Firepower Device Manager, 버전 6.2용 Cisco Firepower Threat Defense 컨피그레이션 가이드

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

이 설명서의 제품 관련 사양 및 정보는 예고 없이 변경될 수 있습니다. 이 설명서의 모든 설명, 정보 및 권장 사항이 정확하다고 판단되더라도 어떠한 형태의 명시적이거나 묵시적인 보증도 하지 않습니다. 모든 제품의 해당 애플리케이션에 대한 사용은 전적으로 사용자에게 책임이 있습니다.

동봉한 제품의 소프트웨어 라이선스 및 제한된 보증은 제품과 함께 제공된 정보 패킷에 설명되어 있으며 본 문서에 참조를 통해 포함됩니다. 소프트웨어 라이선스 또는 제한된 보증을 찾을 수 없는 경우 CISCO 담당자에게 문의하여 복사본을 요청하십시오.

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

여기에 명시된 다른 모든 보증에도 불구하고 이러한 공급업체의 모든 문서 파일 및 소프트웨어는 모든 결점을 포함하여 "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 그 공급자는 이 설명서의 사용 또는 사용할 수 없음으로 인한 모든 파생적, 부수적, 직접, 간접, 특별, 징벌적 또는 기타 모든 손해(영업 이익 손실, 영업 중단, 영업 정보 손실, 또는 그 밖의 금전적 손실로 인한 손해를 포함하되 이에 제한되지 않음)에 대하여 어떠한 경우에도 책임을 지지 않으며, 이는 CISCO 또는 그 공급자가 그와 같은 손해의 가능성을 사전에 알고 있던 경우에도 마찬가지입니다.

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.

Cisco 및 Cisco 로고는 미국 및 기타 국가에서 Cisco Systems, Inc. 및/또는 계열사의 상표 또는 등록 상표입니다. Cisco 상표 목록을 보려면 다음 URL로 이동하십시오. http://www.cisco.com/go/trademarks 여기에 언급된 타사 상표는 해당 소유자의 자산입니다. "파트너"라는 용어는 사용에 있어 Cisco와 기타 회사 간의 파트너 관계를 의미하지는 않습니다. (1110R)

목 차

1 장

시작하기

다음 주제에서는 Firepower Threat Defense 구성을 시작하는 방법을 설명합니다.

가이드의 적합성 확인

이 가이드에서는 Firepower Threat Defense 디바이스에 포함된 Firepower Device Manager 웹 기반 컨피그레이션 인터페이스를 사용하여 Firepower Threat Defense를 구성하는 방법을 설명합니다.

Firepower Device Manager에서는 소규모 네트워크에서 가장 흔히 사용되는 소프트웨어의 기본 기능을 구성할 수 있습니다. Firepower Device Manager는 특히 고성능 다중 디바이스 관리자를 사용해 여러 Firepower Threat Defense 디바이스가 포함된 대규모 네트워크를 제어하지 않으려는 디바이스가 하나 또는 몇 개만 포함된 네트워크용으로 설계되었습니다.

많은 수의 디바이스를 관리하거나 Firepower Threat Defense에서 허용하는 보다 복잡한 기능 및 컨피그레이션을 사용하려는 경우에는 통합형 Firepower Device Manager 대신 Firepower Management Center는를 사용하여 디바이스를 구성합니다.

다음과 같은 디바이스에 Firepower Device Manager를 사용할 수 있습니다.

표 ***1: Firepower Device Manager*** 지원 모델

디바이스 모델	최소 **Firepower Threat Defense** 소프트웨어 버전
ASA 5506-X, 5506H-X, 5506W-X, 5508-X, 5516-X	6.1

디바이스 모델	최소 **Firepower Threat Defense** 소프트웨어 버전
ASA 5512-X, 5515-X, 5525-X, 5545-X, 5555-X	6.1

Firepower Device Manager/Firepower Threat Defense 6.2의 새로운 기능

릴리스 날짜**: 2017**년 **1**월 **23**일

다음 표에는 Firepower Device Manager를 사용하여 구성하면 사용할 수 있는 Firepower Threat Defense 6.2의 새로운 기능이 나와 있습니다.

기능	설명
Cisco Defense Orchestrator 클라우드 관리	Cisco Defense Orchestrator 클라우드 기반 포털을 사용하여 디바이스를 관리할 수 있습니다. 이렇게 하려면 **Device(**디바이스**)** > **System Settings(**시스템 설정**)** > **Cloud Management(**클라우드 관리**)**를 선택합니다. Cisco Defense Orchestrator에 대한 자세한 내용은 http://www.cisco.com/go/cdo를 참조하십시오.
액세스 규칙 끌어 놓기(drag and drop)	액세스 규칙을 끌어다 놓아 규칙 테이블에서 액세스 규칙을 이동할 수 있습니다.
Firepower Threat Defense 소프트웨어 업그레이드	Firepower Device Manager를 통해 소프트웨어 업그레이드를 설치할 수 있습니다. 이렇게 하려면 **Device(**디바이스**)** > **Updates(**업데이트**)**를 선택합니다.

기능	설명
Firepower Threat Defense 기본 컨피그레이션 변경 사항	새 디바이스 또는 재이미징된 디바이스의 경우 기본 컨피그레이션에는 다음과 같은 중요한 변경 사항이 포함되어 있습니다. • (ASA 5506-X, 5506W-X, 5506H-X) 첫 번째 데이터 인터페이스 및 ASA 5506W-X의 Wi-Fi 인터페이스를 제외하고 이러한 디바이스 모델의 다른 모든 데이터 인터페이스는 "내부" 브리지 그룹으로 구성되며 활성화됩니다. 내부 브리지 그룹에는 DHCP 서버가 있습니다. 브리지 인터페이스에 엔드포인트나 스위치를 연결할 수 있으며, 엔드포인트는 192.168.1.0/24 네트워크에서 주소를 가져옵니다. • 이제는 내부 인터페이스 IP 주소가 192.168.1.1이며, DHCP 서버는 주소 풀 192.168.1.5-192.168.1.254가 포함된 인터페이스에서 정의됩니다. • 내부 네트워크에서는 HTTPS 액세스가 활성화되므로 기본 주소 192.168.1.1에서 내부 인터페이스를 통해 Firepower Device Manager를 열 수 있습니다. ASA 5506-X 모델의 경우 임의의 내부 브리지 그룹 구성원 인터페이스를 통해 이 작업을 수행할 수 있습니다. • 관리 포트는 192.168.45.0/24 네트워크에 대해 DHCP 서버를 호스팅합니다. 워크스테이션을 관리 포트에 직접 연결하고 IP 주소를 가져온 다음 Firepower Device Manager를 열어 디바이스를 구성할 수 있습니다. • 이제는 OpenDNS 공용 DNS 서버가 관리 인터페이스의 기본 DNS 서버입니다. 이전에는 기본 DNS 서버가 없었습니다. 디바이스 설정 중에 다른 DNS 서버를 구성할 수 있습니다. • 관리 IP 주소의 기본 게이트웨이는 데이터 인터페이스를 사용하여 인터넷으로 라우팅됩니다. 따라서 관리 실제 인터페이스를 네트워크에 유선으로 연결하지 않아도 됩니다.

기능	설명
관리 인터페이스 및 액세스 변경 사항	관리 주소 및 Firepower Device Manager에 대한 액세스가 작동하는 방식과 관련하여 여러 가지 사항이 변경되었습니다. • 이제는 HTTPS(Firepower Device Manager의 경우) 및 SSH(CLI의 경우) 연결에 대해 데이터 인터페이스를 열 수 있습니다. 따라서 디바이스를 관리하기 위해 별도의 관리 네트워크를 사용하거나 관리/진단 물리적 포트를 내부 네트워크에 연결할 필요가 없습니다. 데이터 인터페이스를 열려면 **Device(**디바이스**)** > **System Settings(**시스템 설정**)** > **Management Access List(**관리 액세스 목록**)**을 선택합니다. • 시스템은 외부 인터페이스에 대해 게이트웨이를 통해 시스템 데이터베이스 업데이트를 가져올 수 있습니다. 그러므로 관리 인터페이스 또는 네트워크에서 인터넷으로의 명시적 경로가 없어도 됩니다. 기본적으로는 데이터 인터페이스를 통해 내부 경로를 사용합니다. 그러나 별도의 관리 네트워크를 사용하려는 경우에는 특정 게이트웨이를 설정할 수 있습니다. 이렇게 하려면 **Device(**디바이스**)** > **System Settings(**시스템 설정**)** > **Management Interface(**관리 인터페이스**)**를 선택합니다. • Firepower Device Manager를 사용하여 DHCP를 통해 IP 주소를 가져오도록 관리 인터페이스를 구성할 수 있습니다. 이렇게 하려면 **Device(**디바이스**)** > **System Settings(**시스템 설정**)** > **Management Interface(**관리 인터페이스**)**를 선택합니다. • 고정 주소를 구성하는 경우 관리 주소에 대해 DHCP 서버를 구성할 수 있습니다. 이렇게 하려면 **Device(**디바이스**)** > **System Settings(**시스템 설정**)** > **Management Interface(**관리 인터페이스**)**를 선택합니다.

기능	설명
기타 사용자 인터페이스 변경 사항	Firepower Device Manager 사용자 인터페이스의 주요 변경 사항은 다음과 같습니다. • 디바이스 주 메뉴 항목. 이전 릴리스에서 이 메뉴 항목은 디바이스의 호스트 이름이었습니다. 또한, 열리는 페이지의 이름은 디바이스 대시보드가 아닌 디바이스 요약입니다. • 초기 디바이스 설정 중에는 대체 외부 인터페이스를 선택할 수 없습니다. 첫 번째 데이터 인터페이스가 기본 외부 인터페이스입니다. • 이제는 **Device(**디바이스**)** > **System Settings(**시스템 설정**)** > **Cloud Preferences(**클라우드 기본 설정**)**의 이름이 **Device(**디바이스**)** > **System Settings(**시스템 설정**)** > **URL Filtering Preferences(URL** 필터링 기본 설정**)**으로 바뀌었습니다. • 이제는 **System Settings(**시스템 설정**)** > **DHCP Server(DHCP** 서버**)** 페이지가 2개 탭으로 구성되어 있으며 DHCP 서버 테이블이 글로벌 파라미터에서 분리되었습니다.
사이트 대 사이트 VPN 연결	사전 공유 키를 사용하여 사이트 대 사이트 VPN(Virtual Private Network) 연결을 구성할 수 있습니다. IKEv1 및 IKEv2 연결을 구성할 수 있습니다.
통합 라우팅 및 브리징 지원	통합 라우팅 및 브리징은 브리지 그룹과 라우팅 인터페이스 간을 라우팅하는 기능을 제공합니다. 브리지 그룹은 Firepower Threat Defense 디바이스가 경로 대신 브리징하는 인터페이스 그룹입니다. Firepower Threat Defense 디바이스는 실제 브리지는 아닙니다. Firepower Threat Defense 디바이스는 계속해서 방화벽으로 작동하며, 이를 통해 인터페이스 간의 액세스 제어가 제어되고 모든 일반 방화벽 검사가 올바르게 수행됩니다. 이 기능을 사용하면 브리지 그룹을 구성하고 브리지 그룹 간, 그리고 브리지 그룹과 라우팅 인터페이스 간을 라우팅할 수 있습니다. 브리지 그룹은 BVI(브리지 가상 인터페이스)를 사용하여 라우팅에 참여함으로써 브리지 그룹의 게이트웨이로 작동합니다. 브리지 그룹에 할당할 추가 인터페이스가 Firepower Threat Defense 디바이스에 있는 경우에는 외부 레이어 2 스위치를 사용하는 대신 통합형 라우팅 및 브리징을 사용할 수 있습니다. BVI는 이름이 지정된 인터페이스일 수 있으며 DHCP 서버 등의 일부 기능에는 구성원 인터페이스와 별도로 포함될 수 있습니다. 이 경우 브리지 그룹 구성원 인터페이스에서 NAT 및 액세스 제어 규칙과 같은 기타 기능을 구성합니다. 브리지 그룹을 구성하려면 **Device(**디바이스**)** > **Interfaces(**인터페이스**)**를 선택합니다.

시스템 로그인

Firepower Threat Defense 디바이스에는 두 가지 인터페이스가 있습니다.

Firepower Device Manager 웹 인터페이스

Firepower Device Manager는 웹 브라우저에서 실행됩니다. 이 인터페이스를 사용하여 시스템을 구성, 관리 및 모니터링합니다.

CLI(Command Line Interface, 콘솔**)**

CLI는 트러블슈팅에 사용합니다. Firepower Device Manager 대신 CLI를 초기 설정에 사용할 수도 있습니다.

다음 주제에서는 이러한 인터페이스에 로그인하고 사용자 어카운트를 관리하는 방법을 설명합니다.

Firepower Device Manager 로그인

Firepower Device Manager를 사용하여 시스템을 구성, 관리 및 모니터링합니다. 브라우저를 통해 구성할 수 있는 기능은 CLI(Command Line Interface)를 통해서는 구성할 수 없습니다. 즉, 반드시 웹 인터페이스를 사용하여 보안 정책을 구현해야 합니다.

최신 버전의 Firefox, Chrome, Safari 또는 Internet Explorer를 사용하십시오.

시작하기 전에

Firepower Device Manager에 로그인할 때는 **admin** 사용자 이름만 사용할 수 있습니다. Firepower Device Manager에 액세스하기 위해 추가 사용자를 생성할 수는 없습니다.

절차

단계 **1** 브라우저를 사용하여 시스템의 홈페이지(예: https://ftd.example.com)를 엽니다.
다음 주소 중 하나를 사용할 수 있습니다. IPv4 또는 IPv6 주소나 DNS 이름(구성한 경우)을 사용할 수 있습니다.

- 관리 주소. 기본적으로 이 주소는 관리/진단 인터페이스의 192.168.45.45입니다.
- HTTPS 액세스를 위해 연 데이터 인터페이스의 주소. 에서는 기본적으로 "내부" 인터페이스가 HTTPS 액세스를 허용하므로 기본 내부 주소 192.168.1.1에 연결할 수 있습니다. 내부 인터페이스가 브리지 그룹인 디바이스 모델에서는 모든 브리지 그룹 구성원 인터페이스를 통해 이 주소에 연결할 수 있습니다.

팁 브라우저가 서버 인증서를 인식하도록 구성되어 있지 않으면 신뢰할 수 없는 인증서에 대한 경고가 표시됩니다. 해당 인증서를 예외적으로 수락하거나 신뢰할 수 있는 루트 인증서 저장소에 저장하십시오.

단계 **2** **admin** 사용자 이름과 비밀번호를 입력하고 로그인을 클릭합니다.
기본 관리자 비밀번호는 Admin123입니다.

비활성 상태가 20분 동안 유지되면 세션이 만료되며, 다시 로그인하라는 메시지가 표시됩니다. 페이지 오른쪽 위에 있는 사용자 아이콘 드롭다운 메뉴에서 로그아웃을 선택하면 로그아웃할 수 있습니다.

CLI(Command Line Interface) 로그인

CLI(Command Line Interface)를 사용하여 시스템을 설정하고 기본적인 시스템 문제해결을 수행합니다. CLI 세션을 통해 정책을 구성할 수는 없습니다.

CLI에 로그인하려면 다음 중 하나를 수행합니다.

- 디바이스에 포함된 콘솔 케이블을 사용하여 PC를 콘솔에 연결합니다(터미널 에뮬레이터 9600 보드, 8 데이터 비트, 패리티 없음, 1 정지 비트, 흐름 제어 없음). 콘솔 케이블에 대한 자세한 내용은 디바이스용 하드웨어 가이드를 참조하십시오.
- 관리 IP 주소에 연결하려면 SSH 클라이언트를 사용합니다. SSH 연결용 인터페이스를 여는 경우 데이터 인터페이스의 주소에 연결할 수도 있습니다(관리 액세스 목록 구성, 287 페이지 참조). 데이터 인터페이스에 대한 SSH 액세스는 기본값으로 비활성화 상태입니다. 사용자 이름 **admin**(기본 비밀번호: Admin123) 또는 다른 CLI 사용자 어카운트를 사용하여 로그인합니다.

로그인한 후 CLI에서 사용 가능한 명령에 대한 정보를 확인하려면 **help** 또는 **?**를 입력합니다. 사용량 정보는 http://www.cisco.com/c/en/us/td/docs/security/firepower/command_ref/b_Command_Reference_for_Firepower_Threat_Defense.html에서 *Firepower Threat Defense* 명령 참조를 참조하십시오.

참고 **configure user add** 명령을 사용하면 CLI에 로그인할 수 있는 사용자 어카운트를 생성할 수 있습니다. 그러나 이러한 사용자는 CLI에만 로그인할 수 있으며 Firepower Device Manager 웹 인터페이스에는 로그인할 수 없습니다.

비밀번호 변경

비밀번호는 정기적으로 변경해야 합니다. 다음 절차에서는 Firepower Device Manager에 로그인한 상태에서 비밀번호를 변경하는 방법을 설명합니다.

참고 CLI에 로그인한 경우 **configure password** 명령을 사용하여 비밀번호를 변경할 수 있습니다. **configure user password***username* 명령을 사용하면 다른 CLI 사용자의 비밀번호를 변경할 수 있습니다.

절차

단계 **1** 메뉴 오른쪽 위에 있는 사용자 아이콘 드롭다운 목록에서 **Profile(**프로필**)**을 선택합니다.

단계 **2** **Password(**비밀번호**)** 탭을 클릭합니다.

단계 **3** 현재 비밀번호를 입력합니다.

단계 **4** 새 비밀번호를 입력하고 확인을 위해 다시 한 번 입력합니다.

단계 **5** **Change(**변경**)**를 클릭합니다.

사용자 프로필 환경 설정 지정

사용자 인터페이스의 기본 설정을 설정하고 비밀번호를 변경할 수 있습니다.

절차

단계 **1** 메뉴 오른쪽 위에 있는 사용자 아이콘 드롭다운 목록에서 프로필을 선택합니다.

단계 **2** **Profile(**프로필**)** 탭에서 다음 항목을 구성하고 **Save(**저장**)**를 클릭합니다.

- 작업 예약을 위한 시간대 - 백업 및 업데이트와 같은 작업을 예약하는 데 사용할 시간대를 선택합니다. 다른 시간대를 설정하는 경우 대시보드와 이벤트에 브라우저 시간대가 사용됩니다.
- 색 구성표 - 사용자 인터페이스에 사용할 색 구성표를 선택합니다.

단계 **3** 비밀번호 탭에서 새 비밀번호를 입력하고 변경을 클릭할 수 있습니다.

Firepower Threat Defense용 CLI 사용자 어카운트 생성

Firepower Threat Defense 디바이스에서 CLI 액세스를 위한 사용자를 생성할 수 있습니다. 이 어카운트는 관리 애플리케이션에 대한 액세스는 허용하지 않으며 CLI에 대한 액세스만 허용합니다. CLI는 트러블슈팅 및 모니터링에 유용합니다.

한 번에 둘 이상의 디바이스에서 어카운트를 생성할 수 없습니다. 각 디바이스에는 고유한 CLI 어카운트로 구성된 고유 집합이 있습니다.

절차

단계 **1** config 권한이 있는 어카운트를 사용하여 디바이스 CLI에 로그인합니다.
관리자 사용자 어카운트는 필수 권한을 갖고 있지만, config 권한이 있는 모든 어카운트도 괜찮습니다. SSH 세션 또는 콘솔 포트를 사용할 수 있습니다.

특정 디바이스 모델의 경우, 콘솔 포트는 사용자를 FXOS CLI에 연결합니다. **connect ftd** 명령을 사용하여 Firepower Threat Defense CLI에 연결합니다.

단계 **2** 사용자 계정을 생성합니다.
configure user add*username* {**basic** | **config**}

다음 권한 레벨을 가진 사용자를 정의할 수 있습니다:

- **config** - 사용자에게 컨피그레이션 액세스 권한을 제공합니다. 이 명령은 사용자에게 모든 명령에 대한 전체 관리자 권한을 제공합니다.
- **basic** - 사용자에게 기본 액세스 권한을 제공합니다. 이 명령은 사용자가 컨피그레이션 명령을 입력하는 것을 허용하지 않습니다.

예제:
다음 예에서는 config 액세스 권한이 있는 joecool이라는 이름의 사용자 어카운트를 추가합니다. 입력하고 있으므로 비밀번호가 표시되지 않습니다.

```
> configure user add joecool config
Enter new password for user joecool: newpassword
Confirm new password for user joecool: newpassword
> show user
Login              UID   Auth Access  Enabled Reset    Exp Warn  Str Lock Max
admin             1000  Local Config  Enabled    No  Never  N/A  Dis   No N/A
joecool           1001  Local Config  Enabled    No  Never  N/A  Dis   No   5
```

참고 **configure password** 명령을 사용하여 비밀번호를 변경할 수 있다고 사용자에게 알려줍니다.

단계 **3** (선택 사항) 보안 요건을 충족하도록 어카운트의 특성을 조정합니다.
다음 명령을 사용하여 기본 어카운트 동작을 변경할 수 있습니다.

- **configure user aging** *username max_days warn_days*

  사용자 비밀번호의 만료일을 설정합니다. 비밀번호가 유효한 최대 일수를 지정한 후 며칠 전부터 사용자에게 다가오는 만료일에 대해 경고할지 일수를 지정합니다. 두 값 모두 1~9999 범위이

지만, 경고 일수는 최대 일수보다 작아야 합니다. 어카운트를 생성할 때 비밀번호 만료일이 없습니다.

- **configure user forcereset** *username*

  사용자가 다음 로그인 시 강제로 비밀번호를 변경하게 합니다.

- **configure user maxfailedlogins** *username number*

  어카운트를 잠그기 전에 허용되는 연속 실패 로그인의 최대 수를 1~9999 범위로 설정합니다. 어카운트의 잠금을 해제하려면 **configure user unlock** 명령을 사용합니다. 새 어카운트에 대한 기본값은 로그인 5회 연속 실패입니다.

- **configure user minpasswdlen** *username number*

  최소 비밀번호 길이를 1~127 범위로 설정합니다.

- **configure user strengthcheck** *username* {**enable** | **disable**}

  비밀번호 강도 검사를 사용하거나 비활성화합니다. 이 경우 비밀번호를 변경할 때 사용자는 특정 비밀번호 기준을 충족해야 합니다. 사용자 비밀번호가 만료되거나 **configure user forcereset** 명령이 사용되면, 사용자가 다음에 로그인할 때 이 요건이 자동으로 활성화됩니다.

단계 **4** 필요 시 사용자 어카운트를 관리합니다.
사용자가 자신의 어카운트를 잠글 수 있게 하거나, 어카운트를 제거하거나 다른 문제를 해결해야 합니다. 시스템에서 사용자 어카운트를 관리하려면 다음 명령을 사용합니다.

- **configure user access** *username* {**basic** | **config**}

  사용자 어카운트에 대한 권한을 변경합니다.

- **configure user delete** *username*

  지정된 어카운트를 삭제합니다.

- **configure user disable** *username*

  지정된 어카운트를 삭제하지 않고 비활성화합니다. 사용자는 어카운트를 활성화할 때까지 로그인할 수 없습니다.

- **configure user enable** *username*

  지정된 어카운트를 활성화합니다.

- **configure user password** *username*

  지정된 사용자에 대한 비밀번호를 변경합니다. 사용자는 일반적으로 **configure password** 명령을 사용하여 자신의 비밀번호를 변경해야 합니다.

- **configure user unlock** *username*

  연속 실패 로그인 시도의 최대 횟수를 초과하므로 잠겨 있는 사용자 어카운트의 잠금을 해제합니다.

시스템 설정

초기 컨피그레이션을 완료해야 네트워크에서 시스템이 정상적으로 작동합니다. 올바른 배포에는 케이블을 적절하게 연결하는 작업과, 디바이스를 네트워크에 삽입하고 인터넷 또는 기타 업스트림 라우터에 연결하는 데 필요한 주소를 구성하는 작업이 포함됩니다. 다음 절차에서는 이러한 프로세스에 대해 설명합니다.

시작하기 전에

초기 설정을 시작하기 전에 디바이스에는 일부 기본 설정이 포함되어 있습니다. 자세한 내용은 초기 설정 전의 기본 컨피그레이션, 22 페이지를 참조해 주십시오.

절차

단계 **1** 인터페이스 연결, 11 페이지

단계 **2** 초기 컨피그레이션 완료, 14 페이지
이 프로세스의 결과로 생성되는 컨피그레이션에 대한 자세한 내용은 초기 설정 후의 컨피그레이션, 24 페이지를 참조하십시오.

단계 **3** 무선 액세스 포인트(ASA 5506W-X) 구성, 19 페이지

인터페이스 연결

기본 컨피그레이션에서는 특정 인터페이스가 내부 및 외부 네트워크에 사용된다고 가정합니다. 이러한 가정에 따라 인터페이스에 네트워크 케이블을 연결하면 초기 컨피그레이션을 더욱 쉽게 완료할 수 있습니다.

의 기본 컨피그레이션에서는 내부 인터페이스에 워크스테이션을 직접 연결할 수 있습니다. 내부 인터페이스가 브리지 그룹인 디바이스 모델의 경우 모든 구성원 인터페이스에 연결할 수 있습니다. 워크스테이션을 관리 포트에 직접 연결할 수도 있습니다. DHCP를 사용하여 정확한 네트워크의 주소를 가져옵니다. 인터페이스는 서로 다른 네트워크에 있으므로 내부 인터페이스와 관리 포트를 같은 네트워크에 연결하지 마십시오.

활성 DHCP 서버가 있는 네트워크에 관리 인터페이스 또는 내부 인터페이스를 연결하지 마십시오. 이와 같이 연결하면 내부 및 관리 포트에서 이미 실행 중인 DHCP 서버와 충돌하게 됩니다. 네트워크에 대해 다른 DHCP 서버를 사용하려는 경우에는 워크스테이션을 관리 포트에 직접 연결하고 초기 컨피그레이션을 완료한 후에 원치 않는 DHCP 서버를 비활성화합니다. 그리고 나면 네트워크에 디바이스를 연결할 수 있습니다.

다음 항목에서는 내부 인터페이스를 사용하여 디바이스를 구성할 때 이 토폴로지에 대해 시스템을 케이블 연결하는 방법을 설명합니다.

ASA 5506-X, 5506W-X 및 5506H-X 케이블 연결

그림 *1: ASA 5506W-X(Wi-Fi 기능 포함), 5506-X(Wi-Fi 기능 미포함)*

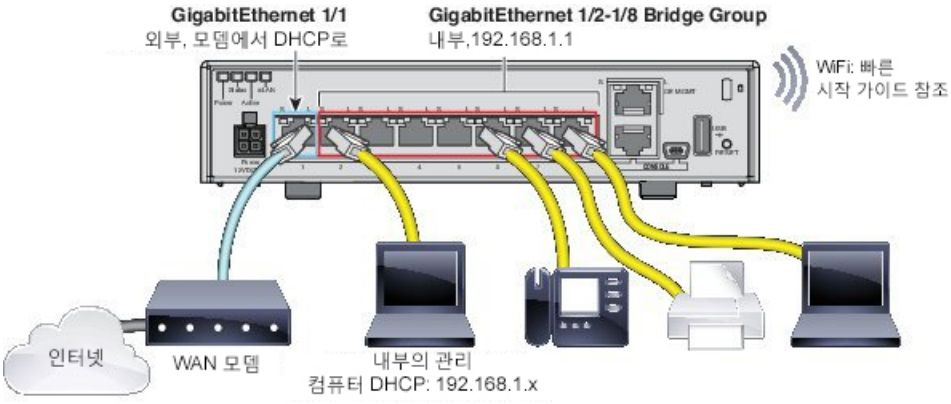
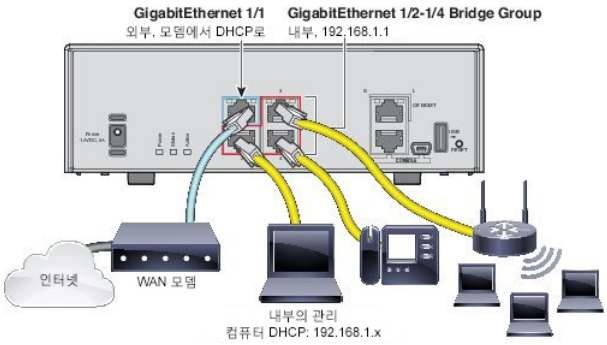


그림 *2: ASA 5506H-X*

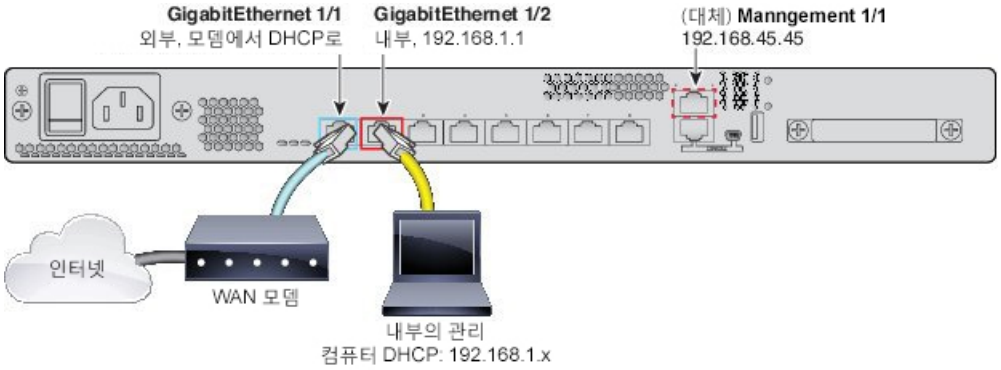


- ISP/WAN 모뎀 또는 기타 외부 디바이스에 GigabitEthernet1/1을 연결합니다. 기본적으로는 DHCP를 사용하여 IP 주소를 가져오지만 초기 컨피그레이션 중에 고정 주소를 설정할 수 있습니다.
- 디바이스를 구성하는 데 사용할 워크스테이션에 GigabitEthernet1/2 또는 내부 브리지 그룹 구성원 포트 중 하나를 연결합니다. 워크스테이션이 DHCP를 사용하여 IP 주소를 가져오도록 구성합니다. 워크스테이션은 192.168.1.0/24 네트워크의 주소를 가져옵니다.

참고 관리 워크스테이션을 연결할 때 몇 가지 다른 옵션을 사용할 수 있습니다. 관리 워크스테이션을 직접 관리 포트에 연결할 수도 있습니다. 워크스테이션은 192.168.45.0/24 네트워크에서 DHCP를 통해 주소를 가져옵니다. 또 다른 옵션은 워크스테이션을 스위치에 연결한 상태로 유지하고 GigabitEthernet1/2와 같은 내부 포트 중 하나에 해당 스위치를 연결하는 것입니다. 그러나 이 경우에는 스위치 네트워크에 DHCP 서버를 실행하는 다른 디바이스가 없는지 확인해야 합니다. 이러한 디바이스가 있으면 내부 브리지 그룹 192.168.1.1에서 실행 중인 디바이스와 충돌하기 때문입니다.

- 필요한 경우 내부 브리지 그룹의 기타 포트에 다른 엔드포인트 또는 스위치를 연결합니다. 엔드포인트를 추가하기 전에 초기 디바이스 설정을 완료할 때까지 기다려야 할 수 있습니다. 스위치를 추가하는 경우에는 해당 네트워크에서 실행 중인 다른 DHCP 서버가 없는지 확인해야 합니다. 이러한 서버가 있으면 내부 브리지 그룹에서 실행 중인 DHCP 서버와 충돌하기 때문입니다.

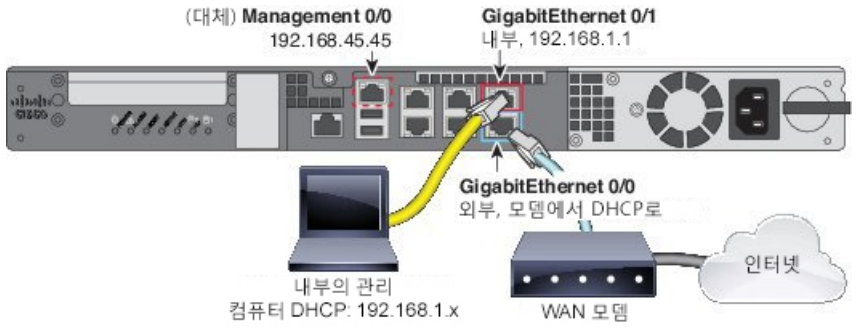
ASA 5508-X 및 5516-X 케이블 연결



- ISP/WAN 모뎀 또는 기타 외부 디바이스에 GigabitEthernet1/1을 연결합니다. 기본적으로는 DHCP를 사용하여 IP 주소를 가져오지만 초기 컨피그레이션 중에 고정 주소를 설정할 수 있습니다.
- 디바이스를 구성하는 데 사용할 워크스테이션에 GigabitEthernet1/2를 연결합니다. 워크스테이션이 DHCP를 사용하여 IP 주소를 가져오도록 구성합니다. 워크스테이션은 192.168.1.0/24 네트워크의 주소를 가져옵니다.

참고 관리 워크스테이션을 연결할 때 몇 가지 다른 옵션을 사용할 수 있습니다. 관리 워크스테이션을 직접 관리 포트에 연결할 수도 있습니다. 워크스테이션은 192.168.45.0/24 네트워크에서 DHCP를 통해 주소를 가져옵니다. 또 다른 옵션은 워크스테이션을 스위치에 연결한 상태로 유지하고 GigabitEthernet1/2에 해당 스위치를 연결하는 것입니다. 그러나 이 경우에는 스위치 네트워크에 DHCP 서버를 실행하는 다른 디바이스가 없는지 확인해야 합니다. 이러한 디바이스가 있으면 내부 인터페이스 192.168.1.1에서 실행 중인 디바이스와 충돌하기 때문입니다.

ASA 5512-X, 5515-X, 5525-X, 5545-X 및 5555-X 케이블 연결



- ISP/WAN 모뎀 또는 기타 외부 디바이스에 GigabitEthernet0/0을 연결합니다. 기본적으로는 DHCP를 사용하여 IP 주소를 가져오지만 초기 컨피그레이션 중에 고정 주소를 설정할 수 있습니다.
- 디바이스를 구성하는 데 사용할 워크스테이션에 GigabitEthernet0/1를 연결합니다. 워크스테이션이 DHCP를 사용하여 IP 주소를 가져오도록 구성합니다. 워크스테이션은 192.168.1.0/24 네트워크의 주소를 가져옵니다.

참고 관리 워크스테이션을 연결할 때 몇 가지 다른 옵션을 사용할 수 있습니다. 관리 워크스테이션을 직접 관리 포트에 연결할 수도 있습니다. 워크스테이션은 192.168.45.0/24 네트워크에서 DHCP를 통해 주소를 가져옵니다. 또 다른 옵션은 워크스테이션을 스위치에 연결한 상태로 유지하고 GigabitEthernet0/1에 해당 스위치를 연결하는 것입니다. 그러나 이 경우에는 스위치 네트워크에 DHCP 서버를 실행하는 다른 디바이스가 없는지 확인해야 합니다. 이러한 디바이스가 있으면 내부 인터페이스 192.168.1.1에서 실행 중인 디바이스와 충돌하기 때문입니다.

초기 컨피그레이션 완료

Firepower Device Manager에 처음 로그인할 때는 디바이스 설정 마법사로 이동하게 되며, 이 마법사에서 초기 시스템 컨피그레이션을 완료해야 합니다.

시작하기 전에

케이블 모뎀이나 라우터와 같은 게이트웨이 디바이스에 데이터 인터페이스를 연결해야 합니다. 이 디바이스는 에지 구축의 경우 인터넷 연결 게이트웨이가 되며, 데이터 센터 구축의 경우에는 백본 라우터가 됩니다. 모델의 기본 "외부" 인터페이스를 사용합니다(인터페이스 연결, 11 페이지 및 초기 설정 전의 기본 컨피그레이션, 22 페이지 참조).

그런 다음 워크스테이션을 하드웨어 모델의 "내부" 인터페이스에 연결합니다. 내부 인터페이스가 브리지 그룹인 모델의 경우 모든 브리지 그룹 구성원 인터페이스(외부 인터페이스가 아닌 모든 데이터 포트)에 연결할 수 있습니다. 또는 관리/진단 실제 인터페이스에 연결할 수도 있습니다.

관리/진단 실제 인터페이스는 네트워크에 연결하지 않아도 됩니다. 기본적으로 시스템은 인터넷에 연결하는 데이터 인터페이스(대개 외부 인터페이스)를 통해 시스템 라이선싱 및 데이터베이스 업데이트와 기타 업데이트를 가져옵니다. 별도의 관리 네트워크를 대신 사용하려는 경우에는 관리/진단 인터페이스를 네트워크에 연결하고 초기 설정을 완료한 후에 별도의 관리 게이트웨이를 구성하면 됩니다.

절차

단계 **1** Firepower Device Manager에 로그인합니다.

a) CLI에서 초기 컨피그레이션을 수행하지 않았다고 가정하겠습니다. **https://***ip-address*에서 Firepower Device Manager를 엽니다. 여기서 주소는 다음 중 하나입니다.

- 내부 인터페이스 또는 내부 브리지 그룹 데이터 인터페이스 중 하나(기본 내부 브리지 그룹이 있는 모델의 경우)에 연결되어 있는 경우: **https://192.168.1.1**
- 관리 실제 인터페이스에 연결되어 있는 경우: **https://192.168.45.45**

b) 사용자 이름 **admin** 및 비밀번호 **Admin123**으로 로그인합니다.

단계 **2** 시스템에 처음으로 로그인하며 CLI 설정 마법사를 사용하지 않은 경우에는 최종 사용자 라이선스 계약을 확인 및 동의하고 관리자 비밀번호를 변경하라는 메시지가 표시됩니다.
계속하려면 이러한 단계를 완료해야 합니다.

단계 **3** 외부 및 관리 인터페이스에 대해 다음 옵션을 구성하고 **Next(**다음**)**를 클릭합니다.

주의 **Next(**다음**)**를 클릭하면 설정이 디바이스에 구축됩니다. 인터페이스는 이름이 "외부"로 지정되어 "outside_zone" 보안 영역에 추가됩니다. 설정이 올바른지 확인합니다. 내부 인터페이스와 동일한 서브넷에 있는 외부 인터페이스에서 IP 주소 구성을 종료했으며 내부 주소에 있는 Firepower Device Manager에 연결되어 있는 경우, 내부 인터페이스에 있는 주소가 제거되므로 **Next(**다음**)**를 클릭할 때 마법사가 중단됩니다. 복구하려면 외부 서브넷이 내부 서브넷과 충돌하는 경우 해야 할 작업(1단계에서 설정 마법사 중단), 17 페이지를 참조하십시오.

외부 인터페이스

- **IPv4** 구성 - 외부 인터페이스의 IPv4 주소를 구성합니다. DHCP를 사용하거나 수동으로 고정 IP 주소, 서브넷 마스크 및 게이트웨이를 입력할 수 있습니다. 끄기를 선택하여 IPv4 주소를 구성하지 않을 수도 있습니다. 기본 내부 주소와 동일한 서브넷에서 정적으로 또는 DHCP를 통해 IP 주소를 구성하지 마십시오(초기 설정 전의 기본 컨피그레이션, 22 페이지 참조).

- **IPv6** 구성 - 외부 인터페이스의 IPv6 주소를 구성합니다. DHCP를 사용하거나 수동으로 고정 IP 주소, 접두사 및 게이트웨이를 입력할 수 있습니다. 끄기를 선택하여 IPv6 주소를 구성하지 않을 수도 있습니다.

관리 인터페이스

- **DNS** 서버 - 시스템 관리 주소용 DNS 서버를 지정합니다. 이름 확인을 위해 DNS 서버의 주소를 하나 이상 입력합니다. 기본값은 OpenDNS 공개 DNS 서버입니다. 필드를 수정하여 기본값으로 되돌리려면 **OpenDNS** 사용을 클릭하여 적절한 IP 주소를 필드에 다시 로드합니다.
- 방화벽 호스트 이름 - 시스템 관리 주소용 호스트 이름을 지정합니다.

단계 **4** 시스템 시간 설정을 구성하고 **Next(**다음**)**를 클릭합니다.

- 표준 시간대 - 시스템의 표준 시간대를 선택합니다.
- **NTP** 시간 서버 - 기본 NTP 서버를 사용할지 아니면 NTP 서버의 주소를 수동으로 입력할지를 선택합니다. 백업을 제공하기 위해 여러 서버를 추가할 수 있습니다.

단계 **5** 시스템에 대한 스마트 라이선스를 구성합니다.
시스템에 필요한 라이선스를 가져오고 적용하려면 스마트 라이선스 어카운트가 있어야 합니다. 처음에는 90일 평가 라이선스를 사용하고 나중에 스마트 라이선싱을 설정할 수 있습니다.

디바이스를 바로 등록하려면 링크를 클릭하여 Smart Software Manager 어카운트에 로그인한 다음 새 토큰을 생성해 수정 상자에 복사합니다.

평가 라이선스를 사용하려면 등록 없이 **90**일 평가 기간 시작을 선택합니다. 나중에 디바이스를 등록하고 스마트 라이선스를 가져오려면 디바이스을 클릭한 다음 **Smart Licenses(**스마트 라이선스**)** 그룹에서 링크를 클릭합니다.

단계 **6** **Finish(**종료**)**를 클릭합니다.

다음에 할 작업

- 범주 기반 URL 필터링, 침입 검사, 악성코드 방지 등 선택 가능한 라이선스에 포함되는 기능을 사용하려면 필요한 라이선스를 활성화합니다. 선택 가능한 라이선스 활성화 또는 비활성화, 67 페이지를 참조하십시오.
- 새 시스템의 경우 기본 내부 브리지 그룹이 포함된 디바이스 모델의 다른 인터페이스는 내부 브리지 그룹의 구성원으로 사용할 수 있는 상태입니다. 인터페이스에 엔드포인트를 직접 연결할 수 있습니다. 단일 기본 실제 인터페이스가 포함된 모델의 경우에는 다른 데이터 인터페이스를 고유 네트워크에 연결한 다음 인터페이스를 구성할 수 있습니다. 브리지 그룹 구성원 인터페이스의 경우에는 브리지 그룹에서 제거하고 추가 고유 네트워크를 구성할 수도 있습니다. 인터페이스 구성에 대한 자세한 내용은 서브넷을 추가하는 방법, 56 페이지 및 인터페이스 구성 , 109 페이지를 참조하십시오.
- 내부 인터페이스 또는 브리지 그룹 구성원 인터페이스를 통해 디바이스를 관리하는 경우 내부 인터페이스를 통해 CLI 세션을 열려면 SSH 연결에 대해 내부 인터페이스 또는 브리지 그룹을 엽니다. 관리 액세스 목록 구성, 287 페이지를 참조하십시오.

- 제품 사용 방법을 파악하려면 활용 사례를 확인하십시오. Firepower Threat Defense 활용 사례, 33 페이지를 참조하십시오.

외부 서브넷이 내부 서브넷과 충돌하는 경우 해야 할 작업(1단계에서 설정 마법사 중단)

내부 인터페이스를 통해 Firepower Device Manager에 연결하는 경우, 외부 인터페이스를 구성하는 1단계에서 **Next**(다음)를 클릭하면 설정 마법사가 중단되는 것을 발견할 수 있습니다. 일반적으로 이 단계를 완료하는 데 시간이 걸리므로 중단은 10분 이상 계속되는 것을 의미합니다. 브라우저를 새로 고치면, Firepower Device Manager에 대한 연결이 손실된 것을 확인할 수 있습니다. (관리 IP 주소를 통해 연결된 경우 마법사가 중단되지 않지만 아래 증상에 설명된 대로 계속해서 문제가 지속될 수 있습니다.)

이러한 문제가 발생하는 가장 큰 이유는 외부 인터페이스 및 내부 인터페이스 모두 동일한 서브넷에 있는 주소를 할당받아 내부 인터페이스가 컨피그레이션을 손실하게 되기 때문입니다.

기본 컨피그레이션에는 내부 인터페이스의 고정 주소와 DHCP 서버가 포함되므로 디바이스는 설정 마법사를 완료한 후 즉시 작동하며 트래픽을 전달하고 연결된 워크스테이션을 지원할 수 있습니다.

그러나, 기본 내부 주소를 사용하면 외부 인터페이스의 동일한 서브넷의 주소를 구성하지 않는 경우에만 작동합니다. 여기에는 DHCP를 통해 외부 주소에 주소를 제공하는 ISP 디바이스에 연결되는 경우가 포함됩니다. 일부 ISP는 내부 인터페이스(외부 인터페이스에 연결되어 있음)에 대해 Firepower Threat Defense에서 내부 주소에 사용하는 것과 동일한 192.168.1.0/24 서브넷을 사용합니다.

이 문제를 해결하려면 내부 인터페이스에서 IP 주소를 변경해야 합니다.

내부/외부 서브넷 충돌 증상

다음은 내부 및 외부 인터페이스에서 동일한 서브넷에 주소를 보유한 경우의 증상입니다.

- 디바이스 설정 마법사를 수행하는 동안 1단계에서 Next(다음)를 클릭하면 마법사가 중단됩니다. 일반적으로 이 단계를 완료하는 데 시간이 걸리므로 중단은 10분 이상 계속되는 것을 의미합니다.
- 콘솔 포트에 연결된 경우, CLI에서 다음 메시지가 표시됩니다. Firepower Device Manager에서 컨피그레이션(후속 변경 없이)을 구축하려고 시도할 경우에도 이 메시지를 받습니다.

```
ERROR: Failed to apply IP address to interface GigabitEthernet1/1,
as the network overlaps with interface GigabitEthernet1/2.
Two interfaces cannot be in the same subnet.
```

- 이 설정을 모두 완료하거나 종료하는 경우 연결 그래픽은 외부 서비스(예: 게이트웨이, DNS 및 NTP 서버, 스마트 라이선싱)에 대한 연결이 없음을 표시합니다. 메뉴의 구축 아이콘은 또한 구축이 필요하다고 표시합니다.
- CLI에서 **show running-config** 및 **show startup-config** 명령을 사용하여 확인할 경우 내부 인터페이스 및 외부 인터페이스에 대해 **interface** 및 **dhcp** 컨피그레이션이 일치하지 않습니다.

절차

단계 **1** 디바이스 설정 중에 내부 인터페이스에 연결된 경우, 설정을 완료합니다.

a) 관리 포트에 연결하여 디바이스에 다시 연결합니다. 필요 시, 관리 네트워크(192.168.45.0/24)에 있는 새 주소를 가져오기 위해 워크스테이션의 DHCP 주소를 해제한 다음 갱신합니다. 필요 시 192.168.45.1~192.168.45.44 범위로 워크스테이션의 고정 주소를 구성합니다.

b) Firepower Device Manager를 https://192.168.45.45에서 엽니다.

c) 90일 평가 라이선스를 시작할지 묻는 프롬프트를 확인해야 합니다. 이 옵션을 선택하고 **Confirm**(확인)을 클릭합니다.

d) **Device**(디바이스) > **System Settings**(시스템 설정) > **NTP**를 선택하고 NTP 서버를 구성한 다음 **Save**(저장)를 클릭합니다. 기본 서버가 요건에 부합하는 경우, 이 단계를 건너뛸 수 있습니다.

e) 메뉴의 오른쪽 상단에 있는 사용자 아이콘 드롭다운 목록에서 **Profile**(프로파일)을 선택하고 디바이스의 시간대를 선택한 다음 **Save**(저장)를 클릭합니다.

f) 평가 라이선스를 사용하지 않으려는 경우, **Device**(디바이스) > **Smart License**(스마트 라이선스) > **View Configuration**(컨피그레이션 보기)을 선택하고 **Request Register**(등록 요청)를 클릭한 다음 디바이스 등록 지침을 따릅니다. 디바이스 등록, 67 페이지를 참조하십시오. 현재 필요한 라이선스(선택 사항)를 활성화할 수 있습니다.

단계 **2** 내부 인터페이스에서 DHCP 서버를 제거합니다.

a) **Device**(디바이스) > **System Settings**(시스템 설정) > **DHCP Server**(DHCP 서버)를 선택합니다.

b) **DHCP** 서버 탭을 클릭합니다.

c) 내부 인터페이스 행에서 **Actions**(작업) 열 위로 마우스를 가져가 삭제 아이콘()을 클릭합니다.

단계 **3** 내부 인터페이스에서 주소를 변경합니다.

a) **Device**(디바이스)를 선택합니다.

b) 인터페이스 그룹에서 활성화된 인터페이스 수를 표시하는 링크(예: **3**개 활성화됨)를 클릭합니다.

c) 내부 인터페이스의 **Actions**(작업) 열 위로 마우스를 가져가 수정 아이콘()을 클릭합니다.

d) **IPv4 Address**(IPv4 주소) 탭에서 고유한 서브넷에 고정 주소를 입력합니다(예: 192.168.2.1/24 또는 192.168.46.1/24). 기본 관리 주소가 192.168.45.45/24인 경우 해당 서브넷을 사용하지 마십시오. 또한 이미 내부 네트워크에서 실행 중인 DHCP 서버가 있는 경우, 주소를 가져오기 위해 DHCP를 사용할 수도 있습니다.

e) **OK**(확인)를 클릭합니다.

단계 **4** (선택 사항). 내부 주소에서 DHCP 서버를 구성합니다.
내부 인터페이스에 대해 고정 주소를 구성할 경우, 내부 네트워크에 연결된 워크스테이션에 주소를 제공하기 위해 DHCP 서버를 구성할 수 있습니다. 이는 일반적인 설정입니다.

a) **Device**(디바이스) > **System Settings**(시스템 설정) > **DHCP Server**(DHCP 서버)를 선택합니다.

b) **DHCP** 서버 탭을 클릭합니다.

c) **+**를 클릭합니다.

d) 서버를 활성화하는 옵션을 선택하고 내부 인터페이스를 선택합니다.

e) 주소 풀의 경우, 내부 주소와 동일한 서브넷의 범위를 입력합니다.
예를 들어, 내부 주소가 192.168.2.1/24인 경우, 192.168.2.5~192.168.2.254를 사용할 수 있습니다. 네트워크에 있는 노드에 정적으로 할당된 주소를 포함하지 마십시오. 필요 시 고정 주소를 할당할 수 있도록 풀 외부에 몇 개의 주소를 남겨두는 것을 고려하십시오.

f) **OK(**확인**)**를 클릭합니다.

단계 **5** 메뉴에서 **Deploy(**구축**)** 버튼을 클릭하여 변경 사항을 구축합니다.

단계 **6** **Deploy Now(**지금 배포**)**를 클릭합니다.
구축을 완료한 후, 연결 그래픽은 외부 서비스에 대해 녹색으로 표시되어야 합니다.

무선 액세스 포인트(ASA 5506W-X) 구성

ASA 5506W-X에는 디바이스에 통합된 Cisco Aironet 702i 무선 액세스 포인트가 포함되어 있습니다. 무선 액세스 포인트는 기본적으로 비됩니다. 무선 장치를 활성화하고 SSID 및 보안 설정을 구성할 수 있도록 액세스 포인트 웹 인터페이스에 연결하십시오.

이 액세스 포인트는 GigabitEthernet1/9 인터페이스를 통해 내부적으로 연결됩니다. 모든 Wi-Fi 클라이언트는 GigabitEthernet1/9 네트워크에 속합니다. 보안 정책은 Wi-Fi 네트워크가 다른 인터페이스에서 네트워크에 액세스하는 방법을 결정합니다. 액세스 포인트에는 외부 인터페이스 또는 스위치 포트가 포함되어 있지 않습니다.

다음 절차에서는 액세스 포인트를 구성하는 방법을 설명합니다. 이 절차에서는 디바이스 설정 마법사를 완료했다고 가정합니다. 대신 수동으로 디바이스를 구성한 경우에는 컨피그레이션에 따라 단계를 조정해야 할 수 있습니다.

자세한 내용은 다음 설명서를 참조하십시오.

- Wireless LAN Controller 사용에 대한 자세한 내용은 Cisco Wireless LAN Controller 소프트웨어 설명서를 참조하십시오.
- 무선 액세스 포인트 하드웨어 및 소프트웨어에 대한 자세한 내용은 Cisco Aironet 700 Series 설명서를 참조하십시오.

시작하기 전에

액세스 포인트에 도달할 수 없고 Firepower Threat Defense 디바이스가 제안된 컨피그레이션 상태이며 다른 네트워크 문제가 발견되지 않으면, 액세스 포인트 기본 컨피그레이션을 복원할 수 있습니다. 이렇게 하려면 Firepower Threat Defense CLI에 액세스해야 합니다(콘솔 포트에 연결하거나 SSH 액세스 구성). Firepower Threat Defense CLI에서 다음 명령을 입력합니다.

```
> system support diagnostic-cli
Attaching to Diagnostic CLI ... Press 'Ctrl+a then d' to detach.
Type help or '?' for a list of available commands.

firepower> enable
Password: <press enter, by default, the password is blank>
```

```
firepower# hw-module module wlan recover configuration
```

액세스 포인트 트러블슈팅을 추가로 수행해야 하는 경우 **session wlan console** 명령을 사용하여 액세스 포인트 CLI에 연결합니다.

절차

단계 **1** 무선 인터페이스 GigabitEthernet1/9를 구성하고 사용합니다.

a) 디바이스을 클릭한 후 **Interfaces(**인터페이스**)** 그룹에서 링크를 클릭하여 인터페이스 목록을 엽니다.

b) GigabitEthernet1/9 인터페이스의 수정 아이콘()을 클릭합니다.

c) 다음 옵션을 구성합니다.

- 인터페이스 이름 - 인터페이스의 이름(예: **wifi**)을 입력합니다.
- 상태 - 슬라이더를 클릭하여 인터페이스를 활성화합니다.
- **IPv4** 주소 - 주소 유형으로 고정을 선택한 후 주소와 서브넷 마스크를 입력합니다. 예를 들면 192.168.10.1/24와 같이 입력합니다.

d) **Save(**저장**)**를 클릭합니다.

단계 **2** 내부 인터페이스와 같은 보안 영역에 Wi-Fi 인터페이스를 추가합니다.
디바이스 설정 마법사는 **inside_zone** 보안 영역에 내부 브리지 그룹의 구성원을 배치합니다. Wi-Fi 인터페이스가 같은 영역에 있어야 액세스 포인트 웹 인터페이스에 연결할 수 있습니다(기본 Inside_Inside_Rule 액세스 규칙을 통해 연결 가능함).

a) 메뉴에서 **Objects(**개체**)**를 클릭한 후 목차에서 **Security Zones(**보안 영역**)**을 선택합니다.

b) **inside_zone**의 수정 아이콘()을 클릭합니다.

c) **Interfaces(**인터페이스**)**에서 +를 클릭하고 **wifi** 인터페이스를 선택합니다.

단계 **3** **inside_zone** 보안 영역의 인터페이스 간에 트래픽을 허용하는 액세스 제어 규칙이 있는지 확인합니다.
디바이스 설정 마법사는 트래픽이 **inside_zone**에서 **outside_zone**으로 이동할 수 있도록 하는 규칙을 생성합니다. 따라서 내부 사용자가 인터넷에 연결할 수 있습니다.

또한 마법사는 내부 호스트가 서로 연결할 수 있도록 **inside_zone**과 **inside_zone** 간의 트래픽 이동을 허용하는 규칙도 생성합니다.

wifi 인터페이스를 **inside_zone**에 추가하면 Wi-Fi 사용자도 이 두 규칙에 모두 포함되므로 인터넷 및 기타 내부 사용자에 연결할 수 있습니다.

마법사를 완료하지 않은 경우에는 이러한 규칙이 없을 수도 있습니다. 기본 작업은 모든 트래픽을 차단하는 것이므로 이러한 규칙을 생성해야 합니다. 다음 절차에서는 **inside_zone** 보안 영역의 인터페이스 간에 트래픽 이동을 활성화하는 규칙을 생성하는 방법을 설명합니다.

a) 메뉴에서 **Policies(**정책**)**를 클릭합니다.

b) 액세스 제어 테이블 위의 +를 클릭하여 규칙을 추가합니다.

c) 최소한 규칙에서 다음과 같은 옵션을 구성합니다.

- 제목 - 규칙의 이름을 입력합니다. 예를 들면 Inside_Inside를 입력합니다.
- 작업 - 허용 또는 신뢰를 선택합니다.
- 원본/대상 > 원본 영역 - inside_zone을 선택합니다.
- 원본/대상 > 대상 영역 - inside_zone을 선택합니다.

d) **OK(**확인**)**를 클릭합니다.

단계 **4** 무선 인터페이스에서 DHCP 서버를 구성합니다.
DHCP 서버는 액세스 포인트에 연결하는 디바이스에 IP 주소를 제공합니다. 또한 액세스 포인트 자체에도 주소를 제공합니다.

a) 디바이스을 클릭합니다.
b) **System Settings(**시스템 설정**)** > **DHCP Server(DHCP** 서버**)**를 클릭합니다.
c) **DHCP** 서버 탭을 클릭합니다.
d) DHCP 서버 테이블 위의 +를 클릭합니다.
e) 다음 DHCP 서버 속성을 구성합니다.

- **DHCP** 서버 사용 - 슬라이더를 클릭하여 DHCP 서버를 사용합니다.
- 인터페이스 - **wifi** 인터페이스를 선택합니다.
- 주소 풀 - DHCP 클라이언트의 주소 풀을 입력합니다. 예를 들어 무선 인터페이스에 대해 예시 주소를 사용한 경우 풀은 192.168.10.2-192.168.10.254가 됩니다. 풀은 인터페이스의 IP 주소와 같은 서브넷에 있어야 하며 인터페이스의 주소나 브로드캐스트 주소는 포함할 수 없습니다.

f) **OK(**확인**)**를 클릭합니다.

단계 **5** 메뉴에서 Deploy(구축) 버튼을 클릭한 다음 **Deploy Now(**지금 구축**)**를 클릭하여 디바이스에 변경 사항을 구축합니다.

계속하기 전에 구축이 완료될 때까지 기다립니다.

단계 **6** 무선 액세스 포인트를 구성합니다.
무선 액세스 포인트는 무선 인터페이스에 대해 정의된 DHCP 풀에서 주소를 가져옵니다. 이때 풀의 첫 번째 주소를 가져와야 합니다. 예시 주소를 사용한 경우 이 주소는 192.168.10.2입니다. 첫 번째 주소가 작동하지 않는 경우에는 풀의 다음 주소를 사용해 봅니다.

a) 새 브라우저 창을 통해 무선 액세스 포인트 IP 주소(예: **http://192.168.10.2**)로 이동합니다.
액세스 포인트 웹 인터페이스가 표시되어야 합니다.

이 주소를 열려면 내부 네트워크 또는 내부 네트워크로 라우팅할 수 있는 네트워크에 있어야 합니다.

b) 사용자 이름 **cisco**, 비밀번호 **Cisco**를 사용하여 로그인합니다.
c) 왼쪽에서 **Easy Setup(**손쉬운 설정**)** > **Network Configuration(**네트워크 컨피그레이션**)**을 클릭합니다.

d) 무선 컨피그레이션 영역에서 무선 **2.4GHz** 및 무선 **5GHz** 섹션 각각에 대해 최소한 다음 파라미터를 설정하고 각 섹션에서 **Apply(**적용**)**를 클릭합니다.

- **SSID** - SSID(Service Set Identifier)로, 무선 네트워크의 이름입니다. 사용자가 Wi-Fi 연결용 무선 네트워크를 선택할 때 이 이름이 표시됩니다.
- 비콘의 브로드캐스트 **SSID** - 이 옵션을 선택합니다.
- 범용 관리 모드**:** 사용하지 않음.
- 보안 - 사용할 보안 옵션을 선택합니다.

단계 **7** 무선 액세스 포인트 웹 인터페이스를 사용하는 동안에는 무선을 사용합니다.

a) 왼쪽에서 **Summary(**요약**)**를 클릭한 다음 기본 페이지의 네트워크 인터페이스 아래에서 2.4GHz 무선에 대한 링크를 클릭합니다.
b) **Settings(**설정**)** 탭을 클릭합니다.
c) **Enable Radio(**무선 활성화**)** 설정에서 **Enable(**활성화**)** 라디오 버튼을 클릭하고 페이지 하단에서 **Apply(**적용**)**를 클릭합니다.
d) 5GHz 무선에 대해 이 프로세스를 반복합니다.

초기 설정 전의 기본 컨피그레이션

로컬 관리자(Firepower Device Manager)를 사용하여 Firepower Threat Defense 디바이스를 처음으로 구성하기 전에 디바이스에는 다음과 같은 기본 컨피그레이션이 포함되어 있습니다.

이 컨피그레이션에서는 대개 인터페이스에 컴퓨터를 직접 연결하는 방식을 사용하여 내부 인터페이스를 통해 Firepower Device Manager를 열며, 내부 인터페이스에 정의된 DHCP 서버를 사용하여 컴퓨터에 IP 주소를 제공한다고 가정합니다. 디바이스 모델별 기본 내부 인터페이스 및 외부 인터페이스는 아래 표를 참조하십시오. 또한, 컴퓨터를 관리/진단 실제 인터페이스에 연결한 다음 DHCP를 사용하여 주소를 가져올 수 있습니다. 브라우저에서 Firepower Device Manager를 여는 데 사용하는 기본 내부 및 관리 IP 주소는 컨피그레이션 설정 표를 참조하십시오.

기본 컨피그레이션 설정

설정	기본	초기 컨피그레이션 중 변경 가능 여부
관리자 사용자의 비밀번호	Admin123	예. 기본 비밀번호를 변경해야 합니다.
관리 IP 주소	192.168.45.45	번호

설정	기본	초기 컨피그레이션 중 변경 가능 여부
관리 게이트웨이	디바이스의 데이터 인터페이스. 일반적으로 외부 인터페이스는 인터넷의 경로가 됩니다. 이 게이트웨이는 from-the-box 트래픽에 대해서만 실행됩니다.	번호
관리 인터페이스의 DHCP 서버	주소 풀 192.168.45.46-192.168.45.254에서 활성화됩니다.	번호
관리 인터페이스의 DNS 서버	OpenDNS 공용 DNS 서버 208.67.220.220 및 208.67.222.222	예
내부 인터페이스 IP 주소	192.168.1.1/24	번호
내부 클라이언트에 대한 DHCP 서버	주소 풀 192.168.1.5-192.168.1.254를 포함하는 내부 인터페이스에서 실행됩니다.	번호
내부 클라이언트에 대한 DHCP 자동 컨피그레이션(자동 컨피그레이션은 클라이언트에 WINS 및 DNS 서버용 주소를 제공)	외부 인터페이스에서 활성화됩니다.	예(간접적). 외부 인터페이스에 대해 고정 IPv4 주소를 구성하는 경우 DHCP 서버 자동 컨피그레이션은 비활성화됩니다.
외부 인터페이스 IP 주소	ISP(Internet Service Provider) 또는 업스트림 라우터에서 DHCP를 통해 가져옵니다.	예

디바이스 모델별 기본 인터페이스

초기 컨피그레이션 중에는 다른 내부 및 외부 인터페이스를 선택할 수 없습니다. 컨피그레이션 후에 인터페이스 할당을 변경하려면 인터페이스 및 DHCP 설정을 수정합니다. 브리지 그룹에서 인터페이스를 제거해야 해당 인터페이스를 비스위치 인터페이스로 구성할 수 있습니다.

Firepower Threat Defense 디바이스	외부 인터페이스	내부 인터페이스
ASA 5506-X ASA 5506H-X ASA 5506W-X	GigabitEthernet1/1	외부 인터페이스를 제외한 기타 모든 데이터 인터페이스와 유선 인터페이스 GigabitEthernet1/9(5506W-X의 경우)를 포함하는 BVI1

Firepower Threat Defense 디바이스	외부 인터페이스	내부 인터페이스
ASA 5508-X ASA 5516-X	GigabitEthernet1/1	GigabitEthernet1/2
ASA 5512-X ASA 5515-X ASA 5525-X ASA 5545-X ASA 5555-X	GigabitEthernet0/0	GigabitEthernet0/1

초기 설정 후의 컨피그레이션

설정 마법사를 완료한 후의 디바이스 컨피그레이션에는 다음 설정이 포함됩니다. 아래 표에는 특정 설정이 명시적으로 선택한 것인지 아니면 다른 선택 항목을 기준으로 하여 정의된 것인지가 나와 있습니다. "암시적" 컨피그레이션을 검증한 후 필요한 사항에 맞지 않으면 수정합니다.

설정	컨피그레이션	명시적, 암시적 또는 기본 컨피그레이션
관리자 사용자의 비밀번호	입력한 내용	명시적
관리 IP 주소	192.168.45.45	기본
관리 게이트웨이	디바이스의 데이터 인터페이스. 일반적으로 외부 인터페이스는 인터넷의 경로가 됩니다. 관리 게이트웨이는 from-the-box 트래픽에 대해서만 실행됩니다.	기본
관리 인터페이스의 DHCP 서버	주소 풀 192.168.45.46-192.168.45.254에서 활성화됩니다.	기본
관리 인터페이스의 DNS 서버	입력한 내용	명시적
관리 호스트 이름	**firepower** 또는 입력한 내용	명시적

설정	컨피그레이션	명시적, 암시적 또는 기본 컨피그레이션
데이터 인터페이스를 통한 관리 액세스	데이터 인터페이스 관리 액세스 목록 규칙을 사용하면 내부 인터페이스를 통한 HTTPS 액세스가 허용됩니다. 내부 브리지 그룹이 있는 모델의 경우 여기에는 내부 브리지 그룹의 모든 구성원 인터페이스가 포함됩니다. SSH 연결은 허용되지 않습니다. IPv4 및 IPv6 연결은 모두 허용됩니다.	암시적
시스템 시간	선택한 표준 시간대 및 NTP 서버	명시적
스마트 라이선스	기본 라이선스를 사용하여 등록된 라이선스 또는 사용 설정된 평가 기간 중 선택하는 항목. 서브스크립션 라이선스는 사용하지 않습니다. 서브스크립션 라이선스를 사용하려면 스마트 라이선싱 페이지로 이동합니다.	명시적
내부 인터페이스 IP 주소	192.168.1.1/24	기본
내부 클라이언트에 대한 DHCP 서버	주소 풀 192.168.1.5-192.168.1.254를 포함하는 내부 인터페이스에서 실행됩니다.	기본
내부 클라이언트에 대한 DHCP 자동 컨피그레이션 (자동 컨피그레이션은 클라이언트에 WINS 및 DNS 서버용 주소를 제공)	DHCP를 사용하여 외부 인터페이스 IPv4 주소를 가져오는 경우 외부 인터페이스에서 사용하는 것으로 설정됩니다. 고정 주소를 사용하는 경우에는 DHCP 자동 컨피그레이션이 비활성화됩니다.	명시적(간접적)
데이터 인터페이스 컨피그레이션	(내부 브리지 그룹이 없는 모델) 외부 및 내부 인터페이스만 구성 및 활성화됩니다. 다른 모든 데이터 인터페이스는 비활성화됩니다. (내부 브리지 그룹이 있는 모델) 외부 인터페이스를 제외한 모든 데이터 인터페이스(예: GigabitEthernet1/2)가 활성화되며 내부 브리지 그룹에 포함됩니다. 엔드포인트 또는 스위치를 이러한 포트에 연결하고 내부 인터페이스용으로 DHCP 서버에서 주소를 가져올 수 있습니다.	기본

설정	컨피그레이션	명시적, 암시적 또는 기본 컨피그레이션
외부 실제 인터페이스 및 IP 주소	디바이스 모델에 따른 기본 외부 포트. 초기 설정 전의 기본 컨피그레이션, 22 페이지를 참조하십시오. IP 주소는 DHCP에서 가져온 주소이거나 입력한 고정 주소(IPv4, IPv6 또는 둘 다)입니다.	인터페이스: 기본 주소 지정: 명시적
정적 경로	외부 인터페이스에 대해 고정 IPv4 또는 IPv6 주소를 구성하는 경우 정적 기본 경로가 IPv4/IPv6에 대해 적절하게 구성되어 해당 주소 유형에 대해 정의한 게이트웨이를 가리킵니다. DHCP를 선택하는 경우 DHCP 서버에서 기본 경로를 가져옵니다. 게이트웨이 및 "임의" 주소에 대한 네트워크 개체도 생성됩니다(IPv4의 경우 0.0.0.0/0, IPv6의 경우 ::/0).	암시적
보안 영역	내부 인터페이스를 포함하는 **inside_zone**. 내부 브리지 그룹이 있는 모델의 경우 이 영역에는 내부 브리지 그룹 인터페이스의 모든 구성원이 포함됩니다. 외부 인터페이스를 포함하는 **outside_zone**. 이러한 영역을 수정하여 다른 인터페이스를 추가하거나 영역을 직접 생성할 수 있습니다.	암시적
액세스 제어 정책	inside_zone에서 outside_zone으로 전송되는 모든 트래픽을 신뢰하는 규칙입니다. 이 규칙을 사용하면 네트워크 내의 사용자가 외부로 전송하는 모든 트래픽 및 해당 연결에 대한 모든 반환 트래픽이 검사 없이 허용됩니다. 내부 브리지 그룹이 있는 모델의 경우 inside_zone의 인터페이스 간 모든 트래픽을 신뢰하는 두 번째 규칙입니다. 이 규칙을 사용하면 내부 네트워크의 사용자 간 모든 트래픽이 검사 없이 허용됩니다. 기타 모든 트래픽에 대한 기본 작업은 차단입니다. 즉, 외부에서 시작되어 네트워크로 진입하는 모든 트래픽은 차단됩니다.	암시적

설정	컨피그레이션	명시적, 암시적 또는 기본 컨피그레이션
NAT	(내부 브리지 그룹이 없는 모델)인터페이스 동적 PAT 규칙이 외부 인터페이스로 전송되는 IPv4 트래픽의 소스 주소를 외부 인터페이스 IP 주소의 고유 포트로 변환합니다. (내부 브리지 그룹이 있는 모델) 내부 브리지 그룹의 각 구성원에 대해 인터페이스 동적 PAT 규칙이 외부 인터페이스로 전송되는 IPv4 트래픽의 소스 주소를 외부 인터페이스 IP 주소의 고유 포트로 변환합니다. 이러한 규칙은 NAT 규칙 테이블에 표시되며, 원하는 경우 나중에 이러한 규칙을 수정할 수 있습니다. 관리 주소의 데이터 인터페이스를 통한 라우팅과 내부 인터페이스를 통한 HTTPS 액세스를 활성화하는 숨겨진 추가 PAT 규칙도 있습니다. 이러한 규칙은 NAT 테이블에는 표시되지 않지만 CLI에서 **show nat** 명령을 사용하면 확인할 수 있습니다.	암시적

컨피그레이션 기본 사항

다음 항목에서는 디바이스 구성을 위한 기본 방법을 설명합니다.

디바이스 구성

Firepower Device Manager에 처음 로그인할 때는 기본 설정을 구성할 수 있도록 설정 마법사로 이동하게 됩니다. 마법사를 완료한 후에 다음 방법을 사용하여 다른 기능을 구성하고 디바이스 컨피그레이션을 관리합니다.

항목을 시각적으로 구분하기가 어려운 경우 사용자 프로필에서 다른 색 구성표를 선택합니다. 페이지 오른쪽 위에 있는 사용자 아이콘 드롭다운 메뉴에서 프로필을 선택합니다.

절차

단계 **1** 디바이스을 클릭하여 **Device Summary(**디바이스 요약**)**로 이동합니다.

대시보드에는 키 설정이 구성되어 있는지(녹색으로 표시됨) 아니면 구성해야 하는지에 대한 정보 및 활성화된 인터페이스를 비롯하여 디바이스의 시각적 상태가 표시됩니다. 자세한 내용은 인터페이스 및 관리 상태 보기, 30 페이지를 참고하십시오.

상태 이미지 위에는 디바이스 모델, 소프트웨어 버전, 시스템 및 VDB(Vulnerability Database) 버전, 침입 규칙을 마지막으로 업데이트한 시간의 요약이 표시됩니다.

이미지 아래에는 구성 가능한 여러 기능의 그룹이 있으며 각 그룹의 컨피그레이션 요약과 시스템 컨피그레이션을 관리하기 위해 수행할 수 있는 작업이 표시됩니다.

단계 **2** 각 그룹의 링크를 클릭하여 설정을 구성하거나 작업을 수행합니다.
아래에는 그룹에 대한 설정이 요약되어 있습니다.

- 인터페이스 - 관리 인터페이스 이외에 둘 이상의 데이터 인터페이스가 구성되어 있어야 합니다. Interfaces, 103 페이지를 참조하십시오.
- 라우팅 - 라우팅 컨피그레이션입니다. 기본 경로를 정의해야 합니다. 컨피그레이션에 따라서는 다른 경로가 필요할 수 있습니다. 라우팅, 121 페이지를 참조하십시오.
- 업데이트 - 지리위치, 침입 규칙, 취약점 데이터베이스 업데이트 및 시스템 소프트웨어 업그레이드가 표시됩니다. 이러한 기능을 사용하려는 경우 최신 데이터베이스 업데이트를 받을 수 있도록 정기 업데이트 일정을 설정하십시오. 정기 일정에 따른 업데이트가 수행되기 전에 업데이트를 다운로드해야 하는 경우에도 이 페이지로 이동할 수 있습니다. 시스템 데이터베이스 업데이트, 299 페이지를 참조하십시오.
- 시스템 설정 - 이 그룹에는 여러 설정이 포함되어 있습니다. 그 중 일부 설정은 디바이스를 초기 설정할 때 구성하며 거의 변경하지 않는 기본 설정입니다. 시스템 설치, 287 페이지를 참조하십시오.
- 스마트 라이선스 - 시스템 라이선스의 현재 상태가 표시됩니다. 시스템을 사용하려면 적절한 라이선스를 설치해야 합니다. 일부 기능의 경우 추가 라이선스가 필요합니다. 시스템 라이선싱, 63 페이지를 참조하십시오.
- 백업 및 복원 - 시스템 컨피그레이션을 백업하거나 이전 백업을 복원합니다. 시스템 백업 및 복원, 303 페이지를 참조하십시오.
- 문제해결 - Cisco Technical Assistance Center에서 요청하는 경우 문제해결 파일을 생성합니다. 문제해결 파일 생성, 315 페이지를 참조하십시오.
- 사이트 대 사이트 **VPN** - 이 디바이스와 원격 디바이스 간의 사이트 대 사이트 VPN(Virtual Private Network) 연결이 표시됩니다. 사이트 대 사이트 VPN 관리, 264 페이지를 참조하십시오.

단계 **3** 메뉴에서 **Deploy(구축)** 버튼을 클릭하여 변경 사항을 구축합니다.

변경 사항은 구축할 때까지 디바이스에서 활성화되지 않습니다. 변경 사항 배포, 29 페이지를 참조하십시오.

다음에 할 작업

주 메뉴에서 **Policies(**정책**)**를 클릭하여 시스템의 보안 정책을 구성합니다. **Objects(**개체**)**를 클릭하여 해당 정책에 필요한 개체를 구성할 수도 있습니다.

변경 사항 배포

정책 또는 설정을 업데이트할 때 변경 사항은 디바이스에 즉시 적용되지 않습니다. 다음과 같은 2단계 프로세스를 통해 컨피그레이션을 변경합니다.

1. 변경 사항을 적용합니다.
2. 변경 사항을 배포합니다.

이 프로세스에서는 "부분 구성" 방식으로 디바이스를 실행할 필요 없이 관련 변경 사항 그룹을 적용할 수 있습니다. 또한 일부 변경의 경우 검사 엔진을 재시작해야 하며 재시작 중에 트래픽이 삭제되므로, 중단 가능성의 영향이 가장 적을 때 변경 사항을 배포하는 것이 좋습니다.

수행하려는 변경을 완료한 후에는 다음 절차에 따라 디바이스에 변경 사항을 배포합니다.

주의 Firepower Device Manager를 사용하는 Firepower Threat Defense 디바이스는 소프트웨어 리소스 문제가 있어 검사 엔진이 사용 중이거나, 컨피그레이션 배포 중에 특정 컨피그레이션으로 인해 엔진을 재시작해야 하여 엔진이 다운되면 트래픽을 삭제합니다. 재시작이 필요한 변경에 대한 자세한 내용은 검사 엔진을 재시작하는 컨피그레이션 변경, 30 페이지를 참조하십시오.

절차

단계 **1** 웹 페이지의 오른쪽 상단에 있는 변경 사항 배포 아이콘을 클릭합니다.
배포되지 않은 변경 사항이 있으면 아이콘이 점으로 강조 표시됩니다.

배포 요약 페이지가 열립니다. 이 페이지의 창에는 이전 배포 목록과 변경 사항("수정된 개체")의 요약 정보, 배포이 시작되고 완료된 시간 및 각 배포의 상태가 표시됩니다.

아이콘이 강조 표시되지 않아도 아이콘을 클릭하면 이전 배포 작업의 결과를 확인할 수 있습니다.

단계 **2** **Deploy Now(**지금 배포**)**를 클릭합니다.

검사 엔진을 재시작하는 컨피그레이션 변경

다음 컨피그레이션 또는 작업 중 하나를 수행하면 컨피그레이션 변경 사항을 구축할 때 검사 엔진이 재시작됩니다.

주의 구축 시에는 리소스 요구사항으로 인해 약간의 패킷이 검사 없이 삭제될 수 있습니다. 또한, 일부 컨피그레이션을 구축하려면 검사 엔진을 재시작해야 하므로 트래픽 검사가 중단되고 트래픽이 삭제됩니다.

구축

모든 구축에서는 검사 엔진이 재시작됩니다.

시스템 업데이트

시스템을 재부팅하지 않으며 이진 변경을 포함하는 시스템 업데이트나 패치를 설치할 때는 검사 엔진을 재시작해야 합니다. 이진 변경에는 검사 엔진, 전처리기, VDB(Vulnerability Database) 또는 공유 개체 규칙 변경이 포함될 수 있습니다. 이진 변경을 포함하지 않는 패치 시에도 Snort를 재시작해야 할 수 있습니다.

인터페이스 및 관리 상태 보기

디바이스 요약에는 디바이스의 그래픽 보기와 관리 주소에 대한 일부 설정이 포함됩니다. 디바이스 요약을 열려면 디바이스를 클릭합니다.

이 그래픽의 요소는 요소 상태에 따라 색이 변경됩니다. 요소 위에 마우스를 놓으면 추가 정보가 제공되는 경우도 있습니다. 이 그래픽을 통해 다음 항목을 모니터링할 수 있습니다.

참고 인터페이스 상태 정보를 비롯한 그래픽의 인터페이스 부분은 인터페이스 페이지와 모니터링 > 시스템 대시보드에서도 제공됩니다.

인터페이스 상태

포트 위에 마우스를 놓으면 해당 IP 주소와 사용 상태 및 링크 상태가 표시됩니다. IP 주소는 정적으로 할당할 수도 있고 DHCP를 사용하여 가져올 수도 있습니다. BVI(브리지 가상 인터페이스) 위에 마우스를 놓으면 구성원 인터페이스의 목록도 표시됩니다.

인터페이스 포트는 다음 색 코드를 사용합니다.

- 녹색 - 인터페이스가 구성되어 있고 활성화된 상태이며 링크가 작동합니다.
- 회색 - 인터페이스를 사용하지 않습니다.

- 주황색/빨간색 - 인터페이스가 구성되어 있고 활성화된 상태이지만 링크가 작동하지 않습니다. 유선 인터페이스의 경우 이 색은 수정해야 하는 오류 상태를 나타냅니다. 유선 인터페이스가 아닌 경우에는 이 색이 표시되는 것이 정상입니다.

내부, 외부 네트워크 연결

그래픽에는 다음 조건에 따라 외부(또는 업스트림) 및 내부 네트워크에 연결된 포트가 표시됩니다.

- 내부 네트워크 - 내부 네트워크의 포트는 이름이 "내부"인 인터페이스에 대해서만 표시됩니다. 추가 내부 네트워크는 있더라도 표시되지 않습니다. 이름을 "내부"로 지정한 인터페이스가 없으면 어떤 포트도 내부 포트로 표시되지 않습니다.
- 외부 네트워크 - 외부 네트워크의 포트는 이름이 "외부"인 인터페이스에 대해서만 표시됩니다. 내부 네트워크와 마찬가지로 이 이름은 필수 항목입니다. 이름을 지정하지 않으면 어떤 포트도 외부 포트로 표시되지 않습니다.

관리 설정 상태

그래픽에는 관리 주소에 대해 게이트웨이, DNS 서버, NTP 서버 및 스마트 라이선싱이 구성되어 있는지와 해당 설정이 올바르게 작동하고 있는지가 표시됩니다.

녹색은 기능이 구성되어 있고 정상적으로 작동함을 나타내며, 회색은 기능이 구성되어 있지 않거나 정상적으로 작동하지 않음을 나타냅니다. 예를 들어 서버에 연결할 수 없으면 DNS 상자가 회색으로 표시됩니다. 요소 위에 마우스를 올려놓으면 추가 정보가 표시됩니다.

문제가 확인되면 다음과 같이 수정하십시오.

- 관리 포트 및 게이트웨이 - **System Settings(**시스템 설정**)** > **Management Interface(**관리 인터페이스**)**를 선택합니다.
- DNS 서버 - **System Settings(**시스템 설정**)** > **DNS Server(DNS** 서버**)**를 선택합니다.
- NTP 서버 - **System Settings(**시스템 설정**)** > **NTP**를 선택합니다. NTP 트러블슈팅, 312 페이지도 참조하십시오.
- 스마트 라이선스 - 스마트 라이선스 그룹에서 **View Configuration(**컨피그레이션 보기**)** 링크를 클릭합니다.

시스템 작업 상태 보기

시스템 작업에는 다양한 데이터베이스 업데이트 검색/적용 등 사용자가 직접 개입하지 않아도 수행되는 작업이 포함됩니다. 이러한 작업 및 해당 상태의 목록을 통해 이러한 시스템 작업이 성공적으로 완료됨을 확인할 수 있습니다.

절차

단계 **1** 주 메뉴에서 작업 목록 버튼을 클릭합니다.

작업 목록이 열리고 시스템 작업의 상태와 세부정보가 표시됩니다.

단계 **2** 작업 상태를 평가합니다.
지속적으로 발생하는 문제가 있으면 디바이스 컨피그레이션을 수정해야 할 수 있습니다. 예를 들어 데이터베이스 업데이트를 가져올 때 지속적으로 장애가 발생하면 인터넷으로 이동하는 디바이스 관리 IP 주소용 경로가 없는 것일 수 있습니다. 일부 문제의 경우 작업 설명에 나와 있는 대로 Cisco TAC(Technical Assistance Center)에 문의해야 할 수 있습니다.

작업 목록을 사용하여 다음 작업을 수행할 수 있습니다.

- 성공 또는 실패 버튼을 클릭하여 이러한 상태를 기준으로 목록을 필터링합니다.
- 작업의 삭제 아이콘()을 클릭하여 목록에서 해당 작업을 제거합니다.
- 완료된 모든 작업 제거를 클릭하여 진행 중이지 않은 모든 작업의 목록을 비웁니다.

2 장

Firepower Threat Defense 활용 사례

다음 주제에서는 Firepower Device Manager를 사용하여 Firepower Threat Defense에서 수행할 수 있는 몇 가지 일반적인 작업에 대해 설명합니다. 이러한 활용 사례에서는 디바이스 컨피그레이션 마법사를 완료했으며 이 초기 컨피그레이션을 유지했다고 가정합니다. 초기 컨피그레이션을 수정했더라도 이러한 예를 통해 제품 사용 방법을 파악할 수 있습니다.

네트워크 트래픽을 파악하는 방법

초기 디바이스 설정을 완료하고 나면 인터넷 또는 기타 업스트림 네트워크에 대한 모든 내부 트래픽 액세스를 허용하는 액세스 제어 정책과, 다른 모든 트래픽을 차단하는 기본 작업이 생성됩니다. 추가 액세스 제어 규칙을 생성하기 전에 실제로 네트워크에서 생성되는 트래픽을 파악해 두면 도움이 될 수 있습니다.

Firepower Device Manager의 모니터링 기능을 사용하여 네트워크 트래픽을 분석할 수 있습니다. Firepower Device Manager 보고 기능을 통해 다음 정보를 파악할 수 있습니다.

- 네트워크가 사용되는 용도
- 네트워크를 가장 많이 사용하는 사람
- 사용자가 이동하는 위치
- 사용자가 사용 중인 디바이스
- 가장 많이 적중된 액세스 제어 규칙(정책)

초기 액세스 규칙은 정책, 대상, 보안 영역 등 트래픽에 대한 일부 정보를 제공할 수 있습니다. 그러나 사용자 정보를 파악하려면 사용자의 인증(신원 증명)을 요구하는 ID 정책을 구성해야 합니다. 네트워크에서 사용되는 애플리케이션에 대한 정보를 파악하려면 몇 가지 추가적인 조정을 수행해야 합니다.

다음 절차에서는 트래픽을 모니터링하도록 Firepower Threat Defense 디바이스를 설정하는 방법을 설명하고, 정책을 구성 및 모니터링하는 엔드 투 엔드 프로세스를 대략적으로 제시합니다.

참고 이 절차에서는 사용자가 방문하는 사이트의 웹 사이트 범주 및 평판 관련 정보는 제공하지 않습니다. 따라서 웹 범주 대시보드에서는 의미 있는 정보를 확인할 수 없습니다. 범주 및 평판 데이터를 파악하려면 범주 기반 URL 필터링을 구현하고 URL 라이선스를 사용해야 합니다. 이 정보만 파악하려는 경우 금융 서비스 등의 적절한 범주 액세스를 허용하는 새 액세스 제어 규칙을 추가하고 액세스 제어 정책의 첫 번째 규칙으로 지정할 수 있습니다. URL 필터링 구현에 대한 자세한 내용은 사용 제한 정책(URL 필터링)을 구현하는 방법, 48 페이지를 참조하십시오.

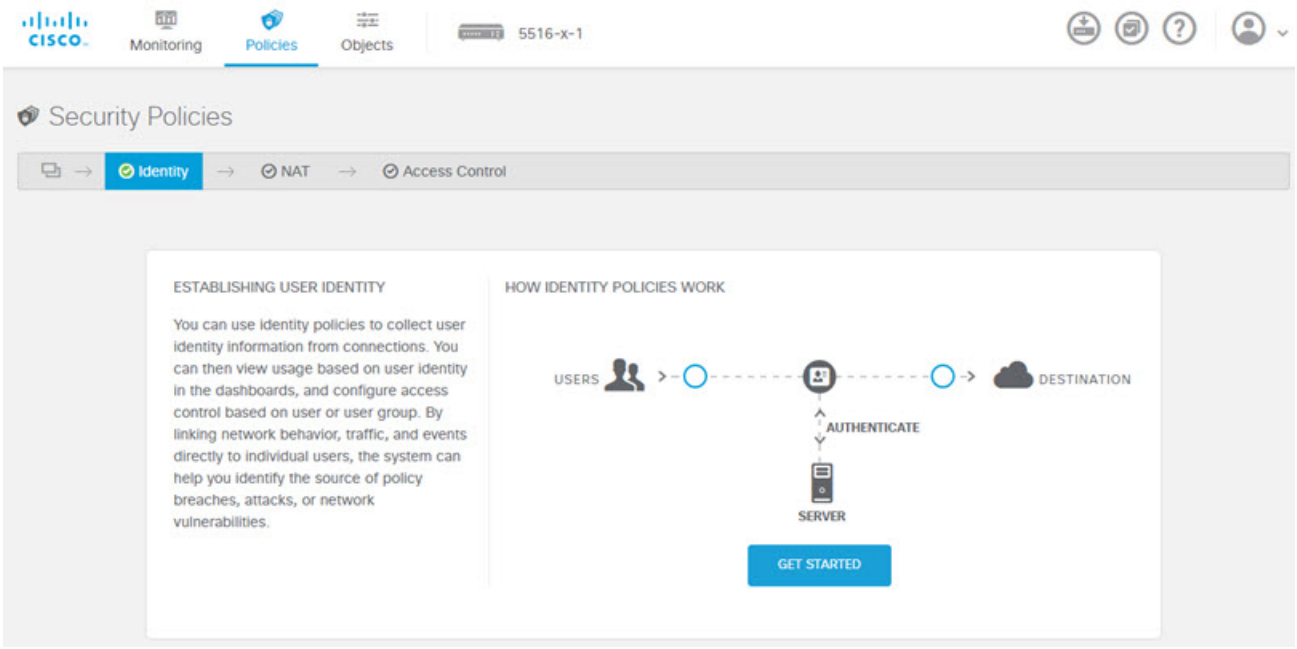
절차

단계 **1** 사용자 동작을 파악하려면 연결과 연관된 사용자를 식별할 수 있도록 ID 정책을 구성해야 합니다. ID 정책을 사용하면 네트워크를 사용 중인 사용자와 이러한 사용자가 사용하고 있는 리소스에 대한 정보를 수집할 수 있습니다. 이 정보는 사용자 모니터링 대시보드에서 제공됩니다. 이벤트 뷰어에서 표시되는 연결 이벤트에 대해서도 사용자 정보가 제공됩니다.

사용자는 HTTP 연결을 위해 웹 브라우저를 사용할 때만 인증을 받습니다.

사용자의 인증 시 장애가 발생해도 웹 연결은 차단되지 않습니다. 인증 장애는 연결을 위한 사용자 ID 정보가 없음을 의미할 뿐입니다. 원하는 경우 실패한 인증으로 표시되는 사용자의 트래픽을 삭제하는 액세스 제어 규칙을 생성할 수 있습니다.

a) 주 메뉴에서 정책을 클릭한 후 **ID**를 클릭합니다.
초기에는 ID 정책이 비활성화되어 있습니다. ID 정책은 Active Directory 서버를 통해 사용자를 인증하며, 사용자가 사용 중인 워크스테이션의 IP 주소와 사용자를 연결합니다. 그 후에 시스템은 해당 IP 주소의 트래픽을 사용자의 트래픽으로 식별합니다.



b) **Get Started**(시작하기) 버튼을 클릭하여 마법사를 시작해 필요한 요소를 구성합니다.

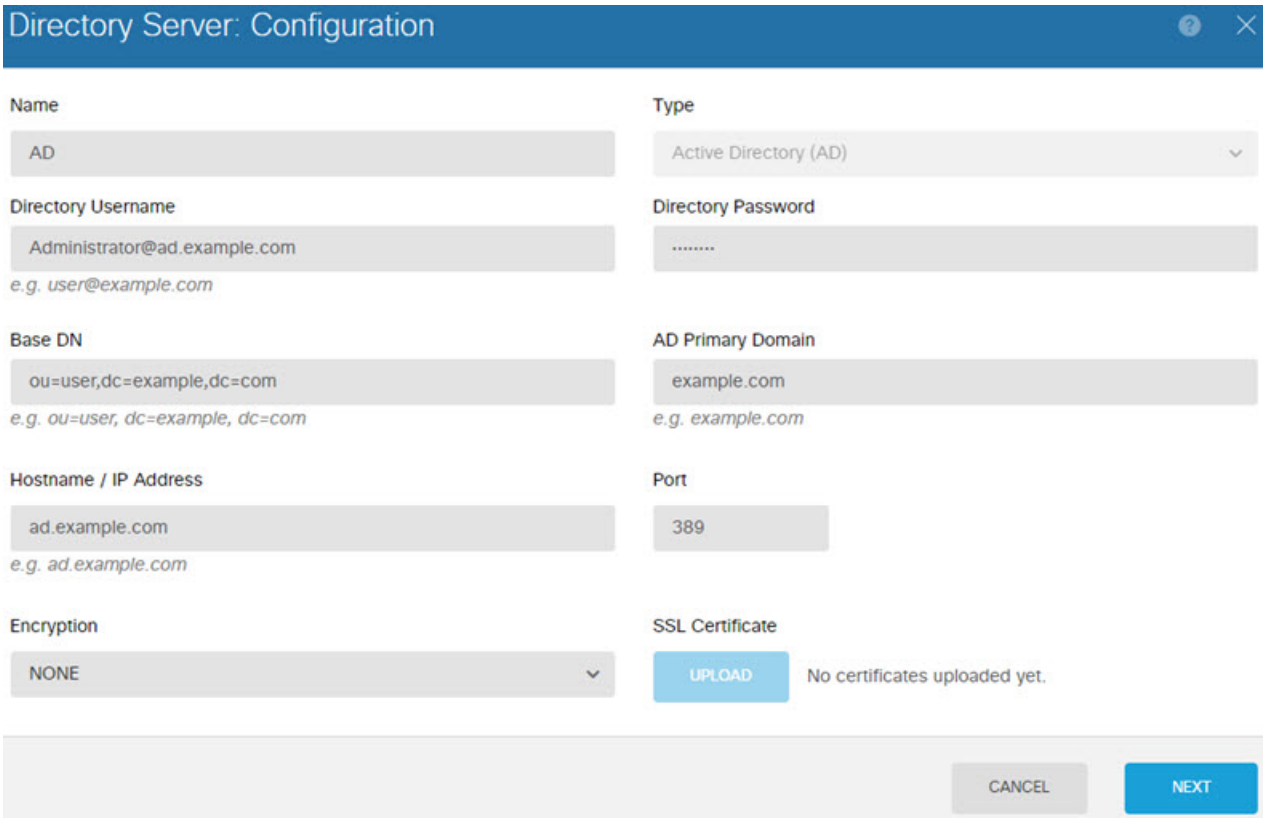
c) Active Directory 서버를 식별합니다.
다음 정보를 입력합니다.

