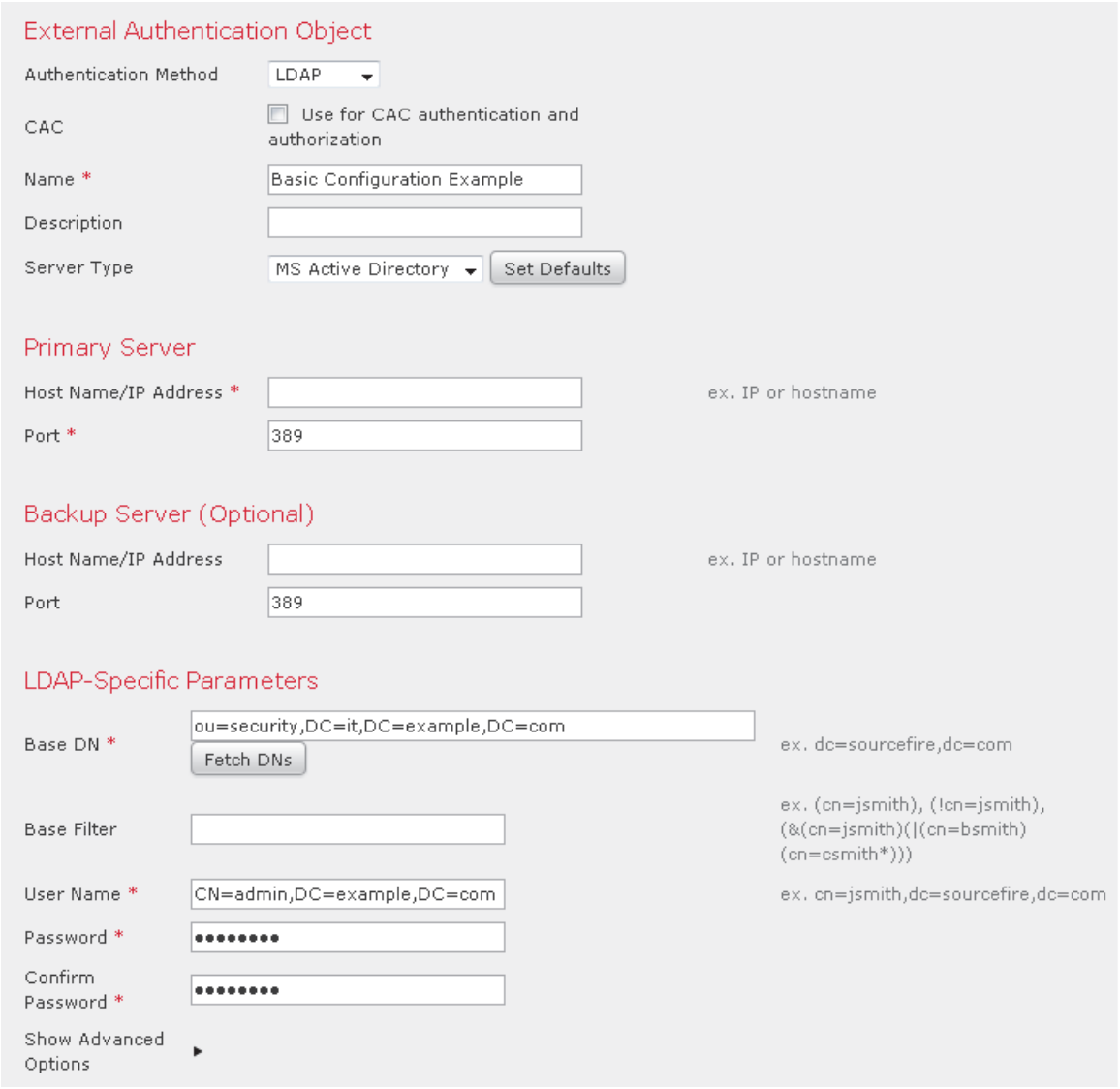
다음 절에서는 기본 설정을 사용한 LDAP 컨피그레이션의 예와 고급 컨피그레이션 옵션을 사용한 예를 보여줍니다.

- 61-26페이지의 예: 기본 LDAP 컨피그레이션
- 61-28페이지의 예: 고급 LDAP 컨피그레이션

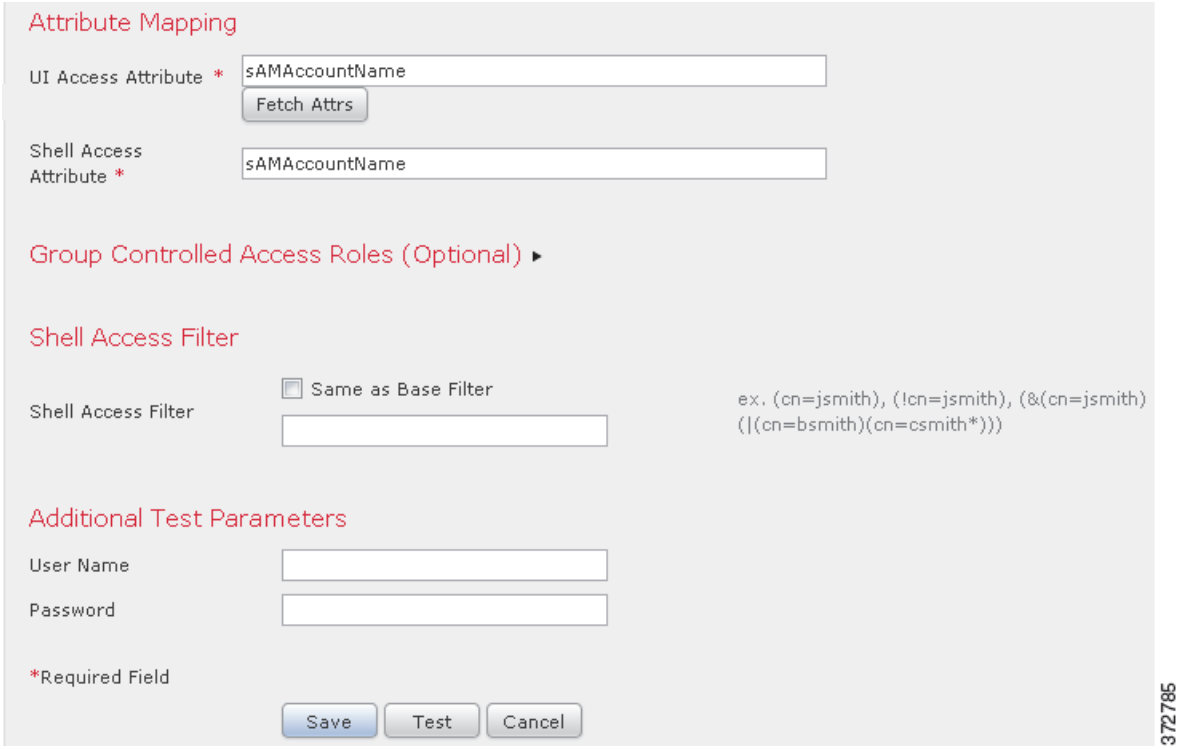
예: 기본 LDAP 컨피그레이션

라이센스: 모두

다음 그림은 Microsoft Active Directory Server를 위한 LDAP 로그인 인증 객체의 기본 컨피그레이션입니다. 여기서 LDAP 서버의 IP 주소는 10.11.3.4입니다. 이 연결은 포트 389를 액세스에 사용합니다.



이 예는 Example 회사의 정보 기술 도메인에 있는 Security 조직에 대해 `OU=security,DC=it,DC=example,DC=com`이라는 기본 DN을 사용하는 연결을 보여줍니다.



그러나 이 서버는 Microsoft Active Directory Server이므로 `uid` 특성이 아닌 `sAMAccountName` 특성을 사용하여 사용자 이름을 저장합니다. MS Active Directory Server 유형을 선택하고 **Set Defaults**를 클릭하면 UI Access Attribute가 `sAMAccountName`으로 설정됩니다. 그러면 FireSIGHT 시스템에서는 사용자가 FireSIGHT 시스템에 대한 로그인을 시도할 때 각 객체에 대해 `sAMAccountName` 특성을 검사하면서 사용자 이름을 매칭합니다.

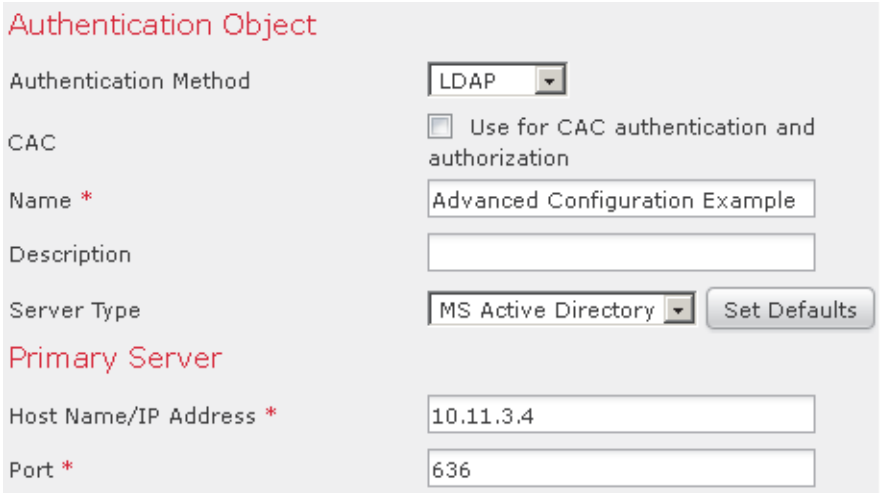
또한 Shell Access Attribute가 `sAMAccountName`이면 사용자가 어플라이언스의 셸 계정에 로그인할 때 디렉토리의 모든 객체에 대해 각 `sAMAccountName` 특성을 검사하여 매칭하는지 확인합니다.

이 서버에는 기본 필터가 적용되지 않으므로 FireSIGHT 시스템에서는 기본 DN이 나타내는 디렉토리의 모든 객체에 대해 특성을 검사합니다. 기본 기간(또는 LDAP 서버에 설정된 시간 초과 기간)이 경과하면 서버와의 연결이 시간 초과됩니다.

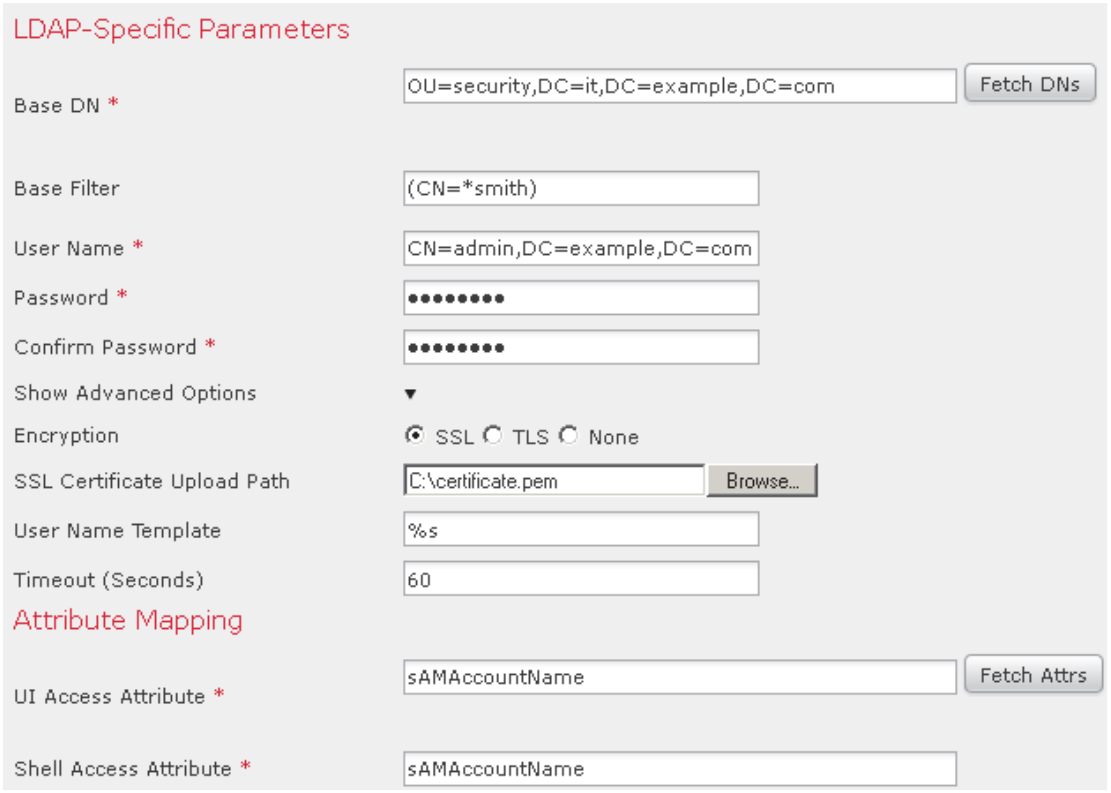
예: 고급 LDAP 컨피그레이션

라이센스: 모두

이 예에서는 Microsoft Active Directory Server에 대한 LDAP 로그인 인증 객체의 고급 컨피그레이션을 보여줍니다. 여기서 LDAP 서버의 IP 주소는 10.11.3.4입니다. 이 연결은 포트 636을 액세스에 사용합니다.



이 예는 Example 회사의 정보 기술 도메인에 있는 Security 조직에 대해 `OU=security,DC=it,DC=example,DC=com`이라는 기본 DN을 사용하는 연결을 보여줍니다. 그러나 이 서버는 기본 필터 `(cn=*smith)`가 있습니다. 이 필터는 CN이 `smith`로 끝나는 사용자만 서버에서 가져오도록 제한합니다.

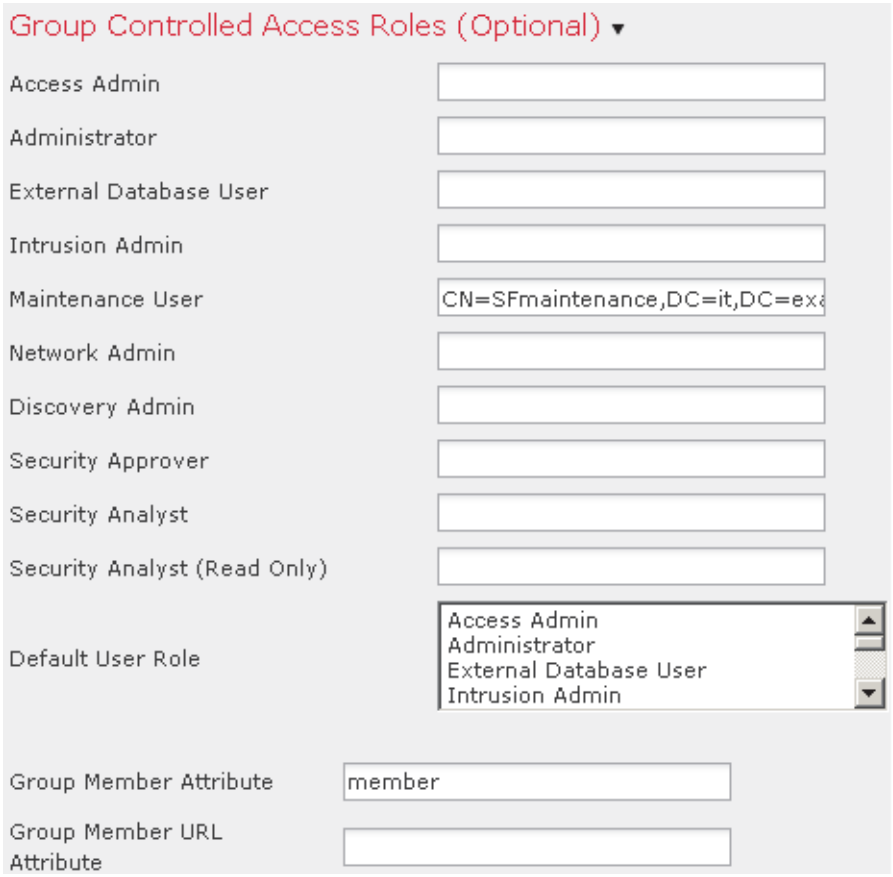


서버와의 연결은 SSL로 암호화되고 `certificate.pem`이라는 인증서가 연결에 사용됩니다. 또한 **Timeout** 설정 때문에 60초가 지나면 서버와의 연결이 시간 초과됩니다.

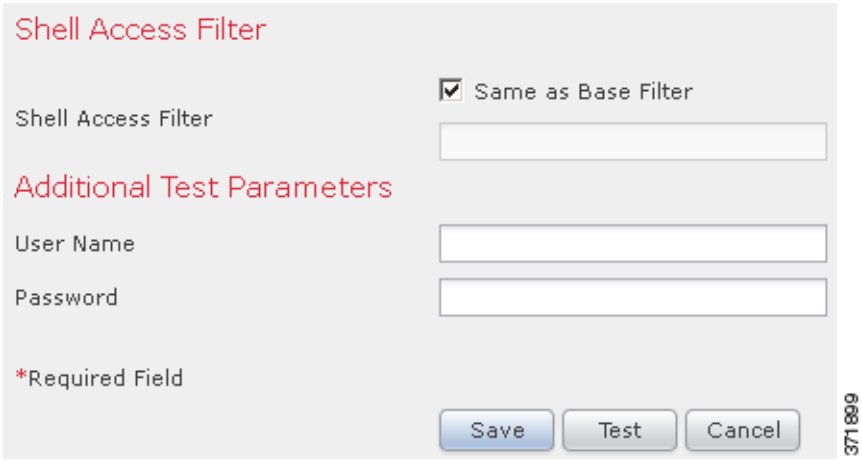
이 서버는 Microsoft Active Directory Server이므로 `uid` 특성이 아닌 `sAMAccountName` 특성을 사용하여 사용자 이름을 저장합니다. 컨피그레이션에 `sAMAccountName`이라는 UI Access Attribute가 포함되어 있습니다. 그러면 FireSIGHT 시스템에서는 사용자가 FireSIGHT 시스템에 대한 로그인을 시도할 때 각 객체에 대해 `sAMAccountName` 특성을 검사하면서 사용자 이름을 매칭합니다.

또한 Shell Access Attribute가 `sAMAccountName`이면 사용자가 어플라이언스의 셸 계정에 로그인할 때 디렉토리의 모든 객체에 대해 각 `sAMAccountName` 특성을 검사하여 매칭하는지 확인합니다.

여기에는 그룹 설정도 포함되어 있습니다. `member` 그룹 특성과 `CN=SFmaintenance,DC=it,DC=example,DC=com`이라는 기본 도메인 이름을 갖는 그룹의 모든 멤버에게 유지 보수 사용자 역할이 자동으로 지정됩니다.



셸 액세스 필터는 기본 필터와 동일하게 설정되므로, 동일한 사용자가 웹 인터페이스뿐 아니라 셸을 통해서도 어플라이언스에 액세스할 수 있습니다.



LDAP 인증 객체 수정

라이센스: 모두

기존 인증 객체를 수정할 수 있습니다. 정책을 다시 적용해야 변경사항이 적용됩니다.

인증 객체를 수정하려면

액세스: Admin

1단계 **System > Local > User Management**를 선택합니다.

User Management 페이지가 나타납니다.

2단계 **External Authentication** 탭을 클릭합니다.

External Authentication 페이지가 나타납니다.

3단계 수정할 객체 옆의 수정 아이콘( )을 클릭합니다.

Create External Authentication Object 페이지가 나타납니다.

4단계 필요에 맞게 객체 설정을 수정합니다.

5단계 **Test**를 클릭합니다.

테스트의 성공을 알리는 메시지 또는 누락되었거나 수정해야 할 설정을 자세히 알려주는 메시지가 나타납니다. 테스트가 성공할 경우 테스트 출력이 페이지의 맨 아래에 나타납니다.

테스트가 실패할 경우 61-15페이지의 기본 LDAP 인증 연결 튜닝를 참조하여 연결의 문제를 해결하십시오. 오류 메시지는 연결이 실패한 이유를 알려줍니다.

6단계 **Save**를 클릭합니다.

변경사항이 저장되었고 External Authentication 페이지가 나타납니다. 객체가 활성화된 시스템 정책을 어플라이언스에 적용해야 해당 어플라이언스에서 인증 변경사항이 적용됩니다. 자세한 내용은 63-12페이지의 외부 인증 활성화및 63-4페이지의 시스템 정책 적용을/를 참조하십시오.

RADIUS 인증

RADIUS(Remote Authentication Dial In User Service)는 네트워크 리소스에 대한 사용자 액세스의 인증, 권한 부여, 어카운팅에 사용되는 인증 프로토콜입니다. RFC 2865를 준수하는 어떤 RADIUS 서버에 대해서도 인증 객체를 생성할 수 있습니다.

자세한 내용은 다음 절을 참조하십시오.

RADIUS 인증 이해

라이센스: 모두

RADIUS 서버에서 인증된 사용자가 처음으로 로그인할 때 인증 객체에서 그 사용자에 대해 지정된 역할을 갖습니다. 사용자가 어떤 사용자 역할에도 등록되지 않은 경우 인증 객체에서 선택한 기본 액세스 역할을 갖습니다. 인증 객체에 어떤 기본 액세스 역할도 선택되지 않은 경우 시스템 정책의 기본 액세스 역할이 적용됩니다. 필요하다면 사용자의 역할을 수정할 수 있습니다. 단, 인증 객체의 사용자 목록을 통해 부여된 설정은 제외됩니다. RADIUS 서버에서 특성 매칭으로 인증된 사용자가 처음으로 로그인을 시도할 때 그 사용자 계정이 생성되므로 로그인이 거부됩니다. 사용자는 다시 로그인해야 합니다.

참고 Series 3가 관리하는 디바이스에서 외부 인증을 활성화하려면 먼저 셸 액세스 필터에 포함된 외부 인증 사용자와 동일한 사용자 이름을 갖는 내부 인증 셸 사용자를 모두 삭제해야 합니다.

FireSIGHT 시스템에서 구현한 RADIUS는 SecurID® 토큰 사용을 지원합니다. SecurID를 사용하여 서버의 인증을 구성할 경우, 그 서버에 대해 인증된 사용자는 SecurID 토큰이 SecurID PIN의 끝에 추가되며 Cisco 어플라이언스에 로그인할 때 이것을 비밀번호로 사용합니다. SecurID 가 FireSIGHT 시스템 외부에서 사용자를 인증할 수 있도록 올바르게 구성되었다면 그 사용자는 어플라이언스에 추가 컨피그레이션이 없더라도 자신의 PIN과 SecurID 토큰을 사용하여 FireSIGHT 시스템 어플라이언스에 로그인할 수 있습니다.

RADIUS 인증 객체 생성

라이센스: 모두

RADIUS 인증 객체를 생성할 때 인증 서버에 연결하기 위한 설정을 정의합니다. 또한 특정 사용자와 기본 사용자에게 사용자 역할을 부여합니다. RADIUS 서버가 인증할 사용자에 대해 사용자 지정 특성을 반환할 경우 그 사용자 지정 특성을 정의해야 합니다. 셸 액세스 인증을 구성할 수도 있습니다.

인증 객체를 생성하려면 로컬 어플라이언스에서 연결하려는 인증 서버까지 TCP/IP 액세스가 필요합니다.

인증 객체를 생성하려면

액세스: Admin

1단계 **System > Local > User Management**를 선택합니다.

User Management 페이지가 나타납니다.

2단계 **External Authentication** 탭을 클릭합니다.

External Authentication 페이지가 나타납니다.

3단계 **Create External Authentication Object**를 클릭합니다.

Create External Authentication Object 페이지가 나타납니다.

4단계 외부 인증을 위한 사용자 데이터를 가져오려는 기본 및 백업 인증 서버를 식별하고 시간 초과 및 재시도 값을 설정합니다. 자세한 내용은 61-33페이지의 RADIUS 연결 설정 구성을/를 참조하십시오.

5단계 기본 사용자 역할을 설정합니다. 특정 FireSIGHT 시스템 액세스 역할을 갖게 될 사용자에 대해 사용자 또는 사용자 특성 값을 지정할 수도 있습니다. 자세한 내용은 61-34페이지의 RADIUS 사용자 역할 구성을/를 참조하십시오.

6단계 관리 셸 액세스를 구성할 수도 있습니다. 자세한 내용은 61-35페이지의 관리 셸 액세스 구성을/를 참조하십시오.

7단계 인증할 사용자의 프로필에서 사용자 지정 RADIUS 특성을 반환할 경우 그 특성을 정의하십시오. 자세한 내용은 61-36페이지의 사용자 지정 RADIUS 특성 정의을/를 참조하십시오.

8단계 성공적으로 인증될 사용자의 이름과 비밀번호를 입력하여 컨피그레이션을 테스트합니다. 자세한 내용은 61-37페이지의 사용자 인증 테스트을/를 참조하십시오.

변경 내용이 저장되었습니다. 객체가 활성화된 시스템 정책을 어플라이언스에 적용해야 해당 어플라이언스에서 인증 변경사항이 적용됩니다. 자세한 내용은 63-12페이지의 외부 인증 활성화및 63-4페이지의 시스템 정책 적용을/를 참조하십시오.

RADIUS 연결 설정 구성

라이센스: 모두

RADIUS 인증 객체를 생성할 때 로컬 어플라이언스(관리되는 디바이스나 방어 센터)에서 인증을 위해 연결할 기본 및 백업 서버와 그 서버 포트를 먼저 지정합니다.

참고 RADIUS가 제대로 작동하려면 방화벽에서 그 인증 및 어카운팅 포트(기본적으로 1812 및 1813)를 열어야 합니다.

백업 인증 서버를 지정할 경우 기본 서버에 대한 연결 시도의 시간 초과를 설정할 수 있습니다. **Timeout** 필드에 초 단위로 표시된 시간(또는 LDAP 서버의 시간 초과)이 경과할 때까지 기본 인증 서버에서 응답이 없으면 어플라이언스는 기본 서버를 다시 쿼리합니다.

어플라이언스에서 **Retries** 필드에 표시된 횟수만큼 기본 인증 서버를 다시 쿼리했고 역시 **Timeout** 필드의 시간만큼 경과할 때까지 기본 인증 서버의 응답이 없을 경우 어플라이언스는 백업 서버로 넘어갑니다.

예를 들어 기본 서버에서 RADIUS가 비활성화된 경우 어플라이언스는 백업 서버를 쿼리합니다. 그러나 RADIUS가 기본 RADIUS 서버의 포트에서 실행 중인데 어떤 이유(잘못된 컨피그레이션 또는 기타 문제)로 요청에 대한 서비스를 거부할 경우에는 백업 서버에 대한 장애 조치가 이루어지지 않습니다.

RADIUS 인증 서버를 식별하려면

액세스: Admin

1단계 **System > Local > User Management**를 선택합니다.

User Management 페이지가 나타납니다.

2단계 **External Authentication** 탭을 클릭합니다.

External Authentication 페이지가 나타납니다.

3단계 **Create External Authentication Object**를 클릭합니다.

Create External Authentication Object 페이지가 나타납니다.

4단계 **Authentication Method** 드롭다운 목록에서 **RADIUS**를 선택합니다.

RADIUS 컨피그레이션 옵션이 나타납니다.

5단계 **Name** 및 **Description** 필드에 인증 서버의 이름과 설명을 입력합니다.

6단계 **Primary Server Host Name/IP Address** 필드에 인증 데이터를 가져올 기본 RADIUS 서버의 IP 주소 또는 호스트 이름을 입력합니다.

참고 IPv6 주소는 셸 인증에서 지원되지 않습니다. 기본 RADIUS 서버에 IPv6 주소를 사용할 때 셸 인증을 허용하려면 해당 서버에 대해 IPv4 주소를 사용하여 인증 객체를 설정하고 그 IPv4 객체를 시스템 정책의 첫 번째 인증 객체로 사용합니다.

7단계 **Primary Server Port** 필드에서 기본 RADIUS 인증 서버가 사용하는 포트를 수정할 수도 있습니다.

참고 인증 포트 번호와 어카운팅 포트 번호가 순차적이지 않을 경우 이 필드를 비워 둡니다. 그러면 어플라이언스의 `/etc/services` 파일에 있는 `radius` 및 `radacct` 데이터로 RADIUS 포트 번호를 결정합니다.

8단계 **RADIUS Secret Key** 필드에 기본 RADIUS 인증 서버의 비밀 키를 입력합니다.

9단계 **Backup Server Host Name/IP Address** 필드에 인증 데이터를 가져올 백업 RADIUS 서버의 IP 주소 또는 호스트 이름을 입력합니다.

10단계 **Backup Server Port** 필드에서 백업 RADIUS 인증 서버가 사용하는 포트를 수정할 수도 있습니다.

참고 인증 포트 번호와 어카운팅 포트 번호가 순차적이지 않을 경우 이 필드를 비워 둡니다. 그러면 어플라이언스의 `/etc/services` 파일에 있는 `radius` 및 `radacct` 데이터로 RADIUS 포트 번호를 결정합니다.

11단계 **RADIUS Secret Key** 필드에 백업 RADIUS 인증 서버의 비밀 키를 입력합니다.

12단계 **Timeout** 필드에 연결을 재시도하기 전에 기다리는 시간(초)을 입력합니다.

13단계 **Retries** 필드에는 백업 연결로 넘어가기 전에 기본 서버 연결을 시도하는 횟수를 입력합니다.

14단계 61-34페이지의 RADIUS 사용자 역할 구성에서 계속하십시오.

RADIUS 사용자 역할 구성

라이센스: 모두

FireSIGHT 시스템에서 사용하는 액세스 역할별로 사용자 이름을 나열하는 방법으로 RADIUS 서버의 기존 사용자에 대한 액세스 역할을 지정할 수 있습니다. 이때 RADIUS에서 탐지했지만 특정 역할이 지정되지 않은 사용자에 대한 기본 액세스 설정도 구성할 수 있습니다.

사용자가 로그인할 때 FireSIGHT 시스템에서는 RADIUS 서버를 확인하고 RADIUS 컨피그레이션에 따라 액세스 권한을 부여합니다.

- 어떤 사용자에 대해 액세스 권한이 구성되지 않았고 기본 액세스 역할도 선택되지 않은 경우, 새 사용자가 로그인하면 FireSIGHT 시스템에서는 RADIUS 서버를 대상으로 사용자를 인증하고 시스템 정책에 설정된 기본 액세스 역할에 따라 사용자 권한을 부여합니다.
- 새 사용자가 어떤 목록에도 지정되지 않았고 인증 객체의 **Default User Role** 목록에 기본 액세스 역할이 선택되어 있다면 그 액세스 역할이 지정됩니다.
- 하나 이상의 역할에 대한 목록에 사용자를 추가할 경우 그 사용자는 지정된 모든 액세스 역할을 갖습니다.

사용자 이름 대신 특성-값 쌍을 사용하여 특정 사용자 역할을 가질 사용자를 식별할 수도 있습니다. 예를 들어 보안 분석가가 되어야 하는 모든 사용자의 `User-Category` 특성의 값이 `Analyst`임을 알고 있다면 Security Analyst List 필드에 `User-Category=Analyst`를 입력하여 해당 사용자에게 이 역할을 부여할 수 있습니다. 사용자 역할 멤버십 설정에 사용할 사용자 지정 특성은 미리 정의해야 합니다. 자세한 내용은 61-36페이지의 사용자 지정 RADIUS 특성 정의을/를 참조하십시오.

특정 역할에 등록되지 않은 외부 인증 사용자에게 부여할 기본 사용자 역할을 지정할 수 있습니다. **Default User Role** 목록에서 여러 역할을 선택할 수 있습니다.

FireSIGHT 시스템에서 지원하는 사용자 역할에 대한 자세한 내용은 61-34페이지의 RADIUS 사용자 역할 구성을/를 참조하십시오.

RADIUS 사용자 목록 멤버십에 따라 액세스 역할을 부여받은 사용자에 대해서는 그 최소 액세스 권한을 FireSIGHT 시스템 사용자 관리 페이지에서 제거할 수 없습니다. 그러나 추가 권한을 지정할 수는 있습니다.

주의 어떤 사용자의 최소 액세스 설정을 변경하려면 RADIUS Specific Parameters 섹션에서 그 사용자를 다른 목록으로 이동하거나 RADIUS 서버에서 사용자의 특성을 변경할 뿐 아니라 시스템 정책을 다시 적용해야 하며, 사용자 관리 페이지에서 지정된 사용자 권한을 제거해야 합니다.

사용자 목록 기반의 액세스를 설정하려면

액세스: Admin

1단계 FireSIGHT 시스템 사용자 역할에 해당하는 필드에 각 사용자의 이름을 입력하거나 해당 역할에 지정될 식별 특성-값 쌍을 입력합니다. 사용자 이름과 특성-값 쌍은 쉼표로 구분합니다.

예를 들어 사용자 `jsmith`와 `jdoe`에게 관리자 역할을 부여하려면 **Administrator** 필드에 `jsmith, jdoe`라고 입력합니다.

또 다른 예로 `User-Category`의 값이 `Maintenance`인 모든 사용자에게 유지 보수 사용자 역할을 부여하려면 **Maintenance User** 필드에 `User-Category=Maintenance`라고 입력합니다.

사용자 액세스 역할에 대한 자세한 내용은 61-48페이지의 사용자 역할 구성을/를 참조하십시오.

2단계 지정된 어떤 그룹에도 속하지 않는 사용자를 위한 기본 최소 액세스 권한을 **Default User Role** 목록에서 선택합니다.

팁 Ctrl 키를 누른 채로 역할 이름을 클릭하여 여러 역할을 선택할 수 있습니다.

3단계 61-35페이지의 관리 셸 액세스 구성에서 계속하십시오.

관리 셸 액세스 구성

라이센스: 모두

로컬 어플라이언스(관리되는 디바이스 또는 방어 센터)에서 셸 액세스를 위한 계정을 인증하는 데에도 RADIUS 서버를 사용할 수 있습니다. 셸 액세스 권한을 부여할 사용자의 사용자 이름을 지정합니다. 시스템 정책의 첫 번째 인증 객체에 대해서만 셸 액세스를 구성할 수 있습니다. 인증 객체의 순서 관리에 대한 자세한 내용은 63-12페이지의 외부 인증 활성화을/를 참조하십시오.

참고 IPv6 주소는 셸 인증에서 지원되지 않습니다. 기본 RADIUS 서버를 IPv6 주소로 구성하고 관리 셸 액세스도 구성할 경우 셸 액세스 설정이 무시됩니다. 기본 RADIUS 서버에 IPv6 주소를 사용할 때 셸 인증을 허용하려면 해당 서버에 대해 IPv4 주소를 사용하여 또 다른 인증 객체를 설정하고 그 IPv4 객체를 시스템 정책의 첫 번째 인증 객체로 사용합니다.

관리 계정을 제외하고 RADIUS 인증 객체에서 설정한 셸 액세스 목록이 어플라이언스에 대한 셸 액세스를 온전히 제어합니다. 시스템 정책이 적용될 때 셸 사용자는 어플라이언스의 로컬 사용자로 구성됩니다. RADIUS 서버에서 특성 매칭으로 인증된 사용자가 처음으로 로그인을 시도할 때 그 사용자 계정이 생성되므로 로그인이 거부됩니다. 사용자는 다시 로그인해야 합니다.

각 셸 사용자의 홈 디렉토리가 로그인 시 생성되며, RADIUS 셸 액세스 사용자 계정이 비활성화된 경우(RADIUS 연결 비활성화) 디렉토리는 남지만, 사용자 셸이 `/etc/password`의 `/bin/false`로 설정되어 셸이 비활성화됩니다. 그런 다음 사용자가 다시 활성화되면 동일한 홈 디렉토리를 사용하여 셸이 재설정됩니다.

셸 사용자는 소문자로 된 사용자 이름으로 로그인할 수 있습니다. 셸에 대한 로그인 인증에서는 대/소문자를 구분합니다.

주의 Series 3 방어 센터에서는 모든 셸 사용자가 `sudoers` 권한을 갖습니다. 셸 액세스 권한을 갖는 사용자의 목록을 적절하게 제한해야 합니다. Series 3 및 가상 디바이스에서는 외부 인증 사용자에게 부여되는 셸 액세스 권한이 기본적으로 명령줄 액세스의 **Configuration** 레벨이며, 여기서도 `sudoers` 권한을 부여합니다.

셸 계정 인증을 구성하려면

액세스: Admin

1단계 **Administrator Shell Access User List** 필드에 사용자 이름을 쉼표로 구분하며 입력합니다.

참고 셸 액세스 필터를 지정하지 않으면 인증 객체를 저장할 때 경고 메시지가 나타나 필터를 비워 둘 것인지 확인합니다.

2단계 61-36페이지의 사용자 지정 RADIUS 특성 정의에서 계속하십시오.

사용자 지정 RADIUS 특성 정의

라이센스: 모두

RADIUS 서버가 `/etc/radiusclient/`의 `dictionary` 파일에 없는 특성의 값을 반환할 경우, 이 특성을 갖는 사용자에 대한 사용자 역할을 설정하는 데 이 특성을 사용하려면 로그인 인증 객체에서 이 특성을 정의해야 합니다.

RADIUS 서버에서 사용자 프로필을 확인하여 사용자에 대해 반환되는 특성을 찾을 수 있습니다.

특성을 정의할 때 영숫자로 구성된 특성의 이름을 제공합니다. 특성 이름의 단어는 공백이 아닌 대시로 구분해야 합니다. 또한 특성 ID를 제공하는데, 이는 정수이며 `etc/radiusclient/dictionary` 파일에 있는 기존 특성 ID와 충돌해서는 안 됩니다. 특성의 유형을 즉 문자열, IP 주소, 정수 또는 날짜로 지정합니다.

예를 들어 RADIUS 서버가 Cisco 라우터가 있는 네트워크에서 사용되는 경우 `Ascend-Assign-IP-Pool` 특성을 사용하여 특정 IP 주소 풀에서 로그인한 모든 사용자에게 어떤 역할을 부여할 수 있습니다. `Ascend-Assign-IP-Pool`은 정수 특성으로서 사용자가 로그인할 수 있는 주소 풀을 정의합니다. 여기서 정수는 지정된 IP 주소 풀의 번호를 나타냅니다. 사용자 지정 특성을 선언하려면 특성 이름 `Ascend-IP-Pool-Definition`, 특성 ID `218`, 특성 유형 `integer`로 사용자 지정 특성을 생성합니다. 그런 다음 `Ascend-Assign-IP-Pool=2`를 **Security Analyst (Read Only)** 필드에 입력하여 `Ascend-IP-Pool-Definition` 특성의 값이 `2`인 모든 사용자에게 읽기 전용 보안 분석가 권한을 부여할 수 있습니다.

RADIUS 인증 객체를 생성할 때 그 객체에 대한 새로운 사전 파일이 FireSIGHT 시스템 어플라이언스의 `/var/sf/userauth` 디렉토리에 생성됩니다. 인증 객체에 추가하는 모든 사용자 지정 특성은 사전 파일에 추가됩니다.

사용자 지정 특성을 정의하려면

액세스: Admin

1단계 화살표를 클릭하여 Define Custom RADIUS Attributes 섹션을 확장합니다.

특성 필드가 나타납니다.

2단계 공백 없이 영숫자와 대시로 이루어진 특성 이름을 **Attribute Name** 필드에 입력합니다.

3단계 **Attribute ID** 필드에 정수 형식의 특성 ID를 입력합니다.

4단계 **Attribute Type** 드롭다운 목록에서 특성 유형을 선택합니다.

5단계 **Add**를 클릭하여 인증 객체에 사용자 지정 특성을 추가합니다.

팁 사용자 지정 특성 옆의 **Delete**를 클릭하여 인증 객체에서 제거할 수 있습니다.

6단계 61-37페이지의 사용자 인증 테스트에서 계속하십시오.

사용자 인증 테스트

라이센스: 모두

RADIUS 연결, 사용자 역할, 사용자 지정 특성 설정을 구성한 다음 이 설정을 테스트하기 위해 어떤 인증 가능 사용자에 대한 사용자 자격 증명을 지정할 수 있습니다.

사용자 이름에는 테스트할 사용자의 이름을 입력할 수 있습니다.

1,000명이 넘는 사용자로 서버와의 연결을 테스트할 경우 UI 페이지 크기 제한 때문에 1,000명의 사용자만 반환됩니다.

팁 테스트 사용자의 이름이나 비밀번호를 잘못 입력할 경우 서버 컨피그레이션이 올바르더라도 테스트는 실패합니다. 서버 컨피그레이션이 올바른지 확인하려면 먼저 **Additional Test Parameters** 필드에 사용자 정보를 입력하지 않은 채로 **Test**를 클릭합니다. 그 테스트가 성공하면 사용자 이름과 비밀번호를 입력하여 특정 사용자로 테스트하십시오.

사용자 인증을 테스트하려면

액세스: Admin

1단계 **User Name** 및 **Password** 필드에는 RADIUS 서버에 대한 액세스를 검증하는 데 자격 증명을 사용할 사용자의 사용자 이름과 비밀번호를 입력합니다.

예를 들어 Example 회사의 `jsmith` 사용자 자격 증명을 가져올 수 있는지 테스트하려면 `jsmith`라고 입력합니다.

2단계 **Show Details**를 클릭하고 **Test**를 클릭합니다.

테스트의 성공을 알리는 메시지 또는 누락되었거나 수정해야 할 설정을 자세히 알려주는 메시지가 나타납니다.

3단계 테스트가 성공할 경우 **Save**를 클릭합니다.

External Authentication 페이지가 나타나며, 새 객체가 표시되어 있습니다.

어플라이언스의 객체를 사용하여 RADIUS 인증을 활성화하려면 그 객체가 활성화된 시스템 정책을 어플라이언스에 적용해야 합니다. 자세한 내용은 63-12페이지의 외부 인증 활성화및 63-4페이지의 시스템 정책 적용을/를 참조하십시오.

RADIUS 인증 객체의 예

라이센스: 모두

여기서는 RADIUS 서버 인증 객체의 예를 통해 FireSIGHT 시스템 RADIUS 인증 기능을 어떻게 사용할 수 있는지 알아봅니다. 자세한 내용은 다음 절을 참조하십시오.

- 61-38페이지의 예: RADIUS를 사용하여 사용자 인증
- 61-40페이지의 예: 사용자 지정 특성으로 사용자 인증

예: RADIUS를 사용하여 사용자 인증

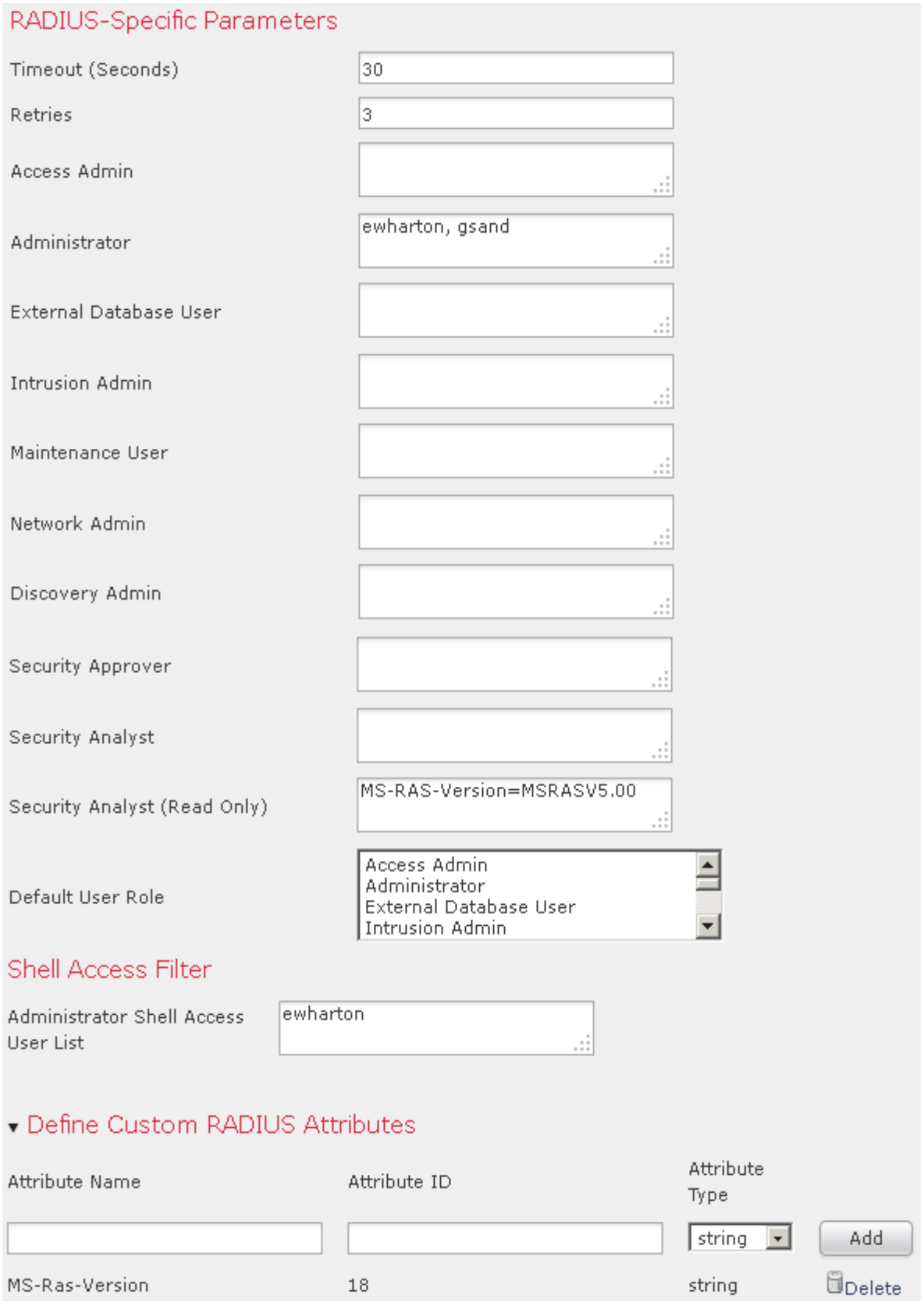
라이센스: 모두

다음 그림은 IP 주소 10.10.10.98을 사용하여 FreeRADIUS를 실행하는 서버를 위한 RADIUS 로그인 인증 객체의 예를 보여줍니다. 이 연결에서는 포트 1812를 사용하여 액세스하고 서버와의 연결은 30초간 사용이 없으면 시간 초과되며 3회 재시도한 다음 백업 인증 서버에 연결을 시도합니다.

이 예에서는 RADIUS 사용자 역할 컨피그레이션의 주요 내용을 보여줍니다.

- 사용자 `ewharton`과 `gsand`는 이 인증 객체가 활성화된 FireSIGHT 시스템 어플라이언스에 대한 관리 액세스 권한을 갖습니다.
- 사용자 `cbronte`는 이 인증 객체가 활성화된 FireSIGHT 시스템 어플라이언스에 대한 유지 보수 사용자 액세스 권한을 갖습니다.
- 사용자 `jausten`은 이 인증 객체가 활성화된 FireSIGHT 시스템 어플라이언스에 대한 보안 분석가 액세스 권한을 갖습니다.
- 사용자 `ewharton`은 셸 계정을 사용하여 어플라이언스에 로그인할 수 있습니다.

다음 그림은 이 예의 역할 컨피그레이션을 나타낸 것입니다.


RADIUS-Specific Parameters
Timeout (Seconds)
30
Retries
3
Access Admin
Administrator
ewharton, gsand
External Database User
Intrusion Admin
Maintenance User
Network Admin
Discovery Admin
Security Approver
Security Analyst
Security Analyst (Read Only)
MS-RAS-Version=MSRASV5.00
Default User Role
Access Admin
Administrator
External Database User
Intrusion Admin
Shell Access Filter
Administrator Shell Access User List
ewharton
Define Custom RADIUS Attributes
Attribute Name
Attribute ID
Attribute Type
string
Add
MS-Ras-Version
18
string
Delete
371901

예: 사용자 지정 특성으로 사용자 인증

라이센스: 모두

특정 사용자 역할을 가져야 하는 사용자를 식별하는 데 특성-값 쌍을 사용할 수 있습니다. 사용하는 특성이 사용자 지정 특성일 경우 그 사용자 지정 특성을 정의해야 합니다.

다음 그림은 이전의 예와 동일한 FreeRADIUS 서버를 위한 샘플 RADIUS 로그인 인증 객체에 포함된 역할 컨피그레이션 및 사용자 지정 특성 정의를 보여줍니다.

그러나 여기서는 Microsoft 원격 액세스 서버가 사용 중이므로 `MS-RAS-Version` 사용자 지정 특성이 하나 이상의 사용자에 대해 반환됩니다. `MS-RAS-Version` 사용자 지정 특성이 문자열입니다. 여기서는 Microsoft v. 5.00 원격 액세스 서버를 통해 RADIUS에 로그인한 모든 사용자가 보안 분석가(읽기 전용) 역할을 가져야 하므로 `MS-RAS-Version=MSRASV5.00`이라는 특성-값 쌍을 **Security Analyst (Read Only)** 필드에 입력합니다.

RADIUS-Specific Parameters

Timeout (Seconds)	30
Retries	3
Access Admin	
Administrator	ewharton, gsand
External Database User	
Intrusion Admin	
Maintenance User	
Network Admin	
Discovery Admin	
Security Approver	
Security Analyst	
Security Analyst (Read Only)	MS-RAS-Version=MSRASV5.00
Default User Role	Access Admin Administrator External Database User Intrusion Admin

Shell Access Filter

Administrator Shell Access User List	ewharton

▾ Define Custom RADIUS Attributes

Attribute Name	Attribute ID	Attribute Type	
		string	Add
MS-Ras-Version	18	string	Delete

371901

RADIUS 인증 객체 수정

라이센스: 모두

기존 인증 객체를 수정할 수 있습니다. 객체가 시스템 정책에서 사용되고 있다면 정책이 적용되는 시점의 설정이 그 정책을 다시 적용할 때까지 유지됩니다.

인증 객체를 수정하려면

액세스: Admin

1단계 **System > Local > User Management**를 선택합니다.

User Management 페이지가 나타납니다.

2단계 **External Authentication** 탭을 클릭합니다.

External Authentication 페이지가 나타납니다.

3단계 수정할 객체 옆의 수정 아이콘( )을 클릭합니다.

Create External Authentication Object 페이지가 나타납니다.

4단계 필요에 맞게 객체 설정을 수정합니다.

5단계 **Save**를 클릭합니다.

변경사항이 저장되었고 External Authentication 페이지가 다시 나타납니다. 객체가 활성화된 시스템 정책을 어플라이언스에 적용해야 해당 어플라이언스에서 인증 변경사항이 적용됩니다. 자세한 내용은 63-12페이지의 외부 인증 활성화및 63-4페이지의 시스템 정책 적용을/를 참조하십시오.

인증 객체 삭제

라이센스: 모두

시스템 정책에서 현재 활성화되지 않은 인증 객체는 삭제할 수 있습니다.

인증 객체를 삭제하려면

액세스: Admin

1단계 **System > Local > User Management**를 선택합니다.

User Management 페이지가 나타납니다.

2단계 **External Authentication** 탭을 클릭합니다.

External Authentication 페이지가 나타납니다.

3단계 삭제할 객체 옆의 삭제 아이콘( )을 클릭합니다.

객체가 삭제되고 External Authentication 페이지가 나타납니다.

사용자 계정 관리

라이센스: 모두

관리자 액세스 권한이 있을 경우 웹 인터페이스를 사용하여 방어 센터 또는 관리되는 디바이스의 사용자 계정을 보고 관리할 수 있습니다. 여기에는 계정을 추가, 수정, 삭제하는 것도 포함됩니다. 또한 사용자 지정 사용자 역할을 생성하고 수정하며 사용자 역할 에스컬레이션을 구성할 수도 있습니다. 관리자 액세스 권한이 없는 사용자 계정은 관리 기능에 대한 액세스가 제한됩니다. 사용자 유형에 따라 탐색 메뉴의 모양이 달라집니다.

사용자 계정 관리에 대한 자세한 내용은 다음 절을 참조하십시오.

- 61-43페이지의 사용자 계정 보기에서는 User Management 페이지에 액세스하는 방법에 대해 설명합니다. 여기서 사용자 계정을 추가, 활성화, 비활성화, 수정, 삭제할 수 있습니다.
- 61-44페이지의 새 사용자 계정 추가에서는 새 사용자 계정을 추가할 때 사용할 수 있는 여러 옵션에 대해 설명합니다.
- 61-45페이지의 명령줄 액세스 관리에서는 Series 3 또는 가상 디바이스의 로컬 디바이스 사용자에게 명령줄 인터페이스 액세스 권한을 지정하는 방법에 대해 설명합니다.
- 61-46페이지의 외부 인증 사용자 계정 관리에서는 외부 인증 사용자를 추가하는 방법과 FireSIGHT 시스템에서 관리할 수 있는 사용자 컨피그레이션의 요소에 대해 설명합니다.
- 61-54페이지의 사용자 권한 및 옵션 수정에서는 기존 사용자 계정에 액세스하고 이를 수정하는 방법에 대해 설명합니다.
- 61-55페이지의 제한적 사용자 액세스 속성 이해에서는 제한적 데이터 액세스 권한으로 어떤 사용자 계정에서 사용 가능한 데이터를 제한하는 방법에 대해 설명합니다.
- 61-56페이지의 사용자 계정 삭제에서는 사용자 계정을 삭제하는 방법에 대해 설명합니다.
- 61-56페이지의 사용자 계정 권한에는 각 사용자 계정 유형에서 액세스할 수 있는 메뉴와 옵션을 정리한 표가 있습니다.

사용자 계정 보기

라이센스: 모두

User Management 페이지에서 기존 계정을 보고 수정하고 삭제할 수 있습니다. **Authentication Method** 열에서 어떤 사용자의 인증 유형을 볼 수 있습니다. **Password Lifetime** 열은 각 사용자 비밀번호의 남은 일수를 나타냅니다. **Action** 열의 아이콘을 사용하여 더 세부적으로 사용자를 수정하고 활성 또는 비활성 상태로 설정할 수 있습니다. 외부 인증 사용자의 경우 서버에 대한 인증 객체가 비활성화된 경우 **Authentication Method** 열에 **External (Disabled)**라고 표시됩니다.

User Management 페이지에 액세스하려면

액세스: Admin

1단계 **System > Local > User Management**를 선택합니다.

User Management 페이지가 나타나고 각 사용자가 사용자 계정 활성화, 비활성화, 수정, 삭제 옵션과 함께 표시됩니다.

User Management 페이지에서 수행할 수 있는 작업에 대해서는 다음 절을 참조하십시오.

- 61-44페이지의 새 사용자 계정 추가
- 61-48페이지의 사용자 역할 구성
- 61-54페이지의 사용자 권한 및 옵션 수정

- 61-55페이지의 제한적 사용자 액세스 속성 이해
- 61-55페이지의 사용자 비밀번호 수정
- 61-56페이지의 사용자 계정 삭제

새 사용자 계정 추가

라이센스: 모두

지원되는 디바이스: 기능에 따라

새 사용자 계정을 설정할 때 이 계정에서 시스템의 어느 부분에 액세스 가능한가를 제어할 수 있습니다. 생성 과정에서 사용자 계정의 비밀번호 만료 및 강도를 설정할 수 있습니다. Series 3 디바이스의 로컬 계정에 대해서는 그 사용자의 명령줄 액세스 레벨도 구성할 수 있습니다.

새 사용자를 추가하려면

액세스: Admin

1단계 **System > Local > User Management**를 선택합니다.

User Management 페이지가 나타납니다.

2단계 **Create User**를 클릭합니다.

Create User 페이지가 나타납니다.

3단계 **User Name** 필드에 새 사용자의 이름을 입력합니다.

새 사용자 이름은 공백 없이 영숫자 또는 하이픈 문자로 구성되며 32자를 초과할 수 없습니다. 사용자 이름은 대/소문자를 구별합니다.

4단계 이 사용자가 로그인할 때 외부 디렉토리 서버에 인증하게 하려면 **Use External Authentication Method**를 선택합니다.

이 옵션을 활성화할 경우 비밀번호 관리 옵션이 사라집니다. 사용자의 액세스 역할 구성을 계속하려면 8단계로 건너뜁니다.

사용자가 외부 디렉토리 서버에 인증하기 위해서는 방어 센터에서 사용할 서버에 대한 인증 객체를 생성하고 인증이 활성화된 상태에서 시스템 정책을 적용해야 합니다. 또한 외부 인증 서버가 사용 가능한 상태여야 이 사용자가 FireSIGHT 시스템 어플라이언스에 로그인할 수 있습니다. 자세한 내용은 61-5페이지의 인증 객체 관리및 63-12페이지의 외부 인증 활성화을/를 참조하십시오.

5단계 **Password** 및 **Confirm Password** 필드에는 (최대 32자의 영숫자로 이루어진) 비밀번호를 입력합니다.

비밀번호 강도 확인을 활성화할 경우 비밀번호는 대/소문자가 혼합된 8자 이상의 영숫자이고 숫자와 특수 문자를 각각 하나 이상 포함해야 합니다. 사전에 나와 있는 단어일 수 없으며, 연속적으로 반복되는 문자를 포함할 수 없습니다.

참고 어플라이언스에서 STIG 규정준수를 활성화할 경우 셸 액세스 사용자를 위한 비밀번호 설정에 대해*FireSIGHT 시스템 STIG 릴리스 정보*를 참조하십시오.

6단계 나머지 사용자 계정 로그인 옵션을 구성합니다.

자세한 내용은 사용자 계정 로그인 옵션 표를 참조하십시오.

7단계 Series 3 디바이스의 웹 인터페이스를 통해 로컬 사용자를 생성하는 경우 사용자에 대해 **Command-Line Interface Access** 레벨을 지정할 수 있습니다.

- 사용자에 대해 명령줄 액세스를 비활성화하려면 **None**을 선택합니다.
- 사용자가 셸에 로그인하고 일부 명령에 액세스하는 것을 허용하려면 **Basic**을 선택합니다.
- 사용자가 셸에 로그인하고 전문가 모드(어플라이언스에서 허용되는 경우)를 포함한 어떤 명령줄 옵션도 사용할 수 있게 하려면 **Configuration**을 선택합니다.

  명령줄 액세스에 대한 자세한 내용은 61-45페이지의 명령줄 액세스 관리을/를 참조하십시오.

8단계 사용자에게 부여할 액세스 역할을 선택합니다.

참고 관리되는 모든 물리적 디바이스의 경우 Cisco에서 제공하는 사전 정의된 사용자 역할이 관리자, 유지 보수 사용자, 보안 분석가로 제한됩니다.

자세한 내용은 61-48페이지의 사용자 역할 구성을/를 참조하십시오.

9단계 **Save**를 클릭합니다.

사용자가 생성되고 User Management 페이지가 다시 나타납니다.

팁 User Management 페이지에서 내부 인증 사용자의 이름 옆에 있는 슬라이더를 클릭하여 비활성화된 사용자를 다시 활성화하거나 활성 사용자 계정을 삭제하지 않고 비활성화할 수 있습니다.

명령줄 액세스 관리

라이센스: 모두

지원되는 디바이스: Series 3, 가상

Series 3 또는 가상 디바이스에서 로컬 디바이스 사용자에 명령줄 인터페이스 액세스 권한을 지정할 수 있습니다.

가상 디바이스의 사용자에도 명령줄 액세스 권한을 지정할 수 있으나, 명령줄 인터페이스에서 명령을 사용합니다. 자세한 내용은 D-1페이지의 명령줄 참조을/를 참조하십시오.

사용자가 실행할 수 있는 명령은 그 사용자에게 지정한 액세스 레벨에 따라 달라집니다. **Command-Line Interface Access**를 **None**으로 설정하면 그 사용자는 명령줄에서 어플라이언스에 로그인할 수 없습니다. 사용자가 시작하는 모든 세션은 사용자가 자격 증명을 제공할 때 종료됩니다. 사용자 생성 시 기본적으로 액세스 레벨은 **None**입니다. **Command-Line Interface Access**를 **Basic**으로 설정하면 사용자가 특정 명령 집합을 실행할 수 있습니다.

표 61-3 기본 명령줄 명령

configure password	interfaces
end	lcd
exit	link-state
help	log-ips-connection
history	managers
logout	memory
?	model
??	mpls-depth

표 61-3 기본 명령줄 명령 (계속)

access-control-config	NAT
alarms	network
arp-tables	network-modules
audit-log	ntp
bypass	perfstats
clustering	portstats
cpu	power-supply-status
database	process-tree
device-settings	processes
disk	routing-table
disk-manager	serial-number
dns	stacking
expert	summary
fan-status	time
fastpath-rules	traffic-statistics
gui	version
hostname	virtual-routers
hyperthreading	virtual-switches
inline-sets	

Command-Line Interface Access를 **Configuration**으로 설정하면 사용자는 어떤 명령줄 옵션도 액세스할 수 있습니다. 사용자에게 이 액세스 레벨을 지정할 때는 각별히 주의하십시오.

주의 외부 인증 사용자에게 부여되는 셸 액세스 권한은 기본적으로 명령줄 액세스 레벨이 **Configuration**이며, 이는 모든 명령줄 유틸리티에 대한 권한을 부여합니다. 외부 인증 사용자의 셸 액세스에 대한 자세한 내용은 61-9페이지의 셸 액세스 이해 및 61-24페이지의 셸 액세스 구성을/를 참조하십시오.

외부 인증 사용자 계정 관리

라이센스: 모두

외부 인증 사용자가 외부 인증이 활성화된 어플라이언스에 로그인할 때 어플라이언스는 인증 객체에서 그룹 멤버십을 지정하는 방법으로 설정했던 기본 액세스 역할을 사용자에게 부여합니다. 액세스 그룹 설정을 구성하지 않은 경우 시스템 정책에 설정했던 기본 사용자 역할을 부여합니다. 그러나 사용자가 어플라이언스에 로그인하기 전에 로컬에서 사용자를 추가할 경우 User Management 페이지에서 구성하는 사용자 권한이 기본 설정을 재정의합니다.

기본 사용자 역할을 선택하는 것에 대한 자세한 내용은 63-12페이지의 외부 인증 활성화 및 61-4페이지의 사용자 권한 이해을/를 참조하십시오. 사전 정의된 사용자 역할과 사용자 지정 사용자 역할 모두 외부 인증 사용자의 기본 사용자 역할로 설정할 수 있습니다. 자세한 내용은 61-48페이지의 사용자 역할 구성을/를 참조하십시오.

내부 인증 사용자는 다음 조건을 모두 충족할 때 외부 인증으로 전환됩니다.

- LDAP(CAC 사용 또는 CAC 없음) 또는 RADIUS 인증을 활성화합니다.
- LDAP 또는 RADIUS 서버의 해당 사용자에 대해 동일한 사용자 이름이 있습니다.

- 사용자가 LDAP 또는 RADIUS 서버에 저장된 자신의 비밀번호를 사용하여 로그인합니다.

방어 센터의 시스템 정책에서는 외부 인증만 활성화할 수 있습니다. 관리되는 디바이스에서 외부 인증을 사용하려면 방어 센터에서 관리되는 디바이스에 정책을 적용해야 합니다.

외부 인증 사용자가 처음으로 어플라이언스에 로그인한 다음에는 어플라이언스가 로컬 사용자 레코드를 생성하여 그 자격 증명을 어떤 명령 집합과 연결합니다. 사용자 로그인에 대한 자세한 내용은 2-1페이지의 어플라이언스에 로그인을/를 참조하십시오. 최초 로그인 이후에는 다음과 같이 로컬 사용자 레코드에 대한 권한을 수정할 수 있습니다. 단, 그룹 또는 목록 멤버십을 통해 부여된 경우는 제외합니다.

- 외부 인증 사용자 계정의 기본 역할이 특정 액세스 역할로 설정된 경우 사용자는 시스템 관리자의 추가 컨피그레이션 없이 외부 계정 자격 증명으로 어플라이언스에 로그인할 수 있습니다.
- 계정이 외부에서 인증되었고 기본적으로 어떤 액세스 권한도 갖지 않을 경우 사용자는 로그인할 수 있으나 어떤 기능에도 액세스할 수 없습니다. 이 경우 사용자 기능에 대한 적절한 액세스 권한을 부여하도록 사용자 권한을 변경할 수 있습니다(시스템 관리자도 가능).

팁 셸 액세스 사용자에 대해서는 로컬 사용자 계정이 생성되지 않습니다. 셸 액세스는 오로지 LDAP 서버에 대해 설정된 셸 액세스 필터나 PAM 로그인 특성을 통해 또는 RADIUS 서버의 셸 액세스 목록을 통해 제어됩니다.

사용자 액세스 수정에 대한 자세한 내용은 61-54페이지의 사용자 권한 및 옵션 수정을/를 참조하십시오. FireSIGHT 시스템 인터페이스에서는 외부 인증 사용자의 비밀번호를 관리하거나 외부 인증 사용자를 비활성화할 수 없습니다. 외부 인증 사용자의 경우, LDAP 그룹이나 RADIUS 목록 멤버십 또는 특성 값에 의해 액세스 역할이 부여된 사용자라면 그 최소 액세스 권한을 FireSIGHT 시스템 사용자 관리 페이지에서 제거할 수 없습니다. 외부 인증 사용자의 Edit User 페이지에서는 외부 인증 서버의 설정에 따라 부여된 권한이 **Externally Modified** 상태로 표시됩니다.

그러나 추가 권한을 지정할 수는 있습니다. 외부 인증 사용자에 대한 액세스 권한을 수정할 때 User Management 페이지의 Authentication Method 열은 상태가 **External - Locally Modified**입니다.

셸 사용자는 소문자로 된 사용자 이름으로 로그인할 수 있습니다. 셸에 대한 로그인 인증에서는 대/소문자를 구분합니다.

주의 Series 3 방어 센터에서는 모든 셸 사용자가 `sudoers` 권한을 갖습니다. 셸 액세스 권한을 갖는 사용자의 목록을 적절하게 제한해야 합니다. Series 3 및 가상 디바이스에서는 외부 인증 사용자에게 부여되는 셸 액세스 권한이 기본적으로 명령줄 액세스의 **Configuration** 레벨이며, 여기서도 `sudoers` 권한을 부여합니다. 셸 액세스 설정에 대한 자세한 내용은 61-9페이지의 셸 액세스 이해 및 61-24페이지의 셸 액세스 구성을/를 참조하십시오.

사용자 로그인 설정 관리

라이센스: 모두

각 사용자 계정의 비밀번호가 변경되는 방식과 시점, 사용자 계정이 비활성화되는 시점을 제어할 수 있습니다. 웹 인터페이스 로그인 세션에 대한 시간 초과를 구성한 경우 사용자가 이 시간 초과에서 면제될 수 있습니다. 다음 표에서는 비밀번호 및 계정 액세스를 제어하는 데 사용할 수 있는 몇 가지 옵션에 대해 설명합니다.

Series 3가 관리하는 디바이스의 로컬 인증 사용자의 경우 웹 인터페이스의 비밀번호를 변경하면 명령줄 인터페이스의 비밀번호도 바뀝니다.

Check Password Strength 옵션을 활성화할 경우 최소 비밀번호 길이가 자동으로 8자로 설정됩니다. 또한 **Minimum Password Length**에서 8자를 초과하는 값을 설정하면 더 높은 값이 적용됩니다.

참고 **Use External Authentication Method**를 활성화하면 더 이상 로그인 옵션이 나타나지 않습니다. 외부 인증 서버를 사용하여 로그인 설정을 관리합니다.

표 61-4 사용자 계정 로그인 옵션

옵션	설명
Use External Authentication Method	이 사용자의 자격 증명을 외부에서 인증하게 하려면 이 확인란을 선택합니다. **참고** 사용자에 대해 이 옵션을 선택했는데 외부 인증 서버가 사용 불가한 상태라면 그 사용자는 웹 인터페이스에 로그인할 수 있으나 어떤 기능도 액세스하지 못합니다.
Maximum Number of Failed Logins	공백 없이 정수를 입력하여 각 사용자가 로그인에 실패한 후 계정이 잠길 때까지 로그인을 시도할 수 있는 최대 횟수를 지정합니다. 기본 설정은 5회입니다. 0을 입력하면 로그인 실패 횟수의 제한이 사라집니다.
Minimum Password Length	공백 없이 정수를 입력하여 사용자 비밀번호의 최소 길이를 글자 수로 지정합니다. 기본 설정은 8입니다. 값이 0이면 최소 길이 제한이 없습니다.
Days Until Password Expiration	여기에 입력한 일 수가 지나면 사용자의 비밀번호가 만료됩니다. 기본 설정은 0이며, 그러면 비밀번호가 절대 만료되지 않습니다.
Days Before Password Expiration Warning	비밀번호가 만료되기 전에 사용자에게 비밀번호를 변경하게 하는 경고 일수입니다. 기본 설정은 0일입니다. **주의** 경고 일수는 비밀번호 만료 시점까지 남은 일수보다 **적어야** 합니다.
Force Password Reset on Login	사용자가 처음 로그인할 때 반드시 비밀번호를 변경하게 하려면 이 옵션을 선택합니다.
Check Password Strength	강력한 비밀번호를 요구하려면 이 옵션을 선택합니다. 강력한 비밀번호는 대/소문자가 혼합된 8자 이상의 영숫자이고 숫자와 특수 문자를 각각 하나 이상 포함해야 합니다. 사전에 나와 있는 단어일 수 없으며, 연속적으로 반복되는 문자를 포함할 수 없습니다.
Exempt from Browser Session Timeout	어떤 사용자의 로그인 세션이 무활동으로 종료되지 않게 하려면 이 옵션을 선택합니다. 관리자 역할의 사용자는 면제받을 수 없습니다. 세션 시간 초과에 대한 자세한 내용은 63-29페이지의 사용자 인터페이스 설정 구성을/를 참조하십시오.

사용자 역할 구성

라이센스: 모두

각 FireSIGHT 시스템 사용자는 사용자 액세스 역할이 있습니다. 예를 들어 분석가는 네트워크의 보안을 분석하기 위해 이벤트 데이터에 액세스해야 하지만, FireSIGHT 시스템 자체의 관리 기능에 대한 액세스 권한은 필요하지 않을 것입니다. 사용자 역할을 통해 이를테면 분석가에게 보안 분석가 액세스 권한을, FireSIGHT 시스템를 관리하는 사용자에게는 사용자 역할을 부여할 수 있습니다. FireSIGHT 시스템에는 다양한 관리자 및 분석가에 맞게 설계된 10가지 사전 정의 사용자 역할이 있습니다. 또한 특수 액세스 권한을 가진 맞춤 사용자 역할을 만들 수도 있습니다.

사용자가 액세스할 수 있는 웹 인터페이스의 메뉴 및 기타 옵션은 그 역할에 따라 달라집니다. 사전 정의된 사용자 역할은 미리 결정된 액세스 권한의 모음을 갖지만, 사용자 지정 사용자 역할은 그 생성자가 결정하는 세분화된 액세스 권한을 갖습니다.

User Roles 페이지에서 사용자 역할을 구성합니다.

User Roles 페이지에 액세스하려면

액세스: Admin

1단계 **System > Local > User Management**를 선택합니다.

User Management 페이지가 나타납니다.

2단계 **User Roles** 탭을 클릭합니다.

User Roles 페이지가 나타나고 모든 사전 정의 및 사용자 지정 사용자 역할을 역할 활성화, 비활성화, 수정, 복사, 삭제, 내보내기 옵션과 함께 표시합니다.

두 가지 유형의 사용자 역할을 구성하는 것에 대한 자세한 내용은 다음 절을 참조하십시오.

- 61-49페이지의 사전 정의 사용자 역할 관리
- 61-51페이지의 사용자 지정 사용자 역할 관리
- 61-53페이지의 사전 정의 사용자 역할의 사용자 지정 복사본 생성
- 61-54페이지의 사용자 지정 사용자 역할 삭제

사전 정의 사용자 역할 관리

라이센스: 모두

FireSIGHT 시스템에서는 10가지 사전 정의 사용자 역할을 통해 광범위한 액세스 권한을 제공하면서 조직의 요구 사항을 해결합니다. User Roles 페이지에서 사전 정의 사용자 역할은 "Cisco Provided"로 표시됩니다. 관리되는 디바이스는 10가지 사전 정의 사용자 역할 중 관리자, 유지 보수 사용자, 보안 분석가의 3가지만 액세스할 수 있습니다.

사전 정의 사용자 역할은 수정할 수 없으나 그 액세스 권한 집합을 기반으로 사용자 지정 사용자 역할을 만들 수 있습니다. 사용자 지정 사용자 역할의 생성 및 수정에 대한 자세한 내용은 61-51페이지의 사용자 지정 사용자 역할 관리을/를 참조하십시오. 또한 사전 정의 사용자 역할은 수정 불가하므로 다른 사용자 역할에 에스컬레이션하도록 구성할 수 없습니다. 자세한 내용은 61-64페이지의 사용자 역할 에스컬레이션 관리을/를 참조하십시오.

다음 표에서는 제공되는 사전 정의 역할에 대해 간략하게 설명합니다. 각 역할에서 사용 가능한 메뉴 및 옵션의 목록은 61-56페이지의 사용자 계정 권한을/를 참조하십시오.

표 61-5 사전 정의 사용자 역할

사용자 역할:	권한
액세스 관리자 (Access Admin)	액세스 제어, SSL 검사, 파일 정책 기능에 대한 액세스를 제공합니다. 그러나 액세스 관리자는 액세스 제어 정책을 적용할 수 없습니다. 액세스 관리자는 **Policies** 메뉴에서 액세스 제어, SSL 검사, 파일 관련 옵션에 대한 액세스를 제공합니다.
관리자(Administrator)	분석 및 보고 기능, 규칙 및 정책 컨피그레이션, 시스템 관리, 모든 유지 보수 기능에 대한 액세스를 제공합니다. 관리자는 모든 메뉴 옵션에 액세스할 수 있습니다. 그 세션은 보안 침해 시 더 심각한 위험을 초래하므로 로그인 세션 시간 초과에서 면제할 수 없습니다. 관리자 역할의 사용은 보안에 필요한 경우로 제한해야 합니다. 이 역할은 관리되는 디바이스에서도 사용 가능합니다.
검색 관리자 (Discovery Admin)	네트워크 검색, 상관관계, 사용자 활동 기능에 대한 액세스를 제공합니다. 검색 관리자는 **Policies** 메뉴에서 해당 옵션에 액세스할 수 있습니다.
외부 데이터베이스 사용자(External Database User)	JDBC SSL 연결을 지원하는 애플리케이션을 사용하여 FireSIGHT 시스템 데이터베이스에 대한 읽기 전용 액세스를 제공합니다. 서드파티 애플리케이션이 FireSIGHT 시스템 어플라이언스에 대한 인증을 수행하기 위해서는 64-7페이지의 데이터베이스에 대한 액세스 활성화의 설명대로 시스템 설정에서 데이터베이스 액세스를 활성화해야 합니다. 외부 데이터베이스 사용자는 웹 인터페이스에서 **Help** 메뉴의 온라인 도움말 관련 옵션에만 액세스할 수 있습니다. 이 역할의 기능이 웹 인터페이스와 무관하므로 용이한 지원 및 비밀번호 변경에 대한 액세스만 제공됩니다.
침입 관리자 (Intrusion Admin)	모든 침입 정책, 침입 규칙, 네트워크 분석 정책 기능에 대한 액세스를 제공합니다. 침입 관리자는 **Policies** 메뉴의 침입 관련 옵션에 액세스할 수 있습니다. 침입 관리자는 액세스 제어 정책의 일부인 침입 또는 네트워크 분석 정책을 적용할 수 없습니다.
유지 보수 사용자 (Maintenance User)	모니터링 및 유지 보수 기능에 대한 액세스를 제공합니다. 유지 보수 사용자는 **Health** 및 **System** 메뉴에서 유지 보수 관련 옵션에 액세스할 수 있습니다. 이 역할은 관리되는 디바이스에서도 사용 가능합니다.
네트워크 관리자 (Network Admin)	액세스 제어, SSL 검사, 디바이스 컨피그레이션 기능에 대한 액세스를 제공합니다. 네트워크 관리자는 **Policies** 및 **Devices** 메뉴에서 액세스 제어, SSL 검사, 디바이스 관련 옵션에 액세스할 수 있습니다.
보안 분석가 (Security Analyst)	보안 이벤트 분석 기능, 이를테면 이벤트 보기, 보고서, 호스트, 호스트 특성, 서비스, 취약성, 클라이언트 애플리케이션에 대한 액세스와 상태 이벤트에 대한 읽기 전용 액세스를 제공합니다. 보안 분석가는 **Overview**, **Analysis**, **Health**, **System** 메뉴의 분석 관련 옵션에 액세스할 수 있습니다. 이 역할은 관리되는 디바이스에서도 사용 가능합니다.
보안 분석가(읽기 전용)	보안 이벤트 분석 기능, 이를테면 이벤트 보기, 보고서, 호스트, 호스트 특성, 서비스, 취약성, 클라이언트 애플리케이션과 상태 이벤트에 대한 읽기 전용 액세스를 제공합니다. 보안 분석가는 **Overview**, **Analysis**, **Health**, **System** 메뉴의 분석 관련 옵션에 액세스할 수 있습니다.
보안 승인자 (Security Approver)	액세스 제어, 침입, 파일, SSL, 네트워크 검색 정책에 대한 제한적 액세스를 제공합니다. 보안 승인자는 이러한 정책을 보고 네트워크 검색, 침입, 액세스 제어 정책을 적용할 수 있으나 정책 변경은 불가합니다. **Policies** 메뉴에서 해당 정책 관련 옵션에 액세스할 수 있습니다.

사용자에게 이벤트 분석가 역할을 지정할 뿐 아니라 그 사용자의 삭제 권한을 제한하여 사용자 본인이 생성한 보고서 프로필, 검색, 북마크, 사용자 지정 테이블, 사용자 지정 워크플로의 삭제만 허용할 수 있습니다. 자세한 내용은 61-44페이지의 새 사용자 계정 추가을/를 참조하십시오.

외부 인증 사용자는 다른 어떤 역할도 갖지 않을 경우 LDAP 또는 RADIUS 인증 객체와 시스템 정책의 설정에 따른 최소 액세스 권한을 갖습니다. 이 사용자에 추가 권한을 줄 수 있으나, 최소 액세스 권한을 제거하거나 변경하려면 다음 작업을 수행해야 합니다.

- 인증 객체에서 그 사용자를 다른 목록으로 이동하거나 외부 인증 서버에서 사용자의 특성 값 또는 그룹 멤버십을 변경합니다.
- 시스템 정책을 다시 적용합니다.
- User Management 페이지에서 그 사용자 계정으로부터 액세스 권한을 제거합니다.

사전 정의 사용자 역할은 삭제할 수 없지만 이를 비활성화할 수는 있습니다. 어떤 역할을 비활성화하면 그 역할이 지정된 모든 사용자에게서 역할 및 관련 권한이 제거됩니다.

주의 비활성화된 역할이 어떤 사용자에게 지정된 유일한 역할일 경우, 그 사용자는 로그인하고 User Preferences 메뉴에 액세스할 수 있지만 그 밖의 방식으로는 FireSIGHT 시스템에 액세스할 수 없습니다.

사용자 역할을 활성화하거나 비활성화하려면

액세스: Admin

1단계 **System > Local > User Management**를 선택합니다.

User Management 페이지가 나타납니다.

2단계 **User Roles** 탭을 클릭합니다.

User Roles 페이지가 나타납니다.

3단계 활성화하거나 비활성화할 사용자 역할의 옆에 있는 슬라이더를 클릭합니다.

참고 어떤 역할의 사용자가 로그인한 상태에서 Lights-Out Management으로 그 역할을 비활성화했다가 다시 활성화할 경우 또는 사용자의 로그인 세션 중에 백업에서 사용자 또는 사용자 역할을 복원할 경우, 사용자가 다시 웹 인터페이스에 로그인해야 IPMItool 명령에 다시 액세스할 수 있습니다. 자세한 내용은 64-25페이지의 Lights-Out Management 사용을/를 참조하십시오.

사용자 지정 사용자 역할 관리

라이센스: 모두

사전 정의 사용자 역할 외에도 특별한 액세스 권한을 가진 사용자 지정 사용자 역할을 생성할 수 있습니다. 사용자 지정 사용자 역할은 어떠한 메뉴 기반 및 시스템 권한도 가질 수 있으며 원래 역할을 그대로 유지하거나 사전 정의된 사용자 역할을 기반으로 하여 변경할 수 있습니다. 사전 정의 사용자 역할과 마찬가지로 외부 인증 사용자에 대한 기본 역할이 될 수 있습니다. 사전 정의 역할과 달리 사용자 지정 역할은 수정하고 삭제할 수 있습니다.

선택 가능한 권한은 계층적이며 FireSIGHT 시스템 메뉴 레이아웃을 기반으로 합니다. 권한에 하위 페이지가 있을 경우 또는 단순 페이지 액세스의 영역 외에서 사용 가능한 더 세분화된 권한을 가질 경우 권한은 확장 가능합니다. 그러한 경우 상위 권한은 페이지 보기 액세스를 제공하며, 하위 권한은 그 페이지의 관련 기능에 대한 세분화된 액세스를 제공합니다. 예를 들어 상관관계 이벤트(Correlation Events) 권한은 Correlation Events 페이지에 대한 액세스를 제공하지만, Modify Correlation Events 확인란에서는 사용자가 그 페이지에서 제공하는 정보를 수정하고 삭제할 수 있게 합니다. "관리"라는 단어가 포함된 권한은 다른 사용자가 생성하는 정보를 수정하고 삭제할 수 있습니다.

팁 메뉴 구조에 포함되지 않은 페이지나 기능의 경우 상위 또는 관련 페이지에서 권한을 부여합니다. 예를 들어 침입 정책 수정(Modify Intrusion Policy) 권한은 네트워크 분석 정책을 수정하는 것도 허용합니다.

사용자 지정 사용자 역할에 제한적 검색을 적용할 수 있습니다. 이는 사용자가 이벤트 뷰어에서 볼 수 있는 데이터를 제한합니다. 먼저 비공개 저장 검색을 생성하고 해당 메뉴 기반 권한의 "Restricted Search" 드롭다운 메뉴에서 이를 선택하는 방법으로 제한적 검색을 구성할 수 있습니다. 자세한 내용은 60-2페이지의 검색 수행을/를 참조하십시오.

방어 센터에서 사용자 지정 사용자 역할을 구성할 때 모든 메뉴 기반 권한이 부여 가능합니다. 관리되는 디바이스에서 사용자 지정 역할을 구성할 때는 디바이스 기능과 관련된 일부 권한만 사용 가능합니다. 구성 가능한 메뉴 기반 권한 및 사전 정의 사용자 역할과의 관계에 대한 자세한 내용은 다음을 참조하십시오.

- 61-58페이지의 Analysis 메뉴
- 61-60페이지의 Policies 메뉴
- 61-62페이지의 Devices 메뉴
- 61-62페이지의 Object Manager
- 61-63페이지의 Health 메뉴
- 61-63페이지의 System 메뉴
- 61-64페이지의 Help 메뉴

System Permissions에서 선택 가능한 옵션을 통해 외부 데이터베이스 쿼리가 가능한 사용자 역할을 생성하거나 대상 사용자 역할의 권한으로 에스컬레이션할 수 있습니다. 자세한 내용은 64-7페이지의 데이터베이스에 대한 액세스 활성화및 61-64페이지의 사용자 역할 에스컬레이션 관리을/를 참조하십시오.

새 사용자 지정 사용자 역할을 생성하지 않고 다른 어플라이언스에서 사용자 지정 사용자 역할을 내보낸 다음 해당 어플라이언스에 가져올 수도 있습니다. 그리고 가져온 역할을 필요에 맞게 수정한 다음 적용할 수 있습니다. 자세한 내용은 A-2페이지의 컨피그레이션 내보내기및 A-5페이지의 컨피그레이션 가져오기을/를 참조하십시오.

사용자 지정 사용자 역할을 생성하려면

액세스: Admin

1단계 **System > Local > User Management**를 선택합니다.

User Management 페이지가 나타납니다.

2단계 **User Roles** 탭을 클릭합니다.

User Roles 페이지가 나타납니다.

3단계 **Create User Role**을 클릭합니다.

User Role Editor 페이지가 나타납니다.

4단계 **Name** 필드에 새 사용자 역할의 이름을 입력합니다.

공백 없이 영숫자 또는 하이픈 문자를 사용할 수 있습니다. 역할 이름은 75자를 초과할 수 없습니다. 사용자 역할 이름은 대/소문자를 구별합니다.

5단계 **Description** 필드에 새 역할에 대한 설명을 추가할 수도 있습니다.

역할 설명은 255자를 초과할 수 없습니다.

6단계 새 역할에 대한 권한을 선택합니다.

선택되지 않은 권한을 선택할 경우 그 하위 권한이 모두 선택되며, 다중 값 권한에서는 첫 번째 값이 선택됩니다. 상위 레벨 권한의 선택을 취소할 경우 모든 하위 권한의 선택도 취소됩니다. 자신은 선택되었지만 모든 하위 항목이 선택되지 않은 권한은 기울임꼴 텍스트로 나타납니다.

사전 정의 사용자 역할을 사용자 지정 역할의 기반으로 사용하기 위해 복사하면 그 사전 정의 역할과 관련된 권한이 미리 선택됩니다. 사전 정의 사용자 역할의 복사에 대한 자세한 내용은 61-53페이지의 사전 정의 사용자 역할의 사용자 지정 복사본 생성을/를 참조하십시오.

현재 에스컬레이션 대상 목표가 역할 에스컬레이션 확인란 옆에 나열됩니다. 이 확인란을 선택할 경우 지정된 사용자의 비밀번호로 또는 다른 지정된 사용자 역할의 비밀번호로 에스컬레이션을 인증하도록 선택할 수 있습니다. 자세한 내용은 61-64페이지의 사용자 역할 에스컬레이션 관리을/를 참조하십시오.

7단계 **Save**를 클릭합니다.

사용자 지정 사용자 역할이 생성되고 User Roles 페이지가 다시 나타납니다.

사전 정의 사용자 역할의 사용자 지정 복사본 생성

라이센스: 모두

새 사용자 지정 역할의 기반으로 사용하기 위해 기존 역할을 복사할 수 있습니다. 그러면 User Role Editor에서 기존 역할의 권한이 미리 선택되어 있으므로 어떤 역할을 다른 역할로 모델링할 수 있습니다.

사전 정의 사용자 역할의 사용자 지정 복사본을 생성하려면

액세스: Admin

1단계 **System > Local > User Management**를 선택합니다.

User Management 페이지가 나타납니다.

2단계 **User Roles** 탭을 클릭합니다.

User Roles 페이지가 나타납니다.

3단계 복사할 사용자 역할의 옆에 있는 복사 아이콘()을 클릭합니다.

User Role Editor 페이지가 나타나며, 복사된 역할의 권한이 미리 선택되어 있습니다.

이렇게 사용자 지정 사용자 역할과 사전 정의 사용자 역할을 모두 복사할 수 있습니다.

사용자 지정 사용자 역할 삭제

라이센스: 모두

사전 정의 사용자 역할과 달리 사용자 지정 사용자 역할은 더 이상 필요하지 않을 때 삭제할 수 있습니다. 사용자 지정 역할을 완전히 제거하지는 않고 비활성화할 수도 있습니다. 자세한 내용은 61-49페이지의 사전 정의 사용자 역할 관리의 절차를 참조하십시오. 본인의 사용자 역할 또는 시스템 정책에서 기본 사용자 역할로 설정된 것은 삭제할 수 없습니다. 자세한 내용은 63-12페이지의 외부 인증 활성화을/를 참조하십시오.

사용자 지정 사용자 역할을 삭제하려면

액세스: Admin

1단계 **System > Local > User Management**를 선택합니다.

User Management 페이지가 나타납니다.

2단계 **User Roles** 탭을 클릭합니다.

User Roles 페이지가 나타납니다.

3단계 삭제할 사용자 지정 역할 옆의 삭제 아이콘( )을 클릭합니다.

사용자 지정 역할이 삭제되었습니다.

삭제된 역할이 어떤 사용자에게 지정된 유일한 역할일 경우, 그 사용자는 로그인하고 User Preferences 메뉴에 액세스할 수 있지만 그 밖의 방식으로는 FireSIGHT 시스템에 액세스할 수 없습니다.

사용자 권한 및 옵션 수정

라이센스: 모두

시스템에 사용자 계정을 추가한 다음 언제라도 액세스 권한, 계정 옵션 또는 비밀번호를 수정할 수 있습니다. 외부 디렉토리 서버에 인증된 사용자에게는 비밀번호 관리 옵션이 적용되지 않습니다. 이 설정은 외부 서버에서 관리합니다. 그러나 외부 인증된 계정을 포함하여 모든 계정에 대해 액세스 권한을 구성해야 합니다.

외부 인증 사용자의 경우, LDAP 그룹이나 RADIUS 목록 멤버십 또는 특성 값에 의해 액세스 역할이 부여된 사용자라면 그 최소 액세스 권한을 FireSIGHT 시스템 사용자 관리 페이지에서 제거할 수 없습니다. 그러나 추가 권한을 지정할 수는 있습니다. 외부 인증 사용자에 대한 액세스 권한을 수정할 때 User Management 페이지의 Authentication Method 열은 상태가 **External - Locally Modified**입니다.

어떤 사용자의 인증을 외부 인증에서 내부 인증으로 변경할 경우 그 사용자에 대해 새 비밀번호를 제공해야 합니다.

사용자 계정 권한을 수정하려면

액세스: Admin

1단계 **System > Local > User Management**를 선택합니다.

User Management 페이지가 나타납니다.

2단계 수정할 사용자 옆의 수정 아이콘( )을 클릭합니다.

Edit User 페이지가 나타납니다.

3단계 필요에 맞게 계정을 수정합니다.

- 외부 서버를 통해 사용자를 인증하는 방법에 대한 설명은 61-46페이지의 외부 인증 사용자 계정 관리을/를 참조하십시오.
- 내부 인증 사용자의 비밀번호 설정 변경에 대해서는 61-47페이지의 사용자 로그인 설정 관리을/를 참조하십시오.
- FireSIGHT 시스템 기능에 대한 액세스를 부여하기 위해 역할을 구성하는 것에 대해서는 61-48페이지의 사용자 역할 구성을/를 참조하십시오.

제한적 사용자 액세스 속성 이해

라이센스: 모두

어떤 사용자 역할에 제한적 검색을 적용함으로써 그 역할이 이벤트 뷰어에서 볼 수 있는 데이터를 제한할 수 있습니다. 역할을 생성하거나 어떤 사용자에게 지정된 역할을 수정할 때 이 정보를 지정할 수 있습니다. 제한적 액세스 권한을 갖는 사용자 지정 역할을 생성하려면 Menu Based Permissions 목록에서 제한할 표를 선택하고 Restrictive Search 드롭다운 목록에서 비공개 저장 검색을 선택해야 합니다. 자세한 내용은 61-51페이지의 사용자 지정 사용자 역할 관리을/를 참조하십시오.

사용자 비밀번호 수정

라이센스: 모두

내부 인증 사용자에 대해 User Management 페이지에서 사용자 비밀번호를 수정할 수 있습니다. LDAP 또는 RADIUS 서버에서 외부 인증 사용자 비밀번호를 관리해야 합니다.

참고 어플라이언스에서 STIG 규정준수 또는 LOM을 활성화할 경우 다른 비밀번호 제한이 적용됩니다. STIG 컴플라이언스가 활성화된 시스템에서 셸 액세스 사용자를 위한 비밀번호를 설정하는 것이 대한 자세한 내용은 *FireSIGHT 시스템 STIG 릴리스 정보*를 참조하십시오. LOM 사용자를 위한 시스템 비밀번호 설정에 대해서는 64-23페이지의 Lights-Out Management 사용자 액세스 활성화을/를 참조하십시오.

사용자의 비밀번호를 변경하려면

액세스: Admin

1단계 **System > Local > User Management**를 선택합니다.

User Management 페이지가 나타납니다.

2단계 사용자 이름 옆의 수정 아이콘( )을 클릭합니다.

Edit User 페이지가 나타납니다.

3단계 **Password** 필드에 새 비밀번호(최대 32자의 영숫자)를 입력합니다.

4단계 **Confirm Password** 필드에 새 비밀번호를 다시 입력합니다.

사용자 계정에 대해 비밀번호 강도 확인이 활성화된 경우 비밀번호는 대/소문자가 혼합된 8자 이상의 영숫자이고 숫자와 특수 문자를 각각 하나 이상 포함해야 합니다. 사전에 나와 있는 단어일 수 없으며, 연속적으로 반복되는 문자를 포함할 수 없습니다.

5단계 사용자 컨피그레이션에서 그 밖의 필요한 변경을 수행합니다.

- 비밀번호 옵션에 대한 자세한 내용은 61-47페이지의 사용자 로그인 설정 관리을/를 참조하십시오.
- 사용자 역할에 대한 자세한 내용은 61-48페이지의 사용자 역할 구성을/를 참조하십시오.

6단계 **Save**를 클릭합니다.

비밀번호가 변경되었고 다른 변경사항도 적용되었습니다.

사용자 계정 삭제

라이센스: 모두

언제라도 시스템에서 사용자 계정을 삭제할 수 있습니다. 단, 관리자 계정은 삭제할 수 없습니다.

사용자 계정을 삭제하려면

액세스: Admin

1단계 **System > Local > User Management**를 선택합니다.

User Management 페이지가 나타납니다.

2단계 계정을 삭제할 사용자 옆의 삭제 아이콘( )을 클릭합니다. 계정이 삭제되었습니다.

사용자 계정 권한

라이센스: 모두

다음 절에서는 FireSIGHT 시스템에서 구성 가능한 사용자 권한 및 그 권한에 액세스할 수 있는 사용자 역할을 나열합니다. 여기에 나열된 권한은 사용자 지정 사용자 역할을 생성할 때 나타나는 Menu Based Permissions 목록의 순서를 따른 것입니다. 관리되는 디바이스에서는 일부 권한을 사용할 수 없습니다. 방어 센터에서만 사용 가능한 권한은 표시되어 있습니다. 자세한 내용은 61-51페이지의 사용자 지정 사용자 역할 관리을/를 참조하십시오.

DC500 방어 센터 및 Series 2 디바이스는 제한적 기능 세트를 지원하므로 일부 권한은 이 어플라이언스에 적용되지 않습니다. 디바이스 모델별 지원되는 액세스 제어 기능 표에서 Series 2 어플라이언스 기능의 요약을 볼 수 있습니다.

다음 표를 비롯하여 이 문서 전반의 표에 사용된 액세스 표기법에 대해서는 1-18페이지의 액세스 표기 규칙을/를 참조하십시오. 다음 절에서는 웹 기반 인터페이스의 각 주메뉴와 관련된 사용자 역할 권한을 보여줍니다.

- 61-57페이지의 Overview 메뉴
- 61-58페이지의 Analysis 메뉴
- 61-60페이지의 Policies 메뉴
- 61-62페이지의 Devices 메뉴
- 61-63페이지의 FireAMP
- 61-62페이지의 Devices 메뉴

Overview 메뉴

라이센스: 모두

다음 표에서는 Overview 메뉴의 각 옵션에 액세스하는 데 필요한 사용자 역할 및 해당 사용자 역할이 하위 권한에 액세스할 수 있는지 여부를 순서대로 나열합니다. 보안 승인자, 검색 관리자, 침입 관리자, 액세스 관리자, 네트워크 관리자, 외부 데이터베이스 사용자 역할은 Overview 메뉴에서 아무런 권한이 없습니다.

표 61-6 Overview 메뉴

권한	관리자	유지 보수 사용자	보안 분석가	보안 분석가 (RO)
Dashboards	예	예	예	예
Manage Dashboards	예	아니요	아니요	아니요
Appliance Information Widget	예	예	예	예
Appliance Status Widget*(방어 센터만)*	예	예	예	예
Correlation Events Widget	예	아니요	예	예
Current Interface Status Widget	예	예	예	예
Current Sessions Widget	예	아니요	아니요	아니요
Custom Analysis Widget*(방어 센터만)*	예	아니요	예	예
Disk Usage Widget	예	예	예	예
Interface Traffic Widget	예	예	예	예
Intrusion Events Widget*(방어 센터만)*	예	아니요	예	예
Network Correlation Widget*(방어 센터만)*	예	아니요	예	예
Product Licensing Widget*(방어 센터만)*	예	예	아니요	아니요
Product Updates Widget	예	예	아니요	아니요
RSS Feed Widget	예	예	예	예
System Load Widget	예	예	예	예
System Time Widget	예	예	예	예
White List Events Widget*(방어 센터만)*	예	아니요	예	예
Reporting*(방어 센터만)*	예	아니요	예	예
Manage Report Templates*(방어 센터만)*	예	아니요	예	예
Summary	예	아니요	예	예
Intrusion Event Statistics*(방어 센터만)*	예	아니요	예	예
Intrusion Event Performance	예	아니요	아니요	아니요
Intrusion Event Graphs*(방어 센터만)*	예	아니요	예	예
Discovery Statistics*(방어 센터만)*	예	아니요	예	예

표 61-6 Overview 메뉴 (계속)

권한	관리자	유지 보수 사용자	보안 분석가	보안 분석가 (RO)
Discovery Performance*(방어 센터만)*	예	아니요	아니요	아니요
Connection Summary*(방어 센터만)*	예	아니요	예	예

Analysis 메뉴

라이센스: 모두

다음 표에서는 Analysis 메뉴의 각 옵션에 액세스하는 데 필요한 사용자 역할 및 해당 사용자 역할이 하위 권한에 액세스할 수 있는지 여부를 순서대로 나열합니다. 다른 제목 아래 여러 번 나타나는 권한은 하위 메뉴 소제목을 나타내는 경우를 제외하고 처음 한 번만 표시합니다. 보안 승인자, 침입 관리자, 액세스 관리자, 네트워크 관리자, 외부 데이터베이스 사용자 역할은 Analysis 메뉴에서 아무런 권한이 없습니다. Analysis 메뉴는 방어 센터에서만 사용할 수 있습니다.

표 61-7 Analysis 메뉴

메뉴	관리자	검색 관리자	유지 보수 사용자	보안 분석가	보안 분석가 (RO)
Application Statistics	예	아니요	아니요	예	예
Geolocation Statistics	예	아니요	아니요	예	예
User Statistics	예	아니요	아니요	예	예
URL Category Statistics	예	아니요	아니요	예	예
URL Reputation Statistics	예	아니요	아니요	예	예
SSL Statistics	예	아니요	아니요	예	예
Intrusion Event Statistics by Application	예	아니요	아니요	예	예
Intrusion Event Statistics by User	예	아니요	아니요	예	예
Security Intelligence Category Statistics	예	아니요	아니요	예	예
File Storage Statistics by Disposition	예	아니요	아니요	예	예
File Storage Statistics by Type	예	아니요	아니요	예	예
Dynamic File Analysis Statistics	예	아니요	아니요	예	예
Context Explorer	예	아니요	아니요	예	예
Connection Events	예	아니요	아니요	예	예
Modify Connection Events	예	아니요	아니요	예	아니요
Connection Summary Events	예	아니요	아니요	예	예
Modify Connection Summary Events	예	아니요	아니요	예	아니요
Security Intelligence Events	예	아니요	아니요	예	예
Modify Security Intelligence Events	예	아니요	아니요	예	아니요
Intrusion	예	아니요	아니요	예	예
Intrusion Events	예	아니요	아니요	예	예
Modify Intrusion Events	예	아니요	아니요	예	아니요
View Local Rules	예	아니요	아니요	예	예

표 61-7 Analysis 메뉴 (계속)

메뉴	관리자	검색 관리자	유지 보수 사용자	보안 분석가	보안 분석가 (RO)
Reviewed Events	예	아니요	아니요	예	예
Clipboard	예	아니요	아니요	예	예
Incidents	예	아니요	아니요	예	예
Files	예	아니요	아니요	예	예
Malware Events	예	아니요	아니요	예	예
Modify Malware Events	예	아니요	아니요	예	아니요
File Events	예	아니요	아니요	예	예
Modify File Events	예	아니요	아니요	예	아니요
Captured Files	예	아니요	아니요	예	예
Modify Captured Files	예	아니요	아니요	예	아니요
File Trajectory	예	아니요	아니요	예	예
File Download	예	아니요	아니요	예	예
Dynamic File Analysis	예	아니요	아니요	예	아니요
Hosts	예	아니요	아니요	예	예
Network Map	예	아니요	아니요	예	예
Hosts	예	아니요	아니요	예	예
Modify Hosts	예	아니요	아니요	예	아니요
Indications of Compromise	예	아니요	아니요	예	예
Modify Indications of Compromise	예	아니요	아니요	예	아니요
Servers	예	아니요	아니요	예	예
Modify Servers	예	아니요	아니요	예	아니요
Vulnerabilities	예	아니요	아니요	예	예
Modify Vulnerabilities	예	아니요	아니요	예	아니요
Host Attributes	예	아니요	아니요	예	예
Modify Host Attributes	예	아니요	아니요	예	아니요
Applications	예	아니요	아니요	예	예
Application Details	예	아니요	아니요	예	예
Modify Application Details	예	아니요	아니요	예	아니요
Host Attribute Management	예	아니요	아니요	아니요	아니요
Discovery Events	예	아니요	아니요	예	예
Modify Discovery Events	예	아니요	아니요	예	아니요
Users	예	예	아니요	예	예
User Activity	예	예	아니요	예	예
Modify User Activity Events	예	예	아니요	예	아니요
Users	예	예	아니요	예	예

표 61-7 Analysis 메뉴 (계속)

메뉴	관리자	검색 관리자	유지 보수 사용자	보안 분석가	보안 분석가 (RO)
Modify Users	예	예	아니요	예	아니요
Vulnerabilities	예	아니요	아니요	예	예
Third-party Vulnerabilities	예	아니요	아니요	예	예
Modify Third-party Vulnerabilities	예	아니요	아니요	예	아니요
Correlation	예	예	아니요	예	예
Correlation Events	예	예	아니요	예	예
Modify Correlation Events	예	예	아니요	예	아니요
White List Events	예	예	아니요	예	예
Modify White List Events	예	예	아니요	예	아니요
White List Violations	예	예	아니요	예	예
Remediation Status	예	예	아니요	아니요	아니요
Modify Remediation Status	예	예	아니요	아니요	아니요
Custom	예	아니요	아니요	예	예
Custom Workflows	예	아니요	아니요	예	예
Manage Custom Workflows	예	아니요	아니요	예	예
Custom Tables	예	아니요	아니요	예	예
Manage Custom Tables	예	아니요	아니요	예	예
Search	예	아니요	예	예	예
Manage Search	예	아니요	아니요	아니요	아니요
Bookmarks	예	아니요	아니요	예	예
Manage Bookmarks	예	아니요	아니요	예	예

Policies 메뉴

라이센스: 모두

다음 표에서는 Policies 메뉴의 각 옵션에 액세스하는 데 필요한 사용자 역할 및 해당 사용자 역할이 하위 권한에 액세스할 수 있는지 여부를 순서대로 나열합니다. 외부 데이터베이스 사용자, 유지 보수 사용자, 보안 분석가, 보안 분석가(읽기 전용) 역할은 Policies 메뉴에서 아무런 권한이 없습니다. Policies 메뉴는 방어 센터에서만 사용할 수 있습니다.

Intrusion Policy 및 Modify Intrusion Policy 권한에서는 네트워크 분석 정책을 생성하고 수정하는 것도 허용합니다.

표 61-8 Policies 메뉴

메뉴	액세스 관리자	관리자	검색 관리자	침입 관리자	네트워크 관리자	보안 승인자
Access Control	예	예	아니요	아니요	예	예
Access Control List	예	예	아니요	아니요	예	예

표 61-8 Policies 메뉴 (계속)

메뉴	액세스 관리자	관리자	검색 관리자	침입 관리자	네트워크 관리자	보안 승인자
Modify Access Control Policy	예	예	아니요	아니요	예	아니요
Modify Administrator Rules	예	예	아니요	아니요	예	아니요
Modify Root Rules	예	예	아니요	아니요	예	아니요
Apply Intrusion Policies	아니요	예	아니요	아니요	아니요	예
Apply Access Control Policies	아니요	예	아니요	아니요	아니요	예
Intrusion	예	예	아니요	예	아니요	예
Intrusion Policy	아니요	예	아니요	예	아니요	예
Rule Editor	아니요	예	아니요	예	아니요	아니요
Email	아니요	예	아니요	예	아니요	아니요
Modify Intrusion Policy	아니요	예	아니요	예	아니요	아니요
File Policy	예	예	아니요	아니요	아니요	아니요
Modify File Policy	예	예	아니요	아니요	아니요	아니요
Network Discovery	아니요	예	예	아니요	아니요	예
Custom Fingerprinting	아니요	예	예	아니요	아니요	아니요
Custom Topology	아니요	예	예	아니요	아니요	아니요
Modify Network Discovery	아니요	예	예	아니요	아니요	아니요
Apply Network Discovery	아니요	예	아니요	아니요	아니요	예
SSL	예	예	아니요	아니요	예	예
Modify SSL Policy	예	예	아니요	아니요	예	아니요
Modify Administrator Rules	예	예	아니요	아니요	예	아니요
Modify Root Rules	예	예	아니요	아니요	예	아니요
Apply SSL Policy	아니요	예	아니요	아니요	아니요	예
Application Detectors	아니요	예	예	아니요	아니요	아니요
User 3rd Party Mappings	아니요	예	예	아니요	아니요	아니요
Custom Product Mappings	아니요	예	예	아니요	아니요	아니요
Users	아니요	예	아니요	아니요	아니요	아니요
Correlation	아니요	예	아니요	아니요	아니요	아니요
Policy Management	아니요	예	아니요	아니요	아니요	아니요
Rule Management	아니요	예	아니요	아니요	아니요	아니요
White List	아니요	예	아니요	아니요	아니요	아니요
Traffic Profiles	아니요	예	아니요	아니요	아니요	아니요
Actions	아니요	예	예	아니요	아니요	아니요
Alerts	아니요	예	예	아니요	아니요	아니요
Impact Flag Alerts	아니요	예	예	아니요	아니요	아니요
Discovery Event Alerts	아니요	예	예	아니요	아니요	아니요

표 61-8 Policies 메뉴 (계속)

메뉴	액세스 관리자	관리자	검색 관리자	침입 관리자	네트워크 관리자	보안 승인자
Scanners	아니요	예	예	아니요	아니요	아니요
Scan Results	아니요	예	예	아니요	아니요	아니요
Modify Scan Results	아니요	예	예	아니요	아니요	아니요
Groups	아니요	예	아니요	아니요	아니요	아니요
Modules	아니요	예	아니요	아니요	아니요	아니요
Instances	아니요	예	아니요	아니요	아니요	아니요

Devices 메뉴

라이센스: 모두

Devices 메뉴 표에서는 Devices 메뉴의 각 옵션 및 그 하위 권한에 액세스하는 데 필요한 사용자 역할 권한을 순서대로 나열합니다. X는 그 사용자 역할이 액세스할 수 있음을 의미합니다. 액세스 관리자, 검색 관리자, 외부 데이터베이스 사용자, 침입 관리자, 유지 보수 사용자, 보안 승인자, 보안 분석가, 보안 분석가(읽기 전용)는 Devices 메뉴에서 아무런 권한이 없습니다. Devices 메뉴는 방어 센터에서만 사용할 수 있습니다.

표 61-9 Devices 메뉴

메뉴	관리자	네트워크 관리자
Device Management	예	예
Modify Devices	예	예
Apply Device Changes	예	예
NAT	예	예
NAT List	예	예
Modify NAT Policy	예	예
Apply NAT Rules	예	아니요
VPN	예	예
Modify VPN	예	예
Apply VPN Changes	예	예

Object Manager

라이센스: 모두

Object Manager 권한은 액세스 관리자, 관리자, 네트워크 관리자 사용자 역할에서 사용할 수 있습니다. Object Manager 권한은 방어 센터에서만 사용할 수 있습니다.

FireAMP

라이센스: 모두

FireAMP 권한은 관리자 사용자 역할만 사용할 수 있습니다. 이 권한은 방어 센터에서만 사용할 수 있습니다.

Health 메뉴

라이센스: 모두

다음 표에서는 Health 메뉴의 각 옵션에 액세스하는 데 필요한 사용자 역할 및 해당 사용자 역할이 하위 권한에 액세스할 수 있는지 여부를 순서대로 나열합니다. 액세스 관리자, 검색 관리자, 침입 관리자, 외부 데이터베이스 사용자, 네트워크 관리자, 보안 승인자 역할은 Health 메뉴에서 아무런 권한이 없습니다. Health 메뉴는 방어 센터에서만 사용할 수 있습니다.

표 61-10 Health 메뉴

메뉴	관리자	유지 보수 사용자	보안 분석가	보안 분석가(RO)
Health Policy	예	예	아니요	아니요
Modify Health Policy	예	예	아니요	아니요
Apply Health Policy	예	예	아니요	아니요
Health Events	예	예	예	예
Modify Health Events	예	예	아니요	아니요

System 메뉴

라이센스: 모두

다음 표에서는 System 메뉴의 각 옵션에 액세스하는 데 필요한 사용자 역할 및 해당 사용자 역할이 하위 권한에 액세스할 수 있는지 여부를 순서대로 나열합니다. 액세스 관리자, 검색 관리자, 침입 관리자, 외부 데이터베이스 사용자, 보안 분석가(읽기 전용) 역할은 System 메뉴에서 아무런 권한이 없습니다.

표 61-11 System 메뉴

메뉴	관리자	유지 보수 사용자	네트워크 관리자	보안 승인자	보안 분석가
Local	예	아니요	아니요	아니요	아니요
Configuration	예	아니요	아니요	아니요	아니요
Registration	예	아니요	아니요	아니요	아니요
High Availability(*DC1000, DC1500, DC2000, DC3000, DC3500, DC4000 만*)	예	아니요	아니요	아니요	아니요
eStreamer	예	아니요	아니요	아니요	아니요
Host Input Client(*방어 센터만*)	예	아니요	아니요	아니요	아니요
User Management	예	아니요	아니요	아니요	아니요
Users	예	아니요	아니요	아니요	아니요

표 61-11 System 메뉴 (계속)

메뉴	관리자	유지 보수 사용자	네트워크 관리자	보안 승인자	보안 분석가
User Roles	예	아니요	아니요	아니요	아니요
Login Authentication*(방어 센터만)*	예	아니요	아니요	아니요	아니요
System Policy*(방어 센터만)*	예	아니요	아니요	아니요	아니요
Apply System Policy*(방어 센터만)*	예	아니요	아니요	아니요	아니요
Modify System Policy*(방어 센터만)*	예	아니요	아니요	아니요	아니요
Updates	예	아니요	아니요	아니요	아니요
Rule Updates*(방어 센터만)*	예	아니요	아니요	아니요	아니요
Rule Update Import Log*(방어 센터만)*	예	아니요	아니요	아니요	아니요
Licenses	예	아니요	아니요	아니요	아니요
Monitoring	예	예	예	예	예
Audit	예	아니요	아니요	아니요	아니요
Modify Audit Log	예	아니요	아니요	아니요	아니요
Syslog	예	예	아니요	아니요	아니요
Task Status	예	예	예	예	예
View Other Users' Tasks	예	아니요	아니요	아니요	아니요
Statistics	예	예	아니요	아니요	아니요
Tools	예	예	아니요	아니요	예
Backup Management	예	예	아니요	아니요	아니요
Restore Backup	예	예	아니요	아니요	아니요
Scheduling	예	예	아니요	아니요	아니요
Delete Other Users' Scheduled Tasks	예	아니요	아니요	아니요	아니요
Import/Export	예	아니요	아니요	아니요	아니요
Discovery Data Purge*(방어 센터만)*	예	아니요	아니요	아니요	예
Whois	예	예	아니요	아니요	예

Help 메뉴

라이센스: 모두

Help 메뉴와 그 권한은 모든 사용자 역할에서 액세스할 수 있습니다. Help 메뉴 옵션은 제한할 수 없습니다.

사용자 역할 에스컬레이션 관리

라이센스: 모두

사용자 지정 사용자 역할은 기반이 된 역할 외에 또 다른 대상 사용자 역할의 권한을 비밀번호와 함께 일시적으로 부여받을 수 있습니다. 그러면 부재 시 어떤 사용자를 손쉽게 다른 사용자로 대체하거나 고급 사용자 권한의 사용을 면밀하게 추적하는 것이 가능합니다.

예를 들어 기반 역할의 권한이 매우 제한적인 사용자가 관리자 역할로 에스컬레이션하여 관리 작업을 수행할 수 있습니다. 사용자가 자신의 비밀번호를 사용하거나 지정된 다른 사용자의 비밀번호를 사용하도록 이 기능을 구성할 수 있습니다. 두 번째 옵션에서는 해당되는 모든 사용자를 대상으로 하나의 에스컬레이션 비밀번호를 손쉽게 관리할 수 있습니다. 자세한 내용은 61-66페이지의 사용자 지정 사용자 역할의 에스컬레이션 구성을/를 참조하십시오.

한 번에 하나의 사용자 역할만 에스컬레이션 대상 역할이 될 수 있습니다. 사용자 지정 또는 사전 정의 사용자 역할을 사용할 수 있습니다. 각 에스컬레이션은 로그인 세션 동안 지속되며 감사 로그에 기록됩니다.

이 기능을 구성하고 사용하는 것에 대한 자세한 내용은 다음 절을 참조하십시오.

에스컬레이션 대상 역할 구성

라이센스: 모두

어떤 사전 정의 또는 사용자 지정 사용자 역할도 시스템 차원 에스컬레이션 대상 역할이 되도록 지정할 수 있습니다. 다른 어떤 역할도 (에스컬레이션 기능이 있다면) 이 역할로 에스컬레이션할 수 있습니다.

에스컬레이션 대상 역할을 구성하려면

액세스: Admin

1단계 **System > Local > User Management**를 선택합니다.

User Management 페이지가 나타납니다.

2단계 **User Roles**를 클릭합니다.

User Roles 페이지가 나타납니다.

3단계 **Configure Permission Escalation**을 클릭합니다.

Configure Permission Escalation 대화 상자가 나타납니다.

4단계 드롭다운 목록에서 사용자 역할을 선택합니다.

5단계 **OK**를 클릭하여 변경 사항을 저장합니다.

변경사항이 저장되었고 User Roles 페이지가 나타납니다.

참고 에스컬레이션 대상 역할의 변경은 즉시 적용됩니다. 에스컬레이션된 세션의 사용자는 이제 새 에스컬레이션 대상의 권한을 갖습니다.

사용자 지정 사용자 역할의 에스컬레이션 구성

라이센스: 모두

사용자 역할 에스컬레이션 기능을 사용하려면 먼저 사용자 지정 사용자 역할에 에스컬레이션 권한을 구성하고 그 에스컬레이션 비밀번호를 선택하고 그 역할을 사용자에게 지정해야 합니다. 자세한 내용은 61-44페이지의 새 사용자 계정 추가및 61-48페이지의 사용자 역할 구성을/를 참조하십시오.

사용자 지정 역할에 대해 에스컬레이션 비밀번호를 구성할 때 조직의 요구 사항을 고려하십시오. 여러 에스컬레이션 사용자를 손쉽게 관리하길 원할 경우 또 다른 사용자를 선택하여 그 비밀번호를 에스컬레이션 비밀번호로 삼는 방법이 있습니다. 그 사용자의 비밀번호를 변경하거나 사용자를 비활성화할 경우 그 비밀번호를 필요로 하는 모든 에스컬레이션 사용자가 영향을 받습니다. 그러면 더 효율적으로 사용자 역할 에스컬레이션을 관리할 수 있습니다. 특히 중앙에서 관리할 수 있는 외부 인증 사용자를 선택할 경우 더욱 그렇습니다.

사용자 지정 사용자 역할에 대해 에스컬레이션을 구성하려면

액세스: Admin

1단계 **System > Local > User Management**를 선택합니다.

User Management 페이지가 나타납니다.

2단계 **User Roles**를 클릭합니다.

User Roles 페이지가 나타납니다.

3단계 **Create User Role**을 클릭하여 새 사용자 지정 사용자 역할을 생성하거나 기존 사용자 지정 사용자 역할 옆의 수정 아이콘( )을 클릭합니다.

User Role Editor 페이지가 나타납니다.

4단계 사용자 지정 사용자 역할의 이름, 설명, 메뉴 기반 권한을 선택합니다.

자세한 내용은 61-51페이지의 사용자 지정 사용자 역할 관리의 절차를 참조하십시오.

5단계 System Permissions에서 **Set this role to escalate to:** 확인란을 선택합니다.

에스컬레이션 비밀번호 옵션이 나타납니다.

6단계 이 역할이 에스컬레이션에 사용할 비밀번호를 선택합니다. 다음 2가지 옵션을 사용할 수 있습니다.

- 이 역할의 사용자가 에스컬레이션할 때 각자의 비밀번호를 사용하게 하려면 **Authenticate with the assigned user's password**를 선택합니다.
- 이 역할의 사용자가 다른 사용자의 비밀번호를 사용하게 하려면 **Authenticate with the specified user's password**를 선택하고 그 사용자 이름을 입력합니다.

참고 다른 사용자의 비밀번호로 인증할 경우 어떤 사용자 이름도, 심지어 비활성화되었거나 존재하지 않는 사용자의 이름도 입력할 수 있습니다. 비밀번호가 에스컬레이션에 사용되는 사용자를 비활성화할 경우 그 비밀번호를 필요로 하는 역할의 사용자는 에스컬레이션이 불가능해집니다. 에스컬레이션을 신속하게 제거해야 하는 경우 이 기능을 사용할 수 있습니다.

7단계 **Save**를 클릭합니다.

변경사항이 저장되었고 User Roles 페이지가 다시 나타납니다. 이 역할의 사용자는 이제 대상 사용자 역할로 에스컬레이션할 수 있습니다. 사용자에게 역할을 지정하는 것에 대한 자세한 내용은 61-44페이지의 새 사용자 계정 추가을/를 참조하십시오.

사용자 역할 에스컬레이션

라이센스: 모두

사용자가 에스컬레이션 권한이 있는 사용자 지정 사용자 역할을 맡은 경우 그 사용자는 언제라도 대상 역할의 권한으로 에스컬레이션할 수 있습니다. 에스컬레이션은 사용자 환경 설정에 영향을 주지 않습니다. 지정된 사용자 역할에서 사용자 역할 에스컬레이션이 구성되지 않은 경우 User 메뉴의 **Escalate Permissions** 옵션은 나타나지 않습니다.

사용자 권한을 에스컬레이션하려면

액세스: 모두

1단계 **Local > User > Escalate Permissions**를 선택합니다.

Escalate User Permissions 대화 상자가 나타납니다.

2단계 인증 비밀번호를 입력합니다.

3단계 **Escalate**를 클릭합니다.

이제 현재 역할 외에도 에스컬레이션 대상 역할의 모든 권한을 갖게 되었습니다.

에스컬레이션은 로그인 세션의 남은 시간 동안 지속됩니다. 다시 기본 역할의 권한만 가지려면 로그아웃했다가 새 세션을 시작해야 합니다.

Security Manager에서 SSO Cisco구성

라이센스: 모두

지원되는 디바이스: ASA FirePOWER

SSO(single sign-on)는 Cisco Security Manager(CSM) Version 4.7 이상과 방어 센터 간의 통합을 가능하게 합니다. 그러면 CSM에서 로그인을 위한 추가 인증 없이 방어 센터에 액세스할 수 있습니다. ASA FirePOWER 디바이스의 ASA 모듈을 관리할 때 디바이스의 FirePOWER 모듈에 적용되는 정책을 수정해야 하는 경우가 있습니다. CSM에서 관리하는 방어 센터를 선택하고 웹 브라우저에서 이를 실행할 수 있습니다. 관리하는 방어 센터가 고가용성 쌍의 멤버일 경우 SSO를 사용하면 기본 피어로 이동합니다.

사용자 역할 기반의 액세스 권한을 갖는 경우 CSM에서 교차 실행한 디바이스의 Device Management 페이지, Device 탭으로 이동합니다. 그렇지 않으면 Summary Dashboard 페이지(**Overview > Dashboards**)로 이동합니다. 단, 대시보드 액세스 권한이 없는 사용자 계정의 경우 Welcome 페이지를 사용합니다.

방어 센터에 대해 SSO하기 위해서는 먼저 CSM에서 방어 센터로 단방향 암호화 인증 경로를 설정해야 합니다. NAT 환경에서는 방어 센터와 CSM이 NAT 경계의 같은 편에 상주해야 합니다. 통신을 활성화하려면 CSM과 방어 센터에서 서로 인식하기 위한 다음 기준을 제공해야 합니다.

- CSM에서는 연결을 식별하는 SSO 공유 암호화 키를 생성해야 합니다. 방어 센터에서 이 키를 입력해야 합니다.
- 방어 센터에서는 CSM 서버 호스트 이름 또는 IP 주소를 서버 포트와 함께 제공합니다. 고가용성을 사용하는 경우 기본 피어에서 SSO를 구성합니다.
- 암호화 인증 매개 변수를 검증하려면 SSO 액세스를 사용할 모든 사용자에 대해 CSM과 방어 센터에서 동일한 사용자 이름(대/소문자 구분)을 설정해야 합니다.

방어 센터에서 STIG 규정준수가 활성화된 경우 SSO는 비활성화됩니다. 자세한 내용은 63-24페이지의 STIG 규정 준수 활성화을/를 참조하십시오.

