FireSIGHT 가상 설치 가이드

버전 5.4.1
2015년 1월 22일 금요일

Cisco Systems, Inc.
www.cisco.com
Cisco has more than 200 offices worldwide.
주소, 전화 번호 및 팩스 번호는
Cisco 웹사이트
www.cisco.com/go/offices.

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 공개 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 and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: www.cisco.com/go/trademarks. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)

이 문서에서 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

가상 어플라이언스 소개

Cisco FireSIGHT® System에서는 업계 최고 네트워크 침입 방지 시스템의 보안을 탐지된 애플리케이션, 사용자, URL을 기준으로 네트워크에 대한 액세스를 제어하는 기능과 결합합니다.

Cisco에서는 VMWare vSphere 및 VMware vCloud Director 호스팅 환경을 위해 64비트 가상 방어 센터® 및 가상 디바이스를 패키징합니다. vCenter 또는 vCloud Director를 사용하면 64비트 가상 방어 센터 및 64비트 가상 관리 디바이스를 ESXi 호스트에 구축할 수 있습니다. 가상 어플라이언스는 e1000(1Gbit/s) 인터페이스를 사용하며, 사용자는 기본 인터페이스를 vmxnet3(10Gbit/s) 인터페이스로 교체할 수 있습니다. 또한 VMware Tools를 사용하여 가상 어플라이언스의 성능 및 관리를 향상할 수 있습니다.

방어 센터에서는 시스템을 위한 중앙 집중식 관리 콘솔 및 데이터베이스 저장소를 제공합니다. 가상 디바이스는 수동 또는 인라인 구축에서 가상 또는 물리적 네트워크의 트래픽을 검사할 수 있습니다.

- 수동 구축 가상 디바이스는 단순히 네트워크에서 이동하는 트래픽을 모니터링합니다.
- 수동 센싱 인터페이스는 모든 트래픽을 조건 없이 수신하며 이러한 인터페이스에서 수신된 트래픽은 재전송되지 않습니다.
- 인라인 방식으로 구축된 가상 디바이스를 사용할 경우 네트워크 호스트의 가용성, 무결성 또는 기밀성에 영향을 미칠 수 있는 공격으로부터 네트워크를 보호할 수 있습니다. 인라인 디바이스는 간단한 침입 방지 시스템으로 구축할 수 있습니다. 또한 인라인 디바이스가 액세스 제어를 수행하고 다른 방식으로 네트워크 트래픽을 관리하도록 구성할 수 있습니다.
- 인라인 인터페이스는 모든 트래픽을 조건 없이 수신하며 이러한 인터페이스에 수신된 트래픽은 구축의 일부 컨피그레이션에 의해 명시적으로 삭제되지 않는 이상 재전송됩니다.

가상 방어 센터는 물리적 디바이스, Cisco NGIPS for Blue Coat X-Series, Cisco ASA with FirePOWER Services(ASA FirePOWER)를 관리할 수 있으며 물리적 방어 센터는 가상 디바이스를 관리할 수 있습니다. 그러나 가상 어플라이언스는 시스템의 하드웨어 기반 기능을 지원하지 않습니다. 가상 방어 센터는 고가용성을 지원하지 않으며 가상 디바이스는 클러스터링, 스태킹, 스위칭, 라우팅 등을 지원하지 않습니다. 물리적 FireSIGHT System 어플라이언스에 대한 자세한 내용은 *FireSIGHT System 설치 가이드*를 참조하십시오.

이 설치 가이드에서는 가상 FireSIGHT System 어플라이언스(디바이스 및 방어 센터)의 구축, 설치, 설정에 대한 정보를 제공합니다. 또한 사용자가 vSphere Client, VMware vCloud Director 웹 포털 및 VMware Tools(선택 사항)를 비롯한 VMWare 제품에 대한 기능과 명명 규칙을 잘 알고 있다고 가정합니다.

아래 항목에서는 FireSIGHT System 가상 어플라이언스에 대해 소개합니다.

FireSIGHT System 가상 어플라이언스

FireSIGHT System *가상 어플라이언스*는 트래픽을 감지하는 관리 *가상 디바이스* 또는 관리하는 *가상 방어 센터*입니다. 자세한 내용은 다음 섹션을 참조하십시오.

가상 방어 센터

방어 센터에서는 FireSIGHT System 구축을 위해 중앙 집중식 관리 지점 및 이벤트 데이터베이스를 제공합니다. 가상 방어 센터는 감염지표를 이용하여 침입, 파일, 악성코드, 검색, 연결, 성능 데이터를 집계하고 상관관계를 분석하며 이벤트가 특정 호스트와 태깅 호스트에 미치는 영향을 평가합니다. 이 기능을 활용하면 보유 디바이스에서 다른 디바이스와 관련하여 보고하는 정보를 모니터링하고 네트워크에서 발생하는 전반적인 활동을 평가 및 제어할 수 있습니다.

가상 방어 센터의 핵심 기능은 다음과 같습니다.

- 디바이스, 라이센스, 정책 관리
- 표, 그래프, 차트로 표시되는 이벤트 및 상황별 정보
- 상태 및 성능 모니터링
- 외부 알림 및 경고
- 실시간 위협 대응을 지원하는 상관관계 분석, 보안 침해 지표 및 치료 기능
- 맞춤형 보고 및 템플릿 기반 보고

가상 관리되는 디바이스

조직 내 네트워크 세그먼트에 구축된 가상 디바이스는 분석용 트래픽을 모니터링합니다. 수동 구축된 가상 디바이스를 이용하면 네트워크 트래픽에 대한 통찰력을 얻을 수 있습니다. 인라인 형태로 구축할 경우 가상 디바이스를 사용하여 여러 가지 기준을 기반으로 트래픽 플로우에 영향을 미칠 수 있습니다. 디바이스는 모델 및 라이센스에 따라 다음을 수행합니다.

- 조직의 호스트, 운영 체제, 애플리케이션, 사용자, 파일, 네트워크, 취약점에 대한 세부 정보 수집

- 다양한 네트워크 기반의 기준은 물론 애플리케이션, 사용자, URL, IP 주소 평판, 침입이나 악성코드 검사의 결과와 같은 기타 기준에 따라 네트워크 트래픽을 차단 또는 허용

가상 디바이스에는 웹 인터페이스가 **없습니다**. 콘솔과 명령어 라인을 통해 이를 구성하고 방어 센터로 관리해야 합니다.

가상 어플라이언스 기능 이해

가상 어플라이언스에는 물리적 어플라이언스의 여러 기능이 있습니다.

- 가상 방어 센터의 경우 가상 방어 센터의 고가용성 쌍을 생성할 수 없다는 점을 제외하고 물리적 방어 센터와 기능이 동일합니다. FireSIGHT 라이센스 하나로 가상 방어 센터에서 50,000개의 호스트 및 사용자를 모니터링할 수 있습니다.
- 가상 디바이스에는 물리적 디바이스의 트래픽 및 차단 분석 기능이 있습니다. 그러나 스위칭, 라우팅, VPN, 기타 하드웨어 기반, 이중화 및 리소스 공유 기능을 수행할 수 없습니다.

가상 방어 센터 기능 이해

표 1-1 가상 방어 센터에 대해 지원되는 기능, 페이지 1-3에는 가상 Defense Center로 구성된 시스템의 주요 기능 및 해당 기능의 지원 여부가 표시되어 있습니다. 여기서는 이러한 기능을 지원하는 관리 디바이스가 있고 올바른 라이센스가 설치 및 적용되어 있다고 가정합니다.

가상 어플라이언스에서 지원되는 기능과 라이센스의 간단한 요약을 보려면 FireSIGHT System 구성 요소, 페이지 1-7 및 가상 어플라이언스 라이센싱, 페이지 1-11을 참조하십시오.

가상 방어 센터는 Series 2, Series 3, ASA FirePOWER, X-Series 디바이스를 관리할 수 있다는 점을 기억하십시오. 마찬가지로, Series 2 및 Series 3 방어 센터는 가상 디바이스를 관리할 수 있습니다. 디바이스 기반 기능(예: 스태킹, 스위칭, 라우팅)에 대한 방어 센터 열은 가상 방어 센터에서 디바이스를 관리 및 구성하여 이러한 기능을 수행하는지 여부를 나타냅니다. 예를 들어, 가상 디바이스에서 VPN을 구성할 수 없는 경우에도 가상 방어 센터를 사용하여 VPN 구축에서 Series 3 디바이스를 관리할 수 있습니다.

표 1-1 가상 방어 센터에 대해 지원되는 기능

기능	가상 방어 센터
관리되는 디바이스가 보고하는 검색 데이터(호스트, 애플리케이션, 사용자) 수집 및 조직의 네트워크 맵 구축	예
네트워크 트래픽의 위치 데이터 보기	예
침입 탐지 및 방지(IPS) 구축 관리	예
보안 인텔리전스 필터링을 수행하는 디바이스 관리	예
위치 기반 필터링을 포함하여 간단한 네트워크 기반 제어를 수행하는 디바이스 관리	예
애플리케이션 제어를 수행하는 디바이스 관리	예
사용자 제어를 수행하는 디바이스 관리	예
리터럴 URL을 통해 네트워크 트래픽을 필터링하는 디바이스 관리	예
범주 및 평판별 URL 필터링을 수행하는 디바이스 관리	예
파일 유형별로 간단한 파일 제어를 수행하는 디바이스 관리	예

표 1-1 가상 방어 센터에 대해 지원되는 기능 (계속)

기능	가상 방어 센터
네트워크 기반 AMP(advanced malware protection)를 수행하는 디바이스 관리	예
FireAMP 구축에서 엔드포인트 기반 악성코드(FireAMP) 이벤트 수신	예
디바이스 기반 하드웨어 기반 기능 관리: • 빠른 경로(Fast-Path) 규칙 • 엄격한 TCP 구현 • 구성 가능한 바이패스 인터페이스 • 탭 모드 • 스위칭 및 라우팅 • NAT 정책 • VPN	예
디바이스 기반 이중화 및 리소스 공유 관리: • 디바이스 스택 • 디바이스 클러스터 • Cisco NGIPS for Blue Coat X-Series VAP 그룹 • 클러스터링 스택	예
트래픽 채널을 이용하여 내부 및 이벤트 트래픽 구분 및 관리	예
복수 관리 인터페이스를 사용하여 서로 다른 네트워크에서 트래픽 격리 및 관리	예
고가용성 구현	아니요
악성코드 스토리지 팩 설치	아니요
eStreamer, 호스트 입력 또는 데이터베이스 클라이언트에 연결	예

관리되는 가상 디바이스 기능 이해

표 1-2 관리되는 가상 디바이스에서 지원되는 기능, 페이지 1-5에는 시스템의 주요 기능과 관리되는 가상 디바이스에서 해당 기능을 지원하는지 여부가 표시되어 있습니다. 여기서는 방어 센터에서 올바른 라이센스를 설치 및 적용했다고 가정합니다.

또한 시스템의 버전 5.4.1을 실행하는 방어 센터 모델을 사용하여 버전 5.4.1 가상 디바이스를 관리할 수 있는 경우에도 몇 가지 시스템 기능은 방어 센터 모델에 따라 제한됩니다. 예를 들어 관리되는 가상 디바이스가 보안 인텔리전스 필터링을 지원하더라도, Series 2 DC500에서는 보안 인텔리전스 필터링을 수행하는 관리되는 가상 디바이스를 관리할 수 없습니다. 자세한 내용은 가상 방어 센터 기능 이해, 페이지 1-3을(를) 참고하십시오.

표 1-2 관리되는 가상 디바이스에서 지원되는 기능

기능	관리되는 가상 디바이스
관리되는 디바이스가 보고하는 검색 데이터(호스트, 애플리케이션, 사용자) 수집 및 조직의 네트워크 맵 구축	예
네트워크 트래픽의 위치 데이터 보기	예
네트워크 검색: 호스트, 애플리케이션, 사용자	예
침입 탐지 및 방지(IPS)	예
보안 인텔리전스 필터링	예
액세스 제어: 기본적인 네트워크 제어	예
액세스 제어: 위치 기반 필터링	예
액세스 제어: 애플리케이션 제어	예
액세스 제어: 사용자 제어	예
액세스 제어: 리터럴 URL	예
액세스 제어: 범주 및 평판별 URL 필터링	예
파일 제어: 파일 유형별	예
네트워크 기반 AMP(Advanced Malware Protection)	예
자동 애플리케이션 바이패스	예
빠른 경로(Fast-Path) 규칙	아니요
엄격한 TCP 적용	아니요
구성 가능한 바이패스 인터페이스	아니요
탭 모드	아니요
스위칭 및 라우팅	아니요
NAT 정책	아니요
VPN	아니요
디바이스 스태킹	아니요
디바이스 클러스터링	아니요
클러스터링 스택	아니요
트래픽 채널	아니요
복수 관리 인터페이스	아니요
악성코드 스토리지 팩	아니요
FireSIGHT System별 대화형 CLI	예
eStreamer 클라이언트에 연결	아니요

운영 환경 전제 조건

다음과 같은 호스팅 환경에서 64비트 가상 어플라이언스를 호스팅할 수 있습니다.

- VMWare ESXi 5.5(vSphere 5.5)
- VMWare ESXi 5.1(vSphere 5.1)
- VMware vCloud Director 5.1

또한 모든 지원되는 ESXi 버전에서 VMWare Tools를 활성화할 수 있습니다. VMWare Tools의 전체 기능에 대한 자세한 내용은 VMWare 웹 사이트(http://www.vmware.com/)를 참조하십시오. 호스팅 환경을 생성하는 방법에 대한 도움말을 보려면 VMware vCloud Director 및 VMware vCenter를 포함하여 VMWare ESXi 설명서를 참조하십시오.

가상 어플라이언스는 OVF(Open Virtual Format) 패키징을 사용합니다. VMWare Workstation, Player, Server 및 Fusion은 OVF 패키징을 인식하지 않으며 지원되지 않습니다. 또한 가상 어플라이언스는 가상 하드웨어 버전 7을 사용하여 가상 머신으로 패키지화되어 있습니다.

ESXi 호스트로 사용할 컴퓨터는 다음과 같은 요구 사항을 충족해야 합니다.

- Intel® VT(Virtualization Technology) 또는 AMD-V™(AMD Virtualization™) 기술이든, 가상화 지원을 제공하는 64비트 CPU가 있어야 합니다.
- BIOS 설정에서 가상화를 활성화해야 합니다.
- 가상 디바이스를 호스팅하려면 컴퓨터에 Intel e1000 드라이버(예: PRO 1000MT 이중 포트 서버 어댑터 또는 PRO 1000GT 데스크톱 어댑터)와 호환되는 네트워크 인터페이스가 있어야 합니다.

자세한 내용은 VMWare 웹 사이트(http://www.vmware.com/resources/guides.html)를 참조하십시오.

각각의 가상 어플라이언스를 만들 경우 ESXi 호스트에 특정 양의 메모리, CPU, 하드 디스크 공간이 있어야 합니다. 기본 설정은 시스템 소프트웨어를 실행하는 데 필요한 최소 설정이므로 기본 설정을 줄이지 **마십시오**. 그러나 성능을 개선하려는 경우 가용 리소스에 따라 가상 어플라이언스의 메모리와 CPU 수를 늘릴 수 있습니다. 다음 표에는 기본 어플라이언스 설정이 나와 있습니다.

표 1-3 기본 가상 어플라이언스 설정

설정	기본	설정의 조정 가능 여부
메모리	4GB	조정 가능하며, 가상 디바이스의 경우 **반드시** 다음을 할당해야 합니다. • 최소 4GB • 범주 및 평판 기반 URL 필터링을 사용하기 위한 5GB • 대용량 동적 피드를 사용하여 보안 인텔리전스 필터링을 수행하기 위한 6GB • URL 필터링 및 보안 인텔리전스를 수행하기 위한 7GB
가상 CPU	4	조정 가능, 최대 8개
하드 디스크 프로비저닝 크기	40GB(디바이스) 250GB(방어 센터)	아니요

가상 어플라이언스 성능

가상 어플라이언스의 처리량과 처리 용량을 정확하게 예측하기란 불가능합니다. 다음을 포함한 여러 요소가 성능에 큰 영향을 미칩니다.

- ESXi 호스트의 메모리 양과 CPU 용량
- ESXi 호스트에서 실행되는 총 가상 머신의 수
- 센싱 인터페이스 수, 네트워크 성능, 인터페이스 속도
- 각 가상 어플라이언스에 할당된 리소스의 양
- 호스트를 공유하는 다른 가상 어플라이언스의 활동 레벨
- 가상 기기에 적용된 정책의 복잡성

정보 VMWare에서는 다양한 성능 측정 및 리소스 할당 툴을 제공합니다. 가상 어플라이언스를 실행하는 동시에 ESXi 호스트에서 이러한 툴을 사용하여 트래픽을 모니터링하고 처리량을 확인하십시오. 처리량이 만족스럽지 않을 경우 ESXi 호스트를 공유하는 가상 어플라이언스에 할당된 리소스를 조정하십시오.

VMWare Tools를 활성화하여 가상 어플라이언스의 성능 및 관리를 개선할 수 있습니다. 또는 툴(예: `esxtop` 또는 VMWare/서드파티 애드온)을 호스트나 ESXi 호스트의 가상화 관리 계층(게스트 레이어 아님)에 설치하여 가상 성능을 검사할 수 있습니다. VMware Tools를 활성화하려면 *FireSIGHT System 사용 설명서*를 참조하십시오.

FireSIGHT System 구성 요소

다음 섹션에서는 가상 방어 센터 및 가상 기기가 조직의 보안, 허용되는 사용 정책, 트래픽 관리 전략에 기여하는 몇 가지 주요 기능에 대해 설명합니다. Series 2 및 Series 3 어플라이언스에서 지원되는 추가 기능은 *FireSIGHT System 설치 가이드* 및 *FireSIGHT System 사용 설명서*를 참조하십시오.

정보 다수의 가상 어플라이언스 기능은 라이센스 및 사용자 역할에 따라 달라집니다. FireSIGHT System 설명서에는 필요에 따라 각 기능 및 작업의 요구 사항이 요약되어 있습니다.

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

- FireSIGHT, 페이지 1-8
- 액세스 제어, 페이지 1-8
- 침입 탐지 및 방지, 페이지 1-8
- 파일 추적, 제어 및 악성코드 차단, 페이지 1-9
- API(Application Programming Interface), 페이지 1-10

FireSIGHT

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

방어 센터의 웹 인터페이스를 통해 FireSIGHT에서 수집한 데이터를 보고 분석할 수 있습니다. 또한 액세스를 제어하고 침입 규칙 상태를 수정하는 데에도 이 데이터를 활용할 수 있습니다. 뿐만 아니라, 호스트에 대한 상관관계 이벤트 데이터를 기준으로 네트워크의 호스트에 대한 감염지표를 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*은 시스템이 네트워크의 트래픽을 처리하는 방식을 결정합니다. *기본 작업*이라고 하는 다음 방법 중 하나를 사용하여 트래픽을 처리하려면 *액세스 제어 규칙*이 포함되지 않은 정책을 사용할 수 있습니다.

- 네트워크에 진입하는 모든 트래픽 차단
- 추가 검사 없이 네트워크에 진입하려는 모든 트래픽 신뢰
- 네트워크에 진입하려는 모든 트래픽을 허용하고, 네트워크 검색 정책만 사용하여 트래픽 검사
- 네트워크에 진입하려는 모든 트래픽을 허용하고, 침입 및 네트워크 검색 정책을 사용하여 트래픽 검사

액세스 제어 정책에 액세스 제어 규칙을 포함하면 간단한 IP 주소 매칭부터 다른 사용자, 애플리케이션, 포트, URL이 관련된 복잡한 시나리오까지 대상 디바이스에서 트래픽을 처리하는 방식을 추가 정의할 수 있습니다. 각 규칙에 대해 *작업*, 즉 침입 또는 파일 정책을 이용하여 일치하는 트래픽을 신뢰, 모니터링, 차단 또는 검사할지를 지정합니다.