- 이름 - 디렉터리 영역의 이름입니다.
- 유형 - 디렉터리 서버의 유형입니다. 지원되는 유형은 Active Directory뿐이며 이 필드의 내용은 변경할 수 없습니다.
- 디렉토리 사용자 이름, 디렉토리 비밀번호 - 검색하려는 사용자 정보에 대한 적절한 권한이 있는 사용자의 고유 사용자 이름 및 비밀번호입니다. admin@ad.example.com 등을 예로 들 수 있습니다.
- 기본 **DN** - 사용자 및 그룹 정보를 검색하거나 쿼리하기 위한 디렉터리 트리, 즉 사용자와 그룹의 공통 상위 항목입니다. dc=example,dc=com을 예로 들 수 있습니다. 기본 DN을 찾는 방법에 대한 자세한 내용은 디렉터리 기본 DN 결정, 129 페이지를 참조하십시오.
- **AD** 기본 도메인 - 디바이스가 죠인해야 하는 정규화된 Active Directory 도메인 이름입니다. example.com 등을 예로 들 수 있습니다.
- 호스트 이름/**IP** 주소 - 디렉토리 서버의 호스트 이름 또는 IP 주소입니다. 서버에 대한 암호화된 연결을 사용하는 경우에는 IP 주소가 아닌 FQDN(Fully-Qualified Domain Name)을 입력해야 합니다.
- 포트 - 서버와의 통신에 사용되는 포트 번호입니다. 기본값은 389입니다. 암호화 방법으로 LDAPS를 선택하는 경우에는 포트 636을 사용합니다.
- 암호화 - 사용자 및 그룹 정보를 다운로드하기 위해 암호화된 연결을 사용하려는 경우에는 **STARTTLS** 또는 **LDAPS** 중에서 원하는 방법을 선택합니다. 기본값은 없음입니다. 이 옵션은 사용자 및 그룹 정보를 일반 텍스트로 다운로드함을 의미합니다.

- **STARTTLS**는 암호화 방법을 협상하여 디렉터리 서버가 지원하는 가장 강력한 방법을 사용하며 포트 389를 사용합니다.
- **LDAPS**를 선택하는 경우 LDAP over SSL이 필요합니다. 이 옵션은 포트 636을 사용합니다.

• **SSL** 인증서 - 암호화 방법을 선택하는 경우 CA 인증서를 업로드하여 시스템과 디렉터리 서버 간에 신뢰할 수 있는 연결을 설정합니다. 인증서를 사용하여 인증하는 경우에는 인증서의 서버 이름이 서버 호스트 이름/IP 주소와 일치해야 합니다. 예를 들어 IP 주소로 10.10.10.250을 사용하는데 인증서의 주소는 ad.example.com이면 연결은 실패합니다.

예제:
예를 들어 다음 그림에는 ad.example.com 서버에 대해 암호화되지 않은 연결을 생성하는 방법이 나와 있습니다. 여기서 기본 도메인은 example.com이고 디렉토리 사용자 이름은 Administrator@ad.example.com입니다. 모든 사용자 및 그룹 정보는 DN(고유 이름) ou=user,dc=example,dc=com 아래에 있습니다.



d) **Next(**다음**)**를 클릭합니다.
e) 액티브 인증 캡티브 포털을 구성합니다.
가장 간단한 옵션은 모든 필드를 그대로 두고 **Save(**저장**)**를 클릭하는 것입니다. 액티브 인증의 기본 포트를 구성하면 사용자가 사용자 이름 및 비밀번호를 제공하기 위해 신뢰해야 하는 셀프 서명

한 인증서를 받게 됩니다. 사용자에게 이러한 과정은 정상적인 현상이며 인증서를 수락해야 함을 알리십시오.

그러나 사용자의 브라우저에서 이미 신뢰하는 인증서를 업로드하는 것이 가장 좋습니다. 이러한 인증서가 있으면 다음 필드에 내용을 입력하여 해당 인증서를 사용합니다.

- 서버 인증서 - 활성 인증 중에 사용자에게 제공할 CA 인증서입니다. 인증서는 PEM 또는 DER 형식의 X509 인증서여야 합니다. 인증서를 붙여넣거나 인증서 업로드를 클릭하고 인증서 파일을 선택합니다. 기본적으로는 사용자 인증 중에 자체 서명 인증서가 제공됩니다.
- 인증서 키 - 서버 인증서의 키입니다. 키를 붙여넣거나 키 업로드를 클릭하고 키 파일을 선택합니다.
- 포트 - 종속 포털 포트입니다. 기본값은 885(TCP)입니다. 다른 포트를 구성하는 경우에는 포트가 1025-65535 범위에 포함되어야 합니다.

f) **Save(**저장**)**를 클릭합니다.
이것으로 설정 마법사가 완료되었습니다. 이제 액티브 인증을 요구하는 ID 규칙을 생성합니다.

g) **ID** 규칙 생성 버튼 또는 + 버튼을 클릭합니다.

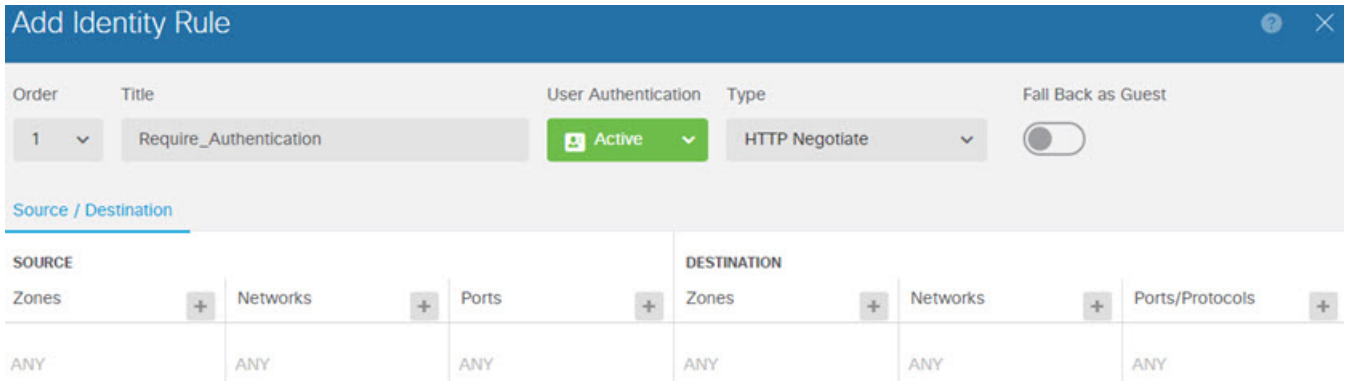
h) ID 규칙 속성을 입력합니다.
모든 사용자에게 인증을 요구한다고 가정할 때 다음 설정을 사용할 수 있습니다.

- 이름 - Require_Authentication 등의 원하는 이름을 선택하면 됩니다.
- 사용자 인증 - 활성이 이미 선택되어 있으므로 그대로 유지합니다.
- 유형 - **HTTP** 협상을 선택합니다. 이 옵션을 선택하면 브라우저와 디렉터리 서버가 가장 강력한 인증 프로토콜(NTLM->HTTP 기본 순서)을 협상할 수 있습니다.

  참고 HTTP 기본, HTTP 대응 페이지 및 NTLM 인증 방법의 경우 사용자는 인터페이스의 IP 주소를 사용하여 종속 포털로 리디렉션됩니다. 그러나 HTTP 협상의 경우에는 사용자가 정규화된 DNS 이름 *firewall-hostname.AD-domain-name*을 사용하여 리디렉션됩니다. HTTP 협상을 사용하려는 경우에는 DNS 서버도 업데이트하여 활성 인증을 수행해야 하는 모든 내부 인터페이스의 IP 주소에 이 이름을 매핑해야 합니다. 이렇게 하지 않으면 리디렉션을 완료할 수 없으며 사용자가 인증할 수 없습니다. 수행할 수 없거나 원치 않는 경우 DNS 서버를 업데이트하고 다른 인증 방법 중 하나를 선택합니다.

- 소스/대상 - 모든 필드의 값을 기본값인 임의로 유지합니다.

보다 제한적인 트래픽 집합으로 정책을 적절하게 제한할 수 있습니다. 그러나 HTTP 트래픽에 대해서만 액티브 인증을 시도하므로 비HTTP 트래픽이 소스/대상 기준과 일치하는지 여부는 관계가 없습니다. ID 정책 속성에 대한 자세한 내용은 ID 규칙 구성, 134 페이지를 참조하십시오.

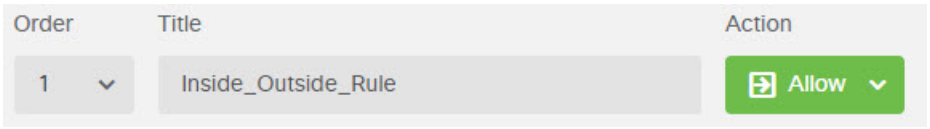


i) **OK(**확인**)**를 클릭하여 규칙을 추가합니다.
이제 창 오른쪽 상단의 구축 아이콘 버튼에 점이 나타납니다. 이 점은 구축되지 않은 변경 사항이 있음을 나타냅니다. 사용자 인터페이스에서 변경을 수행한다고 해서 디바이스에서 변경 사항이 구성되는 것은 아니며, 변경 사항을 구축해야 합니다. 따라서 관련 변경 집합을 먼저 수행한 후에 변경 사항을 구축하면 부분적으로 구성된 변경 사항 집합이 디바이스에서 실행되는 문제가 발생할 가능성이 없습니다. 이 절차의 뒷부분에서 변경 사항을 구축할 것입니다.

단계 **2** Inside_Outside_Rule 액세스 제어 규칙의 작업을 허용으로 변경합니다.
Inside_Outside_Rule 액세스 규칙은 신뢰 규칙으로 생성됩니다. 그러나 신뢰할 수 있는 트래픽은 검사되지 않으므로, 트래픽 일치 기준에 영역, IP 주소 및 포트 외의 기타 조건이나 애플리케이션이 포함되어 있지 않으면 시스템은 신뢰할 수 있는 트래픽의 일부 특성(예: 애플리케이션)을 확인할 수 없습니다. 트래픽을 신뢰하는 대신 허용하도록 규칙을 변경하면 시스템이 트래픽을 완전히 검사합니다.

참고 (ASA 5506-X 모델) Inside_Inside_Rule도 신뢰에서 허용으로 변경하는 것이 좋습니다. 이 규칙은 내부 인터페이스 간에 이동하는 트래픽에 적용됩니다.

a) **Policies(**정책**)** 페이지에서 **Access Control(**액세스 제어**)**을 클릭합니다.
b) Inside_Outside_Rule 행 오른쪽의 작업 셀 위에 마우스를 올려 놓고 수정 및 삭제 아이콘이 표시되면 수정 아이콘( )을 클릭하여 규칙을 엽니다.
c) 작업에 대해 허용을 선택합니다.

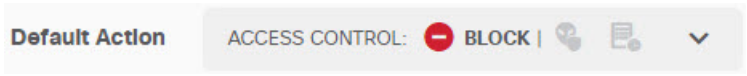


d) **OK(**확인**)**를 클릭하여 변경 사항을 저장합니다.

단계 **3** 액세스 제어 정책 기본 작업에 대해 로깅을 사용합니다.
연결이 연결 로깅을 사용하는 액세스 제어 규칙과 일치하는 경우에만 대시보드에 연결 관련 정보가 포함됩니다. Inside_Outside_Rule은 로깅을 사용하지만 기본 작업에서는 로깅이 비활성화됩니다. 따

라서 대시보드에는 Inside_Outside_Rule에 대한 정보만 표시되며 규칙과 일치하지 않는 연결은 대시보드에 반영되지 않습니다.

a) 액세스 제어 정책 페이지 하단의 기본 작업에서 아무 곳이나 클릭합니다.



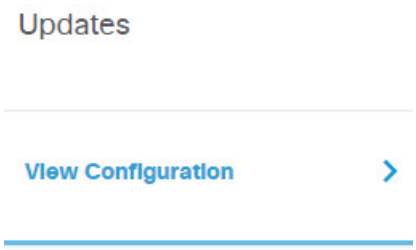
b) **Select Log Action**(로그 작업 선택) > **At Beginning and End of Connection**(연결 시작 및 종료 시)을 선택합니다.

c) **OK**(확인)를 클릭합니다.

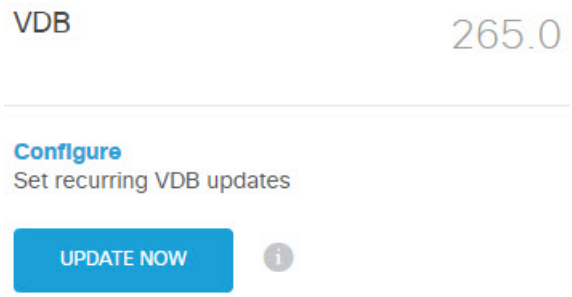
단계 **4** VDB(Vulnerability Database)의 업데이트 일정을 설정합니다.
Cisco는 VDB 업데이트를 정기적으로 제공합니다. 이 업데이트에는 연결에서 사용되는 애플리케이션을 식별할 수 있는 애플리케이션 탐지기가 포함됩니다. VDB는 정기적으로 업데이트해야 합니다. 업데이트는 수동으로 다운로드할 수도 있고 정기 일정을 설정할 수도 있습니다. 다음 절차에서는 일정을 설정하는 방법을 보여줍니다. VDB 업데이트는 기본적으로 비활성화되므로 VDB 업데이트를 받기 위한 작업을 수행해야 합니다.

a) 디바이스을 클릭합니다.

b) 업데이트 그룹에서 **View Configuration**(컨피그레이션 보기)을 클릭합니다.

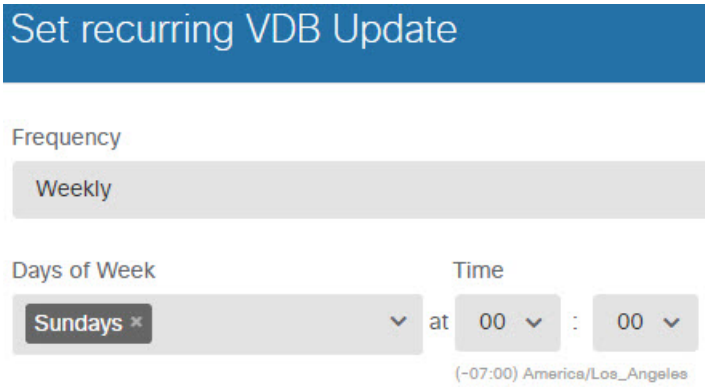


c) VDB 그룹에서 **Configure**(구성)를 클릭합니다.



d) 업데이트 일정을 정의합니다.
네트워크에 영향을 주지 않는 시간과 빈도를 선택합니다. 또한 시스템은 업데이트를 다운로드한 후에 자동 구축을 수행합니다. 새 탐지기를 사용하려면 자동 구축을 수행해야 합니다. 따라서 수행하고 저장했지만 구축하지는 않은 컨피그레이션 변경 사항도 구축됩니다.

예를 들어 다음 일정은 매주 일요일 자정(24시간 표기법 사용)에 VDB를 업데이트합니다.

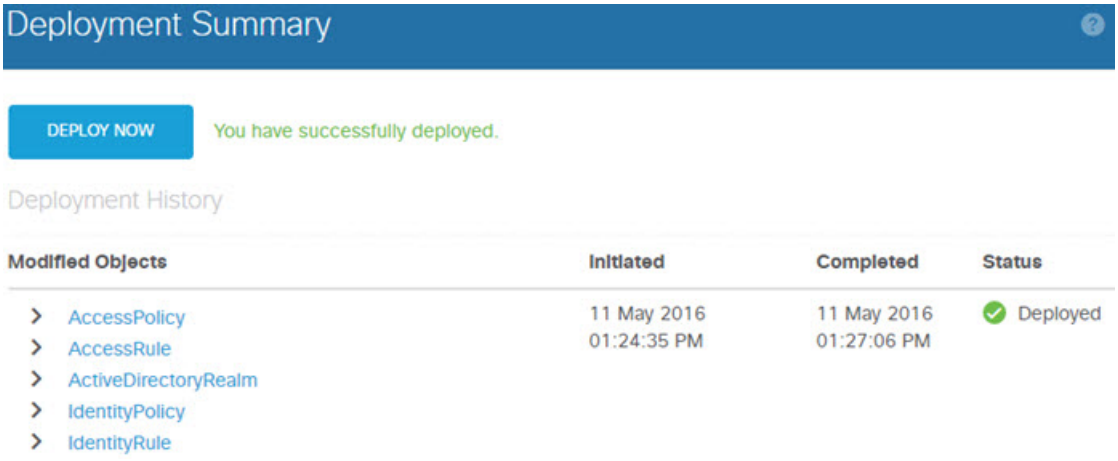


e) **Save(**저장**)**를 클릭합니다.

단계 **5** 변경 사항을 커밋합니다.

a) 웹 페이지의 오른쪽 상단에 있는 변경 사항 구축 아이콘을 클릭합니다.

b) **Deploy Now(**지금 구축**)** 버튼을 클릭하고 구축이 완료될 때까지 기다립니다.
구축 요약에는 변경 사항을 성공적으로 구축했다는 메시지가 표시되며, 작업 상태는 구축됨으로 설정됩니다.



다음에 할 작업

이 시점부터 모니터링 대시보드 및 이벤트에 사용자 및 애플리케이션에 대한 정보가 표시됩니다. 이 정보를 평가하여 부적절한 패턴이 있는지 확인하고 허용할 수 없는 사용을 제한하는 새 액세스 규칙을 개발할 수 있습니다.

침입 및 악성코드 관련 정보 수집을 시작하려면 하나 이상의 액세스 규칙에 대해 침입 및 파일 정책을 사용해야 합니다. 또한 이러한 기능에 대한 라이선스도 사용해야 합니다.

웹 범주 관련 정보 수집을 시작하려면 URL 필터링을 구현해야 합니다.

위협을 차단하는 방법

액세스 제어 규칙에 침입 정책을 추가하여 차세대 IPS(침입 방지 시스템) 필터링을 구현할 수 있습니다. 침입 정책은 네트워크 트래픽을 분석하여 트래픽 콘텐츠와 알려진 위협을 비교합니다. 연결이 모니터링 대상 위협과 일치하는 경우 시스템은 연결을 삭제하여 공격을 방지합니다.

기타 모든 트래픽 처리는 네트워크 트래픽에서 침입을 검사하기 전에 수행됩니다. 침입 정책을 액세스 제어 규칙과 연결하여 시스템이 액세스 제어 규칙의 조건과 일치하는 트래픽을 통과시키기 전에 침입 정책을 사용하여 트래픽을 먼저 검사하도록 명령할 수 있습니다.

트래픽을 허용하는 규칙에 대해서만 침입 정책을 구성할 수 있습니다. 트래픽을 신뢰 또는 차단하도록 설정된 규칙에 대해서는 검사가 수행되지 않습니다. 또한 기본 작업이 허용인 경우 기본 작업의 일부분으로 침입 정책을 구성할 수 있습니다.

Cisco는 Firepower System에서 여러 침입 정책을 제공합니다. 이러한 정책은 Cisco Talos Security Intelligence and Research Group에서 설계했습니다. 여기서는 고급 설정과 침입 및 전처리기 규칙 구문 상태를 설정합니다.

절차

단계 **1** 위협 라이선스를 아직 활성화하지 않은 경우 활성화합니다.
침입 정책을 사용하려면 위협 라이선스를 활성화해야 합니다. 현재 평가 라이선스를 사용 중인 경우에는 라이선스의 평가 버전이 활성화됩니다. 디바이스를 등록한 경우 필요한 라이선스를 구매해 Cisco.com에서 Smart Software Manager 어카운트에 추가해야 합니다.

a) 디바이스을 클릭합니다.

b) 스마트 라이선스 그룹에서 **View Configuration(**컨피그레이션 보기**)**을 클릭합니다.

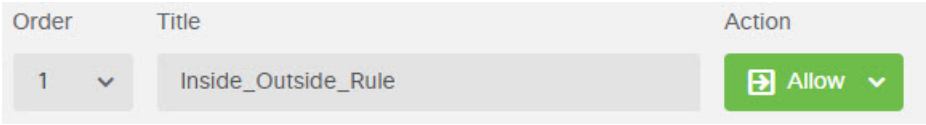
c) **Threat(**위협**)** 그룹에서 **Enable(**활성화**)**을 클릭합니다.
시스템이 적절하게 어카운트에 라이선스를 등록하거나 평가 라이선스를 사용 설정합니다. 그룹에 라이선스가 활성화되었다는 메시지가 표시되며 버튼이 비활성화 버튼으로 변경됩니다.

단계 **2** 하나 이상의 액세스 규칙에 대해 침입 정책을 선택합니다.
위협을 검사해야 하는 트래픽에 적용할 규칙을 결정합니다. 이 예에서는 Inside_Outside_Rule에 침입 검사를 추가합니다. ASA 5506-X 모델의 경우 Inside_Inside_Rule에도 침입 검사를 추가할 수 있습니다.

a) 주 메뉴에서 **Policies(**정책**)**를 클릭합니다.
액세스 제어 정책이 표시되는지 확인합니다.

b) Inside_Outside_Rule 행 오른쪽의 작업 셀 위에 마우스를 올려 놓고 수정 및 삭제 아이콘이 표시되면 수정 아이콘( )을 클릭하여 규칙을 엽니다.

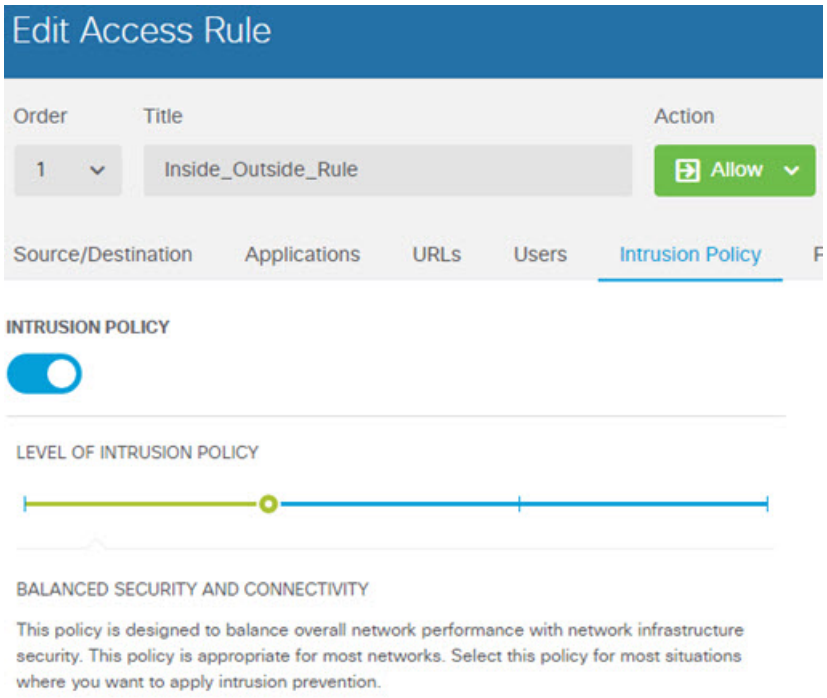
c) 작업에 대해 허용을 아직 선택하지 않았으면 선택합니다.



d) **Intrusion Policy(**침입 정책**)** 탭을 클릭합니다.

e) 침입 정책 토글을 클릭하여 정책을 활성화한 다음 슬라이더에서 침입 정책의 레벨을 선택합니다. 정책은 안전성이 가장 낮은 항목부터 가장 높은 항목 순서로 나열됩니다. 균형 잡힌 보안 및 연결성 정책은 대부분의 네트워크에 적합합니다. 이 정책은 과도하게 적극적이지 않은 적절한 침입 방어 기능을 제공합니다. 침입 방지 기능이 너무 적극적이면 삭제되면 안 되는 트래픽이 삭제될 수 있습니다. 트래픽이 너무 많이 삭제되는지 확인하려는 경우 연결이 보안에 우선함 정책을 선택하여 침입 검사의 레벨을 높일 수 있습니다.

적극적인 보안을 적용해야 하는 경우에는 보안이 연결에 우선함 정책을 사용해 보십시오. 최대 탐지 정책은 네트워크 인프라 보안을 더욱 강화하며, 사용하는 경우 운영에 더 큰 영향을 미칠 수 있습니다.



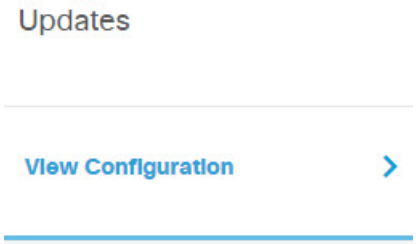
f) **OK(**확인**)**를 클릭하여 변경 사항을 저장합니다.

단계 **3** 침입 규칙 데이터베이스의 업데이트 일정을 설정합니다.

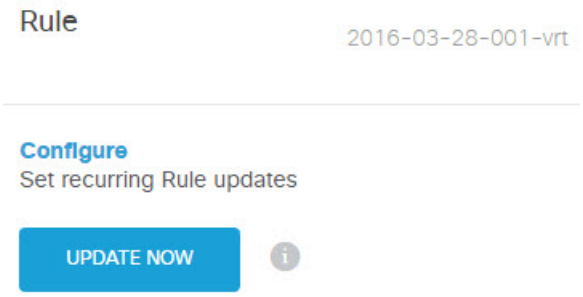
Cisco는 침입 정책이 연결을 삭제해야 하는지 여부를 결정하는 데 사용하는 침입 규칙 데이터베이스에 대한 업데이트를 정기적으로 제공합니다. 규칙 데이터베이스는 정기적으로 업데이트해야 합니다. 업데이트는 수동으로 다운로드할 수도 있고 정기 일정을 설정할 수도 있습니다. 다음 절차에서는 일정을 설정하는 방법을 보여줍니다. 기본값으로 데이터베이스 업데이트는 비활성화되므로 업데이트된 규칙을 받기 위한 작업을 수행해야 합니다.

a) 디바이스을 클릭합니다.

b) 업데이트 그룹에서 컨피그레이션 보기를 클릭합니다.

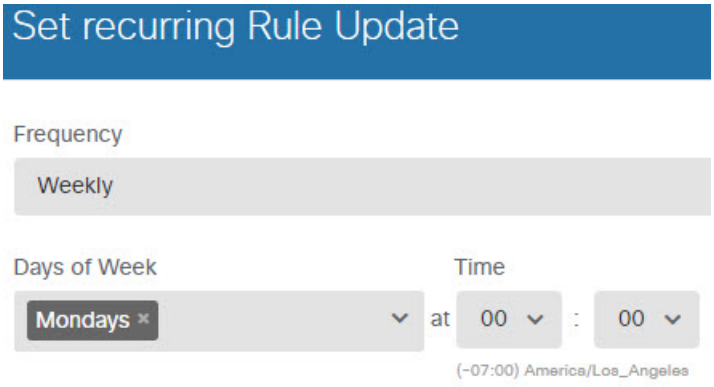


c) 규칙 그룹에서 구성을 클릭합니다.



d) 업데이트 일정을 정의합니다.
네트워크에 영향을 주지 않는 시간과 빈도를 선택합니다. 또한 시스템은 업데이트를 다운로드한 후에 자동 구축을 수행합니다. 새 규칙을 사용하려면 자동 구축을 수행해야 합니다. 따라서 수행하고 저장했지만 구축하지는 않은 컨피그레이션 변경 사항도 구축됩니다.

예를 들어 다음 일정은 매주 월요일 자정(24시간 표기법 사용)에 규칙 데이터베이스를 업데이트합니다.



e) **Save**(저장)를 클릭합니다.

단계 **4** 변경 사항을 커밋합니다.

a) 웹 페이지의 오른쪽 상단에 있는 변경 사항 구축 아이콘을 클릭합니다.

b) **Deploy Now**(지금 구축) 버튼을 클릭하고 구축이 완료될 때까지 기다립니다.
구축 요약에는 변경 사항을 성공적으로 구축했다는 메시지가 표시되며, 작업 상태는 구축됨으로 설정됩니다.

다음에 할 작업

이 시점부터 모니터링 대시보드 및 이벤트에 공격자, 대상 및 위협에 대한 정보가 표시됩니다(침입이 식별된 경우). 이 정보를 평가하여 네트워크에 추가 보안 조치가 필요한지 아니면 사용 중인 침입 정책의 레벨을 낮춰야 하는지를 결정할 수 있습니다.

악성코드를 차단하는 방법

사용자가 인터넷 사이트 또는 이메일 등의 기타 통신 방법을 통해 악성 소프트웨어(악성코드)를 유입할 위험성은 항상 존재합니다. 신뢰할 수 있는 웹 사이트 역시 하이재킹되어 이러한 사이트를 의심하지 않는 사용자에게 악성코드를 전파할 수 있습니다. 웹 페이지는 여러 소스에서 제공되는 개체를 포함할 수 있습니다. 이러한 개체에는 이미지, 실행 파일, Javascript, 광고 등이 포함될 수 있습니다. 보안 침해된 웹 사이트의 경우 외부 소스에서 호스팅되는 개체가 통합되어 있는 경우가 많습니다. 철저한 보안을 유지하려면 초기 요청뿐 아니라 각 개체를 개별적으로 확인해야 합니다.

파일 정책을 사용하여 Advanced Malware Protection for Firepower(AMP for Firepower)를 통해 악성코드를 탐지합니다. 파일 제어를 수행하는 데에도 파일 정책을 사용할 수 있습니다. 그러면 파일에 악성코드가 있는지와 관계없이 특정 유형의 모든 파일에 대한 제어가 가능합니다.

AMP for Firepower는 AMP 클라우드를 사용하여 네트워크 트래픽에서 탐지될 가능성이 있는 악성코드의 상태를 검색합니다. 관리 인터페이스에는 AMP 클라우드에 연결하고 악성코드 조회를 수행하기 위한 인터넷으로 연결되는 경로가 있어야 합니다. 디바이스는 적합한 파일을 탐지하면 파일의 SHA-256 해시 값을 사용하여 AMP 클라우드에서 파일의 상태를 쿼리합니다. 가능한 상태는 정상, 악성코드 또는 알 수 없음(명확한 판정 없음)입니다. AMP 클라우드에 연결할 수 없는 경우의 상태는 알 수 없음입니다.

파일 정책을 액세스 제어 규칙과 연결하여 시스템이 액세스 제어 규칙의 조건과 일치하는 트래픽을 통과시키기 전에 연결의 파일을 먼저 검사하도록 명령할 수 있습니다.

트래픽을 허용하는 규칙에 대해서만 파일 정책을 구성할 수 있습니다. 트래픽을 신뢰 또는 차단하도록 설정된 규칙에 대해서는 검사가 수행되지 않습니다.

절차

단계 **1** 악성코드 라이선스를 아직 활성화하지 않은 경우 활성화합니다.
악성코드 제어를 위한 파일 정책을 사용하려면 악성코드 라이선스를 활성화해야 합니다. 현재 평가 라이선스를 사용 중인 경우에는 라이선스의 평가 버전이 활성화됩니다. 디바이스를 등록한 경우 필요한 라이선스를 구매해 Cisco.com에서 Smart Software Manager 어카운트에 추가해야 합니다.

a) 디바이스을 클릭합니다.

b) 스마트 라이선스 그룹에서 **View Configuration**(컨피그레이션 보기)을 클릭합니다.

c) **Malware**(악성코드) 그룹에서 **Enable**(사용)을 클릭합니다.

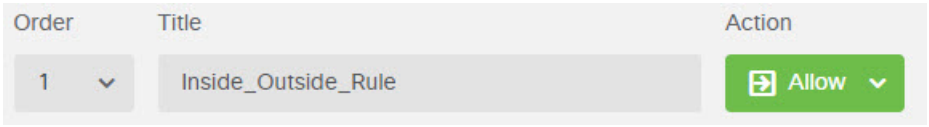
시스템이 적절하게 어카운트에 라이선스를 등록하거나 평가 라이선스를 사용 설정합니다. 그룹에 라이선스가 활성화되었다는 메시지가 표시되며 버튼이 비활성화 버튼으로 변경됩니다.

단계 **2** 하나 이상의 액세스 규칙에 대해 파일 정책을 선택합니다.
악성코드를 검사해야 하는 트래픽에 적용할 규칙을 결정합니다. 이 예에서는 Inside_Outside_Rule에 파일 검사를 추가합니다. ASA 5506-X 모델의 경우 Inside_Inside_Rule에도 파일 검사를 추가할 수 있습니다.

a) 주 메뉴에서 **Policies(**정책**)**를 클릭합니다.
액세스 제어 정책이 표시되는지 확인합니다.

b) Inside_Outside_Rule 행 오른쪽의 작업 셀 위에 마우스를 올려 놓고 수정 및 삭제 아이콘이 표시되면 수정 아이콘( )을 클릭하여 규칙을 엽니다.

c) 작업에 대해 허용을 아직 선택하지 않았으면 선택합니다.

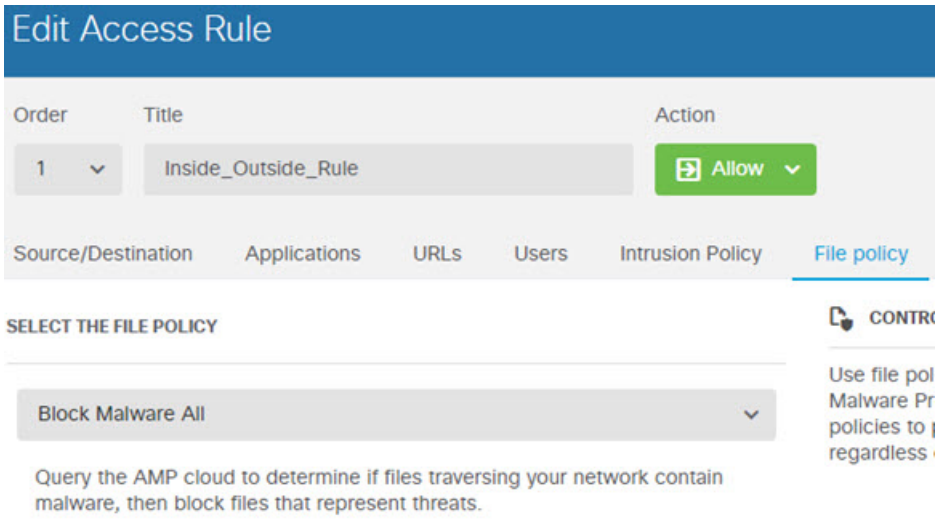


d) **File Policy(**파일 정책**)** 탭을 클릭합니다.

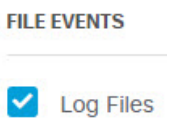
e) 사용하려는 파일 정책을 클릭합니다.
선택할 수 있는 주요 항목은 악성코드로 간주되는 모든 파일을 삭제하는 악성코드 모두 차단이나, 파일 상태를 확인하기 위해 AMP 클라우드를 쿼리하지만 차단은 수행하지 않는 모두 클라우드 조회입니다. 먼저 파일을 평가하는 방법을 확인하려는 경우 클라우드 조회를 사용합니다. 파일을 평가하는 방법이 적절한 경우 나중에 차단 정책으로 전환할 수 있습니다.

악성코드를 차단하는 다른 정책도 제공됩니다. 이러한 정책은 파일 제어와 결합되어 Microsoft Office 또는 Office 및 PDF, 문서 업로드를 차단합니다. 즉, 이러한 정책은 악성코드를 차단할 뿐 아니라 사용자가 다른 네트워크로 이러한 파일 유형을 전송할 수 없도록 합니다. 요구에 맞는 경우 이러한 정책을 선택하면 됩니다.

이 예에서는 악성코드 모두 차단을 선택합니다.



f) 로깅 탭을 클릭하고 파일 이벤트 아래에서 로그 파일이 선택되어 있는지 확인합니다.
기본값으로, 파일 정책을 선택할 때마다 파일 로깅이 사용됩니다. 이벤트와 대시보드에서 파일 및 악성코드 정보를 확인하려면 파일 로깅을 활성화해야 합니다.



g) **OK(**확인**)**를 클릭하여 변경 사항을 저장합니다.

단계 **3** 변경 사항을 커밋합니다.

a) 웹 페이지의 오른쪽 상단에 있는 변경 사항 구축 아이콘을 클릭합니다.

b) **Deploy Now(**지금 구축**)** 버튼을 클릭하고 구축이 완료될 때까지 기다립니다.
구축 요약에는 변경 사항을 성공적으로 구축했다는 메시지가 표시되며, 작업 상태는 구축됨으로 설정됩니다.

다음에 할 작업

이 시점부터 모니터링 대시보드 및 이벤트에 파일 유형과 파일 및 악성코드 이벤트에 대한 정보가 표시됩니다(파일 또는 악성코드가 전송된 경우). 이 정보를 평가하여 네트워크에 파일 전송과 관련된 추가 보안 조치가 필요한지를 결정할 수 있습니다.

사용 제한 정책(URL 필터링)을 구현하는 방법

네트워크에 대한 사용 제한 정책이 있을 수 있습니다. 사용 제한 정책은 조직에서 적절한 네트워크 활동과 부적절한 것으로 간주되는 활동을 구별합니다. 이러한 정책은 대개 인터넷 사용량을 중점적으로 파악하며 생산성을 유지하고, 법적 책임을 방지(예: 적대적이지 않은 업무 환경 유지)하고, 웹 트래픽을 전반적으로 제어할 수 있도록 작성되어 있습니다.

URL 필터링을 사용하여 액세스 정책을 통해 사용 제한 정책을 정의할 수 있습니다. 그러면 도박 등의 광범위한 범주를 필터링할 수 있으므로 차단해야 하는 모든 개별 웹 사이트를 식별할 필요가 없습니다. 범주가 일치하는 경우 허용하거나 차단할 사이트의 상대적 평판을 지정할 수도 있습니다. 사용자가 해당 카테고리 및 평판 조합을 가진 URL 검색을 시도하는 모든 경우, 세션이 차단됩니다.

범주 및 평판 데이터를 사용하면 정책 생성 및 관리도 간소화됩니다. 이를 통해 시스템이 웹 트래픽을 예상대로 제어할 수 있습니다. 마지막으로, Cisco의 위협 인텔리전스는 새로운 URL, 새로운 범주 및 기존 URL의 새로운 범주와 위험이 적용되어 지속적으로 업데이트되므로 시스템은 최신 정보를 사용하여 요청된 URL을 필터링할 수 있습니다. 악성코드, 스팸, 봇넷, 피싱과 같은 보안 위협을 나타내는 악성 사이트는 새로운 정책을 업데이트하고 구축하는 것보다 빠르게 나타났다 사라질 수 있습니다.

다음 절차에서는 URL 필터링을 사용하여 사용 제한 정책을 구현하는 방법을 설명합니다. 이 예시에서는 여러 범주의 사이트(모든 평판), 높은 위험 소셜 네트워킹 사이트 및 분류되지 않은 사이트인 badsite.example.com을 차단합니다.

절차

단계 **1** **URL** 라이선스를 아직 활성화하지 않은 경우 활성화합니다.
웹 범주 및 평판 정보를 사용하거나 대시보드 및 이벤트에서 해당 정보를 확인하려면 URL 라이선스를 활성화해야 합니다. 현재 평가 라이선스를 사용 중인 경우에는 라이선스의 평가 버전이 활성화됩니다. 디바이스를 등록한 경우 필요한 라이선스를 구매해 Cisco.com에서 Smart Software Manager 어카운트에 추가해야 합니다.

a) 디바이스을 클릭합니다.
b) 스마트 라이선스 그룹에서 **View Configuration**(컨피그레이션 보기)을 클릭합니다.

c) **URL** 라이선스 그룹에서 **Enable**(사용)을 클릭합니다.
시스템이 적절하게 어카운트에 라이선스를 등록하거나 평가 라이선스를 사용 설정합니다. 그룹에 라이선스가 활성화되었다는 메시지가 표시되며 버튼이 비활성화 버튼으로 변경됩니다.

단계 **2** URL 필터링 액세스 제어 규칙을 생성합니다.
차단 규칙을 만들기 전에 먼저 사용자들이 방문하는 사이트의 범주를 확인하고자 할 수 있습니다. 이 경우 금융 서비스와 같이 허용 가능한 범주에 대해 허용 작업을 사용하여 규칙을 생성할 수 있습니다. URL이 이 범주에 속하는지를 확인하려면 모든 웹 연결을 검사해야 하므로, 금융 서비스 사이트 이외의 사이트에 대해서도 범주 정보를 가져와야 합니다.

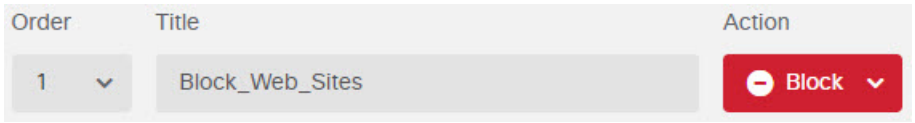
하지만 차단할 것임을 이미 알고 있는 웹 범주도 있을 수 있습니다. 차단 정책은 검사도 강제 수행하므로 차단된 범주뿐 아니라 차단되지 않은 범주에 대한 연결 관련 범주 정보도 가져오게 됩니다.

a) 주 메뉴에서 **Policies(**정책**)**를 클릭합니다.
액세스 제어 정책이 표시되는지 확인합니다.

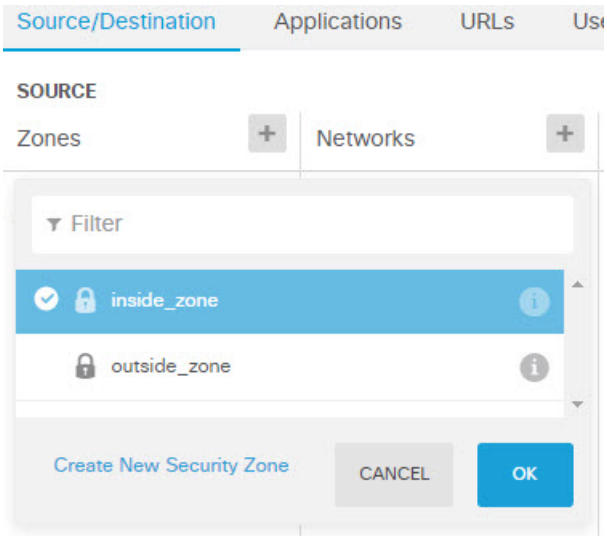
b) +를 클릭하여 새 규칙을 추가합니다.

c) 순서, 제목 및 작업을 구성합니다.

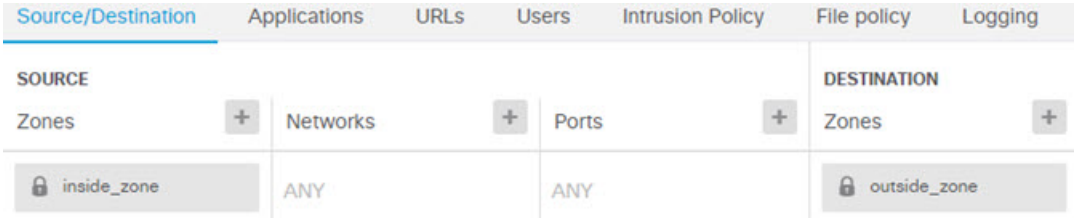
- 순서 - 기본적으로는 액세스 제어 정책 끝에 새 규칙을 추가합니다. 그러나 같은 원본/대상 및 기타 기준과 일치하는 규칙 앞(위)에 이 규칙을 배치해야 합니다. 그렇지 않으면 규칙이 어떤 항목과도 일치하지 않게 됩니다. 연결은 하나의 규칙, 즉 테이블에서 첫 번째로 일치하는 규칙에만 일치합니다. 이 규칙에서는 초기 디바이스 컨피그레이션 중에 생성한 Inside_Outside_Rule과 같은 소스/대상을 사용합니다. 다른 규칙도 생성했을 수 있습니다. 액세스 제어 효율성을 최대화하려면 특정 규칙을 미리 생성해 두는 것이 좋습니다. 그러면 연결을 허용할지 아니면 삭제할지를 가장 빠르게 결정할 수 있습니다. 이 예시에서는 규칙 순서로 **1**을 선택합니다.
- 제목 - Block_Web_Sites와 같이 의미 있는 이름을 규칙에 지정합니다.
- 작업 - 차단을 선택합니다.



d) 소스/대상 탭에서 소스 > 영역의 +를 클릭하고 **inside_zone**을 선택한 후에 영역 대화 상자에서 **OK(**확인**)**를 클릭합니다.
기준을 추가하는 과정도 동일한 방식으로 수행합니다. +를 클릭하면 열리는 작은 대화 상자에서 추가할 항목을 클릭합니다. 여러 항목을 클릭할 수 있으며, 선택한 항목을 클릭하면 선택이 취소됩니다. 선택한 항목에는 확인 표시가 나타납니다. 그러나 **OK(**확인**)** 버튼을 클릭할 때까지는 정책에 아무 항목도 추가되지 않으므로 항목만 선택하는 것으로는 충분하지 않습니다.

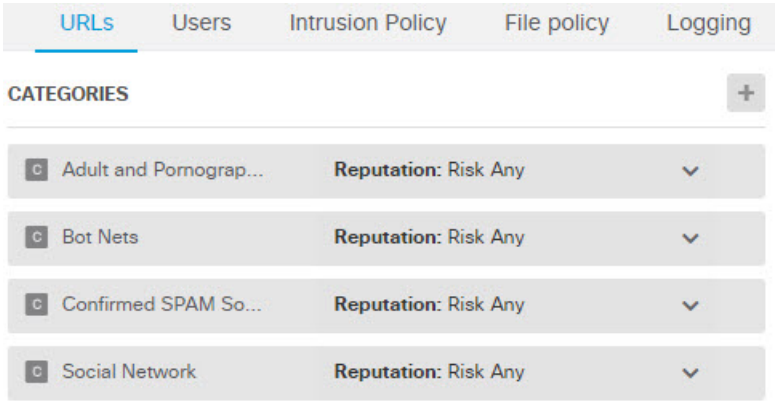


e) 동일한 기술을 사용하여 대상 > 영역에 대해 **outside_zone**을 선택합니다.

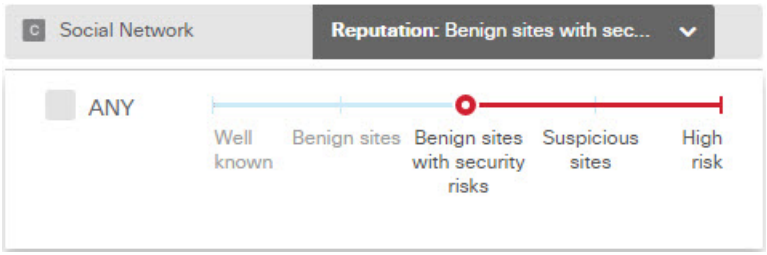


f) **URLs(URL)** 탭을 클릭합니다.

g) 범주의 +를 클릭하고 완전히 차단하거나 부분적으로 차단할 범주를 선택합니다.
이 예시에서는 성인 및 음란물, 봇넷, 확인된 스팸 소스 및 소셜 네트워크를 선택합니다. 차단해야 할 가능성이 높은 추가 범주도 있습니다.



h) 소셜 네트워크 범주에 대해 평판별 차단을 구현하려면 해당 범주에 대해 **Reputation: Risk Any(**평판**:** 모든 위험**)**를 클릭하고 **Any(**모두**)**를 선택 취소한 후에 슬라이더를 보안 위험이 있는 일반 사이트로 이동합니다. 슬라이더 바깥쪽을 클릭하면 슬라이더가 닫힙니다.



평판 슬라이더의 왼쪽은 허용할 사이트를, 오른쪽은 차단할 사이트를 나타냅니다. 이 예시의 경우에는 평판이 의심스러운 사이트 및 높은 위험 범위에 속하는 소셜 네트워킹 사이트만 차단합니다. 따라서 사용자는 위험성이 적은 흔히 사용되는 소셜 네트워킹 사이트에 액세스할 수 있습니다.

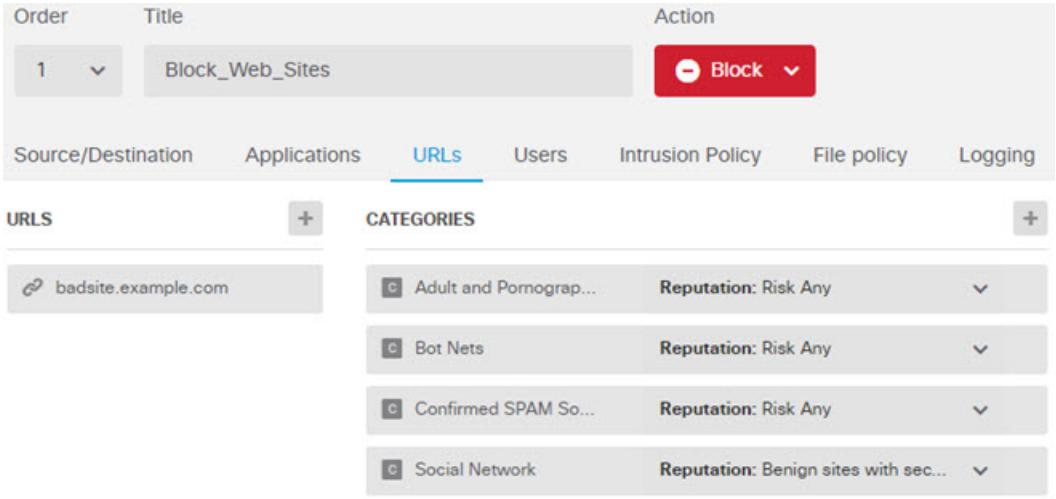
평판을 사용하면 일반적으로는 허용할 범주 내의 사이트를 선택적으로 차단할 수 있습니다.

i) 범주 목록 왼쪽의 **URL** 목록 옆에 있는 +를 클릭합니다.

j) 팝업 대화 상자 하단의 새 **URL** 생성 링크를 클릭합니다.

k) 이름과 URL에 모두 **badsite.example.com**을 입력하고 확인을 클릭하여 개체를 생성합니다.
개체 이름은 URL과 동일하게 지정해도 되고 다른 이름을 지정해도 됩니다. URL의 경우 URL의 프로토콜 부분은 포함하지 말고 서버 이름만 추가합니다.

l) 새 개체를 선택한 다음 **OK(**확인**)**를 클릭합니다.
정책을 수정하는 중에 새 개체를 추가하면 목록에 개체가 추가되지만, 새 개체가 자동으로 선택되지는 않습니다.



m) **Logging**(로깅) 탭을 클릭하고 **Select Log Action**(로그 작업 선택) > **At Beginning and End of Connection**(연결 시작 및 종료 시)을 선택합니다.
웹 범주 대시보드 및 연결 이벤트로 범주 및 평판 정보를 가져오려면 로깅을 사용해야 합니다.

n) **OK**(확인)를 클릭하여 규칙을 저장합니다.

단계 **3** (선택 사항). URL 필터링을 위한 기본 설정을 지정합니다.
URL 라이선스를 활성화하면 시스템에서 웹 범주 데이터베이스에 대한 업데이트를 자동으로 사용합니다. 시스템은 30분마다 업데이트를 확인하지만, 데이터는 대개 매일 한 번씩 업데이트됩니다. 이러한 업데이트를 적용하지 않으려는 경우에는 업데이트를 끌 수 있습니다.

또한, 분석을 위해 Cisco에 분류되지 않은 URL을 전송하도록 선택할 수도 있습니다. 그러므로 사용자가 범주 및 평판이 없는 새 사이트로 이동하는 경우 Cisco에서는 해당 사이트를 평가 및 분류하여 평판을 지정하고 이후 업데이트에 포함할 수 있습니다. 그리고 나면 새 정보를 기반으로 하여 이후 사이트 방문을 허용하거나 차단할 수 있습니다.

a) 디바이스을 클릭합니다.
b) **System Settings**(시스템 설정) > **Traffic Settings**(트래픽 설정) > **URL Filtering Preferences**(URL 필터링 기본 설정)를 클릭합니다.
c) **Cisco CSI**에서 알 수 없는 **URL** 쿼리를 선택합니다.
d) **Save**(저장)를 클릭합니다.

단계 **4** 변경 사항을 커밋합니다.

a) 웹 페이지의 오른쪽 상단에 있는 변경 사항 구축 아이콘을 클릭합니다.

b) **Deploy Now**(지금 구축) 버튼을 클릭하고 구축이 완료될 때까지 기다립니다.
구축 요약에는 변경 사항을 정상적으로 구축했다는 메시지가 표시되며, 작업의 작업 상태는 구축됨으로 설정됩니다.

다음에 할 작업

이 시점부터 모니터링 대시보드 및 이벤트에 웹 범주와 평판 그리고 삭제된 연결에 대한 정보가 표시되어야 합니다. 이 정보를 평가하여 URL 필터링이 부적절한 사이트만 삭제하는지 또는 특정 범주에 대한 평판 설정을 완화해야 하는지를 확인할 수 있습니다.

범주와 평판을 기준으로 웹 사이트 액세스를 차단할 것임을 사용자에게 미리 알리는 것이 좋습니다.

애플리케이션 사용량을 제어하는 방법

웹은 기업에 애플리케이션을 제공하는 데 흔히 사용되는 플랫폼으로 자리잡았습니다. 브라우저 기반 애플리케이션 플랫폼이 사용될 수도 있고, 기업 네트워크 안팎으로 애플리케이션을 전송하는 방법으로 웹 프로토콜을 사용하는 리치 미디어 애플리케이션이 사용될 수도 있습니다.

Firepower Threat Defense에서는 연결을 검사하여 사용 중인 애플리케이션을 확인합니다. 따라서 특정 TCP/UDP 포트만 대상으로 하는 것이 아니라 애플리케이션을 대상으로 하는 액세스 제어 규칙을 작성할 수 있습니다. 그러므로 같은 포트를 사용하는 웹 기반 애플리케이션도 선택적으로 허용하거나 차단할 수 있습니다.

허용하거나 차단할 특정 애플리케이션을 선택할 수도 있지만, 유형/범주/태그/위험/사업 타당성을 기준으로 규칙을 작성할 수도 있습니다. 예를 들어, 위험도가 높고 사업 타당성이 낮은 모든 애플리케이션을 식별하여 차단하는 액세스 제어 규칙을 만들 수 있습니다. 사용자가 이러한 애플리케이션 중 하나를 사용하려고 할 경우, 세션은 차단됩니다.

Cisco에서는 시스템 및 VDB(Vulnerability Database) 업데이트를 통해 추가 애플리케이션 탐지기를 자주 업데이트하고 추가합니다. 따라서 규칙을 수동으로 업데이트하지 않아도 위험도가 높은 애플리케이션을 차단하는 규칙이 새 애플리케이션에 자동으로 적용될 수 있습니다.

이 활용 사례에서는 익명성 도구/프록시 범주에 속하는 모든 애플리케이션을 차단합니다.

시작하기 전에

이 활용 사례에서는 네트워크 트래픽을 파악하는 방법, 33 페이지 활용 사례를 완료했다고 가정합니다. 해당 활용 사례에서는 애플리케이션 사용량 정보를 수집하는 방법을 설명합니다. 이 정보는 애플리케이션 대시보드에서 분석할 수 있습니다. 실제로 사용 중인 애플리케이션을 파악하면 효율적인 애플리케이션 기반 규칙을 디자인하는 데 도움이 될 수 있습니다. VDB 업데이트를 예약하는 방법도 해당 활용 사례에 설명되어 있으므로 이 활용 사례에서 반복 설명하지 않습니다. 애플리케이션을 올바르게 식별할 수 있도록 VBD를 정기적으로 업데이트해야 합니다.

절차

단계 **1** 애플리케이션 기반 액세스 제어 규칙을 생성합니다.

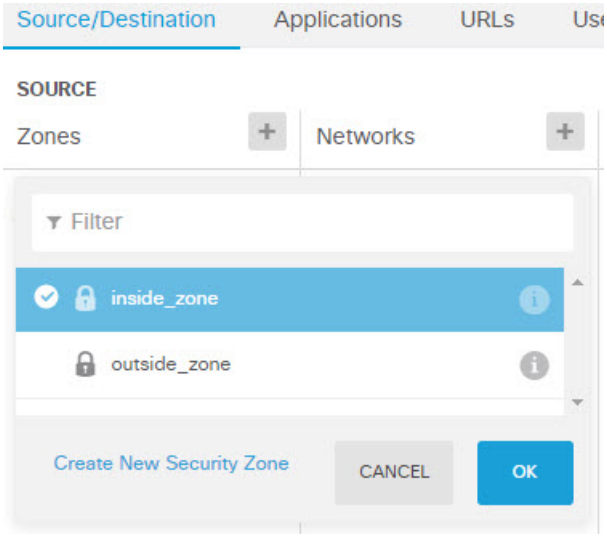
a) 주 메뉴에서 **Policies(**정책**)**를 클릭합니다.
액세스 제어 정책이 표시되는지 확인합니다.

b) +를 클릭하여 새 규칙을 추가합니다.

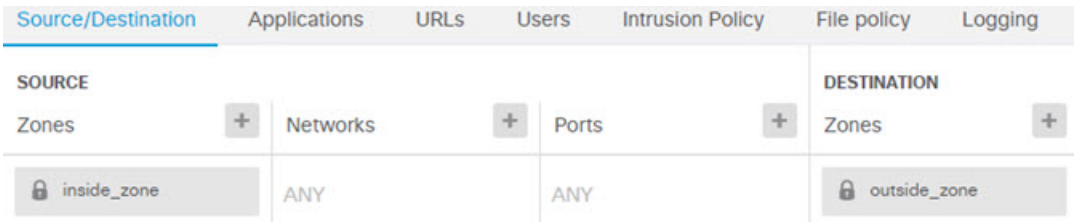
c) 순서, 제목 및 작업을 구성합니다.

- 순서 - 기본적으로는 액세스 제어 정책 끝에 새 규칙을 추가합니다. 그러나 같은 원본/대상 및 기타 기준과 일치하는 규칙 앞(위)에 이 규칙을 배치해야 합니다. 그렇지 않으면 규칙이 어떤 항목과도 일치하지 않게 됩니다. 연결은 하나의 규칙, 즉 테이블에서 첫 번째로 일치하는 규칙에만 일치합니다. 이 규칙에서는 초기 디바이스 컨피그레이션 중에 생성한 Inside_Outside_Rule과 같은 소스/대상을 사용합니다. 다른 규칙도 생성했을 수 있습니다. 액세스 제어 효율성을 최대화하려면 특정 규칙을 미리 생성해 두는 것이 좋습니다. 그러면 연결을 허용할지 아니면 삭제할지를 가장 빠르게 결정할 수 있습니다. 이 예시에서는 규칙 순서로 **1**을 선택합니다.
- 제목 - Block_Anonymizers와 같이 의미 있는 이름을 규칙에 지정합니다.
- 작업 - 차단을 선택합니다.

d) 소스/대상 탭에서 **Source(**소스**)** > **Zones(**영역**)**의 +를 클릭하고 **inside_zone**을 선택한 후에 영역 대화 상자에서 **OK(**확인**)**를 클릭합니다.



e) 동일한 기술을 사용하여 **Destination(**대상**)** > **Zones(**영역**)**에 대해 **outside_zone**을 선택합니다.



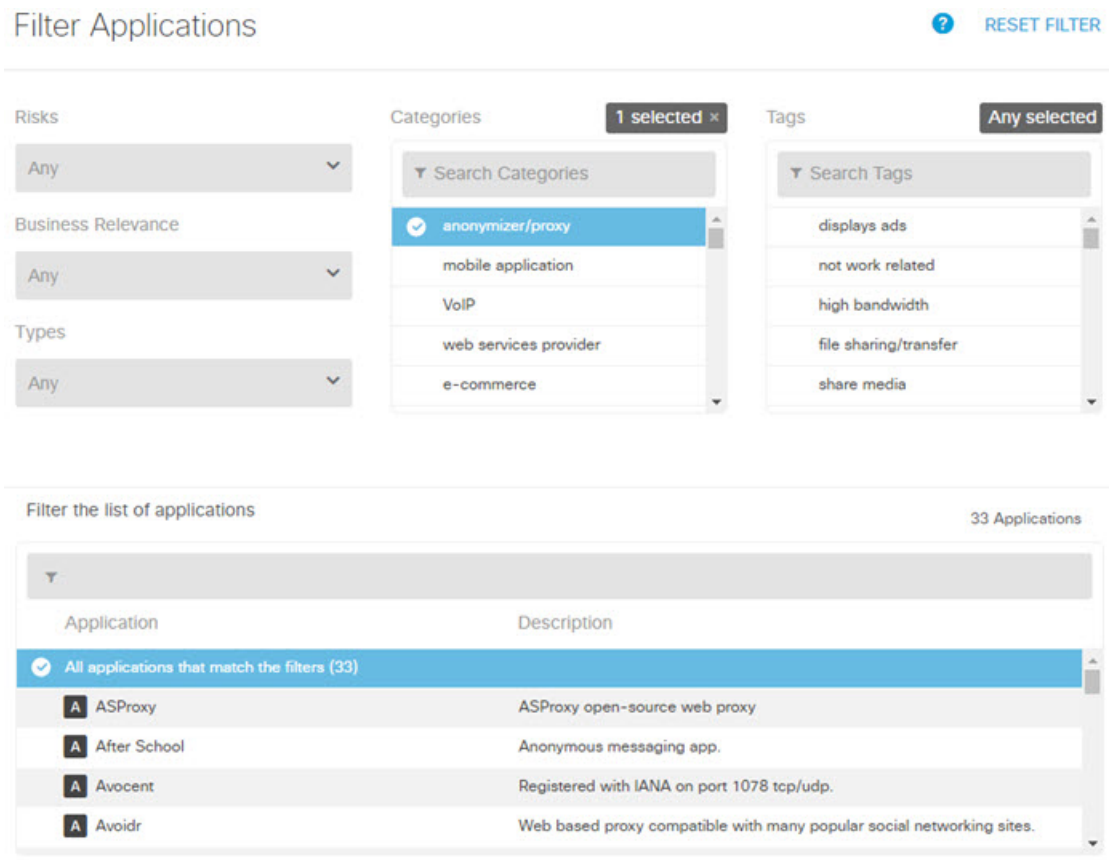
f) **Applications(**애플리케이션**)** 탭을 클릭합니다.

g) 애플리케이션에 대해 +를 클릭하고 팝업 대화 상자 하단의 **Advanced Filter(**고급 필터**)** 링크를 클릭합니다.
애플리케이션 필터 개체를 미리 생성해 두었다가 여기서 애플리케이션 필터 목록을 통해 선택할 수도 있지만, 액세스 제어 규칙에서 기준을 직접 지정하고 필요에 따라 기준을 필터 개체로 저장할 수도 있습니다. 단일 애플리케이션용 규칙을 작성하는 경우가 아니면 고급 필터 대화 상자를 사용하여 애플리케이션을 찾고 적절한 기준을 생성하는 것이 더 쉽습니다.

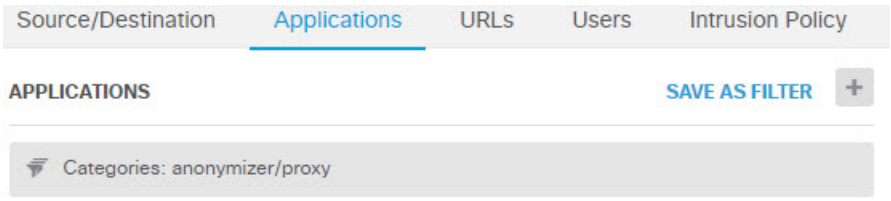
기준을 선택하면 대화 상자 하단의 애플리케이션 목록이 업데이트되어 기준과 일치하는 정확한 애플리케이션이 표시됩니다. 작성하는 규칙은 이러한 애플리케이션에 적용됩니다.

이 목록을 자세히 확인하십시오**.** 예를 들어 위험도가 매우 높은 애플리케이션은 모두 차단하는 경우가 많습니다. 하지만 이 문서를 작성하는 시점에서 Facebook과 TFTP도 위험도가 매우 높은 애플리케이션으로 분류되어 있습니다. 대부분의 조직은 해당 애플리케이션을 차단하기를 원치 않을 것입니다. 시간을 할애하여 다양한 필터 기준을 적용해 보고 선택한 필터와 일치하는 애플리케이션을 확인하십시오. 이러한 목록은 VDB가 업데이트될 때마다 변경될 수 있습니다.

이 예에서는 범주 목록에서 익명성 도구/프록시를 선택합니다.



h) 고급 필터 대화 상자에서 **Add(**추가**)**를 클릭합니다.
필터가 추가되어 애플리케이션 탭에 표시됩니다.



i) **Logging(**로깅**)** 탭을 클릭하고 **Select Log Action(**로그 작업 선택**)** > **At Beginning and End of Connection(**연결 시작 및 종료 시**)**을 선택합니다.
이 규칙에 의해 차단되는 연결에 대한 정보를 확인하려면 로깅을 활성화해야 합니다.

j) **OK(**확인**)**를 클릭하여 규칙을 저장합니다.

단계 **2** 변경 사항을 커밋합니다.

a) 웹 페이지의 오른쪽 상단에 있는 변경 사항 구축 아이콘을 클릭합니다.

b) **Deploy Now(**지금 구축**)** 버튼을 클릭하고 구축이 완료될 때까지 기다립니다.
구축 요약에는 변경 사항을 성공적으로 구축했다는 메시지가 표시되며, 작업 상태는 구축됨으로 설정됩니다.

단계 **3** **Monitoring(**모니터링**)**을 클릭하고 결과를 평가합니다.
이제 애플리케이션 위젯의 네트워크 개요 대시보드에 삭제된 연결이 표시됩니다. **All(**모두**)/Denied(**거부됨**)/Allowed(**허용됨**)** 드롭다운 옵션을 사용하여 삭제된 애플리케이션만 확인합니다.

애플리케이션 대시보드에도 이러한 결과가 표시됩니다. 특정 사용자가 이러한 애플리케이션 사용을 시도하는 경우, ID 정책을 활성화하고 인증을 요구한다는 가정 하에 연결을 시도하는 사용자와 애플리케이션 간의 상관관계를 파악할 수 있어야 합니다.

서브넷을 추가하는 방법

디바이스에 사용 가능한 인터페이스가 있으면 스위치나 다른 라우터에 유선으로 연결하여 다른 서브넷에 서비스를 제공할 수 있습니다.

서브넷은 여러 가지 이유로 인해 추가할 수 있습니다. 이 활용 사례의 경우에는 다음과 같은 일반적인 시나리오를 위해 서브넷을 연결합니다.

- 서브넷은 프라이빗 네트워크 192.168.2.0/24를 사용하는 내부 네트워크입니다.
- 네트워크의 인터페이스 고정 주소는 192.168.2.1입니다. 이 예에서 실제 인터페이스는 네트워크 전용입니다. 이미 유선으로 연결된 인터페이스를 사용하고 새 네트워크용으로 하위 인터페이스를 생성할 수도 있습니다.
- 디바이스는 DHCP를 사용하여 네트워크의 워크스테이션에 주소를 제공하며, 주소 풀 192.168.2.2-192.168.2.254를 사용합니다.

- 다른 내부 네트워크와 외부 네트워크에 대한 네트워크 액세스가 허용됩니다. 외부 네트워크로 이동하는 트래픽은 NAT를 사용하여 공용 주소를 가져옵니다.

참고 이 예에서는 사용되지 않는 인터페이스가 브리지 그룹의 일부분이 아니라고 가정합니다. 현재 해당 인터페이스가 브리지 그룹 구성원인 경우에는 먼저 브리지 그룹에서 인터페이스를 제거해야 이 절차를 수행할 수 있습니다.

시작하기 전에

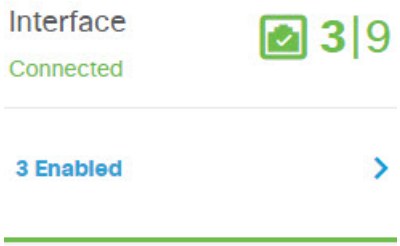
새 서브넷의 스위치와 인터페이스에 네트워크 케이블을 물리적으로 연결합니다.

절차

단계 **1** 인터페이스를 구성합니다.

a) 디바이스을 클릭합니다.

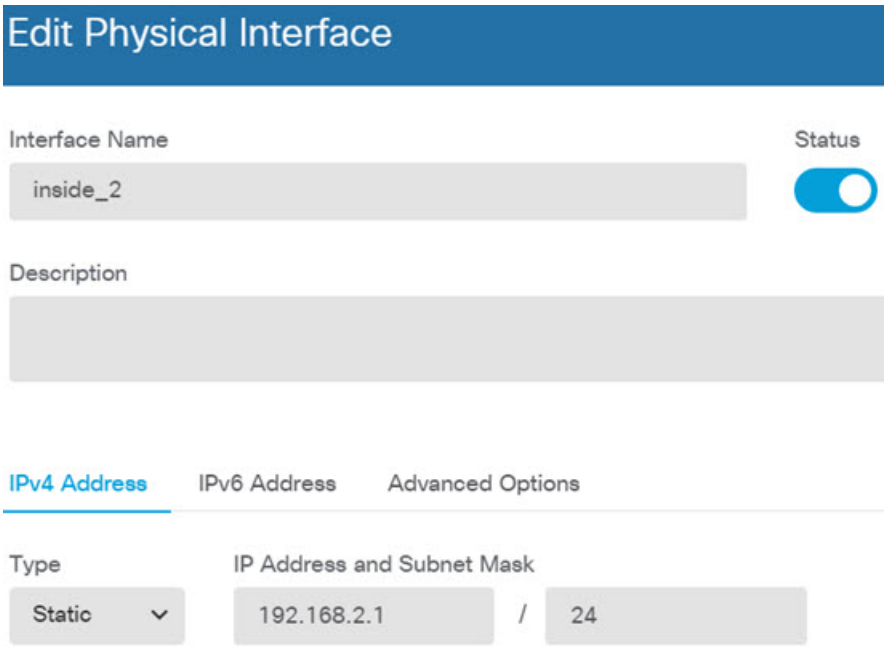
b) 활성화된 인터페이스의 수를 나타내는 인터페이스 그룹의 링크를 클릭합니다.
디바이스의 총 인터페이스 수와 비교한 활성화된 인터페이스 수의 요약이 표시됩니다. 이 수는 모델별로 다릅니다. 이 예에서는 9개 인터페이스 중 3개가 활성화되어 있습니다.



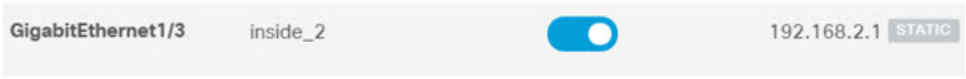
c) 유선으로 연결한 인터페이스 행 오른쪽의 작업 셀 위에 마우스를 올려 놓고 수정 아이콘()을 클릭합니다.

d) 기본 인터페이스 속성을 구성합니다.

- 이름 - 인터페이스의 고유한 이름입니다. 이 예에서 이름은 **inside_2**입니다.
- 상태 - 상태 토글을 클릭하여 인터페이스를 활성화합니다.
- **IPv4** 주소 탭 - 유형으로 고정을 선택하고 **192.168.2.1/24**를 입력합니다.



e) **Save(**저장**)**를 클릭합니다.
인터페이스 목록에 업데이트된 인터페이스 상태와 구성된 IP 주소가 표시됩니다.



단계 **2** 인터페이스용 DHCP 서버를 구성합니다.

a) 디바이스을 클릭합니다.

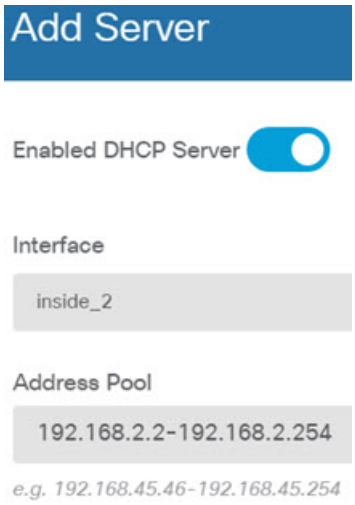
b) **System Settings(**시스템 설정**)** > **DHCP Server(DHCP** 서버**)**를 클릭합니다.

c) **DHCP** 서버 탭을 클릭합니다.
테이블에 기존 DHCP 서버가 나열됩니다. 기본 컨피그레이션을 사용하는 경우 목록에는 내부 인터페이스용 DHCP 서버가 포함되어 있습니다.

d) 테이블 위의 +를 클릭합니다.

e) 서버 속성을 구성합니다.

- **DHCP** 서버 사용 - 이 토글을 클릭하여 서버를 사용합니다.
- 인터페이스 - DHCP 서비스를 제공할 인터페이스를 선택합니다. 이 예에서는 inside_2를 선택합니다.
- 주소 풀 - 서버가 네트워크의 디바이스에 제공할 수 있는 주소입니다. 192.168.2.2-192.168.2.254를 입력합니다. 네트워크 주소(.0), 인터페이스 주소(.1) 또는 브로드캐스트 주소(.255)는 포함하지 마십시오. 또한 네트워크의 디바이스에 고정 주소가 필요한 경우 해당 주소를 풀에서 제외합니다. 풀은 연속하는 주소의 단일 시리즈여야 하므로 범위 시작이나 끝에서 고정 주소를 선택합니다.

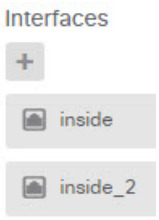


f) **Add(**추가**)**를 클릭합니다.

#	INTERFACE	ENABLED DHCP SERVER	ADDRESS POOL
1	**inside**	Enabled	192.168.1.5-192.168.1.254
2	**inside_2**	Enabled	192.168.2.2-192.168.2.254

단계 **3** 내부 보안 영역에 인터페이스를 추가합니다.
인터페이스에서 정책을 작성하려면 인터페이스가 보안 영역에 속해야 합니다. 보안 영역에 대한 정책을 작성합니다. 그러므로 영역에서 인터페이스를 추가하거나 제거하면 인터페이스에 적용되는 정책이 자동으로 변경됩니다.

a) 주 메뉴에서 **Objects(**개체**)**를 클릭합니다.
b) 개체 목차에서 보안 영역을 선택합니다.
c) **inside_zone** 개체 행 오른쪽의 작업 셀 위에 마우스를 올려 놓고 수정 아이콘( )을 클릭합니다.
d) 인터페이스 아래의 +를 클릭하고 inside_2 인터페이스를 선택한 후에 인터페이스 목록에서 **OK(**확인**)**를 클릭합니다.



e) **Save(**저장**)**를 클릭합니다.

단계 **4** 내부 네트워크 간에 트래픽을 허용하는 액세스 제어 규칙을 생성합니다.
트래픽은 인터페이스 간에 자동으로 허용되지 않습니다. 원하는 트래픽을 허용하는 액세스 제어 규칙을 생성해야 합니다. 단, 액세스 제어 규칙의 기본 작업에서 트래픽을 허용하는 경우는 예외입니다. 이 예에서는 디바이스 설정 마법사가 구성하는 차단 기본 작업을 유지했다고 가정합니다. 따라서 내부 인터페이스 간에 트래픽을 허용하는 규칙을 생성해야 합니다. 이러한 규칙을 이미 생성했다면 이 단계를 건너뛰십시오.

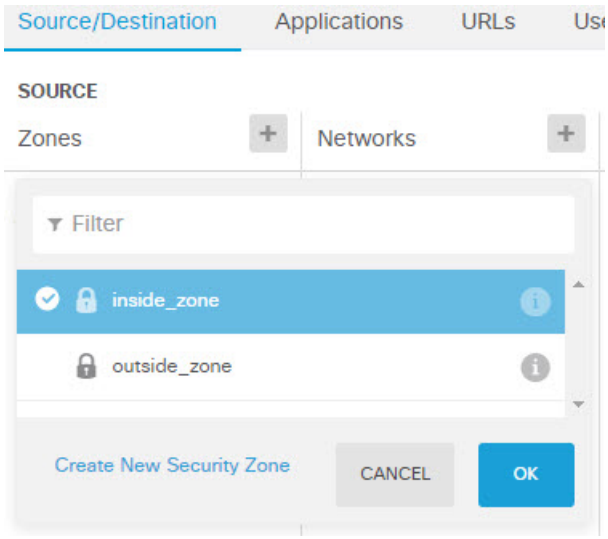
a) 주 메뉴에서 **Policies(**정책**)**를 클릭합니다.
액세스 제어 정책이 표시되는지 확인합니다.

b) +를 클릭하여 새 규칙을 추가합니다.

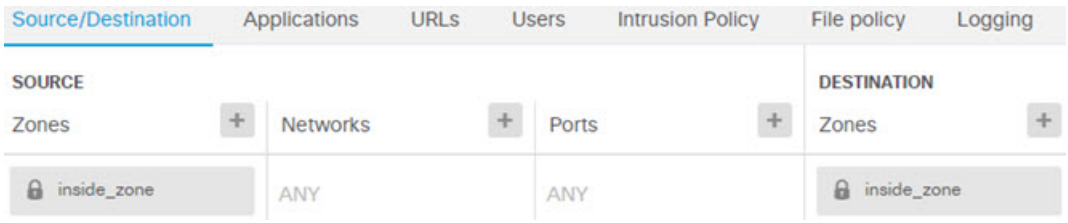
c) 순서, 제목 및 작업을 구성합니다.

- 순서 - 기본적으로는 액세스 제어 정책 끝에 새 규칙을 추가합니다. 그러나 같은 소스/대상 및 기타 기준과 일치하는 규칙 앞(위)에 이 규칙을 배치해야 합니다. 그렇지 않으면 규칙이 어떤 항목과도 일치하지 않게 됩니다. 연결은 하나의 규칙, 즉 테이블에서 첫 번째로 일치하는 규칙에만 일치합니다. 이 규칙의 경우에는 고유한 원본/대상 기준을 사용할 것이므로 목록 끝에 규칙을 추가하면 됩니다.
- 제목 - Allow_Inside_Inside와 같이 의미 있는 이름을 규칙에 지정합니다.
- 작업 - 허용을 선택합니다.

d) 소스/대상 탭에서 **Source(**소스**)** > **Zones(**영역**)**의 +를 클릭하고 **inside_zone**을 선택한 후에 영역 대화 상자에서 **OK(**확인**)**를 클릭합니다.



e) 동일한 기술을 사용하여 **Destination**(대상) > **Zones**(영역)에 대해 **inside_zone**을 선택합니다.
원본과 대상에 대해 같은 영역을 선택하려면 보안 영역이 둘 이상의 인터페이스를 포함해야 합니다.



f) (선택 사항). 침입 및 악성코드 검사를 구성합니다.
내부 인터페이스가 신뢰할 수 있는 영역에 있기는 하지만 사용자는 일반적으로 랩톱을 네트워크에 연결합니다. 따라서 사용자가 의도치 않게 외부 네트워크나 Wi-Fi 핫스팟에서 네트워크 내부로 위협 요소를 유입할 수 있습니다. 그러므로 내부 네트워크 사이를 이동하는 트래픽에서 침입 및 악성코드를 검사할 수 있습니다.

이와 관련하여 다음 사항을 고려하십시오.

- **Intrusion Policy**(침입 정책) 탭을 클릭하고 침입 정책을 활성화한 다음 슬라이더를 사용하여 균형 잡힌 보안 및 연결성 정책을 선택합니다.
- **File Policy**(파일 정책) 탭을 클릭한 후 악성코드 모두 차단 정책을 선택합니다.

g) **Logging**(로깅) 탭을 클릭하고 **Select Log Action**(로그 작업 선택) > **At Beginning and End of Connection**(연결 시작 및 종료 시)을 선택합니다.
이 규칙과 일치하는 연결에 대한 정보를 확인하려면 로깅을 사용해야 합니다. 로깅을 사용하면 대시보드에 통계가 추가되며 이벤트 뷰어에 이벤트가 표시됩니다.

h) **OK**(확인)를 클릭하여 규칙을 저장합니다.

단계 **5** 새 서브넷에 대해 필요한 정책이 정의되어 있는지 확인합니다.

inside_zone 보안 영역에 인터페이스를 추가하면 inside_zone에 대한 모든 기존 정책이 새 서브넷에 자동으로 적용됩니다. 그러나 시간을 할애하여 정책을 검사해 추가 정책이 필요하지 않은지 확인해야 합니다.

초기 디바이스 컨피그레이션을 완료한 경우에는 다음 정책이 이미 적용되어 있어야 합니다.

- 액세스 제어 - Inside_Outside_Rule은 새 서브넷과 외부 네트워크 간의 모든 트래픽을 허용합니다. 이전 활용 사례를 따른 경우 이 정책은 침입 및 악성코드 검사 기능도 제공합니다. 새 네트워크와 외부 네트워크 간의 일부 트래픽을 허용하는 규칙이 있어야 합니다. 그렇지 않으면 사용자가 인터넷 또는 기타 외부 네트워크에 액세스할 수 없습니다.
- **NAT** - InsideOutsideNATrule은 외부 인터페이스로 이동하는 모든 인터페이스에 적용되며 인터페이스 PAT를 적용합니다. 이 규칙을 유지한 경우 새 네트워크에서 외부로 이동하는 트래픽의 IP 주소가 외부 인터페이스 IP 주소에서 고유한 포트로 변환됩니다. 모든 인터페이스 또는 inside_zone 인터페이스에 적용되는 규칙이 없으면 외부 인터페이스로 이동할 때 새 규칙을 생성해야 할 수 있습니다.
- **ID** - 기본 ID 정책은 없습니다. 그러나 이전 활용 사례를 따른 경우 새 네트워크에 대한 인증을 요구하는 ID 정책이 이미 있을 수 있습니다. 적용되는 ID 정책이 없는 경우 새 네트워크에 대해 사용자 기반 정보를 확인하려면 ID 정책을 생성합니다.

단계 **6** 변경 사항을 커밋합니다.

a) 웹 페이지의 오른쪽 상단에 있는 변경 사항 구축 아이콘을 클릭합니다.

b) **Deploy Now(**지금 구축**)** 버튼을 클릭하고 구축이 완료될 때까지 기다립니다.
구축 요약에는 변경 사항을 성공적으로 구축했다는 메시지가 표시되며, 작업 상태는 구축됨으로 설정됩니다.

다음에 할 작업

새 서브넷의 워크스테이션이 DHCP를 사용하여 IP 주소를 받으며, 다른 내부 네트워크 및 외부 네트워크에 연결할 수 있는지 확인합니다. 모니터링 대시보드 및 이벤트 뷰어를 사용하여 네트워크 사용량을 평가합니다.

3 장

시스템 라이선싱

다음 주제에서는 Firepower Threat Defense 디바이스 라이선싱 방법을 설명합니다.

Firepower System 스마트 라이선싱

Cisco Smart Licensing에서는 중앙 집중식으로 라이선스 풀을 구매하여 관리할 수 있습니다. 스마트 라이선스는 PAK(Product Authorization Key) 라이선스와 달리 특정 시리얼 번호 또는 라이선스 키에 연계되어 있지 않습니다. Smart Licensing에서는 라이선스 사용량 및 필요량을 한눈에 평가할 수 있습니다.

또한 Smart Licensing을 사용하는 경우에는 아직 구매하지 않은 제품 기능도 사용할 수 있습니다. Cisco Smart Software Manager에 등록만 되어 있으면 라이선스 사용을 즉시 시작할 수 있으며 나중에 라이선스를 구매할 수 있습니다. 따라서 기능을 구축 및 사용할 수 있으며 구매 발주서 승인 대기로 인한 지연을 방지할 수 있습니다.

Cisco Smart Software Manager

Firepower Threat Defense 디바이스 라이선스를 1개 이상 구매한 경우, Cisco Smart Software Manager(https://software.cisco.com/#SmartLicensing-Inventory)에서 라이선스를 관리할 수 있습니다. Cisco Smart Software Manager에서는 조직의 마스터 어카운트를 생성할 수 있습니다.

기본적으로는 마스터 어카운트의 기본 가상 어카운트에 라이선스가 할당됩니다. 어카운트 관리자는 지역, 부서, 자회사 등에 대해 가상 어카운트를 추가로 생성할 수 있습니다. 여러 가상 어카운트가 있으면 수많은 라이선스 및 어플라이언스를 관리할 수 있습니다.

라이선스 및 어플라이언스는 가상 어카운트별로 관리됩니다. 해당 가상 어카운트의 어플라이언스만 어카운트에 할당된 라이선스를 사용할 수 있습니다. 추가 라이선스가 필요할 경우 다른 가상 계정의 미사용 라이선스를 이전할 수 있습니다. 또한 가상 어카운트 간에 어플라이언스를 전송할 수도 있습니다.

Cisco Smart Software Manager를 사용하여 디바이스를 등록할 때는 Smart Software Manager에서 제품 인스턴스 등록 토큰을 생성한 다음 Firepower Device Manager에 입력합니다. 등록된 디바이스는 사용하는 토큰에 따라 가상 어카운트와 연결됩니다.

Cisco Smart Software Manager에 대한 자세한 내용은 Smart Software Manager 온라인 도움말을 참조하십시오.

License Authority와의 정기적인 통신

제품 인스턴스 등록 토큰을 사용하여 Firepower Threat Defense 디바이스를 등록하면 디바이스가 Cisco License Authority에 등록됩니다. License Authority에서는 디바이스와 License Authority의 통신을 위해 ID 인증서를 발급합니다. 이 인증서는 6개월마다 갱신되지만 1년간 유효합니다. ID 인증서가 만료되면(대개 9개월 후 또는 통신을 수행하지 않는 경우 1년 후) 디바이스는 등록 취소된 상태로 돌아가며 라이선스 기능의 사용이 일시 중단됩니다.

디바이스는 주기적으로 License Authority와 통신합니다. Cisco Smart Software Manager에 변경이 있는 경우 변경 사항이 즉시 적용되도록 디바이스에서 권한 부여를 새로 고칠 수 있습니다. 또는 디바이스에서 예정대로 통신할 때까지 기다릴 수 있습니다. 일반 라이선스 통신은 30일마다 이루어지지만, 유예 기간이 있으므로 디바이스는 최대 90일간 콜 홈 없이 작동할 수 있습니다. 90일이 지나기 전에 License Authority에 접속해야 합니다.

스마트 라이선스 유형

다음 표에서는 Firepower Threat Defense 디바이스에 사용할 수 있는 라이선스에 관해 설명합니다.

Firepower Threat Defense 디바이스를 구매하면 기본 라이선스가 자동으로 포함됩니다. 모든 추가 라이선스는 선택 사항입니다.

표 ***2:*** 스마트 라이선스 유형

라이선스	기간	부여된 기능
기본(자동으로 포함됨)	영구	선택적 기간 라이선스가 적용되지 않는 모든 기능 이 토큰을 사용하여 등록한 제품에서 내보내기 제어 기능을 허용할지도 지정해야 합니다. 현재 거주 국가가 내보내기 제어 표준을 충족하는 경우에만 이 옵션을 선택할 수 있습니다. 이 옵션은 고급 암호화 사용과 고급 암호화를 필요로 하는 기능 사용을 제어합니다.

라이선스	기간	부여된 기능
위협	기간 기준	침입 탐지 및 방지 - 침입 정책은 침입 및 익스플로잇의 트래픽을 분석하고, 선택적으로 문제가 되는 패킷을 삭제할 수 있습니다. 파일 제어 - 파일 정책은 사용자가 특정 유형의 파일을 업로드(전송)하거나 다운로드(수신)하는 것을 탐지하고, 선택적으로 차단할 수 있습니다. 악성코드 라이선스가 필요한 AMP for Firepower를 사용하면 악성코드가 포함된 파일을 검사하고 차단할 수 있습니다.
악성코드	기간 기준	악성코드를 확인하는 파일 정책으로서 Cisco Advanced Malware Protection(AMP)과 AMP for Firepower(네트워크 기반 Advanced Malware Protection) 및 AMP Threat Grid을 함께 사용합니다. 파일 정책은 네트워크를 통해 전송된 파일에서 악성코드를 탐지하고 차단할 수 있습니다.
URL 필터링	기간 기준	범주 및 평판 기반 URL 필터링 이 라이선스가 없어도 개별 URL에 대해 URL 필터링을 수행할 수 있습니다.

만료되거나 비활성화된 선택 가능한 라이선스의 영향

선택 가능한 라이선스가 만료되어도 해당 라이선스를 필요로 하는 기능은 계속 사용할 수 있습니다. 그러나 라이선스는 컴플라이언스 상태가 아닌 것으로 표시되며, 라이선스를 컴플라이언스 상태로 다시 설정하려면 라이선스를 구매하여 어카운트에 추가해야 합니다.

선택 가능한 라이선스를 비활성화하면 시스템은 다음과 같이 대응합니다.

- 악성코드 라이선스 - 시스템이 AMP 클라우드 쿼리를 중지하며 AMP 클라우드에서 전송하는 회귀적 이벤트 확인도 중지합니다. 악성코드 탐지를 적용하는 파일 정책을 포함하는 기존 액세스 제어 정책은 재구축할 수 없습니다. 악성코드 라이선스가 비활성화된 매우 짧은 시간 동안 시스템은 기존에 캐시된 파일 상태를 사용할 수 있습니다. 이 기간이 만료되고 나면 시스템은 해당 파일에 사용할 수 없음 상태를 할당합니다.
- 위협 - 시스템이 더 이상 침입 또는 파일 제어 정책을 적용하지 않습니다. 라이선스가 필요한 기존 정책은 재구축할 수 없습니다.
- **URL** 필터링 - URL 범주 조건이 포함된 액세스 제어 규칙의 URL 필터링이 즉시 중지되며 시스템이 URL 데이터에 대한 업데이트를 더 이상 다운로드하지 않습니다. 범주 및 평판 기반 URL 조건이 들어 있는 규칙을 포함하는 기존 액세스 제어 정책은 재적용할 수 없습니다.

스마트 라이선스 관리

스마트 라이선스 페이지를 사용하여 시스템의 현재 라이선스 상태를 확인합니다. 시스템에 라이선스가 있어야 합니다.

이 페이지에는 90일 평가 라이선스를 사용 중인지 아니면 Cisco Smart Software Manager에 등록되었는지가 표시됩니다. 등록한 경우 Cisco Smart Software Manager에 대한 연결 상태와 각 라이선스 유형의 상태를 확인할 수 있습니다.

사용 권한 부여에서 스마트 라이선스 에이전트 상태를 식별합니다.

- 권한 있음("연결됨", "충분한 라이선스") - 디바이스가 License Authority에 연결하여 정상적으로 등록되었으며, 어플라이언스에 대한 라이선스 자격이 부여되었습니다. 디바이스는 현재 컴플라이언스 상태입니다.
- 규정 미준수 - 디바이스에 대해 사용 가능한 라이선스 자격이 없습니다. 라이선스 기능은 계속 작동합니다. 그러나 추가 자격을 구매하거나 확보해야 디바이스의 컴플라이언스 상태가 될 수 있습니다.
- 권한 부여 만료됨 - 디바이스가 90일 이상 Licensing Authority와 통신하지 않았습니다. 라이선스 기능은 계속 작동합니다. 이 상태에서 스마트 라이선스 에이전트는 권한 부여 요청을 다시 시도합니다. 다시 시도가 성공하면 에이전트는 규정 미준수 또는 권한 있음 상태로 설정되며 새 권한 부여 기간이 시작됩니다. 이 경우 디바이스를 수동으로 동기화해 보십시오.

참고 스마트 라이선스 상태 옆의 **i** 버튼을 클릭하여 가상 어카운트와 내보내기 제어 기능을 확인하고 Cisco Smart Software Manager를 여는 링크를 확인합니다. 내보내기 제어 기능은 국가별 보안, 해외 정책 및 테러 방지법과 규정이 적용되는 소프트웨어를 제어합니다.

다음 절차에서는 시스템의 라이선스를 관리하는 방법을 간략하게 설명합니다.

절차

단계 **1** 디바이스을 클릭한 다음 스마트 라이선스 요약에서 **View Configuration**(컨피그레이션 보기)을 클릭합니다.

단계 **2** 디바이스를 등록합니다.
Cisco Smart Software Manager에 등록해야 선택 가능한 라이선스를 할당할 수 있습니다. 평가 기간이 종료되기 전에 등록하십시오.

디바이스 등록, 67 페이지를 참조하십시오.

단계 **3** 선택 가능한 기능 라이선스를 요청하고 관리합니다.
라이선스를 통해 제어되는 기능을 사용하려면 선택 가능한 라이선스를 등록해야 합니다. 선택 가능한 라이선스 활성화 또는 비활성화, 67 페이지를 참조하십시오.

단계 **4** 시스템 라이선싱을 유지합니다.
다음과 같은 작업을 수행할 수 있습니다.

• Cisco Smart Software Manager와 동기화, 68 페이지
• 디바이스 등록 취소, 69 페이지

디바이스 등록

Firepower Threat Defense 디바이스를 구매하면 기본 라이선스가 자동으로 포함됩니다. 기본 라이선스는 선택 가능한 라이선스에 포함되지 않는 모든 기능을 포함하는 영구 라이선스입니다.

초기 시스템 설정 중에 Cisco Smart Software Manager에 디바이스를 등록하라는 메시지가 표시됩니다. 90일 평가 라이선스를 대신 선택한 경우에는 평가 기간이 종료되기 전에 디바이스를 등록해야 합니다.

디바이스를 등록할 때는 가상 어카운트가 디바이스에 라이선스를 할당합니다. 디바이스를 등록하면 활성화한 선택 가능한 라이선스도 등록됩니다.

절차

단계 **1** 디바이스을 클릭한 다음 스마트 라이선스 요약에서 **View Configuration**(컨피그레이션 보기)을 클릭합니다.

단계 **2** **Request Register**(등록 요청)를 클릭하고 지침을 따릅니다.

a) 링크를 클릭하여 Cisco Smart Software Manager를 열고 어카운트에 로그인하거나 필요한 경우 새 어카운트를 생성합니다.

b) 새 토큰을 생성합니다.
토큰을 생성할 때는 토큰을 사용할 수 있는 유효 기간을 지정합니다. 권장 만료 기간은 30일입니다. 이 기간은 토큰 자체의 만료 날짜를 정의하며 토큰을 사용하여 등록하는 디바이스에는 영향을 주지 않습니다. 토큰이 사용하기 전에 만료되는 경우 새 토큰을 생성하면 됩니다.

이 토큰을 사용하여 등록한 제품에서 내보내기 제어 기능을 허용할지도 지정해야 합니다. 현재 거주 국가가 내보내기 제어 표준을 충족하는 경우에만 이 옵션을 선택할 수 있습니다. 이 옵션은 고급 암호화 사용과 고급 암호화를 필요로 하는 기능 사용을 제어합니다.

c) 토큰을 복사하여 스마트 라이선스 등록 대화 상자의 수정 상자에 붙여넣습니다.

d) **Request Register**(등록 요청)를 클릭합니다.