참고 인증에 CAC를 사용하는 경우 SSO로 로그인할 수 없습니다. 자세한 내용은 61-9페이지의 CAC를 사용하는 LDAP 인증 이해을/를 참조하십시오.

SSO를 설정하려면

액세스: Admin

1단계 CSM에서 SSO 공유 암호화 키를 생성합니다.

자세한 내용은 CSM 설명서를 참조하십시오.

2단계 방어 센터에서 **System > Local > User Management**를 선택합니다.

User Management 페이지가 나타납니다.

3단계 **CSM Single Sign-on**을 선택합니다.

CSM Single Sign-on 페이지가 나타납니다.

4단계 **CSM 호스트 이름** 또는 **IP** 주소와 서버 **포트**를 입력합니다.

5단계 CSM에서 생성한 **공유 키**를 입력합니다.

6단계 또한 방어 센터의 프록시 서버를 CSM과의 통신에 사용하려는 경우 **Use Proxy For Connection** 확인란을 선택합니다. 자세한 내용은 64-9페이지의 관리 인터페이스 옵션 이해을/를 참조하십시오.

7단계 **Submit**을 클릭합니다.

CSM 인증서가 나타납니다.

8단계 **Confirm Certificate**를 클릭하여 인증서를 저장합니다.

이제 추가 로그인 없이 CSM에서 방어 센터로 로그인할 수 있습니다.

62장

작업 예약

서로 다른 많은 유형의 관리 작업이 동시에 또는 반복적으로 지정된 시간에 실행되도록 예약할 수 있습니다.

참고

일부 작업(예: 작동 소프트웨어 업데이트 또는 관리되는 디바이스로의 업데이트 푸시가 필요한 작업)은 저대역폭 네트워크에 상당한 부담이 될 수 있습니다. 이러한 작업은 네트워크 사용량이 적을 때 실행해야 합니다.

자세한 내용은 다음 절을 참조하십시오.

- 62-2페이지의 반복 작업 구성 - 예약 작업이 정기적으로 실행되도록 설정하는 방법에 대해 설명합니다.
- 62-3페이지의 백업 작업 자동화 - 백업 작업 예약에 대한 절차를 제공합니다.
- 62-4페이지의 CRL 다운로드 자동화 - 어플라이언스용 CRL(certificate revocation list)을 자동으로 새로 고치는 절차를 제공합니다.
- 62-5페이지의 Nmap 스캔 자동화 - Nmap 스캔 예약에 대한 절차를 제공합니다.
- 62-6페이지의 침입 정책 적용 자동화 - 관리되는 디바이스에 침입 정책을 적용하는 절차를 제공합니다.
- 62-8페이지의 보고서 생성 자동화 - 보고서 예약에 대한 절차를 제공합니다.
- 62-9페이지의 지오로케이션 데이터베이스 업데이트 자동화 - GeoDB(지오로케이션 데이터베이스)의 자동 업데이트 예약에 대한 절차를 제공합니다.
- 62-9페이지의 권장FireSIGHT 사항 자동화 - 침입 규칙 상태 권장 사항의 자동 업데이트 예약에 대한 절차를 제공합니다.
- 62-11페이지의 소프트웨어 업데이트 자동화 - 소프트웨어 업데이트의 다운로드, 푸시 및 설치 예약에 대한 절차를 제공합니다.
- 62-15페이지의 취약성 데이터베이스 업데이트 자동화 - VDB 업데이트의 다운로드 및 설치 예약에 대한 절차를 제공합니다.
- 62-17페이지의 URL 필터링 업데이트 자동화 - URL 필터링 데이터의 업데이트 자동화에 대한 절차를 제공합니다.
- 62-18페이지의 작업 보기 - 예약된 후 작업을 보고 관리하는 방법에 대해 설명합니다.
- 62-20페이지의 예약 작업 수정 - 기존 작업을 수정하는 방법에 대해 설명합니다.
- 62-21페이지의 예약 작업 삭제 - 1회 작업 및 모든 반복 작업을 삭제하는 방법에 대해 설명합니다.

반복 작업 구성

라이센스: 모두

모든 작업 유형에 동일한 프로세스를 사용하여 반복 작업의 빈도를 설정합니다.

웹 인터페이스에서 대부분의 페이지에 표시되는 시간은 로컬 시간입니다. 이 시간은 로컬 컨피그레이션에서 지정하는 표준 시간대를 사용하여 결정됩니다. 또한 해당되는 경우 방어 센터는 DST(일광 절약 시간)에 맞게 로컬 시간 표시를 자동으로 조정합니다. DST에서 표준 시간으로, 그리고 그 반대로 전환되는 날짜에 발생하는 반복 작업은 전환에 대해 조정되지 않습니다. 즉, 표준 시간 중 오전 2:00에 예약한 작업은 DST 중 오전 3:00에 실행됩니다. 마찬가지로, DST 중 오전 2:00에 예약한 작업은 표준 시간 중 오전 1:00에 실행됩니다.

반복 작업을 구성하려면

액세스: Admin/Maint

1단계 **System > Tools > Scheduling**을 선택합니다.

Scheduling 페이지가 나타납니다.

2단계 **Add Task**를 클릭합니다.

New Task 페이지가 나타납니다.

3단계 **Job Type** 목록에서 예약할 작업 유형을 선택합니다.

예약할 수 있는 각 작업 유형에 대해서는 각 절에서 설명합니다.

4단계 **Schedule task to run** 옵션에 대해 **Recurring**을 선택합니다.

페이지가 다시 로드되고 반복 작업 옵션이 표시됩니다.

5단계 반복 작업을 시작할 날짜를 **Start On** 필드에 지정합니다. 드롭다운 목록을 사용하여 월, 일, 연도를 선택할 수 있습니다.

6단계 작업 발생 빈도를 **Repeat Every** 필드에 지정합니다. 시간, 일, 주 또는 월의 수를 지정할 수 있습니다.

팁 숫자를 입력하거나 위쪽 아이콘(▲) 및 아래쪽 아이콘(▼)을 클릭하여 간격을 지정할 수 있습니다. 예를 들어 작업을 이틀마다 실행하려면 2를 입력하고 Days를 선택합니다.

7단계 반복 작업을 시작할 시간을 **Run At** 필드에 지정합니다.

8단계 **Repeat Every**에 대해 `Weeks`를 선택하면 **Repeat On** 필드가 나타납니다. 작업을 실행할 요일 옆에 있는 확인란을 선택합니다.

9단계 **Repeat Every**에 대해 `Months`를 선택하면 **Repeat On** 필드가 나타납니다. 드롭다운 목록을 사용하여 작업을 실행할 월의 날짜를 선택합니다.

New Task 페이지의 나머지 옵션은 생성하는 작업에 의해 결정됩니다. 자세한 내용은 다음 절을 참조하십시오.

- 62-3페이지의 백업 작업 자동화
- 62-4페이지의 CRL 다운로드 자동화
- 62-5페이지의 Nmap 스캔 자동화
- 62-8페이지의 보고서 생성 자동화
- 62-9페이지의 권장FireSIGHT 사항 자동화
- 62-11페이지의 소프트웨어 업데이트 자동화

백업 작업 자동화

라이센스: 모두

지원되는 디바이스: Series 2 및 Series 3

지원되는 Defense Center: 모두

스케줄러를 사용하면 방어 센터 또는 물리적 관리되는 디바이스의 백업을 자동화할 수 있습니다. 백업을 예약 작업으로 구성하려면 먼저 백업 프로필을 설계해야 합니다. 자세한 내용은 70-6페이지의 백업 프로필 생성을/를 참조하십시오.

가상 관리되는 디바이스, Cisco NGIPS for Blue Coat X-Series 또는 Cisco ASA with FirePOWER Services에서는 예약 백업을 수행할 수 **없습니다**. 물리적 관리되는 디바이스에서 컨피그레이션 데이터의 예약 백업을 수행하려면 디바이스 자체의 웹 인터페이스에서 작업을 예약합니다. 이벤트 데이터의 예약 백업을 수행하려면 관리하는 방어 센터의 예약 백업을 수행합니다.

백업 작업을 자동화하려면

액세스: Admin/Maint

1단계 **System > Tools > Scheduling**을 선택합니다.

Scheduling 페이지가 나타납니다.

2단계 **Add Task**를 클릭합니다.

New Task 페이지가 나타납니다.

3단계 **Job Type** 목록에서 **Backup**을 선택합니다.

페이지가 다시 로드되고 백업 옵션이 표시됩니다.

4단계 백업 예약 방법으로 **Once** 또는 **Recurring**을 지정합니다.

- 1회 작업의 경우 드롭다운 목록을 사용하여 시작 날짜와 시간을 지정합니다. **Current Time** 필드에 어플라이언스의 현재 시간이 표시됩니다.
- 반복 작업의 경우 작업 인스턴스 사이의 간격 설정을 위한 몇 가지 옵션이 있습니다. 자세한 내용은 62-2페이지의 반복 작업 구성을/를 참조하십시오.

5단계 최대 255자의 영숫자 문자, 공백 또는 대시를 사용하여 **Job Name** 필드에 이름을 입력합니다.

6단계 **Backup Profile** 목록에서 적절한 백업 프로필을 선택합니다.

새 백업 프로필 생성에 대한 자세한 내용은 70-6페이지의 백업 프로필 생성을/를 참조하십시오.

7단계 선택적으로, 최대 255자의 영숫자 문자, 공백 또는 대시를 사용하여 **Comment** 필드에 코멘트를 입력합니다.

팁 코멘트 필드가 페이지의 View Tasks 섹션에 나타나므로 되도록 짧게 유지해야 합니다.

8단계 선택적으로, 작업 상태 메시지를 전송할 이메일 주소(또는 쉼표로 구분한 여러 이메일 주소)를 **Email Status To:** 필드에 입력합니다.

상태 메시지를 전송할 유효한 이메일 릴레이 서버를 방어 센터에 구성해야 합니다. 릴레이 호스트 구성에 대한 자세한 내용은 63-18페이지의 메일 릴레이 호스트 및 알림 주소 구성을/를 참조하십시오.

9단계 **Save**를 클릭합니다.

작업이 추가됩니다. Task Status 페이지에서 실행 중인 작업의 상태를 확인할 수 있습니다. C-1페이지의 장기 실행 작업의 상태 보기을/를 참조하십시오.

CRL 다운로드 자동화

라이센스: 모두

스케줄러를 사용하면 사용자 인증서를 활성화할 어플라이언스에서 어플라이언스 웹 서버에 대한 CRL(certificate revocation list)을 자동으로 새로 고칠 수 있습니다. 로컬 어플라이언스 컨피그레이션에서 CRL 가져오기를 활성화하면 Download CRL 작업이 자동으로 생성되므로, 이 절차에서는 예약 작업을 열어 빈도를 설정하는 방법에 대해 설명합니다.

팁 이 작업을 예약하기 전에 사용자 인증서를 활성화 및 구성하고 CRL 다운로드 URL을 설정해야 합니다. 사용자 인증서 구성에 대한 자세한 내용은 64-6페이지의 사용자 인증서 요청을/를 참조하십시오.

CRL의 다운로드를 자동화하려면

액세스: Admin/Maint

1단계 **System > Tools > Scheduling**을 선택합니다.

Scheduling 페이지가 나타납니다.

2단계 Task Details에서 **download CRL** 작업을 찾고 수정 아이콘()을 클릭합니다.

Edit Task 페이지가 나타나고 다운로드 옵션이 표시됩니다.

3단계 CRL 다운로드 예약 방법으로 **Once** 또는 **Recurring**을 지정합니다.

- 1회 작업의 경우 드롭다운 목록을 사용하여 시작 날짜와 시간을 지정합니다. **Current Time** 필드에 어플라이언스의 현재 시간이 표시됩니다.
- 반복 작업의 경우 작업 인스턴스 사이의 간격 설정을 위한 몇 가지 옵션이 있습니다. 자세한 내용은 62-2페이지의 반복 작업 구성을/를 참조하십시오.

4단계 선택적으로, 최대 255자의 영숫자 문자, 공백 또는 대시를 사용하여 **Comment** 필드에 코멘트를 입력합니다.

팁 코멘트 필드가 페이지의 View Tasks 섹션에 나타나므로 되도록 짧게 유지해야 합니다.

5단계 선택적으로, 작업 상태 메시지를 전송할 이메일 주소(또는 쉼표로 구분한 여러 이메일 주소)를 **Email Status To:** 필드에 입력합니다.

상태 메시지를 전송할 유효한 이메일 릴레이 서버를 방어 센터에 구성해야 합니다. 릴레이 호스트 구성에 대한 자세한 내용은 63-18페이지의 메일 릴레이 호스트 및 알림 주소 구성을/를 참조하십시오.

6단계 **Save**를 클릭합니다.

작업이 추가됩니다. Task Status 페이지에서 실행 중인 작업의 상태를 확인할 수 있습니다. C-1페이지의 장기 실행 작업의 상태 보기을/를 참조하십시오.

Nmap 스캔 자동화

라이센스: FireSIGHT

네트워크에서 대상에 대해 정기적인 Nmap 스캔을 예약할 수 있습니다. 스캔을 자동화하면 Nmap 스캔에서 전에 제공한 정보를 새로 고칠 수 있습니다. FireSIGHT 시스템은 Nmap 제공 데이터를 업데이트할 수 없으므로 데이터를 최신 상태로 유지하려면 정기적으로 다시 스캔해야 합니다. 네트워크의 호스트에서 식별되지 않은 애플리케이션이나 서버를 자동으로 테스트하도록 스캔을 예약할 수도 있습니다. 자세한 내용은 다음 절을 참조하십시오.

- Nmap 스캔을 위해 시스템 준비
- Nmap 스캔 예약

Discovery Administrator는 Nmap 스캔을 교정으로서 사용할 수도 있습니다. 예를 들어, 호스트에서 운영 체제 충돌이 발생하면 해당 충돌이 Nmap 스캔을 트리거할 수 있습니다. 스캔을 실행하면 호스트에 대한 업데이트된 운영 체제 정보를 얻게 되며, 이를 통해 충돌이 해결됩니다. 자세한 내용은 54-12페이지의 Nmap 스캔 교정을/를 참조하십시오.

Nmap 스캔을 위해 시스템 준비

라이센스: FireSIGHT

전에 Nmap 스캐닝 기능을 사용하지 않은 경우 예약 스캔을 정의하기 전에 몇 가지 Nmap 컨피그레이션 단계를 완료해야 합니다. 자세한 내용은 다음 절을 참조하십시오.

- 47-9페이지의 Nmap 스캔 인스턴스 생성 - Nmap 서버 연결 프로필 설정에 대한 정보를 제공합니다.
- 47-10페이지의 Nmap 스캔 대상 생성 - 스캔 대상 설정에 대한 정보를 제공합니다.
- 47-11페이지의 Nmap 교정 생성 - 교정 정의 설정에 대한 정보를 제공합니다.

Nmap 스캔 예약

라이센스: FireSIGHT

Nmap 유틸리티를 사용하여 네트워크에서 호스트의 스캔을 예약할 수 있습니다.

시스템에서 탐지된 호스트의 운영 체제, 애플리케이션 또는 서버가 Nmap 스캔 결과와 교체되면, 시스템은 호스트에 대해 Nmap에 의해 교체된 정보를 더 이상 업데이트하지 않습니다. Nmap 제공 서비스 및 운영 체제 데이터는 또 다른 Nmap 스캔을 실행할 때까지 고정 상태로 유지됩니다. Nmap을 사용하여 호스트를 스캔하려는 경우 Nmap 제공 운영 체제, 애플리케이션 및 서버 데이터를 최신 상태로 유지하기 위해 정기적인 예약 스캔을 설정할 수 있습니다. 호스트가 네트워크 맵에서 삭제된 후 다시 추가된 경우, Nmap 스캔 결과가 삭제되며 시스템은 호스트에 대한 모든 운영 체제 및 서비스 데이터의 모니터링을 다시 시작합니다.

Nmap 스캐닝을 자동화하려면

액세스: Admin/Maint

1단계 **System > Tools > Scheduling**을 선택합니다.

Scheduling 페이지가 나타납니다.

2단계 **Add Task**를 클릭합니다.

New Task 페이지가 나타납니다.

3단계 **Job Type** 목록에서 **Nmap Scan**을 선택합니다.

페이지가 다시 로드되고 Nmap 스캔 자동화에 대한 옵션이 표시됩니다.

4단계 작업 예약 방법으로 **Once** 또는 **Recurring**을 지정합니다.

- 1회 작업의 경우 드롭다운 목록을 사용하여 시작 날짜와 시간을 지정합니다. **Current Time** 필드에 어플라이언스의 현재 시간이 표시됩니다.
- 반복 작업의 경우 작업 인스턴스 사이의 간격 설정을 위한 몇 가지 옵션이 있습니다. 자세한 내용은 62-2페이지의 반복 작업 구성을/를 참조하십시오.

5단계 최대 255자의 영숫자 문자, 공백 또는 대시를 사용하여 **Job Name** 필드에 이름을 입력합니다.

6단계 **Nmap Remediation** 필드에서 스캔 실행 시 사용할 Nmap 교정을 선택합니다.

7단계 **Nmap Target** 필드에서 스캔할 대상 호스트를 정의하는 스캔 대상을 선택합니다.

8단계 선택적으로, 최대 255자의 영숫자 문자, 공백 또는 대시를 사용하여 **Comment** 필드에 코멘트를 입력합니다.

팁 코멘트 필드가 페이지의 View Tasks 섹션에 나타나므로 되도록 짧게 유지해야 합니다.

9단계 선택적으로, 작업 상태 메시지를 전송할 이메일 주소(또는 쉼표로 구분한 여러 이메일 주소)를 **Email Status To:** 필드에 입력합니다.

상태 메시지를 전송할 유효한 이메일 릴레이 서버를 구성해야 합니다. 릴레이 호스트 구성에 대한 자세한 내용은 63-18페이지의 메일 릴레이 호스트 및 알림 주소 구성을/를 참조하십시오.

10단계 **Save**를 클릭합니다.

작업이 추가됩니다. Task Status 페이지에서 실행 중인 작업의 상태를 확인할 수 있습니다. C-1페이지의 장기 실행 작업의 상태 보기을/를 참조하십시오.

침입 정책 적용 자동화

라이센스: 보호

관리되는 디바이스에 대한 침입 정책 적용을 대기열에 추가할 수 있습니다. 작업이 실행될 때 침입 정책을 참조하는 액세스 제어 정책이 선택한 디바이스에 적용되는 경우에만 이 작업이 침입 정책에 적용됩니다. 그렇지 않으면 완료 전에 작업이 취소됩니다.

이 작업을 예약하기 전에, 침입 정책을 액세스 제어 정책과 연결하고 액세스 제어 정책을 디바이스에 적용해야 합니다. 18-1페이지의 침입 정책 및 파일 정책을 사용하여 트래픽 제어을/를 참조하십시오.

관리되는 디바이스에 대한 정책 적용을 대기열에 추가하려면

액세스: Admin/Maint

1단계 **System > Tools > Scheduling**을 선택합니다.

현재 달에 대한 예약 달력 페이지가 나타납니다.

2단계 **Add Task**를 클릭합니다.

New Task 페이지가 나타납니다.

3단계 **Job Type** 목록에서 **Queue Intrusion Policy Apply**를 선택합니다.

페이지가 다시 로드되고 정책 적용을 대기열에 추가하기 위한 옵션이 표시됩니다.

4단계 작업 예약 방법으로 **Once** 또는 **Recurring**을 지정합니다.

- 1회 작업의 경우 드롭다운 목록을 사용하여 시작 날짜와 시간을 지정합니다. **Current Time** 필드에 방어 센터의 현재 시간이 표시됩니다.
- 반복 작업의 경우 작업 인스턴스 사이의 간격 설정을 위한 몇 가지 옵션이 있습니다. 자세한 내용은 62-2페이지의 반복 작업 구성을/를 참조하십시오.

5단계 최대 255자의 영숫자 문자, 공백 또는 대시를 사용하여 **Job Name** 필드에 이름을 입력합니다.

6단계 **Intrusion Policy** 필드에 다음 옵션이 있습니다.

- 선택한 대상 디바이스에 적용할 침입 정책을 선택합니다.
- **Device** 필드에서 선택한 디바이스에 이미 적용된 모든 침입 정책을 적용하려면 **All intrusion policies**를 선택합니다.

7단계 **Device** 필드에 다음 옵션이 있습니다.

- **Intrusion Policy** 필드에서 선택한 침입 정책을 적용할 디바이스를 선택합니다.
- 선택한 침입 정책을 해당 침입 정책이 이미 적용된 모든 모니터링되는 디바이스에 적용하려면 **All targeted devices**를 선택합니다.

팁 **Intrusion Policy** 필드에서 선택한 침입 정책이 이미 적용된 디바이스만 이 필드에 표시됩니다.

8단계 선택적으로, 최대 255자의 영숫자 문자, 공백 또는 대시를 사용하여 **Comment** 필드에 코멘트를 입력합니다.

팁 예약 달력 페이지의 아래쪽에 있는 Tasks Details 섹션에 코멘트 필드가 나타나므로 코멘트의 크기를 제한해야 합니다.

9단계 선택적으로, 작업 상태 메시지를 전송할 이메일 주소(또는 쉼표로 구분한 여러 이메일 주소)를 **Email Status To:** 필드에 입력합니다.

상태 메시지를 전송할 유효한 이메일 릴레이 서버를 구성해야 합니다. 릴레이 호스트 구성에 대한 자세한 내용은 63-18페이지의 메일 릴레이 호스트 및 알림 주소 구성을/를 참조하십시오.

10단계 **Save**를 클릭합니다.

작업이 추가됩니다. 달력 페이지의 Task Details 섹션에서 실행 중인 작업의 상태를 확인할 수 있습니다. C-1페이지의 장기 실행 작업의 상태 보기을/를 참조하십시오.

11단계 저장된 작업을 수정하려면 예약 달력 페이지에 나타나는 해당 작업을 클릭합니다.

페이지 아래쪽에 Task Details 섹션이 나타납니다. 내용을 변경하려면 수정 아이콘( )을 클릭합니다.

보고서 생성 자동화

라이센스: 모두

지원되는 디바이스: X-Series 외 모두

일정한 간격으로 실행되도록 보고서를 자동화할 수 있습니다. 그러나 예약 작업으로 구성하기 전에 보고서에 대한 템플릿을 디자인해야 합니다. 보고서 템플릿을 사용하기 위해 보고서 디자이너를 사용하는 방법에 대한 자세한 내용은 57-2페이지의 보고서 템플릿 이해을/를 참조하십시오.

스케줄러를 사용하여 이메일 보고서를 배포하려면 작업을 예약하기 **전에** 보고서 템플릿과 메일 릴레이를 구성해야 합니다. 자세한 내용은 57-29페이지의 생성 시 이메일로 보고서 배포 및 63-18페이지의 메일 릴레이 호스트 및 알림 주소 구성을/를 참조하십시오.

보고서 생성을 자동화하려면

액세스: Admin/Maint

1단계 **System > Tools > Scheduling**을 선택합니다.

현재 달에 대한 예약 달력 페이지가 나타납니다.

2단계 **Add Task**를 클릭합니다.

New Task 페이지가 나타납니다.

3단계 **Job Type** 목록에서 **Report**를 선택합니다.

페이지가 다시 로드되고 자동으로 실행할 보고서를 설정하기 위한 옵션이 표시됩니다.

4단계 작업 예약 방법으로 **Once** 또는 **Recurring**을 지정합니다.

- 1회 작업의 경우 드롭다운 목록을 사용하여 시작 날짜와 시간을 지정합니다. **Current Time** 필드에 방어 센터의 현재 시간이 표시됩니다.
- 반복 작업의 경우 작업 인스턴스 사이의 간격 설정을 위한 몇 가지 옵션이 있습니다. 자세한 내용은 62-2페이지의 반복 작업 구성을/를 참조하십시오.

5단계 최대 255자의 영숫자 문자, 공백 또는 대시를 사용하여 **Job Name** 필드에 이름을 입력합니다.

6단계 **Report Template** 필드의 드롭다운 목록에서 사용할 보고서 템플릿을 선택합니다. 자세한 내용은 57-4페이지의 보고서 템플릿 생성 및 수정을/를 참조하십시오.

7단계 선택적으로, 최대 255자의 영숫자 문자, 공백 또는 대시를 사용하여 **Comment** 필드에 코멘트를 입력합니다.

팁 예약 달력 페이지의 아래쪽에 있는 Tasks Details 섹션에 코멘트 필드가 나타나므로 코멘트의 크기를 제한해야 합니다.

8단계 선택적으로, 작업 상태 메시지를 전송할 이메일 주소(또는 쉼표로 구분한 여러 이메일 주소)를 **Email Status To:** 필드에 입력합니다.

상태 메시지를 전송할 유효한 이메일 릴레이 서버를 구성해야 합니다. 릴레이 호스트 구성에 대한 자세한 내용은 63-18페이지의 메일 릴레이 호스트 및 알림 주소 구성을/를 참조하십시오.

참고 이 옵션을 구성해도 보고서가 배포되지는 **않습니다**. 자세한 내용은 57-29페이지의 생성 시 이메일로 보고서 배포을/를 참조하십시오.

9단계 보고서에 데이터가 없는 경우(예: 보고서 기간에 특정 유형의 이벤트가 발생하지 않은 경우) 보고서 이메일 첨부 파일을 수신하지 않으려면 **If report is empty, still attach to email** 확인란을 선택합니다.

10단계 **Save**를 클릭합니다.

작업이 추가됩니다. 달력 페이지의 Task Details 섹션에서 실행 중인 작업의 상태를 확인할 수 있습니다. C-1페이지의 장기 실행 작업의 상태 보기을/를 참조하십시오.

11단계 저장된 작업을 수정하려면 예약 달력 페이지에 나타나는 해당 작업을 클릭합니다.

페이지 아래쪽에 Task Details 섹션이 나타납니다. 내용을 변경하려면 수정 아이콘( )을 클릭합니다.

지오로케이션 데이터베이스 업데이트 자동화

라이센스: FireSIGHT

지원되는 Defense Center: DC500을 제외한 모든 방어 센터

스케줄러를 사용하면 반복되는 GeoDB(지오로케이션 데이터베이스) 업데이트를 자동화할 수 있습니다. 반복 GeoDB 업데이트는 7일에 한 번(매주) 실행됩니다. 매주 업데이트가 반복되는 시간을 구성할 수 있습니다. GeoDB 업데이트에 대한 자세한 내용은 66-27페이지의 지오로케이션 데이터베이스 업데이트을/를 참조하십시오.

지오로케이션 데이터베이스 업데이트를 자동화하려면

액세스: Admin

1단계 **System > Updates**를 선택합니다.

Product Updates 페이지가 나타납니다.

2단계 **Geolocation Updates** 탭을 클릭합니다.

Geolocation Updates 페이지가 나타납니다.

3단계 **Recurring Geolocation Updates** 아래에서 **Enable Recurring Weekly Updates** 확인란을 선택합니다.

Update Start Time 필드가 나타납니다.

4단계 **Update Start Time** 필드에서 매주 GeoDB 업데이트를 실행할 요일과 시간을 지정합니다.

5단계 **Save**를 클릭합니다.

작업이 추가됩니다. Task Status 페이지에서 실행 중인 작업의 상태를 확인할 수 있습니다. C-1페이지의 장기 실행 작업의 상태 보기을/를 참조하십시오.

권장FireSIGHT 사항 자동화

라이센스: 보호

사용자 지정 침입 정책에서 가장 최근에 저장된 컨피그레이션 설정을 사용하여 네트워크에 대한 네트워크 검색 데이터를 기반으로 규칙 상태 권장 사항을 자동으로 생성할 수 있습니다.

참고 저장되지 않은 변경 사항이 있는 침입 정책에 대해 시스템이 예약 권장 사항을 자동으로 생성하는 경우, 자동으로 생성된 권장 사항을 규칙에 반영하려면 해당 정책에서 변경 사항을 취소하고 정책을 커밋해야 합니다. 자세한 내용은 23-15페이지의 충돌 해결 및 정책 변경 사항 커밋을/를 참조하십시오.

작업이 실행되면 시스템이 권장 규칙 상태를 자동으로 생성합니다. 선택적으로, 33-1페이지의 네트워크 자산에 대한 침입 방지 맞춤화에 설명된 대로 정책의 컨피그레이션에 따라 침입 규칙의 상태도 수정합니다. 다음에 침입 정책을 적용할 때 수정된 규칙 상태가 반영됩니다.

규칙 상태 권장 사항 생성을 자동화하려면

액세스: Admin/Maint

1단계 **System > Tools > Scheduling**을 선택합니다.

Scheduling 페이지가 나타납니다.

2단계 **Add Task**를 클릭합니다.

New Task 페이지가 나타납니다.

3단계 **Job Type** 목록에서 **FireSIGHT Recommended Rules**를 선택합니다.

페이지가 다시 로드되고 FireSIGHT 권장 사항 생성을 위한 옵션이 표시됩니다.

4단계 선택적으로, **Job Type** 필드 옆에 있는 **policies** 링크를 클릭하여 Detection & Prevention 페이지를 표시합니다. 여기서 침입 정책의 FireSIGHT Recommended Rules를 구성할 수 있습니다.

5단계 작업 예약 방법으로 **Once** 또는 **Recurring**을 지정합니다.

- 1회 작업의 경우 드롭다운 목록을 사용하여 시작 날짜와 시간을 지정합니다. **Current Time** 필드에 어플라이언스의 현재 시간이 표시됩니다.
- 반복 작업의 경우 작업 인스턴스 사이의 간격 설정을 위한 몇 가지 옵션이 있습니다. 자세한 내용은 62-2페이지의 반복 작업 구성을/를 참조하십시오.

6단계 최대 255자의 영숫자 문자, 공백 또는 대시를 사용하여 **Job Name** 필드에 이름을 입력합니다.

7단계 **Policies** 옆에서 권장 사항을 생성할 하나 이상의 정책을 선택합니다. 다음 옵션을 이용할 수 있습니다.

- **Policies** 필드에서 하나 이상의 정책을 선택합니다. 여러 정책을 선택하려면 Shift 및 Ctrl 키를 사용합니다.
- 모든 정책을 선택하려면 **All Policies** 확인란을 클릭합니다.

8단계 선택적으로, 최대 255자의 영숫자 문자, 공백 또는 대시를 사용하여 **Comment** 필드에 코멘트를 입력합니다.

팁 코멘트 필드가 페이지의 View Tasks 섹션에 나타나므로 되도록 짧게 유지해야 합니다.

9단계 선택적으로, 작업 상태 메시지를 전송할 이메일 주소(또는 쉼표로 구분한 여러 이메일 주소)를 **Email Status To:** 필드에 입력합니다.

상태 메시지를 전송할 유효한 이메일 릴레이 서버를 구성해야 합니다. 릴레이 호스트 구성에 대한 자세한 내용은 63-18페이지의 메일 릴레이 호스트 및 알림 주소 구성을/를 참조하십시오.

10단계 **Save**를 클릭합니다.

작업이 추가됩니다. Task Status 페이지에서 실행 중인 작업의 상태를 확인할 수 있습니다. C-1페이지의 장기 실행 작업의 상태 보기을/를 참조하십시오.

소프트웨어 업데이트 자동화

라이센스: 모두

대부분의 패치와 기능 릴리스를 자동으로 FireSIGHT 시스템에 다운로드하여 적용할 수 있습니다.

참고 두 가지 상황에서는 수동으로 업데이트를 업로드 및 설치해야 합니다. 첫째, FireSIGHT 시스템에 대한 주 업데이트를 예약할 수 없습니다. 둘째, 지원 사이트에 액세스할 수 없는 어플라이언스에서는 업데이트나 푸시를 예약할 수 없습니다. 어플라이언스가 인터넷에 직접 연결되지 않은 경우 지원 사이트에서 업데이트를 다운로드하도록 하려면 64-8페이지의 관리 인터페이스 구성에 설명된 대로 프록시를 설정해야 합니다. 수동으로 FireSIGHT 시스템을 업데이트하는 방법에 대한 자세한 내용은 66-1페이지의 시스템 소프트웨어 업데이트을/를 참조하십시오.

소프트웨어 업데이트를 설치하기 위해 예약해야 하는 작업은 방어 센터를 업데이트하는지 또는 방어 센터를 사용하여 관리되는 디바이스를 업데이트하는지에 따라 다릅니다. Cisco에서는 방어 센터를 사용하여 관리 대상 디바이스를 업데이트할 것을 **적극** 권장합니다.

방어 센터를 업데이트하려면 Install Latest Update 작업을 사용하여 소프트웨어 설치를 예약하십시오. 관리되는 디바이스에서 소프트웨어 업데이트를 자동화하기 위해 방어 센터를 사용하려면 두 가지 작업을 예약해야 합니다.

1단계 Push Latest Update 작업을 사용하여 관리되는 디바이스에 업데이트를 푸시(복사)합니다.

2단계 Install Latest Update 작업을 사용하여 관리되는 디바이스에 업데이트를 설치합니다.

업데이트를 예약할 때에는 푸시를 예약하고 연속해서 발생할 작업을 설치합니다. 즉, 관리되는 디바이스에서 소프트웨어 업데이트를 자동화하려면, 업데이트를 설치하기 전에 먼저 디바이스에 푸시해야 합니다. 수동 업데이트 프로세스 중에는 업데이트를 설치하기 전에 관리되는 디바이스에 푸시할 필요가 없습니다. 자세한 내용은 66-8페이지의 관리되는 디바이스 업데이트을/를 참조하십시오.

참고 클러스터링된 또는 스태킹된 컨피그레이션에서는 관리되는 디바이스를 위한 개별 업데이트 작업을 생성할 수 없습니다.

프로세스를 완료할 수 있도록 항상 작업 간에 충분한 시간을 두십시오. 최소 30분 정도 후에 작업을 예약하십시오. 예를 들어 업데이트를 설치하기 위해 작업을 예약하는데 방어 센터에서 디바이스로 업데이트 복사가 완료되지 않은 경우 설치 작업이 성공하지 못합니다. 그러나 예약 설치 작업이 매일 반복되면 다음 날 작업이 실행될 때 푸시된 업데이트를 설치합니다.

이 프로세스를 더 세부적으로 제어하려면, 업데이트가 릴리스된 것을 확인한 후 **Once** 옵션을 사용하여 덜 바쁜 시간에 업데이트를 다운로드 및 설치할 수 있습니다.

자세한 내용은 다음 절을 참조하십시오.

- 62-12페이지의 소프트웨어 다운로드 자동화
- 62-13페이지의 소프트웨어 푸시 자동화
- 62-14페이지의 소프트웨어 설치 자동화

소프트웨어 다운로드 자동화

라이센스: 모두

Cisco에서 최신 소프트웨어 업데이트를 자동으로 다운로드하는 예약 작업을 생성할 수 있습니다. 이 작업을 사용하면 수동으로 설치할 업데이트의 다운로드를 예약할 수 있습니다.

소프트웨어 업데이트 다운로드를 자동화하려면

액세스: Admin/Maint

1단계 **System > Tools > Scheduling**을 선택합니다.

Scheduling 페이지가 나타납니다.

2단계 **Add Task**를 클릭합니다.

New Task 페이지가 나타납니다.

3단계 **Job Type** 목록에서 **Download Latest Update**를 선택합니다.

New Task 페이지가 다시 로드되고 업데이트 옵션이 표시됩니다.

4단계 작업 예약 방법으로 **Once** 또는 **Recurring**을 지정합니다.

- 1회 작업의 경우 드롭다운 목록을 사용하여 시작 날짜와 시간을 지정합니다. **Current Time** 필드에 어플라이언스의 현재 시간이 표시됩니다.
- 반복 작업의 경우 작업 인스턴스 사이의 간격 설정을 위한 몇 가지 옵션이 있습니다. 자세한 내용은 62-2페이지의 반복 작업 구성을/를 참조하십시오.

5단계 최대 255자의 영숫자 문자, 공백 또는 대시를 사용하여 **Job Name** 필드에 이름을 입력합니다.

6단계 **Update Items** 섹션에서 **Software**를 선택합니다.

7단계 선택적으로, 최대 255자의 영숫자 문자, 공백 또는 대시를 사용하여 **Comment** 필드에 코멘트를 입력합니다.

팁 코멘트 필드가 페이지의 View Tasks 섹션에 나타나므로 되도록 짧게 유지해야 합니다.

8단계 선택적으로, 작업 상태 메시지를 전송할 이메일 주소(또는 쉼표로 구분한 여러 이메일 주소)를 **Email Status To:** 필드에 입력합니다.

상태 메시지를 전송할 유효한 이메일 릴레이 서버를 구성해야 합니다. 릴레이 호스트 구성에 대한 자세한 내용은 63-18페이지의 메일 릴레이 호스트 및 알림 주소 구성을/를 참조하십시오.

9단계 **Save**를 클릭합니다.

작업이 추가됩니다. Task Status 페이지에서 실행 중인 작업의 상태를 확인할 수 있습니다. C-1페이지의 장기 실행 작업의 상태 보기을/를 참조하십시오.

소프트웨어 푸시 자동화

라이센스: 모두

관리되는 디바이스에서 소프트웨어 업데이트의 설치를 자동화하려면 설치 전에 디바이스에 업데이트를 푸시해야 합니다.

관리되는 디바이스에 업데이트를 푸시하면 Tasks 페이지에서 푸시 프로세스 상태에 대한 정보가 보고됩니다. 자세한 내용은 C-1페이지의 장기 실행 작업의 상태 보기을/를 참조하십시오.

관리되는 디바이스에 소프트웨어 업데이트를 푸시하기 위한 작업을 생성하는 경우, 디바이스에 업데이트를 복사할 수 있도록 푸시 작업과 예약 설치 작업 사이에 충분한 시간을 두어야 합니다.

관리되는 디바이스에 소프트웨어 업데이트를 푸시하려면

액세스: Admin/Maint

1단계 **System > Tools > Scheduling**을 선택합니다.

Scheduling 페이지가 나타납니다.

2단계 **Add Task**를 클릭합니다.

New Task 페이지가 나타납니다.

3단계 **Job Type** 목록에서 **Push Latest Update**를 선택합니다.

페이지가 다시 로드되고 업데이트 푸시를 위한 옵션이 표시됩니다.

4단계 작업 예약 방법으로 **Once** 또는 **Recurring**을 지정합니다.

- 1회 작업의 경우 드롭다운 목록을 사용하여 시작 날짜와 시간을 지정합니다. **Current Time** 필드에 어플라이언스의 현재 시간이 표시됩니다.
- 반복 작업의 경우 작업 인스턴스 사이의 간격 설정을 위한 몇 가지 옵션이 있습니다. 자세한 내용은 62-2페이지의 반복 작업 구성을/를 참조하십시오.

5단계 최대 255자의 영숫자 문자, 공백 또는 대시를 사용하여 **Job Name** 필드에 이름을 입력합니다.

6단계 **Device** 목록에서 업데이트를 수신할 디바이스를 선택합니다.

7단계 선택적으로, 최대 255자의 영숫자 문자, 공백 또는 대시를 사용하여 **Comment** 필드에 코멘트를 입력합니다.

팁 코멘트 필드가 페이지의 View Tasks 섹션에 나타나므로 되도록 짧게 유지해야 합니다.

8단계 선택적으로, 작업 상태 메시지를 전송할 이메일 주소(또는 쉼표로 구분한 여러 이메일 주소)를 **Email Status To:** 필드에 입력합니다.

상태 메시지를 전송할 유효한 이메일 릴레이 서버를 구성해야 합니다. 릴레이 호스트 구성에 대한 자세한 내용은 63-18페이지의 메일 릴레이 호스트 및 알림 주소 구성을/를 참조하십시오.

9단계 **Save**를 클릭합니다.

작업이 추가됩니다. Task Status 페이지에서 실행 중인 작업의 상태를 확인할 수 있습니다. C-1페이지의 장기 실행 작업의 상태 보기을/를 참조하십시오.

소프트웨어 설치 자동화

라이센스: 모두

관리되는 디바이스에 소프트웨어 업데이트를 설치하는 작업을 생성하기 위해 방어 센터를 사용하는 경우 업데이트를 디바이스로 푸시하는 작업과 업데이트를 설치하는 작업 사이에 충분한 시간을 두어야 합니다. 관리되는 디바이스로 업데이트를 푸시하는 방법에 대한 자세한 내용은 62-13페이지의 소프트웨어 푸시 자동화을/를 참조하십시오.

주의 설치할 업데이트에 따라, 소프트웨어가 설치된 후 어플라이언스가 재부팅될 수 있습니다.

소프트웨어 설치 작업을 예약하려면

액세스: Admin/Maint

1단계 **System > Tools > Scheduling**을 선택합니다.

Scheduling 페이지가 나타납니다.

2단계 **Add Task**를 클릭합니다.

New Task 페이지가 나타납니다.

3단계 **Job Type** 목록에서 **Install Latest Update**를 선택합니다.

페이지가 다시 로드되고 업데이트 설치를 위한 옵션이 표시됩니다.

4단계 작업 예약 방법으로 **Once** 또는 **Recurring**을 지정합니다.

- 1회 작업의 경우 드롭다운 목록을 사용하여 시작 날짜와 시간을 지정합니다. **Current Time** 필드에 어플라이언스의 현재 시간이 표시됩니다.
- 반복 작업의 경우 작업 인스턴스 사이의 간격 설정을 위한 몇 가지 옵션이 있습니다. 자세한 내용은 62-2페이지의 반복 작업 구성을/를 참조하십시오.

5단계 최대 255자의 영숫자 문자, 공백 또는 대시를 사용하여 **Job Name** 필드에 이름을 입력합니다.

6단계 **Device** 목록에 다음 옵션이 있습니다.

- 업데이트를 설치할 디바이스를 선택합니다.
- 업데이트를 설치할 방어 센터의 이름을 선택합니다.

7단계 **Update Items** 섹션에서 **Software**를 선택합니다.

8단계 선택적으로, 최대 255자의 영숫자 문자, 공백 또는 대시를 사용하여 **Comment** 필드에 코멘트를 입력합니다.

팁 코멘트 필드가 페이지의 View Tasks 섹션에 나타나므로 되도록 짧게 유지해야 합니다.

9단계 선택적으로, 작업 상태 메시지를 전송할 이메일 주소(또는 쉼표로 구분한 여러 이메일 주소)를 **Email Status To:** 필드에 입력합니다.

상태 메시지를 전송할 유효한 이메일 릴레이 서버를 구성해야 합니다. 릴레이 호스트 구성에 대한 자세한 내용은 63-18페이지의 메일 릴레이 호스트 및 알림 주소 구성을/를 참조하십시오.

10단계 **Save**를 클릭합니다.

작업이 추가됩니다. Task Status 페이지에서 실행 중인 작업의 상태를 확인할 수 있습니다. C-1페이지의 장기 실행 작업의 상태 보기을/를 참조하십시오.

취약성 데이터베이스 업데이트 자동화

라이센스: FireSIGHT

Cisco는 FireSIGHT 시스템에서 인식하는 네트워크 자산, 트래픽 및 취약성 목록을 확장하기 위해 VDB(취약성 데이터베이스) 업데이트를 사용합니다. 최신 VDB 업데이트를 다운로드하여 방어 센터에 설치하려면 예약 기능을 사용할 수 있습니다. 이를 통해 최신 정보를 사용하여 네트워크의 호스트를 평가할 수 있습니다.

참고 지원 사이트에 액세스할 수 없는 어플라이언스에 대해서는 업데이트를 예약할 수 없습니다. 어플라이언스가 인터넷에 직접 연결되지 않은 경우 지원 사이트에서 업데이트를 다운로드하도록 하려면 64-8페이지의 관리 인터페이스 구성에 설명된 대로 프록시를 설정해야 합니다. 수동으로 FireSIGHT 시스템을 업데이트하는 방법에 대한 자세한 내용은 66-1페이지의 시스템 소프트웨어 업데이트을/를 참조하십시오.

VDB 업데이트를 자동화할 때 두 가지 별도의 단계를 자동화해야 합니다.

1단계 VDB 업데이트를 다운로드합니다.

2단계 VDB 업데이트를 설치합니다.

프로세스를 완료할 수 있도록 항상 작업 간에 충분한 시간을 두십시오. 예를 들어 업데이트를 설치하기 위해 작업을 예약하는데 업데이트가 충분히 다운로드되지 않은 경우 설치 작업이 성공하지 못합니다. 그러나 예약 설치 작업이 매일 반복되면 다음 날 작업이 실행될 때 다운로드된 VDB 업데이트를 설치합니다.

이 프로세스를 더 세부적으로 제어하려면, **Once** 옵션을 사용하여 업데이트가 릴리스된 것을 확인한 후 덜 바쁜 시간에 VDB 업데이트를 다운로드 및 설치할 수 있습니다.

참고 VDB 업데이트를 설치하면 트래픽 플로우와 처리가 잠시 중지되고, 소수의 패킷이 검사 없이 통과될 수 있습니다.

자세한 내용은 다음 절을 참조하십시오.

- 62-15페이지의 VDB 업데이트 다운로드 자동화
- 62-16페이지의 VDB 업데이트 설치 자동화

VDB 업데이트 다운로드 자동화

라이센스: FireSIGHT

Cisco에서 최신 VDB 업데이트를 자동으로 다운로드하는 예약 작업을 방어 센터에서 생성할 수 있습니다.

VDB 업데이트 다운로드를 자동화하려면

액세스: Admin/Maint

1단계 **System > Tools > Scheduling**을 선택합니다.

Scheduling 페이지가 나타납니다.

2단계 **Add Task**를 클릭합니다.

New Task 페이지가 나타납니다.

3단계 **Job Type** 목록에서 **Download Latest Update**를 선택합니다.

New Task 페이지가 다시 로드되고 업데이트 옵션이 표시됩니다.

4단계 작업 예약 방법으로 **Once** 또는 **Recurring**을 지정합니다.

- 1회 작업의 경우 드롭다운 목록을 사용하여 시작 날짜와 시간을 지정합니다. **Current Time** 필드에 어플라이언스의 현재 시간이 표시됩니다.
- 반복 작업의 경우 작업 인스턴스 사이의 간격 설정을 위한 몇 가지 옵션이 있습니다. 자세한 내용은 62-2페이지의 반복 작업 구성을/를 참조하십시오.

5단계 최대 255자의 영숫자 문자, 공백 또는 대시를 사용하여 **Job Name** 필드에 이름을 입력합니다.

6단계 **Update Items** 섹션에서 **Vulnerability Database**를 선택합니다.

7단계 선택적으로, 최대 255자의 영숫자 문자, 공백 또는 대시를 사용하여 **Comment** 필드에 코멘트를 입력합니다.

팁 코멘트 필드가 페이지의 View Tasks 섹션에 나타나므로 되도록 짧게 유지해야 합니다.

8단계 선택적으로, 작업 상태 메시지를 전송할 이메일 주소(또는 쉼표로 구분한 여러 이메일 주소)를 **Email Status To:** 필드에 입력합니다.

상태 메시지를 전송할 유효한 이메일 릴레이 서버를 구성해야 합니다. 릴레이 호스트 구성에 대한 자세한 내용은 63-18페이지의 메일 릴레이 호스트 및 알림 주소 구성을/를 참조하십시오.

9단계 **Save**를 클릭합니다.

작업이 추가됩니다. Task Status 페이지에서 실행 중인 작업의 상태를 확인할 수 있습니다. C-1페이지의 장기 실행 작업의 상태 보기을/를 참조하십시오.

VDB 업데이트 설치 자동화

라이센스: FireSIGHT

VDB 업데이트를 다운로드하는 작업과 업데이트를 설치하는 작업 사이에 시간을 충분히 두어야 합니다. 자세한 내용은 62-15페이지의 VDB 업데이트 다운로드 자동화을/를 참조하십시오.

참고 VDB 업데이트를 설치하면 트래픽 플로우와 처리가 잠시 중지되고, 소수의 패킷이 검사 없이 통과될 수 있습니다.

VDB 업데이트를 예약하려면

액세스: Admin/Maint

1단계 **System > Tools > Scheduling**을 선택합니다.

Scheduling 페이지가 나타납니다.

2단계 **Add Task**를 클릭합니다.

New Task 페이지가 나타납니다.

3단계 **Job Type** 목록에서 **Install Latest Update**를 선택합니다.

페이지가 다시 로드되고 업데이트 설치를 위한 옵션이 표시됩니다.

4단계 작업 예약 방법으로 **Once** 또는 **Recurring**을 지정합니다.

- 1회 작업의 경우 드롭다운 목록을 사용하여 시작 날짜와 시간을 지정합니다. **Current Time** 필드에 어플라이언스의 현재 시간이 표시됩니다.
- 반복 작업의 경우 작업 인스턴스 사이의 간격 설정을 위한 몇 가지 옵션이 있습니다. 자세한 내용은 62-2페이지의 반복 작업 구성을/를 참조하십시오.

5단계 최대 255자의 영숫자 문자, 공백 또는 대시를 사용하여 **Job Name** 필드에 이름을 입력합니다.

6단계 **Device** 드롭다운 목록에서 방어 센터의 이름을 선택합니다.

7단계 **Update Items** 섹션에서 **Vulnerability Database**를 선택합니다.

8단계 선택적으로, 최대 255자의 영숫자 문자, 공백 또는 대시를 사용하여 **Comment** 필드에 코멘트를 입력합니다.

팁 코멘트 필드가 페이지의 View Tasks 섹션에 나타나므로 되도록 짧게 유지해야 합니다.

9단계 선택적으로, 작업 상태 메시지를 전송할 이메일 주소(또는 쉼표로 구분한 여러 이메일 주소)를 **Email Status To:** 필드에 입력합니다.

상태 메시지를 전송할 유효한 이메일 릴레이 서버를 구성해야 합니다. 릴레이 호스트 구성에 대한 자세한 내용은 63-18페이지의 메일 릴레이 호스트 및 알림 주소 구성을/를 참조하십시오.

10단계 **Save**를 클릭합니다.

작업이 추가됩니다. Task Status 페이지에서 실행 중인 작업의 상태를 확인할 수 있습니다. C-1페이지의 장기 실행 작업의 상태 보기을/를 참조하십시오.

URL 필터링 업데이트 자동화

라이센스: URL 필터링

지원되는 Defense Center: DC500을 제외한 모든 방어 센터

스케줄러를 사용하면 종합 보안 인텔리전스 클라우드에서 URL 필터링 데이터의 업데이트를 자동화할 수 있습니다. URL 필터링 업데이트 작업이 성공하려면

- 방어 센터가 인터넷에 액세스할 수 있어야 합니다. 그렇지 않으면 클라우드에 연결할 수 없습니다.
- 64-27페이지의 클라우드 통신 활성화에 설명된 대로 URL 필터링을 활성화해야 합니다.

URL 필터링을 활성화할 때 자동 업데이트도 활성화할 수 있습니다. 이렇게 하면 방어 센터는 URL 필터링 업데이트를 위해 30분마다 클라우드에 연결합니다. 자동 업데이트를 활성화한 경우 URL 필터링 데이터를 업데이트하는 예약 작업을 생성해서는 **안 됩니다**.

일일 업데이트 양이 적다고 생각될 수도 있으나, 마지막 업데이트 이후 5일 이상 경과하면 새로운 URL 필터링 데이터를 다운로드하는 데 대역폭에 따라 20분 이상이 소요될 수 있습니다. 그런 다음 업데이트 자체를 수행하는 데 30분이 걸릴 수 있습니다.

URL 필터링 데이터 작업을 자동화하려면

액세스: Admin/Maint

1단계 **System > Tools > Scheduling**을 선택합니다.

Scheduling 페이지가 나타납니다.

2단계 **Add Task**를 클릭합니다.

New Task 페이지가 나타납니다.

3단계 **Job Type** 목록에서 **Update URL Filtering Database**를 선택합니다.

New Task 페이지가 다시 로드되고 URL 필터링 업데이트 옵션이 표시됩니다.

4단계 업데이트 예약 방법으로 **Once** 또는 **Recurring**을 지정합니다.

- 1회 작업의 경우 드롭다운 목록을 사용하여 시작 날짜와 시간을 지정합니다. **Current Time** 필드에 어플라이언스의 현재 시간이 표시됩니다.
- 반복 작업의 경우 작업 인스턴스 사이의 간격 설정을 위한 몇 가지 옵션이 있습니다. 자세한 내용은 62-2페이지의 반복 작업 구성을/를 참조하십시오.

5단계 최대 255자의 영숫자 문자, 공백 또는 대시를 사용하여 **Job Name** 필드에 이름을 입력합니다.

6단계 선택적으로, 최대 255자의 영숫자 문자, 공백 또는 대시를 사용하여 **Comment** 필드에 코멘트를 입력합니다.

팁 코멘트 필드가 페이지의 View Tasks 섹션에 나타나므로 되도록 짧게 유지해야 합니다.

7단계 선택적으로, 작업 상태 메시지를 전송할 이메일 주소(또는 쉼표로 구분한 여러 이메일 주소)를 **Email Status To** 필드에 입력합니다.

상태 메시지를 전송할 유효한 이메일 릴레이 서버를 구성해야 합니다. 릴레이 호스트 구성에 대한 자세한 내용은 63-18페이지의 메일 릴레이 호스트 및 알림 주소 구성을/를 참조하십시오.

8단계 **Save**를 클릭합니다.

작업이 추가됩니다. Task Status 페이지에서 실행 중인 작업의 상태를 확인할 수 있습니다. C-1페이지의 장기 실행 작업의 상태 보기을/를 참조하십시오.

작업 보기

라이센스: 모두

예약 작업을 추가한 후 내용을 보고 상태를 평가할 수 있습니다. 페이지의 View Options 섹션에서는 달력 및 예약 작업 목록을 사용하여 예약 작업을 볼 수 있습니다.

자세한 내용은 다음 절을 참조하십시오.

- 62-19페이지의 달력 사용
- 62-19페이지의 작업 목록 사용

달력 사용

라이센스: 모두

Calendar 보기 옵션에서는 어떤 예약 작업이 언제 발생하는지 확인할 수 있습니다.

달력을 사용하여 예약 작업을 보려면

액세스: Admin/Maint

1단계 **System > Tools > Scheduling**을 선택합니다.

Scheduling 페이지가 나타납니다.

2단계 달력 보기를 사용하여 다음 작업을 수행할 수 있습니다.

- 1년 뒤로 이동하려면 이중 왼쪽 화살표 아이콘(≪)을 클릭합니다.
- 1개월 뒤로 이동하려면 단일 왼쪽 화살표 아이콘(‹)을 클릭합니다.
- 1개월 앞으로 이동하려면 단일 오른쪽 화살표 아이콘(›)을 클릭합니다.
- 1년 앞으로 이동하려면 이중 오른쪽 화살표 아이콘(≫)을 클릭합니다.
- 현재 달과 연도로 돌아가려면 **Today**를 클릭합니다.
- 새 작업을 예약하려면 **Add Task**를 클릭합니다.
- 달력 아래의 작업 목록 테이블에서 특정 날짜의 모든 예약 작업을 보려면 날짜를 클릭합니다.
- 달력 아래의 작업 목록 테이블에서 작업을 보려면 날짜의 특정 작업을 클릭합니다.

참고 작업 목록 사용에 대한 자세한 내용은 작업 목록 사용을/를 참조하십시오.

작업 목록 사용

라이센스: 모두

Task List는 작업 목록을 상태와 함께 표시합니다. 달력을 열면 달력 아래에 작업 목록이 나타납니다. 달력에서 날짜 또는 작업을 선택하여 작업 목록에 액세스할 수도 있습니다. 자세한 내용은 62-19페이지의 달력 사용을/를 참조하십시오.

표 62-1 작업 목록 열

열	설명
이름	예약 작업의 이름 및 이와 관련된 코멘트를 표시합니다.
유형	예약 작업의 유형을 표시합니다.
시작 시간	예약 시작 날짜 및 시간을 표시합니다.
빈도	작업 실행 빈도를 표시합니다.

표 62-1 작업 목록 열 (계속)

열	설명
상태	예약 작업의 현재 상태를 설명합니다. • 확인 표시 아이콘( )은 작업이 성공적으로 실행되었음을 나타냅니다. • 물음표 아이콘( )은 작업이 알 수 없는 상태임을 나타냅니다. • 느낌표 아이콘( )은 작업이 실패했음을 나타냅니다.
작성자	예약 작업을 생성한 사용자의 이름을 표시합니다.
수정	예약 작업을 수정합니다.
삭제	예약 작업을 삭제합니다.

예약 작업 수정

라이센스: 모두

전에 생성한 예약 작업을 수정할 수 있습니다. 이 기능은 매개 변수가 올바른지 확인하기 위해 예약 작업을 1회 테스트하려는 경우 특히 유용합니다. 나중에 작업이 성공적으로 완료되면 반복 작업으로 변경할 수 있습니다.

기존 예약 작업을 수정하려면

액세스: Admin/Maint

1단계 **System > Tools > Scheduling**을 선택합니다.

Scheduling 페이지가 나타납니다.

2단계 수정할 작업 또는 작업이 나타나는 요일을 클릭합니다.

선택한 작업을 포함하는 Task Details 테이블이 나타납니다.

3단계 테이블에서 수정할 작업을 찾고 수정 아이콘( )을 클릭합니다.

Edit Task 페이지가 나타나고 선택한 작업의 세부사항이 표시됩니다.

4단계 시작 시간, 작업 이름, 코멘트, 작업 실행 빈도, 1회 또는 반복 등 필요에 맞게 작업을 수정합니다. 작업 유형은 변경할 수 없습니다.

나머지 옵션은 수정 중인 작업에 의해 결정됩니다. 자세한 내용은 다음 절을 참조하십시오.

- 62-3페이지의 백업 작업 자동화
- 62-4페이지의 CRL 다운로드 자동화
- 62-5페이지의 Nmap 스캔 자동화
- 62-8페이지의 보고서 생성 자동화
- 62-9페이지의 권장FireSIGHT 사항 자동화
- 62-11페이지의 소프트웨어 업데이트 자동화
- 62-15페이지의 취약성 데이터베이스 업데이트 자동화
- 62-17페이지의 URL 필터링 업데이트 자동화

5단계 수정 내용을 저장하려면 **Save**를 클릭합니다.

변경 사항이 저장되고 Scheduling 페이지가 다시 나타납니다.

예약 작업 삭제

라이센스: 모두

Schedule View 페이지에서 수행할 수 있는 삭제 유형에는 두 가지가 있습니다. 아직 실행되지 않은 특정 1회 작업을 삭제하거나 반복 작업의 모든 인스턴스를 삭제할 수 있습니다. 한 반복 작업의 한 인스턴스를 삭제하면 해당 작업의 모든 인스턴스가 삭제됩니다. 한 번 실행하도록 예약된 작업을 삭제하면 해당 작업만 삭제됩니다.

다음 절에서는 작업을 삭제하는 방법에 대해 설명합니다.

- 한 작업의 모든 인스턴스를 삭제하려면 62-21페이지의 반복 작업 삭제을/를 참조하십시오.
- 한 작업의 단일 인스턴스를 삭제하려면 62-22페이지의 1회 작업 삭제을/를 참조하십시오.

반복 작업 삭제

라이센스: 모두

한 반복 작업의 한 인스턴스를 삭제하면 해당 작업의 모든 인스턴스가 자동으로 삭제됩니다.

반복 작업을 삭제하려면

액세스: Admin/Maint

1단계 **System > Tools > Scheduling**을 선택합니다.

Scheduling 페이지가 나타납니다.

2단계 달력에서 삭제하려는 반복 작업의 한 인스턴스를 선택합니다.

페이지가 다시 로드되고 달력 아래에 작업 테이블이 표시됩니다.

3단계 테이블에서 삭제할 반복 작업의 인스턴스를 찾고 삭제 아이콘( )을 클릭합니다.

반복 작업의 모든 인스턴스가 삭제됩니다.

1회 작업 삭제

라이센스: 모두

작업 목록을 사용하여 1회 예약 작업을 삭제하거나 전에 실행된 예약 작업의 기록을 삭제할 수 있습니다.

단일 작업을 삭제하거나, 이미 실행된 경우 작업 레코드를 삭제하려면

액세스: Admin/Maint

1단계 **System > Tools > Scheduling**을 선택합니다.

Scheduling 페이지가 나타납니다.

2단계 삭제할 작업 또는 작업이 나타나는 요일을 클릭합니다.

선택한 작업이 포함된 테이블이 나타납니다.

3단계 테이블에서 삭제할 작업을 찾고 삭제 아이콘( )을 클릭합니다.

선택한 작업의 인스턴스가 삭제됩니다.

63장

시스템 정책 관리

시스템 정책을 사용하면 FireSIGHT 시스템 어플라이언스에서 다음을 관리할 수 있습니다.

- 액세스 제어 환경 설정
- 어플라이언스 액세스 목록
- 감사 로그 설정
- 외부 인증
- 대시보드 설정
- 데이터베이스 이벤트 제한
- DNS 캐시 속성
- 메일 릴레이 호스트 및 알림 주소
- 침입 및 네트워크 분석 정책 변경 사항 추적
- 다른 언어 지정
- 사용자 지정 로그인 배너
- SNMP 폴링 설정
- 시간 동기화
- STIG 규정 준수
- 방어 센터에서 시간 서비스 제공
- 사용자 인터페이스 및 명령줄 인터페이스 시간 초과 설정
- 서버에 대한 취약성 매핑

구축의 다른 어플라이언스에 대한 것과 유사하도록 방어 센터의 여러 부분을 제어하기 위해 시스템 정책을 사용할 수 있습니다. 예를 들어 조직의 보안 정책에서 사용자가 로그인할 때 어플라이언스에 "No Unauthorized Use" 메시지를 표시하도록 요구할 수 있습니다. 시스템 정책을 사용하면, 방어 센터의 시스템 정책에서 한 번 로그인 배너를 설정한 다음 관리하는 모든 디바이스에 정책을 적용할 수 있습니다.

방어 센터에서 여러 시스템 정책을 사용하는 경우에도 혜택을 얻을 수 있습니다. 예를 들어 서로 다른 상황에서 사용하는 여러 메일 릴레이 호스트가 있거나 여러 데이터베이스 제한을 테스트하려는 경우, 단일 정책을 수정하기보다는 여러 시스템 정책을 생성하고 정책 간 전환할 수 있습니다.

구축 전체에서 유사할 수 있는 어플라이언스의 여러 부분을 제어하는 시스템 정책을 특정 어플라이언스에만 해당할 수 있는 시스템 설정과 비교해 보십시오. 자세한 내용은 64-1페이지의 어플라이언스 설정 구성을/를 참조하십시오.

자세한 내용은 다음 절을 참조하십시오.

시스템 정책 생성

라이센스: 모두

지원되는 디바이스: X-Series를 제외한 모두

시스템 정책을 생성할 때 이름과 설명을 할당합니다. 그런 다음 정책의 여러 부분을 구성하게 되는데, 그러한 각 부분을 각 절에서 설명합니다.

새 정책을 생성하는 대신, 다른 어플라이언스에서 시스템 정책을 내보내고 현재 어플라이언스로 가져올 수 있습니다. 그런 다음 가져온 정책을 필요에 맞게 수정한 다음 적용할 수 있습니다. 자세한 내용은 A-1페이지의 컨피그레이션 가져오기 및 내보내기을/를 참조하십시오.

시스템 정책을 생성하려면

액세스: Admin

1단계 **System > Local > System Policy**를 선택합니다.

System Policy 페이지가 나타납니다.

Policy Name 열에는 시스템 정책의 설명이 포함되어 있습니다. **Applied To** 열에는 정책이 적용되는 어플라이언스의 수 및 전에 적용된 정책이 변경되어서 다시 적용해야 하는 **오래된** 어플라이언스의 수가 표시됩니다.

2단계 **Create Policy**를 클릭합니다.

Create Policy 페이지가 나타납니다.

3단계 새 시스템 정책의 템플릿으로 사용할 기존 정책을 드롭다운 목록에서 선택합니다.

4단계 **New Policy Name** 필드에 새 정책의 이름을 입력합니다.

5단계 **New Policy Description** 필드에 새 정책의 설명을 입력합니다.

6단계 **Create**를 클릭합니다.

시스템 정책이 저장되고 Edit System Policy 페이지가 나타납니다. 시스템 정책의 각 부분을 구성하는 방법에 대한 자세한 내용은 다음 절을 참조하십시오.

- 63-9페이지의 어플라이언스에 대한 액세스 목록 구성
- 63-10페이지의 감사 로그 설정 구성
- 63-12페이지의 외부 인증 활성화
- 63-14페이지의 대시보드 설정 구성
- 63-15페이지의 데이터베이스 이벤트 제한 구성
- 63-17페이지의 DNS 캐시 속성 구성
- 63-18페이지의 메일 릴레이 호스트 및 알림 주소 구성

시스템 정책 수정

라이센스: 모두

지원되는 디바이스: X-Series를 제외한 모두

기존 시스템 정책을 수정할 수 있습니다. 현재 어플라이언스에 적용된 시스템 정책을 수정하는 경우 변경 사항을 저장한 후 다시 적용해야 합니다. 자세한 내용은 63-4페이지의 시스템 정책 적용을/를 참조하십시오.

기존 시스템 정책을 수정하려면

액세스: Admin

1단계 **System > Local > System Policy**를 선택합니다.

기존 시스템 정책의 목록이 포함된 System Policy 페이지가 나타납니다.

2단계 수정할 시스템 정책 옆에 있는 수정 아이콘( )을 클릭합니다.

Edit Policy 페이지가 나타납니다. 정책 이름과 정책 설명을 변경할 수 있습니다. 시스템 정책의 각 부분을 구성하는 방법에 대한 자세한 내용은 다음 절을 참조하십시오.

- 63-8페이지의 액세스 제어 정책 환경 설정 구성
- 63-9페이지의 어플라이언스에 대한 액세스 목록 구성
- 63-10페이지의 감사 로그 설정 구성
- 63-12페이지의 외부 인증 활성화
- 63-14페이지의 대시보드 설정 구성
- 63-15페이지의 데이터베이스 이벤트 제한 구성
- 63-17페이지의 DNS 캐시 속성 구성
- 63-18페이지의 메일 릴레이 호스트 및 알림 주소 구성
- 63-19페이지의 네트워크 분석 정책 환경 설정 구성
- 63-20페이지의 침입 정책 환경 설정 구성

- 63-21페이지의 다른 언어 지정
- 63-22페이지의 사용자 지정 로그인 배너 추가
- 63-23페이지의 SNMP 폴링 구성
- 63-26페이지의 시간 동기화
- 63-27페이지의 방어 센터에서 시간 서비스 제공
- 63-29페이지의 사용자 인터페이스 설정 구성
- 63-30페이지의 서버에 대한 취약성 매핑

참고 어플라이언스에 적용된 시스템 정책을 수정 중인 경우, 수정을 완료한 후 업데이트된 정책을 다시 적용해야 합니다. 63-4페이지의 시스템 정책 적용을/를 참조하십시오.

3단계 **Save Policy and Exit**를 클릭하여 변경 사항을 저장합니다. 변경 사항이 저장되고 System Policy 페이지가 나타납니다.

시스템 정책 적용

라이센스: 모두

지원되는 디바이스: X-Series를 제외한 모두

시스템 정책을 어플라이언스에 적용할 수 있습니다. 시스템 정책이 이미 적용된 경우, 다시 적용하기 전에는 변경 사항이 반영되지 않습니다.

참고 Cisco NGIPS for Blue Coat X-Series에는 시스템 정책을 적용할 수 **없습니다**.

시스템 정책을 적용하려면

액세스: Admin

1단계 **System > Local > System Policy**를 선택합니다.

System Policy 페이지가 나타납니다.

2단계 적용할 시스템 정책 옆에 있는 적용 아이콘( )을 클릭합니다.

Apply 페이지가 나타납니다.

3단계 시스템 정책을 적용할 어플라이언스를 선택합니다.

팁 그룹, 모델, 상태 정책 또는 적용된 시스템 정책별로 어플라이언스를 정렬할 수 있습니다. 개별 어플라이언스 또는 전체 그룹을 선택할 수 있습니다.

4단계 **Apply**를 클릭합니다.

System Policy 페이지가 나타납니다. 시스템 정책의 적용 상태를 알리는 메시지가 나타납니다.

시스템 정책 비교

라이센스: 모두

지원되는 디바이스: X-Series를 제외한 모두

액세스할 수 있는 시스템 정책에 대해 두 가지 시스템 정책 또는 동일한 시스템 정책의 두 가지 개정을 비교할 수 있습니다. 이를 통해 조직의 표준 준수 또는 시스템 성능 최적화를 기준으로 정책 변경 사항을 검토할 수 있습니다. 두 가지 활성 시스템 정책을 빠르게 비교하려면 **Running Configuration** 옵션을 선택할 수 있습니다. 선택적으로, 비교 후 시스템 정책 또는 시스템 정책 개정의 차이를 기록하는 PDF 보고서를 생성할 수도 있습니다.

시스템 정책 또는 시스템 정책 개정의 비교에 사용할 수 있는 두 가지 툴이 있습니다.

- 비교 보기에서는 두 시스템 정책 또는 시스템 정책 개정의 차이점만 나란히 표시합니다. 각 정책 또는 정책 개정의 이름은 비교 보기의 좌우 제목 표시줄에 나타납니다.

  이를 사용하여 웹 인터페이스에서 차이점이 강조 표시된 상태로 두 정책 개정을 모두 보고 탐색할 수 있습니다.
- 비교 보고서는 두 시스템 정책 또는 시스템 정책 개정의 차이점에 대한 기록을 생성하는데, 그 형식은 상태 정책 보고서와 비슷하지만 PDF 형식입니다.

  이를 사용하여 향후 점검을 위해 정책 비교를 저장, 복사, 인쇄, 공유할 수 있습니다.

시스템 정책 비교 보기 사용

라이센스: 모두

지원되는 디바이스: X-Series를 제외한 모두

비교 보기에서는 두 시스템 정책 또는 정책 개정을 나란히 표시하며, 각 정책 또는 정책 개정은 비교 보기의 좌우 제목 표시줄에 있는 이름으로 식별됩니다. 모든 개정의 경우, 시스템 정책 비교 보기에서는 마지막 수정 시간 및 마지막 사용자가 정책 이름의 오른쪽에 표시됩니다.

두 가지 시스템 정책 또는 정책 개정 간의 차이점이 강조 표시됩니다.

- 파란색은 강조 표시된 설정이 두 정책 또는 정책 개정에서 다름을 의미하며, 그 차이점이 빨간색 텍스트로 표시됩니다.
- 녹색은 강조 표시된 설정이 둘 중 한 정책 또는 정책 개정에만 나타남을 의미합니다.

다음 표의 작업을 수행할 수 있습니다.

표 63-1 시스템 정책 비교 보기 작업

목적	가능한 작업
개별 변경 사항 탐색	제목 표시줄 위의 **Previous** 또는 **Next**를 선택합니다. 왼쪽과 오른쪽 사이의 중앙에 있는 이중 화살표 아이콘()이 움직이고, 어떤 차이점을 보고 있는지 식별할 수 있도록 **Difference** 번호가 조정됩니다.
새 시스템 정책 비교 보기 생성	**New Comparison**을 선택합니다. **Select Comparison** 창이 나타납니다. 자세한 내용은 시스템 정책 비교 보고서 사용을/를 참조하십시오.
시스템 정책 비교 보고서 생성	**Comparison Report**를 선택합니다. 시스템 정책 비교 보고서는 시스템 정책 비교 보기와 동일한 정보를 포함하는 PDF입니다.

시스템 정책 비교 보고서 사용

라이센스: 모두

지원되는 디바이스: X-Series를 제외한 모두

시스템 정책 비교 보고서는 두 시스템 정책 또는 동일한 시스템 정책의 두 개정 간 모든 차이점을 PDF 형식의 시스템 정책 비교 보기 형태로 기록한 것입니다. 두 시스템 정책 컨피그레이션의 차이점을 더 자세히 살펴보고 조사 결과를 저장하여 배포하는 데 이 보고서를 사용할 수 있습니다.

액세스 권한이 있는 어떤 시스템 정책에 대해서도 비교 보기에서 시스템 정책 비교 보고서를 생성할 수 있습니다. 시스템 정책에 대한 변경 사항은 저장할 때까지 시스템 정책 비교 보고서에 나타나지 않습니다.

컨피그레이션에 따라, 시스템 정책 비교 보고서는 하나 이상의 섹션을 포함할 수 있습니다. 각 섹션은 동일한 형식을 사용하며 동일한 수준의 세부사항을 제공합니다. Value A 및 Value B 열은 비교 보기에서 구성한 정책 또는 정책 개정을 표시합니다.

팁 SSL, 네트워크 분석, 침입, 파일, 액세스 제어 또는 상태 정책을 비교하는 절차도 비슷합니다.

두 시스템 정책 또는 동일한 정책의 두 개정을 비교하려면

액세스: Admin

1단계 **System > Local > System Policy**를 선택합니다.

System Policy 페이지가 나타납니다.

2단계 **Compare Policies**를 클릭합니다.

Select Comparison 팝업 창이 나타납니다.

3단계 **Compare Against** 드롭다운 목록에서 원하는 비교 유형을 선택합니다.

- 두 개의 다른 정책을 비교하려면 **Other Policy**를 선택합니다.
- 동일한 정책의 두 개정을 비교하려면 **Other Revision**을 선택합니다.
- 다른 정책과 현재 활성 정책을 비교하려면 **Running Configuration**을 선택합니다.

4단계 선택한 비교 유형에 따라 다음을 선택할 수 있습니다.

- 두 개의 다른 정책을 비교할 경우 비교할 정책을 **Policy A** 및 **Policy B** 드롭다운 목록에서 각각 선택합니다.
- 동일한 정책의 두 개정을 비교하는 경우 **Policy** 드롭다운 목록에서 정책을 선택한 다음, **Revision A** 및 **Revision B** 드롭다운 목록에서 비교할 개정을 선택합니다.
- 실행 중인 컨피그레이션을 다른 정책과 비교하려는 경우 **Target/Running Configuration A** 드롭다운 목록에서 실행 중인 컨피그레이션을 선택하고 **Policy B** 드롭다운 목록에서 다른 정책을 선택합니다.

5단계 시스템 정책 비교 보기를 표시하려면 **OK**를 클릭합니다.

비교 보기가 나타납니다.

6단계 시스템 정책 비교 보고서를 생성하려면 **Comparison Report**를 클릭합니다.

시스템 정책 비교 보고서가 나타납니다. 브라우저 설정에 따라 보고서가 팝업 창에 나타날 수 있으며, 컴퓨터에 보고서를 저장하는 프롬프트가 표시될 수도 있습니다.

시스템 정책 삭제

라이센스: 모두

지원되는 디바이스: X-Series를 제외한 모두

사용 중인 경우에도 시스템 정책을 삭제할 수 있습니다. 정책이 여전히 사용되고 있는 경우, 해당 정책은 새 정책이 적용될 때까지 사용됩니다. 기본 시스템 정책을 삭제할 수 없습니다.

시스템 정책을 삭제하려면

액세스: Admin

1단계 **System > Local > System Policy**를 선택합니다.

System Policy 페이지가 나타납니다.

2단계 삭제할 시스템 정책 옆에 있는 삭제 아이콘( )을 클릭합니다. 정책을 삭제하려면 **OK**를 클릭합니다.

System Policy 페이지가 나타납니다. 정책 삭제를 확인하는 팝업 메시지가 나타납니다.

시스템 정책 구성

라이센스: 모두

지원되는 디바이스: X-Series를 제외한 모두

다양한 시스템 정책 설정을 구성할 수 있습니다. 시스템 정책의 각 부분을 구성하는 방법에 대한 자세한 내용은 다음 절을 참조하십시오.

- 63-8페이지의 액세스 제어 정책 환경 설정 구성
- 63-9페이지의 어플라이언스에 대한 액세스 목록 구성
- 63-10페이지의 감사 로그 설정 구성
- 63-12페이지의 외부 인증 활성화
- 63-14페이지의 대시보드 설정 구성
- 63-15페이지의 데이터베이스 이벤트 제한 구성
- 63-17페이지의 DNS 캐시 속성 구성
- 63-18페이지의 메일 릴레이 호스트 및 알림 주소 구성
- 63-19페이지의 네트워크 분석 정책 환경 설정 구성
- 63-20페이지의 침입 정책 환경 설정 구성
- 63-21페이지의 다른 언어 지정
- 63-22페이지의 사용자 지정 로그인 배너 추가
- 63-26페이지의 시간 동기화
- 63-27페이지의 방어 센터에서 시간 서비스 제공
- 63-29페이지의 사용자 인터페이스 설정 구성
- 63-30페이지의 서버에 대한 취약성 매핑

액세스 제어 정책 환경 설정 구성

라이센스: 보호

지원되는 디바이스: X-Series를 제외한 모두

액세스 제어 정책에서 규칙을 추가하거나 수정할 때 사용자에게 코멘트를 입력하라는 메시지가 표시되도록 시스템을 구성할 수 있습니다. 이 기능을 사용하면 사용자가 정책을 변경한 이유를 추적할 수 있습니다. 액세스 제어 규칙 변경에 대한 코멘트를 활성화하는 경우 규칙 코멘트를 선택 사항 또는 의무 사항으로 설정할 수 있습니다. 사용자가 규칙에 대한 새로운 변경 사항을 저장할 때 시스템은 코멘트를 입력하라는 메시지를 표시합니다.

사용자가 규칙을 저장하면 코멘트는 규칙의 코멘트 기록에 추가됩니다. 자세한 내용은 14-13페이지의 규칙에 코멘트 추가을/를 참조하십시오.

액세스 제어 정책 규칙 코멘트 설정을 구성하려면

액세스: Admin

1단계 **System > Local > System Policy**를 선택합니다.

System Policy 페이지가 나타납니다.

2단계 다음 옵션을 이용할 수 있습니다.

- 기존 시스템 정책에서 액세스 제어 정책 설정을 수정하려면 시스템 정책 옆에 있는 수정 아이콘( )을 클릭합니다.
- 액세스 제어 정책 설정을 새로운 시스템 정책의 일부로 구성하려면 **Create Policy**를 클릭합니다.

  63-2페이지의 시스템 정책 생성에 설명된 대로 시스템 정책에 대한 이름과 설명을 입력하고 **Save**를 클릭합니다.

어느 경우든 Access List 페이지가 나타납니다.

3단계 **Access Control Preferences**를 클릭합니다.

Access Control Preferences 페이지가 나타납니다.

4단계 다음 옵션을 이용할 수 있습니다.

- 사용자가 코멘트를 입력하지 않고도 액세스 제어 정책에서 규칙을 추가 또는 수정하도록 하려면 드롭다운 목록에서 **Disabled**를 선택합니다.
- 사용자가 액세스 제어 정책 규칙에 대한 변경 사항을 저장할 때 Description of Changes (Optional) 창을 표시하려면 드롭다운 목록에서 **Optional**을 선택합니다. 그러면 사용자는 선택적으로 변경 사항을 코멘트로 설명할 수 있습니다.
- 사용자가 액세스 제어 정책 규칙에 대한 변경 사항을 저장할 때 Description of Changes (Required) 창을 표시하려면 드롭다운 목록에서 **Required**를 선택합니다. 그러면 사용자는 저장하기 전에 변경 사항을 코멘트로 설명해야 합니다.

5단계 **Save Policy and Exit**를 클릭합니다.

시스템 정책이 업데이트됩니다. 시스템 정책을 적용할 때까지는 변경 사항이 반영되지 않습니다. 자세한 내용은 63-4페이지의 시스템 정책 적용을/를 참조하십시오.

어플라이언스에 대한 액세스 목록 구성

라이센스: 모두

지원되는 디바이스: X-Series를 제외한 모두

Access List 페이지에서는 어떤 컴퓨터가 특정 포트에서 어플라이언스에 액세스할 수 있는지를 제어할 수 있습니다. 기본적으로, 웹 인터페이스에 액세스하는 데 사용되는 포트 443(Hypertext Transfer Protocol Secure 또는 HTTPS) 및 명령줄에 액세스하는 데 사용되는 포트 22(Secure Shell 또는 SSH)는 모든 IP 주소에 대해 활성화됩니다. 또한 포트 161을 통해 SNMP 액세스를 추가할 수 있습니다. SNMP 정보를 폴링하는 데 사용할 컴퓨터에 대해서는 SNMP 액세스를 추가해야 합니다.

주의 기본적으로 어플라이언스에 대한 액세스는 제한되지 **않습니다**. 좀 더 안전한 환경에서 어플라이언스를 운영하려면 특정 IP 주소에 대해 어플라이언스에 대한 액세스를 추가하고 기본 `any` 옵션을 삭제하는 것이 좋습니다.

액세스 목록은 시스템 정책의 일부입니다. 새 시스템 정책을 생성하거나 기존 시스템 정책을 수정하여 액세스 목록을 지정할 수 있습니다. 어느 경우든 시스템 정책을 적용하기 전에는 액세스 목록이 반영되지 않습니다.

이 액세스 목록은 외부 데이터베이스 액세스를 제어하지 않습니다. 외부 데이터베이스 액세스 목록에 대한 자세한 내용은 64-7페이지의 데이터베이스에 대한 액세스 활성화을/를 참조하십시오.

액세스 목록을 구성하려면

액세스: Admin

1단계 **System > Local > System Policy**를 선택합니다.

System Policy 페이지가 나타납니다.

2단계 다음 옵션을 이용할 수 있습니다.

- 기존 시스템 정책에서 액세스 목록을 수정하려면 시스템 정책 옆에 있는 수정 아이콘( )을 클릭합니다.
- 액세스 목록을 새로운 시스템 정책의 일부로 구성하려면 **Create Policy**를 클릭합니다.

  63-2페이지의 시스템 정책 생성에 설명된 대로 시스템 정책에 대한 이름과 설명을 입력하고 **Save**를 클릭합니다.

어느 경우든 Access List 페이지가 나타납니다.

3단계 선택적으로, 현재 설정 중 하나를 삭제하려면 삭제 아이콘( )을 클릭합니다.

설정이 제거됩니다.

주의 어플라이언스 인터페이스에 연결하기 위해 현재 사용하는 IP 주소에 대한 액세스를 삭제하고 "`IP=any port=443`"에 대한 항목이 없는 경우, 정책을 적용하면 시스템에 액세스할 수 없게 됩니다.

4단계 선택적으로, 하나 이상의 IP 주소에 대한 액세스를 추가하려면 **Add Rules**를 클릭합니다.

Add IP Address 페이지가 나타납니다.

5단계 추가할 IP 주소에 따라 **IP Address** 필드에 다음을 입력할 수 있습니다.

- 정확한 IP 주소(예: `192.168.1.101`)
- CIDR 표기법을 사용한 IP 주소 블록(예: `192.168.1.1/24`)

FireSIGHT 시스템에서 CIDR을 사용하는 방법에 대한 자세한 내용은 1-19페이지의 IP 주소 표기 규칙을/를 참조하십시오.

- any - 임의의 IP 주소 지정

6단계 이러한 IP 주소를 활성화하는 데 사용할 포트를 지정하려면 **SSH**, **HTTPS**, **SNMP** 또는 이러한 옵션의 조합을 선택합니다.

7단계 **Add**를 클릭합니다.

변경 내용이 반영되어 Access List 페이지가 다시 나타납니다.

8단계 **Save Policy and Exit**를 클릭합니다.

시스템 정책이 업데이트됩니다. 시스템 정책을 적용할 때까지는 변경 사항이 반영되지 않습니다. 자세한 내용은 63-4페이지의 시스템 정책 적용을/를 참조하십시오.

감사 로그 설정 구성

라이센스: 모두

지원되는 디바이스: X-Series를 제외한 모두

어플라이언스가 감사 로그를 외부 호스트로 스트리밍하도록 시스템 정책을 구성할 수 있습니다.

참고 외부 호스트가 작동해야 하며 감사 로그를 보내는 어플라이언스에서 액세스할 수 있어야 합니다.

전송하는 호스트 이름은 전송된 정보의 일부입니다. 기능(facility), 심각도 및 선택적인 태그로 감사 로그 스트림을 식별할 수도 있습니다. 시스템 정책을 적용할 때까지는 어플라이언스에서 감사 로그를 전송하지 않습니다.

이 기능이 활성화된 정책을 적용하고 목적지 호스트가 감사 로그를 허용하도록 구성되면 syslog 메시지가 전송됩니다. 다음은 출력 구조의 예입니다.

```
Date Time Host [Tag] Sender: [User_Name]@[User_IP], [Subsystem], [Action]
```

여기에서는 로컬 날짜, 시간 및 호스트 이름이 괄호로 표시된 선택적인 태그 앞에 오고, 전송하는 디바이스 이름이 감사 로그 메시지 앞에 옵니다.

예를 들면 다음과 같습니다.

```
Mar 01 14:45:24 localhost [TAG] Dev-DC3000: admin@10.1.1.2, Operations > Monitoring, Page
View
```

감사 로그 설정을 구성하려면

액세스: Admin

1단계 **System > Local > System Policy**를 선택합니다.

System Policy 페이지가 나타납니다.

2단계 다음 옵션을 이용할 수 있습니다.

- 기존 시스템 정책에서 감사 로그 설정을 수정하려면 시스템 정책 옆에 있는 수정 아이콘()을 클릭합니다.
- 감사 로그 설정을 새로운 시스템 정책의 일부로 구성하려면 **Create Policy**를 클릭합니다.

63-2페이지의 시스템 정책 생성에 설명된 대로 시스템 정책에 대한 이름과 설명을 입력하고 **Save**를 클릭합니다.

어느 경우든 Access List 페이지가 나타납니다.

3단계 **Audit Log Settings**를 클릭합니다.

Audit Log Settings 페이지가 나타납니다.

4단계 **Send Audit Log to Syslog** 드롭다운 메뉴에서 **Enabled**를 선택합니다. (기본 설정은 **Disabled**입니다.)

5단계 **Host** 필드에서 호스트의 IP 주소 또는 정규화된 도메인 이름을 사용하여 감사 정보에 대한 목적지 호스트를 지정합니다. 기본 포트(514)가 사용됩니다.

주의 감사 로그를 수신하기 위해 구성한 컴퓨터가 원격 메시지를 허용하도록 설정되지 않은 경우, 호스트에서 감사 로그를 허용하지 않습니다.

6단계 **Facility** 필드에서 syslog 기능을 선택합니다.

7단계 **Severity** 필드에서 심각도를 선택합니다.

8단계 선택적으로, **Tag (optional)** 필드에 참조 태그를 삽입합니다.

9단계 외부 HTTP 서버에 일반 감사 로그 업데이트를 전송하려면 **Send Audit Log to HTTP Server** 드롭다운 목록에서 **Enabled**를 선택합니다. 기본 설정은 **Disabled**입니다.

10단계 감사 정보를 전송할 URL을 **URL to Post Audit** 필드에 지정합니다. 다음과 같은 HTTP POST 변수를 예상하는 수신 대기 프로그램에 해당하는 URL을 입력해야 합니다.

- `subsystem`
- `actor`
- `event_type`
- `message`
- `action_source_ip`
- `action_destination_ip`
- `result`
- `time`
- `tag`(위와 같이 정의된 경우)

주의 암호화된 게시를 허용하려면 HTTPS URL을 사용해야 합니다. 외부 URL로 감사 정보를 전송하면 시스템 성능에 영향을 줄 수 있습니다.

11단계 **Save Policy and Exit**를 클릭합니다.

시스템 정책이 업데이트됩니다. 변경 사항을 반영하려면 방어 센터 및 관리되는 디바이스에 시스템 정책을 적용해야 합니다. 자세한 내용은 63-4페이지의 시스템 정책 적용을/를 참조하십시오.

외부 인증 활성화

라이센스: 모두

지원되는 디바이스: X-Series를 제외한 모두

일반적으로 사용자가 어플라이언스에 로그인하면, 어플라이언스는 자격 증명을 어플라이언스의 로컬 데이터베이스에 저장된 사용자 계정과 비교하여 사용자 자격 증명을 확인합니다. 그러나 외부 인증 서버를 참조하는 인증 객체를 생성하는 경우, 방어 센터 또는 관리되는 디바이스에 로그인한 사용자가 해당 서버에 대해 인증을 받도록(로컬 데이터베이스를 사용하는 대신) 시스템 정책의 외부 인증서를 활성화할 수 있습니다.

어플라이언스에 대해 외부 인증이 활성화된 시스템 정책을 적용하면, 어플라이언스는 LDAP 또는 RADIUS 서버의 사용자에 대해 사용자 자격 증명을 확인합니다. 또한 사용자의 로컬 내부 인증이 활성화되었는데 내부 데이터베이스에 사용자 자격 증명이 없으면, 어플라이언스는 일치하는 자격 증명 집합을 외부 서버에서 확인합니다. 여러 시스템에서 사용자의 사용자 이름이 동일하면 모든 서버에서 모든 비밀번호가 작동합니다. 그러나 사용 가능한 외부 인증 서버에서 인증이 실패하면 어플라이언스는 로컬 데이터베이스를 다시 확인하지 않습니다.

외부 인증을 활성화하는 경우, 외부에서 계정이 인증되는 사용자에 대해 기본 사용자 역할을 설정할 수 있습니다. 역할을 결합할 수 있는 한 여러 역할을 선택할 수 있습니다. 예를 들어 회사의 Network Security 그룹의 사용자만 검색하는 외부 인증을 활성화하는 경우, Security Analyst 역할을 포함하도록 기본 사용자 역할을 설정할 수 있습니다. 그러면 추가 사용자 컨피그레이션 없이도 사용자가 수집된 이벤트 데이터에 액세스할 수 있습니다. 그러나 외부 인증에서 보안 그룹 외에도 다른 직원에 대한 레코드를 검색하는 경우, 기본 역할을 선택하지 않고 그대로 둘 수 있습니다. 사용 가능한 사용자 역할에 대한 자세한 내용은 61-4페이지의 사용자 권한 이해을/를 참조하십시오.

액세스 역할을 선택하지 않으면 사용자는 로그인할 수 있지만 어떤 기능에도 액세스할 수 없습니다. 사용자가 로그인을 시도하면 해당 계정이 User Management 페이지에 나열됩니다. 여기에서 추가 권한을 허용하도록 계정 설정을 수정할 수 있습니다. 사용자 계정 수정에 대한 자세한 내용은 61-54페이지의 사용자 권한 및 옵션 수정을/를 참조하십시오.

팁 하나의 사용자 역할을 사용하도록 시스템 정책을 구성하고 적용한 다음 나중에 다른 기본 사용자 역할을 사용하도록 정책을 수정하고 다시 적용하면, 계정을 수정하거나 삭제하고 다시 생성하기 전에는 수정 전에 생성된 사용자 계정에 첫 번째 사용자 역할이 그대로 유지됩니다.

셸 액세스를 위해 LDAP 서버에서 성공적으로 인증할 수 있는 사용자 집합을 지정하려면, 시스템 정책에서 외부 인증을 활성화하기 전에 LDAP 인증 객체 내에 셸 액세스 특성 및 기타 설정을 지정해야 합니다. 자세한 내용은 61-18페이지의 LDAP 관련 매개 변수 구성 및 61-9페이지의 셸 액세스 이해을/를 참조하십시오.

CAC 인증 및 권한 부여를 위해 LDAP 서버에서 성공적으로 인증할 수 있는 사용자 집합을 지정하려면, 시스템 정책에서 외부 인증을 활성화하기 전에 LDAP 인증 객체에서 UI 액세스 특성, 사용자 이름 템플릿 및 기타 설정을 지정해야 합니다. 자세한 내용은 61-18페이지의 LDAP 관련 매개 변수 구성 및 61-9페이지의 CAC를 사용하는 LDAP 인증 이해을/를 참조하십시오.

참고 어플라이언스에서 셸 액세스와 CAC 인증을 모두 활성화하려면 **반드시** 별도의 인증 객체를 생성하고 시스템 정책에서 따로 활성화해야 합니다.

인증 객체 사용자 지정을 완료한 후에는 방어 센터의 시스템 정책에서 외부 인증을 활성화한 다음 관리되는 디바이스에 해당 정책을 푸시해야 합니다. 디바이스에 정책을 적용한 후에는 외부에서 인증된 대상 사용자가 디바이스에 로그인할 수 있습니다. 외부 인증 설정을 변경하려면 방어 센터에서 시스템 정책을 수정한 후 디바이스에 정책을 다시 적용해야 합니다. 관리되는 디바이스에서 인증을 비활성화하려면 방어 센터의 시스템 정책에서 비활성화하고 디바이스에 푸시할 수 있습니다.

물리적 및 가상 방어 센터와 관리되는 디바이스에서만 외부 인증을 활성화할 수 있습니다. 시스템 정책을 적용하여 외부 인증을 활성화하는 것은 Cisco NGIPS for Blue Coat X-Series에서 지원되지 않습니다.

내부에서 인증되는 사용자가 로그인을 시도하면 어플라이언스는 해당 사용자가 로컬 사용자 데이터베이스에 있는지를 우선 확인합니다. 사용자가 있으면 어플라이언스는 로컬 데이터베이스에서 사용자 이름과 비밀번호를 확인합니다. 일치가 확인되면 로그인이 성공합니다. 그러나 로그인이 실패하고 외부 인증이 활성화되면 어플라이언스는 시스템 정책에 명시된 인증 순서에 따라 각 외부 인증 서버에서 사용자를 확인합니다. 사용자 이름 및 비밀번호가 외부 서버의 결과와 일치하면 어플라이언스는 사용자를 해당 인증 객체에 대한 기본 권한이 있는 외부 사용자로 변경합니다.

외부 사용자가 로그인을 시도하면 어플라이언스는 외부 인증 서버에 대해 사용자 이름과 비밀번호를 확인합니다. 일치가 확인되면 로그인이 성공합니다. 로그인이 실패하면 사용자 로그인 시도가 거절됩니다. 외부 사용자는 로컬 데이터베이스의 사용자 목록을 기준으로 인증할 수 없습니다. 사용자가 새로운 외부 사용자이면 외부 인증 객체로부터의 기본 권한과 함께 로컬 데이터베이스에 외부 사용자 계정이 생성됩니다.

외부 서버에서 사용자의 인증을 활성화하려면

액세스: Admin

1단계 **System > Local > System Policy**를 선택합니다.

System Policy 페이지가 나타납니다.

2단계 다음 옵션을 이용할 수 있습니다.

- 기존 시스템 정책에서 외부 인증 설정을 수정하려면 시스템 정책 옆에 있는 수정 아이콘()을 클릭합니다.
- 외부 인증 설정을 새로운 시스템 정책의 일부로 구성하려면 **Create Policy**를 클릭합니다.

  63-2페이지의 시스템 정책 생성에 설명된 대로 시스템 정책에 대한 이름과 설명을 입력하고 **Save**를 클릭합니다.

어느 경우든 Access List 페이지가 나타납니다.

3단계 **External Authentication**을 클릭합니다.

External Authentication 페이지가 나타납니다.

4단계 **Status** 드롭다운 목록에서 **Enabled**를 선택합니다.

5단계 외부에서 인증된 사용자에게 허용할 기본 권한을 정의하기 위한 사용자 역할을 **Default User Role** 드롭다운 목록에서 선택합니다.

팁 여러 기본 사용자 역할을 선택하려면 Ctrl을 누른 상태에서 선택합니다. Security Analyst 역할 및 해당 Security Analyst(Read Only) 역할을 모두 선택할 수 있지만 Security Analyst 역할만 적용됩니다.

6단계 외부 서버를 사용하여 셸 액세스 계정도 인증하려면 **Shell Authentication** 드롭다운 목록에서 **Enabled**를 선택합니다.

7단계 CAC 인증 및 권한 부여를 활성화하려면 **CAC Authentication** 드롭다운 목록에서 사용 가능한 CAC 인증 객체를 선택합니다.

CAC 인증 및 권한 부여에 대한 완전한 절차는 61-9페이지의 CAC를 사용하는 LDAP 인증 이해을/를 참조하십시오.

8단계 사전 구성된 인증 객체의 사용을 활성화하려면 객체 옆에 있는 확인란을 선택합니다. 외부 인증을 활성화하려면 하나 이상의 인증 객체를 **반드시** 선택해야 합니다.

팁 6단계에서 셸 인증을 활성화한 경우 셸 액세스를 허용하도록 구성된 인증 객체를 **반드시** 선택해야 합니다. 동일한 시스템 정책에서 셸 액세스와 CAC 인증을 관리하려면 **반드시** 서로 다른 인증 객체를 사용해야 합니다. 자세한 내용은 61-9페이지의 셸 액세스 이해 및 61-9페이지의 CAC를 사용하는 LDAP 인증 이해을/를 참조하십시오.

9단계 선택적으로, 인증 요청이 발생할 때 인증 서버에 액세스하는 순서를 변경하려면 위쪽 및 아래쪽 화살표를 사용합니다.

참고 셸 액세스 사용자는 프로필 순서에서 인증 객체 순위가 가장 높은 서버에 **대해서만** 인증할 수 있습니다.

10단계 **Save Policy and Exit**를 클릭합니다.

시스템 정책이 업데이트됩니다. 변경 사항을 반영하려면 방어 센터 및 관리되는 디바이스에 시스템 정책을 적용해야 합니다. 자세한 내용은 63-4페이지의 시스템 정책 적용을/를 참조하십시오.

대시보드 설정 구성

라이센스: 모두

지원되는 디바이스: X-Series를 제외한 모두

Custom Analysis 위젯이 대시보드에서 활성화되도록 시스템 정책을 구성할 수 있습니다. 대시보드는 FireSIGHT 시스템의 여러 부분에 대한 통찰력을 제공하는 소규모의 자족적 구성 요소인 위젯을 사용하여 현재 시스템 상태에 대한 간략한 보기를 제공합니다.

Custom Analysis 위젯을 사용하면 어플라이언스의 데이터베이스에서 사용자 구성 가능한 유연한 이벤트 쿼리를 기반으로 이벤트를 시각적으로 표현할 수 있습니다. 사용자 지정 위젯을 사용하는 방법에 대한 자세한 내용은 55-11페이지의 Custom Analysis 위젯 이해을/를 참조하십시오.

Custom Analysis 위젯을 활성화하려면

액세스: Admin

1단계 **System > Local > System Policy**를 선택합니다.

System Policy 페이지가 나타납니다.

2단계 다음 옵션을 이용할 수 있습니다.

- 기존 시스템 정책에서 대시보드 설정을 수정하려면 시스템 정책 옆에 있는 수정 아이콘( )을 클릭합니다.
- 대시보드 설정을 새로운 시스템 정책의 일부로 구성하려면 **Create Policy**를 클릭합니다. 63-2페이지의 시스템 정책 생성에 설명된 대로 시스템 정책에 대한 이름과 설명을 입력하고 **Save**를 클릭합니다.

어느 경우든 Access List 페이지가 나타납니다.

3단계 **Dashboard**를 클릭합니다.

Dashboard Settings 페이지가 나타납니다.

4단계 사용자가 Custom Analysis 위젯을 대시보드에 추가하도록 허용하려면 **Enable Custom Analysis Widgets** 확인란을 선택합니다. 사용자의 위젯 사용을 금지하려면 확인란의 선택을 취소합니다.

5단계 **Save Policy and Exit**를 클릭합니다.

시스템 정책이 업데이트됩니다. 시스템 정책을 적용할 때까지는 변경 사항이 반영되지 않습니다. 자세한 내용은 63-4페이지의 시스템 정책 적용을/를 참조하십시오.

데이터베이스 이벤트 제한 구성

라이센스: 모두

지원되는 디바이스: X-Series를 제외한 모두

데이터베이스 페이지를 사용하여 방어 센터에서 저장할 수 있는 각 이벤트 유형의 최대 수를 지정합니다. 감사 레코드에 대한 설정은 관리되는 디바이스에도 적용됩니다. 성능을 높이려면 정기적으로 작업하는 이벤트 수에 대한 이벤트 제한을 조정해야 합니다. 일부 이벤트 유형의 경우 스토리지를 비활성화할 수 있습니다. 다음 표에는 각 이벤트 유형에 대해 저장할 수 있는 최소 및 최대 레코드 수가 나열되어 있습니다.

표 63-2 데이터베이스 이벤트 제한 수

이벤트 유형	이벤트 개수 상한	이벤트 개수 하한
침입 이벤트	250만(DC500) 1,000만(DC1000, 가상 방어 센터) 2,000만(DC750) 3,000만(DC1500) 6,000만(DC2000) 1억(DC3000) 1억 5,000만(DC3500) 3억(DC4000)	10,000
검색 이벤트	1,000만 2,000만(DC2000, DC4000)	0(스토리지 비활성화)
연결 이벤트 보안 인텔리전스 이벤트	1,000만(DC500, DC1000, 가상 방어 센터) 5,000만(DC750) 1억(DC1500, DC3000) 3억(DC2000) 5억(DC3500) 10억(DC4000) 이벤트 개수 상한은 연결 이벤트와 보안 인텔리전스 이벤트 간에 공유되며, 두 이벤트에 구성된 최대값의 총합은 이벤트 개수 상한을 초과할 수 없습니다.	0(스토리지 비활성화)
연결 요약/(집계된 연결 이벤트)	1,000만(DC500, DC1000, 가상 방어 센터) 5,000만(DC750) 1억(DC1500, DC3000) 3억(DC2000) 5억(DC3500) 10억(DC4000)	0(스토리지 비활성화)
상관관계 및 규정 준수 화이트리스트 이벤트	100만 200만(DC2000, DC4000)	1

표 63-2 데이터베이스 이벤트 제한 수 (계속)

이벤트 유형	이벤트 개수 상한	이벤트 개수 하한
악성코드 이벤트	1,000만 2,000만(DC2000, DC4000)	10,000
파일 이벤트	1,000만 2,000만(DC2000, DC4000)	0(스토리지 비활성화)
상태 이벤트	100만	0(스토리지 비활성화)
감사 레코드	100,000	1
교정 상태 이벤트	1,000만	1
네트워크에 있는 호스트의 화이트리스트 위반 기록	30일 위반 기록	일일 이력
사용자 활동 (사용자 이벤트)	1,000만	1
사용자 로그인 (사용자 기록)	1,000만	1
규칙 업데이트 가져오기 로그 레코드	100만	1

침입 이벤트 데이터베이스의 이벤트 수가 최대 수를 초과할 경우, 데이터베이스가 이벤트 제한 수 내로 돌아오기 전까지 가장 오래된 이벤트 및 패킷 파일이 삭제됩니다. 이벤트가 자동으로 삭제될 때 자동 이메일 알림을 생성하는 방법에 대한 자세한 내용은 63-18페이지의 메일 릴레이 호스트 및 알림 주소 구성을/를 참조하십시오.

검색 및 사용자 데이터베이스를 수동으로 삭제하는 방법에 대한 자세한 내용은 B-1페이지의 데이터베이스에서 검색 데이터 삭제을/를 참조하십시오.

또한 데이터베이스에서 침입 이벤트 및 감사 레코드가 삭제될 때 알림을 받을 이메일 주소를 구성할 수 있습니다.

데이터베이스에서 레코드의 최대 수를 구성하려면

액세스: Admin

1단계 **System > Local > System Policy**를 선택합니다.

System Policy 페이지가 나타납니다.

2단계 다음 옵션을 이용할 수 있습니다.

- 기존 시스템 정책에서 데이터베이스 설정을 수정하려면 시스템 정책 옆에 있는 수정 아이콘()을 클릭합니다.
- 데이터베이스 설정을 새로운 시스템 정책의 일부로 구성하려면 **Create Policy**를 클릭합니다.

  63-2페이지의 시스템 정책 생성에 설명된 대로 시스템 정책에 대한 이름과 설명을 입력하고 **Save**를 클릭합니다.

어느 경우든 Access Control Preferences 페이지가 나타납니다.

3단계 **Database**를 클릭합니다.

Database 페이지가 나타납니다.

4단계 각 데이터베이스에 대해 저장할 레코드의 수를 입력합니다.

각 데이터베이스가 유지 관리할 레코드 수에 대한 정보는 데이터베이스 이벤트 제한 수 표를 참조하십시오.

5단계 선택적으로, 침입 이벤트, 검색 이벤트, 감사 레코드, 보안 인텔리전스 데이터 또는 URL 필터링 데이터가 어플라이언스의 데이터베이스에서 삭제될 때 알림을 받을 이메일 주소를 **Data Pruning Notification Address** 필드에 입력합니다.

이메일 서버도 구성해야 합니다. 자세한 내용은 63-18페이지의 메일 릴레이 호스트 및 알림 주소 구성을/를 참조하십시오.

6단계 **Save Policy and Exit**를 클릭합니다.

시스템 정책이 업데이트됩니다. 시스템 정책을 적용할 때까지는 변경 사항이 반영되지 않습니다. 자세한 내용은 63-4페이지의 시스템 정책 적용을/를 참조하십시오.

DNS 캐시 속성 구성

라이센스: 모두

지원되는 디바이스: X-Series를 제외한 모두

Network 페이지에서 DNS 서버를 구성한 경우, 이벤트 보기 페이지에서 IP 주소를 자동으로 확인하도록 어플라이언스를 구성할 수 있습니다. 사용자가 Administrator 역할을 할당한 경우 어플라이언스에서 수행하는 DNS 캐싱의 기본 속성도 구성할 수 있습니다. DNS 캐싱을 구성하면 추가 조회를 수행하지 않고도 전에 확인한 IP 주소를 식별할 수 있습니다. 이렇게 하면 네트워크의 트래픽 양을 줄이고, IP 주소 확인이 활성화된 경우 이벤트 페이지의 표시 속도를 높일 수 있습니다.

DNS 캐시 속성을 구성하려면

액세스: Admin

1단계 **System > Local > System Policy**를 선택합니다.

System Policy 페이지가 나타납니다.

2단계 다음 옵션을 이용할 수 있습니다.

- 기존 시스템 정책에서 DNS 캐시 설정을 수정하려면 시스템 정책 옆에 있는 수정 아이콘( )을 클릭합니다.
- DNS 캐시 설정을 새로운 시스템 정책의 일부로 구성하려면 **Create Policy**를 클릭합니다.

  63-2페이지의 시스템 정책 생성에 설명된 대로 시스템 정책에 대한 이름과 설명을 입력하고 **Save**를 클릭합니다.

어느 경우든 Access List 페이지가 나타납니다.

3단계 **DNS Cache**를 클릭합니다.

DNS Cache 페이지가 나타납니다.

4단계 캐싱을 활성화하려면 **DNS Resolution Caching** 드롭다운 목록에서 **Enabled**를 선택합니다. 캐싱을 비활성화하려면 **Disabled**를 선택합니다.

참고 DNS 확인 캐싱은 전에 확인된 DNS 조회의 캐싱을 허용하는 시스템 전체의 설정입니다. 사용자 계정 단위 기반으로 IP 주소 확인을 구성하려면 사용자는 **User Preferences** 메뉴에서 **Event View Settings**를 선택하고, **Resolve IP Addresses**를 활성화하고, **Save**를 클릭합니다. DNS 주소 구성에 대한 자세한 내용은 64-8페이지의 관리 인터페이스 구성을/를 참조하십시오. 이벤트 보기 환경 설정에 대한 자

세한 내용은 71-3페이지의 이벤트 보기 설정 구성을/를 참조하십시오.

5단계 DNS 항목이 제거되어 비활성화되기 전 메모리에 캐시되어 머무는 시간(분)을 **DNS Cache Timeout (in minutes)** 필드에 입력합니다.

기본 설정은 300분(5시간)입니다.

6단계 **Save Policy and Exit**를 클릭합니다.

시스템 정책이 업데이트됩니다. 시스템 정책을 적용할 때까지는 변경 사항이 반영되지 않습니다. 자세한 내용은 63-4페이지의 시스템 정책 적용을/를 참조하십시오.

주의 어플라이언스에 대해 DNS 캐싱이 활성화되더라도, User Preferences 메뉴에서 액세스할 수 있는 Events 페이지에서 구성하지 않는 한 IP 주소 확인은 사용자 단위 기반으로 활성화되지 않습니다.

메일 릴레이 호스트 및 알림 주소 구성

라이센스: 모두

지원되는 디바이스: X-Series를 제외한 모두

다음과 같이 하려는 경우 메일 호스트를 구성해야 합니다.

- 이벤트 기반 보고서 이메일 전송
- 예약 작업에 대한 상태 보고서 이메일 전송
- 변경 조정 보고서 이메일 전송
- 데이터 삭제 알림 이메일 전송
- 검색 이벤트, 영향 플래그 및 상관관계 이벤트 알림에 이메일 사용
- 침입 이벤트 알림에 이메일 사용
- 상태 알림에 이메일 사용

어플라이언스와 메일 릴레이 호스트 간 통신에 사용할 암호화 방법을 선택할 수 있으며, 필요 시 메일 서버용 인증 자격 증명을 제공할 수 있습니다. 설정을 구성한 후 제공된 설정을 사용하여 어플라이언스와 메일 서버 간 연결을 테스트할 수 있습니다.

메일 릴레이 호스트를 구성하려면

액세스: Admin

1단계 **System > Local > System Policy**를 선택합니다.

System Policy 페이지가 나타납니다.

2단계 다음 옵션을 이용할 수 있습니다.

- 기존 시스템 정책에서 이메일 설정을 수정하려면 시스템 정책 옆에 있는 수정 아이콘( )을 클릭합니다.
- 이메일 설정을 새로운 시스템 정책의 일부로 구성하려면 **Create Policy**를 클릭합니다.

  63-2페이지의 시스템 정책 생성에 설명된 대로 시스템 정책에 대한 이름과 설명을 입력하고 **Save**를 클릭합니다.

어느 경우든 Access List 페이지가 나타납니다.

3단계 **Email Notification**을 클릭합니다.

Configure Email Notification 페이지가 나타납니다.

4단계 사용할 메일 서버의 호스트 이름 또는 IP 주소를 **Mail Relay Host** 필드에 입력합니다.

참고 입력하는 메일 호스트는 어플라이언스에서의 액세스를 허용해야 합니다.

5단계 이메일 서버에서 사용할 포트 번호를 **Port Number** 필드에 입력합니다. 일반적인 포트에는 25(암호화를 사용하지 않음), 465(SSLv3 사용 시), 587(TLS 사용 시)이 포함됩니다.

6단계 암호화 방법을 선택할 때 다음과 같은 옵션이 있습니다.

- Transport Layer Security를 사용하는 메일 서버와 어플라이언스 간 통신을 암호화하려면 **Encryption Method** 드롭다운 목록에서 **TLS**를 선택합니다.
- Secure Socket Layers를 사용하는 메일 서버와 어플라이언스 간 통신을 암호화하려면 **Encryption Method** 드롭다운 목록에서 **SSLv3**을 선택합니다.
- 메일 서버와 어플라이언스 간 암호화되지 않은 통신을 허용하려면 **Encryption Method** 드롭다운 목록에서 **None**을 선택합니다.

어플라이언스와 메일 서버 간 암호화된 통신에는 인증서 검증이 필요하지 않습니다.

7단계 어플라이언스에서 전송하는 메시지에 대한 소스 이메일 주소로 사용할 유효한 이메일 주소를 **From Address** 필드에 입력합니다.

8단계 선택적으로, 메일 서버에 연결할 때 사용자 이름과 비밀번호를 제공하려면 **Use Authentication**을 선택합니다. **Username** 필드에 사용자 이름을 입력합니다. **Password** 필드에 비밀번호를 입력합니다.

9단계 구성된 메일 서버를 사용하여 테스트 이메일을 전송하려면 **Test Mail Server Settings**를 클릭합니다.

버튼 옆에 테스트의 성공 또는 실패를 나타내는 메시지가 나타납니다.

10단계 **Save Policy and Exit**를 클릭합니다.

시스템 정책이 업데이트됩니다. 시스템 정책을 적용할 때까지는 변경 사항이 반영되지 않습니다. 자세한 내용은 63-4페이지의 시스템 정책 적용을/를 참조하십시오.

네트워크 분석 정책 환경 설정 구성

라이센스: 보호

지원되는 디바이스: X-Series를 제외한 모두

사용자가 네트워크 분석 정책을 수정할 때 코멘트를 입력하라는 메시지를 표시하도록 시스템을 구성할 수 있습니다. 이 기능을 사용하면 사용자가 정책을 변경한 이유를 추적할 수 있습니다. 네트워크 분석 정책 변경에 대한 코멘트를 활성화하는 경우 코멘트를 선택 사항 또는 의무 사항으로 설정할 수 있습니다. 변경 사항 설명은 감사 로그에 기록됩니다.

감사 로그에 모든 네트워크 분석 정책 변경 사항을 기록할 수도 있습니다. 감사 로그에 대한 자세한 내용은 69-1페이지의 감사 레코드 관리을/를 참조하십시오.

네트워크 분석 정책 코멘트 설정을 구성하려면

액세스: Admin

1단계 **System > Local > System Policy**를 선택합니다.

System Policy 페이지가 나타납니다.

2단계 다음 옵션을 이용할 수 있습니다.

- 기존 시스템 정책에서 네트워크 분석 정책 환경 설정을 수정하려면 시스템 정책 옆에 있는 수정 아이콘()을 클릭합니다.
- 네트워크 분석 정책 환경 설정을 새로운 시스템 정책의 일부로 구성하려면 **Create Policy**를 클릭합니다.

  63-2페이지의 시스템 정책 생성에 설명된 대로 시스템 정책에 대한 이름과 설명을 입력하고 **Save**를 클릭합니다.

어느 경우든 Access List 페이지가 나타납니다.

3단계 **Network Analysis Policy Preferences**를 클릭합니다.

Network Analysis Policy Preferences 페이지가 나타납니다.

4단계 **Comments on policy change** 드롭다운 목록에서 다음 옵션을 선택할 수 있습니다.

- 사용자가 변경 사항 설명을 입력하지 않고 네트워크 분석 정책을 수정하도록 허용하려면 **Disabled**를 선택합니다.
- 사용자가 네트워크 분석 정책에 변경 사항을 저장할 때 Description of Changes 창을 표시하려면 **Optional**을 선택합니다. 그러면 사용자는 선택적으로 변경 사항을 코멘트로 설명할 수 있습니다.
- 사용자가 네트워크 분석 정책에 변경 사항을 저장할 때 Description of Changes 창을 표시하려면 **Required**를 선택합니다. 그러면 사용자는 저장하기 전에 변경 사항을 코멘트로 설명해야 합니다.

5단계 선택적으로, 모든 네트워크 분석 정책 변경 사항을 감사 로그에 기록하도록 하려면 **Write changes in Network Analysis Policy to audit log**를 선택합니다.

6단계 **Save Policy and Exit**를 클릭합니다.

시스템 정책이 업데이트됩니다. 시스템 정책을 적용할 때까지는 변경 사항이 반영되지 않습니다. 자세한 내용은 63-4페이지의 시스템 정책 적용을/를 참조하십시오.

침입 정책 환경 설정 구성

라이센스: 보호

지원되는 디바이스: X-Series를 제외한 모두

사용자가 침입 정책을 수정할 때 코멘트를 입력하라는 메시지를 표시하도록 시스템을 구성할 수 있습니다. 이 기능을 사용하면 사용자가 정책을 변경한 이유를 추적할 수 있습니다. 침입 정책 변경에 대한 코멘트를 활성화하는 경우 코멘트를 선택 사항 또는 의무 사항으로 설정할 수 있습니다. 변경 사항 설명은 감사 로그에 기록됩니다.

감사 로그에 모든 침입 정책 변경 사항을 기록할 수도 있습니다. 감사 로그에 대한 자세한 내용은 69-1페이지의 감사 레코드 관리을/를 참조하십시오.

침입 정책 코멘트 설정을 구성하려면

액세스: Admin

1단계 **System > Local > System Policy**를 선택합니다.

System Policy 페이지가 나타납니다.

2단계 다음 옵션을 이용할 수 있습니다.

- 기존 시스템 정책에서 침입 정책 환경 설정을 수정하려면 시스템 정책 옆에 있는 수정 아이콘( )을 클릭합니다.
- 침입 정책 환경 설정을 새로운 시스템 정책의 일부로 구성하려면 **Create Policy**를 클릭합니다.

  63-2페이지의 시스템 정책 생성에 설명된 대로 시스템 정책에 대한 이름과 설명을 입력하고 **Save**를 클릭합니다.

어느 경우든 Access List 페이지가 나타납니다.

3단계 **Intrusion Policy Preferences**를 클릭합니다.

Intrusion Policy Preferences 페이지가 나타납니다.

4단계 **Comments on policy change** 드롭다운 목록에서 다음 옵션을 선택할 수 있습니다.

- 사용자가 변경 사항 설명을 입력하지 않고 침입 정책을 수정하도록 허용하려면 **Disabled**를 선택합니다.
- 사용자가 침입 정책에 변경 사항을 저장할 때 Description of Changes 창을 표시하려면 **Optional**을 선택합니다. 그러면 사용자는 선택적으로 변경 사항을 코멘트로 설명할 수 있습니다.
- 사용자가 침입 정책에 변경 사항을 저장할 때 Description of Changes 창을 표시하려면 **Required**를 선택합니다. 그러면 사용자는 저장하기 전에 변경 사항을 코멘트로 설명해야 합니다.

5단계 선택적으로, 모든 침입 정책 변경 사항을 감사 로그에 기록하도록 하려면 **Write changes in Intrusion Policy to audit log**를 선택합니다.

6단계 **Save Policy and Exit**를 클릭합니다.

시스템 정책이 업데이트됩니다. 시스템 정책을 적용할 때까지는 변경 사항이 반영되지 않습니다. 자세한 내용은 63-4페이지의 시스템 정책 적용을/를 참조하십시오.

다른 언어 지정

라이센스: 모두

지원되는 디바이스: X-Series를 제외한 모두

웹 인터페이스에 대해 다른 언어를 지정하려면 Language 페이지를 사용할 수 있습니다.

주의 여기서 선택하는 언어는 어플라이언스에 로그인하는 모든 사용자에 대한 웹 인터페이스에 사용됩니다.

사용자 인터페이스에 다른 언어를 선택하려면

액세스: Admin

1단계 **System > Local > System Policy**를 선택합니다.

System Policy 페이지가 나타납니다.

2단계 다음 옵션을 이용할 수 있습니다.

- 기존 시스템 정책에서 언어 설정을 수정하려면 시스템 정책 옆에 있는 수정 아이콘( )을 클릭합니다.
- 언어 설정을 새로운 시스템 정책의 일부로 구성하려면 **Create Policy**를 클릭합니다.

  63-2페이지의 시스템 정책 생성에 설명된 대로 시스템 정책에 대한 이름과 설명을 입력하고 **Save**를 클릭합니다.

어느 경우든 Access List 페이지가 나타납니다.

3단계 **Language**를 클릭합니다.

Language 페이지가 나타납니다.

4단계 사용하려는 언어를 선택합니다.

5단계 **Save Policy and Exit**를 클릭합니다.

시스템 정책이 업데이트됩니다. 시스템 정책을 적용할 때까지는 변경 사항이 반영되지 않습니다. 자세한 내용은 63-4페이지의 시스템 정책 적용을/를 참조하십시오.

사용자 지정 로그인 배너 추가

라이센스: 모두

지원되는 디바이스: X-Series를 제외한 모두

사용자가 SSH를 사용하여 어플라이언스에 로그인할 때와 웹 인터페이스의 로그인 페이지에 나타나는 사용자 지정 배너를 생성할 수 있습니다. 배너에는 보다 작음 기호(<) 및 보다 큼 기호(>)를 제외한 인쇄 가능한 모든 문자를 포함할 수 있습니다.

사용자 지정 배너를 추가하려면

액세스: Admin

1단계 **System > Local > System Policy**를 선택합니다.

System Policy 페이지가 나타납니다.

2단계 다음 옵션을 이용할 수 있습니다.

- 기존 시스템 정책에서 로그인 배너를 수정하려면 시스템 정책 옆에 있는 수정 아이콘( )을 클릭합니다.
- 로그인 배너를 새로운 시스템 정책의 일부로 구성하려면 **Create Policy**를 클릭합니다.

  63-2페이지의 시스템 정책 생성에 설명된 대로 시스템 정책에 대한 이름과 설명을 입력하고 **Save**를 클릭합니다.

어느 경우든 Access List 페이지가 나타납니다.

3단계 **Login Banner**를 클릭합니다.

Login Banner 페이지가 나타납니다.

4단계 이 시스템 정책과 함께 사용할 로그인 배너를 **Custom Login Banner** 필드에 입력합니다.

5단계 **Save Policy and Exit**를 클릭합니다.

시스템 정책이 업데이트됩니다. 시스템 정책을 적용할 때까지는 변경 사항이 반영되지 않습니다. 자세한 내용은 63-4페이지의 시스템 정책 적용을/를 참조하십시오.

SNMP 폴링 구성

라이센스: 모두

지원되는 디바이스: X-Series를 제외한 모두

시스템 정책을 사용하여 어플라이언스의 SNMP(Simple Network Management Protocol) 폴링을 활성화할 수 있습니다. SNMP 기능은 SNMP 프로토콜의 1, 2, 3 버전 사용을 지원합니다.

이 기능을 사용하면 다음에 액세스할 수 있습니다.

- 어플라이언스에 대한 표준 MIB(management information base) - 연락처, 관리, 위치, 서비스 정보, IP 주소 지정 및 라우팅 정보, 전송 프로토콜 사용 통계 등의 시스템 세부사항을 포함합니다.
- 관리되는 디바이스에 대한 추가 MIB - 물리적 인터페이스, 논리적 인터페이스, 가상 인터페이스, ARP, NDP, 가상 브리지, 가상 라우터 등을 통과하는 트래픽에 대한 통계를 포함합니다.