각 액세스 제어 정책의 경우 시스템이 HTTP 요청을 차단할 때 사용자에게 표시되는 사용자 정의 HTML 페이지를 만들 수 있습니다. 또는 사용자에게 경고하는 페이지를 표시할 수도 있지만 버튼을 클릭하면 원래 요청된 사이트를 계속 표시할 수도 있습니다.

보안 인텔리전스 기능은 액세스 제어에 포함되며, 액세스 제어 규칙으로 트래픽을 분석하기 전에 특정 IP 주소를 블랙리스트(트래픽의 수신 및 송신 거부)에 추가합니다. 또한 시스템이 위치를 지원할 경우 탐지된 소스, 대상 국가 및 대륙을 기준으로 트래픽을 필터링할 수 있습니다.

액세스 제어에는 침입 탐지 및 방지, 파일 제어, AMP가 포함됩니다. 자세한 내용은 다음 섹션을 참조하십시오.

침입 탐지 및 방지

침입 탐지 및 방지에서는 네트워크 트래픽을 모니터링하여 보안 위반을 찾을 수 있으며 인라인 구축의 경우 악성 트래픽을 차단 또는 변경할 수 있습니다.

침입 방지는 액세스 제어에 통합되므로 침입 정책을 특정 액세스 제어 규칙과 연결할 수 있습니다. 네트워크 트래픽이 규칙의 조건을 충족할 경우 침입 정책으로 일치하는 트래픽을 분석할 수 있습니다. 또한 침입 정책을 액세스 제어 정책의 기본 작업과 연결할 수 있습니다.

침입 정책에는 다음과 같이 다양한 구성 요소가 포함되어 있습니다.

- 프로토콜 헤더 값, 페이로드 콘텐츠, 특정 패킷 크기 특성을 검사하는 규칙
- FireSIGHT 권장 사항을 기반으로 하는 규칙 상태 컨피그레이션

- 고급 설정(예: 프리프로세서), 기타 탐지 및 성능 기능
- 관련 프리프로세서 및 프리프로세서 옵션을 위한 이벤트를 생성할 수 있는 프리프로세서 규칙

파일 추적, 제어 및 악성코드 차단

FireSIGHT System의 파일 제어, 네트워크 파일 전파 흔적 분석(File trajectory) 및 AMP 구성 요소는 악성코드의 효과를 식별하고 완화할 수 있도록 네트워크 트래픽의 파일(악성코드 파일 포함) 전송을 탐지, 추적, 캡처, 분석하고, 선택적으로 차단할 수 있습니다.

파일 제어

관리되는 디바이스에서는 *파일 제어*를 통해 특정 애플리케이션 프로토콜에서 특정 유형의 파일 업로드(보내기) 또는 다운로드(받기)를 탐지하고 사용자가 이러한 작업을 수행하지 못하도록 할 수 있습니다. 파일 제어를 전반적 액세스 제어 컨피그레이션의 일부로 구성하고, 액세스 제어 규칙과 관련된 파일 정책이 규칙 조건을 충족하는 네트워크 트래픽을 검사합니다.

네트워크 기반 AMP(Advanced Malware Protection)

네트워크 기반 *AMP(Advanced Malware Protection)*를 사용하면 네트워크 트래픽에서 몇 가지 파일 유형의 악성코드를 검사할 수 있습니다. 가상 디바이스는 추가 분석을 위해 탐지된 파일을 하드 드라이브에 저장할 수 있습니다.

탐지된 파일의 저장 여부와 상관없이, 파일을 Collective Security Intelligence 클라우드에 제출하고 파일의 SHA-256 해시 값을 이용하여 알려진 속성을 간단히 조회할 수 있습니다. 또한 위협 점수를 생성하는 *동적 분석*을 위해 파일을 제출할 수도 있습니다. 이러한 상황별 정보를 사용하여 특정 파일을 차단하거나 허용하도록 시스템을 구성할 수 있습니다.

악성코드 차단을 전반적 액세스 제어 컨피그레이션의 일부로 구성하며, 액세스 제어 규칙과 관련된 파일 정책은 규칙 조건을 충족하는 네트워크 트래픽을 검사합니다.

FireAMP 통합

FireAMP 는 Cisco의 엔터프라이즈급 지능형 악성코드 분석 및 차단 솔루션으로 지능형 악성코드 보안 침해, APT(advanced persistent threats), 표적 공격을 발견 및 파악하고 차단합니다.

조직에 FireAMP 서브스크립션이 있는 경우 개별 사용자는 컴퓨터와 모바일 디바이스(*엔드포인트*라고도 함)에 *FireAMP Connector*를 설치할 수 있습니다. 이러한 가벼운 에이전트는 Collective Security Intelligence 클라우드와 통신하며, Cisco 클라우드는 방어 센터와 통신합니다.

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

*FireAMP 포털*을 사용하여 FireAMP 구축을 구성합니다. 이 포털을 이용하면 악성코드를 신속하게 식별하고 격리할 수 있습니다. 보안 침해가 발생한 경우 이를 식별하고, 전파 흔적을 추적하고, 파급 효과를 파악하고, 성공적으로 복구하는 방법을 알아볼 수 있습니다. FireAMP를 사용하면 맞춤형 보호를 생성하고, 그룹 정책을 기반으로 특정 애플리케이션의 실행을 차단하며, 맞춤형 화이트리스트를 생성할 수도 있습니다.

자세한 내용은 http://amp.sourcefire.com/을 참조하십시오.

네트워크 파일 전파 흔적 분석

네트워크 파일 전파 흔적 분석 기능은 네트워크에서 파일의 전송 경로를 추적합니다. 시스템은 SHA-256 해시 값을 사용하여 파일을 추적하므로, 파일을 추적하기 위해 시스템은 다음을 수행해야 합니다.

- 파일의 SHA-256 해시 값을 계산하고 해당 값을 사용하여 악성코드 클라우드 조회 수행
- 방어 센터를 조직의 FireAMP 서브스크립션과 통합하여 해당 파일에 대한 엔드포인트 기반 위협 및 격리 데이터 수신

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

API(Application Programming Interface)

API(Application Programming Interface)를 사용하여 시스템과 상호 작용하는 몇 가지 방법이 있습니다. 자세한 내용을 보려면 지원 사이트에서 추가 문서를 다운로드할 수 있습니다.

eStreamer

Event Streamer(eStreamer)를 사용하면 Cisco 어플라이언스에서 맞춤 개발된 클라이언트 애플리케이션으로 여러 종류의 이벤트 데이터를 스트리밍할 수 있습니다. 클라이언트 애플리케이션을 생성한 다음 eStreamer 서버(방어 센터 또는 관리되는 디바이스)에 연결한 후 eStreamer 서비스를 시작하고 데이터 교환을 시작합니다.

eStreamer 통합에는 맞춤형 프로그래밍이 필요하지만, 어플라이언스에서 특정 데이터를 요청할 수 있습니다. 예를 들어, 네트워크 관리 애플리케이션 중 하나에서 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 서드파티 클라이언트를 사용하여 방어 센터에서 여러 데이터베이스 테이블을 쿼리할 수 있습니다.

Crystal Reports, Actuate BIRT 또는 JasperSoft iReport와 같은 업계 표준 보고 툴을 사용하여 쿼리를 설계 및 제출할 수 있습니다. 또는 맞춤형 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 커맨드 라인 파일을 사용하여 서드파티 소스에서 데이터를 가져오는 방법으로 네트워크 맵의 정보를 보강할 수 있습니다.

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

치료

시스템에는 네트워크 조건이 관련 상관관계 정책 또는 규정준수 화이트리스트를 위반할 경우 방어 센터가 자동으로 시작되는 치료를 생성할 수 있도록 지원하는 API가 포함되어 있습니다. 이 프로그램은 문제를 즉시 해결할 수 없을 때 공격을 자동으로 완화할 뿐만 아니라 시스템이 조직의 보안 정책을 준수함을 보장할 수 있습니다. 사용자가 생성하는 치료 외에도, Defense Center에는 여러 개의 사전 정의된 치료 모듈이 포함됩니다.

복수 관리 인터페이스

Series 3어플라이언스 및 가상 방어 센터에서 *복수 관리 인터페이스*를 사용하면 트래픽을 두 개의 트래픽 채널로 구분하여 성능을 향상할 수 있습니다. 즉, *관리 트래픽 채널*에서는 디바이스 간 통신이 이루어지며 *이벤트 트래픽 채널*에서는 웹 액세스와 같은 외부 트래픽이 전송됩니다. 두 트래픽 채널 모두 동일한 관리 인터페이스를 이용할 수도 있고, 각각 하나의 트래픽 채널을 전달하는 두 개의 관리 인터페이스로 분할할 수 있습니다.

방어 센터의 특정 관리 인터페이스에서 다른 네트워크로 경로를 만들 수 있으므로 방어 센터를 통해 한 네트워크에 있는 디바이스의 트래픽을 또 다른 네트워크에 있는 디바이스의 트래픽과 별도로 관리할 수 있습니다.

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

- 기본(`eth0`) 관리 인터페이스에서만 DHCP를 구성할 수 있습니다. 추가(`eth1` 등) 인터페이스에는 고유한 고정 IP 주소 및 호스트 이름이 필요합니다.
- 기본이 아닌 관리 인터페이스를 사용하여 방어 센터 및 관리되는 디바이스를 연결할 경우, 해당 어플라이언스가 NAT 디바이스로 분리되어 있으면 두 트래픽 채널을 모두 구성하여 동일한 관리 인터페이스를 사용해야 합니다.
- 70xx 제품군에서는 트래픽을 두 개의 채널로 구분하고 해당 채널이 트래픽을 가상 방어 센터에 있는 하나 이상의 관리 인터페이스로 전송하도록 구성할 수 있습니다. 그러나 70xx 제품군에는 하나의 관리 인터페이스만 포함되어 있으므로 디바이스에서는 한 관리 인터페이스의 방어 센터에서 전송된 트래픽만 수신합니다.

어플라이언스를 설치한 후 웹 브라우저를 사용하여 복수 관리 인터페이스를 구성합니다. 가상 방어 센터에 관리 인터페이스를 추가하려면 인터페이스 추가 및 구성, 페이지 4-10를 참조하십시오. 자세한 내용은 *FireSIGHT System 사용 설명서*에서 복수 관리 인터페이스를 참조하십시오.

가상 어플라이언스 라이센싱

다양한 기능의 라이센스를 취득하여 조직에 최적의 FireSIGHT System 구축을 조성할 수 있습니다. 방어 센터를 사용하여 자체 라이센스 및 여기에서 관리하는 디바이스의 라이센스를 제어해야 합니다.

조직에서 구매한 라이센스는 방어 센터의 초기 설정 과정에서 추가하는 것이 좋습니다. 그렇지 않을 경우 초기 설정 중 등록하는 디바이스는 방어 센터에 라이센스가 없는 상태로 추가됩니다. 초기 설정 프로세스를 마친 다음 각 디바이스에서 라이센스를 개별적으로 활성화해야 합니다. 자세한 내용은 가상 어플라이언스 설정, 페이지 5-1을(를) 참고하십시오.

FireSIGHT 라이센스는 구매한 각 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 수행하도록 허용할 수 있는 사용자 수가 결정됩니다. 가상 방어 센터의 경우 개별 호스트 및 사용자에 대한 이러한 제한값은 50,000개입니다.

방어 센터에서 이전에 버전 4.10.x를 실행 중이었다면 FireSIGHT 라이센스 대신 레거시 RNA 호스트 및 RUA 사용자 라이센스를 사용할 수 있습니다. 자세한 내용은 라이센스 설정, 페이지 5-10을(를) 참고하십시오.

추가 모델별 라이센스를 사용하면 관리되는 디바이스로 다음과 같이 다양한 기능을 수행할 수 있습니다.

보호

보호 라이센스를 사용하면 침입 탐지 및 방지, 파일 제어, 보안 인텔리전스 필터링을 수행할 수 있습니다.

제어

제어 라이센스를 사용하면 가상 디바이스에서 사용자 및 애플리케이션 제어를 수행할 수 있습니다. 가상 디바이스는 제어 라이센스(예: 스위칭 또는 라우팅)로 Series 2 및 Series 3 디바이스에 부여된 하드웨어 기반 기능을 지원하지 않지만, 가상 방어 센터는 물리적 디바이스에서 이러한 기능을 관리할 수 있습니다. 제어 라이센스에는 보호 라이센스가 필요합니다.

URL 필터링

URL 필터링을 사용하면 가상 디바이스에서는 정기적으로 업데이트된 클라우드 기반 범주 및 평판 데이터를 사용하여 모니터링된 호스트에서 요청한 URL을 기준으로 네트워크를 지나는 트래픽이 무엇인지 확인할 수 있습니다. URL 필터링 라이센스에는 보호 라이센스가 필요합니다.

악성코드

악성코드 라이센스를 사용하면 가상 디바이스가 네트워크에서 전송된 파일에서 악성코드를 탐지 및 차단하는 네트워크 기반 AMP(advanced malware protection)를 수행할 수 있습니다. 또한 네트워크에서 전송된 파일을 추적하는 전파 흔적 분석을 볼 수 있습니다. 악성코드 라이센스에는 보호 라이센스가 필요합니다.

VPN

VPN 라이센스를 사용하면 가상 방어 센터를 활용하여 Series 3 디바이스의 가상 라우터 사이 또는 Series 3 디바이스에서 원격 디바이스 또는 다른 서드파티 VPN 엔드포인트로 보안 VPN 터널을 구축할 수 있습니다. VPN 라이센스에는 보호 및 제어 라이센스가 필요합니다.

아키텍처 및 리소스 제한으로 인해, 모든 라이센스를 모든 관리되는 디바이스에 적용할 수는 없습니다. 일반적으로 디바이스에서 지원하지 않는 기능에 대해서는 라이센스를 취득할 수 없습니다. 가상 어플라이언스 기능 이해, 페이지 1-3를 참조하십시오.

다음 표에는 방어 센터에 추가하고 각 디바이스 모델에 적용할 수 있는 라이센스가 요약되어 있습니다. 방어 센터 행(FireSIGHT를 제외한 모든 라이센스)은 해당 방어 센터에서 이러한 라이센스를 사용하여 디바이스를 관리할 수 있는지 여부를 나타냅니다. 예를 들어, Series 2 DC1000을 사용하면 Series 3 디바이스를 이용한 VPN 구축이 가능하지만, DC500을 사용할 경우 관리하는 디바이스와 상관없이 범주 및 평판 기반 URL 필터링을 수행할 수 없습니다. 해당 없음 표시는 관리되는 디바이스와 관련 없는 방어 센터 기반 라이센스를 나타냅니다.

표 1-4 모델별 지원되는 라이센스

모델	FireSIGHT	보호	제어	URL 필터링	악성코드	VPN
Series 2 디바이스: • 3D500, 3D1000, 3D2000 • 3D2100, 3D2500, 3D3500, 3D4500 • 3D6500 • 3D9900	해당 없음	자동, 보안 인텔리전스 없음	아니요	아니요	아니요	아니요
Series 3 디바이스: • 7000 Series • 8000 Series	해당 없음	예	예	예	예	예
가상 디바이스	해당 없음	예	예. 단, 하드웨어 기능에는 지원되지 않음	예	예	아니요
Cisco ASA with FirePOWER Services	해당 없음	예	예. 단, 하드웨어 기능에는 지원되지 않음	예	예	아니요
Cisco NGIPS for Blue Coat X-Series	해당 없음	예	예. 단, 하드웨어 기능에는 지원되지 않음	예	예	아니요
Series 2 방어 센터: • DC500	예	예. 단, 보안 인텔리전스 없음	예. 단, 사용자 제어 없음	아니요	아니요	예
Series 2 방어 센터: • DC1000, DC3000	예	예	예	예	예	예
Series 3 방어 센터: • DC750, DC1500, DC3500, DC2000, DC4000	예	예	예	예	예	예
가상 방어 센터	예	예	예	예	예	예

라이센싱에 대한 자세한 내용은 *FireSIGHT System 사용 설명서*의 FireSIGHT System 라이센싱 장을 참조하십시오.

보안, 인터넷 액세스 및 통신 포트

방어 센터를 보호하려면 보호된 내부 네트워크에 이를 설치해야 합니다. 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 동일한 네트워크에 상주하는 경우 디바이스의 관리 인터페이스를 방어 센터와 동일한 보호된 내부 네트워크에 연결할 수 있습니다. 이렇게 하면 방어 센터에서 디바이스를 안전하게 제어할 수 있습니다. 또한 복수 관리 인터페이스를 구성하면 방어 센터에서 다른 네트워크에 있는 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 어플라이언스 간 통신이 중단, 차단, 변경되지 않도록 조치를 취해야 합니다.

또한 FireSIGHT System의 특정 기능에는 인터넷 연결이 필요합니다. 기본적으로 모든 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.

정보 Cisco NGIPS for Blue Coat X-Series 및 Cisco ASA with FirePOWER Services를 제외하고 FireSIGHT System 어플라이언스에서는 프록시 서버 사용을 지원합니다. 자세한 내용은 *FireSIGHT System 사용 설명서*를 참조하십시오.

자세한 내용은 다음 링크를 참고하십시오.

- 인터넷 액세스 요구 사항, 페이지 1-14
- 통신 포트 요구 사항, 페이지 1-15

인터넷 액세스 요구 사항

가상 방어 센터는 기본적으로 열려 있는 포트 443/tcp(HTTPS) 및 80/tcp(HTTP)에서 인터넷에 직접 연결하도록 구성되었습니다. 가상 디바이스에서 포트 443은 디바이스가 동적 분석을 위한 파일을 제출할 수 있도록 악성코드 라이센스를 활성화하는 경우에만 열립니다. 자세한 내용은 통신 포트 요구 사항, 페이지 1-15을(를) 참고하십시오. FireSIGHT 가상 어플라이언스에서는 프록시 서버를 지원합니다. 자세한 내용은 *FireSIGHT System 사용 설명서*를 참조하십시오. 프록시 서버는 whois 액세스에 사용할 수 없습니다.

다음 표에는 FireSIGHT System의 특정 기능에 대한 인터넷 액세스 요구 사항이 설명되어 있습니다.

표 1-5 FireSIGHT System 기능의 ?인터넷 액세스 요구 사항

기능	인터넷 액세스가 필요한 이유	어플라이언스
동적 분석: 쿼리	이전에 동적 분석을 위해 제출한 파일의 위협 점수를 Collective Security Intelligence 클라우드에 쿼리	방어 센터
동적 분석: 제출	동적 분석을 위해 Collective Security Intelligence 클라우드에 파일 제출	관리되는 장치
FireAMP 통합	Collective Security Intelligence 클라우드에서 엔드포인트 기반(FireAMP) 악성코드 이벤트 수신	방어 센터
침입 규칙, VDB, GeoDB 업데이트	침입 규칙, GeoDB 또는 VDB 업데이트를 어플라이언스에 직접 다운로드하거나 다운로드 일정 예약	방어 센터
네트워크 기반 AMP	악성코드 클라우드 조회 수행	방어 센터
RSS 피드 대시보드 위젯	Cisco를 포함한 외부 소스에서 RSS 피드 데이터 다운로드	가상 디바이스, X-Series, ASA FirePOWER를 제외한 모든 디바이스
보안 인텔리전스 필터링	FireSIGHT System 인텔리전트 피드를 포함한 외부 소스에서 보안 인텔리전스 피드 데이터 다운로드	방어 센터

표 1-5 FireSIGHT System 기능의 ?인터넷 액세스 요구 사항 (계속)

기능	인터넷 액세스가 필요한 이유	어플라이언스
시스템 소프트웨어 업데이트	시스템 업데이트를 어플라이언스에 직접 다운로드하거나 다운로드 예약	가상 디바이스, X-Series, ASA FirePOWER를 제외한 모든 디바이스
URL 필터링	액세스 제어를 위해 클라우드 기반 URL 범주 및 평판 데이터 다운로드, 분류되지 않은 URL에 대한 조회 수행	방어 센터
whois	외부 호스트의 whois 정보 요청	가상 디바이스, X-Series, ASA FirePOWER를 제외한 모든 디바이스

통신 포트 요구 사항

FireSIGHT System 어플라이언스는 기본적으로 포트 8305/tcp를 사용하는 양방향 SSL-암호화 통신 채널을 사용하여 통신합니다. 이 포트는 기본적인 어플라이언스 간 통신을 위해 **반드시** 열려 있어야 합니다. 열린 다른 포트를 통해 다음과 같은 작업을 수행할 수 있습니다.