선택 가능한 라이선스 활성화 또는 비활성화

선택 가능한 라이선스는 사용(등록)하거나 사용하지 않을(해제) 수 있습니다. 라이선스를 통해 제어되는 기능을 사용하려면 라이선스를 사용하도록 설정해야 합니다.

선택적 기간 라이선스가 적용되는 기능을 더 이상 사용하지 않으려는 경우 라이선스를 비활성화할 수 있습니다. 비활성화하는 라이선스는 Cisco Smart Software Manager 어카운트에서 해제되므로 다른 디바이스에 적용할 수 있습니다.

평가 모드에서 실행 중인 경우 이러한 라이선스의 평가 버전을 사용할 수도 있습니다. 평가 모드에서 라이선스는 디바이스를 등록할 때까지 Cisco Smart Software Manager에 등록되지 않습니다.

시작하기 전에

라이선스를 비활성화하기 전에 해당 라이선스를 사용하고 있지 않은지 확인합니다. 라이선스가 필요한 정책은 재작성하거나 삭제합니다.

절차

단계 **1** 디바이스을 클릭한 다음 스마트 라이선스 요약에서 **View Configuration(**컨피그레이션 보기**)**을 클릭합니다.

단계 **2** 선택 가능한 각 라이선스에 대해 **Enable(**활성화**)/Disable(**비활성화**)** 컨트롤을 필요한 대로 클릭합니다.

- 활성화 - Cisco Smart Software Manager 어카운트에 라이선스를 등록하고 제어되는 기능을 사용합니다. 이제 라이선스를 통해 제어되는 정책을 구성하고 구축할 수 있습니다.
- 비활성화 - Cisco Smart Software Manager 어카운트에서 라이선스를 등록 취소하고 제어되는 기능을 비활성화합니다. 이렇게 하면 새 정책에서 기능을 구성할 수 없으며 해당 기능을 사용하는 정책을 구축할 수도 없습니다.

Cisco Smart Software Manager와 동기화

시스템은 Cisco Smart Software Manager와 주기적으로 라이선스 정보를 동기화합니다. 일반 라이선스 통신은 30일마다 이루어지지만, 유예 기간이 있으므로 어플라이언스는 최대 90일간 콜 홈 없이 작동할 수 있습니다.

그러나 Cisco Smart Software Manager에서 변경을 수행할 경우 변경 사항이 즉시 적용되도록 디바이스에서 권한 부여를 새로 고칠 수 있습니다.

동기화 시에는 라이선스의 현재 상태를 가져오며 권한 부여와 ID 인증서가 갱신됩니다.

절차

단계 **1** 디바이스을 클릭한 다음 스마트 라이선스 요약에서 **View Configuration(**컨피그레이션 보기**)**을 클릭합니다.

단계 **2** 기어 드롭다운 목록에서 **Resync Connection(**연결 재동기화**)**를 선택합니다.

디바이스 등록 취소

더 이상 디바이스를 사용하지 않으려는 경우 Cisco Smart Software Manager에서 디바이스를 등록 취소할 수 있습니다. 등록을 취소하면 디바이스에 연결된 기본 라이선스 및 선택 가능한 모든 라이선스가 가상 어카운트에서 해제됩니다. 선택 가능한 라이선스는 다른 디바이스에 할당할 수 있습니다.

디바이스를 등록 취소한 후에도 디바이스의 현재 컨피그레이션 및 정책은 계속 원래대로 작동하지만 변경을 수행하거나 변경 사항을 구축할 수는 없습니다.

절차

단계 **1** 디바이스을 클릭한 다음 스마트 라이선스 요약에서 **View Configuration(**컨피그레이션 보기**)**을 클릭합니다.

단계 **2** 기어 드롭다운 목록에서 **Unregister Device(**디바이스 등록 취소**)**를 선택합니다.

단계 **3** 경고를 확인한 후에 디바이스를 등록 취소하려면 **Unregister(**등록 취소**)**를 클릭합니다.

4 장

디바이스 모니터링

시스템에는 디바이스 및 디바이스를 통과하는 트래픽을 모니터링하는 데 사용할 수 있는 대시보드와 이벤트 뷰어가 포함되어 있습니다.

트래픽 통계를 가져오도록 로깅 사용

모니터링 대시보드 및 이벤트 뷰어를 사용하여 광범위한 트래픽 통계를 모니터링할 수 있습니다. 그러나 시스템에 수집할 통계를 지시하려면 로깅을사용해야 합니다.

선택적 통계를 수집하고 이벤트를 생성하려면 개별 액세스 규칙에 대해 다음 로깅 유형을 활성화합니다.

- 연결 로깅 - 연결 종료 시 수행되는 로깅은 연결에 대한 대부분의 정보를 제공합니다. 연결 시작 시에 로깅을 수행할 수도 있지만 이러한 이벤트에 포함되는 정보는 불완전합니다. 연결 로깅은 기본적으로 비활성화되므로 추적하려는 트래픽을 대상으로 하는 각 규칙과 기본 작업에 대해 연결 로깅을 사용해야 합니다.
- 파일 로깅 - 탐지된 파일에 대한 정보를 수집하려면 파일 로깅을 사용해야 합니다. 액세스 규칙에서 파일 정책을 선택하면 파일 로깅이 자동으로 활성화되지만, 파일 로깅을 비활성화할 수 있습니다.

시스템은 사용자가 구성하는 로깅 외에도 시스템이 금지된 파일, 악성코드 또는 침입 시도를 탐지한 곳(연결 끝)에서 대부분의 연결을 자동으로 로깅합니다. 단, 기본 작업을 통해 처리되는 침입 이벤트는 예외입니다. 이러한 침입 이벤트를 확인하려면 기본 작업에 대해 연결 로깅을 사용해야 합니다.

팁

로깅 컨피그레이션 및 관련 통계 평가를 고려할 때는 다음 사항에 유의하십시오.

- 사용자가 액세스 제어 규칙을 통해 트래픽을 허용할 때, 연결된 침입 또는 파일 정책을 (또는 둘 다를) 사용하여 트래픽이 최종 목적지에 도달하기 전에 트래픽 및 침입 차단, 금지된 파일과 악성코드를 자세히 검사할 수 있습니다. 하지만. 기본 파일 및 침입에 의해 암호화된 페이로드를 위한 탐지가 비활성화되었음을 참고하시기 바랍니다. 침입 또는 파일 정책이 연결을 차단해야 하는 이유를 확인하는 경우, 시스템은 연결 로그 설정과 관계없이 연결 종료 이벤트를 즉시 로깅합니다. 로깅이 허용되는 연결은 네트워크의 트래픽에 대해 가장 많은 통계 정보를 제공합니다.
- 신뢰할 수 있는 연결이란 액세스 제어 정책에서 신뢰 액세스 제어 규칙 또는 기본 작업이 처리한 것입니다. 그러나 신뢰할 수 있는 연결에서는 검색 데이터, 침입 또는 금지된 파일과 악성코드를 검사하지 않습니다. 따라서, 신뢰할 수 있는 연결에 대한 연결 이벤트는 제한된 정보를 포함합니다.
- 트래픽을 차단하는 액세스 제어 규칙 및 액세스 제어 정책 기본 작업의 경우 시스템은 연결 시작 이벤트를 로깅합니다. 일치하는 트래픽은 추가 검사 없이 거부됩니다.
- 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 이 규칙이 인터넷 연결 인터페이스 또는 DoS 공격에 취약한 다른 인터페이스의 트래픽을 모니터링하는지 여부를 고려하십시오.

트래픽 및 시스템 대시보드 모니터링

시스템에는 디바이스를 통과하는 트래픽과 보안 정책의 결과를 분석하는 데 사용할 수 있는 여러 대시보드가 포함되어 있습니다. 대시보드의 정보를 사용하여 컨피그레이션의 전반적인 효율성을 평가하고 네트워크 문제를 식별 및 해결합니다.

참고 트래픽 관련 대시보드에서 사용되는 데이터는 연결 또는 파일 로깅을 활성화하는 액세스 제어 규칙에서 수집됩니다. 로깅이 활성화되어 있지 않은 규칙과 일치하는 트래픽은 대시보드에 반영되지 않습니다. 따라서 중요한 정보를 로깅하도록 규칙을 구성해야 합니다. 또한, 사용자 정보는 사용자 ID를 수집하는 ID 규칙을 구성한 경우에만 사용할 수 있습니다. 그리고 마지막으로 침입, 파일, 악성코드 및 웹 범주 정보는 해당 기능용 라이선스가 있으며 이러한 기능을 사용하는 규칙을 구성한 경우에만 사용할 수 있습니다.

절차

단계 **1** 주 메뉴에서 **Monitoring(**모니터링**)**을 클릭하여 대시보드 페이지를 엽니다.
지난 1시간, 지난주 등의 사전 정의된 시간 범위를 선택하거나, 특정 시작 시간과 종료 시간을 사용해 맞춤형 시간 범위를 정의하여 대시보드 그래프와 테이블에 표시되는 데이터를 제어할 수 있습니다.

트래픽 관련 대시보드는 다음과 같은 유형으로 표시됩니다.

- 상위 5개 막대 그래프 - 이러한 그래프는 네트워크 개요 대시보드에 표시되며 대시보드 테이블에서 항목을 클릭하면 나타나는 항목별 요약에도 표시됩니다. 표시되는 정보를 트랜잭션 개수 또는 데이터 사용량(전송 및 수신된 총 바이트 수) 간을 전환할 수 있습니다. 모든 트랜잭션, 허용된 트랜잭션 또는 거부된 트랜잭션이 나타나도록 화면표시를 전환할 수도 있습니다. 더 보기 링크를 클릭하면 그래프와 연결된 테이블이 표시됩니다.
- 테이블 - 테이블에는 애플리케이션, 웹 범주 등 특정 유형의 항목과 해당 항목의 총 트랜잭션, 허용된 트랜잭션, 거부된 트랜잭션, 데이터 사용량 및 전송/수신된 바이트 수가 표시됩니다. 표시되는 숫자를 원시 값과 백분율 간을 전환할 수 있으며 상위 10개, 100개, 1000개 항목을 표시할 수 있습니다. 항목이 링크인 경우 링크를 클릭하면 더욱 자세한 정보가 포함된 요약 대시보드를 확인할 수 있습니다.

단계 **2** 목차에서 대시보드 링크를 클릭하여 다음 데이터에 대한 대시보드를 표시합니다.

- 네트워크 개요 - 네트워크의 트래픽에 대한 요약 정보를 표시합니다. 이러한 정보에는 일치한 액세스 규칙(정책), 트래픽을 생성한 사용자, 연결에 사용된 애플리케이션, 일치한 침입 서명, 액세스한 URL의 웹 범주 및 연결에서 가장 많이 사용된 대상이 포함됩니다.
- 사용자 - 네트워크를 많이 사용한 사용자가 표시됩니다. 사용자 정보를 확인하려면 ID 정책을 구성해야 합니다.
- 애플리케이션 - 네트워크에서 많이 사용되는 Facebook 등의 애플리케이션을 표시합니다. 검사된 연결에 대해서만 정보가 제공됩니다. 영역, 주소 및 포트 이외의 기준을 사용하는 차단 규칙이나 "허용" 규칙과 일치하는 연결을 검사합니다. 따라서 검사를 요구하는 규칙에 적중하기 전에 연결이 신뢰 또는 차단되면 애플리케이션 정보가 제공되지 않습니다.
- 웹 범주 - 방문한 웹 사이트의 분류를 기반으로 네트워크에서 많이 사용되는 도박 또는 교육 기관 등의 웹 사이트 범주를 표시합니다. 이 정보를 얻으려면 웹 범주를 사용하는 액세스 제어 규칙 하나 이상을 트래픽 일치 기준으로 포함해야 합니다. 규칙과 일치하는 트래픽 또는 규칙과 일치하는지를 확인하기 위해 검사해야 하는 트래픽에 대한 정보가 제공됩니다. 첫 번째 웹 범주 액세스 제어 규칙 앞에 오는 규칙과 일치하는 연결에 대해서는 범주 또는 평판 정보가 표시되지 않습니다.
- 정책 - 네트워크 트래픽과 가장 많이 일치하는 액세스 규칙을 표시합니다.
- 인그레스 영역 - 트래픽이 디바이스로 들어가는 데 가장 많이 사용되는 보안 영역을 표시합니다.
- 이그레스 영역 - 트래픽이 디바이스에서 나가는 데 가장 많이 사용되는 보안 영역을 표시합니다.
- 목적지 - 네트워크 트래픽에서 가장 많이 사용하는 목적지를 표시합니다.
- 공격자 - 침입 이벤트를 트리거하는 연결의 소스인 상위 공격자를 표시합니다. 이 정보를 보려면 액세스 규칙에 대한 침입 정책을 구성해야 합니다.
- 대상 - 공격의 피해자인 침입 이벤트의 상위 대상을 표시합니다. 이 정보를 보려면 액세스 규칙에 대한 침입 정책을 구성해야 합니다.
- 위협 - 가장 많이 트리거된 침입 규칙을 표시합니다. 이 정보를 보려면 액세스 규칙에 대한 침입 정책을 구성해야 합니다.

- 파일 로그 - 네트워크 트래픽에서 가장 많이 확인된 파일 유형을 표시합니다. 이 정보를 보려면 액세스 규칙에 대한 파일 정책을 구성해야 합니다.
- 시스템 - 인터페이스 및 해당 상태(인터페이스 위에 마우스를 올려놓으면 해당 IP 주소가 표시됨), 전반적인 시스템 성능, 시스템 이벤트/CPU 사용량/메모리 사용량/디스크 사용량 관련 요약 정보의 화면표시를 비롯한 전체 시스템 보기를 표시합니다. 모든 인터페이스가 아닌 특정 인터페이스만 표시하도록 성능 그래프를 제한할 수 있습니다.

  참고 시스템 대시보드에 표시되는 정보는 전체 시스템 레벨의 정보입니다. 디바이스 CLI에 로그인하면 다양한 명령을 사용하여 더욱 자세한 정보를 확인할 수 있습니다. 예를 들어 **show cpu** 및 **show memory** 명령에는 기타 세부사항을 표시하는 파라미터가 포함되어 있는 반면, 이러한 대시보드에는 **show cpu system** 및 **show memory system** 명령에서 제공하는 데이터가 표시됩니다.

단계 **3** 목차에서 이러한 링크를 클릭할 수도 있습니다.

- 이벤트 - 발생하는 이벤트를 확인할 수 있습니다. 개별 액세스 규칙에서 연결 로깅을 활성화해야 해당 규칙과 관련된 연결 이벤트를 확인할 수 있습니다. 이러한 이벤트를 확인하면 사용자의 연결 문제를 쉽게 해결할 수 있습니다.

커맨드 라인을 사용하여 추가 통계 모니터링

Firepower Device Manager 대시보드에서는 디바이스를 통과하는 트래픽 및 일반 시스템 사용량과 관련된 다양한 통계를 제공합니다. 그러나 디바이스 CLI에 로그인하면 대시보드에서 통계를 제공하지 않는 영역에 대한 추가 정보를 확인할 수 있습니다(CLI(Command Line Interface) 로그인, 7 페이지 참조).

CLI에는 이러한 통계를 제공하는 여러 가지 **show** 명령이 포함되어 있습니다. CLI를 사용해 일반 문제해결을 수행할 수도 있습니다. 예를 들어 **ping**, **traceroute** 등의 명령을 사용할 수 있습니다. 대부분의 **show** 명령에는 통계를 0으로 재설정하기 위해 함께 사용할 수 있는 **clear** 명령이 있습니다.

Firepower Threat Defense 명령 참조(http://www.cisco.com/c/en/us/td/docs/security/firepower/command_ref/b_Command_Reference_for_Firepower_Threat_Defense.html)에서 명령의 설명서를 확인할 수 있습니다.

일반적으로 유용하게 활용할 수 있는 명령의 예는 다음과 같습니다.

- **show nat**는 NAT 규칙의 적중 횟수를 표시합니다.
- **show xlate**는 활성 상태인 활성 NAT 변환을 표시합니다.
- **show conn**은 디바이스를 통과하는 현재 연결에 대한 정보를 제공합니다.
- **show dhcpd**는 인터페이스에 대해 구성하는 DHCP 서버에 대한 정보를 제공합니다.
- **show interface**는 각 인터페이스의 사용량 통계를 제공합니다.

이벤트 보기

로깅을 사용하는 액세스 규칙에서 생성된 이벤트를 확인할 수 있습니다. 트리거된 침입 및 파일 정책에 대해서도 이벤트가 생성됩니다.

이벤트 뷰어 테이블에는 생성되는 이벤트가 실시간으로 표시됩니다. 새 이벤트가 생성되면 이전 이벤트는 테이블에 표시되지 않게 됩니다.

시작하기 전에

특정 유형의 이벤트가 생성되는지 여부는 관련 정책과 일치하는 연결 외에 다음 사항에 따라서도 달라집니다.

- 연결 이벤트 - 액세스 규칙이 연결 로깅을 사용해야 합니다.
- 침입 이벤트 - 액세스 규칙이 침입 정책을 적용해야 합니다.
- 파일 및 악성코드 이벤트 - 액세스 규칙이 파일 정책을 적용하고 파일 로깅을 사용해야 합니다.

절차

단계 **1** 주 메뉴에서 **Monitoring(**모니터링**)**을 클릭합니다.

단계 **2** 목차에서 **Events(**이벤트**)**를 선택합니다.
이벤트 뷰어에서는 탭의 이벤트가 이벤트 유형을 기준으로 구성됩니다. 자세한 내용은 이벤트 유형, 76 페이지를 참고하십시오.

단계 **3** 보려는 이벤트의 유형이 표시된 탭을 클릭합니다.
이벤트 목록을 사용하여 다음 작업을 수행할 수 있습니다.

- 이벤트를 보다 쉽게 찾고 분석할 수 있도록 새 이벤트 추가를 중지하려면 **Pause(**일시정지**)**를 클릭합니다. 새 이벤트가 표시되도록 하려면 **Resume(**재시작**)**를 클릭합니다.
- 새 이벤트가 표시되는 속도를 제어하려면 여러 새로고침 속도(5초, 10초, 20초, 60초) 중에서 선택합니다.
- 원하는 열이 포함된 맞춤형 보기를 생성합니다. 맞춤형 보기를 생성하려면 탭 막대에서 + 버튼을 클릭하거나 **Add/Remove Columns(**열 추가/제거**)**를 클릭합니다. 사전 설정된 탭은 변경할 수 없으므로 열을 추가하거나 제거하면 새 보기가 생성됩니다. 자세한 내용은 사용자 지정 보기 구성, 77 페이지를 참고하십시오.
- 열의 폭을 변경하려면 열 제목 구분선을 클릭하여 원하는 폭으로 끌어옵니다.
- 이벤트 위에 마우스를 올려 놓고 **View Details(**세부정보 보기**)**를 클릭하면 이벤트에 대한 전체 정보를 확인할 수 있습니다. 이벤트 내의 여러 필드에 대한 설명은 이벤트 필드 설명, 79 페이지를 참조하십시오.

단계 **4** 필요한 경우 다양한 이벤트 속성에 따라 원하는 이벤트를 쉽게 찾을 수 있도록 테이블에 필터를 적용합니다.

새 필터를 생성하려면 드롭다운 목록에서 원자성 요소를 선택하고 필터 값을 입력하여 필터를 수동으로 입력하거나, 필터링할 값이 포함된 이벤트 테이블에서 셀 하나를 클릭하여 필터를 작성합니다. 같은 열의 여러 셀을 클릭하여 값 간의 OR 조건을 생성할 수도 있고, 서로 다른 열의 셀을 클릭하여 열 간의 AND 조건을 생성할 수도 있습니다. 셀을 클릭하여 필터를 작성하는 경우에는 결과로 생성되는 필터를 수정하여 미세 조정할 수 있습니다. 필터 규칙 생성에 대한 자세한 내용은 이벤트 필터링, 77 페이지를 참조하십시오.

필터를 작성한 후에는 다음 중에서 원하는 작업을 수행합니다.

- 필터를 적용하고 필터와 일치하는 이벤트만 표시되도록 테이블을 업데이트하려면 **Filter(**필터**)** 버튼을 클릭합니다.
- 적용한 전체 필터를 지우고 테이블을 필터링되지 않은 상태로 되돌리려면 **Filter(**필터**)** 상자에서 **Reset Filters(**필터 재설정**)**를 클릭합니다.
- 필터의 원자성 요소 중 하나를 지우려면 해당 요소 위에 마우스를 올려 놓고 요소에 대해 표시되는 **X**를 클릭합니다. 그런 다음 **Filter(**필터**)** 버튼을 클릭합니다.

이벤트 유형

시스템은 다음 이벤트 유형을 생성할 수 있습니다. 모니터링 대시보드에서 이 정보와 관련된 통계를 확인하려면 이러한 이벤트를 생성해야 합니다.

연결 이벤트

사용자가 시스템을 통과하는 트래픽을 생성할 때 연결에 대한 이벤트를 생성할 수 있습니다. 액세스 규칙에 대해 연결 로깅을 사용하는 경우에만 연결 이벤트가 표시됩니다.

연결 이벤트에는 소스/대상 IP 주소와 포트, 사용한 URL 및 애플리케이션, 전송된 바이트 또는 패킷의 수 등 연결에 대한 여러 가지 정보가 포함됩니다. 수행한 작업(예: 연결 허용 또는 차단) 및 연결에 적용된 정책도 이러한 정보에 포함됩니다.

침입 이벤트

시스템은 호스트 및 호스트 데이터의 가용성, 무결성 및 기밀성에 영향을 미칠 수 있는 악성 활동 탐지를 위해 네트워크를 통과하는 패킷을 검토합니다. 시스템은 침입 가능성을 식별하는 경우 익스플로잇의 날짜, 시간, 익스플로잇 유형, 그리고 공격 소스와 대상에 관한 상황 정보의 레코드인 침입 이벤트를 생성합니다.

파일 이벤트

파일 이벤트는 파일 정책을 기준으로 하여 시스템이 네트워크 트래픽에서 탐지하고 선택적으로 차단한 파일을 나타냅니다. 이러한 이벤트를 생성하려면 파일 정책을 적용하는 액세스 규칙에 대해 파일 로깅을 사용해야 합니다.

시스템이 파일 이벤트를 생성하는 경우 호출하는 액세스 제어 규칙의 로깅 컨피그레이션과 관계없이 시스템은 관련 연결의 종료도 로깅합니다.

악성코드 이벤트

시스템은 전체적인 액세스 제어 컨피그레이션의 일부로 네트워크 트래픽에서 악성코드를 탐지할 수 있습니다. AMP for Firepower는 결과 이벤트의 상태와 악성코드가 탐지된 방법, 위치, 시간에 대한 상황 데이터를 포함하는 악성코드 이벤트를 생성할 수 있습니다. 이러한 이벤트를 생성하려면 파일 정책을 적용하는 액세스 규칙에 대해 파일 로깅을 사용해야 합니다.

사용자 지정 보기 구성

이벤트를 확인할 때 원하는 열을 쉽게 볼 수 있도록 맞춤형 보기를 생성할 수 있습니다. 사용자 지정 보기는 수정하거나 삭제할 수도 있습니다. 사전 정의된 보기는 수정하거나 삭제할 수 없습니다.

절차

단계 **1** **Monitoring(**모니터링**)** > **Events(**이벤트**)**를 선택합니다.

단계 **2** 다음 중 하나를 수행합니다.

- 기존 사용자 지정 보기 또는 사전 정의된 보기를 기준으로 새 보기를 생성하려면 보기의 탭을 클릭하고 탭 왼쪽에 있는 + 버튼을 클릭합니다.
- 기존 사용자 지정 보기를 수정하려면, 보기의 탭을 클릭합니다.

참고 사용자 지정 보기를 삭제하려는 경우에는 보기 탭에서 **X** 버튼만 클릭하면 됩니다. 삭제는 취소할 수 없습니다.

단계 **3** 오른쪽의 이벤트 테이블 위에 있는 열 추가/제거 링크를 클릭한 다음, 보기에 포함하려는 열만 선택한 목록에 포함될 때까지 열을 선택하거나 선택을 취소합니다.
열을 클릭한 다음 끌어서 사용할 수 있지만 사용하지 않은 목록과 선택한 목록 간을 이동합니다. 선택한 목록에서 열을 클릭하고 끌어서 테이블 내의 열 순서(왼쪽에서 오른쪽)를 변경할 수도 있습니다. 열에 대한 설명은 이벤트 필드 설명, 79 페이지를 참조하십시오.

작업을 완료한 후 **OK(**확인**)**를 클릭하여 열 변경 사항을 저장합니다.

참고 사전 정의된 보기가 표시된 상태에서 열 선택을 변경하면 새 보기가 생성됩니다.

단계 **4** 필요한 경우 열 구분 기호를 클릭하고 끌어서 열 너비를 변경합니다.

이벤트 필터링

이벤트 테이블에 현재 확인하고자 하는 이벤트만 표시되도록 제한하는 복잡한 필터를 생성할 수 있습니다. 다음과 같은 기술을 단독으로 사용하거나 조합하여 필터를 작성할 수 있습니다.

열 클릭

필터를 작성하는 가장 쉬운 방법은 필터링할 값이 포함된 이벤트 테이블의 셀을 클릭하는 것입니다. 셀을 클릭하면 해당 값 및 필드 조합에 대해 올바르게 작성된 규칙을 사용하여 필터 필드가 업데이트됩니다. 그러나 이 기술을 사용하려면 기존 이벤트 목록에 원하는 값이 포함되어 있어야 합니다.

모든 열을 필터링할 수는 없습니다. 셀의 콘텐츠를 필터링할 수 있는 경우 해당 셀 위에 마우스를 올려놓으면 셀에 밑줄이 표시됩니다.

원자성 요소 선택

필터 필드를 클릭하고 드롭다운 목록에서 원하는 원자성 요소를 선택한 다음 일치 값을 입력하여 필터를 작성할 수도 있습니다. 이러한 요소는 이벤트 테이블에 열로 표시되지 않는 이벤트 필드를 포함합니다. 또한 입력하는 값과 표시할 이벤트 간의 관계를 정의하는 연산자도 포함합니다. 열을 클릭할 때는 항상 "같음(=)" 필터가 적용되는 반면 요소를 선택할 때는 숫자 필드에 대해 "보다 큼(>)" 또는 "보다 작음(<)"도 선택할 수 있습니다.

필터, 필드에 요소를 추가하는 방법과 관계없이 필드에 값을 입력하여 연산자나 값을 조정할 수 있습니다. 테이블에 필터를 적용하려면 필터를 클릭합니다.

이벤트 필터용 연산자

이벤트 필터에서는 다음 연산자를 사용할 수 있습니다.

=	같음. 이벤트가 지정된 값과 일치합니다. 와일드카드는 사용할 수 없습니다.
!=	같지 않음. 이벤트가 지정된 값과 일치하지 않습니다. 같지 않음 식을 작성하려면 !(느낌표)를 입력해야 합니다.
>	보다 큼. 이벤트에 지정된 값보다 큰 값이 포함되어 있습니다. 이 연산자는 포트 및 IP 주소와 같은 숫자 값에만 사용할 수 있습니다.
<	보다 작음. 이벤트에 지정된 값보다 작은 값이 포함되어 있습니다. 이 연산자는 숫자 값에만 사용할 수 있습니다.

복잡한 이벤트 필터에 대한 규칙

여러 원자성 요소가 포함된 복잡한 필터를 작성할 때는 다음 규칙에 주의하십시오.

- 유형이 같은 요소의 경우 해당 유형의 모든 값 간에 OR 관계가 설정됩니다. 예를 들어 이니시에이터 IP=10.100.10.10 및 이니시에이터 IP=10.100.10.11을 포함하는 경우 트래픽 소스로 이러한 주소 중 하나를 포함하는 이벤트가 일치 항목으로 표시됩니다.
- 유형이 다른 요소의 경우 AND 관계가 설정됩니다. 예를 들어 이니시에이터 IP=10.100.10.10 및 대상 포트/ICMP 유형=80을 포함하는 경우 이 소스 주소와 대상 포트를 모두 포함하는 이벤트만 일치 항목으로 표시됩니다. 10.100.10.10에서 다른 대상 포트로 향하는 이벤트는 표시되지 않습니다.

- IPv4 및 IPv6 주소를 포함한 숫자 요소의 경우 범위를 지정할 수 있습니다. 예를 들어 대상 포트 =50-80을 지정하여 해당 범위 내의 포트에 대한 모든 트래픽을 캡처할 수 있습니다. 하이픈을 사용하여 시작 숫자와 종료 숫자를 분리합니다. 모든 숫자 필드에 범위를 사용할 수 있는 것은 아닙니다. 예를 들어 소스 요소에서는 IP 주소 범위를 지정할 수 없습니다.
- 와일드카드나 정규식은 사용할 수 없습니다.

이벤트 필드 설명

이벤트는 다음 정보를 포함할 수 있습니다. 이벤트 세부사항을 볼 때 이 정보를 확인할 수 있습니다. 이벤트 뷰어 테이블에 열을 추가하여 가장 관심이 높은 정보를 표시할 수도 있습니다.

아래에는 사용 가능한 필드의 전체 목록이 나와 있습니다. 모든 이벤트 유형에 모든 필드가 적용되는 것은 아닙니다. 개별 이벤트에 사용 가능한 정보는 시스템에서 연결을 로깅한 방법, 이유 및 시기에 따라 달라질 수 있습니다.

작업

연결 이벤트의 경우 액세스 제어 규칙과 연결된 작업 또는 연결을 로깅한 기본 작업

허용

명시적으로 허용된 연결

신뢰

신뢰할 수 있는 연결. 첫 번째 패킷의 신뢰 규칙에 의해 탐지된 TCP 연결은 연결 종료 이벤트만 생성합니다. 시스템에서는 최종 세션 패킷이 끝난 지 한 시간 후에 이벤트를 생성합니다.

차단

차단된 연결. 다음 상황에서 차단 작업을 허용 액세스 규칙과 연결할 수 있습니다.

- 침입 정책에 따라 익스플로잇이 차단된 연결
- 파일 정책에 따라 파일이 차단된 연결

기본 작업

연결이 기본 작업에 의해 처리되었습니다.

파일 또는 악성코드 이벤트의 경우, 파일과 일치하는 규칙에 대한 규칙 작업과 관련된 파일 규칙 작업 및 관련된 모든 파일 규칙 작업 옵션.

허용된 연결

시스템이 이벤트에 대한 트래픽 흐름을 허용하는지 여부

애플리케이션

연결에서 탐지된 애플리케이션

애플리케이션 비즈니스 관련성

연결에서 탐지된 애플리케이션 트래픽과 연계된 사업 타당성으로, 매우 높음, 높음, 중간, 낮음, 매우 낮음이 있습니다. 연결에서 탐지된 각 애플리케이션 유형에는 관련된 사업 타당성이 있습니다. 이 필드에는 그중 가장 낮은 값(가장 연관성이 적음)이 표시됩니다.

애플리케이션 범주, 애플리케이션 태그

애플리케이션의 기능을 파악하는 데 도움이 될 수 있도록 애플리케이션의 특성을 분류하는 기준입니다.

애플리케이션 위험성

연결에서 탐지된 애플리케이션 트래픽과 관련된 위험성으로, 매우 높음, 높음, 중간, 낮음, 매우 낮음이 있습니다. 연결에서 탐지된 웹 애플리케이션의 각 유형에는 관련된 위험이 있습니다. 이 필드에는 그중 가장 높은 위험이 표시됩니다.

차단 유형

이벤트의 트래픽 흐름과 일치하는 액세스 제어 규칙에서 지정된 차단 유형: 차단 또는 양방향 차단

클라이언트 애플리케이션, 클라이언트 버전

연결에서 탐지된 클라이언트 애플리케이션 및 클라이언트 버전입니다.

클라이언트 비즈니스 관련성

연결에서 탐지된 클라이언트 트래픽과 관련된 사업 타당성으로, 매우 높음, 높음, 중간, 낮음, 매우 낮음이 있습니다. 연결에서 탐지된 각 클라이언트 유형에는 관련된 사업 타당성이 있습니다. 이 필드에는 그중 가장 낮은 값(가장 연관성이 적음)이 표시됩니다.

클라이언트 범주, 클라이언트 태그

애플리케이션의 기능을 파악하는 데 도움이 될 수 있도록 애플리케이션의 특성을 분류하는 기준입니다.

클라이언트 위험성

연결에서 탐지된 클라이언트 트래픽과 관련된 위험성으로, 매우 높음, 높음, 중간, 낮음, 매우 낮음이 있습니다. 연결에서 탐지된 클라이언트의 각 유형에는 관련된 위험이 있습니다. 이 필드에는 그중 가장 높은 위험이 표시됩니다.

연결

내부에서 생성되는 트래픽 흐름의 고유 ID

연결 차단 유형 표시기

이벤트의 트래픽 흐름과 일치하는 액세스 제어 규칙에서 지정된 차단 유형: 차단 또는 양방향 차단

연결 바이트

연결에 대한 총 바이트

연결 시간

연결 시작 시간

연결 타임 스탬프

연결이 탐지된 시간

거부된 연결

시스템이 이벤트에 대한 트래픽 흐름을 거부하는지 여부

대상 국가 및 대륙

수신 호스트의 국가와 대륙

대상 **IP**

수신 호스트의 IP 주소

대상 포트**/ICMP** 코드**,** 대상 포트**,** 대상 **Icode**

세션 responder가 사용하는 포트 또는 ICMP 코드

방향

파일의 전송 방향

속성

파일의 속성

악성코드

AMP 클라우드가 파일을 악성코드로 분류했거나, 파일의 위협 점수가 파일 정책에서 정의된 악성코드 임계값을 초과했음을 나타냅니다.

정상

AMP 클라우드가 파일을 정상으로 분류했음을 나타냅니다.

알 수 없음

시스템이 AMP 클라우드를 쿼리했으나 파일에 상태가 할당되지 않았음을 나타냅니다. 즉, AMP 클라우드에서 파일을 분류하지 않았습니다.

사용 불가능

시스템이 AMP 클라우드를 쿼리하지 못했음을 나타냅니다. 이 속성을 통해 이벤트의 일부를 확인할 수 있습니다. 이는 예상된 작업입니다.

해당 없음

파일 탐지 또는 파일 차단 규칙이 파일을 처리했으며 시스템이 AMP 클라우드를 쿼리하지 않았음을 나타냅니다.

이그레스 인터페이스**,** 이그레스 보안 영역

연결이 디바이스에서 외부로 나간 인터페이스 및 영역

이벤트**,** 이벤트 유형

이벤트 유형.

이벤트 초**,** 이벤트 마이크로초

이벤트가 탐지된 시간(단위: 초 또는 마이크로초)

파일 카테고리

파일 유형의 일반적인 범주(예: Office 문서, 아카이브, 멀티미디어, 실행 파일, PDF 파일, 인코딩, 그래픽 또는 시스템 파일 등)

파일 이벤트 타임 스탬프

파일 또는 악성코드 파일이 생성된 시간 및 날짜

파일 이름

파일의 이름.

파일 규칙 작업

파일을 탐지한 파일 정책 규칙과 연결된 작업 및 관련된 모든 파일 규칙 작업 옵션

파일 **SHA256**

파일의 SHA-256 해시 값

파일 크기**(KB)**

킬로바이트 단위의 파일 크기. 파일이 완전히 수신되기 전에 시스템에서 파일을 차단한 경우에는 파일 크기를 비워 둘 수 있습니다.

파일 유형

HTML 또는 MSEXE 등의 파일 형식

파일/악성 프로그램 정책

이벤트 생성과 관련된 파일 정책.

파일 로그 차단 유형 표시기

이벤트의 트래픽 흐름과 일치하는 파일 규칙에서 지정된 차단 유형: 차단 또는 양방향 차단

방화벽 정책 규칙**,** 방화벽 규칙

연결을 처리한 액세스 제어 규칙 또는 기본 작업

첫 번째 패킷

세션의 첫 번째 패킷이 표시된 날짜 및 시간

HTTP 참조 페이지

연결(다른 URL에 링크를 제공하는 웹 사이트 또는 다른 URL에서 링크를 가져온 웹 사이트 등)에서 탐지된 HTTP 트래픽에 대해 요청된 URL의 참조 페이지를 나타내는 HTTP 참조 페이지

HTTP 응답

연결을 통해 클라이언트의 HTTP 요청에 대한 응답으로 전송된 HTTP 상태 코드

IDS 분류

이벤트를 생성한 규칙이 속하는 분류.

인그레스 인터페이스**,** 인그레스 보안 영역

연결이 디바이스로 들어온 인터페이스 및 영역

이니시에이터 바이트**,** 이니시에이터 패킷

세션 이니시에이터가 전송한 총 바이트 또는 패킷 수

이니시에이터 국가 및 대륙

세션을 시작한 호스트의 국가 및 대륙. 이니시에이터 IP 주소를 라우팅할 수 있는 경우에만 사용 가능합니다.

이니시에이터 **IP**

세션을 시작한 호스트 IP 주소(DNS 확인을 활성화한 경우 호스트 이름)

인라인 결과

인라인 모드에서 작동하는 경우 침입 이벤트를 트리거한 패킷을 시스템에서 삭제했거나 삭제할 수 있었는지 여부. 비워 두는 경우 트리거된 규칙이 삭제 및 이벤트 생성으로 설정되지 않았음을 나타냅니다.

침입 정책

이벤트를 생성한 규칙이 활성화된 침입 정책

IPS 차단 유형 표시기

이벤트의 트래픽 흐름과 일치하는 침입 규칙의 작업

마지막 패킷

세션의 마지막 패킷이 표시된 날짜 및 시간

MPLS 레이블

이 침입 이벤트를 트리거한 패킷에 연결된 Multiprotocol Label Switching(다중 프로토콜 레이블 스위칭) 레이블

악성 프로그램 차단 유형 표시기

이벤트의 트래픽 흐름과 일치하는 파일 규칙에서 지정된 차단 유형: 차단 또는 양방향 차단

메시지

침입 이벤트의 경우 이벤트를 설명하는 텍스트. 악성코드 또는 파일 이벤트의 경우 악성코드 이벤트와 관련된 모든 추가 정보.

NetBIOS 도메인

세션에서 사용되는 NetBIOS 도메인

원본 클라이언트 국가 및 대륙

세션을 시작한 원본 클라이언트 호스트의 국가와 대륙. 원본 클라이언트 IP 주소를 라우팅할 수 있는 경우에만 사용 가능합니다.

원본 클라이언트 **IP**

HTTP 연결을 시작한 클라이언트의 원본 IP 주소. 이 주소는 XFF(X-Forwarded-For) 또는 True-Client-IP HTTP 헤더 필드나 그와 동일한 필드에서 파생됩니다.

정책**,** 정책 수정

이벤트와 연결된 액세스(방화벽) 규칙을 포함하는 액세스 제어 정책 및 해당 수정

우선순위

Cisco Talos Security Intelligence and Research Group(Talos)에서 결정한 이벤트 우선순위(높음, 중간, 낮음)

프로토콜

연결에 사용된 전송 프로토콜

이유

다음과 같은 상황에서 연결이 로깅된 이유

이유	설명
파일 차단	시스템이 전송을 차단한 파일 또는 악성코드 파일이 연결에 포함되었습니다. 파일 차단 이유는 항상 차단 작업과 페어링됩니다.
파일 모니터링	시스템이 연결에서 특정 파일 유형을 탐지했습니다.
파일 재시작 허용	파일 전송이 파일 차단 또는 악성코드 차단 파일 규칙에 의해 원래 차단되었다가, 해당 파일을 허용하는 새 액세스 제어 정책이 구축된 후 HTTP 세션이 자동으로 재시작되었습니다.
파일 재시작 차단	파일 전송이 파일 탐지 또는 악성코드 클라우드 조회 파일 규칙에 의해 원래 허용되었다가, 해당 파일을 차단하는 새 액세스 제어 정책이 구축된 후 HTTP 세션이 자동으로 중지되었습니다.
침입 차단	시스템이 연결에서 탐지된 익스플로잇(침입 정책 위반)을 차단했거나 차단할 수도 있었음을 나타냅니다. 침입 차단 이유는 차단된 익스플로잇의 경우 차단 작업과, 차단될 수도 있었던 익스플로잇의 경우 허용과 페어링됩니다.
침입 모니터링	시스템이 연결에서 탐지된 익스플로잇을 탐지했지만 차단하지는 않았습니다. 트리거된 침입 규칙의 상태가 이벤트 생성으로 설정되어 있으면 이러한 현상이 나타납니다.

수신된 시간

이벤트가 생성된 날짜 및 시간

참조된 호스트

연결의 프로토콜이 HTTP, 또는 HTTPS인 경우 이 필드에는 각 프로토콜이 사용했던 호스트 이름이 표시됩니다.

Responder 바이트**, Responder** 패킷

세션 Responder가 전송한 총 바이트 또는 패킷 수

Responder 국가 및 대륙

세션에 응답한 호스트의 국가 및 대륙. Responder IP 주소를 라우팅할 수 있는 경우에만 사용 가능합니다.

Responder IP

세션 Responder의 호스트 IP 주소(DNS 확인을 활성화한 경우 호스트 이름)

서명

이벤트의 트래픽과 일치하는 침입 규칙의 서명 ID

소스 국가 및 대륙

전송 호스트의 국가와 대륙 소스 IP 주소를 라우팅할 수 있는 경우에만 사용 가능합니다.

소스 **IP**

침입 이벤트에서 전송 호스트가 사용하는 IP 주소

소스 포트**/ICMP** 유형**,** 소스 포트**,** 소스 포트 **Itype**

세션 이니시에이터가 사용하는 포트 또는 ICMP 유형

TCP 플래그

연결에서 탐지된 TCP 플래그

URL, URL 범주**, URL** 평판**, URL** 평판 점수

세션 중에 모니터링된 호스트에서 요청한 URL과 관련 범주, 평판 및 평판 점수(사용 가능한 경우)

시스템에서 SSL 애플리케이션을 식별하거나 차단한 경우, 요청한 URL은 암호화된 트래픽에 있으므로 시스템은 SSL 인증서를 기준으로 해당 트래픽을 식별합니다. 따라서 SSL 애플리케이션의 경우 URL은 인증서에 포함된 공용 이름을 나타냅니다.

사용자

이니시에이터 IP 주소와 연결된 사용자

VLAN

이벤트를 트리거한 패킷에 관련된 가장 안쪽의 VLAN ID

웹 애플리케이션 사업 타당성

연결에서 탐지된 웹 애플리케이션 트래픽과 연계된 사업 타당성으로, 매우 높음, 높음, 중간, 낮음, 매우 낮음이 있습니다. 연결에서 탐지된 웹 애플리케이션의 각 유형은 관련된 비즈니스 관련성을 가지며, 이 필드는 가장 낮은(가장 타당성이 적은) 것을 표시합니다.

웹 애플리케이션 범주**,** 웹 애플리케이션 태그

웹 애플리케이션의 기능을 파악하는 데 도움이 될 수 있도록 웹 애플리케이션의 특성을 분류하는 기준

웹 애플리케이션 위험성

연결에서 탐지된 웹 애플리케이션 트래픽과 관련된 위험성으로, 매우 높음, 높음, 중간, 낮음, 매우 낮음이 있습니다. 연결에서 탐지된 웹 애플리케이션의 각 유형에는 관련된 위험이 있습니다. 이 필드에는 그중 가장 높은 위험이 표시됩니다.

웹 애플리케이션

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.

5 장

개체

개체는 정책이나 기타 설정에서 사용하려는 기준을 정의하는 재사용 가능 컨테이너입니다. 예를 들어 네트워크 개체는 호스트 및 서브넷 주소를 정의합니다.

개체를 사용하면 기준을 정의하여 서로 다른 여러 정책에서 같은 기준을 쉽게 재사용할 수 있습니다. 개체를 업데이트하면 해당 개체를 사용하는 모든 정책이 자동으로 업데이트됩니다.

개체 유형

다음과 같은 유형의 개체를 생성할 수 있습니다. 대부분의 경우에는 정책이나 설정이 개체를 허용하는 경우 개체를 사용해야 합니다.

개체 유형	주요 용도	설명
애플리케이션 필터	액세스 제어 규칙	애플리케이션 필터 개체는 IP 연결에 사용되는 애플리케이션 또는 유형, 범주, 태그, 위험, 사업 타당성에 따라 애플리케이션을 정의하는 필터를 정의합니다. 포트 사양을 사용하는 대신 정책에서 이러한 개체를 사용하여 트래픽을 제어할 수 있습니다. 애플리케이션 필터 개체 구성, 95 페이지를 참조하십시오.
지리위치	보안 정책	지리위치 개체는 트래픽의 소스나 대상인 디바이스를 호스팅하는 국가와 대륙을 정의합니다. IP 주소를 사용하는 대신 정책에서 이러한 개체를 사용하여 트래픽을 제어할 수 있습니다. 지리위치 개체 구성, 98 페이지를 참조하십시오.

개체 유형	주요 용도	설명
IKE 정책	VPN	IKE(Internet Key Exchange) 정책 개체는 IPsec 피어를 인증하고, IPsec 암호화 키를 협상 및 배포하고, IPsec SA(보안 연계)를 자동으로 설정하는 데 사용되는 IKE 제안을 정의합니다. IKEv1과 IKEv2용으로 별도의 개체가 있습니다. 글로벌 IKE 정책 구성, 267 페이지를 참조하십시오.
IPSec 제안	VPN	IPsec 제안 개체는 IKE 2단계 협상 중에 사용되는 IPsec 제안을 구성합니다. IPsec 제안은 IPsec 터널에서 트래픽을 보호하는 보안 프로토콜 및 알고리즘 조합을 정의합니다. IKEv1과 IKEv2용으로 별도의 개체가 있습니다. IPsec 제안 구성, 271 페이지를 참조하십시오.
네트워크	보안 정책 및 다양한 디바이스 설정	네트워크 그룹과 네트워크 개체(네트워크 개체로 총칭함)는 호스트 또는 네트워크의 주소를 정의합니다. 네트워크 개체 및 그룹 구성, 91 페이지를 참조하십시오.
포트	보안 정책	포트 그룹과 포트 개체(포트 개체로 총칭함)는 트래픽용 프로토콜, 포트 또는 ICMP 서비스를 정의합니다. 포트 개체 및 그룹 구성, 92 페이지를 참조하십시오.
Security Zone	보안 정책	보안 영역은 인터페이스의 그룹입니다. 이러한 영역은 트래픽을 쉽게 관리 및 분류할 수 있도록 네트워크를 세그먼트로 구분합니다. 보안 영역 구성, 94 페이지를 참조하십시오.
Syslog 서버	액세스 제어 규칙 진단 로깅 SSL 암호 해독 규칙	syslog 서버 개체는 연결 지향형 또는 진단 시스템 로그(syslog) 메시지를 수신할 수 있는 서버를 식별합니다. syslog 서버 구성, 99 페이지를 참조하십시오.
URL	액세스 제어 규칙	URL 개체 및 그룹(URL 개체로 총칭함)은 웹 요청의 URL 또는 IP 주소를 정의합니다. URL 개체 및 그룹 구성, 97 페이지를 참조하십시오.

개체 관리

개체는 개체 페이지를 통해 직접 구성할 수도 있고 정책을 수정하면서 구성할 수도 있습니다. 둘 중 어떤 방법을 사용하든 결과는 같습니다(새 개체가 생성되거나 기존 개체가 업데이트됨). 그러므로 작업 시 필요에 맞는 기술을 사용하면 됩니다.

다음 절차에서는 개체 페이지를 통해 개체를 직접 생성하고 관리하는 방법에 대해 설명합니다.

참고 정책이나 설정을 수정할 때 속성에 개체가 필요한 경우 이미 정의된 개체 목록이 표시되며, 여기서 적절한 개체를 선택합니다. 원하는 개체가 아직 없는 경우 목록에 표시된 **Create New Object(**새 개체 생성**)** 링크를 클릭하면 됩니다.

절차

단계 **1** **Objects(**개체**)**를 선택합니다.
개체 페이지에는 사용 가능한 개체 유형이 나열된 목차가 있습니다. 개체 유형을 선택할 때는 기존 개체 목록이 표시되며, 이 목록에서 새 개체를 생성할 수 있습니다. 개체 내용과 유형도 확인할 수 있습니다.

단계 **2** 목차에서 개체 유형을 선택하고 다음 중 원하는 작업을 수행합니다.

- 개체를 생성하려면 + 버튼을 클릭합니다. 개체의 내용은 유형에 따라 다릅니다. 구체적인 정보는 각 개체 유형에 대한 컨피그레이션 주제를 참조하십시오.
- 그룹 개체를 생성하려면 **Add Group(**그룹 추가**)**( ) 버튼을 클릭합니다. 그룹 개체에는 항목이 두 개 이상 포함됩니다.
- 개체를 수정하려면 개체의 수정 아이콘( )을 클릭합니다. 사전 정의된 개체의 내용은 수정할 수 없습니다.
- 개체를 삭제하려면 개체의 삭제 아이콘( )을 클릭합니다. 정책 또는 다른 개체에서 현재 사용되고 있는 개체 또는 사전 정의된 개체는 삭제할 수 없습니다.

네트워크 개체 및 그룹 구성

네트워크 그룹과 네트워크 개체(네트워크 개체로 총칭함)를 사용하여 호스트 또는 네트워크의 주소를 정의합니다. 그런 후에는 이러한 개체를 보안 정책에서 사용하여 트래픽 일치 기준을 정의하거나, 설정에서 사용하여 서버 또는 기타 리소스의 주소를 정의할 수 있습니다.

네트워크 개체는 단일 호스트 또는 네트워크 주소를 정의하는 반면 네트워크 그룹 개체는 여러 주소를 정의할 수 있습니다.

다음 절차에서는 개체 페이지를 통해 개체를 직접 생성하고 수정할 수 있는 방법을 설명합니다. 개체 목록에 표시되는 **Create New Network(**새 네트워크 생성**)** 링크를 클릭하여 주소 속성을 수정하면서 네트워크 개체를 생성할 수도 있습니다.

절차

단계 **1** 목차에서 **Objects(**개체**)**와 **Network(**네트워크**)**를 차례로 선택합니다.

단계 **2** 다음 중 하나를 수행합니다.

- 개체를 생성하려면 + 버튼을 클릭합니다.
- 그룹을 생성하려면 그룹 추가( ) 버튼을 클릭합니다.
- 개체 또는 그룹을 수정하려면 개체의 수정 아이콘( )을 클릭합니다.

참조되지 않는 개체를 삭제하려면 해당 개체의 휴지통 아이콘( )을 클릭합니다.

단계 **3** 개체의 이름과 설명(선택 사항)을 입력하고 개체 콘텐츠를 정의합니다.

네트워크 개체

개체 유형을 네트워크 또는 호스트 중에서 선택합니다. 그런 다음 호스트 또는 네트워크 주소를 입력합니다. 다음 형식을 사용할 수 있습니다.

- IPv4 호스트 주소(예: 10.100.10.10)
- 서브넷 마스크가 포함된 IPv4 주소(예: 10.100.10.0/24 또는 10.100.10.0/255.255.255.0)
- IPv6 호스트 주소(예: 2001:DB8::0DB8:800:200C:417A 또는 2001:DB8:0:0:0DB8:800:200C:417A)
- 접두사가 포함된 IPv6 네트워크 주소(예: 2001:DB8:0:CD30::/60)

네트워크 그룹

+ 버튼을 클릭하여 그룹에 추가할 네트워크 개체를 선택합니다. 새 개체를 생성할 수도 있습니다.

단계 **4** **OK(**확인**)**를 클릭하여 변경 사항을 저장합니다.

포트 개체 및 그룹 구성

포트 그룹과 포트 개체(포트 개체로 총칭함)를 사용하여 트래픽용 프로토콜, 포트 또는 ICMP 서비스를 정의합니다. 그런 후에는 이러한 개체를 보안 정책에서 사용하여 트래픽 일치 기준(예: 특정 TCP 포트에 대한 트래픽을 허용하는 액세스 규칙을 사용하기 위한 기준)을 정의할 수 있습니다.

포트 개체는 단일 프로토콜, TCP/UDP 포트나 포트 범위 또는 ICMP 서비스를 정의하는 반면 포트 그룹 개체는 여러 서비스를 정의할 수 있습니다.

시스템에는 일반 서비스를 위해 사전 정의된 개체가 여러 개 포함되어 있으며, 정책에서 이러한 개체를 사용할 수 있습니다. 그러나 시스템 정의 개체는 수정하거나 삭제할 수 없습니다.

참고 포트 그룹 개체를 생성할 때는 개체 조합이 적절한지 확인합니다. 예를 들어 개체를 사용해 액세스 규칙에서 소스 포트와 대상 포트를 모두 지정하는 경우에는 해당 개체 내에 프로토콜을 혼합하여 포함할 수 없습니다. 이미 사용 중인 개체를 수정할 때는 주의해야 합니다. 해당 개체를 사용하는 정책이 무효화되고 비활성화될 수 있기 때문입니다.

다음 절차에서는 개체 페이지를 통해 개체를 직접 생성하고 수정할 수 있는 방법을 설명합니다. 개체 목록에 표시되는 **Create New Port(**새 포트 생성**)** 링크를 클릭하여 서비스 속성을 수정하면서 포트 개체를 생성할 수도 있습니다.

절차

단계 **1** 목차에서 **Objects(**개체**)**와 **Ports(**포트**)**를 차례로 선택합니다.

단계 **2** 다음 중 하나를 수행합니다.

- 개체를 생성하려면 + 버튼을 클릭합니다.
- 그룹을 생성하려면 그룹 추가( ) 버튼을 클릭합니다.
- 개체 또는 그룹을 수정하려면 개체의 수정 아이콘( )을 클릭합니다.

참조되지 않는 개체를 삭제하려면 해당 개체의 휴지통 아이콘( )을 클릭합니다.

단계 **3** 개체의 이름과 설명(선택 사항)을 입력하고 개체 콘텐츠를 정의합니다.

포트 개체

프로토콜을 선택하고 다음과 같이 프로토콜을 구성합니다.

- **TCP**, **UDP** - 80(HTTP) 또는 1~65535(모든 포트 포함)와 같이 단일 포트 또는 포트 범위 번호를 입력합니다.
- **ICMP**, **IPv6-ICMP** - ICMP 유형을 선택하고 필요한 경우 코드를 선택합니다. 해당 유형을 모든 ICMP 메시지에 적용하려면 모두를 선택합니다. 유형과 코드에 대한 자세한 내용은 다음 페이지를 참조하십시오.
  - ICMP -http://www.iana.org/assignments/icmp-parameters/icmp-parameters.xml
  - ICMPv6 -http://www.iana.org/assignments/icmpv6-parameters/icmpv6-parameters.xml
- 기타 - 원하는 프로토콜을 선택합니다.

포트 그룹

+ 버튼을 클릭하여 그룹에 추가할 포트 개체를 선택합니다. 새 개체를 생성할 수도 있습니다.

단계 **4** **OK(**확인**)**를 클릭하여 변경 사항을 저장합니다.

보안 영역 구성

보안 영역은 인터페이스의 그룹입니다. 이러한 영역은 트래픽을 쉽게 관리 및 분류할 수 있도록 네트워크를 세그먼트로 구분합니다. 여러 영역을 정의할 수 있지만, 지정된 인터페이스는 하나의 영역에만 속할 수 있습니다.

시스템은 초기 컨피그레이션 시 다음 영역을 생성합니다. 이러한 영역을 수정하여 인터페이스를 추가하거나 제거할 수도 있고, 더 이상 사용하지 않는 영역을 삭제할 수도 있습니다.

- **inside_zone** - 내부 인터페이스를 포함합니다. 내부 인터페이스가 브리지 그룹인 경우 이 영역에는 내부 BVI(브리지 가상 인터페이스)가 아닌 모든 브리지 그룹 구성원 인터페이스가 포함됩니다.이 영역은 내부 네트워크를 나타내는 데 사용됩니다.
- **outside_zone** - 외부 인터페이스를 포함합니다. 이 영역은 인터넷 등 제어 범위 외부에 있는 네트워크를 나타내는 데 사용됩니다.

일반적으로는 인터페이스가 네트워크에서 수행하는 역할별로 인터페이스를 그룹화합니다. 예를 들어 인터넷에 연결하는 인터페이스는 **outside_zone** 보안 영역에 배치하고 내부 네트워크용의 모든 인터페이스는 **inside_zone** 보안 영역에 배치합니다. 그러면 외부 영역에서 들어오는 트래픽과 내부 영역으로 이동하는 트래픽에 액세스 제어 규칙을 적용할 수 있습니다.

영역을 생성하기 전에 네트워크에 적용할 액세스 규칙 및 기타 정책을 고려하십시오. 예를 들어 모든 내부 인터페이스를 같은 영역에 배치할 필요는 없습니다. 내부 네트워크가 4개인데 그중 하나를 나머지 3개와 다른 방식으로 취급하려는 경우에는 영역을 하나가 아닌 두 개 생성할 수 있습니다. 공개 웹 서버에 대한 외부 액세스를 허용해야 하는 인터페이스가 있는 경우에는 해당 인터페이스용으로 별도의 영역을 사용할 수 있습니다.

다음 절차에서는 개체 페이지를 통해 개체를 직접 생성하고 수정할 수 있는 방법을 설명합니다. 개체 목록에 표시되는 **Create New Security Zone(**새 보안 영역 생성**)** 링크를 클릭하여 보안 영역 속성을 수정하면서 보안 영역을 생성할 수도 있습니다.

절차

단계 **1** 목차에서 **Objects(**개체**)**와 **Security Zones(**보안 영역**)**을 차례로 선택합니다.

단계 **2** 다음 중 하나를 수행합니다.

- 개체를 생성하려면 + 버튼을 클릭합니다.
- 개체를 수정하려면 개체의 수정 아이콘( )을 클릭합니다.

참조되지 않는 개체를 삭제하려면 해당 개체의 휴지통 아이콘( )을 클릭합니다.

단계 **3** 개체의 이름과 설명(선택 사항)을 입력합니다.

단계 **4** 인터페이스 목록에서 +를 클릭하고 영역에 추가할 인터페이스를 선택합니다.
목록에는 현재 영역에 포함되어 있지 않고 이름이 지정된 인터페이스가 모두 표시됩니다. 인터페이스를 구성하고 이름을 지정해야 영역에 추가할 수 있습니다.

이름이 지정된 인터페이스가 모두 이미 영역에 포함되어 있으면 이 목록은 비게 됩니다. 다른 영역으로 인터페이스를 이동하려는 경우에는 먼저 현재 영역에서 인터페이스를 제거해야 합니다.

참고 BVI(브리지 그룹 인터페이스)는 영역에 추가할 수 없습니다. 대신 구성원 인터페이스를 추가합니다. 구성원은 다른 영역에 배치할 수 있습니다.

단계 **5** **OK(**확인**)**를 클릭하여 변경 사항을 저장합니다.

애플리케이션 필터 개체 구성

애플리케이션 필터 개체는 IP 연결에 사용되는 애플리케이션 또는 유형, 범주, 태그, 위험, 사업 타당성에 따라 애플리케이션을 정의하는 필터를 정의합니다. 포트 사양을 사용하는 대신 정책에서 이러한 개체를 사용하여 트래픽을 제어할 수 있습니다.

개별 애플리케이션을 지정할 수 있으나 애플리케이션 필터를 사용하면 정책 생성 및 관리가 간소화됩니다. 예를 들어, 위험도가 높고 사업 타당성이 낮은 모든 애플리케이션을 식별하여 차단하는 액세스 제어 규칙을 만들 수 있습니다. 사용자가 이러한 애플리케이션 중 하나를 사용하려고 할 경우, 세션은 차단됩니다.

애플리케이션 필터 개체를 사용하지 않고 정책에서 애플리케이션과 애플리케이션 필터를 직접 선택할 수 있습니다. 그러나 애플리케이션 또는 필터의 동일 그룹에 대해 여러 정책을 생성하려는 경우에는 개체를 사용하는 것이 편리합니다. 시스템에는 수정하거나 삭제할 수 없는 사전 정의된 여러 애플리케이션 필터가 포함되어 있습니다.

참고 Cisco에서는 시스템 및 VDB(Vulnerability Database) 업데이트를 통해 추가 애플리케이션 탐지기를 자주 업데이트하고 추가합니다. 따라서 규칙을 수동으로 업데이트하지 않아도 위험도가 높은 애플리케이션을 차단하는 규칙이 새 애플리케이션에 자동으로 적용될 수 있습니다.

다음 절차에서는 개체 페이지를 통해 개체를 직접 생성하고 수정할 수 있는 방법을 설명합니다. 애플리케이션 탭에 애플리케이션 기준을 추가한 후에 **Save As Filter(**필터로 저장**)** 링크를 클릭하여 액세스 제어 규칙을 수정하는 동안 애플리케이션 필터 개체를 생성할 수도 있습니다.

절차

단계 **1** 목차에서 **Objects(**개체**)**와 **Application Filters(**애플리케이션 필터**)**를 차례로 선택합니다.

단계 **2** 다음 중 하나를 수행합니다.

- 개체를 생성하려면 + 버튼을 클릭합니다.
- 개체를 수정하려면 개체의 수정 아이콘()을 클릭합니다.

참조되지 않는 개체를 삭제하려면 해당 개체의 휴지통 아이콘()을 클릭합니다.

단계 **3** 개체의 이름과 설명(선택 사항)을 입력합니다.

단계 **4** 애플리케이션 목록에서 추가 +를 클릭하고 개체에 추가할 애플리케이션 및 필터를 선택합니다. 초기 목록(계속 스크롤 가능)에는 애플리케이션이 표시됩니다. 고급 필터를 클릭하면 필터 옵션을 확인하고 애플리케이션을 더 쉽게 선택할 수 있는 보기를 표시할 수 있습니다. 원하는 항목을 선택한 후 **Add(**추가**)**를 클릭합니다. 이 프로세스를 반복하여 애플리케이션이나 필터를 더 추가할 수 있습니다.

참고 단일 필터 기준으로 여러 선택 항목이 OR 관계를 갖습니다. 예를 들어, 위험은 높음 OR 매우 높음입니다. 반면 필터 간의 관계는 AND입니다. 즉, 위험은 높음 OR 매우 높음 AND 사업 타당성은 낮음 OR 매우 낮음과 같습니다. 필터를 선택하면 디스플레이의 애플리케이션 목록이 업데이트되어 기준을 충족하는 애플리케이션만 표시됩니다. 이러한 필터를 사용하여 개별적으로 추가하려는 애플리케이션을 찾거나, 규칙에 추가할 적절한 필터를 선택하고 있는지를 확인할 수 있습니다.

위험

애플리케이션이 조직의 보안 정책과 상반되는 용도로 사용될 가능성(매우 낮음~매우 높음)

사업 타당성

조직의 비즈니스 운영(레크리에이션과 반대) 컨텍스트 내에서 애플리케이션이 사용될 가능성(매우 낮음~매우 높음)

유형

애플리케이션 유형:

- 애플리케이션 프로토콜 - 호스트 간의 통신을 나타내는 HTTP, SSH 등의 애플리케이션 프로토콜
- 클라이언트 프로토콜 - 호스트에서 실행 중인 소프트웨어를 나타내는 웹 브라우저, 이메일 클라이언트 등의 클라이언트
- 웹 애플리케이션 - HTTP 트래픽의 요청 URL 또는 콘텐츠를 나타내는 MPEG 비디오, Facebook 등의 웹 애플리케이션

범주

가장 중요한 기능을 설명하는 일반 애플리케이션 분류.

태그

애플리케이션에 대한 추가 정보로, 범주와 비슷합니다.

암호화된 트래픽의 경우, 시스템은 **SSL** 프로토콜 태그가 지정된 애플리케이션만 사용하여 트래픽을 식별하고 필터링할 수 있습니다. 이 태그가 없는 애플리케이션은 암호화되지 않은 트래픽 또는 해독된 트래픽에서만 탐지할 수 있습니다. 또한 암호화된 트래픽 또는 암호화되지 않은 트래픽이 아닌 암호 해독된 트래픽에서만 탐지할 수 있는 애플리케이션에는 암호 해독된 트래픽 태그가 할당됩니다.

애플리케이션 목록**(**디스플레이 하단**)**

이 목록은 목록 위의 옵션에서 필터를 선택하면 업데이트되므로 현재 필터와 일치하는 애플리케이션을 확인할 수 있습니다. 이 목록을 사용하여 규칙에 필터 기준을 추가하려는 경우 필터가 적절한 애플리케이션을 대상으로 하는지를 확인할 수 있습니다. 특정 애플리케이션을 추가하려는 경우 이 목록에서 선택합니다.

단계 **5** **OK(**확인**)**를 클릭하여 변경 사항을 저장합니다.

URL 개체 및 그룹 구성

URL 개체 및 그룹(URL 개체로 총칭함)을 사용하여 웹 요청의 URL 또는 IP 주소를 정의합니다. 이러한 개체를 사용하여 액세스 제어 정책에서 수동 URL 필터링을 구현할 수 있습니다.

URL 개체는 단일 URL 또는 IP 주소를 정의하는 반면 URL 그룹 개체는 여러 URL 또는 주소를 정의할 수 있습니다.

URL 개체를 생성할 때는 다음 사항에 유의하십시오.

- URL 조건이 네트워크 트래픽과 일치하는지 확인하기 위해 시스템은 간단한 부분 문자열 일치를 실행합니다. 요청한 URL은 문자열의 일부분과 일치하는 경우 일치 항목으로 간주됩니다. 따라서 example.com은 www.example.com, ads.example.com 등 해당 네트워크의 모든 호스트와 일치합니다. 또한 badexample.com과도 일치합니다.
- 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 개체를 생성할 때에는 개체 생성 시 프로토콜을 지정할 필요가 없습니다. 이를테면 http://example.com/ 대신 example.com을 사용하십시오.
- URL 개체를 사용하여 액세스 제어 규칙에서 HTTPS 트래픽을 매칭하려는 경우, 트래픽 암호화에 사용되는 공개 키 인증서에서 주체 CN을 사용하여 개체를 생성합니다. 또한 주체 CN에 포함된 하위 도메인은 무시되므로 하위 도메인 정보를 포함하지 마십시오. 이를테면 www.example.com 대신 example.com을 사용하십시오.

참고 특정 사이트를 대상으로 하도록 URL 개체를 구성하기 전에 액세스 제어 장에서 URL 필터링에 대한 정보를 자세히 확인하십시오. URL 일치는 예상한 방식으로 수행되지 않으므로 의도와 달리 사이트가 차단되기 쉽습니다. 예를 들어 게임 사이트 ign.com을 명시적으로 차단하려는 경우 verisign.com과 "ign"으로 끝나는 기타 모든 사이트도 차단됩니다.

다음 절차에서는 개체 페이지를 통해 개체를 직접 생성하고 수정할 수 있는 방법을 설명합니다. 개체 목록에 표시되는 **Create New URL(**새 **URL** 생성**)** 링크를 클릭하여 URL 속성을 수정하면서 URL 개체를 생성할 수도 있습니다.

절차

단계 **1** 목차에서 **Objects(**개체**)**와 **URL**을 차례로 선택합니다.

단계 **2** 다음 중 하나를 수행합니다.

- 개체를 생성하려면 + 버튼을 클릭합니다.
- 그룹을 생성하려면 그룹 추가( ) 버튼을 클릭합니다.
- 개체 또는 그룹을 수정하려면 개체의 수정 아이콘( )을 클릭합니다.

참조되지 않는 개체를 삭제하려면 해당 개체의 휴지통 아이콘( )을 클릭합니다.

단계 **3** 개체의 이름과 설명(선택 사항)을 입력합니다.

단계 **4** 개체 콘텐츠를 정의합니다.

URL 개체

URL 상자에 URL 또는 IP 주소를 입력합니다. URL에는 와일드카드를 사용할 수 없습니다.

URL 그룹

+ 버튼을 클릭하여 그룹에 추가할 URL 개체를 선택합니다. 새 개체를 생성할 수도 있습니다.

단계 **5** **OK(**확인**)**를 클릭하여 변경 사항을 저장합니다.

지리위치 개체 구성

지리위치 개체는 트래픽의 소스나 대상인 디바이스를 호스팅하는 국가와 대륙을 정의합니다. IP 주소를 사용하는 대신 정책에서 이러한 개체를 사용하여 트래픽을 제어할 수 있습니다. 지리적 위치를 사용하면 특정 국가에서 사용될 수 있는 모든 IP 주소를 몰라도 해당 국가에 대한 액세스를 쉽게 제한할 수 있습니다.

일반적으로는 지리위치 개체를 사용하지 않고 정책에서 직접 지리적 위치를 선택합니다. 그러나 국가와 대륙의 동일 그룹에 대해 여러 정책을 생성하려는 경우에는 개체를 사용하는 것이 편리합니다.

참고 최신 지리적 위치 데이터를 사용하여 트래픽을 필터링하려면 GeoDB(지리위치 데이터베이스)를 정기적으로 업데이트하는 것이 좋습니다.

다음 절차에서는 개체 페이지를 통해 개체를 직접 생성하고 수정할 수 있는 방법을 설명합니다. 개체 목록에 표시되는 **Create New Geolocation(**새 지리위치 생성**)** 링크를 클릭하여 네트워크 속성을 수정하면서 지리위치 개체를 생성할 수도 있습니다.

절차

단계 **1** 목차에서 **Objects(**개체**)**와 **Geolocation(**지리위치**)**을 차례로 선택합니다.

단계 **2** 다음 중 하나를 수행합니다.

- 개체를 생성하려면 + 버튼을 클릭합니다.
- 개체를 수정하려면 개체의 수정 아이콘( )을 클릭합니다.

참조되지 않는 개체를 삭제하려면 해당 개체의 휴지통 아이콘( )을 클릭합니다.

단계 **3** 개체의 이름과 설명(선택 사항)을 입력합니다.

단계 **4** 국가/대륙 목록에서 추가 +를 클릭하고 개체에 추가할 국가 및 대륙을 선택합니다. 대륙을 선택하면 대륙 내의 모든 국가가 선택됩니다.

단계 **5** **OK(**확인**)**를 클릭하여 변경 사항을 저장합니다.

syslog 서버 구성

syslog 서버 개체는 연결 지향형 또는 진단 시스템 로그(syslog) 메시지를 수신할 수 있는 서버를 식별합니다. 로그 수집 및 분석을 위한 syslog 서버를 설정하는 경우 개체를 생성하여 정의한 다음 액세스 규칙 또는 진단 로깅 시스템 설정에서 사용합니다. 시스템 로깅을 설정하는 방법에 대한 자세한 내용은 다음 주제를 참조하십시오.

- 로깅 설정, 159 페이지
- 진단 로깅 구성, 289 페이지

다음 절차에서는 개체 페이지를 통해 개체를 직접 생성하고 수정할 수 있는 방법을 설명합니다. 개체 목록에 표시되는 **Add Syslog Server(Syslog** 서버 추가**)** 링크를 클릭하여 syslog 서버 속성을 수정하면서 syslog 서버 개체를 생성할 수도 있습니다.

절차

단계 **1** 목차에서 **Objects(**개체**)**와 **Syslog Servers(Syslog** 서버**)**를 차례로 선택합니다.

단계 **2** 다음 중 하나를 수행합니다.

- 개체를 생성하려면 + 버튼을 클릭합니다.
- 개체를 수정하려면 개체의 수정 아이콘()을 클릭합니다.

참조되지 않는 개체를 삭제하려면 해당 개체의 휴지통 아이콘()을 클릭합니다.

단계 **3** syslog 서버 속성을 구성합니다.

- 디바이스 인터페이스 - syslog 서버에 연결하는 데 사용되는 인터페이스를 선택합니다. 브리지 그룹 구성원 인터페이스를 통해 서버에 액세스할 수 있는 경우에는 BVI(브리지 그룹 인터페이스)를 대신 선택합니다.
- **IP** 주소 - syslog 서버의 IP 주소를 입력합니다.
- 포트 - 서버가 syslog 메시지를 수신하는 데 사용하는 UDP 포트를 입력합니다. 기본값은 514입니다.

단계 **4** **OK(**확인**)**를 클릭하여 변경 사항을 저장합니다.

부

기본 사항

6 장

Interfaces

다음 주제에서는 Firepower Threat Defense 디바이스에서 인터페이스를 구성하는 방법을 설명합니다.

Firepower Threat Defense 인터페이스 정보

Firepower Threat Defense 디바이스에는 데이터 인터페이스와 관리/진단 인터페이스가 모두 포함되어 있습니다. 다음 항목에서는 Firepower Device Manager를 통해 인터페이스를 구성할 때의 제한사항과 기타 인터페이스 관리 개념에 관해 설명합니다.

인터페이스 컨피그레이션에 대한 제한

Firepower Device Manager를 사용하여 디바이스를 구성할 때는 인터페이스 컨피그레이션에 여러 가지 제한이 적용됩니다. 다음 기능 중 하나가 필요한 경우 Firepower Management Center는를 사용하여 디바이스를 구성해야 합니다.

- 라우팅 방화벽 모드만 지원됩니다. Transparent 방화벽 모드 인터페이스는 구성할 수 없습니다.
- IPS 전용 모드는 지원되지 않습니다. IPS 전용 처리를 위해 인터페이스를 인라인, 인라인 탭, 수동 또는 ERSPAN으로 구성할 수는 없습니다. IPS 전용 모드 인터페이스는 여러 방화벽 검사를 건너뛰며 IPS 보안 정책만 지원합니다. 그에 비해 방화벽 모드 인터페이스는 흐름 유지, IP 및 TCP 레이어 둘 다에서 흐름 상태 추적, IP 조각 모음 및 TCP 표준화와 같은 방화벽 기능에 트래픽을 적용합니다. 보안 정책에 따라 이 방화벽 모드 트래픽에 대해 IPS 기능을 선택 사항으로 구성할 수도 있습니다.
- EtherChannel 또는 이중 인터페이스는 구성할 수 없습니다.

- IPv4에 대해서는 PPPoE를 구성할 수 없습니다. 인터넷 인터페이스가 DSL/케이블 모뎀에 연결되어 있거나 기타 ISP 연결을 사용하며 ISP가 PPPoE를 사용하여 IP 주소를 제공하는 경우에는 Firepower Management Center는를 사용하여 이러한 설정을 구성해야 합니다.
- ASA 5512-X, 5515-X, 5525-X, 5545-X 및 5555-X의 경우, 선택 사항인 NIC(Network Interface Card)를 설치할 수 있습니다. 카드는 부트스트랩 중(즉, 설치하는 동안, 로컬/원격 관리 간 전환 시, 주/부 릴리스 업그레이드 동안, 그러나 패치 또는 핫픽스 업그레이드는 제외)에만 검색됩니다. SFP 인터페이스를 포함하는 카드의 경우, Firepower Device Manager는 속도 및 듀플렉스를 자동으로 설정합니다. 단, SFP 인터페이스는 속도 및 듀플렉스를 자동으로 설정하는 것을 지원하지 않습니다. 이러한 인터페이스에는 알맞은 속도(예: 1000)를 선택하거나 속도 및 듀플렉스를 **Default(**기본값**)**로 선택합니다. Default(기본값) 설정에서는 Firepower Device Manager의 옵션을 구성하지 않으므로, 기본 설정 그대로 유지합니다(모든 기존 컨피그레이션을 지우지 않음). 인터페이스에서 지원되는 최대 속도를 확인하려면 EPM 설명서를 참조하십시오. 인터페이스에서 승인되는 경우 속도 설정을 **No Negotiate(**협상 안 함**)**로 선택할 수 있으나, 이 옵션은 확실히 지원되는 경우에만 선택합니다.

참고 실수로 이를 선택하여 **No Negotiate(**협상 안 함**)**의 구성을 취소해야 하는 경우, 해당 옵션을 **Auto(**자동**)**로 설정하고 구축합니다. 이렇게 하면 구축에 실패합니다. 그러면 옵션을 **Default(**기본값**)**로 설정하고 다시 구축할 수 있으며 이번에는 구축에 성공합니다.

데이터 인터페이스

다음 유형의 인터페이스를 구성할 수 있습니다.

라우팅 모드

각 레이어 3 라우팅 인터페이스(또는 하위 인터페이스)에는 고유한 서브넷의 IP 주소가 필요합니다. 이러한 인터페이스는 보통 스위치, 다른 라우터의 포트 또는 ISP/WAN 게이트웨이에 연결합니다.

고정 주소를 할당할 수도 있고, DHCP 서버에서 주소를 가져올 수도 있습니다. 그러나 DHCP 서버가 디바이스에서 고정으로 정의된 인터페이스와 같은 서브넷의 주소를 제공하는 경우 시스템은 DHCP 인터페이스를 비활성화합니다. DHCP를 사용하여 주소를 가져오는 인터페이스가 트래픽 전달을 중지하는 경우에는 주소가 디바이스의 다른 인터페이스에 대한 서브넷과 중복되는지 확인하십시오.

브리지

브리지 그룹은 Firepower Threat Defense 디바이스가 경로 대신 브리지하는 인터페이스의 그룹입니다. 브리지 인터페이스는 브리지 그룹에 속하며 모든 인터페이스는 동일한 네트워크에 있습니다. 브리지 그룹은 브리지 네트워크에 IP 주소가 있는 BVI(브리지 가상 인터페이스)로 표시됩니다.

BVI의 이름을 지정하면 라우팅 인터페이스와 BVI를 라우팅할 수 있습니다. 이 경우 BVI는 구성원 인터페이스와 라우팅 인터페이스 간의 게이트웨이 역할을 합니다. BVI의 이름을 지정하지 않으면 브리지 그룹 구성원 인터페이스의 트래픽은 브리지 그룹을 벗어날 수 없습니다. 일반적으로는 인터넷에 구성원 인터페이스를 라우팅할 수 있도록 인터페이스 이름을 지정합니다.

라우팅 모드에서 브리지 그룹을 사용하는 방식 중 하나는 외부 스위치 대신 Firepower Threat Defense 디바이스에서 추가 인터페이스를 사용하는 것입니다. 브리지 그룹 구성원 인터페이스에 엔드포인트를 직접 연결할 수 있습니다. 또한 스위치를 연결하여 BVI와 같은 네트워크에 엔드포인트를 더 추가할 수도 있습니다.

라우팅 인터페이스 또는 BVI에서 IPv6 주소와 IPv4 주소를 모두 구성할 수 있습니다. IPv4 및 IPv6 모두에 대한 기본 경로를 구성해야 합니다. 브리지 그룹 구성원 인터페이스에서는 주소를 구성하지 않습니다.

IPv6 주소 지정

IPv6를 위해 2가지 유형의 유니캐스트 주소를 구성할 수 있습니다.

- 전역—전역 주소는 공용 네트워크에서 사용할 수 있는 공용 주소입니다. 브리지 그룹의 경우 각 구성원 인터페이스가 아닌 BVI(브리지 가상 인터페이스)에 대해 글로벌 주소를 구성합니다. 다음 항목은 글로벌 주소로 지정할 수 없습니다.
  - 내부에서 예약된 IPv6 주소: fd00::/56(from=fd00:: to= fd00:0000:0000:00ff:ffff:ffff:ffff:ffff)
  - ::/128 등의 지정되지 않은 주소
  - 루프백 주소(::1/128)
  - 멀티캐스트 주소(ff00::/8)
  - 링크-로컬 주소(fe80::/10)
- 링크-로컬—링크-로컬 주소는 직접 연결된 네트워크에서만 사용할 수 있는 사설 주소입니다. 라우터에서 링크-로컬 주소를 사용하여 패킷을 전달하지 않습니다. 이는 특정 물리적 네트워크 세그먼트에서의 통신에만 사용됩니다. 이러한 주소는 주소 확인 및 네이버 검색과 같은 네트워크 검색 기능이나 주소 컨피그레이션에만 사용할 수 있습니다. 브리지 그룹에서 BVI에 대해 IPv6를 활성화하면 각 브리지 그룹 구성원 인터페이스에 대해 링크-로컬 주소가 자동으로 구성됩니다. 각 인터페이스에는 자체 주소가 있어야 합니다. 링크-로컬 주소는 세그먼트에서만 사용 가능하며 인터페이스 MAC 주소와 연결되기 때문입니다.

적어도 IPv6가 작동하려면 링크-로컬 주소를 구성해야 합니다. 전역 주소를 설정하면 링크-로컬 주소가 인터페이스에서 자동으로 구성되므로 링크-로컬 주소를 특별히 구성하지 않아도 됩니다. 전역 주소를 구성하지 않은 경우 자동으로 또는 수동으로 링크-로컬 주소를 구성해야 합니다.

관리/진단 인터페이스

레이블이 관리인 물리적 포트에는 실제로 두 개별 인터페이스가 연결됩니다.

- 관리 가상 인터페이스 - 시스템 통신에 사용되는 IP 주소입니다. 이 주소는 시스템이 데이터베이스 업데이트를 검색할 때와 스마트 라이선싱에 사용하는 주소입니다. 이 주소에 대해 관리 세션(Firepower Device Manager 및 CLI)을 열 수 있습니다. **System Settings(**시스템 설정**)** > **Management Interface(**관리 인터페이스**)**에서 정의되는 관리 주소를 구성해야 합니다.
- 진단 실제 인터페이스 - 물리적 관리 포트의 실제 이름은 진단입니다. 이 인터페이스를 사용하여 외부 syslog 서버로 syslog 메시지를 전송할 수 있습니다. 진단 실제 인터페이스에 대한 IP 주소는 필요한 경우에만 구성하면 됩니다. 즉, syslog에 사용하려는 경우에만 인터페이스를 구성합니다. 이 인터페이스는 **Device(**디바이스**)** > **Interfaces(**인터페이스**)** 페이지에 표시되며 해당 페이지에서 구성할 수 있습니다. 진단 실제 인터페이스는 관리 트래픽만 허용하며 통과 트래픽은 허용하지 않습니다.

관리/진단을 구성할 때는 물리적 포트를 네트워크에 유선 연결하지 않는 것이 좋습니다. 대신 관리 IP 주소만 구성하고 인터넷에서 업데이트를 가져오는 게이트웨이로 데이터 인터페이스를 사용하도록 해당 주소를 구성합니다. 그런 다음 HTTPS/SSH 트래픽으로 연결되는 내부 인터페이스를 열고(기본값으로 HTTPS는 활성화되어 있음) 내부 IP 주소를 사용하여 Firepower Device Manager를 엽니다(관리 액세스 목록 구성, 287 페이지 참조).

별도의 관리 네트워크 구성에 대한 권장 사항

별도의 관리 네트워크를 사용하려는 경우 스위치 또는 라우터에 물리적 관리/진단 인터페이스를 연결합니다.

그런 후에 다음 항목을 구성합니다.

- **Device(**디바이스**)** > **System Settings(**시스템 설정**)** > **Management Interface(**관리 인터페이스**)**를 선택하고 연결된 네트워크에서 IPv4 또는 IPv6 주소, 또는 두 가지를 모두 구성합니다. 원하는 경우 네트워크의 다른 엔드포인트에 IPv4 주소를 제공하도록 DHCP 서버를 구성할 수 있습니다. 관리 네트워크에 인터넷으로의 경로가 포함된 라우터가 있으면 해당 라우터를 게이트웨이로 사용합니다. 그렇지 않은 경우에는 데이터 인터페이스를 게이트웨이로 사용합니다.
- 인터페이스를 통해 syslog 메시지를 syslog 서버로 보내려는 경우에만 **Device(**디바이스**)** > **Interface(**인터페이스**)**에서 진단 인터페이스의 주소를 구성합니다. 그렇지 않은 경우에는 진단용 주소가 필요하지 않으므로 구성하지 마십시오. 구성하는 모든 IP 주소는 관리 IP 주소와 같은 서브넷에 있어야 하며 DHCP 서버 풀에 있을 수는 없습니다. 예를 들어, 기본 컨피그레이션에서는 관리 주소로 192.168.45.45를 사용하고 DHCP 풀로 192.168.45.46-192.168.45.254를 사용하므로 192.168.45.1-192.168.45.44 범위에 포함되는 임의의 주소를 사용하여 진단을 구성할 수 있습니다.

별도 관리 네트워크용 관리/진단 인터페이스 컨피그레이션의 제한

물리적 관리 인터페이스를 유선으로 연결하거나할 때는 다음 제한을 따르십시오.

- 관리 네트워크에서 DHCP 서버를 사용하려는 경우 관리 인터페이스(**Device(**디바이스**)** > **System Settings(**시스템 설정**)** > **Management Interface(**관리 인터페이스**)**)에서 DHCP 서버를 구성합니다. 진단(물리적) 인터페이스에서는 DHCP 서버를 구성할 수 없습니다.
- 관리 네트워크에 다른 DHCP 서버가 있는 경우에는 해당 서버 또는 관리에서 실행되는 DHCP 서버를 비활성화합니다. 규칙에 따라 지정된 서브넷에는 DHCP 서버가 둘 이상 있을 수 없습니다.
- 관리 및 진단용 주소를 둘 다 구성하는 경우 해당 주소가 같은 서브넷에 있어야 합니다.
- 진단용 IP 주소를 구성하더라도 데이터 인터페이스를 관리 게이트웨이로 사용할 수 있습니다. 그러나 진단에서는 데이터 인터페이스를 게이트웨이로 사용하지 않습니다. 진단에서 다른 네트워크로 이동하는 경로가 필요한 경우 관리 네트워크의 다른 라우터가 진단 IP 주소에서 생성되는 트래픽을 라우팅해야 합니다. 필요한 경우 **Device(**디바이스**)** > **Routing(**라우팅**)**을 선택하여 진단 인터페이스용으로 고정 경로를 구성합니다.

보안 영역

각 인터페이스는 단일 보안 영역에 할당할 수 있습니다. 그런 후에 영역을 기준으로 하여 보안 정책을 적용합니다. 예를 들어 내부 인터페이스는 내부 영역에, 외부 인터페이스는 외부 영역에 할당할 수 있습니다. 예를 들어, 트래픽이 내부에서 외부로는 이동하되 외부에서 내부로는 이동할 수 없도록 액세스 제어 정책을 구성할 수 있습니다.

브리지 그룹의 경우 영역에 구성원 인터페이스를 추가할 수는 있지만 BVI(브리지 가상 인터페이스)는 추가할 수 없습니다.

영역에는 진단/관리 인터페이스를 포함하지 않습니다. 영역은 데이터 인터페이스에만 적용됩니다.

개체 페이지에서 보안 영역을 생성할 수 있습니다.

Auto-MDI/MDIX 기능

RJ-45 인터페이스의 경우 기본 자동 협상 설정에는 Auto-MDI/MDIX 기능도 포함됩니다. Auto-MDI/MDIX는 자동 협상 단계에서 직선 케이블이 감지된 경우 내부 크로스오버를 수행하므로 크로스오버 케이블이 필요 없습니다. 인터페이스에서 Auto-MDI/MDIX를 사용하려면 속도 또는 양방향을 자동 협상하도록 설정해야 합니다. 속도와 양방향 둘 다 명시적으로 고정 값으로 설정한 경우 두 설정 모두에 대해 자동 협상을 비활성화하면 Auto-MDI/MDIX도 비활성화됩니다. 기가비트 인터넷의 경우 속도와 양방향을 1000 및 최대로 설정하면 인터페이스에서 항상 자동 협상이 실행되므로 Auto-MDI/MDIX 기능도 항상 활성화된 상태이고 이를 비활성화할 수 없습니다.

MTU 정보

MTU는 Firepower Threat Defense 디바이스가 지정된 이더넷 인터페이스에서 전송할 수 있는 최대 프레임 페이로드 크기를 지정합니다. MTU 값은 이더넷 헤더, VLAN 태깅 또는 기타 오버헤드가 없는 프레임 크기입니다. 예를 들어, MTU를 1500으로 설정할 경우 예상 프레임 크기는 헤더 포함 시 1518바이트이고 VLAN 사용 시에는 1522입니다. 이러한 헤더를 수용하기 위해 MTU 값을 이보다 더 높게 설정하지 마십시오.

경로 MTU 검색

Firepower Threat Defense 디바이스에서는 RFC 1191에 정의된 경로 MTU 검색을 지원합니다. 이 기능을 사용하면 두 호스트 간의 네트워크 경로에 있는 모든 디바이스에서 MTU를 조율할 수 있으므로, 경로의 최저 MTU에 대한 표준을 설정할 수 있습니다.

MTU 및 단편화

IPv4의 경우 지정된 MTU보다 큰 발신 IP 패킷은 2개 이상의 프레임으로 단편화됩니다. 분할된 패킷은 목적지(또는 일부 경우 중간 홉에서)에서 다시 합쳐지며, 분할이 일어날 경우 성능이 저하될 수 있습니다. IPv6의 경우에는 일반적으로 패킷의 단편화가 전혀 허용되지 않습니다. 따라서 분할을 방지하려면 IP 패킷이 MTU 크기 내에 맞아야 합니다.

UDP 또는 ICMP의 경우 애플리케이션은 단편화 방지를 위해 MTU를 고려해야 합니다.

참고 Firepower Threat Defense 디바이스에서는 메모리에 공간이 있는 한 구성된 MTU보다 큰 프레임을 수신할 수 있습니다.

MTU와 점보 프레임

큰 MTU를 사용하는 경우 더 큰 패킷을 전송할 수 있습니다. 큰 패킷은 네트워크에서 더욱 효율적으로 사용할 수 있습니다. 다음 지침을 참조하십시오.

- 트래픽 경로의 MTU 일치 - 트래픽 경로에서는 모든 Firepower Threat Defense 디바이스 인터페이스 및 기타 디바이스 인터페이스의 MTU를 동일하게 설정하는 것이 좋습니다. MTU를 일치시키면 패킷 분할 시 디바이스가 중간에 끼어드는 현상을 방지할 수 있습니다.
- 점보 프레임 수용 - 점보 프레임은 최대 표준 1522바이트(레이어 2 헤더 및 FCS 포함)보다 큰 이더넷 패킷이며, 최대 9216바이트에 이릅니다. 점보 프레임을 수용하기 위해 MTU를 최대 9198바이트로 설정할 수 있습니다.

  참고 MTU를 늘리면 점보 프레임에 더 많은 메모리가 할당되므로 액세스 규칙 등 다른 기능의 최대 사용량이 제한될 수 있습니다. ASA 5500-X 시리즈 디바이스 에서 MTU를 기본값인 1500보다 크게 늘리는 경우에는 시스템을 재부팅해야 합니다.

인터페이스 구성

인터페이스 연결에 케이블을 연결하려면 인터페이스를 구성해야 합니다. 최소한 인터페이스 이름을 지정하고 트래픽을 전달하도록 인터페이스를 사용해야 합니다. 인터페이스가 브리지 그룹의 구성원인 경우에는 이 작업만 수행하면 됩니다. 비브리지 그룹 구성원의 경우에는 인터페이스에 IP 주소도 지정해야 합니다. 지정된 포트의 단일 실제 인터페이스가 아닌 VLAN 하위 인터페이스를 생성하려는 경우에는 일반적으로 실제 인터페이스가 아닌 하위 인터페이스에 IP 주소를 구성합니다. VLAN 하위 인터페이스를 사용하면 실제 인터페이스를 각기 다른 VLAN ID로 태그가 지정된 여러 논리적 인터페이스로 분할할 수 있습니다.

인터페이스 목록에는 사용 가능한 인터페이스, 해당 이름, 주소 및 상태가 표시됩니다. 인터페이스 목록에서 바로 인터페이스의 상태를 켜기 또는 끄기로 변경할 수 있습니다. 목록에는 컨피그레이션을 기준으로 인터페이스 특성이 표시됩니다. 브리지 그룹 인터페이스의 열기/닫기 화살표를 사용하면 구성원 인터페이스를 확인할 수 있습니다. 이러한 인터페이스는 목록에서 단독으로도 표시됩니다.

포트 그래픽을 사용하여 인터페이스의 현재 상태를 모니터링합니다. 포트 위에 마우스를 놓으면 해당 IP 주소와 사용 상태 및 링크 상태가 표시됩니다. IP 주소는 정적으로 할당할 수도 있고 DHCP를 사용하여 가져올 수도 있습니다.

인터페이스 포트는 다음 색 코드를 사용합니다.

- 녹색 - 인터페이스가 구성되어 있고 활성화된 상태이며 링크가 작동합니다.
- 회색 - 인터페이스를 사용하지 않습니다.
- 주황색/빨간색 - 인터페이스가 구성되어 있고 활성화된 상태이지만 링크가 작동하지 않습니다. 유선 인터페이스의 경우 이 색은 수정해야 하는 오류 상태를 나타냅니다. 유선 인터페이스가 아닌 경우에는 이 색이 표시되는 것이 정상입니다.

다음 항목에서는 인터페이스를 구성하는 방법을 설명합니다.

실제 인터페이스 구성

실제 인터페이스를 사용하려면 최소한 인터페이스를 활성화해야 합니다. 일반적으로는 실제 인터페이스의 이름을 지정하고 IP 주소를 구성합니다. VLAN 하위 인터페이스를 생성하려는 경우 또는 인터페이스를 브리지 그룹에 추가하려는 경우에는 IP 주소를 구성하지 않습니다.

참고 브리지 그룹 구성원 인터페이스에서는 IP 주소를 구성할 수 없습니다. 그러나 필요에 따라 고급 설정을 수정할 수는 있습니다.

인터페이스를 비활성화하여 연결된 네트워크에서 전송을 일시적으로 차단할 수 있습니다. 인터페이스 컨피그레이션을 제거할 필요는 없습니다.

절차

단계 **1** 디바이스을 클릭한 다음 **Interfaces(**인터페이스**)** 요약에서 링크를 클릭합니다.
인터페이스 목록에는 사용 가능한 인터페이스, 해당 이름, 주소 및 상태가 표시됩니다.

단계 **2** 수정할 실제 인터페이스의 수정 아이콘( )을 클릭합니다.