시스템 정책 SNMP 기능을 활성화하는 경우 어플라이언스에서 SNMP 트랩을 전송하지는 않으며, MIB의 정보를 네트워크 관리 시스템을 통한 폴링에 사용할 수 있도록 지원할 뿐입니다.

참고 어플라이언스를 폴링하는 데 사용할 컴퓨터에 대해서는 SNMP 액세스를 추가해야 합니다. 자세한 내용은 63-9페이지의 어플라이언스에 대한 액세스 목록 구성을/를 참조하십시오. SNMP MIB에는 어플라이언스 공격에 사용될 수 있는 정보가 포함됩니다. Cisco에서는 SNMP 액세스에 대한 액세스 목록을 MIB에 대한 폴링에 사용될 특정 호스트로 제한할 것을 권장합니다. Cisco에서는 또한 SNMPv3을 사용하고 네트워크 관리 액세스에 강력한 비밀번호를 사용할 것을 권장합니다.

SNMP 폴링을 구성하려면

액세스: Admin

1단계 **System > Local > System Policy**를 선택합니다.

System Policy 페이지가 나타납니다.

2단계 다음 옵션을 이용할 수 있습니다.

- 기존 시스템 정책에서 SNMP 폴링 설정을 수정하려면 시스템 정책 옆에 있는 수정 아이콘( )을 클릭합니다.
- SNMP 폴링 설정을 새로운 시스템 정책의 일부로 구성하려면 **Create Policy**를 클릭합니다.

  63-2페이지의 시스템 정책 생성에 설명된 대로 시스템 정책에 대한 이름과 설명을 입력하고 **Create**를 클릭합니다.

어느 경우든 Access List 페이지가 나타납니다.

3단계 어플라이언스를 폴링하기 위해 사용할 각 컴퓨터에 대해 아직 SNMP 액세스를 추가하지 않은 경우 지금 추가합니다. 자세한 내용은 63-9페이지의 어플라이언스에 대한 액세스 목록 구성을/를 참조하십시오.

4단계 **SNMP**를 클릭합니다.

SNMP 페이지가 나타납니다.

5단계 사용할 SNMP 버전을 **SNMP Version** 드롭다운 목록에서 선택합니다.

드롭다운 목록에 선택한 버전이 표시됩니다.

6단계 다음 옵션을 이용할 수 있습니다.

- **Version 1** 또는 **Version 2**를 선택한 경우 **Community String** 필드에 SNMP 커뮤니티 이름을 입력합니다. 15단계로 이동합니다.

- **Version 3**을 선택한 경우 **Add User**를 클릭하여 사용자 정의 페이지를 표시합니다.

7단계 **Username** 필드에 사용자 이름을 입력합니다.

8단계 **Authentication Protocol** 드롭다운 목록에서 인증에 사용할 프로토콜을 선택합니다.

9단계 SNMP 서버에서의 인증에 필요한 비밀번호를 **Authentication Password** 필드에 입력합니다.

10단계 **Authentication Password** 필드의 바로 아래에 있는 **Verify Password** 필드에 인증 비밀번호를 다시 입력합니다.

11단계 사용할 비공개 프로토콜을 **Privacy Protocol** 목록에서 선택하거나, 비공개 프로토콜을 사용하지 않으려면 **None**을 선택합니다.

12단계 SNMP 서버에 필요한 SNMP 프라이버시 키를 **Privacy Password** 필드에 입력합니다.

13단계 **Privacy Password** 필드의 바로 아래에 있는 **Verify Password** 필드에 프라이버시 비밀번호를 다시 입력합니다.

14단계 **Add**를 클릭합니다.

사용자가 추가됩니다. 사용자를 더 추가하려면 6단계~13단계를 반복할 수 있습니다. 사용자를 삭제하려면 삭제 아이콘( )을 클릭합니다.

15단계 **Save Policy and Exit**를 클릭합니다.

시스템 정책이 업데이트됩니다. 시스템 정책을 적용할 때까지는 변경 사항이 반영되지 않습니다. 자세한 내용은 63-4페이지의 시스템 정책 적용을/를 참조하십시오.

STIG 규정 준수 활성화

라이센스: 모두

지원되는 디바이스: X-Series를 제외한 모두

미국 연방 정부 내 조직은 때때로 STIG(Security Technical Implementation Guide)에 나와 있는 일련의 보안 체크리스트를 따라야 합니다. STIG Compliance 옵션은 미국 국방성에서 지정한 특정 요구사항을 준수하도록 지원하는 데 필요한 설정을 활성화합니다.

구축의 특정 어플라이언스에서 STIG 규정 준수를 활성화하는 경우 모든 어플라이언스에서 활성화해야 합니다. 비준수 관리되는 디바이스는 STIG 준수 방어 센터에 등록할 수 없으며 STIG 준수 디바이스는 비준수 방어 센터에 등록할 수 없습니다.

STIG 규정 준수를 활성화해도 모든 해당 STIG에 대한 엄격한 준수가 보장되지는 않습니다. 이 제품 버전에서 이 모드를 사용할 경우 FireSIGHT 시스템 STIG 규정 준수에 대해 자세히 알아보려면 고객 지원에 문의하여 버전 5.4.1의 FireSIGHT 시스템 STIG Release Notes의 사본을 받아보십시오.

STIG 규정 준수를 활성화하면 로컬 셸 액세스 계정에 대한 비밀번호 복잡성 및 보유 규칙이 변경됩니다. 이러한 설정에 대한 자세한 내용은 버전 5.4.1의 FireSIGHT 시스템 STIG Release Notes을/를 참조하십시오. 또한 STIG 규정 준수 모드에서는 `ssh` 원격 스토리지를 사용할 수 없습니다.

STIG 규정 준수가 활성화된 시스템 정책을 적용하면 어플라이언스가 재부팅됩니다. STIG가 활성화된 시스템 정책을 STIG가 이미 활성화된 어플라이언스에 적용하면 어플라이언스가 재부팅되지 않습니다. STIG가 비활성화된 시스템 정책을 STIG가 활성화된 어플라이언스에 적용하면 STIG는 활성 상태로 유지되고 어플라이언스는 재부팅되지 않습니다.

버전 5.2.0 이전 버전에서 업그레이드된 어플라이언스의 경우 규정 준수가 활성화된 정책을 적용하면 어플라이언스 인증서가 재생성되므로, 이미 등록된 관리되는 디바이스 또는 피어를 다시 등록해야 합니다.

주의 고객 지원의 도움 없이는 이 설정을 비활성화할 수 없습니다. 또한 이 설정은 실제로 시스템의 성능에 영향을 줄 수 있습니다. Cisco에서는 국방부 보안 요구 사항을 준수하는 경우 외에는 STIG 규정 준수를 활성화하지 않을 것을 권장합니다.

STIG 규정 준수를 활성화하려면

액세스: Admin

1단계 **System > Local > System Policy**를 선택합니다.

System Policy 페이지가 나타납니다.

2단계 다음 옵션을 이용할 수 있습니다.

- 기존 시스템 정책에서 시간 설정을 수정하려면 시스템 정책 옆에 있는 수정 아이콘( )을 클릭합니다.
- 시간 설정을 새로운 시스템 정책의 일부로 구성하려면 **Create Policy**를 클릭합니다.

  63-2페이지의 시스템 정책 생성에 설명된 대로 시스템 정책에 대한 이름과 설명을 입력하고 **Save**를 클릭합니다.

어느 경우든 Access List 페이지가 나타납니다.

3단계 **STIG Compliance**를 클릭합니다.

STIG Configuration 페이지가 나타납니다.

4단계 어플라이언스에서 STIG 규정 준수를 *영구적으로* 활성화하려면 **Enable STIG Compliance**를 선택합니다.

주의 STIG 규정 준수가 활성화된 정책을 적용한 후에는 어플라이언스에서 STIG 규정 준수를 비활성화할 수 없습니다. 규정 준수를 비활성화해야 하는 경우 고객 지원에 문의하십시오.

5단계 **Save Policy and Exit**를 클릭합니다.

시스템 정책이 업데이트됩니다. 시스템 정책을 적용할 때까지는 변경 사항이 반영되지 않습니다. 자세한 내용은 63-4페이지의 시스템 정책 적용을/를 참조하십시오.

STIG 규정 준수를 활성화하는 시스템 정책을 어플라이언스에 적용하면 어플라이언스가 재부팅됩니다. STIG가 활성화된 시스템 정책을 STIG가 이미 활성화된 어플라이언스에 적용하면 어플라이언스가 재부팅되지 않습니다.

또한 디바이스가 버전 5.2.0 이전 버전에서 업그레이드된 경우 STIG 규정 준수를 활성화한 후 디바이스를 다시 등록해야 합니다.

시간 동기화

라이센스: 모두

지원되는 디바이스: X-Series를 제외한 모두

Time Synchronization 페이지를 사용하여 어플라이언스에서 시간 동기화를 관리할 수 있습니다. 다음과 같이 시간을 동기화하도록 선택할 수 있습니다.

- 수동으로
- 하나 이상의 NTP 서버를 사용하여(이 중 하나는 방어 센터일 수 있음)

시간 설정은 시스템 정책의 일부입니다. 새 시스템 정책을 생성하거나 기존 정책을 수정하여 시간 설정을 지정할 수 있습니다. 어느 경우든 시스템 정책을 적용하기 전에는 시간 설정이 사용되지 않습니다.

시간 설정은 Time Zone 페이지(기본값 America/New York)에 설정된 표준 시간대를 사용하여 어플라이언스 대부분의 페이지에 로컬 시간으로 표시되지만, UTC 시간을 사용하여 어플라이언스 자체에 저장됩니다. 또한 현재 시간은 Time Synchronization 페이지 상단에 UTC로 표시됩니다(로컬 시간은 활성화한 경우 Manual 시계 설정 옵션으로 표시됨).

Cisco NGIPS for Blue Coat X-Series에 대한 시간 설정을 관리하려면 명령줄 인터페이스나 운영 체제 인터페이스 등 기본 애플리케이션을 사용해야 합니다. Cisco NGIPS for Blue Coat X-Series 및 해당 관리하는 방어 센터의 시간은 동일한 물리적 어플라이언스 또는 NTP 서버에서 동기화하십시오. 자세한 내용은 *Cisco Software for X-Series Installation Guide*를 참조하십시오.

어플라이언스의 시간을 외부 시간 서버와 동기화할 수 있습니다. 원격 NTP 서버를 지정하는 경우 어플라이언스는 이에 대한 네트워크 액세스를 갖게 됩니다. 신뢰할 수 없는 NTP 서버를 지정하지 마십시오. NTP 서버에 대한 연결에는 구성된 프록시 설정이 사용되지 않습니다. 방어 센터를 NTP 서버로 사용하려면 63-27페이지의 방어 센터에서 시간 서비스 제공을/를 참조하십시오.

Cisco에서는 가상 어플라이언스를 물리적 NTP 서버와 동기화할 것을 권고하고 있습니다. 관리되는 디바이스(가상 또는 물리적)를 가상의 방어 센터에 동기화하지 마십시오.

참고 시간 동기화 후 방어 센터 및 관리되는 디바이스의 시간이 일치하는지 확인하십시오. 일치하지 않는 경우, 관리되는 디바이스가 방어 센터와 통신할 때 예기치 않은 결과가 발생할 수 있습니다.

방어 센터 또는 관리되는 디바이스에서 웹 인터페이스를 사용하는지 여부에 따라 시간 동기화 절차가 약간 다릅니다. 각 절차에 대해서는 아래에서 따로 설명합니다.

시간을 동기화하려면

액세스: Admin

1단계 **System > Local > System Policy**를 선택합니다.

System Policy 페이지가 나타납니다.

2단계 다음 옵션을 이용할 수 있습니다.

- 기존 시스템 정책에서 시간 설정을 수정하려면 시스템 정책 옆에 있는 수정 아이콘( )을 클릭합니다.
- 시간 설정을 새로운 시스템 정책의 일부로 구성하려면 **Create Policy**를 클릭합니다.

  63-2페이지의 시스템 정책 생성에 설명된 대로 시스템 정책에 대한 이름과 설명을 입력하고 **Save**를 클릭합니다.

어느 경우든 Access List 페이지가 나타납니다.

3단계 **Time Synchronization**을 클릭합니다.

Time Synchronization 페이지가 나타납니다.

4단계 방어 센터에서 관리되는 서비스로 시간 서비스를 제공하려면 **Serve time via NTP** 드롭다운 목록에서 **Enabled**를 선택합니다.

5단계 방어 센터에서 시간이 동기화되는 방법을 지정하기 위해 다음과 같은 옵션을 이용할 수 있습니다.

- 시간을 수동으로 설정하려면 **Manually in Local Configuration**을 선택합니다. 시스템 정책을 적용한 후 시간 설정에 대한 자세한 내용은 64-14페이지의 수동으로 시간 설정을/를 참조하십시오.

- 다른 서버에서 NTP를 통해 시간을 수신하려면 **Via NTP from**을 선택하고, 사용할 NTP 서버에 대한 IP 주소의 쉼표로 구분된 목록을 입력하거나 DNS가 활성화된 경우 정규화된 호스트 및 도메인 이름을 입력합니다.

주의 어플라이언스가 재부팅되고 DHCP 서버가 NTP 서버 레코드를 여기에 지정된 것과 다르게 설정하는 경우 DHCP 제공 NTP 서버가 대신 사용됩니다. 이 상황을 피하려면 DHCP 서버를 NTP 서버와 동일하게 구성하십시오.

6단계 관리되는 디바이스에서 시간이 동기화되는 방법을 지정하기 위해 다음과 같은 옵션을 이용할 수 있습니다.

- 시간을 수동으로 설정하려면 **Manually in Local Configuration**을 선택합니다. 시스템 정책을 적용한 후 시간 설정에 대한 자세한 내용은 64-14페이지의 수동으로 시간 설정을/를 참조하십시오.
- 방어 센터에서 NTP를 통해 시간을 수신하려면 **Via NTP from 방어 센터**를 선택합니다. 자세한 내용은 63-27페이지의 방어 센터에서 시간 서비스 제공을/를 참조하십시오.
- 서로 다른 서버에서 NTP를 통해 시간을 수신하려면 **Via NTP from**을 선택합니다. 텍스트 상자에 쉼표로 구분한 NTP 서버의 IP 주소 목록을 입력하거나, DNS가 활성화된 경우 정규화된 호스트 및 도메인 이름을 입력합니다.

참고 관리되는 디바이스를 구성된 NTP 서버와 동기화하는 데 몇 분 정도 걸릴 수 있습니다. 또한 관리되는 서버를 NTP 서버로 구성된 방어 센터와 동기화하고, 방어 센터 자체는 NTP 서버를 사용하도록 구성된 경우, 동기화하는 데 어느 정도 시간이 걸릴 수 있습니다. 이는 방어 센터가 관리되는 디바이스에 시간 서비스를 제공할 수 있으려면 먼저 구성된 NTP 서버와 동기화되어야 하기 때문입니다.

7단계 **Save Policy and Exit**를 클릭합니다.

시스템 정책이 업데이트됩니다. 시스템 정책을 적용할 때까지는 변경 사항이 반영되지 않습니다. 자세한 내용은 63-4페이지의 시스템 정책 적용을/를 참조하십시오.

방어 센터에서 시간 서비스 제공

라이센스: 모두

지원되는 디바이스: X-Series를 제외한 모두

NTP를 사용하여 방어 센터를 시간 서버로 구성한 다음, 이를 이용하여 방어 센터와 관리되는 디바이스 간에 시간을 동기화할 수 있습니다.

NTP를 사용하여 시간을 서비스하도록 방어 센터를 구성한 후에는 시간을 수동으로 설정할 수 없습니다. 시간을 수동으로 변경해야 하는 경우, NTP를 사용하여 시간을 서비스하도록 방어 센터를 구성하기 **전에** 해야 합니다. 방어 센터를 NTP 서버로 구성한 **후에** 수동으로 시간을 변경해야 하는 경우 **Via NTP** 옵션을 비활성화하고 **Save**를 클릭하고, 시간을 수동으로 변경하고 **Save**를 클릭한 다음, **Via NTP**를 활성화하고 **Save**를 클릭하십시오.

참고 NTP를 사용하여 시간을 서비스하도록 방어 센터를 구성한 다음 나중에 이를 비활성화하면, 관리되는 디바이스의 NTP 서비스는 계속해서 방어 센터와 시간을 동기화하려고 시도합니다. 동기화 시도를 중지하려면 관리되는 디바이스의 웹 인터페이스에서 NTP를 비활성화해야 합니다.

방어 센터를 NTP 서버로 구성하려면

액세스: Admin

1단계 **System > Local > System Policy**를 선택합니다.

System Policy 페이지가 나타납니다.

2단계 다음 옵션을 이용할 수 있습니다.

- 기존 시스템 정책에서 NTP 서버 설정을 수정하려면 시스템 정책 옆에 있는 수정 아이콘( )을 클릭합니다.
- NTP 서버 설정을 새로운 시스템 정책의 일부로 구성하려면 **Create Policy**를 클릭합니다.

  63-2페이지의 시스템 정책 생성에 설명된 대로 시스템 정책에 대한 이름과 설명을 입력하고 **Save**를 클릭합니다.

어느 경우든 Access List 페이지가 나타납니다.

3단계 **Time Synchronization**을 클릭합니다.

Time Synchronization 페이지가 나타납니다.

4단계 **Serve Time via NTP** 드롭다운 목록에서 **Enabled**를 선택합니다.

5단계 관리되는 디바이스에 대한 **Set My Clock** 옵션에서 **Via NTP from 방어 센터**를 선택합니다.

6단계 **Save Policy and Exit**를 클릭합니다.

시스템 정책이 업데이트됩니다. 변경 사항을 반영하려면 방어 센터 및 관리되는 디바이스에 시스템 정책을 적용해야 합니다. 자세한 내용은 63-4페이지의 시스템 정책 적용을/를 참조하십시오.

참고 방어 센터와 관리되는 디바이스를 동기화하는 데 몇 분 정도 걸릴 수 있습니다.

사용자 인터페이스 설정 구성

라이센스: 모두

지원되는 디바이스: X-Series를 제외한 모두

FireSIGHT 시스템 웹 인터페이스 또는 명령줄 인터페이스의 무인 로그인 세션에는 보안 위험이 따를 수 있습니다. 비활성으로 인해 사용자 로그인 세션이 시간 초과되기까지의 유휴 시간을 분 단위로 구성할 수 있습니다. 셸(명령줄) 세션에 대해서도 유사한 시간 초과를 설정할 수 있습니다.

오랜 기간에 웹 인터페이스를 수동으로 비밀리에 모니터링하려는 사용자도 있을 수 있습니다. 그러한 사용자는 사용자 컨피그레이션 옵션을 통해 웹 인터페이스 세션 시간 초과에서 제외할 수 있습니다. (메뉴 옵션에 완전히 액세스할 수 있으므로 손상 시 더 큰 위험을 초래하는 Administrator 역할의 사용자는 세션 시간 초과에서 제외할 수 없습니다.) 자세한 내용은 61-47페이지의 사용자 로그인 설정 관리을/를 참조하십시오.

시스템에 대한 셸 액세스를 제한해야 하는 경우, 세 번째 옵션을 사용하면 명령줄에서 `expert` 명령을 영구적으로 비활성화할 수 있습니다. 어플라이언스에서 expert 모드를 비활성화하면 모든 사용자, 심지어 Configuration 셸 액세스가 있는 사용자도 셸에서 expert 모드로 들어갈 수 없습니다. 사용자가 명령줄에서 expert 모드로 들어가면 셸에 해당하는 Linux 명령을 실행할 수 있습니다. expert 모드가 아닌 경우 명령줄 사용자는 명령줄 인터페이스에서 제공하는 명령만 실행할 수 있습니다. 명령줄 인터페이스는 Series 2 어플라이언스에서 지원되지 않습니다.

명령줄 인터페이스 명령에 대한 자세한 내용은 D-1페이지의 명령줄 참조을/를 참조하십시오. 명령줄 액세스에 대해 사용자를 설정하는 방법에 대한 자세한 내용은 61-45페이지의 명령줄 액세스 관리 및 D-1페이지의 명령줄 참조(가상 서비스 CLI 사용자 관리용)을/를 참조하십시오.

사용자 인터페이스 설정을 구성하려면

액세스: Admin

1단계 **System > Local > System Policy**를 선택합니다.

System Policy 페이지가 나타납니다.

2단계 다음 옵션을 이용할 수 있습니다.

- 기존 시스템 정책에서 사용자 인터페이스 설정을 수정하려면 시스템 정책 옆에 있는 수정 아이콘()을 클릭합니다.
- 사용자 인터페이스 설정을 새로운 시스템 정책의 일부로 구성하려면 **Create Policy**를 클릭합니다.

  63-2페이지의 시스템 정책 생성에 설명된 대로 시스템 정책에 대한 이름과 설명을 입력하고 **Save**를 클릭합니다.

어느 경우든 Access List 페이지가 나타납니다.

3단계 **User Interface**를 클릭합니다.

User Interface 페이지가 나타납니다.

4단계 다음 옵션을 이용할 수 있습니다.

- 웹 인터페이스에 대한 세션 시간 초과를 구성하려면 **Browser Session Timeout (Minutes)** 필드에 숫자(분)를 입력합니다. 기본값은 `60`이고 최대값은 `1440`(24시간)입니다.

  이 세션 시간 초과에서 사용자를 제외하는 방법에 대한 자세한 내용은 61-47페이지의 사용자 로그인 설정 관리을/를 참조하십시오.
- 명령줄 인터페이스에 대한 세션 시간 초과를 구성하려면 **Shell Timeout (Minutes)** 필드에 숫자(분)를 입력합니다. 기본값은 `0`이고 최대값은 `1440`(24시간)입니다.

- 명령줄 인터페이스에서 `expert` 명령을 영구적으로 비활성화하려면 **Permanently Disable Expert Access** 확인란을 선택합니다.

주의 expert 모드가 비활성화된 시스템 정책을 어플라이언스에 적용한 후에는 웹 인터페이스 또는 명령줄을 통해 expert 모드에 액세스하는 기능을 복원할 수 없습니다. expert 모드 기능을 복원하려면 고객 지원에 문의해야 합니다.

5단계 **Save Policy and Exit**를 클릭합니다.

시스템 정책이 업데이트됩니다. 변경 사항을 반영하려면 방어 센터 및 관리되는 디바이스에 시스템 정책을 적용해야 합니다. 세션 시간 초과 간격에 대한 변경 사항은 다음 로그인 세션까지 적용되지 않습니다.

서버에 대한 취약성 매핑

라이센스: 보호

지원되는 디바이스: X-Series를 제외한 모두

서버의 검색 이벤트 데이터베이스에 애플리케이션 ID가 있고 트래픽에 대한 패킷 헤더에 공급업체 및 버전이 포함된 경우, 호스트 IP 주소에서 주고받는 모든 애플리케이션 프로토콜 트래픽에 대해 FireSIGHT 시스템은 해당 주소에 취약성을 자동으로 매핑합니다.

그러나 공급업체 및 버전 정보가 포함되지 않은 서버가 많습니다. 시스템 정책에 나열된 서버의 경우, 공급업체 및 버전 없는 서버에 대해 시스템이 취약성을 서버 트래픽과 연결할지 여부를 구성할 수 있습니다.

예를 들어, 호스트가 헤더에 공급업체 또는 버전을 가지고 있지 않은 SMTP 트래픽을 서비스할 수 있습니다. 시스템 정책의 Vulnerability Mapping 페이지에서 SMTP 서버를 활성화한 다음 트래픽을 탐지하는 디바이스를 관리하는 방어 센터에 해당 정책을 적용하면, SMTP 서버와 관련된 모든 취약성이 호스트의 호스트 프로필에 추가됩니다.

탐지기는 서버 정보를 수집하여 호스트 프로필에 추가하지만, 애플리케이션 프로토콜 탐지기는 취약성 매핑에 사용되지 않습니다. 사용자 지정 애플리케이션 프로토콜 탐지기에 대해 공급업체 및 버전을 지정할 수 없으며 시스템 정책에서 취약성 매핑을 위해 서버를 선택할 수 없기 때문입니다.

서버에 대해 취약성 매핑을 구성하려면

액세스: Admin

1단계 **System > Local > System Policy**를 선택합니다.

System Policy 페이지가 나타납니다.

2단계 다음 옵션을 이용할 수 있습니다.

- 기존 시스템 정책에서 취약성 매핑 설정을 수정하려면 시스템 정책 옆에 있는 수정 아이콘( )을 클릭합니다.
- 취약성 매핑 설정을 새로운 시스템 정책의 일부로 구성하려면 **Create Policy**를 클릭합니다.

  63-2페이지의 시스템 정책 생성에 설명된 대로 시스템 정책에 대한 이름과 설명을 입력하고 **Save**를 클릭합니다.

어느 경우든 Access List 페이지가 나타납니다.

3단계 **Vulnerability Mapping**을 클릭합니다.

Vulnerability Mapping 페이지가 나타납니다.

4단계 다음 옵션을 이용할 수 있습니다.

- 서버에 대한 취약성이 공급업체 또는 버전 정보 없는 애플리케이션 프로토콜 트래픽을 수신하는 호스트에 매핑되지 않도록 하려면 해당 서버의 확인란을 선택 취소합니다.
- 서버에 대한 취약성이 공급업체 또는 버전 정보 없는 애플리케이션 프로토콜 트래픽을 수신하는 호스트에 매핑되도록 하려면 해당 서버의 확인란을 선택합니다.

팁 **Enabled** 옆에 있는 확인란을 사용하여 모든 확인란을 동시에 선택하거나 선택 취소할 수 있습니다.

5단계 **Save Policy and Exit**를 클릭합니다.

시스템 정책이 업데이트됩니다. 변경 사항을 반영하려면 방어 센터 및 관리되는 디바이스에 시스템 정책을 적용해야 합니다. 자세한 내용은 63-4페이지의 시스템 정책 적용을/를 참조하십시오.

64장

어플라이언스 설정 구성

어플라이언스의FireSIGHT 시스템 *로컬 컨피그레이션*(**System > Local > Configuration**)은 단일 어플라이언스에 해당될 수 있는 설정 그룹입니다. 구축 전체에서 유사할 수 있는 어플라이언스 설정을 제어하는 시스템 정책(63-1페이지의 시스템 정책 관리)과 로컬 컨피그레이션을 비교해 보십시오.

다음 표에는 어플라이언스의 로컬 컨피그레이션이 요약되어 있습니다.

표 64-1 로컬 컨피그레이션 옵션

옵션	설명	참조 섹션
정보	어플라이언스에 대한 현재 정보를 볼 수 있습니다. 어플라이언스 이름을 변경할 수도 있습니다.	64-2페이지의 어플라이언스 정보 보기 및 수정
HTTPS 인증서	필요한 경우 신뢰할 수 있는 기관에서 HTTPS 서버 인증서를 요청하고 어플라이언스에 업로드할 수 있습니다.	64-3페이지의 사용자 지정 HTTPS 인증서 사용
데이터베이스	어플라이언스 데이터베이스에 대한 외부의 읽기 전용 액세스를 활성화하도록 지원하며, 다운로드할 수 있는 클라이언트 드라이버를 제공합니다.	64-7페이지의 데이터베이스에 대한 액세스 활성화
관리 인터페이스	설치할 때 처음 설정된 어플라이언스의 IP 주소, 호스트 이름 및 프록시 설정과 같은 옵션을 변경할 수 있습니다. 어플라이언스에서 관리 인터페이스의 설정을 보고 수정할 수도 있습니다.	64-8페이지의 관리 인터페이스 구성
프로세스	어플라이언스를 종료하거나 재부팅하고, FireSIGHT 시스템 관련 프로세스를 다시 시작할 수 있습니다.	64-13페이지의 시스템 종료 및 재시작
Time	현재 시간을 표시합니다. 어플라이언스에 대한 현재 시스템 정책의 시간 동기화 설정이 **Manually in Local Configuration**으로 되어 있으면 이 페이지를 사용하여 시간을 변경할 수 있습니다.	64-14페이지의 수동으로 시간 설정
Remote Storage Device	방어 센터에서 백업 및 보고서용 원격 스토리지를 구성할 수 있습니다.	64-15페이지의 원격 스토리지 관리
Change Reconciliation	지난 24시간 동안 시스템 변경 사항의 자세한 보고서를 이메일을 통해 받을 수 있습니다.	64-19페이지의 변경 조정 이해
Console Configuration	VGA나 직렬 포트 또는 LOM(Lights-Out Management)을 통해 콘솔에서 FireSIGHT 시스템 어플라이언스에 액세스하도록 구성할 수 있습니다. 그러면 어플라이언스에 물리적으로 가까이 있지 않아도 제한된 모니터링 및 관리 작업을 수행할 수 있습니다.	64-21페이지의 원격 콘솔 액세스 관리

표 64-1 로컬 컨피그레이션 옵션 (계속)

옵션	설명	참조 섹션
클라우드 서비스	방어 센터에서 종합 보안 인텔리전스 클라우드로부터 URL 필터링 데이터를 다운로드하고, 분류되지 않은 URL에 대한 조회를 수행하고, 탐지된 파일에 대한 진단 정보를 Cisco로 전송할 수 있습니다.	64-27페이지의 클라우드 통신 활성화
VMWare Tools	가상 방어 센터에서 VMWare Tools를 활성화하고 사용할 수 있습니다.	64-30페이지의 VMware Tools 활성화

어플라이언스 정보 보기 및 수정

라이센스: 모두

Information 페이지에서는 어플라이언스에 대한 정보를 제공합니다. 정보에는 읽기 전용 정보(예: 제품 이름과 모델 번호), 운영 체제 및 버전, 현재 어플라이언스 수준 정책 등이 포함됩니다. 또한 어플라이언스의 이름을 변경할 수 있는 옵션도 제공합니다.

다음 표에서는 각 필드에 대해 설명합니다.

표 64-2 어플라이언스 정보

필드	설명
이름	어플라이언스에 할당하는 이름. 이 이름은 FireSIGHT 시스템의 컨텍스트 내에서만 사용됩니다. 호스트 이름을 어플라이언스의 이름으로 사용할 수도 있지만 이 필드에 다른 이름을 입력해도 호스트 이름이 변경되지 않습니다.
제품 모델	어플라이언스의 모델 이름.
소프트웨어 버전	현재 설치된 소프트웨어의 버전.
일련 번호	어플라이언스의 섀시 일련 번호.
Store Events Only on 방어 센터	이벤트 데이터를 방어 센터에 저장하고 관리되는 디바이스에는 저장하지 않으려면 관리되는 디바이스에서 이 확인란을 선택합니다. 이벤트 데이터를 두 어플라이언스에 모두 저장하려면 이 확인란을 지웁니다.
Prohibit Packet Transfer to the 방어 센터	관리되는 디바이스가 이벤트와 함께 패킷 데이터를 전송하지 않도록 하려면 관리되는 디바이스에서 이 확인란을 선택합니다. 패킷 데이터를 이벤트와 함께 방어 센터에 저장하도록 허용하려면 이 확인란을 선택합니다.
운영 체제	현재 어플라이언스에서 실행 중인 운영 체제.
운영 체제 버전	현재 어플라이언스에서 실행 중인 운영 체제의 버전.
IPv4 주소	어플라이언스의 기본(`eth0`) 관리 인터페이스의 IPv4 주소. IPv4 관리가 어플라이언스에 대해 비활성화되어 있으면 이 필드에 표시됩니다.
IPv6 주소	어플라이언스의 기본(`eth0`) 관리 인터페이스의 IPv6 주소. IPv6 관리가 어플라이언스에 대해 비활성화되어 있으면 이 필드에 표시됩니다.
Current Policies	현재 적용된 어플라이언스 레벨 정책. 마지막으로 적용된 이후 정책이 업데이트되었으면 정책 이름이 기울임꼴로 나타납니다.
모델 번호	어플라이언스의 모델 번호. 이 번호는 문제 해결 시 중요할 수 있습니다.

어플라이언스 정보를 수정하려면

액세스: Admin

1단계 **System > Local > Configuration**을 선택합니다.

Information 페이지가 나타납니다.

2단계 어플라이언스 이름을 변경하려면 **Name** 필드에 새 이름을 입력합니다.

이름은 **반드시** 영숫자 문자여야 하며, 숫자로만 구성할 수 없습니다.

3단계 변경 사항을 저장하려면 **Save**를 클릭합니다.

페이지가 새로 고쳐지고 변경 사항이 저장됩니다.

사용자 지정 HTTPS 인증서 사용

라이센스: 모두

Cisco 방어 센터 및 웹 기반 사용자 인터페이스를 지원하는 관리되는 디바이스에는 웹 브라우저와 어플라이언스 간 암호화된 통신 채널을 시작하기 위해 사용할 수 있는 기본 SSL(Secure Sockets Layer) 인증서가 포함되어 있습니다. 그러나 어플라이언스에 대한 기본 인증서는 세계적으로 알려진 CA(인증 기관)에서 신뢰하는 CA로 생성되지 않으므로, 세계적으로 알려지거나 내부적으로 신뢰할 수 있는 CA에서 서명한 사용자 지정 인증서로 교체할 수 있습니다.

어플라이언스에 대한 로컬 컨피그레이션을 통해 인증서를 관리할 수 있습니다. 자세한 내용은 다음을 참조하십시오.

- 64-3페이지의 현재 HTTPS 서버 인증서 보기
- 64-4페이지의 서버 인증서 요청 생성
- 64-5페이지의 서버 인증서 업로드
- 64-6페이지의 사용자 인증서 요청

현재 HTTPS 서버 인증서 보기

라이센스: 모두

현재 어플라이언스에 대한 서버 인증서에서 세부사항을 볼 수 있습니다. 인증서는 다음 정보를 제공합니다.

표 64-3 HTTPS 서버 인증서 정보

필드	설명
제목	인증서가 설치된 어플라이언스의 경우 commonName, countryName, organizationName 및 organizationalUnitName을 제공합니다.
발급 자	인증서를 발행한 어플라이언스의 경우 commonName, countryName, organizationName 및 organizationalUnitName을 제공합니다.
유효성	인증서가 유효한 기간을 나타냅니다.
버전	인증서 버전을 나타냅니다.

표 64-3 HTTPS 서버 인증서 정보 (계속)

필드	설명
일련 번호	인증서 일련 번호를 나타냅니다.
Signature Algorithm	인증서 서명에 사용되는 알고리즘을 나타냅니다.

인증서 세부사항을 보려면

액세스: Admin

1단계 **System > Local > Configuration**을 선택합니다.

Information 페이지가 나타납니다.

2단계 **HTTPS Certificate**를 클릭합니다.

어플라이언스의 현재 인증서에 대한 세부사항이 포함된 HTTPS Certificate 페이지가 나타납니다.

서버 인증서 요청 생성

라이센스: 모두

어플라이언스 정보 및 식별 정보를 기반으로 인증서 요청을 생성할 수 있습니다. 결과 요청을 인증 기관으로 전송하여 서버 인증서를 요청할 수 있습니다. 브라우저에서 신뢰하는 내부 CA(인증 기관)가 설치되어 있는 경우 인증서를 자체 서명하는 데 사용할 수도 있습니다. 생성된 키는 Base-64 encoded PEM 형식입니다.

로컬 컨피그레이션 HTTPS Certificate 페이지를 통해 인증서 요청을 생성하는 경우 단일 서버에 대한 인증서만 생성할 수 있습니다. 인증서의 **Common Name** 필드에 나타나므로 서버의 정규화된 도메인 이름을 정확히 입력해야 합니다. Common Name 및 DNS 호스트 이름이 일치하지 않으면 어플라이언스에 연결할 때 경고가 표시됩니다. 마찬가지로, 세계적으로 알려지거나 내부적으로 신뢰하는 CA에 의해 서명되지 않은 인증서를 설치할 경우 어플라이언스에 연결할 때 보안 경고가 표시됩니다.

인증서 요청을 생성하려면

액세스: Admin

1단계 **System > Local > Configuration**을 선택합니다.

Information 페이지가 나타납니다.

2단계 **HTTPS Certificate**를 클릭합니다.

HTTPS Certificate 페이지가 나타납니다.

3단계 **Generate New CSR**을 클릭합니다.

Generate Certificate Signing Request 팝업 창이 나타납니다.

4단계 해당 국가의 두 자리 국가 코드를 **Country Name (two-letter code)** 필드에 입력합니다.

5단계 거주 지역의 우편번호를 **State or Province** 필드에 입력합니다.

6단계 **Locality or City**의 이름을 입력합니다.

7단계 **Organization** 이름을 입력합니다.

8단계 **Type an Organizational Unit (Department)** 이름을 입력합니다.

9단계 인증서를 요청할 서버의 정규화된 도메인 이름을 인증서에 표시하고자 하는 대로 정확히 **Common Name** 필드에 입력합니다.

10단계 **Generate**를 클릭합니다.

Certificate Signing Request 팝업 창이 나타납니다.

11단계 텍스트 편집기를 엽니다.

12단계 인증서 요청에서 텍스트의 전체 블록(`BEGIN CERTIFICATE REQUEST` 및 `END CERTIFICATE REQUEST` 줄 포함)을 복사하고 빈 텍스트 파일에 붙여넣습니다.

13단계 파일을 *servername*`.csr`로 저장합니다. 여기서 *servername*은 인증서를 사용하려는 서버의 이름입니다.

14단계 인증서를 요청할 인증 기관에 CSR 파일을 업로드하거나, CSR을 사용하여 자체 서명 인증서를 생성합니다.

서버 인증서 업로드

라이센스: 모두

CA(인증 기관)에서 서명된 인증서가 있으면 해당 인증서를 업로드할 수 있습니다. 인증서를 생성한 서명 기관에서 중간 CA를 신뢰하도록 요청하는 경우, 인증서 체인(인증서 경로라고도 함)도 제공해야 합니다. 사용자 인증서가 필요한 경우, 중간 기관이 인증서 체인이 포함된 인증 기관에 의해 생성된 인증서여야 합니다.

인증서를 업로드하려면

액세스: Admin

1단계 **System > Local > Configuration**을 선택합니다.

Information 페이지가 나타납니다.

2단계 **HTTPS Certificate**를 클릭합니다.

HTTPS Certificate 페이지가 나타납니다.

3단계 **Import HTTPS Certificate**를 클릭합니다.

Import HTTPS Certificate 팝업 창이 나타납니다.

4단계 텍스트 편집기에서 서버 인증서를 열고, 전체 텍스트 블록(`BEGIN CERTIFICATE` 및 `END CERTIFICATE` 줄 포함)을 복사하고, **Server Certificate** 필드에 붙여넣습니다.

5단계 선택적으로, 개인 키 파일을 열고, 전체 텍스트 블록(`BEGIN RSA PRIVATE KEY` 및 `END RSA PRIVATE KEY` 줄 포함)을 복사하고, **Private Key** 필드에 붙여넣습니다.

6단계 제공해야 하는 중간 인증서를 열고, 각각에서 전체 텍스트 블록을 복사하고, **Certificate Chain** 필드에 붙여넣습니다.

7단계 **Save**를 클릭하여 인증서를 업로드합니다.

인증서가 업로드되고 HTTPS Certificate 페이지는 새 인증서를 반영하여 업데이트됩니다.

사용자 인증서 요청

라이센스: 모두

클라이언트 브라우저 인증서 확인을 사용하여 FireSIGHT 시스템 웹 서버에 대한 액세스를 제한할 수 있습니다. 사용자 인증서를 활성화하면 웹 서버는 사용자 브라우저의 클라이언트에서 유효한 사용자 인증서가 선택되었는지 확인합니다. 해당 사용자 인증서는 서버 인증서에 사용한 것과 동일한 신뢰할 수 있는 인증 기관에서 생성한 것이어야 합니다. 사용자가 브라우저에서 유효하지 않거나 디바이스의 인증서 체인에 있는 인증 기관에서 생성하지 않은 인증서를 선택하면 브라우저는 웹 인터페이스를 로드할 수 없습니다.

서버에 대한 CRL(certificate revocation list)도 업로드할 수 있습니다. CRL은 인증 기관에 의해 폐기된 인증서를 나열하므로, 웹 서버는 클라이언트 브라우저 인증서가 폐기되지 않았는지를 확인할 수 있습니다. 사용자가 CRL에 폐기된 인증서로 나열된 인증서를 선택하면 브라우저는 웹 인터페이스를 로드할 수 없습니다. 어플라이언스는 DER(Distinguished Encoding Rules) 형식으로 CRL의 업로드를 지원합니다. 한 서버에 하나의 CRL만 로드할 수 있습니다.

폐기된 인증서의 목록을 최신 상태로 유지하려면 CRL을 업데이트하는 예약 작업을 생성할 수 있습니다. 최신 상태의 CRL이 인터페이스에 나열됩니다.

서버 인증서에 사용한 것과 동일한 인증 기관을 사용하는지, 인증서에 대한 중간 인증서를 업로드했는지 확인하십시오. 자세한 내용은 64-5페이지의 서버 인증서 업로드을/를 참조하십시오.

참고 사용자 인증서를 활성화하고 그 후 웹 인터페이스에 액세스하려면 브라우저에 유효한 사용자 인증서가 있어야(또는 Reader에 CAC를 삽입해야) **합니다**.

유효한 사용자 인증서를 요청하려면

액세스: Admin

1단계 **System > Local > Configuration**을 선택합니다.

Information 페이지가 나타납니다.

2단계 **HTTPS Certificate**를 클릭합니다.

HTTPS Certificate 페이지가 나타납니다.

3단계 **Enable User Certificates**를 선택합니다. 프롬프트가 나타나면 드롭다운 목록에서 알맞은 인증서를 선택합니다.

Enable Fetching of CRL 옵션이 나타납니다.

4단계 선택적으로, **Enable Fetching of CRL**을 선택합니다.

나머지 CRL 컨피그레이션 옵션이 나타납니다.

5단계 기존의 CRL 파일에 대한 유효한 URL을 입력하고 **Refresh CRL**을 클릭합니다.

제공된 URL의 현재 CRL이 서버에 로드됩니다.

참고 CRL 가져오기를 활성화하면 CRL을 정기적으로 업데이트하는 예약 작업이 생성됩니다. 작업을 수정하여 업데이트 빈도를 설정할 수 있습니다. 자세한 내용은 62-4페이지의 CRL 다운로드 자동화을/를 참조하십시오.

6단계 서버 인증서를 생성한 인증 기관과 동일한 인증 기관에서 생성한 유효한 사용자 인증서가 있는지 확인합니다.

주의 활성화된 사용자 인증서와 함께 컨피그레이션을 저장할 경우, 브라우저 인증서 저장소에 유효한 사용자 인증서가 없으면 어플라이언스에 대한 모든 웹 서버 액세스가 비활성화됩니다. 설정을 저장하기 전에 유효한 인증서가 설치되어 있는지 확인하십시오.

7단계 웹 서버에 인증서 컨피그레이션을 적용하려면 **Save**를 클릭합니다.

인증서를 활성화했는데 사용자 인증서가 액세스를 활성화하지 않았음을 알게 되는 경우 명령줄을 통해 사용자 인증서 적용을 비활성화할 수 있습니다. 자세한 내용은 D-44페이지의 disable-http-user-cert을/를 참조하십시오.

데이터베이스에 대한 액세스 활성화

라이센스: 모두

서드파티 클라이언트에 데이터베이스에 대한 읽기 전용 액세스를 허용하도록 방어 센터를 구성할 수 있습니다. 그러면 다음 중 하나를 사용하여 SQL로 데이터베이스에 쿼리할 수 있습니다.

- Actuate BIRT, JasperSoft iReport 또는 Crystal Reports와 같은 산업 표준 보고 툴
- JDBC SSL 연결을 지원하는 기타 보고 애플리케이션(사용자 지정 애플리케이션 포함)
- 인터랙티브 방식으로 실행하거나 단일 쿼리에 대해 쉼표로 구분된 결과를 얻기 위해 사용할 수 있는 RunQuery라는 Cisco 제공 명령줄 Java 애플리케이션

Database Settings 로컬 컨피그레이션 페이지에서, 데이터베이스 액세스를 활성화할 수 있으며 선택한 호스트에서 데이터베이스에 쿼리하도록 허용하는 액세스 목록을 생성할 수 있습니다. 이 액세스 목록은 어플라이언스 액세스를 제어하지 않습니다. 어플라이언스 액세스 목록에 대한 자세한 내용은 63-9페이지의 어플라이언스에 대한 액세스 목록 구성을/를 참조하십시오.

다음이 포함된 패키지를 다운로드할 수도 있습니다.

- RunQuery - Cisco 제공 데이터베이스 쿼리 툴
- InstallCert - 액세스하려는 방어 센터에서 SSL 인증서를 검색하고 승인하기 위해 사용할 수 있는 툴
- 데이터베이스에 연결하기 위해 사용해야 하는 JDBC 드라이버

외부 클라이언트에서 데이터베이스에 연결할 때 방어 센터의 Administrator 또는 External Database 사용자에 대한 것과 일치하는 사용자 이름 및 비밀번호를 제공해야 합니다. 자세한 내용은 61-44페이지의 새 사용자 계정 추가을/를 참조하십시오.

데이터베이스 스키마 및 지원되는 쿼리에 대한 정보와 함께 외부에서 FireSIGHT 시스템 데이터베이스에 액세스하도록 구성하는 방법에 대한 자세한 내용은 *FireSIGHT 시스템 Database Access Guide*를 참조하십시오.

데이터베이스 액세스를 활성화하려면

액세스: Admin

1단계 **System > Local > Configuration**을 선택합니다.

Information 페이지가 나타납니다.

2단계 **Database**를 클릭합니다.

Database Settings 페이지가 나타납니다.

3단계 **Allow External Database Access** 확인란을 선택합니다.

Access List 필드가 나타납니다. 자세한 내용은 6단계을/를 참조하십시오.

4단계 서드파티 애플리케이션 요구 사항에 따라 방어 센터의 FQDN(정규화된 도메인 이름), IPv4 주소 또는 IPv6 주소를 **Server Hostname** 필드에 입력합니다.

FQDN을 입력할 경우 클라이언트가 방어 센터의 FQDN을 확인할 수 있도록 해야 합니다. IP 주소를 입력하는 경우 클라이언트가 IP 주소를 사용하여 방어 센터에 연결할 수 있도록 해야 합니다.

5단계 **Client JDBC Driver** 옆에 있는 **Download**를 클릭하고 브라우저의 지시에 따라 `client.zip` 패키지를 다운로드합니다.

다운로드한 패키지의 툴을 사용하여 데이터베이스 액세스를 구성하는 방법에 대한 자세한 내용은 *FireSIGHT 시스템 Database Access Guide*를 참조하십시오.

6단계 하나 이상의 IP 주소에 대한 데이터베이스 액세스를 추가하려면 **Add Hosts**를 클릭합니다.

Access List 필드에 **IP Address** 필드가 나타납니다.

7단계 추가할 IP 주소에 따라 **IP Address** 필드에 다음을 입력할 수 있습니다.

- 정확한 IP 주소(예: 192.168.1.101)
- CIDR 표기법을 사용한 IP 주소 블록(예: 192.168.1.1/24)

  FireSIGHT 시스템에서 CIDR을 사용하는 방법에 대한 자세한 내용은 1-19페이지의 IP 주소 표기 규칙을/를 참조하십시오.
- `any` - 임의의 IP 주소 지정

8단계 **Add**를 클릭합니다.

IP 주소가 데이터베이스 액세스 목록에 추가됩니다.

9단계 선택적으로, 데이터베이스 액세스 목록에서 항목을 제거하려면 삭제 아이콘( )을 클릭합니다.

10단계 **Save**를 클릭합니다.

데이터베이스 액세스 설정이 저장됩니다.

팁 마지막으로 저장된 데이터베이스 설정으로 돌아가려면 **Refresh**를 클릭합니다.

관리 인터페이스 구성

라이센스: 모두

어플라이언스를 처음 설정할 때 내부의 보호된 관리 네트워크에서 통신할 수 있도록 네트워크 설정을 구성하게 됩니다. 어플라이언스를 처음 설정한 다음 프록시 등 추가 네트워크 설정을 구성할 때 네트워크 설정을 변경할 수 있습니다. Series 3 어플라이언스 및 가상 방어 센터에서 트래픽 채널을 활성화하고 추가 관리 인터페이스를 구성하여 성능을 향상할 수 있으며, 방어 센터 및 다른 네트워크의 디바이스 간 트래픽을 관리 및 격리하기 위한 경로를 생성할 수 있습니다. Series 3 디바이스에서는 디바이스에 대한 LCD 패널 액세스를 활성화 또는 비활성화할 수도 있습니다. 이러한 설정을 변경하고 프록시 등 추가 네트워크 설정을 구성하려면 Management Interfaces 페이지(**System > Local > Configuration**을 선택하고 **Management Interfaces** 클릭)를 사용하십시오.

참고 가상 디바이스에 대한 네트워크 및 프록시 설정을 수정하고 Cisco NGIPS for Blue Coat X-Series에 대한 네트워크 설정을 수정하려면 명령줄 툴을 사용해야 합니다. Cisco NGIPS for Blue Coat X-Series는 프록시를 지원하지 **않습니다**. 자세한 내용은 *FireSIGHT 시스템 Virtual Installation Guide* 및 *Cisco NGIPS for Blue Coat X-Series Installation and Configuration Guide*를 참조하십시오.

컨피그레이션 옵션 및 절차에 대해서는 다음 절을 참조하십시오.

- 64-9페이지의 관리 인터페이스 옵션 이해
- 64-11페이지의 관리 인터페이스 수정

관리 인터페이스 옵션 이해

성능을 높이거나 다른 기능을 활성화하거나 구축에서 네트워크 컨피그레이션을 바꾸기 위해 설정을 변경하고자 할 수 있습니다. Series 3 어플라이언스에서는 또한 트래픽 채널을 구성하고, 추가 관리 인터페이스를 활성화하고, 다른 네트워크의 디바이스에서 오는 트래픽을 격리하기 위한 경로를 생성할 수 있습니다. 자세한 내용은 4-3페이지의 관리 인터페이스 이해을/를 참조하십시오.

Interfaces

FireSIGHT 시스템에서는 IPv4 및 IPv6 관리 환경에 이중 스택 구현을 제공합니다. 하나 또는 두 프로토콜을 선택할 수 있으며, 사용하지 않을 프로토콜(있는 경우)을 비활성화할 수 있습니다.

각 관리 프로토콜에 대해 기본(`eth0`) 관리 인터페이스의 IP 주소, 넷마스크나 접두사 길이, 기본 게이트웨이를 지정해야 합니다. 이러한 값을 수동으로 설정할 수도 있고, 로컬 DHCP 서버 또는 IPv6 라우터에서 검색하도록 어플라이언스를 구성할 수도 있습니다. 활성화할 각각의 추가(`eth1` 등) 관리 인터페이스는 수동으로 구성해야 합니다.

관리 인터페이스에서 다음 옵션을 구성할 수 있습니다.

- **Enabled** - 관리 인터페이스를 활성화합니다. 또 다른 관리 인터페이스를 활성화하여 저장하기 전에는 기본 관리 인터페이스를 비활성화하지 **마십시오**.
- **Channels** - 인터페이스에서 **Management Traffic** 및 **Event Traffic** 채널을 활성화합니다.

  관리 인터페이스의 커뮤니케이션 채널에서 다른 연결을 만들려면 트래픽 채널(관리 트래픽, 이벤트 트래픽 또는 둘 다)을 활성화할 수 있습니다. 또한 트래픽 채널을 여러 관리 인터페이스로 분할함으로써 각 인터페이스의 처리량을 결합하여 성능을 더욱 개선할 수 있습니다. 자세한 내용은 4-3페이지의 관리 인터페이스 이해을/를 참조하십시오.
- **Mode** - 기본 Autonegotiation을 변경하거나 링크 모드를 지정할 수 있습니다. Auto Negotiate 값에 대한 변경 사항은 Gigabit 인터페이스에 대해 무시됩니다.

  8000 Series 관리되는 디바이스를 방어 센터에 등록하는 경우 안정적 네트워크 링크를 보장하기 위해 연결 양측에서 자동 협상을 사용하거나 양측을 동일한 정적 속도로 설정해야 합니다. 8000 Series 관리되는 디바이스는 반이중 네트워크 링크를 지원하지 않으며 속도 차이 또는 연결 반대쪽의 이중 컨피그레이션도 지원하지 않습니다.
- **MTU** - 기본 설정을 변경할 수 있습니다.

주의 MTU(최대 전송 단위)를 변경하면 어플라이언스의 트래픽이 중단됩니다. MTU 설정 가능 범위는 FireSIGHT 시스템 어플라이언스 모델 및 인터페이스 유형에 따라 달라질 수 있습니다.

다음 표에는 관리 인터페이스에 대한 MTU 컨피그레이션 범위가 나열되어 있습니다.

표 64-4 디바이스별 관리 인터페이스 MTU 범위

모델 디바이스	MTU 범위
Series 2(3D6500 및 3D9900 제외)	576-1518
3D6500, 3D9900, 가상	576-9018
Series 3 기본(eth0)	576-9234
Series 3 비기본(eth1 등)	1518-9018

시스템은 구성된 MTU 값에서 자동으로 18바이트를 잘라내므로 1298 아래의 값은 최소 IPv6 MTU 설정인 1280을 준수하지 못하며 594 아래의 값은 최소 IPv4 MTU 설정인 576을 준수하지 못합니다. 예를 들면 시스템은 구성된 값 576을 자동으로 558로 자릅니다.

- **MDI/MDIX** - 기본 **Auto-MDIX** 설정을 변경할 수 있습니다.
- **IPv4 Configuration** - **Static**, **DHCP** 또는 **Disabled**를 선택하도록 구성할 수 있습니다.
  - IPv4 관리 IP 주소 및 넷마스크를 입력하려면 **Static**을 선택합니다.
  - DHCP 서버에서 네트워크 설정을 검색하려면 **DHCP**를 선택합니다. (eth0 전용)
  - 프로토콜을 비활성화하려면 **Disabled**를 선택합니다. IPv4와 IPv6을 모두 비활성화해서는 **안 됩니다**.
- **IPv6 Configuration** - **Static**, **DHCP**, **Router Assigned** 또는 **Disabled**를 선택하도록 구성할 수 있습니다.
  - IPv4 관리 IP 주소 및 넷마스크를 입력하려면 **Static**을 선택합니다.
  - DHCP 서버에서 네트워크 설정을 검색하려면 **DHCP**를 선택합니다. (eth0 전용)
  - 로컬 IPv6 라우터에서 네트워크 설정을 검색하려면 **Router Assigned**를 선택합니다.
  - 프로토콜을 비활성화하려면 **Disabled**를 선택합니다. IPv4와 IPv6을 모두 비활성화해서는 **안 됩니다**.

경로

Edit 아이콘을 클릭하면 기본 관리 인터페이스에 대한 경로를 보거나 수정할 수 있고, View 아이콘을 클릭하면 경로 통계를 볼 수 있습니다.

추가 네트워크에 대한 새 경로를 만들 수 있습니다. Add 아이콘을 클릭하면 팝업 창이 표시되는데, 여기에 목적지 네트워크 IP 주소, 넷마스크나 접두사 길이, 인터페이스 드롭다운(eth0 등) 및 게이트웨이를 입력할 수 있습니다. 다음 예에서는 다른 네트워크에 대한 경로를 사용하는 몇 가지 방법을 보여줍니다.

- 방어 센터에서, 하나의 방어 센터가 여러 다른 네트워크의 디바이스에서 오는 트래픽을 관리 및 격리하도록 다른 네트워크의 디바이스에 대한 경로를 생성할 수 있습니다.
- 한 디바이스에서 경로를 생성하고 두 개의 서로 다른 네트워크에 있는 방어 센터에 디바이스를 등록하여, 좀 더 넓은 구축 범위에서 방어 센터에 대한 고가용성을 구성할 수 있습니다.

네트워크에 대한 경로를 생성하려면 특정 관리 인터페이스에서 다음 설정을 구성할 수 있습니다.

- **Destination** - 경로를 생성할 네트워크의 목적지 주소.
- **Netmask** 또는 **Prefix Length** - 네트워크의 넷마스크(IPv4) 또는 접두사 길이(IPv6)
- **Interface** - 새 경로에 할당한 어플라이언스의 관리 인터페이스
- **Gateway** - 새 네트워크의 게이트웨이

공유 설정

관리 환경과 상관없이 최대 3개의 DNS 서버 그리고 디바이스의 호스트 이름 및 도메인을 지정할 수 있습니다.

관리 포트를 변경할 수 있습니다. FireSIGHT 시스템 어플라이언스는 기본적으로 포트 8305를 사용하는 양방향 SSL 암호화 통신 채널을 사용하여 통신합니다. Cisco에서는 기본 설정을 유지할 것을 **적극** 권장하지만, 관리 포트가 네트워크의 다른 통신과 충돌하면 다른 포트를 선택할 수 있습니다.

주의 관리 포트를 변경하는 경우 구축에서 서로 통신해야 하는 모든 어플라이언스에 대해 변경해야 합니다.

LCD 패널

Series 3 디바이스에서는 디바이스 전면에 있는 LCD 패널을 사용하여 디바이스 정보를 볼 수 있습니다. Series 3 Management Interfaces 페이지에서 사용자들이 LCD 패널을 사용하여 네트워크 설정을 변경하도록 허용할 수 있습니다.

LCD 패널을 사용하여 관리되는 디바이스의 IP 주소를 수정하려면 관리하는 방어 센터에 변경 사항이 반영되는지 확인하십시오. 경우에 따라 디바이스 관리 설정을 수동으로 수정해야 할 수 있습니다. 자세한 내용은 4-53페이지의 디바이스 관리 설정 수정을/를 참조하십시오.

주의 LCD 패널을 사용하여 리컨피그레이션을 허용할 경우 보안 위험에 노출될 수 있습니다. LCD 패널을 이용하여 네트워크 설정을 구성할 경우 인증은 필요하지 않으며 물리적 액세스만 필요합니다.

대리인

모든 FireSIGHT 시스템 어플라이언스는 443/tcp(HTTPS) 및 80/tcp(HTTP)에서 인터넷에 직접 연결하도록 구성됩니다. E-1페이지의 보안, 인터넷 액세스, 통신 포트을/를 참조하십시오. Cisco NGIPS for Blue Coat X-Series를 제외하고 FireSIGHT 시스템 어플라이언스는 HTTP Digest를 통해 인증할 수 있는 프록시 서버 사용을 지원합니다.

주의 NTLM(NT LAN Manager) 인증을 사용하는 프록시는 정보 수신을 위해 종합 보안 인텔리전스 클라우드와 통신할 수 없습니다. 클라우드 기반 기능을 사용하려면 프록시에 대해 다른 인증을 구성해야 합니다. 자세한 내용은 64-27페이지의 클라우드 통신 활성화을/를 참조하십시오.

관리 인터페이스 수정

라이센스: 모두

Management Interfaces 페이지를 사용하면 방어 센터에서 기본 관리 인터페이스에 대한 기본 설정을 수정할 수 있습니다. Series 3 어플라이언스 및 가상 방어 센터에서 트래픽 채널 및 추가 관리 인터페이스를 활성화 및 구성할 수도 있습니다. Auto Negotiate 값에 대한 변경 사항은 Gigabit 인터페이스에 대해 무시됩니다.

주의 어플라이언스에 물리적으로 액세스할 수 없다면 관리 인터페이스에 대한 설정을 수정하지 마십시오. 웹 인터페이스에 액세스하기 어렵게 만드는 설정을 선택할 수 있습니다.

관리 인터페이스를 수정하려면

액세스: Admin

1단계 **System > Local > Configuration**을 선택합니다.

Information 페이지가 나타납니다.

2단계 **Management Interfaces**를 클릭합니다.

Management Interfaces 페이지가 나타나서 방어 센터의 각 설정에 대한 현재 설정을 표시합니다.

3단계 선택적으로, **Interfaces** 아래에서 구성할 인터페이스 옆에 있는 **Edit**를 클릭합니다.

기본 관리 인터페이스(`eth0`)를 수정하거나, 추가 관리 인터페이스(`eth1` 등)를 활성화하고 구성할 수 있습니다. 각 추가 관리 인터페이스에 대해 고유한 고정 IP 주소(IPv4 또는 IPv6) 또는 호스트 이름을 할당해야 합니다. 모드, 링크, MTU 및 IP 컨피그레이션을 설정하는 것 외에도 처리할 트래픽 채널을 선택할 수 있습니다.

4단계 선택적으로, **Routes** 아래에서 목적지 네트워크 IP 주소, 넷마스크나 접두사 길이 및 게이트웨이를 입력하고, 이 네트워크 경로에 대해 사용할 관리 인터페이스를 지정합니다.

돋보기 아이콘을 클릭할 때 경로 통계도 볼 수 있습니다.

5단계 선택적으로, 관리 네트워크 프로토콜에 의존하지 않는 네트워크 설정을 **Shared Settings** 아래에서 지정합니다.

또한 최대 3개의 DNS 서버 그리고 어플라이언스의 호스트 이름 및 도메인을 지정할 수 있습니다. 이전 단계에서 **DHCP**를 선택한 경우 이러한 공유 설정을 수동으로 지정할 수 없습니다.

주의 Cisco에서는 기본 설정을 유지할 것을 **적극** 권장하지만, 관리 포트가 네트워크의 다른 통신과 충돌하면 다른 포트를 선택할 수 있습니다. 관리 포트를 변경하는 경우 구축에서 서로 통신해야 하는 **모든** 어플라이언스에 대해 변경해야 합니다.

6단계 선택적으로, 디바이스의 LCD 패널을 사용하여 네트워크 설정을 변경하도록 하려면 Series 3 디바이스의 LCD Panel 아래에서 **Allow reconfiguration of network settings** 확인란을 선택합니다.

주의 LCD 패널을 사용하여 리컨피그레이션을 허용할 경우 보안 위험에 노출될 수 있습니다. LCD 패널을 이용하여 네트워크 설정을 구성할 경우 인증은 필요하지 않으며 물리적 액세스만 필요합니다. 이 옵션을 활성화하면 보안 문제가 발생할 수 있다는 경고 메시지가 표시됩니다.

7단계 선택적으로, **Proxy** 아래에서 프록시를 활성화하는 확인란을 선택하고 다음을 수행합니다.

- 프록시 서버의 IP 주소 또는 정규화된 도메인 이름을 **HTTP Proxy** 필드에 입력합니다. **Port** 필드에 포트를 입력합니다.
- 선택적으로, **Use Proxy Authentication**을 선택하고 **User Name** 및 **Password**를 입력하여 인증 자격 증명을 제공합니다.

8단계 어플라이언스의 네트워크 설정 구성을 완료하고 **Save**를 클릭합니다.

네트워크 설정이 변경됩니다. 어플라이언스의 호스트 이름을 변경한 후 어플라이언스를 재부팅하기 전에는 새 이름이 syslog에 반영되지 않습니다.

시스템 종료 및 재시작

라이센스: 모두

어플라이언스에서 프로세스를 제어하기 위한 몇 가지 옵션이 있습니다. 다음이 가능합니다:

- 어플라이언스 종료
- 어플라이언스 재부팅
- 어플라이언스에서 통신, 데이터베이스, HTTP 서버 프로세스 다시 시작(일반적으로 문제 해결 중에 사용됨)
- Snort 프로세스 다시 시작

주의 전원 버튼을 사용하여 어플라이언스를 종료하지 **마십시오.** 데이터가 손실될 수 있습니다. Appliance Process 페이지를 통해 어플라이언스를 완전히 종료하십시오.

어플라이언스를 종료하거나 다시 시작하려면

액세스: Admin

1단계 **System > Local > Configuration**을 선택합니다.

Information 페이지가 나타납니다.

2단계 **Process**를 클릭합니다.

Appliance Process 페이지가 나타납니다.

3단계 수행할 명령을 지정합니다.

방어 센터 에서

- 어플라이언스를 종료하려면 **Shutdown 방어 센터** 옆에 있는 **Run Command**를 클릭합니다.
- 어플라이언스를 재부팅하려면 **Reboot 방어 센터** 옆에 있는 **Run Command**를 클릭합니다. 이렇게 하면 방어 센터에서 로그아웃됩니다.
- 어플라이언스를 다시 시작하려면 **Restart 방어 센터 Console** 옆에 있는 **Run Command**를 클릭합니다. 방어 센터를 다시 시작하면 삭제된 호스트가 네트워크 맵에 다시 나타날 수 있습니다.

참고 방어 센터를 재부팅하면 시스템에서는 완료하는 데 1시간 정도 걸릴 수 있는 데이터베이스 점검을 실행합니다.

관리되는 디바이스에서

- 어플라이언스를 종료하려면 **Shutdown Appliance** 옆에 있는 **Run Command**를 클릭합니다.
- 어플라이언스를 재부팅하려면 **Reboot Appliance** 옆에 있는 **Run Command**를 클릭합니다. 이렇게 하면 디바이스에서 로그아웃됩니다.
- 어플라이언스를 다시 시작하려면 **Restart Appliance Console** 옆에 있는 **Run Command**를 클릭합니다.
- Snort 프로세스를 다시 시작하려면 **Restart Snort** 옆에 있는 **Run Command**를 클릭합니다.

참고 관리되는 디바이스를 재부팅하면 시스템에서는 완료하는 데 1시간 정도 걸릴 수 있는 데이터베이스 점검을 실행합니다.

수동으로 시간 설정

라이센스: 모두

현재 적용된 시스템 정책에서 Time Synchronization 설정이 **Manually in Local Configuration**이면 로컬 컨피그레이션의 Time 페이지를 사용하여 어플라이언스의 시간을 수동으로 설정할 수 있습니다.

Cisco NGIPS for Blue Coat X-Series에 대한 시간 설정을 관리하려면 명령줄 인터페이스나 운영 체제 인터페이스 등 기본 애플리케이션을 사용해야 합니다. 자세한 내용은 *Cisco NGIPS for Blue Coat X-Series 설치 가이드*을/를 참조하십시오.

어플라이언스가 NTP를 기반으로 시간을 동기화하는 경우 수동으로 시간을 변경할 수 없습니다. 대신 Time 페이지의 NTP Status 섹션에서는 다음 정보를 제공합니다.

표 64-5 NTP 상태

열	설명
NTP 서버	구성된 NTP 서버의 IP 주소 및 이름.
상태	NTP 서버 시간 동기화의 상태. 다음 상태가 나타날 수 있습니다. • **Being Used** - 어플라이언스가 NTP 서버와 동기화됨을 나타냅니다. • **Available** - NTP 서버를 사용할 수 있지만 시간이 아직 동기화되지 않았음을 나타냅니다. • **Not Available** - NTP 서버가 컨피그레이션에 있지만 NTP 디먼이 이를 사용할 수 없음을 나타냅니다. • **Pending** - NTP 서버가 새로운 것이거나 NTP 디먼이 최근에 다시 시작되었음을 나타냅니다. 시간이 지남에 따라 값이 **Being Used**, **Available**, 또는 **Not Available**로 변경되어야 합니다. • **Unknown** - NTP 서버의 상태를 알 수 없음을 나타냅니다.
Offset	어플라이언스 및 구성된 NTP 서버 간 밀리초 단위의 시간 차이. 음수 값은 어플라이언스가 NTP 서버 뒤에 있음을 나타내고, 양수 값은 그 반대를 나타냅니다.
마지막 업데이트	시간이 NTP 서버와 마지막으로 동기화된 후 경과한 기간(초). NTP 디먼은 몇 가지 조건을 기반으로 동기화 시간을 자동으로 조정합니다. 예를 들어 300초와 같이 좀 더 긴 업데이트 시간이 있으면, 이는 시간이 비교적 안정적이며 NTP 디먼이 더 낮은 업데이트 증분을 사용할 필요가 없다고 결정했음을 나타냅니다.

시스템 정책의 시간 설정에 대한 자세한 내용은 63-25페이지의 시간 동기화을/를 참조하십시오.

시간을 수동으로 구성하려면

액세스: Admin

1단계 **System > Local > Configuration**을 선택합니다.

Information 페이지가 나타납니다.

2단계 **Time**을 클릭합니다.

Time 페이지가 나타납니다.

3단계 **Set Time** 드롭다운 목록에서 다음을 선택합니다.

- year
- month
- day
- hour
- minute

4단계 **Apply**를 클릭합니다.

시간이 업데이트됩니다. 표준 시간대 변경에 대한 자세한 내용은 71-7페이지의 기본 표준 시간대 설정을/를 참조하십시오.

원격 스토리지 관리

라이센스: 모두

방어 센터 에서 백업과 보고서를 위한 로컬 또는 원격 스토리지를 사용할 수 있습니다. 백업 및 보고서 원격 스토리지용으로 NFS(Network File System), SSH(Secure Shell) 또는 SMB(Server Message Block)/CIFS(Common Internet File System)를 사용할 수 있습니다. 백업은 한 원격 시스템으로 전송하고 보고서는 다른 원격 시스템으로 전송할 수는 없습니다. 그러나 둘 중 하나는 원격 시스템으로 전송하고 나머지는 로컬 방어 센터에 저장할 수는 있습니다. 백업 및 복원에 대한 자세한 내용은 70-1페이지의 백업 및 복원 사용을/를 참조하십시오.

팁 원격 스토리지를 구성 및 선택한 후, 연결 데이터베이스 한도를 높이지 **않은 경우에만** 로컬 스토리지로 다시 전환할 수 있습니다.

외부 원격 스토리지 시스템이 정상적으로 작동하는지와 방어 센터에서 액세스할 수 있는지를 확인해야 합니다.

백업 및 보고서 스토리지 옵션 중 하나를 선택합니다.

- 외부 원격 스토리지를 비활성화하고 백업 및 보고서 스토리지로 로컬 방어 센터을(를) 사용하려면 64-16페이지의 로컬 스토리지 사용을/를 참조하십시오.
- 백업 및 보고서 스토리지로 NFS를 사용하려면 64-16페이지의 원격 스토리지에 NFS 사용을/를 참조하십시오.
- 백업 및 보고서 스토리지로 SSH(Secure Shell)를 통한 SCP를 사용하려면 64-17페이지의 원격 스토리지에 SSH 사용을/를 참조하십시오.
- 백업 및 보고서 스토리지로 SMB를 사용하려면 64-18페이지의 원격 스토리지에 SMB 사용을/를 참조하십시오.

참고 Cisco NGIPS for Blue Coat X-Series의 데이터를 관리하는 데에는 원격 백업 및 복원을 사용할 수 없습니다.

로컬 스토리지 사용

라이센스: 모두

백업 및 보고서를 로컬 방어 센터에 저장할 수 있습니다.

백업 및 보고서를 로컬에 저장하려면

액세스: Admin

1단계 **System > Local > Configuration**을 선택합니다.

Information 페이지가 나타납니다.

2단계 **Remote Storage Device**를 클릭합니다.

Remote Storage Device 페이지가 나타납니다.

3단계 **Storage Type** 드롭다운 목록에서 **Local (No Remote Storage)**를 선택합니다.

4단계 **Save**를 클릭합니다.

스토리지 위치 선택이 저장됩니다.

팁 로컬 스토리지에서는 **Test** 버튼을 사용하지 않습니다.

원격 스토리지에 **NFS** 사용

라이센스: 모두

보고서 및 백업을 저장하는 데 NFS(Network File System) 프로토콜을 선택할 수 있습니다. 선택적으로, NFS mount man 페이지에 설명된 대로 마운트 이진 옵션 중 하나를 사용하려면 **Use Advanced Options** 확인란을 선택합니다.

NFS를 사용하여 백업 및 보고서를 저장하려면

액세스: Admin

1단계 **System > Local > Configuration**을 선택합니다.

Information 페이지가 나타납니다.

2단계 **Remote Storage Device**를 클릭합니다.

Remote Storage Device 페이지가 나타납니다.

3단계 **Storage Type** 드롭다운 목록에서 **NFS**를 선택합니다.

페이지가 새로 고쳐지고 NFS 스토리지 컨피그레이션 옵션이 표시됩니다.

4단계 연결 정보를 추가합니다.

- 스토리지 시스템의 IPv4 주소 또는 호스트 이름을 **Host** 필드에 입력합니다.
- 스토리지 영역에 대한 경로를 **Directory** 필드에 입력합니다.

5단계 필수 명령줄 옵션이 있는 경우 **Use Advanced Options**를 선택합니다.

마운트 이진 옵션을 입력할 수 있는 **Command Line Options** 필드가 나타납니다.

6단계 **System Usage** 아래에서 다음 중 하나 또는 둘 모두를 선택합니다.

- 지정된 호스트에 백업을 저장하려면 **Use for Backups**를 선택합니다.
- 지정된 호스트에 보고서를 저장하려면 **Use for Reports**를 선택합니다.
- 원격 스토리지용 백업에 대해 **Disk Space Threshold**를 입력합니다. 기본값은 90%입니다.

7단계 선택적으로 **Test**를 클릭합니다.

테스트는 방어 센터가 지정된 호스트 및 디렉토리에 액세스할 수 있는지를 확인합니다.

8단계 **Save**를 클릭합니다.

원격 스토리지 컨피그레이션이 저장됩니다.

원격 스토리지에 SSH 사용

라이센스: 모두

보고서 및 백업을 저장하는 데 SCP(secure copy)를 사용하려면 SSH를 선택할 수 있습니다. 선택적으로, SSH mount man 페이지에 설명된 대로 마운트 이진 옵션 중 하나를 사용하려면 **Use Advanced Options** 확인란을 선택합니다.

주의 어플라이언스에서 STIG 규정 준수를 활성화한 경우 해당 어플라이언스의 원격 스토리지에 SSH를 사용할 수 없습니다. 자세한 내용은 63-24페이지의 STIG 규정 준수 활성화을/를 참조하십시오.

SSH를 사용하여 백업 및 보고서를 저장하려면

액세스: Admin

1단계 **System > Local > Configuration**을 선택합니다.

Information 페이지가 나타납니다.

2단계 **Remote Storage Device**를 클릭합니다.

Remote Storage Device 페이지가 나타납니다.

3단계 **Storage Type**에서 **SSH**를 선택합니다.

페이지가 새로 고쳐지고 SSH를 통한 SCP 스토리지 컨피그레이션 옵션이 표시됩니다.

4단계 연결 정보를 추가합니다.

- 스토리지 시스템의 IP 주소 또는 호스트 이름을 **Host** 필드에 입력합니다.
- 스토리지 영역에 대한 경로를 **Directory** 필드에 입력합니다.
- 스토리지 시스템의 사용자 이름을 **Username** 필드에 입력하고 해당 사용자의 비밀번호를 **Password** 필드에 입력합니다. 도메인을 지정하려면 사용자 이름 앞에 슬래시(/)로 시작되는 도메인을 입력합니다.
- SSH 키를 사용하려면 **SSH Public Key** 필드의 내용을 복사하여 authorized_keys 파일에 붙여넣습니다.

5단계 필수 명령줄 옵션이 있는 경우 **Use Advanced Options**를 선택합니다.

마운트 이진 옵션을 입력할 수 있는 **Command Line Options** 필드가 나타납니다.

6단계 System Usage 아래에서 다음 중 하나 또는 둘 모두를 선택합니다.

- 지정된 호스트에 백업을 저장하려면 **Use for Backups**를 선택합니다.
- 지정된 호스트에 보고서를 저장하려면 **Use for Reports**를 선택합니다.

7단계 선택적으로 **Test**를 클릭합니다.

테스트는 방어 센터가 지정된 호스트 및 디렉토리에 액세스할 수 있는지를 확인합니다.

8단계 **Save**를 클릭합니다.

원격 스토리지 컨피그레이션이 저장됩니다.

원격 스토리지에 SMB 사용

라이센스: 모두

보고서 및 백업을 저장하는 데 SMB(Server Message Block) 프로토콜을 선택할 수 있습니다. 선택적으로, SMB mount man 페이지에 설명된 대로 마운트 이진 옵션 중 하나를 사용하려면 **Use Advanced Options** 확인란을 선택합니다. 예를 들어 SMB를 사용하면 다음 형식으로 **Command Line Options** 필드에서 보안 모드로 들어갈 수 있습니다.

```
sec=mode
```

여기서 *mode*는 원격 스토리지에 사용할 보안 모드입니다. 설정 옵션은 보안 모드 설정 표를 참조하십시오.

표 64-6 보안 모드 설정

Mode	설명
[없음]	Null 사용자(이름 없음)로서 연결을 시도합니다.
krb5	Kerberos 버전 5 인증을 사용합니다.
krb5i	Kerberos 인증 및 패킷 서명을 사용합니다.
ntlm	NTLM 비밀번호 해싱을 사용합니다. (기본값)
ntlmi	서명과 함께 NTLM 비밀번호 해싱을 사용합니다(서버에서 서명을 요구하는 경우 /proc/fs/cifs/PacketSigningEnabled가 On이면 기본값).
ntlmv2	NTLMv2 비밀번호 해싱을 사용합니다.
ntlmv2i	패킷 서명과 함께 NTLMv2 비밀번호 해싱을 사용합니다.

SMB를 사용하여 백업 및 보고서를 저장하려면

액세스: Admin

1단계 **System > Local > Configuration**을 선택합니다.

Information 페이지가 나타납니다.

2단계 **Remote Storage Device**를 클릭합니다.

Remote Storage Device 페이지가 나타납니다.

3단계 **Storage Type**에서 **SMB**를 선택합니다.

페이지가 새로 고쳐지고 SMB 스토리지 컨피그레이션 옵션이 표시됩니다.

4단계 연결 정보를 추가합니다.

- 스토리지 시스템의 IPv4 주소 또는 호스트 이름을 **Host** 필드에 입력합니다.

- 스토리지 영역의 공유를 **Share** 필드에 입력합니다. 시스템에서는 전체 파일 경로가 아니라 상위 레벨의 공유만 인식합니다. 지정한 Share 디렉토리를 원격 백업 목적지로 사용하려면 Windows 시스템에서 공유되는 것이어야 합니다.
- 선택적으로, 원격 스토리지 시스템의 도메인 이름을 **Domain** 필드에 입력합니다.
- 스토리지 시스템의 사용자 이름을 **Username** 필드에 입력하고 해당 사용자의 비밀번호를 **Password** 필드에 입력합니다.

5단계 필수 명령줄 옵션이 있는 경우 **Use Advanced Options**를 선택합니다.

마운트 이진 명령(예: 보안 모드)을 입력할 수 있는 **Command Line Options** 필드가 나타납니다. 자세한 내용은 64-18페이지의 표 64-6보안 모드 설정을/를 참조하십시오.

6단계 System Usage 아래에서 다음 중 하나 또는 둘 모두를 선택합니다.

- 지정된 호스트에 백업을 저장하려면 **Use for Backups**를 선택합니다.
- 지정된 호스트에 보고서를 저장하려면 **Use for Reports**를 선택합니다.

7단계 선택적으로 **Test**를 클릭합니다.

테스트는 방어 센터가 지정된 호스트 및 디렉토리에 액세스할 수 있는지를 확인합니다.

8단계 **Save**를 클릭합니다.

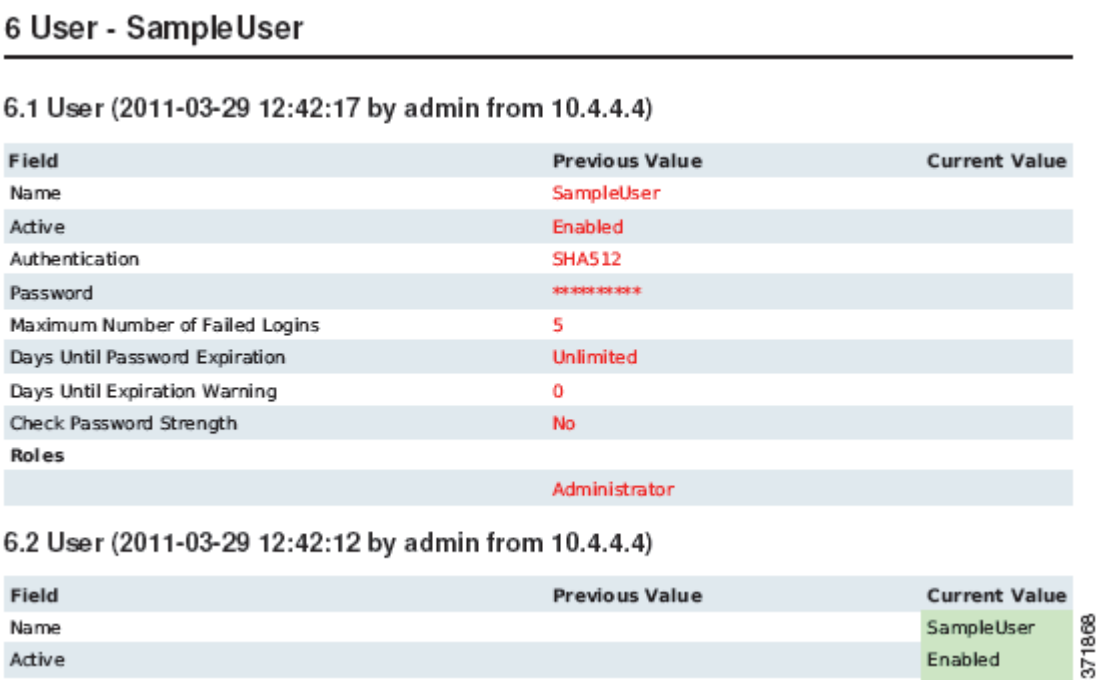
원격 스토리지 컨피그레이션이 저장됩니다.

변경 조정 이해

라이센스: 모두

사용자가 변경하는 내용을 모니터링하고 그러한 변경이 회사의 기본 표준을 따르는지 확인하려면 지난 24시간 동안 시스템에 대한 변경 사항의 자세한 보고서를 이메일로 전송하도록 시스템을 구성할 수 있습니다. 사용자가 시스템 컨피그레이션에 변경 사항을 저장할 때마다 변경에 대한 스냅샷이 생성됩니다. 변경 조정 보고서는 이러한 스냅샷의 정보를 결합하여 최신 시스템 변경 사항에 대한 명확한 요약을 제공합니다.

다음 샘플 그림에는 예제 변경 조정 보고서의 User 페이지가 표시되며, 각 컨피그레이션의 이전 값과 변경 이후의 값이 모두 나열되어 있습니다. 여러 사용자가 동일한 컨피그레이션을 여러 번 변경하면 보고서에는 최근 것부터 시간순으로 각 변경 사항의 요약이 나열됩니다.



6 User - SampleUser

6.1 User (2011-03-29 12:42:17 by admin from 10.4.4.4)

Field	Previous Value	Current Value
Name	SampleUser	
Active	Enabled	
Authentication	SHA512	
Password	********	
Maximum Number of Failed Logins	5	
Days Until Password Expiration	Unlimited	
Days Until Expiration Warning	0	
Check Password Strength	No	
Roles		
	Administrator	

6.2 User (2011-03-29 12:42:12 by admin from 10.4.4.4)

Field	Previous Value	Current Value
Name		SampleUser
Active		Enabled

371868

지난 24시간 동알 변경된 내용을 볼 수 있습니다. 그러나 그 이전 변경 사항을 보려면 감사 로그를 확인해야 합니다. 자세한 내용은 69-7페이지의 변경 사항 검토를 위해 감사 로그 사용을/를 참조하십시오.

변경 조정 기능을 사용하려면

액세스: Admin

1단계 **System > Local > Configuration**을 선택합니다.

Information 페이지가 나타납니다.

2단계 **Change Reconciliation**을 클릭합니다.

Change Reconciliation 페이지가 나타납니다.

3단계 **Enable** 확인란을 선택합니다.

4단계 시스템에서 변경 조정 보고서를 전송하도록 할 시간을 **Time to Run** 드롭다운 목록에서 선택합니다.

5단계 보고서 수신자의 이메일 주소를 **Email to** 필드에 입력합니다. 언제든 최신 변경 조정 보고서의 또 다른 사본을 수신자에게 보내려면 **Resend Last Report**를 클릭할 수 있습니다.

참고 변경 조정 보고서를 받으려면 먼저 메일 릴레이 호스트 및 알림 주소를 구성해야 합니다. 자세한 내용은 63-18페이지의 메일 릴레이 호스트 및 알림 주소 구성을/를 참조하십시오.

6단계 선택적으로, 변경 조정 보고서에 정책 변경 사항의 기록을 포함하려면 **Include Policy Configuration**을 선택합니다. 여기에는 액세스 제어, 침입, 시스템, 상태 및 네트워크 검색 정책에 대한 변경 사항이 포함됩니다. 이 옵션을 선택하지 않으면 정책에 대한 변경 사항이 보고서에 표시되지 않습니다.

참고 관리되는 디바이스에서는 이 옵션을 사용할 수 없습니다.

7단계 선택적으로, 변경 조정 보고서에 지난 24시간 동안의 모든 변경 사항 기록을 포함하려면 **Show Full Change History**를 선택합니다. 이 옵션을 선택하지 않으면 보고서에는 각 카테고리에 대한 변경 사항의 통합된 보기만 포함됩니다.

8단계 **Save**를 클릭합니다.

변경 내용이 저장되었습니다. 선택한 시간에 보고서가 매일 실행됩니다.

원격 콘솔 액세스 관리

라이센스: 모두

지원되는 디바이스: 기능에 따라 다름

지원되는 Defense Center: 기능에 따라 다름

VGA 포트(기본값) 또는 물리적 어플라이언스의 시리얼 포트를 통해 어플라이언스에 원격으로 액세스하도록 하려면 Linux 시스템 콘솔을 사용할 수 있습니다. 조직의 Cisco 구축의 물리적 레이아웃에 가장 적합한 옵션을 선택하십시오.

어플라이언스의 관리 인터페이스에 로그인하지 않고 Series 3 어플라이언스를 원격으로 모니터링 또는 관리하려면 SOL(Serial Over LAN) 연결의 기본(`eth0`) 관리 인터페이스에서 LOM(Lights-Out Management)을 사용할 수 있습니다. OOB(Out of Band) 관리 연결에서 명령줄 인터페이스를 사용하여 섀시 일련 번호 보기, 팬 속도와 온도 등의 조건 모니터링 등 제한적인 작업을 수행할 수 있습니다. Series 2, 가상 어플라이언스, ASA FirePOWER 모듈 및 Cisco NGIPS for Blue Coat X-Series는 LOM을 지원하지 않습니다.

어플라이언스 및 어플라이언스를 관리하는 사용자 모두에 대해 LOM을 활성화해야 합니다. 어플라이언스와 사용자를 활성화한 후 어플라이언스에 대한 액세스 및 관리를 위해 서드파티 IPMI(Intelligent Platform Management Interface) 유틸리티를 사용합니다.

참고 3D71xx, 3D82xx 또는 3D83xx 디바이스에 대한 BMC(baseboard management controller)는 호스트 전원이 켜져 있을 때 1Gbps 링크 속도를 통해서만 액세스할 수 있습니다. 디바이스 전원이 꺼져 있으면 BMC는 10 및 100Mbps의 이더넷 링크만 설정할 수 있습니다. 따라서 LOM을 사용하여 디바이스 전원을 원격으로 제어하는 경우 10 및 100Mbps 링크 속도만을 사용하여 디바이스를 네트워크에 연결하십시오.

자세한 내용은 다음 항목을 참조하십시오.

- 64-21페이지의 어플라이언스에서 원격 콘솔 설정 구성
- 64-23페이지의 Lights-Out Management 사용자 액세스 활성화
- 64-24페이지의 Serial Over LAN 연결 사용
- 64-25페이지의 Lights-Out Management 사용

어플라이언스에서 원격 콘솔 설정 구성

라이센스: 모두

지원되는 디바이스: 기능에 따라 다름

지원되는 Defense Center: 기능에 따라 다름

사용하려는 원격 콘솔 액세스 옵션을 선택하고 구성하려면 원격으로 관리할 어플라이언스의 웹 인터페이스를 사용할 수 있습니다.

Series 2, 가상 어플라이언스, ASA FirePOWER 모듈 및 Cisco NGIPS for Blue Coat X-Series는 LOM을 지원하지 않습니다.

참고 LOM/SOL을 사용하여 Series 3 디바이스에 연결하기 전에 디바이스의 관리 인터페이스에 연결된 모든 타사 스위칭 장비에서 STP(Spanning Tree Protocol)를 비활성화해야 합니다.

원격 콘솔 설정을 구성하려면

액세스: Admin

1단계 **System > Local > Configuration**을 선택합니다.

Information 페이지가 나타납니다.

2단계 **Console Configuration(콘솔 컨피그레이션)**을 선택합니다.

Console Configuration(콘솔 컨피그레이션) 페이지가 나타납니다.

3단계 원격 콘솔 액세스 옵션을 선택합니다.

- 어플라이언스의 VAG 포트를 사용하려면 **VGA**를 선택합니다. 이것이 기본 옵션입니다.
- 어플라이언스의 시리얼 포트를 사용하거나 Series 3 방어 센터, 3D7050 또는 8000 Series 디바이스에서 LOM/SOL을 사용하려면 **Physical Serial Port**를 선택합니다.

  3D2100, 3D2500, 3D3500, 3D4500 관리되는 디바이스에는 시리얼 포트가 없습니다.
- 7000 Series 디바이스에서 LOM/SOL을 사용하려면 **Lights-Out Management**를 선택합니다(3D7050 제외). 이러한 디바이스에서는 SOL과 일반 시리얼 연결을 동시에 사용할 수 없습니다.

Physical Serial Port(물리적 시리얼 포트) 또는 **Lights-Out Management(Lights-Out 관리)**를 선택하면 LOM 설정이 나타납니다.

참고 원격 콘솔을 70xx 제품군 디바이스(3D7050 제외)의 **Physical Serial Port**에서 **Lights-Out Management**로 변경하거나 **Lights-Out Management**에서 **Physical Serial Port**로 변경할 경우 예상 부팅 프롬프트를 확인하려면 어플라이언스를 두 번 재부팅해야 할 수 있습니다.

4단계 SOL을 통해 LOM을 구성하려면 적절한 설정을 입력합니다.

- 어플라이언스의 DHCP **컨피그레이션(DHCP** 또는 **Static(정적))**
- LOM에 사용할 **IP 주소**

참고 LOM IP 주소는 어플라이언스의 관리 인터페이스 IP 주소와 달라야 합니다.

- 어플라이언스의 **Netmask(넷마스크)**
- 어플라이언스의 **Default Gateway(기본 게이트웨이)**

5단계 **Save**를 클릭합니다.

어플라이언스의 원격 콘솔 컨피그레이션이 저장됩니다. Lights-Out Management(Lights-Out 관리)를 구성한 경우 한 명 이상의 사용자를 위해 활성화해야 합니다. 64-23페이지의 Lights-Out Management 사용자 액세스 활성화을/를 참조하십시오.

Lights-Out Management 사용자 액세스 활성화

라이센스: 모두

지원되는 디바이스: Series 3

지원되는 Defense Center: Series 3

또한 기능을 사용할 사용자에게 Lights-Out Management 권한을 명시적으로 부여해야 합니다. 각 어플라이언스의 로컬 웹 인터페이스를 사용하여 어플라이언스별로 LOM 및 LOM 사용자를 구성합니다. 즉, 방어 센터를 사용하여 관리되는 디바이스에서 LOM을 구성할 수 없습니다. 마찬가지로, 사용자는 어플라이언스별로 독립적으로 관리되므로 방어 센터에서 LOM 지원 사용자를 만들 경우 해당 기능이 관리되는 디바이스의 사용자로 전달되지 않습니다.

LOM 사용자는 또한 다음과 같은 제한이 있습니다.

- 사용자에게 관리자 역할을 할당해야 합니다.
- 사용자 이름은 최대 16자의 영숫자로 지정할 수 있습니다. 하이픈과 이보다 긴 사용자 이름은 LOM 사용자에게 지원되지 않습니다.
- 비밀번호는 최대 영숫자 20자로 구성할 수 있습니다(3D7100 제품군 디바이스 제외). LOM이 3D7110, 3D7115, 3D7120 또는 3D7125 디바이스에서 활성화되면 비밀번호는 최대 영숫자 16자로 구성할 수 있습니다. 각각 20자 또는 16자가 넘는 비밀번호는 LOM 사용자에 대해 지원되지 않습니다. 사용자의 LOM 비밀번호는 해당 사용자의 시스템 비밀번호와 동일합니다. Cisco에서는 어플라이언스에서 지원되는 최대 길이로 사전에 없는 복잡한 비밀번호를 사용하고 3개월에 한 번씩 변경할 것을 권장합니다.
- Series 3방어 센터 및 8000 Series 디바이스는 최대 13명의 LOM 사용자를 지원합니다. 7000 Series 디바이스는 최대 8명의 LOM 사용자를 지원합니다.

어떤 역할의 사용자가 로그인한 상태에서 LOM으로 그 역할을 비활성화했다가 다시 활성화할 경우 또는 사용자의 로그인 세션 중에 백업에서 사용자 또는 사용자 역할을 복원할 경우, 사용자가 다시 웹 인터페이스에 로그인해야 IPMItool 명령에 다시 액세스할 수 있습니다. 자세한 내용은 61-49 페이지의 사전 정의 사용자 역할 관리을/를 참조하십시오.

Lights-Out Management 사용자 액세스를 활성화하거나 보려면

액세스: Admin

1단계 **System > Local > User Management**를 선택합니다.

User Management 페이지가 나타납니다.

2단계 다음 옵션을 이용할 수 있습니다.

- 기존 사용자에 대해 LOM 사용자 액세스를 허용하려면 목록의 사용자 이름 옆에 있는 수정 아이콘( )을 클릭합니다.
- 새 사용자에 대한 LOM 사용자 액세스를 허용하려면 **Create User**를 클릭합니다.

3단계 User Configuration 아래에서 Administrator 역할을 활성화합니다.

Administrator Options가 나타납니다.

4단계 **Allow Lights-Out Management Access** 확인란을 선택합니다.

5단계 **Save**를 클릭합니다.

사용자에게 이 어플라이언스에 대한 LOM 액세스가 제공됩니다.

Serial Over LAN 연결 사용

라이센스: 모두

지원되는 디바이스: Series 3

지원되는 Defense Center: Series 3

컴퓨터에서 타사 IPMI 유틸리티를 사용하여 어플라이언스에 대한 Serial Over LAN 연결을 만듭니다. Linux와 유사한 컴퓨터 환경 또는 Mac 환경에서는 IPMItool을 사용하고, Windows 환경에서는 IPMIutil을 사용합니다.

참고 Cisco에서는 IPMItool 버전 1.8.12 이상을 사용할 것을 권장합니다.

Linux

IPMItool은 많은 배포의 표준이며 곧바로 사용 가능합니다.

Mac

Mac에는 IPMItool을 설치해야 합니다. 먼저 Mac에 Apple의 XCode Developer 툴이 설치되었는지 확인하고, 명령줄 개발을 위한 선택적인 구성 요소가 설치되었는지 확인합니다(새 버전에서는 UNIX Development 및 System Tools, 이전 버전에서는 Command Line Support). 그런 다음 macports 및 IPMItool을 설치할 수 있습니다. 자세히 알아보려면 자주 사용하는 검색 엔진을 사용하거나 다음 사이트를 이용하십시오.

```
https://developer.apple.com/technologies/tools/
http://www.macports.org/
```

Windows

Windows에서는 IPMIutil을 컴파일해야 합니다. 컴파일러에 액세스할 수 없는 경우 IPMIutil 자체를 사용하여 컴파일할 수 있습니다. 자세히 알아보려면 자주 사용하는 검색 엔진을 사용하거나 다음 사이트를 이용하십시오.

```
http://ipmiutil.sourceforge.net/
```

IPMI 유틸리티 명령 이해

IPMI 유틸리티에 사용되는 명령은 다음 IPMItool 예와 같은 세그먼트로 구성됩니다.

```
ipmitool -I lanplus -H IP_address -U user_name command
```

여기서 각 항목은 다음을 나타냅니다.

- `ipmitool` - 유틸리티를 호출합니다.
- `-I lanplus` - 세션의 암호화를 활성화합니다.
- `-H IP_address` - 액세스하려는 어플라이언스의 IP 주소를 나타냅니다.
- `-U user_name` - 권한 있는 사용자의 이름입니다.
- `-command` - 사용할 명령의 이름입니다.

참고 Cisco에서는 IPMItool 버전 1.8.12 이상을 사용할 것을 권장합니다.

Windows에서는 동일한 명령이 다음과 같이 표시됩니다.

```
ipmiutil command -V 4 -J 3 -N IP_address -U user_name
```

이 명령을 실행하면 어플라이언스의 명령줄로 연결됩니다. 여기에서 마치 실제 어플라이언스에 있는 것처럼 로그인할 수 있습니다. 비밀번호를 입력하라는 프롬프트가 표시될 수 있습니다.

Serial Over LAN 연결을 생성하려면

액세스: Admin with LOM access

1단계 다음의 명령을 입력합니다.

IPMItool의 경우:

```
ipmitool -I lanplus -H IP_address -U user_name sol activate
```

참고 Cisco에서는 IPMItool 버전 1.8.12 이상을 사용할 것을 권장합니다.

IPMIutil의 경우:

```
ipmiutil -J 3 -H IP_address -U username sol -a
```

어플라이언스에 대한 명령줄 로그인이 나타납니다. 비밀번호를 입력하라는 프롬프트가 표시될 수 있습니다.

Lights-Out Management 사용

라이센스: 모두

지원되는 디바이스: Series 3

지원되는 Defense Center: Series 3

Lights-Out Management를 사용하면 어플라이언스에 로그인하지 않고도 기본(`eth0`) 관리 인터페이스에서 SOL 연결을 통해 제한된 작업을 수행할 수 있습니다. 다음 표에 나열된 명령 중 하나가 뒤에 오는 SOL 연결을 생성하기 위한 명령을 사용합니다. 명령이 완료되면 연결이 종료됩니다. 일부 전원 제어 명령은 70xx 제품군 디바이스에서 유효합니다.

참고 3D71xx, 3D82xx 또는 3D83xx 디바이스에 대한 BMC(baseboard management controller)는 호스트 전원이 켜져 있을 때 1Gbps 링크 속도를 통해서만 액세스할 수 있습니다. 디바이스 전원이 꺼져 있으면 BMC는 10 및 100Mbps의 이더넷 링크만 설정할 수 있습니다. 따라서 LOM을 사용하여 디바이스 전원을 원격으로 제어하는 경우 10 및 100Mbps 링크 속도만을 사용하여 디바이스를 네트워크에 연결하십시오.

주의 드물긴 하지만, 어플라이언스의 관리 인터페이스와 다른 서브넷에 있으며 어플라이언스가 DHCP로 구성되어 있는 경우 Series 3 어플라이언스에서 LOM 기능에 액세스하려고 시도하면 실패할 수 있습니다. 이런 일이 발생하면 어플라이언스에서 LOM을 비활성화한 후 다시 활성화하거나, 동일한 서브넷의 컴퓨터를 어플라이언스로 사용하여 관리 인터페이스를 ping할 수 있습니다. 이렇게 하면 LOM을 사용할 수 있게 됩니다.

주의 Cisco에서는 IPMI(Intelligent Platform Management Interface) 표준(CVE-2013-4786)에 내재된 취약성에 대해 잘 알고 있습니다. 어플라이언스에서 LOM(Lights-Out Management)을 활성화하면 이 취약성이 노출됩니다. 이 취약성을 완화하려면 신뢰할 수 있는 사용자만 액세스할 수 있는 안전한 관리 네트워크에 어플라이언스를 구축하고, 어플라이언스에서 지원되는 최대 길이로 사전에 없는 복잡한 비밀번호를 사용하고 3개월에 한 번씩 변경하십시오. 이 취약성이 노출되지 않도록 하려면 LOM을 활성화하지 마십시오.

어플라이언스에 액세스하려는 모든 시도가 실패한 경우 LOM을 사용하여 어플라이언스를 원격으로 다시 시작할 수 있습니다. SOL 연결이 활성 상태일 때 시스템이 다시 시작되면 LOM 세션이 끊기거나 시간 초과될 수 있습니다.

주의 다시 시작하려는 다른 시도에 응답하지 않는 상황이 아니면 어플라이언스를 다시 시작하지 **마십시오**. 어플라이언스를 원격으로 다시 시작하는 경우 시스템이 정상적으로 재부팅되지 않으며, 데이터가 손실될 수 있습니다.

표 64-7 Lights-Out Management 명령

IPMItool	IPMIutil	설명
(해당 없음)	`-V 4`	IPMI 세션의 관리자 권한을 활성화합니다.
`-I lanplus`	`-J 3`	IPMI 세션의 암호화를 활성화합니다.
`-H`	`-N`	원격 어플라이언스의 IP 주소를 나타냅니다.
`-U`	`-U`	권한이 있는 LOM 계정의 사용자 이름을 나타냅니다.
`sol activate`	`sol -a`	SOL 세션을 시작합니다.
`sol deactivate`	`sol -d`	SOL 세션을 종료합니다.
`chassis power cycle`	`power -c`	어플라이언스를 다시 시작합니다(70xx 제품군 디바이스에서는 유효하지 않음).
`chassis power on`	`power -u`	어플라이언스 전원을 켭니다.
`chassis power off`	`power -d`	어플라이언스의 전원을 끕니다(디바이스에서는 유효하지 않음)
`sdr`	`sensor`	팬 속도와 온도 등 어플라이언스 정보를 표시합니다.

예를 들어 어플라이언스 정보 목록을 표시하려면 다음 IPMItool 명령을 사용합니다.

```
ipmitool -I lanplus -H IP_address -U user_name sdr
```

참고 Cisco에서는 IPMItool 버전 1.8.12 이상을 사용할 것을 권장합니다.

IPMIutil 유틸리티에서는 동일한 명령이 다음과 같습니다.

```
ipmiutil sensor -V 4 -J 3 -N IP_address -U user_name
```

Lights-Out Management를 사용하려면

액세스: Admin with LOM access

1단계 다음의 명령을 입력합니다.

IPMItool의 경우:

```
ipmitool -I lanplus -H IP_address -U user_name command
```

참고 Cisco에서는 IPMItool 버전 1.8.12 이상을 사용할 것을 권장합니다.

IPMIutil의 경우:

```
ipmiutil -J 3 -H IP_address -U username command
```

여기서 *command*는 Lights-Out Management 명령 표에 있는 명령 중 하나입니다.

표에 나와 있는 해당 작업이 수행됩니다. 비밀번호를 입력하라는 프롬프트가 표시될 수 있습니다.

클라우드 통신 활성화

라이센스: URL 필터링 또는 악성코드

지원되는 Defense Center: DC500을 제외한 모든 방어 센터

FireSIGHT 시스템은 Cisco의 종합 보안 인텔리전스 클라우드에 연결하여 다양한 정보를 가져옵니다.

- 조직에서 FireAMP를 구독하는 경우 엔드포인트 기반 악성코드 이벤트를 수신할 수 있습니다. 37-24페이지의 FireAMP를 위한 클라우드 연결 작업을/를 참조하십시오.
- 액세스 제어 규칙과 관련된 파일 정책을 사용하면 네트워크 트래픽에서 전송된 파일을 관리되는 디바이스로 탐지할 수 있습니다. 방어 센터는 Cisco 클라우드를 사용하여 파일에 악성코드가 있는지 확인합니다. 37-9페이지의 파일 정책 이해 및 생성을/를 참조하십시오.
- URL 필터링을 활성화할 경우, 방어 센터에서는 자주 방문하는 URL에 대한 카테고리 및 평판 데이터를 검색하고, 분류되지 않은 URL에 대한 조회를 수행할 수 있습니다. 그러면 액세스 제어 규칙에 대한 URL 조건을 빠르게 생성할 수 있습니다. 16-10페이지의 평판 기반 URL 차단 수행을/를 참조하십시오.

조직에서 추가 보안을 요구하거나 외부 연결을 제한하려는 경우, 파일 및 악성코드 클라우드 기반 기능에 대해 표준 클라우드 연결 대신 FireAMP Private Cloud를 사용할 수 있습니다. 모든 파일 및 악성코드 클라우드 조회는 물론 FireAMP 엔드포인트의 이벤트 데이터 수집 및 전달도 프라이빗 클라우드를 통해 처리됩니다. 프라이빗 클라우드의 퍼블릭 Cisco 클라우드에 대한 접속은 익명의 프록시 연결을 통해 이루어집니다. 동적 분석 또는 비 FireAMP 클라우드 기능(예: 보안 인텔리전스나 URL 필터링)은 지원되지 않지만, 사용자 관점에서 프라이빗 클라우드는 표준 퍼블릭 클라우드 연결과 거의 동일하게 작동합니다. 프라이빗 클라우드 구성에 대한 자세한 내용은 37-27페이지의 FireAMP Private Cloud 작업을/를 참조하십시오.

다음 옵션을 지정하려면 방어 센터의 로컬 컨피그레이션을 사용하십시오.

Enable URL Filtering

카테고리 및 평판 기반 URL 필터링을 수행하려면 이 옵션을 활성화해야 합니다.

Query Cloud for Unknown URL

모니터링되는 네트워크의 사용자가 로컬 데이터 집합에 없는 URL로 이동하려고 시도하는 경우 시스템이 클라우드에 쿼리하도록 허용합니다.

클라우드에서 어떤 URL의 카테고리나 평판을 알지 못할 경우 또는 방어 센터에서 클라우드에 연결할 수 없을 경우 URL은 카테고리 또는 평판 기반 URL 조건이 있는 액세스 제어 규칙을 매칭하지 **않습니다**. URL에 카테고리 또는 평판을 수동으로 할당할 수 없습니다.

예를 들면 프라이버시의 이유로, 카테고리화되지 않은 URL을 Cisco 클라우드로 카탈로그화하하지 않으려면 이 옵션을 비활성화하십시오.

Enable Automatic Updates

시스템이 클라우드에 연결하여 어플라이언스의 로컬 데이터 집합에서 URL 데이터에 대한 업데이트를 정기적으로 가져오도록 허용합니다. 일반적으로 클라우드에서는 하루에 한 번씩 데이터를 업데이트하지만, 자동 업데이트를 사용하면 방어 센터에서 30분마다 업데이트를 확인하여 항상 최신 정보로 업데이트합니다.

일일 업데이트 양이 적다고 생각될 수도 있으나, 마지막 업데이트 이후 5일 이상 경과하면 새로운 URL 필터링 데이터를 다운로드하는 데 대역폭에 따라 20분 이상이 소요될 수 있습니다. 그런 다음 업데이트 자체를 수행하는 데 30분이 걸릴 수 있습니다.

시스템이 클라우드에 연결할 때 엄격하게 제어하려면 자동 업데이트를 비활성화하고 대신 62-17페이지의 URL 필터링 업데이트 자동화에 설명된 대로 스케줄러를 사용할 수 있습니다.

참고 Cisco에서는 자동 업데이트를 활성화하거나 스케줄러를 사용하여 업데이트를 예약할 것을 권장합니다. 온디맨드 업데이트를 수동으로 수행할 수 있지만, 시스템이 정기적으로 클라우드에 자동 연결하도록 허용하면 최신의 관련 URL 데이터를 얻을 수 있습니다.

Share URI Information of malware events with Cisco

선택적으로, 방어 센터는 네트워크 트래픽에서 탐지된 파일에 대한 정보를 클라우드로 전송할 수 있습니다. 이러한 정보에는 탐지된 파일 및 SHA-256 해시 값과 관련된 URI 정보가 포함됩니다. 공유는 선택 사항이지만, 이러한 정보를 Cisco에 전송하면 추후에 악성코드를 식별하고 추적하는 데 도움이 됩니다.

Use legacy port 32137 for network AMP lookups

이 확인란을 선택하면 시스템에서는 네트워크 클라우드 조회에 포트 443/tcp 대신 포트 32137/tcp(이전의 기본 포트)를 사용할 수 있습니다. 어플라이언스를 FireSIGHT 시스템의 이전 버전에서 업데이트한 경우에는 이 확인란이 기본적으로 선택됩니다.

Licensing

카테고리 및 평판 기반 URL 필터링과 디바이스 기반 악성코드 탐지를 수행하려면 관리되는 디바이스에서 적절한 라이센스를 활성화해야 합니다. 65-1페이지의 FireSIGHT 시스템 라이센싱을/를 참조하십시오.

방어 센터에 URL 필터링 또는 악성코드 라이센스가 없으면 클라우드 연결 옵션을 구성할 수 **없습니다**. 두 라이센스 중 하나만 있는 경우 Cloud Services 로컬 컨피그레이션 페이지에는 소유한 라이센스에 대한 옵션만 표시됩니다. 방어 센터의 라이센스가 만료된 경우 클라우드에 연결할 수 없습니다.

URL 필터링 라이센스를 방어 센터에 추가하면 URL Filtering 컨피그레이션 옵션이 나타나는 것 외에도 **Enable URL Filtering** 및 **Enable Automatic Updates**가 자동으로 활성화됩니다. 필요할 경우 옵션을 수동으로 비활성화할 수 있습니다.

FireAMP 서브스크립션을 사용하여 엔드포인트 기반 악성코드 이벤트를 수신하는 데에는 라이센스가 필요하지 않으며, 허용하거나 차단할 개별 URL 또는 URL 그룹을 지정하는 데에도 라이센스가 필요하지 않습니다. 자세한 내용은 37-2페이지의 악성코드 차단 및 파일 제어 이해 및 16-12페이지의 수동 URL 차단 수행을/를 참조하십시오.

인터넷 액세스 및 고가용성

시스템에서는 80/HTTP 및 443/HTTPS 포트를 사용하여 Cisco 클라우드에 연결하며 프록시 사용도 지원합니다. 64-8페이지의 관리 인터페이스 구성을/를 참조하십시오.

고가용성 구축 시 방어 센터 간에 모든 URL 필터링 컨피그레이션 및 정보가 동기화되지만, 기본 방어 센터에서만 URL 필터링 데이터를 다운로드합니다. 기본 방어 센터가 실패하는 경우 보조 방어 센터가 인터넷에 직접 액세스하도록 해야 하며, 자체 웹 인터페이스를 사용하여 보조 방어 센터를 Active로 승격해야 합니다. 자세한 내용은 4-15페이지의 고가용성 상태 모니터링 및 변경을/를 참조하십시오.

반면, 방어 센터는 파일 정책 및 관련 컨피그레이션을 공유하지만 고가용성 쌍에서는 클라우드 연결과 악성코드 성향을 공유하지 않습니다. 운영 연속성을 보장하고, 탐지된 파일의 악성코드 속성을 두 방어 센터에서 동일하게 유지하려면 기본 및 보조 방어 센터에 클라우드에 대한 액세스 권한이 모두 있어야 합니다.

상태 모니터링

기본 상태 정책에는 방어 센터 클라우드 연결의 상태와 안정성을 추적하는 다음 모듈이 포함되어 있습니다.

- URL Filtering Monitor - 방어 센터가 카테고리 및 평판 업데이트를 관리되는 디바이스로 푸시하지 못하는 경우에도 경고합니다.
- AMP(Advanced Malware Protection)

팁 또 다른 모듈인 FireAMP Status Monitor는 Cisco 클라우드에 대한 방어 센터 연결에서 FireAMP 서브스크립션 소유자를 추적합니다. 상태 모니터링에 대한 자세한 내용은 68-41페이지의 상태 모니터 사용을/를 참조하십시오.

다음 절차는 Cisco 클라우드에서 통신을 활성화하는 방법 및 URL 데이터의 온디맨드 업데이트를 수행하는 방법에 대해 설명합니다. 업데이트가 이미 진행 중인 경우에는 온디맨드 업데이트를 시작할 수 없습니다.

클라우드와의 통신을 활성화하려면

액세스: Admin

1단계 **System > Local > Configuration**을 선택합니다.

Information 페이지가 나타납니다.

2단계 **Cloud Services**를 클릭합니다.

Cloud Services 페이지가 나타납니다. URL 필터링 라이센스가 있으면 페이지에 URL 데이터가 마지막으로 업데이트된 시간이 표시됩니다.

3단계 위에서 설명한 대로 클라우드 연결 옵션을 구성합니다.

Enable URL Filtering을 먼저 선택한 후 **Enable Automatic Updates** 또는 **Query Cloud for Unknown URLs**를 선택해야 합니다.

4단계 **Save**를 클릭합니다.

설정이 저장됩니다. URL 필터링을 활성화한 경우 URL 필터링이 마지막으로 활성화된 이후의 경과 시간에 따라 또는 이것이 URL 필터링을 처음 활성화한 것인지에 따라, 방어 센터는 클라우드에서 URL 필터링 데이터를 수신합니다.

시스템 URL 데이터의 온디맨드 업데이트를 수행하려면

액세스: Admin

1단계 **System > Local > Configuration**을 선택합니다.

Information 페이지가 나타납니다.

2단계 **URL Filtering**을 클릭합니다.

URL Filtering 페이지가 나타납니다.

3단계 **Update Now**를 클릭합니다.

업데이트를 사용할 수 있는 경우 방어 센터는 클라우드에 연결하여 URL 필터링 데이터를 업데이트합니다.

VMware Tools 활성화

라이센스: 모두

지원되는 Defense Center: 가상

VMware Tools는 가상 머신의 성능 향상을 위한 유틸리티 제품군입니다. 이러한 유틸리티를 사용하면 VMware 제품의 편리한 기능을 최대한 활용할 수 있습니다. 모든 가상 어플라이언스에서 다음과 같은 플러그인을 지원합니다.

- guestInfo
- powerOps
- timeSync
- vmbackup

또한 지원되는 모든 ESXi 버전에서 VMWare Tools를 활성화할 수 있습니다. 지원되는 버전 목록은 *FireSIGHT 시스템 Virtual Installation Guide*를 참조하십시오. VMWare Tools의 전체 기능에 대한 자세한 내용은 VMWare 웹사이트(http://www.vmware.com/)를 참조하십시오.

다음 절차에서는 가상 방어 센터에서 웹 인터페이스의 Configuration 메뉴를 사용하여 VMWare Tools를 활성화하는 방법에 대해 설명합니다. 가상 디바이스에는 웹 인터페이스가 없으므로 명령줄 인터페이스를 사용하여 가상 디바이스의 VMWare Tools를 활성화해야 합니다. *FireSIGHT 시스템 Virtual Installation Guide*를 참조하십시오.

가상 방어 센터에서 VMWare Tools를 활성화하려면

액세스: Admin

1단계 **System > Local > Configuration**을 선택합니다.

Information 페이지가 나타납니다.

2단계 **VMWare Tools**를 클릭합니다.

VMWare Tools 페이지가 나타납니다.

3단계 **Enable VMWare Tools**와 **Save**를 차례로 클릭합니다.

변경 내용이 저장되었습니다.

65장

FireSIGHT 시스템 라이센싱

다양한 기능의 라이센스를 취득하여 조직에 최적의 FireSIGHT 시스템 구축을 만들 수 있습니다. 방어 센터를 사용하여 이것 자체와 여기에서 관리하는 라이센스를 관리합니다.

자세한 내용은 다음 링크를 참고하십시오.

라이센싱 이해

라이센스: 모두

다양한 기능의 라이센스를 취득하여 조직에 최적의 FireSIGHT 시스템 구축을 만들 수 있습니다. FireSIGHT 라이센스는 구매한 방어 센터에 포함되어 있으며 호스트, 애플리케이션, 사용자 검색을 수행하는 데 필요합니다.

추가 모델별 라이센스에서는 관리되는 디바이스로 다음을 비롯한 다양한 기능을 수행할 수 있습니다.

- 침입 감지 및 방지
- 보안 인텔리전스 필터링
- 파일 제어 및 AMP
- 애플리케이션, 사용자 및 URL 제어
- 스위칭 및 라우팅
- 디바이스 클러스터링
- NAT(network address translation)
- VPN(가상 사설망) 구축

FireSIGHT 시스템에서 라이센스된 기능에 대한 액세스를 제거할 수 있는 몇 가지 방법이 있습니다. 방어 센터에서 라이센스를 제거하면 관리되는 모든 디바이스에 영향이 미칩니다. 특정 관리되는 디바이스에서 라이센스된 기능을 비활성화할 수도 있습니다. 마지막으로, 일부 라이센스는 만료됩니다. 일부 예외가 있기는 하지만 만료되거나 삭제된 라이센스와 관련된 기능은 사용할 수 없습니다.

자세한 내용은 다음 링크를 참고하십시오.

- 65-2페이지의 라이센스 유형 및 제한 사항
- 65-7페이지의 고가용성 쌍 라이센싱
- 65-7페이지의 스태킹된 디바이스 및 클러스터링된 디바이스 라이센싱
- 65-7페이지의 Series 2 어플라이언스 라이센싱
- 65-8페이지의 FireSIGHT 호스트 및 사용자 라이센스 제한 이해

라이센스 유형 및 제한 사항

라이센스: 모두

이 절에서는 FireSIGHT 시스템 구축에서 사용할 수 있는 라이센스 유형에 대해 설명합니다. 어플라이언스에서 활성화할 수 있는 라이센스는 모델, 버전 및 기타 활성화된 라이센스(관리되는 디바이스에 대한)에 따라 다릅니다.

가상 및 Series 3 디바이스에서 라이센스는 모델에 따라 다릅니다. 라이센스가 디바이스 모델과 정확히 일치하지 않으면 관리되는 디바이스에서 라이센스를 활성화할 수 없습니다. 예를 들어 3D8140 디바이스에서 보호 기능을 활성화하는 데 3D8250 보호 라이센스를 사용할 수 없습니다. 조직과 구축의 규모가 커짐에 따라 추가 관리되는 디바이스에 대한 추가 라이센스를 구매할 수 있습니다.

Series 2 디바이스는 보안 인텔리전스 필터링을 제외한 보호 기능을 자동으로 사용할 수 있습니다. 보호을 Series 2 디바이스에서 명시적으로 활성화할 필요는 없지만, 다른 라이센스를 활성화할 수도 없습니다.

사용자 및 애플리케이션 제어를 수행하기 위해 가상 디바이스 또는 ASA FirePOWER 디바이스에서 제어을 활성화할 수 있지만 이러한 디바이스는 스위칭, 라우팅, 스태킹 또는 클러스터링을 지원하지 않습니다.

다음 표에는 FireSIGHT 시스템 라이센스가 요약되어 있습니다.

표 65-1 FireSIGHT 시스템 라이센스

라이센스	플랫폼	허용되는 기능	필요
FireSIGHT	방어 센터s	검색	없음
보호 (라이센스됨)	Series 3, 가상, X-Series, ASA FirePOWER	침입 감지 및 방지 파일 제어 보안 인텔리전스 필터링	없음
보호(자동)	Series 2	침입 감지 및 방지 파일 제어	없음
제어	가상, ASA FirePOWER	사용자 및 애플리케이션 제어	보호
제어	Series 3	사용자 및 애플리케이션 제어 스위칭 및 라우팅 클러스터링	보호
악성코드	Series 3, 가상, ASA FirePOWER	AMP(네트워크 기반 악성코드 방지 및 차단)	보호

표 65-1 FireSIGHT 시스템 라이센스 (계속)

라이센스	플랫폼	허용되는 기능	필요
URL 필터링	Series 3, 가상, X-Series, ASA FirePOWER	카테고리 및 평판 기반 URL 필터링	보호
VPN	Series 3	가상 사설망 구축	제어

DC500 방어 센터는 URL 필터링 또는 악성코드 라이센스로 제공되는 기능을 지원하지 않습니다.

자세한 내용은 다음 링크를 참고하십시오.

- 65-3페이지의 FireSIGHT
- 65-4페이지의 보호
- 65-4페이지의 제어
- 65-6페이지의 악성코드
- 65-5페이지의 URL 필터링
- 65-6페이지의 VPN

FireSIGHT

라이센스: FireSIGHT

FireSIGHT 라이센스는 구매한 방어 센터에 포함되어 있으며 호스트, 애플리케이션, 사용자 검색을 수행하는 데 사용할 수 있습니다. 시스템에서는 검색 데이터를 통해 네트워크의 완전한 최신 프로필을 생성하고 위협, 엔드포인트, 네트워크 인텔리전스를 사용자 ID 정보와 상호 연결할 수 있습니다. 사용자는 검색 데이터를 통해 트래픽 프로파일링을 수행하고, 네트워크 규정 준수를 평가하고, 상관관계 정책을 구현할 수 있습니다.

FireSIGHT 라이센스는 또한 방어 센터 및 관리되는 디바이스로 모니터링할 수 있는 개별 호스트 및 사용자 수를 결정합니다. 사용자 제한은 다음에 *독립적으로* 적용됩니다.

- FireSIGHT 시스템에서 탐지된 각 사용자에 대한 레코드를 포함하는 Users 데이터베이스
- 액세스 제어 규칙에서 사용자 제어를 수행하기 위해 사용할 수 있는 사용자의 수(*액세스 제어 대상 사용자*라고도 함)

라이센스 제한에 도달한 결과에 대한 자세한 내용은 65-8페이지의 FireSIGHT 호스트 및 사용자 라이센스 제한 이해을/를 참조하십시오.

FireSIGHT 라이센스가 없어도 기본 시스템 컨피그레이션, 모니터링, 네트워크 기반 액세스 제어(영역, 네트워크, VLAN 및 포트 규칙 조건), 연결 로깅 및 보고는 수행할 수 있습니다. FireSIGHT 라이센스 없이도 종합 보안 인텔리전스 클라우드에서 엔드포인트 기반 악성코드 이벤트를 수신할 수 있습니다(그러나 이 경우 조직에 FireAMP 서브스크립션이 필요함).