- 어플라이언스의 웹 인터페이스에 액세스
- 어플라이언스에 안전하게 원격 연결
- 시스템의 특정 기능이 올바르게 작동하는 데 필요한 로컬 또는 인터넷 리소스에 액세스

일반적으로 기능과 관련된 포트는 관련 기능을 활성화하거나 구성할 때까지 닫힌 상태를 유지해야 합니다. 예를 들어, 방어 센터를 사용자 에이전트에 연결할 때까지 에이전트 통신 포트(3306/tcp)가 닫혀 있어야 합니다. 또 다른 예를 들면, LOM 포트를 활성화하기 전까지 Series 3 어플라이언스에서 623/udp 포트를 닫아 두어야 합니다.

주의 열린 포트를 닫을 경우 구축에 어떤 영향을 미칠지 숙지하기 전까지는 열린 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(*FireSIGHT System 사용 설명서* 참조). 또 다른 예로, 443/TCP(HTTPS) 포트를 닫음으로써 관리되는 물리적 디바이스의 웹 인터페이스에 대한 액세스를 비활성화할 수 있습니다. 그러나 이 경우 디바이스에서 동적 분석을 위해 의심스러운 악성코드 파일을 Collective Security Intelligence 클라우드에 제출하는 것도 차단됩니다.

사용자는 시스템에서 일부 통신 포트를 변경할 수 있습니다.

- 시스템과 인증 서버 간 연결을 구성할 경우 LDAP 및 RADIUS 인증에 대해 맞춤형 포트를 지정할 수 있습니다. *FireSIGHT System 사용 설명서*를 참조하십시오.
- 관리 포트(8305/tcp)를 변경할 수 있습니다. *FireSIGHT System 사용 설명서*를 참조하십시오. 그러나 기본 설정을 유지하는 것이 **좋습니다**. 관리 포트를 변경할 경우, 구축 과정에서 서로 통신해야 하는 모든 어플라이언스의 설정을 변경해야 합니다.
- 포트 32137/tcp를 사용하면 업그레이드된 방어 센터에서 Collective Security Intelligence 클라우드와 통신할 수 있습니다. 그러나 버전 5.3 이상의 초기 설치에 대한 기본값인 포트 443으로 전환하는 것이 좋습니다. 자세한 내용은 *FireSIGHT System 사용 설명서*를 참조하십시오.

다음 표에는 FireSIGHT System 기능을 충분히 활용할 수 있는 각 어플라이언스 유형에 필요한 열린 포트가 나와 있습니다.

표 1-6 FireSIGHT System 기능 및 운영을 지원하는 기본 통신 포트

포트	설명	방향	열리는 디바이스	수행하는 작업
22/tcp	SSH/SSL	양방향	모든	어플라이언스에 대한 안전한 원격 연결 허용
25/tcp	SMTP	아웃바운드	모든	어플라이언스에서 이메일 알림 및 경고 전송
53/tcp	DNS	아웃바운드	모든	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, X-Series, ASA FirePOWER를 제외한 모든 디바이스	RSS 피드 대시보드 위젯에서 원격 웹 서버에 연결
		양방향	방어 센터	HTTP를 통해 맞춤형 및 서드파티 보안 인텔리전스 피드 업데이트 URL 범주 및 평판 데이터 다운로드(포트 443도 필요)
161/udp	SNMP	양방향	X-Series 및 ASA FirePOWER를 제외한 모든 디바이스	SNMP 폴링을 통해 어플라이언스의 MIB에 대한 액세스 허용
162/udp	SNMP	아웃바운드	모든	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	탐지된 LDAP 사용자의 메타데이터 가져오기
443/tcp	HTTPS	인바운드	가상 디바이스, X-Series, ASA FirePOWER를 제외한 모든 디바이스	어플라이언스의 웹 인터페이스에 액세스

표 1-6 FireSIGHT System 기능 및 운영을 지원하는 기본 통신 포트 (계속)

포트	설명	방향	열리는 디바이스	수행하는 작업
443/tcp	HTTPS AMQP 클라우드 통신	양방향	방어 센터	보기: • 소프트웨어, 침입 규칙, VDB, GeoDB 업데이트 • URL 범주 및 평판 데이터(포트 80도 필요) • 종합적 보안 인텔리전스 피드 및 기타 안전한 보안 인텔리전스 피드 • 엔드포인트 기반(FireAMP) 악성코드 이벤트 • 네트워크 트래픽에서 탐지된 파일의 악성코드 처리 • 전송된 파일에 대한 동적 분석 정보
			Series 2 및 Series 3 디바이스	디바이스의 로컬 웹 인터페이스를 사용하여 소프트웨어 업데이트 다운로드
			Series 3, 가상 디바이스, X-Series, ASA FirePOWER	동적 분석을 위해 파일 제출
514/udp	syslog	아웃바운드	모든	원격 syslog 서버에 경고 전송
623/udp	SOL/LOM	양방향	Series 3	SOL(Serial Over LAN) 연결을 사용하여 Lights-Out 관리 수행
1500/tcp 2000/tcp	인바운드	TCP	방어 센터	서드파티 클라이언트의 데이터베이스에 대한 읽기 전용 액세스 허용
1812/udp 1813/udp	RADIUS	양방향	가상 디바이스, X-Series, ASA FirePOWER를 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
8305/tcp	디바이스 관리	양방향	모든	구축 과정에서 어플라이언스 간에 안전하게 통신. **반드시 필요**.
8307/tcp	호스트 입력 클라이언트	양방향	방어 센터	호스트 입력 클라이언트와 통신
32137/tcp	클라우드 통신	양방향	방어 센터	업그레이드된 방어 센터와 Collective Security Intelligence 클라우드 클라우드의 통신 허용

2장 관리 네트워크에서 구축

FireSIGHT System은 각각의 고유한 네트워크 아키텍처의 요구 사항에 맞게 구축할 수 있습니다. 방어 센터에서는 FireSIGHT System을 위한 중앙 집중식 관리 콘솔 및 데이터베이스 저장소를 제공합니다. 디바이스는 분석용 트래픽 연결을 수집하기 위해 네트워크 세그먼트에 설치됩니다.

방어 센터에서는 관리 인터페이스를 사용하여 *신뢰하는 관리 네트워크*(즉, 외부 트래픽에 노출되지 않는 안전한 내부 네트워크)에 연결합니다. 그런 다음 디바이스는 관리 인터페이스를 사용하여 방어 센터에 연결합니다.

참고 ASA FirePOWER 디바이스의 구축 시나리오에 대한 자세한 내용은 ASA 설명서를 참조하십시오.

인터페이스 옵션에 대한 자세한 내용은 다음 섹션을 참조하십시오.

관리 구축 고려 사항

관리 구축 의사 결정은 다양한 요인을 기반으로 합니다. 다음 질문에 대한 답변을 알고 있을 경우 가장 효율적이고 효과적인 시스템을 구성하기 위한 구축 옵션을 파악하는 데 도움이 될 수 있습니다.

- 기본 단일 관리 인터페이스를 사용하여 디바이스를 방어 센터에 연결할 것입니까? 성능을 향상하거나 서로 다른 네트워크에 있는 방어 센터에서 수신된 트래픽을 격리하기 위해 추가 관리 인터페이스를 활성화할 것입니까? 자세한 내용은 관리 인터페이스 이해, 페이지 2-2을/를 참조하십시오.
- 트래픽 채널을 활성화하여 방어 센터와 관리되는 디바이스 간의 연결을 생성하는 방법을 통해 성능을 향상하고자 합니까? 복수 관리 인터페이스를 사용하여 방어 센터와 관리되는 디바이스 간의 처리 용량을 더욱 늘리고자 합니까? 자세한 내용은 트래픽 채널로 구축, 페이지 2-3을/를 참조하십시오.
- 하나의 방어 센터를 사용하여 다른 네트워크에 있는 디바이스의 트래픽을 관리 및 격리하고자 합니까? 자세한 내용은 네트워크 경로로 구축, 페이지 2-5을/를 참조하십시오.
- 보호된 환경에서 관리 인터페이스를 구축하고 있습니까? 어플라이언스 액세스가 특정 워크스테이션 IP 주소로 제한되어 있습니까? 보안 문제, 페이지 2-5에서는 관리 인터페이스를 안전하게 구축하기 위한 몇 가지 고려 사항에 대해 설명합니다.

관리 인터페이스 이해

관리 인터페이스에서는 방어 센터 및 여기서 관리하는 모든 디바이스 간의 통신 수단을 제공합니다. 어플라이언스 간 트래픽 제어를 올바르게 유지하는 것은 성공적인 구축을 위한 필수 조건입니다.

Series 3 어플라이언스 및 가상 방어 센터의 경우 방어 센터, 디바이스 또는 둘 모두에서 관리 인터페이스를 활성화하여 어플라이언스 간 트래픽을 별도의 두 트래픽 채널로 분류할 수 있습니다. *관리 트래픽 채널*은 모든 내부 트래픽(예: 어플라이언스 및 시스템의 관리에 한정된 디바이스 간 트래픽)을 전달하고, *이벤트 트래픽 채널*은 모든 이벤트 트래픽(예: 웹 이벤트)을 전달합니다. 트래픽을 두 개의 채널로 분리하면 어플라이언스 간 연결 지점이 두 개가 생성되므로 처리량이 증가하여 성능이 향상됩니다. 또한 *복수 관리 인터페이스*를 활성화하여 어플라이언스 간에 더욱 방대한 처리량을 제공하거나, 서로 다른 네트워크에 있는 디바이스 간 트래픽을 관리 및 격리할 수 있습니다.

방어 센터에 디바이스를 등록한 후에는 각 어플라이언스의 웹 브라우저를 사용하여 기본 컨피그레이션을 변경함으로써 트래픽 채널 및 복수 관리 인터페이스를 활성화할 수 있습니다. 컨피그레이션 정보에 대한 내용은 *FireSIGHT System 사용 설명서*의 어플라이언스 설정 구성을 참조하십시오.

관리 인터페이스 사용에 대한 자세한 내용은 다음 섹션을 참조하십시오.

- 단일 관리 인터페이스, 페이지 2-2
- 복수 관리 인터페이스, 페이지 2-3

단일 관리 인터페이스

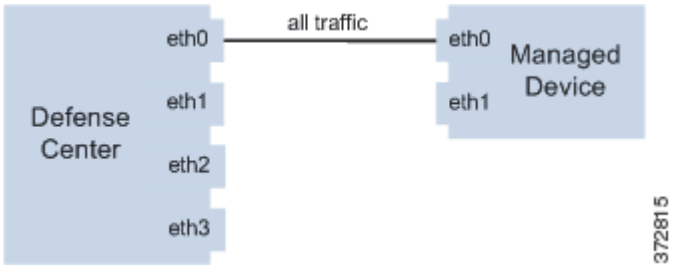
라이센스: 모두

지원되는 Defense Center: 모두

지원되는 디바이스: 모두

방어 센터에 디바이스를 등록할 경우, 방어 센터의 관리 인터페이스와 디바이스의 관리 인터페이스 간의 모든 트래픽을 전달하는 단일 통신 채널이 설정됩니다.

다음 그래픽에는 기본 단일 통신 채널이 나와 있습니다. 단일 인터페이스는 관리 및 이벤트 트래픽을 모두 포함하는 단일 통신 채널을 전달합니다.



복수 관리 인터페이스

라이센스: 모두

지원되는 Defense Center: Series 3, 가상

지원되는 디바이스: Series 3

각각의 고유한 각 IPv4 또는 IPv6 주소 및 고유한 호스트 이름(선택 사항)이 있는 복수 관리 인터페이스를 활성화하고 구성하면 각 트래픽 채널을 서로 다른 관리 인터페이스로 전송하여 더 많은 트래픽 처리량을 제공할 수 있습니다. 가벼운 관리 트래픽을 전달하려면 소형 인터페이스를 구성하고, 무거운 이벤트 트래픽 로드를 전달하려면 대형 인터페이스를 구성합니다. 디바이스를 등록하여 관리 인터페이스를 분리하고 동일한 인터페이스에 대해 두 트래픽 채널을 모두 구성하거나, 전용 관리 인터페이스를 사용하여 방어 센터에서 관리하는 모든 디바이스의 이벤트 트래픽 채널을 전달할 수 있습니다.

또한 방어 센터의 특정 관리 인터페이스에서 다른 네트워크로 경로를 만들 수 있으므로 방어 센터를 통해 한 네트워크에 있는 디바이스의 트래픽을 또 다른 네트워크에 있는 디바이스의 트래픽과 별도로 관리할 수 있습니다.

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

- 기본(`eth0`) 관리 인터페이스에서만 DHCP를 구성할 수 있습니다. 추가(`eth1` 등) 인터페이스에는 고유한 고정 IP 주소 및 호스트 이름이 필요합니다.
- 기본이 아닌 관리 인터페이스를 사용하여 방어 센터 및 관리되는 디바이스를 연결할 경우, 해당 어플라이언스가 NAT 디바이스로 분리되어 있으면 두 트래픽 채널을 모두 구성하여 동일한 관리 인터페이스를 사용해야 합니다.
- 70xx 제품군에서는 트래픽을 두 개의 채널로 구분하고 해당 채널이 트래픽을 가상 방어 센터에 있는 하나 이상의 관리 인터페이스로 전송하도록 구성할 수 있습니다. 그러나 70xx 제품군에는 단일 관리 인터페이스만 포함되어 있으므로 디바이스에서는 단일 관리 인터페이스의 방어 센터에서 전송된 트래픽만 수신합니다.

구축 옵션

하나 이상의 관리 인터페이스를 사용하여 시스템의 성능을 향상하려면 트래픽 채널을 사용하여 트래픽 플로우를 관리할 수 있습니다. 또한 방어 센터 및 관리되는 디바이스에서 특정 관리 인터페이스를 사용하는 서로 다른 네트워크에 경로를 생성하면 다른 네트워크에 있는 디바이스 간에 트래픽을 격리할 수 있습니다. 자세한 내용은 다음 섹션을 참조하십시오.

트래픽 채널로 구축

라이센스: 모두

지원되는 Defense Center: Series 3, 가상

지원되는 디바이스: Series 3

단일 관리 인터페이스에서 트래픽 채널을 2개 사용할 경우 방어 센터와 관리되는 디바이스 간에 연결을 생성할 수 있습니다. 한 채널은 관리 트래픽을 전달하며, 또 다른 채널은 동일한 인터페이스에서 별도로 이벤트 트래픽을 전달합니다.

다음 예에는 동일한 인터페이스에서 별도의 트래픽 채널 2개를 사용하는 통신 채널이 나와 있습니다.

복수 관리 인터페이스를 사용할 경우, 2개의 관리 인터페이스를 통해 트래픽 채널을 분할하여 성능을 향상할 수 있으며 이 경우 결과적으로 두 인터페이스 모두의 용량이 추가되므로 트래픽 플로우가 증대됩니다. 한 인터페이스는 관리 트래픽 채널을 전달하고 다른 하나는 이벤트 트래픽 채널을 전달합니다. 두 인터페이스 중 하나에 오류가 발생하면, 모든 트래픽이 활성 인터페이스로 다시 라우팅되며 연결이 유지됩니다.

다음 그래픽에는 2개의 관리 인터페이스에서 사용되는 관리 트래픽 채널 및 이벤트 트래픽 채널이 나와 있습니다.

전용 관리 인터페이스를 사용하여 여러 개의 디바이스에서 이벤트 트래픽만 전달할 수 있습니다. 이 컨피그레이션에서 각 디바이스는 서로 다른 관리 인터페이스에 등록되어 관리 트래픽 채널을 전달하며, 방어 센터의 단일 관리 인터페이스는 모든 디바이스의 모든 이벤트 트래픽 채널을 전달합니다. 인터페이스에 오류가 발생하면 트래픽은 활성 인터페이스로 다시 라우팅되며 연결이 유지됩니다. 모든 디바이스의 이벤트 트래픽이 동일한 인터페이스에서 전달되므로, 네트워크 간에 트래픽이 격리되지 않습니다.

다음 표에는 이벤트 트래픽 채널에 대해 동일한 전용 인터페이스를 공유하는 서로 다른 관리 채널 트래픽 인터페이스를 사용하는 두 개의 디바이스가 나와 있습니다.

네트워크 경로로 구축

라이센스: 모두

지원되는 Defense Center: Series 3, 가상

지원되는 디바이스: Series 3

방어 센터의 특정 관리 인터페이스에서 다른 네트워크에 대한 경로를 생성할 수 있습니다. 해당 네트워크의 디바이스를 방어 센터에서 지정된 관리 인터페이스에 등록하면 서로 다른 네트워크에 있는 방어 센터와 디바이스 간에 격리된 연결을 제공하게 됩니다. 동일한 관리 인터페이스를 사용하여 두 트래픽 채널을 모두 구성하면 해당 디바이스의 해당 트래픽이 다른 네트워크의 디바이스 트래픽과 격리된 상태를 유지하도록 할 수 있습니다. 라우팅된 인터페이스가 방어 센터의 다른 모든 인터페이스와 격리되므로, 라우팅된 관리 인터페이스에 오류가 발생할 경우 연결이 손실됩니다.

정보 기본(`eth0`) 관리 인터페이스 이외의 모든 관리 인터페이스의 고정 IP 주소에 디바이스를 등록해야 합니다. DHCP는 기본 관리 인터페이스에서만 지원됩니다.

방어 센터를 설치한 후 웹 인터페이스를 사용하여 복수 관리 인터페이스를 구성합니다. 자세한 내용은 *FireSIGHT System 사용 설명서*의 어플라이언스 설정 구성을 참조하십시오.

다음 그래픽에는 모든 트래픽에 별도의 관리 인터페이스를 사용하여 네트워크 트래픽을 격리하는 두 개의 디바이스가 나와 있습니다. 관리 인터페이스를 추가하여 각 디바이스에 별도의 관리 및 이벤트 트래픽 채널 인터페이스를 구성할 수 있습니다.

8000 Series 관리되는 디바이스를 방어 센터에 등록할 경우, 안정적인 네트워크 링크를 보장하려면 연결 양측에서 자동 협상을 사용하거나 양측을 동일한 고정 속도로 설정해야 합니다. 8000 Series 관리되는 디바이스는 반이중 네트워크 링크를 지원하지 않으며 속도 차이 또는 연결 반대쪽의 이중 컨피그레이션도 지원하지 않습니다.

보안 문제

안전한 환경에서 관리 인터페이스를 구축하기 위해 Cisco 에서 권장하는 사항은 다음과 같습니다.

- 관리 인터페이스를 항상 무단 액세스로부터 보호되는 신뢰하는 내부 관리 네트워크에 연결하십시오.
- 어플라이언스에 대한 액세스를 허용할 수 있는 특정 워크스테이션 IP 주소를 식별하십시오. 어플라이언스 시스템 정책 내의 액세스 목록을 이용하여 특정 호스트만 어플라이언스에 액세스할 수 있도록 제한하십시오. 자세한 내용은 *FireSIGHT System 사용 설명서*를 참조하십시오.

가상 어플라이언스 구축

가상 디바이스와 가상 방어 센터를 사용하면 가상 환경에 보안 솔루션을 구축하여 물리적 및 가상 자산에 대한 보호를 강화할 수 있습니다. 가상 디바이스 및 가상 방어 센터로 VMWare 플랫폼에 보안 솔루션을 손쉽게 구현할 수 있습니다. 또한 가상 디바이스를 사용하면 리소스가 제한적일 수 있는 원격 사이트에서 디바이스를 손쉽게 구축 및 관리할 수 있습니다.