단계 **3** 인터페이스를 활성화하려면 **Status(**상태**)** > **On(**켜기**)**을 클릭합니다.
이 실제 인터페이스에 대해 하위 인터페이스를 구성하려는 경우에는 이러한 작업만 수행하면 될 가능성이 높습니다. **Save(**저장**)**를 클릭하고 VLAN 하위 인터페이스 및 802.1Q 트렁킹 구성, 112 페이지를 계속 진행합니다. 그렇지 않으면 아래 작업을 계속합니다.

참고 하위 인터페이스를 구성할 때도 인터페이스 이름을 지정하고 IP 주소를 제공할 수 있습니다. 이러한 방식은 일반적인 설정은 아니지만, 필요한 경우에는 해당 설정을 구성할 수 있습니다.

단계 **4** 다음을 구성합니다.

- 인터페이스 이름 - 인터페이스의 이름(최대 48자)입니다. 영문자는 소문자로 입력해야 합니다. 예를 들면 **inside** 또는 **outside**와 같이 입력합니다. 이름을 입력하지 않으면 나머지 인터페이스 컨피그레이션이 무시됩니다. 하위 인터페이스를 구성하는 경우가 아니면 인터페이스에는 이름이 있어야 합니다.

  참고 이름을 변경하는 경우 보안 영역, syslog 서버 개체, DHCP 서버 정의 등 이전 이름을 사용했던 모든 위치에서 변경 사항이 자동으로 반영됩니다. 그러나 해당 이름을 사용하는 모든 컨피그레이션을 먼저 제거해야 이름을 제거할 수 있습니다. 일반적으로는 정책이나 설정에 대해 이름이 없는 인터페이스를 사용할 수 없기 때문입니다.

- (선택 사항). 설명 - 설명은 줄바꿈 없이 1줄, 최대 200자로 작성합니다.

단계 **5** **IPv4** 주소 탭을 클릭하고 IPv4 주소를 구성합니다.
유형 필드에서 다음 옵션 중 하나를 선택합니다.

- 동적(DHCP) - 네트워크의 DHCP 서버에서 주소를 가져와야 하는 경우 이 옵션을 선택합니다. 필요에 따라 다음 옵션을 변경합니다.
  - 경로 메트릭 - DHCP 서버에서 기본 경로를 가져오는 경우 확인된 경로까지의 관리 거리(1~255)입니다. 기본값은 1입니다.
  - 기본 경로 얻기 - DHCP 서버에서 기본 경로를 가져올지 여부를 선택합니다. 일반적으로는 이 옵션을 선택합니다(기본값).

- 고정 - 변경되면 안 되는 주소를 할당하려면 이 옵션을 선택합니다. 인터페이스에 연결된 네트워크에 대해 인터페이스의 IP 주소와 서브넷 마스크를 입력합니다. 예를 들어 10.100.10.0/24 네트워크를 연결하는 경우 10.100.10.1/24를 입력할 수 있습니다. 주소가 네트워크에서 이미 사용되고 있지 않은지 확인합니다.

  참고 기존 인터페이스의 경우에는 인터페이스에 대해 DHCP 서버가 구성되어 있으면 주소를 변경하는 기능이 제한됩니다. 새 IP 주소는 DHCP 주소 풀과 동일한 서브넷에 있되 해당 풀에 속해서는 안 됩니다. 다른 서브넷에서 주소를 구성해야 하는 경우에는 먼저 DHCP 서버 컨피그레이션을 삭제합니다. DHCP 서버 구성, 290 페이지를 참조하십시오.

단계 **6** (선택 사항). **IPv6 Address(IPv6** 주소**)** 탭을 클릭하고 IPv6 주소를 구성합니다.

- 상태 - 글로벌 어드레스를 구성하지 않는 경우 IPv6 처리를 활성화하고 링크-로컬 주소를 자동으로 구성하려면 사용을 선택합니다. 링크 로컬 주소는 인터페이스 MAC 주소(수정된 EUI-64 형식)를 기반으로 생성됩니다.

  참고 IPv6를 비활성화해도 명시적 IPv6 주소로 구성되었거나 자동 컨피그레이션용으로 활성화된 인터페이스에서 IPv6 처리가 비활성화되지는 않습니다.

- 주소 자동 컨피그레이션 - 주소를 자동으로 구성하려면 이 옵션을 선택합니다. IPv6 스테이트리스 자동 컨피그레이션에서는 디바이스가 있는 링크에 IPv6 서비스를 제공하도록 구성된 라우터가 있는 경우에만 글로벌 IPv6 주소를 생성합니다. 이러한 서비스에는 링크에서 사용할 IPv6 글로벌 접두사 알림이 포함됩니다. 링크에서 IPv6 라우팅 서비스를 사용할 수 없는 경우에는 링크-로컬 IPv6 주소만 제공됩니다. 디바이스의 직접 네트워크 링크 외부에서는 이 주소에 액세스할 수 없습니다. 링크 로컬 주소는 수정된 EUI-64 인터페이스 ID를 기반으로 합니다.

  RFC 4862에서는 스테이트리스 자동 컨피그레이션이 구성된 호스트에서 라우터 알림 메시지를 보내지 않도록 지정하지만, 이 경우에는 Firepower Threat Defense 디바이스에서 라우터 알림 메시지를 전송합니다. 메시지를 표시하지 않고 RFC를 준수하려면 **RA** 표시 안 함을 선택합니다.

- 고정 주소/접두사 - 스테이트리스 자동 컨피그레이션을 사용하지 않는 경우 전체 고정 글로벌 IPv6 주소와 네트워크 접두사를 입력합니다. 예를 들어, 2001:0DB8::BA98:0:3210/48와 같이 입력합니다. IPv6 주소 지정에 대한 자세한 내용은 IPv6 주소 지정, 105 페이지를 참조하십시오.

  주소를 링크 로컬 전용으로 사용하려는 경우 링크-로컬 옵션을 선택합니다. 로컬 네트워크 외부에서는 링크 로컬 주소에 액세스할 수 없습니다. 브리지 그룹 인터페이스에서는 링크-로컬 주소를 구성할 수 없습니다.

  참고 링크-로컬 주소는 FE8, FE9, FEA 또는 FEB로 시작해야 합니다(예: fe80::20d:88ff:feee:6a82). Modified EUI-64 형식으로 링크-로컬 주소를 자동으로 지정하는 것이 좋습니다. 만약 다른 디바이스에서 Modified EUI-64 형식을 강제 적용하는 경우 수동으로 지정된 링크-로컬 주소 때문에 패킷이 폐기될 수 있습니다.

- **RA** 표시 안 함 - 라우터 알림을 표시하지 않을지를 선택합니다. Firepower Threat Defense 디바이스는 네이버 디바이스가 기본 라우터 주소를 동적으로 학습하도록 라우터 알림에 참여할 수 있습니다. 기본적으로 라우터 알림 메시지(ICMPv6 유형 134)는 IPv6가 구성된 각 인터페이스에 주기적으로 전송됩니다.

  라우터 광고는 라우터 요청 메시지에 대한 응답으로도 보내집니다(ICMPv6 Type 133). 예정된 다음 라우터 광고 메시지를 기다릴 필요 없이 호스트가 즉시 자동 구성을 할 수 있도록 시스템 시동 시 라우터 요청 메시지가 전송됩니다.

  Firepower Threat Defense 디바이스가 IPv6 접두사를 제공하지 않도록 하려는 인터페이스(예: 외부 인터페이스)에서는 이러한 메시지를 표시하지 않을 수 있습니다.

단계 **7** (선택 사항). 고급 인터페이스 옵션 구성, 118 페이지.
고급 설정에는 대부분의 네트워크에 적합한 기본값이 있습니다. 네트워크 문제를 해결하는 경우에만 이러한 기본값을 수정하십시오.

단계 **8** **OK(**확인**)**를 클릭합니다.

VLAN 하위 인터페이스 및 802.1Q 트렁킹 구성

VLAN 하위 인터페이스를 사용하면 실제 인터페이스를 각기 다른 VLAN ID로 태그가 지정된 여러 논리적 인터페이스로 분할할 수 있습니다. 하나 이상의 VLAN 하위 인터페이스가 포함된 인터페이스는 자동으로 802.1Q 트렁크로 구성됩니다. VLAN을 사용하면 정해진 실제 인터페이스에서 트래픽을 따로 유지할 수 있으므로, 실제 인터페이스 또는 디바이스를 더 추가하지 않고 네트워크에 사용 가능한 인터페이스 수를 늘릴 수 있습니다.

참고 브리지 그룹 구성원 인터페이스에서는 IP 주소를 구성할 수 없습니다. 그러나 필요에 따라 고급 설정을 수정할 수는 있습니다.

시작하기 전에

물리적 인터페이스의 태그 지정되지 않은 패킷 방지 — 하위 인터페이스를 사용할 경우, 일반적으로 물리적 인터페이스에서 트래픽을 전달하지 않도록 하고자 합니다. 물리적 인터페이스에서는 태그 지정되지 않은 패킷을 전달하기 때문입니다. 하위 인터페이스에서 트래픽을 전달하려면 실제 인터페이스를 활성화해야 하므로, 인터페이스의 이름을 지정하지 않는 방법을 통해 실제 인터페이스가 트래픽을 전달하지 않도록 해야 합니다. 실제 인터페이스에서 태그가 지정되지 않은 패킷을 전달할 수 있도록 하려면 일반적인 방식으로 인터페이스 이름을 지정하면 됩니다.

절차

단계 **1** 디바이스을 클릭한 다음 **Interfaces(**인터페이스**)** 요약에서 링크를 클릭합니다.
인터페이스 목록에는 사용 가능한 인터페이스, 해당 이름, 주소 및 상태가 표시됩니다. 하위 인터페이스는 실제 인터페이스 아래에 그룹화됩니다.

단계 **2** 다음 중 하나를 수행합니다.

- 기어 드롭다운 목록에서 **Add Subinterface(**하위 인터페이스 추가**)**를 선택하여 새 하위 인터페이스를 생성합니다.
- 수정할 하위 인터페이스의 수정 아이콘( )을 클릭합니다.

하위 인터페이스가 더 이상 필요하지 않은 경우 해당 하위 인터페이스의 삭제 아이콘( )을 클릭하여 하위 인터페이스를 삭제합니다.

단계 **3** 인터페이스를 활성화하려면 **Status(**상태**)** > **On(**켜기**)**를 클릭합니다.

단계 **4** 상위 인터페이스, 이름 및 설명을 구성합니다.

- 상위 인터페이스 - 하위 인터페이스를 추가할 실제 인터페이스를 선택합니다. 하위 인터페이스를 생성한 후에는 상위 인터페이스를 변경할 수 없습니다.

- 이름 - 하위 인터페이스의 이름(최대 48자)입니다. 영문자는 소문자로 입력해야 합니다. 예를 들면 **inside** 또는 **outside**와 같이 입력합니다. 이름을 입력하지 않으면 나머지 인터페이스 컨피그레이션이 무시됩니다.

  참고 이름을 변경하는 경우 보안 영역, syslog 서버 개체, DHCP 서버 정의 등 이전 이름을 사용했던 모든 위치에서 변경 사항이 자동으로 반영됩니다. 그러나 해당 이름을 사용하는 모든 컨피그레이션을 먼저 제거해야 이름을 제거할 수 있습니다. 일반적으로는 정책이나 설정에 대해 이름이 없는 인터페이스를 사용할 수 없기 때문입니다.

- (선택 사항). 설명 - 설명은 줄바꿈 없이 1줄, 최대 200자로 작성합니다.

단계 **5** 일반 하위 인터페이스 특성을 구성합니다.

- **VLAN ID** - 이 하위 인터페이스에서 패킷에 태그를 지정하는 데 사용할 1~4094 사이의 VLAN ID를 입력합니다.
- 하위 인터페이스 **ID** - 하위 인터페이스 ID를 1~4294967295 사이의 정수로 입력합니다. 허용되는 하위 인터페이스의 개수는 플랫폼에 따라 다릅니다. 하위 인터페이스를 생성한 후에는 ID를 변경할 수 없습니다.

단계 **6** **IPv4** 주소 탭을 클릭하고 IPv4 주소를 구성합니다.
유형 필드에서 다음 옵션 중 하나를 선택합니다.

- 동적(DHCP) - 네트워크의 DHCP 서버에서 주소를 가져와야 하는 경우 이 옵션을 선택합니다. 필요에 따라 다음 옵션을 변경합니다.
  - 경로 메트릭 - DHCP 서버에서 기본 경로를 가져오는 경우 확인된 경로까지의 관리 거리(1~255)입니다. 기본값은 1입니다.
  - 기본 경로 얻기 - DHCP 서버에서 기본 경로를 가져올지 여부를 선택합니다. 일반적으로는 이 옵션을 선택합니다(기본값).
- 고정 - 변경되면 안 되는 주소를 할당하려면 이 옵션을 선택합니다. 인터페이스에 연결된 네트워크에 대해 인터페이스의 IP 주소와 서브넷 마스크를 입력합니다. 예를 들어 10.100.10.0/24 네트워크를 연결하는 경우 10.100.10.1/24를 입력할 수 있습니다. 주소가 네트워크에서 이미 사용되고 있지 않은지 확인합니다.

  참고 기존 인터페이스의 경우에는 인터페이스에 대해 DHCP 서버가 구성되어 있으면 주소를 변경하는 기능이 제한됩니다. 새 IP 주소는 DHCP 주소 풀과 동일한 서브넷에 있되 해당 풀에 속해서는 안 됩니다. 다른 서브넷에서 주소를 구성해야 하는 경우에는 먼저 DHCP 서버 컨피그레이션을 삭제합니다. DHCP 서버 구성, 290 페이지를 참조하십시오.

단계 **7** (선택 사항). **IPv6 Address(IPv6** 주소**)** 탭을 클릭하고 IPv6 주소를 구성합니다.

- 상태 - 글로벌 어드레스를 구성하지 않는 경우 IPv6 처리를 활성화하고 링크-로컬 주소를 자동으로 구성하려면 사용을 선택합니다. 링크 로컬 주소는 인터페이스 MAC 주소(수정된 EUI-64 형식)를 기반으로 생성됩니다.

  참고 IPv6를 비활성화해도 명시적 IPv6 주소로 구성되었거나 자동 컨피그레이션용으로 활성화된 인터페이스에서 IPv6 처리가 비활성화되지는 않습니다.

- 주소 자동 컨피그레이션 - 주소를 자동으로 구성하려면 이 옵션을 선택합니다. IPv6 스테이트리스 자동 컨피그레이션에서는 디바이스가 있는 링크에 IPv6 서비스를 제공하도록 구성된 라우터가 있는 경우에만 글로벌 IPv6 주소를 생성합니다. 이러한 서비스에는 링크에서 사용할 IPv6 글로벌 접두사 알림이 포함됩니다. 링크에서 IPv6 라우팅 서비스를 사용할 수 없는 경우에는 링크-로컬 IPv6 주소만 제공됩니다. 디바이스의 직접 네트워크 링크 외부에서는 이 주소에 액세스할 수 없습니다. 링크 로컬 주소는 수정된 EUI-64 인터페이스 ID를 기반으로 합니다.

  RFC 4862에서는 스테이트리스 자동 컨피그레이션이 구성된 호스트에서 라우터 알림 메시지를 보내지 않도록 지정하지만, 이 경우에는 Firepower Threat Defense 디바이스에서 라우터 알림 메시지를 전송합니다. 메시지를 표시하지 않고 RFC를 준수하려면 **RA** 표시 안 함을 선택합니다.

- 고정 주소/접두사 - 스테이트리스 자동 컨피그레이션을 사용하지 않는 경우 전체 고정 글로벌 IPv6 주소와 네트워크 접두사를 입력합니다. 예를 들어, 2001:0DB8::BA98:0:3210/48와 같이 입력합니다. IPv6 주소 지정에 대한 자세한 내용은 IPv6 주소 지정, 105 페이지를 참조하십시오.

  주소를 링크 로컬 전용으로 사용하려는 경우 링크-로컬 옵션을 선택합니다. 로컬 네트워크 외부에서는 링크 로컬 주소에 액세스할 수 없습니다. 브리지 그룹 인터페이스에서는 링크-로컬 주소를 구성할 수 없습니다.

  참고 링크-로컬 주소는 FE8, FE9, FEA 또는 FEB로 시작해야 합니다(예: fe80::20d:88ff:feee:6a82). Modified EUI-64 형식으로 링크-로컬 주소를 자동으로 지정하는 것이 좋습니다. 만약 다른 디바이스에서 Modified EUI-64 형식을 강제 적용하는 경우 수동으로 지정된 링크-로컬 주소 때문에 패킷이 폐기될 수 있습니다.

- **RA** 표시 안 함 - 라우터 알림을 표시하지 않을지를 선택합니다. Firepower Threat Defense 디바이스는 네이버 디바이스가 기본 라우터 주소를 동적으로 학습하도록 라우터 알림에 참여할 수 있습니다. 기본적으로 라우터 알림 메시지(ICMPv6 유형 134)는 IPv6가 구성된 각 인터페이스에 주기적으로 전송됩니다.

  라우터 광고는 라우터 요청 메시지에 대한 응답으로도 보내집니다(ICMPv6 Type 133). 예정된 다음 라우터 광고 메시지를 기다릴 필요 없이 호스트가 즉시 자동 구성을 할 수 있도록 시스템 시동 시 라우터 요청 메시지가 전송됩니다.

  Firepower Threat Defense 디바이스가 IPv6 접두사를 제공하지 않도록 하려는 인터페이스(예: 외부 인터페이스)에서는 이러한 메시지를 표시하지 않을 수 있습니다.

단계 **8** (선택 사항). 고급 인터페이스 옵션 구성, 118 페이지.
고급 설정에는 대부분의 네트워크에 적합한 기본값이 있습니다. 네트워크 문제를 해결하는 경우에만 이러한 기본값을 수정하십시오.

단계 **9** **OK**(확인)를 클릭합니다.

브리지 그룹 구성

브리지 그룹은 하나 이상의 인터페이스를 그룹화하는 가상 인터페이스입니다. 인터페이스를 그룹화하는 주요 이유는 스위치 인터페이스 그룹을 생성하기 위해서입니다. 따라서 브리지 그룹에 포함된 인터페이스에 워크스테이션 또는 기타 엔드포인트 디바이스를 직접 연결할 수 있습니다. 이러한 워

크스테이션이나 디바이스는 별도의 물리적 스위치를 통해 연결할 필요는 없지만, 브리지 그룹 구성원에 스위치를 연결할 수도 있습니다.

그룹 구성원에는 IP 주소가 없습니다. 대신 모든 구성원 인터페이스는 BVI(브리지 가상 인터페이스)의 IP 주소를 공유합니다. BVI에서 IPv6를 사용하는 경우 구성원 인터페이스에는 고유한 링크-로컬 주소가 자동으로 할당됩니다.

일반적으로는 BVI(브리지 그룹 인터페이스)에서 DHCP 서버를 구성합니다. 이 서버는 구성원 인터페이스를 통해 연결된 모든 엔드포인트에 대해 IP 주소를 제공합니다. 그러나 원하는 경우에는 구성원 인터페이스에 연결된 엔드포인트에서 고정 주소를 구성할 수 있습니다. 브리지 그룹 내의 모든 엔드포인트에는 브리지 그룹 IP 주소와 같은 서브넷의 IP 주소가 있어야 합니다.

참고 모든 ASA 5506-X 모델의 경우 새 버전 6.2 이상 시스템이나 재이미징된 6.2 이상 시스템에서 디바이스는 브리지 그룹 BVI1(이름: 내부)이 미리 구성된 상태로 제공됩니다. 이 그룹에는 외부 인터페이스를 제외한 모든 데이터 인터페이스가 포함됩니다. 따라서 디바이스에는 인터넷 또는 기타 업스트림 네트워크에 연결하는 데 사용되는 포트 하나가 미리 구성되어 있습니다. 그리고 기타 모든 포트는 엔드포인트에 대한 직접 연결용으로 활성화되어 있으며 사용 가능합니다. 새 서브넷에 대해 내부 인터페이스를 사용하려는 경우에는 먼저 BVI1에서 필요한 인터페이스를 제거해야 합니다.

시작하기 전에

브리지 그룹의 구성원으로 추가할 인터페이스를 구성합니다. 구체적으로 각 구성원 인터페이스는 다음 요건을 충족해야 합니다.

- 인터페이스에 이름이 있어야 합니다.
- 인터페이스에 대해 IPv4 또는 IPv6 주소(고정 주소 또는 DHCP를 통해 제공된 주소)가 정의되어 있으면 안 됩니다. 현재 사용 중인 인터페이스에서 주소를 제거해야 하는 경우에는 주소가 있는 인터페이스를 사용하는 인터페이스의 다른 컨피그레이션(예: 정적 경로, DHCP 서버 또는 NAT 규칙)도 제거해야 할 수 있습니다.
- 인터페이스가 보안 영역에 있는 경우 보안 영역에서 인터페이스를 제거하고 인터페이스에 대한 NAT 규칙을 삭제해야 브리지 그룹에 인터페이스를 추가할 수 있습니다.

또한 구성원 인터페이스는 개별적으로 활성화 및 비활성화됩니다. 그러므로 사용하지 않는 인터페이스는 브리지 그룹에서 제거할 필요 없이 비활성화할 수 있습니다. 브리지 그룹 자체는 항상 활성화됩니다.

절차

단계 **1** **Device(**디바이스**)**를 클릭한 다음 **Interfaces(**인터페이스**)** 요약의 링크를 클릭합니다.
인터페이스 목록에는 사용 가능한 인터페이스, 해당 이름, 주소 및 상태가 표시됩니다. 이미 있는 브리지 그룹은 폴더 형태입니다. 구성원 인터페이스를 보려면 열기/닫기 화살표를 클릭합니다. 구성원 인터페이스는 목록에 개별적으로도 표시됩니다.

단계 **2** 다음 중 하나를 수행합니다.

- BVI1 브리지 그룹의 수정 아이콘()을 클릭합니다.
- 기어 드롭다운 목록에서 브리지 그룹 인터페이스 추가를 선택하여 새 그룹을 생성합니다.

  참고 단일 브리지 그룹을 생성할 수 있습니다. 브리지 그룹을 이미 정의한 경우에는 새 그룹을 생성하는 대신 해당 그룹을 수정해야 합니다. 새 브리지 그룹을 생성해야 하는 경우 먼저 기존 브리지 그룹을 삭제해야 합니다.

- 더 이상 필요하지 않은 브리지 그룹의 삭제 아이콘()을 클릭합니다. 브리지 그룹을 삭제하면 해당 구성원은 표준 라우팅 인터페이스가 되며 모든 NAT 규칙 또는 보안 영역 멤버십은 유지됩니다. 인터페이스를 수정하여 IP 주소를 지정할 수 있습니다. 새 브리지 그룹에 인터페이스를 추가하려는 경우에는 먼저 NAT 규칙을 제거하고 인터페이스를 해당 보안 영역에서 제거해야 합니다.

단계 **3** 다음을 구성합니다.

- 인터페이스 이름 - 브리지 그룹의 이름(최대 48자)입니다. 영문자는 소문자로 입력해야 합니다. 예를 들면 **inside** 또는 **outside**와 같이 입력합니다. 이름을 입력하지 않으면 나머지 인터페이스 컨피그레이션이 무시됩니다.

  참고 이름을 변경하는 경우 보안 영역, syslog 서버 개체, DHCP 서버 정의 등 이전 이름을 사용했던 모든 위치에서 변경 사항이 자동으로 반영됩니다. 그러나 해당 이름을 사용하는 모든 컨피그레이션을 먼저 제거해야 이름을 제거할 수 있습니다. 일반적으로는 정책이나 설정에 대해 이름이 없는 인터페이스를 사용할 수 없기 때문입니다.

- (선택 사항). 설명 - 설명은 줄바꿈 없이 1줄, 최대 200자로 작성합니다.

단계 **4** 브리지 그룹 구성원 목록을 수정합니다.
단일 브리지 그룹에는 인터페이스 또는 하위 인터페이스를 64개까지 추가할 수 있습니다.

- +를 클릭하여 인터페이스를 추가합니다.
- 제거할 인터페이스 위에 마우스를 올려놓고 오른쪽의 **x**를 클릭합니다.

단계 **5** **IPv4 Address(IPv4** 주소**)** 탭을 클릭하고 IPv4 주소를 구성합니다.
Type(유형**)** 필드에서 다음 옵션 중 하나를 선택합니다.

- 고정 - 변경되면 안 되는 주소를 할당하려면 이 옵션을 선택합니다. 브리지 그룹의 IP 주소와 서브넷 마스크를 입력합니다. 연결되는 모든 엔드포인트는 이 네트워크에 포함됩니다. ASA 5506-X 모델의 경우 BVI1 "내부" 네트워크의 기본값은 192.168.1.1/24(255.255.255.0)입니다. 주소가 네트워크에서 이미 사용되고 있지 않은지 확인합니다.

  참고 기존 브리지 그룹의 경우에는 그룹에 대해 DHCP 서버가 구성되어 있으면 주소를 변경하는 기능이 제한됩니다. 새 IP 주소는 DHCP 주소 풀과 동일한 서브넷에 있되 해당 풀에 속해서는 안 됩니다. 다른 서브넷에서 주소를 구성해야 하는 경우에는 먼저 DHCP 서버 컨피그레이션을 삭제합니다. DHCP 서버 구성, 290 페이지를 참조하십시오.

- 동적(DHCP) - 네트워크의 DHCP 서버에서 주소를 가져와야 하는 경우 이 옵션을 선택합니다. 이 옵션은 브리지 그룹에 대해 일반적으로 구성하는 항목은 아니지만 필요한 경우 구성할 수 있습니다. 필요에 따라 다음 옵션을 변경합니다.

◦ 경로 메트릭 - DHCP 서버에서 기본 경로를 가져오는 경우 확인된 경로까지의 관리 거리(1~255)입니다. 기본값은 1입니다.

◦ 기본 경로 얻기 - DHCP 서버에서 기본 경로를 가져올지 여부를 선택합니다. 일반적으로는 이 옵션을 선택합니다(기본값).

단계 **6** (선택 사항). **IPv6 Address(IPv6** 주소**)** 탭을 클릭하고 IPv6 주소를 구성합니다.

- 상태 - 글로벌 어드레스를 구성하지 않는 경우 IPv6 처리를 활성화하고 링크-로컬 주소를 자동으로 구성하려면 사용을 선택합니다. 링크 로컬 주소는 인터페이스 MAC 주소(수정된 EUI-64 형식)를 기반으로 생성됩니다.

  참고 IPv6를 비활성화해도 명시적 IPv6 주소로 구성되었거나 자동 컨피그레이션용으로 활성화된 인터페이스에서 IPv6 처리가 비활성화되지는 않습니다.

- 고정 주소/접두사 - 스테이트리스 자동 컨피그레이션을 사용하지 않는 경우 전체 고정 글로벌 IPv6 주소와 네트워크 접두사를 입력합니다. 예를 들어, 2001:0DB8::BA98:0:3210/48와 같이 입력합니다. IPv6 주소 지정에 대한 자세한 내용은 IPv6 주소 지정, 105 페이지를 참조하십시오.

  주소를 링크 로컬 전용으로 사용하려는 경우 링크-로컬 옵션을 선택합니다. 로컬 네트워크 외부에서는 링크 로컬 주소에 액세스할 수 없습니다. 브리지 그룹 인터페이스에서는 링크-로컬 주소를 구성할 수 없습니다.

  참고 링크-로컬 주소는 FE8, FE9, FEA 또는 FEB로 시작해야 합니다(예: fe80::20d:88ff:feee:6a82). Modified EUI-64 형식으로 링크-로컬 주소를 자동으로 지정하는 것이 좋습니다. 만약 다른 디바이스에서 Modified EUI-64 형식을 강제 적용하는 경우 수동으로 지정된 링크-로컬 주소 때문에 패킷이 폐기될 수 있습니다.

- **RA** 표시 안 함 - 라우터 알림을 표시하지 않을지를 선택합니다. Firepower Threat Defense 디바이스는 네이버 디바이스가 기본 라우터 주소를 동적으로 학습하도록 라우터 알림에 참여할 수 있습니다. 기본적으로 라우터 알림 메시지(ICMPv6 유형 134)는 IPv6가 구성된 각 인터페이스에 주기적으로 전송됩니다.

  라우터 광고는 라우터 요청 메시지에 대한 응답으로도 보내집니다(ICMPv6 Type 133). 예정된 다음 라우터 광고 메시지를 기다릴 필요 없이 호스트가 즉시 자동 구성을 할 수 있도록 시스템 시동 시 라우터 요청 메시지가 전송됩니다.

  Firepower Threat Defense 디바이스가 IPv6 접두사를 제공하지 않도록 하려는 인터페이스(예: 외부 인터페이스)에서는 이러한 메시지를 표시하지 않을 수 있습니다.

단계 **7** (선택 사항). 고급 인터페이스 옵션 구성, 118 페이지.
대부분의 고급 옵션은 브리지 그룹 구성원 인터페이스에 대해 구성하지만 브리지 그룹 인터페이스에 대해 사용할 수 있는 옵션도 있습니다.

고급 설정에는 대부분의 네트워크에 적합한 기본값이 있습니다. 네트워크 문제를 해결하는 경우에만 이러한 기본값을 수정하십시오.

단계 **8** **OK(**확인**)**를 클릭합니다.

다음에 할 작업

- 사용하려는 모든 구성원 인터페이스가 활성화되어 있는지 확인합니다.
- 브리지 그룹에 대해 DHCP 서버를 구성합니다. DHCP 서버 구성, 290 페이지를 참조하십시오.
- 적절한 보안 영역에 구성원 인터페이스를 추가합니다. 보안 영역 구성, 94 페이지를 참조하십시오.
- ID, NAT, 액세스 등의 정책이 브리지 그룹 및 구성원 인터페이스에 필요한 서비스를 제공하는지 확인합니다.

고급 인터페이스 옵션 구성

고급 인터페이스 옵션에는 대부분의 네트워크에 적합한 기본 설정이 있습니다. 네트워킹 문제를 해결하는 경우에만 이러한 설정을 구성하십시오.

다음 절차에서는 인터페이스가 이미 정의되어 있다고 가정합니다. 인터페이스를 처음 수정하거나 생성할 때 이러한 설정을 수정할 수도 있습니다.

브리지 그룹의 경우에는 구성원 인터페이스에서 이러한 옵션 중 대부분을 구성합니다. 이러한 옵션은 DAD 시도를 제외하고는 BVI(브리지 가상 인터페이스)에 사용할 수 없습니다.

절차

단계 **1** 디바이스을 클릭한 다음 **Interfaces(**인터페이스**)** 요약에서 링크를 클릭합니다.
인터페이스 목록에는 사용 가능한 인터페이스, 해당 이름, 주소 및 상태가 표시됩니다.

단계 **2** 수정할 인터페이스의 수정 아이콘( )을 클릭합니다.

단계 **3** **Advanced Options(**고급 옵션**)** 탭을 클릭합니다.

단계 **4** 데이터 인터페이스 관리만 수행하려면 **Management Only(**관리만**)**를 선택합니다.
관리 전용 인터페이스에서는 통과 트래픽을 허용하지 않으므로 데이터 인터페이스를 관리 전용으로 설정할 때 사용할 수 있는 값은 거의 없습니다. 관리/진단 인터페이스(항상 관리 전용)의 경우에는 이 설정을 변경할 수 없습니다.

단계 **5** **MTU**(최대 전송 단위)를 원하는 값으로 변경합니다.
기본 MTU는 1500바이트입니다. 64~9198 사이의 값을 지정할 수 있습니다. 네트워크에서 대개 점보 프레임이 표시되면 높은 값을 설정합니다.

참고 ASA 5500-X Series 디바이스에서 MTU를 1500보다 큰 값으로 늘리는 경우에는 디바이스를 재부팅해야 합니다. 이렇게 하려면 CLI에 로그인하여 **reboot** 명령을 사용합니다.

단계 **6** (실제 인터페이스만 해당됨) 속도 및 이중 설정을 수정합니다.
기본적으로 인터페이스는 연결 반대쪽의 인터페이스와 최적의 이중 및 속도를 협상하지만, 필요한 경우 특정 이중이나 속도를 강제 적용할 수 있습니다. EPM 카드의 인터페이스에 이러한 옵션을 구성하기 전에 인터페이스 컨피그레이션에 대한 제한, 103 페이지를 읽어보십시오.

- **Duplex(**듀플렉스**)** — **Auto(**자동**)**, **Half(**하프**)**, **Full(**풀**)** 또는 **Default(**기본값**)**를 선택합니다. 인터페이스가 지원하는 경우 자동이 기본값입니다.

Firepower Device Manager에서 설정을 구성할 필요가 없음을 나타내려면 **Default(**기본값**)**를 선택합니다. 모든 기존 컨피그레이션이 변경되지 않은 상태로 유지됩니다.

- **Speed(**속도**)** — **Auto(**자동**)**를 선택하여 인터페이스가 속도를 협상하도록 하거나(이 옵션이 기본값임), **10**, **100**, **1000**Mbps 중에서 특정 속도를 선택합니다. 다음과 같은 특수 옵션을 선택할 수도 있습니다.
  - **No Negotiate(**협상 안 함**)** — 파이버 인터페이스의 경우 속도를 1000Mbps로 설정하고 링크 매개변수를 협상하지 않습니다. 이 옵션은 이러한 인터페이스의 기본 구성 설정입니다.
  - **Default(**기본값**)** — Firepower Device Manager에서 설정을 구성할 필요가 없음을 나타냅니다. 모든 기존 컨피그레이션이 변경되지 않은 상태로 유지됩니다.

단계 **7** **IPv6** 컨피그레이션 설정을 수정합니다.

- **IPv6** 주소 컨피그레이션에 **DHCP** 활성화 - IPv6 라우터 알림 패킷에서 관리 주소 컨피그레이션 플래그를 설정할지 여부를 선택합니다. 이 플래그는 IPv6 자동 컨피그레이션 클라이언트에게 DHCPv6를 사용하여 파생된 스테이트리스 자동 컨피그레이션 주소 이외의 주소도 얻도록 안내합니다.
- **IPv6** 비주소 컨피그레이션에 **DHCP** 활성화 - IPv6 라우터 알림 패킷에서 기타 주소 컨피그레이션 플래그를 설정할지 여부를 선택합니다. 이 플래그는 IPv6 자동 컨피그레이션 클라이언트에게 DHCPv6를 사용하여 DHCPv6로부터 추가 정보(예: DNS 서버 주소)를 얻도록 안내합니다.
- **DAD** 시도 - 인터페이스가 DAD(Duplicate Address Detection)를 수행하는 빈도를 0~600 사이의 값으로 설정합니다. 기본값은 1입니다. 스테이트리스 자동 컨피그레이션 프로세스에서 DAD는 새로운 유니캐스트 IPv6 주소가 고유한지 확인한 다음 주소를 인터페이스에 할당합니다. 중복 주소가 인터페이스의 링크-로컬 주소인 경우 인터페이스의 IPv6 패킷 처리가 비활성화됩니다. 중복 주소가 전역 주소인 경우 주소가 사용되지 않습니다. 인터페이스에서는 네이버 요청 메시지를 사용하여 DAD를 수행합니다. DAD(Duplicate Address Detection) 처리를 비활성화하려면 값을 0으로 설정합니다.

단계 **8** **OK(**확인**)**를 클릭합니다.

모니터링 인터페이스

다음 영역에서 인터페이스에 대한 몇 가지 기본 정보를 확인할 수 있습니다.

- **Monitoring(**모니터링**)** > **System(**시스템**)**. 처리량 대시보드에는 시스템을 통과하는 트래픽에 대한 정보가 표시됩니다. 모든 인터페이스에서 정보를 확인할 수도 있고 검사할 특정 인터페이스를 선택할 수도 있습니다.
- **Monitoring(**모니터링**)** > **Ingress Zones(**인그레스 영역**)** 및 이그레스 영역. 이 대시보드에는 인터페이스로 구성된 영역을 기준으로 하는 통계가 표시됩니다. 이 정보를 자세히 확인하여 추가 세부사항을 파악할 수 있습니다.

- 디바이스. 연결 다이어그램에는 인터페이스 상태가 표시됩니다. 포트 위에 마우스를 놓으면 인터페이스의 IP 주소와 인터페이스의 상태 및 링크 상태가 표시됩니다. 이 정보를 통해 작동되어야 하는데 중단되어 있는 인터페이스를 식별할 수 있습니다.

CLI에서 인터페이스 모니터링

디바이스 CLI에 로그인한 후에 다음 명령을 사용하여 인터페이스 관련 행동 및 통계에 대한 상세 정보를 가져올 수도 습니다.

- **show interface**는 인터페이스 통계 및 컨피그레이션 정보를 표시합니다. 이 명령에는 필요한 정보를 가져오는 데 사용할 수 있는 여러 키워드가 있습니다. 사용 가능한 옵션을 확인하려면 키워드로 ?를 사용합니다.
- **show ipv6 interface**는 인터페이스에 대한 IPv6 컨피그레이션 정보를 표시합니다.
- **show bridge-group**은 구성원 정보와 IP 주소를 비롯하여 BVI(브리지 가상 인터페이스)에 대한 정보를 표시합니다.
- **show conn**은 인터페이스를 통해 현재 설정되어 있는 연결에 대한 정보를 표시합니다.
- **show traffic**은 각 인터페이스를 통과하는 트래픽에 대한 통계를 표시합니다.
- **show ipv6 traffic**은 디바이스를 통과하는 IPv6 트래픽에 대한 통계를 표시합니다.
- **show dhcpd**는 인터페이스의 DHCP 사용량에 대한 통계와 기타 정보(특히 인터페이스에 구성된 DHCP 서버 관련 정보)를 표시합니다.

7 장

라우팅

시스템은 라우팅 테이블을 사용하여 시스템으로 들어오는 패킷용 이그레스 인터페이스를 결정합니다. 다음 주제에서는 라우팅의 기본 사항과 디바이스에서 라우팅을 구성하는 방법을 설명합니다.

라우팅 개요

다음 항목에서는 Firepower Threat Defense 디바이스 내에서 라우팅이 동작하는 방식을 설명합니다. 라우팅은 소스에서 목적지까지 네트워크 전반에 걸친 정보의 이동입니다. 그 과정에서 적어도 하나의 중간 노드를 만나게 됩니다. 라우팅에는 2가지 기본적인 작업이 포함됩니다. 최적의 라우팅 경로를 결정하는 것과 인터네트워크를 통한 정보 그룹(패킷이라고 함)을 전송하는 것입니다.

NAT가 경로 선택에 영향을 주는 방식

Firepower Threat Defense는 라우팅 테이블 및 NAT(네트워크 주소 변환) XLATE(변환) 테이블을 둘 다 사용하여 라우팅을 결정합니다. 대상 IP 변환 트래픽, 즉 미변환 트래픽을 처리하기 위해 시스템은 기존 XLATE 또는 고정 변환을 검색하여 이그레스 인터페이스를 선택합니다.

선택 프로세스는 다음 단계를 따릅니다.

1. 대상 IP 변환 XLATE가 이미 있을 경우 패킷에 대한 이그레스 인터페이스는 라우팅 테이블이 아니라 XLATE 테이블에서 결정됩니다.
2. 대상 IP 변환 XLATE가 없지만 일치하는 고정 NAT 변환이 존재하는 경우 이그레스 인터페이스는 고정 NAT 규칙으로부터 결정되고 XLATE가 생성되며 라우팅 테이블은 사용되지 않습니다.
3. 대상 IP 변환 XLATE가 없고 일치하는 고정 변환도 없을 경우 패킷은 대상 IP로 변환되지 않습니다. 시스템에서는 이그레스 인터페이스 선택을 위해 경로를 조회하여 이 패킷을 처리합니다. 그런 다음 필요한 경우 소스 IP 변환이 수행됩니다.

일반 동적 아웃바운드 NAT의 경우 경로 테이블을 사용하여 초기 발신 패킷을 라우팅한 후에 XLATE를 생성합니다. 수신 반환 패킷은 기존 XLATE만 사용하여 전달됩니다. 고정 NAT의 경우 대상 변환 수신 패킷은 항상 기존 XLATE 또는 고정 변환 규칙을 사용하여 전달됩니다.

이그레스 인터페이스를 선택한 다음 선택한 이그레스 인터페이스에 속하는 적당한 다음 홉을 찾기 위해 추가 경로 조회가 수행됩니다. 선택된 인터페이스에 명시적으로 속하는 경로가 라우팅 테이블에 없을 경우, 다른 이그레스 인터페이스에 속하는 지정된 대상 네트워크를 위한 또 다른 경로가 있더라도 패킷은 삭제되고 레벨 6 진단 syslog 메시지 110001(호스트 경로 없음)이 생성됩니다. 선택된 이그레스 인터페이스에 속하는 경로가 있으면 패킷은 해당 다음 홉으로 전달됩니다.

라우팅 테이블과 경로 선택

NAT XLATE 및 규칙이 이그레스 인터페이스를 결정하지 않으면 시스템은 라우팅 테이블을 사용하여 패킷의 경로를 결정합니다.

라우팅 테이블의 경로에는 지정된 경로에 대한 상대적 우선순위를 제공하는 "관리 거리"라는 메트릭이 있습니다. 패킷이 둘 이상의 경로 항목과 일치하는 경우에는 거리가 가장 짧은 항목이 사용됩니다. 직접 연결된 네트워크(인터페이스에서 정의된 네트워크)는 거리가 0이므로 항상 기본적으로 사용됩니다. 고정 경로의 기본 거리는 1이지만 1~254 범위의 원하는 거리를 사용하여 고정 경로를 생성할 수 있습니다.

특정 대상을 식별하는 경로는 기본 경로(대상이 0.0.0.0/0인 경로)보다 우선적으로 적용됩니다.

포워딩 결정 방법

포워딩 결정은 다음과 같이 이루어집니다.

- 목적지가 라우팅 테이블 내의 엔트리와 일치하지 않으면 패킷이 기본 경로에 지정된 인터페이스를 통해 포워딩됩니다. 기본 경로가 구성되지 않은 경우 패킷이 폐기됩니다.
- 목적지가 라우팅 테이블의 단일 엔트리와 일치하는 경우 패킷이 해당 경로와 연결된 인터페이스를 통해 포워딩됩니다.
- 목적지가 라우팅 테이블에 있는 두 개 이상의 항목과 일치하면 패킷은 네트워크 접두사가 더 긴 경로와 연결된 인터페이스를 통해 전달됩니다.

예를 들어 목적지가 192.168.32.1인 패킷은 라우팅 테이블의 다음 경로를 통해 인터페이스에 도착합니다.

- 192.168.32.0/24 게이트웨이 10.1.1.2
- 192.168.32.0/19 게이트웨이 10.1.1.3

이 경우 192.168.32.1이 192.168.32.0/24 네트워크 범위에 해당되기 때문에 목적지가 192.168.32.1인 패킷은 10.1.1.2로 전달됩니다. 이 주소는 라우팅 테이블 내 다른 경로에도 포함되지만, 라우팅 테이블의 다른 경로 접두사는 19비트인 데 비해 192.168.32.0/24의 접두사는 24비트이므로 이 경로의 접두사가 가장 깁니다. 패킷을 전달할 때는 항상 더 긴 접두사가 우선합니다.

참고 새로운 유사한 연결이 경로 변경으로 인해 다른 동작을 유발하는 경우에도 기존의 연결은 계속해서 설정된 인터페이스를 사용합니다.

고정 경로 구성

시스템의 인터페이스에 직접 연결된 네트워크로 이동하지 않는 패킷을 전송할 위치를 시스템에 지시하려면 고정 경로를 정의합니다.

네트워크 0.0.0.0/0에 대해 하나 이상의 고정 경로(기본 경로)가 필요합니다. 이 경로는 기존 NAT xlate(변환)나 고정 NAT 규칙 또는 기타 정적 경로를 통해 이그레스 인터페이스를 확인할 수 없는 패킷을 전송할 위치를 정의합니다.

기본 게이트웨이를 사용하여 모든 네트워크에 액세스할 수 없는 경우 다른 고정 경로가 필요할 수 있습니다. 예를 들어 기본 경로는 대개 외부 인터페이스의 업스트림 라우터입니다. 디바이스에 직접 연결되지 않는 추가 내부 네트워크가 있으며 기본 게이트웨이를 통해 해당 네트워크에 액세스할 수 없는 경우에는 이러한 각 내부 네트워크에 대해 고정 경로가 필요합니다.

시스템 인터페이스에 직접 연결된 네트워크에 대해서는 고정 경로를 정의할 수 없습니다. 시스템에서 이러한 경로를 자동으로 생성합니다.

절차

단계 **1** 디바이스을 클릭한 다음 **Routing(**라우팅**)** 요약에서 링크를 클릭합니다.

단계 **2** **Static Routing(**정적 라우팅**)** 페이지에서 다음 중 하나를 수행합니다.

- 새 경로를 추가하려면 + > **Add Static Route(**정적 경로 추가**)**를 클릭합니다.
- 수정할 경로의 수정 아이콘( )을 클릭합니다.

경로가 더 이상 필요하지 않은 경우 해당 경로의 휴지통 아이콘을 클릭하여 경로를 삭제합니다.

단계 **3** 경로 속성을 구성합니다.

프로토콜

경로가 **IPv4** 주소인지 아니면 **IPv6** 주소인지를 선택합니다.

게이트웨이

게이트웨이의 IP 주소를 식별하는 호스트 네트워크 개체를 선택합니다. 트래픽은 이 주소로 전송됩니다.

인터페이스

트래픽을 전송하는 데 사용할 인터페이스를 선택합니다. 이 인터페이스를 통해 게이트웨이 주소에 액세스할 수 있어야 합니다.

브리지 그룹의 경우 구성원 인터페이스가 아닌 BVI(브리지 그룹 인터페이스)에 대해 경로를 구성합니다.

메트릭

경로의 관리 거리(1~254)입니다. 기본값은 고정 경로의 경우 1입니다. 인터페이스와 게이트웨이 간에 추가 라우터가 있으면 홉 수를 관리 거리로 입력합니다.

관리 거리는 경로를 비교하는 데 사용되는 파라미터입니다. 값이 작을수록 경로에는 더 높은 우선 순위가 지정됩니다. 연결된 경로(디바이스의 인터페이스에 직접 연결되는 네트워크)가 항상 고정 경로보다 우선적으로 사용됩니다.

네트워크

이 경로에서 게이트웨이를 사용해야 하는 대상 네트워크 또는 호스트를 식별하는 네트워크 개체를 선택합니다.

기본 경로를 정의하거나, 사전 정의된 임의의 ipv4 또는 ipv6 네트워크 개체를 사용하거나, 0.0.0.0/0(IPv4) 또는 ::/0(IPv6) 네트워크에 대해 개체를 생성합니다.

단계 **4** **OK(**확인**)**를 클릭합니다.

라우팅 모니터링

라우팅을 모니터링하고 문제해결을 수행하려면 디바이스 CLI에 로그인하여 다음 명령을 사용합니다.

- **show route**는 직접 연결된 네트워크의 경로를 포함하여 데이터 인터페이스에 대한 라우팅 테이블을 표시합니다.
- **show ipv6 route**는 직접 연결된 네트워크의 경로를 포함하여 데이터 인터페이스에 대한 IPv6 라우팅 테이블을 표시합니다.
- **show network**는 관리 게이트웨이를 포함하여 가상 관리 인터페이스의 컨피그레이션을 표시합니다. 관리 게이트웨이로 데이터 인터페이스를 지정하는 경우가 아니면 가상 인터페이스를 통한 라우팅은 데이터 인터페이스 라우팅 테이블에 의해 처리되지 않습니다.
- **show network-static-routes**는 **configure network static-routes** 명령을 사용하여 가상 관리 인터페이스에 대해 구성된 정적 경로를 표시합니다. 대부분의 경우에는 관리 라우팅에 관리 게이트웨이만 사용하면 되므로, 일반적으로는 정적 경로가 없습니다. 데이터 인터페이스의 트래픽에는 이러한 경로를 사용할 수 없습니다.

II 부

보안 정책

8 장

ID 정책

연결에서 사용자 ID 정보를 수집하기 위해 ID 정책을 사용할 수 있습니다. 그런 다음 대시보드에서 사용자 ID를 기준으로 사용량을 보고 사용자 또는 사용자 그룹을 기준으로 액세스 제어를 구성할 수 있습니다.

ID 정책 개요

ID 정책을 사용하여 연결과 연계된 사용자를 탐지할 수 있습니다. 사용자를 식별하면 위협, 엔드포인트 및 네트워크 인텔리전스를 사용자 ID 정보와 연결할 수 있습니다. 시스템에서 네트워크 행동, 트래픽 및 이벤트를 개별 사용자와 직접 연결하므로 정책 위반, 공격 또는 네트워크 취약점의 소스를 손쉽게 식별할 수 있습니다.

예를 들어 침입 이벤트의 대상인 호스트를 소유한 사용자와 내부 공격 또는 포트 스캔을 시작한 사용자를 식별할 수 있습니다. 부적절한 웹 사이트 또는 애플리케이션에 액세스하는 사용자 및 대역폭을 많이 사용하는 사용자도 식별할 수 있습니다.

사용자 탐지에서는 분석용 데이터 수집 이외의 작업도 수행할 수 있습니다. 사용자 이름 또는 사용자 그룹 이름을 기준으로 액세스 규칙을 작성하여 사용자 인증을 기준으로 리소스에 대한 액세스를 선택적으로 허용하거나 차단할 수도 있습니다.

참고 시스템은 다른 사용자가 같은 호스트에 여러 번 로그인하는 경우를 탐지하면 특정 시점에 지정된 호스트에 한 명의 사용자만 로그인하며 호스트의 현재 사용자가 마지막 권한 있는 사용자 로그인이라고 가정합니다. 원격 세션을 통해 여러 사용자가 로그인한 경우 서버에서 보고한 마지막 사용자가 사용자로 간주됩니다.

활성 인증을 통한 사용자 ID 설정

인증은 사용자의 ID를 확인하는 작업입니다.

활성 인증을 사용하는 경우, 시스템에 사용자-ID 매핑이 없는 IP 주소에서 HTTP 트래픽 흐름이 유입되는 경우 시스템에 구성된 디렉터리에 대해 트래픽 흐름을 시작한 사용자를 인증할지를 결정할 수 있습니다. 사용자가 정상적으로 인증하면 해당 IP 주소는 인증된 사용자의 ID를 포함하는 것으로 간주됩니다.

인증이 실패해도 사용자의 네트워크 액세스는 차단되지 않습니다. 최종적으로는 액세스 규칙에 따라 이러한 사용자에게 제공할 액세스 권한이 결정됩니다.

사용자 수 제한사항

Firepower Device Manager는 디렉터리 서버에서 사용자 최대 2,000명에 대한 정보를 다운로드할 수 있습니다.

디렉터리 서버에 2,000개보다 많은 사용자 어카운트가 포함되어 있으면 액세스 규칙에서 사용자를 선택할 때 또는 사용자 기반 대시보드 정보를 확인할 때 가능한 이름이 모두 표시되지 않으며, 다운로드한 이름에 대해서만 규칙을 작성할 수 있습니다.

이 2,000개 제한은 그룹과 연결된 이름에도 적용됩니다. 그룹의 멤버가 2,000명보다 많으면 다운로드한 2,000개의 이름에 대해서만 그룹 멤버십과의 일치 여부를 확인할 수 있습니다.

사용자가 2,000명보다 많은 경우에는 Firepower Device Manager 대신 Firepower Management Center(원격 관리자)를 사용하는 것이 좋습니다. Firepower Management Center는 훨씬 더 많은 사용자를 지원합니다.

지원되는 디렉터리 서버

ID 정책을 통해 Windows Server 2008 및 2012에서 Microsoft Active Directory(AD)를 사용할 수 있습니다.

서버 컨피그레이션과 관련하여 다음 사항에 유의하십시오.

- 사용자 그룹 또는 그룹 내의 사용자에 대해 사용자 제어를 수행하려면 디렉터리 서버에서 사용자 그룹을 구성해야 합니다. 서버가 기본 개체 계층으로 사용자를 구성하는 경우 시스템은 사용자 그룹 제어를 수행할 수 없습니다.
- 디렉터리 서버는 시스템에 대해 다음 표에 나와 있는 필드 이름을 순서대로 사용하여 해당 필드에 대한 사용자 메타데이터를 서버에서 검색해야 합니다.

메타데이터	**Active Directory** 필드
LDAP 사용자 이름	samaccountname
이름	givenname
성	sn

메타데이터	**Active Directory** 필드
이메일 주소	mail userprincipalname(메일에 값이 없는 경우)
부서	department distinguishedname(부서에 값이 없는 경우)
전화번호	telephonenumber

디렉터리 기본 **DN** 결정

디렉터리 속성을 구성할 때는 사용자와 그룹에 대한 공통 기본 DN(고유 이름)을 지정해야 합니다. 이 기준은 디렉터리 서버에서 정의되며 네트워크마다 다릅니다. 올바른 기준을 입력해야 ID 정책이 실행됩니다. 기준이 잘못된 경우 시스템이 사용자 또는 그룹 이름을 확인할 수 없으므로 ID 기반 정책이 실행될 수 없습니다.

팁 올바른 기준을 가져오려면 디렉터리 서버 담당 관리자에게 문의하십시오.

Active Directory의 경우 도메인 관리자로 Active Directory 서버에 로그인하여 다음과 같이 명령 프롬프트에 **dsquery** 명령을 사용해 기준을 확인하여 올바른 기준을 확인할 수 있습니다.

사용자 검색 기준

알려진 사용자 이름(부분 또는 전체)을 포함한 **dsquery user** 명령을 입력하여 기본 고유 이름을 확인합니다. 예를 들어, 다음 명령은 부분 이름 "John*"를 사용하여 "John"으로 시작되는 모든 사용자에 대한 정보를 반환합니다.

```
C:\Users\Administrator>dsquery user -name "John*"
"CN=John Doe,CN=Users,DC=csc-lab,DC=example,DC=com"
```

이 경우 기본 DN은 "DC=csc-lab,DC=example,DC=com"이 됩니다.

그룹 검색 기준

알려진 그룹 이름을 포함한 **dsquery group** 명령을 입력하여 기본 고유 이름을 확인합니다. 예를 들어, 다음 명령은 그룹 이름 Employees를 사용하여 고유 이름을 반환합니다.

```
C:\>dsquery group -name "Employees"
"CN=Employees,CN=Users,DC=csc-lab,DC=example,DC=com"
```

이 경우 그룹 기본 DN은 "DC=csc-lab,DC=example,DC=com"이 됩니다.

ADSI 수정 프로그램을 사용하여 Active Directory 구조를 찾을 수도 있습니다(**Start**(시작) > **Run**(실행) > **adsiedit.msc**). ADSI 수정에서 조직 단위(OU), 그룹, 사용자 등의 개체를 마우스 오른쪽 단추로 클릭

하고 **Properties(**속성**)**를 선택하여 고유 이름을 확인합니다. 그러면 DC 값 문자열을 기준으로 복사할 수 있습니다.

기준이 올바른지를 확인하려면 다음 단계를 수행합니다.

1. 디렉터리 속성의 연결 테스트 버튼을 클릭하여 연결을 확인합니다. 모든 문제를 해결하고 디렉터리 속성을 저장합니다.
2. 디바이스에 변경 사항을 커밋합니다.
3. 액세스 규칙을 생성하고 **Users(**사용자**)** 탭을 선택한 다음 디렉터리에서 알려진 사용자 및 그룹 이름을 추가해 봅니다. 디렉터리가 포함된 영역에서 일치하는 사용자 및 그룹을 입력하면 자동 완성 제안 사항이 표시됩니다. 이러한 제안 사항이 드롭다운 목록에 표시되는 경우 시스템이 디렉터리를 정상적으로 쿼리한 것입니다. 입력한 문자열이 사용자 또는 그룹 이름에 포함되어 있는데 제안 사항이 표시되지 않으면 해당하는 검색 기준을 수정해야 합니다.

알 수 없는 사용자 처리

ID 정책에 대해 디렉터리 서버를 구성할 때 시스템은 디렉터리 서버에서 사용자 및 그룹 멤버십 정보를 다운로드합니다. 이 정보는 24시간마다 자정에 또는 디렉터리 컨피그레이션을 수정하고 저장할 때마다 새로 고침됩니다. 정보를 변경하지 않는 경우에도 마찬가지입니다.

사용자가 활성 인증 ID 규칙에 따라 인증에 성공했으나 사용자 이름이 다운로드된 사용자 ID 정보에 없으면 해당 사용자는 알 수 없음으로 표시됩니다. 사용자 ID와 사용자 일치 그룹 규칙은 ID 관련 대시보드에 표시되지 않습니다.

그러나 알 수 없음 사용자에 대한 모든 액세스 제어 규칙은 적용됩니다. 예를 들어 알 수 없음 사용자에 대한 연결을 차단하는 경우, 해당 사용자는 인증에 성공하더라도(즉, 디렉터리 서버에서 사용자와 비밀번호를 유효한 것으로 인식하더라도) 차단됩니다.

그러므로 사용자를 추가 또는 삭제하거나 그룹 멤버십을 변경하는 등 디렉터리 서버를 변경하면 시스템이 디렉터리에서 업데이트를 다운로드할 때까지는 해당 변경 사항이 정책 시행에 반영되지 않습니다.

매일 자정 업데이트가 수행될 때까지 기다리지 않으려면 **Policies(**정책**)** > **Identity(ID** 영역**)**에서 **Directory Server(**디렉터리 서버**)** 버튼을 클릭하여 디렉터리 서버 정보를 수정하는 방법으로 업데이트를 강제로 수행할 수 있습니다. **Save(**저장**)**를 클릭한 다음 변경 사항을 구축합니다. 그러면 시스템이 업데이트를 즉시 다운로드합니다.

참고 **Policies(**정책**)** > **Access Control(**액세스 제어**)**로 이동하여 **Add Rule (+)(**규칙 추가**(+))** 버튼을 클릭하고 **Users(**사용자**)** 탭에서 사용자 목록을 확인하여 새 사용자 정보 또는 삭제된 사용자 정보가 시스템에 있는지를 확인할 수 있습니다. 새 사용자를 찾을 수 없거나 삭제된 사용자를 찾을 수 있으면 시스템의 정보는 오래된 것입니다.

ID 정책 구성

연결에서 사용자 ID 정보를 수집하기 위해 ID 정책을 사용할 수 있습니다. 그런 다음 대시보드에서 사용자 ID를 기준으로 사용량을 보고 사용자 또는 사용자 그룹을 기준으로 액세스 제어를 구성할 수 있습니다.

아래에서는 ID 정책을 통해 사용자 ID를 가져오는 데 필요한 요소를 구성하는 방법을 간략하게 설명합니다.

절차

단계 **1** 정책 > **ID**를 선택합니다.
ID 정책을 아직 정의하지 않은 경우 마법사를 시작하여 ID 정책을 구성하라는 메시지가 표시됩니다. 시작하기를 클릭하여 마법사를 시작합니다. 마법사에서는 다음 단계를 안내합니다.

a) 디렉터리 서버 구성, 131 페이지
b) 액티브 인증 캡티브 포털 구성, 133 페이지

단계 **2** ID 정책을 관리합니다.
ID 설정을 구성하고 나면 이 페이지에 모든 규칙이 순서대로 나열됩니다. 목록의 맨 위에서부터 규칙과 트래픽의 일치 여부를 확인하며, 첫 번째로 일치하는 규칙에 따라 적용할 작업이 결정됩니다. 이 페이지에서는 다음을 수행할 수 있습니다.

- ID 정책을 활성화하거나 비활성화하려면 **ID** 정책 토글을 클릭합니다.
- 디렉터리 서버 컨피그레이션을 변경하려면 디렉터리 서버 버튼( ).
- 액티브 인증 캡티브 포털 컨피그레이션을 변경하려면 액티브 인증 버튼( ).
- 규칙을 구성하려면 다음을 수행합니다.
  - 새 규칙을 생성하려면 + 버튼을 클릭합니다.
  - 기존 규칙을 수정하려면 해당 규칙의 수정 아이콘( )을 클릭합니다. 테이블에서 속성을 클릭하여 규칙 속성을 선택적으로 수정할 수도 있습니다.
  - 더 이상 필요하지 않은 규칙을 삭제하려면 해당 규칙의 삭제 아이콘( )을 클릭합니다.

ID 규칙 생성 및 수정에 대한 자세한 내용은 ID 규칙 구성, 134 페이지를 참조하십시오.

디렉터리 서버 구성

디렉터리 서버는 네트워크 액세스가 허용되는 사용자 및 사용자 그룹에 대한 정보를 포함합니다. 시스템은 매일 마지막 시간(UTC)에 모든 사용자와 그룹에 대한 업데이트된 정보를 다운로드합니다.

디렉터리 관리자와 협의하여 디렉터리 서버 속성을 구성하는 데 필요한 값을 가져오십시오.

참고 영역을 추가한 후에는 **Directory Server(**디렉터리 서버**)** 버튼을 클릭한 다음 디렉터리 서버 대화 상자에서 **Test(**테스트**)** 버튼을 클릭하여 설정을 확인하고 연결을 테스트할 수 있습니다. 테스트에서 장애가 발생하면 모든 필드를 확인하고 관리 IP 주소와 디렉터리 서버 간에 네트워크 경로가 있는지 확인합니다.

절차

단계 **1** **Policies(**정책**)** > **Identity(ID)**를 선택합니다.

단계 **2** 다음 중 하나를 수행합니다.

- 디렉터리 또는 ID 규칙을 아직 구성하지 않은 경우 **Get Started(**시작하기**)**를 클릭하여 ID 정책 마법사를 시작합니다. 디렉터리 서버를 구성하라는 메시지가 먼저 표시됩니다.
- 디렉터리 서버 버튼().

단계 **3** 디렉터리 서버에 대한 다음 정보를 입력합니다.

- 이름 - 디렉터리 영역의 이름입니다.
- 유형 - 디렉터리 서버의 유형입니다. 지원되는 유형은 Active Directory뿐이며 이 필드의 내용은 변경할 수 없습니다.
- 디렉토리 사용자 이름, 디렉토리 비밀번호 - 검색하려는 사용자 정보에 대한 적절한 권한이 있는 사용자의 고유 사용자 이름 및 비밀번호입니다. admin@ad.example.com 등을 예로 들 수 있습니다.
- 기본 **DN** - 사용자 및 그룹 정보를 검색하거나 쿼리하기 위한 디렉터리 트리, 즉 사용자와 그룹의 공통 상위 항목입니다. dc=example,dc=com을 예로 들 수 있습니다. 기본 DN을 찾는 방법에 대한 자세한 내용은 디렉터리 기본 DN 결정, 129 페이지를 참조하십시오.
- **AD** 기본 도메인 - 디바이스가 죠인해야 하는 정규화된 Active Directory 도메인 이름입니다. example.com 등을 예로 들 수 있습니다.
- 호스트 이름**/IP** 주소 - 디렉토리 서버의 호스트 이름 또는 IP 주소입니다. 서버에 대한 암호화된 연결을 사용하는 경우에는 IP 주소가 아닌 FQDN(Fully-Qualified Domain Name)을 입력해야 합니다.
- 포트 - 서버와의 통신에 사용되는 포트 번호입니다. 기본값은 389입니다. 암호화 방법으로 LDAPS를 선택하는 경우에는 포트 636을 사용합니다.
- 암호화 - 사용자 및 그룹 정보를 다운로드하기 위해 암호화된 연결을 사용하려는 경우에는 **STARTTLS** 또는 **LDAPS** 중에서 원하는 방법을 선택합니다. 기본값은 없음입니다. 이 옵션은 사용자 및 그룹 정보를 일반 텍스트로 다운로드함을 의미합니다.
  - **STARTTLS**는 암호화 방법을 협상하여 디렉터리 서버가 지원하는 가장 강력한 방법을 사용하며 포트 389를 사용합니다.
  - **LDAPS**를 선택하는 경우 LDAP over SSL이 필요합니다. 이 옵션은 포트 636을 사용합니다.

- **SSL** 인증서 - 암호화 방법을 선택하는 경우 CA 인증서를 업로드하여 시스템과 디렉터리 서버 간에 신뢰할 수 있는 연결을 설정합니다. 인증서를 사용하여 인증하는 경우에는 인증서의 서버 이름이 서버 호스트 이름/IP 주소와 일치해야 합니다. 예를 들어 IP 주소로 10.10.10.250을 사용하는데 인증서의 주소는 ad.example.com이면 연결은 실패합니다.

단계 **4** 마법사에서 **Next(**다음**)**를 클릭하거나 **Save(**저장**)**를 클릭합니다.

액티브 인증 캡티브 포털 구성

ID 규칙에서 사용자에 대한 액티브 인증을 요구하는 경우 사용자는 연결 시에 사용한 인터페이스의 캡티브 포털 포트로 리디렉션되며, 그리고 나면 인증하라는 메시지가 표시됩니다. 인증서를 업로드하지 않으면 사용자에게 자체 서명 인증서가 제공됩니다. 사용자의 브라우저에서 이미 신뢰하는 인증서를 업로드하지 않으면 사용자가 인증서를 허용해야 합니다.

참고 HTTP 기본, HTTP 대응 페이지 및 NTLM 인증 방법의 경우 사용자는 인터페이스의 IP 주소를 사용하여 종속 포털로 리디렉션됩니다. 그러나 HTTP 협상의 경우에는 사용자가 정규화된 DNS 이름 *firewall-hostname.AD-domain-name*을 사용하여 리디렉션됩니다. HTTP 협상을 사용하려는 경우에는 DNS 서버도 업데이트하여 활성 인증을 수행해야 하는 모든 내부 인터페이스의 IP 주소에 이 이름을 매핑해야 합니다. 이렇게 하지 않으면 리디렉션을 완료할 수 없으며 사용자가 인증할 수 없습니다.

시작하기 전에

디렉터리 서버, Firepower Threat Defense 디바이스 및 클라이언트에서 시간 설정이 일치하는지 확인합니다. 이러한 디바이스 간에 시간이 바뀌면 사용자가 정상적으로 인증하지 못할 수 있습니다. 모든 연결은 포인트 투 포인트 방식이지만, 디바이스가 참여하는 각 터널을 정의하여 규모가 더 큰 허브 앤 스포크(hub and spoke) 또는 메시 VPN에 연결할 수 있습니다.

절차

단계 **1** **Policies(**정책**)** > **Identity(ID)**를 선택합니다.

단계 **2** 다음 중 하나를 수행합니다.

- **Get Started(**시작하기**)** 마법사를 사용하는 경우 디렉터리 서버를 구성한 후에 **Next(**다음**)**를 클릭합니다.
- 액티브 인증 버튼( ).

단계 **3** 다음 옵션을 구성합니다.

- 서버 인증서 - 활성 인증 중에 사용자에게 제공할 CA 인증서입니다. 인증서는 PEM 또는 DER 형식의 X509 인증서여야 합니다. 인증서를 붙여넣거나 인증서 업로드를 클릭하고 인증서 파일을 선택합니다. 기본적으로는 사용자 인증 중에 자체 서명 인증서가 제공됩니다.

- 인증서 키 - 서버 인증서의 키입니다. 키를 붙여넣거나 키 업로드를 클릭하고 키 파일을 선택합니다.
- 포트 - 종속 포털 포트입니다. 기본값은 885(TCP)입니다. 다른 포트를 구성하는 경우에는 포트가 1025-65535 범위에 포함되어야 합니다.

단계 **4** **Save(**저장**)**를 클릭합니다.

ID 규칙 구성

ID 규칙은 일치하는 트래픽에 대해 사용자 ID 정보를 수집할지 여부를 결정합니다. 일치하는 트래픽에 대해 사용자 ID 정보를 가져오지 않으려는 경우에는 인증 없음을 구성할 수 있습니다.

규칙 컨피그레이션에 관계없이 액티브 인증은 HTTP 트래픽에 대해서만 수행됩니다. 따라서 액티브 인증에서 비 HTTP 트래픽을 제외하는 규칙을 생성할 필요가 없습니다. 모든 HTTP 트래픽에 대해 사용자 ID 정보를 가져오려면 모든 원본과 대상에 대해 액티브 인증 규칙만 적용하면 됩니다.

참고 인증에서 장애가 발생해도 네트워크 액세스에는 아무 영향이 없습니다. ID 정책은 사용자 ID 정보만 수집합니다. 인증 시에 장애가 발생한 사용자의 네트워크 액세스를 차단하려는 경우에는 액세스 규칙을 사용해야 합니다.

절차

단계 **1** **Policies(**정책**)** > **Identity(ID)**를 선택합니다.

단계 **2** 다음 중 하나를 수행합니다.

- 새 규칙을 생성하려면 + 버튼을 클릭합니다.
- 기존 규칙을 수정하려면 해당 규칙의 수정 아이콘()을 클릭합니다.

더 이상 필요하지 않은 규칙을 삭제하려면 해당 규칙의 삭제 아이콘()을 클릭합니다.

단계 **3** 순서에서 순서가 지정된 규칙 목록에 규칙을 삽입할 위치를 선택합니다.
규칙은 처음 일치하는 항목을 기준으로 적용되므로, 매우 구체적인 트래픽 일치 기준이 포함된 규칙이 보다 일반적인 기준이 포함된 정책(규칙이 일치하지 않는 경우 일치하는 트래픽에 적용됨) 위에 표시되도록 삽입해야 합니다.

기본적으로는 규칙이 목록의 끝에 추가됩니다. 나중에 규칙의 위치를 변경하려는 경우 이 옵션을 수정합니다.

단계 **4** 사용자 인증의 유형을 선택합니다.

- 활성 - 액티브 인증을 통해 사용자 ID를 확인합니다. 액티브 인증은 HTTP 트래픽에만 적용됩니다. 다른 트래픽 유형이 액티브 인증을 요구하거나 허용하는 ID 정책과 일치하는 경우에는 액티브 인증을 시도하지 않습니다.

- 인증 없음 - 사용자 ID를 가져오지 않습니다. 이 트래픽에는 ID 기반 액세스 규칙이 적용되지 않습니다. 이러한 사용자는 인증 필요 없음으로 표시됩니다.

단계 **5** (액티브 인증에만 해당됨) 디렉터리 서버에서 지원하는 인증 방법(유형)을 선택합니다.

- **HTTP** 기본 - 암호화되지 않은 HTTP BA(기본 인증) 연결을 통해 사용자를 인증합니다. 사용자는 브라우저의 기본 인증 팝업 창을 통해 네트워크에 로그인합니다. 이는 기본값입니다.
- **NTLM** - NTLM(NT LAN Manager) 연결을 통해 사용자를 인증합니다. 이 선택 사항은 AD 영역을 선택할 때만 사용 가능합니다. 사용자가 브라우저의 기본 인증 팝업 창을 통해 네트워크에 로그인합니다. 그러나 사용자가 Windows 도메인 로그인을 통해 투명하게 인증을 하도록 IE 및 Firefox 브라우저를 구성할 수 있습니다(Transparent 사용자 인증 사용, 137 페이지 참조).
- **HTTP** 협상 - 디바이스가 사용자 에이전트(사용자가 트래픽 흐름을 시작하는 데 사용 중인 애플리케이션)와 Active Directory 서버 간에 방법을 협상할 수 있도록 합니다. 협상 시에는 일반적으로 지원되는 가장 강력한 방법이 순서대로 사용됩니다(NTLM -> 기본). 사용자는 브라우저의 기본 인증 팝업 창을 통해 네트워크에 로그인합니다.
- **HTTP** 대응 페이지 - 시스템 제공 웹 페이지를 통해 인증하라는 메시지를 사용자에게 표시합니다. 이 방법은 일종의 HTTP 기본 인증입니다.

참고 HTTP 기본, HTTP 대응 페이지 및 NTLM 인증 방법의 경우 사용자는 인터페이스의 IP 주소를 사용하여 종속 포털로 리디렉션됩니다. 그러나 HTTP 협상의 경우에는 사용자가 정규화된 DNS 이름 *firewall-hostname.AD-domain-name*을 사용하여 리디렉션됩니다. HTTP 협상을 사용하려는 경우에는 DNS 서버도 업데이트하여 활성 인증을 수행해야 하는 모든 내부 인터페이스의 IP 주소에 이 이름을 매핑해야 합니다. 이렇게 하지 않으면 리디렉션을 완료할 수 없으며 사용자가 인증할 수 없습니다.

단계 **6** (액티브 인증에만 해당됨) 액티브 인증에서 장애가 발생하는 사용자에게 게스트 사용자 레이블을 지정할지를 결정하려면 **Fall Back as Guest**(게스트로 폴백) > **On/Off**(켜기/끄기)를 선택합니다.
사용자에게는 3번의 인증 기회가 제공됩니다. 인증에서 장애가 발생하면 이 옵션의 선택 여부에 따라 사용자 표시 방법이 결정됩니다. 이러한 값을 기준으로 액세스 규칙을 작성할 수 있습니다.

- **Fall Back as Guest**(게스트로 폴백) > **On**(켜기) - 사용자가 게스트로 표시됩니다.
- **Fall Back as Guest**(게스트로 폴백) > **Off**(끄기) - 사용자가 실패한 인증으로 표시됩니다.

단계 **7** **Source/Destination**(원본/대상) 탭에서 트래픽 일치 기준을 정의합니다.
HTTP 트래픽에 대해서만 액티브 인증을 시도합니다. 그러므로 비 HTTP 트래픽에 대해서는 인증 없음 규칙을 구성할 필요가 없으며 액티브 인증 규칙을 생성할 필요도 없습니다.

ID 규칙의 원본/대상 기준은 트래픽이 통과하는 보안 영역(인터페이스), IP 주소나 IP 주소의 국가나 대륙(지리적 위치) 또는 트래픽에서 사용되는 프로토콜과 포트를 정의합니다. 기본값은 모든 영역, 주소, 지리적 위치, 프로토콜 및 포트입니다.

조건을 수정하려면 해당 조건 내의 + 버튼을 클릭하고 필요한 개체나 요소를 선택한 후에 팝업 대화상자에서 **OK**(확인)를 클릭합니다. 기준에 개체가 필요한데 필요한 개체가 없는 경우에는 새 개체 생성을 클릭하면 됩니다. 개체 또는 요소의 **x**를 클릭하면 정책에서 해당 개체나 요소를 제거할 수 있습니다.

다음과 같은 트래픽 일치 기준을 구성할 수 있습니다.

원본 영역, 대상 영역

트래픽이 통과하는 인터페이스를 정의하는 보안 영역 개체입니다. 기준은 하나 또는 둘 다 정의할 수도 있고 둘 다 정의하지 않을 수도 있습니다. 지정되지 않은 기준은 임의 인터페이스의 트래픽에 적용됩니다.

- 영역 내 인터페이스의 디바이스에서 나가는 트래픽에 일치시키기 위해서는 대상 영역에 해당 영역을 추가합니다.
- 영역 내 인터페이스를 통해 디바이스로 들어오는 트래픽에 일치시키기 위해서는 소스 영역에 해당 영역을 추가합니다.
- 규칙에 소스와 대상 영역 조건을 모두 추가한 경우, 일치하는 트래픽은 반드시 지정된 소스 영역 중 하나에서 발생해야 하며 대상 영역 중 하나를 통해 전송되어야 합니다.

트래픽이 디바이스로 들어오거나 디바이스에서 나가는 위치를 기준으로 규칙을 적용해야 하는 경우 이 기준을 사용해야 합니다. 예를 들어 내부 네트워크에서 생성되는 모든 트래픽에서 사용자 ID를 수집하려는 경우 내부 영역을 원본 영역으로 선택하고 대상 영역은 비워 둡니다.

원본 네트워크, 대상 네트워크

트래픽의 네트워크 주소나 위치를 정의하는 네트워크 개체 또는 지리적 위치입니다.

- 특정 IP 주소 또는 지리적 위치에서 나오는 트래픽을 일치시키려면 소스 네트워크를 구성합니다.
- 특정 IP 주소 또는 지리적 위치로 향하는 트래픽을 일치시키려면 대상 네트워크를 구성합니다.
- 규칙에 소스와 대상 네트워크 조건을 모두 추가한 경우, 일치하는 트래픽은 반드시 지정된 IP 주소 중 하나에서 발생해야 하며 그 목적지가 대상 IP 주소 중 하나여야 합니다.

이 기준을 추가할 때는 다음 탭에서 선택합니다.

- 네트워크 - 제어하려는 트래픽의 소스 또는 대상 IP 주소를 정의하는 네트워크 개체 또는 그룹을 선택합니다.
- 지리위치 - 소스 또는 대상 국가나 대륙을 기준으로 트래픽을 제어하려면 지리적 위치를 선택합니다. 대륙을 선택하면 대륙 내의 모든 국가가 선택됩니다. 규칙에서 지리적 위치를 직접 선택하는 방법 외에, 위치를 정의하기 위해 생성한 지리위치 개체를 선택할 수도 있습니다. 지리적 위치를 사용하면 특정 국가에서 사용될 수 있는 모든 IP 주소를 몰라도 해당 국가에 대한 액세스를 쉽게 제한할 수 있습니다.

  참고 최신 지리적 위치 데이터를 사용하여 트래픽을 필터링하려면 GeoDB(지리위치 데이터베이스)를 정기적으로 업데이트하는 것이 좋습니다.

원본 포트, 대상 포트/프로토콜

트래픽에 사용되는 프로토콜을 정의하는 포트 개체입니다. TCP/UDP의 경우 여기에는 포트가 포함될 수 있습니다.

- 특정 프로토콜이나 포트에서 나오는 트래픽을 일치시키려면 원본 포트를 구성합니다. 소스 포트는 TCP/UDP 전용일 수 있습니다.
- 특정 프로토콜이나 포트로 향하는 트래픽을 일치시키려면 대상 포트/프로토콜을 구성합니다.
- 특정 TCP/UDP 포트에서 발생하는 트래픽과 특정 TCP/UDP 포트로 향하는 트래픽을 모두 일치시키려면 두 포트를 모두 구성합니다. 조건에 소스 및 대상 포트를 모두 추가한 경우, 단일 전송 프로토콜(TCP 또는 UDP)을 공유하는 포트만 추가할 수 있습니다. 예를 들어 포트 TCP/80에서 포트 TCP/8080으로 이동하는 트래픽을 대상으로 지정할 수 있습니다.

단계 **8** **OK(**확인**)**를 클릭합니다.

Transparent 사용자 인증 사용

액티브 인증을 허용하도록 ID 정책을 구성하는 경우 다음 인증 방법을 통해 사용자 ID를 가져올 수 있습니다.

HTTP 기본

HTTP 기본 인증을 사용하는 경우 사용자에게 디렉터리 사용자 이름과 비밀번호를 사용하여 인증하라는 메시지가 항상 표시됩니다. 비밀번호는 일반 텍스트로 전송됩니다. 그러므로 기본 인증은 안전한 인증 형식으로 간주되지 않습니다.

기본은 기본적으로 사용되는 인증 메커니즘입니다.

HTTP 대응 페이지

사용자에게 로그인 브라우저 페이지가 표시되는 HTTP 기본 인증 유형입니다.

NTLM, HTTP 협상(Active Directory용 Windows 통합 인증)

Windows 통합 인증을 사용할 때는 사용자가 워크스테이션을 사용하기 위해 도메인에 로그인하는 방식을 활용합니다. 브라우저는 서버에 액세스할 때 이 도메인 로그인 사용을 시도합니다(액티브 인증 중의 Firepower Threat Defense 캡티브 포털 포함). 비밀번호는 전송되지 않습니다. 인증이 성공하면 사용자는 Transparent 방식으로 인증되므로 인증 과정이 수행되었는지 또는 처리되었는지를 알 수 없습니다.

브라우저가 도메인 로그인 크리덴셜을 사용하여 인증 요청을 처리할 수 없으면 사용자에게 사용자 이름과 비밀번호를 입력하라는 메시지가 표시됩니다. 이러한 방식은 기본 인증과 동일한 사용자 환경입니다. 따라서 Windows 통합 인증을 구성하는 경우에는 사용자가 같은 도메인의 네트워크나 서버에 액세스할 때 크리덴셜을 입력해야 할 필요가 감소합니다.

HTTP 협상은 Active Directory 서버와 사용자 에이전트에서 모두 지원하는 가장 강력한 방법을 선택합니다. 협상에서 인증 방법으로 HTTP 기본을 선택하는 경우에는 Transparent 인증 기능이 제공되지 않습니다. 강도의 순서는 NTLM, 기본입니다. Transparent 인증을 수행하려면 협상에서 NTLM을 선택해야 합니다.

Transparent 인증을 사용하려면 클라이언트 브라우저가 Windows 통합 인증을 지원하도록 구성해야 합니다. 다음 섹션에서는 Windows 통합 인증을 지원하는 흔히 사용되는 몇 가지 브라우저에 대한 Windows 통합 인증의 일반적인 요건 및 기본 컨피그레이션에 대해 설명합니다. 사용되는 기술은 소프트웨어 릴리스 간에 변경될 수 있으므로, 사용자는 사용 중인 브라우저나 다른 사용자 에이전트의 도움말을 참조해야 합니다.

팁 모든 브라우저에서 Windows 통합 인증을 지원하는 것은 아닙니다. 예를 들어 이 문서를 작성하는 시점의 버전을 기준으로 할 때 Chrome 및 Safari와 같은 브라우저는 해당 인증을 지원하지 않습니다. 이러한 브라우저의 경우 사용자에게 사용자 이름과 비밀번호를 입력하라는 메시지가 표시됩니다. 브라우저 설명서를 참조하여 사용 중인 버전에서 지원되는지 확인하십시오.

Transparent 인증 요구사항

사용자는 Transparent 인증을 구현하도록 브라우저 또는 사용자 에이전트를 구성해야 합니다. 이 작업은 사용자가 개별적으로 수행할 수도 있고, 관리자가 사용자를 위해 브라우저 또는 사용자 에이전트를 구성한 다음 소프트웨어 배포 툴을 사용해 클라이언트 워크스테이션으로 해당 컨피그레이션을 푸시할 수도 있습니다. 사용자가 이 작업을 직접 수행하도록 하는 경우 네트워크에서 사용되는 특정 컨피그레이션 매개변수를 제공해야 합니다.

브라우저 또는 사용자 에이전트와 관계없이 다음과 같은 일반 컨피그레이션을 구현해야 합니다.

- 사용자가 네트워크에 연결하는 데 사용하는 Firepower Threat Defense 인터페이스를 신뢰할 수 있는 사이트 목록에 추가합니다. IP 주소를 사용할 수도 있고, 사용 가능한 경우 inside.example.com과 같은 FQDN(Fully Qualified Domain Name)을 사용할 수도 있습니다. 와일드카드 또는 부분 주소를 사용하여 일반화된 신뢰할 수 있는 사이트를 생성할 수도 있습니다. 예를 들어, 일반적으로 *.example.com 또는 단순히 example.com을 사용하여 모든 내부 사이트를 포함하면 네트워크의 모든 서버를 신뢰할 수 있습니다(자신의 도메인 이름을 사용). 인터페이스의 특정 주소를 추

가하는 경우에는 모든 사용자 액세스 포인트가 네트워크를 가리키도록 신뢰할 수 있는 사이트에 여러 주소를 추가해야 할 수 있습니다.

- Windows 통합 인증은 프록시 서버를 통해 작동하지 않습니다. 따라서 프록시를 사용하지 않거나, 프록시를 통과하지 않도록 제외되는 주소에 Firepower Threat Defense 인터페이스를 추가해야 합니다. 프록시를 사용해야 하도록 결정하는 경우에는 NTLM을 사용하더라도 사용자에게 인증하라는 메시지가 표시됩니다.

팁 Transparent 인증은 반드시 구성해야 하는 것은 아니며 최종 사용자의 편의를 위해 구성하는 기능입니다. Transparent 인증을 구성하지 않으면 모든 인증 방법에서 사용자에게 로그인 과정이 제공됩니다.

Transparent 인증을 위해 **Internet Explorer** 구성

NTLM Transparent 인증을 위해 Internet Explorer를 구성하려면 다음 단계를 수행합니다.

절차

단계 **1** **Tools(**도구**) > Internet Options(**인터넷 옵션**)**을 선택합니다.

단계 **2** **Security(**보안**)** 탭과 **Local Intranet(**로컬 인트라넷**)** 영역을 차례로 선택하고 다음을 수행합니다.

a) **Sites(**사이트**)** 버튼을 클릭하여 신뢰할 수 있는 사이트 목록을 엽니다.

b) 다음 옵션 중 하나 이상이 선택되어 있는지 확인합니다.

- 인트라넷 네트워크를 자동으로 검색. 이 옵션을 선택하면 다른 옵션은 모두 비활성화됩니다.
- 프록시 서버를 건너뛰는 사이트를 모두 포함

c) **Advanced(**고급**)**를 클릭하여 로컬 인트라넷 사이트 대화 상자를 열고 신뢰하려는 URL을 **Add Site(**사이트 추가**)** 상자에 붙여넣은 후에 **Add(**추가**)**를 클릭합니다.
URL이 두 개 이상인 경우 이 프로세스를 반복합니다. 부분 URL을 지정하려면 와일드카드를 사용합니다. 예를 들어 http://*.example.com과 같이 입력할 수도 있고 *.example.com만 입력할 수도 있습니다.

대화 상자를 닫고 인터넷 옵션 대화 상자로 돌아옵니다.

d) 로컬 인트라넷을 계속 선택한 상태로 사용자 지정 레벨을 클릭하여 보안 설정 대화 상자를 엽니다. **User Authentication(**사용자 인증**)** > **Logon(**로그온**)** 설정을 찾아서 인트라넷 영역에서만 자동으로 로그온을 선택합니다. **OK(**확인**)**를 클릭합니다.

단계 **3** 인터넷 옵션 대화 상자에서 **Connections(**연결**)** 탭을 클릭한 다음 **LAN Settings(LAN** 설정**)**를 클릭합니다.
LAN에 프록시 서버 사용이 선택되어 있으면 Firepower Threat Defense 인터페이스가 프록시를 건너뛰는지 확인해야 합니다. 이렇게 하려면 다음 중 적절한 작업을 수행합니다.

- 로컬 주소에 프록시 서버 건너뛰기를 선택합니다.

- 고급을 클릭하고 다음으로 시작하는 주소에는 프록시 서버 사용 안 함 상자에 주소를 입력합니다. *.example.com과 같은 와일드카드를 사용할 수 있습니다.

Transparent 인증을 위해 Firefox 구성

NTLM Transparent 인증을 위해 Firefox를 구성하려면 다음 단계를 수행합니다.

절차

단계 **1** **about:config**를 엽니다. 필터 막대를 사용하여 수정해야 하는 기본 설정을 찾습니다.

단계 **2** NTLM을 지원하려면 다음 기본 설정을 수정합니다(network.automatic으로 필터링).

- **network.automatic-ntlm-auth.trusted-uris** - 기본 설정을 더블 클릭하고 URL을 입력한 후에 **OK(**확인**)**를 클릭합니다. URL이 여러 개이면 쉼표로 구분하여 입력할 수 있습니다. 프로토콜은 원하는 경우 입력하면 됩니다. 예를 들면 다음과 같습니다.

  ```
  http://host.example.com, http://hostname, myhost.example.com
  ```

  부분 URL을 사용할 수도 있습니다. Firefox는 임의 하위 문자열이 아닌 문자열 끝이 일치하는지를 확인합니다. 그러므로 도메인 이름만 지정하여 전체 내부 네트워크를 포함할 수 있습니다. 예를 들면 다음과 같습니다.

  ```
  example.com
  ```

- **network.automatic-ntlm-auth.allow-proxies** - 값이 기본값인 **true**인지 확인합니다. 값이 현재 false인 경우 더블 클릭하여 값을 변경합니다.

단계 **3** HTTP 프록시 설정을 확인합니다. **Tools(**툴**)** > **Options(**옵션**)**를 선택한 다음 옵션 대화 상자의 **Network(**네트워크**)** 탭을 클릭하여 이러한 옵션을 찾을 수 있습니다. 연결 그룹에서 **Settings(**설정**)** 버튼을 클릭합니다.

- 프록시 없음이 선택되어 있으면 구성할 항목이 없는 것입니다.
- 시스템 프록시 설정 사용이 선택되어 있으면 about:config에서 **network.proxy.no_proxies_on** 속성을 수정하여 **network.automatic-ntlm-auth.trusted-uris**에 포함한 신뢰할 수 있는 URI를 추가해야 합니다.
- 수동 프록시 컨피그레이션이 선택되어 있으면 이러한 신뢰할 수 있는 URI가 포함되도록 프록시 없음 목록을 업데이트합니다.
- 다른 옵션 중 하나가 선택되어 있으면 해당 컨피그레이션에 사용되는 속성에서 동일한 신뢰할 수 있는 URI가 제외되는지를 확인합니다.

ID 정책 모니터링

인증이 필요한 ID 정책이 올바르게 작동하는 경우 **Monitoring(**모니터링**)** > **Users(**사용자**)** 대시보드와 사용자 정보를 포함하는 기타 대시보드에 사용자 정보가 표시됩니다.

또한, **Monitoring(**모니터링**)** > **Events(**이벤트**)**에 표시되는 이벤트에 사용자 정보가 포함됩니다.

사용자 정보가 표시되지 않으면 디렉터리 서버가 올바르게 작동하고 있는지 확인하십시오. 연결을 확인하려면 디렉터리 서버 컨피그레이션 대화 상자의 **Test(**테스트**)** 버튼을 사용합니다.

디렉터리 서버가 작동 중이며 사용 가능한 경우 인증이 필요한 ID 규칙의 기준과 일치하는 트래픽이 사용자와 일치하는 방식으로 작성되어 있는지 확인합니다. 예를 들어 사용자 트래픽이 디바이스에 진입하는 경로로 사용되는 인터페이스가 소스 영역에 포함되어 있는지 확인합니다.

ID 규칙은 HTTP 트래픽에만 일치하므로 사용자는 디바이스를 통해 이 트래픽 유형을 전송해야 합니다.

9 장

액세스 제어

다음 주제에서는 액세스 제어 규칙에 대해 설명합니다. 이러한 규칙은 디바이스를 통과할 수 있는 트래픽을 제어하며 침입 검사와 같은 고급 서비스를 트래픽에 적용합니다.

액세스 제어 개요

다음 항목에서는 액세스 제어 정책에 대해 설명합니다.

액세스 제어 규칙 및 기본 작업

액세스 정책을 사용하여 네트워크 리소스에 대한 액세스를 제어합니다. 이 정책은 하향식으로 평가되는 순서가 지정된 규칙 집합으로 구성됩니다. 트래픽에 적용되는 규칙은 모든 트래픽 기준이 일치하는 첫 번째 규칙입니다.

다음을 기준으로 하여 액세스를 제어할 수 있습니다.

- 소스 및 대상 IP 주소, 프로토콜, 포트 및 인터페이스와 같은 기존 네트워크 특성(보안 영역 형식)
- 사용 중인 애플리케이션. 특정 애플리케이션을 기반으로 액세스를 제어할 수도 있고, 애플리케이션의 범주, 특정 특성으로 태그가 지정된 애플리케이션, 애플리케이션의 유형(클라이언트, 서버, 웹) 또는 애플리케이션의 위험이나 사업 타당성 등급을 포함하는 규칙을 생성할 수도 있습니다.
- 일반화된 URL 범주를 포함한 웹 요청의 대상 URL. 대상 사이트의 공개 평판에 따라 일치하는 범주를 세분화할 수 있습니다.
- 요청을 하는 사용자 또는 사용자가 속한 사용자 그룹

허용한 암호화되지 않은 트래픽에 대해 IPS 검사를 적용하여 위협을 확인하고 공격으로 보이는 트래픽을 차단할 수 있습니다. 또한 파일 정책을 사용하여 금지된 파일이나 악성코드를 확인할 수도 있습니다.

액세스 규칙과 일치하지 않는 모든 트래픽은 액세스 제어 기본 작업에 의해 처리됩니다. 기본적으로 트래픽을 허용하는 경우 트래픽에 IPS 검사를 적용할 수 있습니다. 그러나 기본 작업에 의해 처리되는 트래픽에 대해서는 파일 또는 악성코드 검사를 수행할 수 없습니다.

애플리케이션 필터링

액세스 제어 규칙을 사용하여 연결에 사용되는 애플리케이션을 기반으로 트래픽을 필터링할 수 있습니다. 시스템은 수많은 애플리케이션을 인식할 수 있으므로 모든 웹 애플리케이션을 차단하지 않고 웹 애플리케이션 하나만 차단하는 방법을 알아낼 필요가 없습니다.

널리 사용되는 몇 가지 애플리케이션의 경우 애플리케이션의 여러 측면을 필터링할 수 있습니다. 예를 들어 Facebook 전체를 차단하지 않고 Facebook Games만 차단하는 규칙을 생성할 수 있습니다.

일반 애플리케이션 특성을 기반으로 하는 규칙을 생성할 수도 있습니다. 그러면 위험 또는 사업 타당성, 유형, 범주 또는 태그를 선택하여 전체 애플리케이션 그룹을 차단하거나 허용할 수 있습니다. 그러나 애플리케이션 필터에서 범주를 선택할 때는 원치 않는 애플리케이션이 포함되지 않도록 일치하는 애플리케이션 목록을 확인해야 합니다. 가능한 그룹화에 대한 자세한 설명은 애플리케이션 기준, 154 페이지를 참조하십시오.

애플리케이션 필터링에는 몇 가지 주의해야 하는 제한이 있습니다. 이와 같은 제한에 대한 설명은 애플리케이션 제어의 제한, 162 페이지에 나와 있습니다. 그중에서도 암호화된 트래픽에 대한 제한에 특히 주의해야 합니다.

애플리케이션이 HTTPS 연결과 같은 암호화를 사용하는 경우에는 시스템이 애플리케이션을 식별하지 못할 수도 있습니다. 애플리케이션 필터 대화 상자를 사용하여 다음 태그를 선택한 후에 애플리케이션 목록을 검사하여 애플리케이션에서 암호 해독이 필요한지 확인합니다.