팁 이 가이드에서 라이센스를 설명할 때에는 방어 센터에 FireSIGHT 라이센스가 있다고 가정합니다. 그러나 방어 센터에서 이전에 버전 4.10.x를 실행 중이었다면 FireSIGHT 라이센스 대신 레거시 RNA 호스트 및 RUA 사용자 라이센스를 사용할 수 있습니다. 자세한 내용은 65-4페이지의 보호을/를 참조하십시오.

보호

라이센스: 보호

지원되는 디바이스: Series 3, 가상, X-Series, ASA FirePOWER

보호 라이센스에서는 침입 탐지 및 방지, 파일 제어, 보안 인텔리전스 필터링을 수행할 수 있습니다.

- *침입 탐지 및 방지* - 네트워크 트래픽에서 침입과 익스플로잇을 분석하고, 선택적으로 위반 패킷을 삭제할 수 있습니다.
- *파일 제어* - 특정 애플리케이션 프로토콜을 통한 특정 유형의 파일 업로드(보내기) 또는 다운로드(받기)를 탐지하고, 선택적으로 이러한 작업을 차단할 수 있습니다. 악성코드 라이센스(65-6페이지의 악성코드 참조)가 있으면 또한 악성코드 성향을 기반으로 그러한 파일 형식의 제한된 집합을 검사 및 차단할 수 있습니다.
- *보안 인텔리전스 필터링* - 액세스 제어 규칙에서 트래픽을 분석하기 전에 특정 IP 주소를 블랙리스트에 추가(트래픽 거부)할 수 있습니다. 동적 피드를 사용하면 최신 인텔리전스를 기반으로 연결을 즉시 블랙리스트에 추가할 수 있습니다. 선택적으로, 보안 인텔리전스 필터링에 "모니터링 전용" 설정을 사용할 수 있습니다.

라이센스 없이 보호 관련 검사를 수행하도록 액세스 제어 정책을 구성할 수 있지만, 먼저 보호 라이센스를 방어 센터에 추가할 때까지는 정책을 적용할 수 없습니다. 그런 다음 정책 대상 디바이스에서 이를 활성화할 수 있습니다.

보호 라이센스를 방어 센터에서 삭제하거나 보호을 관리되는 디바이스에서 비활성화하면 방어 센터는 영향받는 디바이스에서 침입 및 파일 이벤트의 인지를 중지합니다. 그 결과 그러한 이벤트를 트리거 기준으로 사용하는 상관관계 규칙의 실행이 중지됩니다. 또한 방어 센터가 인터넷에서 Cisco 제공 또는 서드파티 보안 인텔리전스 정보를 검색하지 않습니다. 보호을 다시 활성화하기 전에는 기존 정책을 다시 적용할 수 없습니다.

보호 라이센스에는 URL 필터링, 악성코드 및 제어 라이센스가 필요하므로 보호 라이센스를 삭제 또는 비활성화하는 것은 URL 필터링, 악성코드 또는 제어 라이센스를 삭제 또는 비활성화하는 것과 같습니다.

참고 Series 2 디바이스에는 대부분의 보호 기능이 자동으로 포함됩니다. 이러한 디바이스에 대해서는 보호 라이센스를 구매하거나 활성화할 필요가 없습니다. 그러나 Series 2 디바이스는 보안 인텔리전스 필터링을 수행할 수 없습니다.

제어

라이센스: 제어

지원되는 디바이스: Series 3, 가상, ASA FirePOWER

지원되는 Defense Center: 기능에 따라 다름

제어 라이센스가 있으면 사용자 및 애플리케이션 조건을 액세스 제어 규칙에 추가하여 사용자 및 애플리케이션 제어를 구현할 수 있습니다. 또한 Series 3 관리되는 디바이스를 구성하여 스위칭 및 라우팅(DHCP 릴레이 및 NAT 포함)을 수행하고 관리되는 디바이스를 클러스터링할 수 있습니다. 관리되는 디바이스에서 제어을 활성화하려면 보호도 활성화해야 합니다.

참고 가상 디바이스 또는 ASA FirePOWER 디바이스에서 제어 라이센스를 활성화할 수 있지만 이러한 디바이스는 스위칭, 라우팅, 스태킹 또는 클러스터링을 지원하지 **않습니다**.

제어 라이센스 없이도 사용자 및 애플리케이션 조건을 액세스 제어 규칙에 추가할 수 있지만, 먼저 제어 라이센스를 방어 센터에 추가할 때까지는 정책을 적용할 수 없습니다. 그런 다음 정책 대상 디바이스에서 이를 활성화할 수 있습니다.

DC500 방어 센터는 액세스 제어 규칙에서 사용자 조건을 추가하는 기능을 지원하지 않습니다.

제어 라이센스가 없으면 관리되는 디바이스에서 스위치드, 라우티드 또는 하이브리드 인터페이스를 생성할 수 없고, NAT 항목을 생성할 수도 없으며, 가상 라우터에 대해 DHCP 릴레이를 구성할 수도 없습니다. 가상 스위치와 라우터를 생성할 수 있지만 이들을 채우기 위한 스위치드 및 라우티드 인터페이스가 없으면 유용하지 않습니다. 나아가, 제어을 활성화하지 않은 관리되는 디바이스에는 스위칭 또는 라우팅을 포함하는 디바이스 컨피그레이션을 적용할 수 없습니다. 또한 관리되는 디바이스 간에 클러스터링을 설정하려면 제어에 대해 디바이스를 활성화해야 합니다.

제어 라이센스를 방어 센터에서 삭제하거나 개별 디바이스에서 제어을 비활성화하는 경우, 영향받는 디바이스가 스위칭 또는 라우팅의 수행을 중지하지 **않으며** 디바이스 클러스터가 분리되지도 않습니다. 기존 컨피그레이션을 수정 및 삭제할 수는 있지만 영향받는 디바이스에 변경 사항을 적용할 수는 없습니다. 새로운 스위치드, 라우티드 또는 하이브리드 인터페이스를 추가할 수 없으며, 새 NAT 항목을 추가하거나 DHCP 릴레이를 구성하거나 디바이스 클러스터링을 설정할 수도 없습니다. 마지막으로, 사용자 또는 애플리케이션 조건과 함께 규칙이 포함된 경우 기존 액세스 제어 정책을 다시 적용할 수 없습니다.

URL 필터링

라이센스: URL 필터링

지원되는 디바이스: Series 3, 가상, X-Series, ASA FirePOWER

지원되는 Defense Center: DC500을 제외한 모든 방어 센터

URL 필터링을 사용하면 모니터링되는 호스트에서 요청하고 URL에 대한 정보(방어 센터가 Cisco 클라우드에서 얻음)와 상호 연결된 URL을 기준으로 네트워크를 이동할 수 있는 트래픽을 결정하는 액세스 제어 규칙을 작성할 수 있습니다. URL 필터링을 활성화하려면 보호 라이센스도 활성화해야 합니다.

팁 URL 필터링 라이센스 없이도 개별 URL 또는 URL 그룹의 허용 또는 차단을 지정할 수 있습니다. 이를 통해 웹 트래픽을 맞춤형으로 세밀하게 제어할 수 있지만, URL 카테고리 및 평판 데이터를 사용하여 네트워크 트래픽을 필터링할 수는 없습니다.

URL 필터링을 이용하려면 서브스크립션 기반 URL 필터링 라이센스가 필요합니다. URL 필터링 라이센스 없이도 액세스 제어 규칙에 카테고리 및 평판 기반 URL 조건을 추가할 수 있지만 방어 센터에서는 URL 정보를 얻기 위해 클라우드에 연결하지 않습니다. URL 필터링 라이센스를 방어 센터에 추가할 때까지는 액세스 제어 정책을 적용할 수 없습니다. 그런 다음 정책 대상 디바이스에서 이를 활성화할 수 있습니다.

방어 센터에서 라이센스를 삭제하거나 관리되는 디바이스에서 URL 필터링을 비활성화하면 URL 필터링에 액세스하지 못할 수 있습니다. 또한 URL 필터링 라이센스는 만료될 수 있습니다. 라이센스가 만료되거나 라이센스를 삭제 또는 비활성화하면, URL 조건이 포함된 액세스 제어 규칙이 필터링 URL을 즉시 중지하고 방어 센터는 더 이상 클라우드에 연결할 수 없습니다. 카테고리 및 평판 기반 URL 조건과 함께 규칙이 포함된 경우 기존 액세스 제어 정책을 다시 적용할 수 없습니다.

악성코드

라이센스: 악성코드

지원되는 디바이스: Series 3, 가상, ASA FirePOWER

지원되는 Defense Center: DC500을 제외한 모든 방어 센터

악성코드 라이센스가 있으면 AMP를 수행할 수 있습니다. 즉, 관리되는 디바이스를 사용하여, 네트워크를 통해 전송되는 파일에서 악성코드를 탐지하여 차단할 수 있습니다. 관리되는 디바이스에서 악성코드을 활성화하려면 보호도 활성화해야 합니다.

참고 동적 분석을 구성하지 않은 경우에도, 활성화된 악성코드 라이센스가 있는 관리되는 디바이스는 Cisco 클라우드에 대한 연결을 주기적으로 시도합니다. 이것 때문에 디바이스의 Interface Traffic 대시보드 위젯에 전송된 트래픽이 표시되며, 이는 예상되는 동작입니다.

파일 정책의 일부로서 악성코드 탐지를 구성한 다음 하나 이상의 액세스 제어 규칙과 연결합니다. 파일 정책에서는 특정 애플리케이션 프로토콜을 통해 특정 유형의 파일을 업로드 또는 다운로드하는 사용자를 탐지할 수 있습니다. 악성코드 라이센스가 있으면 제한된 파일 형식 집합에서 악성코드를 검사하고, 악성코드 포함 여부를 확인하기 위한 동적 및 Spero 분석을 수행하도록 특정 파일 형식을 다운로드하고 Cisco 클라우드에 제출할 수 있습니다. 또한 악성코드 라이센스를 이용하면 특정 파일을 파일 목록에 추가하고 파일 정책 내에서 파일 목록을 활성화하여, 해당 파일 탐지 시 자동으로 허용 또는 차단할 수 있습니다.

악성코드 라이센스 없이도 악성코드 탐지 파일 정책을 액세스 제어 규칙에 추가할 수 있지만, 액세스 제어 규칙 편집기에서 파일 정책에 경고 아이콘(⚠)이 표시됩니다. 파일 정책 내에서 Malware Cloud Lookup 규칙은 또한 경고 아이콘으로 표시됩니다. 악성코드 탐지 파일 정책이 포함된 액세스 제어 정책을 적용하기 전에 **반드시** 악성코드 라이센스를 추가해야 합니다. 그런 다음 정책 대상 디바이스에서 이를 활성화할 수 있습니다. 나중에 디바이스에서 라이센스를 비활성화하는 경우, 악성코드 탐지를 수행하는 파일 정책이 포함되어 있으면 기존 액세스 제어 정책을 해당 디바이스에 다시 적용할 수 없습니다.

모든 악성코드 라이센스가 삭제되거나 라이센스가 만료되는 경우, 방어 센터는 악성코드 클라우드 조회 수행을 중지하고 Cisco 클라우드에서 전송되는 소급 이벤트 인식도 중지합니다. 악성코드 탐지를 수행하는 파일 정책이 포함된 경우 기존 액세스 제어 정책을 다시 적용할 수 없습니다. 악성코드 라이센스가 만료되거나 삭제된 후 매우 짧은 시간 동안 시스템은 Malware Cloud Lookup 파일 규칙에서 탐지된 파일의 캐시된 성향을 사용할 수 있습니다. 이 시간 창이 만료되면 시스템은 조회를 수행하는 대신 해당 파일에 `Unavailable` 성향을 할당합니다.

시스템이 네트워크 트래픽에서 악성코드를 탐지하도록 하려는 경우에만 악성코드 라이센스가 필요합니다. 악성코드 라이센스가 없으면 방어 센터는 Cisco 클라우드에서 엔드포인트 기반 악성코드 이벤트를 수신할 수 있습니다(조직에 FireAMP 서브스크립션이 있는 경우). 자세한 내용은 37-2페이지의 악성코드 차단 및 파일 제어 이해을/를 참조하십시오.

VPN

라이센스: VPN

지원되는 디바이스: Series 3

VPN을 사용하면 인터넷이나 기타 네트워크 등 공개 소스를 통해 엔드포인트 간 안전한 터널을 설정할 수 있습니다. Cisco 관리되는 디바이스의 가상 라우터 간에 안전한 VPN 터널을 구축하도록 FireSIGHT 시스템을 구성할 수 있습니다. VPN을 활성화하려면 보호 및 제어 라이센스도 활성화해야 합니다.

VPN 라이센스가 없으면 관리되는 디바이스에서 VPN 구축을 구성할 수 없습니다. 구축을 생성할 수 있지만 이들을 채우기 위한, VPN이 활성화된 하나 이상의 라우티드 인터페이스가 없으면 유용하지 않습니다.

VPN 라이센스를 방어 센터에서 삭제하거나 개별 디바이스에서 VPN을 비활성화하는 경우, 영향받는 디바이스가 현재 VPN 구축을 중단하지 **않습니다**. 기존 구축을 수정 및 삭제할 수는 있지만 영향받는 디바이스에 변경 사항을 적용할 수는 없습니다.

고가용성 쌍 라이센싱

라이센스: 모두

지원되는 Defense Center: DC1000, DC1500, DC2000, DC3000, DC3500, DC4000

고가용성 쌍의 방어 센터에서는 라이센스를 공유하지 **않습니다**. 쌍의 각 멤버에 동등한 라이센스를 적용해야 합니다. Cisco는 각 방어 센터의 고유한 라이센스 키를 기반으로 라이센스를 생성하므로 서로 다른 방어 센터에서 동일한 라이센스를 사용할 수 없습니다.

스태킹된 디바이스 및 클러스터링된 디바이스 라이센싱

라이센스: 모두

지원되는 디바이스: 기능에 따라 다름

스태킹 또는 클러스터링을 수행하려면 먼저 개별 디바이스에 해당 라이센스가 있어야 합니다. 디바이스를 스태킹한 후에는 전체 스택에 대해서만 라이센스를 변경할 수 있습니다. 그러나 디바이스 클러스터에서는 활성화된 라이센스를 변경할 수 없습니다.

4-43페이지의 스태킹된 디바이스 관리에 설명된 요건을 충족하는 3D8140, 3D8200 제품군, 3D8300 제품군, 동종 모델의 3D9900 디바이스를 스태킹할 수 있습니다. 4-29페이지의 디바이스 클러스터링에 설명된 요건을 충족하는 동종 Series 3 모델의 두 디바이스를 클러스터링할 수 있습니다.

Series 2 어플라이언스 라이센싱

라이센스: 보호

지원되는 디바이스: Series 2

DC500을 제외하고, Series 2 및 Series 3 방어 센터 라이센싱은 동일합니다. DC500은 URL 필터링 또는 네트워크 기반 악성코드 탐지를 지원하지 않으므로 URL 필터링 또는 악성코드 라이센스를 활용할 수 없습니다.

Series 2 디바이스는 자동으로 이러한 기능을 갖습니다(보호 라이센스로 활성화되는 보안 인텔리전스 제외). Series 2 디바이스에서 보호 라이센스를 비활성화할 수 없으며, 다른 라이센스를 활성화할 수도 없습니다.

자세한 내용은 다음 절을 참조하십시오.

- 65-2페이지의 라이센스 유형 및 제한 사항 - FireSIGHT 시스템 구축에서 사용할 수 있는 라이센스 유형에 대해 설명합니다.
- 1-5페이지의 관리되는 디바이스 모델에서 지원되는 기능 요약 - Series 2 어플라이언스에서 지원되는 기능과 지원되지 않는 기능을 요약하여 제공합니다.

FireSIGHT 호스트 및 사용자 라이센스 제한 이해

라이센스: FireSIGHT

방어 센터의 FireSIGHT 라이센스에 따라, 방어 센터를 사용하여 모니터링할 수 있는 개별 호스트 및 사용자의 수, 관리되는 디바이스, 사용자 제어를 수행하는 데 사용할 수 있는 사용자 수가 결정됩니다. FireSIGHT 호스트 및 사용자 라이센스 한도는 아래 표와 같이 모델별로 다릅니다.

표 65-2 방어 센터 모델별 FireSIGHT 한도

방어 센터 모델	FireSIGHT 호스트 및 사용자 한도
DC500	1000
DC750	2000
DC1000	20,000
DC1500	50,000
DC2000	100,000
DC3000	100,000
DC3500	300,000
DC4000	600,000
가상	50,000

예를 들어 DC500을 사용하면 호스트 1,000개와 사용자 1,000명을 모니터링할 수 있습니다.

방어 센터에서 전에 FireSIGHT 시스템의 버전 4.10.x를 실행했으며 버전 5.x 공장 기본값으로 어플라이언스를 "복원"하는 데 ISO 파일을 사용한 경우, FireSIGHT 라이센스 대신 레거시 RNA Host 및 RUA User 라이센스를 사용할 수 있습니다.

자세한 내용은 다음 절을 참조하십시오.

- 65-8페이지의 FireSIGHT 호스트 제한 이해
- 65-9페이지의 FireSIGHT 사용자 제한 이해
- 65-10페이지의 액세스 제어 대상 사용자 제한 이해
- 65-4페이지의 보호

FireSIGHT 호스트 제한 이해

라이센스: FireSIGHT

방어 센터에 대한 FireSIGHT 라이센스는 방어 센터 및 관리되는 디바이스로 모니터링할 수 있는 개별 호스트의 수, 따라서 네트워크 맵에 저장할 수 있는 호스트의 수를 결정합니다.

시스템은 MAC 전용 호스트를 IP 주소와 MAC 주소 모두로 식별하는 호스트와 별도로 계산합니다. 호스트와 연결된 모든 IP 주소는 하나의 호스트로 계산됩니다.

시스템이 모니터링되는 네트워크의 IP 주소의 호스트와 관련된 활동을 탐지하면(네트워크 검색 정책에 정의된 대로) 해당 호스트는 네트워크 맵에 추가됩니다.

호스트 제한에 도달한 상태에서 시스템이 새 호스트를 탐지하는 경우, 새 호스트가 네트워크 맵에 추가되는지 여부는 네트워크 검색 정책의 **When Host Limit Reached** 설정에 따라 달라집니다. 시스템에서 데이터베이스에 새 호스트 추가를 중지하도록 하거나 가장 오랫동안 비활성 상태를 유지해 온 호스트를 대체하도록 구성할 수 있습니다.

참고 네트워크 맵에 새 호스트를 추가할 수 없더라도 시스템은 여전히 해당 호스트의 네트워크 트래픽에서 액세스 제어를 수행합니다. FireSIGHT 호스트 제한에 도달하더라도 라이센스 제한에 도달한 후 검색된 호스트에서 액세스 제어를 수행할 수는 있지만, 호스트 프로필 데이터를 사용하여 해당 호스트를 보거나 분석을 수행할 수는 없습니다. 예를 들면 규정 준수 화이트리스트를 사용하여 해당 호스트에 대해 네트워크 규정 준수를 모니터링하거나 호스트 프로필 자격에서 해당 호스트를 사용하는 등의 작업을 수행할 수 없습니다.

네트워크 맵에서 호스트, 전체 서브넷 또는 모든 호스트를 수동으로 삭제할 수도 있습니다. 그러나 삭제된 호스트와 관련된 활동이 탐지되면 해당 호스트는 네트워크 맵에 다시 추가된다는 점에 유의하십시오.

시스템이 네트워크 검색 정책에 지정된 마지막 **Host Timeout** 기간에 호스트에서 네트워크 트래픽을 탐지하지 못한 경우 해당 호스트는 네트워크 맵에서 제거됩니다. 기본 설정은 10080분(7일)입니다.

호스트 라이센스 사용을 편리하게 추적할 수 있도록, 구성 가능한 호스트 라이센스 수가 얼마 남아 있지 않으면 FireSIGHT Host License Limit 상태 모듈이 경고를 표시합니다.

FireSIGHT 사용자 제한 이해

라이센스: FireSIGHT

방어 센터의 FireSIGHT 라이센스는 모니터링 가능한 개별 사용자 수를 결정합니다. 시스템이 새 사용자의 활동을 탐지하면 해당 사용자는 Users 데이터베이스에 추가됩니다. 다음과 같은 방법으로 사용자를 탐지할 수 있습니다.

- LDAP, AIM, POP3, IMAP, Oracle, SIP(VoIP), FTP, HTTP, MDNS 및 SMTP 사용자의 로그인을 수동적으로 탐지하는 관리되는 디바이스를 구성하려면 네트워크 검색 정책을 사용할 수 있습니다.
- Active Directory 자격 증명을 기준으로 인증을 탐지하려면 Microsoft Active Directory LDAP 서버에 User Agents를 설치할 수 있습니다.

라이센스 제한에 도달하면 대부분의 경우 시스템은 데이터베이스에 대한 새 사용자 추가를 중지합니다. 새 사용자를 추가하려면 데이터베이스에서 사용자를 수동으로 삭제하거나 모든 사용자를 삭제해야 합니다.

그러나 시스템은 권한 있는 사용자 로그인을 선호합니다. 라이센스 제한에 도달한 상태에서 시스템이 전에 탐지하지 못한 권한 있는 사용자의 로그인을 탐지하면, 오랫동안 비활성 상태를 유지한 권한 없는 사용자를 삭제하고 새로운 사용자를 대신 추가합니다.

팁 관리되는 디바이스를 사용하여 사용자 활동을 탐지하는 경우 프로토콜별로 사용자 로깅을 제한하면, 사용자 이름의 혼란을 최소화하고 FireSIGHT 사용자 라이센스를 유지하는 데 도움이 됩니다. 예를 들어 AIM, POP3 및 IMAP를 통해 검색된 사용자를 모니터링하는 경우 계약직원, 방문자, 기타 손님 등의 네트워크 액세스 때문에 조직과 관련이 없는 사용자가 추가될 수 있습니다. 자세한 내용은 45-30페이지의 사용자 로깅 제한을/를 참조하십시오.

액세스 제어 대상 사용자 제한 이해

라이센스: 제어

지원되는 디바이스: Series 3, 가상, ASA FirePOWER

방어 센터의 FireSIGHT 라이센스는 모니터링 가능한 개별 사용자 수를 결정하는 것은 물론, 사용자 제어를 수행하기 위해 액세스 제어 규칙에서 사용할 수 있는 사용자 수도 결정합니다. 이러한 사용자를 *액세스 제어 대상 사용자*라고 부릅니다.

참고 사용자 제어를 수행하려면 조직에서 **반드시** Microsoft Active Directory를 사용해야 합니다. 시스템은 Active Directory 서버에서 실행 중인 User Agents를 사용하여 액세스 제어 대상 사용자와 IP 주소를 연결하며, 이를 통해 액세스 제어 규칙이 트리거됩니다.

방어 센터와 Active Directory 서버 간 연결(*사용자 인식 객체*라고 함)을 구성하여 액세스 제어 대상 사용자가 속해야 하는 그룹을 지정합니다. 그런 후에는 방어 센터에서 정기적으로 서버를 쿼리하여, 인증 객체에서 지정한 그룹에서 사용자 목록을 검색합니다. 그러면 이러한 사용자를 사용하여 액세스 제어를 수행할 수 있습니다.

인증 객체에서 지정하는 그룹의 총 사용자 수는 **반드시** FireSIGHT 사용자 라이센스 수보다 적어야 합니다. 매개변수가 너무 광범위하면, 방어 센터에서는 최대한 많은 사용자의 정보를 가져오며 검색에 실패한 사용자 수를 작업 대기열에 보고합니다. 성능상의 이유로, Cisco에서는 액세스 제어에 사용할 사용자를 대표하는 그룹만 지정할 것을 권장합니다.

라이센스 보기

라이센스: 모두

방어 센터 및 관리되는 디바이스에 대한 라이센스를 보려면 Licenses 페이지를 사용합니다. 구축에 사용된 각 어플라이언스 유형에 대해 현재 보유 중인 라이센스 수 및 사용 중인 라이센스 수가 페이지에 나열됩니다.

이 페이지에서 사용 중인 FireSIGHT User 라이센스 수는 FireSIGHT 시스템에서 탐지된 사용자 수, 즉 Users 데이터베이스에 있는 사용자 수를 나타냅니다. 액세스 제어를 위해 사용 중인 액세스 제어 대상 사용자 수를 나타내지 않습니다. 자세한 내용은 65-8페이지의 FireSIGHT 호스트 및 사용자 라이센스 제한 이해을/를 참조하십시오.

Licenses 페이지는 또한 각 라이센스에 대한 세부사항을 제공합니다. 각 모델에 대해, 가지고 있는 각 유형의 라이센스 수 및 각 라이센스 모델로 라이센스할 수 있는 관리되는 디바이스의 수가 표시됩니다. 만료되는 라이센스에 대해서는 만료 날짜가 제공됩니다.

Licenses 페이지 외에는 라이센스 및 라이센스 제한을 볼 수 있는 몇 가지 다른 방법이 있습니다.

- Product Licensing 대시보드 위젯은 한눈에 볼 수 있는 라이센스 개요를 제공합니다.
- Device Management 페이지(**Devices > Device Management**)에는 관리되는 페이지 각각에 적용된 라이센스를 나열합니다.
- 두 상태 모듈인 License Monitor 및 FireSIGHT Host License Limit는 상태 정책에서 사용될 때 라이센스 상태를 전달합니다.

라이센스를 보려면

액세스: Admin

1단계 **System > Licenses**를 선택합니다.

Licenses 페이지가 나타납니다.

방어 센터에 라이센스 추가

라이센스: 모두

방어 센터에 라이센스를 추가하기 전에, 라이센스 구매 시 Cisco에서 제공한 활성화 키를 확인하십시오.

FireSIGHT를 제외하고는, 라이센스된 기능을 사용하려면 관리되는 디바이스에서 **반드시** 라이센스를 활성화해야 합니다. 방어 센터에 디바이스를 추가할 때, 또는 디바이스를 추가한 후 디바이스의 일반 속성을 수정하여 라이센스를 활성화할 수 있습니다. Series 2 디바이스에는 보호 기능(보안 인텔리전스 필터링 제외)이 자동으로 포함되므로 이러한 기능을 비활성화하거나 Series 2 디바이스에 다른 라이센스를 적용할 수 없습니다. 65-12페이지의 디바이스의 라이센스된 기능 변경을/를 참조하십시오.

참고 백업이 완료된 후 라이센스를 추가하면, 백업을 복원할 때 라이센스를 제거하거나 덮어쓸 수 없습니다. 복원 시 충돌을 방지하려면 백업을 복원하기 전에 라이센스를 제거하고, 라이센스가 사용된 곳을 적어두고, 백업이 복원된 후 추가하여 다시 구성하십시오. 충돌이 발생하면 고객 지원에 문의하십시오.

라이센스를 추가하려면

액세스: Admin

1단계 **System > Licenses**를 선택합니다.

Licenses 페이지가 나타납니다.

2단계 **Add New License**를 클릭합니다.

Add License 페이지가 나타납니다.

3단계 이메일로 라이센스를 수신하셨습니까?

- 그런 경우 이메일에서 라이센스를 복사하고 **License** 필드에 붙여넣은 후 **Submit License**를 클릭합니다.

  라이센스가 올바른 경우 추가됩니다. 나머지 절차는 건너뜁니다.

- 그렇지 않은 경우 **Get License**를 클릭합니다.

  Licensing Center 웹사이트가 나타납니다. 인터넷에 액세스할 수 없으면 인터넷 액세스가 가능한 컴퓨터로 전환합니다. 페이지 아래쪽의 라이센스 키를 확인하고 https://keyserver.sourcefire.com/으로 이동합니다.

4단계 라이센스를 얻기 위한 화면 지침을 따릅니다(이메일을 통해 전송됨).

팁 Support Site에 로그인한 후 **Licenses** 탭에서 라이센스를 요청할 수도 있습니다.

5단계 이메일에서 라이센스를 복사하고 방어 센터 웹 인터페이스의 **License** 필드에 붙여넣은 후 **Submit License**를 클릭합니다.

라이센스가 유효한 경우 추가됩니다. 65-12페이지의 디바이스의 라이센스된 기능 변경에 설명된 대로 이제 관리되는 디바이스에서 라이센스의 기능을 활성화할 수 있습니다.

라이센스 삭제

라이센스: 모두

어떤 이유로 라이센스를 삭제해야 할 경우 다음 절차를 따릅니다. Cisco에서는 각 방어 센터의 고유한 라이센스 키를 기준으로 라이센스를 생성하므로 한 방어 센터에서 라이센스를 삭제한 다음 다른 방어 센터에서 다시 사용할 수 없습니다.

대부분의 경우 라이센스를 삭제하면 해당 라이센스로 활성화된 기능을 사용하지 못하게 됩니다. 자세한 내용은 65-2페이지의 라이센스 유형 및 제한 사항을/를 참조하십시오.

라이센스를 삭제하는 방법

액세스: Admin

1단계 **System > Licenses**를 선택합니다.

Licenses 페이지가 나타납니다.

2단계 삭제하려는 라이센스 옆에 있는 삭제 아이콘( )을 클릭합니다.

라이센스를 삭제하면 해당 라이센스를 사용하는 모든 디바이스에서 라이센스 기능이 제거됩니다. 예를 들어, 보호 라이센스가 유효하고 관리되는 디바이스 100대에 대해 활성화된 경우 라이센스를 삭제하면 전체 디바이스 100대에서 보호 기능이 제거됩니다.

3단계 라이센스를 삭제할 것임을 확인합니다.

라이센스가 삭제됩니다.

디바이스의 라이센스된 기능 변경

라이센스: 모두

지원되는 디바이스: Series 3, 가상, X-Series, ASA FirePOWER

Series 3 디바이스, 가상 디바이스, Cisco NGIPS for Blue Coat X-Series 또는 ASA FirePOWER 디바이스의 라이센스된 기능을 변경하려면 Device Management 페이지에서 디바이스의 일반 속성을 수정합니다. 몇 가지 예외는 있지만 관리되는 디바이스에서 비활성화한 라이센스와 관련된 기능은 사용할 수 없습니다.

Series 2 디바이스는 보안 인텔리전스 필터링을 제외한 보호 기능을 자동으로 사용할 수 있습니다. 이러한 기능을 비활성화할 수 없으며, Series 2 디바이스에 다른 라이센스를 적용할 수도 없습니다. DC500 방어 센터에서는 악성코드 또는 URL 필터링 라이센스를 사용할 수 없지만 DC500을 사용하면 Series 3 디바이스, 가상 디바이스, Cisco NGIPS for Blue Coat X-Series 또는 ASA FirePOWER 디바이스에서 이러한 기능 및 기타 라이센스된 기능을 활성화하거나 변경할 수 있습니다.

버전, 모델 및 기타 요구 사항을 비롯하여 활성화할 수 있는 라이센스에 대한 자세한 내용은 65-2페이지의 라이센스 유형 및 제한 사항을/를 참조하십시오.

디바이스의 라이센스된 기능을 활성화 또는 비활성화하려면

액세스: Admin/Network Admin

1단계 **Devices > Device Management**를 선택합니다.

Device Management(디바이스 관리) 페이지가 나타납니다.

2단계 라이센스를 활성화 또는 비활성화하려는 디바이스 옆에 있는 수정 아이콘( )을 클릭합니다.

해당 디바이스의 Interfaces 탭이 나타납니다.

3단계 **Device**를 클릭합니다.

Device 탭이 나타납니다.

4단계 License 섹션 옆에 있는 수정 아이콘( )을 클릭합니다.

License 팝업 창이 나타납니다.

5단계 해당 확인란을 선택하여 디바이스의 라이센스된 기능을 활성화 또는 비활성화합니다.

6단계 **Save**를 클릭합니다.

변경 사항이 저장되지만 디바이스 컨피그레이션을 적용해야 변경 사항이 반영됩니다. 4-25페이지의 디바이스에 변경 사항 적용을/를 참조하십시오.

66장 시스템 소프트웨어 업데이트

Cisco는 주 업데이트와 부 업데이트는 물론 규칙 업데이트, GeoDB(지오로케이션 데이터베이스) 업데이트, VDB(취약성 데이터베이스) 업데이트 등 여러 가지 서로 다른 유형의 업데이트를 시스템 소프트웨어 자체에 전자적으로 배포합니다.

주의 이 장에는 FireSIGHT 시스템 업데이트에 대한 일반 정보가 포함되어 있습니다. VDB, GeoDB, 침입 규칙을 비롯한 FireSIGHT 시스템의 일부를 업데이트하기 전에 업데이트와 함께 제공되는 릴리스 정보 또는 자문 텍스트를 **반드시** 읽어야 합니다. 릴리스 노트는 지원되는 플랫폼, 호환성, 전제 조건, 경고, 특정 설치 및 제거 지침과 같은 중요 정보를 제공합니다.

릴리스 정보 또는 자문 텍스트에 달리 설명되어 있지 않으면, 어플라이언스를 업데이트해도 컨피그레이션이 수정되지 않습니다. 어플라이언스의 설정이 영향을 받지 않는 것입니다.

자세한 내용은 다음 절을 참조하십시오.

업데이트 유형 이해

라이센스: 모두

Cisco는 주 업데이트와 부 업데이트는 물론 침입 규칙 업데이트와 VDB 업데이트 등 여러 가지 서로 다른 유형의 업데이트를 시스템 소프트웨어 자체에 전자적으로 배포합니다.

다음 표에서는 Cisco에서 제공하는 두 가지 업데이트 유형에 대해 설명합니다. 대부분의 업데이트 유형에 대해 다운로드 및 설치를 예약할 수 있습니다. 62-1페이지의 작업 예약 및 66-18페이지의 반복 규칙 업데이트 사용을/를 참조하십시오.

표 66-1 FireSIGHT 시스템 업데이트 유형

업데이트 유형	설명	예약 여부	제거 여부
FireSIGHT 시스템에 대한 패치	패치에는 제한된 범위의 픽스가 포함됩니다(또한 일반적으로 5.4.0.1과 같이 버전 번호의 네 번째 자릿수를 변경함).	예	예
FireSIGHT 시스템에 대한 기능 업데이트	기능 업데이트는 패치보다 좀 더 포괄적이며 일반적으로 새 기능을 포함합니다(또한 일반적으로 5.4.1과 같이 버전 번호의 세 번째 자릿수를 변경함).	예	예
FireSIGHT 시스템에 대한 주 업데이트(주 및 부 버전 릴리스)	업그레이드라고도 하는 주 업데이트에는 새로운 기능이 포함되며 제품에 대한 대규모 변경이 수반될 수 있습니다(또한 일반적으로 5.3 또는 5.4와 같이 버전 번호의 두 번째 자릿수를 변경함).	아니요	아니요
VDB	VDB 업데이트는 FireSIGHT 시스템에 의해 보고된 취약성은 물론 운영 체제, 애플리케이션 및 클라이언트에도 영향을 미칩니다.	예	아니요
침입 규칙	침입 규칙 업데이트에서는 새로운 침입 규칙과 프리프로세서 규칙 및 업데이트된 침입 규칙과 프리프로세서 규칙, 기존 규칙의 수정된 상태, 수정된 기본 침입 정책 설정을 제공합니다. 규칙 업데이트는 규칙을 삭제하고, 새 규칙 카테고리와 기본 변수를 제공하고, 기본 변수 값을 수정할 수 있습니다.	예	아니요
GeoDB(지오로케이션 데이터베이스)	GeoDB 업데이트는 시스템이 라우팅 가능한 탐지된 IP 주소와 연결할 수 있는 물리적 위치, 연결 유형 등에 대한 업데이트된 정보를 제공합니다. 지오로케이션 데이터를 액세스 제어 규칙의 조건으로 사용할 수 있습니다. 지오로케이션 세부사항을 보려면 GeoDB를 설치해야 합니다. DC500 방어 센터에서는 이 기능을 지원하지 않습니다.	예	아니요

FireSIGHT 시스템에 대한 패치 및 기타 부 업데이트를 제거할 수는 있지만, 주 업데이트를 제거하고 VDB, GeoDB 또는 침입 규칙의 이전 버전으로 돌아갈 수는 없습니다. 어플라이언스를 FireSIGHT 시스템의 새로운 주 버전으로 업데이트했는데 이전 버전으로 돌아가야 하는 경우 고객 지원에 문의하십시오.

소프트웨어 업데이트 수행

라이센스: 모두

FireSIGHT 시스템 구축을 업데이트하기 위한 몇 가지 기본 단계가 있습니다. 먼저, 릴리스 정보를 읽고 필수 사전 업데이트 작업을 완료하여 업데이트를 **준비해야** 합니다. 그런 다음 업데이트를 시작할 수 있습니다. 먼저 방어 센터를 업데이트하고 여기에서 관리하는 디바이스를 업데이트합니다. 완료될 때까지 업데이트 진행 상황을 모니터링해야 하며, 그런 다음 업데이트 성공을 확인해야 합니다. 마지막으로, 필수 사후 업데이트 단계를 완료합니다.

자세한 내용은 다음 절을 참조하십시오.

- 66-3페이지의 업데이트 계획
- 66-4페이지의 업데이트 프로세스 이해
- 66-6페이지의 방어 센터 업데이트
- 66-8페이지의 관리되는 디바이스 업데이트
- 66-10페이지의 주 업데이트 상태 모니터링

업데이트 계획

라이센스: 모두

업데이트를 시작하기 전에 릴리스 정보를 완전히 읽고 이해해야 합니다. 릴리스 정보는 지원 사이트에서 다운로드할 수 있습니다. 릴리스 정보에서는 지원되는 플랫폼, 새 기능, 알려진 문제와 해결된 문제, 제품 호환성 등에 대해 설명합니다. 릴리스 정보에는 또한 전제 조건, 경고, 특정 설치 및 제거 지침에 대한 중요한 정보가 포함되어 있습니다.

다음 절에서는 업데이트 계획 시 고려해야 할 몇 가지 요소의 개요를 제공합니다.

FireSIGHT 시스템 버전 요구 사항

어플라이언스(소프트웨어 기반 디바이스 포함)가 FireSIGHT 시스템의 올바른 버전을 실행 중인지 확인해야 합니다. 릴리스 정보에는 필수 버전이 나와 있습니다. 이전 버전을 실행 중인 경우 지원 사이트에서 업데이트를 다운로드할 수 있습니다.

운영 체제 요구 사항

소프트웨어 기반 디바이스를 설치한 컴퓨터가 올바른 운영 체제 버전을 실행 중인지 확인합니다. 릴리스 정보에는 필수 버전이 나와 있습니다. 가상 디바이스의 지원되는 운영 체제에 대한 자세한 내용은 *FireSIGHT 시스템 Virtual Installation Guide*를 참조하십시오. Cisco NGIPS for Blue Coat X-Series의 지원되는 운영 체제에 대한 자세한 내용은 *Cisco NGIPS for Blue Coat X-Series Installation Guide*를 참조하십시오.

시간 및 디스크 공간 요구 사항

업데이트를 위한 빈 디스크 공간 및 시간이 충분한지 확인합니다. 관리되는 디바이스를 업데이트할 때에는 방어 센터에 추가 디스크 공간이 필요합니다. 릴리스 정보에 공간 및 시간 요구 사항이 나와 있습니다.

컨피그레이션 및 이벤트 백업 지침

주 업데이트를 시작하기 전에 Cisco에서는 백업을 외부로 복사한 후 어플라이언스에 상주하는 백업을 삭제할 것을 권장합니다. 업데이트 유형과 상관없이 현재 이벤트 데이터 및 컨피그레이션 데이터를 외부로 백업해야 합니다. 이벤트 데이터는 업데이트 프로세스의 일부로서 백업되지 **않습니다**.

방어 센터를 사용하면 자체 및 여기에서 관리하는 디바이스의 이벤트와 컨피그레이션 데이터를 백업할 수 있습니다. 70-1페이지의 백업 및 복원 사용을/를 참조하십시오.

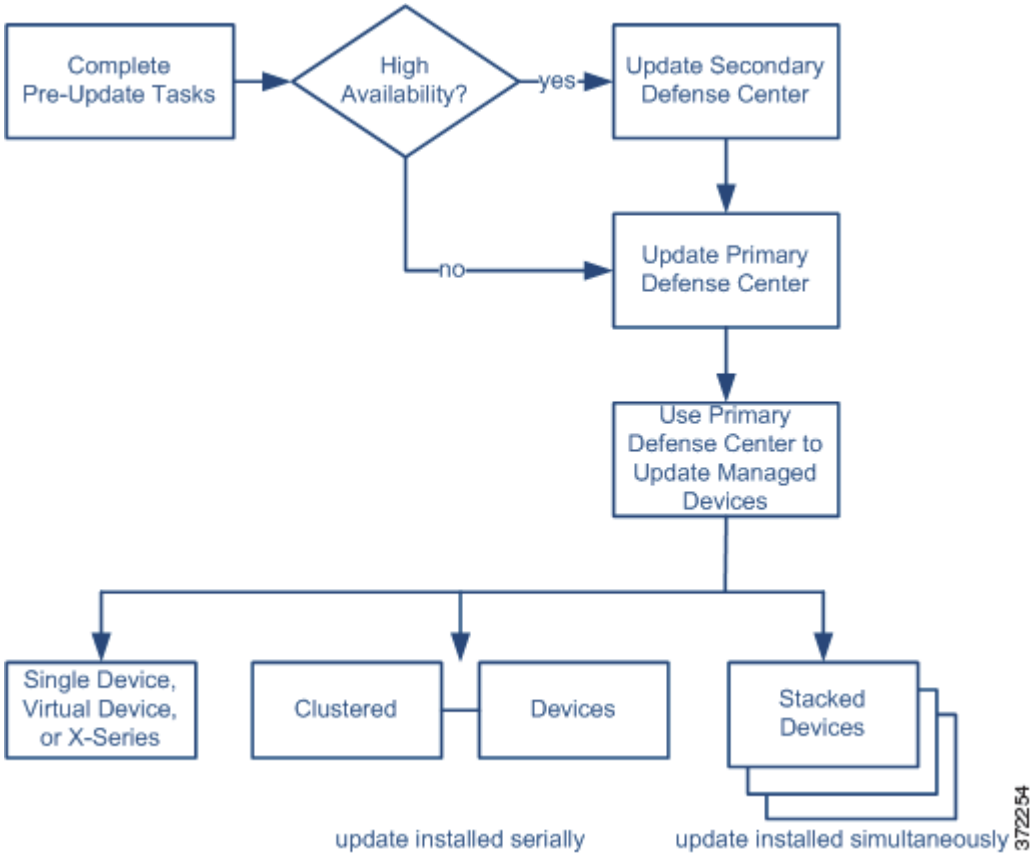
업데이트 수행 시기

업데이트 프로세스는 트래픽 검사, 트래픽 플로우 및 링크 상태에 영향을 미칠 수 있으며 업데이트가 진행 중인 동안에는 Data Correlator가 비활성화되므로 Cisco에서는 유지 관리 기간에 또는 중단이 구축에 미치는 영향이 가장 적을 때 업데이트를 수행할 것을 권장합니다.

업데이트 프로세스 이해

라이센스: 모두

다음 다이어그램에는 업데이트 프로세스가 요약되어 있습니다.



업데이트 순서

방어 센터를 **먼저** 업데이트한 후 여기에서 관리하는 디바이스를 업데이트할 수 있습니다.

방어 센터를 사용하여 업데이트 수행

Cisco에서는 방어 센터 자체는 물론 여기에서 관리하는 디바이스도 해당 웹 인터페이스를 사용하여 업데이트할 것을 권장합니다. 웹 인터페이스가 없는 관리되는 디바이스(예: 가상 디바이스 및 Cisco NGIPS for Blue Coat X-Series)를 업데이트하려면 **반드시** 방어 센터를 사용해야 합니다. Cisco NGIPS for Blue Coat X-Series에 대한 주 업데이트의 경우 이전 버전을 제거하고 새 버전을 설치해야 할 수도 있습니다. 자세한 내용은 *Cisco NGIPS for Blue Coat X-Series Installation Guide*를 참조하십시오.

Product Updates 페이지(**System > Updates**)에는 각 업데이트의 버전은 물론 생성 날짜와 시간도 표시됩니다. 업데이트 과정 중에 재부팅이 필요한지 여부도 페이지에 표시됩니다.

지원 사이트에서 가져온 업데이트를 어플라이언스에 업로드할 경우 해당 업데이트가 페이지에 나타납니다. 패치 및 기능 업데이트에 대한 설치 제거 관리자도 나타납니다. 66-11페이지의 소프트웨어 업데이트 제거을/를 참조하십시오. 방어 센터에서는 페이지에 VDB 업데이트가 나열될 수 있습니다.

팁 패치 및 기능 업데이트의 경우 자동 업데이트 기능을 활용할 수 있습니다. 62-11페이지의 소프트웨어 업데이트 자동화을/를 참조하십시오.

페어링된 방어 센터 업데이트

고가용성 쌍에서 한 방어 센터를 업데이트하기 시작하면 쌍의 다른 방어 센터가 기본 디바이스가 됩니다(아직 아닌 경우). 또한 페어링된 방어 센터는 컨피그레이션 공유를 중지합니다. 페어링된 방어 센터는 일상적인 동기화 프로세스의 일부로서 소프트웨어 업데이트를 수신하지 않습니다.

운영 연속성을 보장하려면 페어링된 방어 센터를 동시에 업데이트하지 **마십시오**. 먼저 보조 방어 센터에 대한 업데이트 절차를 완료하고 기본을 업데이트하십시오.

클러스터링된 디바이스 업데이트

클러스터링된 디바이스 또는 클러스터링된 스택에 업데이트를 설치하면 시스템에서는 한 번에 하나씩 업데이트를 수행합니다. 업데이트가 시작되면 시스템은 먼저 백업 디바이스 또는 스택에 업데이트를 적용합니다. 그러면 이러한 디바이스 또는 스택은 필요한 프로세스가 다시 시작되고 디바이스 또는 스택이 다시 트래픽을 처리할 때까지 유지 관리 모드로 전환됩니다. 그런 다음 시스템은 활성 디바이스 또는 스택에 업데이트를 적용하며, 동일한 프로세스가 이어집니다.

클러스터링된 스택에서 디바이스를 업데이트하려면 클러스터의 모든 멤버에 대해 관리하는 방어 센터에서 동시에 업데이트를 수행해야 합니다. 디바이스에서 직접 업그레이드를 수행할 수 없습니다.

스태킹된 디바이스 업데이트

스태킹된 디바이스에 업데이트를 설치하면 시스템은 동시에 업데이트를 수행합니다. 업데이트가 완료되면 각 디바이스에서 정상 운영이 다시 시작됩니다. 다음 사항에 유의하십시오.

- 모든 보조 디바이스보다 *먼저* 기본 디바이스가 업데이트를 완료하는 경우, 모든 디바이스에서 업데이트가 완료될 때까지 스택이 제한된 혼합 버전 상태에서 운영됩니다.
- 모든 보조 디바이스 *이후* 기본 디바이스가 업그레이드를 완료하는 경우, 기본 디바이스에서 업데이트가 완료되면 스택에서 정상 운영이 다시 시작됩니다.

트래픽 플로우 및 검사

관리되는 디바이스에서 업데이트를 설치하거나 제거할 때 다음 기능이 영향을 받을 수 있습니다.

- 애플리케이션과 사용자 인식 및 제어, URL 필터링, 보안 인텔리전스 필터링, 침입 탐지 및 방지, 연결 로깅을 비롯한 트래픽 검사
- 스위칭, 라우팅 및 관련 기능을 비롯한 트래픽 플로우
- 링크 상태

시스템 업데이트 중에는 Data Correlator가 실행되지 않습니다. 업데이트가 완료될 때 다시 시작됩니다.

네트워크 트래픽 중단의 방법과 기간은 업데이트가 영향을 미치는 FireSIGHT 시스템의 구성 요소, 디바이스의 구성 및 구축 방법, 업데이트가 디바이스를 재부팅하는지 여부에 따라 다릅니다. 네트워크 트래픽이 특정 업데이트에 영향을 미치는 방법과 시기에 대한 내용은 릴리스 정보를 참조하십시오.

팁 클러스터링된 디바이스를 업데이트할 때 시스템은 트래픽 중단을 피하기 위해 한 번에 하나씩 업데이트를 수행합니다.

업데이트 중 웹 인터페이스 사용

업데이트 유형과 상관없이, 업데이트를 모니터링하는 것 외의 작업을 수행하는 데 업데이트 중인 어플라이언스의 웹 인터페이스를 사용하지 **마십시오**.

주 업데이트 중에 어플라이언스를 사용하지 않고 주 업데이트의 진행 상황을 손쉽게 모니터링할 수 있도록 하기 위해 시스템은 어플라이언스의 웹 인터페이스를 간소화합니다. 작업 대기열에서 부 업데이트의 진행 상황을 모니터링할 수 있습니다(**System > Monitoring > Task Status**). 부 업데이트 중에는 웹 인터페이스를 사용하지 못하는 것은 아니지만 Cisco에서는 웹 인터페이스를 사용하지 않을 것을 권장합니다.

팁 관리되는 디바이스에서 업데이트를 모니터링하려면 방어 센터의 작업 대기열을 사용하십시오.

부 업데이트의 경우에도 업데이트 진행 중에 해당 어플라이언스의 웹 인터페이스를 사용하지 못할 수 있습니다. 또는 어플라이언스에서 로그아웃될 수 있습니다. 이는 정상적인 동작입니다. 이런 경우에는 다시 로그인하여 작업 대기열을 살펴보십시오. 업데이트가 여전히 진행 중이면, 업데이트가 완료될 때까지 웹 인터페이스의 사용을 계속 **자제해야** 합니다. 업데이트 중에는 관리되는 디바이스가 두 번째 재부팅될 수 있습니다. 이것 역시 정상적인 동작입니다.

주의 업데이트에 문제가 발생하면(예: 웹 인터페이스에 업데이트가 실패했다는 내용이 표시되거나, 작업 대기열이나 Update Status 페이지를 수동으로 새로 고쳐도 진행 상황이 표시되지 않음) 업데이트를 다시 시작하지 **마십시오**. 대신, 고객 지원에 문의하십시오.

업데이트 후

구축이 제대로 수행되도록 하려면 릴리스 정보에 나열된 모든 사후 업데이트 작업을 **완료해야** 합니다.

가장 중요한 사후 업데이트 작업은 방어 센터를 업데이트한 후와 관리되는 디바이스를 업데이트한 후 액세스 제어 정책을 다시 적용하는 것입니다. 액세스 제어 정책을 적용하면 트래픽 플로우와 처리가 잠시 중지되고, 소수의 패킷이 검사 없이 통과될 수 있습니다. 12-15페이지의 액세스 제어 정책 적용을/를 참조하십시오.

추가로 다음을 수행해야 합니다.

- 업데이트가 성공했는지 확인
- 구축의 모든 어플라이언스가 성공적으로 통신하는지 확인
- 필요한 경우 침입 규칙, VDB 및 GeoDB 업데이트
- 릴리스 정보의 내용을 기반으로 필수 컨피그레이션 변경 수행
- 릴리스 정보에 나열된 추가 사후 업데이트 작업 수행

방어 센터 업데이트

라이센스: 모두

업데이트 유형 및 방어 센터가 인터넷에 액세스할 수 있는지 여부에 따라 두 가지 방법 중 하나로 방어 센터를 업데이트합니다.

- 방어 센터가 인터넷에 액세스할 수 있는 경우 방어 센터를 사용하여 지원 사이트에서 직접 업데이트를 다운로드할 수 있습니다. 주 업데이트에서는 이 옵션이 지원되지 **않습니다**.
- 지원 사이트에서 수동으로 업데이트를 다운로드한 다음 방어 센터에 업로드할 수 있습니다. 방어 센터가 인터넷에 액세스할 수 없거나 주 업데이트를 수행하는 경우 이 옵션을 선택합니다.

주의 운영 연속성을 보장하려면 페어링된 방어 센터를 동시에 업데이트하지 **마십시오**. 66-5페이지의 페어링된 방어 센터 업데이트을/를 참조하십시오.

주 업데이트의 경우 방어 센터를 업데이트하면 이전 업데이트의 설치 제거 관리자가 제거됩니다.

방어 센터를 업데이트하려면

액세스: Admin

1단계 릴리스 정보를 읽고 필수 사전 업데이트 작업을 완료합니다.

사전 업데이트 작업에는 방어 센터가 Cisco 소프트웨어의 올바른 버전을 실행 중인지, 업데이트 수행을 위한 충분한 디스크 공간이 있는지, 업데이트 수행을 위한 적절한 시간을 마련했는지, 이벤트와 컨피그레이션 데이터를 백업했는지 등의 확인 작업이 포함될 수 있습니다.

2단계 업데이트를 방어 센터에 업로드합니다. 업데이트 유형 및 방어 센터가 인터넷에 액세스할 수 있는지 여부에 따라 두 가지 옵션이 있습니다.

- 주 업데이트를 제외하고, 방어 센터가 인터넷에 액세스할 수 있는 경우 **System > Updates**를 선택한 다음 **Download Updates**를 클릭하여 최신 업데이트를 확인합니다. 주 업데이트의 경우 방어 센터가 인터넷에 액세스할 수 없는 경우 먼저 수동으로 업데이트를 다운로드해야 합니다. 다음 지원 사이트 중 하나에서 업데이트를 다운로드하십시오.
  - **모든 Sourcefire 업데이트:** (https://support.sourcefire.com/)
  - **모든 Cisco 업데이트:**

    ```
    Physical Defense Center
    (http://software.cisco.com/download/navigator.html?mdfid=278875421)
    Virtual Defense Center
    (http://software.cisco.com/download/type.html?mdfid=286259687&catid=null)
    ```
- **System > Updates**를 선택한 다음 **Upload Update**를 클릭합니다. 업데이트를 찾은 다음 **Upload**를 클릭합니다.

참고 수동으로 또는 Product Updates 탭에서 **Download Updates**를 클릭하여 지원 사이트에서 직접 업데이트를 다운로드합니다. 업데이트 파일을 이메일로 전송하는 경우 손상될 수 있습니다.

업데이트는 방어 센터에 업로드됩니다.

3단계 구축의 어플라이언스가 성공적으로 통신하는지, 상태 모니터에서 보고하는 문제가 없는지 확인합니다.

4단계 **System > Monitoring > Task Status**를 선택하여 작업 대기열을 보고 진행 중인 작업이 없는지 확인합니다.

업데이트가 시작될 때 실행 중인 작업은 중지되며 다시 시작할 수 없습니다. 업데이트가 완료되면 이러한 작업을 작업 대기열에서 수동으로 삭제해야 합니다. 작업 대기열은 10초마다 자동으로 새로 고쳐집니다. 업데이트를 시작하기 전에 장기 실행 작업이 완료될 때까지 기다려야 합니다.

5단계 **System > Updates**를 선택합니다.

Product Updates 페이지가 나타납니다.

6단계 업로드한 업데이트 옆에 있는 설치 아이콘을 클릭합니다.

Install Update 페이지가 나타납니다.

7단계 방어 센터를 선택하고 **Install**을 클릭합니다. 프롬프트가 표시되면 업데이트 설치를 확인하고 방어 센터를 재부팅합니다.

업데이트 프로세스가 시작됩니다. 업데이트 모니터링 방법은 주 업데이트인지 부 업데이트인지에 따라 다릅니다. 업데이트 유형을 결정하려면 FireSIGHT 시스템 업데이트 유형 표 및 릴리스 정보를 확인하십시오.

- 부 업데이트의 경우 작업 대기열에서 업데이트의 진행 상황을 모니터링할 수 있습니다(**System > Monitoring > Task Status**).
- 주 업데이트의 경우 작업 대기열에서 업데이트의 진행 상황 모니터링을 시작할 수 있습니다. 그러나 방어 센터가 필요한 사전 업데이트 점검을 완료하면 사용자는 로그아웃됩니다. 다시 로그인하면 Upgrade Status 페이지가 나타납니다. 자세한 내용은 66-10페이지의 주 업데이트 상태 모니터링을/를 참조하십시오.

주의 업데이트 유형과 상관없이, 업데이트가 완료되고 필요 시 방어 센터가 재부팅될 때까지는 업데이트 모니터링 외에는 웹 인터페이스를 사용하여 작업을 수행하지 **마십시오**. 자세한 내용은 66-6페이지의 업데이트 중 웹 인터페이스 사용을/를 참조하십시오.

8단계 업데이트가 완료되면 필요 시 방어 센터에 로그인합니다.

주 업데이트 후 로그인한 첫 번째 사용자에게는 EULA(최종 사용자 라이센스 계약)가 나타날 수 있습니다. 계속 진행하려면 EULA를 검토하고 동의해야 합니다.

9단계 브라우저 캐시를 지우고 브라우저를 강제로 다시 로드합니다. 이렇게 하지 않으면 사용자 인터페이스에서 예기치 않은 동작이 발생할 수 있습니다.

10단계 **Help > About**을 선택하고 소프트웨어 버전이 올바르게 나열되는지 확인합니다. 방어 센터에서 규칙 업데이트 및 VDB의 버전도 확인하십시오. 이 정보가 나중에 필요합니다.

11단계 모든 관리되는 디바이스가 방어 센터와 성공적으로 통신하는지 확인합니다.

12단계 지원 사이트에서 사용 가능한 규칙 업데이트가 방어 센터의 규칙보다 새로운 것이면 더 새로운 규칙을 가져옵니다.

자세한 내용은 66-14페이지의 규칙 업데이트 및 로컬 규칙 파일 가져오기을/를 참조하십시오.

13단계 액세스 제어 정책을 다시 적용합니다.

액세스 제어 정책을 적용하면 트래픽 플로우와 처리가 잠시 중지되고, 소수의 패킷이 검사 없이 통과될 수 있습니다. 자세한 내용은 12-15페이지의 액세스 제어 정책 적용을/를 참조하십시오.

14단계 지원 사이트에서 사용 가능한 VDB가 방어 센터의 VDB보다 새로운 것이면 최신 VDB를 설치합니다.

VDB 업데이트를 설치하면 트래픽 플로우와 처리가 잠시 중지되고, 소수의 패킷이 검사 없이 통과될 수 있습니다. 자세한 내용은 66-13페이지의 취약성 데이터베이스 업데이트을/를 참조하십시오.

15단계 방어 센터가 관리하는 디바이스에서 Cisco 소프트웨어를 업데이트하려면 다음 절(관리되는 디바이스 업데이트)을 계속 진행합니다.

관리되는 디바이스 업데이트

라이센스: 모두

Cisco에서는, 방어 센터를 업데이트한 후 이를 사용하여 관리되는 디바이스를 업데이트할 것을 권장합니다. 웹 인터페이스가 없는 관리되는 디바이스(예: 가상 디바이스 및 Cisco NGIPS for Blue Coat X-Series)를 업데이트하려면 **반드시** 방어 센터를 사용해야 합니다. Cisco NGIPS for Blue Coat X-Series에 대한 주 업데이트의 경우 이전 버전을 제거하고 새 버전을 설치해야 할 수도 있습니다.

관리되는 디바이스의 업데이트는 2단계 프로세스입니다. 먼저, 다음 지원 사이트 중 하나에서 업데이트를 다운로드한 후 관리하는 방어 센터에 업로드합니다.

- **Sourcefire:** (https://support.sourcefire.com/)
- **Cisco:** (http://www.cisco.com/cisco/web/support/index.html)

그런 다음 소프트웨어를 설치합니다.

참고 디바이스가 구성되고 구축되는 방법, 업데이트의 영향을 받는 구성 요소, 업데이트가 디바이스를 재부팅하는지 여부 등에 따라 업데이트 중에 트래픽 검사, 트래픽 플로우 및 링크 상태가 영향을 받을 수 있습니다. 네트워크 트래픽이 특정 업데이트에 영향을 미치는 방법과 시기에 대한 내용은 해당 업데이트에 대한 릴리스 정보를 참조하십시오.

관리되는 디바이스를 업데이트하려면

액세스: Admin

1단계 릴리스 정보를 읽고 필수 사전 업데이트 작업을 완료합니다.

사전 업데이트 작업에는 관리하는 방어 센터를 업데이트하고 이벤트 및 컨피그레이션 데이터를 백업하는 것과 디바이스가 올바른 Cisco 소프트웨어 버전을 실행하는지, 소프트웨어 기반 디바이스를 설치한 컴퓨터가 올바른 운영 체제 버전을 실행하는지, 업데이트를 수행할 충분한 디스크 공간이 있는지, 업데이트 수행을 위한 적절한 시간을 배정했는지 등을 확인하는 것이 포함될 수 있습니다.

2단계 디바이스의 관리하는 방어 센터에서 FireSIGHT 시스템 소프트웨어를 업데이트합니다. 66-6페이지의 방어 센터 업데이트을/를 참조하십시오.

3단계 다음 지원 사이트 중 하나에서 업데이트를 다운로드하십시오.

- **모든 Sourcefire 업데이트:** (https://support.sourcefire.com/)
- **모든 Cisco 업데이트:**

물리적 관리되는 디바이스: (http://software.cisco.com/download/navigator.html?mdfid=278875421)
논리적 관리되는 디바이스:
(http://software.cisco.com/download/type.html?mdfid=286259690&flowid=70802)
디바이스 모델마다 각기 다른 업데이트를 사용할 수 있습니다. 다운로드할 수 있는 업데이트에 대한 자세한 내용은 릴리스 정보를 참조하십시오.

참고 지원 사이트에서 업데이트를 직접 다운로드합니다. 업데이트 파일을 이메일로 전송하는 경우 손상될 수 있습니다.

4단계 구축의 어플라이언스가 성공적으로 통신하는지, 상태 모니터에서 보고하는 문제가 없는지 확인합니다.

5단계 관리하는 방어 센터에서 **System > Updates**를 선택합니다.

Product Updates 페이지가 나타납니다.

6단계 **Upload Update**를 클릭하여 다운로드한 업데이트를 찾은 후 **Upload**를 클릭합니다.

업데이트는 방어 센터에 업로드됩니다. Product Updates 탭에는 방금 업로드한 업데이트의 유형, 버전 번호 및 생성된 날짜와 시간이 표시됩니다. 업데이트 과정 중에 재부팅이 필요한지 여부도 페이지에 표시됩니다.

7단계 설치할 업데이트 옆에 있는 설치 아이콘을 클릭합니다.

Install Update 페이지가 나타납니다.

8단계 업데이트를 설치할 디바이스를 선택한 다음 **Install**을 클릭합니다. 동일한 업데이트를 사용하는 경우 여러 디바이스를 업데이트할 수 있습니다. 프롬프트가 표시되면 업데이트 설치를 확인하고 디바이스를 재부팅합니다.

업데이트 프로세스가 시작됩니다. 파일 크기에 따라 모든 디바이스에 업데이트를 설치하는 데 다소 시간이 걸릴 수 있습니다. 방어 센터의 작업 대기열에서 업데이트의 진행 상황을 모니터링할 수 있습니다(**System > Monitoring > Task Status**). 관리되는 디바이스는 업데이트 중 두 번 재부팅될 수 있는데 이는 정상입니다.

주의 업데이트에 문제가 발생하면(예: 웹 인터페이스에 업데이트가 실패했다는 내용이 표시되거나, 작업 대기열을 수동으로 새로 고쳐도 진행 상황이 표시되지 않음) 업데이트를 다시 시작하지 **마십시오**. 대신, 고객 지원에 문의하십시오.

9단계 선택적으로, 주 업데이트 이후 디바이스의 로컬 웹 인터페이스에 로그인합니다.

주 업데이트 후 로그인한 첫 번째 사용자에게는 EULA(최종 사용자 라이센스 계약)가 나타날 수 있습니다. 계속 진행하려면 EULA를 검토하고 동의해야 합니다. 웹 인터페이스가 아니라 명령줄 인터페이스를 통해 처음 로그인한 경우에도 EULA가 나타나며 동의해야 합니다.

10단계 방어 센터에서 **Devices > Device Management**를 선택하고, 업데이트한 디바이스에 올바른 버전이 나열되는지 확인합니다.

11단계 업데이트한 디바이스가 방어 센터와 성공적으로 통신하는지 확인합니다.

12단계 액세스 제어 정책을 다시 적용합니다.

액세스 제어 정책을 적용하면 트래픽 플로우와 처리가 잠시 중지되고, 소수의 패킷이 검사 없이 통과될 수 있습니다. 자세한 내용은 12-15페이지의 액세스 제어 정책 적용을/를 참조하십시오.

주 업데이트 상태 모니터링

라이센스: 모두

주 업데이트의 경우 FireSIGHT 시스템은 업데이트 프로세스를 쉽게 모니터링할 수 있도록 간소화된 웹 인터페이스를 제공합니다. 간소화된 인터페이스를 사용하면 또한 웹 인터페이스를 사용하여 업데이트 모니터링 외의 다른 작업을 수행하는 것을 방지할 수 있습니다.

작업 대기열에서 업데이트 진행 상황의 모니터링을 시작할 수 있습니다(**System > Monitoring > Task Queue**). 그러나 어플라이언스가 필수 사전 업데이트 점검을 완료하면 모든 사용자가 웹 인터페이스에서 로그아웃됩니다. 관리자 또는 유지 관리 사용자가 아니면 업데이트가 완료될 때까지 다시 로그인할 수 없습니다.

관리자의 경우 다시 로그인하면 간소화된 업데이트 페이지가 나타납니다.

방어 센터를 사용하여 관리되는 디바이스를 업데이트하는 경우 Cisco에서는 방어 센터의 작업 대기열에서 업데이트의 진행 상황을 모니터링할 것을 권장합니다. 그러나 어플라이언스가 사전 업데이트 점검을 완료한 후 디바이스의 로컬 웹 인터페이스에 로그인하려고 시도하면, 간소화된 업데이트 페이지가 나타나며 이 페이지를 사용하여 업데이트 진행 상황을 모니터링할 수 있습니다.

이 페이지에는 업데이트하는 FireSIGHT 시스템의 소스 버전, 업데이트하는 대상 버전, 업데이트 시작 후 경과된 시간이 표시됩니다. 또한 진행 표시줄 및 현재 실행 중인 스크립트 세부 사항도 표시됩니다.

팁 업데이트 로그를 보려면 **show log for current script**를 클릭하십시오. 로그를 다시 숨기려면 **hide log for current script**를 클릭하십시오.

어떤 이유로든 업데이트가 실패하면 실패의 시간과 날짜, 업데이트가 실패했을 때 실행 중이던 스크립트, 고객 지원에 문의하는 방법 등이 포함된 오류 메시지가 페이지에 표시됩니다. 업데이트를 다시 시작하지 **마십시오**.

주의 업데이트에서 다른 문제가 발견되면(예: 페이지를 수동으로 새로 고친 후 시간이 지나도 진행 상황이 표시되지 않음) 업데이트를 다시 시작하지 **마십시오**. 대신, 고객 지원에 문의하십시오.

업데이트가 완료되면 어플라이언스가 성공 메시지를 표시한 후 재부팅됩니다. 어플라이언스가 재부팅되면 페이지를 새로 고쳐 로그인하고 필수 사후 업데이트 단계를 완료하십시오.

소프트웨어 업데이트 제거

라이센스: 모두

Cisco 어플라이언스에 패치 또는 기능 업데이트를 적용하면 해당 어플라이언스에서 웹 인터페이스를 사용하여 업데이트를 제거할 수 있는 설치 제거 관리자가 생성됩니다.

업데이트를 제거하면 어플라이언스의 업데이트 경로에 따라 결과 Cisco 소프트웨어 버전이 달라집니다. 예를 들어 버전 5.0에서 버전 5.0.0.2로 직접 어플라이언스를 업데이트하는 시나리오를 가정해보겠습니다. 버전 5.0.0.2 패치를 제거하면, 버전 5.0.0.1 업데이트를 설치한 적이 없더라도 어플라이언스에서 버전 5.0.0.1을 실행하게 될 수 있습니다. 업데이트 제거 시 결과 Cisco 소프트웨어 버전에 대한 자세한 내용은 릴리스 정보를 참조하십시오.

참고 주 업데이트의 경우 웹 인터페이스에서 제거하는 기능이 지원되지 않습니다. 어플라이언스를 FireSIGHT 시스템의 새로운 주 버전으로 업데이트했는데 이전 버전으로 돌아가야 하는 경우 고객 지원에 문의하십시오.

제거 순서

설치한 것과 반대 순서로 업데이트를 제거합니다. 즉, 관리되는 디바이스에스 업데이트를 제거한 다음 방어 센터에서 제거합니다.

로컬 웹 인터페이스를 사용하여 업데이트 제거

업데이트를 제거하려면 로컬 웹 인터페이스를 사용해야 합니다. 관리되는 디바이스에서 업데이트를 제거하는 데에는 방어 센터를 사용할 수 없습니다. 로컬 웹 인터페이스가 없는 디바이스(예: 가상 디바이스 또는 Cisco NGIPS for Blue Coat X-Series)에서 패치를 제거하는 방법에 대한 자세한 내용은 릴리스 정보를 참조하십시오.

Cisco NGIPS for Blue Coat X-Series의 부 업데이트를 제거하는 데에는 이 프로세스를 사용할 수 있지만, X-Series 플랫폼에서 Cisco NGIPS for Blue Coat X-Series 애플리케이션을 제거하는 데에는 이 프로세스를 사용할 수 없습니다. 자세한 내용은 *Cisco NGIPS for Blue Coat X-Series 설치 가이드*을/를 참조하십시오.

클러스터링된 또는 페어링된 어플라이언스에서 업데이트 제거

고가용성 쌍의 클러스터링된 디바이스 및 방어 센터는 FireSIGHT 시스템의 동일한 버전을 실행해야 합니다. 제거 프로세스는 자동 장애 조치를 트리거하지만, 일치하지 않는 쌍 또는 클러스터의 어플라이언스는 컨피그레이션 정보를 공유하지 않으며 동기화의 일부로서 업데이트를 설치 또는 제거하지도 않습니다. 이중 어플라이언스에서 업데이트를 제거해야 하는 경우 바로 이어서 제거를 수행하도록 계획해야 합니다.

업데이트 제거 후 디바이스가 클러스터링된 스태킹이 지원되지 않는 버전으로 돌아가면 클러스터링된 스택의 디바이스에서 업데이트를 제거할 수 없습니다.

운영의 연속성을 보장하려면 클러스터링된 디바이스 및 페어링된 방어 센터에서 한 번에 하나씩 업데이트를 제거하십시오. 먼저 보조 어플라이언스에서 업데이트를 제거합니다. 제거 프로세스가 완료될 때까지 기다린 다음 곧바로 기본 어플라이언스에서 업데이트를 제거합니다.

주의 클러스터링된 디바이스 또는 페어링된 방어 센터에서 제거 프로세스가 실패하는 경우 제거를 다시 시작하거나 피어에서 컨피그레이션을 변경하지 **마십시오**. 대신, 고객 지원에 문의하십시오.

스태킹된 디바이스에서 업데이트 제거

스택의 모든 디바이스는 FireSIGHT 시스템의 동일한 버전을 실행해야 합니다. 스태킹된 디바이스에서 업데이트를 제거하면 해당 스택의 디바이스가 제한된 혼합 버전 상태로 들어갑니다.

구축에 미치는 영향을 최소화하려면 Cisco에서는 스태킹된 디바이스에서 업데이트를 동시에 제거할 것을 권장합니다. 스택의 모든 디바이스에서 업데이트가 완료되면 스택의 정상 운영이 재개됩니다.

업데이트 제거 후 디바이스가 클러스터링된 스태킹이 지원되지 않는 버전으로 돌아가면 클러스터링된 스택의 디바이스에서 업데이트를 제거할 수 없습니다.

트래픽 플로우 및 검사

관리되는 디바이스에서 업데이트를 제거하면 트래픽 검사, 트래픽 플로우 및 링크 상태에 영향을 줄 수 있습니다. 네트워크 트래픽이 특정 업데이트에 영향을 미치는 방법과 시기에 대한 내용은 릴리스 정보를 참조하십시오.

제거 후

업데이트를 제거한 후 구축이 제대로 작동하도록 하려면 수행해야 할 몇 가지 단계가 있습니다. 여기에는 제거가 성공했는지, 구축의 모든 어플라이언스가 성공적으로 통신하는지 확인하는 것이 포함됩니다. 각 업데이트에 해당하는 특정 내용은 릴리스 정보를 확인하십시오.

로컬 웹 인터페이스를 사용하여 패치 또는 기능 업데이트를 제거하려면

액세스: Admin

1단계 **System > Updates**를 선택합니다.

Product Updates 페이지가 나타납니다.

2단계 제거할 업데이트의 설치 제거 관리자 옆에 있는 설치 아이콘을 클릭합니다.

- 방어 센터에서 Install Update 페이지가 나타납니다. 방어 센터를 선택하고 **Install**을 클릭합니다.
- 관리되는 디바이스에는 중간 페이지가 없습니다.

어느 경우든 프롬프트가 표시되면 업데이트를 제거하고 어플라이언스를 재부팅할 것이라고 확인하십시오.

제거 프로세스가 시작됩니다. 작업 대기열에서 진행 상황을 모니터링할 수 있습니다(**System > Monitoring > Task Status**).

주의 제거가 완료되고 필요한 경우 어플라이언스가 재부팅될 때까지는 웹 인터페이스를 사용하여 업데이트 모니터링 이외의 작업을 수행하지 **마십시오**. 자세한 내용은 66-6페이지의 업데이트 중 웹 인터페이스 사용을/를 참조하십시오.

3단계 제거가 완료된 후 필요 시 어플라이언스에 로그인합니다.

4단계 브라우저 캐시를 지우고 브라우저를 강제로 다시 로드합니다. 이렇게 하지 않으면 사용자 인터페이스에서 예기치 않은 동작이 발생할 수 있습니다.

5단계 **Help > About**을 선택하고 소프트웨어 버전이 올바르게 나열되는지 확인합니다.

6단계 패치를 제거한 어플라이언스가 관리되는 디바이스(방어 센터에 대한) 또는 관리하는 방어 센터(관리되는 디바이스에 대한)와 성공적으로 통신하는지 확인합니다.

취약성 데이터베이스 업데이트

라이센스: 모두

Cisco VDB(취약성 데이터베이스)는 호스트가 영향을 받을 수 있는 알려진 취약성과 운영 체제, 클라이언트, 애플리케이션의 핑거프린트로 구성된 데이터베이스입니다. FireSIGHT 시스템은 특정 호스트가 네트워크 손상 위험을 높이는지를 판단하는 데 도움이 되도록 핑거프린트를 취약성과 상호 연결합니다. Cisco VRT(Vulnerability Research Team)는 VDB에 대한 정기적인 업데이트를 제공합니다.

VDB를 업데이트하려면 방어 센터에서 Product Updates 페이지를 사용하십시오. 지원 사이트에서 다운로드한 VDB 업데이트를 어플라이언스에 업로드하면 FireSIGHT 시스템에 대한 업데이트 및 설치 제거 관리자 업데이트와 함께 페이지에 나타납니다.

취약성 매핑 업데이트에 걸리는 시간은 네트워크 맵에 있는 호스트의 수에 따라 달라집니다. 시스템 다운타임의 영향을 최소화하려면 시스템 사용량이 적은 시간에 업데이트를 예약할 수 있습니다. 네트워크에 있는 호스트의 수를 1000으로 나누면 업데이트를 수행하는 데 걸리는 대략적인 시간(분)이 나옵니다.

참고 VDB의 업데이트된 애플리케이션 탐지기 및 운영 체제 핑거프린트를 반영하려면 액세스 제어 정책을 다시 적용해야 합니다. VDB 업데이트를 완료한 후 이전 액세스 제어 정책을 관리되는 디바이스에 다시 적용하십시오. VDB를 설치하거나 액세스 제어 정책을 다시 적용하면 관리되는 디바이스에서 트래픽 플로우와 처리가 잠시 중지되고, 소수의 패킷이 검사 없이 통과될 수 있습니다. 자세한 내용은 12-15페이지의 액세스 제어 정책 적용을/를 참조하십시오.

이 섹션에서는 수동 VDB 업데이트의 계획 및 수행 방법에 대해 설명합니다. 자동 업데이트 기능을 활용하여 VDB 업데이트를 예약할 수 있습니다. 62-15페이지의 취약성 데이터베이스 업데이트 자동화을/를 참조하십시오.

취약성 데이터베이스를 업데이트하려면

액세스: Admin

1단계 업데이트에 대한 VDB Update Advisory Text를 읽습니다.

자문 텍스트에는 업데이트에서 수행된 VDB의 변경 사항에 대한 정보 및 제품 호환성 정보가 포함되어 있습니다.

2단계 **System > Updates**를 선택합니다.

Product Updates 페이지가 나타납니다.

3단계 업데이트를 방어 센터에 업로드합니다.

- 방어 센터가 인터넷에 액세스할 수 있는 경우 **Download Updates**를 클릭하고 다음 지원 사이트 중 하나에서 최신 업데이트를 확인합니다.
  - **Sourcefire:** (https://support.sourcefire.com/)
  - **Cisco:** (http://www.cisco.com/cisco/web/support/index.html)
- 방어 센터가 인터넷에 액세스할 수 없는 경우 다음 지원 사이트 중 하나에서 업데이트를 수동으로 다운로드한 다음 **Upload Update**를 클릭합니다. 업데이트를 찾은 다음 **Upload**를 클릭합니다.
  - **Sourcefire:** (https://support.sourcefire.com/)
  - **Cisco:** (http://www.cisco.com/cisco/web/support/index.html)

참고 수동으로 또는 **Download Updates**를 클릭하여 지원 사이트에서 직접 업데이트를 다운로드합니다. 업데이트 파일을 이메일로 전송하는 경우 손상될 수 있습니다.

업데이트는 방어 센터에 업로드됩니다.

4단계 VDB 업데이트 옆에 있는 설치 아이콘을 클릭합니다.

Install Update 페이지가 나타납니다.

5단계 방어 센터를 선택하고 **Install**을 클릭합니다.

업데이트 프로세스가 시작됩니다. 네트워크 맵의 호스트 수에 따라 업데이트 설치에 시간이 다소 걸릴 수 있습니다. 작업 대기열에서 업데이트의 진행 상황을 모니터링할 수 있습니다(**System > Monitoring > Task Status**).

주의 업데이트가 완료되기 전에는 웹 인터페이스를 사용하여 매핑된 취약성과 관련된 작업을 수행하지 **마십시오**. 업데이트에 문제가 발생하면(예: 웹 인터페이스에 업데이트가 실패했다는 내용이 표시되거나, 작업 대기열을 수동으로 새로 고쳐도 진행 상황이 표시되지 않음) 업데이트를 다시 시작하지 **마십시오**. 대신, 고객 지원에 문의하십시오.

6단계 업데이트가 완료된 후 **Help > About**을 선택하여 VDB 빌드 번호가 설치한 업데이트와 일치하는지 확인합니다.

VDB 업데이트를 반영하려면 이전 액세스 제어 정책을 다시 적용해야 합니다. 12-15페이지의 액세스 제어 정책 적용을/를 참조하십시오.

규칙 업데이트 및 로컬 규칙 파일 가져오기

라이센스: 모두

새 취약성이 알려지면 Cisco VRT(Vulnerability Research Team)은 규칙 업데이트를 제공합니다. 이를 먼저 방어 센터로 가져온 다음 영향받는 액세스 제어, 네트워크 분석 및 침입 정책을 관리되는 디바이스에 적용하여 구현할 수 있습니다.

규칙 업데이트는 누적되므로 Cisco에서는 항상 최신 업데이트를 가져올 것을 권장합니다. 현재 설치된 규칙의 버전과 일치하거나 앞선 규칙 업데이트를 하나만 가져올 수는 없습니다. 구축에 방어 센터의 고가용성 쌍이 포함된 경우 기본 디바이스에서만 업데이트를 가져옵니다. 보조 방어 센터는 일상적인 동기화 프로세스의 일부로서 규칙 업데이트를 수신합니다.

참고 규칙 업데이트에는 새로운 이진 파일이 포함될 수 있으므로, 이를 다운로드하고 설치하는 프로세스가 보안 정책을 준수하도록 해야 합니다. 또한 규칙 업데이트 규모가 클 수 있으므로 네트워크 이용률이 낮은 시간에 규칙을 가져오십시오.

규칙 업데이트는 다음을 제공할 수 있습니다.

- **새로운/수정된 규칙 및 규칙 상태** - 규칙 업데이트는 새로운/수정된 침입 및 프리프로세서 규칙을 제공합니다. 새로운 규칙의 경우 각 시스템 제공 침입 정책에서 규칙 상태가 다를 수 있습니다. 예를 들어 새 규칙이 Security over Connectivity 침입 정책에서는 활성화되고 Connectivity over Security 침입 정책에서는 비활성화될 수 있습니다. 규칙 업데이트는 또한 기존 규칙의 기본 상태를 변경하거나 기존 규칙을 완전히 제거할 수 있습니다.
- **새 규칙 카테고리** - 규칙 업데이트에는 항상 추가되는 새 규칙 카테고리가 포함될 수 있습니다.
- **수정된 프리프로세서 및 고급 설정** - 규칙 업데이트는 시스템 제공 침입 정책에서 고급 설정을 변경하고 시스템 제공 네트워크 분석 정책에서 프리프로세서 설정을 변경할 수 있습니다. 또한 액세스 제어 정책에서 고급 전처리 및 성능 옵션의 기본값을 업데이트할 수도 있습니다.
- **새로운/수정된 변수** - 규칙 업데이트는 기존의 기본 변수에 대한 기본값을 수정할 수 있지만, 변경 사항을 재정의하지는 않습니다. 새 변수가 항상 추가됩니다.

규칙 업데이트가 정책을 수정하는 시기 이해

규칙 업데이트는 액세스 제어 정책은 물론 시스템 제공 및 사용자 지정 네트워크 분석 정책에도 영향을 미칠 수 있습니다.

- **시스템 제공** - 업데이트 후 정책을 다시 적용하면 시스템 제공 네트워크 분석 및 침입 정책에 대한 변경은 물론 고급 액세스 제어 설정에 대한 변경 사항도 자동으로 반영됩니다.
- **사용자 지정** - 모든 사용자 지정 네트워크 분석 및 침입 정책은 시스템 제공 정책을 기반으로 또는 정책 체인의 궁극적 기반으로 사용하므로, 규칙 업데이트는 사용자 지정 네트워크 분석 및 침입 정책에 영향을 미칠 수 있습니다. 그러나 규칙 업데이트에 따라 그러한 변경이 자동으로 수행되지 않도록 설정할 수 있습니다. 그러면 사용자는 규칙 업데이트 가져오기와는 별개의 일정에 따라 수동으로 시스템 제공 기반 정책을 업데이트할 수 있습니다. 무엇을 선택하든(사용자 지정 규칙 기반으로 구현) 시스템 제공 정책에 대한 업데이트로 인해 사용자 지정된 설정이 재정의되지 **않습니다**. 자세한 내용은 24-4페이지의 규칙 업데이트가 시스템 제공 기반 정책을 수정하도록 허용을/를 참조하십시오.

규칙 업데이트를 가져오면 네트워크 분석 및 침입 정책에 대한 모든 캐시된 변경 사항이 취소됩니다. 사용자 편의를 위해 Rule Updates 페이지에 캐시된 변경 사항 및 그러한 변경을 수행한 사용자와 함께 정책이 나열됩니다. 자세한 내용은 23-15페이지의 충돌 해결 및 정책 변경 사항 커밋을/를 참조하십시오.

정책 다시 적용

규칙 업데이트에 따른 변경 사항을 반영하려면 수정된 정책을 다시 적용해야 합니다. 규칙 업데이트를 가져올 때 대상 디바이스에 침입 또는 액세스 제어 정책을 자동으로 다시 적용하도록 시스템을 구성할 수 있습니다. 이는 규칙 업데이트가 시스템 제공 기반 정책을 수정하도록 하려는 경우 특히 유용합니다.

- 액세스 제어 정책을 다시 적용하면 관련 SSL, 네트워크 분석 및 파일 정책도 다시 적용되지만 침입 정책이 다시 적용되지는 **않습니다**. 수정된 고급 설정에 대한 기본값도 업데이트됩니다. 네트워크 분석 정책을 독립적으로 적용할 수 없으므로, 네트워크 분석 정책에서 프리프로세서 설정을 업데이트하려면 액세스 제어 정책을 **반드시** 다시 적용해야 합니다.
- 침입 정책을 다시 적용하면 규칙 및 기타 변경된 침입 정책 설정을 업데이트할 수 있습니다. 침입 정책을 액세스 제어 정책과 함께 다시 적용할 수도 있고, 다른 액세스 제어 컨피그레이션을 업데이트하지 않은 채 침입 규칙을 업데이트하려면 침입 정책만 적용할 수도 있습니다.

규칙 업데이트에 공유 객체 규칙이 포함된 경우 가져온 이후 처음 액세스 제어 또는 침입 정책을 적용하면 트래픽 플로우와 처리가 잠시 중지되고, 소수의 패킷이 검사 없이 통과될 수 있습니다. 요구 사항, 기타 효과 및 권장 사항을 포함하여 액세스 제어 정책 및 침입 정책에 대한 자세한 내용은 12-15페이지의 액세스 제어 정책 적용을/를 참조하십시오.

규칙 업데이트 가져오기에 대한 자세한 내용은 다음을 참조하십시오.

- 66-16페이지의 1회 규칙 업데이트 사용 - 지원 사이트에서 단일 규칙 업데이트를 가져오는 방법에 대해 설명합니다.
- 66-18페이지의 반복 규칙 업데이트 사용 - 지원 사이트에서 규칙 업데이트를 다운로드 및 설치하기 위해 웹 인터페이스에서 자동화 기능을 사용하는 방법에 대해 설명합니다.
- 66-20페이지의 로컬 규칙 파일 가져오기 - 로컬 시스템에서 생성한 표준 텍스트 규칙 파일의 복사본을 가져오는 방법에 대해 설명합니다.
- 66-21페이지의 Rule Update Log 보기 - 규칙 업데이트 로그에 대해 설명합니다.

1회 규칙 업데이트 사용

라이센스: 모두

1회 규칙 업데이트에 대해 사용할 수 있는 두 가지 방법이 있습니다.

- 66-16페이지의 수동 1회 규칙 업데이트 사용 - 지원 사이트에서 로컬 시스템으로 규칙 업데이트를 수동으로 다운로드 및 설치하는 방법에 대해 설명합니다.
- 66-17페이지의 자동 1회 규칙 업데이트 사용 - 지원 사이트에서 새 규칙 업데이트를 검색하고 업로드하기 위해 웹 인터페이스에서 자동화 기능을 사용하는 방법에 대해 설명합니다.

수동 1회 규칙 업데이트 사용

라이센스: 모두

다음 절차는 새 규칙 업데이트를 수동으로 가져오는 방법에 대해 설명합니다. 이 절차는 방어 센터가 인터넷에 액세스할 수 없는 경우 특히 유용합니다.

규칙 업데이트를 수동으로 가져오려면

액세스: Admin

1단계 인터넷에 액세스할 수 있는 컴퓨터에서 다음 사이트 중 하나에 액세스합니다.

- **Sourcefire:** (https://support.sourcefire.com/)
- **Cisco:** (http://www.cisco.com/cisco/web/support/index.html)

2단계 **Download**와 **Rules**를 차례로 클릭합니다.

3단계 최신 규칙 업데이트로 이동합니다.

규칙 업데이트는 누적되므로, 현재 설치된 규칙의 버전과 일치하거나 앞선 규칙 업데이트를 하나만 가져올 수는 없습니다.

4단계 다운로드할 규칙 업데이트 파일을 클릭하고 컴퓨터에 저장합니다.

5단계 어플라이언스의 웹 인터페이스에 로그인합니다.

6단계 **System > Updates**를 선택한 다음 **Rule Updates** 탭을 선택합니다.

Rule Updates 페이지가 나타납니다.

팁 Rule Editor 페이지(**Policies > Intrusion > Rule Editor**)에서 **Import Rules**를 클릭할 수도 있습니다.

7단계 선택적으로, 생성하거나 가져온 모든 사용자 정의 규칙을 삭제 폴더로 이동하려면 **Delete All Local Rules**를 클릭한 다음 **OK**를 클릭합니다. 자세한 내용은 36-106페이지의 사용자 지정 규칙 삭제을/를 참조하십시오.

8단계 규칙 업데이트 파일을 찾아 선택하려면 **Rule Update or text rule file to upload and install**을 선택하고 **Choose File**을 클릭합니다.

9단계 선택적으로, 업데이트가 완료된 후 관리되는 디바이스에 정책을 다시 적용합니다.

- 침입 정책을 자동으로 다시 적용하려면 **Reapply intrusion policies after the rule update import completes**를 선택합니다. 다른 액세스 제어 컨피그레이션을 업데이트하지 않은 채 규칙 및 기타 변경된 침입 정책 설정을 업데이트하려면 이 옵션만 선택합니다. 액세스 제어 정책과 함께 침입 정책을 다시 적용하려면 **반드시** 이 옵션을 선택해야 합니다. 이 경우 액세스 제어 정책을 다시 적용하더라도 완전한 적용이 수행되지는 않습니다.
- 액세스 제어 정책 및 관련 SSL, 네트워크 분석, 파일 정책을 다시 적용하되 침입 정책은 다시 적용하지 않으려면 **Reapply access control policies after the rule update import completes**를 선택합니다. 이 옵션을 선택하면 수정된 액세스 제어 고급 설정에 대한 기본값도 업데이트됩니다. 네트워크 분석 정책을 상위 액세스 제어 정책과 독립적으로 적용할 수 없으므로, 네트워크 분석 정책에서 프리프로세서 설정을 업데이트하려면 액세스 제어 정책을 **반드시** 다시 적용해야 합니다.

10단계 **Import**를 클릭합니다.

시스템이 규칙 업데이트를 설치하고 Rule Update Log 상세 보기를 표시합니다. 66-24페이지의 Rule Update Import Log 상세 보기 이해을/를 참조하십시오. 시스템은 또한 이전 단계에서 지정한 정책을 적용합니다. 12-15페이지의 액세스 제어 정책 적용 및 31-8페이지의 침입 정책 적용을/를 참조하십시오.

참고 규칙 업데이트를 설치하는 동안 오류 메시지가 표시되면 고객 지원에 문의하십시오.

자동 1회 규칙 업데이트 사용

라이센스: 모두

다음 절차는 지원 사이트에 연결하여 새 규칙 업데이트를 자동으로 가져오는 방법에 대해 설명합니다. 어플라이언스가 인터넷에 액세스할 수 있는 경우에만 이 절차를 사용할 수 있습니다.

규칙 업데이트를 자동으로 가져오려면

액세스: Admin

1단계 **System > Updates**를 선택한 다음 **Rule Updates** 탭을 선택합니다.

Rule Updates 페이지가 나타납니다.

팁 Rule Editor 페이지(**Policies > Intrusion > Rule Editor**)에서 **Import Rules**를 클릭할 수도 있습니다.

2단계 선택적으로, 생성하거나 가져온 모든 사용자 정의 규칙을 삭제 폴더로 이동하려면 **Delete All Local Rules**를 클릭한 다음 **OK**를 클릭합니다. 자세한 내용은 36-106페이지의 사용자 지정 규칙 삭제을/를 참조하십시오.

3단계 **Download new Rule Update from the Support Site**를 선택합니다.

4단계 선택적으로, 업데이트가 완료된 후 관리되는 디바이스에 정책을 다시 적용합니다.

- 침입 정책을 자동으로 다시 적용하려면 **Reapply intrusion policies after the rule update import completes**를 선택합니다. 다른 액세스 제어 컨피그레이션을 업데이트하지 않은 채 규칙 및 기타 변경된 침입 정책 설정을 업데이트하려면 이 옵션만 선택합니다. 액세스 제어 정책과 함께 침입 정책을 다시 적용하려면 **반드시** 이 옵션을 선택해야 합니다. 이 경우 액세스 제어 정책을 다시 적용하더라도 완전한 적용이 수행되지는 않습니다.
- 액세스 제어 정책 및 관련 SSL, 네트워크 분석, 파일 정책을 다시 적용하되 침입 정책은 다시 적용하지 않으려면 **Reapply access control policies after the rule update import completes**를 선택합니다. 이 옵션을 선택하면 수정된 액세스 제어 고급 설정에 대한 기본값도 업데이트됩니다. 네트워크 분석 정책을 상위 액세스 제어 정책과 독립적으로 적용할 수 없으므로, 네트워크 분석 정책에서 프리프로세서 설정을 업데이트하려면 액세스 제어 정책을 **반드시** 다시 적용해야 합니다.

5단계 **Import**를 클릭합니다.

시스템이 규칙 업데이트를 설치하고 Rule Update Log 상세 보기를 표시합니다. 66-24페이지의 Rule Update Import Log 상세 보기 이해을/를 참조하십시오. 시스템은 또한 이전 단계에서 지정한 정책을 적용합니다. 12-15페이지의 액세스 제어 정책 적용 및 31-8페이지의 침입 정책 적용을/를 참조하십시오.

참고 규칙 업데이트를 설치하는 동안 오류 메시지가 표시되면 고객 지원에 문의하십시오.

반복 규칙 업데이트 사용

라이센스: 모두

Rule Updates 페이지를 사용하여 매일, 매주 또는 매월 규칙 업데이트를 가져올 수 있습니다. 구축에 방어 센터의 고가용성 쌍이 포함된 경우 기본 디바이스에서만 업데이트를 가져옵니다. 보조 방어 센터는 일상적인 동기화 프로세스의 일부로서 규칙 업데이트를 수신합니다.

규칙 업데이트 가져오기에 해당되는 하위 작업은 다운로드, 설치, 기반 정책 업데이트, 정책 다시 적용의 순서로 발생합니다. 한 하위 작업이 완료되면 다음 하위 작업이 시작됩니다. 반복 가져오기가 구성된 어플라이언스에 의해 전에 적용된 정책만 적용할 수 있습니다.

반복 규칙 업데이트를 예약하려면

액세스: Admin

1단계 **System > Updates**를 선택한 다음 **Rule Updates** 탭을 선택합니다.

Rule Updates 페이지가 나타납니다.

팁 Rule Editor 페이지(**Policies > Intrusion > Rule Editor**)에서 **Import Rules**를 클릭할 수도 있습니다.

2단계 선택적으로, 생성하거나 가져온 모든 사용자 정의 규칙을 삭제 폴더로 이동하려면 **Delete All Local Rules**를 클릭한 다음 **OK**를 클릭합니다. 자세한 내용은 36-106페이지의 사용자 지정 규칙 삭제을/를 참조하십시오.

3단계 **Enable Recurring Rule Update Imports**를 선택합니다.

페이지가 확장되며 반복 가져오기를 구성하기 위한 옵션이 표시됩니다. **Recurring Rule Update Imports** 섹션 제목 아래에 가져오기 상태 메시지가 나타납니다. 설정을 저장하면 반복 가져오기가 활성화됩니다.

팁 반복 가져오기를 비활성화하려면 **Enable Recurring Rule Update Imports** 확인란의 선택을 취소하고 **Save**를 클릭합니다.

4단계 **Import Frequency** 필드의 드롭다운 목록에서 **Daily**, **Weekly** 또는 **Monthly**를 선택합니다.

매주 또는 매월 가져오기 빈도를 선택한 경우 나타나는 드롭다운 목록을 사용하여 규칙 업데이트를 가져올 요일 또는 날짜를 선택합니다. 반복 작업 드롭다운 목록에서 클릭하거나 첫 글자 또는 1회 이상의 선택 횟수를 입력하여 선택한 다음 Enter를 누릅니다.

5단계 반복 규칙 업데이트 가져오기를 시작할 시간을 **Import Frequency** 필드에 지정합니다.

6단계 선택적으로, 업데이트가 완료된 후 관리되는 디바이스에 정책을 다시 적용합니다.

- 침입 정책을 자동으로 다시 적용하려면 **Reapply intrusion policies after the rule update import completes**를 선택합니다. 다른 액세스 제어 컨피그레이션을 업데이트하지 않은 채 규칙 및 기타 변경된 침입 정책 설정을 업데이트하려면 이 옵션만 선택합니다. 액세스 제어 정책과 함께 침입 정책을 다시 적용하려면 **반드시** 이 옵션을 선택해야 합니다. 이 경우 액세스 제어 정책을 다시 적용하더라도 완전한 적용이 수행되지는 않습니다.
- 액세스 제어 정책 및 관련 SSL, 네트워크 분석, 파일 정책을 다시 적용하되 침입 정책은 다시 적용하지 않으려면 **Reapply access control policies after the rule update import completes**를 선택합니다. 이 옵션을 선택하면 수정된 액세스 제어 고급 설정에 대한 기본값도 업데이트됩니다. 네트워크 분석 정책을 상위 액세스 제어 정책과 독립적으로 적용할 수 없으므로, 네트워크 분석 정책에서 프리프로세서 설정을 업데이트하려면 액세스 제어 정책을 **반드시** 다시 적용해야 합니다.

7단계 설정을 사용하여 반복 규칙 업데이트 가져오기를 활성화하려면 **Save**를 클릭합니다.

Recurring Rule Update Imports 섹션 제목 아래의 상태 메시지가 변경되어 규칙 업데이트가 아직 실행되지 않았음을 나타냅니다. 이전 단계에 지정한 대로, 예약된 시간에 시스템이 규칙 업데이트를 설치하고 정책을 적용합니다. 12-15페이지의 액세스 제어 정책 적용 및 31-8페이지의 침입 정책 적용을/를 참조하십시오.

로그오프할 수도 있고 웹 인터페이스를 사용하여 가져오기 전에 또는 가져오는 동안 다른 작업을 수행할 수도 있습니다. 가져오기 중에 액세스하는 경우 Rule Update Log에 빨간색 상태 아이콘( )이 표시되며, Rule Update Log 상세 보기에 나타나는 메시지를 볼 수 있습니다. 규칙 업데이트 크기 및 내용에 따라 상태 메시지가 나타나는 데 몇 분 정도 걸릴 수 있습니다. 자세한 내용은 66-21페이지의 Rule Update Log 보기을/를 참조하십시오.

참고 규칙 업데이트를 설치하는 동안 오류 메시지가 표시되면 고객 지원에 문의하십시오.

로컬 규칙 파일 가져오기

라이센스: 모두

로컬 규칙은 로컬 시스템에서 ASCII 또는 UTF-8 인코딩의 일반 텍스트 파일로서 가져오는 사용자 지정 표준 텍스트 규칙입니다. Snort 사용자 매뉴얼(http://www.snort.org에서 이용 가능)의 지침에 따라 로컬 규칙을 생성할 수 있습니다.

로컬 규칙 가져오기에 대한 다음 내용을/를 참조하십시오.

- 텍스트 파일 이름에는 영숫자 문자와 공백을 사용할 수 있으며 특수 문자 중에는 밑줄(_), 마침표(.), 대시(-)만 사용할 수 있습니다.
- GID(Generator ID)는 지정할 필요가 없습니다. 지정하는 경우 표준 텍스트 규칙에는 GID 1만 지정할 수 있고 민감한 데이터 규칙에는 138만 지정할 수 있습니다.
- 규칙을 처음 가져올 때에는 SID(Snort ID) 또는 개정 번호를 지정하지 **마십시오**. 삭제된 규칙을 포함하여 다른 규칙의 SID와의 충돌을 피하기 위한 것입니다.

  시스템은 다음 사용 가능한 사용자 지정 규칙 SID 1000000 이상과 개정 번호 1을 자동으로 할당합니다.
- 전에 가져온 로컬 규칙의 업데이트된 버전을 가져올 경우 시스템에서 할당한 SID 및 현재 개정 번호보다 큰 개정 번호를 **포함해야** 합니다.

  현재 로컬 규칙의 개정 번호를 보려면 Rule Editor 페이지를 표시하고(**Policies > Intrusion > Rule Editor**), 로컬 규칙 카테고리를 클릭하여 폴더를 확장한 다음, 규칙 옆에 있는 **Edit**를 클릭합니다.
- 시스템이 할당한 SID 및 현재 개정 번호보다 큰 개정 번호를 사용하는 규칙을 가져오면 삭제한 로컬 규칙을 복원할 수 있습니다. 로컬 규칙을 삭제하면 자동으로 개정 번호가 증가합니다. 이 디바이스를 통해 로컬 규칙을 복원할 수 있습니다.

  삭제된 로컬 규칙의 개정 번호를 보려면 Rule Editor 페이지를 표시하고(**Policies > Intrusion > Rule Editor**), 삭제된 규칙 카테고리를 클릭하여 폴더를 확장한 다음, 규칙 옆에 있는 **Edit**를 클릭합니다.
- SID가 2147483647보다 큰 규칙을 포함하는 규칙 파일은 가져올 수 없습니다. 가져오기가 실패합니다.
- 64자보다 긴 소스 또는 목적지 포트의 목록이 포함된 규칙을 가져오는 경우 가져오기가 실패합니다.
- 시스템은 항상 사용자가 가져오는 로컬 규칙을 비활성 규칙 상태로 설정합니다. 침입 정책에서 사용하려면 먼저 수동으로 로컬 규칙의 상태를 설정해야 합니다. 자세한 내용은 32-20페이지의 규칙 상태 설정을/를 참조하십시오.
- 파일의 규칙에 이스케이프 문자가 포함되어 있지 않은지 확인해야 합니다.
- 모든 사용자 지정 규칙은 ASCII 또는 UTF-8 인코딩으로 가져와야 합니다.
- 가져온 모든 로컬 규칙은 자동으로 로컬 규칙 카테고리에 저장됩니다.
- 모든 삭제된 로컬 규칙은 로컬 규칙 카테고리에서 삭제된 규칙 카테고리로 이동합니다.
- 시스템은 단일 파운드 문자(#)로 시작하는 로컬 규칙을 가져옵니다.
- 시스템은 두 개의 파운드 문자(##)로 시작되는 로컬 규칙은 무시하며 가져오지 않습니다.
- Cisco에서는 SID 번호 지정 문제를 피하려면 고가용성 쌍의 기본 방어 센터에서 로컬 규칙을 가져올 것을 적극 권장합니다.
- 사용되지 않는 `threshold` 키워드를 침입 정책에서 침입 이벤트 임계값 지정 기능과 함께 사용하는 가져온 로컬 규칙을 활성화하면 정책 검증이 실패합니다. 자세한 내용은 32-22페이지의 이벤트 임계값 구성을/를 참조하십시오.

로컬 규칙 파일을 가져오려면

액세스: Admin

1단계 **Policies > Intrusion > Rule Editor**를 선택합니다.

Rule Editor 페이지가 나타납니다.

2단계 **Import Rules**를 클릭합니다.

Import Rules 페이지가 나타납니다.

팁 **System > Updates**를 선택한 다음 **Rule Updates** 탭을 선택할 수도 있습니다.

3단계 **Rule Update or text rule file to upload and install**을 선택하고 **Browse**를 클릭하여 규칙 파일을 찾습니다. 이 방식으로 업로드된 모든 규칙은 로컬 규칙 카테고리에 저장됩니다.

팁 ASCII 또는 UTF-8 인코딩의 일반 텍스트 **파일만** 가져올 수 있습니다.

4단계 **Import**를 클릭합니다.

규칙 파일 가져오기가 수행됩니다. 침입 정책에서 적절한 규칙을 활성화해야 합니다. 다음에 영향 받는 정책을 적용할 때까지 규칙이 활성화되지 않습니다.

참고 침입 정책을 적용할 때까지 관리되는 디바이스는 새 규칙 집합을 검사에 사용하지 **않습니다**. 절차는 12-15페이지의 액세스 제어 정책 적용을/를 참조하십시오.

Rule Update Log 보기

라이센스: 모두

방어 센터는 사용자가 가져오는 각 규칙 업데이트 및 로컬 규칙 파일에 대한 레코드를 생성합니다.

각 레코드에는 타임스탬프, 파일을 가져온 사용자의 이름, 가져오기의 성공 여부를 나타내는 상태 아이콘이 포함됩니다. 가져온 모든 규칙 업데이트 및 로컬 규칙 파일의 목록을 유지 관리하고, 목록에서 레코드를 삭제하고, 모든 가져온 규칙 및 규칙 업데이트 구성 요소의 세부 레코드에 액세스할 수 있습니다. 다음 표에서는 Rule Update Log의 필드에 대해 설명합니다.

표 66-2 Rule Update Log 작업

목적	가능한 작업
테이블에서 열의 내용에 대해 자세히 알아보기	66-22페이지의 Rule Update Log 테이블 이해에서 자세히 알아보십시오.

표 66-2 Rule Update Log 작업 (계속)

목적	가능한 작업
가져오기 로그에서 가져오기 파일 레코드 삭제(파일에 포함된 모든 객체에 대한 상세 레코드 포함)	가져오기 파일의 파일 이름 옆에 있는 삭제 아이콘( )을 클릭합니다. **참고** 로그에서 파일을 삭제하면 가져오기 파일에서 가져온 객체는 삭제되지 않고 가져오기 로그 레코드만 삭제됩니다.
규칙 업데이트 또는 로컬 규칙 파일에서 가져온 각 객체의 세부사항 보기	가져오기 파일의 파일 이름 옆에 있는 보기 아이콘( )을 클릭합니다.

자세한 내용은 다음 절을 참조하십시오.

- 66-22페이지의 Rule Update Log 테이블 이해 - 가져온 규칙 업데이트 및 로컬 규칙 파일의 목록에 있는 필드에 대해 설명합니다.
- 66-23페이지의 Rule Update Import Log 세부사항 보기 - 규칙 업데이트 또는 로컬 규칙 파일에서 가져온 각 객체의 자세한 레코드에 대해 설명합니다.
- 66-24페이지의 Rule Update Import Log 상세 보기 이해 - Rule Update Log 상세 보기의 각 필드에 대해 설명합니다.
- 66-25페이지의 Rule Update Import Log 검색 - 검색 기준과 일치하는 모든 레코드 또는 특정 레코드에 대한 가져오기 로그를 검색하는 방법에 대해 설명합니다.

Rule Update Log를 보려면

액세스: Admin

1단계 **System > Updates**를 선택한 다음 **Rule Updates** 탭을 선택합니다.

Rule Updates 페이지가 나타납니다.

팁 **Policies > Intrusion > Rule Editor**를 선택하여 액세스할 수 있는 Rule Editor 페이지에서 **Import Rules**를 클릭할 수도 있습니다.

2단계 **Rule Update Log**를 클릭합니다.

Rule Update Log 페이지가 나타납니다. 이 페이지에는 가져온 각 규칙 업데이트 및 로컬 규칙 파일이 나열됩니다.

Rule Update Log 테이블 이해

라이센스: 모두

다음 표에서는 가져온 규칙 업데이트 및 로컬 규칙 파일의 목록에 있는 필드에 대해 설명합니다.

표 66-3 Rule Update Log 필드

필드	설명
요약	가져오기 파일의 이름. 가져오기가 실패하면 파일 이름 아래에 실패의 원인에 대한 간단한 설명이 표시됩니다.
시간	가져오기가 시작된 시간과 날짜
사용자 ID	가져오기를 트리거한 사용자의 사용자 이름
상태	가져오기의 성공 또는 실패 • 성공( ) • 실패 또는 현재 진행 중( ) 팁 가져오는 동안에는 실패 또는 완료되지 않음을 나타내는 빨간색 상태 아이콘이 Rule Update Log 페이지에 표시되고, 가져오기가 성공적으로 완료된 경우에만 초록색 아이콘으로 교체됩니다.

규칙 업데이트 또는 로컬 규칙 파일에 대한 Rule Update Log 상세 페이지를 보려면 규칙 업데이트 또는 파일 이름 옆에 있는 보기 아이콘( )을 클릭하고, 파일 레코드 및 파일과 함께 가져온 모든 상세 객체 레코드를 삭제하려면 삭제 아이콘( )을 클릭합니다.

팁 규칙 업데이트 가져오기가 진행되는 동안 나타나는 가져오기 세부사항을 볼 수 있습니다.

Rule Update Import Log 세부사항 보기

라이센스: 모두

Rule Update Import Log 세부사항 보기에는 규칙 업데이트 또는 로컬 규칙 파일에서 가져온 각 객체에 대한 상세 레코드가 나열됩니다. 나열되는 레코드에서 특정 요구와 일치하는 정보만 포함하는 사용자 지정 워크플로 또는 보고서를 생성할 수도 있습니다.

다음 표에서는 Rule Update Import Log 상세 보기 워크플로 페이지에서 수행할 수 있는 특정 작업에 대해 설명합니다.

표 66-4 Rule Update Import Log 상세 보기 작업

목적	가능한 작업
테이블에서 열의 내용에 대해 자세히 알아보기	66-24페이지의 Rule Update Import Log 상세 보기 이해에서 자세히 알아보십시오.
현재 워크플로 페이지에서 레코드를 정렬 및 제한	58-34페이지의 드릴다운 워크플로 페이지 정렬에서 자세히 알아보십시오.
일시적으로 다른 워크플로 사용	**(switch workflows)**를 클릭합니다. 워크플로 선택에 대한 자세한 내용은 58-16페이지의 워크플로 선택을/를 참조하십시오. 사용자 지정 워크플로 생성에 대한 자세한 내용은 58-38페이지의 사용자 지정 워크플로 생성을/를 참조하십시오.
신속하게 다시 돌아올 수 있도록 현재 페이지 북마크 지정	**Bookmark This Page**를 클릭합니다. 자세한 내용은 58-36페이지의 북마크 사용을/를 참조하십시오.

표 66-4 Rule Update Import Log 상세 보기 작업 (계속)

목적	가능한 작업
북마크 관리 페이지로 이동	**View Bookmarks**를 클릭합니다. 자세한 내용은 58-36페이지의 북마크 사용을/를 참조하십시오.
현재 보기의 데이터를 기반으로 보고서 생성	**Report Designer**를 클릭합니다. 자세한 내용은 57-9페이지의 이벤트 보기에서 보고서 템플릿 생성을/를 참조하십시오.
전체 Rule Update Import Log 데이터베이스에서 규칙 업데이트 가져오기 레코드 검색	**Search**를 클릭합니다. 자세한 내용은 66-25페이지의 Rule Update Import Log 검색을/를 참조하십시오.
현재 단일 제한 사항으로 채워진 검색 페이지 열기	Search Constraints 옆에 있는 **Edit Search** 또는 **Save Search**를 선택합니다. 자세한 내용은 표 보기 및 드릴다운 페이지 기능 표를 참조하십시오.

Rule Update Import Log 상세 보기를 보려면

액세스: Admin

1단계 **System > Updates**를 선택한 다음 **Rule Updates** 탭을 선택합니다.

Rule Updates 페이지가 나타납니다.

팁 **Policies > Intrusion > Rule Editor**를 선택하여 액세스할 수 있는 Rule Editor 페이지에서 **Import Rules**를 클릭할 수도 있습니다.

2단계 **Rule Update Log**를 클릭합니다.

Rule Update Log 페이지가 나타납니다.

3단계 보려는 상세 레코드의 파일 옆에 있는 보기 아이콘( )을 클릭합니다.

상세 레코드의 테이블 보기가 나타납니다.

Rule Update Import Log 상세 보기 이해

라이센스: 모두

규칙 업데이트 또는 로컬 규칙 파일에서 가져온 각 객체의 자세한 레코드를 볼 수 있습니다. 다음 표에서는 Rule Update Log 상세 보기의 필드에 대해 설명합니다.

표 66-5 Rule Update Import Log 상세 보기 필드

필드	설명
Time	가져오기가 시작된 시간과 날짜.
이름	가져온 객체의 이름. 규칙의 경우 규칙 Message 필드에 해당하는 이름이고, 규칙 업데이트 구성 요소의 경우 구성 요소의 이름입니다.

표 66-5 Rule Update Import Log 상세 보기 필드 (계속)

필드	설명
유형	가져온 객체의 유형. 다음 중 하나일 수 있습니다. • `rule update component`(규칙 팩 또는 정책 팩 등의 가져온 구성 요소) • `rule`(규칙의 경우 새로운 또는 업데이트된 규칙이며, 버전 5.0.1에서는 이 값이 더 이상 사용되지 않는 `update`로 교체됨) • `policy apply`(가져오기에 대해 **Reapply intrusion policies after the Rule Update import completes** 옵션이 활성화됨)
작업	객체 유형에 대해 다음 중 하나가 발생했음을 나타냅니다. • `new`(규칙의 경우, 이 어플라이언스에 규칙이 처음 저장된 것임) • `changed`(규칙 업데이트 구성 요소 또는 규칙의 경우, 규칙 업데이트 구성 요소가 수정되었거나 규칙에 더 높은 개정 번호 및 동일한 GID와 SID가 있음) • `collision`(규칙 업데이트 구성 요소 또는 규칙의 경우, 개정이 어플라이언스에 있는 기존 구성 요소나 규칙과 충돌하므로 가져오기를 건너뛰었음) • `deleted`(규칙의 경우, 규칙 업데이트에서 규칙이 삭제됨) • `enabled`(규칙 업데이트 수정의 경우, 프리프로세서, 규칙 또는 기타 기능이 Cisco에서 제공하는 기본 정책에서 활성화됨) • `disabled`(규칙의 경우, Cisco에서 제공하는 기본 정책에서 규칙이 비활성화됨) • `drop`(규칙의 경우, Cisco에서 제공하는 기본 정책에서 규칙이 Drop and Generate Events로 설정됨) • `error`(규칙 업데이트 또는 로컬 규칙 파일의 경우 가져오기가 실패함) • `apply`(가져오기에 대해 **Reapply intrusion policies after the Rule Update import completes** 옵션이 활성화됨)
기본 작업	규칙 업데이트에 의해 정의된 기본 작업. 가져온 객체 유형이 `rule`이면 기본 작업은 `Pass`, `Alert` 또는 `Drop`입니다. 가져온 다른 모든 규칙 유형의 경우 기본 작업이 없습니다.
GID	규칙의 Generator ID. 예: `1`(표준 텍스트 규칙) 또는 `3`(공유 객체 규칙). 자세한 내용은 41-40 페이지의 표 41-7을/를 참조하십시오.
SID	규칙의 SID.
Rev	규칙의 개정 번호.
정책	가져온 규칙의 경우 이 필드에 `All`이 표시됩니다. 이는 가져온 규칙이 모든 기본 침입 정책에 포함되었음을 나타냅니다. 가져온 객체의 다른 유형에 대해 이 필드는 비어 있습니다.
세부 사항	구성 요소 또는 규칙에 고유한 문자열. 규칙의 경우, `previously (GID:SID:Rev)`로 표시되는 GID, SID, 변경된 규칙의 이전 개정 번호. 변경되지 않은 규칙에 대해서는 이 필드가 비어 있습니다.
개수	각 레코드의 카운트(`1`). Count 필드는 테이블이 제한된 경우 테이블 보기에 나타나며, Rule Update Log 상세 보기는 기본적으로 규칙 업데이트 레코드로 제한됩니다.

Rule Update Import Log 검색

라이센스: 모두

참고 베타 사용자: 이 기능에 대해서는 설명서의 최종 버전에서 자세히 설명합니다.

검색 기준과 일치하는 모든 레코드 또는 특정 레코드에 대한 가져오기 로그를 검색할 수 있습니다. 사용자 지정 검색을 생성하고 나중에 다시 사용할 수 있도록 저장할 수 있습니다.

팁 단일 가져오기 파일에 대한 레코드만 표시된 Rule Update Import Log 상세 보기의 툴바에서 **Search**를 클릭하여 검색을 시작하는 경우에도 전체 Rule Update Import Log 데이터베이스가 검색됩니다. 검색에 포함할 모든 객체를 포함하도록 시간 제약 조건을 설정해야 합니다. 자세한 내용은 60-5페이지의 검색에서 시간 제약 조건 지정을/를 참조하십시오.

사용할 수 있는 검색 기준은 다음 표에 설명되어 있습니다. 레코드 검색은 대/소문자를 구분합니다. 예를 들어 `RULE` 또는 `rule` 검색 모두 동일한 결과를 반환합니다.

표 66-6 Rule Update Import Log 검색 기준

검색 필드	설명	예
Time	레코드가 생성된 날짜와 시간을 지정합니다. 시간 입력을 위한 구문은 60-5페이지의 검색에서 시간 제약 조건 지정을/를 참조하십시오.	`> 2006-01-15 13:30:00`은 2006년 1월 15일 오후 1시 30분 이후 가져온 모든 규칙 레코드를 반환합니다.
이름	규칙 Message 필드의 내용 중 일부 또는 전체를 지정합니다. 이 필드에서는 와일드카드 문자로 별표(*)를 사용할 수 있습니다.	`*dhcp*`는 Message 필드에 DHCP가 있는 모든 규칙 레코드를 반환합니다.
유형	레코드의 유형을 지정합니다. `rule update component`, `rule` 또는 `policy apply`일 수 있습니다. 버전 5.0.1 이전에 가져온 규칙을 검색하려면 `update` 검색 값을 사용할 수 있습니다.	`update`는 규칙 팩 또는 정책 팩과 같은 가져온 규칙 업데이트 구성 요소를 반환합니다. `rule`은 새 규칙을 포함한 규칙 업데이트를 반환합니다. `policy apply`는 업데이트에 이어 침입 정책이 자동으로 다시 적용된 규칙 업데이트에 대한 정보의 테이블 행을 반환합니다.
작업	보려는 규칙에 대한 작업을 지정합니다. 지정할 수 있는 작업의 목록을 보려면 Rule Update Import Log 상세 보기 필드 표를 참조하십시오.	유형이 `rule`이면 `new`는 어플라이언스에서 처음 가져온 모든 규칙을 반환합니다.
GID	규칙의 Generator ID를 지정합니다.	`3`은 모든 공유 객체 규칙을 반환합니다.
SID	규칙의 Signature ID 또는 SID 범위를 지정합니다.	`923`은 SID 923의 규칙에 대한 레코드를 반환합니다.
Rev	규칙의 개정 번호를 지정합니다.	`3`은 개정 번호 3의 규칙을 반환합니다.
정책	규칙을 가져오는 기본 정책을 지정합니다.	`All`은 모든 기본 정책으로 가져오는 규칙을 반환합니다.
Rule Update	Rule Update 파일 이름을 지정합니다.	*`filename`*은 지정된 가져오기 파일의 모든 레코드를 반환합니다.
세부 사항	가져온 객체에 대한 세부사항을 지정합니다.	`previously*`는 변경된 모든 규칙의 레코드를 반환합니다.

저장된 검색을 로드 및 삭제하는 방법을 포함하여 검색에 대한 자세한 내용은 60-1페이지의 이벤트 검색을/를 참조하십시오.

Rule Update Import Log를 검색하려면

액세스: Admin/Intrusion Admin

1단계 **Analysis > Search**를 선택합니다.

Search 페이지가 나타납니다.

2단계 **Table** 드롭다운 목록에서 **Rule Update Import Log**를 선택합니다.

해당 제약 조건으로 페이지가 다시 로드됩니다.

팁 Rule Update Log 상세 보기에서 **Search**를 클릭할 수도 있습니다. 66-23페이지의 Rule Update Import Log 세부사항 보기을/를 참조하십시오.

3단계 선택적으로, 검색을 저장하려면 **Name** 필드에 검색의 이름을 입력합니다.

이름을 입력하지 않으면 저장 시 웹 인터페이스에서 자동으로 이름을 생성합니다.

4단계 Rule Update Import Log 검색 기준 표에 설명된 대로 해당 필드에 검색 기준을 입력합니다. 여러 기준을 입력하면 모든 기준과 일치하는 레코드가 반환됩니다.

5단계 다른 사용자가 액세스할 수 있도록 검색을 저장하려면 **Save As Private** 확인란의 선택을 취소합니다. 검색을 비공개로 저장하려면 확인란을 선택된 상태로 둡니다.

사용자 지정 사용자 역할에 대한 데이터 제한으로서 검색을 사용하려면 **반드시** 비공개 검색으로 저장해야 합니다.

6단계 다음 옵션을 이용할 수 있습니다.

- 검색을 시작하려면 **Search**를 클릭합니다.

  검색 결과가 기본 Rule Update Import Log 상세 보기 워크플로에 나타납니다. 사용자 지정 워크플로를 비롯한 다른 워크플로를 사용하려면 **(switch workflows)**를 클릭합니다. 다른 기본 워크플로 지정에 대한 자세한 내용은 71-3페이지의 이벤트 보기 설정 구성을/를 참조하십시오.
- 기존 검색을 수정하고 변경 사항을 저장하려면 **Save**를 클릭합니다.
- 검색 기준을 저장하려면 **Save as New Search**를 클릭합니다. 나중에 실행할 수 있도록 검색이 저장됩니다(**Save As Private**을 선택한 경우 사용자 계정과 연결됨).

지오로케이션 데이터베이스 업데이트

라이센스: FireSIGHT

지원되는 Defense Center: DC500을 제외한 모든 방어 센터

Cisco GeoDB(지오로케이션 데이터베이스)는 지리적 데이터(예: 국가, 도시, 좌표 등) 및 라우팅 가능한 IP 주소와 연결된 연결 관련 데이터(예: 인터넷 서비스 공급자, 도메인 이름, 연결 유형 등)로 구성된 데이터베이스입니다. 시스템이 탐지된 IP 주소와 일치하는 GeoDB 정보를 탐지하면, 해당 IP 주소와 연결된 지오로케이션 정보를 볼 수 있습니다. 국가 또는 대륙 이외의 지오로케이션 세부사항을 보려면 시스템에 GeoDB를 설치해야 합니다. Cisco에서는 GeoDB의 업데이트를 정기적으로 제공합니다.