이 예에서는 물리적 또는 가상 방어 센터를 사용하여 물리적 또는 가상 디바이스를 관리할 수 있습니다. IPv4 또는 IPv6 네트워크에 구축할 수 있습니다. 또한 방어 센터에 복수의 관리 인터페이스를 구성할 수 있습니다. 이를 통해 서로 다른 두 개의 네트워크를 격리하고 모니터링하거나 단일 네트워크에서 내부 및 이벤트 트래픽을 분리할 수 있습니다. 단, 가상 디바이스에서는 여러 개의 관리 인터페이스를 지원하지 않습니다.

가상 방어 센터에 두 번째 관리 인터페이스를 구성하여 성능을 향상하거나 두 개의 다른 네트워크에서 트래픽을 별도로 관리할 수 있습니다. 추가 인터페이스와 추가 가상 스위치를 구성하여 두 번째 관리 인터페이스를 두 번째 네트워크의 관리되는 디바이스에 연결합니다. 복수 관리 인터페이스에 대한 자세한 내용은 FireSIGHT System 사용 설명서의 디바이스 관리를 참조하십시오.

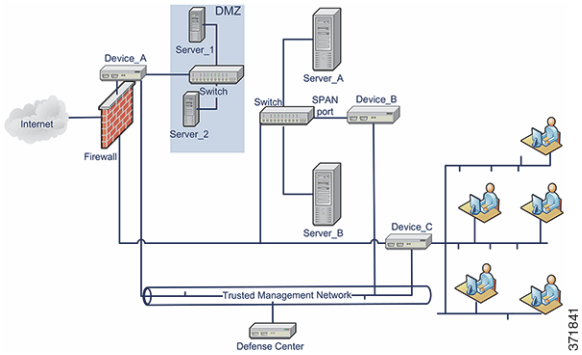
두 번째 관리 인터페이스를 가상 어플라이언스에 추가하려면 VMware vSphere(http://vmware.com)를 참조하십시오.

주의 Cisco에서는 운영 네트워크 트래픽과 신뢰하는 관리 네트워크 트래픽을 다른 네트워크 세그먼트에 유지할 것을 **강력하게** 권고하고 있습니다. 어플라이언스 및 관리 트래픽 데이터 스트림을 보호하기 위한 주의 사항을 준수해야 합니다.

이 장에서는 다음에 대한 구축 예를 제공합니다.

일반적인 FireSIGHT System 구축

물리적 어플라이언스 환경에서는 일반적인 FireSIGHT System 구축 시 물리적 디바이스와 물리적 방어 센터를 사용합니다. 다음 그래픽에는 구축 예가 나와 있습니다. 아래와 같이 디바이스 A와 디바이스 C를 인라인 컨피그레이션으로 구축하고 디바이스 B를 수동 컨피그레이션으로 구축할 수 있습니다.



대부분의 네트워크 스위치에서 포트 미러링을 구성하여 하나의 스위치 포트(또는 전체 VLAN)에서 볼 수 있는 네트워크 패킷의 복사본을 네트워크 모니터링 연결로 전송할 수 있습니다. 포트 미러링은 주요 네트워크 장비 제공업체에서 SPAN(Switch Port Analyzer)이라고도 하며 네트워크 트래픽 모니터링 기능을 제공합니다. 디바이스 B는 서버 A와 서버 B 사이의 스위치에 있는 SPAN 포트를 통해 서버 A와 서버 B 사이의 트래픽을 모니터링합니다.

VMWare 가상 어플라이언스 구축

아래의 가상 어플라이언스 구축 시나리오에서 일반 구축 예를 참조하십시오.

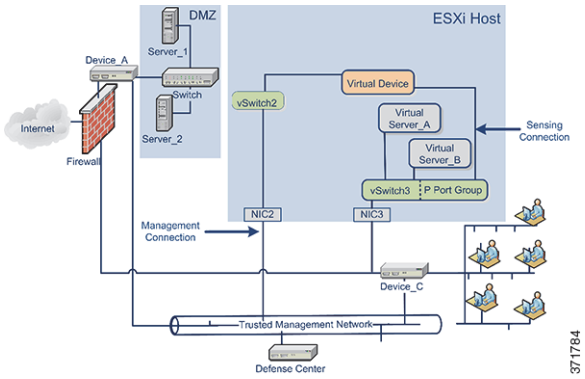
- 가상화 및 가상 디바이스 추가, 페이지 3-3
- 인라인 탐지에 가상 디바이스 사용, 페이지 3-4
- 가상 방어 센터 추가, 페이지 3-5
- 원격사무실 구축 사용, 페이지 3-6

가상화 및 가상 디바이스 추가

가상 인프라를 사용하여 일반적인 FireSIGHT System 구축, 페이지 3-2의 물리적 내부 서버를 교체할 수 있습니다. 다음 예에서 ESXi 호스트를 사용하고 서버 A와 서버 B를 가상화할 수 있습니다.

가상 디바이스를 사용하여 서버 A와 서버 B 사이의 트래픽을 모니터링할 수 있습니다.

가상 디바이스 센싱 인터페이스는 아래 그림과 같이 프로미스큐어스 모드(promiscuous mode) 트래픽을 수신하는 스위치 또는 포트 그룹에 연결해야 합니다.



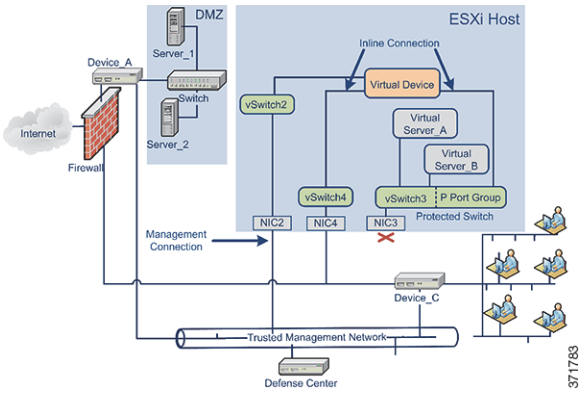
참고 모든 트래픽을 감지하려면 디바이스 센싱 인터페이스가 연결된 가상 스위치 또는 포트 그룹에서 프로미스큐어스 모드 트래픽을 허용해야 합니다. 가상 디바이스 센싱 인터페이스 구성, 페이지 4-10을 참조하십시오.

이 예에는 하나의 센싱 인터페이스만 있지만 가상 디바이스에서는 기본적으로 두 개의 센싱 인터페이스를 사용할 수 있습니다. 가상 디바이스 관리 인터페이스는 신뢰하는 관리 네트워크 및 방어 센터에 연결됩니다.

인라인 탐지에 가상 디바이스 사용

가상 디바이스의 인라인 인터페이스 세트를 통해 트래픽을 전달하여 가상 서버 주위에 보안 경계를 제공할 수 있습니다. 이 시나리오는 일반적인 FireSIGHT System 구축, 페이지 3-2 및 가상화 및 가상 디바이스 추가, 페이지 3-3의 예를 기준으로 합니다.

먼저 보호된 가상 스위치를 만들고 가상 서버에 연결합니다. 그런 다음 보호된 스위치를 가상 디바이스를 통해 외부 네트워크에 연결합니다. 자세한 내용은 *FireSIGHT System 사용 설명서*를 참조하십시오.



참고 모든 트래픽을 감지하려면 디바이스 센싱 인터페이스가 연결된 가상 스위치 또는 포트 그룹에서 프로미스큐어스 모드 트래픽을 허용해야 합니다. 가상 디바이스 센싱 인터페이스 구성, 페이지 4-10을 참조하십시오.

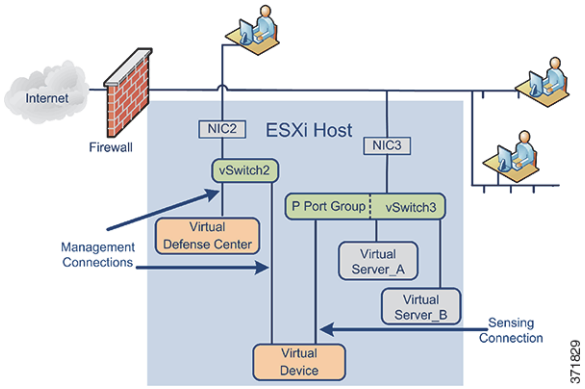
가상 디바이스는 침입 정책에 따라 서버 A 및 서버 B에 대한 트래픽을 모니터링하고 악성 트래픽을 삭제합니다.

가상 방어 센터 추가

ESXi 호스트에 가상 방어 센터를 구축하고 아래 그림과 같이 가상 네트워크 및 물리적 네트워크에 연결합니다. 이 시나리오는 일반적인 FireSIGHT System 구축, 페이지 3-2 및 인라인 탐지에 가상 디바이스 사용, 페이지 3-4의 예를 기준으로 합니다.

가상 방어 센터에서 NIC2를 통해 신뢰하는 관리 네트워크로 연결할 경우 가상 방어 센터에서 물리적 및 가상 디바이스를 관리할 수 있습니다.

Cisco 가상 디바이스는 필수 애플리케이션 소프트웨어가 사전 구성되어 있으므로 ESXi 호스트에 구축하여 실행할 수 있습니다. 이 경우 복잡한 하드웨어 및 소프트웨어 호환성 문제가 감소하므로 구축을 가속화하고 FireSIGHT System의 이점에 주력할 수 있습니다. ESXi 호스트에 가상 서버, 가상 방어 센터, 가상 디바이스를 구축하고, 아래 그림과 같이 가상 방어 센터에서 구축을 관리할 수 있습니다.

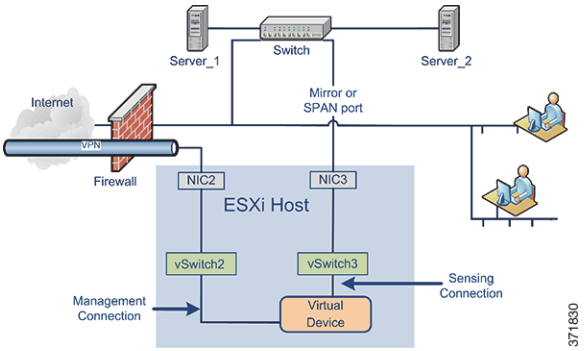


네트워크 트래픽을 모니터링하려면 가상 디바이스의 센싱 연결을 허용해야 합니다. 가상 스위치 또는 해당 스위치에서 가상 인터페이스가 연결되는 포트 그룹은 프로미스큐어스 모드 트래픽을 허용해야 합니다. 그럴 경우 가상 디바이스가 다른 장비 또는 네트워크 장비로 보내는 패킷을 읽을 수 있습니다. 이 예에서 P 포트 그룹은 프로미스큐어스 모드 트래픽을 허용하도록 설정되어 있습니다. 가상 디바이스 센싱 인터페이스 구성, 페이지 4-10을 참조하십시오.

가상 어플라이언스 관리 연결은 보다 일반적인 비 프로미스큐어스 모드 연결입니다. 가상 방어 센터에서는 가상 디바이스에 명령 및 제어를 제공합니다. ESXi 호스트의 네트워크 인터페이스 카드(이 예에서는 NIC2)를 통해 연결할 경우 가상 방어 센터에 액세스할 수 있습니다. 가상 방어 센터 및 가상 디바이스 관리 연결을 설정하는 방법은 가상 방어 센터 네트워크 설정 자동화, 페이지 5-7 및 CLI를 사용하여 가상 디바이스 설정, 페이지 5-3을 참조하십시오.

원격사무실 구축 사용

가상 디바이스는 리소스가 제한적인 원격사무실을 모니터링하기에 적합한 방법입니다. 아래 그림과 같이 ESXi 호스트에 가상 디바이스를 구축하고 로컬 트래픽을 모니터링할 수 있습니다.



네트워크 트래픽을 모니터링하려면 가상 디바이스의 센싱 연결을 허용해야 합니다. 그러려면 센싱 인터페이스가 연결된 가상 스위치 또는 스위치의 포트 그룹에서 프로미스큐어스 모드 트래픽을 허용해야 합니다. 그럴 경우 가상 디바이스가 다른 장비 또는 네트워크 장비로 보내는 패킷을 읽을 수 있습니다. 이 예에서는 모든 vSwitch3가 프로미스큐어스 모드 트래픽을 허용하도록 설정되어 있습니다. vSwitch3도 NIC3를 통해 SPAN 포트로 연결되어 있어 원격사무실의 스위치를 통과하는 트래픽을 모니터링할 수 있습니다. 가상 디바이스 센싱 인터페이스 구성, 페이지 4-10을 참조하십시오.

가상 디바이스는 반드시 방어 센터로 관리해야 합니다. ESXi 호스트의 네트워크 인터페이스 카드(이 예에서는 NIC2)를 통해 연결할 경우 원격 방어 센터을 통해 가상 디바이스에 액세스할 수 있습니다.

디바이스를 각각 다른 지리적 위치에 구축할 경우 디바이스를 보호되지 않은 네트워크로부터 격리하여 디바이스 및 데이터 스트림을 보호해야 합니다. 이렇게 하려면 VPN 또는 다른 보안 터널링 프로토콜에서 디바이스의 데이터 스트림을 전송합니다. 가상 디바이스 관리 연결을 설정하는 방법은 CLI를 사용하여 가상 디바이스 설정, 페이지 5-3을 참조하십시오.

가상 어플라이언스 설치

Cisco에서는 지원 사이트의 VMWare ESXi 호스트 환경을 위해 패키지형 가상 어플라이언스를 압축된 아카이브(.tar.gz) 파일로 제공합니다. Cisco 가상 어플라이언스는 가상 하드웨어 버전 7을 사용하여 가상 머신으로 패키지화됩니다.

가상 인프라(VI) 또는 ESXi OVF(Open Virtual Format) 템플릿으로 가상 어플라이언스를 구축합니다.

- VI OVF 템플릿으로 구축할 경우, 구축 과정에서 설정 마법사를 사용하여 FireSIGHT System의 필수 설정(예: 관리 계정의 비밀번호 및 어플라이언스가 네트워크에서 통신할 수 있는 설정)을 구성할 수 있습니다.
- 관리하는 플랫폼, 즉 VMware vCloud Director 또는 VMware vCenter로 구축해야 합니다.
- ESXi OVF 템플릿으로 구축할 경우 설치 후 가상 어플라이언스의 VMWare 콘솔에 CLI (Command Line Interface)를 사용하여 설정을 구성해야 합니다.
- 관리하는 플랫폼(VMware vCloud Director 또는 VMware vCenter)으로 구축하거나 독립형 어플라이언스로 구축할 수 있습니다.

참고 Cisco 가상 어플라이언스의 VMWare 스냅샷은 지원되지 **않습니다**.

이 장의 지침을 사용하여 Cisco 가상 어플라이언스를 다운로드, 설치 및 구성하십시오. 가상 호스트 환경을 만드는 방법은 VMWare ESXi 설명서를 참조하십시오.

다음 절차에 따라 가상 어플라이언스를 설치 및 구성한 다음 전원을 켜서 초기화하고 다음 장에 설명된 대로 초기 설정 프로세스를 시작합니다. 가상 어플라이언스 제거에 대한 내용은 가상 어플라이언스 제거, 페이지 4-11를 참조하십시오.

Cisco 가상 어플라이언스를 설치 및 구축하려면 다음을 수행합니다.

단계 1 계획된 구축이 운영 환경 전제 조건, 페이지 1-6에 설명된 전제 조건을 충족하는지 확인합니다.

단계 2 지원 사이트에서 올바른 아카이브 파일을 얻고 적절한 저장 매체로 복사한 다음 압축을 풉니다. 설치 파일 가져오기, 페이지 4-2를 참조하십시오.

단계 3 웹 포털 VMware vCloud Director 또는 vSphere Client를 사용하여 가상 어플라이언스를 설치하되, 전원을 *끄지* 마십시오. 가상 어플라이언스 설치, 페이지 4-3를 참조하십시오.

단계 4 네트워크, 하드웨어, 메모리 설정을 확인 및 조정합니다. 설치 후 중요 설정 업데이트, 페이지 4-8를 참조하십시오.

단계 5 선택적으로, 기본 e1000 인터페이스를 vnxnet3 인터페이스로 교체하거나, 추가 관리 인터페이스를 만들거나, 두 가지를 모두 수행합니다. 자세한 내용은 인터페이스 추가 및 구성, 페이지 4-10을(를) 참고하십시오.

단계 6 가상 디바이스의 센싱 인터페이스가 ESXi 호스트 가상 스위치에 올바르게 연결되었는지 확인합니다. 가상 디바이스 센싱 인터페이스 구성, 페이지 4-10을 참조하십시오.

설치 파일 가져오기

Cisco에서는 가상 어플라이언스를 설치할 수 있는 방어 센터용 압축 아카이브(`.tar.gz`) 파일 하나와 디바이스용 파일 하나를 제공합니다. 각 아카이브에는 다음 파일이 포함되어 있습니다.

- 파일 이름에 `-ESXi-`가 포함된 Open Virtual Format(`.ovf`) 템플릿
- 파일 이름에 `-VI-`가 포함된 Open Virtual Format(`.ovf`) 템플릿
- 파일 이름에 `-ESXi-`가 포함된 매니페스트 파일(`.mf`)
- 파일 이름에 `-VI-`가 포함된 매니페스트 파일(`.mf`)
- 가상 머신 디스크 형식(`.vmdk`)

가상 어플라이언스를 설치하기 전에 지원 사이트에서 올바른 아카이브 파일을 가져오십시오. Cisco에서는 언제든 사용 가능한 최신 패키지를 이용할 것을 권장합니다. 가상 어플라이언스 패키지는 일반적으로 주 버전의 시스템 소프트웨어와 연결되어 있습니다(예: 5.2 또는 5.3).

가상 어플라이언스 아카이브 파일을 가져오려면 다음을 수행합니다.

단계 1 지원 계정의 사용자 이름과 비밀번호를 사용하여 지원 사이트(https://support.sourcefire.com/)에 로그인합니다.

단계 2 **Downloads**를 클릭하고 표시되는 페이지에서 **3D System** 탭을 선택한 다음 설치하려는 시스템 소프트웨어의 주 버전을 클릭합니다.

예를 들어, 아카이브 파일을 다운로드하려면 버전 5.4.1 **Downloads > 3D System > 5.4.1**을 클릭합니다.

단계 3 다음의 명명 규칙 따라 가상 디바이스 또는 가상 방어 센터용으로 다운로드할 아카이브 파일을 검색합니다.

```
Sourcefire_3D_Device_Virtual64_VMware-X.X.X-xxx.tar.gz
Sourcefire_Defense_Center_Virtual64_VMware-X.X.X-xxx.tar.gz
```

여기서 *X.X.X-xxx*는 다운로드하려는 아카이브 파일의 버전 및 빌드 번호입니다.

페이지의 해당 섹션을 보려면 페이지의 왼쪽에 있는 링크 중 하나를 클릭합니다. 예를 들어, FireSIGHT System의 버전 5.4.1용 아카이브 파일을 보려면 **5.4.1 Virtual Appliances**를 클릭합니다.

단계 4 다운로드하려는 아카이브를 클릭합니다.

파일 다운로드가 시작됩니다.

정보 지원 사이트에 로그인되어 있는 동안에는 가상 어플라이언스를 주 버전으로 설치한 다음 시스템 소프트웨어를 업데이트할 수 있도록 가상 어플라이언스에 사용 가능한 모든 업데이트를 다운로드하는 것이 좋습니다. 또한 항상 어플라이언스에서 지원하는 최신 버전의 시스템 소프트웨어를 실행해야 합니다. 방어 센터의 경우 새로운 침입 규칙 및 VDB(Vulnerability Database)도 모두 다운로드해야 합니다.

단계 5 vSphere Client 또는 VMware vCloud Director 웹 포털을 실행하는 워크스테이션 또는 서버가 액세스할 수 있는 위치로 아카이브 파일을 복사합니다.

주의 아카이브 파일을 이메일로 전송하지 **마십시오**. 파일이 손상될 수 있습니다.

단계 6 선호하는 툴을 사용하여 아카이브 파일의 압축을 풀고 설치 파일을 추출합니다.