- **SSL** 프로토콜 - SSL 프로토콜로 태그가 지정된 트래픽은 암호를 해독할 필요가 없습니다. 시스템은 이 트래픽을 인식할 수 있으며 액세스 제어 작업을 적용할 수 있습니다. 나열된 애플리케이션에 대한 액세스 제어 규칙이 필요한 연결과 일치하는지를 확인해야 합니다.
- 암호 해독된 트래픽 - 트래픽을 먼저 암호 해독해야 시스템이 해당 트래픽을 인식할 수 있습니다. Firepower Device Manager를 사용하여 SSL 암호 해독을 구성할 수는 없으므로 이와 같은 애플리케이션에 대한 액세스 제어 규칙은 실행되지 않습니다. 예를 들어 이 문서를 작성하는 시점에서 Dropbox에는 이 태그가 적용되어 있습니다. 따라서 Dropbox 애플리케이션에 대한 액세스 규칙은 Dropbox 연결과 일치하지 않습니다.

URL 필터링

URL 조건은 네트워크의 사용자가 액세스할 수 있는 웹 사이트를 제어합니다. 이 기능을 *URL* 필터링이라고 합니다.

다음 기술을 사용하여 URL 필터링을 구현할 수 있습니다.

- 범주 및 평판 기반 URL 필터링 - URL 필터링 라이선스를 사용하면 URL의 일반 분류(범주) 및 위험 레벨(평판)을 기준으로 웹 사이트에 대한 액세스를 제어할 수 있습니다.
- 수동 URL 필터링 - 임의의 라이선스를 사용하여 개별 URL과 URL 그룹을 수동으로 지정해 웹 트래픽을 맞춤형 방식으로 더 상세하게 제어할 수 있습니다.

다음 항목에서는 URL 필터링에 대해 자세히 설명합니다.

평판 기반 **URL** 필터링

ULR 필터링 라이선스가 있으면 요청한 URL의 범주 및 평판을 기준으로 웹 사이트에 대한 액세스를 제어할 수 있습니다.

- 범주 - URL의 일반 분류입니다. 예를 들어 ebay.com은 경매 범주에 속하고 monster.com은 구직 범주에 속합니다. 하나의 URL이 여러 카테고리에 속할 수 있습니다.
- 평판 - URL이 사용자가 속한 조직의 보안 정책에 어긋나는 용도로 사용될 가능성입니다. 평판의 범위는 높은 위험(레벨 1)~잘 알려짐(레벨 5)입니다.

참고 이벤트 및 애플리케이션 세부사항에서 URL 범주 및 평판 정보를 확인하려면 URL 조건을 사용하여 규칙을 하나 이상 생성해야 합니다. 또한 최신 위협 인텔리전스를 가져올 수 있도록 Cisco CSI(Collective Security Intelligence)와의 통신을 활성화해야 합니다.

평판 기반 **URL** 필터링의 이점

URL 범주 및 평판을 사용하면 URL 필터링을 빠르게 구성할 수 있습니다. 예를 들어, 액세스 제어를 사용해 남용 약물 범주에서 높은 위험의 URL을 차단할 수 있습니다.

범주 및 평판 데이터를 사용하면 정책 생성 및 관리가 간소화됩니다. 이를 통해 시스템이 웹 트래픽을 정상적으로 제어할 수 있습니다. Cisco에서는 새로운 URL 및 기존 URL에 대한 새 범주와 위험을 포함하여 위협 인텔리전스를 지속적으로 업데이트하므로 시스템이 최신 정보를 사용하여 요청된 URL을 필터링할 수 있습니다. 보안 위협을 나타내거나 부적절한 콘텐츠를 제공하는 사이트가 나타나고 사라지는 속도는 새 정책을 업데이트하고 구축하는 속도보다 빠를 수 있습니다.

시스템을 조정할 수 있는 방법의 몇 가지 예는 다음과 같습니다.

- 액세스 제어 규칙이 모든 게임 사이트를 차단하는 경우, 새로운 도메인이 게임으로 등록되고 분류되면 시스템은 해당 사이트를 자동으로 차단할 수 있습니다.
- 액세스 제어 규칙이 모든 악성코드 사이트를 차단하는 경우, 블로그 페이지 하나가 악성코드에 감염되면 시스템은 블로그의 URL을 악성코드로 재분류하고 해당 사이트를 차단할 수 있습니다.
- 액세스 제어 규칙이 높은 위험의 소셜 네트워킹 사이트를 차단하고 누군가가 악성 페이로드 링크를 포함하는 프로필 페이지에 링크를 게시하는 경우, 시스템은 해당 페이지의 평판을 일반 사이트에서 높은 위험으로 변경하고 해당 페이지를 차단할 수 있습니다.

수동 **URL** 필터링

액세스 제어 규칙에서는 개별 URL 또는 URL 그룹을 수동으로 필터링하여 범주 및 평판 기반 URL 필터링을 보완하거나 선택적으로 재정의할 수 있습니다. 이러한 유형의 URL 필터링을 수행하는 데는 특별한 라이선스가 필요하지 않습니다.

예를 들어 액세스 제어를 사용하여 조직에 적합하지 않은 웹 사이트 범주를 차단할 수 있습니다. 그러나 해당 범주에 액세스 권한을 제공하려는 적절한 웹 사이트가 포함된 경우에는 해당 사이트용으로 수동 허용 규칙을 생성한 다음 범주에 대한 차단 규칙 앞에 배치할 수 있습니다.

특정 URL을 수동으로 필터링할 때는 영향을 받을 수 있는 다른 트래픽을 신중하게 고려하십시오. URL 조건이 네트워크 트래픽과 일치하는지 확인하기 위해 시스템은 간단한 부분 문자열 일치를 실행합니다. 요청한 URL은 문자열의 일부분과 일치하는 경우 일치 항목으로 간주됩니다.

예를 들어, example.com의 모든 트래픽을 허용하는 경우, 사용자는 다음을 포함하는 URL을 찾아볼 수 있습니다.

- http://example.com/
- http://example.com/newexample
- http://www.example.com/

다른 예로, ign.com(게임 사이트)의 차단을 명시적으로 원하는 경우의 차단 시나리오를 생각해 보십시오. 그러나 하위 문자열 일치 시에는 ign.com을 차단하면 원래 의도와는 달리 verisign.com도 차단됩니다.

HTTPS 트래픽 필터링

시스템은 암호화된 트래픽을 필터링하기 위해 SSL 핸드셰이크 중에 전달된 정보(트래픽을 암호화하는 데 사용된 공개 키 인증서의 주체 공용 이름)를 기준으로 요청된 URL을 확인합니다.

HTTP 필터링과 달리, HTTPS 필터링은 주체 공용 이름 내의 서브도메인을 무시합니다. 에서 HTTPS URL을 수동으로 필터링할 경우 서브도메인 정보를 포함하지 마십시오. 이를테면 www.example.com 대신 example.com을 사용하십시오.

암호화 프로토콜을 통해 트래픽 제어

시스템은에서 URL 필터링을 수행할 때 암호화 프로토콜(HTTP 또는 HTTPS)을 무시합니다. 이는 수동 및 평판 기반 URL 조건 모두에 해당됩니다. 즉, URL 필터링에서는 다음 웹 사이트에 대한 트래픽을 동일하게 처리합니다.

- http://example.com/
- https://example.com/

HTTP 또는 HTTPS 트래픽에만 일치하는 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.

작업: 허용
애플리케이션: HTTPS
URL: example.com

두 번째 규칙은 동일한 웹 사이트에 대한 HTTP 액세스를 차단합니다.

작업: 차단
애플리케이션: HTTP
URL: example.com

웹 사이트를 차단할 때 사용자에게 표시되는 내용

URL 필터링 규칙을 사용하여 웹 사이트를 차단할 때 사용자에게 표시되는 내용은 사이트가 암호화되어 있는지에 따라 달라집니다.

- HTTP 연결 - 사용자에게는 시간이 초과되거나 재설정된 연결의 경우에 표시되는 일반적인 브라우저 페이지가 아닌 시스템 기본 차단 응답 페이지가 표시됩니다. 이 페이지에서는 연결이 의도적으로 차단되었다는 내용이 명확하게 표시됩니다.
- HTTPS(암호화된) 연결 - 사용자에게 시스템 기본 차단 응답 페이지가 표시되지 않습니다. 대신 보안 연결 실패를 나타내는 브라우저의 기본 페이지가 표시됩니다. 오류 메시지는 사이트가 정책으로 인해 차단되었음을 나타내지 않습니다. 대신 일반적인 암호화 알고리즘이 없다는 오류가 표시될 수 있습니다. 이 메시지만으로는 연결이 의도적으로 차단되었는지를 명확하게 파악할 수 없습니다.

또한, 명시적 URL 필터링 규칙이 아닌 다른 액세스 제어 규칙이나 기본 작업에 의해 웹 사이트가 차단될 수도 있습니다. 예를 들어 전체 네트워크 또는 지리위치를 차단하는 경우 해당 네트워크나 지리위치의 웹 사이트도 모두 차단됩니다. 이러한 규칙으로 인해 차단된 사용자에게는 아래 제한에서 설명하는 응답 페이지가 표시될 수도 있고 표시되지 않을 수도 있습니다.

URL 필터링을 구현할 때는 사이트가 의도적으로 차단될 때 표시될 수 있는 내용 및 차단 대상 사이트 유형을 최종 사용자에게 설명하는 것이 좋습니다. 그렇지 않으면 최종 사용자가 차단된 연결의 트러블슈팅을 수행하는 데 오랜 시간을 쓸 수 있습니다.

HTTP 대응 페이지의 제한

시스템에서 웹 트래픽을 차단할 때 HTTP 대응 페이지가 항상 표시되는 것은 아닙니다.

- 승격된 액세스 제어 규칙(단순한 네트워크 조건만 사용하여 초기에 배치된 차단 규칙)으로 인해 웹 트래픽이 차단될 때는 시스템에서 응답 페이지를 표시하지 않습니다.
- 시스템에서 요청된 URL을 식별하기 전에 웹 트래픽이 차단되면 시스템은 응답 페이지를 표시하지 않습니다.
- 액세스 제어 규칙에 의해 차단되는 암호화된 연결에 대해서는 시스템이 응답 페이지를 표시하지 않습니다.

침입, 파일 및 악성코드 검사

침입 정책 및 파일 정책은 트래픽이 원하는 대상에 도달하도록 허용하기 전에 최종 방어선으로 함께 사용됩니다.

- 침입 정책은 시스템의 침입 방지 기능을 제어합니다.
- 파일 정책은 시스템의 파일 제어 및 AMP for Firepower 기능을 제어합니다.

기타 모든 트래픽 처리는 네트워크 트래픽에서 침입, 금지된 파일 및 악성코드를 검사하기 전에 수행됩니다. 침입 또는 파일 정책을 액세스 제어 규칙과 연결하여 시스템이 액세스 제어 규칙의 조건과 일치하는 트래픽을 통과시키기 전에 침입 정책이나 파일 정책 또는 두 정책을 모두 사용하여 트래픽을 먼저 검사하도록 명령할 수 있습니다.

트래픽을 허용하는 규칙에 대해서만 침입 및 파일 정책을 구성할 수 있습니다. 트래픽을 신뢰 또는 차단하도록 설정된 규칙에 대해서는 검사가 수행되지 않습니다. 또한, 액세스 제어 정책의 기본 작업이 허용이면 침입 정책은 구성할 수 있지만 파일 정책은 구성할 수 없습니다.

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. 세션에서 파일이 탐지되고 차단될 때까지, 세션의 패킷은 침입 검사 대상이 될 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. 검사는 암호화되지 않은 트래픽에 대해서만 작동합니다.

NAT 및 액세스 규칙

NAT를 구성한 경우라도, 액세스 규칙은 액세스 규칙 일치를 확인할 때 항상 실제 IP 주소를 사용합니다. 예를 들어 내부 서버 10.1.1.5가 외부에서 공개적으로 라우팅 가능한 IP 주소 209.165.201.5를 갖도록 NAT를 구성할 경우, 외부 트래픽이 내부 서버에 액세스하는 것을 허용하는 액세스 규칙은 서버의 매핑된 주소(209.165.201.5)가 아니라 실제 IP 주소(10.1.1.5)를 참조해야 합니다.

액세스 제어 정책 구성

액세스 제어 정책을 사용하여 네트워크 리소스에 대한 액세스를 제어합니다. 이 정책은 하향식으로 평가되는 순서가 지정된 규칙 집합으로 구성됩니다. 트래픽에 적용되는 규칙은 모든 트래픽 기준이 일치하는 첫 번째 규칙입니다. 트래픽과 일치하는 규칙이 없으면 페이지 맨 아래에 표시된 기본 작업이 적용됩니다.

액세스 제어 정책을 구성하려면 **Policies(**정책**)** > **Access Control(**액세스 제어**)**을 선택합니다.

액세스 제어 테이블에는 모든 규칙이 순서대로 나열됩니다. 각 규칙에 대해 다음을 수행합니다.

- 맨 왼쪽 열의 규칙 번호 옆에 있는 > 버튼을 클릭하여 규칙 다이어그램을 엽니다. 다이어그램을 통해 규칙이 어떻게 트래픽을 제어하는지 시각화할 수 있습니다. 버튼을 다시 클릭하여 다이어그램을 닫습니다.
- 대부분의 셀에서는 인라인 수정이 허용됩니다. 예를 들어, 작업을 클릭하여 다른 작업을 선택하거나 소스 네트워크 개체를 클릭하여 소스 기준을 추가 또는 변경할 수 있습니다.
- 규칙을 이동하려면 규칙 위에 마우스를 올려놓고 이동 아이콘()이 나타나면 이를 클릭하여 새 위치로 끌어 놓습니다. 규칙을 수정하고 순서 목록에서 새 위치를 선택하여 규칙을 이동할 수도 있습니다. 규칙은 처리할 순서대로 배치해야 합니다. 특정 규칙, 특히 더 일반적인 규칙에 대한 예외를 정의하는 규칙은 목록 위쪽에 있어야 합니다.
- 맨 오른쪽 열에는 규칙의 작업 버튼이 포함되어 있습니다. 셀 위에 마우스를 올려 놓으면 버튼이 표시됩니다. 규칙은 수정()하거나 삭제()할 수 있습니다.

다음 항목에서는 정책을 구성하는 방법을 설명합니다.

기본 작업 구성

특정 액세스 규칙과 일치하지 않는 연결은 액세스 제어 정책의 기본 작업에 의해 처리됩니다.

절차

단계 **1** **Policies**(정책) > **Access Control**(액세스 제어)을 선택합니다.

단계 **2** **Default Action**(기본 작업) 필드에서 아무 곳이나 클릭합니다.

단계 **3** 일치하는 트래픽에 적용할 작업을 선택합니다.

- 신뢰 - 어떤 종류든 추가 검사 없이 트래픽을 허용합니다.
- 허용 - 침입 정책이 적용되는 트래픽을 허용합니다.
- 차단 - 트래픽을 무조건 삭제합니다. 트래픽은 검사되지 않습니다.

단계 **4** 작업이 허용인 경우 침입 정책 아래에서 **Enable Policy**(정책 활성화) > **On**(켜기)을 선택하고 침입 정책을 선택합니다.
정책 옵션에 대한 설명은 침입 정책 설정, 157 페이지를 참조하십시오.

단계 **5** (선택 사항). 기본 작업에 대한 로깅을 구성합니다.
기본 작업과 일치하는 트래픽에 대한 로깅을 활성화해야 대시보드 데이터 또는 이벤트 뷰어에 해당 트래픽이 포함됩니다. 로깅 설정, 159 페이지을 참조하십시오.

단계 **6** **OK**(확인)를 클릭합니다.

액세스 제어 규칙 구성

액세스 제어 규칙을 사용하여 네트워크 리소스에 대한 액세스를 제어합니다. 액세스 제어 정책의 규칙은 위에서부터 아래로 평가됩니다. 트래픽에 적용되는 규칙은 모든 트래픽 기준이 일치하는 첫 번째 규칙입니다.

절차

단계 **1** **Policies**(정책) > **Access Control**(액세스 제어)을 선택합니다.

단계 **2** 다음 중 하나를 수행합니다.

- 새 규칙을 생성하려면 + 버튼을 클릭합니다.
- 기존 규칙을 수정하려면 해당 규칙의 수정 아이콘( )을 클릭합니다.

더 이상 필요하지 않은 규칙을 삭제하려면 해당 규칙의 삭제 아이콘( )을 클릭합니다.

단계 **3** 순서에서 순서가 지정된 규칙 목록에 규칙을 삽입할 위치를 선택합니다.
규칙은 처음 일치하는 항목을 기준으로 적용되므로, 매우 구체적인 트래픽 일치 기준이 포함된 규칙이 보다 일반적인 기준이 포함된 정책(규칙이 일치하지 않는 경우 일치하는 트래픽에 적용됨) 위에 표시되도록 삽입해야 합니다.

기본적으로는 규칙이 목록의 끝에 추가됩니다. 나중에 규칙의 위치를 변경하려는 경우 이 옵션을 수정합니다.

단계 **4** 제목에서 규칙의 이름을 입력합니다.
이름에는 공백을 포함할 수 없지만, 영숫자 및 특수 문자(+, ., _, -)는 사용할 수 있습니다.

단계 **5** 일치하는 트래픽에 적용할 작업을 선택합니다.

- 신뢰 - 어떤 종류든 추가 검사 없이 트래픽을 허용합니다.
- 허용 - 정책에서 침입 및 기타 검사 설정이 적용되는 트래픽을 허용합니다.
- 차단 - 트래픽을 무조건 삭제합니다. 트래픽은 검사되지 않습니다.

단계 **6** 다음 탭을 적절하게 조합하여 트래픽 일치 기준을 정의합니다.

- 원본/대상 - 트래픽이 통과하는 보안 영역(인터페이스), IP 주소/IP 주소의 국가나 대륙(지리적 위치) 또는 트래픽에서 사용되는 프로토콜과 포트입니다. 기본값은 모든 영역, 주소, 지리적 위치, 프로토콜 및 포트입니다. 소스/대상 기준, 151 페이지를 참조하십시오.
- 애플리케이션 - 유형, 범주, 태그, 위험, 사업 타당성에 따라 애플리케이션을 정의하는 필터 또는 애플리케이션입니다. 기본값은 모든 애플리케이션입니다. 애플리케이션 기준, 154 페이지를 참조하십시오.
- **URL** - 웹 요청의 URL 또는 URL 범주입니다. 기본값은 모든 URL입니다. URL 기준, 155 페이지를 참조하십시오.

- 사용자 - 사용자 또는 사용자 그룹입니다. ID 정책에 따라 트래픽 일치에 사용자 및 그룹 정보를 사용할 수 있는지가 결정됩니다. 이 기준을 사용하려면 ID 정책을 구성해야 합니다. 사용자 기준, 156 페이지를 참조하십시오.

조건을 수정하려면 해당 조건 내의 + 버튼을 클릭하고 필요한 개체나 요소를 선택한 후에 팝업 대화상자에서 **OK(**확인**)**를 클릭합니다. 기준에 개체가 필요한데 필요한 개체가 없는 경우에는 새 개체 생성을 클릭하면 됩니다. 개체 또는 요소의 **x**를 클릭하면 정책에서 해당 개체나 요소를 제거할 수 있습니다.

조건을 액세스 제어 규칙에 추가할 경우 다음 팁을 고려하십시오.

- 규칙마다 여러 조건을 구성할 수 있습니다. 규칙을 트래픽에 적용하려면 트래픽이 규칙의 모든 조건과 일치해야 합니다. 예를 들어 특정 호스트에 대해 URL 필터링을 수행하는 단일 규칙을 사용할 수 있습니다.
- 규칙의 각 조건에 대해 최대 50개의 기준을 추가할 수 있습니다. 조건의 기준 중 어느 것이든 모두 일치하는 트래픽은 조건을 만족합니다. 예를 들어, 최대 50개의 애플리케이션 또는 애플리케이션 필터에 대해 애플리케이션 제어를 적용하는 단일 규칙을 사용할 수 있습니다. 따라서 단일 조건의 항목 간 관계는 OR이고 조건 유형 간의 관계(예: 원본/대상과 애플리케이션 간의 관계)는 AND가 됩니다.
- 일부 기능을 사용하려면 적절한 라이선스를 활성화해야 합니다.

단계 **7** (선택 사항). 허용 작업을 사용하는 정책의 경우 암호화되지 않은 트래픽에 대한 추가 검사를 구성할 수 있습니다. 다음 링크 중 하나를 클릭합니다.

- 침입 정책 - **Intrusion Policy(**침입 정책**)** > **On(**켜기**)**을 선택하고 트래픽에서 침입과 익스플로잇을 검사할 IPS 침입 검사 정책을 선택합니다. 침입 정책 설정, 157 페이지를 참조하십시오.
- 파일 정책 - 트래픽에서 차단해야 하는 파일과 악성코드가 포함된 파일을 검사하기 위한 파일 정책을 선택합니다. 파일 정책 설정, 158 페이지를 참조하십시오.

단계 **8** (선택 사항). 규칙에 대해 로깅을 구성합니다.
기본적으로 규칙과 일치하는 트래픽에 대해서는 연결 이벤트가 생성되지 않습니다. 단, 파일 정책을 선택하면 파일 이벤트가 기본적으로 생성됩니다. 이 행동은 변경할 수 있습니다. 정책과 일치하는 트래픽에 대한 로깅을 사용하도록 설정해야 대시보드 데이터 또는 이벤트 뷰어에 해당 트래픽이 포함됩니다. 로깅 설정, 159 페이지을 참조하십시오.

단계 **9** **OK(**확인**)**를 클릭합니다.

소스/대상 기준

액세스 규칙의 소스/대상 기준은 트래픽이 통과하는 보안 영역(인터페이스), IP 주소나 IP 주소의 국가나 대륙(지리적 위치) 또는 트래픽에서 사용되는 프로토콜과 포트를 정의합니다. 기본값은 모든 영역, 주소, 지리적 위치, 프로토콜 및 포트입니다.

조건을 수정하려면 해당 조건 내의 + 버튼을 클릭하고 필요한 개체나 요소를 선택한 후에 **OK(**확인**)**를 클릭합니다. 기준에 개체가 필요한데 필요한 개체가 없는 경우에는 새 개체 생성을 클릭하면 됩니다. 개체 또는 요소의 **x**를 클릭하면 정책에서 해당 개체나 요소를 제거할 수 있습니다.

다음 기준을 사용하여 규칙과 일치하는 소스 및 대상을 식별할 수 있습니다.

소스 영역**,** 대상 영역

트래픽이 통과하는 인터페이스를 정의하는 보안 영역 개체입니다. 기준은 하나 또는 둘 다 정의할 수도 있고 둘 다 정의하지 않을 수도 있습니다. 지정되지 않은 기준은 임의 인터페이스의 트래픽에 적용됩니다.

- 영역 내 인터페이스의 디바이스에서 나가는 트래픽에 일치시키기 위해서는 대상 영역에 해당 영역을 추가합니다.
- 영역 내 인터페이스를 통해 디바이스로 들어오는 트래픽에 일치시키기 위해서는 소스 영역에 해당 영역을 추가합니다.
- 규칙에 소스와 대상 영역 조건을 모두 추가한 경우, 일치하는 트래픽은 반드시 지정된 소스 영역 중 하나에서 발생해야 하며 대상 영역 중 하나를 통해 전송되어야 합니다.

트래픽이 디바이스로 들어오거나 디바이스에서 나가는 위치를 기준으로 규칙을 적용해야 하는 경우 이 기준을 사용해야 합니다. 예를 들어 내부 호스트로 이동하는 모든 트래픽에서 IPS를 검사하려는 경우에는 내부 영역을 대상 영역으로 선택하고 소스 영역은 비워 둡니다. 규칙에서 IPS 필터링을 구현하려면 규칙 작업이 허용이어야 하며 규칙에서 침입 정책을 선택해야 합니다.

소스 네트워크, 대상 네트워크

트래픽의 네트워크 주소나 위치를 정의하는 네트워크 개체 또는 지리적 위치입니다.

- 특정 IP 주소 또는 지리적 위치에서 나오는 트래픽을 일치시키려면 소스 네트워크를 구성합니다.
- 특정 IP 주소 또는 지리적 위치로 향하는 트래픽을 일치시키려면 대상 네트워크를 구성합니다.
- 규칙에 소스와 대상 네트워크 조건을 모두 추가한 경우, 일치하는 트래픽은 반드시 지정된 IP 주소 중 하나에서 발생해야 하며 그 목적지가 대상 IP 주소 중 하나여야 합니다.

이 기준을 추가할 때는 다음 탭에서 선택합니다.

- 네트워크 - 제어하려는 트래픽의 소스 또는 대상 IP 주소를 정의하는 네트워크 개체 또는 그룹을 선택합니다.
- 지리위치 - 소스 또는 대상 국가나 대륙을 기준으로 트래픽을 제어하려면 지리적 위치를 선택합니다. 대륙을 선택하면 대륙 내의 모든 국가가 선택됩니다. 규칙에서 지리적 위치를 직접 선택하는 방법 외에, 위치를 정의하기 위해 생성한 지리위치 개체를 선택할 수도 있습니다. 지리적 위치를 사용하면 특정 국가에서 사용될 수 있는 모든 IP 주소를 몰라도 해당 국가에 대한 액세스를 쉽게 제한할 수 있습니다.

참고 최신 지리적 위치 데이터를 사용하여 트래픽을 필터링하려면 GeoDB(지리위치 데이터베이스)를 정기적으로 업데이트하는 것이 좋습니다.

소스 포트, 대상 포트/프로토콜

트래픽에 사용되는 프로토콜을 정의하는 포트 개체입니다. TCP/UDP의 경우 여기에는 포트가 포함될 수 있습니다. ICMP의 경우에는 코드와 유형이 포함될 수 있습니다.

- 특정 프로토콜이나 포트에서 나오는 트래픽을 일치시키려면 소스 포트를 구성합니다. 소스 포트는 TCP/UDP 전용일 수 있습니다.
- 특정 프로토콜이나 포트로 향하는 트래픽을 일치시키려면 대상 포트/프로토콜을 구성합니다. 조건에 대상 포트만 추가할 경우, 다른 전송 프로토콜을 사용하는 포트를 추가할 수 있습니다. ICMP 및 기타 비TCP/UDP 사양은 대상 포트에서만 허용되며 소스 포트에서는 허용되지 않습니다.
- 특정 TCP/UDP 포트에서 발생하는 트래픽과 특정 TCP/UDP 포트로 향하는 트래픽을 모두 일치시키려면 두 포트를 모두 구성합니다. 조건에 소스 및 대상 포트를 모두 추가한 경우, 단일 전송 프로토콜(TCP 또는 UDP)을 공유하는 포트만 추가할 수 있습니다. 예를 들어 포트 TCP/80에서 포트 TCP/8080으로 이동하는 트래픽을 대상으로 지정할 수 있습니다.

애플리케이션 기준

액세스 규칙의 애플리케이션 기준은 IP 연결 또는 필터에 사용되는 애플리케이션을 정의하며 유형, 범주, 태그, 위험 또는 사업 타당성에 따라 애플리케이션을 정의합니다. 기본값은 모든 애플리케이션입니다.

규칙에서 개별 애플리케이션을 지정할 수 있으나 애플리케이션 필터를 사용하면 정책 생성 및 관리가 간소화됩니다. 예를 들어, 위험도가 높고 사업 타당성이 낮은 모든 애플리케이션을 식별하여 차단하는 액세스 제어 규칙을 만들 수 있습니다. 사용자가 이러한 애플리케이션 중 하나를 사용하려고 할 경우, 세션은 차단됩니다.

이와 더불어 Cisco에서는 시스템 및 VDB(Vulnerability Database)를 통해 추가 애플리케이션 탐지기를 자주 업데이트하고 추가합니다. 따라서 규칙을 수동으로 업데이트하지 않아도 위험도가 높은 애플리케이션을 차단하는 규칙이 새 애플리케이션에 자동으로 적용될 수 있습니다.

규칙에서 애플리케이션 및 필터를 직접 지정하거나 이러한 특성을 정의하는 애플리케이션 필터 개체를 생성할 수 있습니다. 이 두 가지 경우의 사양은 동일하지만, 개체를 사용하면 복잡한 규칙을 생성할 때에도 시스템 제한(기준당 항목 50개)을 유지하기가 더욱 쉽습니다.

애플리케이션 및 필터 목록을 수정하려면 조건 내에서 + 버튼을 클릭하고 개별 탭에 나열된 원하는 애플리케이션 또는 애플리케이션 필터 개체를 선택한 후에 팝업 대화 상자에서 **OK(**확인**)**를 클릭합니다. 탭 중 하나에서 **Advanced Filter(**고급 필터**)**를 클릭하면 필터 기준을 선택하거나 특정 애플리케이션을 검색할 수 있습니다. 애플리케이션, 필터 또는 개체에 대해 **x**를 클릭하면 정책에서 해당 항목을 제거할 수 있습니다. **Save As Filter(**필터로 저장**)** 링크를 클릭하면 아직 개체가 아닌 결합된 기준을 새 애플리케이션 필터 개체로 저장할 수 있습니다.

다음과 같은 고급 필터 기준을 사용하여 규칙과 일치하는 애플리케이션이나 필터를 식별할 수 있습니다. 이러한 애플리케이션 또는 필터는 애플리케이션 필터 개체에서 사용되는 것과 같은 요소입니다.

참고 단일 필터 기준으로 여러 선택 항목이 OR 관계를 갖습니다. 예를 들어, 위험은 높음 OR 매우 높음입니다. 반면 필터 간의 관계는 AND입니다. 즉, 위험은 높음 OR 매우 높음 AND 사업 타당성은 낮음 OR 매우 낮음과 같습니다. 필터를 선택하면 디스플레이의 애플리케이션 목록이 업데이트되어 기준을 충족하는 애플리케이션만 표시됩니다. 이러한 필터를 사용하여 개별적으로 추가하려는 애플리케이션을 찾거나, 규칙에 추가할 적절한 필터를 선택하고 있는지를 확인할 수 있습니다.

위험

애플리케이션이 조직의 보안 정책과 상반되는 용도로 사용될 가능성(매우 낮음~매우 높음)

사업 타당성

조직의 비즈니스 운영(레크리에이션과 반대) 컨텍스트 내에서 애플리케이션이 사용될 가능성(매우 낮음~매우 높음)

유형

애플리케이션 유형:

- 애플리케이션 프로토콜 - 호스트 간의 통신을 나타내는 HTTP, SSH 등의 애플리케이션 프로토콜
- 클라이언트 프로토콜 - 호스트에서 실행 중인 소프트웨어를 나타내는 웹 브라우저, 이메일 클라이언트 등의 클라이언트
- 웹 애플리케이션 - HTTP 트래픽의 요청 URL 또는 콘텐츠를 나타내는 MPEG 비디오, Facebook 등의 웹 애플리케이션

범주

가장 중요한 기능을 설명하는 일반 애플리케이션 분류.

태그

애플리케이션에 대한 추가 정보로, 범주와 비슷합니다.

암호화된 트래픽의 경우, 시스템은 **SSL** 프로토콜 태그가 지정된 애플리케이션만 사용하여 트래픽을 식별하고 필터링할 수 있습니다. 이 태그가 없는 애플리케이션은 암호화되지 않은 트래픽 또는 해독된 트래픽에서만 탐지할 수 있습니다. 또한 암호화된 트래픽 또는 암호화되지 않은 트래픽이 아닌 암호 해독된 트래픽에서만 탐지할 수 있는 애플리케이션에는 암호 해독된 트래픽 태그가 할당됩니다.

애플리케이션 목록**(**디스플레이 하단**)**

이 목록은 목록 위의 옵션에서 필터를 선택하면 업데이트되므로 현재 필터와 일치하는 애플리케이션을 확인할 수 있습니다. 이 목록을 사용하여 규칙에 필터 기준을 추가하려는 경우 필터가 적절한 애플리케이션을 대상으로 하는지를 확인할 수 있습니다. 특정 애플리케이션을 추가하려는 경우 이 목록에서 선택합니다.

URL 기준

액세스 규칙의 URL 기준은 웹 요청에 사용되는 URL 또는 요청된 URL이 속하는 범주를 정의합니다. 범주가 일치하는 경우 허용하거나 차단할 사이트의 상대적 평판을 지정할 수도 있습니다. 기본적으로는 모든 URL이 허용됩니다.

URL 카테고리 및 평판을 통해 액세스 제어 규칙의 URL 조건을 신속하게 만들 수 있습니다. 예를 들어 모든 게임 사이트를 차단하거나 모든 높은 위험의 소셜 네트워킹 사이트를 차단할 수 있습니다. 사용자가 해당 카테고리 및 평판 조합을 가진 URL 검색을 시도하는 모든 경우, 세션이 차단됩니다.

범주 및 평판 데이터를 사용하면 정책 생성 및 관리도 간소화됩니다. 이를 통해 시스템이 웹 트래픽을 예상대로 제어할 수 있습니다. 마지막으로, Cisco의 위협 인텔리전스는 새로운 URL, 새로운 범주 및 기존 URL의 새로운 범주와 위험이 적용되어 지속적으로 업데이트되므로 시스템은 최신 정보를 사용하여 요청된 URL을 필터링할 수 있습니다. 악성코드, 스팸, 봇넷, 피싱과 같은 보안 위협을 나타내는 악성 사이트는 새로운 정책을 업데이트하고 구축하는 것보다 빠르게 나타났다 사라질 수 있습니다.

URL 목록을 수정하려면 조건 내의 + 버튼을 클릭하고 다음 기술 중 하나를 사용하여 원하는 범주 또는 URL을 선택합니다. 범주 또는 개체의 **x**를 클릭하면 정책에서 해당 범주나 개체를 제거할 수 있습니다.

URL 탭

+를 클릭하고 URL 개체 또는 그룹을 선택한 후에 **OK(**확인**)**를 클릭합니다. 필요한 개체가 없는 경우에는 **Create New URL(**새 **URL** 생성**)**을 클릭하면 됩니다.

참고 특정 사이트를 대상으로 하도록 URL 개체를 구성하기 전에 수동 URL 필터링에 대한 정보를 자세히 확인하십시오. URL 일치는 예상한 방식으로 수행되지 않으므로 의도와 달리 사이트가 차단되기 쉽습니다. 예를 들어, 명시적으로 게임 사이트 ign.com을 차단하려는 경우 verisign.com과 "ign"으로 끝나는 기타 모든 사이트도 차단됩니다.

범주 탭

+를 클릭하고 원하는 범주를 선택한 후에 **OK(**확인**)**를 클릭합니다.

기본적으로는 평판과 관계없이 선택한 각 범주의 모든 URL에 규칙을 적용합니다. 평판을 기준으로 하여 규칙을 제한하려면 각 범주의 아래쪽 화살표를 클릭하고 임의 체크 박스 선택을 취소한 후에 평판 슬라이더를 사용하여 평판 레벨을 선택합니다. 평판 슬라이더의 왼쪽은 허용할 사이트를, 오른쪽은 차단할 사이트를 나타냅니다. 평판 사용 방식은 규칙 작업에 따라 달라집니다.

- 규칙이 웹 액세스를 차단하거나 모니터링하는 경우 평판 레벨을 선택하면 해당 레벨보다 심각도가 높은 모든 평판도 선택됩니다. 예를 들어, **Suspicious sites(**의심스러운 사이트**)**(레벨 2)를 모니터링하거나 차단하는 규칙을 구성하는 경우, 이는 또한 **High risk(**고위험**)**(레벨 1) 사이트를 자동으로 모니터링하거나 차단합니다.
- 규칙이 웹 액세스를 허용하는 경우 평판 레벨을 선택하면 해당 레벨보다 심각도가 낮은 모든 평판도 선택됩니다. 예를 들어, **Benign sites(**안전한 사이트**)**(레벨 4)를 허용하는 규칙을 구성하는 경우, 이는 또한 **Well known(**잘 알려진**)**(레벨 5) 사이트를 자동으로 허용합니다.

사용자 기준

액세스 규칙의 사용자 기준은 IP 연결의 사용자 또는 사용자 그룹을 정의합니다. 액세스 규칙에 사용자 또는 사용자 그룹 기준을 포함하려면 ID 정책 및 연관된 디렉터리 서버를 구성해야 합니다.

ID 정책에 따라 특정 연결에 대해 사용자 ID가 수집되는지가 결정됩니다. ID가 설정된 경우에는 호스트의 IP 주소가 식별된 사용자와 연결됩니다. 그러므로 해당 소스 IP 주소가 사용자에 매핑된 트래픽은 해당 사용자가 보내는 것으로 간주됩니다. IP 패킷 자체는 사용자 ID 정보를 포함하지 않으므로 이 IP 주소에서 사용자로의 매핑은 가능한 최적의 근사치입니다.

규칙에는 최대 50개의 사용자나 그룹을 추가할 수 있으므로 일반적으로는 개별 사용자를 선택하는 것보다 그룹을 선택하는 것이 더 효율적입니다. 예를 들어 엔지니어링 그룹의 개발 네트워크 액세스

를 허용하는 규칙을 생성한 다음 네트워크에 대한 기타 모든 액세스를 거부하는 후속 규칙을 생성할 수 있습니다. 그러면 신규 엔지니어에 대해 규칙을 적용하려는 경우 디렉터리 서버의 엔지니어링 그룹에 해당 엔지니어를 추가하기만 하면 됩니다.

사용자 목록을 수정하려면 조건 내의 + 버튼을 클릭하고 다음 기술 중 하나를 사용하여 원하는 사용자 또는 사용자 그룹을 선택합니다. 사용자 또는 그룹의 **x**를 클릭하면 정책에서 해당 사용자나 그룹을 제거할 수 있습니다.

- 사용자 및 그룹 탭 - 원하는 사용자 또는 사용자 그룹을 선택합니다. 그룹은 디렉터리 서버에서 그룹을 구성하는 경우에만 사용할 수 있습니다. 그룹을 선택하면 하위 그룹을 포함하여 그룹의 모든 구성원에게 규칙이 적용됩니다. 하위 그룹을 다르게 처리하려는 경우에는 하위 그룹용으로 별도의 액세스 규칙을 생성한 다음 액세스 제어 정책에서 상위 그룹용 규칙 위에 배치해야 합니다.

  참고 기본적으로 Active Directory 서버는 보조 그룹에서 보고하는 사용자 수를 제한합니다. 보조 그룹의 모든 사용자가 보고되고 사용자 조건이 포함된 액세스 제어 규칙에서 사용할 수 있도록 설정하려는 경우에는 이 제한을 맞춤화해야 합니다. 또한, Firepower Device Manager에서는 전체 사용자가 2,000명으로 제한되므로 디렉터리의 사용자가 2,000명보다 많으면 가능한 사용자 이름이 일부만 표시됩니다.

- 특수 엔티티 탭 - 다음 옵션 중에서 선택합니다.
  - 실패한 인증 - 사용자에게 인증하라는 메시지가 표시되었는데 사용자가 허용되는 최대 횟수 이내에 유효한 사용자 이름/비밀번호 쌍을 입력하지 못했습니다. 인증에 실패해도 사용자의 네트워크 액세스가 차단되지는 않지만, 이러한 사용자의 네트워크 액세스를 제한하는 액세스 규칙을 작성할 수 있습니다.
  - 게스트 - 게스트 사용자는 ID 규칙이 이러한 사용자를 게스트로 지칭하도록 구성된다는 점을 제외하면 실패한 인증 사용자와 비슷합니다. 즉, 게스트 사용자 역시 인증하라는 메시지가 표시되었지만, 최대 시도 횟수 이내에 인증하지 못한 사용자입니다.
  - 인증 필요 없음 - 사용자의 연결이 인증을 지정하지 않은 ID 규칙과 일치하여 인증하라는 메시지가 표시되지 않았습니다.
  - 알 수 없음 - IP 주소에 대한 사용자 매핑이 없으며 아직 실패한 인증 기록이 없습니다.

침입 정책 설정

Cisco는 Firepower System에서 여러 침입 정책을 제공합니다. 이러한 정책은 Cisco Talos Security Intelligence and Research Group에서 설계했습니다. 여기서는 고급 설정과 침입 및 전처리기 규칙 구문 상태를 설정합니다. 이러한 정책은 수정할 수 없습니다.

트래픽을 허용하는 액세스 제어 규칙의 경우 다음 침입 정책 중 하나를 선택하여 트래픽에서 침입 및 익스플로잇을 검사할 수 있습니다. 침입 정책은 패턴을 기반으로 디코딩된 패킷에서 공격을 검사하며 악의적인 트래픽을 차단하거나 변경할 수 있습니다.

침입 검사를 활성화하려면 **Intrusion Policy(**침입 정책**)** > **On(**켜기**)**을 선택하고 슬라이더를 사용하여 원하는 정책을 선택합니다. 정책은 안전성이 가장 낮은 항목부터 가장 높은 항목 순서로 나열됩니다.

- 연결이 보안에 우선함 - 모든 리소스에 접근할 수 있는 연결이 네트워크 인프라 보안에 우선하는 조직을 위해 작성된 정책입니다. 침입 정책은 Security Over Connectivity(연결성에 우선하는 보안)에서 활성화된 것보다 훨씬 더 적은 규칙을 활성화합니다. 트래픽을 차단하는 가장 중요한 규칙만 활성화됩니다. 네트워크의 보안을 크게 신뢰하는 경우 어느 정도 침입 차단을 적용하려면 이 정책을 선택합니다.
- 균형 잡힌 보안 및 연결성 - 전반적인 네트워크 성능과 네트워크 인프라 보안의 균형을 유지할 수 있도록 설계된 정책입니다. 이 정책은 대부분의 네트워크에 적합합니다. 침입 방지를 적용하려는 대부분의 상황에 대해 이 정책을 선택합니다.
- 보안이 연결에 우선함 - 네트워크 인프라 보안이 사용자 편의에 우선하는 조직을 위해 작성된 정책입니다. 침입 정책은 적합한 트래픽에 대해 경계하거나 중단할 수 있는 다양한 네트워크 이상 침입 규칙을 활성화합니다. 보안이 가장 중요할 때나 트래픽의 위험성이 높을 때는 이 정책을 선택합니다.
- 최대 탐지 - 보안이 연결에 우선함 정책을 통해 지정할 수 있는 것보다 네트워크 인프라 보안이 더욱 강조되는 조직을 위해 작성된 정책이며, 사용하는 경우 운영에 더 큰 영향을 미칠 수 있습니다. 예를 들어 이 침입 정책에서는 악성코드, 익스플로잇 킷, 오래된 일반적인 취약점, 통제되지 않은 알려진 익스플로잇 등 다수의 위협 범주에서 규칙을 사용합니다. 이 정책을 선택할 경우 정상적인 트래픽이 너무 많이 삭제되지 않는지 신중하게 평가해야 합니다.

파일 정책 설정

AMP for Firepower(Advanced Malware Protection for Firepower)를 사용하여 악성 소프트웨어, 즉 악성코드를 탐지할 때 파일 정책을 사용합니다. 파일 제어를 수행하는 데에도 파일 정책을 사용할 수 있습니다. 그러면 파일에 악성코드가 있는지와 관계없이 특정 유형의 모든 파일에 대한 제어가 가능합니다.

AMP for Firepower는 AMP 클라우드를 사용하여 네트워크 트래픽에서 탐지될 가능성이 있는 악성코드의 상태를 검색하고 로컬 악성코드 분석 및 파일 사전 분류 업데이트를 가져옵니다. 관리 인터페이스에는 AMP 클라우드에 연결하고 악성코드 조회를 수행하기 위한 인터넷으로 연결되는 경로가 있어야 합니다. 디바이스는 적합한 파일을 탐지하면 파일의 SHA-256 해시 값을 사용하여 AMP 클라우드에서 파일의 상태를 쿼리합니다. 가능한 상태는 다음과 같습니다.

- 악성코드 - AMP 클라우드가 파일을 악성코드로 분류했습니다. 아카이브 파일(예: zip 파일)은 해당 파일 내에 악성코드인 파일이 있으면 악성코드로 표시됩니다.
- 정상 - AMP 클라우드가 파일을 악성코드가 포함되어 있지 않은 정상 파일로 분류했습니다. 아카이브 파일은 해당 파일 내의 모든 파일이 정상이면 정상으로 표시됩니다.
- 알 수 없음 - AMP 클라우드가 파일에 상태를 아직 할당하지 않았습니다. 아카이브 파일은 해당 파일 내에 알 수 없는 상태의 파일이 있으면 알 수 없음으로 표시됩니다.
- 사용할 수 없음 - 시스템이 AMP 클라우드를 쿼리하여 파일의 상태를 확인하지 못했음을 나타냅니다. 이 속성을 통해 이벤트의 일부를 확인할 수 있습니다. 이는 예상된 행동입니다. "사용할 수 없음" 이벤트가 연속하여 여러 개 표시되는 경우에는 관리 주소에 대한 인터넷 연결이 정상적으로 작동하는지 확인하십시오.

사용 가능한 파일 정책

다음 파일 정책 중 하나를 선택할 수 있습니다.

- 없음 - 전송된 파일에서 악성코드를 평가하지 않으며 파일별 차단을 수행하지 않습니다. 파일 전송을 신뢰할 수 있거나 거의 또는 전혀 수행될 가능성이 없는 규칙 또는 애플리케이션이나 URL 필터링이 네트워크를 적절하게 보호한다고 확신할 수 있는 규칙의 경우 이 옵션을 선택합니다.
- 악성코드 모두 차단 - 네트워크를 지나는 파일이 악성코드를 포함하는지 확인한 다음 위협이 되는 파일을 차단하기 위해 AMP 클라우드에 쿼리합니다.
- 모두 클라우드 조회 - 네트워크를 지나는 파일의 전송을 허용하되 그 파일의 속성을 확인하고 로깅하기 위해 AMP 클라우드에 쿼리합니다.
- **Office** 문서 및 **PDF** 업로드 차단**,** 악성코드 기타 차단 - 사용자가 Microsoft Office 문서 및 PDF 업로드를 업로드하지 못하도록 차단합니다. 또한 네트워크를 지나는 파일이 악성코드를 포함하는지 확인한 다음 위협이 되는 파일을 차단하기 위해 AMP 클라우드에 쿼리합니다.
- **Office** 문서 업로드 차단**,** 악성코드 기타 차단 - 사용자가 Microsoft Office 문서를 업로드하지 못하도록 차단합니다. 또한 네트워크를 지나는 파일이 악성코드를 포함하는지 확인한 다음 위협이 되는 파일을 차단하기 위해 AMP 클라우드에 쿼리합니다.

로깅 설정

액세스 규칙의 로깅 설정에 따라 규칙과 일치하는 트래픽에 대해 연결 이벤트가 생성되는지가 결정됩니다. 이벤트 뷰어에서 규칙과 관련된 이벤트를 확인하려면 로깅을 활성화해야 합니다. 또한, 시스템을 모니터링하는 데 사용할 수 있는 여러 대시보드에 일치하는 트래픽을 반영하려는 경우에도 로깅을 활성화해야 합니다.

조직의 보안 및 규정 준수 필요에 따라 연결을 로깅해야 합니다. 사용자가 생성하고 기능을 향상시키는 이벤트의 수를 제한하는 것이 사용자의 목표라면 사용자의 분석에 중요한 연결에 대한 로깅만 활성화합니다. 그러나, 자료 수집을 목적으로 사용자의 네트워크 트래픽에 대한 광범위한 견해를 원할 경우, 추가 연결에 대한 로깅을 활성화할 수 있습니다.

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 이 규칙이 인터넷 연결 인터페이스 또는 DoS 공격에 취약한 다른 인터페이스용인지를 고려하십시오.

다음과 같은 로깅 작업을 구성할 수 있습니다.

로그 작업 선택

다음 작업 중 하나를 선택할 수 있습니다.

- 연결 시작 및 종료 시 로깅 - 연결 시작 및 종료 시에 이벤트를 생성합니다. 연결 종료 이벤트는 연결 시작 이벤트에 포함된 모든 항목과 연결 중에 수집되었을 수 있는 모든 정보를 포함하므로 허용하는 트래픽에 대해서는 이 옵션을 선택하지 않는 것이 좋습니다. 두 이벤트를 모두 로깅하면 시스템 성능에 영향을 줄 수 있습니다. 하지만 차단된 트래픽의 경우에는 이 옵션만 사용할 수 있습니다.
- 연결 종료 시 로깅 - 연결 종료 시에 연결 로깅을 사용하려면 이 옵션을 선택합니다. 허용되는 트래픽이나 신뢰하는 트래픽의 경우 이 옵션을 선택하는 것이 좋습니다.
- 연결 시 로깅하지 않음 - 규칙에 대해 로깅을 비활성화하려면 이 옵션을 선택합니다. 이는 기본값입니다.

참고 액세스 제어 규칙이 호출한 침입 정책이 침입을 탐지하고 침입 이벤트를 생성하면, 시스템은 규칙의 로깅 컨피그레이션에 상관없이 침입이 발생한 연결의 종료를 자동으로 로깅합니다. 침입이 차단된 연결을 위한 연결 로그 내 연결 작업은 **Block(**차단**)**입니다. 그 이유는 **Intrusion Block(**침입 차단**)**이며, 침입 탐지 수행을 위해서라면 반드시 Allow(허용) 규칙을 사용해야 합니다.

파일 이벤트

금지된 파일 또는 악성코드 이벤트 로깅을 사용하지 않으려면 **Log Files(**로그 파일**)**를 선택합니다. 이 옵션을 구성하려면 규칙에서 파일 정책을 선택해야 합니다. 규칙에 대해 파일 정책을 선택하는 경우 기본값으로 이 옵션을 사용합니다. 이 옵션은 활성화된 상태로 유지하는 것이 좋습니다.

시스템은 금지된 파일을 탐지하면 다음과 같은 유형의 이벤트 중 하나를 자동으로 로깅합니다.

- 파일 이벤트 - 악성코드 파일을 포함하여 탐지되거나 차단된 파일을 나타냅니다.
- 악성코드 이벤트 - 탐지되거나 차단된 악성코드 파일만 나타냅니다.
- 소급 적용되는 악성코드 이벤트 - 이전에 탐지된 파일에 대한 악성코드 상태가 변경되는 경우 생성됩니다.

파일이 차단된 경우의 연결을 위한 연결 로그 내 연결 작업은 **Block(**차단**)**입니다. 파일 또는 악성코드 탐지를 수행하려는 경우에도 Allow(허용) 규칙을 사용해야 합니다. 연결하는 이유는 파일 모니터링(파일 유형 또는 악성코드가 탐지된 경우), 악성코드 차단 또는 파일 차단(파일이 차단된 경우)입니다.

다음으로 연결 이벤트 보내기

외부 syslog 서버로 이벤트의 복사본을 전송하려는 경우 syslog 서버를 정의하는 서비스 개체를 선택합니다. 필요한 개체가 아직 없으면 **Create New Syslog Server**(새 **Syslog** 서버 생성)를 클릭하여 개체를 생성합니다. syslog 서버에 대한 로깅을 사용하지 않으려면 서버 목록에서 임의를 선택합니다.

디바이스의 이벤트 스토리지는 제한되어 있으므로 외부 syslog 서버로 이벤트를 전송하면 더 장기적으로 저장할 수 있으며 이벤트 분석 성능이 개선됩니다.

액세스 제어 정책 모니터링

모니터링 대시보드에 있는 대부분의 데이터는 액세스 제어 정책과 직접적으로 관련되어 있습니다. 트래픽 및 시스템 대시보드 모니터링, 72 페이지를 참조하십시오.

- **Monitoring**(모니터링) > **Policies**(정책)에는 가장 많이 적중한 액세스 제어 규칙 및 관련 통계가 표시됩니다.
- 일반적인 통계는 **Network Overview**(네트워크 개요), **Destinations**(목적지), **Ingress Zones**(인그레스 영역) 및 **Egress Zones**(이그레스 영역) 대시보드에서 확인할 수 있습니다.
- URL 필터링 결과는 **Web Categories**(웹 범주) 및 **Destinations**(목적지) 대시보드에서 확인할 수 있습니다. 웹 범주 대시보드에서 정보를 확인하려면 최소한 URL 필터링 정책이 있어야 합니다.
- 애플리케이션 필터링 결과는 **Applications**(애플리케이션) 대시보드에서 확인할 수 있습니다.
- 사용자 기반 통계는 **Users**(사용자) 대시보드에서 확인할 수 있습니다. 사용자 정보를 수집하려면 ID 정책을 구현해야 합니다.
- 침입 정책 통계는 **Attackers**(공격자) 및 **Targets**(대상) 대시보드에서 확인할 수 있습니다. 이러한 대시보드에서 정보를 확인하려면 하나 이상의 액세스 제어 규칙에 침입 정책을 적용해야 합니다.
- 파일 정책 및 악성코드 필터링 통계는 **File Logs**(파일 로그) 대시보드에서 확인할 수 있습니다. 이 대시보드에서 정보를 확인하려면 하나 이상의 액세스 제어 규칙에 파일 정책을 적용해야 합니다.
- **Monitoring**(모니터링) > **Events**(이벤트)에는 액세스 제어 규칙과 관련된 데이터 및 연결에 대한 이벤트도 표시됩니다.

CLI에서 액세스 제어 정책 모니터링

디바이스 CLI에 로그인한 후에 다음 명령을 사용하여 액세스 제어 정책과 통계에 대한 상세 정보를 가져올 수도 있습니다.

- **show access-control-config**는 액세스 제어 규칙에 대한 요약 정보를 규칙별 적중 횟수와 함께 표시합니다.
- **show access-list**는 액세스 제어 규칙에서 생성된 ACL(Access Control Lists)을 표시합니다. ACL은 초기 필터를 제공하며 가능한 경우 항상 빠른 결정 제공을 시도하므로, 삭제해야 하는 연결

을 검사할 필요가 없어 리소스가 불필요하게 사용되지 않습니다. 이 정보에는 적중 횟수가 포함됩니다.

- **show snort statistics**는 기본 검사기인 Snort 검사 엔진에 대한 정보를 표시합니다. Snort는 애플리케이션 필터링, URL 필터링, 침입 차단, 파일 및 악성코드 필터링을 구현합니다.
- **show conn**은 인터페이스를 통해 현재 설정되어 있는 연결에 대한 정보를 표시합니다.
- **show traffic**은 각 인터페이스를 통과하는 트래픽에 대한 통계를 표시합니다.
- **show ipv6 traffic**은 디바이스를 통과하는 IPv6 트래픽에 대한 통계를 표시합니다.

액세스 제어 제한

다음 항목에서는 액세스 제어 정책의 몇 가지 제한에 대해 설명합니다.

애플리케이션 제어의 제한

애플리케이션 식별 속도

다음을 수행하기 전에는 시스템이 애플리케이션 제어를 수행할 수 없습니다.

- 클라이언트와 서버 간에 모니터링된 연결 설정
- 시스템이 세션에서 애플리케이션 식별

이 식별은 3개 ~ 5개 패킷 내에서 또는 트래픽이 암호화된 경우에는 SSL 핸드셰이크의 서버 인증서 교환 후에 이루어져야 합니다.

초기 트래픽이 기타 모든 기준과는 일치하는데 애플리케이션 식별이 불완전한 경우 시스템은 패킷 통과 및 연결 설정 또는 SSL 핸드셰이크 완료를 허용합니다. 시스템은 식별을 완료하면 나머지 세션 트래픽에 적절한 작업을 적용합니다.

액세스 제어의 경우 이와 같이 통과되는 패킷은 액세스 제어 정책의 기본 침입 정책(기본 작업 침입 정책도 아니고 거의 일치하는 규칙의 침입 정책도 아님)에 의해 검사됩니다.

암호화된 트래픽과 암호 해독된 트래픽에 대한 애플리케이션 제어

시스템은 암호화된 트래픽과 암호 해독된 트래픽을 식별하고 필터링할 수 있습니다.

- 암호화된 트래픽 - 시스템은 SMTPS, POPS, FTPS, TelnetS, IMAPS를 비롯하여 StartTLS로 암호화된 애플리케이션 트래픽을 탐지할 수 있습니다. 또한, TLS ClientHello 메시지 내 서버 이름 지표 또는 서버 인증서의 주체로 구별되는 이름 값에 따라 암호화된 특정 애플리케이션을 식별할 수 있습니다. 이러한 애플리케이션에는 `SSL Protocol`. 이 태그가 없는 애플리케이션은 암호화되지 않은 트래픽 또는 해독된 트래픽에서만 탐지할 수 있습니다.
- 암호 해독된 트래픽 - 시스템은 암호화되거나 암호화되지 않은 트래픽이 아닌 암호 해독된 트래픽에서만 탐지할 수 있는 애플리케이션에 `decrypted traffic` 태그를 할당합니다.

페이로드 없이 애플리케이션 트래픽 패킷 처리

액세스 제어를 수행할 때 시스템은 애플리케이션이 식별된 연결에서 페이로드가 없는 패킷에 기본 정책 작업을 적용합니다.

참조된 애플리케이션 트래픽 처리

광고물 트래픽과 같이 웹 서버에서 참조된 트래픽을 처리하려면 참조하는 애플리케이션이 아닌 참조되는 애플리케이션의 일치 여부를 확인합니다.

다중 프로토콜을 사용하는 애플리케이션 트래픽 제어**(Skype)**

시스템은 Skype 애플리케이션 트래픽의 여러 유형을 탐지할 수 있습니다. Skype 트래픽을 제어하려면 개별 애플리케이션을 선택하지 말고 애플리케이션 필터 목록에서 **Skype** 태그를 선택합니다. 이렇게 하면 시스템이 동일한 방법으로 모든 Skype 트래픽을 탐지하고 제어할 수 있도록 할 수 있습니다.

사용자 또는 그룹 제어의 제한사항

Firepower Device Manager는 디렉터리 서버에서 사용자 최대 2,000명에 대한 정보를 다운로드할 수 있습니다.

디렉터리 서버에 2,000개보다 많은 사용자 어카운트가 포함되어 있으면 액세스 규칙에서 사용자를 선택할 때 또는 사용자 기반 대시보드 정보를 확인할 때 가능한 이름이 모두 표시되지 않으며, 다운로드한 이름에 대해서만 규칙을 작성할 수 있습니다.

이 2,000개 제한은 그룹과 연결된 이름에도 적용됩니다. 그룹의 멤버가 2,000명보다 많으면 다운로드한 2,000개의 이름에 대해서만 그룹 멤버십과의 일치 여부를 확인할 수 있습니다.

사용자가 2,000명보다 많은 경우에는 Firepower Device Manager 대신 Firepower Management Center(원격 관리자)를 사용하는 것이 좋습니다. Firepower Management Center는 훨씬 더 많은 사용자를 지원합니다.

URL 필터링의 제한

URL 식별 속도

시스템은 다음 작업을 수행한 후 URL을 필터링할 수 있습니다.

- 클라이언트와 서버 간에 모니터링된 연결 설정
- 시스템이 세션에서 HTTP 또는 HTTPS 애플리케이션 식별
- 시스템이 요청된 URL 식별(암호화된 세션의 경우 ClientHello 메시지 또는 서버 인증서로부터)

이 식별은 3개 ~ 5개 패킷 내에서 또는 트래픽이 암호화된 경우에는 SSL 핸드셰이크의 서버 인증서 교환 후에 이루어져야 합니다.

초기 트래픽이 기타 모든 규칙 조건과는 일치하는데 식별이 불완전한 경우 시스템은 패킷 통과 및 연결 설정 또는 SSL 핸드셰이크 완료를 허용합니다. 시스템은 식별을 완료하면 나머지 세션 트래픽에 적절한 규칙 작업을 적용합니다.

액세스 제어의 경우 이와 같이 통과되는 패킷은 액세스 제어 정책의 기본 침입 정책(기본 작업 침입 정책도 아니고 거의 일치하는 규칙의 침입 정책도 아님)에 의해 검사됩니다.

수동 **URL** 필터링

특정 URL을 수동으로 필터링할 때는 영향을 받을 수 있는 다른 트래픽을 신중하게 고려하십시오. URL 조건이 네트워크 트래픽과 일치하는지 확인하기 위해 시스템은 간단한 부분 문자열 일치를 실행합니다. 요청한 URL은 문자열의 일부분과 일치하는 경우 일치 항목으로 간주됩니다.

암호화된 웹 트래픽에 대한 **URL** 필터링

암호화된 웹 트래픽에 대해 URL 필터링을 수행할 때 시스템은 다음 작업을 수행합니다.

- 암호화 프로토콜을 무시합니다. 규칙에 URL 조건은 있지만 프로토콜을 지정하는 애플리케이션 조건이 없는 경우 해당 규칙은 HTTPS 및 HTTP 트래픽 두 가지 모두와 일치합니다.
- 트래픽을 암호화하는 데 사용된 공개 키 인증서의 주체 일반 이름을 기준으로 HTTPS 트래픽 일치를 확인하고 주체 일반 이름 내의 서브도메인을 무시합니다.

URL 내 검색 쿼리 매개변수

시스템은 URL 조건과 일치하도록 URL에서 검색 쿼리 매개변수를 사용하지 않습니다. 예를 들어, 모든 쇼핑 트래픽을 차단하는 시나리오를 생각해 보십시오. 이 경우, amazon.com을 검색하기 위해 웹 검색을 사용하는 것은 차단되지 않지만 amazon.com 브라우징은 차단됩니다.

선택한 디바이스 모델의 메모리 제한

메모리 제한으로 인해, 일부 디바이스 모델은 더 작고 대략적인 카테고리 및 평판 집합을 사용하여 대부분의 URL 필터링을 수행합니다. 예를 들어 상위 URL의 하위 사이트에 여러 가지 URL 카테고리 및 평판이 있는 경우에도, 일부 디바이스에서는 상위 URL의 데이터를 저장만 할 수 있습니다. 이러한 디바이스에서 처리된 웹 트래픽의 경우, 시스템은 클라우드 조회를 수행하여 로컬 데이터베이스에 없는 사이트의 카테고리 및 평판을 확인할 수 있습니다.

저용량 메모리 디바이스에는 ASA 모델 ASA5506-X, ASA5506H-X, ASA5506W-X, ASA5508-X, ASA5512-X, ASA5515-X, ASA5516-X, ASA5525-X가 포함됩니다.

10 장

NAT(네트워크 주소 변환)

다음 주제에서는 NAT(네트워크 주소 변환)에 대한 내용 및 NAT를 구성하는 방법을 설명합니다.

NAT를 사용해야 하는 이유

IP 네트워크 내의 각 컴퓨터와 디바이스에는 호스트를 식별하는 고유한 IP 주소가 할당됩니다. 공용 IPv4 주소의 부족 때문에 이러한 IP 주소는 대부분 사설이며, 사설 회사 네트워크 외부로 라우팅되지 않습니다. RFC 1918의 정의에 따르면 사설 IP 주소는 내부적으로 사용할 수 있지만 외부에 알려서는 안 되는 주소입니다.

- 10.0.0.0~10.255.255.255
- 172.16.0.0 ~ 172.31.255.255
- 192.168.0.0~192.168.255.255

NAT의 주요 기능 중 하나는 사설 IP 네트워크가 인터넷에 연결되도록 하는 것입니다. NAT는 사설 IP 주소를 공용 IP 주소로 교체하여, 내부 사설 네트워크의 사설 주소를 공용 인터넷에서 사용할 수 있는 합법적이고 라우팅 가능한 주소로 전환합니다. 이렇게 하여 NAT는 공용 주소를 절약합니다. 전체 네트워크에 대해 최소 하나의 공용 주소만 외부에 알리도록 구성할 수 있기 때문입니다.

NAT의 기타 기능은 다음과 같습니다.

- 보안 - 직접 공격을 피할 수 있도록 내부 IP 주소를 숨깁니다.

- IP 라우팅 솔루션 - NAT를 사용할 때에는 중첩 IP 주소 문제가 발생하지 않습니다.
- 유연성 - 외부적으로 사용 가능한 공용 주소에 영향을 주지 않고 내부 IP 주소 지정 방식을 변경할 수 있습니다. 예를 들어 인터넷에 액세스할 수 있는 서버의 경우, 인터넷용으로는 고정 IP 주소를 유지하고 내부적으로는 서버 주소를 변경할 수 있습니다.
- IPv4와 IPv6 간 변환(라우팅된 방식 전용) - IPv6 네트워크를 IPv4 네트워크에 연결하려는 경우 NAT를 이용하면 두 가지 주소 유형 간에 변환할 수 있습니다.

참고 NAT는 필수 항목이 아닙니다. 특정 트래픽에 대해 NAT를 구성하지 않으면 해당 트래픽은 변환되지 않지만, 모든 보안 정책은 정상적으로 적용됩니다.

NAT 기본 사항

다음 주제에서는 NAT의 기본 사항 일부를 설명합니다.

NAT 용어

이 설명서는 다음과 같은 용어를 사용합니다.

- 실제 주소/호스트/네트워크/인터페이스 - 실제 주소는 변환되기 전 호스트에서 정의된 주소입니다. 외부에 액세스할 때 내부 네트워크를 변환하는 일반적인 NAT 시나리오에서는 내부 네트워크가 "실제" 네트워크일 수 있습니다. 내부 네트워크뿐 아니라 디바이스에 연결된 모든 네트워크를 변환할 수 있습니다. 따라서 외부 주소를 변환하도록 NAT를 구성하는 경우 "실제"는 내부 네트워크에 액세스하는 외부 네트워크를 지칭할 수 있습니다.
- 매핑된 주소/호스트/네트워크/인터페이스 - 매핑된 주소는 실제 주소가 변환되는 주소입니다. 외부에 액세스할 때 내부 네트워크를 변환하는 일반적인 NAT 시나리오에서는 외부 네트워크가 "매핑된" 네트워크일 수 있습니다.

  참고 주소 변환 중에 디바이스 인터페이스용으로 구성된 IP 주소는 변환되지 않습니다.

- 양방향 시작 - 고정 NAT에서는 연결이 양방향으로 시작될 수 있습니다(호스트에서 나가기도 하고 호스트로 들어오기도 함).
- 소스 및 대상 NAT - 모든 패킷에 대해 소스 및 대상 IP 주소를 NAT 규칙과 비교하며, 하나 또는 둘 모두를 변환하거나 변환하지 않을 수 있습니다. 고정 NAT의 경우에는 규칙이 양방향이므로, 이 가이드 전체에서 명령 및 설명에 "소스"와 "대상"이 사용됩니다. 특정 연결이 "대상" 주소에서 시작되는 경우에도 마찬가지입니다.

NAT 유형

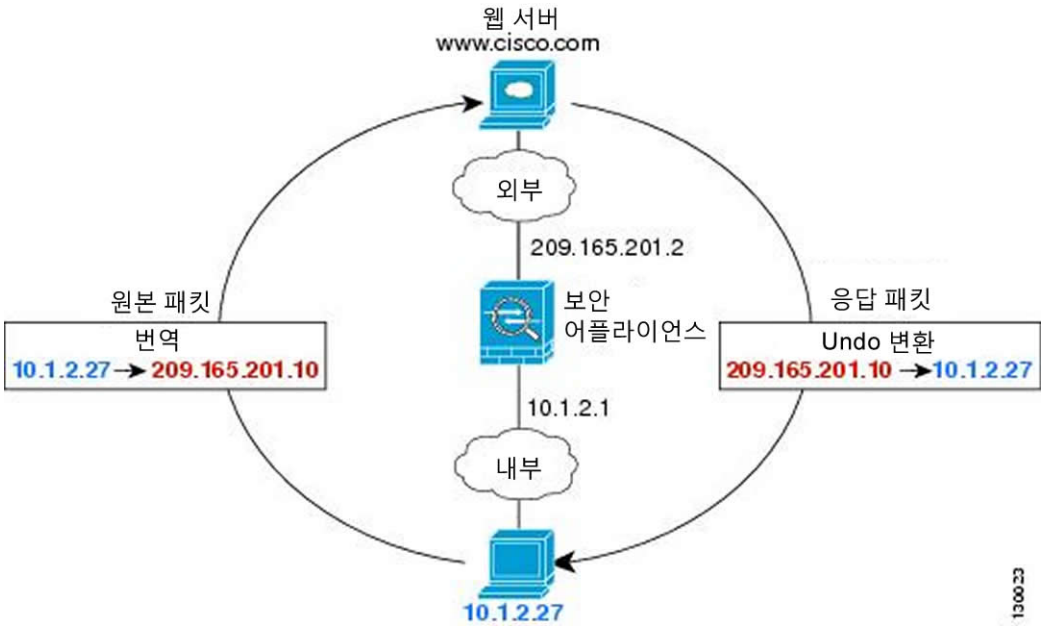
다음 방법을 사용하여 NAT를 구현할 수 있습니다.

- 동적 NAT - 실제 IP 주소의 그룹이 매핑된 IP 주소의 그룹(대개 더 작음)에 선착순으로 매핑됩니다. 실제 호스트만 트래픽을 시작할 수 있습니다. 동적 NAT, 177 페이지를 참조하십시오.
- 동적 PAT(동적 포트 주소 변환) - 실제 IP 주소의 그룹이 해당 IP 주소의 고유한 소스 포트를 사용하여 단일 IP 주소로 매핑됩니다. 동적 PAT, 183 페이지를 참조하십시오.
- 고정(Static) NAT - 실제 IP 주소와 매핑된 IP 주소 간의 일관된 매핑입니다. 양방향 트래픽 시작이 허용됩니다. 고정 NAT, 189 페이지를 참조하십시오.
- ID NAT - 실제 주소가 기본적으로 NAT를 우회하여 자신에게 고정으로 변환됩니다. 대규모 주소 그룹을 변환하되 좀 더 작은 규모의 주소 하위 집합을 제외하고자 할 경우 이 방법으로 NAT를 구성할 수 있습니다. ID NAT, 198 페이지를 참조하십시오.

라우팅 모드의 NAT

다음 그림은 내부에 사설 네트워크가 있는 라우팅된 모드의 일반적인 NAT 예를 보여줍니다.

그림 ***3: NAT*** 예*:* 라우팅된 모드



1 10.1.2.27의 내부 호스트가 웹 서버로 패킷을 전송하면, 패킷의 실제 소스 주소 10.1.2.27이 매핑된 주소 209.165.201.10으로 변환됩니다.

2 서버는 응답할 때 응답을 매핑된 주소 209.165.201.10으로 전송하며 Firepower Threat Defense 디바이스에서 패킷을 수신합니다. Firepower Threat Defense 디바이스에서 프록시 ARP를 수행하여 패킷을 요청하기 때문입니다.

3 그런 다음 Firepower Threat Defense 디바이스에서는 호스트로 전송하기 전에 매핑된 주소 209.165.201.10에서 다시 실제 주소 10.1.2.27로의 변환을 변경합니다.

자동 NAT 및 수동 NAT

자동 *NAT* 및 수동 *NAT*의 두 가지 방법으로 주소 변환을 구현할 수 있습니다.

수동 NAT가 제공하는 추가적인 기능이 필요한 경우가 아니면 자동 NAT를 사용하는 것이 좋습니다. 자동 NAT가 구성이 더 쉽고, VoIP(Voice over IP) 등의 애플리케이션에서 좀 더 안정적일 수 있습니다. VoIP의 경우 규칙에서 사용되는 개체 중 하나에 속하지 않는 간접 주소를 변환할 때 오류가 발생할 수 있습니다.

자동 NAT

네트워크 개체의 파라미터로 구성되는 모든 NAT 규칙은 자동 *NAT* 규칙으로 간주됩니다. NAT 규칙을 사용하면 네트워크 개체에 대해 NAT를 빠르고 쉽게 구성할 수 있습니다. 그러나 그룹 개체에 대해서는 이러한 규칙을 생성할 수 없습니다.

이러한 규칙은 개체 자체의 일부분으로 구성되지만, 개체 관리자를 통해 개체 정의에서 NAT 컨피그레이션을 확인할 수는 없습니다.

패킷이 인터페이스로 들어가면 소스 및 대상 IP 주소 둘 다에서 자동 NAT 규칙을 확인합니다. 별도의 일치를 만든 경우 별도의 규칙을 통해 패킷의 소스 및 대상 주소를 변환할 수 있습니다. 이러한 규칙은 서로 연결되어 있지 않습니다. 트래픽에 따라 규칙의 서로 다른 조합을 사용할 수 있습니다.

규칙은 쌍을 이루지 않으므로 소스A/대상A가 소스A/대상B 이외의 다른 변환을 갖도록 지정할 수 없습니다. 이러한 종류의 기능이 필요한 경우 수동 NAT를 사용하십시오. 그러면 단일 규칙으로 소스 및 대상 주소를 식별할 수 있습니다.

수동 NAT

수동 NAT에서는 소스 주소와 대상 주소를 단일 규칙에서 식별할 수 있습니다. 소스 주소와 대상 주소를 모두 지정하면 소스A/대상A가 소스A/대상B 이외의 다른 변환을 갖도록 지정할 수 있습니다.

참고 고정 NAT의 경우에는 규칙이 양방향이므로, 이 가이드 전체에서 명령 및 설명에 "소스"와 "대상"이 사용됩니다. 특정 연결이 "대상" 주소에서 시작되는 경우에도 마찬가지입니다. 예를 들어 포트 주소 변환 고정 NAT를 구성하고, 소스 주소를 텔넷 서버로 지정하며, 텔넷 서버로 이동하는 모든 트래픽에 대해 포트를 2323에서 23으로 변환하려면 소스 포트가 변환되도록 지정해야 합니다(실제 포트: 23, 매핑된 포트: 2323). 텔넷 서버 주소를 소스 주소로 지정했기 때문에 소스 포트를 지정하는 것입니다.

대상 주소는 선택 사항입니다. 대상 주소를 지정하는 경우 이를 대상 주소 자신에게 매핑할 수도 있고(ID NAT) 다른 주소에 매핑할 수도 있습니다. 대상 주소 매핑은 항상 고정 매핑입니다.

네트워크 자동 NAT와 수동 NAT

이 두 NAT 유형의 주요 차이점은 다음과 같습니다.

- 실제 주소를 정의하는 방법
  - 자동 NAT - NAT 규칙은 네트워크 개체의 매개변수가 됩니다. 네트워크 개체 IP 주소는 원래(실제) 주소 역할을 합니다.
  - 수동 NAT - 실제 주소와 매핑된 주소 모두에서 네트워크 개체 또는 네트워크 개체 그룹을 식별합니다. 이 경우 NAT는 네트워크 개체의 매개변수가 아닙니다. 네트워크 개체 또는 그룹은 NAT 컨피그레이션의 매개변수입니다. 실제 주소에 네트워크 개체 그룹을 사용할 수 있으므로 수동 NAT의 확장성이 더 뛰어납니다.
- 소스 및 대상 NAT의 구현 방법
  - 자동 NAT - 각 규칙을 패킷의 소스 또는 대상에 적용할 수 있습니다. 따라서 소스 IP 주소와 대상 IP 주소에 각각 하나씩 두 개의 규칙이 사용될 수 있습니다. 소스/대상조합에 특정 변환을 적용하기 위해 이러한 두 규칙을 결합할 수 없습니다.
  - 수동 NAT - 단일 규칙이 소스와 대상을 모두 변환합니다. 패킷은 하나의 규칙에서만 일치하며, 더 이상 규칙이 점검되지 않습니다. 선택적인 대상 주소를 구성하지 않더라도 일치하는 패킷은 여전히 하나의 수동 NAT 규칙과만 일치합니다. 소스와 대상이 결합되어 있으므로, 소스/대상조합에 따라 서로 다른 변환을 적용할 수 있습니다. 예를 들어 소스A/대상A의 변환은 소스A/대상B의 변환과 다를 수 있습니다.
- NAT 규칙의 순서
  - 자동 NAT - NAT 테이블에서 순서가 자동으로 지정됩니다.
  - 수동 NAT - NAT 테이블에서 순서를 수동으로 지정합니다(자동 NAT 규칙 앞 또는 뒤).

NAT 규칙 순서

자동 NAT 및 수동 NAT 규칙은 세 개의 섹션으로 구분되는 단일 테이블에 저장됩니다. 섹션 1 규칙이 먼저 적용된 다음, 일치가 발견될 때까지 섹션 2, 마지막으로 섹션 3이 적용됩니다. 예를 들어 섹션 1에서 일치가 발견되면 섹션 2와 3은 평가되지 않습니다. 다음 표는 각 섹션 내의 규칙 순서를 보여줍니다.

표 *3: NAT* 규칙 테이블

테이블 섹션	규칙 유형	섹션 내 규칙의 순서
섹션 1	수동 NAT	첫 번째 일치부터 컨피그레이션에 나타나는 순서대로 적용됩니다. 첫 번째 일치가 적용되므로, 일반 규칙 앞에 특수 규칙이 오도록 해야 합니다. 그렇지 않으면 특수 규칙이 원하는 대로 적용되지 않을 수 있습니다. 기본적으로 수동 NAT 규칙은 섹션 1에 추가됩니다.
섹션 2	자동 NAT	섹션 1에서 일치하는 항목을 찾을 수 없으면 섹션 2 규칙이 다음 순서로 적용됩니다. **1** 고정 규칙. **2** 동적 규칙. 각 규칙 유형 내에서는 다음의 순서 지침이 사용됩니다. **1** 실제 IP 주소의 수량 - 가장 적은 것에서 가장 많은 것. 예를 들면 주소가 1개인 개체가 주소가 10개인 개체보다 먼저 평가됩니다. **2** 수량이 동일한 경우 IP 주소 번호가 낮은 것에서 높은 것 순으로 사용됩니다. 예를 들면, 10.1.1.0이 11.1.1.0보다 먼저 평가됩니다. **3** IP 주소가 동일한 경우 네트워크 개체의 이름이 알파벳순으로 사용됩니다. 예를 들면 abracadabra가 catwoman보다 먼저 평가됩니다.
섹션 3	수동 NAT	아직도 일치가 발견되지 않으면 섹션 3 규칙이 첫 번째부터 컨피그레이션에 나타나는 순서대로 적용됩니다. 이 섹션에는 가장 일반적인 규칙을 포함해야 합니다. 또한 이 섹션에서는 특정 규칙이 일반 규칙보다 먼저 적용되도록 해야 합니다.

예를 들어 섹션 2 규칙의 경우 네트워크 개체 내에서 다음 IP 주소를 정의합니다.

- 192.168.1.0/24 (static)
- 192.168.1.0/24 (dynamic)
- 10.1.1.0/24 (static)
- 192.168.1.1/32 (static)
- 172.16.1.0/24 (dynamic) (object def)
- 172.16.1.0/24 (dynamic) (object abc)

결과 순서는 다음과 같습니다.

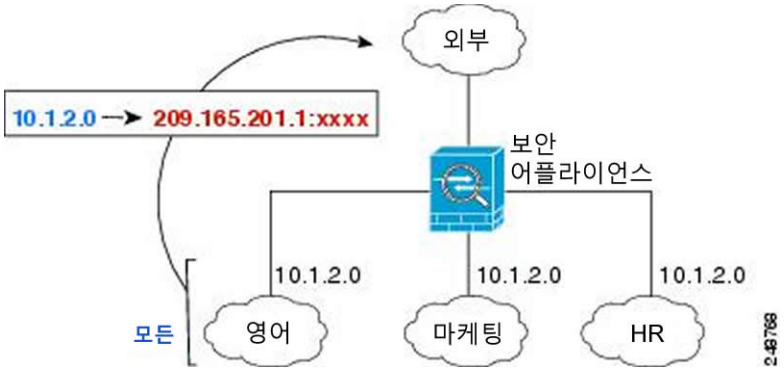
- 192.168.1.1/32 (static)
- 10.1.1.0/24 (static)
- 192.168.1.0/24 (static)
- 172.16.1.0/24 (dynamic) (object abc)
- 172.16.1.0/24 (dynamic) (object def)
- 192.168.1.0/24 (dynamic)

NAT 인터페이스

브리지 그룹 구성원 인터페이스를 제외한 임의의 인터페이스(즉, 모든 인터페이스)에 적용할 NAT 규칙을 구성할 수도 있고, 특정 실제 및 매핑된 인터페이스를 지정할 수도 있습니다. 실제 주소에는 임의의 인터페이스를 지정하고, 매핑된 주소에는 특정 인터페이스를 지정하거나, 그 반대로 지정할 수도 있습니다.

예를 들어, 여러 인터페이스에서 동일한 사설 주소를 사용하며, 외부에 액세스할 때 이들을 모두 동일한 전역 풀로 변환하려는 경우 실제 주소에는 임의의 인터페이스를 지정하고, 매핑된 주소에는 외부 인터페이스를 지정할 수 있습니다.

그림 *4:* 임의의 인터페이스 지정



그러나 브리지 그룹 구성원 인터페이스에는 "임의" 인터페이스라는 개념이 적용되지 않습니다. "임의" 인터페이스를 지정하면 모든 브리지 그룹 구성원 인터페이스는 제외됩니다. 따라서 브리지 그룹 구성원에 NAT를 적용하려면 구성원 인터페이스를 지정해야 합니다. 이렇게 하면 유사한 여러 규칙에서 인터페이스 하나만 다른 현상이 발생할 수 있습니다. BVI(브리지 가상 인터페이스) 자체에 대해서는 NAT를 구성할 수 없으며 구성원 인터페이스에 대해서만 NAT를 구성할 수 있습니다.

NAT 라우팅 구성

Firepower Threat Defense 디바이스는 변환(매핑)된 주소로 전송되는 모든 패킷의 대상이 되어야 합니다.

패킷을 전송할 때 디바이스는 대상 인터페이스를 지정한 경우 해당 인터페이스를 사용하고, 그렇지 않으면 라우팅 테이블 조회를 사용하여 이그레스 인터페이스를 결정합니다. ID NAT의 경우에는 대상 인터페이스를 지정하더라도 경로 조회를 사용하는 옵션이 있습니다.

필요한 라우팅 컨피그레이션의 유형은 다음 항목에서 설명하는 것처럼 매핑된 주소의 유형에 따라 다릅니다.

매핑된 인터페이스와 동일한 네트워크의 주소

대상(매핑된) 인터페이스와 동일한 네트워크의 주소를 사용하는 경우 Firepower Threat Defense 디바이스는 매핑된 주소에 대한 ARP 요청에 답하기 위해 프록시 ARP를 사용하며, 이에 따라 매핑된 주소로 가야 하는 트래픽을 가로챕니다. Firepower Threat Defense 디바이스가 추가 네트워크에 대한 게이트웨이가 될 필요가 없으므로 이 솔루션은 라우팅을 간소화합니다. 이 솔루션은 외부 네트워크에 적절한 수의 여유 주소가 있는 경우 이상적이며, 동적 NAT 또는 고정 NAT 등 1:1 변환을 사용하는 경우 고려해볼 수 있습니다. 동적 PAT는 소수의 주소로 사용 가능한 변환의 수를 크게 확장합니다. 따라서 외부 네트워크에 사용 가능한 주소가 적어도 이 방법을 사용할 수 있습니다. PAT의 경우 매핑된 인터페이스의 IP 주소를 사용할 수도 있습니다.

고유한 네트워크의 주소

대상(매핑된) 인터페이스 네트워크에서 사용할 수 있는 것보다 더 많은 주소가 필요한 경우 별도의 서브넷에서 주소를 지정할 수 있습니다. 업스트림 라우터에는 Firepower Threat Defense 디바이스를 가리키는, 매핑된 주소에 대한 고정 경로가 필요합니다.

실제 주소와 동일한 주소**(ID NAT)**

ID NAT의 기본 동작은 프록시 ARP를 활성화하고 기타 고정 NAT 규칙을 확인하는 것입니다. 원하는 경우 프록시 ARP를 비활성화할 수 있습니다. 원하는 경우 정기적인 고정 NAT에 대해 프록시 ARP를 비활성화할 수도 있습니다. 이 경우 업스트림 라우터에 적절한 경로가 있어야 합니다.

일반적으로 ID NAT에는 프록시 ARP가 필요하지 않으며, 프록시 ARP를 사용할 경우 연결 문제가 발생할 수도 있습니다. 예를 들어 "any" IP 주소에 대해 광범위한 ID NAT 규칙을 구성하고 프록시 ARP를 활성 상태로 유지하면 매핑된 인터페이스에 직접 연결된 네트워크에서 호스트 문제가 발생할 수 있습니다. 이 경우 매핑된 네트워크의 호스트가 동일한 네트워크의 다른 호스트와 통신하려면 ARP 요청의 주소가 NAT 규칙과 일치해야 합니다("any" 주소와 일치). 그러면 Firepower Threat Defense 디바이스는 패킷이 실제로 Firepower Threat Defense 디바이스로 이동하도록 지정되지 않아도 주소에 대해 ARP를 프록시 설정합니다. (이 문제는 수동 NAT 규칙이 있는 경우에도 발생합니다. NAT 규칙은 소스 주소 및 대상 주소와 모두 일치해야 하지만 프록시 ARP 결정은 "소스" 주소에 대해서만 내려집니다.) 실제 호스트 ARP 응답 전에 Firepower Threat Defense 디바이스 ARP 응답이 수신되는 경우에는 트래픽이 Firepower Threat Defense 디바이스로 잘못 전송됩니다.

NAT용 지침

다음 주제에서는 NAT 구현에 대한 자세한 지침을 제공합니다.

인터페이스 지침

NAT는 표준 라우팅 물리적 또는 하위 인터페이스에 대해 지원됩니다.

그러나 브리지 그룹 구성원 인터페이스, 즉 BVI(브리지 가상 인터페이스)에 속하는 인터페이스에 대해 NAT를 구성할 때는 다음과 같은 제한이 있습니다.

- 브리지 그룹 구성원에 대해 NAT를 구성할 때는 구성원 인터페이스를 지정합니다. BVI(브리지 그룹 인터페이스) 자체에 대해서는 NAT를 구성할 수 없습니다.
- 브리지 그룹 구성원 인터페이스 간에 NAT를 수행할 때는 소스 및 대상 인터페이스를 지정해야 합니다. 인터페이스로 "임의"를 지정할 수는 없습니다.
- 대상 인터페이스가 브리지 그룹 구성원 인터페이스일 때는 인터페이스 PAT를 구성할 수 없습니다. 인터페이스에 연결된 IP 주소가 없기 때문입니다.
- 원본 및 대상 인터페이스가 동일한 브리지 그룹의 구성원이면 IPv4 및 IPv6 네트워크(NAT64/46) 간을 변환할 수 없습니다. 지원되는 방법은 고정 NAT/PAT 44/66, 동적 NAT44/66 및 동적 PAT44 뿐이며 동적 PAT66은 지원되지 않습니다.

IPv6 NAT 지침

NAT는 다음 지침 및 제약 사항과 함께 IPv6를 지원합니다.

- 표준 라우팅 모드 인터페이스에서는 IPv4와 IPv6 간을 변환할 수도 있습니다.
- 동일한 브리지 그룹의 구성원인 인터페이스에 대해서는 IPv4 및 IPv6 간을 변환할 수 없습니다. 두 IPv6 또는 두 IPv4 네트워크 간에만 변환을 수행할 수 있습니다. 브리지 그룹 구성원과 표준 라우팅 인터페이스 간 변환에는 이 제한이 적용되지 않습니다.
- 같은 브리지 그룹의 인터페이스 간 변환에는 IPv6에 대해 동적 PAT(NAT66)를 사용할 수 없습니다. 브리지 그룹 구성원과 표준 라우팅 인터페이스 간 변환에는 이 제한이 적용되지 않습니다.
- 고정 NAT에서는 IPv6 서브넷을 최대 /64까지 지정할 수 있습니다. 더 큰 서브넷은 지원되지 않습니다.
- FTP with NAT46을 사용할 때, IPv4 FTP 클라이언트가 IPv6 FTP 서버에 연결될 때 클라이언트는 확장 패시브 모드(EPSV) 또는 확장 포트 모드(EPRT)를 사용해야 하며, PASV 및 PORT 명령은 IPv6에서 지원되지 않습니다.

IPv6 NAT 권장 사항

IPv6 네트워크 간 변환 및 IPv4와 IPv6 네트워크 간 변환(라우팅된 모드 전용)을 위해 NAT를 사용할 수 있습니다. 다음의 모범 사례를 권장합니다.

- NAT66(IPv6-IPv6) - 고정 NAT를 사용하는 것이 좋습니다. 동적 NAT 또는 PAT를 사용할 수 있고 IPv6 주소가 대량으로 공급되지만, 동적 NAT를 반드시 사용할 필요는 없습니다. 반환 트래픽을 허용하지 않으려면 고정 NAT 규칙을 단방향으로 설정할 수 있습니다(수동 NAT에만 해당함).

- NAT46(IPv4-IPv6) - 고정 NAT를 사용하는 것이 좋습니다. IPv6 주소 공간이 IPv4 주소 공간보다 훨씬 크기 때문에 고정 변환을 손쉽게 수용할 수 있습니다. 반환 트래픽을 허용하지 않으려면 고정 NAT 규칙을 단방향으로 설정할 수 있습니다(수동 NAT에만 해당함). IPv6 서브넷(/96 이하)으로 변환하면 결과로 나타나는 매핑된 주소는 기본적으로 IPv4가 포함된 IPv6 주소입니다. 이 경우 IPv6 접두사 뒤에 IPv4 주소의 32비트가 포함됩니다. 예를 들어 IPv6 접두사가 /96 접두사이면, 주소의 마지막 32비트에 IPv4 주소가 첨부됩니다. 예를 들어 192.168.1.0/24를 201b::0/96에 매핑하면 192.168.1.4는 201b::0.192.168.1.4(혼합된 표기로 표시됨)에 매핑됩니다. 접두사가 더 작으면(예: /64) IPv4 주소가 접두사 뒤에 첨부되고, 접미사 0이 IPv4 주소 뒤에 첨부됩니다.
- NAT64(IPv6-to-IPv4) - IPv6 주소의 수를 수용할 만큼 IPv4 주소가 충분하지 않을 수 있습니다. 대량의 IPv4 변환을 제공하려면 동적 PAT 풀을 사용하는 것이 좋습니다.

검사된 프로토콜에 대한 **NAT** 지원

보조 연결을 열거나 패킷에 IP 주소를 포함한 일부 애플리케이션 레이어 프로토콜을 검사하여 다음 서비스를 제공합니다.

- 핀홀 생성 - 일부 애플리케이션 프로토콜은 표준 포트 또는 협상된 포트에서 보조 TCP 또는 UDP 연결을 엽니다. 검사에서는 이러한 보조 포트를 허용하기 위한 액세스 제어 규칙을 생성할 필요가 없도록 해당 포트에 대해 핀홀을 엽니다.
- NAT 재작성 - FTP 등의 프로토콜은 프로토콜의 일부분으로 패킷 데이터에 보조 연결용 IP 주소 및 포트를 포함합니다. 엔드포인트 중 하나에서 NAT 변환이 수행되는 경우 검사 엔진은 포함된 주소와 포트의 NAT 변환을 반영하기 위해 패킷 데이터를 재작성합니다. NAT 재작성이 수행되지 않으면 보조 연결은 작동하지 않습니다.
- 프로토콜 적용 - 일부 검사에서는 검사된 프로토콜에 대해 특정 수준의 RFC 적합성을 적용합니다.

다음 표에는 NAT 재작성을 적용하는 검사된 프로토콜 및 이러한 프로토콜의 NAT 제한이 나와 있습니다. 이러한 프로토콜을 포함하는 NAT 규칙을 작성할 때는 이와 같은 제한에 주의해야 합니다. 여기에 나와 있지 않은 검사된 프로토콜은 NAT 재작성을 적용하지 않습니다. 이러한 검사에는 GTP, HTTP, IMAP, POP, SMTP, SSH 및 SSL이 포함됩니다.

참고 NAT 재작성은 여기에 나와 있는 포트에서만 지원됩니다. 비표준 포트에서 이러한 프로토콜을 사용하는 경우에는 연결에 NAT를 사용하지 마십시오.

표 ***4: NAT***가 지원되는 애플리케이션 검사

애플리케이션	검사된 프로토콜, 포트	**NAT** 제한	핀홀 생성 여부
DCERPC	TCP/135	NAT64 없음.	예
DNS over UDP	UDP/53	WINS를 통한 이름 확인에 NAT 지원을 이용할 수 없음.	아니요

애플리케이션	검사된 프로토콜, 포트	NAT 제한	핀홀 생성 여부
ESMTP	TCP/25	NAT64 없음.	아니요
FTP	TCP/21	제한 없음	예
H.323 H.225(호출 신호) H.323 RAS	TCP/1720 UDP/1718 RAS의 경우 UDP/1718-1719	NAT64 없음.	예
ICMP ICMP Error	ICMP (디바이스 인터페이스로 전달된 ICMP 트래픽은 검사되지 않음)	제한 없음	아니요
IP Options	RSVP	NAT64 없음.	아니요
NetBIOS Name Server over IP	UDP/137, 138(소스 포트)	NAT64 없음.	아니요
RSH	TCP/514	PAT 없음. NAT64 없음.	예
RTSP	TCP/554 (HTTP 클로킹을 처리하지 않음)	NAT64 없음.	예
SIP	TCP/5060 UDP/5060	확장 PAT 없음. NAT64 또는 NAT46 없음.	예
Skinny(SCCP)	TCP/2000	NAT64, NAT46 또는 NAT66 없음.	예
SQL*Net (버전 1, 2)	TCP/1521	NAT64 없음.	예
Sun RPC	TCP/111 UDP/111	NAT64 없음.	예
TFTP	UDP/69	NAT64 없음. 페이로드 IP 주소는 변환되지 않습니다.	예
XDMCP	UDP/177	NAT64 없음.	예

NAT 추가 지침

- 브리지 그룹 구성원인 인터페이스의 경우 구성원 인터페이스용 NAT 규칙을 작성합니다. BVI(브리지 가상 인터페이스) 자체에 대해서는 NAT 규칙을 작성할 수 없습니다.
- (자동 NAT만 해당) 한 개체에는 단일 NAT 규칙만 정의할 수 있습니다. 한 개체에 대해 여러 NAT 규칙을 구성하려면 동일한 IP 주소를 지정하는 서로 다른 이름의 여러 개체를 생성해야 합니다.
- 인터페이스에 VPN이 정의되어 있으면 인터페이스의 인바운드 ESP 트래픽에는 NAT 규칙이 적용되지 않습니다. 시스템은 설정된 VPN 터널에 대해서만 ESP 트래픽을 허용하며 기존 터널과 연결되지 않은 트래픽은 삭제합니다. 이러한 제한은 ESP 및 UDP 포트 500과 4500에 적용됩니다.
- NAT 컨피그레이션을 변경할 때 새 NAT 컨피그레이션이 사용되기 전에 기존 변환이 시간 초과되기까지 기다리지 않으려면 디바이스 CLI에서 **clear xlate** 명령을 사용하여 변환 테이블을 지울 수 있습니다. 그러나 변환 테이블을 지우면 변환을 사용하는 현재의 모든 연결이 해제됩니다.