GeoDB를 업데이트하려면 방어 센터의 Geolocation Updates 페이지를 사용하십시오(**System > Updates > Geolocation Updates**). 지원 사이트 또는 어플라이언스에서 가져온 GeoDB 업데이트를 업로드할 경우 해당 업데이트가 이 페이지에 나타납니다.

GeoDB 업데이트에 필요한 시간은 어플라이언스에 따라 다릅니다. 설치하는 데 일반적으로 30~40분이 소요됩니다. GeoDB 업데이트는 다른 시스템 기능(지오로케이션 정보의 지속적인 수집 포함)을 중단하지 않지만, 완료되는 동안 시스템 리소스가 소모됩니다. 업데이트를 계획할 때에는 이를 고려하십시오.

이 섹션에서는 수동 GeoDB 업데이트의 계획 및 수행 방법에 대해 설명합니다. 자동 업데이트 기능을 활용하여 GeoDB 업데이트를 예약할 수도 있습니다. 자세한 내용은 62-9페이지의 지오로케이션 데이터베이스 업데이트 자동화을/를 참조하십시오. 지오로케이션에 대한 자세한 내용은 58-20페이지의 지오로케이션 사용을/를 참조하십시오.

지오로케이션 데이터베이스를 업데이트하려면

액세스: Admin

1단계 **System > Updates**를 선택합니다.

Product Updates 페이지가 나타납니다.

2단계 **Geolocation Updates** 탭을 클릭합니다.

Geolocation Updates 페이지가 나타납니다.

3단계 업데이트를 방어 센터에 업로드합니다.

- 방어 센터가 인터넷에 액세스할 수 있는 경우 다음 지원 사이트 중 하나에서 최신 업데이트를 확인하려면 **Download and install geolocation update from the Support Site**를 클릭합니다.
  - **Sourcefire:** (https://support.sourcefire.com/)
  - **Cisco:** (http://www.cisco.com/cisco/web/support/index.html)
- 방어 센터가 인터넷에 액세스할 수 없는 경우 다음 지원 사이트 중 하나에서 업데이트를 수동으로 다운로드한 다음 **Upload and install geolocation update**를 클릭합니다. 업데이트를 찾은 다음 **Import**를 클릭합니다.
  - **Sourcefire:** (https://support.sourcefire.com/)
  - **Cisco:** (http://www.cisco.com/cisco/web/support/index.html)

참고 Geolocation Updates 페이지에서 수동으로 또는 **Download and install geolocation update from the Support Site**를 클릭하여 지원 사이트에서 직접 업데이트를 다운로드하십시오. 업데이트 파일을 이메일로 전송하는 경우 손상될 수 있습니다.

업데이트 프로세스가 시작됩니다. 업데이트 설치의 평균 시간은 30~40분입니다. 이 시간은 어플라이언스 하드웨어에 따라 다를 수 있습니다. 작업 대기열에서 업데이트의 진행 상황을 모니터링할 수 있습니다(**System > Monitoring > Task Status**).

4단계 업데이트가 완료된 후 Geolocation Updates 페이지로 돌아가거나 **Help > About**을 선택하여 GeoDB 빌드 번호가 설치한 업데이트와 일치하는지 확인합니다.

GeoDB 업데이트는 GeoDB 이전 버전을 재정의하며 즉시 적용됩니다. GeoDB를 업데이트하면 방어 센터는 해당 관리되는 디바이스를 자동으로 업데이트합니다. GeoDB 업데이트가 구축 전체에서 반영되는 데 몇 분 정도 걸릴 수 있지만 업데이트 후 액세스 제어 정책을 다시 적용할 필요는 없습니다.

67장

시스템 모니터링

FireSIGHT 시스템은 일상적인 시스템 관리 업무에 도움이 되는 많은 유용한 모니터링 기능을 단일 페이지에서 모두 제공합니다. 예를 들어 Host Statistics 페이지에서는 기본 호스트 통계 및 침입 이벤트 정보는 물론 Data Correlator에 대한 통계와 현재 날짜의 네트워크 검색 프로세스도 모니터링할 수 있습니다. 또한 현재 방어 센터 또는 관리되는 디바이스에서 실행 중인 모든 프로세스에 대한 요약 및 자세한 정보를 모두 모니터링할 수 있습니다. 다음 절에서는 시스템에서 제공하는 모니터링 기능에 대해 자세히 설명합니다.

- 67-2페이지의 호스트 통계 보기 - 다음과 같은 호스트 정보를 보는 방법에 대해 설명합니다.
- 시스템 작동 시간
- 디스크 및 메모리 사용량
- Data Correlator 통계
- 시스템 프로세스
- 침입 이벤트 정보
- 방어 센터에서는 또한 상태 모니터를 사용하여 디스크 사용량을 모니터링하고 디스크 공간 부족에 대해 알림을 전송할 수 있습니다. 자세한 내용은 68-2페이지의 상태 모니터링 이해을/를 참조하십시오.
- 67-3페이지의 시스템 상태 및 디스크 공간 사용량 모니터링 - 기본 이벤트 및 디스크 파티션 정보를 보는 방법에 대해 설명합니다.
- 67-4페이지의 시스템 프로세스 상태 보기 - 기본 프로세스 상태를 보는 방법에 대해 설명합니다.
- 67-6페이지의 실행 중인 프로세스 이해 - 어플라이언스에서 실행되는 기본 시스템 프로세스에 대해 설명합니다.

Overview > Summary의 옵션을 사용하면 침입 및 검색 이벤트에 대한 통계를 보고 그래프로 표시할 수 있습니다. 자세한 내용은 다음 링크를 참고하십시오.

- 41-2페이지의 침입 이벤트 통계 보기
- 41-8페이지의 침입 이벤트 그래프 보기
- 50-2페이지의 검색 이벤트 통계 보기
- 50-6페이지의 검색 성능 그래프 보기

호스트 통계 보기

라이센스: 모두

Statistics 페이지에는 다음에 대한 현재 상태가 나열됩니다.

- 일반 호스트 통계. 자세한 내용은 호스트 통계 표 참조.
- Data Correlator 통계(방어 센터 전용 - FireSIGHT 필요). 자세한 내용은 Data Correlator 프로세스 통계 표 참조.
- 침입 이벤트 정보(보호 필요). 자세한 내용은 침입 이벤트 정보 표 참조.

다음 표에서는 Statistics 페이지에 나열되는 호스트 통계에 대해 설명합니다.

표 67-1 호스트 통계

카테고리	설명
Time	시스템의 현재 시간.
실행 시간	시스템이 마지막으로 시작된 이후의 일수(해당되는 경우), 시간 및 분.
Memory Usage	사용되고 있는 시스템 메모리의 비율.
로드 평균	지난 1분, 5분 및 15분 동안 CPU 대기열의 평균 프로세스 수.
Disk Usage	사용되고 있는 디스크의 비율. 자세한 호스트 통계를 보려면 화살표를 클릭하십시오. 자세한 내용은 67-3페이지의 시스템 상태 및 디스크 공간 사용량 모니터링을/를 참조하십시오.
프로세스	시스템에서 실행 중인 프로세스의 요약. 자세한 내용은 67-4페이지의 시스템 프로세스 상태 보기을/를 참조하십시오.

FireSIGHT 시스템 구축에 방어 센터(FireSIGHT 라이센스 포함)가 포함되어 있는 경우 Data Correlator에 대한 통계와 현재 날짜의 네트워크 검색 프로세스도 볼 수 있습니다. 관리되는 디바이스가 데이터 수집, 디코딩 및 분석을 수행하는 동안 네트워크 검색 프로세스는 데이터를 핑거프린트 및 취약성 데이터베이스와 상호 연결한 다음, 방어 센터에서 실행되는 Data Correlator에 의해 처리되는 이진 파일을 생성합니다. Data Correlator는 이진 파일의 정보를 분석하고, 이벤트를 생성하고, 검색 네트워크 맵을 만듭니다.

네트워크 검색 및 Data Correlator에 대해 표시되는 통계는 현재 날짜의 평균으로, 각 디바이스에 대해 오전 12:00에서 오후 11:59 사이에 수집된 통계가 사용됩니다.

다음 표에서는 Data Correlator 프로세스에 대해 표시되는 통계에 대해 설명합니다.

표 67-2 Data Correlator 프로세스 통계

카테고리	설명
Events/Sec	Data Correlator에서 초당 수신하여 처리하는 검색 이벤트의 수
Connections/Sec	Data Correlator에서 초당 수신하여 처리하는 연결의 수
CPU Usage — User (%)	현재 날짜에 대해 사용자 프로세스에 소비되는 평균 CPU 시간의 비율
CPU Usage — System (%)	현재 날짜에 대해 시스템 프로세스에 소비되는 평균 CPU 시간의 비율
VmSize (KB)	현재 날짜에 대해 Data Correlator에 할당된 평균 메모리의 크기(킬로바이트 단위)
VmRSS (KB)	현재 날짜에 대해 Data Correlator에서 사용하는 평균 메모리의 양(킬로바이트 단위)

관리되는 디바이스 및 디바이스를 관리하는 방어 센터에서는 마지막 침입 이벤트의 날짜와 시간, 지난 한 시간과 지난 하루 동안 발생한 총 이벤트의 수, 데이터베이스에 있는 총 이벤트의 수도 볼 수 있습니다.

참고 Statistics 페이지의 Intrusion Event Information 섹션은 방어 센터에 전송된 것이 아니라 관리되는 디바이스에 저장된 침입 이벤트를 기반으로 합니다. 침입 이벤트가 로컬에 저장되지 않도록 디바이스를 관리하는 경우 이 페이지에 침입 이벤트 정보가 나열되지 않습니다. 이는 이벤트를 로컬에 저장할 수 없는 관리되는 디바이스에도 해당됩니다.

다음 표에서는 Statistics 페이지의 Intrusion Event Information 섹션에 표시되는 통계에 대해 설명합니다.

표 67-3 침입 이벤트 정보

통계	설명
Last Alert Was	마지막 이벤트가 발생한 날짜 및 시간
Total Events Last Hour	지난 1시간 동안 발생한 총 이벤트의 수
Total Events Last Day	지난 24시간 동안 발생한 총 이벤트의 수
Total Events in Database	이벤트 데이터베이스에 있는 총 이벤트의 수

Statistics 페이지를 보려면

액세스: Admin/Maint

1단계 **System > Monitoring > Statistics**를 선택합니다.

Statistics 페이지가 나타납니다.

2단계 방어 센터에서는 관리되는 디바이스에 대한 통계도 나열해야 합니다. **Select Device(s)** 상자에서 **Select Devices**를 클릭합니다. 여러 디바이스를 동시에 선택하려면 Shift 키와 Ctrl 키를 사용할 수 있습니다.

Statistics 페이지는 사용자가 선택한 디바이스에 대한 통계로 업데이트됩니다.

시스템 상태 및 디스크 공간 사용량 모니터링

라이센스: 모두

Statistics 페이지의 Disk Usage 섹션은 카테고리 및 파티션 상태별 디스크 사용량의 빠른 개요를 제공합니다. 디바이스에 악성코드 스토리지 팩을 설치한 경우 파티션 상태도 점검할 수 있습니다. 시스템 프로세스와 데이터베이스에 사용할 수 있는 디스크 공간이 충분한지 확인하기 위해 수시로 이 페이지를 모니터링할 수 있습니다.

팁 방어 센터에서는 또한 상태 모니터를 사용하여 디스크 사용량을 모니터링하고 디스크 공간 부족에 대해 알림을 전송할 수 있습니다. 자세한 내용은 68-2페이지의 상태 모니터링 이해을/를 참조하십시오.

디스크 사용량 정보에 액세스하려면

액세스: Admin/Maint

1단계 **System > Monitoring > Statistics**를 선택합니다.

Statistics 페이지가 나타납니다.

2단계 보려는 By Category 누적 막대에서 디스크 사용량 카테고리 위로 포인터를 이동합니다(순서대로).

- 해당 카테고리에 사용되는 사용 가능한 디스크 공간의 비율
- 디스크의 실제 저장 공간
- 해당 카테고리에 사용할 수 있는 총 디스크 공간

디스크 사용량 카테고리에 대한 자세한 내용은 55-26페이지의 Disk Usage 위젯 이해을/를 참조하십시오.

3단계 **Total** 옆에 있는 아래쪽 화살표를 클릭하여 확장합니다.

Disk Usage 섹션이 확장되면서 파티션 사용량이 표시됩니다. 악성코드 스토리지 팩을 설치한 경우 `/var/storage` 파티션 사용량도 표시됩니다.

구축에 관리되는 디바이스가 여러 개 포함된 경우 특정 디바이스 단위로 디스크 사용량 데이터를 제한할 수 있습니다.

방어 센터에서 특정 디바이스에 대한 디스크 사용량 정보를 보려면

액세스: Admin/Maint

1단계 **Select Device(s)** 상자에서 디바이스 이름을 선택하고 **Select Devices**를 클릭합니다.

페이지가 다시 로드되면서, 선택한 각 디바이스에 대한 호스트 통계가 나열됩니다.

2단계 **Disk Usage** 옆에 있는 아래쪽 화살표를 클릭하여 확장합니다.

Disk Usage 섹션이 확장됩니다.

시스템 프로세스 상태 보기

라이센스: 모두

Host Statistics 페이지의 Processes 섹션에서는 어플라이언스에서 현재 실행 중인 프로세스를 볼 수 있습니다. 일반 프로세스 정보 및 각 실행 프로세스에 대한 특정 정보가 제공됩니다. 방어 센터에서 디바이스를 관리하는 경우 방어 센터의 웹 인터페이스를 사용하여 관리되는 디바이스의 프로세스 상태를 볼 수 있습니다.

다음 표에서는 프로세스 목록에 나타나는 각 열에 대해 설명합니다.

표 67-4 처리 상태

열	설명
Pid	프로세스 ID 번호
아이디	프로세스를 실행하는 사용자 또는 그룹의 이름
Pri	프로세스 우선순위

표 67-4 처리 상태 (계속)

열	설명
Nice	프로세스의 예약 우선순위를 나타내는 값인 *nice* 값. 값의 범위는 -20(가장 높은 우선순위)에서 19(가장 낮은 우선순위)까지입니다.
크기	프로세스에서 사용하는 메모리 크기(메가바이트를 나타내는 m이 값 뒤에 오지 않는 한 킬로바이트 단위)
Res	메모리에 상주하는 페이징 파일의 양(메가바이트를 나타내는 m이 값 뒤에 오지 않는 한 킬로바이트 단위)
주	프로세스 상태: • D - 프로세스가 무정전 슬립 상태임(대개 Input/Output) • N - 프로세스에 양의 nice 값이 있음 • R - 프로세스가 실행 가능함(실행할 대기열에 있음) • S - 프로세스가 슬립 모드에 있음 • T - 프로세스가 추적 중이거나 중지 상태임 • W - 프로세스가 페이징되고 있음 • X - 프로세스가 dead 상태임 • Z - 프로세스가 작동하지 않음 • < - 프로세스에 음의 nice 값이 있음
Time	프로세스가 실행된 시간의 양(시:분:초 형식)
Cpu	프로세스가 사용하는 CPU의 비율
명령	프로세스의 실행 파일 이름

프로세스 목록을 확장하려면

액세스: Admin/Maint

1단계 **System > Monitoring > Statistics**를 선택합니다.

Statistics 페이지가 나타납니다.

2단계 방어 센터에서, 프로세스 통계를 보려는 디바이스를 **Select Device(s)** 상자에서 선택하고 **Select Devices**를 클릭합니다.

3단계 **Processes** 옆에 있는 아래쪽 화살표를 클릭합니다.

프로세스 목록이 확장되면서, 실행 중인 작업의 수와 유형이 포함된 일반 프로세스 상태 정보, 현재 시간, 현재 시스템 가동 시간, 시스템 로드 평균, CPU 메모리, 스왑 정보, 그리고 실행 중인 각 프로세스에 대한 특정 정보가 나열됩니다.

Cpu(s) - 다음 CPU 사용량 정보가 나열됩니다.

- 사용자 프로세스 사용량 비율
- 시스템 프로세스 사용량 비율
- nice 사용량 비율(음의 nice 값이 있는 프로세스의 CPU 사용량으로 더 높은 우선순위를 나타냄)

  Nice 값은 시스템 프로세스에 대해 예약된 우선순위를 나타내며 범위는 -20(가장 높은 우선순위)에서 19(가장 낮은 우선순위)까지입니다.
- 유휴 사용량 비율

Mem - 다음 메모리 사용량 정보가 나열됩니다.

- 메모리의 총 킬로바이트 수
- 사용된 메모리의 총 킬로바이트 수
- 여유 메모리의 총 킬로바이트 수
- 버퍼링된 메모리의 총 킬로바이트 수

Swap - 다음 스왑 사용량 정보가 나열됩니다.

- 스왑의 총 킬로바이트 수
- 사용된 스왑의 총 킬로바이트 수
- 여유 스왑의 총 킬로바이트 수
- 캐시된 스왑의 총 킬로바이트 수

참고 어플라이언스에서 실행되는 프로세스 유형에 대한 자세한 내용은 67-6페이지의 실행 중인 프로세스 이해을/를 참조하십시오.

프로세스 목록을 축소하려면

액세스: Admin/Maint

1단계 **Processes** 옆에 있는 위쪽 화살표를 클릭합니다.

프로세스 목록이 축소됩니다.

실행 중인 프로세스 이해

라이센스: 모두

어플라이언스에서 실행되는 프로세스에는 두 가지 유형, 즉 디먼과 실행 파일이 있습니다. 디먼은 항상 실행되며 실행 파일은 필요할 때 실행됩니다.

자세한 내용은 다음 절을 참조하십시오.

- 67-6페이지의 시스템 디먼 이해
- 67-8페이지의 실행 파일 및 시스템 유틸리티 이해

시스템 디먼 이해

라이센스: 모두

디먼은 어플라이언스에서 지속적으로 실행됩니다. 디먼은 서비스의 가용성을 보장하며 필요 시 프로세스의 생성을 보장합니다. 다음 표에서는 Process Status 페이지에 나타날 수 있는 디먼 및 각 기능에 대한 간단한 설명을 제공합니다.

참고 아래의 표는 어플라이언스에서 실행될 수 있는 모든 프로세스의 완전한 목록이 아닙니다.

표 67-5 시스템 디먼

디먼	설명
crond	예약된 명령의 실행을 관리합니다(cron 작업).
dhclient	동적 호스트 IP 주소 지정을 관리합니다.
fpcollect	클라이언트 및 서버 핑거프린트의 수집을 관리합니다.
httpd	HTTP(Apache 웹 서버) 프로세스를 관리합니다.
httpsd	HTTPS(SSL의 Apache 웹 서버) 서비스를 관리하고, 작동하는 SSL 및 유효한 인증서 인증을 점검하며, 배경에서 실행되면서 어플라이언스에 대한 보안 웹 액세스를 제공합니다.
keventd	Linux 커널 이벤트 알림 메시지를 관리합니다.
klogd	Linux 커널 메시지의 차단 및 로깅을 관리합니다.
kswapd	Linux 커널 스왑 메모리를 관리합니다.
kupdated	디스크 동기화를 수행하는 Linux 커널 업데이트 프로세스를 관리합니다.
mysqld	FireSIGHT 시스템 데이터베이스 프로세스를 관리합니다.
ntpd	NTP(Network Time Protocol) 프로세스를 관리합니다.
pm	모든 Cisco 프로세스를 관리하고, 필요한 프로세스를 시작하며, 예기치 않게 실패한 프로세스를 다시 시작합니다.
reportd	보고서를 관리합니다.
safe_mysqld	데이터베이스의 안전 모드 작동을 관리하고, 오류 발생 시 데이터베이스 디먼을 다시 시작하고 런타임 정보를 파일에 로깅합니다.
SFDataCorrelator	데이터 전송을 관리합니다.
sfestreamer (방어 센터 전용)	Event Streamer를 사용하는 타사 클라이언트 애플리케이션에 대한 연결을 관리합니다.
sfmgr	어플라이언스에 대한 sftunnel 연결을 사용하여 어플라이언스를 원격으로 관리 및 구성할 수 있도록 RPC 서비스를 제공합니다.
SFRemediateD (방어 센터 전용 - FireSIGHT 필요)	교정 응답을 관리합니다.
sftimeserviced (방어 센터 전용)	시간 동기화 메시지를 관리되는 디바이스에 전달합니다.
sfmbservice (보호 필요)	어플라이언스에 대한 sftunnel 연결을 사용하여 원격 어플라이언스에서 실행되는 sfmb 메시지 브로커 프로세스에 대한 액세스를 제공합니다. 관리되는 디바이스의 상태 이벤트와 알림을 방어 센터로(또는 고가용성 환경에서는 방어 센터 간에) 전송하기 위해 현재 상태 모니터링에서만 사용합니다.
sftroughd	수신 소켓에서 연결을 수신 대기하고, 요청을 처리하기 위한 올바른 실행 파일(일반적으로 Cisco 메시지 브로커, sfmb)을 호출합니다.
sftunnel	원격 어플라이언스와의 통신을 요구하는 모든 프로세스를 위한 안전한 통신 채널을 제공합니다.
sshd	SSH(Secure Shell) 프로세스를 관리하고, 어플라이언스에 SSH 액세스를 제공하기 위해 배경에서 실행됩니다.
syslogd	시스템 로깅(syslog) 프로세스를 관리합니다.

실행 파일 및 시스템 유틸리티 이해

라이센스: 모두

시스템에는 다른 프로세스에 의해 실행되거나 사용자 작업을 통해 실행되는 여러 실행 파일이 있습니다. 다음 표에서는 Process Status 페이지에 나타날 수 있는 실행 파일에 대해 설명합니다.

표 67-6 시스템 실행 파일 및 유틸리티

실행 파일	설명
awk	awk 프로그래밍 언어로 작성된 프로그램을 실행하는 유틸리티
bash	GNU Bourne-Again SHell
cat	파일을 읽고 내용을 표준 출력에 기록하는 유틸리티
chown	사용자 및 그룹 파일 권한을 변경하는 유틸리티
chsh	기본 로그인 셸을 변경하는 유틸리티
SFDataCorrelator (방어 센터 전용 - FireSIGHT 필요)	이벤트, 연결 데이터 및 네트워크 맵을 생성하기 위해 FireSIGHT에서 만드는 이진 파일 분석
cp	파일을 복사하는 유틸리티
df	어플라이언스의 여유 공간을 나열하는 유틸리티
echo	내용을 표준 출력에 기록하는 유틸리티
egrep	파일과 폴더에서 지정된 입력을 검색하고, 표준 grep에서 지원되지 않는 확장 정규식 집합을 지원하는 유틸리티
find	지정된 입력에 대한 디렉토리를 재귀적으로 검색하는 유틸리티
grep	지정된 입력에 대한 파일과 디렉토리를 검색하는 유틸리티
halt	서버를 중지하는 유틸리티
httpsdctl	Apache Web 프로세스를 안전하게 처리
hwclock	하드웨어 시계에 대한 액세스를 허용하는 유틸리티
ifconfig	네트워크 컨피그레이션 실행 파일을 나타내며, MAC 주소가 일정하게 유지되도록 보장
iptables	Access Configuration 페이지에 대한 변경 사항을 기반으로 액세스 제한 처리. 액세스 컨피그레이션에 대한 자세한 내용은 63-9페이지의 어플라이언스에 대한 액세스 목록 구성을/를 참조하십시오.
iptables-restore	iptables 파일 복원 처리
iptables-save	iptables에 대한 저장된 변경 사항 처리
kill	한 세션과 프로세스를 종료하기 위해 사용할 수 있는 유틸리티
killall	모든 세션과 프로세스를 종료하기 위해 사용할 수 있는 유틸리티
ksh	Korn 셸의 퍼블릭 도메인 버전
logger	명령줄에서 syslog 디먼에 액세스하는 방법을 제공하는 유틸리티
md5sum	지정된 파일에 대한 체크섬과 블록 카운트를 출력하는 유틸리티
mv	파일을 이동(이름 변경)하는 유틸리티
myisamchk	데이터베이스 테이블 검사 및 복구를 나타냄
MySQL	데이터베이스 프로세스를 나타내며, 여러 인스턴스가 나타날 수 있음

표 67-6 시스템 실행 파일 및 유틸리티 (계속)

실행 파일	설명
openssl	인증 인증서 생성을 나타냄
perl	perl 프로세스를 나타냄
ps	프로세스 정보를 표준 출력에 기록하는 유틸리티
sed	하나 이상의 텍스트 파일을 수정하는 데 사용되는 유틸리티
sfheartbeat	어플라이언스가 활성 상태임을 나타내는 하트비트 브로드캐스트 식별. 하트비트는 디바이스와 방어 센터 사이의 연결을 유지하는 데 사용됨.
sfmb	메시지 브로커 프로세스를 나타내며, 방어 센터와 디바이스 간 통신을 처리
sh	Korn 셸의 퍼블릭 도메인 버전
shutdown	어플라이언스를 종료하는 유틸리티
sleep	지정 기간(초) 동안 프로세스를 일시 중단하는 유틸리티
smtpclient	이메일 이벤트 알림 기능이 활성화될 때 이메일 전송을 처리하는 메일 클라이언트
snmptrap	SNMP 알림 기능이 활성화될 때 SNMP 트랩 데이터를 지정된 SNMP 트랩 서버로 전달
snort (보호 필요)	Snort가 실행 중임을 나타냄
SSH	어플라이언스에 대한 SSH(Secure Shell) 연결을 나타냄
sudo	관리자 이외의 사용자가 실행 파일을 실행하도록 허용하는 sudo 프로세스를 나타냄
top	상위 CPU 프로세스에 대한 정보를 표시하는 유틸리티
touch	지정된 파일의 액세스 및 수정 시간을 변경하는 데 사용할 수 있는 유틸리티
vim	텍스트 파일 수정에 사용되는 유틸리티
wc	지정된 파일에서 줄, 단어 및 바이트 카운트를 수행하는 유틸리티

68장

상태 모니터링 사용

상태 모니터는 방어 센터에서 어플라이언스의 상태를 확인할 수 있는 다양한 테스트를 제공합니다. 상태 모니터를 사용하면 테스트 집합(*상태 정책*이라고 함)을 생성하고 하나 이상의 어플라이언스에 상태 정책을 적용할 수 있습니다. 시스템의 모든 어플라이언스에 대해 하나의 상태 정책을 생성하거나, 특정 어플라이언스에 적용하고자 하는 상태 정책을 사용자 지정하거나, 기본 상태 정책을 사용할 수 있습니다. 다른 방어 센터에서 내보낸 상태 정책을 가져올 수도 있습니다.

*상태 모듈*이라고도 하는 테스트는 지정한 기준을 테스트하는 스크립트입니다. 테스트를 활성화 또는 비활성화하거나 테스트 설정을 변경하여 상태 정책을 수정할 수 있으며, 더 이상 필요하지 않은 상태 정책을 삭제할 수 있습니다. 선택한 어플라이언스를 블랙리스트에 추가하여 해당 메시지를 억제할 수도 있습니다.

상태 정책의 테스트는 구성한 간격으로 자동 실행됩니다. 필요에 따라 모든 테스트 또는 특정 테스트를 실행할 수 있습니다. 상태 모니터는 구성한 테스트 조건을 기반으로 상태 이벤트를 수집합니다. 선택적으로, 상태 이벤트에 대한 응답으로 이메일, SNMP 또는 syslog 알림을 구성할 수도 있습니다.

방어 센터에서 전체 시스템 또는 특정 어플라이언스에 대한 상태 정보를 볼 수 있습니다. 완전히 사용자 지정 가능한 이벤트 보기에서는 상태 모니터에서 수집한 상태 이벤트를 빠르고 쉽게 분석할 수 있습니다. 이러한 이벤트 보기에서는 이벤트 데이터를 검색하고 볼 수 있으며, 조사 중인 이벤트와 관련이 있을 수 있는 다른 정보에 액세스할 수 있습니다.

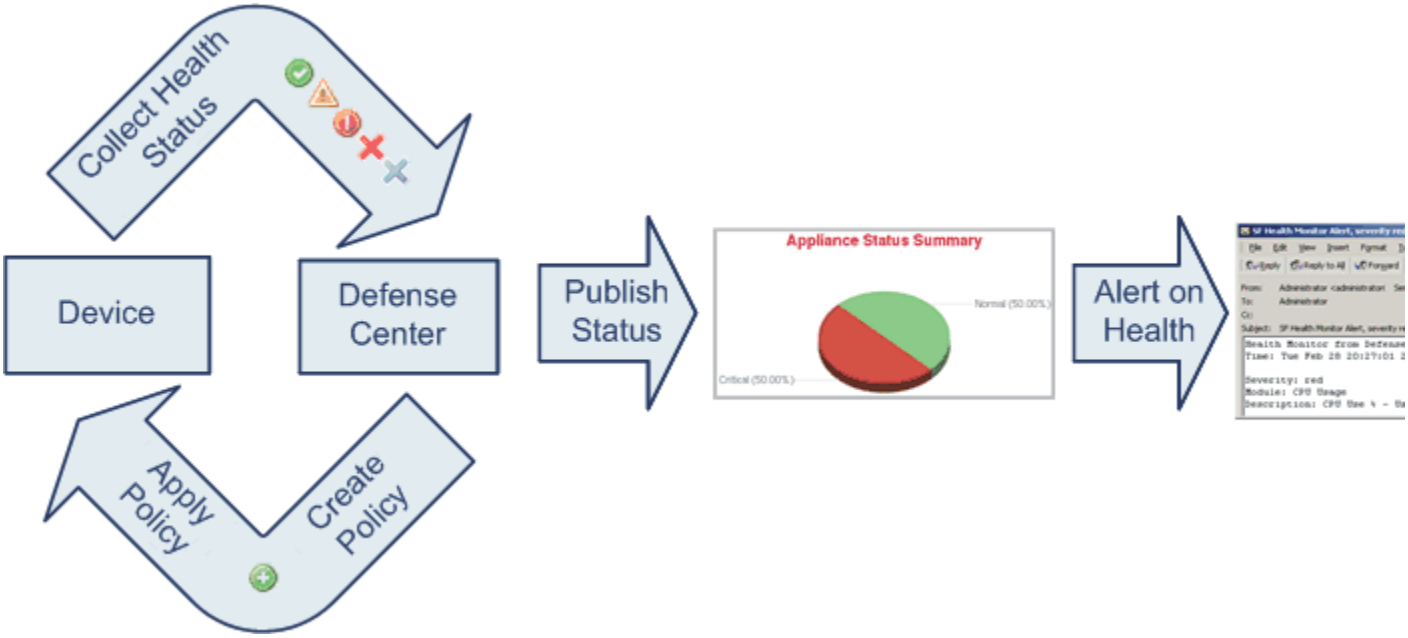
또한 고객 지원에서 요청할 경우 어플라이언스에 대한 문제 해결 파일을 생성할 수도 있습니다.

자세한 내용은 다음 절을 참조하십시오.

상태 모니터링 이해

라이센스: 모두

상태 모니터를 사용하면 FireSIGHT 시스템 구축 전체에서 중요한 기능의 상태를 확인할 수 있습니다. 각각의 관리되는 디바이스에 상태 정책을 적용하고 방어 센터에서 결과 상태 데이터를 수집하여 방어 센터를 통해 전체 FireSIGHT 시스템에서 상태를 모니터링합니다. Health Monitor 페이지의 원 그래프와 상태 테이블은 모니터링되는 어플라이언스의 상태를 시각적으로 표현하므로, 한눈에 상태를 확인한 다음 필요할 경우 상태 세부사항으로 드릴다운할 수 있습니다.



상태 모니터를 사용하면 전체 시스템 또는 특정 어플라이언스에 대한 상태 정보를 볼 수 있습니다. Health Monitor 페이지는 시스템의 모든 어플라이언스 상태를 시각적으로 요약하여 보여줍니다. 개별 어플라이언스 상태 모니터에서는 특정 어플라이언스의 상태로 드릴다운할 수 있습니다.

표준 FireSIGHT 시스템 테이블 보기에서도 상태 이벤트를 볼 수 있습니다. 개별 어플라이언스의 상태 모니터에서 특정 이벤트 발생의 테이블 보기를 열 수도 있고, 해당 어플라이언스에 대한 모든 상태 이벤트를 검색할 수도 있습니다. 특정 상태 이벤트를 검색할 수도 있습니다. 예를 들어 CPU 사용량이 특정 비율에 도달한 모든 경우를 보려면 CPU 사용량 모듈을 검색하고 비율 값을 입력합니다.

상태 이벤트에 대한 응답으로 이메일, SNMP 또는 syslog 알림을 구성할 수도 있습니다. *상태 알림*은 표준 알림과 상태 레벨을 연결한 것입니다. 하드웨어 과부하 때문에 어플라이언스가 실패하지 않도록 하려면 이메일 알림을 설정할 수 있습니다. 그런 다음 CPU, 디스크 또는 메모리 사용량이 어플라이언스에 적용된 상태 정책에서 구성한 경고(Warning) 레벨에 도달할 때마다 이메일 알림을 트리거하는 상태 알림을 생성할 수 있습니다. 반복해서 알림을 수신하는 횟수를 최소화하려면 알림 임계값을 설정할 수 있습니다.

상태 모니터링은 관리 활동이므로 관리자 사용자 역할 권한이 있는 사용자만 시스템 상태 데이터에 액세스할 수 있습니다. 사용자 권한 할당에 대한 자세한 내용은 61-54페이지의 사용자 권한 및 옵션 수정을/를 참조하십시오.

참고 방어 센터를 제외하고, 기본적으로 FireSIGHT 시스템 디바이스에는 상태 모니터링 정책이 적용되지 않습니다. 관리되는 디바이스는 Hardware Alarms 상태 모듈을 통해 자동으로 하드웨어 상태를 보고합니다. 관리되는 디바이스를 모니터링하는 데 다른 모듈을 사용하려면 해당 디바이스에 상태 정책을 적용해야 합니다. Cisco에서 제공하는 어플라이언스용 기본 상태 정책에 대한 자세한 내용은 68-7페이지의 기본 상태 정책 이해을/를 참조하십시오. 사용자 지정 상태 정책 생성에 대한 자세한 내용은 68-9페이지의 상태 정책 생성을/를 참조하십시오. 정책 적용에 대한 자세한 내용은 68-29페이지의 상태 정책 적용을/를 참조하십시오.

시스템 상태를 테스트하기 위해 실행할 수 있는 상태 정책 및 상태 모듈에 대한 자세한 내용은 다음 항목을 참조하십시오.

- 68-3페이지의 상태 정책 이해
- 68-3페이지의 상태 모듈 이해
- 68-6페이지의 상태 모니터링 컨피그레이션 이해

상태 정책 이해

라이센스: 모두

*상태 정책*이란 방어 센터가 어플라이언스의 상태를 확인할 때 사용하는 기준을 정의하기 위해 어플라이언스에 적용하는 상태 모듈 설정의 모음입니다. 상태 모니터는 FireSIGHT 시스템 하드웨어 및 소프트웨어가 올바르게 작동하는지 확인하기 위해 다양한 상태 지표를 추적합니다.

상태 정책을 생성할 때 어플라이언스 상태 확인을 위해 어떤 테스트를 실행할지 선택합니다. 또한 어떤 어플라이언스에나 기본 상태 정책을 적용할 수 있습니다.

상태 모듈 이해

라이센스: 모두

*상태 테스트*라고도 하는 *상태 모듈*은 상태 정책에서 지정하는 기준을 테스트하는 스크립트입니다. 사용 가능한 상태 모듈에 대해 다음 표에서 설명합니다.

표 68-1 상태 모듈

모듈	설명
Advanced Malware Protection	이 모듈은 방어 센터가 네트워크 트래픽에서 탐지된 파일의 파일 성향 정보를 검색하거나 동적 분석을 위해 파일을 제출하기 위해 종합 보안 인텔리전스 클라우드에 접속할 수 없는 경우 또는 파일 정책 컨피그레이션을 기반으로 네트워크 트래픽에서 너무 많은 파일이 탐지되는 경우 알림을 전송합니다. 프라이빗 클라우드가 퍼블릭 Cisco 클라우드에 연결할 수 없는 경우에도 FireAMP Private Cloud를 통한 연결은 알림을 생성합니다. 이 모듈은 AMP를 지원하지 않는 DC500을 제외한 모든 방어 센터에서 실행됩니다.
Appliance Heartbeat	이 모듈은 어플라이언스에서 어플라이언스 하트비트가 전송되는지 확인하고, 어플라이언스 하트비트 상태를 기반으로 알림을 전송합니다.
Automatic Application Bypass Status	이 모듈은 어플라이언스가 우회 임계값에 설정된 시간(초 단위) 내에 응답하지 않아서 우회되었는지 확인하고, 우회가 발생하면 알림을 전송합니다.

표 68-1 상태 모듈 (계속)

모듈	설명
CPU Usage	이 모듈은 어플라이언스의 CPU가 과부하되지 않았는지 확인하고, CPU 사용량이 모듈에 대해 구성된 비율을 초과하면 알림을 전송합니다. 3D9900 디바이스에 적용된 상태 정책에는 이 모듈을 사용할 수 없습니다.
Card Reset	이 모듈은 하드웨어 장애 때문에 다시 시작된 네트워크 카드를 확인하고, 재설정이 발생하면 알림을 전송합니다.
Disk Status	이 모듈은 하드 디스크의 성능과 어플라이언스의 악성코드 스토리지 팩(설치된 경우)을 점검합니다. 하드 디스크와 RAID 컨트롤러(설치된 경우)가 실패할 위험이 있을 때 또는 악성코드 스토리지 팩이 설치 후 탐지되지 않거나 인증되지 않을 때 알림을 전송합니다.
Disk Usage	이 모듈은 어플라이언스 하드 드라이브 및 악성코드 스토리지 팩의 디스크 사용량을 모듈에 대해 구성된 제한과 비교하고, 사용량이 모듈에 대해 구성된 비율을 초과하면 알림을 전송합니다. 또한 시스템이 모니터링되는 디스크 사용량 카테고리에서 과도하게 파일을 삭제하는 경우 또는 모듈 임계값을 기반으로 그러한 카테고리 외의 디스크 사용량이 과도한 수준에 도달하는 경우에도 알림을 전송합니다.
FireAMP Status Monitor	이 모듈은 초기의 성공적인 연결 이후 방어 센터가 Cisco 클라우드에 연결할 수 없는 경우, 사용자가 FireAMP 포털을 사용하여 클라우드 연결을 등록 취소하는 경우, 또는 프라이빗 클라우드가 퍼블릭 Cisco 클라우드와 통신할 수 없는 경우 알림을 전송합니다. 이 모듈은 방어 센터에서만 실행됩니다.
FireSIGHT Host License Limit	이 모듈은 FireSIGHT 호스트 라이센스가 충분히 남아 있는지 확인하고, 모듈에 대해 구성된 경고 레벨을 기반으로 알림을 전송합니다. 이 모듈은 방어 센터에서만 실행됩니다.
Hardware Alarms	이 모듈은 Series 3 또는 3D9900 디바이스에서 하드웨어의 교체가 필요한지 여부를 판단하고, 하드웨어 상태를 기반으로 알림을 전송합니다. 이 모듈은 또한 하드웨어와 관련된 디먼의 상태 및 클러스터링된 어플라이언스의 상태에 대해 보고합니다. 이러한 디바이스에 대해 보고되는 세부사항에 대한 자세한 내용은 68-51페이지의 3D9900 디바이스에 대한 하드웨어 알림 세부사항 해석 및 68-52페이지의 Series 3 디바이스에 대한 하드웨어 알림 세부사항 해석을/를 참조하십시오.
Health Monitor Process	이 모듈은 상태 모니터 자체의 상태를 모니터링하고, 방어 센터에서 마지막으로 상태 이벤트를 수신한 후 시간(분 단위)이 Warning 또는 Critical 제한을 초과하면 알림을 전송합니다. 이 모듈은 방어 센터에서만 실행됩니다.
Inline Link Mismatch Alarms	이 모듈은 인라인 집합과 관련된 포트를 모니터링하고, 인라인 쌍의 두 인터페이스가 서로 다른 속도를 협상하는 경우 알림을 전송합니다.
Intrusion Event Rate	이 모듈은 초당 침입 이벤트 수를 모듈에 대해 구성된 제한과 비교하고, 제한을 초과하는 경우 알림을 전송합니다. Intrusion Event Rate가 0이면 침입 프로세스가 다운되거나 관리되는 디바이스가 이벤트를 전송하지 못할 수 있습니다. 디바이스에서 이벤트가 수신되면 **Analysis > Intrusions > Events**를 선택합니다.
Interface Status	이 모듈은 디바이스가 현재 트래픽을 수집하는지 확인하고, 물리적 인터페이스와 집계 인터페이스의 트래픽 상태를 기준으로 알림을 제공합니다. 물리적 인터페이스의 경우 정보에 인터페이스 이름, 링크 상태 및 대역폭이 포함됩니다. 집계 인터페이스의 경우 정보에 인터페이스 이름, 활성 링크의 수, 총 집계 대역폭이 포함됩니다.

표 68-1 상태 모듈 (계속)

모듈	설명
License Monitor	이 모듈은 제어, 보호, URL 필터링, 악성코드 및 VPN에 대한 라이센스가 충분히 남아 있는지를 확인합니다. 스택의 디바이스가 라이센스 세트와 일치하지 않는 경우에도 알림을 전송합니다. 모듈에 대해 자동으로 구성된 경고 레벨을 기반으로 알림이 전송됩니다. 이 모듈의 컨피그레이션을 변경할 수 없습니다. 이 모듈은 방어 센터에서만 실행됩니다.
Link State Propagation	페어링된 인라인 집합의 링크가 실패하는 경우를 확인하고 링크 상태 전파 모드를 트리거합니다.
Memory Usage	이 모듈은 어플라이언스의 메모리 사용량을 모듈에 대해 구성된 제한과 비교하고, 사용량이 모듈에 대해 구성된 레벨을 초과하면 알림을 전송합니다.
Power Supply	이 모듈은 디바이스의 전력 공급 장치를 교체해야 하는지 여부를 확인하고, 전력 공급 장치 상태를 기반으로 알림을 전송합니다. 이 모듈은 방어 센터 DC1500, DC2000, DC3500, DC4000에서 실행됩니다. 이 모듈은 3D3500, 3D4500, 3D6500, 3D9900 및 Series 3에서 실행됩니다.
Process Status	이 모듈은 어플라이언스의 프로세스가 프로세스 관리자 외부에서 종료되는지를 확인합니다. 프로세스가 프로세스 관리자 외부에서 고의로 종료되면 모듈 상태가 Warning으로 변경되며, 모듈이 다시 실행되고 프로세스가 다시 시작될 때까지 상태 이벤트 메시지에 프로세스가 종료되었음이 표시됩니다. 프로세스가 프로세스 관리자 외부에서 비정상적으로 종료되거나 충돌되면 모듈 상태가 Critical로 변경되며, 모듈이 다시 실행되고 프로세스가 다시 시작될 때까지 상태 이벤트 메시지에 프로세스가 종료되었음이 표시됩니다.
Reconfiguring Detection	이 모듈은 실패한 정책이 등록된 관리되는 디바이스에 적용된 후에도 탐지 기능이 지속되는지를 확인합니다. 정책 적용이 실패한 후 탐지 기능이 작동하지 않는 것으로 나타나면, 탐지 기능이 다시 설정될 때까지 모듈에서 상태 알림을 생성합니다.
RRD Server Process	이 모듈은 시계열 데이터를 저장하는 라운드 로빈 데이터 서버가 제대로 실행 중인지를 확인하고, 최신 RRD 서버 재시동 횟수를 기반으로 알림을 전송합니다. 이 모듈은 방어 센터에서만 실행됩니다.
Security Intelligence	이 모듈은 피드 업데이트, 피드 손상, 메모리 문제 등 보안 인텔리전스 필터링과 관련된 다양한 상황에서 알림을 전송합니다. 이 모듈은 보안 인텔리전스 필터링을 지원하지 않는 DC500을 제외한 모든 방어 센터에서 실행됩니다.
Time Series Data Monitor	이 모듈은 시계열 데이터(예: 규정 준수 이벤트 카운트)가 저장된 디렉토리에 손상된 파일이 있는지를 추적하고, 손상되어 제거된 것으로 파일에 플래그가 표시되는 경우 알림을 전송합니다. 이 모듈은 방어 센터에서만 실행됩니다.
Time Synchronization Status	이 모듈은 NTP를 사용하여 시간을 가져오는 디바이스 시계와 NTP 서버에 있는 시계의 동기화를 추적하고, 두 시계 간 차이가 10초를 넘으면 알림을 전송합니다.

표 68-1 상태 모듈 (계속)

모듈	설명
URL Filtering Monitor	이 모듈은 방어 센터와 Cisco 클라우드 간 통신을 추적합니다. 여기서 시스템은 일반적으로 방문되는 URL에 대한 URL 필터링(카테고리 및 평판) 데이터를 가져옵니다. 방어 센터가 성공적으로 통신하지 못하거나 클라우드에서 업데이트를 검색하지 못하면 알림이 전송됩니다. 이 모듈은 방어 센터와 URL 필터링을 활성화한 관리되는 디바이스 간 통신도 추적합니다. 방어 센터가 그러한 디바이스에 URL 필터링 데이터를 푸시하지 못하는 경우 알림이 전송됩니다. 이 모듈은 URL 필터링을 지원하지 않는 DC500을 제외한 모든 방어 센터에서만 실행됩니다.
User Agent Status Monitor	이 모듈은 방어 센터에 연결된 User Agents에 대한 하트비트가 탐지되지 않으면 알림을 전송합니다. 이 모듈은 방어 센터에서만 실행됩니다.
VPN Status	이 모듈은 VPN 기능이 작동하지 않음을 시스템이 탐지할 때 알림을 전송합니다. 이 모듈은 방어 센터에서만 실행됩니다.

상태 모니터링 컨피그레이션 이해

라이센스: 모두

다음 절차에 나와 있듯이, FireSIGHT 시스템에서 상태 모니터링을 설정하기 위한 몇 가지 단계가 있습니다.

1단계 어플라이언스용 상태 정책을 생성합니다.

FireSIGHT 시스템에 있는 각 어플라이언스 종류에 대해 특정 정책을 설정하고 해당 어플라이언스에 맞는 테스트만 활성화할 수 있습니다.

팁 모니터링 동작을 사용자 지정하지 않고 빠르게 상태 모니터링을 활성화하려면 이 용도로 제공되는 기본 정책을 적용할 수 있습니다.

상태 정책 설정에 대한 자세한 내용은 68-7페이지의 상태 정책 구성을/를 참조하십시오.

2단계 상태를 추적하려는 각 어플라이언스에 상태 정책을 적용합니다. 즉시 적용 가능한 기본 상태 정책에 대한 자세한 내용은 68-7페이지의 기본 상태 정책 이해을/를 참조하십시오.

3단계 선택적으로, 상태 모니터 알림을 구성합니다.

상태 레벨이 특정 상태 모듈에 대해 특정 심각도에 도달할 때 트리거되는 이메일, syslog 또는 SNMP 알림을 설정할 수 있습니다.

상태 모니터 설정에 대한 자세한 내용은 68-38페이지의 상태 모니터 알림 구성을/를 참조하십시오.

시스템에서 상태 모니터링을 설정한 후 Health Monitor 페이지 또는 Health Events 테이블 보기에서 언제든지 상태를 볼 수 있습니다. 시스템 상태 데이터 보기에 대한 자세한 내용은 다음 항목을 참조하십시오.

- 68-41페이지의 상태 모니터 사용
- 68-42페이지의 어플라이언스 상태 모니터 사용
- 68-48페이지의 상태 이벤트 작업

상태 정책 구성

라이센스: 모두

상태 정책에는 여러 모듈용으로 구성된 상태 테스트 기준이 포함되어 있습니다. 각 어플라이언스에 대해 어떤 상태 모듈을 실행할지 제어할 수 있으며, 각 모듈에 의해 실행되는 테스트에서 사용할 특정 제한을 구성할 수 있습니다. 상태 정책에서 구성할 수 있는 상태 모듈에 대한 자세한 내용은 68-2페이지의 상태 모니터링 이해을/를 참조하십시오.

시스템의 모든 어플라이언스에 적용할 수 있는 하나의 상태 정책을 생성하거나, 특정 어플라이언스에 적용하고자 하는 각 상태 정책을 사용자 지정하거나, 제공되는 기본 상태 정책을 사용할 수 있습니다. 다른 방어 센터에서 내보낸 상태 정책을 가져올 수도 있습니다.

상태 정책을 구성할 때에는 해당 정책에 대해 각 상태 모듈을 활성화할지 여부를 결정합니다. 또한 활성화된 각 모듈이 프로세스의 상태를 평가할 때마다 보고할 상태를 제어하는 기준을 선택할 수 있습니다.

방어 센터 에 자동으로 적용되는 기본 상태 정책에 대한 자세한 내용은 68-7페이지의 기본 상태 정책 이해을/를 참조하십시오.

자세한 내용은 다음 항목을 참조하십시오.

- 68-7페이지의 기본 상태 정책 이해
- 68-9페이지의 상태 정책 생성
- 68-29페이지의 상태 정책 적용
- 68-30페이지의 상태 정책 수정
- 68-32페이지의 상태 정책 비교
- 68-34페이지의 상태 정책 삭제

기본 상태 정책 이해

라이센스: 모두

방어 센터 상태 모니터에는 어플라이언스에 대한 상태 모니터링을 빠르고 쉽게 구현할 수 있도록 도와주는 기본 상태 정책이 포함되어 있습니다. 기본 상태 정책은 자동으로 방어 센터에 적용됩니다. 기본 상태 정책은 수정할 수 없지만, 이를 복사하여 해당 컨피그레이션을 기반으로 사용자 지정 정책을 생성할 수 있습니다. 자세한 내용은 68-9페이지의 상태 정책 생성을/를 참조하십시오.

디바이스 상태를 모니터링하려면 관리되는 디바이스에 상태 정책을 푸시할 수 있습니다.

참고 Cisco NGIPS for Blue Coat X-Series에는 상태 정책을 적용할 수 없습니다.

기본 상태 정책에서는 실행 중인 플랫폼에서 사용할 수 있는 상태 모듈이 대부분 자동으로 활성화됩니다. 다음 표는 방어 센터 및 관리되는 디바이스에 대한 기본 정책에서 활성화되는 모듈에 대해 자세히 설명합니다.

표 68-2 기본 활성 상태 모듈

모듈	방어 센터	관리되는 디바이스
AMP(Advanced Malware Protection)	예	아니요
Appliance Heartbeat	예	아니요
자동 애플리케이션 바이패스	아니요	예
CPU 사용	아니요	아니요
Card Reset	아니요	아니요
Disk Status	예	예
Disk Usage	예	예
FireAMP Status Monitor	예	아니요
FireSIGHT Host License Limit	예	아니요
Hardware Alarm	아니요	예
Health Monitor Process	아니요	아니요
Inline Link Mismatch Alarms	아니요	예
Interface Status	아니요	예
Intrusion Event Rate	아니요	예
License Monitor	예	아니요
Link State Propagation	아니요	예
Memory Usage	예	예
전력 공급 장치	아니요	예
처리 상태	예	예
Reconfiguring Detection	아니요	예
RRD Server Process	예	아니요
보안 인텔리전스	예	아니요
Time Series Data Monitor	예	아니요
Time Synchronization Status	예	예
URL Filtering Monitor	예	아니요
User Agent Status Monitor	예	아니요
VPN 상태	예	아니요

상태 정책 생성

라이센스: 모두

어플라이언스와 함께 사용할 상태 정책을 사용자 지정하려면 새 정책을 생성할 수 있습니다. 초기에는 정책의 설정이 새 정책의 기반으로 선택한 상태 정책에서 오는 설정으로 채워집니다. 정책 내 모듈을 활성화 또는 비활성화할 수 있으며 필요에 따라 각 모듈의 알림 기준을 변경할 수 있습니다.

팁 새 정책을 생성하는 대신, 다른 방어 센터에서 상태 정책을 내보내고 현재 방어 센터로 가져올 수 있습니다. 그런 다음 가져온 정책을 필요에 맞게 수정한 다음 적용할 수 있습니다. 자세한 내용은 A-1페이지의 컨피그레이션 가져오기 및 내보내기을/를 참조하십시오.

상태 정책을 생성하려면

액세스: Admin/Maint

1단계 **Health > Health Policy**를 선택합니다.

Health Policy 페이지가 나타납니다.

2단계 **Create Policy**를 클릭합니다.

Create Health Policy 페이지가 나타납니다.

3단계 새 정책의 기본으로 사용할 기존 정책을 **Copy Policy** 드롭다운 목록에서 선택합니다.

4단계 정책의 이름을 입력합니다.

5단계 정책의 설명을 추가합니다.

6단계 **Save**를 선택하여 정책 정보를 저장합니다.

모듈 목록이 포함된 Health Policy Configuration 페이지가 나타납니다.

7단계 다음 절에서 설명한 대로, 어플라이언스의 상태를 테스트할 각 모듈에서 설정을 구성합니다.

- 68-10페이지의 Policy Run Time Interval 구성
- 68-11페이지의 AMP 모니터링 구성
- 68-12페이지의 Appliance Heartbeat 모니터링 구성
- 68-12페이지의 Automatic Application Bypass 모니터링 구성
- 68-13페이지의 CPU Usage 모니터링 구성
- 68-14페이지의 Card Reset 모니터링 구성
- 68-14페이지의 Disk Status 모니터링 구성
- 68-15페이지의 Disk Usage 모니터링 구성
- 68-16페이지의 Status MonitorFireAMP 구성
- 68-16페이지의 Host FireSIGHTUsage 모니터링 구성
- 68-17페이지의 Hardware Alarm 모니터링 구성
- 68-18페이지의 Health Status 모니터링 구성
- 68-19페이지의 Inline Link Mismatch Alarm 모니터링 구성
- 68-19페이지의 Interface Status 모니터링 구성
- 68-20페이지의 Intrusion Event Rate 모니터링 구성
- 68-21페이지의 License Monitoring 이해

- 68-21페이지의 Link State Propagation 모니터링 구성
- 68-22페이지의 Memory Usage 모니터링 구성
- 68-23페이지의 Power Supply 모니터링 구성
- 68-23페이지의 Process Status 모니터링 구성
- 68-24페이지의 Reconfiguring Detection 모니터링 구성
- 68-25페이지의 RRD Server Process 모니터링 구성
- 68-25페이지의 Security Intelligence 모니터링 구성
- 68-26페이지의 Time Series Data 모니터링 구성
- 68-27페이지의 Time Synchronization 모니터링 구성
- 68-27페이지의 URL Filtering 모니터링 구성
- 68-28페이지의 User Agent Status 모니터링 구성
- 68-29페이지의 VPN Status 모니터링 구성

참고 설정을 구성할 때 각 Health Policy Configuration 페이지에서 상태를 테스트하기 위해 실행할 각 모듈을 활성화해야 합니다. 모듈을 포함하는 정책이 어플라이언스에 적용되었더라도, 비활성화된 모듈은 상태 피드백을 생성하지 않습니다.

8단계 **Save Policy and Exit**를 클릭하여 정책을 저장합니다.

정책을 반영하려면 각 어플라이언스에 적용해야 합니다. 상태 정책 적용에 대한 자세한 내용은 68-29페이지의 상태 정책 적용을/를 참조하십시오.

Policy Run Time Interval 구성

라이센스: 모두

상태 정책에 대한 Policy Run Time Interval을 수정하여 상태 테스트의 실행 빈도를 제어할 수 있습니다. 설정 가능한 시간 최대 실행 시간 간격은 99999분입니다.

주의 실행 간격을 5분 미만으로는 설정하지 마십시오.

정책 실행 시간 간격을 구성하려면

액세스: Admin/Maint

1단계 Health Policy Configuration 페이지에서 **Policy Run Time Interval**을 선택합니다.

Health Policy Configuration — Policy Run Time Interval 페이지가 나타납니다.

2단계 테스트의 자동 반복 수행 간격(분 단위)을 **Run Interval (mins)** 필드에 입력합니다.

3단계 3가지 옵션이 제공됩니다.

- 이 모듈에 대한 변경 사항을 저장하고 Health Policy 페이지로 돌아가려면 **Save Policy and Exit**를 클릭합니다.
- 이 모듈에 대한 설정을 저장하지 않은 채 Health Policy 페이지로 돌아가려면 **Cancel**을 클릭합니다.

- 이 모듈에 대한 변경 사항을 임시로 저장하고 다른 수정할 모듈 설정으로 전환하려면 페이지의 왼쪽에 있는 목록에서 다른 모듈을 선택합니다. 수정을 마친 후 **Save Policy and Exit**를 클릭하면 변경한 모든 내용이 저장됩니다. **Cancel**을 클릭하면 모든 변경 사항이 취소됩니다.

설정이 반영되도록 하려면 해당 어플라이언스에 상태 정책을 적용해야 합니다. 자세한 내용은 68-29페이지의 상태 정책 적용을/를 참조하십시오.

AMP 모니터링 구성

라이센스: 악성코드

이 모듈은 Cisco 클라우드에 대해 쿼리하고 네트워크 트래픽에서 파일을 탐지하는 방어 센터 기능의 상태 및 안정성을 추적합니다. 클라우드와의 연결이 중단되었음을 시스템이 탐지하거나, 연결에 사용된 암호화 키가 잘못되었거나, 지정된 기간에 너무 많은 파일이 탐지되면 이 모듈에 대한 상태 분류가 Warning으로 변경되고 모듈이 상태 알림을 생성합니다. 사용 중인 FireAMP Private Cloud가 퍼블릭 Cisco 클라우드와 통신할 수 없으면 프라이빗 클라우드 자체가 알림을 생성합니다. 자세한 내용은 *FireAMP Private Cloud Administration Portal User Guide*를 참조하십시오.

참고 방어 센터가 인터넷 연결이 끊어지면 시스템에서 Advanced Malware Protection 상태 알림을 생성하는 데 최대 30분 정도 걸릴 수 있습니다.

Advanced Malware Protection 상태 모듈 설정을 구성하려면

액세스: Admin/Maint

1단계 Health Policy Configuration 페이지에서 Advanced Malware Protection을 선택합니다.

Health Policy Configuration — Advanced Malware Protection 페이지가 나타납니다.

2단계 상태를 테스트할 모듈의 사용을 활성화하려면 **Enabled** 옵션에 대해 **On**을 선택합니다.

3단계 3가지 옵션이 제공됩니다.

- 이 모듈에 대한 변경 사항을 저장하고 Health Policy 페이지로 돌아가려면 **Save Policy and Exit**를 클릭합니다.
- 이 모듈에 대한 설정을 저장하지 않은 채 Health Policy 페이지로 돌아가려면 **Cancel**을 클릭합니다.
- 이 모듈에 대한 변경 사항을 임시로 저장하고 다른 수정할 모듈 설정으로 전환하려면 페이지의 왼쪽에 있는 목록에서 다른 모듈을 선택합니다. 수정을 마친 후 **Save Policy and Exit**를 클릭하면 변경한 모든 내용이 저장됩니다. **Cancel**을 클릭하면 모든 변경 사항이 취소됩니다.

설정이 반영되도록 하려면 해당 어플라이언스에 상태 정책을 적용해야 합니다. 자세한 내용은 68-29페이지의 상태 정책 적용을/를 참조하십시오.

Appliance Heartbeat 모니터링 구성

라이센스: 모두

이는 디바이스가 실행 중이며 방어 센터와 제대로 통신 중임을 나타내는 지표로서 방어 센터는 2분마다 또는 200개의 이벤트마다(먼저 발생하는 것으로) 관리되는 디바이스에서 하트비트를 수신합니다. 방어 센터가 관리되는 어플라이언스에서 하트비트를 수신하는지 여부를 추적하려면 Appliance Heartbeat 상태 모듈을 사용하십시오. 방어 센터가 디바이스에서 하트비트를 탐지하지 못하면 이 모듈의 상태 분류가 Critical로 변경됩니다. 해당 상태 데이터가 상태 모니터로 공급됩니다.

Appliance Heartbeat 상태 모듈 설정을 구성하려면

액세스: Admin/Maint

1단계 Health Policy Configuration 페이지에서 **Appliance Heartbeat**를 선택합니다.

Health Policy Configuration — Appliance Heartbeat 페이지가 나타납니다.

2단계 상태를 테스트할 모듈의 사용을 활성화하려면 **Enabled** 옵션에 대해 **On**을 선택합니다.

3단계 3가지 옵션이 제공됩니다.

- 이 모듈에 대한 변경 사항을 저장하고 Health Policy 페이지로 돌아가려면 **Save Policy and Exit**를 클릭합니다.
- 이 모듈에 대한 설정을 저장하지 않은 채 Health Policy 페이지로 돌아가려면 **Cancel**을 클릭합니다.
- 이 모듈에 대한 변경 사항을 임시로 저장하고 다른 수정할 모듈 설정으로 전환하려면 페이지의 왼쪽에 있는 목록에서 다른 모듈을 선택합니다. 수정을 마친 후 **Save Policy and Exit**를 클릭하면 변경한 모든 내용이 저장됩니다. **Cancel**을 클릭하면 모든 변경 사항이 취소됩니다.

설정이 반영되도록 하려면 해당 어플라이언스에 상태 정책을 적용해야 합니다. 자세한 내용은 68-29페이지의 상태 정책 적용을/를 참조하십시오.

Automatic Application Bypass 모니터링 구성

라이센스: 모두

이 모듈을 사용하면 우회 임계값으로 구성된 기간(초 단위) 내에 응답하지 않아서 관리되는 디바이스가 우회되는 경우를 탐지할 수 있습니다. 우회가 발생하면 이 모듈은 알림을 생성합니다. 해당 상태 데이터가 상태 모니터로 공급됩니다.

자동 애플리케이션 우회에 대한 자세한 내용은 4-55페이지의 자동 애플리케이션 바이패스을/를 참조하십시오.

Automatic Application Bypass 모니터링 상태를 구성하려면

액세스: Admin/Maint

1단계 Health Policy Configuration 페이지에서 **Automatic Application Bypass Status**를 선택합니다.

Health Policy Configuration — Automatic Application Bypass Status 페이지가 나타납니다.

2단계 상태를 테스트할 모듈의 사용을 활성화하려면 **Enabled** 옵션에 대해 **On**을 선택합니다.

3단계 3가지 옵션이 제공됩니다.

- 이 모듈에 대한 변경 사항을 저장하고 Health Policy 페이지로 돌아가려면 **Save Policy and Exit**를 클릭합니다.

- 이 모듈에 대한 설정을 저장하지 않은 채 Health Policy 페이지로 돌아가려면 **Cancel**을 클릭합니다.
- 이 모듈에 대한 변경 사항을 임시로 저장하고 다른 수정할 모듈 설정으로 전환하려면 페이지의 왼쪽에 있는 목록에서 다른 모듈을 선택합니다. 수정을 마친 후 **Save Policy and Exit**를 클릭하면 변경한 모든 내용이 저장됩니다. **Cancel**을 클릭하면 모든 변경 사항이 취소됩니다.

설정이 반영되도록 하려면 해당 관리되는 디바이스에 상태 정책을 적용해야 합니다. 자세한 내용은 68-29페이지의 상태 정책 적용을/를 참조하십시오.

CPU Usage 모니터링 구성

라이센스: 모두

지원되는 디바이스: 3D9900을 제외한 모두

지원되는 Defense Center: 모두

CPU 사용량이 과도하면 하드웨어를 업그레이드해야 함을 나타내거나, 정확하게 작동하지 않는 프로세스가 있음을 나타낼 수 있습니다. CPU 사용량 제한을 설정하려면 CPU Usage 상태 모듈을 사용하십시오.

모니터링되는 어플라이언스의 CPU 사용량이 Warning 제한을 초과하면 해당 모듈에 대한 상태 분류가 Warning으로 변경됩니다. 모니터링되는 어플라이언스의 CPU 사용량이 Critical 제한을 초과하면 해당 모듈에 대한 상태 분류가 Critical로 변경됩니다. 해당 상태 데이터가 상태 모니터로 공급됩니다.

두 가지 제한 중 하나에 대해 설정할 수 있는 최대 비율은 100퍼센트이며, Critical 제한이 Warning 제한보다 높아야 합니다.

CPU Usage 제한을 구성하려면

액세스: Admin/Maint

1단계 Health Policy Configuration 페이지에서 **CPU Usage**를 선택합니다.

Health Policy Configuration — CPU Usage 페이지가 나타납니다.

2단계 상태를 테스트할 모듈의 사용을 활성화하려면 **Enabled** 옵션에 대해 **On**을 선택합니다.

3단계 Critical 상태를 트리거할 CPU 사용량의 비율을 **Critical Threshold %** 필드에 입력합니다.

4단계 Warning 상태를 트리거할 CPU 사용량의 비율을 **Warning Threshold %** 필드에 입력합니다.

5단계 3가지 옵션이 제공됩니다.

- 이 모듈에 대한 변경 사항을 저장하고 Health Policy 페이지로 돌아가려면 **Save Policy and Exit**를 클릭합니다.
- 이 모듈에 대한 설정을 저장하지 않은 채 Health Policy 페이지로 돌아가려면 **Cancel**을 클릭합니다.
- 이 모듈에 대한 변경 사항을 임시로 저장하고 다른 수정할 모듈 설정으로 전환하려면 페이지의 왼쪽에 있는 목록에서 다른 모듈을 선택합니다. 수정을 마친 후 **Save Policy and Exit**를 클릭하면 변경한 모든 내용이 저장됩니다. **Cancel**을 클릭하면 모든 변경 사항이 취소됩니다.

설정이 반영되도록 하려면 해당 어플라이언스에 상태 정책을 적용해야 합니다. 자세한 내용은 68-29페이지의 상태 정책 적용을/를 참조하십시오.

Card Reset 모니터링 구성

라이센스: 모두

Card Reset 모니터링 상태 모듈을 사용하면 하드웨어 장애 때문에 네트워크 카드가 다시 시작되는 경우를 추적할 수 있습니다. 재설정이 발생하면 이 모듈은 알림을 생성합니다. 해당 상태 데이터가 상태 모니터로 공급됩니다.

Card Reset 모니터링을 구성하려면

액세스: Admin/Maint

1단계 Health Policy Configuration 페이지에서 **Card Reset**을 선택합니다.

Health Policy Configuration — Card Reset Monitoring 페이지가 나타납니다.

2단계 상태를 테스트할 모듈의 사용을 활성화하려면 **Enabled** 옵션에 대해 **On**을 선택합니다.

3단계 3가지 옵션이 제공됩니다.

- 이 모듈에 대한 변경 사항을 저장하고 Health Policy 페이지로 돌아가려면 **Save Policy and Exit**를 클릭합니다.
- 이 모듈에 대한 설정을 저장하지 않은 채 Health Policy 페이지로 돌아가려면 **Cancel**을 클릭합니다.
- 이 모듈에 대한 변경 사항을 임시로 저장하고 다른 수정할 모듈 설정으로 전환하려면 페이지의 왼쪽에 있는 목록에서 다른 모듈을 선택합니다. 수정을 마친 후 **Save Policy and Exit**를 클릭하면 변경한 모든 내용이 저장됩니다. **Cancel**을 클릭하면 모든 변경 사항이 취소됩니다.

설정이 반영되도록 하려면 해당 방어 센터에 상태 정책을 적용해야 합니다. 자세한 내용은 68-29페이지의 상태 정책 적용을/를 참조하십시오.

Disk Status 모니터링 구성

라이센스: 모두

Disk Status 상태 모듈을 사용하면 어플라이언스 하드 디스크와 악성코드 스토리지 팩(설치된 경우)의 현재 상태를 모니터링할 수 있습니다. 이 모듈에서는 하드 디스크와 RAID 컨트롤러(설치된 경우)가 실패할 위험이 있을 때 또는 악성코드 스토리지 팩이 아닌 추가 하드 드라이브가 설치된 경우 Warning(노란색) 상태 알림을 생성합니다. 설치된 악성코드 스토리지 팩을 탐지할 수 없는 경우에는 Alert(빨간색) 상태 알림이 생성됩니다.

Disk Status 상태 모듈 설정을 구성하려면

액세스: Admin/Maint

1단계 Health Policy Configuration 페이지에서 **Disk Status**를 클릭합니다.

Health Policy Configuration — Disk Status 페이지가 나타납니다.

2단계 상태를 테스트할 모듈의 사용을 활성화하려면 **Enabled** 옵션에 대해 **On**을 선택합니다.

3단계 3가지 옵션이 제공됩니다.

- 이 모듈에 대한 변경 사항을 저장하고 Health Policy 페이지로 돌아가려면 **Save Policy and Exit**를 클릭합니다.
- 이 모듈에 대한 설정을 저장하지 않은 채 Health Policy 페이지로 돌아가려면 **Cancel**을 클릭합니다.

- 이 모듈에 대한 변경 사항을 임시로 저장하고 다른 수정할 모듈 설정으로 전환하려면 페이지의 왼쪽에 있는 목록에서 다른 모듈을 선택합니다. 수정을 마친 후 **Save Policy and Exit**를 클릭하면 변경한 모든 내용이 저장됩니다. **Cancel**을 클릭하면 모든 변경 사항이 취소됩니다.

설정이 반영되도록 하려면 해당 디바이스에 상태 정책을 적용해야 합니다. 자세한 내용은 68-29페이지의 상태 정책 적용을/를 참조하십시오.

Disk Usage 모니터링 구성

라이센스: 모두

디스크 공간이 충분하지 않으면 어플라이언스를 실행할 수 없습니다. 상태 모니터는 공간이 소진되기 전에 어플라이언스의 하드 드라이브 및 악성코드 스토리지 팩에서 디스크 공간 부족 상태를 식별할 수 있습니다. 이 상태 모니터는 하드 드라이브 파일 유출이 너무 자주 발생하는 경우에도 알림을 전송할 수 있습니다. Disk Usage 상태 모듈을 사용하면 어플라이언스에서 / 및 /volume 파티션의 디스크 사용량을 모니터링하고 유출 빈도를 추적할 수 있습니다.

참고 Disk Usage 모듈은 /boot 파티션을 모니터링되는 파티션으로 나열하지만, 파티션의 크기는 정적이어서 모듈이 부트 파티션에 대해 알림을 전송하지 않습니다.

모니터링되는 어플라이언스의 디스크 사용량이 Warning 제한을 초과하면 해당 모듈에 대한 상태 분류가 Warning으로 변경됩니다. 모니터링되는 어플라이언스의 디스크 사용량이 Critical 제한을 초과하면 해당 모듈에 대한 상태 분류가 Critical로 변경됩니다. 두 가지 제한 중 하나에 대해 설정할 수 있는 최대 비율은 100퍼센트이며, Critical 제한이 Warning 제한보다 높아야 합니다.

시스템이 처리되지 않은 이벤트를 삭제하면 해당 모듈에 대한 상태 분류가 Warning으로 변경됩니다. 시스템이 모듈 임계값을 기반으로 디스크 사용량 카테고리에서 파일을 너무 자주 유출하는 경우 또는 모니터링되는 디스크 사용량 카테고리에 없는 파일의 디스크 사용량이 모듈 임계값을 기반으로 너무 커지는 경우 해당 모듈에 대한 상태 분류가 Critical로 변경됩니다. 디스크 사용량 카테고리에 대한 자세한 내용은 55-26페이지의 Disk Usage 위젯 이해을/를 참조하십시오.

Disk Usage 상태 모듈 설정을 구성하려면

액세스: Admin/Maint

1단계 Health Policy Configuration 페이지에서 **Disk Usage**를 선택합니다.

Health Policy Configuration — Disk Usage 페이지가 나타납니다.

2단계 상태를 테스트할 모듈의 사용을 활성화하려면 **Enabled** 옵션에 대해 **On**을 선택합니다.

3단계 Critical 상태를 트리거할 디스크 사용량의 비율을 **Critical Threshold %** 필드에 입력합니다.

4단계 Warning 상태를 트리거할 디스크 사용량의 비율을 **Warning Threshold %** 필드에 입력합니다.

5단계 3가지 옵션이 제공됩니다.

- 이 모듈에 대한 변경 사항을 저장하고 Health Policy 페이지로 돌아가려면 **Save Policy and Exit**를 클릭합니다.
- 이 모듈에 대한 설정을 저장하지 않은 채 Health Policy 페이지로 돌아가려면 **Cancel**을 클릭합니다.
- 이 모듈에 대한 변경 사항을 임시로 저장하고 다른 수정할 모듈 설정으로 전환하려면 페이지의 왼쪽에 있는 목록에서 다른 모듈을 선택합니다. 수정을 마친 후 **Save Policy and Exit**를 클릭하면 변경한 모든 내용이 저장됩니다. **Cancel**을 클릭하면 모든 변경 사항이 취소됩니다.

설정이 반영되도록 하려면 해당 어플라이언스에 상태 정책을 적용해야 합니다. 자세한 내용은 68-29페이지의 상태 정책 적용을/를 참조하십시오.

Status MonitorFireAMP 구성

라이센스: 모두

FireAMP Status Monitor 모듈을 사용하면 다음과 같은 상황에서 알림을 전송할 수 있습니다.

- 초기의 성공적인 연결 이후 방어 센터가 Cisco 클라우드에 연결할 수 없는 경우
- FireAMP 포털을 사용하여 클라우드 연결을 등록 취소하는 경우
- FireAMP Private Cloud가 퍼블릭 Cisco 클라우드와 통신할 수 없는 경우

이러한 경우 모듈 상태는 Critical로 변경되고 실패한 연결과 관련된 클라우드 이름이 제공됩니다. 클라우드 연결을 구성하는 방법에 대한 자세한 내용은 37-24페이지의 FireAMP를 위한 클라우드 연결 작업을/를 참조하십시오.

FireAMP Status Monitor 모듈 설정을 구성하려면

액세스: Admin/Maint

1단계 Health Policy Configuration 페이지에서 **FireAMP Status Monitor**를 선택합니다.

Health Policy Configuration — FireAMP Status Monitor 페이지가 나타납니다.

2단계 FireAMP 상태를 모니터링할 모듈의 사용을 활성화하려면 **Enabled** 옵션에 대해 **On**을 선택합니다.

3단계 3가지 옵션이 제공됩니다.

- 이 모듈에 대한 변경 사항을 저장하고 Health Policy 페이지로 돌아가려면 **Save Policy and Exit**를 클릭합니다.
- 이 모듈에 대한 설정을 저장하지 않은 채 Health Policy 페이지로 돌아가려면 **Cancel**을 클릭합니다.
- 이 모듈에 대한 변경 사항을 임시로 저장하고 다른 수정할 모듈 설정으로 전환하려면 페이지의 왼쪽에 있는 목록에서 다른 모듈을 선택합니다. 수정을 마친 후 **Save Policy and Exit**를 클릭하면 변경한 모든 내용이 저장됩니다. **Cancel**을 클릭하면 모든 변경 사항이 취소됩니다.

설정이 반영되도록 하려면 방어 센터에 상태 정책을 적용해야 합니다. 자세한 내용은 68-29페이지의 상태 정책 적용을/를 참조하십시오.

Host FireSIGHTUsage 모니터링 구성

라이센스: FireSIGHT

FireSIGHT Host License Limit 상태 모듈을 사용하면 FireSIGHT Host Amount 경고 제한을 설정할 수 있습니다. 모니터링되는 디바이스에 남아 있는 FireSIGHT Host 수가 Warning Hosts 제한 아래로 떨어지면 해당 모듈에 대한 상태 분류가 Warning으로 변경됩니다. 모니터링되는 디바이스에 남아 있는 FireSIGHT Host 수가 Critical Hosts 제한 아래로 떨어지면 해당 모듈에 대한 상태 분류가 Critical로 변경됩니다. 해당 상태 데이터가 상태 모니터로 공급됩니다.

두 가지 제한 중 하나에 대해 설정할 수 있는 최대 호스트 수는 1000이며, Critical 호스트 제한 수가 Warning 제한보다 커야 합니다.

FireSIGHT Host License Limit 상태 모듈 설정을 구성하려면

액세스: Admin/Maint

1단계 Health Policy Configuration 페이지에서 **FireSIGHT Host License Limit**를 선택합니다.

Health Policy Configuration — FireSIGHT Host License Limit 페이지가 나타납니다.

2단계 상태를 테스트할 모듈의 사용을 활성화하려면 **Enabled** 옵션에 대해 **On**을 선택합니다.

3단계 Critical 상태를 트리거할 사용 가능한 호스트의 남은 수를 **Critical number Hosts** 필드에 입력합니다.

4단계 Warning 상태를 트리거할 사용 가능한 호스트의 남은 수를 **Warning number Hosts** 필드에 입력합니다.

5단계 3가지 옵션이 제공됩니다.

- 이 모듈에 대한 변경 사항을 저장하고 Health Policy 페이지로 돌아가려면 **Save Policy and Exit**를 클릭합니다.
- 이 모듈에 대한 설정을 저장하지 않은 채 Health Policy 페이지로 돌아가려면 **Cancel**을 클릭합니다.
- 이 모듈에 대한 변경 사항을 임시로 저장하고 다른 수정할 모듈 설정으로 전환하려면 페이지의 왼쪽에 있는 목록에서 다른 모듈을 선택합니다. 수정을 마친 후 **Save Policy and Exit**를 클릭하면 변경한 모든 내용이 저장됩니다. **Cancel**을 클릭하면 모든 변경 사항이 취소됩니다.

설정이 반영되도록 하려면 해당 디바이스에 상태 정책을 적용해야 합니다. 자세한 내용은 68-29페이지의 상태 정책 적용을/를 참조하십시오.

Hardware Alarm 모니터링 구성

라이센스: 모두

지원되는 디바이스: Series 3, 3D9900

Hardware Alarms 상태 모듈을 사용하면 Series 3 또는 3D9900 디바이스에서 하드웨어 장애를 탐지할 수 있습니다. Hardware Alarms 모듈이 장애를 일으킨 하드웨어 구성 요소 또는 상호 통신하지 않는 클러스터링된 디바이스를 탐지하면 해당 모듈에 대한 상태 분류가 Critical로 변경됩니다. 해당 상태 데이터가 상태 모니터로 공급됩니다.

3D9900 디바이스에서 하드웨어 알림을 일으킬 수 있는 하드웨어 상태 조건에 대한 자세한 내용은 68-51페이지의 3D9900 디바이스에 대한 하드웨어 알림 세부사항 해석을/를 참조하십시오.

Hardware Alarm 상태 모듈 설정을 구성하려면

액세스: Admin/Maint

1단계 Health Policy Configuration 페이지에서 **Hardware Alarms**를 선택합니다.

Health Policy Configuration — Hardware Alarm Monitor 페이지가 나타납니다.

2단계 상태를 테스트할 모듈의 사용을 활성화하려면 **Enabled** 옵션에 대해 **On**을 선택합니다.

3단계 3가지 옵션이 제공됩니다.

- 이 모듈에 대한 변경 사항을 저장하고 Health Policy 페이지로 돌아가려면 **Save Policy and Exit**를 클릭합니다.
- 이 모듈에 대한 설정을 저장하지 않은 채 Health Policy 페이지로 돌아가려면 **Cancel**을 클릭합니다.
- 이 모듈에 대한 변경 사항을 임시로 저장하고 다른 수정할 모듈 설정으로 전환하려면 페이지의 왼쪽에 있는 목록에서 다른 모듈을 선택합니다. 수정을 마친 후 **Save Policy and Exit**를 클릭하면 변경한 모든 내용이 저장됩니다. **Cancel**을 클릭하면 모든 변경 사항이 취소됩니다.

설정이 반영되도록 하려면 해당 디바이스에 상태 정책을 적용해야 합니다. 자세한 내용은 68-29페이지의 상태 정책 적용을/를 참조하십시오.

Health Status 모니터링 구성

라이센스: 모두

Health Monitor Process 모듈을 사용하면 모니터링되는 어플라이언스에서 수신하는 상태 이벤트 간 경과 시간이 너무 길 때 알림을 생성하여 방어 센터에서 상태 모니터의 상태를 모니터링할 수 있습니다.

예를 들어 방어 센터(`myrtle.example.com`)에서 디바이스(`dogwood.example.com`)을 모니터링하는 경우 Health Monitor Process 모듈이 활성화된 상태 정책을 `myrtle.example.com`에 적용할 수 있습니다. 그러면 Health Monitor Process 모듈은 `dogwood.example.com`에서 마지막 이벤트를 수신한 후 경과한 시간을 나타내는 이벤트를 보고합니다.

알림을 생성할 이벤트 간 경과 기간을 분 단위로 구성할 수 있습니다. 대기 시간이 마지막 이벤트 제한 이후 Warning Minutes에 구성된 시간(분)을 초과하면 해당 모듈에 대한 상태 분류가 Warning으로 변경됩니다. 대기 시간이 마지막 이벤트 제한 이후 Critical Minutes를 초과하면 해당 모듈에 대한 상태 분류가 Critical로 변경됩니다. 해당 상태 데이터가 상태 모니터로 공급됩니다.

두 가지 제한 중 하나에 대해 설정할 수 있는 최대 시간은 144분이며, Critical 제한이 Warning 제한보다 높아야 합니다. 최소 시간은 5분입니다.

Health Monitor Process 모듈 설정을 구성하려면

액세스: Admin/Maint

1단계 Health Policy Configuration 페이지에서 **Health Monitor Process**를 선택합니다.

Health Policy Configuration — Health Monitor Process 페이지가 나타납니다.

2단계 상태를 테스트할 모듈의 사용을 활성화하려면 **Enabled** 옵션에 대해 **On**을 선택합니다.

3단계 Critical 상태를 트리거하기까지 이벤트 간 최대 대기 시간(분 단위)을 **Critical Minutes since last event** 필드에 입력합니다.

4단계 Warning 상태를 트리거하기까지 이벤트 간 최대 대기 시간(분 단위)을 **Warning Minutes since last event** 필드에 입력합니다.

5단계 3가지 옵션이 제공됩니다.

- 이 모듈에 대한 변경 사항을 저장하고 Health Policy 페이지로 돌아가려면 **Save Policy and Exit**를 클릭합니다.
- 이 모듈에 대한 설정을 저장하지 않은 채 Health Policy 페이지로 돌아가려면 **Cancel**을 클릭합니다.
- 이 모듈에 대한 변경 사항을 임시로 저장하고 다른 수정할 모듈 설정으로 전환하려면 페이지의 왼쪽에 있는 목록에서 다른 모듈을 선택합니다. 수정을 마친 후 **Save Policy and Exit**를 클릭하면 변경한 모든 내용이 저장됩니다. **Cancel**을 클릭하면 모든 변경 사항이 취소됩니다.

설정이 반영되도록 하려면 방어 센터에 상태 정책을 적용해야 합니다. 자세한 내용은 68-29페이지의 상태 정책 적용을/를 참조하십시오.

Inline Link Mismatch Alarm 모니터링 구성

라이센스: 모두

Inline Link Mismatch Alarm 상태 모듈을 사용하면 인라인 집합의 어느 한쪽에 있는 인터페이스가 서로 다른 연결 속도를 협상하는 경우를 추적할 수 있습니다. 서로 다른 협상된 속도가 탐지되면 알림이 생성됩니다.

Inline Link Mismatch 모니터링을 구성하려면

액세스: Admin/Maint

1단계 Health Policy Configuration 페이지에서 **Inline Link Mismatch Alarms**를 선택합니다.

Health Policy Configuration — Inline Link Mismatch Alarms 페이지가 나타납니다.

2단계 상태를 테스트할 모듈의 사용을 활성화하려면 **Enabled** 옵션에 대해 **On**을 선택합니다.

3단계 3가지 옵션이 제공됩니다.

- 이 모듈에 대한 변경 사항을 저장하고 Health Policy 페이지로 돌아가려면 **Save Policy and Exit**를 클릭합니다.
- 이 모듈에 대한 설정을 저장하지 않은 채 Health Policy 페이지로 돌아가려면 **Cancel**을 클릭합니다.
- 이 모듈에 대한 변경 사항을 임시로 저장하고 다른 수정할 모듈 설정으로 전환하려면 페이지의 왼쪽에 있는 목록에서 다른 모듈을 선택합니다. 수정을 마친 후 **Save Policy and Exit**를 클릭하면 변경한 모든 내용이 저장됩니다. **Cancel**을 클릭하면 모든 변경 사항이 취소됩니다.

설정이 반영되도록 하려면 해당 방어 센터에 상태 정책을 적용해야 합니다. 자세한 내용은 68-29페이지의 상태 정책 적용을/를 참조하십시오.

Interface Status 모니터링 구성

라이센스: FireSIGHT

Interface Status 상태 모듈을 사용하면 디바이스가 트래픽을 수신하는지 여부를 탐지할 수 있습니다. 디바이스가 트래픽을 수신하지 않는 것으로 Interface Status 모듈이 확인하면, 해당 모듈에 대한 상태 분류가 Critical로 변경됩니다. 해당 상태 데이터가 상태 모니터로 공급됩니다.

참고 `DataPlaneInterfacex`라는 레이블의 인터페이스(여기서 `x`는 숫자 값)는 내부 ASA 인터페이스이며 (사용자 정의가 아님) 시스템 내 패킷 플로우에 관여합니다.

Interface Status 상태 모듈 설정을 구성하려면

액세스: Admin/Maint

1단계 Health Policy Configuration 페이지에서 **Interface Status**를 선택합니다.

Health Policy Configuration — Interface Status 페이지가 나타납니다.

2단계 상태를 테스트할 모듈의 사용을 활성화하려면 **Enabled** 옵션에 대해 **On**을 선택합니다.

3단계 3가지 옵션이 제공됩니다.

- 이 모듈에 대한 변경 사항을 저장하고 Health Policy 페이지로 돌아가려면 **Save Policy and Exit**를 클릭합니다.

- 이 모듈에 대한 설정을 저장하지 않은 채 Health Policy 페이지로 돌아가려면 **Cancel**을 클릭합니다.
- 이 모듈에 대한 변경 사항을 임시로 저장하고 다른 수정할 모듈 설정으로 전환하려면 페이지의 왼쪽에 있는 목록에서 다른 모듈을 선택합니다. 수정을 마친 후 **Save Policy and Exit**를 클릭하면 변경한 모든 내용이 저장됩니다. **Cancel**을 클릭하면 모든 변경 사항이 취소됩니다.

설정이 반영되도록 하려면 해당 디바이스에 상태 정책을 적용해야 합니다. 자세한 내용은 68-29페이지의 상태 정책 적용을/를 참조하십시오.

Intrusion Event Rate 모니터링 구성

라이센스: 보호

Intrusion Event Rate 상태 모듈을 사용하면 상태의 변경을 트리거하는 초당 패킷 수에 대한 제한을 설정할 수 있습니다. 모니터링되는 디바이스의 이벤트 속도가 Events per second (Warning) 제한에 구성된 초당 이벤트 수를 초과하면 해당 모듈에 대한 상태 분류가 Warning으로 변경됩니다. 이벤트 속도가 Events per second (Critical) 제한에 구성된 초당 이벤트 수를 초과하면 해당 모듈에 대한 상태 분류가 Critical로 변경됩니다. 해당 상태 데이터가 상태 모니터로 공급됩니다.

일반적으로 네트워크 세그먼트의 이벤트 속도는 초당 이벤트 20개입니다. 이 평균 속도의 네트워크 세그먼트에서 Events per second (Critical)는 50, Events per second (Warning)는 30으로 설정해야 합니다. 시스템에 대한 제한을 결정하려면 디바이스의 Statistics 페이지(**System > Monitoring > Statistics**)에서 Events/Sec 값을 찾고 다음 공식을 사용하여 제한을 계산합니다.

- Events per second (Critical) = Events/Sec * 2.5
- Events per second (Warning) = Events/Sec * 1.5

두 가지 제한 중 하나에 대해 설정할 수 있는 최대 이벤트 수는 999이며, Critical 제한이 Warning 제한보다 높아야 합니다.

Intrusion Event Rate Monitor 상태 모듈 설정을 구성하려면

액세스: Admin/Maint

1단계 Health Policy Configuration 페이지에서 **Intrusion Event Rate**를 선택합니다.

Health Policy Configuration — Intrusion Event Rate 페이지가 나타납니다.

2단계 상태를 테스트할 모듈의 사용을 활성화하려면 **Enabled** 옵션에 대해 **On**을 선택합니다.

3단계 Critical 상태를 트리거할 초당 이벤트 수를 **Events per second (Critical)** 필드에 입력합니다.

4단계 Warning 상태를 트리거할 초당 이벤트 수를 **Events per second (Warning)** 필드에 입력합니다.

5단계 3가지 옵션이 제공됩니다.

- 이 모듈에 대한 변경 사항을 저장하고 Health Policy 페이지로 돌아가려면 **Save Policy and Exit**를 클릭합니다.
- 이 모듈에 대한 설정을 저장하지 않은 채 Health Policy 페이지로 돌아가려면 **Cancel**을 클릭합니다.
- 이 모듈에 대한 변경 사항을 임시로 저장하고 다른 수정할 모듈 설정으로 전환하려면 페이지의 왼쪽에 있는 목록에서 다른 모듈을 선택합니다. 수정을 마친 후 **Save Policy and Exit**를 클릭하면 변경한 모든 내용이 저장됩니다. **Cancel**을 클릭하면 모든 변경 사항이 취소됩니다.

설정이 반영되도록 하려면 해당 디바이스에 상태 정책을 적용해야 합니다. 자세한 내용은 68-29페이지의 상태 정책 적용을/를 참조하십시오.

License Monitoring 이해

라이센스: 모두

License Monitoring 상태 모듈을 사용하면 제어, 보호, URL 필터링, 악성코드 및 VPN에 대한 라이센스가 충분히 남아 있는지 확인할 수 있습니다. 남아 있는 라이센스 수가 적거나 부족하면 알림이 전송됩니다.

스태킹된 컨피그레이션의 디바이스에서 라이센스 세트가 일치하지 않음을 시스템에서 탐지하는 경우에도 알림이 전송됩니다(스태킹된 디바이스의 라이센스 세트가 동일해야 함).

License Monitoring 모듈은 자동으로 구성됩니다. 이 모듈은 변경하거나 비활성화할 수 없으므로 Health Policy Configuration 페이지에 나타나지 않습니다.

Link State Propagation 모니터링 구성

라이센스: 모두

Link State Propagation 상태 모듈을 사용하면 인라인 쌍에서 링크 상태 전파 상태를 탐지할 수 있습니다. 링크 상태가 쌍으로 전파되면 해당 모듈에 대한 상태 분류가 Critical로 변경되고 다음과 같은 메시지가 나타납니다.

```
Module Link State Propagation: ethx_ethy is Triggered
```

여기서 *x*와 *y*는 쌍을 이룬 인터페이스 번호입니다.

Link State Propagation 상태 모듈 설정을 구성하려면

액세스: Admin/Maint

1단계 Health Policy Configuration 페이지에서 **Link State Propagation**을 선택합니다.

Health Policy Configuration — Link State Propagation monitor 페이지가 나타납니다.

2단계 상태를 테스트할 모듈의 사용을 활성화하려면 **Enabled** 옵션에 대해 **On**을 선택합니다.

3단계 3가지 옵션이 제공됩니다.

- 이 모듈에 대한 변경 사항을 저장하고 Health Policy 페이지로 돌아가려면 **Save Policy and Exit**를 클릭합니다.
- 이 모듈에 대한 설정을 저장하지 않은 채 Health Policy 페이지로 돌아가려면 **Cancel**을 클릭합니다.
- 이 모듈에 대한 변경 사항을 임시로 저장하고 다른 수정할 모듈 설정으로 전환하려면 페이지의 왼쪽에 있는 목록에서 다른 모듈을 선택합니다. 수정을 마친 후 **Save Policy and Exit**를 클릭하면 변경한 모든 내용이 저장됩니다. **Cancel**을 클릭하면 모든 변경 사항이 취소됩니다.

설정이 반영되도록 하려면 해당 디바이스에 상태 정책을 적용해야 합니다. 자세한 내용은 68-29페이지의 상태 정책 적용을/를 참조하십시오.

Memory Usage 모니터링 구성

라이센스: 모두

Memory Usage 상태 모듈을 사용하면 메모리 사용량 제한을 설정할 수 있습니다. 이 모듈은 여유 메모리, 캐시된 메모리 및 스왑 메모리를 고려하여 여유 메모리를 계산합니다. 모니터링되는 어플라이언스의 메모리 사용량이 Warning 제한을 초과하면 해당 모듈에 대한 상태 분류가 Warning으로 변경됩니다. 모니터링되는 어플라이언스의 메모리 사용량이 Critical 제한을 초과하면 해당 모듈에 대한 상태 분류가 Critical로 변경됩니다. 해당 상태 데이터가 상태 모니터로 공급됩니다.

메모리가 4GB를 넘는 어플라이언스의 경우 프리셋 알림 임계값은 시스템 문제를 일으킬 수 있는 사용 가능한 메모리의 비율을 고려하는 공식을 기반으로 합니다.

참고 4GB를 넘는 어플라이언스에서는 Warning 임계값과 Critical 임계값 사이의 간격이 매우 좁기 때문에 Cisco에서는 **Warning Threshold %** 값을 50으로 직접 설정할 것을 권장합니다. 이렇게 하면 문제를 해결할 수 있도록 적시에 어플라이언스에 대한 메모리 알림을 받을 수 있습니다.

두 가지 제한 중 하나에 대해 설정할 수 있는 최대 비율은 100퍼센트이며, Critical 제한이 Warning 제한보다 높아야 합니다.

참고 많은 FireSIGHT 기능(예: 보안 인텔리전스, 파일 캡처, 많은 규칙의 침입 정책 또는 URL 필터링)이 있는 액세스 제어 정책을 적용하는 경우 일부 로우엔드 ASA FirePOWER 디바이스는 간헐적인 메모리 사용량 경고를 생성할 수 있습니다. 이는 디바이스의 메모리 할당이 가능한 최대 범위까지 사용되고 있기 때문입니다.

Memory Usage 상태 모듈 설정을 구성하려면

액세스: Admin/Maint

1단계 Health Policy Configuration 페이지에서 **Memory Usage**를 선택합니다.

Health Policy Configuration — Memory Usage 페이지가 나타납니다.

2단계 상태를 테스트할 모듈의 사용을 활성화하려면 **Enabled** 옵션에 대해 **On**을 선택합니다.

3단계 Critical 상태를 트리거할 메모리 사용량의 비율을 **Critical Threshold %** 필드에 입력합니다.

4단계 Warning 상태를 트리거할 메모리 사용량의 비율을 **Warning Threshold %** 필드에 입력합니다.

5단계 3가지 옵션이 제공됩니다.

- 이 모듈에 대한 변경 사항을 저장하고 Health Policy 페이지로 돌아가려면 **Save Policy and Exit**를 클릭합니다.
- 이 모듈에 대한 설정을 저장하지 않은 채 Health Policy 페이지로 돌아가려면 **Cancel**을 클릭합니다.
- 이 모듈에 대한 변경 사항을 임시로 저장하고 다른 수정할 모듈 설정으로 전환하려면 페이지의 왼쪽에 있는 목록에서 다른 모듈을 선택합니다. 수정을 마친 후 **Save Policy and Exit**를 클릭하면 변경한 모든 내용이 저장됩니다. **Cancel**을 클릭하면 모든 변경 사항이 취소됩니다.

설정이 반영되도록 하려면 해당 어플라이언스에 상태 정책을 적용해야 합니다. 자세한 내용은 68-29페이지의 상태 정책 적용을/를 참조하십시오.

Power Supply 모니터링 구성

라이센스: 모두

지원되는 디바이스: 3D3500, 3D4500, 3D6500, 3D9900, Series 3

지원되는 Defense Center: DC1500, DC2000, DC3500, DC4000

Power Supply 상태 모듈을 사용하면 지원되는 플랫폼에서 전력 공급 장치 실패를 탐지할 수 있습니다. 전력이 없는 전력 공급 장치가 발견되면 해당 모듈의 상태 분류가 No Power로 변경됩니다. 전력 공급 장치가 탐지되지 않으면 상태가 Critical Error로 변경됩니다. 해당 상태 데이터가 상태 모니터로 공급됩니다. 각 전력 공급 장치에 대한 특정 상태 항목을 보려면 상태 모니터의 Alert Detail에서 Power Supply 항목을 확장할 수 있습니다.

Power Supply 상태 모듈 설정을 구성하려면

액세스: Admin/Maint

1단계 Health Policy Configuration 페이지에서 **Power Supply**를 선택합니다.

Health Policy Configuration — Power Supply 페이지가 나타납니다.

2단계 상태를 테스트할 모듈의 사용을 활성화하려면 **Enabled** 옵션에 대해 **On**을 선택합니다.

3단계 3가지 옵션이 제공됩니다.

- 이 모듈에 대한 변경 사항을 저장하고 Health Policy 페이지로 돌아가려면 **Save Policy and Exit**를 클릭합니다.
- 이 모듈에 대한 설정을 저장하지 않은 채 Health Policy 페이지로 돌아가려면 **Cancel**을 클릭합니다.
- 이 모듈에 대한 변경 사항을 임시로 저장하고 다른 수정할 모듈 설정으로 전환하려면 페이지의 왼쪽에 있는 목록에서 다른 모듈을 선택합니다. 수정을 마친 후 **Save Policy and Exit**를 클릭하면 변경한 모든 내용이 저장됩니다. **Cancel**을 클릭하면 모든 변경 사항이 취소됩니다.

설정이 반영되도록 하려면 해당 디바이스에 상태 정책을 적용해야 합니다. 자세한 내용은 68-29페이지의 상태 정책 적용을/를 참조하십시오.

Process Status 모니터링 구성

라이센스: 모두

Process Status 상태 모듈을 사용하면 프로세스 관리자 외부에서 종료되는, 어플라이언스에서 실행 중인 프로세스를 모니터링할 수 있습니다. 프로세스 종료에 대한 Process Status 모듈의 응답은 프로세스 종료 방법에 따라 다릅니다.

- 프로세스가 프로세스 관리자 내부에서 종료되면 모듈은 상태 이벤트를 보고하지 않습니다.
- 프로세스가 프로세스 관리자 외부에서 고의로 종료되면 모듈 상태가 Warning으로 변경되며, 모듈이 다시 실행되고 프로세스가 다시 시작될 때까지 상태 이벤트 메시지에 프로세스가 종료되었음이 표시됩니다.
- 프로세스가 프로세스 관리자 외부에서 비정상적으로 종료되거나 충돌되면 모듈 상태가 Critical로 변경되며, 모듈이 다시 실행되고 프로세스가 다시 시작될 때까지 상태 이벤트 메시지에 프로세스가 종료되었음이 표시됩니다.

Process Status 상태 모듈 설정을 구성하려면

액세스: Admin/Maint

1단계 Health Policy Configuration 페이지에서 **Process Status**를 선택합니다.

Health Policy Configuration — Process Status 페이지가 나타납니다.

2단계 상태를 테스트할 모듈의 사용을 활성화하려면 **Enabled** 옵션에 대해 **On**을 선택합니다.

3단계 3가지 옵션이 제공됩니다.

- 이 모듈에 대한 변경 사항을 저장하고 Health Policy 페이지로 돌아가려면 **Save Policy and Exit**를 클릭합니다.
- 이 모듈에 대한 설정을 저장하지 않은 채 Health Policy 페이지로 돌아가려면 **Cancel**을 클릭합니다.
- 이 모듈에 대한 변경 사항을 임시로 저장하고 다른 수정할 모듈 설정으로 전환하려면 페이지의 왼쪽에 있는 목록에서 다른 모듈을 선택합니다. 수정을 마친 후 **Save Policy and Exit**를 클릭하면 변경한 모든 내용이 저장됩니다. **Cancel**을 클릭하면 모든 변경 사항이 취소됩니다.

설정이 반영되도록 하려면 해당 어플라이언스에 상태 정책을 적용해야 합니다. 자세한 내용은 68-29페이지의 상태 정책 적용을/를 참조하십시오.

Reconfiguring Detection 모니터링 구성

라이센스: 모두

Reconfiguring Detection Monitor 모듈을 사용하면 관리되는 디바이스에 정책을 적용한 후 탐지 기능의 상태를 확인할 수 있습니다. 정책 적용이 실패하고 탐지 기능이 중단되면 Health Events에서 알림이 생성됩니다.

시계열 데이터 모니터링 설정을 구성하려면

액세스: Admin/Maint

1단계 Health Policy Configuration 페이지에서 **Reconfiguring Detection**을 선택합니다.

Health Policy Configuration — Reconfiguring Detection 페이지가 나타납니다.

2단계 상태 알림을 제공할 모듈의 사용을 활성화하려면 **Enabled** 옵션에 대해 **On**을 선택합니다.

3단계 3가지 옵션이 제공됩니다.

- 이 모듈에 대한 변경 사항을 저장하고 Health Policy 페이지로 돌아가려면 **Save Policy and Exit**를 클릭합니다.
- 이 모듈에 대한 설정을 저장하지 않은 채 Health Policy 페이지로 돌아가려면 **Cancel**을 클릭합니다.
- 이 모듈에 대한 변경 사항을 임시로 저장하고 다른 수정할 모듈 설정으로 전환하려면 페이지의 왼쪽에 있는 목록에서 다른 모듈을 선택합니다. 수정을 마친 후 **Save Policy and Exit**를 클릭하면 변경한 모든 내용이 저장됩니다. **Cancel**을 클릭하면 모든 변경 사항이 취소됩니다.

설정이 반영되도록 하려면 해당 디바이스에 상태 정책을 적용해야 합니다. 자세한 내용은 68-29페이지의 상태 정책 적용을/를 참조하십시오.

RRD Server Process 모니터링 구성

라이센스: 모두

RRD Server Process 모듈을 사용하면 시계열 데이터를 저장하는 RRD 서버가 제대로 작동하는지 알 수 있습니다. 마지막으로 업데이트된 이후 RRD 서버가 다시 시작되면 알림이 전송됩니다. RRD 서버 다시 시작의 연속 업데이트 수가 모듈 컨피그레이션에 지정된 수에 도달하면 Critical 또는 Warning 상태로 들어가게 됩니다.

RRD Server Process 모니터링 설정을 구성하려면

액세스: Admin/Maint

1단계 Health Policy Configuration 페이지에서 **RRD Server Process**를 선택합니다.

Health Policy Configuration — RRD Server Process 페이지가 나타납니다.

2단계 상태를 테스트할 모듈의 사용을 활성화하려면 **Enabled** 옵션에 대해 **On**을 선택합니다.

3단계 Critical 상태를 트리거할, 연속적으로 탐지된 RRD 서버 재설정의 수를 **Critical Number of restarts** 필드에 입력합니다.

4단계 Warning 상태를 트리거할, 연속적으로 탐지된 RRD 서버 재설정의 수를 **Warning Number of restarts** 필드에 입력합니다.

5단계 3가지 옵션이 제공됩니다.

- 이 모듈에 대한 변경 사항을 저장하고 Health Policy 페이지로 돌아가려면 **Save Policy and Exit**를 클릭합니다.
- 이 모듈에 대한 설정을 저장하지 않은 채 Health Policy 페이지로 돌아가려면 **Cancel**을 클릭합니다.
- 이 모듈에 대한 변경 사항을 임시로 저장하고 다른 수정할 모듈 설정으로 전환하려면 페이지의 왼쪽에 있는 목록에서 다른 모듈을 선택합니다. 수정을 마친 후 **Save Policy and Exit**를 클릭하면 변경한 모든 내용이 저장됩니다. **Cancel**을 클릭하면 모든 변경 사항이 취소됩니다.

설정이 반영되도록 하려면 해당 디바이스에 상태 정책을 적용해야 합니다. 자세한 내용은 68-29페이지의 상태 정책 적용을/를 참조하십시오.

Security Intelligence 모니터링 구성

라이센스: 보호

지원되는 Defense Center: DC500을 제외한 모든 방어 센터

Security Intelligence 모듈을 사용하면 보안 인텔리전스 필터링과 관련된 다양한 상황에서 알림을 받을 수 있습니다. 보안 인텔리전스를 사용 중일 때 다음과 같은 경우에 알림이 전송됩니다.

- 방어 센터에서 피드를 업데이트할 수 없는 경우, 또는 피드 데이터가 손상되었거나 인식할 수 없는 IP 주소를 포함하는 경우
- 관리되는 디바이스가 방어 센터에서 업데이트된 보안 인텔리전스 데이터를 수신하는 데 문제가 있는 경우
- 메모리 문제 때문에 관리되는 디바이스가 방어 센터에서 제공되는 보안 인텔리전스 데이터의 일부를 로드할 수 없는 경우

팁 상태 모니터에 보안 인텔리전스 메모리 경고가 나타나는 경우, 보안 인텔리전스에 할당되는 메모리를 늘리려면 영향받는 디바이스의 액세스 제어 정책을 다시 적용할 수 있습니다. 12-15페이지의 액세스 제어 정책 적용을/를 참조하십시오.

보안 인텔리전스 필터링에 대한 자세한 내용은 13-1페이지의 보안 인텔리전스 IP 주소 평판 블랙리스트에 추가 및 3-4페이지의 보안 인텔리전스 목록 및 피드 작업을/를 참조하십시오.

Security Intelligence 모듈 설정을 구성하려면

액세스: Admin/Maint

1단계 Health Policy Configuration 페이지에서 **Security Intelligence**를 선택합니다.

Health Policy Configuration — Security Intelligence 페이지가 나타납니다.

2단계 보안 인텔리전스를 모니터링할 모듈의 사용을 활성화하려면 **Enabled** 옵션에 대해 **On**을 선택합니다.

3단계 3가지 옵션이 제공됩니다.

- 이 모듈에 대한 변경 사항을 저장하고 Health Policy 페이지로 돌아가려면 **Save Policy and Exit**를 클릭합니다.
- 이 모듈에 대한 설정을 저장하지 않은 채 Health Policy 페이지로 돌아가려면 **Cancel**을 클릭합니다.
- 이 모듈에 대한 변경 사항을 임시로 저장하고 다른 수정할 모듈 설정으로 전환하려면 페이지의 왼쪽에 있는 목록에서 다른 모듈을 선택합니다. 수정을 마친 후 **Save Policy and Exit**를 클릭하면 변경한 모든 내용이 저장됩니다. **Cancel**을 클릭하면 모든 변경 사항이 취소됩니다.

설정이 반영되도록 하려면 해당 디바이스에 상태 정책을 적용해야 합니다. 자세한 내용은 68-29페이지의 상태 정책 적용을/를 참조하십시오.

Time Series Data 모니터링 구성

라이센스: 모두

Time Series Data Monitor 모듈을 사용하면 시스템이 저장한 시계열 데이터(예: 규정 준수 이벤트의 목록)의 상태를 모니터링할 수 있습니다. 이 모듈은 손상된 파일의 시계열 데이터 스토리지 디렉토리를 스캔합니다. 모듈은 손상된 데이터를 발견하면 Warning 상태로 들어가서 영향받는 모든 파일의 이름을 보고합니다.

시계열 데이터 모니터링 설정을 구성하려면

액세스: Admin/Maint

1단계 Health Policy Configuration 페이지에서 **Time Series Data Monitor**를 선택합니다.

Health Policy Configuration — Time Series Data Monitor 페이지가 나타납니다.

2단계 상태를 테스트할 모듈의 사용을 활성화하려면 **Enabled** 옵션에 대해 **On**을 선택합니다.

3단계 3가지 옵션이 제공됩니다.

- 이 모듈에 대한 변경 사항을 저장하고 Health Policy 페이지로 돌아가려면 **Save Policy and Exit**를 클릭합니다.
- 이 모듈에 대한 설정을 저장하지 않은 채 Health Policy 페이지로 돌아가려면 **Cancel**을 클릭합니다.

- 이 모듈에 대한 변경 사항을 임시로 저장하고 다른 수정할 모듈 설정으로 전환하려면 페이지의 왼쪽에 있는 목록에서 다른 모듈을 선택합니다. 수정을 마친 후 **Save Policy and Exit**를 클릭하면 변경한 모든 내용이 저장됩니다. **Cancel**을 클릭하면 모든 변경 사항이 취소됩니다.

설정이 반영되도록 하려면 해당 디바이스에 상태 정책을 적용해야 합니다. 자세한 내용은 68-29페이지의 상태 정책 적용을/를 참조하십시오.

Time Synchronization 모니터링 구성

라이센스: 모두

Time Synchronization Status 모듈을 사용하면 NTP 서버에서 시간을 가져오기 위해 NTP를 사용하는 관리되는 디바이스의 시간이 서버의 시간과 10초 넘게 차이가 나는 시점을 탐지할 수 있습니다.

시간 동기화 모니터링 설정을 구성하려면

액세스: Admin/Maint

1단계 Health Policy Configuration 페이지에서 **Time Synchronization Status**를 선택합니다.

Health Policy Configuration — Time Synchronization Status 페이지가 나타납니다.

2단계 상태를 테스트할 모듈의 사용을 활성화하려면 **Enabled** 옵션에 대해 **On**을 선택합니다.

3단계 3가지 옵션이 제공됩니다.

- 이 모듈에 대한 변경 사항을 저장하고 Health Policy 페이지로 돌아가려면 **Save Policy and Exit**를 클릭합니다.
- 이 모듈에 대한 설정을 저장하지 않은 채 Health Policy 페이지로 돌아가려면 **Cancel**을 클릭합니다.
- 이 모듈에 대한 변경 사항을 임시로 저장하고 다른 수정할 모듈 설정으로 전환하려면 페이지의 왼쪽에 있는 목록에서 다른 모듈을 선택합니다. 수정을 마친 후 **Save Policy and Exit**를 클릭하면 변경한 모든 내용이 저장됩니다. **Cancel**을 클릭하면 모든 변경 사항이 취소됩니다.

설정이 반영되도록 하려면 해당 디바이스에 상태 정책을 적용해야 합니다. 자세한 내용은 68-29페이지의 상태 정책 적용을/를 참조하십시오.

URL Filtering 모니터링 구성

라이센스: URL 필터링

지원되는 Defense Center: DC500을 제외한 모든 방어 센터

URL Filtering Monitor 모듈을 사용하면 방어 센터 및 Cisco 클라우드 간 통신을 추적할 수 있습니다. 여기에서 시스템은 방문 빈도가 높은 URL에 대한 URL 필터링(카테고리 및 평판) 데이터를 가져옵니다. 방어 센터가 클라우드와 성공적으로 통신하지 못하거나 업데이트를 검색하지 못하면 해당 모듈에 대한 상태 분류가 Critical로 변경됩니다.

고가용성 컨피그레이션에서는 주 방어 센터만 URL 필터링 클라우드와 통신합니다. 이 모듈의 모든 데이터는 해당 주 어플라이언스만 참조합니다.

URL Filtering Monitor 모듈은 URL 필터링을 활성화한 관리되는 디바이스와 방어 센터 간 통신도 추적합니다. 방어 센터와 클라우드가 성공적으로 통신하는 경우, 방어 센터가 관리되는 디바이스로 새 URL 필터링 데이터를 푸시할 수 없으면 모듈 상태가 Warning으로 변경됩니다.

URL Filtering Monitor 상태 모듈 설정을 구성하려면

액세스: Admin/Maint

1단계 Health Policy Configuration 페이지에서 **URL Filtering Monitor**를 선택합니다.

Health Policy Configuration — URL Filtering Monitor 페이지가 나타납니다.

2단계 상태를 테스트할 모듈의 사용을 활성화하려면 **Enabled** 옵션에 대해 **On**을 선택합니다.

3단계 3가지 옵션이 제공됩니다.

- 이 모듈에 대한 변경 사항을 저장하고 Health Policy 페이지로 돌아가려면 **Save Policy and Exit**를 클릭합니다.
- 이 모듈에 대한 설정을 저장하지 않은 채 Health Policy 페이지로 돌아가려면 **Cancel**을 클릭합니다.
- 이 모듈에 대한 변경 사항을 임시로 저장하고 다른 수정할 모듈 설정으로 전환하려면 페이지의 왼쪽에 있는 목록에서 다른 모듈을 선택합니다. 수정을 마친 후 **Save Policy and Exit**를 클릭하면 변경한 모든 내용이 저장됩니다. **Cancel**을 클릭하면 모든 변경 사항이 취소됩니다.

설정이 반영되도록 하려면 방어 센터에 상태 정책을 적용해야 합니다. 자세한 내용은 68-29페이지의 상태 정책 적용을/를 참조하십시오.

User Agent Status 모니터링 구성

라이센스: FireSIGHT

User Agent Status Monitor 상태 모듈을 사용하면 방어 센터에 연결된 에이전트의 하트비트를 모니터링할 수 있습니다. 적용된 상태 정책에서 모듈을 활성화하면, 방어 센터에서 방어 센터에 구성된 에이전트의 하트비트를 탐지하지 못하는 경우 상태 알림이 생성됩니다.

User Agent Status Monitor 상태 모듈 설정을 구성하려면

액세스: Admin/Maint

1단계 Health Policy Configuration 페이지에서 **User Agent Status Monitor**를 선택합니다.

Health Policy Configuration — User Agent Status Monitor 페이지가 나타납니다.

2단계 상태를 테스트할 모듈의 사용을 활성화하려면 **Enabled** 옵션에 대해 **On**을 선택합니다.

3단계 3가지 옵션이 제공됩니다.

- 이 모듈에 대한 변경 사항을 저장하고 Health Policy 페이지로 돌아가려면 **Save Policy and Exit**를 클릭합니다.
- 이 모듈에 대한 설정을 저장하지 않은 채 Health Policy 페이지로 돌아가려면 **Cancel**을 클릭합니다.
- 이 모듈에 대한 변경 사항을 임시로 저장하고 다른 수정할 모듈 설정으로 전환하려면 페이지의 왼쪽에 있는 목록에서 다른 모듈을 선택합니다. 수정을 마친 후 **Save Policy and Exit**를 클릭하면 변경한 모든 내용이 저장됩니다. **Cancel**을 클릭하면 모든 변경 사항이 취소됩니다.

설정이 반영되도록 하려면 방어 센터에 상태 정책을 적용해야 합니다. 자세한 내용은 68-29페이지의 상태 정책 적용을/를 참조하십시오.

VPN Status 모니터링 구성

라이센스: VPN

지원되는 Defense Center: Series 2를 제외한 모두

VPN Status 상태 모듈을 사용하면 구성된 Gateway VPN 터널의 현재 상태를 모니터링할 수 있습니다. 개별 터널에 대한 정보가 표시됩니다. 작동하지 않는 VPN 터널이 있으면 이 모듈은 Critical(빨간색) 상태 알림을 생성합니다.

VPN Status 상태 모듈 설정을 구성하려면

액세스: Admin/Maint

1단계 Health Policy Configuration 페이지에서 **VPN Status**를 클릭합니다.

Health Policy Configuration — VPN Status 페이지가 나타납니다.

2단계 상태를 테스트할 모듈의 사용을 활성화하려면 **Enabled** 옵션에 대해 **On**을 선택합니다.

3단계 3가지 옵션이 제공됩니다.

- 이 모듈에 대한 변경 사항을 저장하고 Health Policy 페이지로 돌아가려면 **Save Policy and Exit**를 클릭합니다.
- 이 모듈에 대한 설정을 저장하지 않은 채 Health Policy 페이지로 돌아가려면 **Cancel**을 클릭합니다.
- 이 모듈에 대한 변경 사항을 임시로 저장하고 다른 수정할 모듈 설정으로 전환하려면 페이지의 왼쪽에 있는 목록에서 다른 모듈을 선택합니다. 수정을 마친 후 **Save Policy and Exit**를 클릭하면 변경한 모든 내용이 저장됩니다. **Cancel**을 클릭하면 모든 변경 사항이 취소됩니다.

설정이 반영되도록 하려면 해당 디바이스에 상태 정책을 적용해야 합니다. 자세한 내용은 68-29페이지의 상태 정책 적용을/를 참조하십시오.

상태 정책 적용

라이센스: 모두

어플라이언스에 상태 정책을 적용하면, 정책에서 활성화한 모든 모듈에 대한 상태 테스트가 어플라이언스의 프로세스 및 하드웨어의 상태를 모니터링합니다. 상태 테스트는 정책에 구성된 간격으로 계속 실행되면서 어플라이언스에 대한 상태 데이터를 수집한 다음 방어 센터로 전달합니다.

상태 정책에서 모듈을 활성화한 다음 상태 테스트가 필요하지 않은 어플라이언스에 정책을 적용하면, 상태 모니터는 해당 상태 모듈의 상태를 비활성으로 보고합니다.

모든 모듈이 비활성화된 정책을 어플라이언스에 적용하면, 적용된 모든 상태 정책이 어플라이언스에서 제거됩니다.

정책이 이미 적용된 어플라이언스에 다른 정책을 적용하면, 새로 적용된 테스트를 기반으로 새 데이터의 표시에 약간의 레이턴시가 발생합니다.

참고 고가용성 쌍으로 방어 센터에 생성된 사용자 지정 상태 정책은 두 어플라이언스 간에 복제됩니다. 그러나 기본 상태 정책에 대한 변경 사항은 복제되지 않습니다. 각 어플라이언스는 해당 어플라이언스에 대해 구성된 로컬 기본 상태 정책을 사용합니다.

상태 정책을 적용하려면

액세스: Admin/Maint

1단계 **Health > Health Policy**를 선택합니다.

Health Policy 페이지가 나타납니다.

2단계 적용할 정책 옆에 있는 적용 아이콘( )을 클릭합니다.

Health Policy Apply 페이지가 나타납니다.

팁 Health Policy 열 옆의 상태 아이콘( )은 어플라이언스의 현재 상태를 나타냅니다. System Policy 열 옆의 상태 아이콘( )은 방어 센터와 디바이스 간 통신 상태를 나타냅니다. 현재 적용된 정책을 제거하려면 제거 아이콘( )을 클릭할 수 있습니다.

3단계 상태 정책을 적용할 어플라이언스를 선택합니다.

4단계 선택한 어플라이언스에 정책을 적용하려면 **Apply**를 클릭합니다.

정책이 성공적으로 적용되었는지를 나타내는 메시지와 함께 Health Policy 페이지가 나타납니다. 정책이 성공적으로 적용됨과 동시에 어플라이언스의 모니터링이 시작됩니다.

상태 정책 수정

라이센스: 모두

모듈을 활성화하거나 비활성화하여, 또는 모듈 설정을 변경하여 상태 정책을 수정할 수 있습니다. 이미 어플라이언스에 적용된 정책을 수정하면 정책을 다시 적용할 때까지 변경 사항이 반영되지 않습니다.

다음 표에는 여러 어플라이언스에 적용되는 상태 모듈이 나열되어 있습니다.

표 68-3 어플라이언스에 해당되는 상태 모듈

모듈	해당 어플라이언스
AMP(Advanced Malware Protection)	방어 센터(DC500 제외)
Appliance Heartbeat	방어 센터
Automatic Application Bypass Status	모든 관리되는 디바이스
CPU Usage	3D9900을 제외한 모두
Card Reset	모든 관리되는 디바이스
Disk Status	모두
Disk Usage	모두
FireAMP Status Monitor	방어 센터
FireSIGHT Host License Limit	방어 센터
Hardware Alarms	Series 3, 3D9900
Health Monitor Process	방어 센터
Inline Link Mismatch Alarms	모든 관리되는 디바이스
Interface Status	모든 관리되는 디바이스

표 68-3 어플라이언스에 해당되는 상태 모듈 (계속)

모듈	해당 어플라이언스
Intrusion Event Rate	관리되는 디바이스(보호 포함)
License Monitor	방어 센터
Link State Propagation	관리되는 디바이스(보호 포함)
Memory Usage	모두
Power Supply	방어 센터: DC1500, DC2000, DC3500, DC4000 Devices: 3D3500, 3D4500, 3D6500, 3D9900, Series 3
Process Status	모두
Reconfiguring Detection	
RRD Server Process	방어 센터
Security Intelligence	방어 센터(DC500 제외)
Time Series Data Monitor	방어 센터
Time Synchronization Status	모두
URL Filtering Monitor	방어 센터(DC500 제외)
User Agent Status Monitor	방어 센터
VPN Status	방어 센터

상태 정책을 수정하려면

액세스: Admin/Maint

1단계 **Health > Health Policy**를 선택합니다.

Health Policy 페이지가 나타납니다.

2단계 수정할 정책 옆에 있는 수정 아이콘()을 클릭합니다.

Policy Run Time Interval 설정이 선택된 상태로 Health Policy Configuration 페이지가 나타납니다.

3단계 다음 섹션의 설명에 따라 필요한 대로 설정을 수정합니다.

- 68-10페이지의 Policy Run Time Interval 구성
- 68-11페이지의 AMP 모니터링 구성
- 68-12페이지의 Appliance Heartbeat 모니터링 구성
- 68-12페이지의 Automatic Application Bypass 모니터링 구성
- 68-13페이지의 CPU Usage 모니터링 구성
- 68-14페이지의 Card Reset 모니터링 구성
- 68-14페이지의 Disk Status 모니터링 구성
- 68-15페이지의 Disk Usage 모니터링 구성
- 68-16페이지의 Status MonitorFireAMP 구성
- 68-16페이지의 Host FireSIGHTUsage 모니터링 구성
- 68-17페이지의 Hardware Alarm 모니터링 구성

- 68-18페이지의 Health Status 모니터링 구성
- 68-19페이지의 Inline Link Mismatch Alarm 모니터링 구성
- 68-20페이지의 Intrusion Event Rate 모니터링 구성
- 68-21페이지의 License Monitoring 이해
- 68-21페이지의 Link State Propagation 모니터링 구성
- 68-22페이지의 Memory Usage 모니터링 구성
- 68-23페이지의 Power Supply 모니터링 구성
- 68-23페이지의 Process Status 모니터링 구성
- 68-24페이지의 Reconfiguring Detection 모니터링 구성
- 68-25페이지의 RRD Server Process 모니터링 구성
- 68-25페이지의 Security Intelligence 모니터링 구성
- 68-26페이지의 Time Series Data 모니터링 구성
- 68-27페이지의 Time Synchronization 모니터링 구성
- 68-27페이지의 URL Filtering 모니터링 구성
- 68-27페이지의 URL Filtering 모니터링 구성
- 68-28페이지의 User Agent Status 모니터링 구성
- 68-29페이지의 VPN Status 모니터링 구성

4단계 3가지 옵션이 제공됩니다.