가상 디바이스의 경우:

```
Sourcefire_3D_Device_Virtual64_VMware-X.X.X-xxx-disk1.vmdk
Sourcefire_3D_Device_Virtual64_VMware-ESXi-X.X.X-xxx.ovf
Sourcefire_3D_Device_Virtual64_VMware-ESXi-X.X.X-xxx.mf
Sourcefire_3D_Device_Virtual64_VMware-VI-X.X.X-xxx.ovf
Sourcefire_3D_Device_Virtual64_VMware-VI-X.X.X-xxx.mf
```

가상 방어 센터의 경우:

```
Sourcefire_Defense_Center_Virtual64_VMware-X.X.X-xxx-disk1.vmdk
Sourcefire_Defense_Center_Virtual64_VMware-ESXi-X.X.X-xxx.ovf
Sourcefire_Defense_Center_Virtual64_VMware-ESXi-X.X.X-xxx.mf
Sourcefire_Defense_Center_Virtual64_VMware-VI-X.X.X-xxx.ovf
Sourcefire_Defense_Center_Virtual64_VMware-VI-X.X.X-xxx.mf
```

여기서 *X.X.X-xxx*는 다운로드하려는 아카이브 파일의 버전 및 빌드 번호입니다.

모든 파일을 동일한 디렉토리에 보관합니다.

단계 7 가상 어플라이언스 설치를 계속 진행하여 가상 어플라이언스를 구축합니다.

가상 어플라이언스 설치

가상 어플라이언스를 설치하려면 플랫폼 인터페이스(VMware vCloud Director 웹 포털 또는 vSphere Client)를 사용하여 관리하는 플랫폼(VMware vCloud Director 또는 VMware vCenter)에 OVF(VI 또는 ESXi) 템플릿을 구축합니다.

- VI OVF 템플릿을 사용하여 구축하는 경우 설치 중 FireSIGHT System의 필수 설정을 구성할 수 있습니다. VMware vCloud Director 또는 VMware vCenter를 사용하여 이 가상 어플라이언스를 관리해야 합니다.
- ESXi OVF 템플릿을 사용하여 구축할 경우 설치 후 FireSIGHT System의 필수 설정을 구성해야 합니다. 이 가상 어플라이언스를 VMware vCloud Director 또는 VMware vCenter를 사용하여 관리하거나 독립형 어플라이언스로 사용할 수 있습니다.

계획된 구축이 전제 조건(운영 환경 전제 조건, 페이지 1-6에서 설명)을 충족하는지 확인하고 필요한 아카이브 파일을 다운로드한 다음 VMware vCloud Director 웹 포털 또는 vSphere Client를 사용하여 가상 어플라이언스를 설치합니다.

가상 어플라이언스를 설치하려는 경우 다음과 같은 설치 옵션이 있습니다.

- 가상 방어 센터의 경우:

```
Sourcefire_Defense_Center_Virtual64_VMware-VI-X.X.X-xxx.ovf
Sourcefire_Defense_Center_Virtual64_VMware-ESXi-X.X.X-xxx.ovf
```

- 가상 디바이스의 경우:

```
Sourcefire_3D_Device_Virtual64_VMware-VI-X.X.X-xxx.ovf
Sourcefire_3D_Device_Virtual64_VMware-ESXi-X.X.X-xxx.ovf
```

여기서 *X.X.X-xxx*는 사용하려는 파일의 버전 및 빌드 번호입니다.

다음 표에는 구축에 필요한 정보가 나와 있습니다.

표 4-1 VMWare OVF 템플릿

설정	조치
Import/Deploy OVF Template	이전 절차에서 사용하기 위해 다운로드한 OVF 템플릿을 찾습니다.
OVF 템플릿 세부 정보	설치할 어플라이언스(가상 방어 센터 또는 가상 디바이스) 및 구축 옵션(VI 또는 ESXi)을 확인합니다.
Name and Location	가상 어플라이언스에 고유하고 의미 있는 이름을 입력하고 어플라이언스의 인벤토리 위치를 선택합니다.
Host / Cluster	가상 디바이스의 경우에만, 디바이스를 구축하려는 호스트 또는 클러스터를 선택합니다.
Disk Format	가상 디스크를 저장할 형식(thick provision lazy zeroed, thick provision eager zeroed 또는 thin provision)을 선택합니다.
Network Mapping	가상 어플라이언스의 관리 인터페이스를 선택합니다.

VI OVF 템플릿을 구축할 경우 설치 프로세스에서 가상 방어 센터의 기본 설정 및 가상 디바이스의 전체 초기 설정을 수행할 수 있습니다. 다음을 지정할 수 있습니다.

- 관리자 계정의 새 비밀번호
- 어플라이언스가 관리 네트워크에서 통신하도록 지원하는 네트워크 설정
- 가상 디바이스에서만 초기 탐지 모드
- 가상 디바이스에서만 관리하는 방어 센터

ESXi OVF 템플릿으로 구축하거나 설정 마법사로 구성하지 않을 경우 VMWare 콘솔을 사용하여 가상 어플라이언스의 초기 설정을 수행해야 합니다. 지정할 컨피그레이션에 대한 지침을 포함하여, 초기 설정 수행에 대한 자세한 내용은 가상 어플라이언스 설정, 페이지 5-1을 참조하십시오.

다음 중 한 가지 옵션을 사용하여 가상 어플라이언스를 설치합니다.

- VMware vCloud Director 웹 포털로 설치, 페이지 4-5에서는 가상 어플라이언스를 VMware vCloud Director에 구축하는 방법에 대해 설명합니다.
- vSphere Client로 설치, 페이지 4-7에서는 가상 어플라이언스를 VMware vCenter에 구축하는 방법에 대해 설명합니다.

네트워크 설정 및 탐지 모드에 대해 숙지하려면 CLI를 사용하여 가상 디바이스 설정, 페이지 5-3 및 가상 방어 센터 설정, 페이지 5-6을 참조하십시오.

VMware vCloud Director 웹 포털로 설치

VMware vCloud Director 웹 포털을 사용하여 다음 단계에 따라 가상 어플라이언스를 구축할 수 있습니다.

- vApp 템플릿을 포함할 조직 및 카탈로그를 생성합니다. 자세한 내용은 *VMware vCloud Director 사용 설명서*를 참조하십시오.
- FireSIGHT System 가상 어플라이언스 OVF 패키지를 vApp 템플릿으로 카탈로그에 업로드합니다. 자세한 내용은 가상 어플라이언스 OVF 패키지 업로드, 페이지 4-5을(를) 참고하십시오.
- vApp 템플릿을 사용하여 가상 어플라이언스를 만듭니다. 자세한 내용은 vApp 템플릿 사용, 페이지 4-6을(를) 참고하십시오.

가상 어플라이언스 OVF 패키지 업로드

다음 OVF 패키지를 VMware vCloud Director 조직 카탈로그에 업로드할 수 있습니다.

가상 방어 센터의 경우:

```
Sourcefire_Defense_Center_Virtual64_VMware-VI-X.X.X-xxx.ovf
```

가상 디바이스의 경우:

```
Sourcefire_3D_Device_Virtual64_VMware-VI-X.X.X-xxx.ovf
```

여기서 *X.X.X-xxx*는 업로드하려는 OVF 패키지의 버전 및 빌드 번호입니다.

가상 어플라이언스 OVF 패키지를 업로드하려면 다음을 수행합니다.

단계 1 VMware vCloud Director 웹 포털에서 **Catalogs** > *Organization* > **vApp Templates**를 선택합니다. 여기서, *Organization*은 vApp 템플릿을 포함하려는 조직의 이름입니다.

단계 2 vApp Templates 미디어 탭에서 업로드 아이콘( )을 클릭합니다.

vApp Template 팝업 창에 Upload OVF 패키지가 나타납니다.

단계 3 OVF 패키지 필드에서 OVF 패키지의 위치를 입력하거나 **Browse**를 클릭하여 OVF 패키지로 이동합니다.

- 가상 방어 센터의 경우:

  ```
  Sourcefire_Defense_Center_Virtual64_VMware-VI-X.X.X-xxx.ovf
  ```

- 가상 디바이스의 경우:

  ```
  Sourcefire_3D_Device_Virtual64_VMware-VI-X.X.X-xxx.ovf
  ```

- 여기서 *X.X.X-xxx*는 업로드하려는 OVF 패키지의 버전 및 빌드 번호입니다.

단계 4 OVF 패키지의 이름과 설명(선택 사항)을 입력합니다.

단계 5 드롭다운 목록에서 가상 데이터센터, 스토리지 프로파일, vApp 템플릿을 포함할 카탈로그를 선택합니다.

단계 6 **Upload**를 클릭하여 OVF 패키지를 vApp 템플릿을 카탈로그에 업로드합니다.

OVF 패키지가 조직 카탈로그에 업로드됩니다.

단계 7 vApp 템플릿 사용을 계속 진행하여 vApp 템플릿에서 가상 어플라이언스를 만듭니다.

vApp 템플릿 사용

vApp 템플릿을 사용하여 가상 어플라이언스를 만들면 설정 마법사로 설치하는 동안 FireSIGHT System의 필수 설정을 구성할 수 있습니다. 마법사의 각 페이지에서 설정을 지정한 다음 **Next**를 클릭하여 계속합니다. 사용자의 편의를 위해, 절차를 완료하기 전에 마법사의 마지막 페이지에서 설정을 확인할 수 있습니다.

vApp 템플릿을 사용하여 가상 어플라이언스를 만드는 방법

단계 1 VMware vCloud Director 웹 포털에서 **My Cloud > vApps**를 선택합니다.

단계 2 vApps 미디어 탭에서 추가 아이콘()을 클릭하여 카탈로그의 vApp을 추가합니다.

Add vApp from Catalog 팝업 창이 나타납니다.

단계 3 템플릿 메뉴 모음에서 **All Templates**를 클릭합니다.

사용 가능한 모든 vApp 템플릿 목록이 표시됩니다.

단계 4 추가할 vApp 템플릿을 선택하여 가상 어플라이언스에 대한 설명을 표시합니다.

- 가상 방어 센터의 경우:

  `Sourcefire_Defense_Center_Virtual64_VMware-VI-X.X.X-xxx.ovf`

- 가상 디바이스의 경우:

  `Sourcefire_3D_Device_Virtual64_VMware-VI-X.X.X-xxx.ovf`

- 여기서 *X.X.X-xxx*는 아카이브 파일의 버전 및 빌드 번호입니다.

EULA(End User License Agreement)가 나타납니다.

단계 5 EULA를 읽고 그 내용에 동의합니다.

Name this vApp 화면이 표시됩니다.

단계 6 vApp의 이름과 설명(선택 사항)을 입력합니다.

Configure Resources 화면이 나타납니다.

단계 7 Configure Resources 화면에서 가상 데이터베이스를 선택한 후 컴퓨터 이름을 입력하고(또는 기본 컴퓨터 이름 사용) 스토리지 프로파일을 선택합니다.

Network Mapping 화면이 나타납니다.

단계 8 외부, 관리, 내부 소스 및 IP 할당의 대상을 선택하여 OVF 템플릿에 사용된 네트워크를 인벤토리의 네트워크로 매핑합니다.

Custom Properties 화면이 나타납니다.

단계 9 선택적으로, Custom Properties 화면의 설정 마법사에서 FireSIGHT System의 필수 설정을 입력하여 어플라이언스의 초기 설정을 수행합니다. 지금 초기 설정을 수행하지 않을 경우 가상 어플라이언스 설정, 페이지 5-1의 지침에 따라 나중에 수행할 수 있습니다.

가상 어플라이언스의 컨피그레이션을 표시하는 Ready to Complete 화면이 나타납니다.

단계 10 설정을 확인하고 **Finish**를 클릭합니다.

참고 가상 디바이스의 **Power on after deployment** 옵션을 활성화하지 **마십시오**. 센싱 인터페이스를 매핑해야 하며, 어플라이언스 전원을 켜기 전에 연결되도록 설정해야 합니다. 자세한 내용은 가상 어플라이언스 초기화, 페이지 5-2을(를) 참고하십시오.

단계 11 설치 후 중요 설정 업데이트, 페이지 4-8를 계속 진행합니다.

vSphere Client로 설치

vSphere Client를 사용하여 VI OVF 또는 ESXi OVF 템플릿으로 구축할 수 있습니다.

- VI OVF 템플릿을 사용하여 구축할 경우 어플라이언스를 VMware vCenter 또는 VMware vCloud Director로 관리해야 합니다.
- ESXi OVF 템플릿을 사용하여 구축할 경우 어플라이언스를 VMware vCenter, VMware vCloud Director로 관리하거나 독립형 호스트에 구축할 수 있습니다. 어떤 경우든 설치 후 FireSIGHT System의 필수 설정을 구성해야 합니다.

마법사의 각 페이지에서 설정을 지정한 다음 **Next**를 클릭하여 계속합니다. 사용자의 편의를 위해, 절차를 완료하기 전에 마법사의 마지막 페이지에서 설정을 확인할 수 있습니다.

vSphere Client를 사용하여 가상 어플라이언스를 설치하려면 다음을 수행합니다.

단계 1 vSphere Client를 사용하여 **File > Deploy OVF Template**을 클릭하여 앞에서 다운로드한 OVF 템플릿 파일을 구축합니다.

Source 화면이 나타나면 드롭다운 목록에서 구축할 템플릿을 검색할 수 있습니다.

단계 2 드롭다운 목록에서 구축할 OVF 템플릿을 선택합니다.

- 가상 방어 센터의 경우:

```
Sourcefire_Defense_Center_Virtual64_VMware-VI-X.X.X-xxx.ovf
Sourcefire_Defense_Center_Virtual64_VMware-ESXi-X.X.X-xxx.ovf
```

- 가상 디바이스의 경우:

```
Sourcefire_3D_Device_Virtual64_VMware-VI-X.X.X-xxx.ovf
Sourcefire_3D_Device_Virtual64_VMware-ESXi-X.X.X-xxx.ovf
```

- 여기서 *X.X.X-xxx*는 다운로드하려는 아카이브 파일의 버전 및 빌드 번호입니다.

OVF Template Details 화면이 나타납니다.

단계 3 올바른 가상 머신을 선택했는지 확인합니다.

- ESXi OVF 템플릿의 경우:
- Name and Location 화면이 나타납니다.
- VI OVF 템플릿의 경우:
- EULA(End User License Agreement) 화면이 나타납니다.
- EULA를 읽고 동의하면 Name and Location 화면이 나타납니다.

단계 4 텍스트 필드에 가상 어플라이언스의 이름을 입력하고 어플라이언스를 구축하려는 인벤토리 위치를 선택합니다.

Host / Cluster 화면이 나타납니다.

단계 5 템플릿을 구축할 호스트 또는 클러스터를 선택합니다.

Specific Host 화면이 나타납니다.

단계 6 템플릿을 구축하려는 클러스터 내에서 특정 호스트를 선택합니다.

Storage 화면이 나타납니다.

단계 7 가상 머신의 대상 스토리지를 선택합니다.

Disk Format 화면이 나타납니다.

단계 8 다음 옵션 중에서 가상 디스크를 저장할 형식을 선택합니다.

- thick provision lazy zeroed
- thin provision eager zeroed
- thin provision

Network Mapping 화면이 나타납니다.

단계 9 템플릿을 구축할 네트워크를 선택합니다.

- ESXi OVF 템플릿의 경우:
- ESXi Finish 화면이 나타납니다.
- VI OVF 템플릿의 경우:
- Properties 화면이 나타납니다.
- 어플라이언스에 대한 FireSIGHT System의 필수 설정을 입력하거나 나중에 설정을 완료하도록 클릭하고 설정을 확인한 다음 **Finish**를 클릭합니다.

참고 가상 디바이스의 **Power on after deployment** 옵션을 활성화하지 **마십시오**. 센싱 인터페이스를 매핑해야 하며, 어플라이언스 전원을 켜기 전에 연결되도록 설정해야 합니다. 자세한 내용은 가상 어플라이언스 초기화, 페이지 5-2을(를) 참고하십시오.

단계 10 설치가 완료되면 상태 창을 닫습니다.

단계 11 설치 후 중요 설정 업데이트를 계속 진행합니다.

설치 후 중요 설정 업데이트

가상 어플라이언스를 설치한 다음 가상 어플라이언스의 하드웨어 및 메모리 설정이 구축 요구 사항을 충족하는지 확인해야 합니다. 기본 설정은 시스템 소프트웨어를 실행하는 데 필요한 최소 설정이므로 기본 설정을 줄이지 **마십시오**. 그러나 성능을 개선하려는 경우 가용 리소스에 따라 가상 어플라이언스의 메모리와 CPU 수를 늘릴 수 있습니다. 다음 표에는 기본 어플라이언스 설정이 나와 있습니다.

표 4-2 기본 가상 어플라이언스 설정

설정	기본	설정의 조정 가능 여부
메모리	4GB	조정 가능하며, 가상 디바이스의 경우 **반드시** 다음을 할당해야 합니다. • 최소 4GB • 범주 및 평판 기반 URL 필터링을 추가하기 위한 5GB • 대용량 동적 피드를 사용하여 보안 인텔리전스 필터링을 추가하기 위한 6GB • URL 필터링 및 보안 인텔리전스를 추가하기 위한 7GB

표 4-2 기본 가상 어플라이언스 설정 (계속)

설정	기본	설정의 조정 가능 여부
가상 CPU	4	조정 가능, 최대 8개
하드 디스크 프로비저닝 크기	40GB(디바이스) 250GB(방어 센터)	아니요

다음 절차에서는 가상 어플라이언스의 하드웨어 및 메모리 설정을 확인하고 조정하는 방법에 대해 설명합니다.

가상 어플라이언스 설정을 확인하려면 다음을 수행합니다.

단계 1 새 가상 어플라이언스의 이름을 마우스 오른쪽 버튼으로 클릭한 다음 컨텍스트 메뉴에서 **Edit Settings**를 선택하거나 기본 창의 **Getting Started** 탭에서 **Edit virtual machine settings**를 클릭합니다.

Hardware 탭이 표시된 Virtual Machine Properties 팝업 창이 나타납니다.

단계 2 **Memory**, **CPUs**, **Hard disk 1** 설정이 표 4-2기본 가상 어플라이언스 설정, 페이지 4-8에 설명된 대로 기본값 미만으로 설정되지 않았는지 확인합니다.

어플라이언스의 메모리 설정 및 가상 CPU 수가 창 왼쪽에 나열됩니다. 하드 디스크의 **Provisioned Size**를 보려면 **Hard disk 1**을 클릭합니다.

단계 3 선택적으로, 창 왼쪽에서 해당 설정을 클릭하여 메모리 및 가상 CPU의 수를 늘린 다음 창 오른쪽에서 변경 사항을 적용합니다.

단계 4 **Network adapter 1** 설정이 다음과 같은지 확인하고, 필요한 경우 변경합니다.

- **Device Status** 아래에서 **Connect at power on** 확인란을 활성화합니다.
- **MAC Address** 아래에서 가상 어플라이언스 관리 인터페이스의 MAC 주소를 수동으로 설정합니다.
- MAC 주소가 변경되거나 동적 풀의 다른 시스템과 충돌하지 않도록 MAC 주소를 가상 디바이스에 수동으로 할당합니다.
- 또한, 가상 방어 센터에서 MAC 주소를 수동으로 설정하면 어플라이언스를 이미지로 다시 설치해야 할 경우 Cisco에서 라이센스를 다시 요청하지 않아도 됩니다.
- **Network Connection** 아래에서 **Network label**을 가상 어플라이언스의 관리 네트워크 이름으로 설정합니다.

단계 5 **OK**를 클릭합니다.

변경 내용이 저장되었습니다.

단계 6 선택적으로, 어플라이언스의 전원을 켜기 전에 기본 e1000 인터페이스를 vnxnet3 인터페이스로 교체하거나, 추가 관리 인터페이스를 만들거나, 두 가지를 모두 수행합니다. 자세한 내용은 인터페이스 추가 및 구성, 페이지 4-10을(를) 참고하십시오.

단계 7 다음 단계는 설치한 어플라이언스 유형에 따라 달라집니다.