  참고 동적 NAT 또는 PAT 규칙을 제거한 후 제거된 규칙의 주소와 겹치는 매핑된 주소가 포함된 새 규칙을 추가하는 경우, 새 규칙을 사용하려면 제거된 규칙과 관련된 모든 연결이 시간 초과되기까지 기다리거나 **clear xlate** 명령으로 해당 연결을 지워야 합니다. 이러한 안전 조치는 동일한 주소가 여러 호스트에 할당되는 것을 방지합니다.

- IPv4 및 IPv6 주소를 모두 포함하는 개체 그룹은 사용할 수 없습니다. 개체 그룹에는 한 가지 주소 유형만 포함해야 합니다.
- (수동 NAT에만 해당함) NAT 규칙에서 **any**를 소스 주소로 사용하는 경우 "any" 트래픽의 정의(IPv4 대 IPv6)는 규칙에 따라 다릅니다. Firepower Threat Defense 디바이스가 패킷에 대해 NAT를 수행하기 전에 패킷은 IPv6-IPv6 또는 IPv4-IPv4여야 합니다. 이 전제 조건 하에 Firepower Threat Defense 디바이스는 NAT 규칙에서 **any**의 값을 결정할 수 있습니다. 예를 들어 **any**에서 IPv6 서버로 규칙을 구성하며 해당 서버가 IPv4 주소에서 매핑된 것이면 any는 "모든 IPv6 트래픽"을 의미합니다. “any” to “any”로 규칙을 구성하며 소스를 인터페이스 IPv4 주소로 매핑하면 **any**는 “모든 IPv4 트래픽”을 의미합니다. 매핑된 인터페이스 주소는 대상 주소도 IPv4임을 암시하기 때문입니다.
- 여러 NAT 규칙에서 동일한 매핑된 개체 또는 그룹을 사용할 수 있습니다.
- 매핑된 IP 주소 풀에는 다음을 포함할 수 없습니다.
  - 매핑된 인터페이스 IP 주소. 규칙에 대해 "any" 인터페이스를 지정하면 모든 인터페이스 IP 주소가 허용되지 않습니다. 인터페이스 PAT(라우팅 모드만 해당함)의 경우 인터페이스 주소 대신 인터페이스 이름을 사용합니다.
  - 장애 조치 인터페이스 IP 주소
  - (동적 NAT) VPN이 활성화된 경우의 스탠바이 인터페이스 IP 주소

- 고정 및 동적 NAT 정책에서는 겹치는 주소 사용을 피해야 합니다. 예를 들어, PPTP의 보조 연결이 동적 xlate 대신 고정 상태인 경우 겹치는 주소를 사용하면 PPTP 연결 설정에 실패할 수 있습니다.
- 규칙에서 대상 인터페이스를 지정하는 경우에는 라우팅 테이블에서 경로를 조회하지 않고 해당 인터페이스를 이그레스 인터페이스로 사용합니다. 그러나 ID NAT의 경우에는 경로 조회를 대신 사용할 수 있는 옵션이 제공됩니다.

NAT 구성

네트워크 주소 변환은 매우 복잡해질 수 있습니다. 따라서 변환 문제와 까다로운 트러블슈팅 상황을 방지하기 위해 규칙을 최대한 단순하게 유지하는 것이 좋습니다. 그리고 NAT를 구현하기 전에 면밀한 계획을 세워야 합니다. 다음 절차에서는 기본적인 구성 방식에 대해 설명합니다.

절차

단계 **1** **Policies(**정책**)** > **NAT**를 선택합니다.

단계 **2** 필요한 규칙의 종류를 결정합니다.
동적 NAT, 동적 PAT, 고정 NAT 및 ID NAT 규칙을 생성할 수 있습니다. 이와 관련된 개요는 NAT 유형, 167 페이지를 참조하십시오.

단계 **3** 수동 또는 자동 NAT로 구현할 규칙을 결정합니다.
이 두 가지 구현 옵션을 비교한 내용은 자동 NAT 및 수동 NAT, 168 페이지를 참조하십시오.

단계 **4** 다음 섹션에서 설명하는 대로 규칙을 생성합니다.

- 동적 NAT, 177 페이지
- 동적 PAT, 183 페이지
- 고정 NAT, 189 페이지
- ID NAT, 198 페이지

단계 **5** NAT 정책 및 규칙을 관리합니다.
다음을 수행하여 정책과 해당 규칙을 관리할 수 있습니다.

- 규칙을 수정하려면 해당 규칙의 수정 아이콘()을 클릭합니다.
- 규칙을 삭제하려면 해당 규칙의 삭제 아이콘()을 클릭합니다.

동적 NAT

다음 주제에서는 동적 NAT 및 동적 NAT를 구성하는 방법에 대해 설명합니다.

동적 NAT 정보

동적 NAT는 실제 주소의 그룹을 대상 네트워크에서 라우팅 가능한 매핑된 주소의 풀로 변환합니다. 매핑된 풀에는 일반적으로 실제 그룹보다 더 적은 수의 주소가 포함되어 있습니다. 변환하려는 호스트가 대상 네트워크에 액세스하면 NAT에서는 매핑된 풀의 IP 주소를 호스트에 할당합니다. 실제 호스트가 연결을 시작하는 경우에만 변환이 생성됩니다. 변환은 연결되어 있는 동안에만 이루어지며, 변환 시간이 초과된 후에는 사용자의 IP 주소가 동일하게 유지되지 않습니다. 따라서 액세스 규칙에서 연결을 허용하더라도, 대상 네트워크의 사용자는 동적 NAT를 사용하는 호스트에 대해 안정적인 연결을 시작할 수 없습니다.

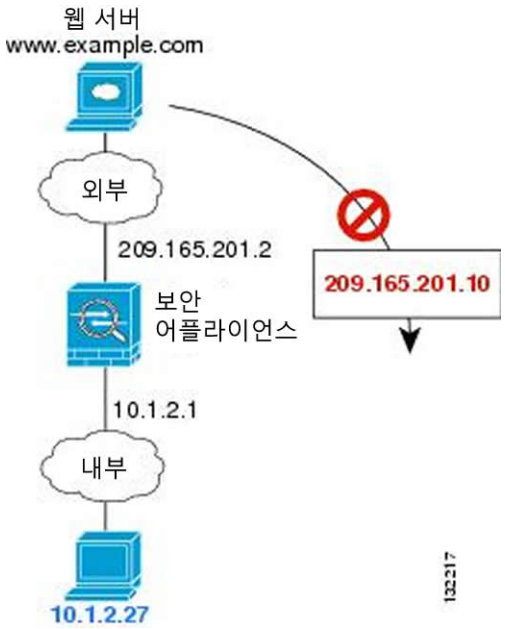
참고 액세스 규칙에서 허용하는 경우, 변환 기간 동안 원격 호스트는 변환된 호스트로의 연결을 시작할 수 있습니다. 주소는 예측할 수 없으므로 호스트로의 연결이 실패할 수 있습니다. 그럼에도 불구하고 이 경우 사용자는 액세스 규칙의 보안에 의존할 수 있습니다.

다음 그림은 일반적인 동적 NAT 시나리오를 보여줍니다. 실제 호스트만 NAT 세션을 생성할 수 있으며 응답 트래픽이 허용됩니다.

그림 *5:* 동적 ***NAT***

다음 그림은 매핑된 주소로 연결을 시작하려고 시도하는 원격 호스트를 보여줍니다. 이 주소는 현재 변환 테이블에 있지 않으므로 패킷이 삭제됩니다.

그림 *6:* 매핑된 주소로 연결을 시작하려고 시도하는 원격 호스트



동적 NAT의 단점 및 장점

동적 NAT의 단점은 다음과 같습니다.

- 매핑된 풀의 주소 수가 실제 그룹의 주소 수보다 적은 경우, 트래픽의 양이 예상보다 많아지면 주소가 부족해질 수 있습니다.

  PAT는 단일 주소의 포트를 사용하여 64,000이 넘는 변환을 제공하므로, 이러한 상황이 발생하면 PAT 또는 PAT 대안을 사용하십시오.

- 매핑된 풀에서 대량의 라우팅 가능한 주소를 사용해야 하는데, 라우팅 가능한 주소는 대량으로 사용 가능하지 않을 수 있습니다.

동적 NAT의 장점은 일부 프로토콜이 PAT를 사용할 수 없다는 것입니다. PAT는 다음과 작동하지 않습니다.

- GRE 버전 0과 같이 오버로드할 포트가 없는 IP 프로토콜.
- 한 포트에 데이터 스트림이 있고 다른 포트에 제어 경로가 있으며 개방형 표준이 아닌 일부 멀티미디어 애플리케이션.

동적 자동 NAT 구성

동적 자동 NAT 규칙을 사용하여 주소를 대상 네트워크에서 라우팅할 수 있는 서로 다른 IP 주소로 변환합니다.

시작하기 전에

개체를 선택하여 규칙에 필요한 네트워크 개체 또는 그룹을 생성합니다. NAT 규칙을 정의하면서 개체를 생성할 수도 있습니다. 개체는 다음 요건을 충족해야 합니다.

- 원 주소 - 이 주소는 그룹이 아닌 네트워크 개체여야 하며 호스트나 서브넷일 수 있습니다.
- 변환된 주소 - 이 주소는 네트워크 개체 또는 그룹일 수는 있지만 서브넷을 포함할 수는 없습니다. IPv4 주소와 IPv6 주소를 모두 포함할 수는 없으며 한 유형만 포함해야 합니다.

절차

단계 **1** **Policies(**정책**)** > **NAT**를 선택합니다.

단계 **2** 다음 중 하나를 수행합니다.

- 새 규칙을 생성하려면 + 버튼을 클릭합니다.
- 기존 규칙을 수정하려면 해당 규칙의 수정 아이콘()을 클릭합니다.

더 이상 필요하지 않은 규칙을 삭제하려면 해당 규칙의 휴지통 아이콘을 클릭합니다.

단계 **3** 기본 규칙 옵션을 구성합니다.

- 제목 - 규칙의 이름을 입력합니다.
- 규칙 생성 - 자동 **NAT**를 선택합니다.
- 유형 - 동적을 선택합니다.

단계 **4** 다음 패킷 변환 옵션을 구성합니다.

- **Source Interface(**소스 인터페이스**)**, **Destination Interface(**대상 인터페이스**)** — (브리지 그룹 구성원 인터페이스의 경우 필수)이 NAT 규칙이 적용되는 인터페이스를 선택합니다. **Source(**소스**)**는 트래픽이 디바이스로 들어가는 데 사용되는 실제 인터페이스입니다. **Destination(**대상**)**은 트래픽이 디바이스에서 나오는 데 사용되는 매핑된 인터페이스입니다. 기본적으로 규칙은 브리지 그룹 구성원 인터페이스를 제외한 모든 인터페이스**(Any(**모두**))**에 적용됩니다.
- 원본 주소 - 변환하는 주소가 포함된 네트워크 개체입니다.
- 변환된 주소 - 매핑된 주소를 포함하는 네트워크 개체 또는 그룹입니다.

단계 **5** (선택 사항). 고급 옵션 링크를 클릭하고 원하는 옵션을 선택합니다.

- **Translate DNS replies that match this rule(**이 규칙과 일치하는 **DNS** 응답 변환**)** — DNS 응답의 IP 주소를 변환할지 여부를 선택합니다. 매핑된 인터페이스에서 실제 인터페이스로 이동하는

DNS 응답의 경우 주소(IPv4 A 또는 IPv6 AAAA) 레코드가 매핑된 값에서 실제 값으로 재작성됩니다. 반대로, 실제 인터페이스에서 매핑된 인터페이스로 이동하는 DNS 응답의 경우 실제 값에서 매핑된 값으로 레코드가 재작성됩니다. 이 옵션은 특정 상황에서 사용되며, 재작성 시 A 레코드와 AAAA 레코드 간의 변환도 수행되는 NAT64/46 변환에 필요한 경우도 있습니다. 자세한 내용은 NAT를 사용하여 DNS 쿼리 및 응답 재작성, 242 페이지를 참고하십시오.

- **Fallthrough to Interface PAT (Destination Interface)(**인터페이스 **PAT(**대상 인터페이스**)**로 폴스루**)** — 다른 매핑된 주소가 이미 할당된 경우 대상 인터페이스의 IP 주소를 백업 방법으로 사용할지 여부를 선택합니다(인터페이스 PAT 대체). 이 옵션은 브리지 그룹의 구성원이 아닌 대상 인터페이스를 선택한 경우에만 사용할 수 있습니다.

단계 **6** **OK(**확인**)**를 클릭합니다.

동적 수동 **NAT** 구성

자동 NAT가 요구를 충족하지 않을 때는 동적 수동 NAT 규칙을 사용합니다. 대상에 따라 다른 변환을 수행하려는 경우를 예로 들 수 있습니다. 동적 NAT는 주소를 대상 네트워크에서 라우팅할 수 있는 서로 다른 IP 주소로 변환합니다.

시작하기 전에

개체를 선택하여 규칙에 필요한 네트워크 개체 또는 그룹을 생성합니다. 그룹은 IPv4 주소와 IPv6 주소를 모두 포함할 수는 없으며 한 유형만 포함해야 합니다. NAT 규칙을 정의하면서 개체를 생성할 수도 있습니다. 개체는 다음 요건도 충족해야 합니다.

- 원본 소스 주소 - 이 주소는 네트워크 개체 또는 그룹일 수 있으며 호스트나 서브넷을 포함할 수 있습니다. 모든 원 원본 트래픽을 변환하려는 경우 이 단계를 건너뛰고 규칙에서 임의를 지정하면 됩니다.
- 변환된 원본 주소 - 이 주소는 네트워크 개체 또는 그룹일 수는 있지만 서브넷을 포함할 수는 없습니다.

규칙에서 원 대상 주소 및 변환된 대상 주소에 대해 정적 변환을 구성하는 경우 이러한 주소에 대해 네트워크 개체를 생성할 수도 있습니다.

동적 NAT의 경우 대상에 대해 포트 변환을 수행할 수도 있습니다. 개체 관리자에서 원 대상 포트 및 변환된 대상 포트에 사용할 수 있는 포트 개체가 있는지 확인합니다. 소스 포트를 지정하면 무시됩니다.

절차

단계 **1** **Policies(**정책**)** > **NAT**를 선택합니다.

단계 **2** 다음 중 하나를 수행합니다.

- 새 규칙을 생성하려면 + 버튼을 클릭합니다.

- 기존 규칙을 수정하려면 해당 규칙의 수정 아이콘( )을 클릭합니다.

더 이상 필요하지 않은 규칙을 삭제하려면 해당 규칙의 휴지통 아이콘을 클릭합니다.

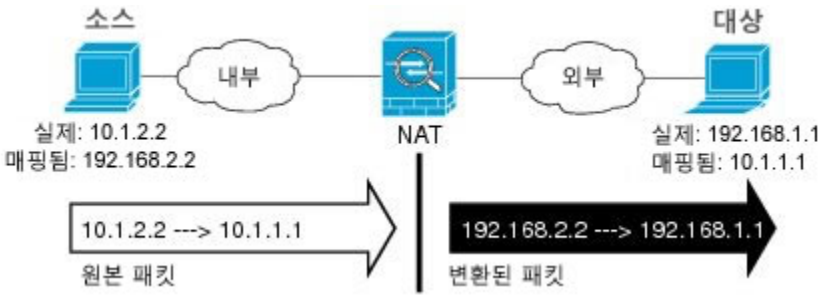
단계 **3** 기본 규칙 옵션을 구성합니다.

- 제목 - 규칙의 이름을 입력합니다.
- 규칙 생성 - 수동 **NAT**를 선택합니다.
- **Rule Placement(**규칙 배치**)** - 규칙을 추가할 위치를 선택합니다. 규칙은 카테고리에서 자동 NAT 규칙 앞이나 뒤에 삽입할 수도 있고, 선택한 규칙 위나 아래에 삽입할 수도 있습니다.
- 유형 - 동적을 선택합니다. 이 설정은 원본 주소에만 적용됩니다. 대상 주소에 대한 변환을 정의하는 경우 변환은 항상 고정입니다.

단계 **4** 다음 인터페이스 옵션을 구성합니다.

- **Source Interface(**소스 인터페이스**)**, **Destination Interface(**대상 인터페이스**)** — (브리지 그룹 구성원 인터페이스의 경우 필수)이 NAT 규칙이 적용되는 인터페이스를 선택합니다. **Source(**소스**)**는 트래픽이 디바이스로 들어가는 데 사용되는 실제 인터페이스입니다. **Destination(**대상**)**은 트래픽이 디바이스에서 나오는 데 사용되는 매핑된 인터페이스입니다. 기본적으로 규칙은 브리지 그룹 구성원 인터페이스를 제외한 모든 인터페이스**(Any(**모두**))**에 적용됩니다.

단계 **5** 원본 패킷 주소(IPv4 또는 IPv6)를 식별합니다. 이 주소는 원본 패킷에 표시되는 패킷 주소입니다. 원본 패킷 대 변환된 패킷의 예는 다음 그림을 참조하십시오.



- **Original Source Address(**원본 소스 주소**)** - 변환 중인 주소가 포함된 네트워크 개체 또는 그룹입니다.
- **Original Destination Address(**원본 대상주소**)** - (선택 사항) 대상의 주소를 포함하는 네트워크 개체입니다. 이 옵션을 비워 두면 대상에 관계없이 소스 주소 변환이 적용됩니다. 대상 주소를 지정하면 해당 주소에 대해 고정 변환을 구성할 수도 있고 단순히 ID NAT를 사용할 수도 있습니다.

  Interface(인터페이스**)**를 선택하여 소스 인터페이스(Any(모두)일 수 없음)를 기준으로 원본 대상을 지정할 수 있습니다. 이 옵션을 선택할 경우 변환된 대상 개체도 선택해야 합니다. 대상 주소에 대해 포트 변환을 사용하여 고정 인터페이스 NAT를 구현하려면 이 옵션을 선택하고 대상 포트에 대해 적절한 포트 개체도 선택합니다.

단계 **6** 변환된 패킷 주소(IPv4 또는 IPv6), 즉 대상 인터페이스 네트워크에 나타나는 패킷 주소를 확인합니다. 필요에 따라 IPv4 및 IPv6 간에 변환할 수 있습니다.

- 변환된 원본 주소 - 매핑된 주소를 포함하는 네트워크 개체 또는 그룹입니다.
- 변환된 대상 주소 - (선택 사항) 변환된 패킷에서 사용되는 대상 주소를 포함하는 네트워크 개체 또는 그룹입니다. 원 대상 주소에 대해 개체를 선택한 경우 동일한 개체를 선택하여 ID NAT(변환 없음)를 설정할 수 있습니다.

단계 **7** (선택 사항). 서비스 변환용 대상 서비스 포트(**Original Destination Port**(원본 대상 포트), **Translated Destination Port**(변환된 대상 포트))를 식별합니다.
동적 NAT는 포트 변환을 지원하지 않으므로 **Original Destination Port**(원본 대상 포트) 및 **Translated Destination Port**(변환된 대상 포트) 필드를 비워 둡니다. 그러나 대상 변환은 항상 고정이므로 대상 포트의 포트 변환을 수행할 수 있습니다.

NAT는 TCP 또는 UDP만 지원합니다. 포트를 변환할 때는 실제 서비스 개체의 프로토콜과 매핑된 서비스 개체의 프로토콜이 동일해야 합니다(둘 다 TCP거나 둘 다 UDP). ID NAT의 경우 실제 포트와 매핑된 포트에 동일한 서비스 개체를 사용할 수 있습니다.

단계 **8** (선택 사항). 고급 옵션 링크를 클릭하고 원하는 옵션을 선택합니다.

- **Translate DNS replies that match this rule**(이 규칙과 일치하는 **DNS** 응답 변환) — DNS 응답의 IP 주소를 변환할지 여부를 선택합니다. 매핑된 인터페이스에서 실제 인터페이스로 이동하는 DNS 응답의 경우 주소(IPv4 A 또는 IPv6 AAAA) 레코드가 매핑된 값에서 실제 값으로 재작성됩니다. 반대로, 실제 인터페이스에서 매핑된 인터페이스로 이동하는 DNS 응답의 경우 실제 값에서 매핑된 값으로 레코드가 재작성됩니다. 이 옵션은 특정 상황에서 사용되며, 재작성 시 A 레코드와 AAAA 레코드 간의 변환도 수행되는 NAT64/46 변환에 필요한 경우도 있습니다. 자세한 내용은 NAT를 사용하여 DNS 쿼리 및 응답 재작성, 242 페이지를 참고하십시오.
- **Fallthrough to Interface PAT (Destination Interface)**(인터페이스 **PAT**(대상 인터페이스)로 폴스루) — 다른 매핑된 주소가 이미 할당된 경우 대상 인터페이스의 IP 주소를 백업 방법으로 사용할지 여부를 선택합니다(인터페이스 PAT 대체). 이 옵션은 브리지 그룹의 구성원이 아닌 대상 인터페이스를 선택한 경우에만 사용할 수 있습니다.

단계 **9** **OK**(확인)를 클릭합니다.

동적 **PAT**

다음 주제에서는 동적 PAT에 대해 설명합니다.

동적 **PAT** 정보

동적 PAT는 실제 주소 및 소스 포트를 매핑된 주소 및 고유한 포트로 변환함으로써 여러 실제 주소를 단일 매핑된 IP 주소로 변환합니다. 사용 가능한 경우 매핑된 포트에 실제 소스 포트 번호가 사용됩니다. 그러나 실제 포트를 사용할 수 없는 경우, 기본적으로 실제 포트 번호와 동일한 포트 범위(0~511,

512~1023 및 1024~65535)에서 매핑된 포트가 선택됩니다. 따라서 1024 아래의 포트는 작은 PAT 풀만 사용할 수 있습니다.

소스 포트는 각 연결에 대해 다르므로 연결마다 별도의 변환 세션이 필요합니다. 예를 들어 10.1.1.1:1025를 사용하려면 10.1.1.1:1026에서 별도로 변환해야 합니다.

다음 그림은 일반적인 동적 PAT 시나리오를 보여줍니다. 실제 호스트만 NAT 세션을 생성할 수 있으며 응답 트래픽이 허용됩니다. 매핑된 주소는 각 변환에 대해 동일하지만 포트는 동적으로 할당됩니다.

그림 *7:* 동적 ***PAT***

액세스 규칙에서 허용하는 경우, 변환 기간 동안 대상 네트워크의 원격 호스트는 변환된 호스트로의 연결을 시작할 수 있습니다. 포트 주소(실제 및 매핑된 주소 모두)는 예측할 수 없으므로 호스트에 대한 연결이 실패할 수 있습니다. 그럼에도 불구하고 이 경우 사용자는 액세스 규칙의 보안에 의존할 수 있습니다.

연결이 만료되면 포트 변환도 만료됩니다.

동적 **PAT**의 단점 및 장점

동적 PAT에서는 단일 매핑된 주소를 사용하여 라우팅 가능한 주소를 아낄 수 있습니다. Firepower Threat Defense 디바이스 인터페이스 IP 주소를 PAT 주소로 사용할 수도 있습니다. 그러나 인터페이스의 IPv6 주소에 대해서는 인터페이스 PAT를 사용할 수 없습니다.

같은 브리지 그룹의 인터페이스 간 변환에는 IPv6에 대해 동적 PAT(NAT66)를 사용할 수 없습니다. 브리지 그룹 구성원과 표준 라우팅 인터페이스 간 변환에는 이 제한이 적용되지 않습니다.

데이터 스트림이 제어 경로와 다른 일부 멀티미디어 애플리케이션에서는 동적 PAT가 작동하지 않습니다. 자세한 내용은 검사된 프로토콜에 대한 NAT 지원, 174 페이지를 참조하십시오.

동적 PAT는 단일 IP 주소에서 오는 것으로 보이는 대량의 연결을 생성할 수 있으며, 서버는 이 트래픽을 DoS 공격으로 해석할 수 있습니다.

동적 자동 **PAT** 구성

동적 자동 PAT 규칙을 사용하여 주소를 여러 IP 주소만으로 변환하는 대신 고유한 IP 주소/포트 조합으로 변환합니다. 단일 주소(대상 인터페이스의 주소 또는 다른 주소)로 변환할 수 있습니다.

시작하기 전에

개체를 선택하여 규칙에 필요한 네트워크 개체 또는 그룹을 생성합니다. NAT 규칙을 정의하면서 개체를 생성할 수도 있습니다. 개체는 다음 요건을 충족해야 합니다.

- 원본 주소 - 이 주소는 그룹이 아닌 네트워크 개체여야 하며 호스트나 서브넷일 수 있습니다.
- 변환된 주소 - 다음 옵션을 사용하여 PAT 주소를 지정할 수 있습니다.
  - 대상 인터페이스 - 대상 인터페이스 IPv4 주소를 사용하려는 경우 네트워크 개체가 필요하지 않습니다. IPv6에는 인터페이스 PAT를 사용할 수 없습니다.
  - 단일 **PAT** 주소 - 단일 호스트를 포함하는 네트워크 개체를 생성합니다.

절차

단계 **1** **Policies(**정책**)** > **NAT**를 선택합니다.

단계 **2** 다음 중 하나를 수행합니다.

- 새 규칙을 생성하려면 + 버튼을 클릭합니다.
- 기존 규칙을 수정하려면 해당 규칙의 수정 아이콘( )을 클릭합니다.

더 이상 필요하지 않은 규칙을 삭제하려면 해당 규칙의 휴지통 아이콘을 클릭합니다.

단계 **3** 기본 규칙 옵션을 구성합니다.

- 제목 - 규칙의 이름을 입력합니다.
- 규칙 생성 - 자동 **NAT**를 선택합니다.
- 유형 - 동적을 선택합니다.

단계 **4** 다음 패킷 변환 옵션을 구성합니다.

- **Source Interface(**소스 인터페이스**)**, **Destination Interface(**대상 인터페이스**)** — (브리지 그룹 구성원 인터페이스의 경우 필수)이 NAT 규칙이 적용되는 인터페이스를 선택합니다. **Source(**소스**)**는 트래픽이 디바이스로 들어가는 데 사용되는 실제 인터페이스입니다. **Destination(**대상**)**은 트래픽이 디바이스에서 나오는 데 사용되는 매핑된 인터페이스입니다. 기본적으로 규칙은 브리지 그룹 구성원 인터페이스를 제외한 모든 인터페이스(**Any(**모두**)**)에 적용됩니다.
- 원 주소 - 변환하는 주소가 포함된 네트워크 개체입니다.
- 변환된 주소 - 다음 중 하나입니다.
  - (인터페이스 PAT) 대상 인터페이스의 IPv4 주소를 사용하려면 인터페이스를 선택합니다. 특정 대상 인터페이스도 선택해야 합니다. 이 인터페이스는 브리지 그룹 구성원 인터페이스일 수 없습니다. IPv6에는 인터페이스 PAT를 사용할 수 없습니다.

◦ 대상 인터페이스 주소가 아닌 단일 주소를 사용하려면 이러한 용도로 생성한 호스트 네트워크 개체를 선택합니다.

단계 **5** (선택 사항). 고급 옵션 링크를 클릭하고 원하는 옵션을 선택합니다.

- **Fallthrough to Interface PAT (Destination Interface)(**인터페이스 **PAT(**대상 인터페이스**)**로 폴스루**)** — 다른 매핑된 주소가 이미 할당된 경우 대상 인터페이스의 IP 주소를 백업 방법으로 사용할지 여부를 선택합니다(인터페이스 PAT 대체). 이 옵션은 브리지 그룹의 구성원이 아닌 대상 인터페이스를 선택한 경우에만 사용할 수 있습니다. 인터페이스 PAT를 변환된 주소로 이미 구성한 경우에는 이 옵션을 선택할 수 없습니다. 또한 IPv6 네트워크에서는 이 옵션을 사용할 수 없습니다.

단계 **6** **OK(**확인**)**를 클릭합니다.

동적 수동 **PAT** 구성

자동 PAT가 요구를 충족하지 않을 때는 동적 수동 PAT 규칙을 사용합니다. 대상에 따라 다른 변환을 수행하려는 경우를 예로 들 수 있습니다. 동적 PAT는 주소를 여러 IP 주소만으로 변환하는 대신 고유한 IP 주소/포트 조합으로 변환합니다. 단일 주소(대상 인터페이스의 주소 또는 다른 주소)로 변환할 수 있습니다.

시작하기 전에

개체를 선택하여 규칙에 필요한 네트워크 개체 또는 그룹을 생성합니다. 그룹은 IPv4 주소와 IPv6 주소를 모두 포함할 수는 없으며 한 유형만 포함해야 합니다. NAT 규칙을 정의하면서 개체를 생성할 수도 있습니다. 개체는 다음 요건도 충족해야 합니다.

- 원본 소스 주소 - 이 주소는 네트워크 개체 또는 그룹일 수 있으며 호스트나 서브넷을 포함할 수 있습니다. 모든 원본 소스 트래픽을 변환하려는 경우 이 단계를 건너뛰고 규칙에서 임의를 지정하면 됩니다.
- 변환된 소스 주소 - 다음 옵션을 사용하여 PAT 주소를 지정할 수 있습니다.
  - 대상 인터페이스 - 대상 인터페이스 IPv4 주소를 사용하려는 경우 네트워크 개체가 필요하지 않습니다. IPv6에는 인터페이스 PAT를 사용할 수 없습니다.
  - 단일 **PAT** 주소 - 단일 호스트를 포함하는 네트워크 개체를 생성합니다.

규칙에서 원본 대상 주소 및 변환된 대상 주소에 대해 정적 변환을 구성하는 경우 이러한 주소에 대해 네트워크 개체를 생성할 수도 있습니다.

동적 PAT의 경우 대상에 대해 포트 변환을 수행할 수도 있습니다. 개체 관리자에서 원본 대상 포트 및 변환된 대상 포트에 사용할 수 있는 포트 개체가 있는지 확인합니다. 소스 포트를 지정하면 무시됩니다.

절차

단계 **1** **Policies(**정책**)** > **NAT**를 선택합니다.

단계 **2** 다음 중 하나를 수행합니다.

- 새 규칙을 생성하려면 + 버튼을 클릭합니다.
- 기존 규칙을 수정하려면 해당 규칙의 수정 아이콘( )을 클릭합니다.

더 이상 필요하지 않은 규칙을 삭제하려면 해당 규칙의 휴지통 아이콘을 클릭합니다.

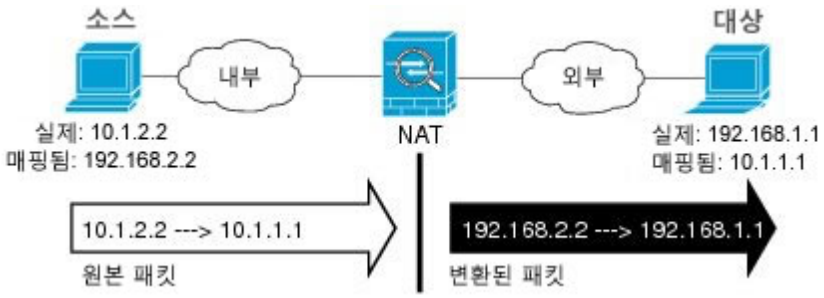
단계 **3** 기본 규칙 옵션을 구성합니다.

- 제목 - 규칙의 이름을 입력합니다.
- 규칙 생성 - 수동 **NAT**를 선택합니다.
- **Rule Placement(**규칙 배치**)** - 규칙을 추가할 위치를 선택합니다. 규칙은 카테고리에서 자동 NAT 규칙 앞이나 뒤에 삽입할 수도 있고, 선택한 규칙 위나 아래에 삽입할 수도 있습니다.
- 유형 - 동적을 선택합니다. 이 설정은 원본 주소에만 적용됩니다. 대상 주소에 대한 변환을 정의하는 경우 변환은 항상 고정입니다.

단계 **4** 다음 인터페이스 옵션을 구성합니다.

- **Source Interface(**소스 인터페이스**)**, **Destination Interface(**대상 인터페이스**)** — (브리지 그룹 구성원 인터페이스의 경우 필수)이 NAT 규칙이 적용되는 인터페이스를 선택합니다. **Source(**소스**)**는 트래픽이 디바이스로 들어가는 데 사용되는 실제 인터페이스입니다. **Destination(**대상**)**은 트래픽이 디바이스에서 나오는 데 사용되는 매핑된 인터페이스입니다. 기본적으로 규칙은 브리지 그룹 구성원 인터페이스를 제외한 모든 인터페이스**(Any(**모두**))**에 적용됩니다.

단계 **5** 원본 패킷 주소(IPv4 또는 IPv6)를 식별합니다. 이 주소는 원본 패킷에 표시되는 패킷 주소입니다. 원본 패킷 대 변환된 패킷의 예는 다음 그림을 참조하십시오.



- **Original Source Address(**원본 소스 주소**)** - 변환 중인 주소가 포함된 네트워크 개체 또는 그룹입니다.
- **Original Destination Address(**원본 대상주소**)** - (선택 사항) 대상의 주소를 포함하는 네트워크 개체입니다. 이 옵션을 비워 두면 대상에 관계없이 소스 주소 변환이 적용됩니다. 대상 주소를 지

정하면 해당 주소에 대해 고정 변환을 구성할 수도 있고 단순히 ID NAT를 사용할 수도 있습니다.

Interface(인터페이스**)**를 선택하여 소스 인터페이스(Any(모두)일 수 없음)를 기준으로 원본 대상을 지정할 수 있습니다. 이 옵션을 선택할 경우 변환된 대상 개체도 선택해야 합니다. 대상 주소에 대해 포트 변환을 사용하여 고정 인터페이스 NAT를 구현하려면 이 옵션을 선택하고 대상 포트에 대해 적절한 포트 개체도 선택합니다.

단계 **6** 변환된 패킷 주소(IPv4 또는 IPv6), 즉 대상 인터페이스 네트워크에 나타나는 패킷 주소를 확인합니다. 필요에 따라 IPv4 및 IPv6 간에 변환할 수 있습니다.

- 변환된 소스 주소 - 다음 중 하나입니다.
  - (인터페이스 PAT) 대상 인터페이스의 IPv4 주소를 사용하려면 인터페이스를 선택합니다. 특정 대상 인터페이스도 선택해야 합니다. 이 인터페이스는 브리지 그룹 구성원 인터페이스일 수 없습니다. IPv6에는 인터페이스 PAT를 사용할 수 없습니다.
  - 대상 인터페이스 주소가 아닌 단일 주소를 사용하려면 이러한 용도로 생성한 호스트 네트워크 개체를 선택합니다.
- 변환된 대상 주소 - (선택 사항) 변환된 패킷에서 사용되는 대상 주소를 포함하는 네트워크 개체 또는 그룹입니다. 원본 대상에 대해 개체를 선택한 경우 동일한 개체를 선택하여 ID NAT(변환 없음)를 설정할 수 있습니다.

단계 **7** (선택 사항). 서비스 변환용 대상 서비스 포트**(Original Destination Port(**원본 대상 포트**)**, **Translated Destination Port(**변환된 대상 포트**))**를 식별합니다.
동적 NAT는 포트 변환을 지원하지 않으므로 **Original Destination Port(**원본 대상 포트**)** 및 **Translated Destination Port(**변환된 대상 포트**)** 필드를 비워 둡니다. 그러나 대상 변환은 항상 고정이므로 대상 포트의 포트 변환을 수행할 수 있습니다.

NAT는 TCP 또는 UDP만 지원합니다. 포트를 변환할 때는 실제 서비스 개체의 프로토콜과 매핑된 서비스 개체의 프로토콜이 동일해야 합니다(둘 다 TCP거나 둘 다 UDP). ID NAT의 경우 실제 포트와 매핑된 포트에 동일한 서비스 개체를 사용할 수 있습니다.

단계 **8** (선택 사항). 고급 옵션 링크를 클릭하고 원하는 옵션을 선택합니다.

- **Fallthrough to Interface PAT (Destination Interface)(**인터페이스 **PAT(**대상 인터페이스**)**로 폴스루**)** — 다른 매핑된 주소가 이미 할당된 경우 대상 인터페이스의 IP 주소를 백업 방법으로 사용할지 여부를 선택합니다(인터페이스 PAT 대체). 이 옵션은 브리지 그룹의 구성원이 아닌 대상 인터페이스를 선택한 경우에만 사용할 수 있습니다. 인터페이스 PAT를 변환된 주소로 이미 구성한 경우에는 이 옵션을 선택할 수 없습니다. 또한 IPv6 네트워크에서는 이 옵션을 사용할 수 없습니다.

단계 **9** **OK(**확인**)**를 클릭합니다.

고정 NAT

다음 주제에서는 고정 NAT 및 고정 NAT를 구현하는 방법에 대해 설명합니다.

고정 NAT 정보

고정 NAT는 실제 주소에서 매핑된 주소로의 고정된 변환을 생성합니다. 매핑된 주소는 각각의 연속 연결에 대해 동일하므로 NAT는 양방향 연결 시작을 허용합니다. 이를 허용하는 액세스 규칙이 있는 경우 호스트에서 나가기도 하고 호스트로 들어오기도 합니다. 반면 동적 NAT 및 PAT의 경우, 각 호스트는 각 후속 변환에 대해 서로 다른 주소 또는 포트를 사용하므로 양방향 시작이 지원되지 않습니다.

다음 그림은 일반적인 고정 NAT 시나리오를 보여줍니다. 변환이 항상 활성 상태이므로 실제 호스트와 원격 호스트 모두 연결을 시작할 수 있습니다.

그림 ***8:*** 고정 ***NAT***

포트 변환 고정 *NAT*

포트 변환 고정 NAT를 사용하면 실제 및 매핑된 프로토콜과 포트를 지정할 수 있습니다.

고정 NAT로 포트를 지정하는 경우 포트 및/또는 IP 주소를 동일한 값으로 매핑할지 아니면 다른 값으로 매핑할지를 선택할 수 있습니다.

다음 그림은 자신에게 매핑되는 포트와 다른 값으로 매핑되는 포트 모두를 보여주는 포트 변환 시나리오의 일반적인 고정 NAT를 보여줍니다. 두 경우 모두 IP 주소는 다른 값으로 매핑됩니다. 변환이 항상 활성 상태이므로 변환된 호스트와 원격 호스트 모두 연결을 시작할 수 있습니다.

그림 ***9:*** 일반적인 포트 변환 고정 ***NAT*** 시나리오

참고 보조 채널(예: FTP 및 VoIP)에 대해 애플리케이션 검사를 요구하는 애플리케이션의 경우 NAT에서는 자동으로 보조 포트를 변환합니다.

포트 변환 고정 NAT의 몇 가지 다른 사용 방식은 다음과 같습니다.

ID 포트 변환 고정 **NAT**

내부 리소스에 대한 외부 액세스를 간소화할 수 있습니다. 예를 들어, FTP, HTTP, SMTP 등 각기 다른 포트에서 서비스를 제공하는 개별 서버 3개가 있는 경우 외부 사용자에게 해당 서비스 액세스를 위한 단일 IP 주소를 제공할 수 있습니다. 그런 후에 외부 사용자들이 액세스하려는 포트를 기준으로 하여 실제 서버의 올바른 IP 주소에 단일 외부 IP 주소를 매핑하도록 ID 포트 변환 고정 NAT를 구성할 수 있습니다. 이러한 서버는 표준 포트(각각 21, 80, 25)를 사용하므로 포트를 변경할 필요는 없습니다.

비표준 포트에 대한 포트 변환 고정 **NAT**

잘 알려진 포트를 비표준 포트로 또는 그 반대로 변환하려는 경우에도 포트 변환 고정 NAT를 사용할 수 있습니다. 예를 들어 내부 웹 서버가 포트 8080을 사용하는 경우 외부 사용자가 포트 80에 연결하도록 허용한 다음 원본 포트 8080으로의 변환을 취소할 수 있습니다. 마찬가지로, 보안을 강화하려면 웹 사용자에게 비표준 포트 6785로 연결하도록 안내한 다음 포트 80으로의 변환을 취소할 수 있습니다.

포트 변환 고정 인터페이스 **NAT**

실제 주소를 인터페이스 주소/포트 조합으로 매핑하도록 고정 NAT를 구성할 수 있습니다. 예를 들어 디바이스의 외부 인터페이스에 대한 텔넷 액세스를 내부 호스트로 리디렉션하려는 경우 내부 호스트 IP 주소/포트 23을 외부 인터페이스 주소/포트 23에 매핑할 수 있습니다.

일대다 고정 *NAT*

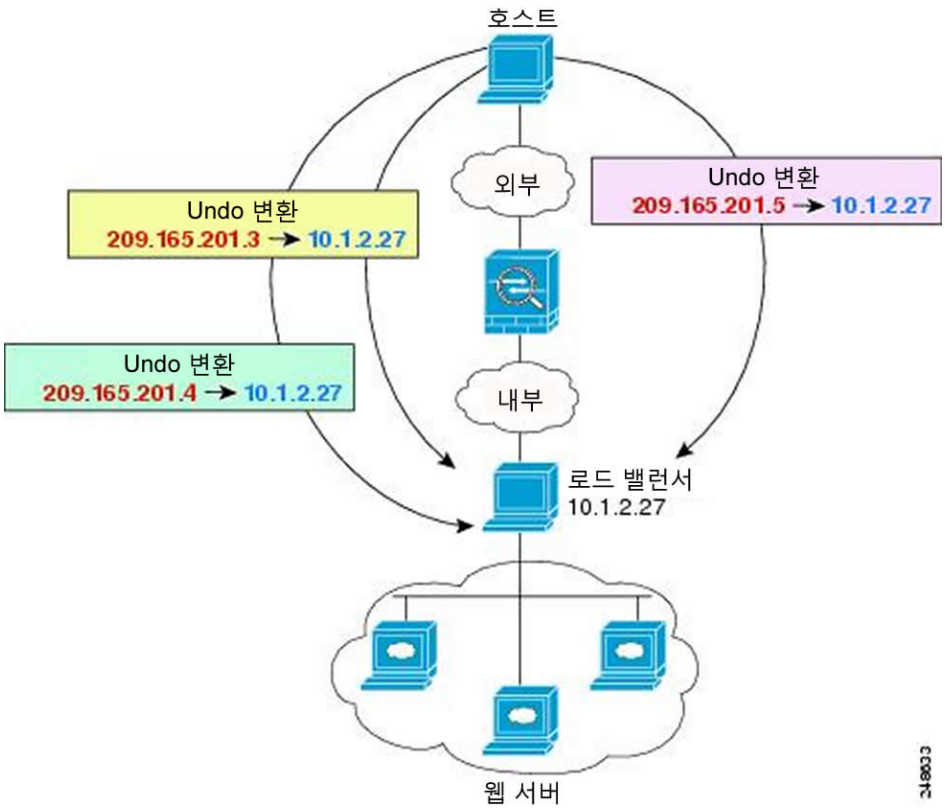
일반적으로 NAT는 일대일 매핑으로 구성합니다. 그러나 경우에 따라 여러 매핑된 주소에 대해 단일 실제 주소를 구성해야 할 수도 있습니다(일대다). 일대다 고정 NAT를 구성할 경우, 실제 호스트가 트래픽을 시작하면 항상 첫 번째 매핑된 주소를 사용합니다. 그러나 호스트에 대해 시작된 트래픽의 경우, 매핑된 주소 중 하나에 대해 트래픽을 시작할 수 있습니다. 이러한 주소는 단일 실제 주소로 변환되지 않습니다.

다음 그림은 일반적인 일대다 고정 NAT 시나리오를 보여줍니다. 실제 호스트에 의한 시작은 항상 첫 번째 매핑된 주소를 사용하므로, 실제 호스트 IP/첫 번째 매핑된 IP의 변환이 기술적으로 유일한 양방향 변환입니다.

그림 ***10:*** 일대다 고정 ***NAT***

예를 들어 10.1.2.27에 로드 밸런서가 있으면, 요청된 URL에 따라 트래픽이 올바른 웹 서버로 리디렉션됩니다.

그림 ***11:*** 일대다 고정 ***NAT*** 예



기타 매핑 시나리오*(권장되지 않음)*

NAT에서는 일대일, 일대다, 소수대다수, 다수대소수, 다대일 등 모든 종류의 고정 매핑 시나리오를 유연하게 허용합니다. 그러나 일대일 또는 일대다 매핑만 사용하는 것이 좋습니다. 다른 매핑 옵션을 사용할 경우 예기치 않은 결과가 발생할 수 있습니다.

소수대다수는 기능상 일대다와 같지만, 컨피그레이션이 좀 더 복잡하고 실제 매핑이 한눈에 명확히 파악되지 않을 수 있으므로 필요한 경우 각 실제 주소에 대해 일대다 컨피그레이션을 만드는 것이 좋습니다. 소수대다수 시나리오에서는 소수의 실제 주소가 다수의 매핑된 주소로 순서대로 매핑됩니다(A-1, B-2, C-3). 모든 실제 주소가 매핑되면 다음의 매핑된 주소는 첫 번째 실제 주소로 매핑되며, 모든 매핑된 주소가 매핑될 때까지 같은 방식이 반복됩니다(A-4, B-5, C-6). 그 결과 각 실제 주소에 다수의 매핑된 주소가 연결됩니다. 일대다 컨피그레이션의 경우와 마찬가지로 첫 번째 매핑만 양방향이고 이후 매핑에서는 실제 호스트로만 트래픽이 시작되고, 실제 호스트로부터의 모든 트래픽은 소스에 대해 첫 번째 매핑된 주소만 사용합니다.

다음 그림은 일반적인 소수대다수 고정 NAT 시나리오를 보여줍니다.

그림 ***12:*** 소수대다수 고정 ***NAT***

매핑된 주소보다 실제 주소가 더 많은 다수대소수 또는 다대일 컨피그레이션의 경우, 실제 주소가 소진되기 전에 매핑된 주소가 소진됩니다. 가장 낮은 실제 IP 주소와 매핑된 풀 간의 매핑만 양방향 시작이 가능합니다. 나머지 더 높은 실제 주소는 트래픽을 시작할 수 있지만 이러한 주소로 트래픽이 시작될 수는 없습니다. 연결에 대한 고유한 5튜플(소스/대상 IP 주소, 소스/대상 포트 및 프로토콜) 때문에 연결에 대한 반환 트래픽은 정확한 실제 주소로 전달됩니다.

참고 다수대소수 또는 다대일 NAT는 PAT가 아닙니다. 두 개의 실제 호스트가 동일한 소스 포트 번호를 사용하고 동일한 외부 서버 및 동일한 TCP 대상 포트로 이동하며 두 호스트가 동일한 IP 주소로 변환되면, 주소 충돌 때문에(5튜플이 고유하지 않음) 두 연결이 재설정됩니다.

다음 그림은 일반적인 다수대소수 고정 NAT 시나리오를 보여줍니다.

그림 ***13:*** 다수대소수 고정 ***NAT***

고정 규칙을 이 방식으로 사용하는 대신, 양방향 시작이 필요한 트래픽에 대해 일대일 규칙을 만든 다음 나머지 주소에 대해 동적 규칙을 만드는 방식을 권장합니다.

고정 자동 **NAT** 구성

고정 자동 NAT 규칙을 사용하여 주소를 대상 네트워크에서 라우팅할 수 있는 서로 다른 IP 주소로 변환합니다. 또한 고정 NAT 규칙을 사용하여 포트 변환을 수행할 수도 있습니다.

시작하기 전에

Objects(개체**)**를 선택하여 규칙에 필요한 네트워크 개체 또는 그룹을 생성합니다. NAT 규칙을 정의하면서 개체를 생성할 수도 있습니다. 개체는 다음 요건을 충족해야 합니다.

- 원 주소 - 이 주소는 그룹이 아닌 네트워크 개체여야 하며 호스트나 서브넷일 수 있습니다.
- 변환된 주소 - 다음 옵션을 사용하여 변환된 주소를 지정할 수 있습니다.
  - 대상 인터페이스 - 대상 인터페이스 IPv4 주소를 사용하려는 경우 네트워크 개체가 필요하지 않습니다. 이 경우 포트 변환 고정 인터페이스 NAT가 구성됩니다. 소스 주소/포트는 인터페이스의 주소 및 동일한 포트 번호로 변환됩니다. IPv6에는 인터페이스 PAT를 사용할 수 없습니다.
  - 주소 - 호스트나 서브넷이 포함된 네트워크 개체 또는 그룹을 생성합니다. 그룹은 IPv4 주소와 IPv6 주소를 모두 포함할 수는 없으며 한 유형만 포함해야 합니다. 일반적으로 일대일 매핑의 경우 동일한 수의 매핑된 주소를 실제 주소로 구성합니다. 그러나 주소의 수가 일치하지 않아도 됩니다.

절차

단계 **1** **Policies(**정책**)** > **NAT**를 선택합니다.

단계 **2** 다음 중 하나를 수행합니다.

- 새 규칙을 생성하려면 + 버튼을 클릭합니다.

- 기존 규칙을 수정하려면 해당 규칙의 수정 아이콘()을 클릭합니다.

더 이상 필요하지 않은 규칙을 삭제하려면 해당 규칙의 휴지통 아이콘을 클릭합니다.

단계 **3** 기본 규칙 옵션을 구성합니다.

- 제목 - 규칙의 이름을 입력합니다.
- 규칙 생성 - 자동 **NAT**를 선택합니다.
- 유형 - 고정을 선택합니다.

단계 **4** 다음 패킷 변환 옵션을 구성합니다.

- **Source Interface**(소스 인터페이스), **Destination Interface**(대상 인터페이스) — (브리지 그룹 구성원 인터페이스의 경우 필수)이 NAT 규칙이 적용되는 인터페이스를 선택합니다. **Source**(소스)는 트래픽이 디바이스로 들어가는 데 사용되는 실제 인터페이스입니다. **Destination**(대상)은 트래픽이 디바이스에서 나오는 데 사용되는 매핑된 인터페이스입니다. 기본적으로 규칙은 브리지 그룹 구성원 인터페이스를 제외한 모든 인터페이스(**Any**(모두))에 적용됩니다.
- 원 주소 - 변환하는 주소가 포함된 네트워크 개체입니다.
- 변환된 주소 - 다음 중 하나입니다.
  - 설정된 주소 그룹을 사용하려면 매핑된 주소를 포함하는 네트워크 개체 또는 그룹을 선택합니다. 일반적으로 일대일 매핑의 경우 동일한 수의 매핑된 주소를 실제 주소로 구성합니다. 그러나 주소의 수가 일치하지 않아도 됩니다.
  - (포트 변환 기능이 있는 고정 인터페이스 NAT) 대상 인터페이스의 주소를 사용하려면 인터페이스를 선택합니다. 특정 대상 인터페이스도 선택해야 합니다. 이 인터페이스는 브리지 그룹 구성원 인터페이스일 수 없습니다. IPv6에 대해서는 인터페이스 PAT를 사용할 수 없습니다.이렇게 하면 포트 변환 고정 인터페이스 NAT가 구성됩니다. 원본 주소/포트는 인터페이스의 주소 및 동일한 포트 번호로 변환됩니다.
- (선택 사항). 원 포트, 변환된 포트 - TCP 또는 UDP 포트를 변환해야 하는 경우 원 포트와 변환된 포트를 정의하는 포트 개체를 선택합니다. 이 경우 동일한 프로토콜의 개체를 선택해야 합니다. 개체가 아직 없으면 새 개체 생성 링크를 클릭합니다. 예를 들어, 필요에 따라 TCP/80을 TCP/8080으로 변환할 수 있습니다.

단계 **5** (선택 사항). 고급 옵션 링크를 클릭하고 원하는 옵션을 선택합니다.

- **Translate DNS replies that match this rule**(이 규칙과 일치하는 **DNS** 응답 변환) — DNS 응답의 IP 주소를 변환할지 여부를 선택합니다. 매핑된 인터페이스에서 실제 인터페이스로 이동하는 DNS 응답의 경우 주소(IPv4 A 또는 IPv6 AAAA) 레코드가 매핑된 값에서 실제 값으로 재작성됩니다. 반대로, 실제 인터페이스에서 매핑된 인터페이스로 이동하는 DNS 응답의 경우 실제 값에서 매핑된 값으로 레코드가 재작성됩니다. 이 옵션은 특정 상황에서 사용되며, 재작성 시 A 레코드와 AAAA 레코드 간의 변환도 수행되는 NAT64/46 변환에 필요한 경우도 있습니다. 자세한 내용은 NAT를 사용하여 DNS 쿼리 및 응답 재작성, 242 페이지를 참고하십시오. 포트 변환을 수행 중인 경우 이 옵션을 사용할 수 없습니다.

- **Do not proxy ARP on Destination Interface(**대상 인터페이스에서 **ARP** 프록시 설정 안 함**)** - 매핑된 IP 주소로 들어오는 패킷에 대해 프록시 ARP를 비활성화합니다. 매핑된 인터페이스와 동일한 네트워크의 주소를 사용하는 경우 시스템은 매핑된 주소에 대한 ARP 요청에 답하기 위해 프록시 ARP를 사용하며, 이에 따라 매핑된 주소로 가야 하는 트래픽을 가로챕니다. 디바이스가 추가 네트워크에 대한 게이트웨이가 될 필요가 없으므로 이 솔루션은 라우팅을 간소화합니다. 원하는 경우 프록시 ARP를 비활성화할 수 있습니다. 이 경우 업스트림 라우터에 적절한 경로가 있어야 합니다. 일반적으로 ID NAT에는 프록시 ARP가 필요하지 않으며, 프록시 ARP를 사용할 경우 연결 문제가 발생할 수도 있습니다.

단계 **6** **OK(**확인**)**를 클릭합니다.

고정 수동 **NAT** 구성

자동 NAT가 요구를 충족하지 않을 때는 고정 수동 NAT 규칙을 사용합니다. 대상에 따라 다른 변환을 수행하려는 경우를 예로 들 수 있습니다. 고정 NAT는 주소를 대상 네트워크에서 라우팅할 수 있는 서로 다른 IP 주소로 변환합니다. 또한 고정 NAT 규칙을 사용하여 포트 변환을 수행할 수도 있습니다.

시작하기 전에

Objects(개체**)**를 선택하여 규칙에 필요한 네트워크 개체 또는 그룹을 생성합니다. 그룹은 IPv4 주소와 IPv6 주소를 모두 포함할 수는 없으며 한 유형만 포함해야 합니다. NAT 규칙을 정의하면서 개체를 생성할 수도 있습니다. 개체는 다음 요건도 충족해야 합니다.

- 원본 소스 주소 - 이 주소는 네트워크 개체 또는 그룹일 수 있으며 호스트나 서브넷을 포함할 수 있습니다. 모든 원본 소스 트래픽을 변환하려는 경우 이 단계를 건너뛰고 규칙에서 임의를 지정하면 됩니다.
- 변환된 소스 주소 - 다음 옵션을 사용하여 변환된 주소를 지정할 수 있습니다.
  - 대상 인터페이스 - 대상 인터페이스 IPv4 주소를 사용하려는 경우 네트워크 개체가 필요하지 않습니다. 이 경우 포트 변환 고정 인터페이스 NAT가 구성됩니다. 소스 주소/포트는 인터페이스의 주소 및 동일한 포트 번호로 변환됩니다. IPv6에는 인터페이스 PAT를 사용할 수 없습니다.
  - 주소 - 호스트나 서브넷이 포함된 네트워크 개체 또는 그룹을 생성합니다. 그룹은 IPv4 주소와 IPv6 주소를 모두 포함할 수는 없으며 한 유형만 포함해야 합니다. 일반적으로 일대일 매핑의 경우 동일한 수의 매핑된 주소를 실제 주소로 구성합니다. 그러나 주소의 수가 일치하지 않아도 됩니다.

규칙에서 원본 대상 주소 및 변환된 대상 주소에 대해 정적 변환을 구성하는 경우 이러한 주소에 대해 네트워크 개체를 생성할 수도 있습니다. 포트 변환 대상 고정 인터페이스 NAT만 구성하려면 대상 매핑된 주소에 대한 개체 추가를 건너뛰고 규칙에서 인터페이스를 지정할 수 있습니다.

소스나 대상 또는 둘 다에 대해 포트 변환을 수행할 수도 있습니다. 개체 관리자에서 원본 및 변환된 포트에 사용할 수 있는 포트 개체가 있는지 확인합니다.

절차

단계 **1** **Policies(**정책**)** > **NAT**를 선택합니다.

단계 **2** 다음 중 하나를 수행합니다.

- 새 규칙을 생성하려면 + 버튼을 클릭합니다.
- 기존 규칙을 수정하려면 해당 규칙의 수정 아이콘( )을 클릭합니다.

더 이상 필요하지 않은 규칙을 삭제하려면 해당 규칙의 휴지통 아이콘을 클릭합니다.

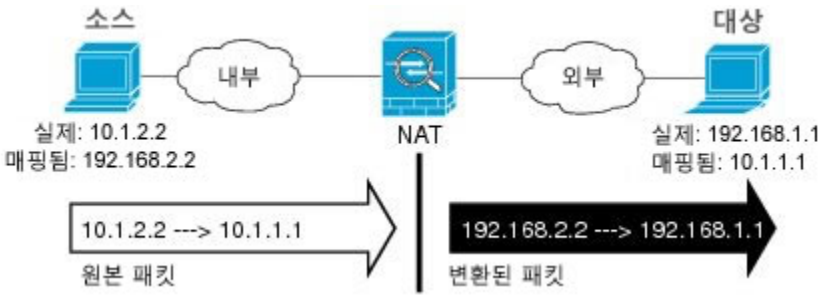
단계 **3** 기본 규칙 옵션을 구성합니다.

- 제목 - 규칙의 이름을 입력합니다.
- 규칙 생성 - 수동 **NAT**를 선택합니다.
- **Rule Placement(**규칙 배치**)** - 규칙을 추가할 위치를 선택합니다. 규칙은 카테고리에서 자동 NAT 규칙 앞이나 뒤에 삽입할 수도 있고, 선택한 규칙 위나 아래에 삽입할 수도 있습니다.
- 유형 - 고정을 선택합니다. 이 설정은 소스 주소에만 적용됩니다. 대상 주소에 대한 변환을 정의하는 경우 변환은 항상 고정입니다.

단계 **4** 다음 인터페이스 옵션을 구성합니다.

- **Source Interface(**소스 인터페이스**)**, **Destination Interface(**대상 인터페이스**)** — (브리지 그룹 구성원 인터페이스의 경우 필수)이 NAT 규칙이 적용되는 인터페이스를 선택합니다. **Source(**소스**)**는 트래픽이 디바이스로 들어가는 데 사용되는 실제 인터페이스입니다. **Destination(**대상**)**은 트래픽이 디바이스에서 나오는 데 사용되는 매핑된 인터페이스입니다. 기본적으로 규칙은 브리지 그룹 구성원 인터페이스를 제외한 모든 인터페이스**(Any(**모두**))**에 적용됩니다.

단계 **5** 원본 패킷 주소(IPv4 또는 IPv6)를 식별합니다. 이 주소는 원본 패킷에 표시되는 패킷 주소입니다. 원본 패킷 대 변환된 패킷의 예는 다음 그림을 참조하십시오.



- **Original Source Address(**원본 소스 주소**)** - 변환 중인 주소가 포함된 네트워크 개체 또는 그룹입니다.
- **Original Destination Address(**원본 대상주소**)** - (선택 사항) 대상의 주소를 포함하는 네트워크 개체입니다. 이 옵션을 비워 두면 대상에 관계없이 소스 주소 변환이 적용됩니다. 대상 주소를 지

정하면 해당 주소에 대해 고정 변환을 구성할 수도 있고 단순히 ID NAT를 사용할 수도 있습니다.

Interface(인터페이스**)**를 선택하여 소스 인터페이스(Any(모두)일 수 없음)를 기준으로 원본 대상을 지정할 수 있습니다. 이 옵션을 선택할 경우 변환된 대상 개체도 선택해야 합니다. 대상 주소에 대해 포트 변환을 사용하여 고정 인터페이스 NAT를 구현하려면 이 옵션을 선택하고 대상 포트에 대해 적절한 포트 개체도 선택합니다.

단계 **6** 변환된 패킷 주소(IPv4 또는 IPv6), 즉 대상 인터페이스 네트워크에 나타나는 패킷 주소를 확인합니다. 필요에 따라 IPv4 및 IPv6 간에 변환할 수 있습니다.

- 변환된 소스 주소 - 다음 중 하나입니다.
  - 설정된 주소 그룹을 사용하려면 매핑된 주소를 포함하는 네트워크 개체 또는 그룹을 선택합니다. 일반적으로 일대일 매핑의 경우 동일한 수의 매핑된 주소를 실제 주소로 구성합니다. 그러나 주소의 수가 일치하지 않아도 됩니다.
  - (포트 변환 고정 인터페이스 NAT) 대상 인터페이스의 IPv4 주소를 사용하려면 인터페이스를 선택합니다. 특정 대상 인터페이스도 선택해야 합니다. 이 인터페이스는 브리지 그룹 구성원 인터페이스일 수 없습니다. 이 경우 포트 변환 고정 인터페이스 NAT가 구성됩니다. 소스 주소/포트는 인터페이스의 주소 및 동일한 포트 번호로 변환됩니다. IPv6에는 인터페이스 PAT를 사용할 수 없습니다.
- 변환된 대상 주소 - (선택 사항) 변환된 패킷에서 사용되는 대상 주소를 포함하는 네트워크 개체 또는 그룹입니다. 원본 대상에 대해 개체를 선택한 경우 동일한 개체를 선택하여 ID NAT(변환 없음)를 설정할 수 있습니다.

단계 **7** (선택 사항) 서비스 변환의 소스 또는 대상 서비스 포트를 식별합니다.
포트 변환 고정 NAT를 구성하는 경우 소스나 대상 또는 둘 다에 대해 포트를 변환할 수 있습니다. 예를 들어 TCP/80과 TCP/8080 간에 변환할 수 있습니다.

NAT는 TCP 또는 UDP만 지원합니다. 포트를 변환할 때는 실제 서비스 개체의 프로토콜과 매핑된 서비스 개체의 프로토콜이 동일해야 합니다(둘 다 TCP거나 둘 다 UDP). ID NAT의 경우 실제 포트와 매핑된 포트에 동일한 서비스 개체를 사용할 수 있습니다.

- 원본 소스 포트, 변환된 소스 포트 - 소스 주소에 대한 포트 변환을 정의합니다.
- 원본 대상 포트, 변환된 대상 포트 - 대상 주소에 대한 포트 변환을 정의합니다.

단계 **8** (선택 사항). 고급 옵션 링크를 클릭하고 원하는 옵션을 선택합니다.

- **Translate DNS replies that match this rule(**이 규칙과 일치하는 **DNS** 응답 변환**)** — DNS 응답의 IP 주소를 변환할지 여부를 선택합니다. 매핑된 인터페이스에서 실제 인터페이스로 이동하는 DNS 응답의 경우 주소(IPv4 A 또는 IPv6 AAAA) 레코드가 매핑된 값에서 실제 값으로 재작성됩니다. 반대로, 실제 인터페이스에서 매핑된 인터페이스로 이동하는 DNS 응답의 경우 실제 값에서 매핑된 값으로 레코드가 재작성됩니다. 이 옵션은 특정 상황에서 사용되며, 재작성 시 A 레코드와 AAAA 레코드 간의 변환도 수행되는 NAT64/46 변환에 필요한 경우도 있습니다. 자세한 내

용은 NAT를 사용하여 DNS 쿼리 및 응답 재작성, 242 페이지를 참고하십시오. 포트 변환을 수행 중인 경우 이 옵션을 사용할 수 없습니다.

- **Do not proxy ARP on Destination Interface(**대상 인터페이스에서 **ARP** 프록시 설정 안 함**)** - 매핑된 IP 주소로 들어오는 패킷에 대해 프록시 ARP를 비활성화합니다. 매핑된 인터페이스와 동일한 네트워크의 주소를 사용하는 경우 시스템은 매핑된 주소에 대한 ARP 요청에 답하기 위해 프록시 ARP를 사용하며, 이에 따라 매핑된 주소로 가야 하는 트래픽을 가로챕니다. 디바이스가 추가 네트워크에 대한 게이트웨이가 될 필요가 없으므로 이 솔루션은 라우팅을 간소화합니다. 원하는 경우 프록시 ARP를 비활성화할 수 있습니다. 이 경우 업스트림 라우터에 적절한 경로가 있어야 합니다. 일반적으로 ID NAT에는 프록시 ARP가 필요하지 않으며, 프록시 ARP를 사용할 경우 연결 문제가 발생할 수도 있습니다.

단계 **9** **OK(**확인**)**를 클릭합니다.

ID NAT

IP 주소를 자신으로 변환해야 하는 NAT 컨피그레이션이 있을 수 있습니다. 예를 들어 NAT를 모든 네트워크에 적용하는 광범위한 규칙을 만들되 NAT에서 하나의 네트워크만 제외하고 싶은 경우, 주소를 자신으로 변환하는 고정 NAT 규칙을 만들 수 있습니다.

다음 그림은 일반적인 ID NAT 시나리오를 보여줍니다.

그림 ***14: ID NAT***

다음 주제에서는 ID NAT를 구성하는 방법에 대해 설명합니다.

ID 자동 NAT 구성

주소 변환을 방지하려면 고정 ID 자동 NAT 규칙을 사용합니다. 이 경우 주소가 자체로 변환됩니다.

시작하기 전에

개체를 선택하여 규칙에 필요한 네트워크 개체 또는 그룹을 생성합니다. NAT 규칙을 정의하면서 개체를 생성할 수도 있습니다. 개체는 다음 요건을 충족해야 합니다.

- 원본 주소 - 이 주소는 그룹이 아닌 네트워크 개체여야 하며 호스트나 서브넷일 수 있습니다.

- 변환된 주소 - 원본 소스 개체와 내용이 정확히 동일한 네트워크 개체 또는 그룹입니다. 동일한 개체를 사용할 수 있습니다.

절차

단계 **1** **Policies(**정책**)** > **NAT**를 선택합니다.

단계 **2** 다음 중 하나를 수행합니다.

- 새 규칙을 생성하려면 **+** 버튼을 클릭합니다.
- 기존 규칙을 수정하려면 해당 규칙의 수정 아이콘( )을 클릭합니다.

더 이상 필요하지 않은 규칙을 삭제하려면 해당 규칙의 휴지통 아이콘을 클릭합니다.

단계 **3** 기본 규칙 옵션을 구성합니다.

- 제목 - 규칙의 이름을 입력합니다.
- 규칙 생성 - 자동 **NAT**를 선택합니다.
- 유형 - 고정을 선택합니다.

단계 **4** 다음 패킷 변환 옵션을 구성합니다.

- **Source Interface(**소스 인터페이스**)**, **Destination Interface(**대상 인터페이스**)** — (브리지 그룹 구성원 인터페이스의 경우 필수)이 NAT 규칙이 적용되는 인터페이스를 선택합니다. **Source(**소스**)**는 트래픽이 디바이스로 들어가는 데 사용되는 실제 인터페이스입니다. **Destination(**대상**)**은 트래픽이 디바이스에서 나오는 데 사용되는 매핑된 인터페이스입니다. 기본적으로 규칙은 브리지 그룹 구성원 인터페이스를 제외한 모든 인터페이스(**Any(**모두**)**)에 적용됩니다.
- 원본 주소 - 변환하는 주소가 포함된 네트워크 개체입니다.
- 변환된 주소 - 원본 소스와 동일한 개체입니다. 원하는 경우 콘텐츠가 정확히 동일한 다른 개체를 선택할 수 있습니다.

ID NAT의 경우에는 원본 포트 및 변환된 포트 옵션을 구성하지 마십시오.

단계 **5** (선택 사항). 고급 옵션 링크를 클릭하고 원하는 옵션을 선택합니다.

- 이 규칙과 일치하는 **DNS** 응답 변환 - ID NAT의 경우에는 이 옵션을 구성하지 마십시오.
- **Do not proxy ARP on Destination Interface(**대상 인터페이스에서 **ARP** 프록시 설정 안 함**)** - 매핑된 IP 주소로 들어오는 패킷에 대해 프록시 ARP를 비활성화합니다. 매핑된 인터페이스와 동일한 네트워크의 주소를 사용하는 경우 시스템은 매핑된 주소에 대한 ARP 요청에 답하기 위해 프록시 ARP를 사용하며, 이에 따라 매핑된 주소로 가야 하는 트래픽을 가로챕니다. 디바이스가 추가 네트워크에 대한 게이트웨이가 될 필요가 없으므로 이 솔루션은 라우팅을 간소화합니다. 원하는 경우 프록시 ARP를 비활성화할 수 있습니다. 이 경우 업스트림 라우터에 적절한 경로가 있어야 합니다. 일반적으로 ID NAT에는 프록시 ARP가 필요하지 않으며, 프록시 ARP를 사용할 경우 연결 문제가 발생할 수도 있습니다.

- **Perform Route Lookup for Destination Interface(**대상 인터페이스에 대해 경로 조회 수행**)** - 원본 및 변환된 소스 주소에 대해 동일한 개체를 선택할 때 소스 및 대상 인터페이스를 선택하는 경우 이 옵션을 선택하면 시스템이 NAT 규칙에 구성된 대상 인터페이스를 사용하는 대신 라우팅 테이블을 기준으로 하여 대상 인터페이스를 결정하도록 할 수 있습니다.

단계 **6** **OK(**확인**)**를 클릭합니다.

ID 수동 NAT 구성

자동 NAT가 요구를 충족하지 않을 때는 고정 ID 수동 NAT 규칙을 사용합니다. 대상에 따라 다른 변환을 수행하려는 경우를 예로 들 수 있습니다. 주소 변환을 방지하려면 고정 ID NAT 규칙을 사용합니다. 이 경우 주소가 자체로 변환됩니다.

시작하기 전에

개체를 선택하여 규칙에 필요한 네트워크 개체 또는 그룹을 생성합니다. 그룹은 IPv4 주소와 IPv6 주소를 모두 포함할 수는 없으며 한 유형만 포함해야 합니다. NAT 규칙을 정의하면서 개체를 생성할 수도 있습니다. 개체는 다음 요건도 충족해야 합니다.

- 원본 소스 주소 - 이 주소는 네트워크 개체 또는 그룹일 수 있으며 호스트나 서브넷을 포함할 수 있습니다. 모든 원 원본 트래픽을 변환하려는 경우 이 단계를 건너뛰고 규칙에서 임의를 지정하면 됩니다.
- 변환된 원본 주소 - 원 원본과 동일한 개체입니다. 원하는 경우 콘텐츠가 정확히 동일한 다른 개체를 선택할 수 있습니다.

규칙에서 원 대상 주소 및 변환된 대상 주소에 대해 정적 변환을 구성하는 경우 이러한 주소에 대해 네트워크 개체를 생성할 수도 있습니다. 포트 변환 대상 고정 인터페이스 NAT만 구성하려면 대상 매핑된 주소에 대한 개체 추가를 건너뛰고 규칙에서 인터페이스를 지정할 수 있습니다.

소스나 대상 또는 둘 다에 대해 포트 변환을 수행할 수도 있습니다. 개체 관리자에서 원 포트와 변환된 포트에 사용할 수 있는 포트 개체가 있는지 확인합니다. ID NAT에 대해 동일한 개체를 사용할 수 있습니다.

절차

단계 **1** **Policies(**정책**)** > **NAT**를 선택합니다.

단계 **2** 다음 중 하나를 수행합니다.

- 새 규칙을 생성하려면 + 버튼을 클릭합니다.
- 기존 규칙을 수정하려면 해당 규칙의 수정 아이콘()을 클릭합니다.

더 이상 필요하지 않은 규칙을 삭제하려면 해당 규칙의 휴지통 아이콘을 클릭합니다.

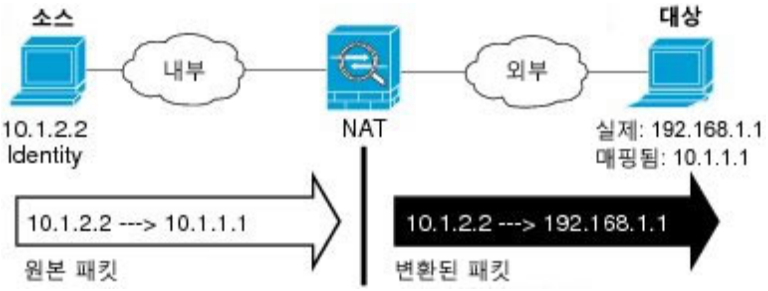
단계 **3** 기본 규칙 옵션을 구성합니다.

- 제목 - 규칙의 이름을 입력합니다.
- 규칙 생성 - 수동 **NAT**를 선택합니다.
- **Rule Placement(**규칙 배치**)** - 규칙을 추가할 위치를 선택합니다. 규칙은 카테고리에서 자동 NAT 규칙 앞이나 뒤에 삽입할 수도 있고, 선택한 규칙 위나 아래에 삽입할 수도 있습니다.
- 유형 - 고정을 선택합니다. 이 설정은 소스 주소에만 적용됩니다. 대상 주소에 대한 변환을 정의하는 경우 변환은 항상 고정입니다.

단계 **4** 다음 인터페이스 옵션을 구성합니다.

- **Source Interface(**소스 인터페이스**)**, **Destination Interface(**대상 인터페이스**)** — (브리지 그룹 구성원 인터페이스의 경우 필수)이 NAT 규칙이 적용되는 인터페이스를 선택합니다. **Source(**소스**)**는 트래픽이 디바이스로 들어가는 데 사용되는 실제 인터페이스입니다. **Destination(**대상**)**은 트래픽이 디바이스에서 나오는 데 사용되는 매핑된 인터페이스입니다. 기본적으로 규칙은 브리지 그룹 구성원 인터페이스를 제외한 모든 인터페이스(**Any(**모두**)**)에 적용됩니다.

단계 **5** 원본 패킷 주소(IPv4 또는 IPv6)를 식별합니다. 이 주소는 원본 패킷에 표시되는 패킷 주소입니다. 원본 패킷 대 변환된 패킷의 예는 다음 그림을 참조하십시오. 여기서 내부 호스트에 대해서는 ID NAT를 수행하지만 외부 호스트는 변환합니다.



- 원 원본 주소 - 변환하는 주소가 포함된 네트워크 개체 또는 그룹입니다.
- 원 대상 주소 - (선택 사항) 대상의 주소를 포함하는 네트워크 개체입니다. 이 옵션을 비워 두면 대상에 관계없이 소스 주소 변환이 적용됩니다. 대상 주소를 지정하면 해당 주소에 대해 고정 변환을 구성할 수도 있고 단순히 ID NAT를 사용할 수도 있습니다.

  인터페이스를 선택하여 소스 인터페이스(임의일 수 없음)를 기준으로 원본 대상을 지정할 수 있습니다. 이 옵션을 선택할 경우 변환된 대상 개체도 선택해야 합니다. 대상 주소에 대한 포트 변환 고정 인터페이스 NAT를 구현하려면 이 옵션을 선택하고 대상 포트에 대해 적절한 포트 개체도 선택합니다.

단계 **6** 변환된 패킷 주소(IPv4 또는 IPv6), 즉 대상 인터페이스 네트워크에 나타나는 패킷 주소를 확인합니다. 필요에 따라 IPv4 및 IPv6 간에 변환할 수 있습니다.

- 변환된 원본 주소 - 원 원본과 동일한 개체입니다. 원하는 경우 콘텐츠가 정확히 동일한 다른 개체를 선택할 수 있습니다.

- 변환된 대상 주소 - (선택 사항) 변환된 패킷에서 사용되는 대상 주소를 포함하는 네트워크 개체 또는 그룹입니다. 원 대상 주소에 대해 개체를 선택한 경우 동일한 개체를 선택하여 ID NAT(변환 없음)를 설정할 수 있습니다.

단계 **7** (선택 사항) 서비스 변환의 소스 또는 대상 서비스 포트를 식별합니다.
포트 변환 고정 NAT를 구성하는 경우 소스나 대상 또는 둘 다에 대해 포트를 변환할 수 있습니다. 예를 들어 TCP/80과 TCP/8080 간에 변환할 수 있습니다.

NAT는 TCP 또는 UDP만 지원합니다. 포트를 변환할 때는 실제 서비스 개체의 프로토콜과 매핑된 서비스 개체의 프로토콜이 동일해야 합니다(둘 다 TCP거나 둘 다 UDP). ID NAT의 경우 실제 포트와 매핑된 포트에 동일한 서비스 개체를 사용할 수 있습니다.

- 원본 소스 포트, 변환된 소스 포트 - 소스 주소에 대한 포트 변환을 정의합니다.
- 원본 대상 포트, 변환된 대상 포트 - 대상 주소에 대한 포트 변환을 정의합니다.

단계 **8** (선택 사항). 고급 옵션 링크를 클릭하고 원하는 옵션을 선택합니다.

- 이 규칙과 일치하는 **DNS** 응답 변환 - ID NAT의 경우에는 이 옵션을 구성하지 마십시오.
- **Do not proxy ARP on Destination Interface(**대상 인터페이스에서 **ARP** 프록시 설정 안 함**)** - 매핑된 IP 주소로 들어오는 패킷에 대해 프록시 ARP를 비활성화합니다. 매핑된 인터페이스와 동일한 네트워크의 주소를 사용하는 경우 시스템은 매핑된 주소에 대한 ARP 요청에 답하기 위해 프록시 ARP를 사용하며, 이에 따라 매핑된 주소로 가야 하는 트래픽을 가로챕니다. 디바이스가 추가 네트워크에 대한 게이트웨이가 될 필요가 없으므로 이 솔루션은 라우팅을 간소화합니다. 원하는 경우 프록시 ARP를 비활성화할 수 있습니다. 이 경우 업스트림 라우터에 적절한 경로가 있어야 합니다. 일반적으로 ID NAT에는 프록시 ARP가 필요하지 않으며, 프록시 ARP를 사용할 경우 연결 문제가 발생할 수도 있습니다.
- **Perform route lookup for Destination interface(**대상 인터페이스에 대해 경로 조회 수행**)** - 원본 및 변환된 소스 주소에 대해 동일한 개체를 선택할 때 소스 및 대상 인터페이스를 선택하는 경우 이 옵션을 선택하면 시스템이 NAT 규칙에 구성된 대상 인터페이스를 사용하는 대신 라우팅 테이블을 기준으로 하여 대상 인터페이스를 결정하도록 할 수 있습니다.

단계 **9** **OK(**확인**)**를 클릭합니다.

Firepower Threat Defense의 NAT 규칙 속성

NAT(네트워크 주소 변환) 규칙을 사용하여 IP 주소를 다른 IP 주소로 변환합니다. 일반적으로는 NAT 규칙을 사용하여 전용 어드레스를 공개적으로 라우팅 가능한 주소로 변환합니다. 변환을 주소 간에 수행할 수도 있고, PAT(포트 주소 변환)를 사용해 여러 주소를 하나의 주소로 변환하고 포트 번호를 사용해 각 소스 주소를 구분할 수도 있습니다.

NAT 규칙은 다음 기본 속성을 포함합니다. 이러한 속성은 별도로 명시된 경우를 제외하면 자동 NAT 및 수동 NAT 규칙에 대해 동일합니다.

제목

규칙의 이름을 입력합니다. 이름은 공백을 포함할 수 없습니다.

규칙 생성

변환 규칙이 자동 **NAT**인지 아니면 수동 **NAT**인지를 나타냅니다. 자동 NAT는 수동 NAT보다 간단하지만, 수동 NAT를 수행하는 경우에는 대상 주소를 기준으로 하여 소스 주소에 대해 별도의 변환을 생성할 수 있습니다.

Status(상태**)**

규칙을 활성화할지 아니면 끌지를 나타냅니다.

배치**(**수동 **NAT**에만 해당함**)**

규칙을 추가할 위치를 선택합니다. 규칙은 카테고리에서 자동 NAT 규칙 앞이나 뒤에 삽입할 수도 있고, 선택한 규칙 위나 아래에 삽입할 수도 있습니다.

Type(유형**)**

변환 규칙이 동적인지 아니면 정적인지를 나타냅니다. 동적 변환에서는 주소 풀에서 매핑된 주소를 자동으로 선택하며, PAT를 구현할 때는 주소/포트 조합을 선택합니다. 매핑된 주소/포트를 정확하게 정의하려면 정적 변환을 사용하십시오.

다음 주제에서는 나머지 NAT 규칙 속성에 대해 설명합니다.

자동 **NAT**의 패킷 변환 속성

패킷 변환 옵션을 사용하여 소스 주소와 매핑된 변환 주소를 정의합니다. 다음 속성은 자동 NAT에만 적용됩니다.

소스 인터페이스**,** 대상 인터페이스

(브리지 그룹 구성원 인터페이스의 경우 필수)이 NAT 규칙이 적용되는 인터페이스를 선택합니다. **Source(**소스**)**는 트래픽이 디바이스로 들어가는 데 사용되는 실제 인터페이스입니다. **Destination(**대상**)**은 트래픽이 디바이스에서 나오는 데 사용되는 매핑된 인터페이스입니다. 기본적으로 규칙은 브리지 그룹 구성원 인터페이스를 제외한 모든 인터페이스**(Any(**모두**))**에 적용됩니다.

원본 주소**(**항상 필수**)**

변환 중인 소스 주소를 포함하는 네트워크 개체입니다. 그룹이 아닌 네트워크 개체여야 하며, 호스트나 서브넷일 수 있습니다.

변환된 주소(대개 필수)

원본 주소를 변환하는 매핑된 주소입니다. 여기서 선택하는 항목에 따라 정의하는 변환 규칙의 유형이 달라집니다.

- 동적 **NAT** - 매핑된 주소를 포함하는 네트워크 오브젝트 또는 그룹입니다. 네트워크 오브젝트 또는 그룹일 수 있지만 서브넷을 포함할 수는 없습니다. IPv4 주소와 IPv6 주소를 모두 포함할 수는 없으며 한 유형만 포함해야 합니다.
- 동적 **PAT** - 다음 중 하나입니다.
  - (인터페이스 PAT) 대상 인터페이스의 IPv4 주소를 사용하려면 인터페이스를 선택합니다. 특정 대상 인터페이스도 선택해야 합니다. 이 인터페이스는 브리지 그룹 구성원 인터페이스일 수 없습니다. IPv6에는 인터페이스 PAT를 사용할 수 없습니다.
  - 대상 인터페이스 주소가 아닌 단일 주소를 사용하려면 이러한 용도로 생성한 호스트 네트워크 오브젝트를 선택합니다.
- 고정 **NAT** - 다음 중 하나입니다.
  - 설정된 주소 그룹을 사용하려면 매핑된 주소를 포함하는 네트워크 개체 또는 그룹을 선택합니다. 개체 또는 그룹은 호스트나 서브넷을 포함할 수 있습니다. 일반적으로 일대일 매핑의 경우 동일한 수의 매핑된 주소를 실제 주소로 구성합니다. 그러나 주소의 수가 일치하지 않아도 됩니다.
  - (포트 변환 기능이 있는 고정 인터페이스 NAT) 대상 인터페이스의 주소를 사용하려면 인터페이스를 선택합니다. 특정 대상 인터페이스도 선택해야 합니다. 이 인터페이스는 브리지 그룹 멤버 인터페이스일 수 없습니다. 이 경우 포트 변환 고정 인터페이스 NAT가 구성됩니다. 소스 주소/포트는 인터페이스의 주소 및 동일한 포트 번호로 변환됩니다. IPv6에는 인터페이스 PAT를 사용할 수 없습니다.
- **ID NAT** - 원본 소스와 동일한 오브젝트입니다. 원하는 경우 콘텐츠가 정확히 동일한 다른 개체를 선택할 수 있습니다.

원본 포트, 변환된 포트(고정 **NAT**에만 해당됨)

TCP 또는 UDP 포트를 변환해야 하는 경우 원본 포트와 변환된 포트를 정의하는 포트 개체를 선택합니다. 이 경우 동일한 프로토콜의 개체를 선택해야 합니다. 예를 들어, 필요에 따라 TCP/80을 TCP/8080으로 변환할 수 있습니다.

수동 **NAT**의 패킷 변환 속성

패킷 변환 옵션을 사용하여 소스 주소와 매핑된 변환 주소를 정의합니다. 다음 속성은 수동 NAT에만 적용됩니다. 별도로 표시된 항목을 제외한 모든 항목은 선택 사항입니다.

소스 인터페이스, 대상 인터페이스

(브리지 그룹 구성원 인터페이스의 경우 필수)이 NAT 규칙이 적용되는 인터페이스를 선택합니다. **Source(**소스**)**는 트래픽이 디바이스로 들어가는 데 사용되는 실제 인터페이스입니다. **Destination(**대상**)**은 트래픽이 디바이스에서 나오는 데 사용되는 매핑된 인터페이스입니다. 기본적으로 규칙은 브리지 그룹 구성원 인터페이스를 제외한 모든 인터페이스(**Any(**모두**)**)에 적용됩니다.

원본 소스 주소(항상 필수)

변환 중인 주소를 포함하는 네트워크 개체 또는 그룹입니다. 네트워크 개체 또는 그룹일 수 있으며, 호스트나 서브넷을 포함할 수 있습니다. 모든 원본 소스 트래픽을 변환하려는 경우 규칙에서 임의를 지정하면 됩니다.

변환된 소스 주소(대개 필수)

원본 주소를 변환하는 매핑된 주소입니다. 여기서 선택하는 항목에 따라 정의하는 변환 규칙의 유형이 달라집니다.

- 동적 **NAT** - 매핑된 주소를 포함하는 네트워크 오브젝트 또는 그룹입니다. 네트워크 오브젝트 또는 그룹일 수 있지만 서브넷을 포함할 수는 없습니다. IPv4 주소와 IPv6 주소를 모두 포함할 수는 없으며 한 유형만 포함해야 합니다.
- 동적 **PAT** - 다음 중 하나입니다.
  - (인터페이스 PAT) 대상 인터페이스의 주소를 사용하려면 인터페이스를 선택합니다. 특정 대상 인터페이스도 선택해야 합니다. 이 인터페이스는 브리지 그룹 멤버 인터페이스일 수 없습니다. IPv6에는 인터페이스 PAT를 사용할 수 없습니다.
  - 대상 인터페이스 주소가 아닌 단일 주소를 사용하려면 이러한 용도로 생성한 호스트 네트워크 오브젝트를 선택합니다.
- 고정 **NAT** - 다음 중 하나입니다.
  - 설정된 주소 그룹을 사용하려면 매핑된 주소를 포함하는 네트워크 오브젝트 또는 그룹을 선택합니다. 일반적으로 일대일 매핑의 경우 동일한 수의 매핑된 주소를 실제 주소로 구성합니다. 그러나 주소의 수가 일치하지 않아도 됩니다.
  - (포트 변환 기능이 있는 고정 인터페이스 NAT) 대상 인터페이스의 주소를 사용하려면 인터페이스를 선택합니다. 특정 대상 인터페이스도 선택해야 합니다. 이 인터페이스는 브리지 그룹 멤버 인터페이스일 수 없습니다. 이 경우 포트 변환 고정 인터페이스 NAT가 구성됩니다. 소스 주소/포트는 인터페이스의 주소 및 동일한 포트 번호로 변환됩니다. IPv6에는 인터페이스 PAT를 사용할 수 없습니다.
- **ID NAT** - 원본 소스와 동일한 오브젝트입니다. 원하는 경우 콘텐츠가 정확히 동일한 다른 오브젝트를 선택할 수 있습니다.

원본 대상 주소

대상의 주소를 포함하는 네트워크 개체입니다. 이 옵션을 비워 두면 대상에 관계없이 소스 주소 변환이 적용됩니다. 대상 주소를 지정하면 해당 주소에 대해 고정 변환을 구성할 수도 있고 단순히 ID NAT를 사용할 수도 있습니다.

인터페이스를 선택하여 소스 인터페이스(임의일 수 없음)를 기준으로 원본 대상을 지정할 수 있습니다. 이 옵션을 선택할 경우 변환된 대상 개체도 선택해야 합니다. 대상 주소에 대한 포트 변환 고정 인터페이스 NAT를 구현하려면 이 옵션을 선택하고 대상 포트에 대해 적절한 포트 개체도 선택합니다.

변환된 대상 주소

변환된 패킷에서 사용되는 대상 주소를 포함하는 네트워크 개체 또는 그룹입니다. 원본 대상에 대해 개체를 선택한 경우 동일한 개체를 선택하여 ID NAT(변환 없음)를 설정할 수 있습니다.

원본 소스 포트, 변환된 소스 포트, 원본 대상 포트, 변환된 대상 포트

원본 및 변환된 패킷의 소스 및 대상 서비스를 정의하는 포트 개체입니다. 포트를 변환할 수도 있고, 동일한 개체를 선택하여 포트를 변환하지 않고 규칙이 서비스에 따라 달라지도록 설정할 수도 있습니다. 서비스를 구성할 때는 다음 규칙에 유의하십시오.

- (동적 NAT 또는 PAT) 원본 소스 포트 및 변환된 소스 포트에 대해서는 변환을 수행할 수 없습니다. 대상 포트에 대해서만 변환을 수행할 수 있습니다.
- NAT는 TCP 또는 UDP만 지원합니다. 포트를 변환할 때는 실제 서비스 개체의 프로토콜과 매핑된 서비스 개체의 프로토콜이 동일해야 합니다(둘 다 TCP거나 둘 다 UDP). ID NAT의 경우 실제 포트와 매핑된 포트에 동일한 개체를 사용할 수 있습니다.

고급 NAT 속성

NAT를 구성할 때는 고급 옵션에서 특수 서비스를 제공하는 속성을 구성할 수 있습니다. 이러한 모든 속성은 선택 사항이므로 서비스가 필요할 때만 구성하면 됩니다.

이 규칙과 일치하는 **DNS** 응답 변환

DNS 응답의 IP 주소를 변환할지 여부를 선택합니다. 매핑된 인터페이스에서 실제 인터페이스로 이동하는 DNS 응답의 경우 주소(IPv4 A 또는 IPv6 AAAA) 레코드가 매핑된 값에서 실제 값으로 재작성됩니다. 반대로, 실제 인터페이스에서 매핑된 인터페이스로 이동하는 DNS 응답의 경우 실제 값에서 매핑된 값으로 레코드가 재작성됩니다. 이 옵션은 특정 상황에서 사용되며, 재작성 시 A 레코드와 AAAA 레코드 간의 변환도 수행되는 NAT64/46 변환에 필요한 경우도 있습니다. 자세한 내용은 NAT를 사용하여 DNS 쿼리 및 응답 재작성, 242 페이지를 참고하십시오. 고정 NAT 규칙에서 포트 변환을 수행하는 경우에는 이 옵션을 사용할 수 없습니다.

인터페이스 **PAT(**대상 인터페이스**)**로 폴스루**(**동적 **NAT**만 해당됨**)**

다른 매핑된 주소가 이미 할당된 경우 대상 인터페이스의 IP 주소를 백업 방법으로 사용할지 여부를 선택합니다(인터페이스 PAT 대체). 이 옵션은 브리지 그룹의 구성원이 아닌 대상 인터페이스를 선택한 경우에만 사용할 수 있습니다. 인터페이스 PAT를 변환된 주소로 이미 구성한 경우에는 이 옵션을 선택할 수 없습니다. IPv6 네트워크에서는 이 옵션을 사용할 수 없습니다.

대상 인터페이스에서 **ARP** 프록시 설정 안 함**(**고정 **NAT**만 해당됨**)**

매핑된 IP 주소로 들어오는 패킷에 대해 프록시 ARP를 비활성화합니다. 매핑된 인터페이스와 동일한 네트워크의 주소를 사용하는 경우 시스템은 매핑된 주소에 대한 ARP 요청에 답하기 위해 프록시 ARP를 사용하며, 이에 따라 매핑된 주소로 가야 하는 트래픽을 가로챕니다. 디바이스가 추가 네트워크에 대한 게이트웨이가 될 필요가 없으므로 이 솔루션은 라우팅을 간소화합니다. 원하는 경우 프록시 ARP를 비활성화할 수 있습니다. 이 경우 업스트림 라우터에 적절한 경로가 있어야 합니다. 일반적으로 ID NAT에는 프록시 ARP가 필요하지 않으며, 프록시 ARP를 사용할 경우 연결 문제가 발생할 수도 있습니다.

대상 인터페이스에 대해 경로 조회 수행**(**고정 **ID NAT** 및 라우팅 모드만 해당됨**)**

원본 및 변환된 소스 주소에 대해 동일한 개체를 선택할 때 소스 및 대상 인터페이스를 선택하는 경우 이 옵션을 선택하면 시스템이 NAT 규칙에 구성된 대상 인터페이스를 사용하는 대신 라우팅 테이블을 기준으로 하여 대상 인터페이스를 결정하도록 할 수 있습니다.

IPv6 네트워크 변환

IPv6 전용 및 IPv4 전용 네트워크 간에 트래픽을 전달해야 하는 경우에는 NAT를 사용해 주소 유형을 변환해야 합니다. 두 IPv6 네트워크 간에 트래픽을 전달할 때도 외부 네트워크에서 내부 네트워크를 숨기려는 경우가 있습니다.

IPv6 네트워크에서는 다음 변환 유형을 사용할 수 있습니다.

- NAT64, NAT46 - IPv6 패킷에서 IPv4 패킷으로, 또는 그 반대로 변환합니다. 이 경우 두 개의 정책(IPv6에서 IPv4로의 변환 정책과 IPv4에서 IPv6으로의 변환 정책)을 정의해야 합니다. 단일 수동 NAT 규칙을 사용하여 정책 2개를 정의할 수는 있지만, DNS 서버가 외부 네트워크에 있으면 DNS 응답을 재작성해야 할 수도 있습니다. 대상을 지정할 때는 수동 NAT 규칙에 대해 DNS 재작성을 활성화할 수 없으므로, 자동 NAT 규칙 2개를 생성하는 것이 더 효율적인 방법입니다.

  참고 NAT46은 정적 매핑만 지원합니다.