- 이 모듈에 대한 변경 사항을 저장하고 Health Policy 페이지로 돌아가려면 **Save Policy and Exit**를 클릭합니다.
- 이 모듈에 대한 설정을 저장하지 않은 채 Health Policy 페이지로 돌아가려면 **Cancel**을 클릭합니다.
- 이 모듈에 대한 변경 사항을 임시로 저장하고 다른 수정할 모듈 설정으로 전환하려면 페이지의 왼쪽에 있는 목록에서 다른 모듈을 선택합니다. 수정을 마친 후 **Save Policy and Exit**를 클릭하면 변경한 모든 내용이 저장됩니다. **Cancel**을 클릭하면 모든 변경 사항이 취소됩니다.

5단계 68-29페이지의 상태 정책 적용에 설명된 대로 정책을 해당 어플라이언스에 다시 적용합니다.

상태 정책 비교

라이센스: 모두

조직의 표준을 준수하거나 상태 모니터링 성능을 최적화하기 위해 정책 변경 사항을 검토할 경우 두 상태 정책 간의 차이를 확인할 수 있습니다. 액세스할 수 있는 상태 정책에 대해 두 가지 상태 정책 또는 동일한 상태 정책의 두 가지 개정을 비교할 수 있습니다. 두 가지 활성 상태 정책을 빠르게 비교하려면 **Running Configuration** 옵션을 선택할 수 있습니다. 선택적으로, 비교 후 두 정책 또는 정책 개정의 차이를 기록하는 PDF 보고서를 생성할 수도 있습니다.

상태 정책 또는 상태 정책 개정의 비교에 사용할 수 있는 두 가지 툴이 있습니다.

- 비교 보기에는 두 상태 정책 또는 상태 정책 개정 간의 차이점만 나란히 표시됩니다. 각 정책 또는 정책 개정의 이름은 비교 보기 왼쪽과 오른쪽의 제목 표시줄에 나타납니다..

  이를 사용하여 웹 인터페이스에서 차이점이 강조 표시된 상태로 두 정책 개정을 모두 보고 탐색할 수 있습니다.

- 비교 보고서는 두 상태 정책 또는 상태 정책 개정의 차이점에 대해서만 기록을 생성하는데, 그 형식은 상태 정책 보고서와 비슷하지만 PDF 형식입니다.

  이를 사용하여 향후 점검을 위해 정책 비교를 저장, 복사, 인쇄, 공유할 수 있습니다.

상태 정책 비교 툴을 이해하고 사용하는 방법에 대한 자세한 내용은 다음을 참조하십시오.

- 68-33페이지의 상태 정책 비교 보기 사용
- 68-33페이지의 상태 정책 비교 보고서 사용

상태 정책 비교 보기 사용

라이센스: 모두

비교 보기에서는 두 상태 정책 또는 정책 개정을 나란히 표시하며, 각 정책 또는 정책 개정은 비교 보기의 좌우 제목 표시줄에 있는 이름으로 식별됩니다. 마지막 수정 시간 및 마지막 수정자가 정책 이름의 오른쪽에 표시됩니다. Health Policy 페이지에는 정책의 마지막 수정 시간이 현지 시간으로 표시되지만, 상태 정책 보고서에는 수정 시간이 UTC로 표시됩니다.

두 가지 상태 정책 또는 정책 개정 간의 차이점이 강조 표시됩니다.

- 파란색은 강조 표시된 설정이 두 정책 또는 정책 개정에서 다름을 의미하며, 그 차이점이 빨간색 텍스트로 표시됩니다.
- 녹색은 강조 표시된 설정이 둘 중 한 정책 또는 정책 개정에만 나타남을 의미합니다.

다음 표의 작업을 수행할 수 있습니다.

표 68-4 상태 정책 비교 보기의 작업

목적	가능한 작업
개별 변경 사항 탐색	제목 표시줄 위의 **Previous** 또는 **Next**를 클릭합니다. 왼쪽과 오른쪽 사이의 중앙에 있는 이중 화살표 아이콘( )이 움직이고, 어떤 차이점을 보고 있는지 식별할 수 있도록 **Difference** 번호가 조정됩니다.
새 상태 정책 비교 보기 생성	**New Comparison**을 클릭합니다. **Select Comparison** 창이 나타납니다. 자세한 내용은 상태 정책 비교 보고서 사용을/를 참조하십시오.
상태 정책 비교 보고서 생성	**Comparison Report**를 클릭합니다. 상태 정책 비교 보고서는 비교 보기와 동일한 정보를 포함하는 PDF를 생성합니다.

상태 정책 비교 보고서 사용

라이센스: 모두

상태 정책 비교 보고서는 두 상태 정책 또는 동일한 상태 정책의 두 개정 간 모든 차이점을 PDF에서 상태 정책 비교 보기 형태로 기록한 것입니다. 두 상태 정책 컨피그레이션의 차이점을 더 자세히 살펴보고 조사 결과를 저장하여 배포하는 데 이 보고서를 사용할 수 있습니다.

액세스 권한이 있는 어떤 상태 정책에 대해서도 비교 보기에서 상태 정책 비교 보고서를 생성할 수 있습니다. 상태 정책 보고서를 생성하기 전에 모든 잠재적인 변경 사항을 커밋해야 합니다. 커밋된 변경 사항만 보고서에 나타납니다.

컨피그레이션에 따라, 상태 정책 비교 보고서는 하나 이상의 섹션을 포함할 수 있습니다. 각 섹션은 동일한 형식을 사용하며 동일한 수준의 세부사항을 제공합니다. Value A 및 Value B 열은 비교 보기에서 구성한 정책 또는 정책 개정을 표시합니다.

팁 SSL, 네트워크 분석, 침입, 파일, 시스템 또는 액세스 제어 정책을 비교하는 절차도 비슷합니다.

두 상태 정책 또는 동일한 정책의 두 개정을 비교하려면

액세스: Admin/Maint

1단계 **Health > Health Policy**를 선택합니다.

Health Policy 페이지가 나타납니다.

2단계 **Compare Policies**를 클릭합니다.

Select Comparison 창이 나타납니다.

3단계 **Compare Against** 드롭다운 목록에서 원하는 비교 유형을 선택합니다.

- 두 개의 다른 정책을 비교하려면 **Other Policy**를 선택합니다.
- 동일한 정책의 두 개정을 비교하려면 **Other Revision**을 선택합니다.
- 다른 정책과 현재 활성 정책을 비교하려면 **Running Configuration**을 선택합니다.

상태 정책 보고서를 생성하기 전에 모든 변경 사항을 커밋해야 합니다. 커밋된 변경 사항만 보고서에 나타납니다.

4단계 선택한 비교 유형에 따라 다음을 선택할 수 있습니다.

- 두 개의 다른 정책을 비교할 경우 비교할 정책을 **Policy A** 및 **Policy B** 드롭다운 목록에서 각각 선택합니다.
- 동일한 정책의 두 개정을 비교하는 경우 **Policy** 드롭다운 목록에서 정책을 선택한 다음, **Revision A** 및 **Revision B** 드롭다운 목록에서 비교할 개정을 선택합니다.
- 실행 중인 컨피그레이션을 다른 정책과 비교할 경우 **Policy B** 드롭다운 목록에서 두 번째 정책을 선택합니다.

5단계 상태 정책 비교 보기를 표시하려면 **OK**를 클릭합니다.

비교 보기가 나타납니다.

6단계 상태 정책 비교 보고서를 생성하려면 **Comparison Report**를 클릭합니다.

상태 정책 보고서가 나타납니다. 브라우저 설정에 따라 보고서가 팝업 창에 나타날 수 있으며, 컴퓨터에 보고서를 저장하는 프롬프트가 표시될 수도 있습니다.

상태 정책 삭제

라이센스: 모두

더 이상 필요 없는 상태 정책을 삭제할 수 있습니다. 어플라이언스에 여전히 적용된 정책을 삭제하면, 다른 정책을 적용할 때까지 정책 설정이 그대로 유지됩니다. 또한 디바이스에 적용된 상태 정책을 삭제하면, 연결된 기반 알림 응답을 비활성화할 때까지 디바이스에 적용된 상태 모니터링 알림은 활성 상태로 유지됩니다. 43-8페이지의 알림 응답 활성화 및 비활성화을/를 참조하십시오.

팁 어플라이언스에 대한 상태 모니터링을 중지하려면 모든 모듈이 비활성화된 상태 정책을 생성하여 어플라이언스에 적용합니다. 상태 정책 생성에 대한 자세한 내용은 68-9페이지의 상태 정책 생성을/를 참조하십시오. 상태 정책 적용에 대한 자세한 내용은 68-29페이지의 상태 정책 적용을/를 참조하십시오.

상태 정책을 삭제하려면

액세스: Admin/Maint

1단계 **Health > Health Policy**를 선택합니다.

Health Policy 페이지가 나타납니다.

2단계 삭제할 정책 옆에 있는 삭제 아이콘( )을 클릭합니다.

성공적으로 삭제했음을 알리는 메시지가 나타납니다.

상태 모니터 블랙리스트 사용

라이센스: 모두

일반적인 네트워크 유지 보수 과정에서 어플라이언스를 비활성화하거나 일시적으로 사용할 수 없도록 만들 수 있습니다. 이러한 중단은 고의적인 것이므로 해당 어플라이언스의 상태가 방어 센터의 요약 상태에 영향을 미치지 않도록 할 수 있습니다.

어플라이언스나 모듈에 대한 상태 모니터링 상태 보고를 비활성화하려면 상태 모니터 블랙리스트 기능을 사용할 수 있습니다. 예를 들어 네트워크의 한 세그먼트를 사용할 수 없게 될 것임을 알고 있는 경우 해당 세그먼트의 관리되는 디바이스에 대한 상태 모니터링을 일시적으로 비활성화할 수 있습니다. 그러면 디바이스에 대한 연결이 무효화되므로 방어 센터의 상태가 Warning 또는 Critical 상태로 표시되지 않습니다.

상태 모니터링 상태를 비활성화하면 상태 이벤트는 여전히 생성되지만 비활성화된 상태를 갖게 되어 상태 모니터의 상태에 영향을 미치지 않습니다. 어플라이언스나 모듈을 블랙리스트에서 제거하면 블랙리스트에 있는 동안 생성된 이벤트는 계속해서 비활성 상태를 표시합니다.

어플라이언스에서 일시적으로 상태 이벤트를 비활성화하려면 블랙리스트 컨피그레이션 페이지로 이동하고 블랙리스트에 어플라이언스를 추가합니다. 설정이 적용되면 시스템은 전체적인 상태를 계산할 때 블랙리스트의 어플라이언스를 더 이상 포함하지 않습니다. Health Monitor Appliance Status Summary에는 어플라이언스가 비활성 상태로 나열됩니다.

때로는 어플라이언스에서 개별 상태 모니터링 모듈만 블랙리스트에 추가하는 것이 좀 더 실용적일 수 있습니다. 예를 들어 어플라이언스에서 FireSIGHT 호스트 라이센스가 부족해지면 FireSIGHT Host License Limit 상태 메시지를 블랙리스트에 추가할 수 있습니다.

기본 Health Monitor 페이지에서, 특정 상태 행의 화살표를 클릭하여 해당 상태의 어플라이언스 목록을 볼 수 있도록 확장하면 블랙리스트에 추가된 여러 어플라이언스를 구분할 수 있습니다. 보기 확장에 대한 자세한 내용은 68-41페이지의 상태 모니터 사용을/를 참조하십시오.

블랙리스트에 추가되거나 부분적으로 추가된 어플라이언스의 보기를 확장하면 블랙리스트 아이콘( )과 표기법이 표시됩니다.

참고 방어 센터에서 Health Monitor 블랙리스트 설정은 로컬 컨피그레이션 설정입니다. 따라서 디바이스를 블랙리스트에 추가한 다음, 삭제 후 방어 센터에서 다시 등록하는 경우 블랙리스트 설정이 계속 유지됩니다. 새롭게 다시 등록한 디바이스는 계속 블랙리스트에 유지됩니다.

자세한 내용은 다음 링크를 참고하십시오.

- 68-36페이지의 상태 정책 또는 어플라이언스를 블랙리스트에 추가
- 68-37페이지의 어플라이언스를 블랙리스트에 추가
- 68-37페이지의 상태 정책 모듈을 블랙리스트에 추가

상태 정책 또는 어플라이언스를 블랙리스트에 추가

라이센스: 모두

특별한 상태 정책이 있는 모든 어플라이언스에 대해 상태 이벤트를 비활성으로 설정하려면 정책을 블랙리스트에 추가할 수 있습니다. 어플라이언스 그룹의 상태 모니터링을 비활성화해야 하는 경우 어플라이언스 그룹을 블랙리스트에 추가할 수 있습니다. 블랙리스트 설정이 적용되면 어플라이언스가 Health Monitor Appliance Module Summary 및 Device Management 페이지에서 비활성으로 표시됩니다. 어플라이언스에 대한 상태 이벤트에 상태가 Disabled로 표시됩니다.

방어 센터가 고가용성 컨피그레이션이면 한 고가용성 피어의 관리되는 디바이스는 블랙리스트에 추가하고 다른 하나는 추가하지 않을 수 있습니다. 또한 고가용성 피어를 블랙리스트에 추가하여 그곳에서 생성되는 이벤트 및 상태 이벤트를 받는 디바이스를 비활성으로 표시할 수 있습니다.고가용성 쌍의 방어 센터에서는 피어를 완전히 또는 부분적으로 블랙리스트에 추가할 수 있습니다.

전체 상태 정책 또는 어플라이언스 그룹을 블랙리스트에 추가하려면

액세스: Admin/Maint

1단계 **Health > Blacklist**를 선택합니다.

Blacklist 페이지가 나타납니다.

2단계 오른쪽에 있는 드롭다운 목록을 사용하여 그룹별, 정책별 또는 모델별로 목록을 정렬합니다. (NO MDC THIS TIME방어 센터의 그룹은 관리되는 디바이스이고)

전체가 아닌 일부 모듈이 블랙리스트에 추가된 어플라이언스는 **(Partially Blacklisted)**로 나타납니다. 기본 블랙리스트 페이지의 블랙리스트 상태를 수정할 경우 어플라이언스의 모든 모듈을 블랙리스트에 추가하거나 블랙리스트에서 제거할 수 있습니다. 어플라이언스의 개별 상태 모듈을 블랙리스트에 추가하는 방법에 대한 자세한 내용은 68-37페이지의 상태 정책 모듈을 블랙리스트에 추가을/를 참조하십시오.

팁 Health Policy 열 옆의 상태 아이콘( )은 어플라이언스의 현재 상태를 나타냅니다. System Policy 열 옆의 상태 아이콘( )은 방어 센터와 디바이스 간 통신 상태를 나타냅니다.

3단계 다음 2가지 옵션을 사용할 수 있습니다.

- 그룹, 모델 또는 정책 카테고리의 모든 어플라이언스를 블랙리스트에 추가하려면 카테고리를 선택하고 **Blacklist Selected Devices**를 클릭합니다.
- 그룹, 모델 또는 정책 카테고리의 모든 어플라이언스를 블랙리스트에서 지우려면 카테고리를 선택한 다음 **Clear Blacklist on Selected Devices**를 클릭합니다.

페이지가 새로 고쳐지고, 이제 어플라이언스의 새로운 블랙리스트 상태가 표시됩니다.

어플라이언스를 블랙리스트에 추가

라이센스: 모두

개별 어플라이언스의 이벤트 및 상태를 비활성으로 설정하려면 어플라이언스를 블랙리스트에 추가할 수 있습니다. 블랙리스트 설정이 적용되면 어플라이언스가 Health Monitor Appliance Module Summary에서 비활성으로 표시되고, 어플라이언스에 대한 상태 이벤트에 상태가 Disabled로 표시됩니다.

개별 어플라이언스를 블랙리스트에 추가하려면

액세스: Admin/Maint

1단계 **Health > Blacklist**를 선택합니다.

Blacklist 페이지가 나타납니다.

2단계 오른쪽에 있는 드롭다운 목록을 사용하여 어플라이언스 그룹별, 모델별 또는 정책별로 목록을 정렬합니다.

3단계 다음 2가지 옵션을 사용할 수 있습니다.

- 그룹, 모델 또는 정책 카테고리의 모든 어플라이언스를 블랙리스트에 추가하려면 카테고리를 선택하고 **Blacklist Selected Devices**를 클릭합니다.
- 그룹, 모델 또는 정책 카테고리의 모든 어플라이언스를 블랙리스트에서 지우려면 카테고리를 선택한 다음 **Clear Blacklist on Selected Devices**를 클릭합니다.

페이지가 새로 고쳐지고 어플라이언스의 새로운 블랙리스트 상태가 표시됩니다. 개별 상태 정책 모듈을 블랙리스트에 추가하려면 **Edit**를 클릭하고 68-37페이지의 상태 정책 모듈을 블랙리스트에 추가을/를 참조하십시오.

상태 정책 모듈을 블랙리스트에 추가

라이센스: 모두

어플라이언스에서 개별 상태 정책 모듈을 블랙리스트에 추가할 수 있습니다. 모듈의 이벤트가 어플라이언스의 상태를 Warning 또는 Critical로 변경하지 못하게 하려면 이 기능을 사용할 수 있습니다.

모듈의 일부가 블랙리스트에 추가되면 해당 모듈에 대한 줄이 방어 센터 웹 인터페이스에서 굵은 글꼴로 표시됩니다.

팁 블랙리스트 설정이 적용되면 Blacklist 페이지 및 Appliance Health Monitor Module Status Summary에서 어플라이언스가 **Partially Blacklisted** 또는 **All Modules Blacklisted**로 표시됩니다. 단, 기본 Appliance Status Summary 페이지에서는 확장된 보기에만 표시됩니다. 개별적으로 블랙리스트에 추가한 모듈은 필요 시 다시 활성화할 수 있도록 계속 추적해야 합니다. 실수로 모듈을 비활성 상태로 남겨 두면 필요한 Warning 또는 Critical 메시지를 놓칠 수 있습니다.

개별 상태 정책 모듈을 블랙리스트에 추가하려면

액세스: Admin/Maint

1단계 **Health > Blacklist**를 선택합니다.

Blacklist 페이지가 나타납니다.

2단계 Group, Policy 또는 Model별로 정렬한 다음 **Edit**를 클릭하여 어플라이언스에 대한 상태 정책 모듈의 목록을 표시합니다.

상태 정책 모듈이 나타납니다.

3단계 블랙리스트에 추가할 각 모듈을 선택합니다.

4단계 **Save**를 클릭합니다.

상태 모니터 알림 구성

라이센스: 모두

상태 정책에서 모듈에 대한 상태가 변경될 때 이메일, SNMP 또는 시스템 로그를 통해 알리도록 알림을 설정할 수 있습니다. 기존 알림 응답을 트리거할 상태 이벤트 레벨과 연결하고, 특별한 레벨의 상태 이벤트가 발생할 때 알릴 수 있습니다.

예를 들어 어플라이언스의 하드 디스크 공간이 부족해질 것이 우려되면, 남은 디스크 공간이 Warning 레벨에 도달할 때 시스템 관리자에게 이메일을 자동으로 전송할 수 있습니다. 하드 디스크가 계속 채워지면 하드 드라이브가 Critical 레벨에 도달할 때 두 번째 이메일을 전송할 수 있습니다.

자세한 내용은 다음 항목을 참조하십시오.

- 68-38페이지의 상태 모니터 알림 생성
- 68-39페이지의 상태 모니터 알림 해석
- 68-40페이지의 상태 모니터 알림 수정
- 68-40페이지의 상태 모니터 알림 삭제

상태 모니터 알림 생성

라이센스: 모두

상태 모니터 알림을 생성할 때 심각도, 상태 모듈 및 알림 응답 간에 연결을 생성합니다. 기존 알림을 사용할 수도 있고 특별히 시스템 상태에 대해 보고하도록 새 알림을 구성할 수도 있습니다. 선택한 모듈에 대해 심각도가 발생하면 알림이 트리거됩니다.

기존 임계값을 복제하는 방식으로 임계값을 생성하거나 업데이트하는 경우 충돌이 발생합니다. 중복된 임계값이 존재하면 상태 모니터는 가장 적은 알림을 생성하는 임계값을 사용하고 나머지는 무시합니다. 임계값의 시간 제한 값은 범위가 5~4,294,967,295분이어야 합니다.

상태 모니터 알림을 생성하려면

액세스: Admin

1단계 **Health > Health Monitor Alerts**를 선택합니다.

Health Monitor Alerts 페이지가 나타납니다.

2단계 **Health Alert Name** 필드에 상태 알림의 이름을 입력합니다.

3단계 알림을 트리거하기 위해 사용할 심각도를 **Severity** 목록에서 선택합니다.

4단계 알림을 적용할 모듈을 **Module** 목록에서 선택합니다.

팁 여러 모듈을 선택하려면 Shift + Ctrl을 누른 상태에서 모듈 이름을 클릭합니다.

5단계 선택한 심각도에 도달할 때 트리거할 알림 응답을 **Alert** 목록에서 선택합니다.

팁 Alerts 페이지를 열려면 **Alerts**를 클릭합니다. 알림 생성에 대한 자세한 내용은 43-2페이지의 알림 응답 작업을/를 참조하십시오.

6단계 선택적으로, 각 임계값 기간이 끝나고 임계값 카운트가 재설정되기까지의 시간(분 단위)을 **Threshold Timeout** 필드에 입력합니다. 기본값은 5분입니다.

정책 실행 시간 간격 값이 임계값 시간 제한 값보다 작더라도 지정된 모듈에서 보고된 두 상태 이벤트 사이의 간격은 항상 더 큽니다. 임계값 시간 제한이 8분이고 정책 실행 시간 간격이 5분이면 보고된 이벤트 사이에 10분의 간격(5 x 2)이 발생합니다.

7단계 **Save**를 클릭하여 상태 알림을 저장합니다.

컨피그레이션이 성공적으로 저장되었음을 알리는 메시지가 나타납니다. 이제 생성한 알림이 Active Health Alerts 목록에 포함됩니다.

상태 모니터 알림 해석

라이센스: 모두

상태 모니터에 의해 생성되는 알림에는 다음 정보가 포함됩니다.

- 심각도 - 알림의 심각도를 나타냅니다.
- 모듈 - 테스트 결과가 알림을 트리거한 상태 모듈을 지정합니다.
- 설명 - 테스트 결과가 알림을 트리거한 상태 테스트를 포함합니다.

상태 알림 심각도에 대한 자세한 내용은 다음 표를 참조하십시오.

표 68-5 알림 심각도

심각도	설명
Critical	상태 테스트 결과가 Critical 알림 상태를 트리거하는 기준을 충족함
Warning	상태 테스트 결과가 Warning 알림 상태를 트리거하는 기준을 충족함
Normal	상태 테스트 결과가 Normal 알림 상태를 트리거하는 기준을 충족함
Error	상태 테스트가 실행되지 않음
Recovered	상태 테스트 결과가 Critical 또는 Warning 알림 상태에 이어 Normal 알림 상태를 반환하는 기준을 충족함

상태 모듈에 대한 자세한 내용은 68-3페이지의 상태 모듈 이해을/를 참조하십시오.

상태 모니터 알림 수정

라이센스: 모두

상태 모니터 알림과 관련된 심각도, 상태 모듈 또는 알림 응답을 변경하려면 기존의 상태 모니터 알림을 수정할 수 있습니다.

상태 모니터 알림을 수정하려면

액세스: Admin

1단계 **Health > Health Monitor Alerts**를 선택합니다.

Health Monitor Alerts 페이지가 나타납니다.

2단계 수정할 알림을 **Active Health Alerts** 목록에서 선택합니다.

3단계 선택한 알림에 대해 구성된 설정을 로드하려면 **Load**를 클릭합니다.

4단계 필요에 따라 설정을 수정합니다. 자세한 내용은 68-38페이지의 상태 모니터 알림 생성을/를 참조하십시오.

5단계 수정된 상태 알림을 저장하려면 **Save**를 클릭합니다.

컨피그레이션이 성공적으로 저장되었음을 알리는 메시지가 나타납니다.

상태 모니터 알림 삭제

라이센스: 모두

기존의 상태 모니터 알림을 삭제할 수 있습니다.

참고 상태 모니터 알림을 삭제해도 연결된 알림 응답은 삭제되지 않습니다. 알림이 계속 전송되지 않도록 하려면 기본 알림 응답을 비활성화하거나 삭제해야 합니다. 자세한 내용은 43-8페이지의 알림 응답 활성화 및 비활성화 및 43-7페이지의 알림 응답 삭제을/를 참조하십시오.

상태 모니터 알림을 삭제하려면

액세스: Admin

1단계 **Health > Health Monitor Alerts**를 선택합니다.

Health Monitor Alerts 페이지가 나타납니다.

2단계 삭제할 알림을 **Active Health Alerts** 목록에서 선택합니다.

3단계 **Delete**를 클릭합니다.

컨피그레이션이 성공적으로 삭제되었음을 알리는 메시지가 나타납니다.

상태 모니터 사용

라이센스: 모두

Health Monitor 페이지는 방어 센터 및 방어 센터에서 관리하는 모든 디바이스에 대한 복합적인 상태를 제공합니다. Status 테이블은 전체적인 상태를 기준으로 이 방어 센터에 대한 관리되는 어플라이언스의 카운트를 제공합니다. 원 그래프는 상태 분석의 또 다른 보기를 제공하며, 현재 각 상태 카테고리에서 어플라이언스의 비율을 나타냅니다.

상태 모니터를 사용하려면

액세스: Admin/Maint/Any Security Analyst

1단계 **Health > Health Monitor**를 클릭합니다.

Health Monitor 페이지가 나타납니다.

2단계 테이블의 Status 열이나 해당 상태의 목록 어플라이언스에 대한 원 그래프의 원하는 부분에서 원하는 상태를 선택합니다.

팁 상태 레벨에 대한 행의 화살표가 아래쪽을 가리키면 해당 상태의 어플라이언스 목록은 아래쪽 테이블에 표시됩니다. 화살표가 오른쪽을 가리키면 어플라이언스 목록은 숨겨집니다.

다음 항목은 Health Monitor 페이지에서 수행할 수 있는 작업에 대한 세부사항을 제공합니다.

- 68-41페이지의 상태 모니터 상태 해석
- 68-42페이지의 어플라이언스 상태 모니터 사용
- 68-7페이지의 상태 정책 구성
- 68-38페이지의 상태 모니터 알림 구성

상태 모니터 상태 해석

라이센스: 모두

심각도별 사용 가능한 상태 카테고리는 다음 표에 설명한 대로 Error, Critical, Warning, Normal, Recovered 및 Disabled입니다.

표 68-6 상태 지표

상태 레벨	상태 아이콘	상태 색상	설명
Error		백	어플라이언스에서 하나 이상의 상태 모니터링 모듈이 실패했으며, 실패 이후 성공적으로 다시 실행되지 않았음을 나타냅니다. 상태 모니터링 모듈의 업데이트를 얻으려면 기술 지원 담당자에게 문의하십시오.
Critical		빨간색	어플라이언스에서 하나 이상의 상태 모듈에 대해 Critical 제한이 초과되었으며 문제가 해결되지 않았음을 나타냅니다.
Warning		노란색	어플라이언스에서 하나 이상의 상태 모듈에 대해 Warning 제한이 초과되었으며 문제가 해결되지 않았음을 나타냅니다.
Normal		녹색	어플라이언스의 모든 상태 모듈이 어플라이언스에 적용된 상태 정책에 구성된 제한 내에서 실행되고 있음을 나타냅니다.

표 68-6 상태 지표 (계속)

상태 레벨	상태 아이콘	상태 색상	설명
Recovered		녹색	어플라이언스의 모든 상태 모듈(Critical 또는 Warning 상태에 있던 모듈 포함)이 어플라이언스에 적용된 상태 정책에 구성된 제한 내에서 실행되고 있음을 나타냅니다.
Disabled		파란색	어플라이언스가 비활성화되었거나 블랙리스트에 추가되었거나, 어플라이언스에 상태 정책이 적용되지 않았거나, 어플라이언스에 현재 도달할 수 없음을 나타냅니다.

어플라이언스 상태 모니터 사용

라이센스: 모두

Appliance 상태 모니터는 어플라이언스의 상태에 대한 자세한 보기를 제공합니다.

참고 비활성 상태가 1시간(또는 구성된 다른 간격 동안) 지속되면 일반적으로 세션에서 로그아웃됩니다. 상태 모니터를 오랫동안 수동으로 모니터링할 계획이면 세션 시간 초과에서 일부 사용자를 제외하거나 시스템 시간 초과 설정을 변경하는 방법을 고려해 보십시오. 자세한 내용은 61-47페이지의 사용자 로그인 설정 관리 및 63-29페이지의 사용자 인터페이스 설정 구성을/를 참조하십시오.

특정 어플라이언스의 상태 요약을 보려면

액세스: Admin/Maint/Any Security Analyst

1단계 **Health > Health Monitor**를 선택합니다.

Health Monitor 페이지가 나타납니다.

2단계 특정 상태의 어플라이언스 목록을 표시하려면 해당 상태 열의 화살표를 클릭합니다.

팁 상태 레벨에 대한 행의 화살표가 아래쪽을 가리키면 해당 상태의 어플라이언스 목록은 아래쪽 테이블에 표시됩니다. 화살표가 오른쪽을 가리키면 어플라이언스 목록은 숨겨집니다.

3단계 어플라이언스 목록의 **Appliance** 열에서 상태 모니터 툴바에 세부사항을 표시할 어플라이언스의 이름을 클릭합니다.

Health Monitor Appliance 페이지가 나타납니다.

4단계 선택적으로, 보려는 이벤트 상태 카테고리의 색상을 **Module Status Summary** 그래프에서 클릭합니다. 이벤트를 표시하거나 숨기도록 Alert Detail 목록이 전환됩니다.

자세한 내용은 다음 절을 참조하십시오.

- 68-3페이지의 상태 모듈 이해
- 68-41페이지의 상태 모니터 상태 해석
- 68-43페이지의 상태별 알림 보기
- 68-43페이지의 어플라이언스에 대해 모든 모듈 실행
- 68-44페이지의 특정 상태 모듈 실행

- 68-45페이지의 상태 모듈 알림 그래프 생성
- 68-46페이지의 문제 해결을 위해 상태 모니터 사용

상태별 알림 보기

라이센스: 모두

상태별 알림의 카테고리를 표시하거나 숨길 수 있습니다.

상태별 알림을 표시하려면

액세스: Admin/Maint/Any Security Analyst

1단계 보려는 알림의 상태에 해당하는 원 그래프에서 상태 아이콘 또는 색상 세그먼트를 클릭합니다. 해당 카테고리의 알림이 Alert Detail 목록에 나타납니다.

상태별 알림을 숨기려면

액세스: Admin/Maint/Any Security Analyst

1단계 보려는 알림의 상태에 해당하는 원 그래프에서 상태 아이콘 또는 색상 세그먼트를 클릭합니다. 해당 카테고리에 대한 Alert Detail 목록의 알림이 사라집니다.

어플라이언스에 대해 모든 모듈 실행

라이센스: 모두

상태 모듈 테스트는 상태 정책을 생성할 때 구성하는 정책 실행 시간 간격으로 자동 실행됩니다. 그러나 어플라이언스에 대한 최신 상태 정보를 수집하기 위해 온디맨드 방식으로 모든 상태 모듈 테스트를 실행할 수도 있습니다.

어플라이언스에 대한 모든 상태 모듈을 실행하려면

액세스: Admin/Maint/Any Security Analyst

1단계 **Health > Health Monitor**를 선택합니다.

Health Monitor 페이지가 나타납니다.

2단계 어플라이언스 목록을 확장하여 특정 상태의 어플라이언스를 표시하려면 해당 상태 열의 화살표를 클릭합니다.

팁 상태 레벨에 대한 행의 화살표가 아래쪽을 가리키면 해당 상태의 어플라이언스 목록은 아래쪽 테이블에 표시됩니다. 화살표가 오른쪽을 가리키면 어플라이언스 목록은 숨겨집니다.

3단계 어플라이언스 목록의 **Appliance** 열에서 세부사항을 표시할 어플라이언스의 이름을 클릭합니다.

Health Monitor Appliance 페이지가 나타납니다.

4단계 **Run All Modules**를 클릭합니다.

상태 표시줄에 테스트의 진행 상황이 표시되고, Health Monitor Appliance 페이지가 새로 고쳐집니다.

참고 상태 모듈을 수동으로 실행할 때, 자동으로 수행되는 첫 번째 새로 고침에서는 수동으로 실행한 테스트의 데이터가 반영되지 않을 수 있습니다. 방금 수동으로 실행한 모듈에 대한 값이 변경되지 않은 경우 잠시 기다렸다가 디바이스 이름을 클릭하여 페이지를 새로 고치십시오. 페이지의 자동 새로 고침이 다시 수행될 때까지 기다릴 수도 있습니다.

특정 상태 모듈 실행

라이센스: 모두

상태 모듈 테스트는 상태 정책을 생성할 때 구성하는 정책 실행 시간 간격으로 자동 실행됩니다. 그러나 모듈에 대한 최신 상태 정보를 수집하기 위해 온디맨드 방식으로 해당 상태 모듈 테스트를 실행할 수도 있습니다.

특정 상태 모듈을 실행하려면

액세스: Admin/Maint/Any Security Analyst

1단계 **Health > Health Monitor**를 선택합니다.

Health Monitor 페이지가 나타납니다.

2단계 어플라이언스 목록을 확장하여 특정 상태의 어플라이언스를 표시하려면 해당 상태 열의 화살표를 클릭합니다.

팁 상태 레벨에 대한 행의 화살표가 아래쪽을 가리키면 해당 상태의 어플라이언스 목록은 아래쪽 테이블에 표시됩니다. 화살표가 오른쪽을 가리키면 어플라이언스 목록은 숨겨집니다.

3단계 어플라이언스 목록의 **Appliance** 열에서 세부사항을 표시할 어플라이언스의 이름을 클릭합니다.

Health Monitor Appliance 페이지가 나타납니다.

4단계 Health Monitor Appliance 페이지의 **Module Status Summary** 그래프에서, 보려는 상태 알림 상태 카테고리의 색상을 클릭합니다.

Alert Detail 목록이 확장되면서 상태 카테고리에 대해 선택한 어플라이언스의 상태 알림이 나열됩니다.

5단계 이벤트 목록을 보려는 알림에 대한 **Alert Detail** 열에서 **Run**을 클릭합니다.

상태 표시줄에 테스트의 진행 상황이 표시되고, Health Monitor Appliance 페이지가 새로 고쳐집니다.

참고 상태 모듈을 수동으로 실행할 때, 자동으로 수행되는 첫 번째 새로 고침에서는 수동으로 실행한 테스트의 데이터가 반영되지 않을 수 있습니다. 방금 수동으로 실행한 모듈에 대한 값이 변경되지 않은 경우 잠시 기다렸다가 디바이스 이름을 클릭하여 페이지를 새로 고치십시오. 페이지의 자동 새로 고침이 다시 수행될 때까지 기다릴 수도 있습니다.

상태 모듈 알림 그래프 생성

라이센스: 모두

특정 어플라이언스에 대한 특별한 상태 테스트 기간 중에 발생한 결과를 그래프로 표시할 수 있습니다.

상태 모듈 알림 그래프를 생성하려면

액세스: Admin/Maint/Any Security Analyst

1단계 **Health > Health Monitor**를 선택합니다.

Health Monitor 페이지가 나타납니다.

2단계 어플라이언스 목록을 확장하여 특정 상태의 어플라이언스를 표시하려면 해당 상태 열의 화살표를 클릭합니다.

팁 상태 레벨에 대한 행의 화살표가 아래쪽을 가리키면 해당 상태의 어플라이언스 목록은 아래쪽 테이블에 표시됩니다. 화살표가 오른쪽을 가리키면 어플라이언스 목록은 숨겨집니다.

3단계 어플라이언스 목록의 **Appliance** 열에서 세부사항을 표시할 어플라이언스의 이름을 클릭합니다.

Health Monitor Appliance 페이지가 나타납니다.

4단계 Health Monitor Appliance 페이지의 **Module Status Summary** 그래프에서, 보려는 상태 알림 상태 카테고리의 색상을 클릭합니다.

Alert Detail 목록이 확장되면서 상태 카테고리에 대해 선택한 어플라이언스의 상태 알림이 나열됩니다.

5단계 이벤트 목록을 보려는 알림에 대한 **Alert Detail** 열에서 **Graph**를 클릭합니다.

시간에 따른 이벤트의 상태를 보여주는 그래프가 나타납니다. 그래프 아래의 Alert Detail 섹션에는 선택한 어플라이언스에 대한 모든 상태 알림이 나열됩니다.

팁 이벤트가 나타나지 않으면 시간 범위를 조정해야 할 수 있습니다. 자세한 내용은 58-22페이지의 이벤트 시간 제약 조건 설정을/를 참조하십시오.

문제 해결을 위해 상태 모니터 사용

라이센스: 모두

경우에 따라, 어플라이언스에 문제가 있으면 고객 지원에서 문제 분석에 사용할 수 있도록 문재 해결 파일을 생성해달라고 요청할 수 있습니다. 상태 모니터가 보고하는 문제 해결 데이터를 사용자 지정하기 위해 다음 표에 나열된 옵션 중에서 선택할 수 있습니다.

표 68-7 선택 가능한 문제 해결 옵션

옵션	보고 내용
Snort Performance and Configuration	어플라이언스의 Snort와 관련된 데이터 및 컨피그레이션 설정
Hardware Performance and Logs	어플라이언스 하드웨어의 성능과 관련된 데이터 및 로그
System Configuration, Policy, and Logs	어플라이언스의 현재 시스템 컨피그레이션과 관련된 컨피그레이션 설정, 데이터 및 로그
Detection Configuration, Policy, and Logs	어플라이언스에서의 탐지와 관련된 컨피그레이션 설정, 데이터 및 로그
Interface and Network Related Data	어플라이언스의 인라인 집합 및 네트워크 컨피그레이션과 관련된 컨피그레이션 설정, 데이터 및 로그
Discovery, Awareness, VDB Data, and Logs	어플라이언스의 현재 검색 및 인식 컨피그레이션과 관련된 컨피그레이션 설정, 데이터 및 로그
Upgrade Data and Logs	어플라이언스의 이전 업그레이드와 관련된 데이터 및 로그
All Database Data	문제 해결 보고서에 포함된 모든 데이터베이스 관련 데이터
All Log Data	어플라이언스 데이터베이스에 의해 수집된 모든 로그
Network Map Information	현재 네트워크 토폴로지 데이터

일부 옵션은 보고하는 데이터 관점에서 중복되지만, 사용자가 선택하는 옵션과 상관없이 문제 해결 파일에는 중복된 사본이 포함되지 않습니다.

자세한 내용은 다음 절을 참조하십시오.

- 68-46페이지의 어플라이언스 문제 해결 파일 생성
- 68-47페이지의 문제 해결 파일 다운로드

어플라이언스 문제 해결 파일 생성

라이센스: 모두

고객 지원에 보낼 사용자 지정된 문제 해결 파일을 생성하려면 다음 절차를 사용합니다.

참고 고가용성 컨피그레이션의 주 방어 센터를 사용하여 보조 방어 센터용 문제 해결 파일을 생성할 수 **없으며**, 그 반대의 경우도 마찬가지입니다. 방어 센터에 대한 문제 해결 파일은 자체 웹 인터페이스에서 생성해야 합니다.

문제 해결 파일을 생성하려면

액세스: Admin/Maint/Any Security Analyst

1단계 **Health > Health Monitor**를 선택합니다.

Health Monitor 페이지가 나타납니다.

2단계 어플라이언스 목록을 확장하여 특정 상태의 어플라이언스를 표시하려면 해당 상태 열의 화살표를 클릭합니다.

팁 상태 레벨에 대한 행의 화살표가 아래쪽을 가리키면 해당 상태의 어플라이언스 목록은 아래쪽 테이블에 표시됩니다. 화살표가 오른쪽을 가리키면 어플라이언스 목록은 숨겨집니다.

3단계 어플라이언스 목록의 **Appliance** 열에서 세부사항을 표시할 어플라이언스의 이름을 클릭합니다.

Health Monitor Appliance 페이지가 나타납니다.

4단계 **Generate Troubleshooting Files**를 클릭합니다.

Troubleshooting Options 팝업 창이 나타납니다.

5단계 가능한 모든 문제 해결 데이터를 생성하려면 **All Data**를 선택합니다. 또는 개별 확인란을 선택하여 보고서를 사용자 지정할 수도 있습니다. 자세한 내용은 선택 가능한 문제 해결 옵션 표를 참조하십시오.

6단계 **OK**를 클릭합니다.

방어 센터는 문제 해결 파일을 생성합니다. 작업 대기열에서 파일 생성 프로세스를 모니터링할 수 있습니다(**System > Monitoring > Task Status**).

7단계 다음 절, 문제 해결 파일 다운로드에서 절차를 계속 진행합니다.

문제 해결 파일 다운로드

라이센스: 모두

생성된 문제 해결 파일의 사본을 다운로드하려면 다음 절차를 사용합니다.

문제 해결 파일을 다운로드하려면

액세스: Admin/Maint/Any Security Analyst

1단계 **System > Monitoring > Task Status**를 선택합니다.

Task Status 페이지가 나타납니다.

2단계 생성한 문제 해결 파일에 해당하는 작업을 찾습니다.

3단계 어플라이언스가 문제 해결 파일을 생성하고 작업 상태가 `Completed`로 바뀌면 **Click to retrieve generated files**를 클릭합니다.

4단계 브라우저의 프롬프트에 따라 파일을 다운로드합니다.

여러 파일이 단일 `.tar.gz` 파일로 다운로드됩니다.

5단계 고객 지원의 안내에 따라 문제 해결 파일을 Cisco로 전송합니다.

상태 이벤트 작업

라이센스: 모두

방어 센터는 상태 모니터에서 수집한 상태 이벤트를 빠르고 쉽게 분석할 수 있는 완전히 사용자 지정 가능한 이벤트 보기를 제공합니다. 이러한 이벤트 보기에서는 이벤트 데이터를 검색하고 볼 수 있으며, 조사 중인 이벤트와 관련이 있을 수 있는 다른 정보에 손쉽게 액세스할 수 있습니다.

상태 이벤트 보기 페이지에서 수행할 수 있는 많은 기능은 여러 이벤트 보기 페이지에서도 일관되게 수행할 수 있습니다. 이러한 공통된 절차에 대한 자세한 내용은 68-48페이지의 상태 이벤트 보기 이해을/를 참조하십시오.

Health > Health Events 메뉴 옵션에서 상태 이벤트를 볼 수 있으며 특정 이벤트를 검색할 수도 있습니다.

이벤트 보기에 대한 자세한 내용은 다음 절을 참조하십시오.

- 68-48페이지의 상태 이벤트 보기 이해 - FireSIGHT에서 생성하는 이벤트 유형에 대해 설명합니다.
- 68-48페이지의 상태 이벤트 보기 - Event View 페이지에 액세스하고 이 페이지를 사용하는 방법에 대해 설명합니다.
- 68-54페이지의 상태 이벤트 검색 - Event Search 페이지를 사용하여 특정 이벤트를 검색하는 방법에 대해 설명합니다.

상태 이벤트 보기 이해

라이센스: 모두

방어 센터 상태 모니터는 Health Event View 페이지에서 볼 수 있는 상태 이벤트를 로깅합니다. 각 상태 모듈이 테스트하는 조건을 이해하면 상태 이벤트에 대한 알림을 좀 더 효과적으로 구성할 수 있습니다. 상태 이벤트를 생성하는 서로 다른 상태 모듈 유형에 대한 자세한 내용은 68-3페이지의 상태 모듈 이해을/를 참조하십시오.

상태 이벤트 보기 및 검색에 대한 자세한 내용은 다음 절을 참조하십시오.

- 68-48페이지의 상태 이벤트 보기
- 68-53페이지의 상태 이벤트 테이블 이해
- 68-54페이지의 상태 이벤트 검색

상태 이벤트 보기

라이센스: 모두

상태 모니터에 의해 수집되는 어플라이언스 상태 데이터를 여러 방법으로 모니터링할 수 있습니다.

자세한 내용은 다음 항목을 참조하십시오.

- 68-49페이지의 모든 상태 이벤트 보기
- 68-49페이지의 모듈 및 어플라이언스별로 상태 이벤트 보기
- 68-50페이지의 Health Events 테이블 보기 작업
- 68-51페이지의 3D9900 디바이스에 대한 하드웨어 알림 세부사항 해석
- 68-52페이지의 Series 3 디바이스에 대한 하드웨어 알림 세부사항 해석

모든 상태 이벤트 보기

라이센스: 모두

Health Events 페이지의 테이블 보기에는 선택한 어플라이언스의 모든 상태 이벤트가 나열됩니다. 이 페이지에 표시될 수 있는 이벤트를 생성한 상태 모듈에 대한 설명은 68-3페이지의 상태 모듈 이해을/를 참조하십시오.

방어 센터의 Health Monitor 페이지에서 상태 이벤트에 액세스하면 모든 관리되는 어플라이언스에 대한 모든 상태 이벤트가 검색됩니다.

모든 관리되는 어플라이언스에서 모든 상태 이벤트를 보려면

액세스: Admin/Maint/Any Security Analyst

1단계 **Health > Health Events**를 선택합니다.

모든 상태 이벤트가 포함된 Events 페이지가 나타납니다.

참고 이벤트가 나타나지 않으면 시간 범위를 조정해야 할 수 있습니다. 자세한 내용은 58-22페이지의 이벤트 시간 제약 조건 설정을/를 참조하십시오.

팁 Health Events 테이블이 포함된 상태 이벤트 워크플로의 페이지로 돌아가려면 이 보기에 북마크를 지정할 수 있습니다. 북마크 지정된 보기는 현재 보고 있는 시간 범위 내에서 이벤트를 검색하지만, 필요한 경우 시간 범위를 수정하여 좀 더 최신 정보로 테이블을 업데이트할 수 있습니다. 자세한 내용은 58-22페이지의 이벤트 시간 제약 조건 설정을/를 참조하십시오.

모듈 및 어플라이언스별로 상태 이벤트 보기

라이센스: 모두

특정 어플라이언스에서 특정 상태 모듈에 의해 생성된 이벤트를 쿼리할 수 있습니다.

특정 모듈에 대한 상태 이벤트를 보려면

액세스: Admin/Maint/Any Security Analyst

1단계 **Health > Health Monitor**를 선택합니다.

Health Monitor 페이지가 나타납니다.

2단계 어플라이언스 목록을 확장하여 특정 상태의 어플라이언스를 표시하려면 해당 상태 열의 화살표를 클릭합니다.

팁 상태 레벨에 대한 행의 화살표가 아래쪽을 가리키면 해당 상태의 어플라이언스 목록은 아래쪽 테이블에 표시됩니다. 화살표가 오른쪽을 가리키면 어플라이언스 목록은 숨겨집니다.

3단계 어플라이언스 목록의 Appliance 열에서 세부사항을 표시할 어플라이언스의 이름을 클릭합니다.

Health Monitor Appliance 페이지가 나타납니다.

4단계 Health Monitor Appliance 페이지의 **Module Status Summary** 그래프에서, 보려는 상태 알림 상태 카테고리의 색상을 클릭합니다.

Alert Detail 목록이 확장되면서 상태 카테고리에 대해 선택한 어플라이언스의 상태 알림이 나열됩니다.

5단계 이벤트 목록을 보려는 알림에 대한 Alert Detail 열에서 **Events**를 클릭합니다.

어플라이언스의 이름 및 제약 조건으로써 선택한 상태 알림 모듈의 이름과 함께 쿼리에 대한 쿼리 결과가 포함된 Health Events 페이지가 나타납니다.

이벤트가 나타나지 않으면 시간 범위를 조정해야 할 수 있습니다. 자세한 내용은 58-22페이지의 이벤트 시간 제약 조건 설정을/를 참조하십시오.

6단계 선택한 어플라이언스에 대한 모든 상태 이벤트를 보려면 **Search Constraints**를 확장하고 **Module Name** 제약 조건을 클릭하여 제거합니다.

Health Events 테이블 보기 작업

라이센스: 모두

다음 표에서는 Event View 페이지에서 수행할 수 있는 각 작업에 대해 설명합니다.

표 68-8 상태 이벤트 보기 기능

목적	가능한 작업
상태 이벤트 보기에 나타나는 열의 내용에 대해 자세히 알아보기	68-53페이지의 상태 이벤트 테이블 이해에서 자세히 알아보십시오.
상태 테이블 보기에 나열된 이벤트의 시간 및 날짜 범위 수정	58-22페이지의 이벤트 시간 제약 조건 설정에서 자세히 알아보십시오. 어플라이언스의 구성된 시간 창(전역이든 이벤트 전용이든)을 벗어나 생성된 이벤트는 시간 기준으로 이벤트 보기를 제한할 경우 이벤트 보기에 나타날 수 있습니다. 이는 어플라이언스에 대한 슬라이딩 시간 창을 구성한 경우에도 발생할 수 있습니다.
나타나는 이벤트 정렬, 이벤트 테이블에 표시되는 열 변경, 나타나는 이벤트 제한	58-34페이지의 드릴다운 워크플로 페이지 정렬에서 자세히 알아보십시오.
상태 이벤트 삭제	삭제할 이벤트 옆에 있는 확인란을 선택하고 **Delete**를 클릭합니다. 현재 제한된 보기에서 모든 이벤트를 삭제하려면 **Delete All**을 클릭하고 모든 이벤트를 삭제할 것인지를 확인합니다.
이벤트 보기 페이지 탐색	58-35페이지의 워크플로의 다른 페이지로 이동에서 자세히 알아보십시오.
관련 이벤트를 보기 위해 다른 이벤트 테이블로 이동	58-35페이지의 워크플로 간 이동에서 자세히 알아보십시오.
신속하게 다시 돌아올 수 있도록 현재 페이지 북마크 지정	**Bookmark This Page**를 클릭하고 북마크의 이름을 입력하고 **Save**를 클릭합니다. 자세한 내용은 58-36페이지의 북마크 사용을/를 참조하십시오.
북마크 관리 페이지로 이동	임의의 이벤트 보기에서 **View Bookmarks**를 클릭합니다. 자세한 내용은 58-36페이지의 북마크 사용을/를 참조하십시오.
테이블 보기의 데이터를 기반으로 보고서 생성	**Report Designer**를 클릭합니다. 자세한 내용은 57-9페이지의 이벤트 보기에서 보고서 템플릿 생성을/를 참조하십시오.

표 68-8 상태 이벤트 보기 기능 (계속)

목적	가능한 작업
또 다른 상태 이벤트 워크플로 선택	**(switch workflow)**를 클릭합니다. 자세한 내용은 58-16페이지의 워크플로 선택을/를 참조하십시오.
단일 상태 이벤트와 관련된 세부사항 보기	이벤트의 왼쪽에 있는 아래쪽 화살표 링크를 클릭합니다.
여러 상태 이벤트의 이벤트 세부사항 보기	세부사항을 볼 이벤트에 해당하는 행의 옆에 있는 확인란을 선택하고 **View**를 클릭합니다.
보기의 모든 이벤트에 대한 이벤트 세부사항 보기	**View All**을 클릭합니다.
특정 상태의 모든 이벤트 보기	해당 상태의 이벤트에 대한 Status 열에서 상태 아이콘을 클릭합니다.

3D9900 디바이스에 대한 하드웨어 알림 세부사항 해석

라이센스: 모두

3D9900 디바이스 모델의 경우, 다음 표에 설명된 대로 이벤트에 대한 반응으로 하드웨어 알람이 생성됩니다. 알림에 대한 메시지 세부사항에서 트리거링 조건을 찾을 수 있습니다.

표 68-9 3D9900 디바이스에 대해 모니터링되는 조건

모니터링된 상태	노란색 또는 빨간색 오류 조건의 원인
NFE 카드 프레즌스	어플라이언스에 대해 유효하지 않은 NFE 하드웨어가 탐지되면 Hardware Alarms 모듈에 대한 상태가 빨간색으로 변경되고 메시지 세부사항에 NFE 카드 프레즌스에 대한 참조가 포함됩니다.
NFE 온도	NFE 온도가 섭씨 35도(화씨 95도)를 넘으면 Hardware Alarms 모듈의 상태가 노란색으로 변경되고 메시지 세부사항에 NFE 온도에 대한 참조가 포함됩니다. NFE 온도가 섭씨 37.3도(화씨 99도)를 넘으면 Hardware Alarms 모듈의 상태가 빨간색으로 변경되고 메시지 세부사항에 NFE 온도에 대한 참조가 포함됩니다.
NFE Platform 디먼	NFE Platform 디먼이 다운되면 Hardware Alarms 모듈의 상태가 빨간색으로 변경되고 메시지 세부사항에 디먼에 대한 참조가 포함됩니다.
NFE Message 디먼	NFE Message 디먼이 다운되면 Hardware Alarms 모듈의 상태가 빨간색으로 변경되고 메시지 세부사항에 디먼에 대한 참조가 포함됩니다.
NFE `TCAM` 디먼	NFE `TCAM` 디먼이 다운되면 Hardware Alarms 모듈의 상태가 빨간색으로 변경되고 메시지 세부사항에 디먼에 대한 참조가 포함됩니다.
LBIM 프레즌스	LBIM(Load Balancing Interface Module) 스위치 어셈블리가 없거나 통신하지 않으면 Hardware Alarms 모듈의 상태가 빨간색으로 변경되고 메시지 세부사항에 LBIM 프레즌스에 대한 참조가 포함됩니다.
`Scmd` 디먼	`Scmd` 디먼이 다운되면 Hardware Alarms 모듈의 상태가 빨간색으로 변경되고 메시지 세부사항에 디먼에 대한 참조가 포함됩니다.
`Psls` 디먼	`Psls` 디먼이 다운되면 Hardware Alarms 모듈의 상태가 빨간색으로 변경되고 메시지 세부사항에 디먼에 대한 참조가 포함됩니다.

표 68-9 3D9900 디바이스에 대해 모니터링되는 조건 (계속)

모니터링된 상태	노란색 또는 빨간색 오류 조건의 원인
Ftwo 디먼	Ftwo 디먼이 다운되면 Hardware Alarms 모듈의 상태가 빨간색으로 변경되고 메시지 세부사항에 디먼에 대한 참조가 포함됩니다.
Rulesd(호스트 규칙) 디먼	Rulesd 디먼이 다운되면 Hardware Alarms 모듈의 상태가 노란색으로 변경되고 메시지 세부사항에 디먼에 대한 참조가 포함됩니다.
nfm_ipfragd(호스트 플래그) 디먼	nfm_ipfragd 디먼이 다운되면 Hardware Alarms 모듈의 상태가 빨간색으로 변경되고 메시지 세부사항에 디먼에 대한 참조가 포함됩니다.

Series 3 디바이스에 대한 하드웨어 알림 세부사항 해석

Series 3 디바이스의 경우, 다음 표에 설명된 대로 이벤트에 대한 반응으로 하드웨어 알람이 생성됩니다. 알림에 대한 메시지 세부사항에 트리거링 조건이 나타납니다.

표 68-10 Series 3 디바이스에 대해 모니터링되는 조건

모니터링된 상태	노란색 또는 빨간색 오류 조건의 원인
클러스터 상태	클러스터링된 디바이스가 테이블 문제 등으로 인해 더 이상 상호 통신할 수 없으면 Hardware Alarms 모듈이 빨간색으로 변경됩니다.
ftwo 디먼 상태	ftwo 디먼이 다운되면 Hardware Alarms 모듈의 상태가 빨간색으로 변경되고 메시지 세부사항에 디먼에 대한 참조가 포함됩니다.
NFE 카드 탐지됨	시스템에서 탐지된 NFE 카드의 수를 나타냅니다. 이 값이 어플라이언스의 예상 NFE 카운트와 일치하지 않으면 Hardware Alarms 모듈이 빨간색으로 변경됩니다.
NFE 하드웨어 상태	하나 이상의 NFE 카드가 통신하지 않으면 Hardware Alarms 모듈은 빨간색으로 변경되고 메시지 세부사항에 해당 카드가 나타납니다.
NFE 하트비트	시스템이 NFE 하트비트를 탐지하면 Hardware Alarms 모듈이 빨간색으로 변경되고 메시지 세부사항에 관련 카드에 대한 참조가 포함됩니다.
NFE 내부 링크 상태	NMSB 및 NFE 카드 간 링크가 다운되면 Hardware Alarms 모듈이 빨간색으로 변경되고 메시지 세부사항에 관련 포트에 대한 참조가 포함됩니다.
NFE Message 디먼	NFE Message 디먼이 다운되면 Hardware Alarms 모듈의 상태가 빨간색으로 변경되고 메시지 세부사항에 디먼에 대한 참조(그리고 해당되는 경우 NFE 카드 번호)가 포함됩니다.
NFE 온도	NFE 온도가 섭씨 36.2도(화씨 97도)를 넘으면 Hardware Alarms 모듈의 상태가 노란색으로 변경되고 메시지 세부사항에 NFE 온도에 대한 참조(그리고 해당되는 경우 NFE 카드 번호)가 포함됩니다. NFE 온도가 섭씨 38.9도(화씨 102도)를 넘으면 Hardware Alarms 모듈의 상태가 빨간색으로 변경되고 메시지 세부사항에 NFE 온도에 대한 참조(그리고 해당되는 경우 NFE 카드 번호)가 포함됩니다.

표 68-10 Series 3 디바이스에 대해 모니터링되는 조건 (계속)

모니터링된 상태	노란색 또는 빨간색 오류 조건의 원인
NFE 온도 상태	특정 NFE 카드의 현재 온도 상태를 나타냅니다. Hardware Alarms 모듈은 OK에 녹색, Warning에 노란색, Critical에 빨간색을 나타냅니다(그리고 해당되는 경우 NFE 카드 번호).
NFE TCAM 디먼	NFE TCAM 디먼이 다운되면 Hardware Alarms 모듈의 상태가 빨간색으로 변경되고 메시지 세부사항에 디먼에 대한 참조(그리고 해당되는 경우 NFE 카드 번호)가 포함됩니다.
nfm_ipfragd(호스트 플래그) 디먼	nfm_ipfragd 디먼이 다운되면 Hardware Alarms 모듈의 상태가 빨간색으로 변경되고 메시지 세부사항에 디먼에 대한 참조(그리고 해당되는 경우 NFE 카드 번호)가 포함됩니다.
NFE Platform 디먼	NFE Platform 디먼이 다운되면 Hardware Alarms 모듈의 상태가 빨간색으로 변경NFE Platform되고 메시지 세부사항에 디먼에 대한 참조(그리고 해당되는 경우 NFE 카드 번호)가 포함됩니다.
NMSB 커뮤니케이션	Media 어셈블리가 없거나 통신하지 않으면 Hardware Alarms 모듈의 상태가 빨간색으로 변경되고 메시지 세부사항에 NFE 온도에 대한 참조(그리고 해당되는 경우 NFE 카드 번호)가 포함됩니다.
psls 디먼 상태	psls 디먼이 다운되면 Hardware Alarms 모듈의 상태가 빨간색으로 변경되고 메시지 세부사항에 디먼에 대한 참조가 포함됩니다.
Rulesd(호스트 규칙) 디먼	Rulesd 디먼이 다운되면 Hardware Alarms 모듈의 상태가 노란색으로 변경되고 메시지 세부사항에 디먼에 대한 참조(그리고 해당되는 경우 NFE 카드 번호)가 포함됩니다.
scmd 디먼 상태	scmd 디먼이 다운되면 Hardware Alarms 모듈의 상태가 빨간색으로 변경되고 메시지 세부사항에 디먼에 대한 참조가 포함됩니다.

상태 이벤트 테이블 이해

라이센스: 모두

방어 센터의 상태 모니터를 사용하면 FireSIGHT 시스템 내에서 중요한 기능의 상태를 확인할 수 있습니다. 상태 정책을 생성하여 어플라이언스에 적용하면, 하드웨어와 소프트웨어 상태를 비롯한 다양한 부분을 모니터링하게 됩니다. 상태 정책에서 활성화하기 위해 선택하는 Health Monitor 모듈은 다양한 테스트를 실행하여 어플라이언스 상태를 결정합니다. 상태가 지정된 기준을 충족하면 상태 이벤트가 생성됩니다. 상태 모니터링에 대한 자세한 내용은 67-1페이지의 시스템 모니터링을/를 참조하십시오.

다음 표에서는 상태 이벤트 테이블의 필드에 대해 설명합니다.

표 68-11 상태 이벤트 필드

필드	설명
Test Name	이벤트를 생성한 상태 모듈의 이름. 상태 모듈의 목록은 상태 모듈 표를 참조하십시오.
Time	상태 이벤트의 타임스탬프.
설명	이벤트를 생성한 상태 모듈의 설명. 예를 들어 프로세스를 실행할 수 없을 때 생성되는 상태 이벤트에는 Unable to Execute라는 레이블이 지정됩니다.

표 68-11 상태 이벤트 필드 (계속)

필드	설명
가치	이벤트를 생성한 상태 테스트에서 얻은 결과의 값(단위의 수). 예를 들어 방어 센터에서 모니터링 중인 디바이스가 CPU 리소스의 80% 이상을 사용할 때마다 상태 이벤트가 생성된다면 값은 80~100의 숫자가 될 수 있습니다.
Units	결과의 단위 설명자. 와일드카드 검색을 생성하려면 별표(*)를 사용할 수 있습니다. 예를 들어 방어 센터에서 모니터링 중인 디바이스가 CPU 리소스의 80% 이상을 사용할 때 상태 이벤트가 생성된다면 단위 설명자는 퍼센트 기호(%)입니다.
상태	어플라이언스에 대해 보고된 상태(Critical, Yellow, Green 또는 Disabled).
디바이스	상태 이벤트가 보고된 어플라이언스.

상태 이벤트의 테이블 보기를 표시하려면

액세스: Admin/Maint/Any Security Analyst

1단계 **Health > Health Events**를 선택합니다.

테이블 보기가 나타납니다. 상태 이벤트 작업에 대한 자세한 내용은 68-48페이지의 상태 이벤트 작업을/를 참조하십시오.

팁 상태 이벤트의 테이블 보기가 포함되지 않은 사용자 지정 워크플로를 사용 중인 경우 **(switch workflow)**를 클릭하십시오. Select Workflow 페이지에서 **Health Events**를 클릭하십시오.

상태 이벤트 검색

라이센스: 모두

특정 상태 이벤트를 검색할 수 있습니다. 네트워크 환경에 맞춤화된 검색을 생성한 다음 나중에 다시 사용할 수 있도록 저장할 수 있습니다. 다음 표에는 사용할 수 있는 검색 기준이 설명되어 있습니다.

표 68-12 상태 이벤트 검색 기준

검색 필드	설명
Module Name	보려는 상태 이벤트를 생성한 모듈의 이름을 지정합니다. 예를 들어 CPU 성능을 측정하는 이벤트를 보려면 CPU를 입력합니다. 그러면 해당 CPU Usage 및 CPU 온도 이벤트가 검색됩니다.
가치	보려는 이벤트에 대한 상태 테스트에서 얻은 결과의 값(단위의 수)을 지정합니다. 예를 들어 값 15를 지정하고 Units 필드에 CPU를 입력하면 테스트 실행 시 어플라이언스 CPU가 15% 활용률로 실행되던 이벤트가 검색됩니다.

표 68-12 상태 이벤트 검색 기준

검색 필드	설명
설명	보려는 이벤트의 설명을 지정합니다. 예를 들어 프로세스를 실행할 수 없었던 상태 이벤트를 보려면 `Unable to Execute`를 입력합니다. 와일드카드 검색을 생성하려면 이 필드에 별표(*)를 사용할 수 있습니다.
Units	보려는 이벤트에 대한 상태 테스트에서 얻은 결과의 단위 설명자를 지정합니다. 와일드카드 검색을 생성하려면 이 필드에 별표(*)를 사용할 수 있습니다. 예를 들어 Units 필드에 `%`를 입력하면, Disk Usage 모듈의 Units 필드에는 "%" 레이블이 있고 추가 텍스트가 없으므로 Disk Usage 모듈에 대한 모든 이벤트가 검색됩니다. 그러나 Units 필드에 `*%`를 입력하면 Units 필드에서 "%" 기호 앞에 텍스트가 포함된 모듈에 대한 모든 이벤트가 검색됩니다.
상태	보려는 상태 이벤트에 대한 상태를 지정합니다. 유효한 상태 레벨은 Critical, Warning, Normal, Error 및 Disabled입니다. 예를 들어 Critical 상태를 나타내는 모든 상태 이벤트를 검색하려면 `Critical`을 입력합니다.
디바이스	하나 이상의 특정 디바이스에 의해 생성된 상태 이벤트로 검색을 제한하려면 디바이스 이름이나 IP 주소, 디바이스 그룹, 스택 또는 클러스터 이름을 입력합니다. FireSIGHT 시스템에서 검색 시 디바이스 필드를 처리하는 방법에 대한 자세한 내용은 60-7페이지의 검색에서 디바이스 지정을/를 참조하십시오.

특수 검색 구문, 검색 저장과 로드에 대한 정보 등 검색에 대한 자세한 내용은 60-1페이지의 검색 수행 및 저장을/를 참조하십시오.

상태 이벤트를 검색하려면

액세스: Admin/Maint/Any Security Analyst

1단계 **Analysis > Search**를 선택합니다.

Search 페이지가 나타납니다.

2단계 테이블 드롭다운 목록에서 **Health Events**를 선택합니다.

해당 제약 조건으로 페이지가 업데이트됩니다.

3단계 상태 이벤트 검색 기준 표에 설명된 대로 해당 필드에 검색 기준을 입력합니다.

여러 기준을 입력하면 모든 기준과 일치하는 레코드만 반환됩니다.

4단계 선택적으로, 검색을 저장하려면 Private 확인란을 선택하여 자신만 액세스할 수 있는 비공개로 검색을 저장할 수 있습니다. 또는 모든 사용자가 사용할 수 있도록 검색을 저장하려면 확인란을 선택하지 않습니다.

팁 사용자 지정 사용자 역할에 대한 데이터 제한으로서 검색을 사용하려면 **반드시** 비공개 검색으로 저장해야 합니다.

5단계 선택적으로, 나중에 다시 사용할 수 있도록 검색을 저장할 수 있습니다. 다음 옵션을 이용할 수 있습니다.

- 검색 기준을 저장하려면 **Save**를 클릭합니다.

  새 검색인 경우 검색 이름을 입력하도록 대화 상자가 나타납니다. 고유한 검색 이름을 입력하고 **Save**를 클릭합니다. 이미 존재하는 검색에 대한 새 조건을 저장하는 경우 프롬프트가 나타나지 않습니다. 나중에 실행할 수 있도록 검색이 저장됩니다(**Private**을 선택한 경우 자신만 볼 수 있음).

- 새 검색을 저장하거나, 저장된 기존 검색을 변경하여 만든 검색에 새 이름을 할당하려면 **Save As New**를 클릭합니다.

  검색 이름을 입력하도록 대화 상자가 나타납니다. 고유한 검색 이름을 입력하고 **Save**를 클릭합니다. 나중에 실행할 수 있도록 검색이 저장됩니다(**Private**을 선택한 경우 자신만 볼 수 있음).

6단계 검색을 시작하려면 **Search**를 클릭합니다.

검색 결과는 현재의 시간 범위로 제한되어 기본 상태 이벤트 워크플로에 나타납니다. 사용자 지정 워크플로를 비롯한 다른 워크플로를 사용하려면 **(switch workflow)**를 클릭합니다. 다른 기본 워크플로 지정에 대한 자세한 내용은 71-3페이지의 이벤트 보기 설정 구성을/를 참조하십시오.

69장 시스템 감사

시스템 활동에 대한 감사를 두 가지 방법으로 수행할 수 있습니다. FireSIGHT 시스템에 속하는 어플라이언스에서는 사용자와 웹 인터페이스의 각 상호 작용에 대한 감사 기록을 생성하며, 시스템 로그에 시스템 상태 메시지도 기록합니다.

다음 절에서는 시스템에서 제공하는 모니터링 기능에 대해 자세히 설명합니다.

- 69-1페이지의 감사 레코드 관리에서는 시스템 감사 정보를 보고 관리하는 방법에 대해 설명합니다.
- 69-10페이지의 시스템 로그 보기에서는 시스템 상태 메시지가 포함된 시스템 로그를 보는 방법에 대해 설명합니다.

팁 방어 센터와 보호 라이센스가 있는 관리되는 디바이스 역시 감사 데이터를 비롯하여 이벤트 보기에서 액세스할 수 있는 거의 모든 유형의 데이터에 대한 보고서를 생성할 수 있도록 완전한 보고 기능을 제공합니다. 자세한 내용은 57-1페이지의 보고서 작업을/를 참조하십시오.

감사 레코드 관리

라이센스: 모두

방어 센터 및 관리되는 디바이스는 사용자 활동에 대한 읽기 전용 감사 정보를 로깅합니다. 감사 로그는 감사 보기의 특정 항목을 기준으로 감사 로그 메시지를 필터링하고 정렬하고 볼 수 있는 표준 이벤트 보기에서 제공됩니다. 감사 정보를 손쉽게 삭제하고 보고할 수 있으며, 사용자가 변경한 내용에 대한 자세한 보고서를 볼 수 있습니다.

감사 로그에는 최대 100,000개의 항목이 저장됩니다. 감사 로그 항목 수가 100,000개를 초과하면 어플라이언스는 데이터베이스에서 가장 오래된 기록을 삭제하여 항목 수를 100,000개로 줄입니다.

참고 Series 3 어플라이언스를 재부팅하고 가능한 한 빨리 CLI에 로그인하면, 웹 인터페이스를 사용할 수 있을 때까지 감사 로그에 실행한 명령이 기록되지 않습니다.

자세한 내용은 다음 절을 참조하십시오.

- 69-2페이지의 감사 레코드 보기
- 69-4페이지의 감사 레코드 억제
- 69-7페이지의 Audit Log 테이블 이해
- 69-7페이지의 변경 사항 검토를 위해 감사 로그 사용
- 69-8페이지의 감사 레코드 검색

감사 레코드 보기

라이센스: 모두

어플라이언스를 사용하여 감사 레코드의 테이블을 볼 수 있습니다. 그런 다음 찾고 있는 정보에 따라 보기를 조작할 수 있습니다. 사전 정의된 감사 워크플로에는 이벤트의 단일 테이블 보기가 포함되어 있습니다. 특정 요구와 일치하는 정보만 표시하는 사용자 지정 워크플로를 생성할 수도 있습니다. 사용자 지정 워크플로 생성에 대한 자세한 내용은 58-38페이지의 사용자 지정 워크플로 생성을/를 참조하십시오.

다음 표에서는 감사 로그 워크플로 페이지에서 수행할 수 있는 몇 가지 특정 작업에 대해 설명합니다.

표 69-1 Audit Log 작업

목적	가능한 작업
테이블에서 열의 내용에 대해 자세히 알아보기	69-7페이지의 Audit Log 테이블 이해에서 자세히 알아보십시오.
감사 레코드를 볼 때 사용되는 시간 범위 수정	58-22페이지의 이벤트 시간 제약 조건 설정에서 자세히 알아보십시오. 어플라이언스의 구성된 시간 창(전역이든 이벤트 전용이든)을 벗어나 생성된 이벤트는 시간 기준으로 이벤트 보기를 제한할 경우 이벤트 보기에 나타날 수 있습니다. 이는 어플라이언스에 대한 슬라이딩 시간 창을 구성한 경우에도 발생할 수 있습니다.
현재 워크플로 페이지에서 이벤트를 정렬 및 제한	58-33페이지의 표 보기 페이지 정렬 및 표 보기 페이지의 레이아웃 변경에서 자세히 알아보십시오.
현재 워크플로 페이지 내에서 이동	58-35페이지의 워크플로의 다른 페이지로 이동에서 자세히 알아보십시오.
현재의 제약 조건을 유지한 채 현재 워크플로에서 페이지 간 이동	워크플로 페이지의 왼쪽 위에서 적절한 페이지 링크를 클릭합니다. 자세한 내용은 58-18페이지의 워크플로 페이지 사용을/를 참조하십시오.
워크플로의 다음 페이지로 드릴다운	다음 방법 중 하나를 사용합니다. • 특정 값으로 제한하여 다음 워크플로 페이지로 드릴다운하려면 행 내의 값을 클릭합니다. 이 방법은 드릴다운 페이지에만 해당됩니다. 테이블 보기의 행 내에서 값을 클릭하면 테이블 보기가 제한되며 다음 페이지로 드릴다운되지 **않습니다**. • 일부 이벤트로 제한하여 다음 워크플로 페이지로 드릴다운하려면, 다음 워크플로 페이지에서 볼 이벤트의 옆에 있는 확인란을 선택하고 **View**를 클릭합니다. • 현재의 제약 조건을 유지한 채 다음 워크플로 페이지로 드릴다운하려면 **View All**을 클릭합니다. **팁** 테이블 보기의 페이지 이름에는 항상 "Table View"가 포함됩니다. 자세한 내용은 58-30페이지의 이벤트 제한을/를 참조하십시오.
특정 값으로 제한	행 내의 값을 클릭합니다. 드릴다운 페이지에서 값을 클릭하면 다음 페이지로 이동하며 해당 값으로 제한됩니다. 테이블 보기의 행 내에서 값을 클릭하면 테이블 보기가 제한되며 다음 페이지로 드릴다운되지 **않습니다**. **팁** 테이블 보기의 페이지 이름에는 항상 "Table View"가 포함됩니다. 자세한 내용은 58-30페이지의 이벤트 제한을/를 참조하십시오.

표 69-1 Audit Log 작업 (계속)

목적	가능한 작업
감사 레코드 삭제	다음 방법 중 하나를 사용합니다. • 일부 항목을 삭제하려면 삭제할 이벤트 옆에 있는 확인란을 선택하고 **Delete**를 클릭합니다. • 현재 제한된 보기에서 모든 항목을 삭제하려면 **Delete All**을 클릭하고 모든 이벤트를 삭제할 것인지를 확인합니다.
일시적으로 다른 워크플로 사용	**(switch workflow)**를 클릭합니다. 자세한 내용은 58-16페이지의 워크플로 선택을/를 참조하십시오.
신속하게 다시 돌아올 수 있도록 현재 페이지 북마크 지정	**Bookmark This Page**를 클릭합니다. 자세한 내용은 58-36페이지의 북마크 사용을/를 참조하십시오.
북마크 관리 페이지로 이동	**View Bookmarks**를 클릭합니다. 자세한 내용은 58-36페이지의 북마크 사용을/를 참조하십시오.
현재 보기의 데이터를 기반으로 보고서 생성	**Report Designer**를 클릭합니다. 자세한 내용은 57-9페이지의 이벤트 보기에서 보고서 템플릿 생성을/를 참조하십시오.
감사 로그에 기록된 변경 사항 요약 보기	**Message** 열의 해당 이벤트 옆에 있는 비교 아이콘( )을 클릭합니다. 자세한 내용은 69-7페이지의 변경 사항 검토를 위해 감사 로그 사용을/를 참조하십시오.

감사 레코드를 보려면

액세스: Admin

1단계 **System > Monitoring > Audit**를 선택합니다.

기본 감사 로그 워크플로의 첫 번째(유일한) 페이지가 나타납니다. 사용자 지정 워크플로를 비롯한 다른 워크플로를 사용하려면 **(switch workflow)**를 클릭합니다. 다른 기본 워크플로 지정에 대한 자세한 내용은 71-3페이지의 이벤트 보기 설정 구성을/를 참조하십시오. 이벤트가 나타나지 않으면 시간 범위를 조정해야 할 수 있습니다. 자세한 내용은 58-22페이지의 이벤트 시간 제약 조건 설정을/를 참조하십시오.

팁 감사 이벤트의 테이블 보기가 포함되지 않은 사용자 지정 워크플로를 사용 중인 경우 **(switch workflow)**를 클릭한 다음 **Audit Log**를 선택하십시오.

감사 이벤트 작업

라이센스: 모두

이벤트 보기의 레이아웃을 변경하거나, 보기의 이벤트를 필드 값으로 제한할 수 있습니다. 열이 비활성화된 경우, 나타나는 팝업 창에서 숨기고자 하는 열 머리글의 닫기 아이콘( )을 클릭한 다음 **Apply**를 클릭합니다. 열을 비활성화할 경우 (나중에 다시 추가하지 않는 한) 세션 기간 동안 비활성화됩니다. 첫 번째 열을 비활성화할 때 Count 열이 추가됩니다.

다른 열을 숨기거나 표시하려면, 또는 비활성화된 열을 다시 보기에 추가하려면, 해당 확인란을 선택하거나 선택 취소한 후 **Apply**를 클릭하십시오.

테이블 보기의 행 내에서 값을 클릭하면 테이블 보기가 제한되며 다음 페이지로 드릴다운되지 않습니다.

팁 테이블 보기의 페이지 이름에는 항상 "Table View"가 포함됩니다.

자세한 내용은 다음 항목을 참조하십시오.

- 58-30페이지의 이벤트 제한.
- 58-32페이지의 복합 제약 조건 사용
- 58-34페이지의 드릴다운 워크플로 페이지 정렬
- 69-7페이지의 Audit Log 테이블 이해

감사 레코드 억제

라이센스: 모두

감사 정책에서 FireSIGHT 시스템과의 특정 사용자 상호 작용 유형을 감사하도록 요구하지 않는 경우, 그러한 상호 작용에서 감사 레코드가 생성되는 것을 차단할 수 있습니다. 예를 들면, 기본적으로 사용자가 온라인 도움말을 볼 때마다 FireSIGHT 시스템은 감사 레코드를 생성합니다. 이러한 상호 작용 레코드를 유지할 필요가 없으면 자동으로 억제할 수 있습니다.

감사 이벤트 억제를 구성하려면 어플라이언스의 `admin` 사용자 계정에 액세스해야 하며, 어플라이언스의 콘솔에 액세스하거나 SSH(Secure Shell)를 열 수 있어야 합니다.

주의 권한이 있는 사용자만이 어플라이언스 및 `admin` 계정에 액세스할 수 있습니다.

감사 레코드를 억제하려면 `/etc/sf` 디렉토리에 다음 형식으로 하나 이상의 파일을 생성해야 합니다.

`AuditBlock.`*`type`*

여기서 *`type`*은 `address`, `message`, `subsystem` 또는 `user`입니다.

참고 특정 유형의 감사 메시지에 대해 `AuditBlock.`*`type`* 파일을 생성한 후 억제를 해제하려는 경우 `AuditBlock.`*`type`* 파일의 내용을 삭제하되 파일 자체는 FireSIGHT 시스템에 남겨두어야 합니다.

각 감사 블록 유형의 내용은 다음 표에 설명한 것처럼 특정 형식으로 지정해야 합니다. 파일 이름에 대/소문자를 정확하게 사용해야 합니다. 파일의 내용 역시 대/소문자를 구분합니다.

표 69-2 감사 블록 유형

유형	설명
주소	`AuditBlock.address` 파일을 생성하고, 감사 로그에서 억제하려는 각 IP 주소를 한 줄에 하나씩 포함합니다. 주소의 시작 부분부터 매핑되는 것이라면 부분적인 IP 주소를 사용할 수 있습니다. 예를 들어 부분 주소 `10.1.1`은 `10.1.1.0~10.1.1.255` 범위의 주소와 일치합니다.
메시지	`AuditBlock.message` 파일을 생성하고, 억제하려는 메시지 하위 문자열을 한 줄에 하나씩 포함합니다. 파일에 `backup`을 포함하면 `backup`이란 단어가 포함된 모든 메시지가 억제되는 방식으로 하위 문자열이 확인됩니다.

표 69-2 감사 블록 유형 (계속)

유형	설명
Subsystem	`AuditBlock.subsystem` 파일을 생성하고, 억제하려는 각 하위 시스템을 한 줄에 하나씩 포함합니다. 하위 문자열은 확인되지 **않습니다**. 정확한 문자열을 사용해야 합니다. 감사 대상 하위 시스템 목록은 하위 시스템 이름 표를 참조하십시오.
사용자	`AuditBlock.user` 파일을 생성하고, 억제하려는 각 사용자 계정을 한 줄에 하나씩 포함합니다. 사용자 이름의 시작 부분부터 매핑되는 것이라면 부분적인 문자열 매칭을 사용할 수 있습니다. 예를 들어 `IPSAnalyst`는 `IPSAnalyst1` 및 `IPSAnalyst2` 사용자 이름과 일치합니다.

`AuditBlock` 파일을 추가하면 `Audit` 하위 시스템과 `Audit Filter type Changed` 메시지의 감사 레코드가 감사 이벤트에 추가됩니다. 보안상의 이유로, 이 감사 레코드는 억제할 수 **없습니다**.

다음 표에는 감사 대상 하위 시스템이 나열되어 있습니다.

표 69-3 하위 시스템 이름

이름	사용자 상호 작용 포함 대상
관리자	시스템 및 액세스 컨피그레이션, 시간 동기화, 백업 및 복원, 디바이스 관리, 사용자 계정 관리, 예약 등의 관리 기능
경고	이메일, SNMP, syslog 알림 등의 알림 기능
Audit Log	감사 이벤트 보기
Audit Log Search	감사 이벤트 검색
명령행	명령줄 인터페이스
컨피그레이션	이메일 알림
COOP	운영 연속성 기능
날짜	이벤트 보기의 날짜 및 시간 범위
Default Subsystem	할당된 하위 시스템이 없는 옵션
Detection & Prevention Policy	침입 정책에 대한 메뉴 옵션
오류	시스템 레벨 오류
eStreamer	eStreamer 컨피그레이션
EULA	최종 사용자 라이센스 계약 검토
이벤트	침입 및 검색 이벤트 보기
Events Clipboard	침입 이벤트 클립보드
Events Reviewed	검토된 침입 이벤트
Events Search	모든 이벤트 검색
Failed to install rule update *rule_update_id*	규칙 업데이트 설치
헤더	사용자 로그인 후 사용자 인터페이스의 초기 표시
상태	상태 모니터링
Health Events	상태 모니터링 이벤트 보기
도움말	온라인 도움말

표 69-3 하위 시스템 이름 (계속)

이름	사용자 상호 작용 포함 대상
고가용성	고가용성 기능
IDS Impact Flag	영향 플래그 컨피그레이션
IDS Policy(IKE 정책)	침입 정책
IDSPolicy > *policy_name* > Appliance > *det_engine_name*	침입 정책 적용
IDSRule sid:*sig_id* rev:*rev_num*	SID 기준 침입 규칙
인시던트	침입 인시던트
Insert Policy Apply Job	정책 적용
설치	업데이트 설치
Intrusion Events	침입 이벤트
로그인	웹 인터페이스 로그인 및 로그아웃 기능
Menu	메뉴 옵션
Configuration export > *config_type* > *config_name*	특정 유형 및 이름의 컨피그레이션 가져오기
Permission Escalation	사용자 역할 에스컬레이션
Preferences	사용자 계정의 표준 시간대와 개별 이벤트 환경 설정 등의 사용자 환경 설정
정책	침입 정책을 비롯한 모든 정책
등록하기	방어 센터에서 디바이스 등록
RemoteStorageDevice	원격 스토리지 디바이스 구성
보고서	보고서 나열 및 보고서 디자이너 기능
규칙	규칙 편집기 및 규칙 가져오기 프로세스를 비롯한 침입 규칙
Rule Update Import Log	규칙 업데이트 가져오기 로그 보기
Rule Update Install	규칙 업데이트 설치
상태	Syslog, 호스트 및 성능 통계
시스템	시스템 전체의 여러 설정
System Policy > *policy_name* Appliance > *appliance_name*	시스템 정책 적용
Task Queue	작업 대기열 보기
사용자	사용자 계정과 역할 생성 및 수정

Audit Log 테이블 이해

라이센스: 모두

각 어플라이언스는 각 사용자와 웹 인터페이스의 상호 작용에 대해 감사 이벤트를 생성합니다. 각 이벤트에는 타임스탬프, 이벤트를 생성한 작업을 수행한 사용자의 사용자 이름, 소스 IP, 이벤트 설명 텍스트가 포함됩니다. 다음 표에서는 감사 로그 테이블의 필드에 대해 설명합니다.

표 69-4 Audit Log 필드

필드	설명
Time	어플라이언스가 감사 레코드를 생성한 시간과 날짜.
사용자	감사 이벤트를 트리거한 사용자의 사용자 이름.
Subsystem	감사 레코드를 생성하기 위해 사용자가 따른 메뉴 경로. 예를 들어 **System > Monitoring > Audit**은 감사 로그를 보기 위한 메뉴 경로입니다. 메뉴 경로와 관련이 없는 몇몇 경우에는 Subsystem 필드에 이벤트 유형만 표시됩니다. 예를 들어 **Login**은 사용자 로그인 시도를 분류합니다.
메시지	사용자가 수행한 작업. 예를 들어 `Page View`는 단순히 사용자가 하위 시스템에 표시된 페이지를 봤음을 의미하는 반면, `Save`는 사용자가 페이지에서 **Save** 버튼을 클릭했음을 의미합니다. FireSIGHT 시스템에 대한 변경 사항은 변경 요약을 보기 위해 클릭할 수 있는 비교 아이콘(FireSIGHT 시스템)과 함께 나타납니다.FireSIGHT 시스템 자세한 내용은 69-7페이지의 변경 사항 검토를 위해 감사 로그 사용을/를 참조하십시오.
소스 IP	사용자가 사용한 호스트와 연결된 IP 주소.
개수	각 행에 표시되는 정보와 매칭되는 이벤트의 수. 둘 이상의 동일한 행을 생성하는 제약 조건을 적용한 경우에만 Count 필드가 나타납니다.

변경 사항 검토를 위해 감사 로그 사용

라이센스: 모두

시스템 변경 사항에 대한 자세한 보고서를 보려면 감사 로그를 사용할 수 있습니다. 이러한 보고서는 시스템의 현재 컨피그레이션을 특정 변경 이전의 최신 컨피그레이션과 비교합니다.

시스템에 대한 변경 사항을 반영하는 감사 로그 이벤트 옆에 비교 아이콘()이 나타납니다. Compare Configurations 페이지에 액세스하여 자세한 변경 보고서를 보려면 변경 아이콘을 클릭할 수 있습니다.

Compare Configurations 페이지에는 차이점을 쉽게 파악할 수 있도록 변경 이전의 시스템 컨피그레이션과 실행 중인 컨피그레이션이 나란히 배치됩니다. 각 컨피그레이션 위의 제목 표시줄에는 감사 이벤트 유형, 마지막 수정 시간, 변경한 사용자의 이름이 표시됩니다.

두 컨피그레이션의 차이점이 강조 표시됩니다.

- 파란색은 강조 표시된 설정이 두 컨피그레이션에서 다름을 의미하며, 그 차이점이 빨간색 텍스트로 표시됩니다.
- 녹색은 강조 표시된 설정이 둘 중 한 컨피그레이션에만 나타남을 의미합니다.

감사 로그에서 변경 사항을 검토하려면

액세스: Admin

1단계 **System > Monitoring > Audit**를 선택합니다.

기본 감사 로그 워크플로의 첫 번째 페이지가 나타납니다.

감사 이벤트의 테이블 보기가 포함되지 않은 사용자 지정 워크플로를 사용 중인 경우 **(switch workflow)**를 클릭한 다음 **Audit Log**를 선택하십시오.

2단계 **Message** 열의 해당 감사 로그 이벤트 옆에 있는 비교 아이콘( )을 클릭합니다.

Compare Configurations 페이지가 나타납니다. 제목 표시줄 위에 있는 **Previous** 또는 **Next**를 클릭하여 변경 사항을 개별적으로 탐색할 수 있습니다. 변경 요약의 길이가 한 페이지를 넘으면 오른쪽에 있는 스크롤바를 이용해 추가 변경 내용을 볼 수 있습니다.

감사 레코드 검색

라이센스: 모두

사용자, 특정 하위 시스템 또는 감사 레코드 메시지에 해당하는 정보를 찾기 위해 감사 레코드를 검색할 수 있습니다.

네트워크 환경에 맞춤화된 검색을 생성한 다음 나중에 다시 사용할 수 있도록 저장할 수 있습니다. 사용할 수 있는 검색 기준은 다음 표에 설명되어 있습니다. 감사 검색에서는 대/소문자를 구분하지 않습니다. 예를 들어 `Analyst01` 또는 `analyst01` 검색 모두 동일한 결과를 반환합니다.

표 69-5 감사 레코드 검색 기준

검색 필드	설명	예
사용자	보려는 감사 이벤트를 트리거한 사용자의 사용자 이름을 입력합니다. 이 필드에서는 와일드카드 문자로 별표(*)를 사용할 수 있습니다.	`jsmith`는 사용자 jsmith와 관련된 모든 감사 레코드를 반환합니다.
Subsystem	보려는 감사 레코드를 생성하기 위해 사용자가 선택했을 전체 경로를 입력합니다. 이 필드에서는 와일드카드 문자로 별표(*)를 사용할 수 있습니다.	`System > Monitoring > Audit`과 `*Audit` 모두 감사 로그 사용과 관련된 감사 레코드를 반환합니다. `*Audit*`는 위의 레코드 모두 외에 감사 레코드 검색과 관련된 레코드도 추가로 반환합니다.
메시지	사용자가 수행한 작업 또는 사용자가 페이지에서 클릭한 버튼. 이 필드에서는 와일드카드 문자로 별표(*)를 사용할 수 있습니다.	`Apply` - 사용자가 침입 정책을 적용한 감사 레코드를 반환합니다. `Save Rule` - 사용자가 상관관계 규칙을 저장한 감사 레코드를 반환합니다. `Page View` - 사용자가 페이지를 본 감사 레코드를 반환합니다.
Time	감사 레코드가 생성된 날짜와 시간을 지정합니다. 시간 입력을 위한 구문은 60-5페이지의 검색에서 시간 제약 조건 지정을/를 참조하십시오.	`> 2006-01-15 13:30:00`은 2006년 1월 15일 오후 1시 30분 이후 생성된 모든 감사 레코드를 반환합니다.

표 69-5 감사 레코드 검색 기준 (계속)

검색 필드	설명	예
소스 IP	감사 레코드를 보고자 하는 호스트의 IP 주소를 입력합니다. **참고** **반드시** 특정 IP 주소를 입력해야 합니다. 감사 로그를 검색할 때에는 IP 범위를 사용할 수 없습니다.	`172.16.1.37`은 172.16.1.37 IP 주소에서 사용자가 생성한 모든 감사 레코드를 반환합니다.
컨피그레이션 변경	컨피그레이션 변경의 감사 레코드를 볼 것인지 여부를 지정합니다.	`yes`는 컨피그레이션 변경의 감사 레코드를 반환합니다.

저장된 검색을 로드 및 삭제하는 방법을 포함하여 검색에 대한 자세한 내용은 60-1페이지의 이벤트 검색을/를 참조하십시오.

감사 레코드를 검색하려면

액세스: Admin

1단계 **Analysis > Search**를 선택합니다.

Search 페이지가 나타납니다.

2단계 테이블 드롭다운 목록에서 **Audit Log Events**를 선택합니다.

Audit Log 검색 페이지가 나타납니다.

팁 데이터베이스에서 서로 다른 종류의 이벤트를 검색하려면 테이블 드롭다운 목록에서 선택합니다.

3단계 감사 레코드 검색 기준 표에 설명된 대로 해당 필드에 검색 기준을 입력합니다.

여러 필드에 대한 조건을 입력하는 경우 모든 필드에 대해 지정한 검색 기준과 일치하는 레코드만 반환됩니다.

4단계 선택적으로, 검색을 저장하려면 **Private** 확인란을 선택하여 자신만 액세스할 수 있는 비공개로 검색을 저장할 수 있습니다. 또는 모든 사용자가 사용할 수 있도록 검색을 저장하려면 확인란을 선택하지 않습니다.

팁 사용자 지정 사용자 역할에 대한 데이터 제한으로서 검색을 사용하려면 **반드시** 비공개 검색으로 저장해야 합니다.

5단계 선택적으로, 나중에 다시 사용할 수 있도록 검색을 저장할 수 있습니다. 다음 옵션을 이용할 수 있습니다.

- 검색 기준을 저장하려면 **Save**를 클릭합니다.

  새 검색인 경우 검색 이름을 입력하도록 대화 상자가 나타납니다. 고유한 검색 이름을 입력하고 **Save**를 클릭합니다. 이미 존재하는 검색에 대한 새 조건을 저장하는 경우 프롬프트가 나타나지 않습니다. 나중에 실행할 수 있도록 검색이 저장됩니다(**Private**을 선택한 경우 자신만 볼 수 있음).
- 새 검색을 저장하거나, 저장된 기존 검색을 변경하여 만든 검색에 새 이름을 할당하려면 **Save As New**를 클릭합니다.

검색 이름을 입력하도록 대화 상자가 나타납니다. 고유한 검색 이름을 입력하고 **Save**를 클릭합니다. 나중에 실행할 수 있도록 검색이 저장됩니다(**Private**을 선택한 경우 자신만 볼 수 있음).

6단계 검색을 시작하려면 **Search**를 클릭합니다.

검색 결과는 현재의 시간 범위로 제한되어 기본 감사 로그 워크플로에 나타납니다. 사용자 지정 워크플로를 비롯한 다른 워크플로를 사용하려면 **(switch workflow)**를 클릭합니다. 다른 기본 워크플로 지정에 대한 자세한 내용은 71-3페이지의 이벤트 보기 설정 구성을/를 참조하십시오.

시스템 로그 보기

라이센스: 모두

시스템 로그(syslog) 페이지에서는 어플라이언스에 대한 시스템 로그 정보를 제공합니다. 시스템 로그는 시스템에서 생성된 각 메시지를 표시합니다. 다음 항목이 순서대로 나열됩니다.

- 메시지가 생성된 날짜
- 메시지가 생성된 시간
- 메시지가 생성된 호스트
- 메시지 내용

참고 시스템 로그 정보는 로컬입니다. 예를 들어 관리되는 디바이스에서 시스템 로그의 시스템 상태 메시지를 보는 데에는 방어 센터를 사용할 수 **없습니다**.

필터 기능을 사용하면 특정 구성 요소에 대한 시스템 로그 메시지를 볼 수 있습니다. 자세한 내용은 69-11페이지의 시스템 로그 메시지 필터링을/를 참조하십시오.

Syslog를 보려면

액세스: Admin/Maint

1단계 **System > Monitoring > Syslog**를 선택합니다.

System Log 페이지가 나타납니다.

팁 3D9900에서 LBIM(Load Balancing Interface Module)은 메시지를 디바이스의 syslog로 전달합니다. `lbim`으로 필터링하여 이러한 메시지를 찾을 수 있습니다.

시스템 로그 메시지 필터링

라이센스: 모두

필터 기능을 사용하면 특정 구성 요소에 대한 시스템 로그 메시지를 볼 수 있습니다. 또한 내용을 기반으로 특정 메시지를 검색할 수 있습니다.

필터 기능에서는 UNIX 파일 검색 유틸리티인 Grep를 사용하므로, 사용자는 Grep에서 허용되는 대부분의 구문을 사용할 수 있습니다. 이에 따라 패턴 매칭에 Grep 호환 정규식을 사용할 수 있습니다. 필터로 단일 단어를 사용할 수도 있고, 내용 검색을 위해 Grep 지원 정규식을 사용할 수도 있습니다.

다음 표에서는 System Log 필터에서 사용할 수 있는 정규식 구문을 보여줍니다.

표 69-6 시스템 로그 필터 구문

구문 구성 요소	설명	예
.	문자나 공백 매칭	`Admi.` Admin, AdmiN, Admi1 및 Admi& 매칭
`[[:alpha:]]`	알파벳 문자 매칭	`[[:alpha:]]dmin` - Admin, bdmin 및 Cdmin 매칭
`[[:upper:]]`	알파벳 대문자 매칭	`[[:upper:]]dmin` - Admin, Bdmin 및 Cdmin 매칭
`[[:lower:]]`	알파벳 소문자 매칭	`[[:lower:]]dmin` - admin, bdmin 및 cdmin 매칭
`[[:digit:]]`	숫자 문자 매칭	`[[:digit:]]dmin` - 0dmin, 1dmin 및 2dmin 매칭
`[[:alnum:]]`	영숫자 문자 매칭	`[[:alnum:]]dmin` - 1dmin, admin, 2dmin 및 bdmin 매칭
`[[:space:]]`	탭 포함, 공백 매칭	`Feb[[:space:]]29` - 2월 29일의 로그 매칭
*	그 뒤에 오는 0개 이상의 문자 또는 식 인스턴스 매칭	`ab*` - a, ab, abb, ca, cab 및 cabb 매칭 `[ab]*` - 모두 매칭
	0 또는 1 인스턴스 매칭	`ab? a` 또는 ab 매칭
\	일반적으로 정규식 구문으로 해석되는 문자에 대한 검색 허용	`alert\? alert?` 매칭

다음 표는 System Log 페이지에서 사용할 수 있는 몇 가지 예제 필터를 보여줍니다.

표 69-7 시스템 로그 필터 예제

모든 로그 항목에서 검색할 내용	사용
11월 5일에 생성됨	`Nov[[:space:]]*5`
사용자 이름 "Admin" 포함	`Admin`
11월 5일 자 권한 부여 디버깅 정보 포함	`Nov[[:space:]]*5.*AUTH.*DEBUG`

시스템 로그에서 특정 메시지 내용을 검색하려면

액세스: Admin/Maint

1단계 **System > Monitoring > Syslog**를 선택합니다.

System Log 페이지가 나타납니다.

2단계 필터 필드에 단어나 쿼리를 입력합니다.

사용할 수 있는 필터 구문에 대한 자세한 내용은 위의 표를 참조하십시오.

참고 Grep 호환 검색 구문만 지원됩니다. 예를 들면, `ntp`를 필터로 사용하여 모든 NTP 관련 시스템 로그 메시지를 검색하거나 `Nov`를 필터로 사용하여 11월에 생성된 모든 메시지를 검색할 수 있습니다. 11월 27일의 메시지를 보기 위해 `Nov[[:space:]]*27` 또는 `Nov.*27`은 사용할 수 있지만 `Nov 27` 또는 `Nov*27`은 사용할 수 없습니다.

3단계 선택적으로, 대/소문자를 구분하여 검색하려면 **Case-sensitive**를 선택합니다. (기본적으로 필터는 대/소문자를 구분하지 않습니다.)

4단계 선택적으로, 입력한 기준과 일치하지 **않는** 모든 시스템 로그 메시지를 검색하려면 **Exclusion**을 선택합니다.

5단계 **Go**를 클릭합니다.

필터와 일치하는 메시지가 나타납니다.

70장

백업 및 복원 사용

백업 및 복원은 모든 시스템 유지 보수 계획의 중요한 일부입니다. 각 조직의 백업 계획은 매우 개별화되어 있지만 FireSIGHT 시스템은 재해가 발생할 경우 방어 센터 또는 관리되는 물리적 디바이스의 데이터를 복원할 수 있도록 데이터를 아카이빙하는 메커니즘을 제공합니다.

백업 및 복원에 대한 다음과 같은 제한 사항에 유의하십시오.

- 백업은 백업을 생성한 제품 버전에 대해서만 유효합니다.
- 캡처된 파일 데이터는 백업에 포함되지 않습니다.
- 관리되는 가상 디바이스, Cisco NGIPS for Blue Coat X-Series 또는 Cisco ASA with FirePOWER Services에 대해서는 백업 파일을 생성하거나 복원할 수 없습니다. 모든 이벤트 데이터를 백업하려면 관리하는 방어 센터의 백업을 수행합니다.
- 두 어플라이언스가 동일한 모델이며 FireSIGHT 시스템 소프트웨어의 동일한 버전을 실행하는 경우에만 교체 어플라이언스에 백업을 복원할 수 있습니다.

주의 관리되는 디바이스 간에 컨피그레이션 파일을 복사하려면 백업 및 복원 프로세스를 사용하지 마십시오. 컨피그레이션 파일은 디바이스를 고유하게 식별하는 정보를 포함하며, 공유할 수 없습니다.

주의 침입 규칙 업데이트를 적용한 경우 이러한 업데이트는 백업되지 않습니다. 복원한 **후에는** 최신 규칙 업데이트를 적용해야 합니다.

백업 파일은 어플라이언스 또는 로컬 컴퓨터에 저장할 수 있습니다. 추가로 방어 센터를 사용 중인 경우 원격 스토리지를 사용할 수 있습니다(64-15페이지의 원격 스토리지 관리 참조).

주의 3D9900의 USB 포트에 USB 드라이브를 삽입하지 마십시오. 또한 디바이스를 업그레이드 또는 복원하기 전에 3D9900에서 외부 스토리지가 있는 디바이스(예: 외부 스토리지가 있는 KVM 스위치)를 제거하십시오.

자세한 내용은 다음 절을 참조하십시오.

- 방어 센터 및 관리되는 물리적 디바이스용 백업 파일을 만드는 방법에 대한 자세한 내용은 70-2페이지의 백업 파일 생성을/를 참조하십시오.
- 나중에 백업 생성을 위한 템플릿으로 사용할 수 있는 백업 프로필을 생성하는 방법에 대한 자세한 내용은 70-6페이지의 백업 프로필 생성을/를 참조하십시오.
- 로컬 호스트에서 백업 파일을 업로드하는 방법에 대한 자세한 내용은 70-6페이지의 로컬 호스트에서 백업 업로드을/를 참조하십시오.

- 백업 파일을 어플라이언스에 복원하는 방법에 대한 자세한 내용은 70-7페이지의 백업 파일에서 어플라이언스 복원을/를 참조하십시오.

백업 파일 생성

라이센스: 모두

지원되는 디바이스: 가상 X-Series 및 ASA FirePOWER를 제외한 모두

지원되는 Defense Center: 모두

디바이스 자체에서 관리되는 물리적 디바이스의 백업을 수행하거나, 관리하는 방어 센터에서 관리되는 물리적 디바이스의 백업을 수행하거나, 방어 센터의 백업을 수행할 수 있습니다. 수행하는 백업 유형에 따라 시스템은 서로 다른 데이터를 백업합니다. 캡처된 파일 데이터는 백업되지 **않습니다**. 수행할 백업 종류를 결정하려면 다음 표를 사용하십시오.

표 70-1 백업 유형에 의해 저장된 데이터

백업 유형	컨피그레이션 데이터를 포함합니까?	이벤트 데이터를 포함합니까?	통합 파일을 포함합니까?
방어 센터	예	예	아니요
디바이스 자체에서 수행되는 관리되는 물리적 디바이스	예	아니요	아니요
관리하는 방어 센터에서 수행되는 관리되는 물리적 디바이스	예	아니요	예

참고 관리되는 가상 디바이스, Cisco NGIPS for Blue Coat X-Series 또는 Cisco ASA with FirePOWER Services에 대해서는 백업 파일을 생성하거나 복원할 수 **없습니다**. 이벤트 데이터를 백업하려면 관리하는 방어 센터의 백업을 수행하십시오.

기존 시스템 백업을 보고 사용하려면 Backup Management 페이지로 이동합니다. 이벤트 데이터는 물론, 어플라이언스 복원에 필요한 모든 컨피그레이션 파일이 포함된 백업 파일을 주기적으로 저장해야 합니다. 또한 필요 시 저장된 컨피그레이션으로 돌아갈 수 있도록, 컨피그레이션 변경 사항을 테스트할 때 시스템을 백업할 수 있습니다. 어플라이언스 또는 로컬 컴퓨터에 백업 파일을 저장하도록 선택할 수 있습니다.

어플라이언스에 디스크 공간이 충분하지 않은 경우 백업 파일을 생성할 수 없습니다. 백업 프로세스가 여유 디스크 공간의 90% 이상을 사용하는 경우 백업이 실패할 수 있습니다. 필요한 경우 이전 백업 파일을 삭제하거나, 이전 백업 파일을 어플라이언스에서 다른 곳으로 전송하거나, 원격 스토리지를 사용하십시오.

대안으로, 백업 파일이 4GB보다 큰 경우 SCP를 통해 원격 호스트에 복사하십시오. 4GB가 넘는 백업 파일은 로컬 컴퓨터에서 업로드할 수 없는데, 이는 웹 브라우저에서 그렇게 큰 파일의 업로드를 지원하지 않기 때문입니다. 방어 센터에서는 백업 파일을 원격 위치에 저장할 수 있습니다. 자세한 내용은 64-15페이지의 원격 스토리지 관리을/를 참조하십시오.

참고 백업 작업이 검색 이벤트를 수집하는 동안에는 데이터 상관관계가 일시적으로 중단됩니다.

다음에 유의하십시오.

- PKI 객체와 연결된 개인 키는 어플라이언스에 저장될 때 무작위로 생성된 키로 암호화됩니다. PKI 객체와 연결된 개인 키를 포함하는 백업을 수행할 경우, 개인 키는 암호화되지 않은 백업 파일에 포함되기 전에 해독됩니다. 백업 파일을 안전한 곳에 저장하십시오.
- PKI 객체와 연결된 개인 키를 포함하는 백업을 복원할 경우, 시스템은 어플라이언스에 저장하기 전에 무작위로 생성된 키로 해당 키를 암호화합니다.
- 백업을 수행한 후 검토한 침입 이벤트를 삭제하면, 백업은 삭제된 침입 이벤트를 복원하지만 검토된 상태는 복원하지 않습니다. 복원된 침입 이벤트는 Reviewed Events가 아니라 Intrusion Events에서 볼 수 있습니다. 41-16페이지의 침입 이벤트 검토을/를 참조하십시오.
- 이미 침입 이벤트 데이터가 포함된 어플라이언스에 해당 데이터가 포함된 백업을 복원하는 경우 중복 이벤트가 생성됩니다. 이 문제를 피하려면 이전 침입 이벤트 데이터가 없는 어플라이언스에서만 침입 이벤트 백업을 복원하십시오.

주의 보안 영역과의 인터페이스 연결을 구성한 경우 이러한 연결은 백업되지 않습니다. 복원 후에 다시 구성해야 합니다. 자세한 내용은 3-38페이지의 보안 영역 작업을/를 참조하십시오.

방어 센터의 백업 파일을 생성하려면

액세스: Admin/Maint

1단계 **System > Tools > Backup/Restore**를 선택합니다.

Backup Management 페이지가 나타납니다.

2단계 **방어 센터 Backup**을 클릭합니다.

Create Backup 페이지가 나타납니다.

3단계 **Name** 필드에 백업 파일의 이름을 입력합니다. 영숫자, 구두점 및 공백을 사용할 수 있습니다.

4단계 방어 센터에는 두 가지 옵션이 더 있습니다.

- 컨피그레이션을 아카이브하려면 **Back Up Configuration**을 선택합니다.
- 전체 이벤트 데이터베이스를 아카이브하려면 **Back Up Events**를 선택합니다.

5단계 선택적으로, 백업이 완료될 때 알림을 받으려면 **Email** 확인란을 선택하고 해당 텍스트 상자에 이메일 주소를 입력합니다.

참고 이메일 알림을 받으려면 63-18페이지의 메일 릴레이 호스트 및 알림 주소 구성에 설명된 대로 릴레이 호스트를 구성해야 합니다.

6단계 선택적으로, 방어 센터에서 SCP(Secure Copy)를 사용하여 백업 아카이브를 다른 시스템에 복사하려면 **Copy when complete** 확인란을 선택하고 해당 텍스트 상자에 다음 정보를 입력합니다.

- **Host** 필드 - 백업을 복사하려는 시스템의 호스트 이름 또는 IP 주소
- **Path** 필드 - 백업을 복사하려는 디렉토리의 경로
- **User** 필드 - 원격 시스템에 로그인하는 데 사용하려는 사용자 이름
- **Password** 필드 - 해당 사용자 이름의 비밀번호
  비밀번호 대신 SSH 공개 키를 사용하여 원격 시스템에 액세스하려면 **SSH Public Key** 필드의 내용을 해당 시스템에 있는 지정된 사용자의 `authorized_keys` 파일에 복사해야 합니다.

이 옵션을 선택하지 않으면 시스템은 백업 중에 사용되는 임시 파일을 원격 서버에 저장합니다. 이 옵션을 선택하면 임시 파일이 원격 서버에 저장되지 **않습니다**.

팁 Cisco에서는 시스템 장애 발생 시 어플라이언스를 복원할 수 있도록 백업을 원격 위치에 주기적으로 저장할 것을 권장합니다.

7단계 다음 옵션을 이용할 수 있습니다.

- 백업 파일을 어플라이언스에 저장하려면 **Start Backup**을 클릭합니다.

  백업 파일은 `/var/sf/backup` 디렉토리에 저장됩니다. 백업 파일을 원격 위치로 보낼 수 있습니다. 64-15페이지의 원격 스토리지 관리을/를 참조하십시오.

  백업 프로세스가 완료되면 Restoration Database 페이지에서 파일을 볼 수 있습니다. 백업 파일의 복원에 대한 자세한 내용은 70-7페이지의 백업 파일에서 어플라이언스 복원을/를 참조하십시오.

- 이 컨피그레이션을 나중에 사용할 수 있는 백업 프로필로 저장하려면 **Save As New**를 클릭합니다.

  System > Tools > Backup/Restore를 선택한 다음 **Backup Profiles**를 클릭하여 백업 프로필을 수정 또는 삭제할 수 있습니다. 자세한 내용은 70-6페이지의 백업 프로필 생성을/를 참조하십시오.

관리되는 물리적 디바이스의 백업 파일을 디바이스 자체에서 생성하려면

액세스: Admin/Maint

1단계 **System > Tools > Backup/Restore**를 선택합니다.

Device Backups 페이지가 나타납니다.

2단계 **Device Backup**을 클릭합니다.

Create Backup 페이지가 나타납니다.

3단계 **Name** 필드에 백업 파일의 이름을 입력합니다. 영숫자, 구두점 및 공백을 사용할 수 있습니다.

4단계 선택적으로, 백업이 완료될 때 알림을 받으려면 **Email** 확인란을 선택하고 해당 텍스트 상자에 이메일 주소를 입력합니다.

참고 이메일 알림을 받으려면 63-18페이지의 메일 릴레이 호스트 및 알림 주소 구성에 설명된 대로 릴레이 호스트를 구성해야 합니다.

5단계 선택적으로, `SCP`(Secure Copy)를 사용하여 백업 아카이브를 다른 시스템에 복사하려면 **Copy when complete** 확인란을 선택하고 해당 텍스트 상자에 다음 정보를 입력합니다.

- **Host** 필드 - 백업을 복사하려는 시스템의 호스트 이름 또는 IP 주소
- **Path** 필드 - 백업을 복사하려는 디렉토리의 경로
- **User** 필드 - 원격 시스템에 로그인하는 데 사용하려는 사용자 이름
- **Password** 필드 - 해당 사용자 이름의 비밀번호
  비밀번호 대신 SSH 공개 키를 사용하여 원격 시스템에 액세스하려면 **SSH Public Key** 필드의 내용을 해당 시스템에 있는 지정된 사용자의 `authorized_keys` 파일에 복사해야 합니다.

이 옵션을 선택하지 않으면 시스템은 백업 중에 사용되는 임시 파일을 원격 서버에 저장합니다. 이 옵션을 선택하면 임시 파일이 원격 서버에 저장되지 **않습니다**.

팁 Cisco에서는 시스템 장애 발생 시 어플라이언스를 복원할 수 있도록 백업을 원격 위치에 주기적으로 저장할 것을 권장합니다.

6단계 다음 옵션을 이용할 수 있습니다.

- 백업 파일을 어플라이언스에 저장하려면 **Start Backup**을 클릭합니다.

  백업 파일은 `/var/sf/backup` 디렉토리에 저장됩니다. 방어 센터에서 백업 파일을 원격 위치로 보낼 수 있습니다. 64-15페이지의 원격 스토리지 관리을/를 참조하십시오.

  백업 프로세스가 완료되면 Restoration Database 페이지에서 파일을 볼 수 있습니다. 백업 파일의 복원에 대한 자세한 내용은 70-7페이지의 백업 파일에서 어플라이언스 복원을/를 참조하십시오.

- 이 컨피그레이션을 나중에 사용할 수 있는 백업 프로필로 저장하려면 **Save As New**를 클릭합니다.

  System > Tools > Backup/Restore를 선택한 다음 **Backup Profiles**를 클릭하여 백업 프로필을 수정 또는 삭제할 수 있습니다. 자세한 내용은 70-6페이지의 백업 프로필 생성을/를 참조하십시오.

관리되는 물리적 디바이스의 백업 파일을 관리하는 방어 센터에서 생성하려면

액세스: Admin/Maint

1단계 **System > Tools > Backup/Restore**를 선택합니다.

Backup Management 페이지가 나타납니다.

2단계 **Managed Device Backup**을 클릭합니다.

Create Backup 페이지가 나타납니다.

3단계 **Managed Devices** 필드에서 하나 이상의 관리되는 디바이스를 선택합니다. 관리되는 디바이스를 여러 개 선택하려면 Shift 또는 Ctrl 키를 사용합니다.

4단계 컨피그레이션 데이터 외에 통합 파일도 포함하려면 **Include All Unified Files** 확인란을 선택합니다.

5단계 백업 파일을 방어 센터에 저장하려면 **Retrieve to 방어 센터** 확인란을 선택합니다. 각 디바이스의 백업 파일을 디바이스 자체에 저장하려면 이 확인란을 선택하지 않습니다.

참고 **Retrieve to 방어 센터**를 선택하고 백업의 원격 스토리지를 이용하도록 방어 센터를 구성하면, 디바이스 백업 파일은 구성된 원격 위치가 아니라 방어 센터 자체에 저장됩니다.

6단계 **Start Backup**을 클릭합니다.

성공 메시지가 나타나고 백업 작업이 생성됩니다.

백업 파일은 `/var/sf/backup` 디렉토리에 저장됩니다. 방어 센터를 사용하면 백업 파일을 원격 위치로 보낼 수 있습니다. 64-15페이지의 원격 스토리지 관리을/를 참조하십시오.

백업 프로세스가 완료되면 Restoration Database 페이지에서 파일을 볼 수 있습니다. 백업 파일의 복원에 대한 자세한 내용은 70-7페이지의 백업 파일에서 어플라이언스 복원을/를 참조하십시오.

7단계 선택적으로, 이 컨피그레이션을 나중에 사용할 수 있는 백업 프로필로 저장하려면 **Save As New**를 클릭합니다.

System > Tools > Backup/Restore를 선택한 다음 **Backup Profiles**를 클릭하여 백업 프로필을 수정 또는 삭제할 수 있습니다. 자세한 내용은 70-6페이지의 백업 프로필 생성을/를 참조하십시오.

백업 프로필 생성

라이센스: 모두

지원되는 디바이스: 가상 X-Series 및 ASA FirePOWER를 제외한 모두

지원되는 Defense Center: 모두

서로 다른 유형의 백업에 사용할 설정을 포함하는 백업 프로필을 생성하려면 Backup Profiles 페이지를 사용할 수 있습니다. 나중에 어플라이언스에서 파일을 백업할 때 이러한 프로필 중 하나를 선택할 수 있습니다.

팁 70-2페이지의 백업 파일 생성에 설명된 대로 백업 파일을 생성하면 백업 프로필이 자동으로 생성됩니다.

백업 프로필을 생성하려면

액세스: Admin/Maint

1단계 **System > Tools > Backup/Restore**를 선택합니다.

Backup Management 페이지가 나타납니다.

2단계 **Backup Profiles** 탭을 클릭합니다.

기존 백업 프로필 목록과 함께 Backup Profiles 페이지가 나타납니다.

팁 기존 프로필을 수정하려면 수정 아이콘( )을 클릭하고, 목록에서 프로필을 삭제하려면 삭제 아이콘( )을 클릭할 수 있습니다.

3단계 **Create Profile**을 클릭합니다.

Create Backup 페이지가 나타납니다.

4단계 백업 프로필의 이름을 입력합니다. 영숫자, 구두점 및 공백을 사용할 수 있습니다.

5단계 필요에 따라 백업 프로필을 구성합니다.

이 페이지의 옵션에 대한 자세한 내용은 70-2페이지의 백업 파일 생성을/를 참조하십시오.

6단계 백업 프로필을 저장하려면 **Save As New**를 클릭합니다.

Backup Profiles 페이지가 나타나고 새 프로필이 목록에 나타납니다.

로컬 호스트에서 백업 업로드

라이센스: 모두

지원되는 디바이스: Series 2 및 Series 3

지원되는 Defense Center: 모두

Backup Management 표에 설명된 다운로드 기능을 사용하여 백업 파일을 로컬 호스트에 다운로드한 경우 이 파일을 방어 센터에 업로드할 수 있습니다.

백업 파일에 PKI 객체가 포함되어 있으면 내부 CA 및 내부 인증서 객체와 연결된 개인 키가 업로드 시 무작위로 생성된 키로 다시 암호화됩니다.

팁 4GB가 넘는 백업은 로컬 호스트에서 업로드할 수 없는데, 이는 웹 브라우저에서 그렇게 큰 파일의 업로드를 지원하지 않기 때문입니다. 대안으로, SCP를 통해 백업을 원격 호스트에 복사하고 그곳에서 검색하십시오. 방어 센터에서는 백업 파일을 원격 위치에 저장하고 그곳에서 검색할 수 있습니다. 자세한 내용은 64-15페이지의 원격 스토리지 관리을/를 참조하십시오.

로컬 호스트에서 백업을 업로드하려면

액세스: Admin/Maint

1단계 **System > Tools > Backup/Restore**를 선택합니다.

Backup Management 페이지가 나타납니다.

2단계 **Upload Backup**을 클릭합니다.

Upload Backup 페이지가 나타납니다.

3단계 **Browse**를 클릭하고 업로드할 백업 파일로 이동합니다.

업로드할 파일을 선택한 다음 **Upload Backup**을 클릭합니다.

4단계 Backup Management 페이지로 돌아가려면 **Backup Management**를 클릭합니다.

백업 파일이 업로드되고 백업 목록에 나타납니다. 방어 센터 어플라이언스에서 파일 무결성이 확인되면, Backup Management 페이지를 새로 고쳐 자세한 파일 시스템 정보를 표시하십시오.

백업 파일에서 어플라이언스 복원

라이센스: 모두

지원되는 디바이스: Series 2 및 Series 3

지원되는 Defense Center: 모두

Backup Management 페이지를 사용하여 백업 파일에서 어플라이언스를 복원할 수 있습니다. 백업을 복원하려면 백업 파일의 VDB 버전이 어플라이언스의 현재 VDB 버전과 일치해야 합니다. 복원 프로세스가 완료되면 **반드시** 최근 Sourcefire Rule Update를 적용해야 합니다.

주의 가상 방어 센터에서 생성된 백업을 물리적 방어 센터에 복원하지 마십시오. 시스템 리소스에 부담이 될 수 있습니다. 가상 백업을 물리적 방어 센터에서 복원해야 하는 경우 고객 지원에 문의하십시오.

백업 파일에 PKI 객체가 포함되어 있으면 내부 CA 및 내부 인증서 객체와 연결된 개인 키가 업로드 시 무작위로 생성된 키로 다시 암호화됩니다.

로컬 스토리지를 사용하면 백업 파일은 `/var/sf/backup`에 저장됩니다. 이 디렉토리는 `/var` 파티션에 사용된 디스크 공간과 함께 Backup Management 페이지의 아래쪽에 나열됩니다. 방어 센터에서 원격 스토리지 옵션을 구성하려면 Backup Management 페이지 상단의 **Remote Storage**를 선택합니다. 그런 다음, 원격 스토리지를 활성화하려면 Backup Management 페이지에서 **Enable Remote Storage for Backups** 확인란을 선택합니다. 원격 스토리지를 사용하는 경우 페이지 하단에 프로토콜, 백업 시스템 및 백업 디렉토리가 나열됩니다.

참고 백업이 완료된 후 라이센스를 추가하면, 백업을 복원할 때 라이센스를 제거하거나 덮어쓸 수 없습니다. 복원 시 충돌을 방지하려면 백업을 복원하기 전에 라이센스를 제거하고, 라이센스가 사용된 곳을 적어두고, 백업이 복원된 후 추가하여 다시 구성하십시오. 충돌이 발생하면 고객 지원에 문의하십시오.

다음 표에서는 Backup Management 페이지의 각 열과 아이콘에 대해 설명합니다.