- 가상 방어 센터를 초기화할 준비가 되었습니다. 가상 어플라이언스 설정, 페이지 5-1을 계속 진행하십시오.
- 가상 디바이스에 몇 가지 추가 컨피그레이션이 필요합니다. 가상 디바이스 센싱 인터페이스 구성을 계속 진행하십시오.

인터페이스 추가 및 구성

모든 e1000 인터페이스를 삭제하고 이를 vmxnet3 인터페이스로 교체하여 기본 e1000(1Gbit/s) 인터페이스를 vmxnet3(10Gbit/s) 인터페이스로 교체할 수 있습니다.

구축 과정에서 인터페이스를 혼합할 수 있는 경우에도(예: 가상 방어 센터의 e1000 인터페이스 및 해당 관리되는 가상 디바이스의 vmxnet3 인터페이스) 동일한 어플라이언스에서 인터페이스를 혼합할 수 없습니다. 어플라이언스의 모든 센싱 및 관리 인터페이스는 동일해야 하며 e1000 또는 vmxnet3이어야 합니다.

e1000 인터페이스를 vmxnet3 인터페이스로 교체하려면 vSphere Client를 사용하여 우선 기존 e1000 인터페이스를 제거한 다음 새로운 vmxnet3 인터페이스를 추가하고 적절한 어댑터 유형 및 네트워크 연결을 선택합니다.

또한 동일한 가상 방어 센터에 두 번째 관리 인터페이스를 추가하여 두 개의 서로 다른 네트워크에서 트래픽을 별도로 관리할 수 있습니다. 추가 가상 스위치를 구성하여 두 번째 관리 인터페이스를 두 번째 네트워크의 관리되는 디바이스에 연결합니다. vSphere Client를 사용하여 두 번째 관리 인터페이스를 가상 어플라이언스에 추가합니다.

vSphere Client 사용에 대한 자세한 내용은 VMware 웹 사이트(http://vmware.com)를 참조하십시오. 복수 관리 인터페이스에 대한 자세한 내용은 FireSIGHT System 사용 설명서의 디바이스 관리를 참조하십시오.

정보 어플라이언스를 켜기 전에 인터페이스에 대한 모든 변경 사항을 적용합니다. 인터페이스를 변경하려면 어플라이언스 전원을 끈 다음 인터페이스를 삭제하고 새 인터페이스를 추가한 다음 어플라이언스 전원을 켜야 합니다.

가상 디바이스 센싱 인터페이스 구성

가상 디바이스의 센싱 인터페이스에는 프로미스큐어스 모드를 허용하는 ESXi 호스트 가상 스위치의 포트에 대한 네트워크 연결이 있어야 합니다.

정보 가상 스위치에 포트 그룹을 추가하여 운영 트래픽에서 프로미스큐어스 모드 가상 네트워크 연결을 격리합니다. 포트 그룹 추가 및 보안 속성 설정에 대한 자세한 내용은 VMWare 설명서를 참조하십시오.

프로미스큐어스 모드를 허용하려면 다음을 수행합니다.

단계 1 vSphere Client를 사용하여 서버에 로그인하고 서버의 **Configuration** 탭을 클릭합니다.

Hardware 및 **Software** 선택 목록이 나타납니다.

단계 2 **Hardware** 목록에서 **Networking**을 클릭합니다.

가상 스위치 다이어그램이 나타납니다.

단계 3 가상 디바이스의 센싱 인터페이스를 연결하는 스위치 및 포트 그룹에서 **Properties**를 클릭합니다.

Switch Properties 팝업 창이 나타납니다.

단계 4 **Switch Properties** 팝업 창에서 **Edit**를 클릭합니다.

Detailed Properties 팝업 창이 나타납니다.

단계 5 **Detailed Properties** 팝업 창에서 **Security** 탭을 선택합니다.

Policy Exceptions > Promiscuous Mode 아래에서 Promiscuous Mode가 **Accept**로 설정되어 있는지 확인합니다.

정보 가상 환경에서 VLAN 트래픽을 모니터링하려면 프로미스큐어스 포트의 VLAN ID를 4095로 설정합니다.

단계 6 변경 사항을 저장합니다.

디바이스를 초기화할 준비가 되었습니다.

단계 7 다음 장 가상 어플라이언스 설정, 페이지 5-1을 계속 진행하십시오.

가상 어플라이언스 제거

가상 어플라이언스를 제거해야 할 수 있습니다. 가상 어플라이언스를 종료한 다음 가상 어플라이언스를 삭제하여 제거합니다.

정보 가상 디바이스를 제거한 다음 반드시 센싱 연결 가상 스위치 포트 그룹을 기본 설정인 **Promiscuous Mode**: **Reject**로 복원하십시오. 자세한 내용은 가상 디바이스 센싱 인터페이스 구성, 페이지 4-10을(를) 참고하십시오.

가상 어플라이언스 종료

다음 절차에 따라 가상 어플라이언스를 올바르게 종료합니다.

가상 어플라이언스를 종료하려면 다음을 수행합니다.

단계 1 VMWare 콘솔에서 관리자(가상 디바이스의 경우 CLI Configuration) 권한이 있는 사용자로 로그인합니다. 가상 디바이스를 사용하는 경우 `expert`를 입력하여 셸 프롬프트를 표시합니다.

어플라이언스에 대한 프롬프트가 나타납니다.

단계 2 가상 어플라이언스를 종료합니다.

- 가상 방어 센터에서 `sudo shutdown -h now`를 입력합니다.
- 가상 디바이스에서 `system shutdown`을 입력합니다.

가상 어플라이언스가 종료됩니다.

가상 어플라이언스 삭제

가상 어플라이언스의 전원을 끈 다음 가상 어플라이언스를 삭제할 수 있습니다.

다음 절차에 따라 VMware vCloud Director에 구축된 가상 어플라이언스를 삭제합니다.

VMware vCloud Director 웹 포털을 사용하여 가상 어플라이언스를 삭제하려면 다음을 수행합니다.

단계 1 **My Cloud > vApps**를 선택하고 삭제하려는 vApp을 마우스 오른쪽 버튼으로 클릭한 다음 메뉴에서 **Delete**를 클릭하고 확인 팝업 창에서 **Yes**를 클릭합니다.

가상 어플라이언스가 제거됩니다.

다음 절차에 따라 VMware vCenter에 구축된 가상 어플라이언스를 삭제합니다.

vSphere Client를 사용하여 가상 어플라이언스를 삭제하려면 다음을 수행합니다.

단계 1 vSphere Client 컨텍스트 메뉴에서 어플라이언스 이름을 클릭하고, Inventory 메뉴를 사용하여 **Delete**를 클릭한 다음 확인 대화 상자에서 **Yes**를 클릭합니다.

가상 어플라이언스가 제거됩니다.

5장

가상 어플라이언스 설정

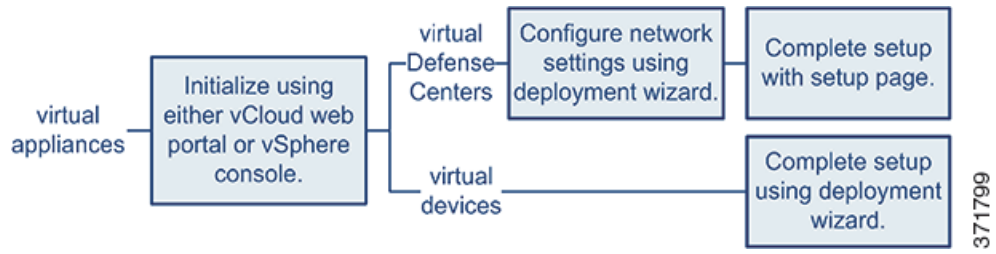
가상 어플라이언스를 설치한 다음 새 어플라이언스가 신뢰하는 관리 네트워크에서 통신할 수 있도록 설정 프로세스를 완료해야 합니다. 또한 관리자 비밀번호를 변경하고 최종 사용자 라이센스 계약(EULA)에 동의해야 합니다.

설정 프로세스에서는 시간 설정, 디바이스 등록 및 라이센싱, 업데이트 예약 등 관리 레벨의 많은 초기 작업을 실행할 수 있습니다. 설정 및 등록 과정에서 선택하는 옵션에 따라 기본 인터페이스, 인라인 세트, 영역, 시스템에서 생성하고 적용하는 정책이 결정됩니다.

이러한 초기 컨피그레이션 및 정책의 목적은 즉시 사용 가능한 환경을 제공하고 옵션을 제한하는 대신 구축을 빠르게 설정할 수 있도록 돕는 것입니다. 디바이스를 초기에 어떻게 구성하는지와 상관없이, 방어 센터를 사용하여 해당 컨피그레이션을 언제든지 변경할 수 있습니다. 예를 들어, 설정 중 탐지 모드 또는 액세스 제어 정책을 선택할 경우 반드시 특정 디바이스, 영역 또는 정책 컨피그레이션을 사용해야 하는 것은 아닙니다.

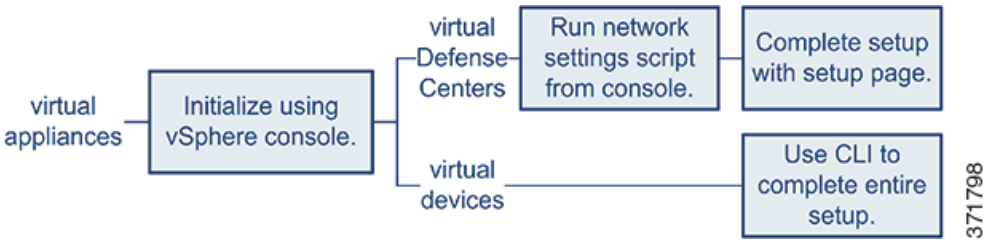
VI OVF 템플릿 구축

다음 다이어그램은 VI OVF 템플릿으로 구축하는 경우 가상 방어 센터 및 관리되는 디바이스를 설치하는 일반 프로세스입니다.



ESXi OVF 템플릿 구축

다음 다이어그램은 ESXi OVF 템플릿으로 구축할 경우 가상 방어 센터 및 관리되는 디바이스를 설정하는 일반 프로세스입니다.



구축 방법과 상관없이 어플라이언스 전원을 켜고 초기화하는 것으로 시작합니다. 초기화가 완료된 후 VMWare 콘솔을 사용하여 로그인하고 어플라이언스 유형에 따라 다음 중 한 가지 방법으로 설정을 완료합니다.

가상 디바이스

가상 디바이스에는 웹 인터페이스가 없습니다. VI OVF 템플릿으로 구축할 경우 구축 마법사를 사용하여 방어 센터에 등록하는 작업을 비롯한 디바이스의 초기 설정을 수행할 수 있습니다. ESXi OVF 템플릿으로 구축할 경우 대화형 CLI(Command Line Interface)를 사용하여 초기 설정을 수행해야 합니다.

가상 방어 센터

VI OVF 템플릿으로 구축할 경우 구축 시 마법사를 사용하여 네트워크 컨피그레이션을 수행할 수 있습니다. 설정 마법사를 사용하지 않거나 ESXi OVF 템플릿으로 구축할 경우 스크립트를 사용하여 네트워크 설정을 구성합니다. 네트워크를 구성한 후 관리 네트워크의 컴퓨터를 사용하여 설정 프로세스를 완료하고 방어 센터의 웹 인터페이스로 이동합니다.

정보 여러 어플라이언스를 구축하는 경우 우선 디바이스를 설정한 다음 이러한 디바이스를 관리하는 방어 센터를 설정합니다. 디바이스의 초기 설정 프로세스에서는 디바이스를 방어 센터에 사전 등록할 수 있으며, 방어 센터 설정 프로세스에서는 사전 등록된 관리되는 디바이스를 추가 및 라이센싱할 수 있습니다.

자세한 내용은 다음 링크를 참고하십시오.

- 가상 어플라이언스 초기화, 페이지 5-2
- CLI를 사용하여 가상 디바이스 설정, 페이지 5-3
- 가상 방어 센터 설정, 페이지 5-6
- VMWare Tools 활성화, 페이지 5-12
- 다음 단계, 페이지 5-13

가상 어플라이언스 초기화

가상 어플라이언스를 설치한 다음 처음으로 가상 어플라이언스의 전원을 켜면 초기화가 자동으로 시작됩니다.

주의 시작 시간은 서버 리소스 가용성을 포함한 여러 요소에 따라 달라집니다. 초기화가 완료될 때까지 최대 40분이 소요될 수 있습니다. 초기화를 중단하지 **마십시오**. 초기화를 중단할 경우 어플라이언스를 삭제하고 다시 시작해야 할 수 있습니다.

다음 절차를 사용하여 가상 어플라이언스를 초기화합니다.

가상 어플라이언스를 초기화하려면 다음을 수행합니다.

단계 1 어플라이언스의 전원을 켭니다.

- VMware vCloud Director 웹 포털에서 vApp을 선택한 다음 **Start**를 클릭합니다.
- vSphere Client의 인벤토리 목록에서 가져온 가상 어플라이언스의 이름을 마우스 오른쪽 버튼으로 클릭한 다음, 컨텍스트 메뉴에서 **Power > Power On**을 클릭합니다.

단계 2 VMWare 콘솔 탭에서 초기화를 모니터링합니다.

이 프로세스의 가장 긴 2개 부분에서 메시지가 나타납니다. 프로세스가 종료되면 로그인 프롬프트가 나타납니다.

다음 단계는 어플라이언스 유형 및 구축에 따라 다릅니다.

구축 과정에서 VI OVF 템플릿을 사용하고 FireSIGHT System의 필수 설정을 구성한 경우

- 가상 방어 센터의 경우 가상 방어 센터 설정, 페이지 5-6을 계속 진행하여 설정을 완료합니다.
- 가상 디바이스의 경우 추가 컨피그레이션이 필요하지 않습니다.

VI OVF 템플릿으로 구축할 때 ESXi OVF 템플릿을 사용했거나 FireSIGHT System의 필수 설정을 구성하지 않은 경우

- 가상 방어 센터의 경우 가상 방어 센터 설정, 페이지 5-6을 계속 진행하면서 스크립트를 사용하여 네트워크 설정을 구성함으로써 가상 방어 센터를 설정합니다.
- 가상 디바이스의 경우 CLI를 사용하여 가상 디바이스 설정, 페이지 5-3을 계속 진행하면서 CLI를 사용하여 가상 디바이스를 설정합니다.

CLI를 사용하여 가상 디바이스 설정

가상 디바이스에는 웹 인터페이스가 없으므로 ESXi OVF 템플릿으로 구축한 경우 CLI를 사용하여 가상 디바이스를 설정해야 합니다. 또한 구축 과정에서 VI OVF 템플릿으로 구축하고 설정 마법사를 사용하지 않은 경우에도 CLI를 사용하여 FireSIGHT System의 필수 설정을 구성해야 합니다.

정보 VI OVF 템플릿으로 구축하면서 설정 마법사를 사용한 경우, 가상 디바이스가 구성되어 있으며 추가 작업이 필요하지 않습니다.

새로 구성된 디바이스에 처음으로 로그인하면 EULA를 읽고 동의해야 합니다. 그런 다음 설정 프롬프트에 따라 관리자 비밀번호를 변경하고 디바이스의 네트워크 설정 및 탐지 모드를 구성합니다.

설정 프롬프트를 진행하는 동안 선택형 질문의 경우 `(y/n)`과 같이 선택 사항이 괄호 안에 나열됩니다. 기본값은 `[y]`와 같이 대괄호에 나열됩니다. Enter 키를 눌러 선택을 확인합니다.

CLI의 프롬프트에 입력해야 할 설정 정보는 물리적 디바이스의 설정 웹 페이지와 거의 동일합니다. 자세한 내용은 *FireSIGHT System 설치 가이드*를 참조하십시오.

정보 초기 설정을 완료한 후 가상 디바이스의 이러한 설정을 변경하려면 CLI를 사용해야 합니다. 자세한 내용은 *FireSIGHT System 사용 설명서*의 명령행 참조 장을 참조하십시오.

디바이스 네트워크 설정 이해

FireSIGHT System에서는 IPv4 및 IPv6 관리 환경을 모두 지원하는 이중 스택 구현을 제공합니다. IPv4 또는 IPv6 관리 IP 주소, 넷마스크 또는 접두사 길이, 기본 게이트웨이를 설정해야 합니다. 또한 최대 3개의 DNS 서버와 디바이스의 호스트 이름 및 도메인을 지정할 수 있습니다. 호스트 이름은 디바이스를 재부팅하기 전까지 syslog에 반영되지 않습니다.

탐지 모드 이해

가상 디바이스에 대해 선택하는 탐지 모드에 따라 시스템이 초기에 디바이스 인터페이스를 구성하는 방식 및 이러한 인터페이스가 인라인 세트 또는 보안 영역에 속하는지 여부가 결정됩니다. 탐지 모드는 나중에 변경할 수 있는 설정이 아니며 시스템이 디바이스의 초기 컨피그레이션을 맞춤 설정하는 데 도움이 되도록 설정 과정에서 선택하는 옵션에 불과합니다. 일반적으로, 디바이스가 구축된 방식을 기준으로 탐지 모드를 선택해야 합니다.

수동

디바이스가 IDS(Intrusion Detection System)로서 수동으로 구축된 경우 이 모드를 선택합니다. 수동 구축에서 가상 디바이스는 네트워크 기반 파일 및 악성코드 탐지, 보안 인텔리전스 모니터링, 네트워크 검색을 수행할 수 있습니다.

인라인

디바이스가 IPS(intrusion prevention system)로서 인라인으로 구축된 경우 이 모드를 선택합니다.

참고 IPS 구축은 일반적으로 Fail Open 및 일치하지 않는 트래픽을 허용하지만 가상 디바이스의 인라인 세트에는 바이패스 기능이 없습니다.

네트워크 검색

디바이스가 호스트, 애플리케이션, 사용자 검색만 수행하도록 수동으로 구축된 경우 이 모드를 선택합니다.

다음 표에는 사용자가 선택하는 탐지 모드에 따라 시스템에서 생성되는 인터페이스, 인라인 세트, 영역이 나와 있습니다.

표 5-1 탐지 모드 기반의 초기 컨피그레이션

탐지 모드	보안 영역	인라인 세트	인터페이스
인라인	내부 및 외부	기본 인라인 세트	첫 번째 쌍이 기본 인라인 세트에 추가됨(하나는 내부, 다른 하나는 외부 영역)
수동	수동	없음	첫 번째 쌍이 수동 영역에 할당됨
네트워크 검색	수동	없음	첫 번째 쌍이 수동 영역에 할당됨

보안 영역은 사용자가 실제로 디바이스를 방어 센터에 추가할 때까지 시스템에서 생성하지 않는 방어 센터 레벨의 컨피그레이션입니다. 이때 방어 센터에 이미 적절한 영역(내부, 외부, 수동)이 있는 경우 시스템에서는 나열된 인터페이스를 기존 영역에 추가합니다. 해당 영역이 없을 경우 시스템에서는 영역을 생성하고 인터페이스를 추가합니다. 인터페이스, 인라인 세트, 보안 영역에 대한 자세한 내용은 *FireSIGHT System 사용 설명서*를 참조하십시오.

CLI를 사용하여 가상 디바이스를 설정하려면 다음을 수행합니다.

액세스: Admin

단계 1 콘솔에서 사용자 이름으로 `admin`을 사용하고 구축 설정 마법사에서 지정한 새로운 관리자 계정 비밀번호를 사용하여 VMWare 가상 디바이스에 로그인합니다.

마법사를 사용하여 비밀번호를 변경하지 않은 경우 또는 ESXi OVF 템플릿으로 구축하는 경우 `Cisco`를 비밀번호로 사용합니다.

EULA를 읽으라는 메시지가 디바이스에 즉시 표시됩니다.

단계 2 EULA를 읽고 그 내용에 동의합니다.

단계 3 `admin` 계정의 비밀번호를 변경합니다. 이 계정은 컨피그레이션 CLI 액세스 레벨을 보유하며 삭제할 수 없습니다.

대문자, 소문자, 1개 이상의 숫자가 포함된 8자 이상의 영숫자로 만든 강력한 비밀번호를 사용하는 것이 좋습니다. 사전에 나오는 단어를 사용하지 마십시오.