- NAT66 - IPv6 패킷을 다른 IPv6 주소로 변환합니다. 고정 NAT를 사용하는 것이 좋습니다. 동적 NAT 또는 PAT를 사용할 수 있고 IPv6 주소가 대량으로 공급되지만, 동적 NAT를 반드시 사용할 필요는 없습니다.

참고 NAT64 및 NAT 46은 표준 라우팅 인터페이스에서만 사용할 수 있습니다. NAT66은 라우팅 인터페이스 및 브리지 그룹 구성원 인터페이스에서 모두 사용 가능합니다.

NAT64/46: IPv6 주소를 IPv4로 변환

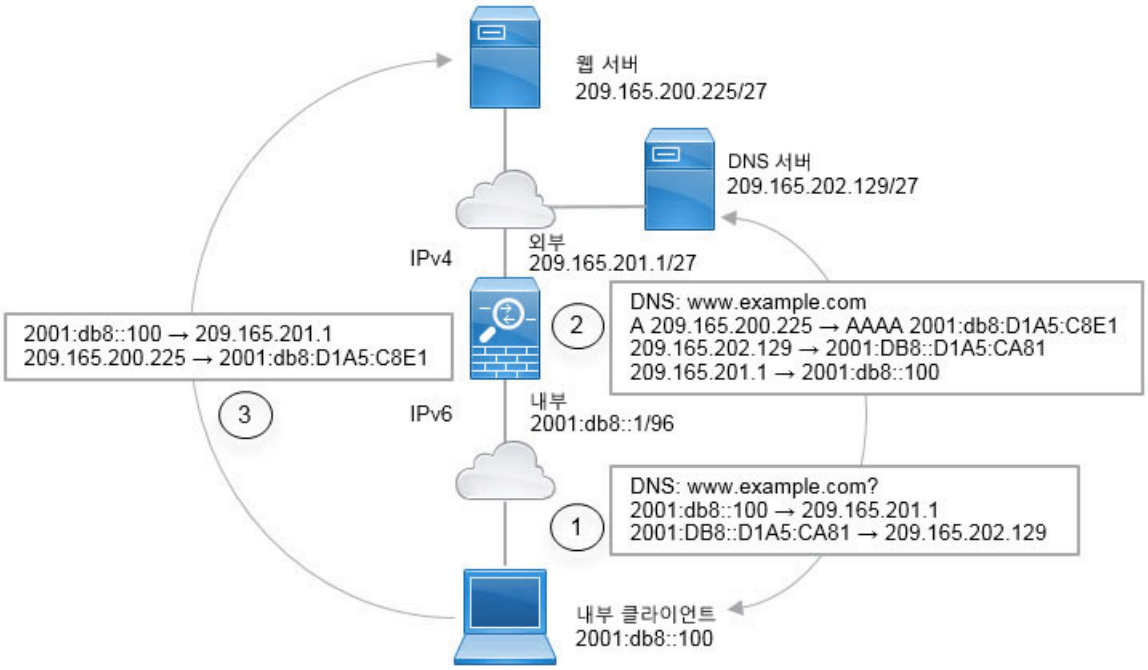
트래픽이 IPv6 네트워크에서 IPv4 전용 네트워크로 이동하는 경우에는 IPv6 주소를 IPv4로 변환해야 하며, 반환 트래픽은 IPv4에서 IPv6으로 변환해야 합니다. 따라서 주소 풀 2개(IPv4 네트워크에서 IPv6 주소를 바인딩하기 위한 IPv4 주소 풀과 IPv6 네트워크에서 IPv4 주소를 바인딩하기 위한 IPv6 주소 풀)를 정의해야 합니다.

- NAT64 규칙용 IPv4 주소 풀은 일반적으로 크기가 작으므로 대개 IPv6 클라이언트 주소와 일대일로 매핑할 주소를 충분히 포함하지 않을 수 있습니다. 동적 PAT의 경우 동적 또는 고정 NAT에 비해 더 쉽게 많은 IPv6 클라이언트 주소를 포함할 수 있습니다.
- NAT46 규칙용 IPv6 주소 풀은 매핑할 IPv4 주소보다 많은 수의 주소를 포함할 수 있습니다. 따라서 각 IPv4 주소를 서로 다른 IPv6 주소에 매핑할 수 있습니다. NAT46은 고정 매핑만 지원하므로 동적 PAT는 사용할 수 없습니다.

소스 IPv6 네트워크와 대상 IPv4 네트워크 중에 하나씩 2개의 정책을 정의해야 합니다. 단일 수동 NAT 규칙을 사용하여 정책 2개를 정의할 수는 있지만, DNS 서버가 외부 네트워크에 있으면 DNS 응답을 재작성해야 할 수도 있습니다. 대상을 지정할 때는 수동 NAT 규칙에 대해 DNS 재작성을 활성화할 수 없으므로, 자동 NAT 규칙 2개를 생성하는 것이 더 효율적인 방법입니다.

NAT64/46 예: 내부 IPv6 네트워크 및 외부 IPv4 인터넷

아래에는 내부 IPv6 전용 네트워크가 있는데 내부 사용자에게 필요한 일부 IPv4 전용 서비스는 외부 인터넷에 있는 일반적인 예가 나와 있습니다.



이 예에서는 외부 인터페이스의 IP 주소가 포함된 동적 인터페이스 PAT를 사용하여 내부 IPv6 네트워크를 IPv4로 변환합니다. 외부 IPv4 트래픽은 2001:db8::/96 네트워크의 주소로 정적 변환되어 내부 네트워크에서 전송을 허용합니다. 외부 DNS 서버의 회신을 A(IPv4) 레코드에서 AAAA(IPv6) 레코드로 변환하고 주소를 IPv4에서 IPv6으로 변환할 수 있도록 NAT46 규칙에 대해 DNS 재작성을 사용합니다.

내부 IPv6 네트워크의 2001:DB8::100에 있는 클라이언트가 www.example.com을 열려고 하는 웹 요청의 일반적인 순서는 다음과 같습니다.

1. 클라이언트의 컴퓨터가 2001:DB8::D1A5:CA81에 있는 DNS 서버에 DNS 요청을 보냅니다. NAT 규칙이 DNS 요청에서 소스 및 대상을 다음과 같이 변환합니다.
   - 2001:DB8::100을 209.165.201.1의 고유 포트로 변환합니다(NAT64 인터페이스 PAT 규칙).
   - 2001:DB8::D1A5:CA81을 209.165.202.129로 변환합니다(NAT46 규칙. D1A5:CA81은 209.165.202.129에 해당하는 IPv6 주소입니다.).
2. DNS 서버가 www.example.com이 209.165.200.225에 있음을 나타내는 A 레코드로 응답합니다. DNS 재작성을 사용하는 NAT46 규칙이 A 레코드를 IPv6의 동일 AAAA 레코드로 변환하고 AAAA 레코드의 209.165.200.225를 2001:db8:D1A5:C8E1로 변환합니다. 또한 DNS 응답의 소스 및 대상 주소는 변환되지 않은 상태입니다.
   - 209.165.202.129 -> 2001:DB8::D1A5:CA81
   - 209.165.201.1 -> 2001:db8::100
3. 이제 IPv6 클라이언트는 웹 서버의 IP 주소를 포함하며 2001:db8:D1A5:C8E1의 www.example.com에 대한 HTTP 요청을 수행합니다. D1A5:C8E1은 209.165.200.225에 해당하는 IPv6 주소입니다. 그리고 HTTP 요청의 소스 및 대상이 변환됩니다.

- 2001:DB8::100을 209.156.101.54의 고유 포트로 변환합니다(NAT64 인터페이스 PAT 규칙).
- 2001:db8:D1A5:C8E1을 209.165.200.225로 변환합니다(NAT46 규칙).

다음 절차에서는 이 예를 구성하는 방법을 설명합니다.

참고 이 예에서는 내부 인터페이스가 BVI(브리지 그룹 인터페이스)가 아닌 표준 라우팅 인터페이스라고 가정합니다. 내부 인터페이스가 BVI인 경우에는 각 구성원 인터페이스에 대한 규칙을 중복 생성해야 합니다.

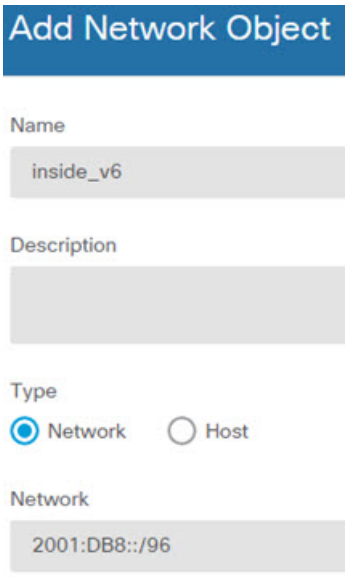
절차

단계 **1** 내부 IPv6 및 외부 IPv4 네트워크를 정의하는 네트워크 개체를 생성합니다.

a) **Objects**(개체)를 선택합니다.

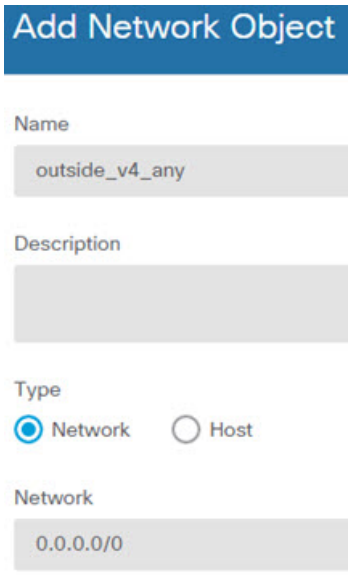
b) 목차에서 **Network**(네트워크)를 선택하고 +를 클릭합니다.

c) 내부 IPv6 네트워크를 정의합니다.
네트워크 개체의 이름을 inside_v6과 같이 지정하고 **Network**(네트워크)를 선택한 후에 네트워크 주소 2001:db8::/96을 입력합니다.



d) **OK**(확인)를 클릭합니다.

e) +를 클릭하여 외부 IPv4 네트워크를 정의합니다.
네트워크 개체의 이름을 outside_v4_any와 같이 지정하고 **Network**(네트워크)를 선택한 후에 네트워크 주소 0.0.0.0/0을 입력합니다.



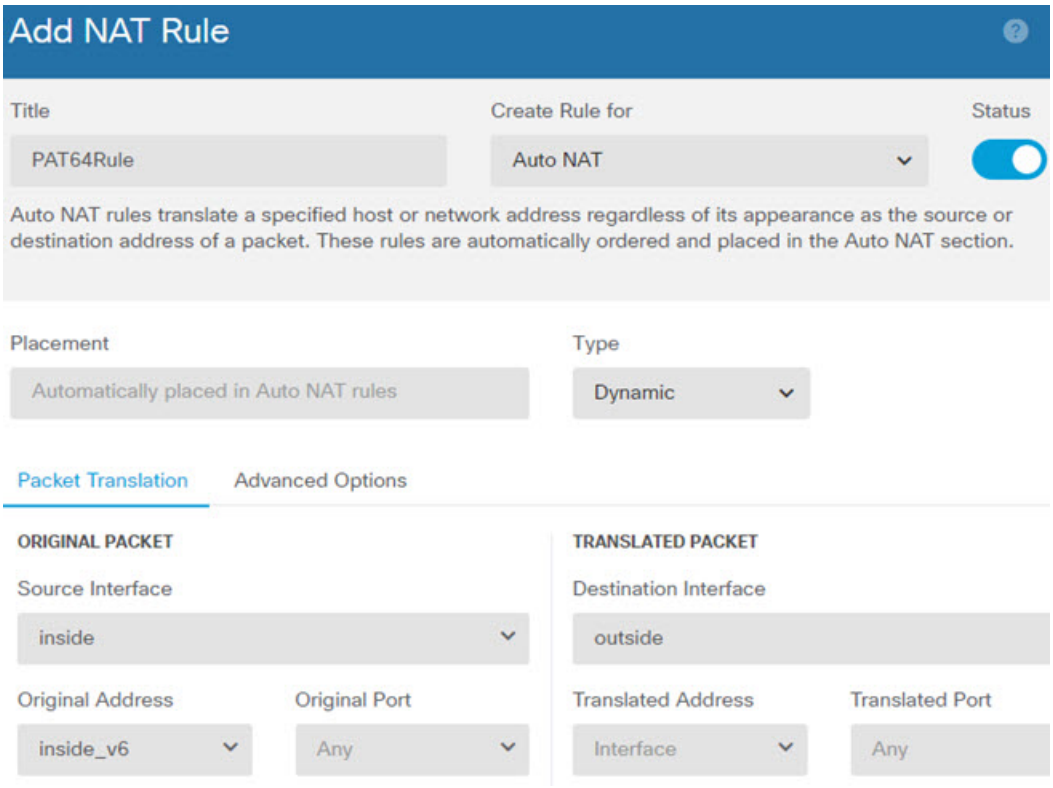
단계 **2** 내부 IPv6 네트워크용 NAT64 동적 PAT 규칙을 구성합니다.

a) **Policies(**정책**)** > **NAT**를 선택합니다.

b) + 버튼을 클릭합니다.

c) 다음 속성을 구성합니다.

- 제목 = PAT64Rule 또는 원하는 다른 이름
- 규칙 생성 = 자동 NAT
- 유형 = 동적
- 원본 인터페이스 = inside
- 대상 인터페이스 = outside
- 원본 주소 = inside_v6 네트워크 개체
- 변환된 주소 = **Interface**. 이 옵션은 PAT 주소로 대상 인터페이스의 IPv4 주소를 사용합니다.



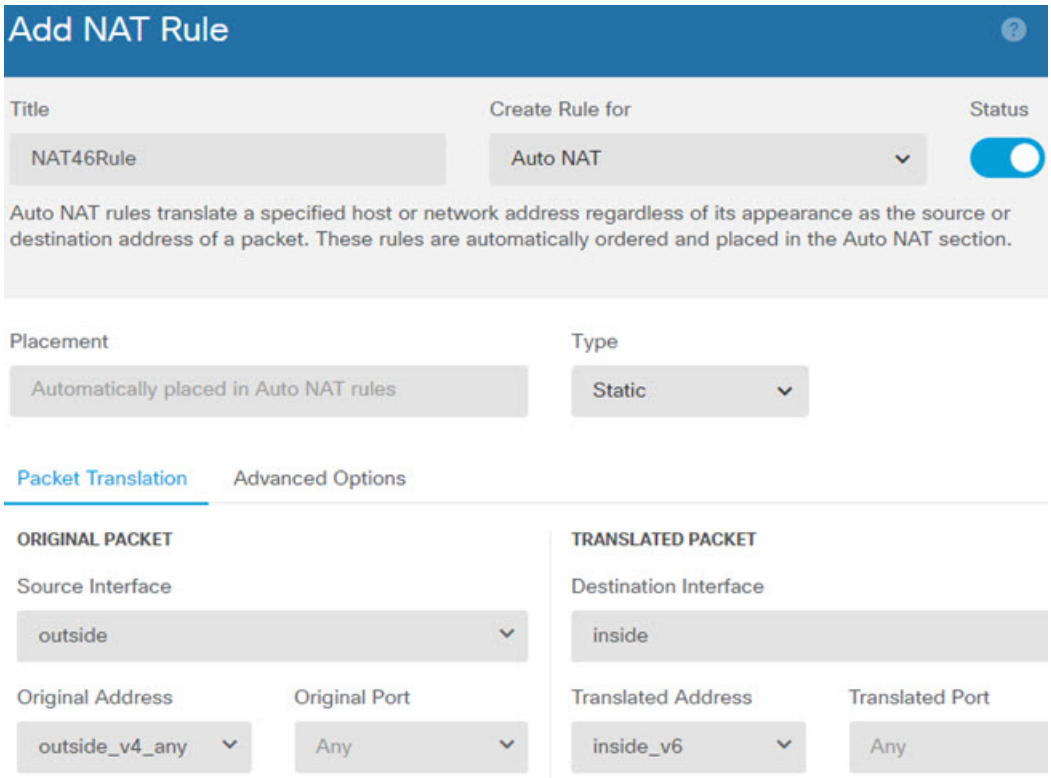
d) **OK**(확인)를 클릭합니다.
이 규칙을 사용하는 경우 내부 인터페이스의 2001:db8::/96 서브넷에서 외부 인터페이스로 이동하는 모든 트래픽은 외부 인터페이스의 IPv4 주소를 사용하여 NAT64 PAT로 변환됩니다.

단계 **3** 외부 IPv4 네트워크용 고정 NAT46 규칙을 구성합니다.

a) + 버튼을 클릭합니다.

b) 다음 속성을 구성합니다.

- 제목 = NAT46Rule 또는 원하는 다른 이름
- 규칙 생성 = 자동 NAT
- 유형 = 고정
- 원본 인터페이스 = outside
- 대상 인터페이스 = inside
- 원본 주소 = outside_v4_any 네트워크 개체
- 변환된 주소 = inside_v6 네트워크 개체
- 고급 옵션 탭에서 이 규칙과 일치하는 **DNS** 응답 변환을 선택합니다.



c) **OK**(확인)를 클릭합니다.
이 규칙을 사용하는 경우 외부 네트워크에서 내부 인터페이스로 들어오는 모든 IPv4 주소는 임베디드 IPv4 주소 방법을 사용하여 2001:db8::/96 네트워크의 주소로 변환됩니다. 또한 DNS 응답은 A(IPv4) 레코드에서 AAAA(IPv6) 레코드로 변환되며 주소는 IPv4에서 IPv6으로 변환됩니다.

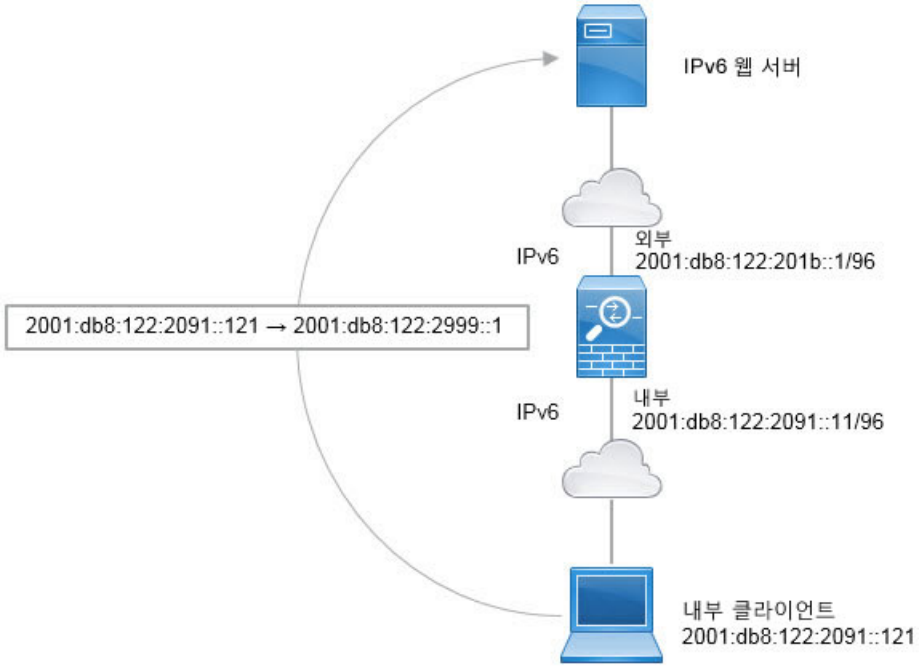
NAT66: IPv6 주소를 다른 IPv6 주소로 변환

IPv6 네트워크 간을 이동할 때는 주소를 외부 네트워크의 다른 IPv6 주소로 변환할 수 있습니다. 고정 NAT를 사용하는 것이 좋습니다. 동적 NAT 또는 PAT를 사용할 수 있고 IPv6 주소가 대량으로 공급되지만, 동적 NAT를 반드시 사용할 필요는 없습니다.

서로 다른 주소 유형 간을 변환하는 것이 아니므로 NAT66 변환을 위한 규칙 하나만 있으면 됩니다. 자동 NAT를 사용하면 이러한 규칙을 쉽게 모델링할 수 있습니다. 그러나 반환 트래픽을 허용하지 않으려는 경우에는 수동 NAT만 사용하여 고정 NAT 규칙을 단방향으로 설정할 수 있습니다.

NAT66 예, 네트워크 간의 고정 변환

자동 NAT를 사용하여 IPv6 주소 간의 고정 변환을 구성할 수 있습니다. 다음 예에서는 2001:db8:122:2091::/96 네트워크의 내부 주소를 2001:db8:122:2999::/96 네트워크의 외부 주소로 변환하는 방법을 설명합니다.



참고 이 예에서는 내부 인터페이스가 BVI(브리지 그룹 인터페이스)가 아닌 표준 라우팅 인터페이스라고 가정합니다. 내부 인터페이스가 BVI인 경우에는 각 구성원 인터페이스에 대한 규칙을 중복 생성해야 합니다.

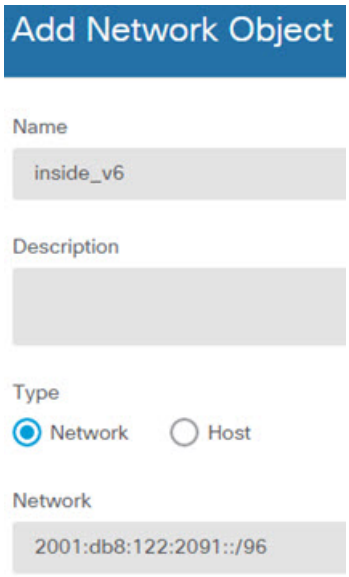
절차

단계 **1** 내부 IPv6 및 외부 IPv6 NAT 네트워크를 정의하는 네트워크 개체를 생성합니다.

a) **Objects(**개체**)**를 선택합니다.

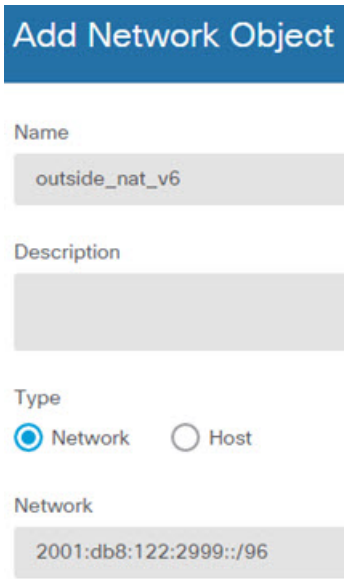
b) 목차에서 **Network(**네트워크**)**를 선택하고 +를 클릭합니다.

c) 내부 IPv6 네트워크를 정의합니다.
네트워크 개체의 이름을 inside_v6과 같이 지정하고 **Network(**네트워크**)**를 선택한 후에 네트워크 주소 2001:db8:122:2091::/96을 입력합니다.



d) **OK(**확인**)**를 클릭합니다.

e) +를 클릭하여 외부 IPv6 NAT 네트워크를 정의합니다.
네트워크 개체의 이름을 outside_nat_v6과 같이 지정하고 **Network(**네트워크**)**를 선택한 후에 네트워크 주소 2001:db8:122:2999::/96을 입력합니다.



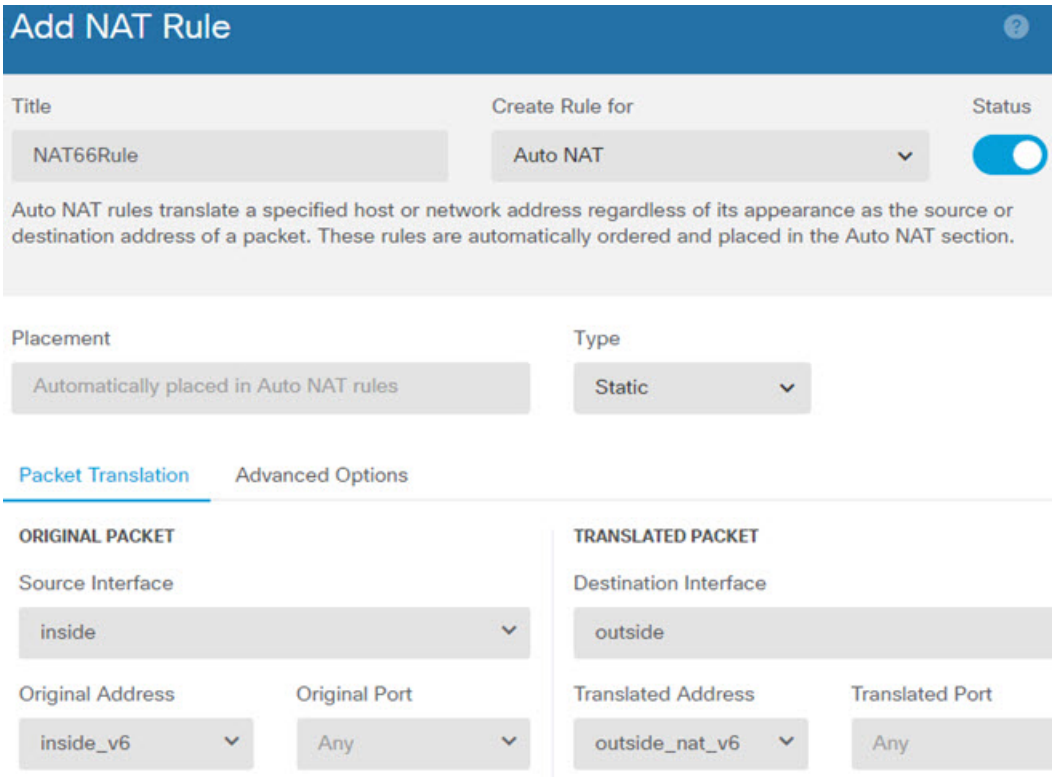
단계 **2** 내부 IPv6 네트워크용 고정 NAT 규칙을 구성합니다.

a) **Policies(**정책**)** > **NAT**를 선택합니다.

b) + 버튼을 클릭합니다.

c) 다음 속성을 구성합니다.

- 제목 = NAT66Rule 또는 원하는 다른 이름
- 규칙 생성 = 자동 NAT
- 유형 = 고정
- 소스 인터페이스 = inside
- 대상 인터페이스 = outside
- 원본 주소 = inside_v6 네트워크 개체
- 변환된 주소 = outside_nat_v6 네트워크 개체

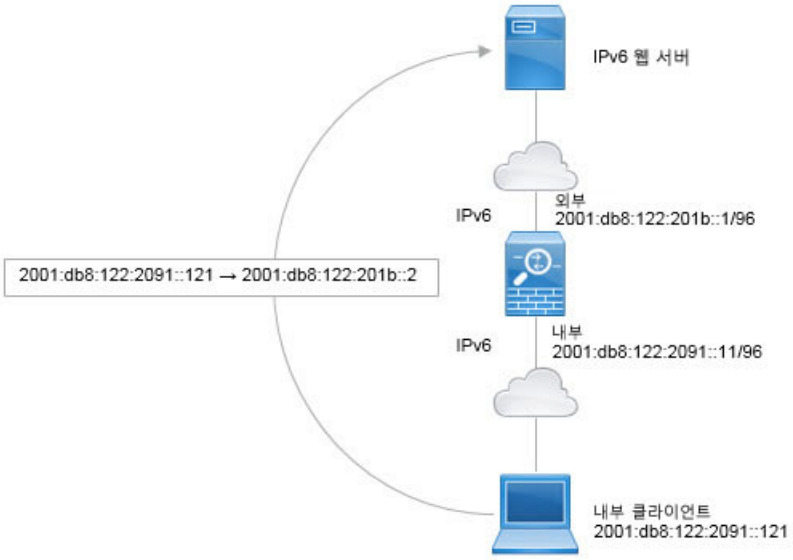


d) **OK(**확인**)**를 클릭합니다.
이 규칙을 사용하는 경우 내부 인터페이스의 2001:db8:122:2091::/96 서브넷에서 외부 인터페이스로 이동하는 모든 트래픽은 2001:db8:122:2999::/96 네트워크의 주소로 고정 NAT66 변환됩니다.

NAT66 예, 간단한 IPv6 인터페이스 PAT

NAT66을 구현하는 단순한 방식은 내부 주소를 외부 인터페이스 IPv6 주소의 각기 다른 포트에 동적으로 할당하는 것입니다.

그러나 Firepower Device Manager를 사용하는 인터페이스의 IPv6 주소를 사용하여 인터페이스 PAT를 구성할 수는 없습니다. 대신 동적 PAT 풀과 같은 네트워크에 있는 단일 사용 가능 주소를 사용합니다.



참고 이 예에서는 내부 인터페이스가 BVI(브리지 그룹 인터페이스)가 아닌 표준 라우팅 인터페이스라고 가정합니다. 내부 인터페이스가 BVI인 경우에는 각 구성원 인터페이스에 대한 규칙을 중복 생성해야 합니다.

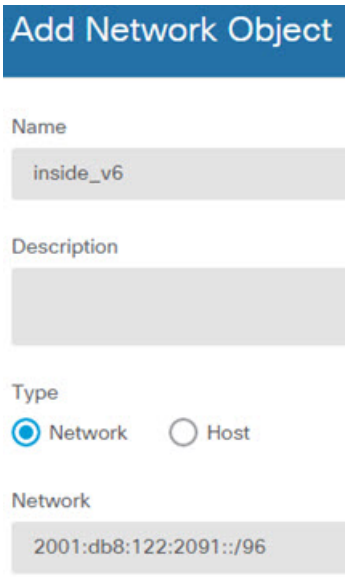
절차

단계 **1** 내부 IPv6 네트워크 및 IPv6 PAT 주소를 정의하는 네트워크 개체를 생성합니다.

a) **Objects(**개체**)**를 선택합니다.

b) 목차에서 **Network(**네트워크**)**를 선택하고 +를 클릭합니다.

c) 내부 IPv6 네트워크를 정의합니다.
네트워크 개체의 이름을 inside_v6과 같이 지정하고 **Network(**네트워크**)**를 선택한 후에 네트워크 주소 2001:db8:122:2091::/96을 입력합니다.



d) **OK(**확인**)**를 클릭합니다.

e) +를 클릭하여 외부 IPv6 PAT 주소를 정의합니다.
네트워크 개체의 이름을 ipv6_pat와 같이 지정하고 **Host(**호스트**)**를 선택한 후에 호스트 주소 2001:db8:122:201b::2를 입력합니다.

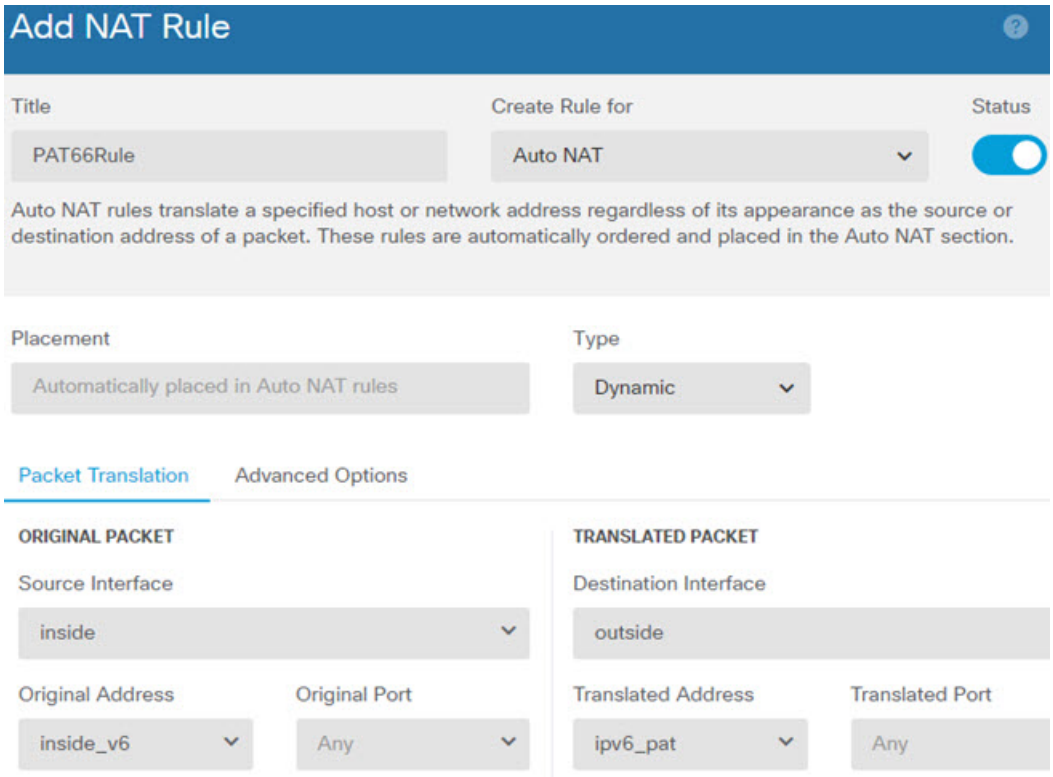
단계 **2** 내부 IPv6 네트워크용 동적 PAT 규칙을 구성합니다.

a) **Policies(**정책**)** > **NAT**를 선택합니다.

b) + 버튼을 클릭합니다.

c) 다음 속성을 구성합니다.

- 제목 = PAT66Rule 또는 원하는 다른 이름
- 규칙 생성 = 자동 NAT
- 유형 = 동적
- 원본 인터페이스 = inside
- 대상 인터페이스 = outside
- 원본 주소 = inside_v6 네트워크 개체
- 변환된 주소 = ipv6_pat 네트워크 개체



d) **OK(**확인**)**를 클릭합니다.
이 규칙을 사용하는 경우 내부 인터페이스의 2001:db8:122:2091::/96 서브넷에서 외부 인터페이스로 이동하는 모든 트래픽은 2001:db8:122:201b::2의 포트로 동적 PAT66 변환됩니다.

NAT 모니터링

NAT 연결을 모니터링하고 문제해결을 수행하려면 디바이스 CLI에 로그인하여 다음 명령을 사용합니다.

- **show nat**는 NAT 규칙 및 규칙별 적중 횟수를 표시합니다. NAT의 다른 측면을 표시하는 추가 키워드도 있습니다.
- **show xlate**는 현재 활성 상태인 활성 NAT 변환을 표시합니다.
- **clear xlate**를 사용하면 활성 NAT 변환을 제거할 수 있습니다. NAT 규칙을 변경하는 경우에는 활성 변환을 제거해야 할 수 있습니다. 기존 연결은 종료될 때까지 이전 변환 슬롯을 계속 사용하기 때문입니다. 변환을 지우면 시스템에서 새 규칙을 기반으로 하여 클라이언트의 다음 연결 시도 시 클라이언트에 대한 새 변환을 작성할 수 있습니다.

NAT의 예

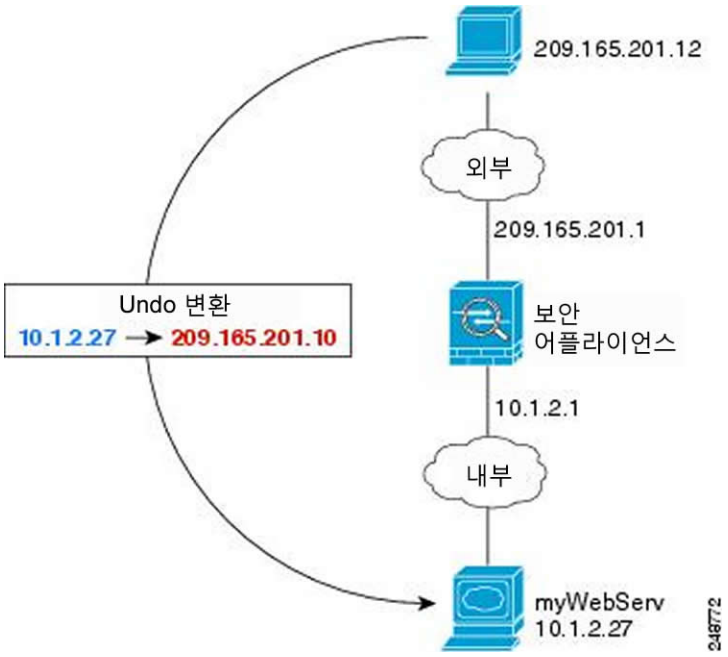
다음 항목에서는 Threat Defense 디바이스에서 NAT를 구성하는 예를 제공합니다.

내부 웹 서버에 대한 액세스 제공(고정 자동 NAT)

다음 예제는 내부 웹 서버에 대해 고정 NAT를 수행합니다. 실제 주소는 사설 네트워크에 있으므로 공용 주소가 필요합니다. 호스트가 고정된 주소에서 웹 서버에 대한 트래픽을 시작할 수 있으려면 고정 NAT가 필요합니다.

참고 이 예에서는 내부 인터페이스가 BVI(브리지 그룹 인터페이스)가 아닌 표준 라우팅 인터페이스라고 가정합니다. 내부 인터페이스가 BVI인 경우 웹 서버가 연결된 특정 브리지 그룹 구성원 인터페이스(예: inside1_3)를 선택합니다.

그림 ***15:*** 내부 웹 서버에 대한 고정 ***NAT***



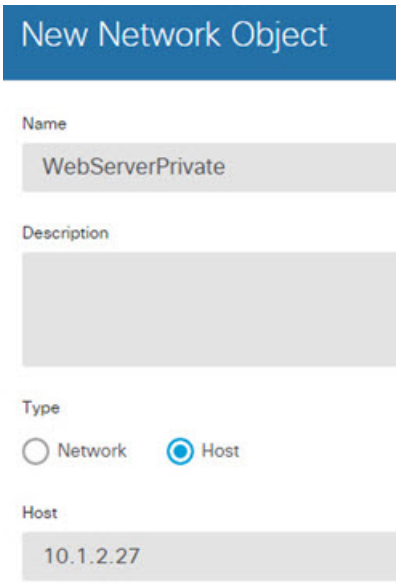
절차

단계 **1** 서버의 전용 및 공용 호스트 주소를 정의하는 네트워크 개체를 생성합니다.

a) **Objects(**개체**)**를 선택합니다.

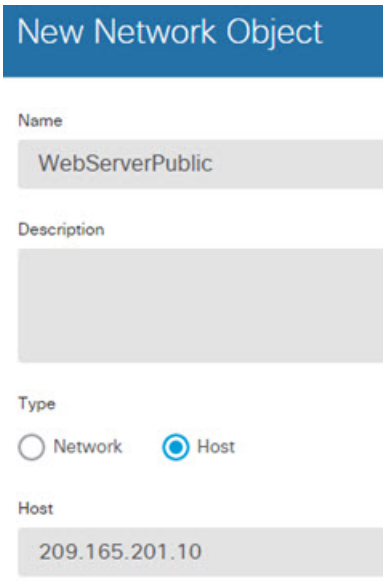
b) 목차에서 **Network(**네트워크**)**를 선택하고 +를 클릭합니다.

c) 웹 서버의 전용 어드레스를 정의합니다.
네트워크 개체의 이름을 WebServerPrivate과 같이 지정하고 **Host(**호스트**)**를 선택한 후에 실제 호스트 IP 주소 10.1.2.27을 입력합니다.



d) **OK(**확인**)**를 클릭합니다.

e) +를 클릭하여 공용 주소를 정의합니다.
네트워크 개체의 이름을 WebServerPublic과 같이 지정하고 **Host(**호스트**)**를 선택한 후에 호스트 주소 209.165.201.10을 입력합니다.



f) **OK(**확인**)**를 클릭합니다.

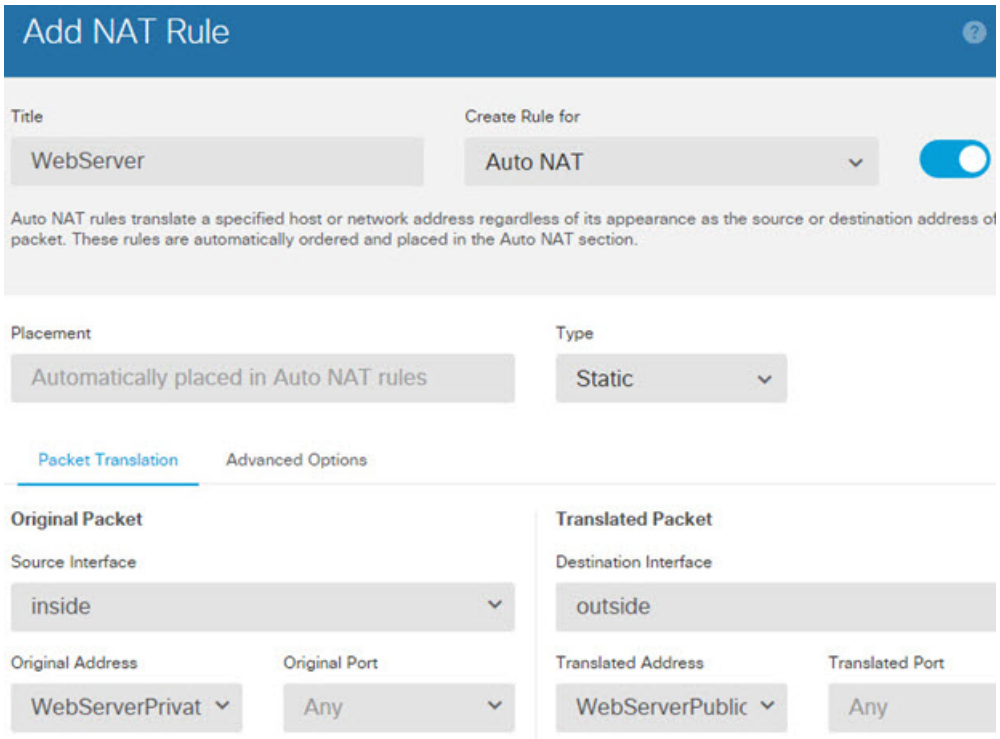
단계 **2** 개체용 고정 NAT를 구성합니다.

a) **Policies(**정책**)** > **NAT**를 선택합니다.

b) + 버튼을 클릭합니다.

c) 다음 속성을 구성합니다.

- 제목 = WebServer 또는 원하는 다른 이름
- 규칙 생성 = 자동 NAT
- 유형 = 고정
- 소스 인터페이스 = inside
- 대상 인터페이스 = outside
- 원본 주소 = WebServerPrivate 네트워크 개체
- 변환된 주소 = WebServerPublic 네트워크 개체



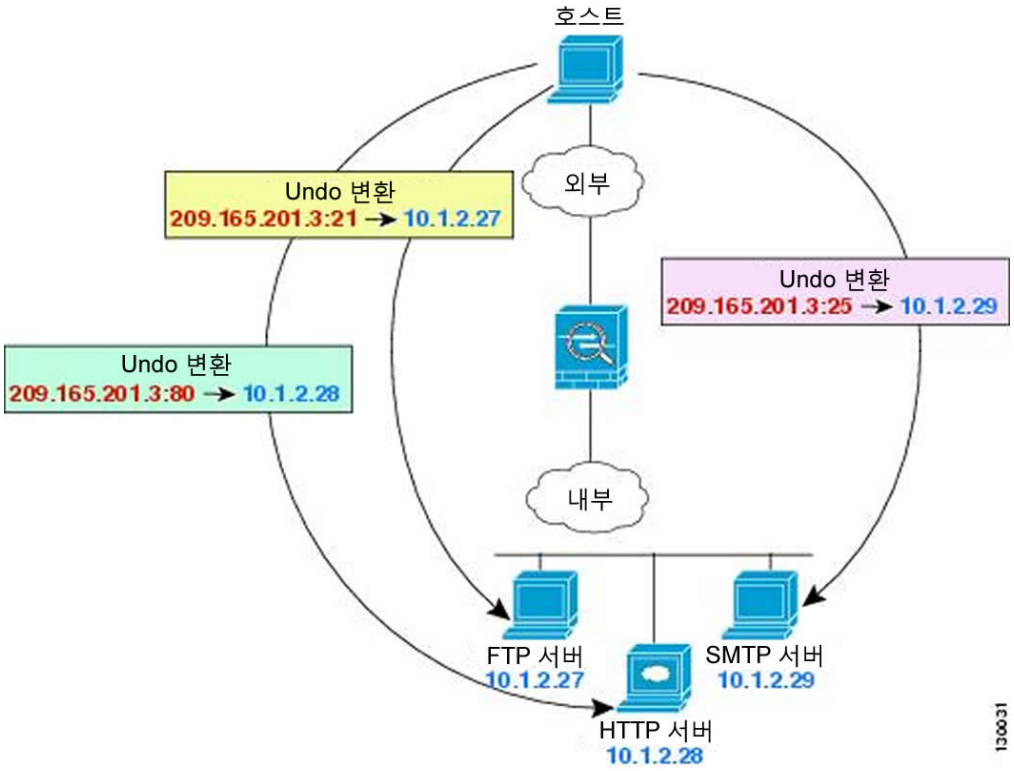
d) **OK(**확인**)**를 클릭합니다.

FTP, HTTP 및 SMTP용 단일 주소(포트 변환 고정 자동 NAT)

다음과 같은 포트 변환 고정 NAT의 예는 원격 사용자가 FTP, HTTP 및 SMTP에 액세스하기 위해 사용할 단일 주소를 제공합니다. 이러한 서버는 실제 네트워크에서 실제로 서로 다른 디바이스이지만, 각 서버에 대해 동일하게 매핑된 IP 주소를 사용하되 포트는 다른 포트 변환 고정 NAT 규칙을 지정할 수 있습니다.

참고 이 예에서는 내부 인터페이스가 스위치에 연결된 표준 라우팅 인터페이스이며 서버가 스위치에 연결되어 있다고 가정합니다. 내부 인터페이스가 BVI(브리지 그룹 인터페이스)이며 서버가 별도의 브리지 그룹 구성원 인터페이스에 연결되어 있으면 해당하는 규칙에 대해 각 서버가 연결된 특정 구성원 인터페이스를 선택합니다. 예를 들어 규칙이 소스 인터페이스에 대해 inside가 아닌 inside1_2, inside1_3 및 inside1_4를 포함할 수 있습니다.

그림 ***16:*** 포트 변환 고정 ***NAT***



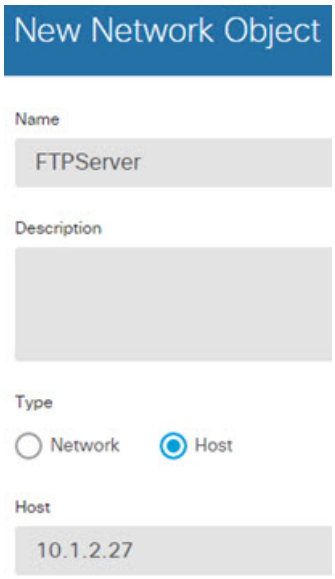
절차

단계 **1** FTP 서버용 네트워크 개체를 만듭니다.

a) **Objects(**개체**)**를 선택합니다.

b) 목차에서 **Network(**네트워크**)**를 선택하고 +를 클릭합니다.

c) 네트워크 개체의 이름을 FTPserver와 같이 지정하고 **Host(**호스트**)**를 선택한 후에 FTP 서버의 실제 IP 주소 10.1.2.27을 입력합니다.

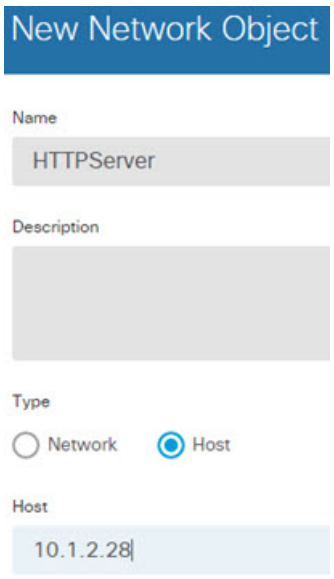


d) **OK(**확인**)**를 클릭합니다.

단계 **2** HTTP 서버용 네트워크 개체를 생성합니다.

a) +를 클릭합니다.

b) 네트워크 개체의 이름을 HTTPserver와 같이 지정하고 호스트를 선택한 후에 호스트 주소 10.1.2.28을 입력합니다.

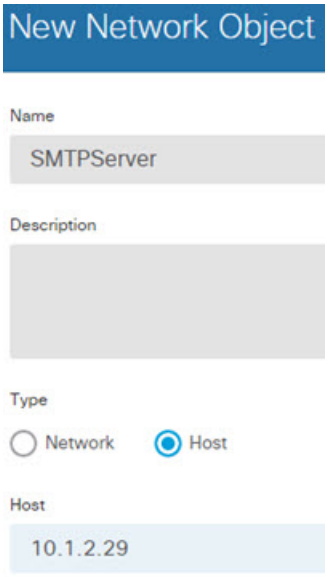


c) **OK(**확인**)**를 클릭합니다.

단계 **3** SMTP 서버용 네트워크 개체를 생성합니다.

a) +를 클릭합니다.

b) 네트워크 개체의 이름을 SMTPserver와 같이 지정하고 호스트를 선택한 후에 호스트 주소 10.1.2.29를 입력합니다.

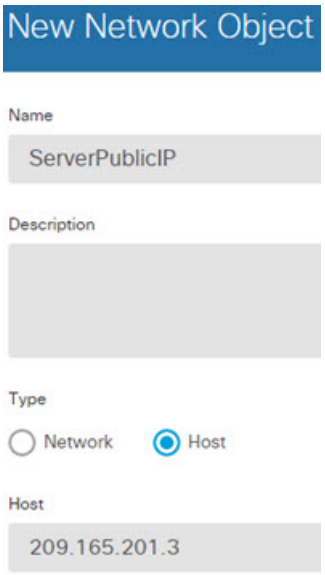


c) **OK(**확인**)**를 클릭합니다.

단계 **4** 서버 3대에 사용되는 공용 IP 주소용 네트워크 개체를 생성합니다.

a) +를 클릭합니다.

b) 네트워크 개체의 이름을 ServerPublicIP와 같이 지정하고 **Host(**호스트**)**를 선택한 후에 호스트 주소 209.165.201.3을 입력합니다.



c) **OK**(확인)를 클릭합니다.

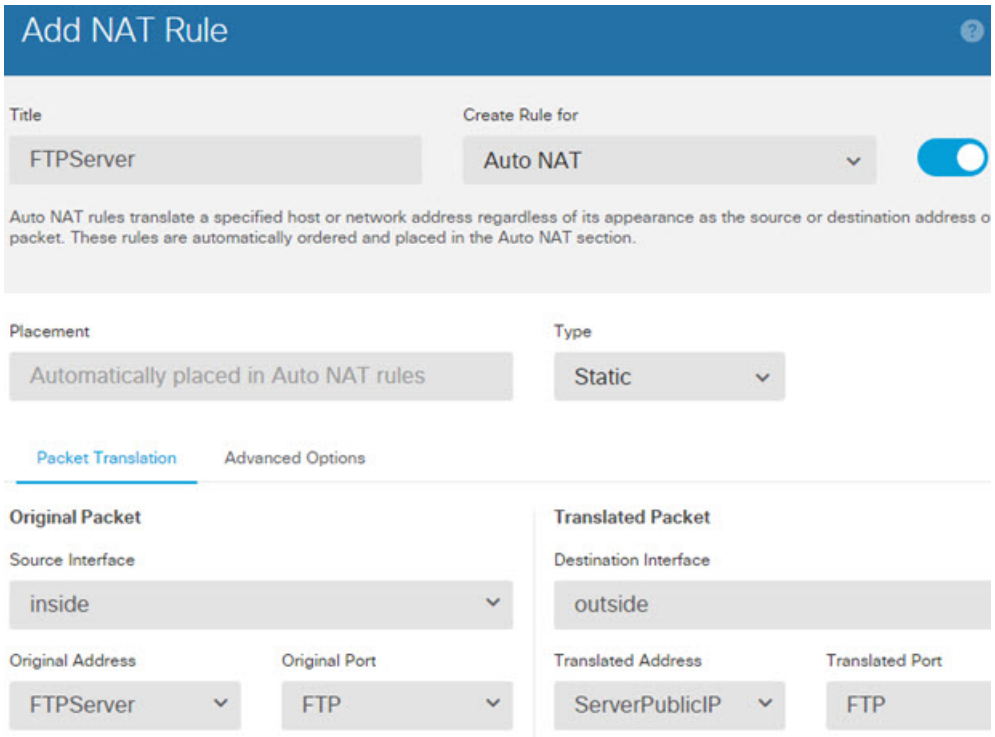
단계 **5** FTP 포트를 자기 자신에 매핑하는 FTP 서버용 포트 변환 고정 NAT를 구성합니다.

a) **Policies**(정책) > **NAT**를 선택합니다.

b) + 버튼을 클릭합니다.

c) 다음 속성을 구성합니다.

- 제목 = FTPServer 또는 원하는 다른 이름
- 규칙 생성 = 자동 NAT
- 유형 = 고정
- 소스 인터페이스 = inside
- 대상 인터페이스 = outside
- 원본 주소 = FTPserver 네트워크 개체
- 변환된 주소 = ServerPublicIP 네트워크 개체
- 원본 포트 = FTP 포트 개체
- 변환된 포트 = FTP 포트 개체

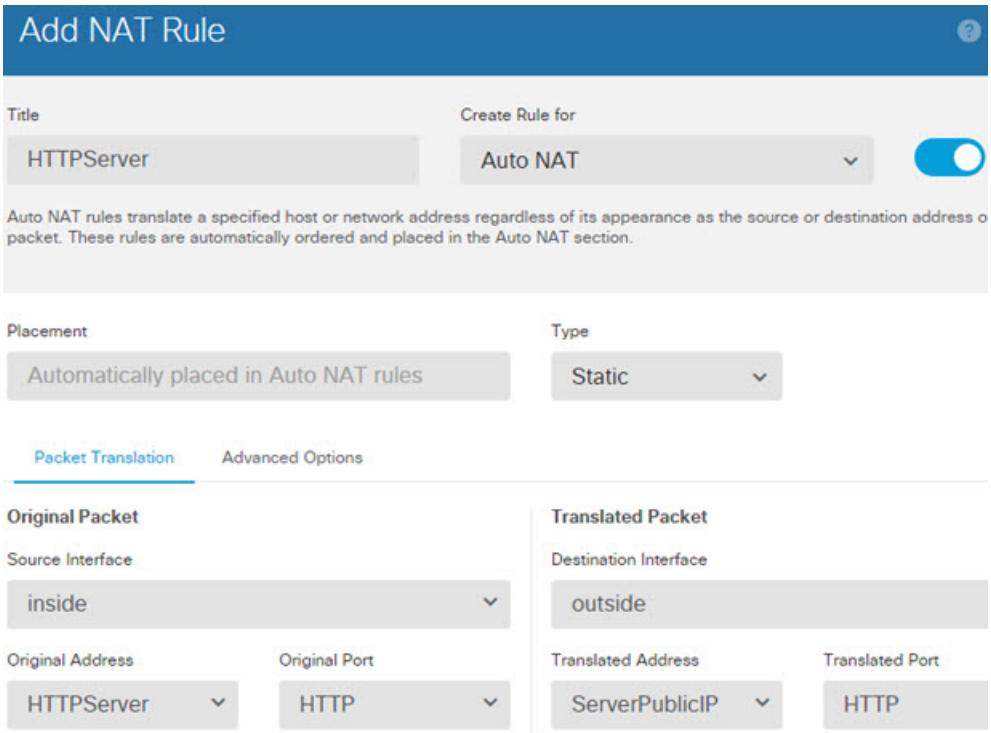


d) **OK**(확인)를 클릭합니다.

단계 **6** HTTP 포트를 자기 자신에 매핑하는 HTTP 서버용 포트 변환 고정 NAT를 구성합니다.

a) + 버튼을 클릭합니다.
b) 다음 속성을 구성합니다.

- 제목 = HTTPServer 또는 원하는 다른 이름
- 규칙 생성 = 자동 NAT
- 유형 = 고정
- 소스 인터페이스 = inside
- 대상 인터페이스 = outside
- 원본 주소 = HTTPserver 네트워크 개체
- 변환된 주소 = ServerPublicIP 네트워크 개체
- 원본 포트 = HTTP 포트 개체
- 변환된 포트 = HTTP 포트 개체



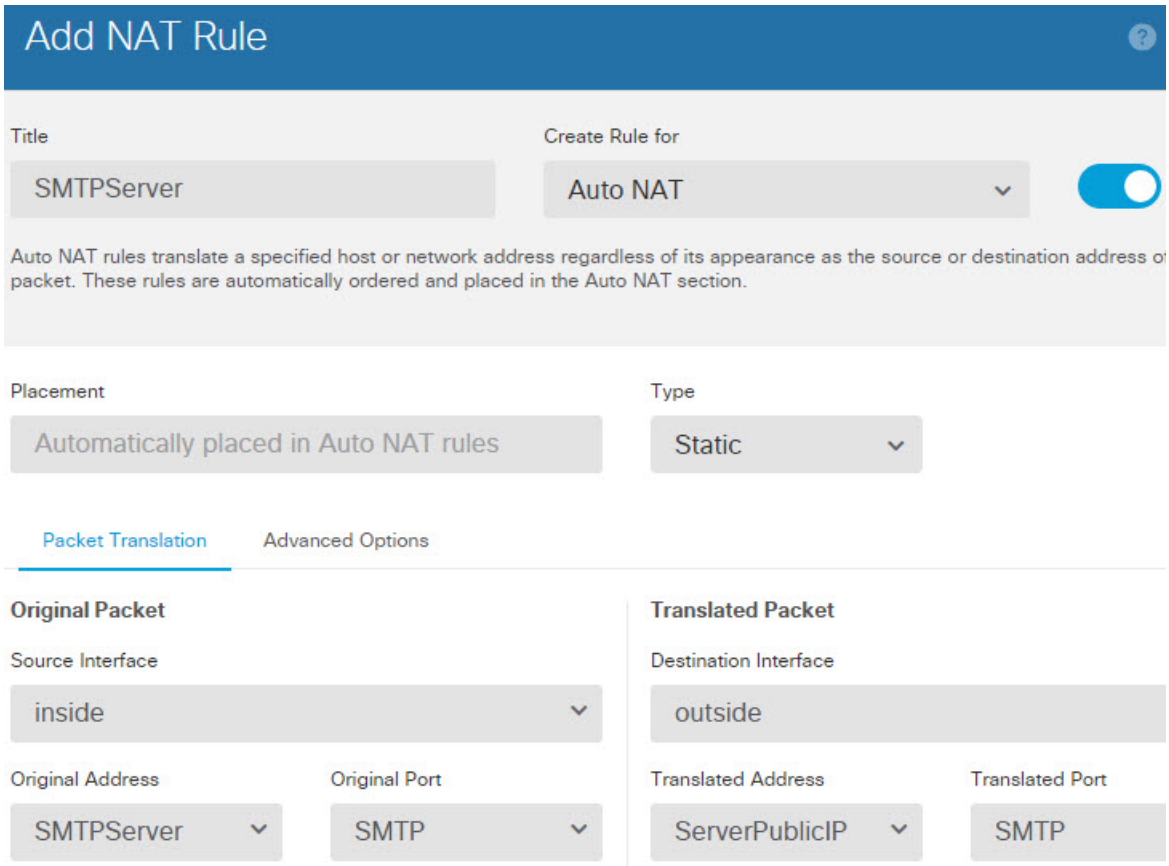
c) **OK(**확인)를 클릭합니다.

단계 **7** SMTP 포트를 자기 자신에 매핑하는 SMTP 서버용 포트 변환 고정 NAT를 구성합니다.

a) + 버튼을 클릭합니다.
b) 다음 속성을 구성합니다.

- 제목 = SMTPServer 또는 원하는 다른 이름

- 규칙 생성 = 자동 NAT
- 유형 = 고정
- 소스 인터페이스 = inside
- 대상 인터페이스 = outside
- 원본 주소 = SMTPserver 네트워크 개체
- 변환된 주소 = ServerPublicIP 네트워크 개체
- 원본 포트 = SMTP 포트 개체
- 변환된 포트 = SMTP 포트 개체



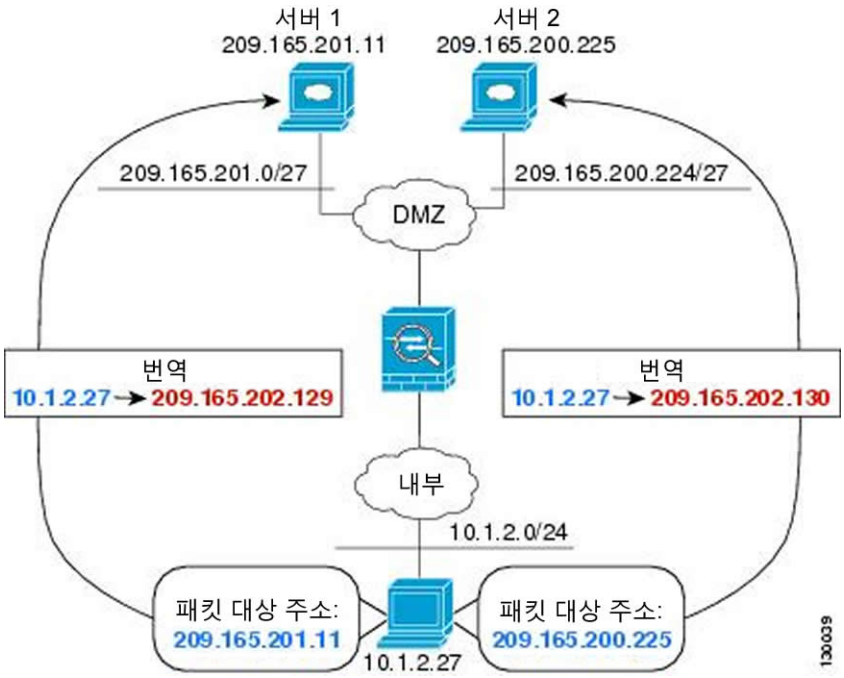
c) **OK**(확인)를 클릭합니다.

대상에 따라 다른 변환(동적 수동 PAT)

다음 그림은 두 개의 서로 다른 서버에 액세스하는 10.1.2.0/24 네트워크의 호스트를 보여줍니다. 호스트가 209.165.201.11의 서버에 액세스하면 실제 주소가 209.165.202.129:*port*로 변환됩니다. 호스트가 209.165.200.225의 서버에 액세스하면 실제 주소가 209.165.202.130:*port*로 변환됩니다.

참고 이 예에서는 내부 인터페이스가 스위치에 연결된 표준 라우팅 인터페이스이며 서버가 스위치에 연결되어 있다고 가정합니다. 내부 인터페이스가 BVI(브리지 그룹 인터페이스)이며 서버가 별도의 브리지 그룹 구성원 인터페이스에 연결되어 있으면 해당하는 규칙에 대해 각 서버가 연결된 특정 구성원 인터페이스를 선택합니다. 예를 들어 규칙이 소스 인터페이스에 대해 inside가 아닌 inside1_2 및 inside1_3을 포함할 수 있습니다.

그림 ***17:*** 서로 다른 대상 주소를 사용하는 수동 ***NAT***



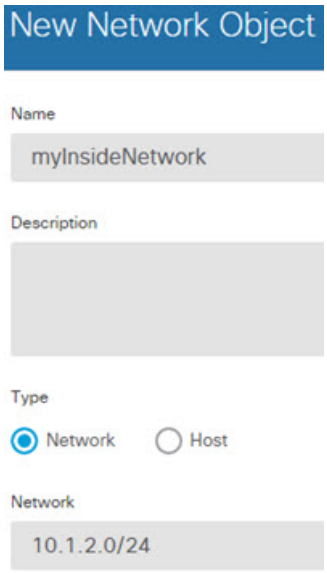
절차

단계 **1** 내부 네트워크용 네트워크 개체를 만듭니다.

a) **Objects(**개체**)**를 선택합니다.

b) 목차에서 **Network(**네트워크**)**를 선택하고 +를 클릭합니다.

c) 네트워크 개체의 이름을 myInsideNetwork와 같이 지정하고 **Network(**네트워크**)**를 선택한 후에 실제 네트워크 주소 10.1.2.0/24를 입력합니다.

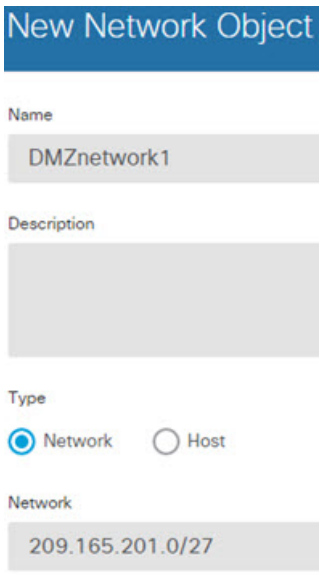


d) **OK(**확인**)**를 클릭합니다.

단계 **2** DMZ 네트워크 1용 네트워크 개체를 생성합니다.

a) +를 클릭합니다.

b) 네트워크 개체의 이름을 DMZnetwork1과 같이 지정하고 **Network(**네트워크**)**를 선택한 후에 네트워크 주소 209.165.201.0/27(서브넷 마스크 255.255.255.224)을 입력합니다.

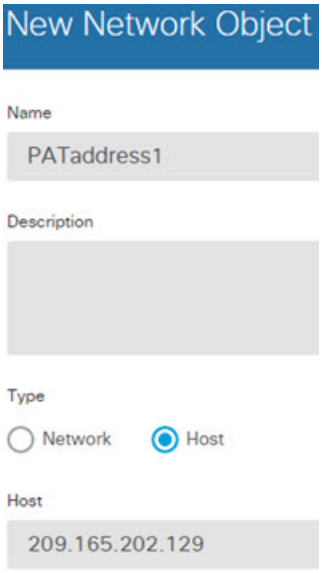


c) **OK(**확인**)**를 클릭합니다.

단계 **3** DMZ 네트워크 1용 PAT 주소의 네트워크 개체를 생성합니다.

a) +를 클릭합니다.

b) 네트워크 개체의 이름을 PATaddress1과 같이 지정하고 **Host(**호스트**)**를 선택한 후에 호스트 주소 209.165.202.129를 입력합니다.

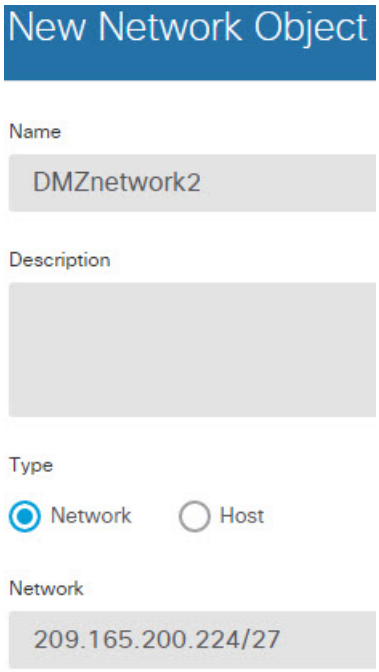


c) **OK(**확인**)**를 클릭합니다.

단계 **4** DMZ 네트워크 2용 네트워크 개체를 생성합니다.

a) +를 클릭합니다.

b) 네트워크 개체의 이름을 DMZnetwork2와 같이 지정하고 **Network(**네트워크**)**를 선택한 후에 네트워크 주소 209.165.200.224/27(서브넷 마스크 255.255.255.224)을 입력합니다.

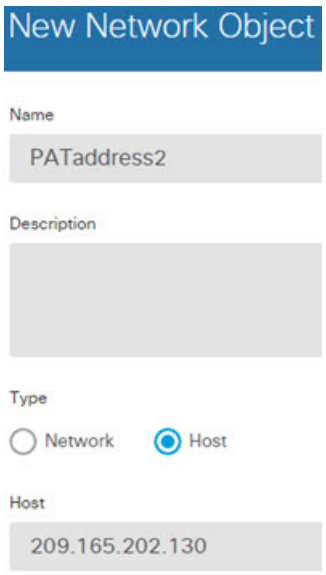


c) **OK(**확인**)**를 클릭합니다.

단계 **5** DMZ 네트워크 2용 PAT 주소의 네트워크 개체를 생성합니다.

a) +를 클릭합니다.

b) 네트워크 개체의 이름을 PATaddress2와 같이 지정하고 **Host(**호스트**)**를 선택한 후에 호스트 주소 209.165.202.130을 입력합니다.



c) **OK(**확인**)**를 클릭합니다.

단계 **6** DMZ 네트워크 1용 동적 수동 PAT를 구성합니다.

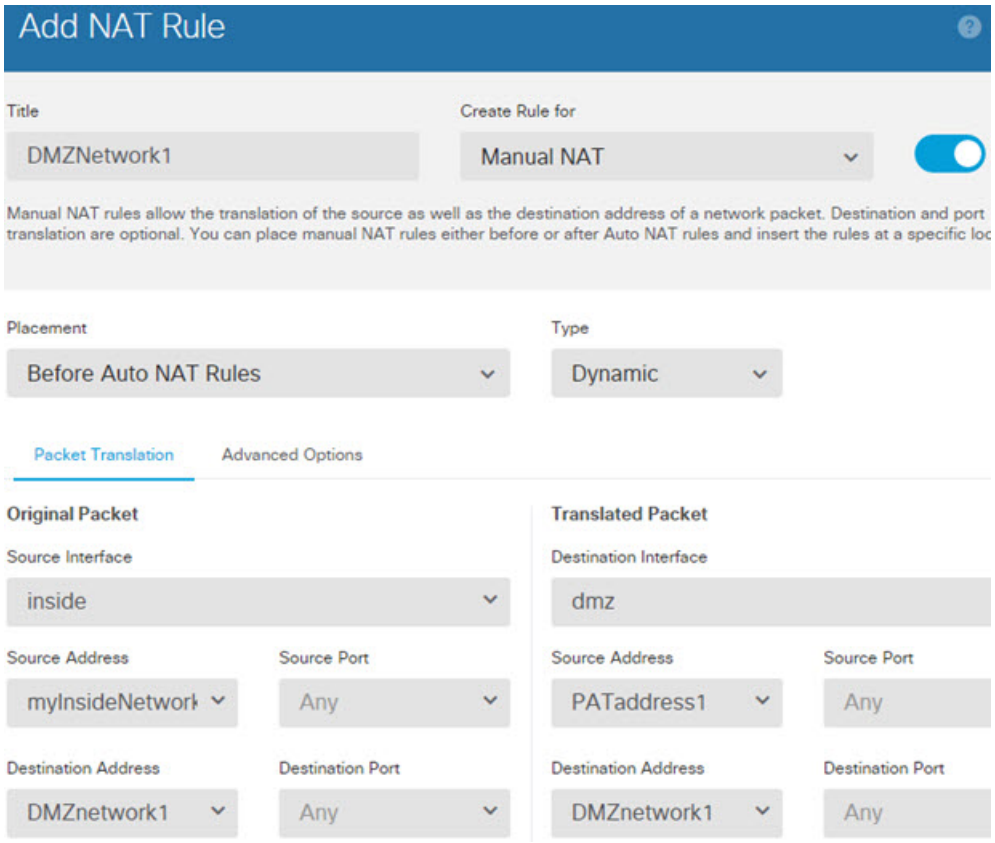
a) **Policies(**정책**)** > **NAT**를 선택합니다.

b) + 버튼을 클릭합니다.

c) 다음 속성을 구성합니다.

- 제목 = DMZNetwork1 또는 원하는 다른 이름
- 규칙 생성 = 수동 NAT
- 유형 = 동적
- 소스 인터페이스 = inside
- 대상 인터페이스 = dmz
- 원본 소스 주소 = myInsideNetwork 네트워크 개체
- 변환된 소스 주소 = PATaddress1 네트워크 개체
- 원본 대상 주소 = DMZnetwork1 네트워크 개체
- 변환된 대상 주소 = DMZnetwork1 네트워크 개체

참고 대상 주소를 변환하지 않을 것이기 때문에 원본 주소 및 변환된 대상 주소에 대해 동일한 주소를 지정하여 대상 주소에 대한 ID NAT를 구성해야 합니다. 포트 필드는 모두 비워 둡니다.



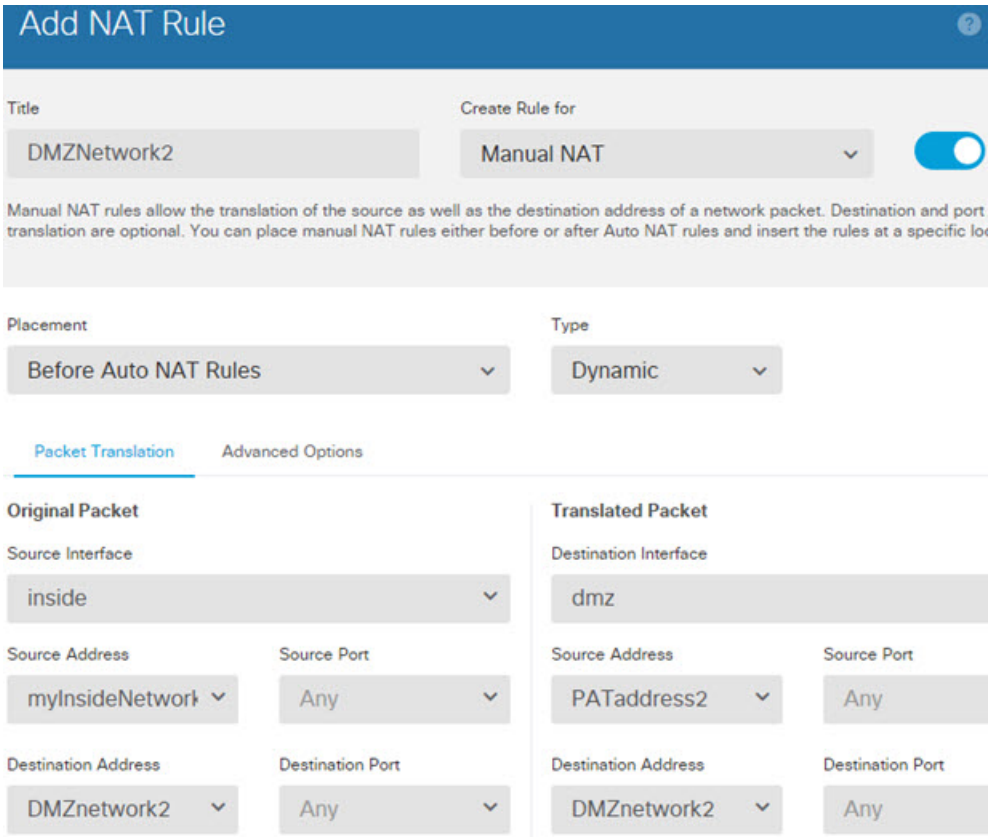
d) **OK(**확인**)**를 클릭합니다.

단계 **7** DMZ 네트워크 2용 동적 수동 PAT를 구성합니다.

a) + 버튼을 클릭합니다.

b) 다음 속성을 구성합니다.

- 제목 = DMZNetwork2 또는 원하는 다른 이름
- 규칙 생성 = 수동 NAT
- 유형 = 동적
- 소스 인터페이스 = inside
- 대상 인터페이스 = dmz
- 원본 소스 주소 = myInsideNetwork 네트워크 개체
- 변환된 소스 주소 = PATaddress2 네트워크 개체
- 원본 대상 주소 = DMZnetwork2 네트워크 개체
- 변환된 대상 주소 = DMZnetwork2 네트워크 개체



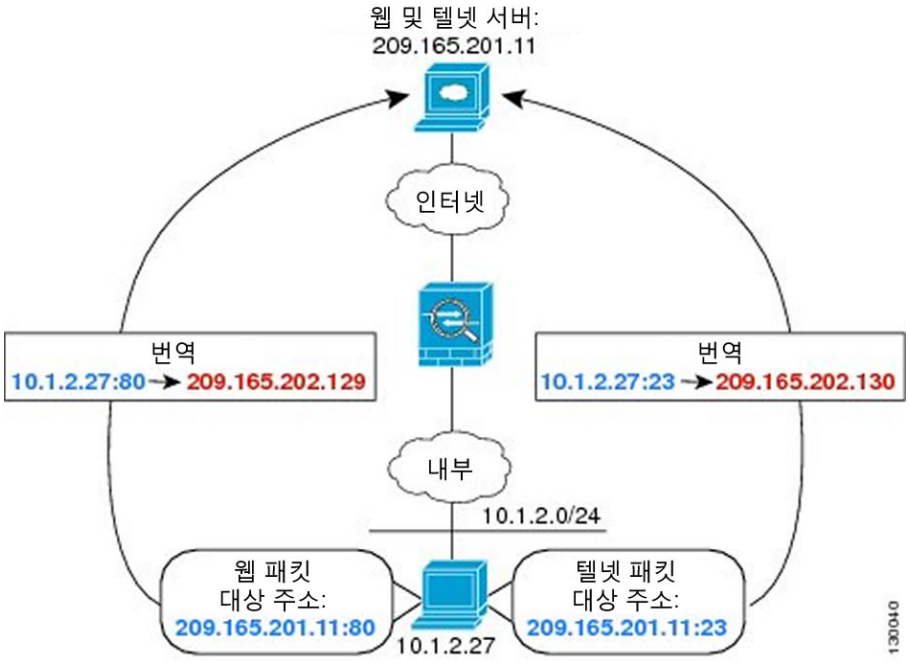
c) **OK**(확인)를 클릭합니다.

대상 주소 및 포트에 따라 다른 변환(동적 수동 **PAT**)

다음 그림은 소스 포트와 대상 포트의 사용법을 보여줍니다. 10.1.2.0/24 네트워크의 호스트가 웹 서비스와 텔넷 서비스를 모두 제공하는 단일 호스트에 액세스합니다. 호스트가 텔넷 서비스용 서버에 액세스하면 실제 주소가 209.165.202.129:*port*로 변환됩니다. 호스트가 동일한 웹 서비스용 서버에 액세스하면 실제 주소가 209.165.202.130:*port*로 변환됩니다.

참고 이 예에서는 내부 인터페이스가 스위치에 연결된 표준 라우팅 인터페이스이며 서버가 스위치에 연결되어 있다고 가정합니다. 내부 인터페이스가 BVI(브리지 그룹 인터페이스)이며 서버가 브리지 그룹 구성원 인터페이스에 연결되어 있으면 서버가 연결된 특정 구성원 인터페이스를 선택합니다. 예를 들어 규칙이 소스 인터페이스에 대해 inside가 아닌 inside1_2를 포함할 수 있습니다.

그림 ***18:*** 서로 다른 대상 포트를 사용하는 수동 ***NAT***



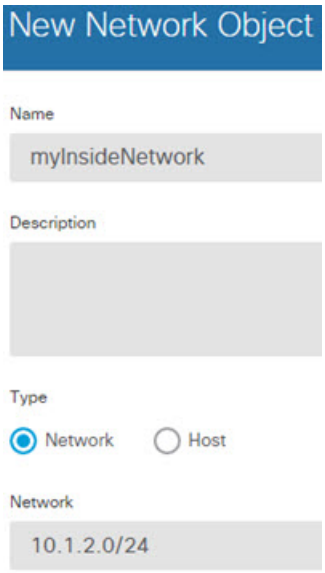
절차

단계 **1** 내부 네트워크용 네트워크 개체를 만듭니다.

a) **Objects(**개체**)**를 선택합니다.

b) 목차에서 **Network(**네트워크**)**를 선택하고 +를 클릭합니다.

c) 네트워크 개체의 이름을 myInsideNetwork와 같이 지정하고 **Network(**네트워크**)**를 선택한 후에 실제 네트워크 주소 10.1.2.0/24를 입력합니다.

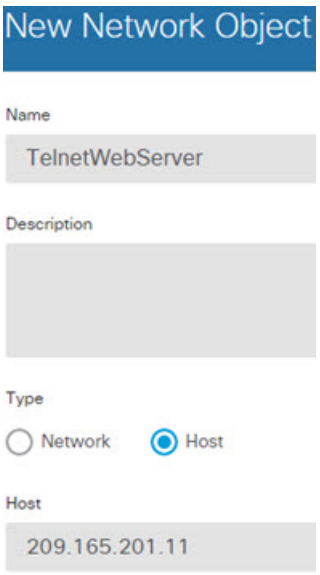


d) **OK(**확인**)**를 클릭합니다.

단계 **2** 텔넷/웹 서버용 네트워크 개체를 생성합니다.

a) +를 클릭합니다.

b) 네트워크 개체의 이름을 TelnetWebServer와 같이 지정하고 **Host(**호스트**)**를 선택한 후에 호스트 주소 209.165.201.11을 입력합니다.

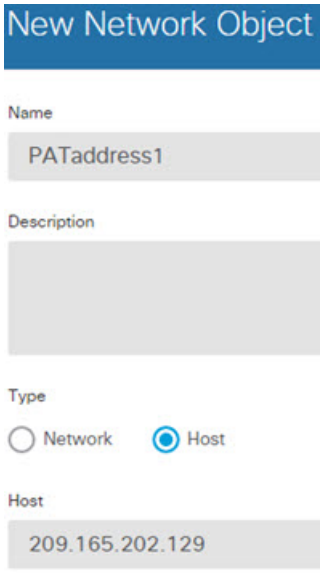


c) **OK(**확인**)**를 클릭합니다.

단계 **3** 텔넷 사용 시의 PAT 주소용 네트워크 개체를 생성합니다.

a) +를 클릭합니다.

b) 네트워크 개체의 이름을 PATaddress1과 같이 지정하고 **Host(**호스트**)**를 선택한 후에 호스트 주소 209.165.202.129를 입력합니다.

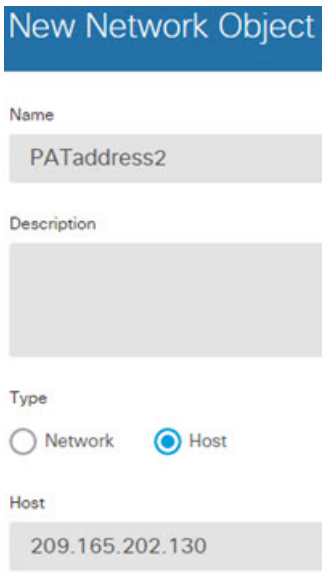


c) **OK(**확인**)**를 클릭합니다.

단계 **4** HTTP 사용 시의 PAT 주소용 네트워크 개체를 생성합니다.

a) +를 클릭합니다.

b) 네트워크 개체의 이름을 PATaddress2와 같이 지정하고 **Host(**호스트**)**를 선택한 후에 호스트 주소 209.165.202.130을 입력합니다.



c) **OK(**확인**)**를 클릭합니다.

단계 **5** 텔넷 액세스용 동적 수동 PAT를 구성합니다.

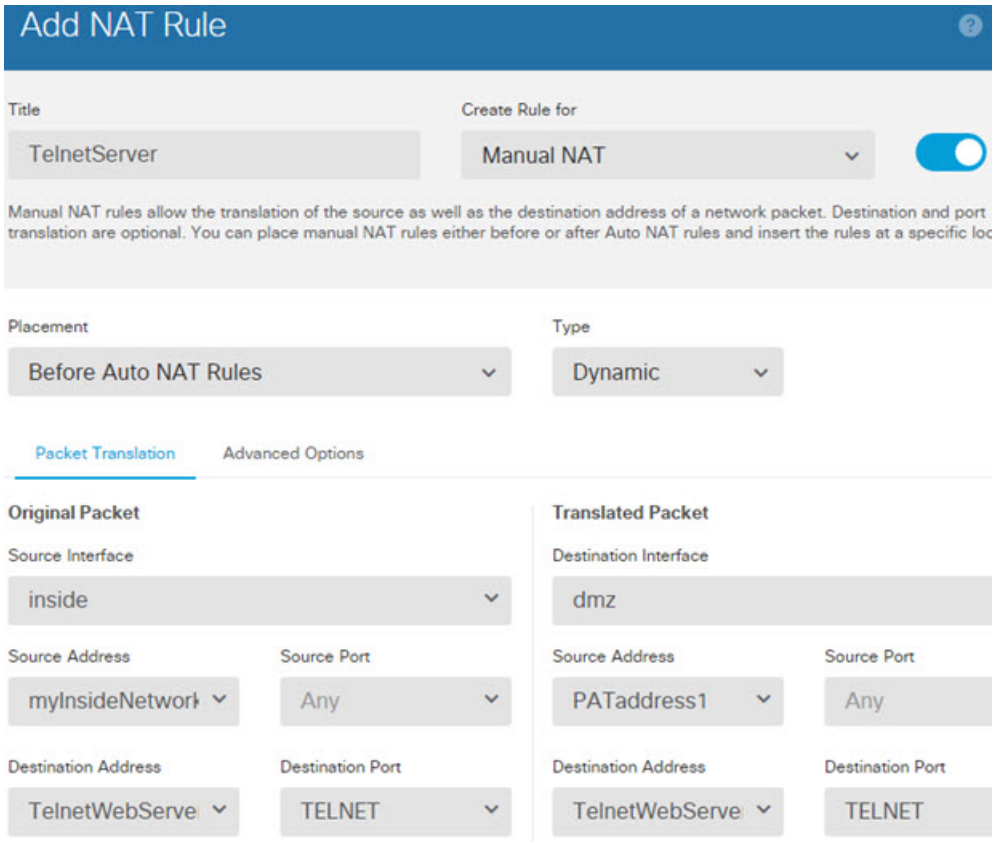
a) **Policies(**정책**)** > **NAT**를 선택합니다.

b) + 버튼을 클릭합니다.

c) 다음 속성을 구성합니다.

- 제목 = TelnetServer 또는 원하는 다른 이름
- 규칙 생성 = 수동 NAT
- 유형 = 동적
- 소스 인터페이스 = inside
- 대상 인터페이스 = dmz
- 원본 소스 주소 = myInsideNetwork 네트워크 개체
- 변환된 소스 주소 = PATaddress1 네트워크 개체
- 원본 대상 주소 = TelnetWebServer 네트워크 개체
- 변환된 대상 주소 = TelnetWebServer 네트워크 개체
- 원본 대상 포트 = TELNET 포트 개체
- 변환된 대상 포트 = TELNET 포트 개체

참고 대상 주소 또는 포트를 변환하지 않을 것이기 때문에 원본 및 변환된 대상 주소에 대해 동일한 주소를 지정하고 원본 및 변환된 포트에 대해 동일한 포트를 지정하여, 대상 주소 또는 포트에 대한 ID NAT를 구성해야 합니다.



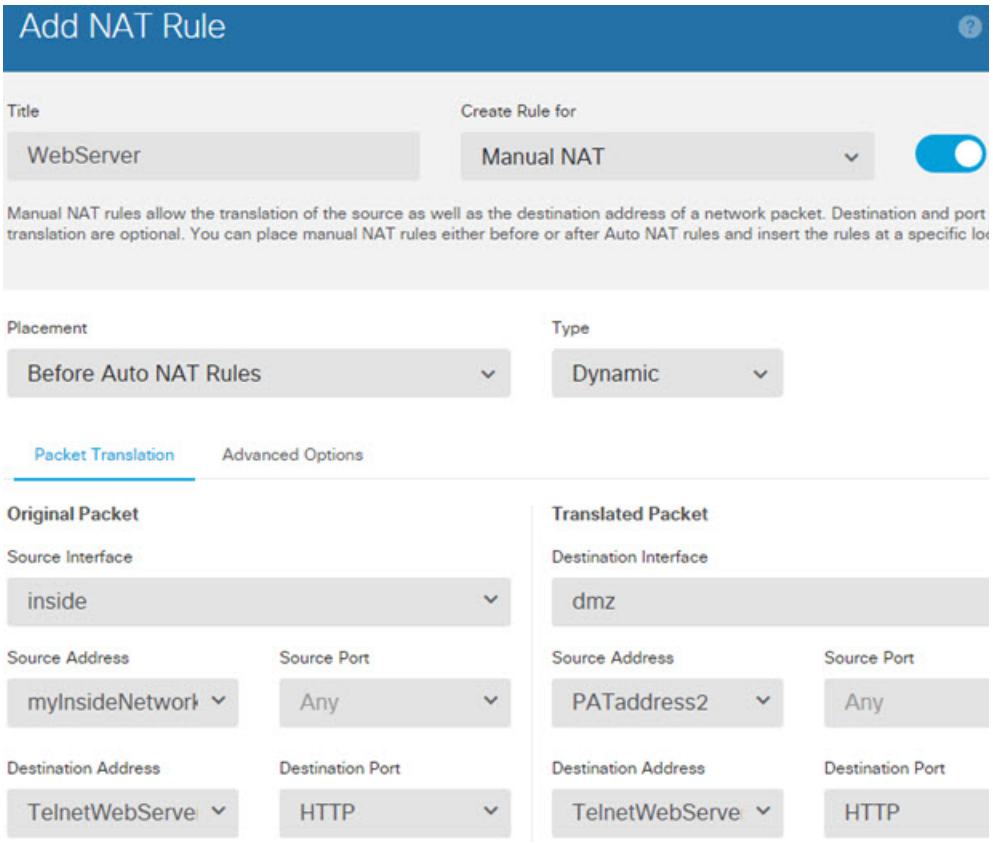
d) **OK(**확인**)**를 클릭합니다.

단계 **6** 웹 액세스용 동적 수동 PAT를 구성합니다.

a) + 버튼을 클릭합니다.

b) 다음 속성을 구성합니다.

- 제목 = WebServer 또는 원하는 다른 이름
- 규칙 생성 = 수동 NAT
- 유형 = 동적
- 소스 인터페이스 = inside
- 대상 인터페이스 = dmz
- 원본 소스 주소 = myInsideNetwork 네트워크 개체
- 변환된 소스 주소 = PATaddress2 네트워크 개체
- 원본 대상 주소 = TelnetWebServer 네트워크 개체
- 변환된 대상 주소 = TelnetWebServer 네트워크 개체
- 원본 대상 포트 = HTTP 포트 개체
- 변환된 대상 포트 = HTTP 포트 개체



c) **OK**(확인)를 클릭합니다.

NAT를 사용하여 DNS 쿼리 및 응답 재작성

회신의 주소를 NAT 컨피그레이션과 일치하는 주소로 교체하여 DNS 회신을 수정하도록 Firepower Threat Defense 디바이스를 구성해야 할 수 있습니다. 각 변환 규칙을 구성할 때 DNS 수정을 구성할 수 있습니다.

이 기능은 NAT 규칙과 일치하는 DNS 쿼리 및 회신의 주소를 재작성합니다(예: IPv4의 A 레코드, IPv6의 AAAA 레코드 또는 역방향 DNS 쿼리의 PTR 레코드). 매핑된 인터페이스에서 다른 임의의 인터페이스로 이동하는 DNS 회신의 경우 매핑된 값에서 실제 값으로 레코드가 재작성됩니다. 반대로, 임의의 인터페이스에서 매핑된 인터페이스로 이동하는 DNS 회신의 경우 실제 값에서 매핑된 값으로 레코드가 재작성됩니다.

다음은 NAT 규칙에 DNS 재작성을 구성해야 하는 몇 가지 주요 상황입니다.

- 규칙이 NAT64 또는 NAT46이며 DNS 서버가 외부 네트워크에 있는 경우. DNS A 레코드(IPv4의 경우)를 AAAA 레코드(IPv6의 경우)로 변환하려면 DNS 재작성이 필요합니다.
- DNS 서버가 외부에 있고 클라이언트는 내부에 있으며 클라이언트가 사용하는 일부 FQDN(Fully Qualified Domain Name)이 다른 내부 호스트로 확인되는 경우.

- DNS 서버가 내부에 있고 프라이빗 IP 어드레스로 응답하며, 클라이언트는 외부에 있고 내부에서 호스팅되는 서버를 가리키는 FQDN(Fully Qualified Domain Name)에 액세스하는 경우.

DNS 재작성 제한

다음은 DNS 재작성의 몇 가지 제한 사항입니다.

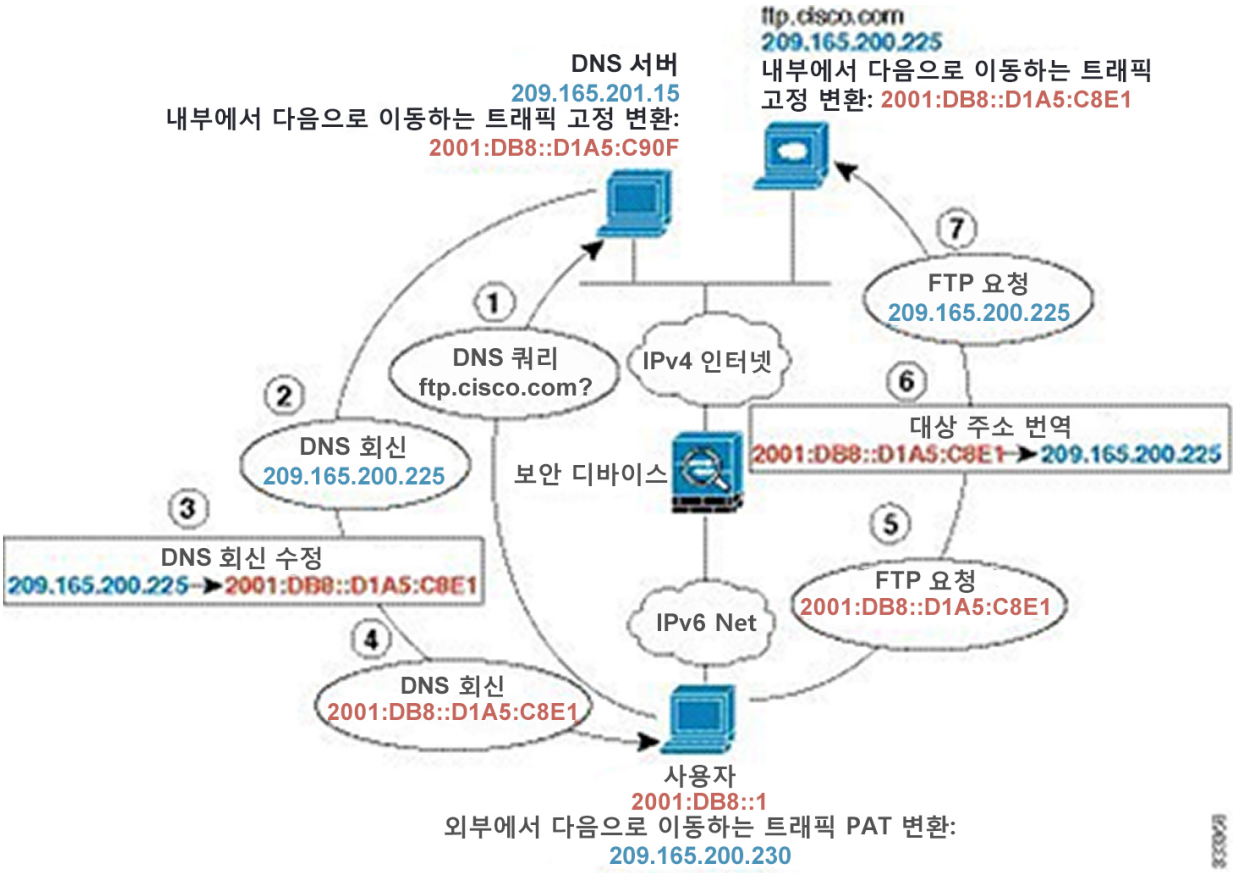
- 각 A 또는 AAAA 레코드에 여러 PAT 규칙을 적용할 수 있으며 사용할 PAT 규칙이 모호하므로 PAT에는 DNS 재작성이 적용되지 않습니다.
- 수동 NAT 규칙을 구성할 때 소스 주소와 대상 주소를 모두 지정하는 경우에는 DNS 수정을 구성할 수 없습니다. A와 B를 비교하여 전송하는 경우 이러한 종류의 규칙에는 잠재적으로 단일 주소에 다른 변환이 있을 수 있습니다. 따라서 Firepower Threat Defense 디바이스는 DNS 회신 내부의 IP 주소를 정확한 2회 NAT 규칙에 대해 올바르게 확인할 수 없습니다. DNS 회신에는 DNS 요청을 표시한 패킷에 어떤 source/destination 주소 조합이 있었는지에 대한 정보가 포함되어 있지 않습니다.
- DNS 재작성은 실제로 NAT 규칙이 아니라 xlate 항목에서 수행됩니다. 따라서 동적 규칙에 대한 xlate가 없으면 재작성을 정확히 수행할 수 없습니다. 고정 NAT에 대해서는 동일한 문제가 발생하지 않습니다.
- DNS 재작성에서는 DNS 동적 업데이트 메시지(opcode 5)를 재작성하지 않습니다.