표 70-2 Backup Management

기능	설명
시스템 정보	원래 어플라이언스 이름, 유형 및 버전. 동일한 어플라이언스 유형 및 버전에만 백업을 복원할 수 있습니다.
생성 날짜	백업 파일이 생성된 날짜 및 시간
파일 이름	백업 파일의 전체 이름
VDB 버전	백업 시 어플라이언스에서 실행되는 VDB(취약성 데이터베이스)의 빌드
장소	백업 파일의 위치
크기(MB)	메가바이트 단위의 백업 파일의 크기
이벤트?	"Yes"는 백업에 이벤트 데이터가 포함됨을 나타냄
View	압축된 백업 파일에 포함된 파일 목록을 보려면 백업 파일의 이름을 클릭합니다.
복원	어플라이언스에 복원하려면 선택한 백업 파일을 클릭합니다. VDB 버전이 백업 파일의 VDB 버전과 일치하지 않으면 이 옵션이 비활성화됩니다.
다운로드	로컬 컴퓨터에 저장하려면 선택한 백업 파일을 클릭합니다.
삭제	삭제하려면 선택한 백업 파일을 클릭합니다.
이동	방어 센터에서 전에 생성한 로컬 백업을 선택하고 클릭하여, 지정된 원격 백업 위치로 백업을 전송합니다.

백업 파일에서 어플라이언스를 복원하려면

액세스: Admin

1단계 **System > Tools > Backup/Restore**를 선택합니다.

Backup Management 페이지가 나타납니다.

2단계 백업 파일의 내용을 보려면 파일의 이름을 클릭합니다.

각 파일의 이름, 소유자와 권한, 파일 크기와 날짜가 나열된 매니페스트가 나타납니다.

3단계 Backup Management 페이지로 돌아가려면 **Backup Management**를 클릭합니다.

4단계 복원하려는 백업 파일을 선택하고 **Restore**를 클릭합니다.

Restore Backup 페이지가 나타납니다.

백업의 VDB 버전이 어플라이언스에 현재 설치된 VDB 버전과 일치하지 않으면 **Restore** 버튼이 회색으로 표시됩니다.

주의 이 절차는 모든 컨피그레이션 파일과 모든 이벤트 데이터(관리되는 디바이스에 있는)를 덮어씁니다.

5단계 파일을 복원하려면 다음 중 하나 또는 둘을 모두 선택합니다.

- **Replace Configuration Data**
- **Restore Event Data**

참고 백업 파일에서 관리되는 디바이스의 컨피그레이션을 복원하면, 디바이스의 관리하는 방어 센터에서 변경한 모든 디바이스 컨피그레이션은 물론 백업 파일을 생성한 이후의 변경 사항도 복원됩니다.

6단계 복원을 시작하려면 **Restore**를 클릭합니다.

지정한 백업 파일을 사용하여 어플라이언스가 복원됩니다.

7단계 어플라이언스를 재부팅합니다.

8단계 규칙 업데이트를 다시 적용하려면 최신 Sourcefire Rule Update를 적용합니다.

9단계 복원된 시스템에 모든 액세스 제어, 침입, 네트워크 검색, 상태 및 시스템 정책을 다시 적용합니다.

71장 사용자 환경 설정 지정

단일 사용자 계정과 연결된 환경 설정, 이를테면 홈 페이지, 계정 비밀번호, 표준 시간대, 대시보드, 이벤트 보기 환경 설정 등을 구성할 수 있습니다.

사용자 역할에 따라 사용자 계정에 대한 환경 설정, 즉 비밀번호, 이벤트 보기 환경 설정, 표준 시간대 설정, 홈 페이지 환경 설정 등을 구체적으로 지정할 수 있습니다. 자세한 내용은 다음 절을 참조하십시오.

- 71-1페이지의 비밀번호 변경에서는 사용자 계정의 비밀번호를 변경하는 방법에 대해 설명합니다.
- 71-2페이지의 홈 페이지 지정에서는 기존 페이지 중 하나를 기본 홈 페이지로 사용하는 방법에 대해 설명합니다. 이 값을 설정하면 어플라이언스에 로그인할 때 이 페이지가 가장 먼저 표시됩니다.
- 71-3페이지의 이벤트 보기 설정 구성에서는 사용자가 이벤트를 볼 때 표시되는 내용에 이벤트 환경 설정이 어떻게 적용되는지 설명합니다.
- 71-7페이지의 기본 표준 시간대 설정에서는 사용자 계정의 표준 시간대를 설정하는 방법 및 그에 따라 사용자가 보는 이벤트의 타임스탬프의 변화에 대해 설명합니다.
- 71-8페이지의 기본 대시보드 지정에서는 기본 대시보드로 사용할 대시보드를 선택하는 방법에 대해 설명합니다.

비밀번호 변경

라이센스: 모두

지원되는 디바이스: Series 2, Series 3

지원되는 Defense Center: 모두

모든 사용자 계정이 비밀번호로 보호받습니다. 언제라도 비밀번호를 변경할 수 있으며, 사용자 계정에 대한 설정에 따라 정기적으로 비밀번호를 변경해야 하는 경우도 있습니다. 71-2페이지의 만료된 비밀번호 변경을/를 참조하십시오.

비밀번호 길이 검사가 활성화된 경우 비밀번호는 대/소문자가 혼합된 영숫자 8자 이상이고 숫자를 하나 이상 포함해야 합니다. 비밀번호는 사전에 나와 있는 단어일 수 없으며, 연속적으로 반복되는 문자를 포함할 수 없습니다.

참고 LDAP 또는 RADIUS 사용자일 경우 웹 인터페이스를 통해 비밀번호를 변경할 수 없습니다.

비밀번호를 변경하려면

액세스: 모두

1단계 사용자 이름 아래의 드롭다운 목록에서 **User Preferences**를 선택합니다.

Change Password 페이지가 나타납니다.

2단계 **Current Password** 필드에 현재 비밀번호를 입력하고 **Change**를 클릭합니다.

3단계 **New Password**와 **Confirm** 필드에 새 비밀번호를 입력합니다.

4단계 **Change**를 클릭합니다.

시스템에서 새 비밀번호를 승인하면 성공 메시지가 페이지에 나타납니다.

만료된 비밀번호 변경

라이센스: 모두

지원되는 디바이스: Series 2, Series 3

지원되는 Defense Center: 모두

사용자 계정의 설정에 따라 비밀번호가 만료될 수 있습니다. 비밀번호 만료 기한은 계정 생성 시 설정되며 변경되지 않습니다. 비밀번호가 만료된 경우 Password Expiration Warning 페이지가 나타납니다.

비밀번호 만료 경고에 응답하려면:

액세스: 모두

1단계 2가지 옵션이 있습니다.

- 당장 비밀번호를 변경하려면 **Change Password**를 클릭합니다.

  남은 경고 일수가 0일 경우 **반드시** 비밀번호를 변경해야 합니다. 또한 비밀번호 길이 검사가 활성화된 경우 비밀번호는 대/소문자가 혼합된 영숫자 8자 이상이고 숫자를 하나 이상 포함해야 합니다. 비밀번호는 사전에 나와 있는 단어일 수 없으며, 연속적으로 반복되는 문자를 포함할 수 없습니다.
- 비밀번호를 나중에 변경하려면 **Skip**을 클릭합니다.

홈 페이지 지정

라이센스: 모두

웹 인터페이스의 어떤 페이지를 어플라이언스의 홈 페이지로 지정할 수 있습니다. 기본 홈 페이지는 Summary Dashboard(**Overview > Dashboards**)입니다. 대시보드 액세스 권한이 없는 사용자 계정의 경우 Welcome 페이지를 사용합니다.

홈 페이지를 지정하려면

액세스: 외부 데이터베이스 사용자를 제외하고 모두

1단계 사용자 이름 아래의 드롭다운 목록에서 **User Preferences**를 선택합니다.

Change Password 페이지가 나타납니다.

2단계 **Home Page**를 클릭합니다.

Home Page 페이지가 나타납니다.

3단계 홈 페이지로 사용할 페이지를 드롭다운 목록에서 선택합니다.

드롭다운 목록의 옵션은 사용자 계정의 액세스 권한에 따라 달라집니다. 자세한 내용은 61-56페이지의 사용자 계정 권한을/를 참조하십시오.

4단계 **Save**를 클릭합니다.

홈 페이지 환경 설정이 저장되었습니다.

이벤트 보기 설정 구성

라이센스: 모두

FireSIGHT 시스템의 이벤트 보기 특성을 구성하려면 Event View Settings 페이지를 사용합니다. 일부 이벤트 보기 컨피그레이션은 특정 사용자 역할만 사용할 수 있습니다. 외부 데이터베이스 사용자 역할의 사용자는 이벤트 보기 설정 사용자 인터페이스의 일부를 볼 수 있으나, 그 설정을 변경하더라도 아무런 효과가 없습니다. 자세한 내용은 아래에 링크된 각 절을 참조하십시오.

이벤트 환경 설정을 구성하려면

액세스: 기능에 따라

1단계 사용자 이름 아래의 드롭다운 목록에서 **User Preferences**를 선택합니다.

User Preferences 페이지가 나타납니다.

2단계 **Event View Settings**를 클릭합니다.

Event View Settings 페이지가 나타납니다.

3단계 이벤트 보기의 기본 특성을 구성합니다.

자세한 내용은 71-4페이지의 이벤트 환경 설정을/를 참조하십시오.

4단계 파일 다운로드 환경 설정을 구성합니다.

자세한 내용은 71-5페이지의 파일 환경 설정을/를 참조하십시오.

5단계 기본 시간 창을 구성합니다.

자세한 내용은 71-5페이지의 기본 시간 창을/를 참조하십시오.

6단계 기본 워크플로를 구성합니다.

자세한 내용은 71-7페이지의 기본 워크플로을/를 참조하십시오.

7단계 **Save**를 클릭합니다.

변경 사항이 적용되었습니다.

이벤트 환경 설정

라이센스: 모두

FireSIGHT 시스템에서 이벤트 보기의 기본 특성을 구성하려면 Event View Settings 페이지의 Event Preferenes 섹션을 사용합니다. 이 섹션은 모든 사용자 역할에서 사용할 수 있으나 이벤트 보기 권한이 없는 사용자에게는 별 의미가 없습니다.

다음 필드가 Event Preferences 섹션에 나타납니다.

- **Confirm "All" Actions** 필드는 어플라이언스에서 이벤트 보기의 모든 이벤트에 적용될 작업에 대해 반드시 사용자에게 확인하는지 여부를 제어합니다.

  예를 들어 이 설정이 활성화된 상태에서 이벤트 보기의 **Delete All**을 클릭할 경우, 현재 제약 조건을 충족하는 모든 이벤트(현재 페이지에 표시되지 않은 이벤트 포함)를 삭제할 것임을 사용자가 확인해야 어플라이언스가 데이터베이스에서 이를 삭제합니다.

- **Resolve IP Addresses** 필드는 어플라이언스에서 이벤트 보기에 가급적 IP 주소 대신 호스트 이름을 표시할 수 있게 합니다.

  많은 IP 주소가 포함되었는데 이 옵션을 활성화한 경우 이벤트 보기를 표시하는 속도가 느려질 수 있습니다. 또한 이 설정이 적용되려면 시스템 설정에 DNS 서버가 구성되어 있어야 합니다. 64-8페이지의 관리 인터페이스 구성을/를 참조하십시오.

- **Expand Packet View** 필드에서는 침입 이벤트에 대한 패킷 보기가 나타나는 방식을 구성할 수 있습니다. 기본적으로 어플라이언스는 패킷 보기의 축소 버전을 표시합니다.
  - **None** - 패킷 보기 중 Packet Information 섹션의 모든 하위 섹션을 축소합니다.
  - **Packet Text** - Packet Text 하위 섹션만 확장합니다.
  - **Packet Bytes** - Packet Bytes 하위 섹션만 확장합니다.
  - **All** - 모든 섹션을 확장합니다.

  기본 설정과 무관하게 언제라도 패킷 보기에서 섹션을 수동 확장하여 캡처된 패킷에 대한 세부 정보를 볼 수 있습니다. 패킷 보기에 대한 자세한 내용은 41-22페이지의 패킷 보기 사용을/를 참조하십시오.

- **Rows Per Page** 필드에서는 페이지당 몇 개의 이벤트 행을 드릴다운 페이지 및 테이블 보기에 표시할 것인지를 제어합니다.

- **Refresh Interval** 필드에서는 이벤트 보기의 새로 고침 간격을 분 단위로 설정합니다. 0을 입력하면 새로 고침 옵션이 비활성화됩니다. 이 간격은 대시보드에 적용되지 않습니다.

- **Statistics Refresh Interval**은 Intrusion Event Statistics 페이지, Discovery Statistics 페이지와 같은 이벤트 요약 페이지의 새로 고침 간격을 제어합니다. 0을 입력하면 새로 고침 옵션이 비활성화됩니다. 이 간격은 대시보드에 적용되지 않습니다.

- **Deactivate Rules** 필드는 표준 텍스트 규칙에 의해 생성된 침입 이벤트의 패킷 보기에 어떤 링크가 나타날 것인지를 제어합니다.
  - **All Policies** - 로컬에 정의된 모든 사용자 지정 침입 정책에서 표준 텍스트 규칙을 비활성화하는 단일 링크
  - **Current Policy** - 현재 적용된 침입 정책에서만 표준 텍스트 규칙을 비활성화하는 단일 링크 기본 정책의 규칙은 비활성화할 수 없습니다.
  - **Ask** - 이 옵션 각각의 링크

  패킷 보기에서 이 링크를 표시하려면 사용자 계정이 관리자 또는 침입 관리자 액세스 권한을 가져야 합니다.

파일 환경 설정

라이센스: 모두

지원되는 디바이스: 기능에 따라

지원되는 Defense Center: 기능에 따라

로컬 파일 다운로드의 기본 특성을 구성하려면 Event View Settings 페이지의 File Preferences 섹션을 사용합니다. 이 섹션은 관리자, 보안 분석가 또는 보안 분석가(읽기 전용) 사용자 역할만 사용할 수 있습니다.

어플라이언스에서 캡처된 파일의 다운로드를 지원하지 않을 경우 이 옵션은 비활성화됩니다. 악성코드 라이센스를 DC500과 함께 사용할 수 없으므로 이 어플라이언스에서는 파일 다운로드 또는 이 옵션의 수정이 불가합니다.

다음 필드가 File Preferences 섹션에 나타납니다.

- **Confirm 'Download File' Actions** 확인란은 파일을 다운로드할 때마다 File Download 팝업 창이 나타나 경고를 표시하고 계속 또는 취소를 선택하게 할지를 제어합니다.

주의 Cisco 사용자는 유해한 결과로 이어질 수 있는 악성코드를 다운로드해서는 **안 됩니다**. 어떤 파일을 다운로드할 때 악성코드를 포함했을 수도 있으므로 각별히 주의하십시오. 파일을 다운로드하기 전에 다운로드할 위치를 보호하기 위해 필요한 모든 예방 조치를 취해야 합니다.

파일을 다운로드할 때 언제라도 이 옵션을 비활성화할 수 있습니다. 파일 다운로드에 대한 자세한 내용은 40-4페이지의 다른 위치에 저장된 파일 다운로드을/를 참조하십시오.

- 캡처된 파일을 다운로드할 때 비밀번호로 보호되는 .zip 아카이브가 생성되며 여기에 파일이 들어 있습니다. **Zip File Password** 필드에서는 .zip 파일에 대한 액세스 권한을 제한하기 위해 사용할 비밀번호를 정의합니다. 이 필드를 비워 둘 경우 비밀번호 없이 아카이브 파일이 생성됩니다.
- **Show Zip File Password** 확인란에서는 **Zip File Password** 파일에 일반 텍스트 아니면 난독 문자를 표시할지 선택합니다. 이 필드의 값을 지우면 **Zip File Password**는 난독 문자를 표시합니다.

기본 시간 창

라이센스: 모두

시간 범위라고도 하는 시간 창은 임의의 이벤트 보기에서 이벤트에 대한 시간 제약 조건을 부여합니다. 시간 창의 기본 동작을 제어하려면 Event View Settings 페이지의 Default Time Windows 섹션을 사용합니다.

이 섹션에 대한 사용자 역할 액세스 권한은 다음과 같습니다.

- 관리자 및 유지 보수 사용자는 전체 섹션에 액세스할 수 있습니다.
- 보안 분석가 및 보안 분석가(읽기 전용)는 **Audit Log Time Window**를 제외한 모든 옵션에 액세스할 수 있습니다.
- 액세스 관리자, 검색 관리자, 외부 데이터베이스 사용자, 침입 관리자, 네트워크 관리자, 보안 승인자는 **Events Time Window** 옵션만 액세스할 수 있습니다.

기본 시간 창 설정과 무관하게 이벤트 분석 중 언제라도 개별 이벤트 보기의 시간 창을 수동 변경할 수 있습니다. 또한 시간 창 설정은 현재 세션에 대해서만 유효합니다. 로그아웃했다가 다시 로그인하면 시간 창은 이 페이지에서 구현한 기본값으로 재설정됩니다. 자세한 내용은 58-22페이지의 이벤트 시간 제약 조건 설정을/를 참조하십시오.

3가지 이벤트 유형에 대해 기본 시간 창을 설정할 수 있습니다.

- **Events Time Window**에서는 시간에 의한 제약이 가능한 대부분의 이벤트에 대해 단일 기본 시간 창을 설정합니다.
- **Audit Log Time Window**에서는 감사 로그에 대한 기본 시간 창을 설정합니다.
- **Health Monitoring Time Window**에서는 상태 이벤트에 대한 기본 시간 창을 설정합니다.

사용자 계정에서 액세스 가능한 이벤트 유형에 대해서만 시간 창을 설정할 수 있습니다. 모든 사용자 유형이 이벤트 시간 창을 설정할 수 있습니다. 관리자, 유지 보수 사용자, 보안 분석가는 상태 모니터링 시간 창을 설정할 수 있습니다. 관리자와 유지 보수 사용자는 감사 로그 시간 창을 설정할 수 있습니다.

모든 이벤트 보기가 시간에 의한 제약이 가능하지는 않으므로, 시간 창 설정은 호스트, 호스트 특성, 애플리케이션, 클라이언트, 취약점, 사용자 ID 또는 화이트리스트 위반을 표시하는 이벤트 보기에는 적용되지 않습니다.

이벤트 유형별로 하나씩 **Multiple** 시간 창을 사용하거나 모든 이벤트에 적용되는 **Single** 시간 창을 사용할 수 있습니다. 단일 시간 창을 사용할 경우 3가지 시간 창 유형에 대한 설정이 사라지고 새로운 **Global Time Window** 설정이 나타납니다.

시간 창에는 3가지 유형이 있습니다.

- *고정(static)* 유형은 특정 시작 시간부터 종료 시간까지 생성된 모든 이벤트를 표시합니다.
- *확장(expanding)* 유형은 특정 시작 시간부터 현재까지 생성된 모든 이벤트를 표시합니다. 시간이 흐르면서 시간 창이 확장되고 새 이벤트가 이벤트 보기에 추가됩니다.
- *슬라이딩(sliding)* 유형은 특정 시작 시간(예: 1일 전)부터 현재까지 생성된 모든 이벤트를 표시합니다. 시간이 흐르면서 시간 창이 "슬라이딩"하므로 구성된 범위(이 예에서는 지난 1일)의 이벤트만 볼 수 있습니다.

모든 시간 창의 최대 시간 범위는 1970년 1월 1일 자정(UTC)부터 2038년 1월 19일 오전 03:14:07(UTC)까지입니다.

다음 옵션이 **Time Window Settings** 드롭다운 목록에 나타납니다.

- **Show the Last - Sliding** 옵션에서는 사용자가 지정한 길이의 슬라이딩 기본 시간 창을 구성할 수 있습니다.

  어플라이언스는 특정 시작 시간(예: 1시간 전)부터 현재까지 생성된 모든 이벤트를 표시합니다. 이벤트 보기를 변경하면 시간 창이 "슬라이딩"하므로 항상 지난 1시간의 이벤트가 표시됩니다.

- **Show the Last - Static/Expanding** 옵션에서는 사용자가 지정한 길이의 고정 또는 확장 기본 시간 창을 구성할 수 있습니다.

  static 시간 창에서는 **Use End Time** 확인란을 활성화합니다. 어플라이언스는 특정 시작 시간(예: 1시간 전)부터 사용자가 처음으로 이벤트를 본 시점까지 생성된 모든 이벤트를 표시합니다. 이벤트 보기를 변경할 때 시간 창이 고정되어 있으므로 고정 시간 창에 발생한 이벤트만 표시됩니다.

  expanding 시간 창에서는 **Use End Time** 확인란을 비활성화합니다. 어플라이언스는 특정 시작 시간(예: 1시간 전)부터 현재까지 생성된 모든 이벤트를 표시합니다. 이벤트 보기를 변경할 때 시간 창이 현재 시간으로 확장됩니다.

- **Current Day - Static/Expanding** 옵션에서는 현재 일에 대해 고정 또는 확장 기본 시간 창을 구성할 수 있습니다. 현재 일은 현재 세션의 표준 시간대 설정에 따라 자정에 시작합니다.

  static 시간 창에서는 **Use End Time** 확인란을 활성화합니다. 어플라이언스는 자정부터 사용자가 처음으로 이벤트를 본 시점까지 생성된 모든 이벤트를 표시합니다. 이벤트 보기를 변경할 때 시간 창이 고정되어 있으므로 고정 시간 창에 발생한 이벤트만 표시됩니다.

expanding 시간 창에서는 **Use End Time** 확인란을 비활성화합니다. 어플라이언스는 자정부터 현재까지 생성된 모든 이벤트를 표시합니다. 이벤트 보기를 변경할 때 시간 창이 현재 시간으로 확장됩니다. 로그아웃하기 전 24시간 이상 분석이 계속될 경우 이 시간 창이 24시간을 초과할 수 있습니다.

- **Current Week - Static/Expanding** 옵션에서는 현재 주에 대해 고정 또는 확장 기본 시간 창을 구성할 수 있습니다. 현재 주는 현재 세션의 표준 시간대 설정에 따라 이전 일요일 자정에 시작합니다.

  static 시간 창에서는 **Use End Time** 확인란을 활성화합니다. 어플라이언스는 자정부터 사용자가 처음으로 이벤트를 본 시점까지 생성된 모든 이벤트를 표시합니다. 이벤트 보기를 변경할 때 시간 창이 고정되어 있으므로 고정 시간 창에 발생한 이벤트만 표시됩니다.

  expanding 시간 창에서는 **Use End Time** 확인란을 비활성화합니다. 어플라이언스는 일요일 자정부터 현재까지 생성된 모든 이벤트를 표시합니다. 이벤트 보기를 변경할 때 시간 창이 현재 시간으로 확장됩니다. 로그아웃하기 전 1주일 이상 분석이 계속될 경우 이 시간 창이 1주를 초과할 수 있습니다.

기본 워크플로

라이센스: 모두

워크플로는 분석가가 이벤트 평가에 사용하는 데이터를 표시하는 일련의 페이지입니다. 어플라이언스는 이벤트 유형별로 하나 이상의 사전 정의된 워크플로를 기본적으로 제공합니다. 예를 들어 보안 분석가라면 수행하는 분석 유형에 따라 10가지 침입 이벤트 워크플로 중에서 선택할 수 있으며, 각 워크플로는 각기 다른 방식으로 침입 이벤트 데이터를 전달합니다.

어플라이언스는 이벤트 유형별로 하나의 기본 워크플로가 구성되어 있습니다. 예를 들어 Events by Priority and Classification 워크플로는 침입 이벤트의 기본 워크플로입니다. 즉 침입 이벤트(검토된 침입 이벤트 포함)를 볼 때마다 Events by Priority and Classification 워크플로가 표시됩니다.

그러나 Event View Settings 페이지의 Default Workflows 섹션을 사용하여 각 이벤트 유형의 기본 워크플로를 변경할 수 있습니다.

구성 가능한 기본 워크플로는 사용자 역할에 따라 달라집니다. 예를 들어 침입 이벤트 분석가는 기본 검색 이벤트 워크플로를 설정할 수 없습니다. 워크플로에 대한 일반적인 정보는 58-1페이지의 워크플로의 이해 및 사용을/를 참조하십시오.

기본 표준 시간대 설정

라이센스: 모두

이벤트 표시에 쓰이는 표준 시간대를 어플라이언스에서 사용하는 표준 UTC 시간과 다른 시간대로 변경할 수 있습니다. 표준 시간대를 구성하면 해당 사용자 계정에만 적용되며 표준 시간대를 추가로 변경할 때까지 유효합니다.

주의 표준 시간대 기능에서는 기본 시스템 시계가 UTC 시간으로 설정되었다고 가정합니다. 현지 표준 시간대를 사용하도록 어플라이언스의 시스템 시계를 변경한 경우 어플라이언스에서 정확한 현지 시간을 보려면 UTC 시간으로 되돌려야 합니다. 방어 센터와 관리되는 디바이스 간의 시간 동기화에 대한 자세한 내용은 63-25페이지의 시간 동기화을/를 참조하십시오.

표준 시간대를 변경하려면

액세스: 모두

1단계 사용자 이름 아래의 드롭다운 목록에서 **User Preferences**를 선택합니다.

Change Password 페이지가 나타납니다.

2단계 **Time Zone Settings**를 클릭합니다.

Time Zone Preference 페이지가 나타납니다.

3단계 왼쪽 목록 상자에서 사용할 표준 시간대가 속한 대륙이나 지역을 선택합니다.

예를 들어 북미, 남미 또는 캐나다의 표준 시간대를 사용하려면 **America**를 선택합니다.

4단계 오른쪽 목록 상자에서 사용할 표준 시간대에 해당하는 지역(도시 이름)을 선택합니다.

예를 들어 동부 표준시를 사용하려면 첫 번째 표준 시간대 상자에서 **America**를 선택한 다음 **New York**을 선택합니다.

5단계 **Save**를 클릭합니다.

표준 시간대가 설정되었습니다.

기본 대시보드 지정

라이센스: 모두

어플라이언스의 대시보드 중 하나를 기본 대시보드로 지정할 수 있습니다. 기본 대시보드는 **Overview > Dashboards**를 선택하면 나타납니다. 기본 대시보드가 정의되지 않은 경우 Dashboard List 페이지가 나타납니다. 대시보드에 대한 일반적인 정보는 55-1페이지의 대시보드 사용을/를 참조하십시오.

기본 대시보드를 지정하려면

액세스: Admin/Maint/Any Security Analyst

1단계 사용자 이름 아래의 드롭다운 목록에서 **User Preferences**를 선택합니다.

Change Password 페이지가 나타납니다.

2단계 **Dashboard Settings**를 클릭합니다.

Dashboard Settings 페이지가 나타납니다.

3단계 기본 대시보드로 사용할 대시보드를 드롭다운 목록에서 선택합니다.

None을 선택한 경우 **Overview > Dashboards**를 선택하면 Dashboard List 페이지가 나타납니다. 그러면 표시할 대시보드를 선택할 수 있습니다.

4단계 **Save**를 클릭합니다.

기본 대시보드 환경 설정이 저장되었습니다.

컨피그레이션 가져오기 및 내보내기

가져오기/내보내기 기능을 사용하면 정책을 비롯한 여러 유형의 컨피그레이션을 한 어플라이언스에서 동일한 유형의 다른 어플라이언스로 복사할 수 있습니다. 컨피그레이션 가져오기 및 내보내기는 백업 툴로 사용하기 위한 것이 아니라, FireSIGHT 시스템에 새 어플라이언스를 추가하는 프로세스를 간소화하는 데 사용할 수 있습니다.

다음 컨피그레이션을 가져오고 내보낼 수 있습니다.

- 액세스 제어 정책 및 관련 네트워크 분석, SSL, 파일 정책
- 침입 정책
- 상태 및 시스템 정책
- 알림 응답
- 애플리케이션 탐지기
- 대시보드, 사용자 지정 테이블, 사용자 지정 워크플로 및 저장된 검색
- 사용자 지정 사용자 역할
- 보고서 템플릿
- 서드파티 제품 및 취약성 매핑

내보낸 컨피그레이션을 가져오려면 두 어플라이언스가 모두 FireSIGHT 시스템의 동일한 버전을 실행해야 합니다. 내보낸 침입 또는 액세스 제어 정책을 가져오려면 두 어플라이언스의 규칙 업데이트 버전도 일치해야 합니다.

자세한 내용은 다음 절을 참조하십시오.

- A-2페이지의 컨피그레이션 내보내기
- A-5페이지의 컨피그레이션 가져오기

컨피그레이션 내보내기

라이센스: 모두

단일 컨피그레이션을 내보낼 수도 있고, 동일한 유형 또는 서로 다른 유형의 컨피그레이션 집합을 동시에 내보낼 수도 있습니다. 나중에 패키지를 다른 어플라이언스로 가져올 때 패키지의 어떤 컨피그레이션을 가져올지 선택할 수 있습니다.

컨피그레이션을 내보낼 때 어플라이언스는 해당 컨피그레이션의 개정 정보도 내보냅니다. FireSIGHT 시스템에서는 이 정보를 사용하여 해당 컨피그레이션을 다른 어플라이언스로 가져올 수 있는지를 결정합니다. 이미 어플라이언스에 있는 컨피그레이션 개정은 가져올 수 없습니다.

또한 컨피그레이션을 내보낼 때 어플라이언스는 컨피그레이션이 의존하는 시스템 컨피그레이션(예: 인증 객체)도 내보냅니다. 예를 들어 방어 센터에서 LDAP 서버에 대한 인증을 설정한 다음 방어 센터 시스템 정책을 활성화된 인증과 함께 내보내면 인증 객체도 함께 내보내게 됩니다.

팁 FireSIGHT 시스템의 목록 페이지 중 다수에는 목록 항목 옆에 내보내기 아이콘( )이 있습니다. 이 아이콘이 있으면 내보내기 절차의 빠른 대안으로서 사용할 수 있습니다.

다음 컨피그레이션을 내보낼 수 있습니다.

- *알림 응답* - 알림 응답은 알림을 전송할 외부 시스템과 FireSIGHT 시스템의 상호 작용을 허용하는 컨피그레이션 집합입니다.
- *사용자 지정 테이블* - 사용자 지정 테이블은 FireSIGHT 시스템에서 제공된 둘 이상의 사전 정의 테이블에서 온 필드를 결합하여 만들 수 있는 테이블입니다.
- *사용자 지정 사용자 역할* - 사용자 지정 사용자 역할은 액세스 권한의 특수 집합으로 생성하는 사용자 역할입니다. 저장된 검색을 요구하는 사용자 지정 사용자 역할을 내보내면 필요한 모든 저장된 검색도 함께 내보내게 됩니다.
- *사용자 지정 워크플로* - 사용자 지정 워크플로는 조직의 고유한 필요에 맞게 생성하는 워크플로입니다. 방어 센터에서는 자신이 만든 사용자 지정 워크플로는 물론 어플라이언스와 함께 제공된 사전 정의 사용자 지정 워크플로도 내보낼 수 있습니다.

  내보낸 사용자 지정 워크플로의 기반이 되는 테이블을 방어 센터에서 볼 수 없는 경우, 워크플로를 가져올 수는 있지만 볼 수는 없습니다.
- *Dashboards* - 대시보드는 현재 시스템 상태를 한눈에 볼 수 있는, 탭으로 구성된 사용자 지정 가능한 보기입니다. 구축에 포함된 어플라이언스의 전체적인 상태에 대한 정보는 물론 FireSIGHT 시스템에서 수집 및 생성한 데이터를 보여주기 위해 대시보드에는 다양한 위젯이 사용됩니다.

  표시되는 대시보드 위젯은 사용 중인 어플라이언스 유형 및 사용자 역할에 따라 달라집니다. 자세한 내용은 55-4페이지의 위젯 가용성 이해을/를 참조하십시오.
- *액세스 제어 정책* - 액세스 제어 정책에는 시스템이 네트워크의 트래픽을 관리하는 방법을 결정하기 위해 구성할 수 있는 다양한 구성 요소가 포함되어 있습니다. 이러한 구성 요소에는 액세스 제어 규칙, 관련 침입, 파일, 네트워크 분석, SSL 정책, 규칙과 정책에서 사용하는 객체(침입 변수 집합 포함) 등이 포함됩니다. 액세스 제어 정책을 내보내면 정책에 대한 모든 설정과 구성 요소도 내보내게 됩니다. 단, 모든 어플라이언스에서 동일하며 사용자가 변경할 수 없는 URL 평가 및 카테고리는 제외됩니다. 액세스 제어 정책을 가져오려면, 내보내고 가져오는 방어 센터의 규칙 업데이트 버전이 일치해야 합니다.

  내보내는 액세스 제어 정책 또는 이 정책이 호출하는 SSL 정책에 지오로케이션 데이터를 참조하는 규칙이 포함되어 있으면, 가져오는 방어 센터의 GeoDB(지오로케이션 데이터베이스) 업데이트 버전이 사용됩니다.

개인 키 정보가 포함된 PKI 객체는, 어플라이언스에 저장될 때 무작위로 생성되는 키로 암호화됩니다. 내보내는 액세스 제어 정책이 개인 키가 포함된 PKI 객체를 사용하는 SSL 정책을 참조하는 경우 개인 키는 내보내기 전에 해독됩니다.

내보내는 액세스 제어 정책이 지원되지 않는 DC500 또는 Series 2 디바이스 정책 기능이나 규칙 조건을 참조하는 경우 DC500을 사용하여 정책을 적용할 수 없으며 Series 2 디바이스에 정책을 적용할 수 없습니다. DC500과 Series 2 디바이스 모두 Block Malware나 Malware Cloud Lookup 작업을 사용하는 규칙이 포함된 파일 정책, 보안 인텔리전스, 사용자 또는 URL 규칙 조건을 지원하지 않습니다. Series 2 디바이스는 애플리케이션 규칙 조건도 지원하지 않습니다.

- *상태 정책* - 상태 정책에는 구축에 포함된 어플라이언스의 상태(Cisco 하드웨어 및 소프트웨어가 제대로 작동하는지 여부)를 확인할 때 사용되는 기준이 포함되어 있습니다.
- *침입 정책* - 침입 정책에는 네트워크에서 침입 및 정책 위반을 검사하기 위해 구성할 수 있는 다양한 구성 요소가 포함되어 있습니다. 이러한 구성 요소는 프로토콜 헤더 값, 페이로드 내용 및 특정 패킷 크기 특성을 검사하는 침입 규칙, FireSIGHT 권장 규칙 컨피그레이션 및 기타 고급 설정으로 구성됩니다.

  침입 정책을 내보내면 정책에 대한 모든 설정도 내보내게 됩니다. 예를 들어, 이벤트를 생성하기 위한 규칙을 설정하거나, 규칙에 대한 SNMP 알림을 설정하거나, 정책에서 민감한 데이터 프리프로세서를 설정하는 경우 내보낸 정책에서도 그러한 설정은 그대로 유지됩니다. 사용자 지정 규칙, 사용자 지정 규칙 분류 및 사용자 정의 변수 역시 정책과 함께 내보내게 됩니다.

  두 번째 침입 정책과 공유되는 레이어를 사용하는 침입 정책을 내보내는 경우, 해당 공유 레이어는 내보내는 정책에 복사되며 공유 관계는 해제됩니다. 다른 어플라이언스로 침입 정책을 가져오면, 레이어를 삭제, 추가 및 공유하는 등 가져온 정책을 필요에 맞게 수정할 수 있습니다.

  한 방어 센터에서 다른 곳으로 침입 정책을 내보내는 경우, 두 번째 방어 센터에서 기본 변수가 다르게 구성되어 있으면 가져온 정책이 다르게 작동할 수 있습니다.

참고 가져오기/내보내기 기능은 Cisco의 VRT(Vulnerability Research Team)에서 생성한 규칙을 업데이트하는 데 사용할 수 없습니다. 대신, 최신 규칙 업데이트 버전을 다운로드하여 적용할 수 있습니다. 66-14페이지의 규칙 업데이트 및 로컬 규칙 파일 가져오기을/를 참조하십시오.

- *보고서 템플릿* - 보고서는 특정 FireSIGHT 시스템 데이터를 취합하는 PDF, HTML 또는 CSV의 문서 파일입니다. 보고서 템플릿은 보고서 및 보고서 섹션에 대한 데이터 검색과 형식을 지정합니다. 보고서 템플릿을 내보내면 모든 저장된 검색, 이미지, 객체 관리자에서 생성한 객체, 보고서에 필요한 사용자 지정 테이블도 함께 내보내게 됩니다.
- *저장된 검색* - 저장된 검색은 제한된 권한을 보유한 사용자에게 사전 정의 FireSIGHT 시스템 데이터에 대한 액세스를 제공합니다. 저장된 검색을 요구하는 사용자 지정 사용자 역할을 내보내면 필요한 저장된 검색도 함께 내보내게 됩니다. 개별 사용자 정의 저장된 검색도 내보낼 수 있습니다.
- *SSL 정책* - SSL 정책에는 SSL 규칙 및 참조 재사용 가능한 객체를 포함하여, 시스템이 네트워크의 암호화된 트래픽을 관리하는 방법을 결정하기 위해 구성할 수 있는 다양한 구성 요소가 포함되어 있습니다. SSL 정책을 내보내면 정책에 대한 모든 설정과 구성 요소도 함께 내보내게 됩니다. 단, 모든 어플라이언스에서 동일하며 사용자가 변경할 수 없는 URL 평가 및 카테고리는 제외됩니다. SSL 정책을 가져오려면, 내보내고 가져오는 방어 센터의 규칙 업데이트 버전이 일치해야 합니다.

  개인 키 정보가 포함된 PKI 객체는, 어플라이언스에 저장될 때 무작위로 생성되는 키로 암호화됩니다. 내보내는 SSL 정책이 개인 키가 포함된 PKI 객체를 사용하는 경우, 개인 키는 내보내기 전에 해독됩니다.

  내보내는 SSL 정책에 지오로케이션 데이터를 참조하는 규칙이 포함되어 있으면, 가져오는 방어 센터의 GeoDB(지오로케이션 데이터베이스) 업데이트 버전이 사용됩니다.

- *시스템 정책* - 시스템 정책은 데이터베이스 이벤트 제한, 시간 설정, 로그인 배너 등 구축의 다른 FireSIGHT 시스템 어플라이언스와 유사할 수 있는 어플라이언스의 여러 부분을 제어합니다.

  내보내는 시스템 정책에서 외부 인증이 활성화되면 관련 인증 객체도 함께 내보내게 됩니다.

  방어 센터의 시스템 정책에는 관리되는 디바이스에 적용되지 않는 데이터베이스 설정이 포함됩니다. 관리되는 디바이스에서 시스템 정책을 내보내고 방어 센터로 가져오면, 디바이스에서 구성할 수 없는 데이터베이스 제한은 방어 센터에서 기본값으로 설정됩니다.
- *서드파티 제품 매핑* - 서드파티 애플리케이션에서 데이터를 가져오는 경우 취약성을 할당하고 해당 데이터로 영향 상관관계를 수행하려면 제품을 서드파티 이름에 매핑해야 합니다. 제품을 매핑하면 Cisco 취약성 정보가 서드파티 제품 이름과 연결되며, 이를 통해 FireSIGHT 시스템에서는 해당 데이터를 사용해 영향 상관관계를 수행할 수 있습니다. 서드파티 제품 매핑 생성에 대한 자세한 내용은 46-31페이지의 서드파티 제품 매핑을/를 참조하십시오.
- *서드파티 취약성 매핑* - 서드파티 애플리케이션의 취약성 정보를 취약성 데이터베이스에 추가하려면 가져온 각 취약성에 대한 서드파티 식별 문자열을 기존의 Cisco, Bugtraq 또는 Snort ID에 매핑해야 합니다. 취약성에 대한 매핑을 생성하면 네트워크 맵에서 호스트로 가져온 모든 취약성에 대해 매핑이 제대로 작동하며, 그러한 취약성에 대해 영향 상관관계를 수행할 수 있게 됩니다. 서드파티 취약성 매핑에 대한 자세한 내용은 46-33페이지의 서드파티 취약성 매핑을/를 참조하십시오.
- *애플리케이션 탐지기* - 시스템은 IP 트래픽을 분석할 때 탐지기를 사용하여 정보를 수집하고, 네트워크의 호스트에서 실행 중인 일반적으로 사용되는 애플리케이션을 식별합니다. 두 가지 종류의 탐지기를 내보낼 수 있습니다. 하나는 사용자 정의 탐지기이고, 다른 하나는 Cisco Professional Services에서 제공하는 개별 애드온 탐지기입니다. 탐지기에 대한 자세한 내용은 46-17페이지의 애플리케이션 탐지기 작업을/를 참조하십시오.

참고 내보내는 컨피그레이션 수 및 그러한 컨피그레이션이 참조하는 객체의 수에 따라 내보내기 프로세스가 몇 분 정도 걸릴 수 있습니다.

하나 이상의 컨피그레이션을 내보내려면

액세스: Admin

1단계 컨피그레이션을 내보내는 어플라이언스 및 컨피그레이션을 가져오려는 어플라이언스에서 동일한 버전의 FireSIGHT 시스템이 실행 중인지 확인합니다. 침입 또는 액세스 제어 정책을 내보내는 경우 규칙 업데이트 버전이 일치하는지 확인합니다.

FireSIGHT 시스템(및 해당되는 경우 규칙 업데이트 버전)의 버전이 일치하지 않으면 가져오기가 실패합니다.

2단계 **Systems > Tools > Import/Export**를 선택합니다.

어플라이언스에 대한 컨피그레이션 목록이 포함된 Import/Export 페이지가 나타납니다. 내보낼 컨피그레이션이 없는 컨피그레이션 카테고리는 이 목록에 나타나지 않습니다.

팁 컨피그레이션 목록을 축소하려면 컨피그레이션 옆에 있는 축소 아이콘( )을 클릭할 수 있습니다. 컨피그레이션을 표시하려면 컨피그레이션 옆에 있는 폴더 확장 아이콘( )을 클릭합니다.

3단계 내보낼 컨피그레이션 옆에 있는 확인란을 선택한 다음 **Export**를 클릭합니다.

4단계 웹 브라우저의 지침에 따라, 내보낸 패키지를 컴퓨터에 저장합니다.

컨피그레이션 가져오기

라이센스: 모두

어플라이언스에서 컨피그레이션을 내보냈으면, 이를 지원하는 다른 어플라이언스로 가져올 수 있습니다. 그러나 사용 중인 어플라이언스 및 사용자 역할에 따라 일부 가져온 컨피그레이션은 유용하지 않을 수 있습니다.

가져오는 컨피그레이션 유형에 따라 다음 사항에 유의해야 합니다.

- 컨피그레이션을 가져오는 어플라이언스가 컨피그레이션을 내보내는 데 사용한 어플라이언스와 동일한 버전의 FireSIGHT 시스템을 실행 중인지 확인해야 합니다. 침입 또는 액세스 제어 정책을 가져오려면 두 어플라이언스의 규칙 업데이트 버전도 일치해야 합니다. 버전이 일치하지 않으면 가져오기가 실패합니다.
- 저장된 검색을 요구하는 사용자 지정 사용자 역할을 가져오면 필요한 저장된 검색도 함께 가져오게 됩니다.
- 볼 수 있는 대시보드 위젯은 사용 중인 어플라이언스의 유형 및 사용자 역할에 따라 다릅니다. 예를 들어 방어 센터에서 생성하여 관리되는 디바이스에 가져온 대시보드에는 몇몇 비활성화되고 잘못된 위젯이 표시될 수 있습니다.
- 영역을 기반으로 트래픽을 평가하는 액세스 제어 정책을 가져오는 경우, 가져온 정책의 영역을 가져오는 방어 센터에 의해 관리되는 디바이스의 영역에 매핑해야 합니다. 영역을 매핑할 때에는 유형도 일치해야 합니다. 따라서 가져오기를 시작하기 전에, 가져오는 방어 센터에서 필요한 영역 유형을 생성해야 합니다. 보안 영역에 대한 자세한 내용은 3-38페이지의 보안 영역 작업을/를 참조하십시오.
- 기존 객체 또는 그룹에 대해 동일한 이름이 있는 객체나 객체 그룹이 포함된 저장된 검색 또는 액세스 제어 정책을 가져오는 경우 객체 또는 그룹의 이름을 변경해야 합니다.
- 액세스 제어 정책 또는 침입 정책을 가져오는 경우, 가져오기 프로세스 중에 기존 변수 집합의 기존 기본 변수가 가져온 기본 변수로 교체됩니다. 가져온 기본 변수 집합에 없는 사용자 지정 변수가 기존 기본 변수 집합에 포함되어 있으면, 고유한 변수가 유지됩니다.
- 공유 레이어를 사용한 침입 정책을 두 번째 침입 정책에서 가져오는 경우, 내보내기 프로세스 중에 공유 관계가 해제되고 전에 공유한 레이어가 패키지로 복사됩니다. 다시 말하면, 가져온 침입 정책에는 공유 레이어가 포함되지 않습니다.

참고 가져오기/내보내기 기능은 Cisco의 VRT(Vulnerability Research Team)에서 생성한 규칙을 업데이트하는 데 사용할 수 없습니다. 대신, 최신 규칙 업데이트 버전을 다운로드하여 적용할 수 있습니다. 66-14페이지의 규칙 업데이트 및 로컬 규칙 파일 가져오기을/를 참조하십시오.

- 개인 키를 포함하는 PKI 객체를 참조하는 SSL 정책을 가져오는 경우, 어플라이언스에 저장되기 전에 무작위로 생성되는 키로 해당 키가 암호화됩니다.
- 외부 인증이 활성화된 방어 센터에서 내보낸 시스템 정책을 가져오면, 시스템 정책이 의존하는 인증 객체도 함께 가져오게 됩니다.

단일 패키지의 여러 컨피그레이션을 내보낼 수 있으므로 패키지를 가져올 때에는 패키지의 어떤 컨피그레이션을 가져올지 선택해야 합니다. 대상 어플라이언스에서 지원되는 컨피그레이션만 가져올 수 있습니다.

컨피그레이션을 가져오려 할 경우, 어플라이언스에서는 해당 컨피그레이션이 어플라이언스에 이미 있는지를 확인합니다. 충돌이 존재하는 경우 다음과 같이 할 수 있습니다.

- 기존 컨피그레이션 유지
- 기존 컨피그레이션을 새 컨피그레이션과 교체

- 최신 컨피그레이션 유지
- 컨피그레이션을 새 컨피그레이션으로 가져오기

컨피그레이션을 가져온 후 대상 시스템에서 컨피그레이션을 수정하고 다시 가져오는 경우, 어떤 컨피그레이션 버전을 유지할 것인지 선택해야 합니다.

가져오는 컨피그레이션 수 및 그러한 컨피그레이션이 참조하는 객체의 수에 따라 가져오기 프로세스가 몇 분 정도 걸릴 수 있습니다.

하나 이상의 컨피그레이션을 가져오려면

액세스: Admin

1단계 컨피그레이션을 내보내는 어플라이언스 및 컨피그레이션을 가져오려는 어플라이언스에서 동일한 버전의 FireSIGHT 시스템이 실행 중인지 확인합니다. 침입 또는 액세스 제어 정책을 가져오려는 경우 규칙 업데이트 버전이 일치하는지도 확인해야 합니다.

FireSIGHT 시스템(및 해당되는 경우 규칙 업데이트 버전)의 버전이 일치하지 않으면 가져오기가 실패합니다.

2단계 가져오고자 하는 컨피그레이션을 내보냅니다. A-2페이지의 컨피그레이션 내보내기을/를 참조하십시오.

3단계 컨피그레이션을 가져오려는 어플라이언스에서 **System > Tools > Import/Export**를 선택합니다.

Import/Export 페이지가 나타납니다.

팁 컨피그레이션 목록을 축소하려면 컨피그레이션 옆에 있는 축소 아이콘()을 클릭합니다. 컨피그레이션을 표시하려면 컨피그레이션 옆에 있는 폴더 확장 아이콘()을 클릭합니다.

4단계 **Upload Package**를 클릭합니다.

Upload Package 페이지가 나타납니다.

5단계 다음 2가지 옵션을 사용할 수 있습니다.

- 업로드하려는 패키지의 경로를 입력합니다.
- 패키지를 찾아보려면 **Browse**를 클릭합니다.

6단계 **Upload**를 클릭합니다.

업로드 결과는 패키지의 내용에 따라 달라집니다.

- 패키지의 컨피그레이션이 어플라이언스에 이미 있는 버전과 정확히 일치하는 경우 버전이 이미 있음을 알리는 메시지가 표시됩니다. 어플라이언스에 최신 컨피그레이션이 있으면 가져올 필요가 없습니다.
- 현재 어플라이언스와 패키지를 내보낸 어플라이언스 간에 FireSIGHT 시스템 또는 규칙 업데이트 버전(해당되는 경우) 불일치가 존재하는 경우, 패키지를 가져올 수 없음을 알리는 메시지가 표시됩니다. FireSIGHT 시스템 또는 규칙 업데이트 버전을 업데이트하고 프로세스를 다시 시도하십시오.
- 어플라이언스에 없는 컨피그레이션 또는 규칙 버전이 패키지에 포함되어 있는 경우 Package Import 페이지가 나타납니다. 다음 단계로 계속 진행합니다.

7단계 가져오려는 컨피그레이션을 선택하고 **Import**를 클릭합니다.

가져오기 프로세스가 진행되며 다음과 같은 결과가 나타납니다.

- 가져오는 컨피그레이션에 어플라이언스에 대한 이전 개정이 없으면 가져오기가 자동으로 완료되고 성공 메시지가 나타납니다. 나머지 절차는 건너뜁니다.

- 보안 영역이 포함된 액세스 제어 정책을 가져오면 Access Control Import Resolution 페이지가 나타납니다. 8단계로 계속 진행합니다.
- 가져오는 컨피그레이션에 어플라이언스에 대한 이전 개정이 있으면 Import Resolution 페이지가 나타납니다. 9단계로 계속 진행합니다.

8단계 각 수신 보안 영역 옆에서, 매핑할 매칭 유형의 기존 로컬 보안 영역을 선택하고 **Import**를 클릭합니다.

7단계로 돌아갑니다.

9단계 각 컨피그레이션을 확장하고 적절한 옵션을 선택합니다.

- 어플라이언스에 대한 컨피그레이션을 유지하려면 **Keep existing**을 선택합니다.
- 어플라이언스에 대한 컨피그레이션을 가져온 컨피그레이션으로 교체하려면 **Replace existing**을 선택합니다.
- 최신 컨피그레이션을 유지하려면 **Keep newest**를 선택합니다.
- 가져온 컨피그레이션을 새 컨피그레이션으로 저장하려면 **Import as new**를 선택하고, 선택적으로 컨피그레이션 이름을 수정합니다.

  활성화된 정상 목록 또는 사용자 지정 탐지 목록의 파일 정책이 포함된 액세스 제어 정책을 가져오는 경우 **Import as new** 옵션을 사용할 수 없습니다.
- 종속 객체가 포함된 저장된 검색 또는 액세스 제어 정책을 가져오는 경우, 제안 이름을 사용할 수도 있고 객체의 이름을 변경할 수도 있습니다. 시스템은 이러한 종속 객체를 항상 새로운 객체로 가져옵니다. 기존 객체를 유지 또는 교체할 옵션이 제공되지 않습니다. 시스템은 객체 또는 객체 그룹도 동일한 방식으로 취급합니다.

10단계 **Import**를 클릭합니다.

컨피그레이션 가져오기가 수행됩니다.

데이터베이스에서 검색 데이터 삭제

네트워크 검색 및 사용자 검색 이벤트 데이터베이스에서 파일을 삭제하려면 Discovery Data Purge 페이지를 사용할 수 있습니다. 데이터베이스를 삭제하면 해당 프로세스가 다시 시작됩니다.

주의 데이터베이스를 삭제하면 방어 센터에서 지정한 데이터가 제거됩니다. 삭제된 데이터는 복구할 수 **없습니다**.

네트워크 및 사용자 검색 데이터베이스를 삭제하려면

액세스: Admin/Any Security Analyst

1단계 **System > Tools > Data Purge**를 선택합니다.

Data Purge 페이지가 나타납니다.

2단계 **Network Discovery** 아래에서 다음 중 하나 또는 모두를 실행합니다.

- 데이터베이스에서 모든 네트워크 검색 이벤트를 제거하려면 **Network Discovery Events**를 선택합니다.
- 데이터베이스에서 모든 호스트 및 IOC 플래그를 제거하려면 **Hosts**를 선택합니다.
- 데이터베이스에서 모든 사용자 이벤트를 제거하려면 **User Activity**를 선택합니다.
- 데이터베이스에서 모든 사용자 로그인 및 사용자 기록 데이터를 제거하려면 **User Identities**를 선택합니다.

3단계 **Connections** 아래에서 다음 중 하나 또는 모두를 실행합니다.

- 데이터베이스에서 모든 연결 데이터를 제거하려면 **Connection Events**를 선택합니다.
- 데이터베이스에서 모든 연결 요약 데이터를 제거하려면 **Connection Summary Events**를 선택합니다.
- 데이터베이스에서 모든 보안 인텔리전스 데이터를 제거하려면 **Security Intelligence Events**를 선택합니다.

참고 **Connection Events**를 선택하는 경우 보안 인텔리전스 이벤트가 제거되지 않습니다. 보안 인텔리전스 데이터와의 연결은 여전히 보안 인텔리전스 이벤트 뷰어에 나타납니다. 마찬가지로, **Security Intelligence Events**를 선택하는 경우 보안 인텔리전스 데이터와 관련된 연결 이벤트가 제거되지 않습니다.

4단계 **Purge Selected Events**를 클릭합니다.

항목이 삭제되고 해당 프로세스가 다시 시작됩니다.

장기 실행 작업의 상태 보기

정책 적용이나 업데이트 설치 등 FireSIGHT 시스템에서 수행할 수 있는 일부 작업은 즉시 완료되는 것이 아니라 실행에 다소 시간이 걸립니다. 작업 대기열에서 이런 장기 실행 작업의 진행 상황을 확인할 수 있습니다. 작업 대기열이 성공적으로 실행되거나 실행되지 못한 경우도 작업 대기열에 보고됩니다.

자세한 내용은 다음 절을 참조하십시오.

작업 대기열 보기

라이센스: 모두

정책 적용이나 업데이트 설치 등의 장기 실행 작업을 수행할 경우 이러한 작업의 상태가 작업 대기열에 보고됩니다. 작업 대기열은 복잡한 작업에 대한 정보를 제공하고 완료 시 보고합니다.

Task Status 페이지에서 작업 대기열을 볼 수 있으며, 작업 대기열은 10초마다 새로 고쳐집니다. 시작한 작업의 상태를 항상 볼 수 있습니다. 사용자 계정에 Administrator 사용자 역할 또는 **View Other Users' Tasks** 권한이 활성화된 사용자 역할이 있으면, 누가 시작을 했는지와 상관없이 모든 작업의 상태를 볼 수 있습니다. 사용자 역할 구성에 대한 자세한 내용은 61-48페이지의 사용자 역할 구성을/를 참조하십시오.

Job Summary 절에는 다음 표에 설명된 대로 페이지에 나열된 작업의 상태가 표시됩니다.

표 C-1 작업 대기열 작업 유형

작업 유형	설명
Running	현재 진행 중인 작업의 수.
Waiting	실행 전에 진행 중인 작업이 완료되기를 기다리는 작업의 수.
Completed	성공적으로 완료된 작업의 수.
Retrying	자동으로 재시도 중인 작업의 수. 모든 작업을 재시도할 수 있는 것은 아닙니다.
Stopped	시스템 업데이트 때문에 중단된 작업의 수. 중단된 작업은 다시 시작할 수 없습니다. 작업 대기열에서 수동으로 삭제해야 합니다.
Failed	성공적으로 완료되지 않은 작업의 수.

Jobs 섹션에서는 짧은 설명, 작업이 시작된 시기, 작업의 현재 상태, 상태가 마지막으로 변경된 시기를 비롯한 각 작업에 대한 정보를 제공합니다. Network Discovery Policy Apply와 같은 동일한 유형의 작업이 작업 그룹에 함께 나타납니다.

Task Status 페이지가 빠르게 로드될 수 있도록 FireSIGHT 시스템은 1000개가 넘는 작업이 포함된 작업 그룹에서 가장 오래된 작업을 제거하는 것은 물론 한 달이 넘은 모든 Completed, Failed 및 Stopped 유형의 작업을 대기열에서 제거합니다. 대기열에서 수동으로 작업을 제거할 수도 있습니다. 자세한 내용은 작업 대기열 관리을/를 참조하십시오.

작업 대기열을 보려면

액세스: Admin/Maint/Network Admin/Security Approver/Security Analyst

1단계 다음 2가지 옵션을 사용할 수 있습니다.

- 작업을 수동으로 시작한 경우, 작업 시작 시 나타난 알림 상자에서 **Task Status** 링크를 클릭합니다.

  팝업 창에 Task Status 페이지가 나타납니다.
- 작업을 예약한 경우 또는 보고 있지 않은 페이지에서 작업을 시작한 경우 **System > Monitoring > Task Status**를 선택합니다.

  Task Status 페이지가 나타납니다.

Task Status 페이지에서 수행할 수 있는 작업에 대한 자세한 내용은 작업 대기열 관리을/를 참조하십시오.

작업 대기열 관리

라이센스: 모두

사용자 계정에 Administrator, Maintenance User, Network Admin, Security Approver 또는 Security Analyst 사용자 역할이 할당된 경우 다음 표에 설명된 대로, 작업 대기열을 보면서 수행할 수 있는 몇 가지 작업이 있습니다(C-1페이지의 작업 대기열 보기 참조).

표 C-2 작업 대기열 작업

목적	가능한 작업
작업 대기열에서 완료된 모든 작업 제거	**Remove Completed Jobs**를 클릭합니다.
작업 대기열에서 실패한 모든 작업 제거	**Remove Failed Jobs**를 클릭합니다.
작업 대기열에서 단일 작업 제거	삭제할 작업 옆에 있는 삭제 아이콘( )을 클릭합니다. 실행 중인 작업을 삭제할 수 없습니다. 실행 중인 작업을 삭제해야 하는 경우(예: 작업이 반복해서 실패함) 고객 지원에 문의하십시오.
작업 그룹 축소 및 작업 숨기기	확장된 작업 그룹 옆에 있는 열린 폴더 아이콘( )을 클릭합니다.
작업 그룹 확장 및 작업 보기	축소된 작업 그룹 옆에 있는 닫힌 폴더 아이콘( )을 클릭합니다.

명령줄 참조

이 부록에서는 FirePOWER 어플라이언스, 가상 디바이스 및 ASA FirePOWER 디바이스의 ASA FirePOWER 모듈에 대한 CLI(명령줄 인터페이스)에 대해 설명합니다. CLI를 사용하여 FireSIGHT 시스템을 보고 구성하며 문제를 해결할 수 있습니다.

참고 방어 센터, Series 2 어플라이언스, Cisco NGIPS for Blue Coat X-Series 또는 ASA FirePOWER 디바이스의 ASA 모듈에서는 명령줄 인터페이스가 지원되지 않습니다.

모드 이름으로 시작하는 명령 집합을 포함하는 다양한 CLI 모드(예: `show` 및 `configure`)가 있습니다. 모드로 들어간 다음 해당 모드 내에서 유효한 명령을 입력할 수도 있고, 어떤 모드에서든 전체 명령을 입력할 수도 있습니다. 예를 들어 Analyst1이라는 사용자 계정에 대한 정보를 표시하려면 CLI 프롬프트에서 다음을 입력할 수 있습니다.

```
show user Analyst1
```

전에 `show` 모드로 들어갔으면 CLI 프롬프트에서 다음을 입력합니다.

```
사용자 Analyst1
```

각 모드 내에서 사용자가 이용할 수 있는 명령은 사용자의 CLI 액세스에 따라 다릅니다. 사용자 계정을 만들 때 다음 CLI 액세스 레벨 중 하나를 할당할 수 있습니다.

- 기본

  사용자는 읽기 전용 액세스 권한을 가지고 있으며 시스템 성능에 영향을 미치는 명령을 실행할 수 없습니다.

- 컨피그레이션

  사용자는 읽기-쓰기 액세스 권한을 가지고 있으며 시스템 성능에 영향을 미치는 명령을 실행할 수 있습니다.

- 없음

  사용자는 셸에 로그인할 수 없습니다.

Series 3 디바이스에서는 웹 인터페이스의 User Management 페이지에서 명령줄 권한을 할당할 수 있습니다. 자세한 내용은 61-1페이지의 사용자 관리을/를 참조하십시오. 가상 디바이스 및 ASA FirePOWER 디바이스에서는 CLI 자체를 통해 명령줄 권한을 할당합니다.

참고 Series 3 디바이스를 재부팅하고 가능한 한 빨리 CLI에 로그인하면, 웹 인터페이스를 사용할 수 있을 때까지 감사 로그에 실행한 명령이 기록되지 않습니다.

CLI 명령은 대/소문자를 구분하지 않습니다. 단, 텍스트가 CLI 프레임워크의 일부가 아닌 매개 변수(예: 사용자 이름 및 검색 필터)는 제외입니다.

명령줄에 로그인하는 방법에 대한 자세한 내용은 2-1페이지의 어플라이언스에 로그인을/를 참조하십시오.

다음 절에서는 CLI 명령에 대해 설명합니다.

기본 CLI 명령

기본 CLI 명령은 CLI와 상호 작용하는 기능을 제공하며, 디바이스의 작동에는 영향을 미치지 않습니다. 기본 명령은 모든 CLI 사용자가 이용할 수 있습니다.

다음 절에서는 기본 명령에 대해 설명합니다.

configure password

현재 사용자가 자신의 비밀번호를 변경하도록 허용합니다. 이 명령을 실행하면 현재(또는 이전) 비밀번호를 입력하라는 CLI 프롬프트가 표시된 다음 새 비밀번호를 두 번 입력하라는 프롬프트가 표시됩니다.

액세스

기본

구문

```
configure password
```

예

```
> configure password
Enter current password:
Enter new password:
Confirm new password:
```

end

사용자를 기본 모드로 되돌립니다. (더 낮은 레벨의 CLI 컨텍스트에서 기본 모드로 사용자를 이동합니다.)

액세스

기본

구문

```
end
```

예

```
configure network ipv4> end
>
```

exit

CLI 컨텍스트를 다음으로 가장 높은 CLI 컨텍스트 레벨로 이동합니다. 기본 모드에서 이 명령을 실행하면 사용자가 현재 CLI 세션에서 로그아웃되며, `logout` CLI 명령 실행과 동일한 결과가 나타납니다.

액세스

기본

구문

```
exit
```

예

```
configure network ipv4> exit
configure network>
```

help

CLI 구문의 개요를 표시합니다.

액세스

기본

구문

```
help
```

예

```
> help
```

history

현재 세션의 명령줄 기록을 표시합니다.

액세스

기본

구문

```
history limit
```

여기서 *limit*는 기록 목록의 크기를 설정합니다. 크기를 무제한으로 설정하려면 영(0)을 입력합니다.

예

```
history 25
```

logout

현재 사용자를 현재 CLI 콘솔 세션에서 로그아웃합니다.

액세스

기본

구문

```
logout
```

예

```
> logout
```

? (물음표)

CLI 명령 및 매개 변수에 대한 상황별 도움말을 표시합니다. 물음표(?) 명령은 다음과 같이 사용하십시오.

- 현재 CLI 컨텍스트 내에서 사용 가능한 명령의 도움말을 표시하려면 명령 프롬프트에서 물음표(?)를 입력합니다.
- 특별한 문자 집합으로 시작되는 사용 가능한 명령 목록을 표시하려면 약식 명령 바로 뒤에 물음표(?)를 입력합니다.
- 명령의 공식적인 인수에 대한 도움말을 표시하려면 명령 프롬프트에서 인수 자리에 물음표(?)를 입력합니다.

물음표(?)는 콘솔로 다시 에코되지 않습니다.

액세스

기본

구문

```
?
abbreviated_command ?
command [arguments] ?
```

예

```
> ?
```

?? (이중 물음표)

CLI 명령 및 매개 변수에 대한 자세한 상황별 도움말을 표시합니다.

액세스

기본

구문

```
??
abbreviated_command end??
command [arguments] ??
```

예

```
> configure manager add ??
```

Show 명령

Show 명령은 디바이스의 상태에 대한 정보를 제공합니다. 이러한 명령은 디바이스의 운영 모드를 변경하지 않으며, 명령 실행 시 시스템 운영에 미치는 영향이 최소 수준입니다. 모든 CLI 사용자가 대부분의 show 명령을 이용할 수 있지만, 컨피그레이션 CLI 액세스 권한이 있는 사용자만 `show user` 명령을 실행할 수 있습니다.

다음 절에서는 show 명령에 대해 설명합니다.

access-control-config

보안 인텔리전스 설정, 참조된 SSL의 이름, 네트워크 분석, 침입, 파일 정책, 침입 변수 설정 데이터, 로깅 설정, 기타 고급 설정(정책 레벨 성능, 전처리, 일반 설정) 등 현재 적용된 액세스 제어 컨피그레이션을 표시합니다.

또한 소스 및 목적지 포트 데이터(ICMP 항목의 유형 및 코드 포함)와 같은 정책 관련 연결 정보와 각 액세스 제어 규칙과 일치하는 연결 수(히트 수)도 표시합니다.

액세스

기본

구문

```
show access-control-config
```

예

```
> show access-control-config
```

alarms

디바이스에서 현재 활성 상태인(failed/down) 하드웨어 알람을 표시합니다. 가상 디바이스 또는 ASA FirePOWER 디바이스에서는 이 명령을 이용할 수 없습니다.

액세스

기본

구문

```
show alarms
```

예

```
> show alarms
```

arp-tables

네트워크에 해당되는 Address Resolution Protocol 테이블을 표시합니다. 가상 디바이스 또는 ASA FirePOWER 디바이스에서는 이 명령을 이용할 수 없습니다.

액세스

기본

구문

```
show arp-tables
```

예

```
> show arp-tables
```

audit-log

감사 로그를 역시간순으로 표시합니다. 최근 감사 로그가 가장 먼저 나열됩니다.

액세스
기본

구문
```
show audit-log
```

예
```
> show audit-log
```

bypass

사용 중인 인라인 집합을 나열하고 이러한 집합의 bypass 모드 상태를 보여줍니다(normal 또는 bypass). 가상 디바이스 또는 ASA FirePOWER 디바이스에서는 이 명령을 이용할 수 없습니다.

액세스
기본

구문
```
show bypass
```

예
```
> show bypass
```

clustering

디바이스 클러스터링 컨피그레이션, 상태 및 멤버 스택에 대한 정보를 표시합니다. 가상 디바이스 또는 ASA FirePOWER 디바이스에서는 이 명령을 이용할 수 없습니다.

액세스
기본

config

디바이스에 대한 클러스터링 컨피그레이션을 표시합니다.

구문
```
show clustering config
```

예
```
> show clustering config
```

clustering ha-statistics

클러스터의 디바이스에 대한 상태 공유 통계를 표시합니다.

구문

```
show clustering ha-statistics
```

예

```
> show clustering ha-statistics
```

cpu

디바이스의 모든 CPU에 대한 플랫폼에 해당하는 현재 CPU 사용량을 표시합니다. 관리되는 디바이스의 경우 다음 값이 표시됩니다.

- CPU

  프로세서 수.

- 로드

  CPU 사용률은 0~100의 숫자로 표시됩니다. 0은 로드되지 않은 것이고 100은 완전히 로드된 것입니다.

가상 디바이스 및 ASA FirePOWER 디바이스의 경우 다음 값이 표시됩니다.

- CPU

  프로세서 수.

- %user

  사용자 레벨(애플리케이션)에서 실행되는 동안 발생한 CPU 사용률.

- %nice

  사용자 레벨(nice 우선순위)에서 실행되는 동안 발생한 CPU 사용률.

- %sys

  시스템 레벨(커널)에서 실행되는 동안 발생한 CPU 사용률. interrupt 또는 softirq의 서비스에 사용된 시간은 포함되지 않습니다. softirq(software interrupt)는 여러 CPU에서 동시에 실행할 수 있는 32개의 열거된 software interrupt 중 하나입니다.

- %iowait

  시스템에 해결되지 않은 디스크 I/O 요청이 있을 때 CPU가 유휴 상태인 시간의 백분율.

- %irq

  interrupt 서비스에 CPU가 사용된 시간의 백분율.

- %soft

  softirq 서비스에 CPU가 사용된 시간의 백분율.

- %steal

  하이퍼바이저가 다른 가상 프로세서를 서비스하는 동안 가상 CPU가 비자발적으로 대기하는 데 사용된 시간의 백분율.

- %guest

  가상 프로세서 실행에 CPU가 사용된 시간의 백분율.

- %idle

  CPU가 유휴 상태이고 시스템에 해결되지 않은 디스크 I/O 요청이 없는 시간의 백분율.

액세스
기본

구문

```
show cpu [procnum]
```

여기서 *procnum*은 사용률 정보를 표시할 프로세서의 수입니다. 유효한 값의 범위는 0부터 시스템의 총 프로세서 수 빼기 1까지입니다. 관리되는 디바이스에 대해 *procnum*을 사용하면 무시됩니다. 해당 플랫폼에서는 사용률 정보를 모든 프로세서에 대해서만 표시할 수 있기 때문입니다.

예

```
> show cpu
```

database

`show database` 명령은 디바이스의 관리 인터페이스를 구성합니다.

액세스
기본

processes

실행 중인 데이터베이스 쿼리의 목록을 표시합니다.

액세스
기본

구문

```
show database processes
```

예

```
> show database processes
```

slow-query-log

데이터베이스의 slow query log를 표시합니다.

액세스
기본

구문

```
show database slow-query-log
```

예

```
> show database slow-query-log
```

device-settings

현재 디바이스에 해당하는 애플리케이션 우회 설정에 대한 정보를 표시합니다.

액세스
기본

구문
```
show device-settings
```

예
```
> show device-settings
```

disk

현재 디스크 사용량을 표시합니다.

액세스
기본

구문
```
show disk
```

예
```
> show disk
```

disk-manager

시스템의 각 부분(silos, low watermarks, high watermarks 등)에 대한 자세한 디스크 사용량 정보를 표시합니다.

액세스
기본

구문
```
show disk-manager
```

예
```
> show disk-manager
```

dns

현재 DNS 서버 주소 및 검색 도메인을 표시합니다.

액세스
기본

구문

```
show dns
```

예

```
> show dns
```

expert

셸을 호출합니다.

액세스

기본

구문

```
expert
```

예

```
> expert
```

fan-status

하드웨어 팬의 현재 상태를 표시합니다. 가상 디바이스 또는 ASA FirePOWER 디바이스에서는 이 명령을 이용할 수 없습니다.

액세스

기본

구문

```
show fan-status
```

예

```
> show fan-status
```

fastpath-rules

현재 구성된 fastpath 규칙을 표시합니다. 가상 디바이스 또는 ASA FirePOWER 디바이스에서는 이 명령을 이용할 수 없습니다.

액세스

기본

구문

```
show fastpath-rules
```

예

```
> show fastpath-rules
```

gui

웹 인터페이스의 현재 상태를 표시합니다. 가상 디바이스 또는 ASA FirePOWER 디바이스에서는 이 명령을 이용할 수 없습니다.

액세스
기본

구문
```
show gui
```

예
```
> show gui
```

hostname

디바이스의 호스트 이름 및 어플라이언스 UUID를 표시합니다. CLI를 사용하여 디바이스의 호스트 이름을 수정하려면 관리하는 방어 센터에 변경 사항이 반영되는지 확인하십시오. 경우에 따라 디바이스 관리 설정을 수동으로 수정해야 할 수 있습니다. 자세한 내용은 4-53페이지의 디바이스 관리 설정 수정을/를 참조하십시오.

액세스
기본

구문
```
show hostname
```

예
```
> show hostname
```

hosts

ASA FirePOWER 모듈의 /etc/hosts 파일 내용을 표시합니다.

액세스
기본

구문
```
show hosts
```

예
```
> show hosts
```

hyperthreading

hyperthreading의 활성화 여부를 표시합니다. ASA FirePOWER 디바이스에서는 이 명령을 이용할 수 없습니다.

액세스

기본

구문

```
show hyperthreading
```

예

```
> show hyperthreading
```

inline-sets

모든 인라인 보안 영역 및 관련 인터페이스의 컨피그레이션 데이터를 표시합니다. ASA FirePOWER 디바이스에서는 이 명령을 이용할 수 없습니다.

액세스

기본

구문

```
show inline-sets
```

예

```
> show inline-sets
```

interfaces

매개 변수를 지정하지 않으면 구성된 모든 인터페이스의 목록이 표시됩니다. 매개 변수를 지정하면 지정된 인터페이스에 대한 자세한 정보가 표시됩니다.

액세스

기본

구문

```
show interfaces [interface]
```

여기서 *interface*는 자세한 정보를 원하는 특정 인터페이스입니다.

예

```
> show interfaces
```

ifconfig

ASA FirePOWER 모듈에 대한 인터페이스 컨피그레이션을 표시합니다.

액세스
기본

구문
```
show ifconfig
```

예
```
> show ifconfig
```

lcd

LCD 하드웨어 디스플레이의 활성화 여부를 표시합니다. 가상 디바이스 또는 ASA FirePOWER 디바이스에서는 이 명령을 이용할 수 없습니다.

액세스
기본

구문
```
show lcd
```

예
```
> show lcd
```

link-aggregation

`show link-aggregation` 명령은 LAG(link aggregation group)에 대한 디스플레이 컨피그레이션 및 통계 정보를 표시합니다. 가상 디바이스 또는 ASA FirePOWER 디바이스에서는 이 명령을 이용할 수 없습니다.

액세스
기본

configuration

LAG ID, 인터페이스 수, 컨피그레이션 모드, 로드 밸런싱 모드, LACP 정보, 물리적 인터페이스 유형 등 구성된 각 LAG에 대한 컨피그레이션 세부사항을 표시합니다.

액세스
기본

구문
```
show link-aggregation configuration
```

예

```
> show link-aggregation configuration
```

statistics

상태, 링크 상태와 속도, 컨피그레이션 모드, 수신/송신된 패킷의 카운터, 수신/송신된 바이트의 카운터를 비롯한 구성된 각 LAG에 대한 통계를 인터페이스별로 표시합니다.

액세스

기본

구문

```
show link-aggregation statistics
```

예

```
> show link-aggregation statistics
```

link-state

디바이스에 있는 포트의 유형, 링크, 속도, 이중 상태 및 우회 모드를 표시합니다. ASA FirePOWER 디바이스에서는 이 명령을 이용할 수 없습니다.

액세스

기본

구문

```
show link-state
```

예

```
> show link-state
```

log-ips-connection

로깅된 침입 이벤트와 관련된 연결 이벤트 로깅의 활성화 여부를 표시합니다.

액세스

기본

구문

```
show log-ips-connection
```

예

```
> show log-ips-connection
```

managers

방어 센터의 컨피그레이션 및 통신 상태를 표시합니다. 등록이 보류 중이면 등록 키와 NAT ID만 표시됩니다. 디바이스가 고가용성 쌍에 등록되면 관리하는 두 방어 센터에 대한 정보가 표시됩니다. 디바이스가 스태킹된 컨피그레이션에서 보조 디바이스로 구성된 경우, 관리하는 방어 센터 및 기본 디바이스 모두에 대한 정보가 표시됩니다.

액세스
기본

구문
```
show managers
```

예
```
> show managers
```

memory

디바이스에 대한 총 메모리, 사용 중인 메모리 및 사용 가능한 메모리를 표시합니다.

액세스
기본

구문
```
show memory
```

예
```
> show memory
```

model

디바이스에 대한 모델 정보를 표시합니다.

액세스
기본

구문
```
show model
```

예
```
> show model
```

mpls-depth

관리 인터페이스에 구성된 MPLS 레이어의 수(0~6)를 표시합니다. 가상 디바이스 또는 ASA FirePOWER 디바이스에서는 이 명령을 이용할 수 없습니다.

액세스
기본

구문
```
show mpls-depth
```

예
```
> show mpls-depth
```

NAT

`show nat` 명령은 관리 인터페이스에 대한 NAT 데이터 및 컨피그레이션 정보를 표시합니다. 가상 디바이스 또는 ASA FirePOWER 디바이스에서는 이 명령을 이용할 수 없습니다.

액세스
기본

active-dynamic

동적 규칙에 따라 변환된 NAT 플로우를 표시합니다. 이러한 항목은 플로우가 규칙과 일치할 때 표시되며, 규칙이 시간 초과될 때까지 지속됩니다. 따라서 목록이 부정확할 수 있습니다. 시간 초과는 프로토콜에 따라 다릅니다. ICMP는 5초, UDP는 120초, TCP는 3600초, 나머지 모든 프로토콜은 60초입니다.

구문
```
show nat active-dynamic
```

예
```
> show nat active-dynamic
```

active-static

고정 규칙에 따라 변환된 NAT 플로우를 표시합니다. 이러한 항목은 디바이스에 규칙을 적용하자마자 표시되며, 목록은 고정 NAT 규칙과 일치하는 활성 플로우를 나타내지 않습니다.

구문
```
show nat active-static
```

예
```
> show nat active-static
```

allocators

동적 규칙에 사용되는 변환된 주소의 풀인 모든 NAT allocator에 대한 정보를 표시합니다.

구문

```
show nat allocators
```

예

```
> show nat allocators
```

config

관리 인터페이스에 대한 현재 NAT 정책 컨피그레이션을 표시합니다.

구문

```
show nat config
```

예

```
> show nat config
```

dynamic-rules

지정된 allocator ID를 사용하는 동적 NAT 규칙을 표시합니다.

구문

```
show nat dynamic-rules allocator_id
```

예

```
> show nat dynamic-rules 9
```

여기서 *allocator_id*는 유효한 allocator ID 번호입니다.

flows

지정된 allocator ID를 사용하는 규칙에 대한 플로우의 수를 표시합니다.

구문

```
show nat flows allocator-id
```

예

```
> show nat flows 81
```

여기서 *allocator_id*는 유효한 allocator ID 번호입니다.

static-rules

모든 고정 NAT 규칙을 표시합니다.

구문

```
show nat static-rules
```

예

```
> show nat static-rules
```

netstat

ASA FirePOWER 모듈에 대한 활성 네트워크 연결을 표시합니다.

액세스

기본

구문

```
show netstat
```

예

```
> show netstat
```

network

관리 인터페이스의 IPv4 및 IPv6 컨피그레이션, MAC 주소, HTTP 프록시 주소, 포트 및 사용자 이름을 표시합니다(구성된 경우).

액세스

기본

구문

```
show network
```

예

```
> show network
```

network-modules

설치된 모든 모듈 및 해당 정보를 일련 번호와 함께 표시합니다. 가상 디바이스 또는 ASA FirePOWER 디바이스에서는 이 명령을 이용할 수 없습니다.

액세스

기본

구문

```
show network-modules
```

예

```
> show network-modules
```

network-static-routes

구성된 모든 네트워크 고정 경로와 해당 정보(인터페이스, 대상 주소, 네트워크 마스크, 게이트웨이 주소 포함)를 표시합니다.

액세스
기본

구문
```
show network-static-routes
```

예
```
> show network-static-routes
```

ntp

ntp 컨피그레이션을 표시합니다.

액세스
기본

구문
```
show ntp
```

예
```
> show ntp
```

perfstats

디바이스에 대한 성능 통계를 표시합니다.

액세스
기본

구문
```
show perfstats
```

예
```
> show perfstats
```

portstats

디바이스에 설치된 모든 포트에 대한 포트 통계를 표시합니다. 가상 디바이스 또는 ASA FirePOWER 디바이스에서는 이 명령을 이용할 수 없습니다.

액세스
기본

구문

```
show portstats [copper | fiber | internal | external | all]
```

여기서 `copper`는 모든 copper 포트를, fiber는 모든 fiber 포트를, internal은 모든 internal 포트를, external은 모든 external 포트를, all은 모든 포트(external 및 internal)를 지정합니다.

예

```
> show portstats fiber
```

power-supply-status

하드웨어 전력 공급 장치의 현재 상태를 표시합니다. 가상 디바이스 또는 ASA FirePOWER 디바이스에서는 이 명령을 이용할 수 없습니다.

액세스

기본

구문

```
show power-supply-status
```

예

```
> show power-supply-status
```

process-tree

디바이스에서 현재 실행 중인 프로세스를 바이트 기준의 트리 형식으로 정렬하여 표시합니다.

액세스

기본

구문

```
show process-tree
```

예

```
> show process-tree
```

processes

디바이스에서 현재 실행 중인 프로세스를 CPU 사용량 내림차순으로 정렬하여 표시합니다.

액세스

기본

구문

```
show processes [sort-flag] [filter]
```

여기서 `sort-flag`에는 `-m`(메모리 기준 내림차순 정렬), `-u`(프로세스 이름보다는 사용자 이름 기준 정렬) 또는 `verbose`(명령의 전체 이름 및 경로 표시)를 사용할 수 있습니다. *`filter`* 매개 변수는 결과를 필터링할 명령 및 사용자 이름의 검색어를 지정합니다. 헤더 행은 여전히 표시됩니다.

예

```
> show processes -u user1
```

route

ASA FirePOWER 모듈의 라우팅 정보를 표시합니다.

액세스

기본

구문

```
show route
```

예

```
> show route
```

routing-table

매개 변수를 지정하지 않으면 모든 가상 라우터에 대한 라우팅 정보가 표시됩니다. 매개 변수를 지정하면 지정한 라우터 및 지정한 라우팅 프로토콜 유형(해당되는 경우)이 표시됩니다. 모든 매개 변수는 선택 사항입니다. 가상 디바이스 또는 ASA FirePOWER 디바이스에서는 이 명령을 이용할 수 없습니다.

액세스

기본

구문

```
show routing-table [name] [ ospf | rip | static ]
```

여기서 *name*은 정보를 원하는 특정 라우터의 이름이고 `ospf`, `rip` 및 `static`은 라우팅 프로토콜 유형을 지정합니다.

예

```
> show routing-table Vrouter1 static
```

serial-number

섀시 일련 번호를 표시합니다. 가상 디바이스에서는 이 명령을 이용할 수 없습니다.

액세스

기본

구문

```
show serial-number
```

예

```
> show serial-number
```

ssl-policy-config

정책 설명, 기본 로깅 설명, 활성화된 모든 SSL 규칙 및 규칙 컨피그레이션, 신뢰받는 CA 인증서, 해독 불가 트래픽 작업을 포함하여 현재 적용된 SSL 정책 컨피그레이션을 표시합니다.

액세스

기본

구문

```
show ssl-policy-config
```

예

```
> show ssl-policy-config
```

stacking

관리되는 디바이스 및 기본으로 구성된 디바이스에 대한 스태킹 컨피그레이션과 위치를 표시하고, 모든 보조 디바이스에 대한 데이터도 나열합니다. 클러스터링된 스택의 경우 이 명령은 또한 스택이 클러스터의 멤버임을 나타냅니다. 사용자는 스태킹의 활성화 또는 비활성화(대부분의 경우)를 위해 웹 인터페이스를 사용해야 합니다. 스태킹이 활성화되어 있지 않으면 `Stacking not currently configured`가 반환됩니다. 가상 디바이스 또는 ASA FirePOWER 디바이스에서는 이 명령을 이용할 수 없습니다.

액세스

기본

구문

```
show stacking
```

예

```
> show stacking
```

summary

디바이스에 대한 가장 일반적인 정보(버전, 유형 UUID 등)의 요약을 표시합니다. 자세한 정보는 다음의 `show` 명령 D-26페이지의 version, D-14페이지의 interfaces, D-11페이지의 device-settings 및 D-7페이지의 access-control-config을/를 참조하십시오.

액세스

기본

구문

```
show summary
```

예

```
> show summary
```

time

현재 날짜와 시간을 현재 사용자에 대해 구성된 UTC 및 현지 표준 시간대로 표시합니다.

액세스
기본

구문
```
show time
```

예
```
> show time
```

traffic-statistics

매개 변수를 지정하지 않으면 모든 포트에서 전송 및 수신된 바이트에 대한 세부사항이 표시됩니다. 포트를 지정하면 지정한 포트에 대한 정보만 표시됩니다. ASA FirePOWER 디바이스에 대해서는 포트를 지정할 수 없으며, 시스템은 데이터 평면 인터페이스만 표시합니다.

액세스
기본

구문
```
show traffic-statistics [port]
```
여기서 `port`는 정보를 원하는 특정 포트입니다.

예
```
> show traffic-statistics s1p1
```

user

가상 디바이스에만 적용 가능합니다. 지정한 사용자에 대한 자세한 컨피그레이션 정보를 표시합니다. 다음 값이 표시됩니다.

- Login - 로그인 이름
- UID - 숫자 사용자 ID
- Auth(`Local` 또는 `Remote`) - 사용자를 인증하는 방법
- Access(`Basic` 또는 `Config`) - 사용자의 권한 레벨
- Enabled (`Enabled` 또는 `Disabled`) - 사용자의 활성화 여부
- Reset(`Yes` 또는 `No`) - 다음 로그인 때 사용자가 비밀번호를 변경해야 하는지 여부
- Exp(`Never` 또는 a number) - 사용자 비밀번호를 변경해야 할 때까지의 일수
- Warn(`N/A` 또는 a number) - 비밀번호가 만료되기 전 사용자에게 변경을 알리는 일수
- Str(`Yes` 또는 `No`) - 사용자 비밀번호가 강도 검사 기준을 충족해야 하는지 여부
- Lock(`Yes` 또는 `No`) - 로그인 실패가 많을 경우 사용자 계정을 잠글지 여부
- Max(`N/A` 또는 a number) - 사용자 계정이 잠길 때까지 최대 실패 로그인 수

액세스
컨피그레이션

구문
```
show user username username username ...
```
여기서 *username*은 사용자의 이름을 지정하며, 사용자 이름은 공백으로 분리합니다.

예
```
> show user jdoe
```

users

가상 디바이스에만 적용 가능합니다. 모든 로컬 사용자에 대한 자세한 컨피그레이션 정보를 표시합니다. 다음 값이 표시됩니다.

- Login - 로그인 이름
- UID - 숫자 사용자 ID
- Auth(`Local` 또는 `Remote`) - 사용자를 인증하는 방법
- Access(`Basic` 또는 `Config`) - 사용자의 권한 레벨
- Enabled (`Enabled` 또는 `Disabled`) - 사용자의 활성화 여부
- Reset(`Yes` 또는 `No`) - 다음 로그인 때 사용자가 비밀번호를 변경해야 하는지 여부
- Exp(`Never` 또는 a number) - 사용자 비밀번호를 변경해야 할 때까지의 일수
- Warn(`N/A` 또는 a number) - 비밀번호가 만료되기 전 사용자에게 변경을 알리는 일수
- Str(`Yes` 또는 `No`) - 사용자 비밀번호가 강도 검사 기준을 충족해야 하는지 여부
- Lock (`Yes` or `No`) - 로그인 실패가 많을 경우 사용자 계정을 잠글지 여부
- Max(`N/A` 또는 a number) - 사용자 계정이 잠길 때까지 최대 실패 로그인 수

액세스
컨피그레이션

구문
```
show users
```

예
```
> show users
```

version

제품 버전 및 빌드를 표시합니다. *detail* 매개 변수를 지정하면 추가 구성 요소의 버전이 표시됩니다.

액세스
기본

구문
```
show version [detail]
```

예

```
> show version
```

virtual-routers

매개 변수를 지정하지 않으면 DHCP 릴레이, OSPF 및 RIP 정보와 함께 현재 구성된 모든 가상 라우터 목록이 표시됩니다. 매개 변수를 지정하면 지정된 경로 유형으로 제한되어, 지정된 라우터에 대한 정보가 표시됩니다. 모든 매개 변수는 선택 사항입니다. 가상 디바이스 또는 ASA FirePOWER 디바이스에서는 이 명령을 이용할 수 없습니다.

액세스

기본

구문

```
show virtual-routers [ dhcprelay | ospf | rip ] [name]
```

여기서 `dhcprelay`, `ospf` 및 `rip`는 경로 유형을 지정하고 *`name`*은 정보를 원하는 특정 라우터의 이름입니다. `ospf`를 지정하면 경로 유형과 라우터 이름(있는 경우) 간 `neighbors`, `topology` 또는 `lsadb`를 추가로 지정할 수 있습니다.

예

```
> show virtual-routers ospf VRouter2
```

virtual-switches

매개 변수를 지정하지 않으면 현재 구성된 모든 가상 스위치의 목록이 표시됩니다. 매개 변수를 지정하면 지정한 스위치에 대한 정보가 표시됩니다. 가상 디바이스 또는 ASA FirePOWER 디바이스에서는 이 명령을 이용할 수 없습니다.

액세스

기본

구문

```
show virtual-switches [name]
```

예

```
> show virtual-switches Vswitch1
```

vmware-tools

가상 디바이스에서 VMWare Tools가 현재 활성화되었는지를 나타냅니다. 이 명령은 가상 디바이스에서만 이용할 수 있습니다.

VMWare Tools는 가상 머신의 성능 향상을 위한 유틸리티 제품군입니다. 이러한 유틸리티를 사용하면 VMware 제품의 편리한 기능을 최대한 활용할 수 있습니다. 모든 가상 어플라이언스에서 다음과 같은 플러그인을 지원합니다.

- guestInfo
- powerOps

- timeSync
- vmbackup

VMWare Tools 및 지원되는 플러그인에 대한 자세한 내용은 VMWare 웹사이트 (http://www.vmware.com)를 참조하십시오.

액세스
기본

구문
```
show vmware-tools
```

예
```
> show vmware-tools
```

VPN

`show VPN` 명령은 VPN 연결에 대한 VPN 상태 및 컨피그레이션 정보를 표시합니다. 가상 디바이스 또는 ASA FirePOWER 디바이스에서는 이 명령을 이용할 수 없습니다.

액세스
기본

config

모든 VPN 연결의 컨피그레이션을 표시합니다.

구문
```
show vpn config
```

예
```
> show vpn config
```

config by virtual router

가상 라우터에 대한 모든 VPN 연결의 컨피그레이션을 표시합니다.

구문
```
show vpn config [virtual router]
```

예
```
> show vpn config VRouter1
```

status

모든 VPN 연결의 상태를 표시합니다.

구문
```
show vpn status
```

예

```
> show vpn status
```

status by virtual router

가상 라우터에 대한 모든 VPN 연결의 상태를 표시합니다.

구문

```
show vpn status [virtual router]
```

예

```
> show vpn status VRouter1
```

counters

모든 VPN 연결의 카운터를 표시합니다.

구문

```
show vpn counters
```

예

```
> show vpn counters
```

counters by virtual router

가상 라우터에 대한 모든 VPN 연결의 카운터를 표시합니다.

구문

```
show vpn counters [virtual router]
```

예

```
> show vpn counters VRouter1
```

Configuration 명령

Configuration 명령을 통해 사용자는 시스템을 구성 및 관리할 수 있습니다. 이러한 명령은 시스템 운영에 영향을 미치므로, 기본 레벨 `configure password`를 제외하고는 컨피그레이션 CLI 액세스 권한이 있는 사용자만 이러한 명령을 실행할 수 있습니다.

다음 절에서는 configuration 명령에 대해 설명합니다.

- D-32페이지의 network
- D-39페이지의 password
- D-39페이지의 stacking disable
- D-39페이지의 user
- D-42페이지의 vmware-tools

clustering

디바이스에서 클러스터링에 대한 우회를 비활성화 또는 구성합니다. 가상 디바이스, ASA FirePOWER 디바이스 또는 보조 스택 멤버로 구성된 디바이스에서는 이 명령을 이용할 수 없습니다.

액세스

컨피그레이션

구문

```
configure clustering {disable | bypass}
```

예

```
> configure clustering disable
```

bypass

인라인 쌍의 우회 모드를 열거나 닫습니다. 가상 디바이스 또는 ASA FirePOWER 디바이스에서는 이 명령을 이용할 수 없습니다.

액세스

컨피그레이션

구문

```
configure bypass {open | close} {interface}
```

여기서 *interface*는 인라인 쌍에 있는 두 하드웨어 포트 중 하나의 이름입니다.

예

```
> configure bypass open s1p1
```

gui

시스템에 대한 주요 업데이트 중 나타나는 원활한 업그레이드 웹 인터페이스를 비롯한 디바이스 웹 인터페이스를 활성화 또는 비활성화합니다. 가상 디바이스 또는 ASA FirePOWER 디바이스에서는 이 명령을 이용할 수 없습니다.

액세스

컨피그레이션

구문

```
configure gui {enable | disable}
```

예

```
> configure gui disable
```

lcd

디바이스 앞쪽에 있는 LCD 디스플레이를 활성화 또는 비활성화합니다. 가상 디바이스 또는 ASA FirePOWER 디바이스에서는 이 명령을 이용할 수 없습니다.

액세스

컨피그레이션

구문

```
configure lcd {enable | disable}
```

예

```
> configure lcd disable
```

log-ips-connections

로깅된 침입 이벤트와 관련이 있는 연결 이벤트의 로깅을 활성화 또는 비활성화합니다.

액세스

컨피그레이션

구문

```
configure log-ips-connections {enable | disable}
```

예

```
> configure log-ips-connections disable
```

manager

`configure manager` 명령은 관리하는 방어 센터에 대한 디바이스의 연결을 구성합니다.

액세스

컨피그레이션

add

관리하는 방어 센터로부터의 연결을 허용하도록 디바이스를 구성합니다. 이 명령은 디바이스가 적극적으로 관리되는 경우에만 작동합니다.

디바이스를 방어 센터에 등록하려면 고유한 영숫자 등록 키가 항상 필요합니다. 대부분의 경우 등록 키와 함께 호스트 이름 또는 IP 주소를 제공해야 합니다. 그러나 디바이스와 방어 센터가 NAT 디바이스에 의해 분리된 경우, 등록 키와 함께 고유한 NAT ID를 입력하고 호스트 이름 대신 DONTRESOLVE를 지정해야 합니다.

구문

```
configure manager add {hostname | IPv4_address | IPv6_address | DONTRESOLVE} regkey
[nat_id]
```

여기서 {*hostname* | *IPv4_address* | *IPv6_address* | DONTRESOLVE}는 이 디바이스를 관리하는 방어 센터의 DNS 호스트 이름 또는 IP 주소(IPv4 또는 IPv6)를 지정합니다. 방어 센터의 주소를 직접 지정할 수 없는 경우 DONTRESOLVE 를 사용합니다.DONTRESOLVE를 사용하는 경우 *nat_id*가 필요합니다. *regkey*는 디바이스를 방어 센터에 등록하기 위해 필요한 고유한 영숫자 등록 키입니다. *nat_id*-방어 센터와 디바이스 간 등록 프로세스 중에 사용되는 선택적인 영숫자 문자열입니다. 이 문자열은 호스트 이름이 DONTRESOLVE로 설정된 경우 필요합니다.

예

```
> configure manager add DONTRESOLVE abc123 efg456
```

delete

디바이스에서 방어 센터의 연결 정보를 제거합니다. 이 명령은 디바이스가 적극적으로 관리되는 경우에만 작동합니다.

구문

```
configure manager delete
```

예

```
> configure manager delete
```

mpls-depth

관리 인터페이스에서 MPLS 레이어의 멤버를 구성합니다. 가상 디바이스 또는 ASA FirePOWER 디바이스에서는 이 명령을 이용할 수 없습니다.

액세스

컨피그레이션

구문

```
configure mpls-depth {depth}
```

여기서 *depth*는 0~6의 숫자입니다.

예

```
> configure mpls-depth 3
```

network

configure network 명령은 디바이스의 관리 인터페이스를 구성합니다.

액세스
컨피그레이션

dns searchdomains

DNS 검색 도메인의 현재 목록을 명령에 지정된 목록으로 교체합니다.

구문

```
configure network dns searchdomains {searchlist}
```

여기서 *searchlist*는 쉼표로 구분된 도메인 목록입니다.

예

```
> configure network dns searchdomains foo.bar.com,bar.com
```

dns servers

DNS 서버의 현재 목록을 명령에 지정된 목록으로 교체합니다.

구문

```
configure nework dns servers {dnslist}
```

여기서 *dnslist*는 쉼표로 구분된 DNS 서버 목록입니다.

예

```
> configure network dns servers 10.123.1.10,10.124.1.10
```

hostname

디바이스의 호스트 이름을 설정합니다.

구문

```
configure network hostname {name}
```

여기서 *name*은 새 호스트 이름입니다.

예

```
> configure network hostname sfrocks
```

http-proxy

Series 3 및 가상 디바이스에서 HTTP 프록시를 구성합니다. 명령을 실행하면 HTTP 프록시 주소와 포트, 프록시 인증이 필요한지 여부에 대한 CLI 프롬프트가 표시되며, 해당 인증이 필요한 경우 프록시 사용자 이름, 프록시 비밀번호, 프록시 비밀번호의 확인에 대한 프롬프트가 표시됩니다.

가상 디바이스가 동적 분석을 위해 종합 보안 인텔리전스 클라우드에 파일을 제출할 수 있도록 HTTP 프록시 서버를 구성하려면 가상 디바이스에서 이 명령을 사용하십시오.

구문

```
configure network http-proxy
```

예

```
> configure network http-proxy
Manual proxy configuration
Enter HTTP Proxy address:
Enter HTTP Proxy Port:
Use Proxy Authentication? (y/n) [n]:
Enter Proxy Username:
Enter Proxy Password:
Confirm Proxy Password:
```

http-proxy-disable

Series 3 및 가상 디바이스에서 HTTP 프록시 컨피그레이션을 삭제합니다.

구문

```
configure network http-proxy-disable
```

예

```
> configure network http-proxy-disable
Are you sure that you wish to delete the current http-proxy configuration? (y/n):
```

ipv4 delete

디바이스 관리 인터페이스의 IPv4 컨피그레이션을 표시합니다.

구문

```
configure network ipv4 delete
```

예

```
> configure network ipv4 delete
```

ipv4 dhcp

디바이스 관리 인터페이스의 IPv4 컨피그레이션을 DHCP로 설정합니다. 관리 인터페이스는 DHCP 서버와 통신하여 컨피그레이션 정보를 가져옵니다.

구문

```
configure network ipv4 dhcp
```

예

```
> configure network ipv4 dhcp
```

ipv4 manual

디바이스 관리 인터페이스의 IPv4 컨피그레이션을 수동으로 구성합니다.

구문

```
configure network ipv4 manual ipaddr netmask gw
```

여기서 *ipaddr*은 IP 주소, *netmask*는 서브넷 마스크, *gw*는 기본 게이트웨이의 IPv4 주소입니다.

예

```
> configure network ipv4 manual 10.123.1.10 255.255.0.0 10.123.1.1
```

ipv6 delete

디바이스 관리 인터페이스의 IPv6 컨피그레이션을 표시합니다.

구문

```
configure network ipv6 delete
```

예

```
> configure network ipv6 delete
```

ipv6 dhcp

디바이스 관리 인터페이스의 IPv6 컨피그레이션을 DHCP로 설정합니다. 관리 인터페이스는 DHCP 서버와 통신하여 컨피그레이션 정보를 가져옵니다.

구문

```
configure network ipv6 dhcp
```

예

```
> configure network ipv6 dhcp
```

ipv6 router

디바이스 관리 인터페이스의 IPv6 컨피그레이션을 Router로 설정합니다. 관리 인터페이스는 IPv6 라우터와 통신하여 컨피그레이션 정보를 가져옵니다.

구문

```
configure network ipv6 router
```

예

```
> configure network ipv6 router
```

ipv6 manual

디바이스 관리 인터페이스의 IPv6 컨피그레이션을 수동으로 구성합니다.

구문

```
configure network ipv6 manual ip6addr/ip6prefix [ip6gw]
```

여기서 *ip6addr/ip6prefix*는 IP 주소 및 접두사 길이이며 ip6*gw*는 기본 게이트웨이의 IPv6 주소입니다.

예

```
> configure network ipv6 manual 2001:DB8:3ffe:1900:4545:3:200:f8ff:fe21:67cf 64
```

management-interface disable

지정된 관리 인터페이스를 비활성화합니다.

구문

```
configure network management-interface disable ethn
```

여기서 *n*은 비활성화하려는 관리 인터페이스의 번호입니다.

예

```
> configure network management-interface disable eth1
```

management-interface disable-event-channel

지정된 관리 인터페이스를 통한 이벤트 전송을 비활성화합니다.

구문

```
configure network management-interface disable-event-channel ethn
```

여기서 *n*은 비활성화하려는 관리 인터페이스의 번호입니다.

예

```
> configure network management-interface disable-event-channel eth1
```

management-interface disable-management-channel

지정된 관리 인터페이스를 통한 관리 전송을 비활성화합니다.

구문

```
configure network management-interface disable-management-channel ethn
```

여기서 *n*은 비활성화하려는 관리 인터페이스의 번호입니다.

예

```
> configure network management-interface disable-management-channel eth1
```

management-interface enable

지정된 관리 인터페이스를 활성화합니다.

구문

```
configure network management-interface enable ethn
```

여기서 *n*은 활성화하려는 관리 인터페이스의 번호입니다.

예

```
> configure network management-interface enable eth1
```

management-interface enable-event-channel

지정된 관리 인터페이스를 통한 이벤트 전송을 활성화합니다.

구문

```
configure network management-interface enable-event-channel ethn
```

여기서 *n*은 활성화하려는 관리 인터페이스의 번호입니다.

예

```
> configure network management-interface enable-event-channel eth1
```

management-interface enable-management-channel

지정된 관리 인터페이스를 통한 관리 전송을 활성화합니다.

구문

```
configure network management-interface enable-management-channel ethn
```

여기서 *n*은 활성화하려는 관리 인터페이스의 번호입니다.

예

```
> configure network management-interface enable-management-channel eth1
```

management-interface tcpport

관리용 TCP 포트의 값을 변경합니다.

구문

```
configure network management-interface tcpport port
```

여기서 *port*는 구성하려는 관리 포트 값입니다.

예

```
> configure network management-interface tcpport 8500
```

management-port

디바이스의 TCP 관리 포트 값을 설정합니다.

구문

```
configure network management-port number
```

여기서 *number*는 구성하려는 관리 포트 값입니다.

예

```
> configure network management-port 8500
```

static-routes ipv4 add

지정된 관리 인터페이스에 대한 IPv4 고정 경로를 추가합니다.

구문

```
configure network static-routes ipv4 add interface destination netmask gateway
```

여기서 *interface*는 관리 인터페이스, *destination*은 목적지 IP 주소, *netmask*는 네트워크 마스크 주소, *gateway*는 추가하려는 게이트웨이 주소입니다.

예

```
> configure network static-routes ipv4 add eth1 10.115.24.0 255.255.255.0 10.115.9.2
```

static-routes ipv4 delete

지정된 관리 인터페이스에 대한 IPv4 고정 경로를 삭제합니다.

구문

```
configure network static-routes ipv4 delete interface destination netmask gateway
```

여기서 *interface*는 관리 인터페이스, *destination*은 목적지 IP 주소, *netmask*는 네트워크 마스크 주소, *gateway*는 삭제하려는 게이트웨이 주소입니다.

예

```
> configure network static-routes ipv4 delete eth1 10.115.24.0 255.255.255.0
10.115.9.2
```

static-routes ipv6 add

지정된 관리 인터페이스에 대한 IPv6 고정 경로를 추가합니다.

구문

```
configure network static-routes ipv6 add interface destination prefix gateway
```

여기서 *interface*는 관리 인터페이스, *destination*은 목적지 IP 주소, *prefix*는 IPv6 접두사 길이, *gateway*는 추가하려는 게이트웨이 주소입니다.

예

```
> configure network static-routes ipv6 add eth1 2001:DB8:3ffe:1900:4545:3:200:
f8ff:fe21:67cf 64
```

static-routes ipv6 delete

지정된 관리 인터페이스에 대한 IPv6 고정 경로를 삭제합니다.

구문

```
configure network static-routes ipv6 delete interface destination prefix gateway
```

여기서 *interface*는 관리 인터페이스, *destination*은 목적지 IP 주소, *prefix*는 IPv6 접두사 길이, *gateway*는 삭제하려는 게이트웨이 주소입니다.

예

```
> configure network static-routes ipv6 delete eth1 2001:DB8:3ffe:1900:4545:3:200:f8ff:
fe21:67cf 64
```

password

현재 사용자가 자신의 비밀번호를 변경하도록 허용합니다. 이 명령을 실행하면 현재(또는 이전) 비밀번호를 입력하라는 CLI 프롬프트가 표시된 다음 새 비밀번호를 두 번 입력하라는 프롬프트가 표시됩니다.

액세스

기본

구문

```
configure password
```

예

```
> configure password
Enter current password:
Enter new password:
Confirm new password:
```

stacking disable

관리되는 디바이스에서 스태킹 컨피그레이션을 제거합니다. 기본으로 구성된 디바이스에서는 스택이 완전히 제거되고, 보조로 구성된 디바이스에서는 해당 디바이스가 스택에서 제거됩니다. 가상 디바이스 또는 ASA FirePOWER 디바이스에서는 이 명령을 이용할 수 없으며, 클러스터링된 스택을 분리하는 데 이 명령을 사용할 수 없습니다.

스태킹 계층 구조에서 더 위에 있는 어플라이언스와 통신을 설정할 수 없는 경우 이 명령을 사용하십시오. 방어 센터를 통신에 이용할 수 있는 경우 대신 방어 센터 웹 인터페이스를 사용하라는 메시지가 표시됩니다. 마찬가지로, 기본 디바이스를 이용할 수 있는 경우 보조로 구성된 디바이스에서 `stacking disable`을 입력하면 기본 디바이스에서 명령을 입력하라는 메시지가 나타납니다.

액세스

컨피그레이션

구문

```
configure stacking disable
```

예

```
> configure stacking disable
```

user

가상 디바이스에만 적용 가능한 `configure user` 명령은 디바이스의 로컬 사용자 데이터베이스를 관리합니다.

액세스

컨피그레이션

액세스

지정된 사용자의 액세스 레벨을 수정합니다. 이 명령은 지정된 사용자가 다음에 로그인할 때 적용됩니다.

구문

```
configure user access username [basic | config]
```

예

```
> configure user access jdoe basic
```

여기서 *username*은 액세스를 수정할 사용자의 이름을 지정하고, `basic`은 기본 액세스를 나타내며, `config`는 컨피그레이션 액세스를 나타냅니다.

add

지정된 이름 및 액세스 레벨로 새 사용자를 생성합니다. 사용자의 비밀번호를 입력하라는 프롬프트가 표시됩니다.

구문

```
configure user add username [basic | config]
```

여기서 *username*은 새 사용자의 이름을 지정하고, `basic`은 기본 액세스를 나타내며, `config`는 컨피그레이션 액세스를 나타냅니다.

예

```
> configure user add jdoe basic
Enter new password for user jdoe:
Confirm new password for user jdoe:
```

aging

사용자 비밀번호의 만료를 강제로 적용합니다.

구문

```
configure user aging username max_days warn_days
```

여기서 *username*은 사용자의 이름을 지정하고, *max_days*는 비밀번호가 유효한 최대 일수를 나타내며, *warn_days*는 비밀번호 만료 전 사용자에게 변경을 알리는 일수를 나타냅니다.

예

```
> configure user aging jdoe 100 3
```

delete

사용자 및 사용자 홈 디렉토리를 삭제합니다.

구문

```
configure user delete username
```

여기서 *username*은 사용자의 이름입니다.

예

```
> configure user delete jdoe
```

disable

사용자를 비활성화합니다. 비활성화된 사용자는 로그인할 수 없습니다.

구문

```
configure user disable username
```

여기서 *username*은 사용자의 이름입니다.

예

```
> configure user disable jdoe
```

enable

사용자를 활성화합니다.

구문

```
configure user enable username
```

여기서 *username*은 사용자의 이름입니다.

예

```
> configure user enable jdoe
```

forcereset

사용자가 다음에 로그인할 때 비밀번호를 변경하도록 합니다. 사용자가 로그인하여 비밀번호를 변경하면 강도 확인이 자동으로 활성화됩니다.

구문

```
configure user forcereset username
```

여기서 *username*은 사용자의 이름입니다.

예

```
> configure user forcereset jdoe
```

maxfailedlogins

지정된 사용자에 대한 최대 실패 로그인 수를 설정합니다.

구문

```
configure user maxfailedlogins username number
```

여기서 *username*은 사용자의 이름을, *number*는 최대 실패 로그인 수를 지정합니다.

예

```
> configure user maxfailedlogins jdoe 3
```

password

사용자의 비밀번호를 설정합니다. 사용자의 비밀번호를 입력하라는 프롬프트가 표시됩니다.

구문

```
configure user password username
```

여기서 *username*은 사용자의 이름입니다.

예

```
> configure user pasword jdoe
Enter new password for user jdoe:
Confirm new password for user jdoe:
```

strengthcheck

사용자 비밀번호의 강도 요구 사항을 활성화 또는 비활성화합니다. 사용자 비밀번호가 만료되거나 configure user forcereset 명령이 사용되면, 사용자가 다음에 로그인할 때 이 요구 사항이 자동으로 활성화됩니다.

구문

```
configure user strengthcheck username {enable | disable}
```

여기서 *username*은 사용자의 이름을 지정하고 `enable`은 지정된 사용자 비밀번호의 요구 사항을 설정하고, `disable`은 지정된 사용자 비밀번호의 요구 사항을 제거합니다.

예

```
> configure user strengthcheck jdoe enable
```

unlock

최대 실패 로그인 수를 초과한 사용자의 잠금을 해제합니다.

구문

```
configure user unlock username
```

여기서 *username*은 사용자의 이름입니다.

예

```
> configure user unlock jdoe
```

vmware-tools

가상 디바이스에서 VMWare Tools 기능을 활성화 또는 비활성화합니다. 이 명령은 가상 디바이스에서만 이용할 수 있습니다.

VMWare Tools는 가상 머신의 성능 향상을 위한 유틸리티 제품군입니다. 이러한 유틸리티를 사용하면 VMware 제품의 편리한 기능을 최대한 활용할 수 있습니다. 모든 가상 어플라이언스에서 다음과 같은 플러그인을 지원합니다.

- guestInfo
- powerOps
- timeSync

- vmbackup

VMWare Tools 및 지원되는 플러그인에 대한 자세한 내용은 VMWare 웹사이트 (http://www.vmware.com)를 참조하십시오.

액세스

기본

구문

```
configure vmware-tools (enable | disable)
```

예

```
> configure vmware-tools enable
```

System 명령

System 명령을 사용하면 시스템 전반의 파일 및 액세스 제어 설정을 관리할 수 있습니다. 컨피그레이션 CLI 액세스 권한이 있는 사용자만 시스템 모드에서 명령을 실행할 수 있습니다.

다음 절에서는 system 명령에 대해 설명합니다.

access-control

`system access-control` 명령을 사용하면 디바이스에서 액세스 제어 컨피그레이션을 관리할 수 있습니다.

액세스

컨피그레이션

archive

현재 적용된 액세스 제어 정책을 /var/common에 텍스트 파일로 저장합니다.

구문

```
system access-control archive
```

예

```
> system access-control archive
```

clear-rule-counts

액세스 제어 규칙 히트 수를 0으로 재설정합니다.

구문

```
system access-control clear-rule-counts
```

예

```
> system access-control clear-rule-counts
```

rollback

전에 적용된 액세스 제어 컨피그레이션으로 시스템을 되돌립니다. 클러스터링된 또는 스태킹된 디바이스에서는 이 명령을 이용할 수 없습니다.

구문

```
system access-control rollback
```

예

```
> system access-control rollback
```

disable-http-user-cert

시스템에 있는 모든 HTTP 사용자 인증서를 제거합니다.

액세스
컨피그레이션

구문

```
system disable-http-user-cert
```

예

```
> system disable-http-user-cert
```

file

system file 명령을 사용하면 디바이스의 공통 디렉토리에서 파일을 관리할 수 있습니다.

액세스
컨피그레이션

copy

로그인 사용자 이름을 사용하여 호스트에서 원격 위치로 파일을 전송하려면 FTP를 사용합니다. 로컬 파일은 공통 디렉토리에 두어야 합니다.

구문

```
system file copy hostname username path filenames filenames ...
```

여기서 *hostname*은 대상 원격 호스트의 이름 또는 IP 주소, *username*은 원격 호스트에 있는 사용자의 이름, *path*는 원격 호스트에 있는 대상 경로, *filenames*는 전송할 로컬 파일을 지정합니다. 파일 이름은 공백으로 구분합니다.

예

```
> system file copy sfrocks jdoe /pub *
```

delete

공통 디렉토리에서 지정된 파일을 제거합니다.

구문

```
system file delete filenames filenames ...
```

여기서 *filenames*는 삭제할 파일을 지정합니다. 파일 이름은 공백으로 구분됩니다.

예

```
> system file delete *
```

list

파일 이름을 지정하지 않으면 공통 디렉토리의 모든 파일에 대한 수정 시간, 크기 및 파일 이름이 표시됩니다. 파일 이름을 지정하면 지정된 파일 이름과 일치하는 파일에 대한 수정 시간, 크기 및 파일 이름이 표시됩니다.

구문

```
system file list {filenames filenames ...}
```

여기서 filenames는 표시할 파일을 지정합니다. 파일 이름은 공백으로 구분됩니다.

예

```
> system file list
```

secure-copy

로그인 사용자 이름을 사용하여 호스트에서 원격 위치로 파일을 전송하려면 SCP를 사용합니다. 로컬 파일은 /var/common 디렉토리에 두어야 합니다.

구문

```
system file secure-copy hostname username path filenames filenames ...
```

여기서 *hostname*은 대상 원격 호스트의 이름 또는 IP 주소, *username*은 원격 호스트에 있는 사용자의 이름, *path*는 원격 호스트에 있는 대상 경로, *filenames*는 전송할 로컬 파일을 지정합니다. 파일 이름은 공백으로 구분합니다.

예

```
> system file secure-copy 10.123.31.1 jdoe /tmp *
```

generate-troubleshoot

Cisco에서 분석할 문제 해결 데이터를 생성합니다.

액세스

컨피그레이션

구문

```
system generate-troubleshoot
```

이 구문은 어떤 문제 해결 데이터를 표시해야 하는지를 지정하는 선택적인 매개 변수의 목록을 표시합니다.

예

```
> system generate-troubleshoot
```

ldapsearch

지정된 LDAP 서버의 쿼리를 수행할 수 있도록 지원합니다. 모든 매개 변수가 필요한 것은 아닙니다.

액세스

컨피그레이션

구문

```
system ldapsearch host port baseDN userDN basefilter
```

여기서 *host*는 LDAP 서버 도메인, *port*는 LDAP 서버 포트, *baseDN*은 검색을 위한 DN(고유 이름), *userDN*은 LDAP 디렉토리에 바인딩되는 사용자의 DN, *basefilter*는 검색하려는 레코드를 지정합니다.

예

```
> system ldapsearch ldap.example.com 389 cn=users,
dc=example,dc=com cn=user1,cn=users,dc=example,dc=com, cn=user2
```

lockdown-sensor

expert 명령을 제거하고 디바이스의 bash 셸에 액세스합니다.

주의 이 명령은 고객 지원의 핫픽스 없이는 취소할 수 없습니다. 주의해서 사용해야 합니다.

액세스
컨피그레이션

구문
```
system lockdown-sensor
```

예
```
> system lockdown-sensor
```

nat rollback

전에 적용된 NAT 컨피그레이션으로 시스템을 되돌립니다. 가상 디바이스 또는 ASA FirePOWER 디바이스에서는 이 명령을 이용할 수 없습니다. 클러스터링된 또는 스태킹된 디바이스에서는 이 명령을 이용할 수 없습니다.

액세스
컨피그레이션

구문
```
system nat rollback
```

예
```
> system nat rollback
```

reboot

디바이스를 재부팅합니다.

액세스
컨피그레이션

구문
```
system reboot
```

예
```
> system reboot
```

restart

디바이스 애플리케이션을 다시 시작합니다.

액세스
컨피그레이션

구문
```
system restart
```

예
```
> system restart
```

shutdown

디바이스를 종료합니다. ASA FirePOWER 모듈에서는 이 명령을 이용할 수 없습니다.

액세스
컨피그레이션

구문
```
system shutdown
```

예
```
> system shutdown
```

보안, 인터넷 액세스, 통신 포트

방어 센터를 보호하려면 보호된 내부 네트워크에 설치합니다. 방어 센터에서 필수 서비스와 사용 가능한 포트만 사용하도록 구성한 경우에도 방화벽 밖의 공격이 방어 센터(또는 관리되는 디바이스)에 도달할 수 없도록 해야 합니다.

방어 센터 및 관리되는 디바이스가 동일 네트워크에 상주하는 경우 디바이스의 관리 인터페이스를 방어 센터와 동일한 보호된 내부 네트워크에 연결할 수 있습니다. 그럼으로써 방어 센터에서 디바이스를 안전하게 제어할 수 있습니다. 또한 복수 관리 인터페이스를 구성하면 방어 센터에서 다른 네트워크의 디바이스의 트래픽을 관리 및 격리할 수도 있습니다.

어플라이언스를 구축하는 방식과 상관없이 어플라이언스 간 통신은 암호화됩니다. 하지만 DDoS(Distributed Denial of Service) 또는 중간자(man-in-the-middle) 등의 공격으로 FireSIGHT 시스템 어플라이언스 간 통신이 중단, 차단, 변경되지 않도록 조치를 취해야 합니다.

또한 FireSIGHT 시스템의 특정 기능에는 인터넷 연결이 필요합니다. 기본적으로 모든 FireSIGHT 시스템 어플라이언스는 인터넷에 직접 연결할 수 있도록 구성됩니다. 또한 특정 포트는 보안 어플라이언스 액세스를 제공하고 특정 시스템 기능이 올바르게 작동하는 데 필요한 로컬 또는 인터넷 리소스에 액세스할 수 있도록 개방하여 기본적인 어플라이언스 간 통신을 제공해야 합니다.

팁 Cisco NGIPS for Blue Coat X-Series를 제외하고 FireSIGHT 시스템 어플라이언스는 프록시 서버 사용을 지원합니다. 자세한 내용은 64-8페이지의 관리 인터페이스 구성 및 D-33페이지의 http-proxy을/를 참조하십시오.

자세한 내용은 다음 링크를 참고하십시오.

인터넷 액세스 요구 사항

기본적으로, FireSIGHT 시스템 어플라이언스는 모든 FireSIGHT 시스템 어플라이언스에서 기본적으로 개방되는 포트 443/tcp(HTTPS) 및 80/tcp(HTTP)에서 인터넷에 직접 연결하도록 구성됩니다. E-3페이지의 통신 포트 요구 사항을/를 참조하십시오. 대부분의 FireSIGHT 시스템 어플라이언스는 프록시 서버의 사용을 지원합니다. 64-8페이지의 관리 인터페이스 구성을/를 참조하십시오. 프록시 서버는 whois 액세스에 사용할 수 없습니다.

운영 연속성을 보장하려면 고가용성 페어의 두 방어 센터에 인터넷 액세스가 있어야 합니다. 특정 기능의 경우 기본 방어 센터에서 인터넷에 접속한 다음 동기화 프로세스 중 보조 방어 센터와 정보를 공유합니다. 기본 방어 센터에 장애가 발생할 경우 4-15페이지의 고가용성 상태 모니터링 및 변경에 설명된 대로 보조 방어 센터를 활성으로 승격합니다.

다음 표는 FireSIGHT 시스템의 특정 기능에 대한 인터넷 액세스 요구 사항을 설명합니다.

표 E-1 FireSIGHT 시스템 기능의 인터넷 액세스 요구 사항

기능	인터넷 액세스가 필요한 이유	어플라이언스	고가용성 고려 사항
동적 분석: 쿼리	이전에 동적 분석을 위해 제출한 파일의 위협 점수를 확인하기 위해 클라우드에 쿼리	방어 센터	페어의 방어 센터에서는 클라우드에 쿼리하여 위협 스코어를 독립적으로 확인합니다.
동적 분석: 제출	동적 분석을 위해 클라우드로 파일 제출	Series 2 및 X-Series를 제외한 모든 디바이스	해당 없음
FireAMP 통합	Cisco 클라우드에서 엔드포인트 기반(FireAMP) 악성코드 이벤트 수신	방어 센터	클라우드 연결은 동기화되지 않습니다. 두 방어 센터에 구성하십시오.
침입 규칙, VDB, GeoDB 업데이트	침입 규칙, GeoDB 또는 VDB 업데이트를 어플라이언스로 직접 다운로드하거나 다운로드 일정 예약	방어 센터	침입 규칙, GeoDB, VDB 업데이트가 동기화됩니다.
네트워크 기반 AMP	악성코드 클라우드 조회 수행	방어 센터	페어의 방어 센터에서는 클라우드 조회를 독립적으로 수행합니다.
RSS 피드 대시보드 위젯	Cisco를 포함한 외부 소스에서 RSS 피드 데이터 다운로드	가상 디바이스 및 X-Series를 제외한 모든 디바이스	피드 데이터는 동기화되지 않습니다.
보안 인텔리전스 필터링	인텔리전트 피드를 포함한 외부 소스에서 보안 인텔리전스 피드 데이터 다운로드	방어 센터	기본 방어 센터에서는 피드 데이터를 다운로드한 다음 보조 방어 센터와 공유합니다. 기본 방어 센터에 장애가 발생할 경우 보조 방어 센터를 활성으로 승격합니다.
시스템 소프트웨어 업데이트	시스템 업데이트를 어플라이언스로 직접 다운로드하거나 다운로드 일정 예약	가상 디바이스 및 X-Series를 제외한 모든 디바이스	시스템 업데이트는 동기화되지 않습니다.
URL 필터링	액세스 제어를 위해 클라우드 기반 URL 카테고리 및 평판 데이터 다운로드, 분류되지 않은 URL에 대한 조회 수행	방어 센터	기본 방어 센터에서는 URL 필터링 데이터를 다운로드한 다음 보조 방어 센터와 공유합니다. 기본 방어 센터에 장애가 발생할 경우 보조 방어 센터를 활성으로 승격합니다.
whois	외부 호스트의 whois 정보 요청	가상 디바이스 및 X-Series를 제외한 모든 디바이스	whois 정보를 요청하는 어플라이언스는 인터넷에 액세스할 수 있어야 합니다.