단계 4 디바이스의 네트워크 설정을 구성합니다.

IPv4 및 IPv6 관리 설정을 차례로 구성(또는 비활성화)합니다. 네트워크 설정을 수동으로 지정할 경우 다음 작업을 수행해야 합니다.

- 넷마스크를 포함한 IPv4 주소를 점으로 구분된 10진수로 입력합니다. 예를 들어, 넷마스크로 `255.255.0.0`을 지정할 수 있습니다.
- IPv6 주소를 콜론으로 구분된 16진수 양식으로 입력합니다. IPv6 접두사의 경우 비트 수를 지정합니다. 예를 들어, 접두사 길이로 `112`를 입력합니다.

설정이 구현되면 VMWare 콘솔에 메시지가 표시될 수 있습니다.

단계 5 디바이스를 구축한 방식에 따라 탐지 모드를 지정합니다.

설정이 구현되면 VMWare 콘솔에 메시지가 표시될 수 있습니다. 완료되면 이 디바이스를 방어 센터에 등록하라는 알림이 디바이스에 나타나고 CLI 프롬프트가 표시됩니다.

단계 6 CLI를 사용하여 디바이스를 관리할 방어 센터에 해당 디바이스를 등록하려면 다음 섹션 가상 디바이스를 방어 센터에 등록, 페이지 5-5을 계속 진행하십시오.

방어 센터를 사용하여 디바이스를 관리해야 합니다. 지금 디바이스를 등록하지 않으면 나중에 방어 센터에 추가하기 전에 로그인하고 등록해야 합니다.

가상 디바이스를 방어 센터에 등록

가상 디바이스에는 웹 인터페이스가 없으므로 CLI를 사용하여 가상 디바이스를 물리적 또는 가상 방어 센터에 등록해야 합니다. 디바이스의 CLI에 이미 로그인되어 있으므로, 초기 설정 프로세스 중에 디바이스를 방어 센터에 등록하는 것이 가장 쉬운 방법입니다.

디바이스를 등록하려면 `configure manager add` 명령을 사용합니다. 디바이스를 방어 센터에 등록하려면 항상 자체 생성된 고유한 영숫자 등록 키가 필요합니다. 등록 키는 사용자가 지정할 수 있는 간단한 키이며, 라이센스 키와는 다릅니다.

대부분의 경우 등록 키와 함께 방어 센터의 IP 주소를 입력해야 합니다. 예를 들면 다음과 같습니다.

```
configure manager add XXX.XXX.XXX.XXX my_reg_key
```

여기서 *XXX.XXX.XXX.XXX*는 관리하는 방어 센터의 IP 주소이며 *my_reg_key*는 가상 디바이스에 입력한 등록 키입니다.

참고 vSphere Client를 사용하여 가상 디바이스를 방어 센터에 등록할 경우 관리하는 방어 센터의 IP 주소(호스트 이름이 아님)를 사용해야 합니다.

그러나 디바이스와 방어 센터가 NAT(Network Address Translation) 디바이스에 의해 분리되는 경우, 등록 키와 고유한 NAT ID를 입력하고 IP 주소 대신 `DONTRESOLVE`를 지정합니다. 예를 들면 다음과 같습니다.

```
configure manager add DONTRESOLVE my_reg_key my_nat_id
```

여기서 *my_reg_key*는 가상 디바이스에 입력한 등록 키이며 *my_nat_id* 는 NAT 디바이스의 NAT ID입니다.

가상 디바이스를 방어 센터에 등록하려면 다음을 수행합니다.

액세스: CLI 컨피그레이션

단계 1 CLI 컨피그레이션(관리자) 권한이 있는 사용자로 가상 디바이스에 로그인합니다.

- VMWare 콘솔에서 초기 설정을 수행 중인 경우, 필요한 액세스 레벨이 있는 `admin` 사용자로 이미 로그인되어 있습니다.
- 그렇지 않을 경우 VMWare 콘솔을 사용하여 디바이스에 로그인합니다. 디바이스의 네트워크 설정을 이미 구성한 경우에는 디바이스의 IP 주소 또는 호스트 이름으로 SSH를 통해 연결합니다.

단계 2 프롬프트에서 다음과 같은 구문의 `configure manager add` 명령을 사용하여 디바이스를 방어 센터에 등록합니다.

```
configure manager add {hostname | IPv4_address | IPv6_address | DONTRESOLVE} reg_key
[nat_id]
```

여기서 각 항목은 다음을 나타냅니다.

- {*hostname* | *IPv4_address* | *IPv6_address* | `DONTRESOLVE`}는 방어 센터의 IP 주소를 지정합니다. 방어 센터의 주소를 직접 지정할 수 없는 경우 `DONTRESOLVE`를 사용합니다.
- *reg_key*는 디바이스를 방어 센터에 등록하는 데 필요한 영숫자 등록 키입니다.
- *nat_id*는 방어 센터와 디바이스 간의 등록 프로세스 동안 사용되는 선택적인 영숫자 문자열입니다. 이 문자열은 호스트 이름이 `DONTRESOLVE`로 설정된 경우 필요합니다.

단계 3 어플라이언스에서 로그아웃합니다.

단계 4 다음 단계는 관리하는 방어 센터를 이미 설정했는지 여부와 방어 센터 모델에 따라 달라집니다.

- 이미 방어 센터를 설정한 경우 웹 인터페이스에 로그인하고 Device Management(**Devices > Device Management**) 페이지를 사용하여 디바이스를 추가합니다. 자세한 내용은 *FireSIGHT System 사용 설명서*의 디바이스 관리 장을 참조하십시오.
- 아직 방어 센터를 설정하지 않았다면 가상 방어 센터의 경우 가상 방어 센터 설정, 페이지 5-6을 참조하거나, 물리적 방어 센터의 경우 *FireSIGHT System 설치 가이드*를 참조하십시오.

가상 방어 센터 설정

가상 방어 센터를 설정하는 데 필요한 단계는 VI OVF 템플릿으로 구축했는지, ESXi OVF 템플릿으로 구축했는지에 따라 달라집니다.

- VI OVF 템플릿으로 구축하고 설정 마법사를 사용한 경우 FireSIGHT System의 필수 설정을 구성할 때 지정한 비밀번호를 사용하여 가상 방어 센터로 로그인한 다음 FireSIGHT System을 사용하여 로컬 어플라이언스 컨피그레이션을 설정하고 라이센스와 디바이스를 추가하며 트래픽을 모니터링 및 관리하기 위한 정책을 적용합니다. 자세한 내용은 *FireSIGHT System 사용 설명서*를 참조하십시오.
- ESXi OVF 템플릿을 구축했거나 VI OVF 템플릿 구축 시 FireSIGHT System의 필수 설정을 구성하지 않은 경우 가상 방어 센터 설정은 2단계 프로세스입니다. 가상 방어 센터를 초기화한 다음, 어플라이언스가 관리 네트워크에서 통신하도록 구성할 수 있는 VMWare 콘솔에서 스크립트를 실행합니다. 그런 다음 관리 네트워크에서 컴퓨터를 사용하여 설정 프로세스를 완료하고 어플라이언스의 웹 인터페이스를 탐색합니다.
- ESXi OVF 템플릿으로 가상 방어 센터를 구축하고 VI OVF 템플릿으로 모든 가상 디바이스를 구축한 경우 한 페이지 설정 마법사를 통해 가상 방어 센터에 모든 디바이스를 동시에 등록할 수 있습니다. 자세한 내용은 초기 설정 페이지: 가상 방어 센터, 페이지 5-8을/를 참조하십시오.

자세한 내용은 다음 링크를 참고하십시오.

- 가상 방어 센터 네트워크 설정 자동화, 페이지 5-7
- 초기 설정 페이지: 가상 방어 센터, 페이지 5-8

가상 방어 센터 네트워크 설정 자동화

새로운 가상 방어 센터를 초기화한 다음, 어플라이언스가 관리 네트워크에서 통신하도록 하는 설정을 구성해야 합니다. VMWare 콘솔에서 스크립트를 실행하여 이 단계를 완료합니다.

FireSIGHT System에서는 IPv4 및 IPv6 관리 환경을 모두 지원하는 이중 스택 구현을 제공합니다. 스크립트에서 IPv4 관리 설정을 구성(또는 비활성화)한 다음 IPv6 관리 설정을 구성하라는 메시지가 차례로 표시됩니다. IPv6 구축의 경우 로컬 라우터에서 설정을 검색할 수 있습니다. IPv4 또는 IPv6 관리 IP 주소, 넷마스크 또는 접두사 길이, 기본 게이트웨이를 입력해야 합니다.

스크립트의 프롬프트를 진행하는 동안 선택형 질문의 경우 `(y/n)`과 같이 선택 사항이 괄호 안에 나열됩니다. 기본값은 `[y]`와 같이 대괄호에 나열됩니다. Enter 키를 눌러 선택을 확인합니다.

스크립트를 사용하여 방어 센터의 네트워크 설정을 구성하려면 다음을 수행합니다.

액세스: Admin

단계 1 초기화 프로세스가 완료되면 VMWare 콘솔에서 사용자 이름으로 `admin`을 사용하고 VI OVF 템플릿으로 구축할 때 설정 마법사에서 지정한 관리자 어카운트에 지정한 비밀번호를 사용하여 가상 방어 센터에 로그인합니다.

마법사를 사용하여 비밀번호를 변경하지 않은 경우 또는 ESXi OVF 템플릿으로 구축하는 경우 `Cisco`를 비밀번호로 사용합니다.

단계 2 admin 프롬프트에서 다음 스크립트를 실행합니다.

```
sudo /usr/local/sf/bin/configure-network
```

단계 3 스크립트의 프롬프트를 따릅니다.

IPv4 및 IPv6 관리 설정을 차례로 구성(또는 비활성화)합니다. 네트워크 설정을 수동으로 지정할 경우 다음 작업을 수행해야 합니다.

- 넷마스크를 포함한 IPv4 주소를 점으로 구분된 10진수로 입력합니다. 예를 들어, 넷마스크로 `255.255.0.0`을 지정할 수 있습니다.
- IPv6 주소를 콜론으로 구분된 16진수 양식으로 입력합니다. IPv6 접두사의 경우 비트 수를 지정합니다. 예를 들어, 접두사 길이로 `112`를 입력합니다.

단계 4 설정이 올바른지 확인합니다.

설정을 잘못 입력한 경우 프롬프트에서 `n`을 입력하고 Enter 키를 누릅니다. 그런 다음 올바른 정보를 입력할 수 있습니다. 설정이 구현되면 VMWare 콘솔에 메시지가 표시될 수 있습니다.

단계 5 어플라이언스에서 로그아웃합니다.

단계 6 초기 설정 페이지: 가상 방어 센터, 페이지 5-8를 계속 진행하고 방어 센터의 웹 인터페이스를 사용하여 설정을 완료합니다.

초기 설정 페이지: 가상 방어 센터

가상 방어 센터의 경우, 방어 센터의 웹 인터페이스에 로그인하고 설정 페이지에서 초기 컨피그레이션 옵션을 지정하여 설정 프로세스를 완료해야 합니다. 관리자 비밀번호를 변경하고, 네트워크 설정을 지정한 다음(아직 지정하지 않은 경우), EULA에 동의해야 합니다.

설정 프로세스에서는 디바이스를 등록 및 라이센싱할 수도 있습니다. 디바이스를 등록하기 전에 디바이스 자체에서 설정 프로세스를 완료하고 방어 센터를 원격 관리자로 추가해야 하며, 그렇지 않을 경우 등록이 실패합니다.

웹 인터페이스를 사용하여 방어 센터에서 초기 설정을 완료하려면 다음을 수행합니다.

액세스: Admin

단계 1 관리 네트워크의 컴퓨터에서 지원되는 브라우저의 주소 표시줄에 `https://DC_name/`을 입력합니다. 여기서 *DC_name*은 이전 절차에서 방어 센터의 관리 인터페이스에 할당한 호스트 이름 또는 IP 주소입니다.

로그인 페이지가 나타납니다.

단계 2 사용자 이름으로 `admin`을 사용하고 VI OVF 템플릿 구축 시 설정 마법사에서 지정한 관리자 계정의 비밀번호를 사용하여 로그인합니다. 마법사를 사용하여 비밀번호를 변경하지 않은 경우 `Cisco`를 비밀번호로 사용합니다.

설정 페이지가 표시됩니다. 설정 완료에 대한 자세한 내용은 다음 섹션을 참조하십시오.

- 비밀번호 변경, 페이지 5-9
- 네트워크 설정, 페이지 5-9
- 시간 설정, 페이지 5-9
- 반복 규칙 업데이트 가져오기, 페이지 5-9
- 반복 위치 업데이트, 페이지 5-10
- 자동 백업, 페이지 5-10
- 라이센스 설정, 페이지 5-10
- 디바이스 등록, 페이지 5-11
- VMWare Tools 활성화, 페이지 5-12
- 최종 사용자 라이센스 계약, 페이지 5-12

단계 3 완료되면 **Apply**를 클릭합니다.

선택 사항에 따라 방어 센터가 구성됩니다. 중간 페이지가 나타나면 관리자 역할이 있는 `admin` 사용자로 웹 인터페이스에 로그인된 것입니다.

단계 4 Task Status 페이지(**System > Monitoring > Task Status**)를 사용하여 초기 설정이 성공적인지 확인합니다.

페이지가 10초마다 자동으로 새로 고쳐집니다. 초기 디바이스 등록 및 정책 적용 작업에 대해 **Completed**가 표시될 때까지 페이지를 모니터링합니다. 설정 과정에서 침입 규칙 또는 위치 업데이트를 구성한 경우 해당 작업도 모니터링할 수 있습니다.

방어 센터를 사용할 준비가 되었습니다. 구축 구성에 대한 자세한 내용은 *FireSIGHT System 사용 설명서*를 참조하십시오.

단계 5 다음 단계, 페이지 5-13를 계속 진행합니다.

비밀번호 변경

admin 계정의 비밀번호를 변경해야 합니다. 이 계정에는 관리자 권한이 있으며 삭제할 수 없습니다. 대문자, 소문자, 1개 이상의 숫자가 포함된 8자 이상의 영숫자로 만든 강력한 비밀번호를 사용하는 것이 좋습니다. 사전에 나오는 단어를 사용하지 마십시오.

네트워크 설정

방어 센터의 네트워크 설정을 사용하면 관리 네트워크에서 통신할 수 있습니다. 이미 스크립트를 사용하여 네트워크 설정을 구성했으므로 이 페이지의 섹션은 미리 채워져 있습니다.

미리 채워진 설정을 변경하려는 경우 FireSIGHT System에서 IPv4 및 IPv6 관리 환경 모두에 대한 이중 스택 구현을 제공하는 점을 기억하십시오. 관리 네트워크 프로토콜(**IPv4**, **IPv6** 또는 **둘 다**)을 지정해야 합니다. 선택 사항에 따라, 설정 페이지에 IPv4 또는 IPv6 관리 IP 주소, 넷마스크 또는 접두사 길이, 기본 게이트웨이를 설정해야 하는 다양한 필드가 표시됩니다.

- IPv4의 경우 주소와 넷마스크를 점으로 구분된 10진수 형식으로 설정해야 합니다(예: 넷마스크 255.255.0.0).
- IPv6 넷마스크의 경우 **Assign the IPv6 address using router autoconfiguration** 확인란을 선택하여 IPv6 네트워크 설정을 자동으로 할당할 수 있습니다. 그렇지 않을 경우 콜론으로 구분된 16진수 형식의 주소와 접두사의 비트 수를 설정해야 합니다(예: 접두사 길이 112).

또한 최대 3개의 DNS 서버와 디바이스의 호스트 이름 및 도메인을 지정할 수 있습니다.

시간 설정

방어 센터 시간을 수동으로 설정하거나 NTP 서버의 NTP(Network Time Protocol)를 통해 설정할 수 있습니다.

또한 admin 계정의 로컬 웹 인터페이스에 사용되는 시간대를 지정할 수 있습니다. 팝업 창을 사용하여 변경할 현재 시간대를 클릭합니다.

물리적 NTP 서버를 사용하여 시간을 설정하는 것이 좋습니다.

반복 규칙 업데이트 가져오기

새로운 취약성이 알려지면 Cisco VRT(Vulnerability Research Team)에서 침입 규칙 업데이트를 릴리스합니다. 규칙 업데이트는 업데이트된 새로운 침입 규칙과 프리프로세서 규칙, 기존 규칙의 수정된 상태, 수정된 기본 침입 정책 설정을 제공합니다. 또한 규칙 업데이트는 규칙을 삭제하고 새로운 규칙 범주 및 시스템 변수를 제공할 수 있습니다.

구축 과정에서 침입 탐지 및 방지를 수행하려는 경우 **Enable Recurring Rule Update Imports**를 수행하는 것이 좋습니다.

Import Frequency를 지정하고 규칙이 업데이트될 때마다 침입 **Policy Reapply**를 수행하도록 시스템을 구성할 수 있습니다. 초기 컨피그레이션 프로세스에서 규칙 업데이트를 수행하려면 **Install Now**를 선택합니다.

참고 규칙 업데이트에는 새로운 이진수가 포함될 수 있습니다. 규칙 업데이트를 다운로드 및 설치하는 과정에서 보안 정책을 준수하는지 확인해야 합니다. 또한 규칙 업데이트 규모가 클 수 있으므로 네트워크 이용률이 낮은 시간 동안 규칙을 가져오십시오.

반복 위치 업데이트

가상 방어 센터를 사용하여 시스템에서 생성한 이벤트와 관련 있는 라우팅된 IP 주소에 대한 위치 정보를 보고 대시보드 및 Context Explorer에서 위치 통계를 모니터링할 수 있습니다.

방어 센터의 위치 데이터베이스(GeoDB)에는 IP 주소의 관련 ISP(Internet Service Provider), 연결 유형, 프록시 정보, 정확한 위치 등의 정보가 포함됩니다. 일반 GeoDB 업데이트를 활성화할 경우 시스템에서는 최신 위치 정보를 사용합니다. 구축 과정에서 위치 관련 분석을 수행하려는 경우 **Enable Recurring Weekly Updates**를 수행하는 것이 좋습니다.

GeoDB의 주간 업데이트 빈도를 지정할 수 있습니다. 팝업 창을 사용하여 변경할 현재 시간대를 클릭합니다. 초기 컨피그레이션 프로세스에서 데이터베이스를 다운로드하려면 **Install Now**를 선택합니다.

참고 GeoDB 업데이트는 규모가 클 수 있으며 다운로드 후 설치까지 최대 45분이 소요될 수 있습니다. GeoDB는 네트워크 이용률이 낮은 시간 동안 업데이트해야 합니다.

자동 백업

방어 센터에서는 장애 발생 시 컨피그레이션을 복원할 수 있는 데이터 아카이브 메커니즘을 제공합니다. 초기 설정 과정에서 **Enable Automatic Backups**를 수행할 수 있습니다.

이 설정을 활성화하면 방어 센터의 컨피그레이션을 매주 백업하는 예약 작업을 만들 수 있습니다.

라이센스 설정

다양한 기능의 라이센스를 취득하여 조직에 최적의 FireSIGHT System 구축을 조성할 수 있습니다. 호스트, 애플리케이션, 사용자 검색을 수행하려면 방어 센터의 FireSIGHT 라이센스가 필요합니다. 추가 모델별 라이센스를 사용하면 관리되는 디바이스로 다음과 같이 다양한 기능을 수행할 수 있습니다. 아키텍처 및 리소스 제한으로 인해, 모든 라이센스를 모든 관리되는 디바이스에 적용할 수는 없습니다. 가상 어플라이언스 기능 이해, 페이지 1-3 및 가상 어플라이언스 라이센싱, 페이지 1-11을 참조하십시오.

초기 설정 페이지를 사용하여 조직에서 구입한 라이센스를 추가하는 것이 좋습니다. 지금 라이센스를 추가하지 않을 경우 초기 설정 중 등록하는 디바이스는 라이센스 없이 방어 센터에 추가됩니다. 그런 다음 초기 설정 프로세스가 완료되면 각각의 디바이스를 개별적으로 라이센싱해야 합니다.