통신 포트 요구 사항

FireSIGHT 시스템 어플라이언스는 기본적으로 포트 8305/tcp를 사용하는 양방향 SSL-암호화 통신을 사용하여 통신합니다. 이 포트는 기본적 어플라이언스 간 통신을 위해 **반드시** 개방되어 있어야 합니다. 개방된 다른 포트를 통해 다음과 같은 작업을 수행할 수 있습니다.

- 어플라이언스의 웹 인터페이스에 액세스
- 어플라이언스로 안전하게 원격 연결
- 시스템의 특정 기능이 올바르게 작동하는 데 필요한 로컬 또는 인터넷 리소스에 액세스

일반적으로 기능과 관련된 포트는 관련 기능을 활성화 또는 구성할 때까지 닫은 상태를 유지해야 합니다. 예를 들어, 방어 센터를 사용자 에이전트에 연결할 때까지 에이전트 통신 포트(3306/tcp)를 닫아야 합니다. 다른 예를 들어, LOM 포트를 활성화하기 전까지 Series 3에서 623/udp 포트를 닫아 두어야 합니다.

주의 개방된 포트를 닫음으로써 구축에 어떤 영향을 미칠지 이해하기 전까지 개방된 포트를 **닫지 마십시오**.

예를 들어, 관리되는 디바이스 블록에서 아웃바운드 25/tcp(SMTP) 포트를 닫을 경우 디바이스가 개별 침입 이벤트에 대한 이메일 알림을 전송할 수 없습니다(44-1페이지의 침입 규칙에 대한 외부 알림 구성 참조). 다른 예를 들어, 포트 443/tcp(HTTPS)를 닫아 물리적 관리되는 디바이스의 웹 인터페이스에 대한 액세스를 비활성화할 수 있지만, 그럴 경우 디바이스가 의심되는 악성코드 파일을 동적 분석을 위해 클라우드로 제출하지 못하게 됩니다.

일부 통신 포트는 변경할 수 있습니다.

- 시스템과 인증 서버 간 연결을 구성할 경우 LDAP 및 RADIUS 인증에 대해 사용자 정의 포트를 지정할 수 있습니다. 61-17페이지의 LDAP 인증 서버 식별 및 61-33페이지의 RADIUS 연결 설정 구성을/를 참조하십시오.
- 관리 포트(8305/tcp)를 변경할 수 있습니다. 64-8페이지의 관리 인터페이스 구성을/를 참조하십시오. 그러나 Cisco에서는 기본 설정을 유지할 것이 **적극** 권장합니다. 관리 포트를 변경하는 경우 구축에서 서로 통신해야 하는 모든 어플라이언스에 대해 변경해야 합니다.
- 32137/tcp 포트를 사용하면 업그레이드된 방어 센터에서 Cisco 클라우드와 통신할 수 없습니다. 그러나 Cisco에서는 버전 5.3 이상의 초기 설치에 대한 기본 설정인 포트 443으로 전환할 것을 권장합니다. 자세한 내용은 64-27페이지의 클라우드 통신 활성화을/를 참조하십시오.

다음 표는 FireSIGHT 시스템 기능을 완전히 활용하기 위해 각 어플라이언스 유형에 필요한 개방 포트입니다.

표 E-2 FireSIGHT 시스템 기능 및 작동을 위한 기본 통신 포트

포트	설명	방향	개방 위치	목적
22/tcp	SSH/SSL	양방향	모두	어플라이언스에 대한 안전한 원격 연결 허용
25/tcp	SMTP	아웃바운드	모두	어플라이언스의 이메일 알림 및 경고 전송
53/tcp	DNS	아웃바운드	모두	DNS 사용
67/udp 68/udp	DHCP	아웃바운드	X-Series를 제외한 모든 디바이스	DHCP 사용 **참고** 이러한 포트는 기본적으로 **닫혀** 있습니다.
80/tcp	HTTP	아웃바운드	가상 디바이스 및 X-Series를 제외한 모든 디바이스	RSS 피드 대시보드 위젯에서 원격 웹 서버에 연결

표 E-2 FireSIGHT 시스템 기능 및 작동을 위한 기본 통신 포트 (계속)

포트	설명	방향	개방 위치	목적
		양방향	방어 센터	HTTP를 통해 사용자 정의 및 타사 보안 인텔리전스 피드 업데이트 URL 카테고리 및 평판 데이터 다운로드(포트 443도 필요)
161/udp	SNMP	양방향	X-Series를 제외한 모든 디바이스	SNMP 폴링을 통해 어플라이언스의 MIB에 대한 액세스 허용
162/udp	SNMP	아웃바운드	모두	SNMP 경고를 원격 트랩 서버로 전송
389/tcp 636/tcp	LDAP	아웃바운드	가상 디바이스 및 X-Series를 제외한 모든 디바이스	외부 인증을 위해 LDAP 서버와 통신
389/tcp 636/tcp	LDAP	아웃바운드	방어 센터	감지된 LDAP 사용자의 메타데이터 가져오기
443/tcp	HTTPS	인바운드	가상 디바이스 및 X-Series를 제외한 모든 디바이스	어플라이언스의 웹 인터페이스에 액세스
443/tcp	HTTPS AMQP 클라우드 통신	양방향	방어 센터	가져오기: • 소프트웨어, 침입 규칙, VDB, GeoDB 업데이트 • URL 카테고리 및 평판 데이터(포트 80도 필요) • 인텔리전트 피드 및 다른 보안 인텔리전스 피드 • 엔드 포인트 기반(FireAMP) 악성코드 이벤트 • 네트워크 트래픽에서 감지된 파일의 악성코드 처리 • 전송된 파일에 대한 동적 분석 정보
			Series 2 및Series 3 디바이스	디바이스의 로컬 웹 인터페이스를 사용하여 소프트웨어 업데이트 다운로드
			Series 3 및 가상 디바이스	동적 분석을 위해 파일 제출
514/udp	syslog	아웃바운드	모두	원격 syslog 서버에 대한 경보 전송
623/udp	SOL/LOM	양방향	Series 3	SOL(Serial Over LAN) 연결을 사용하여 Lights-Out 관리 수행
1500/tcp 2000/tcp	데이터베이스 액세스	인바운드	방어 센터	타사 클라이언트의 데이터베이스에 대한 읽기 전용 액세스 허용
1812/udp 1813/udp	RADIUS	양방향	가상 디바이스 및 X-Series를 제외한 모든 디바이스	외부 인증 및 계정 관리를 위해 RADIUS 서버와 통신
3306/tcp	사용자 에이전트	인바운드	방어 센터	사용자 에이전트와 통신
8302/tcp	eStreamer	양방향	가상 디바이스 및 X-Series를 제외한 모든 디바이스	eStreamer 클라이언트와 통신

표 E-2 FireSIGHT 시스템 기능 및 작동을 위한 기본 통신 포트 (계속)

포트	설명	방향	개방 위치	목적
8305/tcp	어플라이언스 통신	양방향	모두	구축의 어플라이언스 간 안전하게 통신. **필수.**
8307/tcp	호스트 입력 클라이언트	양방향	방어 센터	호스트 입력 클라이언트와 통신
32137/tcp	클라우드 통신	양방향	방어 센터	업그레이드된 방어 센터와 종합 보안 인텔리전스 클라우드의 통신 허용

Third-Party 제품

FireSIGHT 시스템 제품에는 FireSIGHT 시스템 제품과 함께 사용하도록 배포된 특정 서드파티 오픈 소스 코드 제품이 포함되어 있습니다. 이러한 제품은 무료이며 각각의 해당 라이센스 계약에 따라 "있는 그대로" 배포됩니다. 다음 표에는 FireSIGHT 시스템 제품과 함께 사용하도록 Cisco에서 배포한 주요 오픈 소스 코드 제품 및 해당 라이센스 계약이 나열되어 있습니다.

표 F-1 오픈 소스 소프트웨어 라이센싱

오픈 소스 소프트웨어	라이센스 계약
Apache HTTPD Web Server 2.4.3	Apache License
Linux Kernel 2.6.32.24(Series 2)	GNU General Public License Version 2(GPLv2)
Linux Kernel 2.6.35.14(Series 3)	GNU General Public License Version 2(GPLv2)
Perl 5.10.1 및 관련 모듈	Perl Artistic License
Snort 2.9.7	GNU General Public License Version 2(GPLv2)

서드파티 오픈 소스 코드 제품의 전체 목록 및 FireSIGHT 시스템 제품과 함께 배포된 모든 해당 라이센스 계약의 전체 내용은 제품 명령줄에 로그인하여 다음을 통해 얻을 수 있습니다.

```
/usr/share/license-files
```

FireSIGHT 시스템 제품과 함께 사용된 서드파티 오픈 소스 코드 제품에 대한 소스 코드를 받아보고 싶은 경우 지원 사이트에 요청을 제출하여 구할 수 있습니다.

용 어

7000 Series

Series 3 관리되는 디바이스의 그룹. 이 시리즈의 디바이스에는 70xx 제품군(3D7010/7020/7030/7050 모델) 및 71xx 제품군(3D7110/7120/3D7115/3D7125 및 AMP7150 모델)이 포함됩니다.

8000 Series

Series 3 관리되는 디바이스의 그룹. 이 시리즈의 디바이스에는 81xx 제품군(3D8120/8130/8140 및 AMP8150 모델), 82xx 제품군(3D8250/8260/8270/8290 모델) 및 83xx 제품군(3D8350/8360/8370/8390 모델)이 포함됩니다. 8000 Series 디바이스는 일반적으로 7000 Series 디바이스보다 강력합니다.

AAB(Automatic Application Bypass)

인터페이스를 통과하는 패킷 처리에 허용되는 시간을 제한하며 시간이 초과되는 경우 패킷이 탐지를 우회하도록 허용하는 고급 디바이스 설정.

action

시스템이 특정 기준을 충족하는(또는 충족하지 않는) 네트워크 트래픽을 처리, 검사 또는 로깅하는 방법을 결정하는 설정. 작업은 다양한 유형의 규칙과 연결되며, 정책의 기본 작업으로서 특정 정책과도 연결됩니다.

AMP(Advanced Malware Protection)

약어로 AMP이며, FireSIGHT 시스템의 네트워크 기반 악성코드 탐지 및 악성코드 차단 기능. 이 기능을 FireAMP, 즉 Cisco의 엔드포인트 기반 AMP 툴(FireAMP 구독 필요)과 비교해 보십시오.

application

탐지된 네트워크 자산, 통신 메서드 또는 HTTP content. 시스템은 세 가지 유형의 애플리케이션인 애플리케이션 프로토콜, 클라이언트 애플리케이션 및 애플리케이션을 탐지합니다.

ASA FirePOWER

Cisco ASA with FirePOWER Services의 간단한 이름.

CAC 인증 및 권한 부여

사용자가 CAC(Common Access Card)에서 제공하는 자격 증명만을 사용하여 어플라이언스의 웹 인터페이스에 로그인하도록 하는 LDAP 인증의 유형.

CAC(Common Access Card)

미국 국방성에서 발행한 ID 카드로 CAC 인증 및 권한 부여에 사용됨.

Cisco ASA with FirePOWER Services

ASA FirePOWER 모듈이 설치된 Cisco ASA(Adaptive Security Appliance) 관리되는 디바이스의 그룹. 이 시리즈의 디바이스에는 ASA 5506-X, ASA5512-X, ASA5515-X, ASA5525-X, ASA5545-X, ASA5555-X, ASA5585-X-SSP-10, ASA5585-X-SSP-20, ASA5585-X-SSP-40 및 ASA5585-X-SSP-60 모델이 포함됩니다.

Cisco Cloud

종합 보안 인텔리전스 클라우드을/를 참조하십시오.

Cisco NGIPS for Blue Coat X-Series

가상 디바이스의 기능 대부분을 제공하는 Blue Coat의 확장 가능한 섀시 기반 시스템에 구축된 소프트웨어 기반 애플리케이션.

Cisco VRT

Cisco의 Vulnerability Research Team.

CLI

CLI(명령줄 인터페이스)을/를 참조하십시오.

CLI(명령줄 인터페이스)

Series 3 및 가상 디바이스의 제한적 텍스트 기반 인터페이스. CLI 사용자가 실행할 수 있는 명령은 사용자에게 할당된 액세스 레벨에 따라 달라집니다.

Context Explorer

모니터링되는 네트워크에 대한 자세한 상호 작용 그래픽 정보를 표시하는 페이지. 각 섹션은 선명한 선, 막대, 파이, 도넛 그래프 형식과 자세한 목록으로 정보를 표시합니다. 사용자 정의 필터를 만들고 적용하여 정밀 분석을 수행할 수 있으며 그래프 영역을 클릭하거나 커서를 올려놓으면 데이터 섹션을 자세히 확인할 수 있습니다. 세부적으로 맞춤화 및 구획화할 수 있고 실시간으로 업데이트되는 대시보드와는 달리, Context Explorer는 수동으로 업데이트되고, 데이터에 대한 더 넓은 범위의 컨텍스트를 제공하도록 설계되었으며, 활성 사용자 탐색에 편리하도록 일관된 단일 레이아웃을 제공합니다.

CRL

CRL(certificate revocation list)을/를 참조하십시오.

CRL(certificate revocation list)

어플라이언스에 대한 사용자 인증서를 발급한 인증 기관에서 호출한 인증서 목록. 이 목록을 사용하면 클라이언트 브라우저 인증서 확인을 통해 FireSIGHT 시스템 웹 인터페이스에 대한 액세스를 제한할 수 있습니다. 사용자가 CRL에 폐기된 인증서로 나열된 인증서를 선택하면 브라우저는 웹 인터페이스를 로드할 수 없습니다. SSL 검사 중에 디바이스는 CRL의 공개 키 인증서를 탐지할 수 있으며 암호화된 트래픽을 신뢰할 수 없습니다.

Data Correlator

시스템에서 수집한 데이터를 사용하여 방어 센터에서 이벤트 및 네트워크 맵을 생성하는 프로그램.

DN 객체

공개 키 인증서의 주체 또는 발급자 DN을 나타내는 재사용 가능한 객체.

EC(Elliptic Curve) 암호화

한정된 필드에서 임의의 EC에 대한 점수 계산을 기반으로 하는 암호화 방법. RSA 암호화와 비교해 보십시오.

eStreamer

방어 센터 또는 관리되는 디바이스에서 외부 클라이언트 애플리케이션으로 이벤트 데이터를 스트리밍하는 데 사용할 수 있는 FireSIGHT 시스템의 구성 요소.

Event Streamer

eStreamer을/를 참조하십시오.

failsafe

내부 트래픽 버퍼가 꽉 찼을 때 패킷이 프로세싱을 우회하고 디바이스를 계속해서 통과하도록 허용하는 인라인 집합의 특성.

FireAMP

악성코드 침투, 지속적인 위협, 표적 공격을 발견, 이해 및 차단하는 Cisco의 엔터프라이즈급, 엔드포인트 기반 고급 악성코드 분석 및 방지 솔루션입니다. 조직에 FireAMP 구독이 있는 경우 개별 사용자는 엔드포인트(컴퓨터, 모바일 디바이스)에 경량의 FireAMP Connector를 설치하며, 이를 통해 종합 보안 인텔리전스 클라우드와 통신합니다. 이렇게 하면 악성코드를 빠르게 식별 및 격리하는 것은 물론, 발생 시 즉시 파악하고, 궤적을 추적하고, 영향을 파악하고, 성공적으로 복구하는 방법을 알아볼 수 있습니다. 또한 FireAMP 포털을 사용하여 사용자 지정 보호를 만들고 특정 애플리케이션의 실행을 차단하며 사용자 정의 화이트리스트를 작성할 수 있습니다. 네트워크 기반 AMP(Advanced Malware Protection)와 비교해 보십시오.

FireAMP Connector

서브스크립션 기반 FireAMP 구축의 사용자가 엔드포인트(예: 컴퓨터와 모바일 디바이스)에 설치하는 경량 에이전트. Connector는 종합 보안 인텔리전스 클라우드와 통신하며, 조직 전체에서 악성코드를 빠르게 식별 및 격리하기 위해 사용할 수 있는 정보를 교환합니다. 또한 엔드포인트 호스트에서 IOC(indications of compromise)를 식별할 수도 있습니다.

FireAMP 구독

조직이 FireAMP를 AMP(AMP(Advanced Malware Protection)) 솔루션으로 사용하도록 허용하는 별도 구매 서브스크립션. 네트워크 기반 AMP를 수행하기 위해 관리되는 디바이스에서 활성화하는 악성코드 라이센스와 비교해 보십시오.

FireAMP 포털

조직의 구독 기반 FireAMP 구축을 구성할 수 있는 웹사이트(http://amp.sourcefire.com/).

FireAMP 프라이빗 클라우드

모니터링되는 네트워크와 FireAMP 기반(파일 및 악성코드) 기능용 종합 보안 인텔리전스 클라우드 간 보안 중재자 역할을 하는 FireAMP 제공 가상 머신. 클라우드에 대한 모든 연결은 개별 에이전트 또는 네트워크의 어플라이언스에서 발생하기보다는 프라이빗 클라우드의 익명 프록시 연결을 통해 발생합니다.

FireSIGHT 권장 규칙

네트워크 맵에서의 정보를 기반으로 침입 정책에서 활성화 또는 비활성화해야 할 규칙을 권장하는 기능. 시스템이 권장 사항을 기반으로 규칙 상태를 수정하도록 허용할 수 있습니다. 이 경우 시스템은 읽기 전용 FireSIGHT 권장 레이어를 추가합니다.

FireSIGHT 권장 레이어

시스템이 규칙 상태를 FireSIGHT 권장 규칙 기능에서 권장하는 것으로 수정하도록 허용할 때 존재하는 침입 정책의 내장형 레이어.

FireSIGHT 라이센스

host, application 및 사용자 검색을 수행하도록 허용하는 방어 센터의 기본 라이센스. 또한 FireSIGHT 라이센스에 따라 방어 센터 및 관리되는 디바이스를 사용하여 모니터링할 수 있는 개별 host 수 및 사용자 수와 사용자 제어를 수행하기 위해 액세스 제어 규칙에서 사용할 수 있는 액세스 제어 대상 사용자 수가 결정됩니다.

GeoDB

GeoDB(지오로케이션 데이터베이스)을/를 참조하십시오.

GeoDB(지오로케이션 데이터베이스)

라우팅 가능한 IP 주소와 연결된 알려진 지오로케이션 데이터의 정기적으로 업데이트되는 데이터베이스.

GID

GID(generator ID)을/를 참조하십시오.

GID(generator ID)

시스템의 어떤 구성 요소가 침입 이벤트를 생성했는지를 나타내는 번호. GID를 사용하면 SID(Signature ID)가 규칙을 트리거한 패킷의 컨텍스트를 제공하는 것과 동일한 방법으로 이벤트 유형을 카테고리화하여 이벤트를 좀 더 효과적으로 분석할 수 있습니다.

HA 링크 인터페이스

디바이스 간 상태 정보 공유를 위한 이중 통신 채널 역할을 하도록 클러스터링된 디바이스 쌍의 각 멤버에 구성하는 물리적 인터페이스로, 고가용성 링크 인터페이스라고도 함.

host

네트워크에 연결되며 고유한 IP 주소가 있는 디바이스. FireSIGHT 시스템에서 볼 때 호스트란 모바일 디바이스, 브리지, 라우터, NAT 디바이스 또는 로드 밸런서로 분류되지 않은 식별된 호스트입니다.

HTTP 응답 페이지

사용자의 HTTP 요청이 액세스 제어에 의해 차단될 때 표시되도록 시스템을 구성할 수 있는 웹 페이지. 일반 Cisco 제공 응답 페이지를 표시하거나 사용자 지정 HTML을 제공할 수 있습니다. 요청이 인터랙티브 차단 규칙에 의해 차단된 경우, 사용자가 응답 페이지의 버튼을 클릭하여 원래 요청된 사이트로 계속 이동하도록 허용할 수 있습니다.

ID 충돌

시스템이 현재 능동 ID와 충돌하며 전에는 수동 ID로 보고되었던 새로운 수동 운영 체제 또는 서버 ID를 보고하는 경우 발생하는 충돌.

IOC(indications of compromise)

시스템이 FireAMP 엔드포인트 데이터를 모니터링되는 네트워크의 호스트와 연결하는, 네트워크 검색 정책에 구성된 기능. 손상 가능성이 있는 호스트는 상태를 나타내는 태그로 표시되며, 호스트 프로필 및 관련 이벤트 보기에서 확인할 수 있습니다.

LACP(Link Aggregation Control Protocol)

여러 물리적 포트의 결합을 제어하여 LAG(link aggregation group)라는 단일 논리적 데이터 채널을 형성하기 위해 시스템 및 포트 정보를 교환하는 방법을 제공하는 IEEE 802.3ad 사양의 구성 요소. LACP를 활성화하면 채널의 끝에 있는 각 디바이스는 LACP를 사용하여 어떤 링크가 집계에서 적극적으로 사용될지를 파악할 수 있습니다.

LAG(Link Aggregation Group)

네트워크 간에 전환되는 패킷을 제공하는 레이어 2 구축 또는 인터페이스 간에 트래픽을 라우팅하는 레이어 3 구축으로 구성된 관리되는 디바이스에서 단일 논리적 링크로 여러 물리적 이더넷 인터페이스를 그룹화하기 위해 사용할 수 있는 Series 3 기능. 이 단일 집계 논리적 링크는 두 엔드포인트 간에 더 우수한 대역폭, 이중화, 로드 밸런싱을 제공합니다.

LDAP 인증

사용자 자격 증명을 LDAP(Lightweight Directory Access Protocol) 디렉토리 서버에 저장된 LDAP 디렉토리와 비교하여 검증하는 외부 인증의 형식.

LOM(Lights-Out Management)

어플라이언스의 웹 인터페이스에 로그인하지 않고도 OOB(Out of Band) SOL(Serial over LAN) 관리를 사용하여 특정 어플라이언스를 원격으로 모니터링 또는 관리할 수 있는 Series 3 기능. 섀시 일련 번호 보기, 팬 속도와 온도 등의 조건 모니터링 등 제한적인 작업을 수행할 수 있습니다.

NAT

사설 네트워크의 여러 host 사이에서 단일 인터넷 연결을 공유하기 위해 가장 일반적으로 사용하는 네트워크 주소 변환 기능. 시스템에서는 검색을 사용하여 네트워크 디바이스를 로드 밸런서로 식별할 수 있습니다. 또한 FireSIGHT 시스템 레이어 3 구축의 경우 NAT 정책을 사용하여 NAT로 라우팅을 구성할 수 있습니다.

NAT 규칙

네트워크 트래픽을 평가하고 해당 자격과 일치하는 트래픽을 변환하는 방법을 지정하는 컨피그레이션 및 조건의 집합. NAT를 사용하여 라우팅을 수행할 수 있도록 NAT 규칙이 기존의 NAT 정책에 추가됩니다.

NAT 정책

NAT 규칙을 사용하여 NAT로 라우팅을 수행하는 정책.

NetFlow

Cisco IOS 지원 장비에서 실행하도록 Cisco에 의해 개발되었으며 개방형이지만 독점적인, IP 트래픽 정보 수집을 위한 프로토콜. FireSIGHT 시스템에 의해 수집된 검색 및 연결 데이터를 보충하고 관리되는 디바이스에서 다루지 못하는 네트워크를 모니터링하기 위해 NetFlow 지원 디바이스에 의해 수집된 정보를 사용할 수 있습니다.

NetMod

센싱 인터페이스가 포함된 관리되는 디바이스의 섀시에 설치하는 모듈.

Nmap

호스트에서 실행되는 운영 체제 및 애플리케이션 프로토콜을 탐지하기 위해 사용할 수 있는 오픈 소스 활성 스캐너인 Network Mapper. Nmap 스캔을 수행하면 탐지된 정보가 네트워크 맵에 추가됩니다.

PKI

PKI(Public Key Infrastructure)을/를 참조하십시오.

PKI 객체

공개 키 인증서 및 페어링된 사설 키를 나타내는 재사용 가능한 객체.

PKI(Public Key Infrastructure)

인증 기관이 개인에게 공개 키 인증서 및 페어링된 사설 키를 발급하는 방법을 관리하는 시스템.

RADIUS 인증

네트워크 리소스에 대한 사용자 액세스의 인증, 권한 부여, 어카운팅에 사용되는 서비스인 Remote Authentication Dial In User Service. FireSIGHT 시스템 사용자가 RADIUS 서버를 통해 인증할 수 있도록 허용하는 외부 인증 객체를 만들 수 있습니다.

RSA 암호화

큰 숫자를 두 개의 소수로 인수분해하는 것을 기반으로 하는 암호화 방법. EC(Elliptic Curve) 암호화와 비교해 보십시오.

Series 2

FireSIGHT 시스템 어플라이언스 모델의 두 번째 시리즈. 리소스, 아키텍처, 라이센싱 제한으로 인해 Series 2 어플라이언스는 제한적 기능 집합을 지원합니다. Series 2 디바이스에는 3D500, 3D1000, 3D2000, 3D2100, 3D2500, 3D3500, 3D4500, 3D6500 및 3D9900이 포함됩니다. Series 2 방어 센터에는 DC500, DC1000 및 DC3000이 포함됩니다.

Series 3

FireSIGHT 시스템 어플라이언스 모델의 세 번째 시리즈. Series 3 어플라이언스에는 7000 Series 및 8000 Series 디바이스와 DC750, DC1500, DC2000, DC3500, DC4000 방어 센터가 포함됩니다.

SFP 모듈

71xx 제품군 디바이스에서 네트워크 모듈에 삽입되는 SFP(Small Form-Factor Pluggable) 트랜시버. SFP 모듈의 센싱 인터페이스는 구성 가능한 우회를 허용하지 않습니다.

SHA-256 해시 값

때때로 SHA256으로 약식 표기되며, 악성코드 클라우드 조회를 수행하는 파일을 나타내는 32비트 문자열. 해시 값은 암호 해시 함수를 사용하여 계산되므로 동일한 SHA-256 값의 파일은 내용이 동일할 가능성이 매우 높습니다.

SID

SID(Signature ID)을/를 참조하십시오.

SID(Signature ID)

각 침입 규칙에 할당된 고유 식별 번호(Snort ID라고도 함). 새 규칙을 생성하거나 기존 표준 텍스트 규칙을 수정하는 경우 1,000,000 이상의 SID가 지정됩니다. FireSIGHT 시스템에서 제공하는 공유 객체 규칙 및 표준 텍스트 규칙의 SID는 1,000,000 미만입니다. 또한 프리프로세서 및 디코더는 SID를 사용하여 탐지되는 서로 다른 패킷 유형을 식별합니다.

Snort

IP 네트워크에서 실시간 트래픽 분석 및 패킷 로깅을 수행하는 오픈 소스 침입 탐지 시스템. Snort는 프로토콜 분석, 내용 검색 및 매칭을 수행할 수 있으며, 다양한 공격과 프로브를 탐지할 수 있습니다. Snort는 유연한 규칙 언어를 사용하여 수집 또는 전달해야 할 네트워크 트래픽을 설명합니다. FireSIGHT 시스템은 Snort를 사용하여 디코더, 프리프로세서 및 침입 규칙에 대해 패킷을 테스트합니다.

Spero 분석

악성 코드 분석을 위해 종합 보안 인텔리전스 클라우드로 파일 구조 특성을 제출하는 방법. 그 결과는 동적 분석을 보완합니다.

SSL

SSL(Secure Sockets Layer)을/를 참조하십시오.

SSL 검사

네트워크를 이동하는 암호화된 트래픽을 검사, 해독 및 로깅할 수 있는 기능. 해독하지 않도록 선택한 트래픽 및 해독된 트래픽 모두 액세스 제어로 더 검사할 수 있습니다.

SSL 규칙

시스템이 암호화된 트래픽을 검토하기 위해 사용하고 SSL 검사를 허용하는 조건 집합. SSL 정책을 채우는 SSL 규칙은 IP 주소 매칭을 수행하거나 다른 사용자, 애플리케이션, 포트, URL 및 암호화된 세션 특성이 포함된 복잡한 연결의 특성을 파악할 수 있습니다. SSL 규칙 작업은 시스템이 규칙 조건을 충족하는 트래픽을 처리하는 방법을 결정합니다. 다른 규칙 설정은 연결 로깅의 방법 및 로깅 여부를 결정합니다.

SSL 규칙 작업

시스템이 SSL 규칙 조건을 충족하는 암호화된 네트워크 트래픽을 처리하는 방식을 결정하는 설정. 일치하는 트래픽을 차단할 수 있습니다(연결 재설정 포함 또는 포함하지 않음). 또한 암호화된 트래픽, 업로드된 사설 키가 포함된 수신 트래픽, 재서명된 공개 키 인증서가 포함된 발신 트래픽을 해독할 수 없거나, 추가 SSL 규칙이 포함된 트래픽을 계속 모니터링할 수 없습니다.

SSL 정책

상위 액세스 제어 정책의 일부로 적용하며, 정책 대상 디바이스에서 모니터링하는 암호화된 트래픽에서 SSL 검사를 수행하는 정책. SSL 정책에는 복수의 SSL 규칙이 포함될 수 있으며, 해당 규칙의 기준을 충족하지 않는 트래픽에 대한 처리 및 로깅을 결정하는 기본 작업도 지정합니다. SSL 정책은 또한 CA 공개 키 인증서를 기반으로 어떤 암호화된 트래픽을 신뢰할지, 해독 불가 트래픽을 어떻게 처리할지를 지정합니다.

SSL(Secure Sockets Layer)

Transport Layer Security 프로토콜 앞에 오는 암호 애플리케이션 레이어 프로토콜. SSL 검사 기능을 사용하면 SSL 프로토콜로 암호화된 트래픽을 해독할 수 있습니다.

SVID

취약성 ID을/를 참조하십시오.

TLS

Transport Layer Security을/를 참조하십시오.

Transport Layer Security

SSL(Secure Sockets Layer) 프로토콜 뒤에 오는 암호 애플리케이션 레이어 프로토콜. SSL 검사 기능을 사용하면 TLS 프로토콜로 암호화된 트래픽을 해독할 수 있습니다.

URL 객체

개별 URL을 나타내는 재사용 가능한 객체.

URL 카테고리

악성코드나 소셜 네트워킹 등 URL에 대한 일반 분류.

URL 평판

종합 보안 인텔리전스 클라우드에 의해 결정된 대로, 웹사이트가 조직의 보안 정책에 반할 수 있는 목적에 사용될 가능성을 표시한 것.

URL 필터링

모니터링되는 호스트에서 요청하고 URL에 대한 URL 카테고리 및 URL 평판 정보(방어 센터가 종합 보안 인텔리전스 클라우드에서 얻음)의 상관관계를 분석한 URL을 기준으로 네트워크를 이동할 수 있는 트래픽을 결정하는 액세스 제어 규칙을 작성할 수 있는 기능. 허용 또는 차단할 개별 URL이나 URL 그룹을 지정하여 웹 트래픽을 좀 더 세부적으로 맞춤화하여 제어할 수 있습니다.

URL 필터링 라이센스

URL 카테고리 및 URL 평판 정보를 기준으로 URL 필터링을 수행할 수 있는 라이센스. URL 필터링 라이센스는 만료될 수 있습니다.

UTC 시간

협정 세계시. GMT(그리니치 표준시)로도 알려진 UTC는 세계 모든 곳에 공통된 표준 시간입니다. 표준 시간대 기능을 사용하여 로컬 시간을 설정할 수 있지만 FireSIGHT 시스템은 UTC를 사용합니다.

VDB

취약성 데이터베이스을/를 참조하십시오.

VLAN

VLAN(Virtual Extended Local Area Network)을/를 참조하십시오.

VLAN 태그 객체

개별 VLAN(Virtual Extended Local Area Network) 태그를 나타내는 재사용 가능한 객체.

VLAN(Virtual Extended Local Area Network)

VLAN은 지리적 위치가 아닌 부문 또는 기본 용도와 같이 몇 가지 다른 기준으로 호스트를 매핑합니다. 모니터링되는 호스트의 호스트 프로필에는 호스트와 관련된 VALN 정보가 표시됩니다. 가장 안쪽 VLAN 태그 정보는 다양한 이벤트에도 포함됩니다. 시스템은 연결의 VLAN 태그를 기반으로 액세스 제어를 비롯한 여러 유형의 트래픽 처리를 수행할 수 있습니다. 레이어 2 및 레이어 3 구축의 경우 관리되는 디바이스의 가상 스위치 및 가상 라우터가 VALN 태그가 포함된 트래픽을 적절히 처리하도록 구성할 수 있습니다.

VPN

FireSIGHT 시스템 관리되는 디바이스의 가상 라우터 간에 안전한 VPN 터널을 구축할 수 있는 기능.

VPN 라이센스

FireSIGHT 시스템 관리되는 디바이스의 가상 라우터 간에 안전한 VPN 터널을 구축할 수 있는 라이센스.

VRT

Cisco VRT을/를 참조하십시오.

VRT 분석 보고서

동적 분석을 위해 제출된 캡처된 파일의 Cisco VRT 분석 레코드. 동적 분석 요약 보고서에 있는 정보는 물론 동적 분석 중에 검색된 추가 정보에 대해서도 자세히 설명합니다.

whitelist

특정 종류의 작업에서 IP 주소를 제외하기 위해 위협 요소 제거 내에서 구성할 수 있는 규정 준수 화이트리스트, 보안 인텔리전스 화이트리스트, HA 링크 인터페이스 또는 IP 주소의 목록.

X-Series

Cisco NGIPS for Blue Coat X-Series의 간단한 이름.

가상 디바이스

가상 호스팅 환경에서 자체 장비에 구축할 수 있는 관리되는 디바이스. 가상 디바이스는 하드웨어 기반 기능(예: 고가용성, 클러스터링, 스태킹, NAT, VPN 및 빠른 경로 규칙)을 지원하지 않으며, 가상 디바이스를 가상 스위치 또는 가상 라우터로 구성할 수 없습니다.

가상 라우터

레이어 3 트래픽을 라우팅하는 라우티드 인터페이스의 그룹. 레이어 3 구축에서, 목적지 IP 주소에 따라 패킷 전달 결정을 내려 패킷을 라우팅하도록 가상 라우터를 구성할 수 있습니다. 고정 경로를 정의하고, RIP(Routing Information Protocol) 및 OSPF(Open Shortest Path First) 동적 라우팅 프로토콜을 구성하고, NAT(Network Address Translation)를 구현할 수 있습니다.

가상 방어 센터

가상 호스팅 환경에서 자체 장비에 구축할 수 있는 방어 센터.

가상 스위치

네트워크를 지나는 인바운드 및 아웃바운드 트래픽을 처리하는 스위치드 인터페이스의 그룹. 레이어 2 구축의 경우 관리되는 디바이스의 가상 스위치가 독립형 브로드캐스트 도메인으로 작동하도록 구성하여 네트워크를 논리적 세그먼트로 분할합니다. 가상 스위치는 호스트의 MAC(Media Access Control) 주소를 사용하여 패킷을 보낼 대상을 결정합니다.

가져오기

어플라이언스에서 어플라이언스로 다양한 컨피그레이션을 전달하는 데 사용할 수 있는 방법. 이전에 동일한 유형의 다른 어플라이언스에서 내보내기한 컨피그레이션을 가져올 수 있습니다.

감사 로그

시스템과의 사용자 상호 작용 레코드. 감사 로그는 감사 이벤트로 구성됩니다.

감사 이벤트

특정 FireSIGHT 시스템 사용자 상호 작용을 설명하는 이벤트. 각 감사 이벤트에는 타임스탬프, 이벤트를 생성한 작업을 수행한 사용자의 사용자 이름, 소스 IP 주소, 이벤트 설명 텍스트가 포함됩니다. 감사 이벤트는 감사 로그에 기록됩니다.

객체

이름을 값(예: IP 주소 또는 URL)과 연결하는 재사용 가능한 컨피그레이션. 웹 인터페이스에서 이 값을 사용할 때 대신 명명된 객체를 사용할 수 있습니다. 객체는 객체 관리자를 사용하여 생성합니다. 참조: 네트워크 객체, 보안 인텔리전스 객체, 포트 객체, VLAN 태그 객체, URL 객체, 애플리케이션 필터, 변수 집합, 파일 목록, HA 링크 인터페이스, 보안 영역, 암호 그룹 목록, DN 객체 및 PKI 객체.

객체 관리자

객체 및 객체 그룹을 관리하는 웹 인터페이스의 페이지.

검색

네트워크를 모니터링하고 네트워크에 대한 완전하고 지속적인 보기를 제공하기 위해 관리되는 디바이스를 사용하는 FireSIGHT 시스템의 구성 요소. 네트워크 검색은 네트워크에서 host(네트워크 디바이스 및 모바일 디바이스 포함)의 수와 유형은 물론 해당 호스트의 운영 체제, 활성 application 및 열린 포트에 대한 정보도 확인합니다. 또한 관리되는 디바이스를 구성하여 네트워크의 사용자 활동을 모니터링하면 정책 위반, 공격 또는 네트워크 취약성을 식별할 수 있습니다.

검색 규칙

네트워크 검색 정책 내에서, 모니터링할 네트워크와 영역 그리고 모니터링하는 데 사용할 디바이스(NetFlow 지원 디바이스)는 물론 모니터링에서 제외할 포트도 지정합니다. 각 규칙은 또한 모니터링되는 네트워크에서 host, 사용자 또는 application을 검색할지 여부도 지정합니다.

검색 데이터

검색 기능에 의해 수집된 네트워크 자산과 트래픽 플로우를 확인하는 호스트, 사용자 및 application 정보.

검색 이벤트

새 자산 또는 기존 자산에 대한 변경 사항의 검색을 자세히 설명하는 이벤트. 호스트 입력 이벤트는 특별한 종류의 검색 이벤트입니다. 때때로 "검색 이벤트"는 검색 데이터 또는 취약성 정보를 가리킵니다.

검색 정책

네트워크 검색 정책을/를 참조하십시오.

경고

시스템이 특정 이벤트를 생성한 알림. 알림은 침입 이벤트(영향 포함), 검색 이벤트, 네트워크 기반 악성코드 이벤트, 상관관계 정책 침입, 상태 변경 및 로깅된 연결을 기반으로 할 수 있습니다. 대부분의 경우 이메일, syslog 또는 SNMP 트랩을 통해 알릴 수 있습니다.

고가용성

디바이스 그룹을 관리하기 위해 이중 물리적 방어 센터를 구성할 수 있는 기능. 이벤트 데이터는 관리되는 디바이스에서 두 방어 센터로 스트리밍되며 대부분의 컨피그레이션 요소가 두 방어 센터에서 유지됩니다. 기본 방어 센터가 실패할 경우 보조 방어 센터를 사용하여 중단 없이 네트워크를 모니터링할 수 있습니다. 이중 디바이스를 지정할 수 있는 클러스터링과 비교해 보십시오.

공개 키

모든 사용자가 사용할 수 있는 공개 키 인증서와 관련된 암호 키. 공개 키 및 페어링된 사설 키는 SSL(Secure Sockets Layer) 및 Transport Layer Security의 암호화와 해독에 사용됩니다.

공개 키 인증서

개인에게 속한 인증서에 저장된 공개 키를 확인하는 개인을 대상으로 인증 기관에서 발급하는 디지털 문서.

공유 객체 규칙

C 소스 코드에서 컴파일된 이진 모듈로써 제공되는 침입 규칙. 공유 객체 규칙을 사용하면 표준 텍스트 규칙에서 할 수 없는 방법으로 공격을 탐지할 수 있습니다. 공유 객체 규칙에서는 규칙 키워드와 인수를 수정할 수 없습니다. 규칙에서 사용되는 변수를 수정하거나, 소스/목적지 포트 및 IP 주소와 같은 정보를 수정하고 규칙의 새 인스턴스를 사용자 지정 공유 객체 규칙으로서 저장할 수 있을 뿐입니다. 공유 객체 규칙의 GID(generator ID)는 3입니다.

공유 레이어

다른 정책에서 사용되도록 허용하는 침입 정책 또는 네트워크 분석 정책 레이어. 공유 레이어를 사용하는 정책은 사용자가 변경을 커밋하는 공유 레이어의 변경 사항으로 업데이트됩니다. 공유 레이어는 공유를 허용한 정책에서만 수정할 수 있으며, 이를 사용하는 정책에서는 읽기 전용입니다.

관리 인터페이스

FireSIGHT 시스템 어플라이언스를 관리하기 위해 사용하는 네트워크 인터페이스. 대부분의 구축에서 관리 인터페이스는 내부 보호되는 네트워크에 연결되어 있습니다. 센싱 인터페이스과 비교해 보십시오. 가상 방어 센터 및 모든 Series 3 어플라이언스에서, 채널에 대한 트래픽을 분리함으로써 성능을 개선하기 위해 또는 방어 센터가 다른 네트워크의 트래픽을 격리할 수 있도록 추가 네트워크에 대한 경로를 생성하기 위해 여러 관리 인터페이스를 구성할 수 있습니다. 트래픽 채널을 별도의 네트워크로 라우팅하여 처리 용량을 늘릴 수 있습니다.

관리 트래픽 채널

트래픽 채널을/를 참조하십시오.

관리되는 디바이스

디바이스을/를 참조하십시오.

교정 모듈

교정 인스턴스라고 하는 컨피그레이션 집합을 사용하여 위협 요소 제거를 실행하는 프로그램. FireSIGHT 시스템에는 다양한 작업을 수행하는 여러 교정 모듈이 포함되어 있습니다. 유연한 API를 사용하여 자체 모듈을 생성할 수도 있습니다.

교정 상태 이벤트

위협 요소 제거이 실행될 때 이벤트가 생성됩니다.

교정 인스턴스

교정 모듈에 대한 컨피그레이션 집합. 모듈당 여러 인스턴스를 구성할 수 있습니다. 예를 들어 모듈은 동일하지만 설정이 다른 인스턴스를 사용하여 서로 다른 상관관계 정책 위반에 응답할 수 있습니다. 교정 인스턴스가 트리거될 때 그 결과 작업을 위협 요소 제거라고 합니다.

구성 가능한 우회

우회 모드 구성을 허용하는 인라인 집합의 특성.

규정 준수 화이트리스트

상관관계 규칙과 더불어, 네트워크 트래픽이 상관관계 정책을 위반하기 위해 충족해야 하는 기준을 지정할 수 있는 방법 중 하나. 특정 서브넷의 host에서 실행을 허용할 운영 체제, application 및 프로토콜을 지정하려면 방어 센터를 사용하여 규정 준수 화이트리스트를 구성할 수 있습니다. 또한 화이트리스트 위반 시 응답(예: 경고 또는 위협 요소 제거)을 실행하도록 방어 센터를 구성할 수도 있습니다. 규정 준수 화이트리스트는 다른 whitelist 유형과 연결되지 않습니다.

규정 준수 화이트리스트 위반

화이트리스트 위반을/를 참조하십시오.

규정 준수 화이트리스트 이벤트

화이트리스트 이벤트을/를 참조하십시오.

규칙

종종 정책 내에서 네트워크 트래픽을 검사할 기준을 제공하는 구문. 참조: 액세스 제어 규칙, 상관관계 규칙, 검색 규칙, 빠른 경로 규칙, 파일 규칙, 침입 규칙, 네트워크 분석 규칙, 전처리기 규칙 및 SSL 규칙.

규칙 상태

침입 정책 내에서 침입 규칙의 활성화(Generate Events 또는 Drop and Generate Events로 설정됨) 또는 비활성화(Disable로 설정됨). 규칙을 활성화하면 네트워크 트래픽을 평가하는 데 사용되고, 비활성화하면 사용되지 않습니다.

규칙 업데이트

필요에 따라 침입 규칙을 업데이트하여 새로 업데이트되는 표준 텍스트 규칙, 공유 객체 규칙, 전처리기 규칙을 포함합니다. 규칙 업데이트는 규칙을 삭제하고, 기본 침입 정책, 네트워크 분석 정책 및 고급 액세스 제어 정책 설정을 수정하고, 기본 변수와 규칙 카테고리를 추가하거나 삭제할 수 있습니다.

규칙 작업

시스템이 규칙 조건을 충족하는 네트워크 트래픽을 처리하는 방식을 결정하는 설정. 참조: 액세스 제어 규칙 작업, 파일 규칙 작업 및 SSL 규칙 작업.

기반 정책

사용자 지정 정책에 대해 기반 정책 레이어 역할을 하는 침입 정책 또는 네트워크 분석 정책.

기반 정책 레이어

침입 정책 또는 네트워크 분석 정책의 가장 낮은 내장형 레이어. 기반 정책은 기반 정책 레이어의 설정, 따라서 정책의 기본 설정을 결정합니다.

기본 작업

액세스 제어 정책 또는 SSL 정책의 일부로서, 정책에서 비 모니터 규칙의 조건을 충족하지 않는 트래픽을 처리하고 검사하고 로깅하는 방법을 지정하는 action.

내보내기

어플라이언스에서 어플라이언스로 다양한 컨피그레이션(예: 정책)을 전달하는 데 사용할 수 있는 방법. 한 어플라이언스에서 컨피그레이션을 내보낸 후 동일한 유형의 다른 어플라이언스로 가져오기를 수행할 수 있습니다.

내부 인증

어플라이언스의 로컬 데이터베이스에 사용자 자격 증명을 저장하는 인증 방법. 사용자가 어플라이언스에 로그인하면 데이터베이스의 정보를 기준으로 사용자 이름 및 비밀번호가 확인됩니다. 외부 인증과 비교해 보십시오.

내장형 레이어

침입 정책 또는 네트워크 분석 정책의 읽기 전용 레이어. 이러한 정책에는 항상 기반 정책 레이어가 포함되며, 침입 정책에는 또한 내장형 FireSIGHT 권장 레이어도 포함됩니다.

네트워크 File trajectory(파일 전파 흔적 분석)

host가 네트워크에서 파일을 전송할 때 파일의 경로를 시각적으로 표시한 것. 관련 SHA-256 해시 값이 있는 파일의 경우 전파 흔적 맵은 파일을 전송한 모든 호스트의 IP 주소, 파일이 탐지된 시간, 파일의 악성코드 성향, 관련 파일 이벤트 및 악성코드 이벤트 등을 표시합니다.

네트워크 객체

하나 이상의 IP 주소, CIDR 블록 또는 접두사 길이를 나타내는 재사용 가능한 객체.

네트워크 검색

검색을/를 참조하십시오.

네트워크 검색 정책

NetFlow 지원 디바이스에서 모니터링하는 네트워크를 포함하여, 시스템이 특정 네트워크 세그먼트에 대해 수집하는 검색 데이터(host, 사용자 및 application 데이터 포함)의 종류를 지정하는 정책. 네트워크 검색 정책은 또한 ID 충돌 해결 환경 설정, 능동 탐지 소스 우선순위 및 IOC(indications of compromise)를 관리합니다.

네트워크 디바이스

FireSIGHT 시스템에서 브리지, 라우터, NAT 디바이스 또는 로드 밸런서로 식별되는 host.

네트워크 맵

네트워크의 자세한 표시. 네트워크 맵을 사용하면 네트워크에서 실행되고 있는 host, 모바일 디바이스, 네트워크 디바이스뿐만 아니라 관련 호스트 특성, 애플리케이션 프로토콜, 취약성 측면에서 네트워크 토폴로지를 볼 수 있습니다.

네트워크 분석 규칙

여러 사용자 지정 네트워크 분석 정책을 통해 대상을 지정하여 전처리를 수행하기 위해 사용할 수 있는 고급 FireSIGHT 시스템 사용자를 위한 조건 집합. 액세스 제어 규칙을 액세스 제어 정책의 고급 옵션으로 구성할 수 있습니다.

네트워크 분석 정책

침입 정책에 의한 이후 분석을 준비하기 위해 네트워크 트래픽을 디코딩, 표준화 및 전처리하도록 구성할 수 있는 다양한 프리프로세서. 기본적으로 단일 시스템 제공 네트워크 분석 정책이 액세스 제어 정책에서 다루는 모든 트래픽을 전처리합니다. 그러나 이 전처리를 수행하려면 사용자 지정 네트워크 분석 정책을 선택할 수 있습니다. 고급 사용자는 네트워크 분석 규칙을 사용하여 여러 사용자 지정 네트워크 분석 정책이 보안 영역, 네트워크 또는 VLAN 태그를 기반으로 트래픽을 전처리하도록 허용할 수 있습니다.

논리적 인터페이스

태그된 트래픽이 물리적 인터페이스를 통과할 때 특정 VLAN(Virtual Extended Local Area Network) 태그로 트래픽을 처리하기 위해 정의하는 가상 하위 인터페이스.

능동 탐지

활성 소스를 사용하여 host, application 및 사용자 정보를 검색. 활성 소스에는 Nmap과 같은 스캐너, 시스템의 웹 인터페이스에 대한 사용자 입력, 또는 명령줄이나 서드파티 애플리케이션 API 호출을 사용하는 네트워크 맵에 대한 호스트 입력이 포함됩니다. 수동 탐지과 비교해 보십시오.

대상 디바이스

정책 대상을/를 참조하십시오.

대시보드

시스템에 의해 수집 및 생성된 이벤트에 대한 데이터를 비롯하여 현재 시스템 상태를 한눈에 볼 수 있는 보기를 제공하는 디스플레이. 시스템과 함께 제공되는 대시보드를 늘리려면 여러 사용자 지정 대시보드를 생성하여 선택한 대시보드 위젯으로 채울 수 있습니다. 모니터링하는 네트워크의 모습과 동작을 광범위하고 개략적인 컬러 그림으로 보여주는 Context Explorer와 비교해 보십시오.

대시보드 위젯

FireSIGHT 시스템의 한 부분에 대한 통찰력을 제공하는 자체 포함형 소형 대시보드 구성 요소.

대응

상관관계 정책 위반에 대한 대응으로 경고 또는 위협 요소 제거.

데이터베이스 액세스

서드파티 클라이언트에 방어 센터 데이터베이스에 대한 읽기 전용 액세스를 제공하는 기능.

동적 규칙 상태

규칙과 일치하는 트래픽에서 탐지된 속도 이상에 응답하여 지정된 기간 동안 설정되는 침입 규칙 상태.

동적 분석

악성 코드 분석을 위해 디바이스에서 종합 보안 인텔리전스 클라우드로 캡처된 파일을 제출하는 방법. 클라우드는 파일을 테스트 환경에서 실행하며 위협 점수 및 동적 분석 요약 보고서를 방어 센터로 반환합니다. 동적 분석 요약 보고서에서 VRT 분석 보고서를 볼 수도 있습니다.

동적 분석 요약 보고서

동적 분석 중 검색된 위협은 물론 테스트 환경에서 파일을 실행할 때 탐지된 추가 프로세스를 포함하여 종합 보안 인텔리전스 클라우드에서 파일에 위협 점수를 할당한 이유의 요약. 여기에서 VRT 분석 보고서를 볼 수도 있습니다.

드릴다운 페이지

이벤트 보기를 제한하는 데 사용되는 중간 워크플로 페이지. 일반적으로 드릴다운 페이지는 좀 더 좁게 제한된 페이지 또는 테이블 보기로 진행하기 위해 선택할 수 있는 제약 조건을 표시합니다.

디바이스

광범위한 처리량에 사용할 수 있는 물리적 폴트 톨러런트(fault-tolerant)의 특별히 구축된 어플라이언스(Cisco ASA with FirePOWER Services 포함), 또는 다수의 동일한 기능이 포함된 소프트웨어 기반 구축. 디바이스에서 활성화하는 라이센스 기능에 따라, 트래픽을 수동적으로 모니터링하는 데 사용하여 네트워크 자산, application 트래픽, 사용자 활동에 대한 포괄적 맵을 구축하고 액세스 제어를 수행할 수 있습니다. 많은 디바이스는 또한 스위칭, 라우팅(DHCP 릴레이 및 NAT 포함), VPN을 수행할 수 있습니다. 디바이스는 방어 센터를 사용하여 관리해야 합니다.

디바이스 스태킹

스태킹을/를 참조하십시오.

디바이스 클러스터링

클러스터링을/를 참조하십시오.

디코더

스니핑된 패킷을 프리프로세서에서 인식할 수 있는 형식으로 전환하는 네트워크 분석 정책에 구성된 침입 감지 및 방지의 구성 요소.

디프래그먼트화 정책

대상 host의 운영 체제를 기반으로 IP 디프래그먼트화 프리프로세서(네트워크 분석 정책에서 구성)가 프래그먼트된 IP 패킷을 리어셈블하는 방법을 설명하는 하위 정책. 적응형 프로필은 적응형 디프래그먼트화 정책을 사용합니다.

라우터

네트워크 간에 패킷을 전달하는, 게이트웨이에 있는 네트워크 디바이스. 시스템에서는 네트워크 검색을 사용하여 라우터를 식별할 수 있습니다. 또한 관리되는 디바이스를 두 개 이상의 인터페이스 간 트래픽을 라우팅하는 가상 라우터로 구성할 수 있습니다.

라우티드 인터페이스

레이어 3 구축에서 트래픽을 라우팅하는 인터페이스. 태그가 지정되지 않은 VLAN(Virtual Extended Local Area Network) 트래픽 처리를 위한 물리적 라우티드 인터페이스 및 VLAN 태그가 지정된 트래픽을 처리하기 위한 논리적 라우티드 인터페이스를 설정할 수 있습니다. 또한 라우팅된 인터페이스에 정적 ARP(Address Resolution Protocol) 항목을 추가할 수 있습니다.

레이어

침입 정책 또는 네트워크 분석 정책 내부의 완전한 컨피그레이션 집합. 정책의 내장형 레이어에 사용자 지정 사용자 레이어를 추가할 수 있습니다. 더 높은 레이어의 설정이 더 낮은 레이어의 설정을 재정의합니다.

로드 밸런서

성능과 리소스 사용을 최적화하기 위해 트래픽을 분산하는 네트워크 디바이스. 시스템에서는 검색을 사용하여 로드 밸런서를 식별할 수 있습니다.

링크 상태 전파

인라인 집합의 인터페이스 중 하나가 다운될 때 쌍의 두 번째 인터페이스를 자동으로 중단하는 우회 모드의 인라인 집합의 옵션. 장애가 발생한 인터페이스가 복원되면 두 번째 인터페이스도 자동으로 활성화됩니다. 다시 말해, 페어링된 인터페이스의 링크 상태가 변경되면 다른 인터페이스의 링크 상태도 이에 맞게 자동으로 변경됩니다.

모니터

일치하는 트래픽을 로깅하되, 시스템이 연결을 즉시 허용 또는 차단하기보다는 계속해서 평가하도록 허용하는 방법. 보안 인텔리전스 블랙리스트를 위반하는 트래픽, 액세스 제어 규칙 또는 SSL 규칙에서 임의의 기준 조합과 일치하는 트래픽을 모니터링할 수 있습니다.

모바일 디바이스

FireSIGHT 시스템에서 검색 기능에 의해 모바일 핸드헬드 디바이스(예: 휴대폰이나 태블릿)로 식별된 host. 시스템은 종종 모바일 디바이스의 탈옥 여부를 탐지할 수 있습니다.

목록

보안 인텔리전스 목록을/를 참조하십시오.

물리적 인터페이스

NetMod에서 물리적 포트를 나타내는 인터페이스.

방어 센터

디바이스를 관리하고 생성되는 이벤트를 자동으로 집계 및 연결할 수 있는 중앙 관리 지점.

배너

서버 배너을/를 참조하십시오.

변경 조정 보고서

새 컨피그레이션이 저장될 때마다 생성되는 스냅샷을 기반으로 지난 24시간 동안의 모든 시스템 변경 사항에 대한 자세한 보고서. 매일 지정된 시간에 이러한 보고서를 이메일로 전송하도록 시스템을 구성할 수 있습니다.

변수

침입 규칙에서 일반적으로 사용되는 값의 표현. FireSIGHT 시스템은 네트워크 및 포트 번호를 정의하기 위해 변수 집합에 포함된 사전 구성된 변수를 사용합니다. 규칙을 맞춤화하여 네트워크 환경을 정확히 반영하려면 여러 규칙에서 이러한 값을 하드 코딩하기보다는 변수 값을 변경할 수 있습니다.

변수 집합

네트워크 트래픽과 좀 더 일치하도록 각 침입 정책에서 활성화된 침입 규칙을 맞춤화하기 위해 침입 정책에 연결하는 변수 컨피그레이션 모음.

보고서 템플릿

보고서 및 섹션에 대한 데이터 제약 조건과 형식을 지정하는 템플릿.

보류 중(애플리케이션 프로토콜)

시스템이 애플리케이션 프로토콜을 긍정적으로도 부정적으로 식별할 수 없을 때 애플리케이션 프로토콜 ID에 부여되는 지정. 대부분의 경우 시스템은 보류 중인 애플리케이션 프로토콜을 식별하려면 더 많은 데이터를 수집 및 분석해야 합니다.

보안 영역

다양한 정책과 컨피그레이션에서 트래픽 플로우를 관리 및 분류하기 위해 사용할 수 있는 인라인, 패시브, 스위치드 또는 라우티드 인터페이스의 그룹. 단일 영역의 인터페이스를 여러 디바이스에서 사용할 수 있으며 복수 보안 영역을 단일 디바이스에 구성할 수도 있습니다. 한 보안 영역에 트래픽을 매칭하기 위해 적어도 하나의 인터페이스를 할당해야 하며, 각 인터페이스는 한 영역에만 속할 수 있습니다.

보안 인텔리전스

소스 또는 목적지 IP 주소를 기반으로 액세스 제어 정책당 네트워크를 통과할 수 있는 트래픽을 지정하는 기능. 이 기능은 액세스 제어 규칙에서 트래픽을 분석하기 전에 특정 IP 주소 사이에서 이동하는 트래픽을 블랙리스트(거부)하려는 경우 특히 유용합니다. 선택적으로, 보안 인텔리전스 필터링에 대한 모니터 설정을 사용하면 시스템은 블랙리스트에 추가되었을 수 있는 연결을 분석할 수 있으며, 일치 항목을 블랙리스트에 로깅할 수도 있습니다.

보안 인텔리전스 객체

하나 이상의 IP 주소를 나타내고 액세스 제어 정책의 보안 인텔리전스 블랙리스트 및 보안 인텔리전스 화이트리스트에 추가되는 단일 컨피그레이션. 보안 인텔리전스 객체에는 보안 인텔리전스 목록, 보안 인텔리전스 피드, 네트워크 객체 및 그룹이 포함됩니다. 또한 전역 블랙리스트, 전역 화이트리스트 및 인텔리전스 피드의 카테고리도 보안 인텔리전스 객체로 간주됩니다.

보안 인텔리전스 목록

보안 인텔리전스 객체로 방어 센터에 수동으로 업로드하는 IP 주소의 단순한 정적 컬렉션. 전역 블랙리스트 및 전역 화이트리스트와 함께 이 목록을 사용하여 보안 인텔리전스 피드를 늘리고 조정할 수 있습니다.

보안 인텔리전스 블랙리스트

액세스 제어 정책의 액세스 제어 규칙에서 트래픽을 분석하기 전에 호스트를 왕래하는 트래픽을 거부할 수 있는 IP 주소의 목록. 블랙리스트는 전역 블랙리스트를 비롯한 보안 인텔리전스 객체로 구성됩니다. 액세스 제어 정책의 보안 인텔리전스 화이트리스트는 블랙리스트를 재정의합니다.

보안 인텔리전스 이벤트

보안 인텔리전스 블랙리스트에서 차단하거나 모니터링하는 트래픽에 의해 생성된 연결 이벤트. 일반 연결 이벤트와는 독립적으로 보안 인텔리전스 이벤트를 보고 상호 작용할 수 있습니다.

보안 인텔리전스 피드

보안 인텔리전스 객체 중 하나이며, 시스템이 사용자가 구성하는 간격에 따라 정기적으로 다운로드하는 IP 주소의 동적 컬렉션. 피드는 정기적으로 업데이트되므로 시스템에서는 최신 정보와 함께 보안 인텔리전스 기능을 사용하여 네트워크 트래픽을 필터링할 수 있습니다. 인텔리전스 피드 절도 참조하십시오.

보안 인텔리전스 화이트리스트

액세스 제어 정책의 액세스 제어 규칙을 사용하여(보안 인텔리전스를 사용하는 트래픽을 거부하지 않음) 호스트를 왕래하는 트래픽을 검사하도록 정책을 적용하는 IP 주소의 목록. 정책의 화이트리스트는 보안 인텔리전스 블랙리스트를 재정의하므로 이를 사용하여 블랙리스트를 세부적으로 조정할 수 있습니다. 화이트리스트는 전역 화이트리스트를 비롯한 보안 인텔리전스 객체로 구성됩니다.

보안 정책

네트워크를 보호하기 위한 조직의 지침. 예를 들어 보안 정책에서는 무선 액세스 포인트의 사용을 금지할 수 있습니다. 보안 정책에는 직원의 조직 시스템 이용 지침을 제공하는 AUP(Acceptable Use Policy)도 포함됩니다.

보안 정책 위반

보안 위반, 공격, 익스플로잇 또는 네트워크의 기타 오용.

보호 라이센스

침입 감지 및 방지, 파일 제어, 보안 인텔리전스 필터링을 수행할 수 있는 라이센스. 라이센스가 없으면 Series 2 디바이스는 보안 인텔리전스를 제외한 보호 기능을 자동으로 갖게 됩니다.

보호되는 네트워크

방화벽 등의 디바이스에 의해 다른 네트워크 사용자로부터 보호되는 조직의 내부 네트워크. 시스템에 기본 제공되는 대부분의 침입 규칙에서는 변수를 사용하여 보호된 네트워크와 보호되지 않는(또는 외부) 네트워크를 정의합니다.

복잡한 제약 조건

특정 이벤트의 모든 기준을 사용하여 이벤트 쿼리를 제한하는 이벤트 보기 또는 이벤트 검색에 설정된 제약 조건.

북마크

이벤트 분석에서 특정 위치 및 시간에 대한 저장된 링크. 북마크에는 사용 중인 워크플로에 대한 정보, 보고 있는 워크플로의 부분, 보고 있는 워크플로 내의 페이지 번호, 선택한 시간 창, 비활성화한 열은 물론 부과한 제약 조건도 포함됩니다.

블랙리스트

상태 모니터 블랙리스트 또는 보안 인텔리전스 블랙리스트을/를 참조하십시오.

비 액세스 제어 대상 사용자

사용자 에이전트 또는 관리되는 디바이스에 의해 탐지된, 액세스 제어에 사용되지 않는 모든 사용자. 호스트에 로깅된 액세스 제어 대상 사용자가 없는 경우 비 액세스 제어 대상 사용자는 host의 현재 사용자만 가능합니다.

비공개 검색

사용자 계정과 연결된, 특정 테이블에 대한 검색 기준의 명명된 집합. 사용자 본인 및 Administrator 액세스 권한이 있는 사용자만 비공개 검색을 사용할 수 있습니다.

비-바이패스 모드

집합의 센싱 인터페이스가 어떤 이유로든 실패하는 경우 트래픽을 차단하는 인라인 집합의 특성.

비즈니스 연관성

조직의 비즈니스 운영(레크리에이션과 반대) 컨텍스트 내에서 application이 사용될 가능성. 애플리케이션 비즈니스 연관성의 범위는 Very Low에서 Very High까지입니다.

비활성 기간

상관관계 규칙이 트리거되지 않는 동안의 간격. 비활성 기간의 시간, 빈도 및 지속 시간을 구성할 수 있습니다. 유휴 기간도 참조하십시오.

빠른 경로 규칙

분석할 필요가 없는 트래픽이 처리를 우회할 수 있도록 제한된 기준 집합을 사용하여 디바이스의 하드웨어 레벨에서 구성하는 규칙.

사설 키

페어링된 공개 키 인증서의 소유자에게만 알려진 암호 키. 공개 키 및 공개 키는 SSL(Secure Sockets Layer) 및 Transport Layer Security의 암호화와 해독에 사용됩니다.

사용자

관리되는 디바이스 또는 사용자 에이전트에 의해 네트워크 활동이 탐지된 사용자.

사용자 ID

사용자을/를 참조하십시오.

사용자 기록

host에 대한 마지막 24시간의 사용자 활동을 그래프로 보여주는 것. 호스트의 호스트 프로필에서 볼 수 있는 사용자 기록은 호스트에 로그인한 것으로 탐지된 사용자의 사용자 이름과 함께 대략적인 로그인 및 로그아웃 시간을 막대 그래프로 표시합니다.

사용자 레이어

정책의 설정을 수정할 수 있는 침입 정책의 레이어.

사용자 세부사항

사용자 ID 및 사용자 활동 워크플로의 마지막 페이지. 사용자 세부사항에는 사용자에 대한 일반 정보와 함께 마지막 24시간 동안 사용자의 활동을 그래프로 보여주는 호스트 기록도 표시됩니다.

사용자 에이전트

네트워크에 로그인할 때 또는 다른 목적으로 Active Directory 자격 증명에 대해 인증할 때 사용자를 모니터링하기 위해 서버에 설치하는 에이전트. 액세스 제어 대상 사용자에 의한 활동은 User Agent에서 보고할 경우 액세스 제어 목적으로만 사용됩니다.

사용자 역할

FireSIGHT 시스템의 사용자에게 허용된 액세스 레벨. 예를 들어 이벤트 분석가, FireSIGHT 시스템을 관리하는 관리자, 서드파티 툴을 사용하여 방어 센터 데이터베이스에 액세스하는 사용자에게 웹 인터페이스에 대한 서로 다른 액세스 권한을 부여할 수 있습니다. 또한 특수 액세스 권한의 사용자 지정 역할을 만들 수도 있습니다.

사용자 역할 에스컬레이션

로그인 세션 중 또 다른 사용자 역할의 권한을 얻기 위해 비밀번호를 입력하도록 하는 사용자 지정 사용자 역할에 부여할 수 있는 권한.

사용자 인식

조직이 위협, 엔드포인트, 네트워크 인텔리전스와 사용자 ID 정보의 상관관계를 분석하고 사용자 제어를 수행할 수 있는 기능.

사용자 인식 객체

네트워크 트래픽에서 또는 사용자 에이전트에 의해 활동이 탐지된 사용자에 대해 메타데이터를 검색하도록 LDAP 서버에 연결할 수 있는 설정 모음. Microsoft Active Directory를 사용하는 조직의 경우 사용자 인식 객체는 액세스 제어 대상 사용자를 지정할 수도 있습니다.

사용자 인증서

서버가 사용자 ID의 보조 확인을 수행하도록 FireSIGHT 시스템 웹 서버에 대해 사용자의 브라우저를 식별하는 암호화된 인증서. 인증서는 어플라이언스에 대한 서버 인증서를 발급한 동일한 인증 기관에서 발급한 것이어야 합니다.

사용자 제어

액세스 제어에 따라 네트워크를 이동할 수 있는 사용자 관련 트래픽을 지정 및 로깅할 수 있는 기능.

사용자 지정 사용자 역할

특별한 액세스 권한이 있는 사용자 역할. 사용자 정의 사용자 역할은 임의 집합의 메뉴 기반 및 시스템 권한을 가질 수 있으며 원래 역할을 그대로 유지하거나 사전 정의된 사용자 역할을 기준으로 변경할 수 있습니다.

사용자 지정 워크플로

조직의 고유한 필요에 맞게 생성하는 워크플로.

사용자 지정 탐지 목록

SHA-256 해시 값으로 표시되는 파일의 목록. 시스템은 이 목록에서 파일을 탐지하면, 종합 보안 인텔리전스 클라우드에서 파일의 성향이 Clean일지라도 악성코드 클라우드 조회를 수행하지 않고 파일을 악성코드로 취급합니다.

사용자 지정 테이블

FireSIGHT 시스템에서 제공된 둘 이상의 사전 정의 테이블에서 온 필드를 결합하여 만들 수 있는 테이블. 예를 들어 호스트 특성 테이블의 호스트 중요도 정보를 연결 데이터 테이블의 정보와 결합하여 새 컨텍스트에서 연결 데이터를 검토할 수 있습니다.

사용자 지정 토폴로지

host, 모바일 디바이스 및 네트워크 디바이스 네트워크 맵에서 서브넷을 의미 있게 구성 및 식별하기 위해 사용할 수 있는 기능.

사용자 지정 핑거프린트

핑거프린트을/를 참조하십시오.

사용자 활동

시스템이 사용자 로그인 또는 로그오프(선택적으로, 일부 실패한 로그인 시도 포함)를 감지하거나 방어 센터 데이터베이스에서 사용자 레코드의 추가 또는 삭제를 감지할 경우 생성되는 이벤트.

삭제 규칙

규칙 상태가 Drop and Generate Events로 설정된 침입 규칙. 악의적인 패킷이 인라인 구축에서 규칙을 트리거하고, 적용하는 침입 정책이 인라인 상태에서 삭제되도록 설정된 경우 시스템은 패킷을 삭제하고 침입 이벤트(특히 삭제 이벤트)를 생성합니다.

삭제 이벤트

삭제 규칙이 트리거될 때 생성되는 침입 이벤트. 이벤트 뷰어에서 삭제 이벤트는 검은색 아래쪽 화살표로 표시됩니다.

상관관계 규칙

규정 준수 화이트리스트과 더불어, 네트워크 트래픽이 상관관계 정책을 위반하기 위해 충족해야 하는 기준을 지정할 수 있는 방법 중 하나. 특정 이벤트가 발생할 때 또는 네트워크 패턴이 트래픽 프로필에 설명된 정상적인 네트워크 트래픽 패턴을 벗어날 때 트리거되는(그리고 상관관계 이벤트를 생성하는) 상관관계 규칙을 구성하려면 방어 센터를 사용할 수 있습니다. 상관관계 규칙은 호스트 프로필 자격, 연결 추적기, 유휴 기간, 비활성 기간 등으로 제한할 수 있습니다. 또한 상관관계 규칙이 트리거될 때 응답(예: 경고 또는 위협 요소 제거)을 실행하도록 방어 센터를 구성할 수도 있습니다.

상관관계 분석

네트워크 위협에 실시간으로 대응하는 상관관계 정책을 구축하는 데 사용할 수 있는 기능. 상관관계의 위협 요소 제거 구성 요소는 정책 위반에 응답하는 사용자 지정 교정 모듈을 생성 및 업로드하기 위해 사용할 수 있는 유연한 API를 제공합니다.

상관관계 이벤트

상관관계 규칙이 트리거될 때 방어 센터에 의해 생성되는 이벤트. 화이트리스트 위반에 의해 생성되는 화이트리스트 이벤트는 특별한 종류의 상관관계 이벤트입니다.

상관관계 정책

상관관계 규칙 및 규정 준수 화이트리스트을 사용하여, 보안 정책 위반을 일으키는 네트워크 활동을 설명하는 정책. 정책 내 각 규칙 또는 화이트리스트에 대한 대응을 지정할 수 있습니다.

상태 공유

디바이스나 스택이 실패할 경우 중단 없이 피어가 트래픽 플로우를 인수할 수 있도록 클러스터링된 디바이스 또는 스택의 동기화를 허용하는 기능. 상태 공유는 엄격한 TCP 적용, 단방향 액세스 제어 규칙, blocking persistence 및 동적 NAT의 적절한 장애 조치를 보장합니다.

상태 모니터

구축에서 어플라이언스의 성능을 지속적으로 모니터링하는 기능. 상태 모니터는 제공된 상태 정책 내 상태 모듈을 사용하여 어플라이언스를 테스트합니다.

상태 모니터 블랙리스트

불필요한 상태 이벤트의 생성을 막기 위해 상태 모니터링의 일부를 일시적으로 비활성화하는 컨피그레이션. 어플라이언스 그룹, 단일 어플라이언스 또는 특정 상태 모듈에 대한 모니터링을 비활성화할 수 있습니다.

상태 모듈

구축에서 어플라이언스의 특정 성능 부문(예: CPU 사용량 또는 사용 가능한 디스크 공간)에 대한 테스트. 상태 모듈은 상태 정책에서 활성화하며 모니터링하는 성능 측면이 특정 수준에 도달하면 상태 이벤트를 생성합니다.

상태 이벤트

구축에서 어플라이언스 중 하나가 상태 모듈에 지정된 성능 기준을 충족할 때(또는 충족하지 못할 때) 생성되는 이벤트. 상태 이벤트는 또한 경고을 생성할 수 있습니다.

상태 정책

구축에서 어플라이언스의 상태를 확인할 때 사용되는 기준. 상태 정책은 상태 모듈을 사용하여 시스템 하드웨어 및 소프트웨어가 올바르게 작동하는지 여부를 나타냅니다. 기본 상태 정책을 사용할 수도 있고 고유한 상태 정책을 생성할 수도 있습니다.

서드파티 취약성

서드파티에서 수집하는 취약성 데이터. 조직이 서드파티 application에서 네트워크 맵 데이터를 가져오기 위해 스크립트를 작성하거나 명령줄 가져오기 파일을 생성할 수 있는 경우, 시스템의 취약성 데이터를 보강하기 위해 서드파티 취약성 데이터를 가져오기 위한 호스트 입력 기능을 사용할 수 있습니다.

서버

host에 설치되며 애플리케이션 프로토콜 트래픽으로 식별되는 서버 application(클라이언트 애플리케이션과 비교).

서버 ID

host의 서버에 대한 애플리케이션 프로토콜 유형, 공급업체 및 버전 세부사항.

서버 배너

서버 식별에 도움이 될 추가 정보를 제공할 수 있는, 서버에 대해 탐지된 첫 번째 패킷의 처음 256 바이트. 시스템은 서버가 처음 탐지되었을 때 서버 배너를 한 번만 수집합니다.

서버 인증서

변경할 수 없는 서버 ID 확인을 제공하는 인증 기관에서 발급한 암호화된 인증서. 모든 인증 기관의 인증서를 요청할 수 있으며 해당 사용자 지정 인증서를 어플라이언스에 업로드할 수 있습니다.

성향

악성코드 성향을/를 참조하십시오.

센싱 인터페이스

네트워크 세그먼트를 모니터링하기 위해 사용하는 디바이스의 네트워크 인터페이스. 관리 인터페이스과 비교해 보십시오.

소급 악성코드 이벤트

전에 감지된 파일에 대한 악성코드 성향이 변경될 때 생성되는 네트워크 기반 악성코드 이벤트. 이 경우 시스템은 소급 이벤트의 SHA-256 해시 값을 공유하는 파일 및 악성코드에 대한 성향을 업데이트합니다.

속도 필터링

일치하는 트래픽의 속도를 기반으로 규칙에 대한 새 침입 규칙 상태를 설정하는 변칙 탐지의 형식.

수동 탐지

관리되는 디바이스에 의해 수동적으로 수집된 트래픽의 분석을 거치는 검색 데이터의 모음. 능동 탐지과 비교해 보십시오.

스위치

다중 포트 브리지 역할을 하는 네트워크 디바이스. 시스템은 네트워크 검색을 사용하여 스위치를 브리지로서 식별합니다. 또한 관리되는 디바이스를 가상 스위치로서 구성하여, 패킷을 둘 이상의 네트워크 간에 전환할 수 있습니다.

스위치드 인터페이스

레이어 2 구축에서 트래픽을 전환하기 위해 사용할 인터페이스. 태그가 지정되지 않은 VLAN(Virtual Extended Local Area Network) 트래픽 처리를 위한 물리적 스위치드 인터페이스 및 VLAN 태그가 지정된 트래픽을 처리하기 위한 논리적 스위치드 인터페이스를 설정할 수 있습니다.

스태킹

스택 컨피그레이션의 물리적 디바이스 2~4개에 연결하여 네트워크 세그먼트에서 검사하는 트래픽의 양을 늘릴 수 있는 기능. 스태킹된 컨피그레이션을 구축하면 각 스태킹된 디바이스의 리소스를 공유된 단일 컨피그레이션으로 결합합니다.

스택

탐지 리소스를 공유하는 2~4개의 연결된 디바이스.

시간 창

이벤트 보기에서 이벤트에 대한 시간 제약 조건. 사용자 환경 설정에 따라, 서로 다른 이벤트 보기에는 서로 다른 기본 시간 창이 있을 수 있습니다. 모든 이벤트 보기가 시간의 제한을 받는 것은 아닙니다.

시스템 정책

구축의 여러 어플라이언스에 대해 유사할 수 있는 설정(예: 메일 릴레이 호스트 환경 설정 및 시간 동기화 설정). 시스템 정책을 자체 및 관리되는 디바이스에 적용하려면 방어 센터를 사용하십시오.

식별되지 않은 호스트

시스템이 호스트에 대한 정보를 충분히 수집하지 못했기 때문에 운영 체제를 식별할 수 없는 host. 알 수 없는 호스트과 비교해 보십시오.

악성코드 라이센스

네트워크 트래픽에서 AMP(AMP(Advanced Malware Protection))를 수행하도록 허용하는 라이센스. 파일 정책을 사용하면 관리되는 디바이스에서 탐지한 특정 파일 형식에서 악성코드 클라우드 조회를 수행하도록 시스템을 구성할 수 있습니다. FireAMP 구독과 비교해 보십시오.

악성코드 방지

AMP(Advanced Malware Protection)을/를 참조하십시오.

악성코드 성향

파일의 SHA-256 해시 값, 위협 점수, 그리고 파일이 정상 목록 또는 사용자 지정 탐지 목록에 있는지를 기반으로 파일에 악성코드가 포함되었는지 여부를 종합 보안 인텔리전스 클라우드에서 결정한 내용.

악성코드 성향 캐시

파일에 대한 악성코드 성향 및 위협 점수를 저장하는 방어 센터의 캐시. 시스템이 이미 SHA-256 해시 값을 기반으로 파일의 성향 또는 위협 점수를 알고 있는 경우 방어 센터는 성능 향상을 위해 악성코드 클라우드 조회를 수행하기보다는 캐시된 정보를 사용합니다. 캐시 데이터가 오래되어 쓸모없는 상태가 되지 않도록, 캐시의 정보는 일정 기간 후 시간 초과됩니다.

악성코드 스토리지 팩

캡처된 파일을 저장하기 위해 특정 디바이스에 설치할 수 있는, Cisco에서 제공하는 보조 SSD. 이를 통해 이벤트 및 컨피그레이션 스토리지에 대한 디바이스의 기본 하드 드라이브에서 여유 공간을 확보할 수 있습니다.

악성코드 이벤트

Cisco의 AMP(Advanced Malware Protection) 솔루션 중 하나에 의해 생성된 이벤트. 종합 보안 인텔리전스 클라우드에서 네트워크 트래픽에서 감지된 파일의 악성코드 성향을 반환하면 네트워크 기반 악성코드 이벤트가 생성되고, 해당 특성이 변경되면 소급 악성코드 이벤트가 생성됩니다. 구축된 FireAMP Connector가 위협을 탐지하거나, 악성코드 실행을 차단하거나, 악성코드를 격리하거나 격리에 실패할 때 생성되는 엔드포인트 기반 악성코드 이벤트와 비교해 보십시오.

악성코드 차단

Cisco의 네트워크 기반 AMP(AMP(Advanced Malware Protection)) 솔루션 구성 요소 인라인 구축에서, 악성코드 탐지가 탐지된 파일에 대해 악성코드 성향을 부여하거나 탐지된 파일이 사용자 지정 탐지 목록에 있는 경우 파일을 차단하거나 업로드 또는 다운로드를 허용할 수 있습니다. 이 기능을 FireAMP, 즉 Cisco의 엔드포인트 기반 AMP 툴(FireAMP 구독 필요)과 비교해 보십시오.

악성코드 클라우드 조회

방어 센터가 종합 보안 인텔리전스 클라우드와 통신하여 파일의 SHA-256 해시 값을 기준으로 네트워크 트래픽에서 감지된 파일의 악성코드 성향을 확인하는 프로세스.

악성코드 탐지

Cisco의 네트워크 기반 AMP(AMP(Advanced Malware Protection)) 솔루션 구성 요소 전반적인 액세스 제어 컨피그레이션 검사 네트워크 트래픽의 일부로서 관리되는 디바이스에 적용되는 파일 정책. 그런 다음 방어 센터에서 감지된 특정 파일 형식에 대해 악성코드 클라우드 조회를 수행하고 파일의 악성코드 성향에 대해 경고하는 이벤트를 생성합니다. 이어서 AMP 악성코드 차단이 실행되고 파일을 차단하거나 업로드 또는 다운로드를 허용합니다. 이 기능을 FireAMP, 즉 Cisco의 엔드포인트 기반 AMP 툴(FireAMP 구독 필요)과 비교해 보십시오.

알 수 없는 호스트

시스템에 의해 트래픽이 분석되었지만 운영 체제가 알려진 핑거프린트과 일치하지 않는 host. 식별되지 않은 호스트과 비교해 보십시오.

알림 응답

시스템이 이메일, syslog 또는 SNMP 트랩을 통해 경고을 전송하도록 하는 컨피그레이션 집합. 다양한 유형의 이벤트에 대한 알림을 받기 위해 단일 알림 응답을 사용할 수 있습니다.

암호 그룹 목록

트래픽 암호화에 사용된 여러 암호 그룹을 나타내는 재사용 가능한 객체.

애플리케이션

HTTP 트래픽의 내용 또는 요청 URL을 나타내는 application의 유형.

애플리케이션 비즈니스 연관성

비즈니스 연관성을/를 참조하십시오.

애플리케이션 위험

application 사용이 조직의 보안 정책을 위반할 수 있는 가능성. 애플리케이션 위험의 범위는 Very Low에서 Very High까지입니다.

애플리케이션 유형

application이 애플리케이션 프로토콜, 클라이언트 애플리케이션 또는 애플리케이션인지 여부.

애플리케이션 제어

액세스 제어의 일부로서, 네트워크를 이동할 수 있는 application 트래픽을 지정할 수 있는 기능.

애플리케이션 카테고리

가장 중요한 기능을 설명하는 일반 application 분류. 각 애플리케이션은 적어도 하나의 카테고리에 속합니다.

애플리케이션 탐지기

시스템이 네트워크에서 application을 식별하기 위해 사용하는 툴. 애플리케이션 탐지기는 ASCII 또는 16진수 패턴을 사용하여 패킷 헤더, 트래픽이 사용하는 포트 또는 둘 모두에서 애플리케이션을 식별합니다. Cisco는 시스템 업데이트, 취약성 데이터베이스 업데이트 또는 가져오기/내보내기 기능을 통해 추가 탐지기를 제공할 수 있습니다. 자체 애플리케이션 프로토콜 탐지기를 생성할 수도 있습니다.

애플리케이션 태그

애플리케이션 카테고리에서 처리되지 않는 application에 대한 정보. 예를 들어 비디오 스트리밍 애플리케이션에는 종종 "high bandwidth" 및 "displays ads" 태그가 추가됩니다. 애플리케이션에 포함할 태그 수에는 제한이 없으며 0도 가능합니다.

애플리케이션 프로토콜

호스트의 클라이언트 애플리케이션과 서버 간 통신 중에 탐지되는 애플리케이션 프로토콜 트래픽을 나타내는 application의 유형(예: SSH 또는 HTTP).

애플리케이션 필터

애플리케이션 위험, 비즈니스 연관성, 유형, 카테고리 및 태그와 관련된 기준에 따라 그룹화된 하나 이상의 application. 애플리케이션 필터는 객체 관리자에서 생성합니다.

액세스 목록

어플라이언스에 액세스할 수 있는 host를 나타내는, 시스템 정책에 구성된 IP 주소의 목록. 기본적으로 누구나 포트 443(HTTPS)을 사용하여 어플라이언스의 웹 인터페이스에 액세스하고, 포트 22(SSH)를 사용하여 명령줄에 액세스할 수 있습니다. 또한 포트 161을 사용하여 SNMP 액세스를 추가할 수 있습니다.

액세스 제어

네트워크를 이동하는 트래픽을 지정, 검사, 로깅할 수 있는 FireSIGHT 시스템의 기능. 액세스 제어는 보안 인텔리전스, SSL 검사, 프리프로세서 옵션, 침입 감지 및 방지, 파일 제어 및 AMP(Advanced Malware Protection)를 호출합니다. 또한 검색으로 검사할 수 있는 트래픽을 결정합니다.

액세스 제어 규칙

FireSIGHT 시스템에서 모니터링되는 네트워크 트래픽을 검사하고 구체적인 액세스 제어를 달성하기 위한 조건 집합. 액세스 제어 규칙은 액세스 제어 정책을 채우며 간단한 IP 주소 매칭을 수행하거나 다른 기준이 포함된 복잡한 연결의 특성을 지정할 수 있습니다. 액세스 제어 규칙 작업은 시스템이 규칙 조건을 충족하는 트래픽을 처리하는 방법을 결정합니다. 다른 규칙 설정은 연결 로깅의 방법 및 로깅 여부, 침입 정책 또는 파일 정책에서 규칙이 허용하는 트래픽을 검사하는지 여부를 결정합니다.

액세스 제어 규칙 작업

시스템이 액세스 제어 규칙의 조건을 충족하는 네트워크 트래픽을 처리하는 방식을 결정하는 설정. 일치하는 트래픽(연결의 재설정과 함께 또는 없이)을 *차단*할 수 있습니다. HTTP 트래픽의 경우 차단을 우회할 수 있는 옵션을 사용자에게 제공할 수 있습니다. 추가 검사 없이 통과하도록 트래픽을 *신뢰*하거나, 일치하는 트래픽을 *허용*(선택적으로 침입 정책 및 파일 정책으로 검사 가능)하거나, 추가 액세스 제어 규칙으로 트래픽을 계속 *모니터링*할 수 있습니다.

액세스 제어 대상 사용자

액세스 제어로 제어할 수 있는 네트워크를 사용하는 사용자. Microsoft Active Directory 서버와 방어 센터 간 연결을 구성할 때 액세스 제어 대상 사용자가 속해야 하는 LDAP 그룹을 지정합니다. 사용자 에이전트가 액세스 제어 대상 사용자에 의한 로그인을 보고하면 해당 사용자는 IP 주소와 연결되며, 이에 따라 사용자 조건이 있는 액세스 제어 규칙이 트리거됩니다. 비 액세스 제어 대상 사용자과 비교해 보십시오.

액세스 제어 정책

디바이스에 의해 모니터링되는 네트워크 트래픽에서 액세스 제어를 수행하기 위해 관리되는 디바이스에 적용하는 정책. 액세스 제어 정책에는 복수의 액세스 제어 규칙이 포함될 수 있으며, 해당 규칙의 기준을 충족하지 않는 트래픽에 대한 처리 및 로깅을 결정하는 기본 작업도 지정합니다. 액세스 제어 정책의 다른 설정은 보안 인텔리전스, SSL 검사, 성능 옵션, 프리프로세서 옵션 및 기타 고급 컨피그레이션을 관리합니다.

어플라이언스

FireSIGHT 시스템 방어 센터, 관리되는 디바이스, Cisco ASA with FirePOWER Services 또는 Cisco NGIPS for Blue Coat X-Series. 어플라이언스는 물리적 기반일 수도 있고 소프트웨어 기반일 수도 있습니다.

어플라이언스 통계

가동 시간, 로드 평균, 디스크 사용량, 시스템 프로세스 요약 등 어플라이언스에 대해 얻을 수 있는 정보, 그리고 방어 센터에서는 Data Correlator 프로세스에 대한 정보.

억제

이벤트 억제을/를 참조하십시오.

엔드포인트

사용자가 조직의 AMP(Advanced Malware Protection) 전략의 일부로서 FireAMP Connector를 설치하는 컴퓨터 또는 모바일 디바이스.

연결

두 host 간에 모니터링되는 세션. FireSIGHT 시스템 관리되는 디바이스에서 탐지된 연결을 로깅하는 것은 물론 NetFlow 지원 디바이스에서 연결 데이터를 가져올 수도 있습니다.

연결 그래프

연결 이벤트를 그래픽 형태로 표시하는 방법.

연결 로그

연결 이벤트을/를 참조하십시오.

연결 요약

5분 간격으로 집계되는 연결 데이터. 시스템은 연결 요약을 사용하여 연결 그래프 및 트래픽 프로필을 작성합니다. 집계하려면 여러 연결이 연결의 끝을 나타내야 하고, 동일한 소스 및 목적지 IP 주소를 가지고 있어야 하며, responder(목적지 host)에서 동일한 포트를 사용해야 합니다. 또한 동일한 프로토콜(TCP 또는 UDP) 및 애플리케이션 프로토콜을 사용해야 합니다. 마지막으로, 이러한 연결을 동일한 관리되는 디바이스에서 탐지하거나 동일한 NetFlow 지원 디바이스에서 내보내야 합니다.

연결 이벤트

시스템이 모니터링되는 host 및 다른 호스트 간에 연결을 탐지할 때 생성되는 이벤트. 보안 인텔리전스 이벤트는 특별한 종류의 연결 이벤트입니다. 연결 이벤트는 탐지된 트래픽에 대한 정보를 포함합니다. 다양한 설정을 통해 어떤 연결을 로깅하고 언제 로깅하며 그 데이터를 어디에 저장하는가를 세부적으로 제어할 수 있습니다. 관리되는 디바이스에서 탐지하는 연결의 경우 시작과 끝에 차단 해제된 연결을 로깅할 수 있지만, 대부분의 차단된 연결은 시작 부분에만 로깅할 수 있습니다.

이러한 연결을 방어 센터 데이터베이스에 로깅할 수 있습니다. 규칙 또는 기본 작업에 따라 외부 syslog 또는 SNMP 트랩 서버에 연결 이벤트를 로깅할 수도 있습니다. NetFlow 레코드는 연결의 끝을 로깅하며 항상 데이터베이스에 저장됩니다.

연결 추적기

규칙의 초기 기준이 충족된 후 시스템이 특정 연결 추적을 시작할 수 있도록 상관관계 규칙을 제한하는 하나 이상의 조건. 그러면 추적된 연결이 추가 조건을 충족하는 경우에만 규칙이 트리거됩니다.

영역

보안 영역을/를 참조하십시오.

영향

침입 이벤트에 대해 침입 데이터, 검색 데이터, 취약성 정보 간 상관관계를 숫자로 표시한 지표. 영향 레벨 1(빨간색 영향 아이콘)은 대상 host가 침입 이벤트로 표시된 공격에 *취약*함을 의미하며, 영향 레벨 2(주황색 영향 아이콘)는 *잠재적으로 취약*함을 의미합니다. 네트워크 검색 정책에 의해 모니터링되지 않는 네트워크의 호스트에서 온 공격은 영향 레벨 0(회색 영향 아이콘)입니다. 이는 방어 센터가 이벤트의 영향을 확인할 수 없음을 나타냅니다.

예약된 작업

한 번 또는 반복하여 실행하도록 예약할 수 있는 관리 작업.

외부 인증

사용자가 FireSIGHT 시스템 어플라이언스에 로그인할 때 외부에 저장된 사용자 자격 증명을 사용하여 사용자 이름과 비밀번호를 인증하는 방법(예: LDAP 인증 또는 RADIUS 인증) 내부 인증과 비교해 보십시오.

우회 모드

집합의 센싱 인터페이스가 어떤 이유로든 실패하는 경우 트래픽이 계속 흐르도록 허용하는 인라인 집합의 특성.

운영 체제 ID

host의 운영 체제에 대한 운영 체제 공급업체 및 버전 세부사항.

워크플로

이벤트 데이터의 넓은 보기에서 관심이 있는 이벤트만을 포함하는 좀 더 집중된 보기로 이동하여 이벤트를 보고 평가하기 위해 사용할 수 있는 일련의 페이지. 워크플로에는 각각 고유한 기능을 수행하는 세 가지 유형의 페이지, 즉 드릴다운 페이지, 테이블 보기 및 마지막 페이지가 포함될 수 있습니다. 워크플로 유형에 따라 마지막 페이지는 테이블 보기, 패킷 보기, 호스트 보기, 취약성 세부사항 또는 사용자 세부사항이 될 수 있습니다.

위젯

대시보드 위젯을/를 참조하십시오.

위험

애플리케이션 위험을/를 참조하십시오.

위협 요소 제거

시스템에 대한 잠재적인 공격을 완화하는 작업. 교정을 구성하고, 트리거될 때 방어 센터가 교정을 실행하도록 상관관계 정책 내에서 상관관계 규칙 및 규정 준수 화이트리스트과 연결할 수 있습니다. 이 프로그램은 문제를 즉시 해결할 수 없을 때 공격을 자동으로 완화할 뿐만 아니라 시스템이 조직의 보안 정책을 준수함을 보장할 수 있습니다. 방어 센터에는 사전 정의된 교정 모듈이 기본 제공되며 유연한 API를 사용하여 사용자 정의 위협 요소 제거를 만들 수 있습니다.

위협 점수

파일에 악성코드가 포함되어 있을 가능성을 측정하는 동적 분석을 위해 종합 보안 인텔리전스 클라우드에 제출한 결과 파일에 할당되는 1~100의 점수.

유휴 기간

상관관계 규칙이 트리거된 후 시스템이 해당 규칙 실행을 중지하는(간격 중에 규칙이 위반되더라도) 초, 분 또는 시로 지정된 간격. 유휴 기간이 끝나면 규칙을 다시 트리거할 수 있습니다(그리고 새 유휴 기간을 시작할 수 있습니다). 비활성 기간도 참조하십시오.

이벤트

워크플로를 사용하여 이벤트 뷰어에서 확인할 수 있는 특정 발생 상황에 대한 상세 정보의 컬렉션. 이벤트는 네트워크에서의 공격, 탐지된 네트워크 자산의 변경 사항, 조직의 보안 및 네트워크 사용 정책 위반 등을 나타낼 수 있습니다. 시스템은 또한 어플라이언스의 변경되는 상태, 웹 인터페이스, 규칙 업데이트, 실행된 위협 요소 제거의 사용에 대한 정보를 포함하는 이벤트를 생성합니다. 마지막으로, "이벤트"가 특별한 발생을 나타내지 않는 경우에도 시스템은 다른 특정 정보를 이벤트로 표시합니다. 예를 들면 이벤트 뷰어를 사용하면 탐지된 host, application 및 해당 취약성에 대한 자세한 정보를 볼 수 있습니다.

이벤트 뷰어

이벤트를 보고 조작하기 위해 사용할 수 있는 시스템의 구성 요소. 이벤트 뷰어는 워크플로를 사용하여 포괄적 정보를 표시한 다음 관심이 있는 이벤트만 포함된 더욱 집중적인 이벤트 보기를 표시합니다. 워크플로를 드릴다운하여 또는 검색을 사용하여 이벤트 보기에서 이벤트를 제한할 수 있습니다.

이벤트 억제

특정 IP 주소 또는 IP 주소의 범위가 침입 규칙을 트리거할 때 침입 이벤트를 억제하기 위해 사용할 수 있는 기능. 이벤트 억제는 오탐을 없애는 데 도움이 됩니다. 예를 들어 특정 익스플로잇처럼 보이는 패킷을 전송하는 이메일 서버가 있는 경우, 합당한 공격에 대한 이벤트만 볼 수 있도록 해당 서버에서 트리거되는 규칙에 대해 이벤트를 억제할 수 있습니다.

이벤트 임계값 지정

지정된 기간 내 이벤트 생성 횟수를 기반으로 시스템이 침입 이벤트를 로깅 및 표시하는 횟수를 제한하도록 설정할 수 있는 기능. 이벤트 수가 너무 많아서 혼란스러운 경우 이벤트 임계값을 사용할 수 있습니다.

이벤트 트래픽 채널

트래픽 채널을/를 참조하십시오.

인라인 구축

관리되는 디바이스가 네트워크에서 인라인으로 배치되는 FireSIGHT 시스템의 구축. 이 컨피그레이션에서는 디바이스가 네트워크 트래픽 플로우에 영향을 미칠 수 있습니다. 트래픽의 플로우를 분석하고 이에 응답할 수 있지만 영향을 미치지는 않는 패시브 탐지와 비교해 보십시오.

인라인 인터페이스

인라인 구축에서 트래픽을 처리하도록 구성된 센싱 인터페이스. 인라인 인터페이스를 인라인 집합에 쌍으로 추가해야 합니다.

인라인 집합

하나 이상의 인라인 인터페이스의 쌍.

인시던트

보안 정책 위반과 관련된 것으로 의심되는 하나 이상의 침입 이벤트. 시스템은 인시던트의 조사와 관련이 있는 정보를 수집 및 처리하는 데 사용할 수 있는 인시던트 처리 기능을 제공합니다.

인증 객체

FireSIGHT 시스템의 웹 인터페이스에 대한 외부 인증(RADIUS 또는 LDAP)을 활성화하기 위해 연결할 수 있는 설정 모음.

인증 기관

서버 인증서 또는 공개 키 인증서 생성에 사용된 인증서 발급자. 서버 및 사용자 인증서는 서버 또는 사용자 식별의 추가 확인을 제공합니다.

인증서

공개 키 인증서을/를 참조하십시오.

인터랙티브 차단

HTTP 응답 페이지의 버튼을 클릭하여 초기에 차단된 웹 사이트로 계속 이동하도록 허용하는 액세스 제어 규칙 작업.

인텔리전스 피드

Cisco VRT에서 평판이 나쁜 것으로 판단하고 정기적으로 업데이트하는 IP 주소 목록의 컬렉션. 인텔리전스 피드의 각 목록은 특정 카테고리, 즉 오픈 릴레이, 알려진 공격, bogon(bogus IP 주소) 등을 나타냅니다. 액세스 제어 정책에서는 보안 인텔리전스를 사용하여 모든 카테고리를 블랙리스트에 추가할 수 있습니다. 인텔리전스 피드는 정기적으로 업데이트되므로 이 피드를 사용하면 시스템에서 최신 정보를 사용하여 네트워크 트래픽을 필터링할 수 있습니다.

임계값 지정

이벤트 임계값 지정을/를 참조하십시오.

자동 인라인 모드

디바이스가 "bump in the wire" 역할을 하고, 소스 및 목적지와 상관없이 관찰하는 모든 네트워크 트래픽을 전달하도록 허용하는 고급 인라인 집합 옵션.

작업 대기열

어플라이언스에서 수행해야 할 작업의 대기열. 정책을 적용하고 소프트웨어 업데이트를 설치하고 기타 장기 실행 작업을 수행할 경우 작업이 대기열에 추가되고 Task Status 페이지에 상태가 보고됩니다. Task Status 페이지는 작업의 자세한 목록을 제공하고 10초마다 새로 고쳐지며 상태를 업데이트합니다.

저장된 파일

디바이스의 하드 드라이브 또는 악성코드 스토리지 팩에 저장되는 캡처된 파일. 저장된 파일은 나중에 다운로드 및 분석할 수 있습니다.

적용

정책 또는 해당 정책에 대한 변경 사항을 적용하기 위해 수행하는 작업. 방어 센터의 정책 대부분을 관리되는 디바이스에 적용합니다. 그러나 관리되는 디바이스의 컨피그레이션에 대한 변경과 관련이 없기 때문에 사용자는 상관관계 분석 정책을 활성화 및 비활성화합니다.

적응형 프로필

검색 데이터를 사용하여 패킷의 대상 host에 대한 운영 체제를 결정하는 고급 액세스 제어 정책 설정으로, 수동 구축에 권장됨. 네트워크 분석 정책 내 대상 프로필은 대상 호스트의 운영 체제와 동일한 방식으로 IP 패킷을 디프래그먼트하고 스트림을 리어셈블합니다. 침입 정책은 목적지 호스트에서 사용되는 것과 동일한 형식으로 데이터를 분석합니다.

전역 블랙리스트

모든 액세스 제어 정책의 보안 인텔리전스 블랙리스트에 기본적으로 포함되는 보안 인텔리전스 객체. 전역 블랙리스트는 모든 보안 영역에 적용됩니다. 대시보드, Context Explorer 및 많은 이벤트 뷰어 페이지에서 IP 주소 콘텍스트 메뉴를 사용하여 개별 IP 주소를 전역 블랙리스트에 추가할 수 있습니다.

전역 화이트리스트

모든 액세스 제어 정책의 보안 인텔리전스 화이트리스트에 기본적으로 포함되는 보안 인텔리전스 객체. 전역 화이트리스트는 모든 보안 영역에 적용됩니다. 대시보드, Context Explorer 및 많은 이벤트 뷰어 페이지에서 IP 주소 콘텍스트 메뉴를 사용하여 개별 IP 주소를 전역 화이트리스트에 추가할 수 있습니다.

전처리기 규칙

프리프로세서 또는 포트스캔 플로우 탐지기와 연결된 침입 규칙. 전처리기 규칙에서 이벤트를 생성하도록 하려면 해당 규칙을 활성화해야 합니다. 프리프로세서 규칙에는 프리프로세서별 GID(generator ID)가 있습니다.

정상 목록

SHA-256 해시 값으로 표시되는 파일의 목록. 시스템은 이 목록에서 파일을 탐지하면, 종합 보안 인텔리전스 클라우드에서 파일의 성향이 Malware일지라도 악성코드 클라우드 조회를 수행하지 않고 파일을 정상으로 취급합니다.

정책

설정을 적용하기 위한 메커니즘(대부분의 경우 어플라이언스에). 참조: 액세스 제어 정책, 상관관계 정책, 파일 정책, 상태 정책, 침입 정책, 네트워크 분석 정책, 네트워크 검색 정책, SSL 정책 및 시스템 정책.

정책 대상

정책을 적용하는 어플라이언스 또는 영역. 한 정책에 여러 대상이 있을 수 있습니다.

제어 라이센스

사용자 제어 및 애플리케이션 제어을 구현하기 위해 사용할 수 있는 라이센스. 또한 지원되는 관리되는 디바이스를 구성하여 스위칭과 라우팅(DHCP 릴레이 및NAT 포함), VPN, 디바이스 클러스터링 등 하드웨어 기반 작업을 수행할 수 있습니다.

종합 보안 인텔리전스 클라우드

클라우드 서비스 또는 *Cisco 클라우드*라고도 하며, 방어 센터에서 악성코드, 보안 인텔리전스, URL 필터링 데이터 등의 최신 관련 정보를 얻을 수 있고 Cisco에서 호스팅하는 서버. 악성코드 클라우드 조회 및 FireAMP 프라이빗 클라우드도 참조하십시오.

지오로케이션

연결 유형, 인터넷 서비스 공급자 등 모니터링되는 네트워크의 트래픽에서 감지된 라우팅 가능한 IP 주소의 위치에 대한 데이터를 제공하는 기능. 이벤트와 호스트 프로필에서 지오로케이션 정보를 보고, 이를 사용하여 액세스 제어 정책 또는 SSL 정책에서 트래픽을 필터링할 수 있습니다.

취약성

host가 영향을 받기 쉬운 특정 손상에 대한 설명. 방어 센터에서는 각 호스트가 취약해질 수 있는 취약성에 대한 정보를 해당 호스트 프로필에 제공합니다. 또한 취약성 네트워크 맵을 사용하여 모니터링되는 전체 네트워크에서 시스템이 탐지한 전반적인 취약성 보기를 얻을 수 있습니다. 하나 이상의 host가 특정 손상에 대해 더 이상 취약하지 않다고 판단되면, 특정 취약성을 비활성화하거나 유효하지 않은 것으로 표시할 수 있습니다.

취약성 ID

특정 취약성과 관련된 식별 번호. Bugtraq 및 CVE와 같은 Cisco 취약성 데이터베이스 및 서드파티 취약성 데이터베이스에서는 취약성 ID 번호 매기기 체계가 서로 다릅니다.

취약성 데이터베이스

host가 영향을 받기 쉬운 알려진 취약성의 데이터베이스로, VDB라고도 함. 특정 호스트가 네트워크 손상의 위험을 높이는지 여부를 판단할 수 있도록 시스템은 각 호스트에서 탐지된 운영 체제, 애플리케이션 프로토콜 및 클라이언트를 VDB와 연결합니다. VDB 업데이트에는 새로 업데이트된 취약성 및 새로 업데이트된 애플리케이션 탐지기가 포함될 수 있습니다.

취약성 매핑

영향 상관관계 분석를 수행할 수 있도록 취약성 정보와 검색 데이터를 연결하는 것.

취약성 세부사항

취약성 워크플로의 마지막 페이지. 취약성 세부사항은 기술 세부사항 및 알려진 해결책을 포함하여 특정 취약성에 대한 정보를 제공합니다.

침입

네트워크에서 발생하는 보안 위반, 공격 또는 익스플로잇.

침입 감지 및 방지

네트워크 트래픽에서 보안 정책 위반을 모니터링하는 것, 그리고 인라인 구축에서는 악성 트래픽을 차단 또는 변경하는 기능. FireSIGHT 시스템에서는 네트워크 분석 정책로 트래픽을 전처리한 다음 침입 정책을 액세스 제어 규칙 또는 기본 작업과 연결할 때 침입 탐지 및 방지를 수행합니다.

침입 규칙

모니터링되는 네트워크 트래픽에 적용될 때 잠재적인 침입, 보안 정책 위반 및 보안 침해를 식별하는 키워드 및 인수의 집합. 시스템은 패킷을 규칙 조건과 비교합니다. 패킷 데이터가 조건과 일치하면 규칙이 트리거되고 침입 이벤트가 생성됩니다. 침입 규칙에는 삭제 규칙 및 통과 규칙이 포함됩니다.

침입 이벤트

침입 정책 위반을 기록하는 이벤트. 침입 이벤트 데이터에는 날짜, 시간 및 익스플로잇 유형은 물론 공격 및 대상에 대한 기타 컨텍스트 정보도 포함됩니다.

침입 정책

네트워크 트래픽에서 침입 및 보안 정책 위반을 검사하도록 구성할 수 있는 다양한 구성 요소. 네트워크 트래픽이 액세스 제어 규칙의 조건을 충족할 경우 침입 정책으로 트래픽을 검사할 수 있습니다. 또한 침입 정책을 액세스 제어 정책의 기본 작업과 연결할 수 있습니다. 침입 정책의 주 구성 요소는 트래픽을 검사하는 침입 규칙 및 네트워크 분석 정책의 관련 프리프로세서 옵션에 대해 이벤트를 생성하는 전처리기 규칙입니다. 선택적인 FireSIGHT 권장 레이어를 추가하는 것은 물론 민감한 데이터를 검사하거나 특별한 침입 이벤트 처리를 수행하기 위한 고급 설정을 구성할 수도 있습니다. 침입 정책은 항상 변수 집합과 쌍을 이룹니다.

카테고리

애플리케이션 카테고리, 파일 카테고리 또는 URL 카테고리 항목을 참조하십시오.

캐나다

인증 기관을/를 참조하십시오.

캡처된 파일

디바이스가 동적 분석이나 Spero 분석 또는 디바이스에 대한 파일 스토리지용으로 종합 보안 인텔리전스 클라우드에 제출하기 위해 복사하는 네트워크 트래픽에서 탐지된 파일.

컨피그레이션 가져오기 또는 내보내기

어플라이언스에서 생성하고 내보내기 후 다른 어플라이언스에서 가져오기할 수 있는 컨피그레이션 집합(예: 정책 또는 사용자 지정 워크플로).

콘텍스트 메뉴

FireSIGHT 시스템의 다른 기능에 액세스하기 위한 바로가기로 사용할 수 있는, 웹 인터페이스의 여러 페이지에서 사용 가능한 팝업 메뉴. 메뉴의 내용은 보고 있는 페이지, 조사 중인 특정 데이터 및 사용자 역할 등 여러 요소에 따라 달라집니다.

클라우드 서비스

종합 보안 인텔리전스 클라우드을/를 참조하십시오.

클라이언트

한 host에서 실행되며 또 다른 호스트(서버)에 의존하여 작업을 수행하는 application으로, 클라이언트 애플리케이션이라고도 함. 예를 들어 이메일 클라이언트를 사용하면 이메일을 주고받을 수 있습니다. 시스템이 호스트의 사용자가 특정 클라이언트를 사용하여 다른 호스트에 액세스하는 것을 감지할 경우, 클라이언트의 이름과 버전(확인 가능한 경우)을 포함하여 호스트 프로필 및 네트워크 맵에 있는 해당 정보를 보고합니다.

클라이언트 애플리케이션

클라이언트을/를 참조하십시오.

클러스터링

두 개의 피어 디바이스 Series 3 또는 스택 사이에서 네트워크 기능 및 컨피그레이션 데이터의 이중화를 달성할 수 있는 기능. 클러스터링은 정책 적용, 시스템 업데이트 및 등록을 위한 논리적 단일 시스템을 제공합니다. 이중 방어 센터를 구성할 수 있는 고가용성과 비교해 보십시오.

클립보드

나중에 인시던트에 추가할 수 있는 최대 25,000개의 침입 이벤트를 복사할 수 있는 보유 영역.

태그(애플리케이션)

애플리케이션 태그을/를 참조하십시오.

탭 모드

각 패킷의 복사본이 분석되고 네트워크 트래픽 플로우가 디바이스를 통과하는 대신 방해받지 않는 3D9900 및 Series 3 디바이스에서 사용할 수 있는 고급 인라인 집합 옵션. 패킷 자체가 아니라 패킷의 복사본으로 작업하므로, 트래픽을 삭제, 수정 또는 차단하도록 액세스 제어 및 침입 정책을 구성하더라도 디바이스는 패킷 스트림에 영향을 미치지 못합니다.

테이블 보기

열마다 데이터베이스 테이블의 각 필드를 포함하여 이벤트 정보를 표시하는 워크플로 페이지의 유형. 이벤트 분석을 수행할 경우 관심 이벤트에 대한 상세 정보를 표시하는 표 보기로 이동하기 전에 드릴다운 페이지를 사용하여 조사하려는 이벤트만 포함할 수 있습니다. 테이블 보기는 종종 시스템에서 제공하는 워크플로의 마지막에서 두 번째 페이지입니다.

통과 규칙

트리거될 때 침입 이벤트를 생성하지 않으며 규칙을 트리거한 패킷의 세부사항을 로깅하지 않는 침입 규칙. 침입 규칙의 비활성화에 대한 대안으로 통과 규칙을 사용하면 특정 상황에서 특정 기준을 충족하는 패킷으로 인한 이벤트 생성을 막을 수 있습니다. 삭제 규칙과 비교해 보십시오.

통합 파일

FireSIGHT 시스템에서 이벤트 데이터 로깅에 사용하는 이진 파일 형식.

트래픽 채널

Series 3, 어플라이언스 또는 가상 방어 센터의 관리 인터페이스에 구성하여 관리 또는 이벤트 트래픽을 운반하도록 구성할 수 있는 연결. 이벤트 트래픽 채널은 관리되는 디바이스의 네트워크 세그먼트에서 생성된 이벤트 데이터만 전달하며, 관리 트래픽 채널은 내부적으로 생성된 트래픽(즉, 방어 센터와 디바이스 간 관리 트래픽)만 전달합니다. 관리 인터페이스을/를 참조하십시오.

트래픽 프로필

지정된 기간 동안 로깅된 연결 이벤트를 기반으로 하는 네트워크 트래픽의 프로필. 모니터링되는 네트워크 세그먼트의 모든 트래픽을 사용하여 프로필을 생성하거나 더 명확한 대상의 프로필을 생성할 수 있습니다. 그런 다음 상관관계 분석 기능을 사용하여 기존 프로필을 기준으로 새 프로필을 평가함으로써 비정상적인 네트워크 트래픽을 탐지할 수 있습니다.

파생된 핑거프린트

수집된 각 핑거프린트의 신뢰 가치 및 ID 간 확증 핑거프린트 데이터의 양을 사용하여 가장 근접한 ID를 계산하는 공식을 적용함으로써 host에 대해 수동적으로 수집한 모든 핑거프린트로부터 시스템이 생성한 운영 체제 핑거프린트.

파일 규칙

FireSIGHT 시스템이 네트워크 트래픽을 검사하기 위해 사용하는 파일 정책 내 기준 집합. 전송된 파일이 규칙 기준과 일치하면 규칙이 트리거되고 파일 이벤트가 생성됩니다. 파일 규칙 작업은 파일을 차단할지(파일 형식 또는 악성코드 성향 기준) 또는 단순히 파일 통과를 허용하고 전송을 로깅할지 여부를 결정합니다.

파일 규칙 작업

시스템이 파일 규칙의 조건을 충족하는 파일을 처리하는 방식을 결정하는 설정. 특정 파일 형식을 탐지하고 알릴 수 있으며 그러한 파일의 전송을 차단할 수도 있습니다. 그러한 파일 형식의 일부에 대해 악성코드 클라우드 조회를 수행하고 악성코드 성향을 기반으로 그러한 파일의 전송을 차단할 수도 있습니다.

파일 목록

정상 목록 및 사용자 지정 탐지 목록을/를 참조하십시오.

파일 성향

악성코드 성향을/를 참조하십시오.

파일 스토리지

저장된 파일을/를 참조하십시오.

파일 이벤트

관리되는 디바이스에 의해 네트워크 트래픽에서 탐지되는 파일을 나타내는 이벤트.

파일 전파 흔적

네트워크 File trajectory(파일 전파 흔적 분석)을/를 참조하십시오.

파일 정책

시스템에서 파일 제어 및 네트워크 기반 AMP(Advanced Malware Protection)를 수행하기 위해 사용하는 정책. 파일 규칙으로 채워지는 파일 정책은 액세스 제어 정책 내에서 액세스 제어 규칙에 의해 호출됩니다.

파일 제어

액세스 제어에 따라 네트워크를 이동할 수 있는 파일의 유형을 지정 및 로깅할 수 있는 기능

파일 카테고리

그래픽, 실행 파일 또는 아카이브 등 파일 형식에 대한 일반 분류.

파일 캡처

캡처된 파일을/를 참조하십시오.

파일 형식

PDF, EXE, MP3 등 파일의 특정 형식.

패시브 인터페이스

패시브 구축에서 트래픽을 분석하도록 구성된 센싱 인터페이스.

패킷 보기

침입 규칙을 트리거한 패킷 또는 침입 이벤트를 생성한 프리프로세서에 대한 자세한 정보를 제공하는 워크플로 페이지의 유형. 패킷 보기는 침입 이벤트를 기반으로 하는 워크플로의 최종 페이지입니다.

평판(IP 주소)

보안 인텔리전스을/를 참조하십시오.

평판(URL)

URL 평판을/를 참조하십시오.

포트 객체

전송 레이어 프로토콜(예: TCP, UDP 또는 ICMP)을 사용하는 열린 포트를 나타내는 재사용 가능한 객체.

표준 텍스트 규칙

규칙 편집기에서 사용할 수 있는 식별자, 키워드 및 인수를 기반으로 생성된 침입 규칙. 자신의 고유한 사용자 지정 표준 텍스트 규칙을 생성하고 Cisco 제공 표준 텍스트 규칙을 수정할 수 있습니다. 표준 텍스트 규칙의 GID(generator ID)는 1입니다.

프리프로세서

침입 및 익스플로잇을 더 검사하도록 트래픽을 준비하는 시스템의 구성 요소. 프리프로세서는 부적절한 헤더 옵션을 식별하고, IP 데이터그램을 디프래그먼트하고, TCP 스테이트풀 검사 및 스트림 리어셈블리를 제공하고, 체크섬을 검증하여 트래픽을 표준화하며 네트워크 레이어 및 전송 레이어 프로토콜 변칙의 식별을 지원합니다. 프리프로세서는 또한 특정 유형의 패킷 데이터를 시스템이 분석할 수 있는 형식으로 렌더링할 수 있습니다. 이러한 프리프로세서를 데이터 표준화 프리프로세서 또는 애플리케이션 레이어 프로토콜 프리프로세서라고 합니다. 애플리케이션 레이어 프로토콜 인코딩을 정규화함으로써 시스템에서는 데이터가 다르게 표현된 패킷에 동일한 콘텐츠 관련 침입 규칙을 효과적으로 적용하고 의미 있는 결과를 얻을 수 있습니다. 사용자가 구성한 프리프로세서 옵션을 패킷이 트리거할 때마다 프리프로세서는 프리프로세서 이벤트를 생성합니다. 프리프로세서를 구성하려면 특정 전문 지식이 필요합니다. 프리프로세서는 일반적으로 수정이 거의 또는 전혀 필요하지 않으며 모든 구축에 공통된 요소도 아닙니다.

프리프로세서 이벤트

패킷이 지정된 프리프로세서 옵션을 트리거할 때 생성되는 침입 이벤트의 유형. 프리프로세서는 비정상적인 프로토콜 익스플로잇을 탐지하는 데 도움이 될 수 있습니다.

피드

보안 인텔리전스 피드을/를 참조하십시오.

핑거프린트

시스템이 host의 운영 체제를 식별하기 위해 네트워크 트래픽에서 특정 패킷 헤더 값 및 기타 고유한 데이터에 대해 비교하는 설정된 정의. 시스템이 호스트의 운영 체제를 잘못 식별하거나 식별할 수 없는 경우 호스트를 식별하는 사용자 지정 핑거프린트를 생성할 수 있습니다.

하위 서버

동일한 호스트의 다른 서버에 의해 호출된 서버.

하이브리드 인터페이스

시스템이 가상 라우터 및 가상 스위치 간 트래픽을 연결하도록 허용하는 관리되는 디바이스의 논리적 인터페이스.

현재 ID

시스템이 특정 네트워크 자산에 대해 가장 정확할 것으로 판단하여 찾는 운영 체제 또는 서버 ID. 시스템은 통계 계산, 취약성 정보 할당, 공격의 영향 평가, 상관관계 규칙 평가 등 여러 방법으로 이 데이터를 사용합니다.

현재 사용자

시스템이 host와 연결하는 사용자. 사용자가 액세스 제어 대상 사용자이면 시스템은 트래픽에 대해 또는 해당 호스트에서 사용자 제어를 수행할 수 있습니다. 호스트와 연결된 액세스 제어 대상 사용자가 없는 경우, 비 액세스 제어 대상 사용자가 호스트의 현재 사용자가 될 수 있습니다. 그러나 액세스 제어 대상 사용자가 호스트에 로그인한 후에는 또 다른 액세스 제어 대상 사용자의 로그인에 의해서만 현재 사용자가 변경됩니다.

호스트 기록

사용자 활동의 마지막 24시간을 그래프로 표시한 것. 사용자의 사용자 세부사항에서 볼 수 있는 호스트 기록은 사용자가 로그인한 host의 IP 주소와 함께 대략적인 로그인 및 로그아웃 시간을 막대 그래프로 표시합니다.

호스트 보기

검색 이벤트 또는 네트워크 자산을 표시하는 워크플로의 첫 번째 페이지. 호스트 보기에는 현재 보고 있는 이벤트 또는 자산과 관련된 host의 호스트 프로필이 표시됩니다.

호스트 입력

스크립트 또는 명령행 파일을 사용하여 서드파티 소스에서 데이터를 가져와 네트워크 맵의 정보를 확장할 수 있는 기능. 웹 인터페이스는 또한 몇 가지 호스트 입력 기능을 제공합니다. 운영 체제 또는 애플리케이션 프로토콜을 수정하거나 취약성을 식별, 검증, 무효화하고 클라이언트 및 서버 포트를 포함한 다양한 네트워크 맵에서 다양한 항목을 삭제할 수 있습니다.

호스트 입력 이벤트

호스트 입력 기능을 사용할 때 생성되는 일종의 검색 이벤트. 호스트 입력과 패시브 검색 이벤트는 상관관계 규칙 작성 시 구분되지만, 시스템에서는 일반적으로 이 둘을 동일하게 취급합니다.

호스트 중요도

시스템에서 탐지한 특정 host의 비즈니스 중요도를 나타내는 호스트 특성.

호스트 특성

시스템에서 탐지한 host를 네트워크 환경에 중요한 방식으로 분류하여, 이에 대한 정보를 제공하기 위해 사용하는 툴. 시스템에는 두 가지 사전 정의된 호스트 특성인 호스트 중요도 및 메모가 있으며, 각 호스트가 각 활성 규정 준수 화이트리스트를 따르는지를 나타내는 호스트 특성도 있습니다. 자신의 고유한 호스트 특성을 생성할 수도 있습니다.

호스트 프로필

탐지된 특정 host에 대해 수집된 정보. 여기에는 호스트 이름과 운영 체제, 호스트에서 실행 중인 application 및 프로토콜 등 일반 host 정보가 포함됩니다. 호스트 프로필에는 또한 사용자 기록, 호스트 특성, VLAN(Virtual Extended Local Area Network) 정보, 해당 화이트리스트 위반, 탐지된 취약성, IOC(indications of compromise), 해당 호스트의 스캔 결과도 포함됩니다.

호스트 프로필 자격

트래픽 프로필 또는 상관관계 규칙에 적용된 제약 조건. 상관관계 규칙 내 호스트 프로필 자격은 관련된 host가 특정 기준을 충족하는 경우에만 방어 센터가 상관관계 이벤트를 생성하도록 지정합니다. 트래픽 프로필 내 호스트 프로필 자격은 프로필이 작성되는 호스트를 제한합니다.

화이트리스트 위반

호스트가 어떻게 규정 준수 화이트리스트를 준수하지 않을 수 있는지를 자세히 설명하는, 이벤트 뷰어에서 볼 수 있는 정보.

화이트리스트 이벤트

유효한 대상 호스트가 규정 준수 화이트리스트를 준수하지 않게 되었음을 시스템이 탐지할 때 생성되는 이벤트. 화이트리스트 이벤트는 특수한 종류의 상관관계 이벤트입니다.