정보 가상 방어 센터를 다시 만들었으며 삭제된 어플라이언스와 동일한 MAC 주소를 관리 인터페이스에 사용한 경우 기존 라이센스를 사용할 수 있습니다. 동일한 MAC 주소를 사용할 수 없는 경우(예: 동적으로 할당된 경우) 고객 지원에 문의하여 새 라이센스를 받으십시오.

라이센스를 아직 받지 못한 경우 `https://keyserver.sourcefire.com/` 링크를 클릭하여 이동한 다음 화면의 지침을 따르십시오. 라이센스 키(초기 설정 페이지에 나열됨) 및 활성화 키(지원 계약과 연결된 연락처로 이메일을 통해 이전에 제공됨)가 필요합니다.

라이센스를 텍스트 상자에 붙여넣어 추가하고 **Submit License**를 클릭합니다. 유효한 라이센스를 추가하면 페이지가 업데이트되고 추가한 라이센스를 추적할 수 있습니다. 라이센스를 한 번에 하나씩 추가하십시오.

디바이스 등록

가상 방어 센터에서는 FireSIGHT System에서 지원하는 모든 가상 또는 물리적 디바이스를 관리할 수 있습니다. 초기 설정 프로세스 중 대부분의 사전 등록된 디바이스를 방어 센터에 추가할 수 있습니다. 그러나 디바이스와 방어 센터가 NAT 디바이스에 의해 분리되는 경우 설정 프로세스가 완료된 후에 추가해야 합니다.

관리된 디바이스를 방어 센터에 등록할 때 등록된 디바이스에 액세스 제어 정책을 적용하려면 **Apply Default Access Control Policies** 확인란을 활성화된 상태로 둡니다. 방어 센터에서 각 디바이스에 어떤 정책을 적용하는지는 선택할 수 없으며, 적용 여부만 선택할 수 있습니다. 각 디바이스에 적용되는 정책은 다음 표와 같이 디바이스를 구성할 때 선택한 탐지 모드에 따라 달라집니다.

표 5-2 탐지 모드별로 적용되는 기본 액세스 제어 정책

탐지 모드	기본 액세스 제어 정책
인라인	기본 침입 방지
수동	기본 침입 방지
액세스 제어	기본 액세스 제어
네트워크 검색	기본 네트워크 검색

이전에 디바이스를 방어 센터로 관리하면서 디바이스의 초기 인터페이스 컨피그레이션을 변경한 경우 예외가 발생합니다. 이 경우 이 새로운 방어 센터 페이지에서 적용하는 정책은 디바이스의 변경된 (현재) 컨피그레이션에 따라 다릅니다. 구성된 인터페이스가 있는 경우 방어 센터에서는 기본 침입 방지 정책을 적용합니다. 그렇지 않을 경우 방어 센터에서는 기본 액세스 제어 정책을 적용합니다.

가상 디바이스의 탐지 모드에 대한 자세한 내용은 CLI를 사용하여 가상 디바이스 설정, 페이지 5-3을 참조하십시오. 물리적 디바이스의 경우 *FireSIGHT System 설치 가이드*를 참조하십시오.

참고 디바이스가 액세스 제어 정책과 호환되지 않을 경우 정책 적용이 실패합니다. 이러한 문제는 라이센싱 불일치, 모델 제약 조건, 수동 대 인라인 문제, 기타 잘못된 컨피그레이션을 비롯한 여러 가지 이유로 인해 발생할 수 있습니다. 초기 액세스 제어 정책 적용이 실패하면 초기 네트워크 검색 정책 적용도 실패합니다. 오류를 일으킨 문제를 해결한 후에는 액세스 제어 및 네트워크 검색 정책을 디바이스에 수동으로 적용해야 합니다. 액세스 제어 정책 적용의 실패를 일으키는 문제에 대한 자세한 내용은 *FireSIGHT System 사용 설명서*를 참조하십시오.

디바이스를 추가하려면 **Hostname** 또는 **IP Address**, 그리고 디바이스를 등록할 때 지정한 **Registration Key**를 입력합니다. 등록 키는 사용자가 지정한 간단한 키이며, 라이센스 키와는 다릅니다.

그런 다음 확인란을 사용하여 디바이스에 라이센스된 기능을 추가합니다. 방어 센터에 이미 추가된 라이센스만 선택할 수 있습니다. 또한 특정 라이센스의 경우 다른 라이센스를 활성화하기 전에는 활성화할 수 없습니다. 예를 들어, 보호을 활성화하기 전까지 디바이스에서 을 활성화할 수 없습니다.제어

아키텍처 및 리소스 제한으로 인해, 모든 라이센스가 모든 관리되는 디바이스에서 지원되지는 않습니다. 그러나 설정 페이지에서는 관리되는 디바이스에서 지원되지 않는 라이센스를 활성화하는 것을 차단하지 **않습니다**. 그 이유는 방어 센터에서 아직 디바이스 모델을 확인하지 않았기 때문입니다. 시스템에서는 유효하지 않은 라이센스를 활성화할 수 없으며, 유효하지 않은 라이센스를 활성화하려고 시도할 경우 사용 가능한 라이센스 수가 줄어들지 않습니다. 자세한 내용은 가상 어플라이언스 기능 이해, 페이지 1-3 및 가상 어플라이언스 라이센싱, 페이지 1-11을 참조하십시오.

라이센스를 활성화한 후 **Add**를 클릭하여 디바이스의 등록 설정을 저장하고, 선택적으로 디바이스를 추가합니다. 잘못된 옵션을 선택했거나 디바이스 이름을 잘못 입력한 경우 **Delete**를 클릭하여 제거합니다. 그런 다음 디바이스를 다시 추가할 수 있습니다.

최종 사용자 라이센스 계약

EULA를 주의하여 읽고 조항을 준수하는 것에 동의할 경우 확인란을 선택합니다. 입력한 모든 정보가 올바른지 확인하고 **Apply**를 클릭합니다.

선택 사항에 따라 방어 센터가 구성됩니다. 중간 페이지가 나타나면 관리자 역할이 있는 `admin` 사용자로 웹 인터페이스에 로그인된 것입니다. 초기 설정 페이지: 가상 방어 센터, 페이지 5-8의 3단계를 계속 진행하여 방어 센터의 초기 설정을 완료합니다.

VMWare Tools 활성화

VMWare Tools는 가상 머신의 운영 체제에 설치하여 가상 머신의 성능을 향상하고 VMWare 제품의 다양한 사용 편의성 기능을 지원하기 위해 설치하는 유틸리티 모음입니다. 다음 플러그인은 모든 가상 어플라이언스에서 지원됩니다.

- guestInfo
- powerOps
- timeSync
- vmbackup

지원되는 플러그인 및 VMWare Tools의 전체 기능에 대한 자세한 내용은 VMWare 웹사이트(http://www.vmware.com/)를 참조하십시오.

가상 어플라이언스를 설정한 다음 관리되는 디바이스에서 CLI(Command Line Interface)를 사용하거나 가상 방어 센터에서 브라우저를 사용하여 가상 어플라이언스에서 VMWare Tools를 활성화할 수 있습니다. 자세한 내용은 다음 섹션을 참조하십시오.

- 가상 디바이스에서 VMWare Tools 구성, 페이지 5-12
- 가상 방어 센터에서 VMWare Tools 구성, 페이지 5-13

가상 디바이스에서 VMWare Tools 구성

가상 디바이스에 로그인하고 다음 중 한 가지 명령을 입력합니다.

- `show vmware-tools`는 VMWare Tools가 시스템에서 실행 중인지를 나타냅니다.
- `configure vmware-tools enable` </code>는 가상 디바이스에서 VMWare Tools를 활성화합니다.
- `configure vmware-tools disable`은 가상 디바이스에서 VMWare Tools를 비활성화합니다.

가상 디바이스에서 VMWare Tools를 활성화하려면 다음을 수행합니다.

액세스: Admin

단계 1 콘솔에서 가상 디바이스에 로그인한 다음, CLI 프롬프트에서 VMWare Tools를 활성화/비활성화하거나 VMWare Tools가 활성화되었는지 여부를 표시하기 위한 적절한 명령을 입력하고 **Enter** 키를 누릅니다.

VMWare Tools가 실행 중인지, 활성화되었는지 또는 비활성화되었는지를 나타내는 메시지가 나타납니다.

가상 방어 센터에서 VMWare Tools 구성

웹 인터페이스를 사용하여 Configuration 메뉴에서 확인란을 선택하거나 취소할 수 있습니다. CLI를 사용하여 가상 방어 센터에서 VMWare Tools를 활성화할 수 없습니다.

가상 방어 센터에서 VMWare Tools를 활성화 또는 비활성화하려면 다음을 수행합니다.

액세스: Admin

단계 1 웹 브라우저를 사용하여 방어 센터에 로그인하고 **System > Local > Configuration > VMWare Tools**를 선택한 다음 **Enable VMWare Tools** 확인란을 선택 또는 취소하고 **Save**를 클릭합니다.

변경 사항이 적용되었음을 알리는 메시지가 나타납니다.

다음 단계

가상 어플라이언스의 초기 설정 프로세스를 마치고 성공적인지 확인한 다음 구축을 쉽게 관리할 수 있는 다양한 관리 작업을 완료하는 것이 좋습니다. 또한 디바이스 등록, 라이센싱과 같이 초기 설정 중 생략한 작업을 완료해야 합니다. 다음 섹션에서 설명하는 작업 및 구축을 구성하기 시작하는 방법에 대한 자세한 내용은 *FireSIGHT System 사용 설명서*를 참조하십시오.

개별 사용자 계정

초기 설정을 완료하면 시스템에는 관리자 역할 및 액세스 권한을 가진 `admin` 사용자 한 명만 있게 됩니다. 이 역할의 사용자는 셸 또는 CLI를 포하여 전체 시스템 메뉴 및 컨피그레이션에 액세스할 수 있습니다. 보안 및 감사 이유로 `admin` 계정(및 관리자 역할)의 사용을 제한하는 것이 좋습니다.

시스템을 사용할 각 사용자에 대해 별도의 계정을 만들 경우, 조직이 각 사용자의 작업과 각 사용자에 의한 변경 사항을 감사할 수 있을 뿐만 아니라 각 사용자와 관련된 사용자 액세스 역할을 제한할 수 있습니다. 이러한 조치는 대부분의 컨피그레이션 및 분석 작업을 수행하는 방어 센터에서 특히 중요합니다. 예를 들어, 분석가는 네트워크 보안을 분석하기 위해 이벤트 데이터에 대한 액세스가 필요할 수 있지만 구축 관리 기능에는 액세스가 필요하지 않을 수 있습니다.

시스템에는 다양한 관리자 및 분석가에게 맞게 설계된 10개의 사전 정의 사용자 역할이 포함되어 있습니다. 또한 특수 액세스 권한의 맞춤형 사용자 역할을 생성할 수도 있습니다.

상태 및 시스템 정책

기본적으로, 모든 어플라이언스에는 초기 시스템 정책이 적용되어 있습니다. 시스템 정책은 메일 릴레이 호스트 기본 설정, 시간 동기화 설정 등 구축의 여러 어플라이언스에서 유사할 수 있는 설정을 관리합니다. 방어 센터 자체와 여기에서 관리하는 모든 디바이스에 동일한 시스템 정책을 적용하는 것이 좋습니다.

기본적으로, 방어 센터에도 상태 정책이 적용되어 있습니다. 상태 정책은 상태 모니터링 기능에 포함되어 있으며 구축된 어플라이언스의 성능을 지속적으로 모니터링하는 기준을 제공합니다. 방어 센터를 사용하여 여기에서 관리하는 모든 디바이스에 상태 정책을 적용하는 것이 좋습니다.

소프트웨어 및 데이터베이스 업데이트

구축을 시작하기 전에 어플라이언스에서 시스템 소프트웨어를 업데이트해야 합니다. 구축된 모든 어플라이언스에서 최신 버전의 FireSIGHT System을 실행하는 것이 좋습니다. 구축 시 최신 버전을 사용하고 있는 경우 최신 침입 규칙 업데이트, VDB, GeoDB도 설치해야 합니다.

주의 FireSIGHT System의 일부를 업데이트하기 전에 업데이트에 포함된 릴리스 노트 또는 권고 문구를 **반드시** 읽어야 합니다. 릴리스 노트에서는 지원되는 플랫폼, 호환성, 전제 조건, 경고, 특정 설치 및 제거 지침과 같은 중요 정보를 제공합니다.

가상 어플라이언스 구축 문제 해결

이 장에서는 가장 일반적인 설정 문제에 대해 알아보고, 질문을 제출하거나 지원을 받는 방법에 대해 설명합니다.

시간 동기화

상태 모니터에 가상 어플라이언스의 클록 설정이 동기화되지 않은 것으로 표시될 경우 시스템 정책 시간 동기화 설정을 확인하십시오. 가상 어플라이언스는 물리적 NTP 서버와 동기화하는 것이 좋습니다. 관리되는 디바이스(가상 또는 물리적)를 가상 방어 센터에 동기화하지 마십시오. 시간 동기화가 올바르게 설정되었는지 확인하려면 *FireSIGHT System 사용 설명서*에서 시간 동기화를 참조하십시오. 가상 어플라이언스의 클록 설정이 올바른지 확인한 다음 ESXi 호스트 관리자에게 문의하여 서버의 시간 컨피그레이션이 올바른지 확인하십시오.

성능 문제

성능 문제가 발생할 경우, 가상 어플라이언스에 영향을 미치는 요소에는 여러 가지가 있습니다. 성능에 영향을 미칠 수 있는 요소 목록은 가상 어플라이언스 성능, 페이지 1-7을 참조하십시오. ESXi 호스트 성능을 모니터링하려는 경우 vSphere Client 및 **Performance** 탭 아래에 있는 정보를 사용할 수 있습니다.

연결 문제

VMware vCloud Director 웹 포털 및 vSphere Client를 사용하여 관리 및 센싱 인터페이스의 연결을 보고 확인할 수 있습니다.

VMware vCloud Director 웹 포털 사용

VMware vCloud Director 웹 포털을 사용하여 관리 연결 및 센싱 인터페이스가 올바르게 연결되었는지 알아보고 확인할 수 있습니다.

연결을 확인하려면 다음을 수행합니다.

단계 1 **My Cloud > VMs**를 선택하고 보려는 가상 어플라이언스에 커서를 올려놓은 다음 마우스 오른쪽 버튼으로 클릭합니다.

Actions 창이 나타납니다.

단계 2 Actions 창에서 **Properties**를 클릭합니다.

Virtual Machine Properties 창이 나타납니다.

단계 3 **Hardware** 탭에서 관리 및 센싱 인터페이스의 NIC를 보고 연결을 확인합니다.

vSphere Client 사용

vSphere Client를 사용하여 관리 연결 및 센싱 인터페이스가 올바르게 연결되었는지 확인할 수 있습니다.

관리 연결

초기 설정 중에는 전원을 켤 때 네트워크 어댑터가 연결되는지 확인하는 것이 중요합니다. 그렇지 않을 경우 초기 관리 연결 설정이 올바르게 완료되지 않으며, 다음과 같은 메시지와 함께 종료됩니다.

```
ADDRCONF (NETDEV_UP): eth0 : link is not ready
```

관리 연결이 설정되었는지 확인하려면 다음을 수행합니다.

단계 1 vSphere Client에서 가상 어플라이언스의 이름을 마우스 오른쪽 버튼으로 클릭하고 표시되는 컨텍스트 메뉴에서 **Edit Settings**를 선택합니다. **Hardware** 목록에서 **Network adapter 1**을 선택하고 **Connect at power on** 확인란이 선택되었는지 확인합니다.

초기 관리 연결이 올바르게 완료되면 다음 메시지에서 `/var/log/messages` 디렉토리를 확인합니다.

```
ADDRCONF (NETDEV_CHANGE): eth0 : link becomes ready
```

센싱 인터페이스

초기 설정 중에는 전원을 켤 때 센싱 인터페이스가 연결되는지 확인하는 것이 중요합니다.

전원을 켤 때 센싱 인터페이스가 연결되는지 확인하려면 다음을 수행합니다.

단계 1 vSphere Client에서 가상 디바이스의 이름을 마우스 오른쪽 버튼으로 클릭하고 표시되는 컨텍스트 메뉴에서 **Edit Settings**를 선택합니다. **Hardware** 목록에서 **Network adapter 2** 및 **Network adapter 3**를 선택합니다. 사용 중인 각 어댑터에 **Connect at power on** 확인란이 선택되었는지 확인합니다.

가상 디바이스 센싱 인터페이스는 프로미스큐어스 모드 트래픽을 허용하는 가상 스위치 또는 가상 스위치 그룹에 연결해야 합니다. 그렇지 않을 경우 디바이스가 브로드캐스트 트래픽만 탐지할 수 있습니다. 센싱 인터페이스가 모든 악성코드를 탐지하는지 확인하려면 가상 디바이스 센싱 인터페이스 구성, 페이지 4-10을 참조하십시오.

인라인 인터페이스 컨피그레이션

인라인 인터페이스가 대칭적인지, 그리고 인터페이스 간에 트래픽이 이동하는지 확인할 수 있습니다. VMWare 콘솔을 가상 디바이스로 열려면 VMware vCloud Director 웹 포털 또는 vSphere Client를 사용합니다.

인라인 센싱 인터페이스가 올바르게 구성되었는지 확인하려면 다음을 수행합니다.

액세스: CLI 컨피그레이션

단계 1 콘솔에서 CLI 컨피그레이션(관리자) 권한이 있는 사용자로 로그인합니다.

CLI 프롬프트가 나타납니다.

단계 2 `expert`를 입력하여 셸 프롬프트를 표시합니다.

단계 3 `cat /proc/sf/sfe1000.*` 명령을 입력합니다.

다음 예와 유사한 정보가 포함된 텍스트 파일이 나타납니다.

```
SFE1000 driver for eth1 is Fast, has link, is bridging, not MAC filtering, MAC timeout
7500, Max Latency 0.
  39625470 packets received.
         0 packets dropped by user.
  13075508 packets sent.
0 Mode 1 LB Total 0 Bit 000...
.
.
SFE1000 driver for eth2 is Fast, has link, is bridging, not MAC filtering, MAC timeout
7500, Max Latency 0.
  13075508 packets received.
         0 packets dropped by user.
  39625470 packets sent.
0 Mode 1 LB Total 0 Bit 00
```

`eth1`에서 수신한 패킷 수는 `eth2`에서 전송한 패킷 수와 일치하며 `eth1`에서 전송한 패킷 수는 `eth2`에서 수신한 패킷 수와 일치합니다.

단계 4 가상 디바이스에서 로그아웃합니다.

단계 5 선택적으로, 보호된 도메인에 대한 직접 라우팅이 지원되는 경우 가상 디바이스의 인라인 인터페이스가 연결되어 있는 보호된 가상 어플라이언스에 대해 ping을 수행합니다.

Ping이 반환되면 가상 디바이스의 인라인 인터페이스 세트를 통해 연결이 설정된 것입니다.

지원이 필요할 경우

Cisco 제품을 사용해 주셔서 감사합니다.

Sourcefire 지원

FireSIGHT 가상 디바이스 또는 가상 방어 센터에 대해 질문이 있거나 지원이 필요한 경우 Sourcefire 지원으로 문의하시기 바랍니다.

- Sourcefire 지원 사이트 방문(https://support.sourcefire.com/)
- Sourcefire 지원에 이메일 전송(support@sourcefire.com).
- Sourcefire 지원에 전화로 문의(1.410.423.1901 또는 1.800.917.4134)

시스코 지원

Cisco ASA 어플라이언스에 대해 궁금한 사항이 있거나 지원이 필요한 경우 Cisco 지원에 문의하십시오.

- Cisco 지원 사이트 방문(http://www.cisco.com/cisco/web/support/index.html)
- Cisco 고객 지원에 이메일 전송(tac@cisco.com)
- Cisco 고객 지원에 전화로 문의(1.408.526.7209 또는 1.800.553.2447)