다음 항목에서는 NAT 규칙의 DNS 재작성 예를 제공합니다.

DNS 64 회신 수정

다음 그림은 외부 IPv4 네트워크의 FTP 서버 및 DNS 서버를 보여줍니다. 시스템은 외부 서버에 대해 고정 변환을 수행합니다. 이 경우 내부 IPv6 사용자가 DNS 서버에서 ftp.cisco.com에 대한 주소를 요청하면 DNS 서버는 실제 주소인 209.165.200.225로 응답합니다.

내부 사용자가 ftp.cisco.com(2001:DB8::D1A5:C8E1, 여기서 D1A5:C8E1은 209.165.200.225에 해당하는 IPv6 주소)에 대한 매핑된 주소를 사용하도록 하려면 고정 변환에 대해 DNS 회신 수정을 구성해야 합니다. 이 예에는 DNS 서버용 고정 NAT 변환 및 내부 IPv6 호스트용 PAT 규칙도 포함되어 있습니다.



참고 이 예에서는 내부 인터페이스가 BVI(브리지 그룹 인터페이스)가 아닌 표준 라우팅 인터페이스라고 가정합니다. 내부 인터페이스가 BVI인 경우에는 각 구성원 인터페이스에 대한 규칙을 중복 생성해야 합니다.

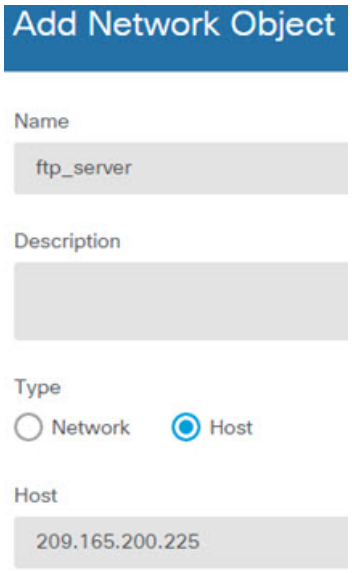
절차

단계 **1** FTP 서버, DNS 서버, 내부 네트워크 및 PAT 풀용 네트워크 개체를 생성합니다.

a) **Objects**(개체)를 선택합니다.

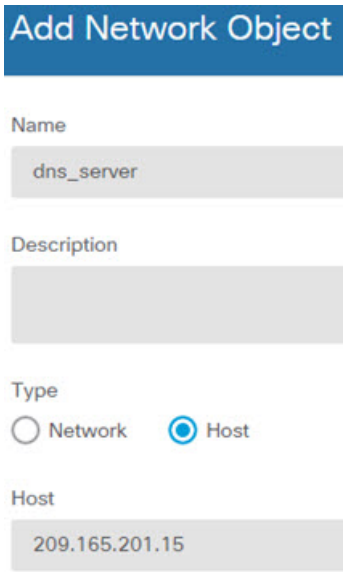
b) 목차에서 **Network**(네트워크)를 선택하고 +를 클릭합니다.

c) 실제 FTP 서버 주소를 정의합니다.
네트워크 개체의 이름을 ftp_server와 같이 지정하고 **Host**(호스트)를 선택한 후에 실제 호스트 IP 주소 209.165.200.225를 입력합니다.



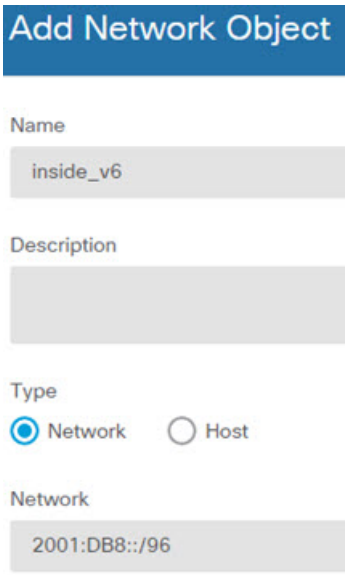
d) **OK(**확인**)**를 클릭합니다.

e) +를 클릭하여 DNS 서버의 실제 주소를 정의합니다.
네트워크 개체의 이름을 dns_server와 같이 지정하고 **Host(**호스트**)**를 선택한 후에 호스트 주소 209.165.201.15를 입력합니다.



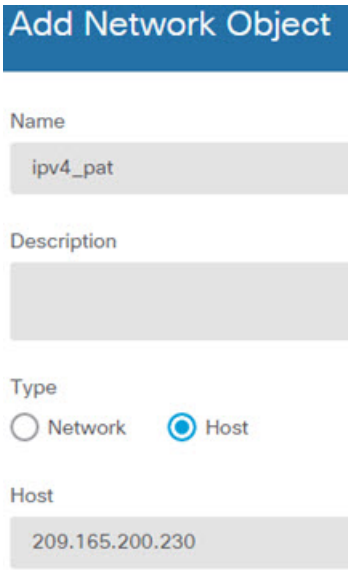
f) **OK(**확인**)**를 클릭합니다.

g) +를 클릭하여 내부 IPv6 네트워크를 정의합니다.
네트워크 개체의 이름을 inside_v6과 같이 지정하고 **Network(**네트워크**)**를 선택한 후에 네트워크 주소 2001:DB8::/96을 입력합니다.



h) **OK(**확인**)**를 클릭합니다.

i) +를 클릭하여 내부 IPv6 네트워크용 IPv4 PAT 주소를 정의합니다.
네트워크 개체의 이름을 ipv4_pat와 같이 지정하고 **Host(**호스트**)**를 선택한 후에 호스트 주소 209.165.200.230을 입력합니다.



j) **OK(**확인**)**를 클릭합니다.

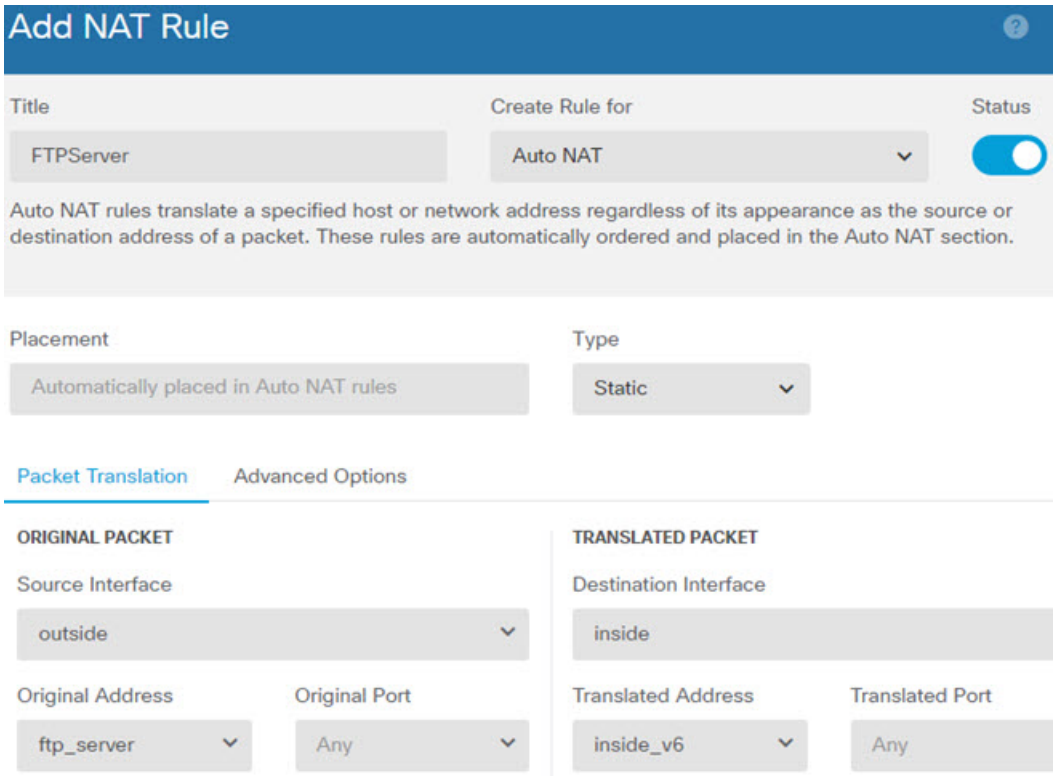
단계 **2** FTP 서버에 대해 DNS를 수정하여 고정 NAT 규칙을 구성합니다.

a) **Policies(**정책**)** > **NAT**를 선택합니다.

b) + 버튼을 클릭합니다.

c) 다음 속성을 구성합니다.

- 제목 = FTPServer 또는 원하는 다른 이름
- 규칙 생성 = 자동 NAT
- 유형 = 고정
- 원본 인터페이스 = outside
- 대상 인터페이스 = inside
- 원본 주소 = ftp_server 네트워크 개체
- 변환된 주소 = inside_v6 네트워크 개체 IPv4 주소를 IPv6 주소로 변환할 때는 IPv4 임베디드 주소 방법이 사용되므로 209.165.200.225는 동일한 IPv6 주소인 D1A5:C8E1로 변환되며, 네트워크 접두사가 추가되어 전체 주소는 2001:DB8::D1A5:C8E1이 됩니다.
- **Advanced Options(**고급 옵션**)** 탭에서 이 규칙과 일치하는 **DNS** 응답 변환을 선택합니다.



d) **OK(**확인**)**를 클릭합니다.

단계 **3** DNS 서버용 고정 NAT 규칙을 구성합니다.

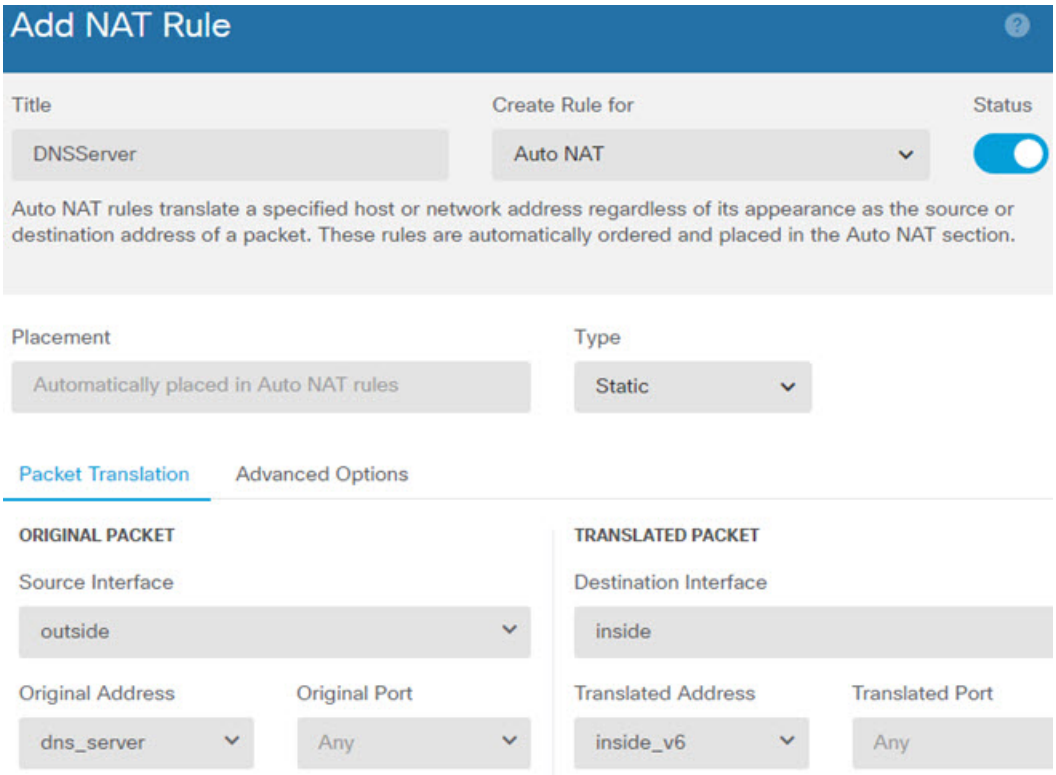
a) **Policies(**정책**)** > **NAT**를 선택합니다.

b) + 버튼을 클릭합니다.

c) 다음 속성을 구성합니다.

- 제목 = DNSServer 또는 원하는 다른 이름

- 규칙 생성 = 자동 NAT
- 유형 = 고정
- 원본 인터페이스 = outside
- 대상 인터페이스 = inside
- 원본 주소 = dns_server 네트워크 개체
- 변환된 주소 = inside_v6 네트워크 개체 IPv4 주소를 IPv6 주소로 변환할 때는 IPv4 임베디드 주소 방법이 사용되므로 209.165.201.15는 동일한 IPv6 주소인 D1A5:C90F로 변환되며, 네트워크 접두사가 추가되어 전체 주소는 2001:DB8::D1A5:C90F가 됩니다.



d) **OK(**확인**)**를 클릭합니다.

단계 **4** 내부 IPv6 네트워크용 동적 PAT 규칙을 구성합니다.

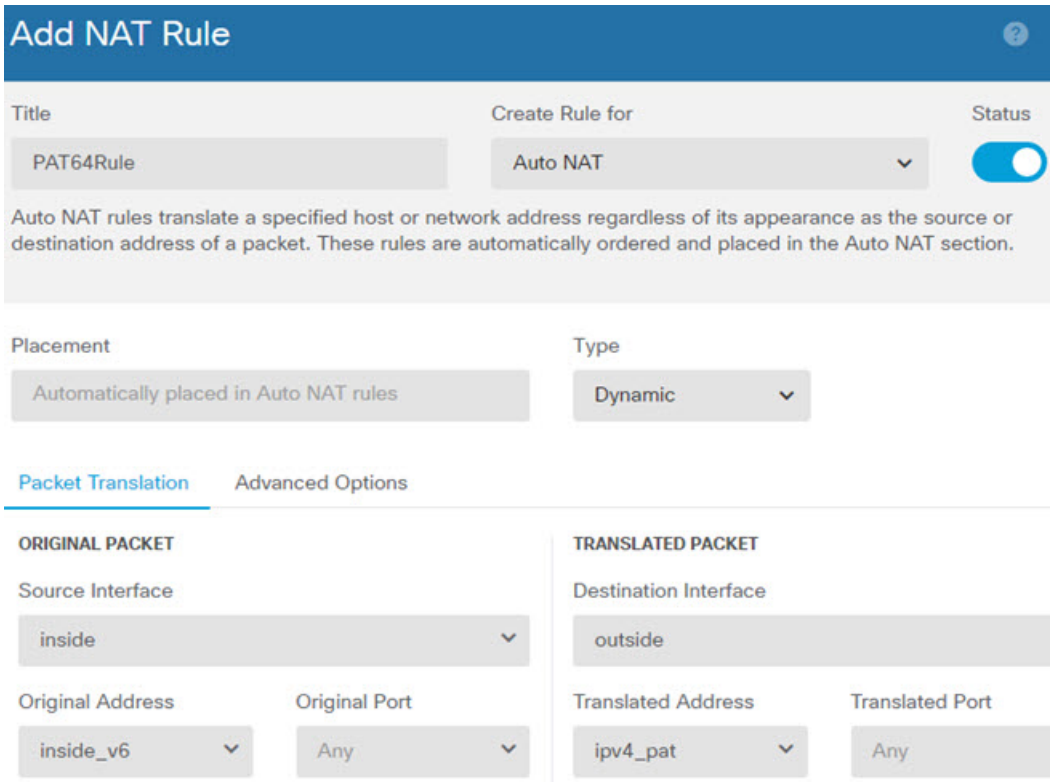
a) **Policies(**정책**)** > **NAT**를 선택합니다.

b) + 버튼을 클릭합니다.

c) 다음 속성을 구성합니다.

- 제목 = PAT64Rule 또는 원하는 다른 이름
- 규칙 생성 = 자동 NAT
- 유형 = 동적

- 원본 인터페이스 = inside
- 대상 인터페이스 = outside
- 원본 주소 = inside_v6 네트워크 개체
- 변환된 주소 = ipv4_pat 네트워크 개체



d) **OK**(확인)를 클릭합니다.

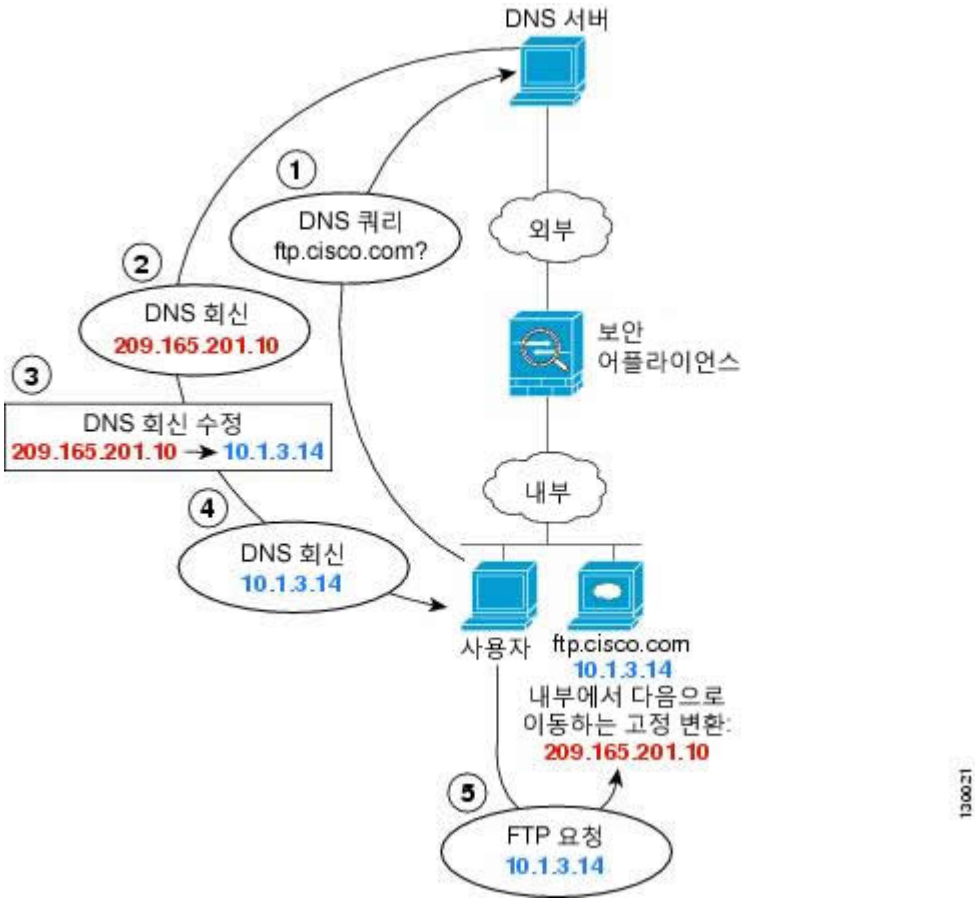
DNS 회신 수정, 외부의 **DNS** 서버

다음 그림은 인터페이스 외부에서 액세스할 수 있는 DNS 서버를 보여줍니다. ftp.cisco.com 서버는 내부 인터페이스에 있습니다. ftp.cisco.com 실제 주소(10.1.3.14)를 외부 네트워크에서 보이는 매핑된 주소(209.165.201.10)로 고정 변환하도록 NAT를 구성하십시오.

이 경우, 실제 주소를 사용하여 ftp.cisco.com에 액세스할 수 있는 내부 사용자가 DNS 서버에서 실제 주소(매핑된 주소가 아님)를 받을 수 있도록 고정 규칙에 대한 DNS 회신 수정을 활성화할 수 있습니다.

내부 호스트가 ftp.cisco.com 주소에 DNS 요청을 전송하면, DNS 서버는 매핑된 주소(209.165.201.10)로 회신합니다. 시스템은 내부 서버에 대한 고정 규칙을 참조하여 DNS 회신에 있는 주소를 10.1.3.14

로 변환합니다. DNS 회신 수정을 활성화하지 않으면 내부 호스트는 ftp.cisco.com에 직접 액세스하는 대신 트래픽을 209.165.201.10으로 전송하려고 시도하게 됩니다.



참고 이 예에서는 내부 인터페이스가 BVI(브리지 그룹 인터페이스)가 아닌 표준 라우팅 인터페이스라고 가정합니다. 내부 인터페이스가 BVI인 경우에는 각 구성원 인터페이스에 대한 규칙을 중복 생성해야 합니다.

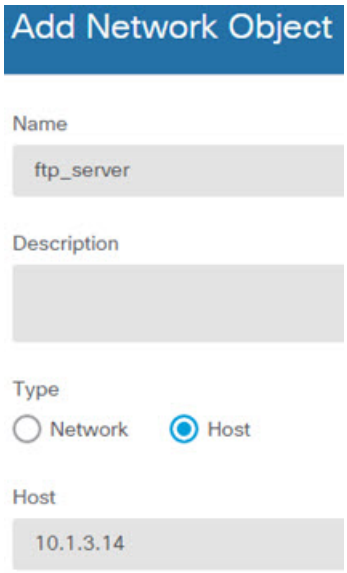
절차

단계 **1** FTP 서버용 네트워크 개체를 생성합니다.

a) **Objects(**개체**)**를 선택합니다.

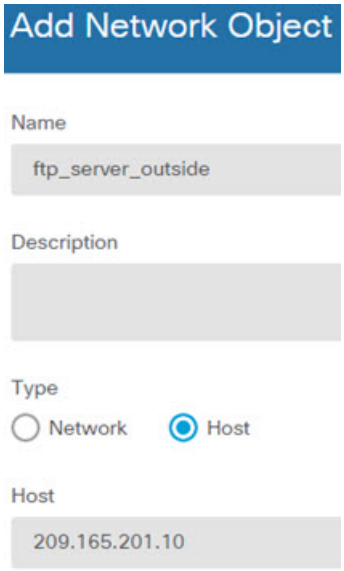
b) 목차에서 **Network(**네트워크**)**를 선택하고 +를 클릭합니다.

c) 실제 FTP 서버 주소를 정의합니다.
네트워크 개체의 이름을 ftp_server와 같이 지정하고 **Host(**호스트**)**를 선택한 후에 실제 호스트 IP 주소 10.1.3.14를 입력합니다.



d) **OK(**확인**)**를 클릭합니다.

e) +를 클릭하여 FTP 서버의 변환된 주소를 정의합니다.
네트워크 개체의 이름을 ftp_server_outside와 같이 지정하고 **Host(**호스트**)**를 선택한 후에 호스트 주소 209.165.201.10을 입력합니다.



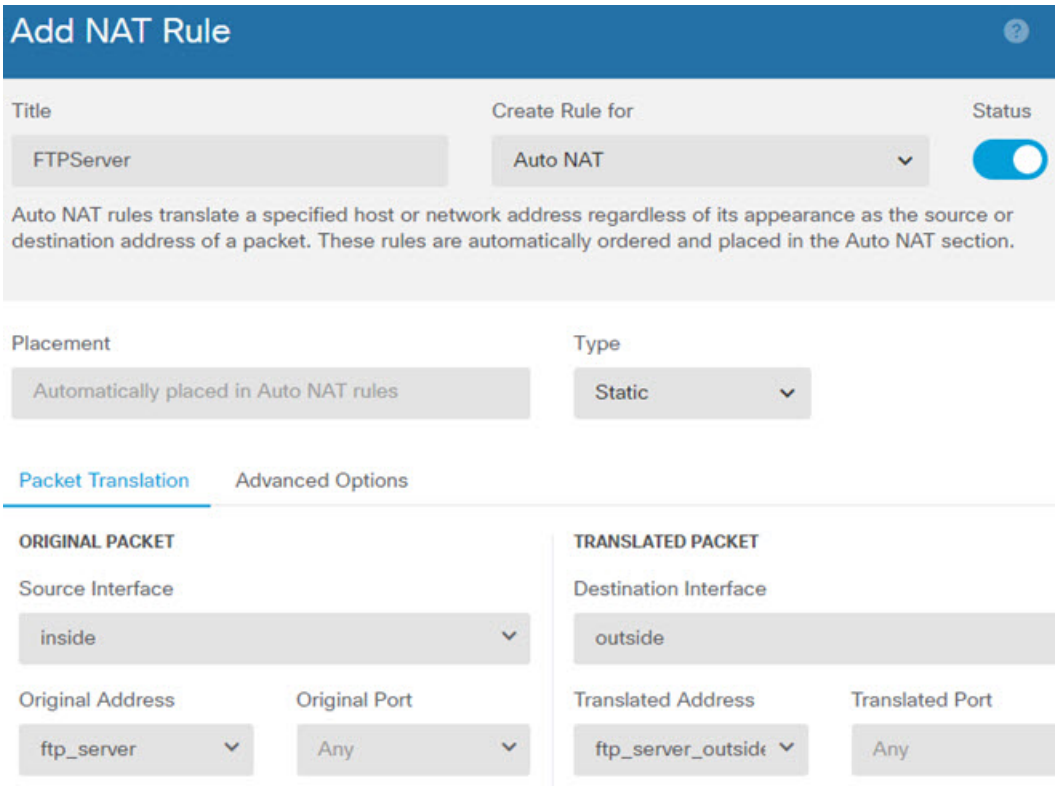
단계 **2** FTP 서버에 대해 DNS를 수정하여 고정 NAT 규칙을 구성합니다.

a) **Policies(**정책**)** > **NAT**를 선택합니다.

b) + 버튼을 클릭합니다.

c) 다음 속성을 구성합니다.

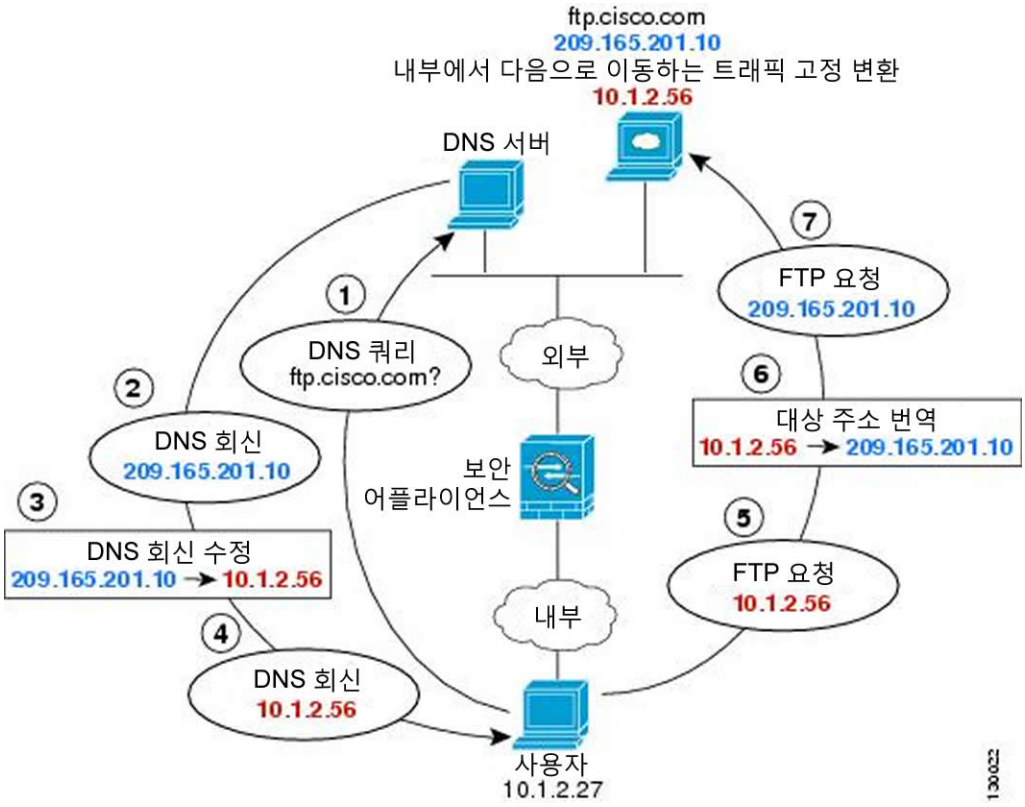
- 제목 = FTPServer 또는 원하는 다른 이름
- 규칙 생성 = 자동 NAT
- 유형 = 고정
- 소스 인터페이스 = inside
- 대상 인터페이스 = outside
- 원본 주소 = ftp_server 네트워크 개체
- 변환된 주소 = ftp_server_outside 네트워크 개체
- **Advanced Options(**고급 옵션**)** 탭에서 이 규칙과 일치하는 **DNS** 응답 변환을 선택합니다.



d) **OK(**확인**)**를 클릭합니다.

DNS 회신 수정**,** 호스트 네트워크의 **DNS** 서버

다음 그림은 외부의 FTP 서버 및 DNS 서버를 보여줍니다. 시스템은 외부 서버에 대해 고정 변환을 수행합니다. 이 경우 내부 사용자가 DNS 서버에서 ftp.cisco.com에 대한 주소를 요청하면 DNS 서버는 실제 주소인 209.165.20.10으로 응답합니다. 내부 사용자가 ftp.cisco.com(10.1.2.56)에 대한 매핑된 주소를 사용하도록 하려면 고정 변환에 대해 DNS 회신 수정을 구성해야 합니다.



참고 이 예에서는 내부 인터페이스가 BVI(브리지 그룹 인터페이스)가 아닌 표준 라우팅 인터페이스라고 가정합니다. 내부 인터페이스가 BVI인 경우에는 각 구성원 인터페이스에 대한 규칙을 중복 생성해야 합니다.

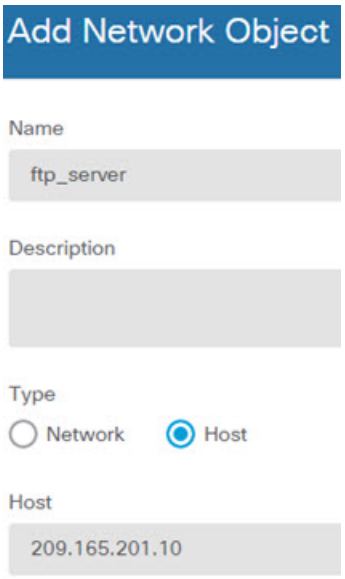
절차

단계 **1** FTP 서버용 네트워크 개체를 생성합니다.

a) **Objects(**개체**)**를 선택합니다.

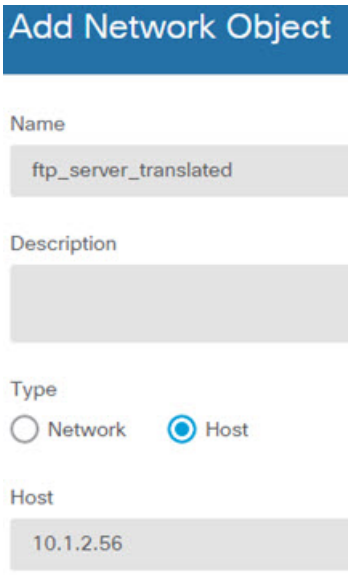
b) 목차에서 **Network(**네트워크**)**를 선택하고 +를 클릭합니다.

c) 실제 FTP 서버 주소를 정의합니다.
네트워크 개체의 이름을 ftp_server와 같이 지정하고 **Host(**호스트**)**를 선택한 후에 실제 호스트 IP 주소 209.165.201.10을 입력합니다.



d) **OK(**확인**)**를 클릭합니다.

e) +를 클릭하여 FTP 서버의 변환된 주소를 정의합니다.
네트워크 개체의 이름을 ftp_server_translated와 같이 지정하고 **Host(**호스트**)**를 선택한 후에 호스트 주소 10.1.2.56을 입력합니다.



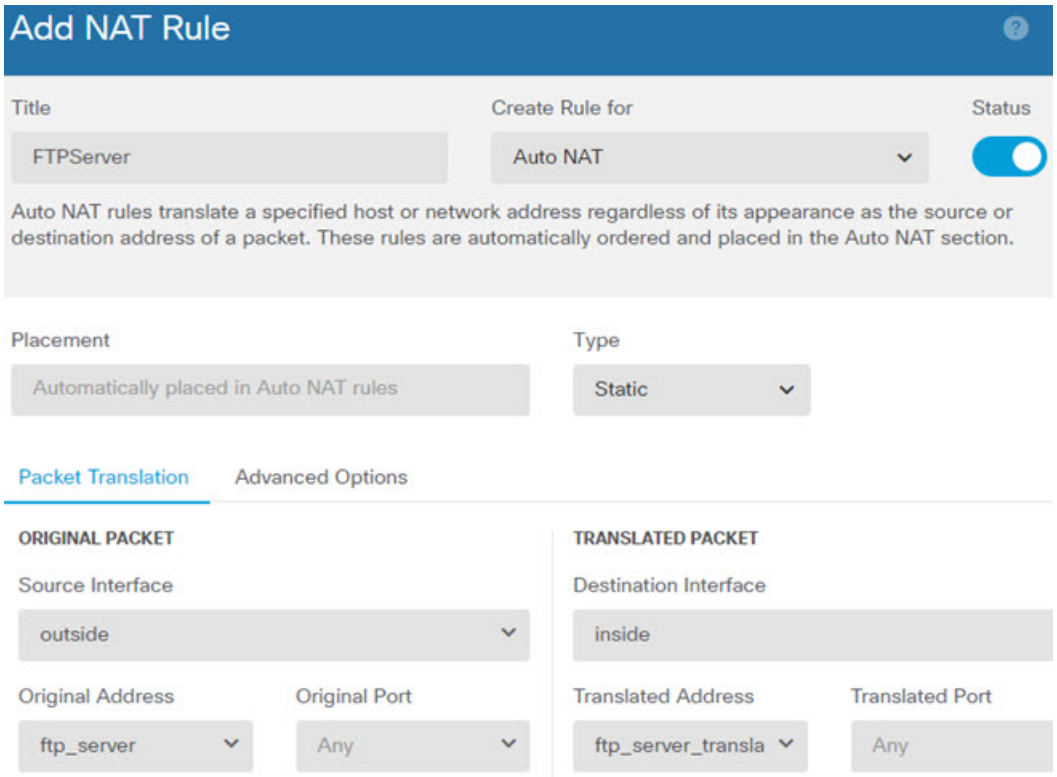
단계 **2** FTP 서버에 대해 DNS를 수정하여 고정 NAT 규칙을 구성합니다.

a) **Policies(**정책**)** > **NAT**를 선택합니다.

b) + 버튼을 클릭합니다.

c) 다음 속성을 구성합니다.

- 제목 = FTPServer 또는 원하는 다른 이름
- 규칙 생성 = 자동 NAT
- 유형 = 고정
- 원본 인터페이스 = outside
- 대상 인터페이스 = inside
- 원 주소 = ftp_server 네트워크 개체
- 변환된 주소 = ftp_server_translated 네트워크 개체
- 고급 옵션 탭에서 이 규칙과 일치하는 **DNS** 응답 변환을 선택합니다.



d) **OK(**확인**)**를 클릭합니다.

III 부

VPN(가상 사설망)

11 장

사이트 대 사이트 VPN

VPN(Virtual Private Network)은 인터넷과 같은 공개 소스나 기타 네트워크를 통해 원격 피어 간에 보안 터널을 설정하는 네트워크 연결입니다. VPN은 터널을 사용하여 IP 기반 네트워크로를 통해 전달할 수 있도록 일반 IP 패킷 내의 데이터 패킷을 캡슐화합니다. VPN은 암호화를 사용해 개인 정보와 인증을 확인함으로써 데이터의 무결성을 보장합니다.

VPN 기본 사항

터널링을 통해 인터넷과 같은 공용 TCP/IP 네트워크를 사용하고 원격 사용자와 사설 기업 네트워크 간의 안전한 연결을 생성할 수 있습니다. 각 보안 연결을 터널이라고 부릅니다.

IPsec 기반 VPN 기술은 ISAKMP/IKE(Internet Security Association and Key Management Protocol) 및 IPsec 터널링 표준을 사용하여 터널을 작성하고 관리합니다. ISAKMP 및 IPsec는 다음 사항을 수행합니다.

- 터널 파라미터 협상
- 터널 설정
- 사용자 및 데이터 인증
- 보안 키 관리
- 데이터 암호화 및 암호 해독
- 터널을 통한 데이터 전송 관리
- 터널 엔드포인트 또는 라우터로 데이터 전송 인바운드 및 아웃바운드 관리

VPN의 디바이스는 양방향 터널 엔드포인트로 작동합니다. 사설 네트워크에서 일반 패킷을 수신하여 캡슐화하고 터널을 생성하며, 캡슐 해제하여 최종 대상에 전송하는 다른 쪽 터널의 끝으로 보낼

수 있습니다. 또한 공용 네트워크에서 캡슐화된 패킷을 수신하여 캡슐을 해제하여 사설 네트워크의 최종 대상에 보낼 수 있습니다.

사이트 대 사이트 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 게이트웨이가 상호 인증에 사용하는 방법으로 구성됩니다.

Firepower Threat Defense에서 시스템은 VPN 트래픽이 액세스 제어 정책을 통과할 때까지는 해당 트래픽을 전송하지 않습니다. 수신 터널 패킷은 Snort 프로세스로 전송되기 전에 암호 해독됩니다. 발신 패킷은 암호화 전에 Snort에 의해 처리됩니다. VPN 터널의 각 엔드포인트 노드에 대해 보호된 네트워크를 식별하여 Firepower Threat Defense 디바이스를 통과해 내부 호스트로 이동할 수 있는 트래픽을 결정합니다. 또한 터널이 다운된 상태에서는 공개 소스에 터널 트래픽을 보내지 않습니다.

IKE(Internet Key Exchange)

IKE(Internet Key Exchange)는 IPsec 피어를 인증하고, IPsec 암호화 키를 협상 및 배포하고, IPsec SA(Security Association, 보안 연계)를 자동으로 설정하는 데 사용되는 키 관리 프로토콜입니다.

IKE 협상은 2단계로 구성됩니다. 1단계에서는 두 IKE 피어 간의 보안 연계를 협상합니다. 그러면 피어가 2단계에서 안전하게 통신할 수 있습니다. 2단계 협상 중에는 IKE가 IPsec 등의 기타 애플리케이션에 대해 SA를 설정합니다. 두 단계에서는 모두 연결을 협상할 때 제안을 사용합니다.

IKE 정책은 두 피어가 상호 간의 KIE 협상을 보호하는 데 사용하는 알고리즘 집합입니다. IKE 협상에서는 두 피어가 먼저 공통(공유) IKE 정책을 합의합니다. 이 정책은 후속 IKE 협상을 보호하는 보안 파라미터를 제시합니다. IKEv1(IKE 버전 1)의 경우 IKE 정책에는 단일 알고리즘 집합과 모듈러스 그룹이 포함됩니다. IKEv1과 달리 IKEv2 정책에서는 피어가 1단계 협상 중에 선택할 수 있는 여러 알고리즘 및 모듈러스 그룹을 선택할 수 있습니다. 단일 IKE 정책을 생성할 수도 있지만, 여러 정책을 생성해 가장 적절한 옵션에 더 높은 우선 순위를 지정할 수도 있습니다. 사이트 대 사이트 VPN의 경우에는 단일 IKE 정책을 생성할 수 있습니다.

IKE 정책을 정의하려면 다음 사항을 지정합니다.

- 고유한 우선 순위(1~65,543, 1이 우선 순위가 가장 높음)
- 데이터 및 개인정보를 보호하기 위한 IKE 협상의 암호화 방법
- 보낸 사람의 ID를 확인하고 메시지가 전송 중에 수정되지 않았는지 확인할 HMAC(Hashed Message Authentication Codes, 해시 메시지 인증 코드) 방법(IKEv2에서는 무결성 알고리즘이라고 함)
- IKEv2의 경우 IKEv2 터널 암호화에 필요한 키 요소 및 해싱 작업을 파생시키기 위한 알고리즘으로 사용되는 별도의 PRF(Pseudo Random Function, 의사 난수 함수). 옵션은 해시 알고리즘에 사용되는 것과 동일합니다.
- encryption-key-determination 알고리즘의 수준을 결정하는 Diffie-Hellman 그룹. 디바이스는 이 알고리즘을 사용하여 암호화 및 해시 키를 파생합니다.
- 피어의 ID를 확인할 인증 방법

참고 인증에는 사전 공유 키만 사용됩니다.

• 디바이스가 교체 전 암호화 키를 사용하는 시간제한

IKE 협상이 시작되면 협상을 시작한 피어가 활성화된 모든 정책을 원격 피어로 보내고 원격 피어는 우선 순위대로 자신의 정책과 일치하는 정책을 검색합니다. 암호화, 해시(IKEv2의 경우 무결성 및 PRF), 인증 및 Diffie-Hellman 값이 동일하고 SA 수명이 전송된 정책의 수명보다 작거나 같으면 IKE 정책은 서로 일치하는 것으로 간주됩니다. 수명이 동일하지 않은 경우에는 원격 피어에서 가져온 더 짧은 수명이 적용됩니다. 기본적으로는 DES를 사용하는 단순 IKE 정책만 활성화됩니다. 우선 순위가 더 높은 다른 IKE 정책을 활성화하여 더욱 강력한 암호화 표준을 협상할 수도 있지만, DES 정책으로도 협상은 정상적으로 진행됩니다.

VPN 연결의 보안 수준 결정

VPN 터널은 일반적으로 공용 네트워크(대개 인터넷)를 통과하므로 연결을 암호화하여 트래픽을 보호해야 합니다. IKE 정책 및 IPsec 제안을 사용하여 적용할 암호화 및 기타 보안 기술을 정의합니다.

디바이스 라이선스에서 강력한 암호화 적용이 허용되는 경우에는 광범위한 암호화 및 해시 알고리즘과 Diffie-Hellman 그룹 중에서 선택할 수 있습니다. 그러나 일반적으로는 터널에 적용하는 암호화가 강력할수록 시스템 성능은 더 나빠집니다. 따라서 효율성을 저하하지 않으면서 충분한 보호 기능을 제공하는 보안과 성능 간의 적절한 균형 지점을 찾아야 합니다.

Cisco는 선택할 수 있는 옵션에 대한 구체적인 지침을 제공하지는 않습니다. 대규모 기업이나 기타 조직 내에서 보안을 담당하는 경우 충족해야 하는 표준이 이미 정의되어 있을 수 있습니다. 그렇지 않은 경우, 선택할 수 있는 옵션에 대해 조사해야 합니다.

다음 주제에서는 사용 가능한 옵션에 대해 설명합니다.

사용할 암호화 알고리즘 결정

IKE 정책 또는 IPsec 제안에 사용할 암호화 알고리즘을 결정할 때는 VPN의 디바이스가 지원하는 알고리즘으로 선택이 제한됩니다.

IKEv2의 경우 여러 암호화 알고리즘을 구성할 수 있습니다. 시스템은 가장 안전한 항목부터 가장 안전하지 않은 항목 순으로 설정 순서를 지정하고 해당 순서를 사용하여 피어와 협상합니다. IKEv1의 경우 단일 옵션만 선택할 수 있습니다.

IPsec 제안의 경우 알고리즘은 인증, 암호화 및 재생 방지 서비스를 제공하는 ESP(Encapsulating Security Protocol)에서 사용됩니다. ESP는 IP 프로토콜 유형 50입니다. IKEv1 IPsec 제안에서 알고리즘 이름에는 ESP- 접두사가 붙습니다.

디바이스 라이선스에 따라 강력한 암호화를 사용할 수 있는 경우 다음 암호화 알고리즘 중에서 선택할 수 있습니다. 강력한 암호화를 사용할 수 없으면 DES만 선택할 수 있습니다.

- AES-GCM - (IKEv2에만 해당됨) 기밀 유지 및 데이터 원본 인증 기능을 제공하는 블록 암호화 작동 모드인 AES-GCM(Advanced Encryption Standard in Galois/Counter Mode)은 AES보다 보안성이 뛰어납니다. AES-GCM은 세 가지 키 강도(128비트, 192비트 및 256비트 키)를 제공합니다. 키 길이가 길수록 보안성은 더 높지만 성능은 낮습니다. GCM은 NSA Suite B를 지원하는 데 필요한 AES의 모드입니다. NSA Suite B는 암호화 강도에 대한 연방 기준을 충족시키기 위해 디바이스가 지원해야 하는 암호화 알고리즘 세트입니다. .

- AES-GMAC - (IKEv2 IPsec 제안에만 해당됨) AES-GMAC(Advanced Encryption Standard Galois Message Authentication Code)는 데이터 원본 인증 기능만 제공하는 블록 암호화 작동 모드입니다. 이 모드는 데이터를 암호화하지 않고 데이터 인증을 허용하는 AES-GCM의 변형입니다. AES-GMAC는 세 가지 키 강도(128비트, 192비트 및 256비트 키)를 제공합니다.
- AES - AES(Advanced Encryption Standard)는 DES보다 보안성이 뛰어나며 3DES보다 계산 효율성이 높은 대칭 암호화 알고리즘입니다. AES는 세 가지 키 강도(128비트, 192비트 및 256비트 키)를 제공합니다. 키 길이가 길수록 보안성은 더 높지만 성능은 낮습니다.
- 3DES - 56비트 키를 사용하여 암호화를 3회 수행하는 3DES(Triple DES)는 서로 다른 키를 사용하여 각 데이터 블록을 3회 처리하므로 DES보다 안전합니다. 그러나 시스템 리소스를 더 많이 사용하며 DES보다 속도가 느립니다.
- DES - 56비트 키를 사용하여 암호화를 수행하는 DES(Data Encryption Standard)는 대칭 보안 키 블록 알고리즘입니다. 3DES보다 속도가 빠르며 시스템 리소스를 더 적게 사용하지만 보안성은 더 낮습니다. 강력한 데이터 기밀 유지 기능이 필요하지 않으며 시스템 리소스나 속도가 중요한 경우에는 DES를 선택하십시오.
- null - null 암호화 알고리즘은 암호화를 수행하지 않는 인증 기능을 제공합니다. 이 알고리즘은 대개 테스트용으로만 사용됩니다.

사용할 해시 알고리즘 결정

IKE 정책에서 해시 알고리즘은 메시지 무결성을 보장하는 데 사용되는 메시지 다이제스트를 생성합니다. IKEv2에서 해시 알고리즘은 두 가지 옵션으로 구분됩니다. 그중 하나는 무결성 알고리즘 옵션이고 다른 하나는 PRF(Pseudo-Random Function: 의사 난수 함수) 옵션입니다.

IPsec 제안에서 해시 알고리즘은 인증을 위한 ESP(Encapsulating Security Protocol)에서 사용됩니다. IKEv2 IPsec 제안에서는 이러한 알고리즘을 무결성 해시라고 합니다. IKEv1 IPsec 제안에서는 알고리즘 이름에 ESP- 접두사가 붙으며 -HMAC(Hash Method Authentication Code) 접미사도 붙습니다.

IKEv2의 경우 여러 해시 알고리즘을 구성할 수 있습니다. 시스템은 가장 안전한 항목부터 가장 안전하지 않은 항목 순으로 설정 순서를 지정하고 해당 순서를 사용하여 피어와 협상합니다. IKEv1의 경우 단일 옵션만 선택할 수 있습니다.

다음 해시 알고리즘 중에서 선택할 수 있습니다.

- SHA(Secure Hash Algorithm) - 160비트 다이제스트를 생성합니다. SHA는 MD5보다 무차별 암호 대입 공격에 대한 방어력이 뛰어납니다. 그러나 MD5보다 리소스를 많이 사용합니다. 최고 보안 레벨이 필요한 구현의 경우 SHA 해시 알고리즘을 사용합니다.

  SHA1(Standard SHA)에서는 160비트 다이제스트를 생성합니다.

  IKEv2 컨피그레이션에는 다음과 같은 더욱 안전한 SHA-2 옵션을 사용할 수 있습니다. NSA Suite B 암호화 사양을 구현하려는 경우 이러한 옵션 중 하나를 선택합니다.

  - SHA256 - 256비트 다이제스트를 생성하는 Secure Hash Algorithm SHA 2를 지정합니다.
  - SHA384 - 384비트 다이제스트를 생성하는 Secure Hash Algorithm SHA 2를 지정합니다.
  - SHA512 - 512비트 다이제스트를 생성하는 Secure Hash Algorithm SHA 2를 지정합니다.

- MD5(Message Digest 5) - 128비트 다이제스트를 생성합니다. MD5는 SHA보다 전반적으로 성능이 우수하여 처리 시간이 짧지만 SHA보다 취약한 것으로 간주됩니다.
- null 또는 None(NULL, ESP-NONE) - (IPsec 제안에만 해당됨) null 해시 알고리즘으로, 대개 테스트용으로만 사용됩니다. 그러나 암호화 알고리즘으로 AES-GCM/GMAC 옵션 중 하나를 선택하는 경우에는 null 무결성 알고리즘을 선택해야 합니다. null 이외의 옵션을 선택하더라도 이러한 암호화 표준에 대해서는 무결성 해시가 무시됩니다.

사용할 **Diffie-Hellman** 모듈러스 그룹 결정

다음 Diffie-Hellman 키 파생 알고리즘을 사용하여 IPsec 보안 연계(SA) 키를 생성할 수 있습니다. 각 그룹의 크기 모듈러스는 서로 다릅니다. 대형 모듈러스는 보안성은 더 높지만, 처리 시간이 더 오래 걸립니다. 두 피어에 일치하는 모듈러스 그룹이 있어야 합니다.

AES 암호화를 선택하는 경우 AES에 필요한 큰 키를 지원하려면 DH(Diffie-Hellman) 그룹 5 이상을 사용해야 합니다. IKEv1 정책은 그룹 1, 2, 및 5만 허용합니다.

NSA Suite B 암호화 사양을 구현하려면 IKEv2를 사용하고 ECDH(Elliptic Curve Diffie-Hellman) 옵션 19, 20, 21 중 하나를 선택합니다. 2048비트 모듈러스를 사용하는 엘립틱 커브 옵션과 그룹은 Logjam과 같은 공격에 노출될 가능성이 작습니다.

IKEv2의 경우에는 여러 그룹을 구성할 수 있습니다. 시스템은 가장 안전한 항목부터 가장 안전하지 않은 항목 순으로 설정 순서를 지정하고 해당 순서를 사용하여 피어와 협상합니다. IKEv1의 경우 단일 옵션만 선택할 수 있습니다.

- 1 - Diffie-Hellman 그룹 1: 768비트 모듈러스
- 2 - Diffie-Hellman 그룹 2: 1024비트 모듈러스
- 5 - Diffie-Hellman 그룹 5: 1536비트 모듈러스. 128비트 키에 적합한 보호를 제공합니다.
- 14 - Diffie-Hellman 그룹 14: 2048비트 모듈러스. 192비트 키에 적합한 보호를 제공합니다.
- 19 - Diffie-Hellman 그룹 19: 256비트 엘립틱 커브
- 20 - Diffie-Hellman 그룹 20: 384비트 엘립틱 커브
- 21 - Diffie-Hellman 그룹 21: 521비트 엘립틱 커브
- 24 - Diffie-Hellman 그룹 24: 2048비트 모듈러스 및 256비트 소수 위수 하위 그룹

VPN 토폴로지

Firepower Device Manager를 통해서는 포인트 투 포인트 VPN 연결만 구성할 수 있습니다. 모든 연결은 포인트 투 포인트 방식이지만, 디바이스가 참여하는 각 터널을 정의하여 규모가 더 큰 허브 앤 스포크(hub and spoke) 또는 메시 VPN에 연결할 수 있습니다.

다음 다이어그램은 일반적인 포인트 투 포인트 VPN 토폴로지를 보여줍니다. 포인트 투 포인트 VPN 토폴로지에서는 2개의 엔드포인트가 서로 직접 통신합니다. 두 엔드포인트를 피어 디바이스로 구성하며, 두 디바이스 중 하나가 보안 연결을 시작할 수 있습니다.

사이트 대 사이트 VPN 관리

VPN(Virtual Private Network)은 인터넷과 같은 공개 소스나 기타 네트워크를 통해 원격 피어 간에 보안 터널을 설정하는 네트워크 연결입니다. VPN은 터널을 사용하여 IP 기반 네트워크로를 통해 전달할 수 있도록 일반 IP 패킷 내의 데이터 패킷을 캡슐화합니다. VPN은 암호화를 사용해 개인 정보와 인증을 확인함으로써 데이터의 무결성을 보장합니다.

피어 디바이스에 대한 VPN 연결을 생성할 수 있습니다. 모든 연결은 포인트 투 포인트 방식이지만, 모든 관련 연결을 구성하여 규모가 더 큰 허브 앤 스포크(hub and spoke) 또는 메시 VPN에 디바이스를 연결할 수 있습니다.

참고

VPN 연결은 암호화를 사용하여 네트워크 개인 정보를 보호합니다. 사용할 수 있는 암호화 알고리즘은 기본 라이선스가 강력한 암호화를 허용하는지에 따라 달라집니다. 강력한 암호화 허용 여부는 Cisco Smart License Manager에 등록할 때 디바이스에서 내보내기 제어 기능을 허용하는 옵션을 선택했는지에 따라 제어됩니다. 평가 라이선스를 사용 중이거나 내보내기 제어 기능을 활성화하지 않은 경우에는 강력한 암호화를 사용할 수 없습니다.

절차

단계 1 디바이스을 클릭한 다음 사이트 대 사이트 VPN 그룹에서 **View Configuration**(컨피그레이션 보기)을 클릭합니다.
그러면 구성한 모든 연결이 나열되는 사이트 대 사이트 VPN 페이지가 열립니다.

단계 2 다음 중 하나를 수행합니다.

- 새 사이트 대 사이트 VPN 연결을 생성하려면 + 버튼을 클릭합니다. 사이트 대 사이트 VPN 연결 구성, 265 페이지를 참조하십시오.

  아직 연결이 없는 경우에는 **Create Site-to-Site Connection**(사이트 대 사이트 연결 생성) 버튼을 클릭할 수도 있습니다.

- 기존 연결을 수정하려면 해당 연결의 수정 아이콘()을 클릭합니다. 사이트 대 사이트 VPN 연결 구성, 265 페이지를 참조하십시오.

- 연결 컨피그레이션 요약을 클립보드에 복사하려면 해당 연결의 복사 아이콘()을 클릭합니다. 이 정보를 문서에 붙여넣은 다음 원격 디바이스 관리자에게 보내면 관리자가 해당 연결 쪽을 쉽게 구성할 수 있습니다.
- 더 이상 필요하지 않은 연결을 삭제하려면 해당 연결의 삭제 아이콘()을 클릭합니다.

사이트 대 사이트 VPN 연결 구성

원격 디바이스 소유자가 협조하며 권한을 제공한다고 가정할 때 디바이스를 서로 연결하기 위한 포인트 투 포인트 VPN 연결을 생성할 수 있습니다. 모든 연결은 포인트 투 포인트 방식이지만, 디바이스가 참여하는 각 터널을 정의하여 보다 규모가 큰 허브 앤 스포크(hub and spoke) 또는 메시 VPN에 연결할 수 있습니다.

참고 로컬 네트워크/원격 네트워크 조합별로 단일 VPN 연결을 생성할 수 있습니다. 그러나 각 연결 프로필에서 원격 네트워크가 고유한 경우에는 로컬 네트워크에 대해 여러 연결을 생성할 수 있습니다.

절차

단계 **1** 디바이스을 클릭한 다음 사이트 대 사이트 VPN 그룹에서 **View Configuration**(컨피그레이션 보기)을 클릭합니다.

단계 **2** 다음 중 하나를 수행합니다.

- 새 사이트 대 사이트 VPN 연결을 생성하려면 + 버튼을 클릭합니다.

  아직 연결이 없는 경우에는 사이트 대 사이트 연결 생성 버튼을 클릭할 수도 있습니다.

- 기존 연결을 수정하려면 해당 연결의 수정 아이콘()을 클릭합니다.

더 이상 필요하지 않은 연결을 삭제하려면 해당 연결의 삭제 아이콘()을 클릭합니다.

단계 **3** 포인트 투 포인트 VPN 연결의 엔드포인트를 정의합니다.

- 연결 프로필 이름 - 이 연결의 이름을 공백 없이 64자까지 입력합니다. 예를 들면 MainOffice를 입력합니다. IP 주소는 이름으로 사용할 수 없습니다.
- 로컬 사이트 - 이러한 옵션은 로컬 엔드포인트를 정의합니다.
  - 로컬 **VPN** 액세스 인터페이스 - 원격 피어가 연결할 수 있는 인터페이스를 선택합니다. 이 인터페이스는 대개 외부 인터페이스이며, 브리지 그룹의 구성원일 수는 없습니다.

◦ 로컬 네트워크 - +를 클릭하고 VPN 연결에 참여해야 하는 로컬 네트워크를 식별하는 네트워크 개체를 선택합니다. 이러한 네트워크의 사용자는 해당 연결을 통해 원격 네트워크에 접속할 수 있습니다.

참고 이러한 네트워크에는 IPv4 또는 IPv6 주소를 사용할 수 있지만, 연결 양쪽의 주소 유형이 일치해야 합니다. 예를 들어 로컬 IPv4 네트워크에 대한 VPN 연결에는 원격 IPv4 네트워크가 하나 이상 있어야 합니다. 단일 연결의 양쪽에서 IPv4 및 IPv6를 함께 사용할 수 있습니다. 엔드포인트에 대한 보호된 네트워크는 겹칠 수 없습니다.

- 원격 사이트 - 이러한 옵션은 원격 엔드포인트를 정의합니다.
  - 원격 **IP** 주소 - VPN 연결을 호스팅할 원격 VPN 피어 인터페이스의 IP 주소를 입력합니다.
  - 원격 네트워크 - +를 클릭하고 VPN 연결에 참여해야 하는 원격 네트워크를 식별하는 네트워크 개체를 선택합니다. 이러한 네트워크의 사용자는 해당 연결을 통해 로컬 네트워크에 접속할 수 있습니다.

단계 **4** **Next(**다음**)**를 클릭합니다.

단계 **5** VPN에 대한 프라이버시 컨피그레이션을 정의합니다.

참고 라이선스에 따라 선택 가능한 암호화 프로토콜이 결정됩니다. 가장 기본적인 옵션 외의 옵션을 선택하려면 강력한 암호화를 사용할 수 있어야 합니다(내보내기 제어를 충족해야 함).

- **IKE** 버전 **2**, **IKE** 버전 **1** - IKE(Internet Key Exchange) 협상 중에 사용할 IKE 버전을 선택합니다. 필요에 따라 두 옵션 중 하나를 선택하거나 두 옵션을 모두 선택합니다. 디바이스는 다른 피어와의 연결 협상을 시도할 때 사용자가 허용하며 다른 피어가 수락하는 버전을 사용합니다. 두 버전을 모두 허용하는 경우 디바이스는 처음 선택한 버전을 통한 협상이 실패하면 다른 버전으로 자동 대체합니다. IKEv2가 구성되어 있으면 IKEv2 사용을 항상 먼저 시도합니다. IKEv2를 협상에서 사용하려면 두 피어가 모두 IKEv2를 지원해야 합니다.
- **IKE** 정책 - IKE(Internet Key Exchange)는 IPsec 피어를 인증하고, IPsec 암호화 키를 협상 및 배포하고, IPsec SA(보안 연계)를 자동으로 설정하는 데 사용되는 키 관리 프로토콜입니다. IKE는 글로벌 정책이므로 사용하는 개체가 모든 VPN에 적용됩니다. **Edit(**수정**)**을 클릭하여 IKE 버전별로 현재 전체적으로 활성화된 정책을 점검하고 새 정책을 활성화 및 생성합니다. 자세한 내용은 글로벌 IKE 정책 구성, 267 페이지를 참고하십시오.
- **IPsec** 제안 - IPsec 제안은 IPsec 터널에서 트래픽을 보호하는 보안 프로토콜 및 알고리즘 조합을 정의합니다. **Edit(**수정**)**을 클릭하고 각 IKE 버전에 대한 제안을 선택합니다. 허용하려는 모든 제안을 선택합니다. 시스템 기본값만 선택하려면 **Set Default(**기본값 설정**)**를 클릭합니다. 이러한 기본값은 내보내기 컴플라이언스에 따라 다릅니다. 시스템은 일치하는 항목이 합의될 때까지 가장 강력한 제안에서 가장 취약한 제안 순서대로 피어와 협상을 합니다. 자세한 내용은 IPsec 제안 구성, 271 페이지를 참고하십시오.
- (IKEv2) 로컬 사전 공유 키, 원격 피어 사전 공유 키 - VPN 연결을 위한 원격 디바이스와 이 디바이스에 정의된 키입니다. IKEv2에서는 이러한 키가 다를 수 있습니다. 키는 영숫자 1~127자가 될 수 있습니다.
- (IKEv1) 사전 공유 키 - 로컬 디바이스와 원격 디바이스에 모두 정의된 키입니다. 키는 영숫자 1~127자가 될 수 있습니다.

- **NAT** 제외 - 로컬 VPN 액세스 인터페이스의 NAT 정책에서 VPN 트래픽을 제외할지 여부를 선택합니다. NAT 규칙을 로컬 네트워크에 적용하지 않으려는 경우 로컬 네트워크를 호스팅하는 인터페이스를 선택합니다. 이 옵션은 로컬 네트워크가 단일 라우팅 인터페이스(브리지 그룹 구성원 아님) 뒤에 있는 경우에만 작동합니다. 로컬 네트워크가 둘 이상의 라우팅 인터페이스 또는 하나 이상의 브리지 그룹 구성원 뒤에 있는 경우에는 NAT 제외 규칙을 수동으로 생성해야 합니다. 필요한 규칙을 수동으로 생성하는 방법에 대한 자세한 내용은 NAT에서 사이트 대 사이트 VPN 트래픽 제외, 274 페이지를 참조하십시오.
- **PFS(Perfect Forward Secrecy)**에 대한 **Diffie-Helman** 그룹 - PFS(Perfect Forward Secrecy)를 사용하여 암호화된 각 교환에 대해 고유 세션 키를 생성하고 사용할지 여부를 선택합니다. 고유 세션 키는 전체 교환이 기록되었으며 공격자가 엔드포인트 디바이스에서 사용하는 사전 공유 키 또는 개인 키를 확보했더라도 후속 암호 해독에서 교환을 보호합니다. PFS(Perfect Forward Secrecy)를 사용하려면 모듈러스 그룹 목록에서 PFS 세션 키를 생성할 때 사용할 Diffie-Hellman 키 파생 알고리즘을 선택합니다. IKEv1 및 IKEv2를 모두 사용하면 IKEv1에서 지원하는 옵션만 선택할 수 있습니다. 옵션에 대한 설명은 사용할 Diffie-Hellman 모듈러스 그룹 결정, 263 페이지를 참조하십시오.

단계 **6** **Next(**다음**)**를 클릭합니다.

단계 **7** 요약을 검토하고 **Finish(**종료**)**를 클릭합니다.
요약 정보가 클립보드에 복사됩니다. 해당 정보를 문서에 붙여넣은 다음 원격 피어를 구성하는 데 사용하거나 피어 구성 담당자에게 보낼 수 있습니다.

컨피그레이션을 구축한 후, 디바이스 CLI에 로그인하고 **show ipsec sa** 명령을 사용하여 엔드포인트가 보안 연결을 설정하는지 확인합니다. 사이트 대 사이트 VPN 연결 확인, 280 페이지를 참조하십시오.

글로벌 **IKE** 정책 구성

IKE(Internet Key Exchange)는 IPsec 피어를 인증하고, IPsec 암호화 키를 협상 및 배포하고, IPsec SA(보안 연계)를 자동으로 설정하는 데 사용되는 키 관리 프로토콜입니다.

IKE 협상은 2단계로 구성됩니다. 1단계에서는 두 IKE 피어 간의 보안 연계를 협상합니다. 그러면 피어가 2단계에서 안전하게 통신할 수 있습니다. 2단계 협상 중에는 IKE가 IPsec 등의 기타 애플리케이션에 대해 SA를 설정합니다. 두 단계에서는 모두 연결을 협상할 때 제안을 사용합니다. IKE 제안은 두 피어가 상호 간의 IKE 협상을 보호하는 데 사용하는 알고리즘 집합입니다. IKE 협상에서는 두 피어가 먼저 공통(공유) IKE 정책을 합의합니다. 이 정책은 후속 IKE 협상을 보호하는 데 사용되는 보안 파라미터를 제시합니다.

IKE 정책 개체는 이러한 협상을 위한 IKE 제안을 정의합니다. 활성화하는 개체는 피어가 VPN 연결을 협상할 때 사용됩니다. 연결당 서로 다른 IKE 정책을 지정할 수는 없습니다. 각 개체의 상대 우선순위에 따라 이러한 정책 중 먼저 사용을 시도할 정책이 결정되며, 숫자가 작을수록 우선 순위는 높습니다. 협상에서 장애가 발생하여 두 피어가 모두 지원할 수 있는 정책을 찾지 못하면 연결이 설정되지 않습니다.

글로벌 IKE 정책을 정의하려면 각 IKE 버전에 대해 활성화할 개체를 선택합니다. 사전 정의된 개체가 요건을 충족하지 않는 경우 새 정책을 생성하여 보안 정책을 적용합니다.

다음 절차에서는 개체 페이지를 통해 글로벌 정책을 구성하는 방법을 설명합니다. IKE 정책 설정에서 **Edit(**수정**)**을 클릭하여 VPN 연결을 수정할 때 정책을 활성화, 비활성화 및 생성할 수도 있습니다.

절차

단계 **1** 목차에서 **Objects(**개체**)**와 **IKE Policies(IKE** 정책**)**를 차례로 선택합니다.
IKEv1과 IKEv2에 대한 정책이 개별 목록에 표시됩니다.

단계 **2** 각 IKE 버전에 대해 허용할 IKE 정책을 활성화합니다.

a) 개체 테이블 위의 **IKEv1** 또는 **IKEv2**를 선택하여 해당 버전의 정책을 표시합니다.

b) **State(**상태**)** 토글을 클릭하여 적절한 개체를 활성화하고 요건을 충족하지 않는 개체를 비활성화합니다.
보안 요건 중 일부가 기존 개체에 반영되어 있지 않은 경우에는 새 개체를 정의하여 요건을 구현합니다. 자세한 내용은 다음 항목을 참조하십시오.

- IKEv1 정책 구성, 268 페이지
- IKEv2 정책 구성, 270 페이지

c) 상대 우선 순위가 요건과 일치하는지 확인합니다.
정책 우선 순위를 변경해야 하는 경우 정책을 수정합니다. 사전 정의된 시스템 정책의 경우에는 정책의 고유 버전을 생성하여 우선 순위를 변경해야 합니다.

우선 순위는 절대값이 아닌 상대값입니다. 예를 들어 우선 순위 80이 160보다 높습니다. 최고 우선 순위 개체로 80을 활성화하면 해당 정책이 첫 번째로 선택됩니다. 그런 후에 우선 순위가 25인 정책을 사용하도록 설정하면 해당 정책이 최우선으로 선택됩니다.

d) 두 IKE 버전을 모두 사용하는 경우에는 다른 버전에 대해 프로세스를 반복합니다.

IKEv1 정책 구성

IKE(Internet Key Exchange) 버전 1 정책 개체에는 VPN 연결을 정의할 때 IKEv1 정책에 필요한 파라미터가 포함되어 있습니다. IKE는 IPsec 기반 통신을 쉽게 관리할 수 있도록 하는 키 관리 프로토콜이며 IPsec 피어를 인증하고, IPsec 암호화 키를 협상 및 배포하고, IPsec SA(보안 연계)를 자동으로 설정하는 데 사용됩니다.

여러 가지 사전 정의된 IKEv1 정책이 있습니다. 필요에 맞는 정책이 있으면 **State(**상태**)** 토글을 클릭하여 활성화하면 됩니다. 새 정책을 생성하여 다른 보안 설정 조합을 구현할 수도 있습니다. 시스템 정의 개체는 수정하거나 삭제할 수 없습니다.

다음 절차에서는 개체 페이지를 통해 개체를 직접 생성하고 수정할 수 있는 방법을 설명합니다. 개체 목록에 표시되는 **Create New IKE Policy(**새 **IKE** 정책 생성**)** 링크를 클릭하여 VPN 연결에서 IKEv1 설정을 수정하면서 IKEv1 정책 개체를 생성할 수도 있습니다.

절차

단계 1 목차에서 **Objects(**개체**)**와 **IKE Policies(IKE** 정책**)**를 차례로 선택합니다.

단계 2 개체 테이블 위의 **IKEv1**을 선택하여 IKEv1 정책을 표시합니다.

단계 3 요구사항에 맞는 시스템 정의 정책이 있으면 **State(**상태**)** 토글을 클릭하여 활성화합니다.
원치 않는 정책을 비활성화할 때도 **State(**상태**)** 토글을 사용합니다. 상대 우선 순위에 따라 이러한 정책 중 먼저 사용을 시도할 정책이 결정되며, 숫자가 작을수록 우선 순위가 높습니다.

단계 4 다음 중 하나를 수행합니다.

- 개체를 생성하려면 + 버튼을 클릭합니다.
- 개체를 수정하려면 개체의 수정 아이콘( )을 클릭합니다.

참조되지 않는 개체를 삭제하려면 해당 개체의 휴지통 아이콘( )을 클릭합니다.

단계 5 IKEv1 속성을 구성합니다.

- 우선 순위 - IKE 정책의 상대 우선 순위는 1~65,535입니다. 우선 순위에 따라 일반 SA(보안 연계) 찾기를 시도할 때 두 협상 피어가 비교하는 IKE 정책의 순서가 결정됩니다. 원격 IPsec 피어는 최고 우선 순위 정책에서 선택한 파라미터를 지원하지 않는 경우 그 다음 우선 순위에 정의된 파라미터 사용을 시도합니다. 번호가 낮을수록 우선 순위가 높습니다.
- 이름 - 개체의 이름(최대 128자)입니다.
- 상태 - IKE 정책이 활성화되어 있는지 여부입니다. 토글을 클릭하여 상태를 변경합니다. IKE 협상 중에는 활성화된 정책만 사용됩니다.
- 인증 - 두 피어 간에 사용할 인증 방법입니다. 사전 공유 키를 선택합니다. 사전 공유 키를 사용하면 보안 키를 두 피어 간에 공유할 수 있으며 인증 단계 수행 시 IKE에서 보안 키를 사용할 수 있습니다. 동일한 사전 공유 키를 사용하여 피어를 구성하지 않으면 IKE SA를 설정할 수 없습니다.
- 암호화 - 2단계 협상 보호를 위한 1단계 SA(보안 연계)를 설정하는 데 사용되는 암호화 알고리즘입니다. 옵션에 대한 설명은 사용할 암호화 알고리즘 결정, 261 페이지를 참조하십시오.
- **Diffie-Hellman** 그룹 - 공유 암호를 각 IPsec 피어에 전송하지 않고 두 IPsec 피어 간에 파생하는 데 사용할 Diffie Hellman 그룹입니다. 대형 모듈러스는 보안성은 더 높지만, 처리 시간이 더 오래 걸립니다. 두 피어의 모듈러스 그룹이 일치해야 합니다. 옵션에 대한 설명은 사용할 Diffie-Hellman 모듈러스 그룹 결정, 263 페이지를 참조하십시오.
- 해시 - 메시지 무결성을 보장하는 데 사용되는 메시지 다이제스트를 생성하기 위한 해시 알고리즘입니다. 옵션에 대한 설명은 사용할 해시 알고리즘 결정, 262 페이지를 참조하십시오.
- 수명 - SA(보안 연계)의 라이프타임(초)으로, 120~2147483647입니다. 라이프타임이 초과되면 SA는 만료되며 두 피어 간에 SA를 재협상해야 합니다. 일반적으로 특정 지점까지는 라이프타임이 짧을수록 IKE 협상이 보다 안전합니다. 그러나 라이프타임이 길면 라이프타임이 짧은 경우에 비해 이후 IPsec 보안 연계를 더 빠르게 설정할 수 있습니다. 기본값은 86400입니다.

단계 6 **OK(확인)**를 클릭하여 변경 사항을 저장합니다.

IKEv2 정책 구성

IKE(Internet Key Exchange) 버전 2 정책 개체에는 VPN 연결을 정의할 때 IKEv2 정책에 필요한 파라미터가 포함되어 있습니다. IKE는 IPsec 기반 통신을 쉽게 관리할 수 있도록 하는 키 관리 프로토콜이며 IPsec 피어를 인증하고, IPsec 암호화 키를 협상 및 배포하고, IPsec SA(보안 연계)를 자동으로 설정하는 데 사용됩니다.

여러 가지 사전 정의된 IKEv2 정책이 있습니다. 필요에 맞는 정책이 있으면 **State(상태)** 토글을 클릭하여 활성화하면 됩니다. 새 정책을 생성하여 다른 보안 설정 조합을 구현할 수도 있습니다. 시스템 정의 개체는 수정하거나 삭제할 수 없습니다.

다음 절차에서는 개체 페이지를 통해 개체를 직접 생성하고 수정할 수 있는 방법을 설명합니다. 개체 목록에 표시되는 **Create New IKE Policy(새 IKE 정책 생성)** 링크를 클릭하여 VPN 연결에서 IKEv2 설정을 수정하면서 IKEv2 정책 개체를 생성할 수도 있습니다.

절차

단계 1 목차에서 **Objects(개체)**와 **IKE Policies(IKE 정책)**를 차례로 선택합니다.

단계 2 개체 테이블 위의 **IKEv2**를 선택하여 IKEv2 정책을 표시합니다.

단계 3 요구사항에 맞는 시스템 정의 정책이 있으면 **State(상태)** 토글을 클릭하여 활성화합니다.
원치 않는 정책을 비활성화할 때도 **State(상태)** 토글을 사용합니다. 상대 우선 순위에 따라 이러한 정책 중 먼저 사용을 시도할 정책이 결정되며, 숫자가 작을수록 우선 순위가 높습니다.

단계 4 다음 중 하나를 수행합니다.

- 개체를 생성하려면 + 버튼을 클릭합니다.
- 개체를 수정하려면 개체의 수정 아이콘( )을 클릭합니다.

참조되지 않는 개체를 삭제하려면 해당 개체의 휴지통 아이콘( )을 클릭합니다.

단계 5 IKEv2 속성을 구성합니다.

- 우선 순위 - IKE 정책의 상대 우선 순위는 1~65,535입니다. 우선 순위에 따라 일반 SA(보안 연계) 찾기를 시도할 때 두 협상 피어가 비교하는 IKE 정책의 순서가 결정됩니다. 원격 IPsec 피어는 최고 우선 순위 정책에서 선택한 파라미터를 지원하지 않는 경우 그 다음 우선 순위에 정의된 파라미터 사용을 시도합니다. 번호가 낮을수록 우선 순위가 높습니다.
- 이름 - 개체의 이름(최대 128자)입니다.
- 상태 - IKE 정책이 활성화되어 있는지 여부입니다. 토글을 클릭하여 상태를 변경합니다. IKE 협상 중에는 활성화된 정책만 사용됩니다.
- 암호화 - 2단계 협상 보호를 위한 1단계 SA(보안 연계)를 설정하는 데 사용되는 암호화 알고리즘입니다. 허용하려는 모든 알고리즘을 선택합니다. 단, 같은 정책에 혼합 모드(AES-GCM) 및 일반 모드 옵션을 둘 다 포함할 수는 없습니다. 일반 모드에서는 무결성 해시를 선택해야 하는

반면 혼합 모드에서는 개별 무결성 해시 선택이 금지됩니다. 시스템은 일치하는 항목이 합의될 때까지 가장 강력한 알고리즘에서 가장 취약한 알고리즘 순서대로 피어와 협상을 합니다. 옵션에 대한 설명은 사용할 암호화 알고리즘 결정, 261 페이지를 참조하십시오.

- **Diffie-Hellman** 그룹 - 공유 암호를 각 IPsec 피어에 전송하지 않고 두 IPsec 피어 간에 파생하는 데 사용할 Diffie Hellman 그룹입니다. 대형 모듈러스는 보안성은 더 높지만, 처리 시간이 더 오래 걸립니다. 두 피어의 모듈러스 그룹이 일치해야 합니다. 허용하려는 모든 알고리즘을 선택합니다. 시스템은 일치하는 항목이 합의될 때까지 가장 강력한 그룹에서 가장 취약한 그룹 순서대로 피어와 협상을 합니다. 옵션에 대한 설명은 사용할 Diffie-Hellman 모듈러스 그룹 결정, 263 페이지를 참조하십시오.
- 무결성 해시 - 메시지 무결성을 보장하는 데 사용되는 메시지 다이제스트를 생성하기 위한 해시 알고리즘의 무결성 부분입니다. 허용하려는 모든 알고리즘을 선택합니다. 시스템은 일치하는 항목이 합의될 때까지 가장 강력한 알고리즘에서 가장 취약한 알고리즘 순서대로 피어와 협상을 합니다. AES-GCM 암호화 옵션에서는 무결성 해시가 사용되지 않습니다. 옵션에 대한 설명은 사용할 해시 알고리즘 결정, 262 페이지를 참조하십시오.
- **PRF(Pseudo Random Function)** 해시 - 해시 알고리즘의 PRF(Pseudo Random Function) 부분으로, IKEv2 터널 암호화에 필요한 키 요소 및 해싱 작업을 파생시키기 위해 알고리즘으로 사용됩니다. IKEv1에서는 무결성 및 PRF 알고리즘이 구분되지 않지만 IKEv2에서는 이러한 요소에 대해 서로 다른 알고리즘을 지정할 수 있습니다. 허용하려는 모든 알고리즘을 선택합니다. 시스템은 일치하는 항목이 합의될 때까지 가장 강력한 알고리즘에서 가장 취약한 알고리즘 순서대로 피어와 협상을 합니다. 옵션에 대한 설명은 사용할 해시 알고리즘 결정, 262 페이지를 참조하십시오.
- 수명 - SA(보안 연계)의 라이프타임(초)으로, 120~2147483647입니다. 라이프타임이 초과되면 SA는 만료되며 두 피어 간에 SA를 재협상해야 합니다. 일반적으로 특정 지점까지는 라이프타임이 짧을수록 IKE 협상이 보다 안전합니다. 그러나 라이프타임이 길면 라이프타임이 짧은 경우에 비해 이후 IPsec 보안 연계를 더 빠르게 설정할 수 있습니다. 기본값은 86400입니다.

단계 **6** **OK**(확인)를 클릭하여 변경 사항을 저장합니다.

IPsec 제안 구성

IPsec는 가장 안전하게 VPN 설정을 하는 방법 중 하나입니다. IPsec는 IP 패킷 레벨에서 데이터 암호화 기능을 제공하는 강력한 표준 기반 솔루션입니다. IPsec를 사용하는 경우 데이터는 터널을 통해 공용 네트워크를 사용하여 전송됩니다. 터널은 두 피어 간의 안전한 논리적 통신 경로입니다. IPsec 터널로 진입하는 트래픽은 보안 프로토콜 및 알고리즘이 조합된 변환 집합에 의해 보호됩니다. IPsec 보안 연계(SA) 협상 중에 피어는 두 피어에서 동일한 변환 집합을 검색합니다.

IKE 버전(IKEv1 또는 IKEv2)에 따라 각기 다른 IPsec 제안 개체가 있습니다.

- IKEv1 IPsec 제안을 생성할 때는 IPsec가 동작하는 모드를 선택하고 필요한 암호화 및 인증 유형을 정의합니다. 알고리즘에 대해서는 단일 옵션을 선택할 수 있습니다. VPN에서 여러 조합을 지원하려면 여러 IKEv1 IPsec 제안 개체를 생성하여 선택합니다.

- IKEv2 IPsec 제안을 생성할 때는 VPN에서 허용되는 모든 암호화 및 해시 알고리즘을 선택할 수 있습니다. 시스템은 가장 안전한 항목부터 가장 안전하지 않은 항목 순으로 설정 순서를 지정하고 일치하는 항목을 찾을 때까지 피어와 협상합니다. 이를 통해 IKEv1과 마찬가지로 허용된 각 조합을 개별적으로 전송하는 대신 모든 허용된 조합을 전달하는 단일 제안서를 보낼 수 있습니다.

IKEv1 및 IKEv2 IPsec 제안에는 모두 ESP(Encapsulating Security Protocol)가 사용됩니다. ESP는 인증, 암호화 및 재생 방지 서비스를 제공합니다. ESP는 IP 프로토콜 유형 50입니다.

참고 IPsec 터널에서는 암호화 및 인증을 모두 사용하는 것이 좋습니다.

다음 항목에서는 각 IKE 버전에 대해 IPsec 제안을 구성하는 방법을 설명합니다.

IKEv1용 **IPsec** 제안 구성

IKEv1 IPsec 제안 개체를 사용하여 IKE 2단계 협상 시 사용되는 IPsec 제안을 구성합니다. IPsec 제안은 IPsec 터널에서 트래픽을 보호하는 보안 프로토콜 및 알고리즘 조합을 정의합니다.

여러 가지 사전 정의된 IKEv1 IPsec 제안이 있습니다. 새 제안을 생성하여 다른 보안 설정 조합을 구현할 수도 있습니다. 시스템 정의 개체는 수정하거나 삭제할 수 없습니다.

다음 절차에서는 개체 페이지를 통해 개체를 직접 생성하고 수정할 수 있는 방법을 설명합니다. 개체 목록에 표시되는 **Create New IPsec Proposal(**새 **IPsec** 제안 생성**)** 링크를 클릭하여 VPN 연결에서 IKEv1 IPsec 설정을 수정하면서 IKEv1 IPsec 제안 개체를 생성할 수도 있습니다.

절차

단계 **1** 목차에서 **Objects(**개체**)**와 **IPsec Proposals(IPsec** 제안**)**를 차례로 선택합니다.

단계 **2** 개체 테이블 위의 **IKEv1**을 선택하여 IKEv1 IPsec 제안을 표시합니다.

단계 **3** 다음 중 하나를 수행합니다.

- 개체를 생성하려면 + 버튼을 클릭합니다.
- 개체를 수정하려면 개체의 수정 아이콘()을 클릭합니다.

참조되지 않는 개체를 삭제하려면 해당 개체의 휴지통 아이콘()을 클릭합니다.

단계 **4** IKEv1 IPsec 제안 속성을 구성합니다.

- 이름 - 개체의 이름(최대 128자)입니다.
- 모드 - IPSec 터널이 작동하는 모드입니다.
  - 터널 모드에서는 전체 IP 패킷이 캡슐화됩니다. IPSec 헤더는 원본 IP 헤더와 새 IP 헤더 사이에 추가됩니다. 이는 기본값입니다. 방화벽 뒤에 배치되어 있는 호스트와 주고받는 트래픽을 방화벽이 보호하는 경우 터널 모드를 사용합니다. 터널 모드는 인터넷 등의 신뢰할 수

없는 네트워크를 통해 연결하는 두 방화벽 또는 기타 보안 게이트웨이 간에 일반 IPsec가 구현되는 통상적인 방식입니다.

◦ 전송 모드에서는 IP 패킷의 상위 레이어 프로토콜만 캡슐화됩니다. IPSec 헤더는 TCP 등의 상위 계층 프로토콜 헤더와 IP 헤더 사이에 삽입됩니다. 전송 모드에서는 소스 호스트와 대상 호스트가 모두 IPsec를 지원해야 합니다. 터널의 대상 피어가 IP 패킷의 최종 대상인 경우에만 전송 모드를 사용할 수 있습니다. 전송 모드는 대개 GRE, L2TP, DLSW 등의 레이어 2 또는 레이어 3 터널링 프로토콜을 보호할 때만 사용됩니다.

- **ESP** 암호화 - 이 제안에 대한 ESP(Encapsulating Security Protocol) 암호화 알고리즘입니다. 옵션에 대한 설명은 사용할 암호화 알고리즘 결정, 261 페이지를 참조하십시오.
- **ESP** 해시 - 인증에 사용할 해시 또는 무결성 알고리즘입니다. 옵션에 대한 설명은 사용할 해시 알고리즘 결정, 262 페이지를 참조하십시오.

단계 **5** **OK(**확인**)**를 클릭하여 변경 사항을 저장합니다.

IKEv2용 **IPsec** 제안 구성

IKEv2 IPsec 제안 개체를 사용하여 IKE 2단계 협상 시 사용되는 IPsec 제안을 구성합니다. IPsec 제안은 IPsec 터널에서 트래픽을 보호하는 보안 프로토콜 및 알고리즘 조합을 정의합니다.

여러 가지 사전 정의된 IKEv2 IPsec 제안이 있습니다. 새 제안을 생성하여 다른 보안 설정 조합을 구현할 수도 있습니다. 시스템 정의 개체는 수정하거나 삭제할 수 없습니다.

다음 절차에서는 개체 페이지를 통해 개체를 직접 생성하고 수정할 수 있는 방법을 설명합니다. 개체 목록에 표시되는 **Create New IPsec Proposal(**새 **IPsec** 제안 생성**)** 링크를 클릭하여 VPN 연결에서 IKEv2 IPsec 설정을 수정하면서 IKEv2 IPsec 제안 개체를 생성할 수도 있습니다.

절차

단계 **1** 목차에서 **Objects(**개체**)**와 **IPsec Proposals(IPsec** 제안**)**를 차례로 선택합니다.

단계 **2** 개체 테이블 위의 **IKEv2**를 선택하여 IKEv2 IPsec 제안을 표시합니다.

단계 **3** 다음 중 하나를 수행합니다.

- 개체를 생성하려면 + 버튼을 클릭합니다.
- 개체를 수정하려면 개체의 수정 아이콘()을 클릭합니다.

참조되지 않는 개체를 삭제하려면 해당 개체의 휴지통 아이콘()을 클릭합니다.

단계 **4** IKEv2 IPsec 제안 속성을 구성합니다.

- 이름 - 개체의 이름(최대 128자)입니다.

- 암호화 - 이 제안에 대한 ESP(Encapsulating Security Protocol) 암호화 알고리즘입니다. 허용하려는 모든 알고리즘을 선택합니다. 시스템은 일치하는 항목이 합의될 때까지 가장 강력한 알고리즘에서 가장 취약한 알고리즘 순서대로 피어와 협상을 합니다. 옵션에 대한 설명은 사용할 암호화 알고리즘 결정, 261 페이지를 참조하십시오.
- 무결성 해시 - 인증에 사용할 해시 또는 무결성 알고리즘입니다. 허용하려는 모든 알고리즘을 선택합니다. 시스템은 일치하는 항목이 합의될 때까지 가장 강력한 알고리즘에서 가장 취약한 알고리즘 순서대로 피어와 협상을 합니다. 옵션에 대한 설명은 사용할 해시 알고리즘 결정, 262 페이지를 참조하십시오.

  참고 암호화 알고리즘으로 AES-GCM/GMAC 옵션 중 하나를 선택하는 경우에는 null 무결성 알고리즘을 선택해야 합니다. null이 아닌 옵션을 선택하더라도 이러한 암호화 표준은 무결성 해시를 사용하지 않습니다.

단계 **5** **OK(확인)**를 클릭하여 변경 사항을 저장합니다.

NAT에서 사이트 대 사이트 VPN 트래픽 제외

인터페이스에 사이트 대 사이트 VPN 연결이 정의되어 있고 해당 인터페이스에 대한 NAT 규칙도 있는 경우 NAT 규칙에서 VPN의 트래픽을 선택적으로 제외할 수 있습니다. VPN 연결의 원격 쪽에서 내부 주소를 처리할 수 있는 경우 이러한 VPN 트래픽을 제외할 수 있습니다.

VPN 연결을 생성할 때 **NAT Exempt(NAT 제외)** 옵션을 선택하여 규칙을 자동으로 생성할 수 있습니다. 그러나 브리지 그룹 구성원이 아닌 단일 라우팅 인터페이스를 통해 보호된 로컬 네트워크에 연결하는 경우에만 이 방법을 사용할 수 있습니다. 그렇지 않고 연결의 로컬 네트워크가 둘 이상의 라우팅 인터페이스 또는 하나 이상의 브리지 그룹 구성원에 있는 경우에는 NAT 제외 규칙을 수동으로 구성해야 합니다.

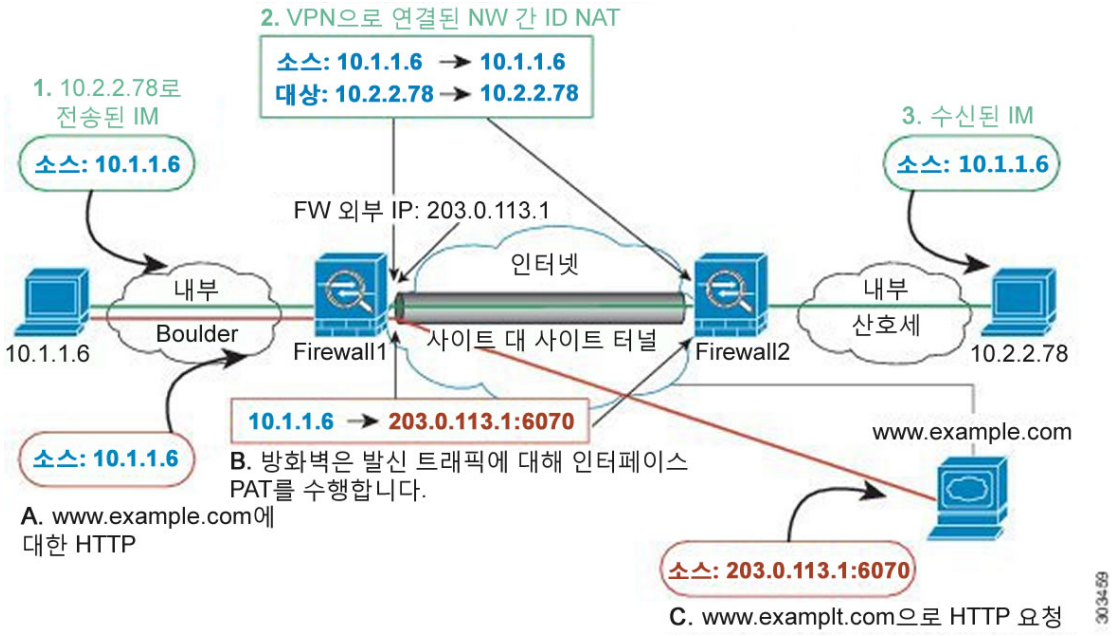
NAT 규칙에서 VPN 트래픽을 제외하려면 대상이 원격 네트워크일 때 로컬 트래픽에 대한 ID 수동 NAT 규칙을 생성합니다. 그런 다음 대상이 인터넷 등의 다른 항목일 때 트래픽에 NAT를 적용합니다. 로컬 네트워크의 인터페이스가 여러 개인 경우 각 인터페이스에 대해 규칙을 생성합니다. 또한 다음과 같은 제안 사항을 고려합니다.

- 연결에 로컬 네트워크가 여러 개 있으면 네트워크를 정의하는 개체를 포함할 네트워크 개체 그룹을 생성합니다.
- VPN에 IPv4 및 IPv6 네트워크를 둘 다 포함하는 경우 각 네트워크에 대해 별도의 ID NAT 규칙을 생성합니다.

볼더 사무실과 산호세 사무실을 연결하는 사이트 대 사이트 터널을 보여주는 다음 예를 살펴보십시오. 인터넷으로 이동할 트래픽(예: 볼더의 10.1.1.6에서 www.example.com으로)의 경우 인터넷 액세스를 위해 NAT에서 제공하는 공용 IP 주소가 필요합니다. 아래의 예에서는 인터페이스 PAT 규칙을 사용합니다. 그러나 VPN 터널을 지나갈 트래픽(예: 볼더의 10.1.1.6에서 산호세의 10.2.2.78로)에 대해서

는 NAT를 수행하지 않으려고 합니다. 그렇게 하려면 ID NAT 규칙을 만들어 해당 트래픽을 제외해야 합니다. ID NAT는 단순히 주소를 동일한 주소로 변환합니다.

그림 ***19:*** 사이트 대 사이트 ***VPN***을 위한 인터페이스 ***PAT*** 및 ***ID NAT***



다음 예에서는 방화벽1(볼더)의 컨피그레이션에 대해 설명합니다. 이 예에서는 내부 인터페이스가 브리지 그룹이라고 가정하므로 각 구성원 인터페이스에 대해 규칙을 작성해야 합니다. 라우팅 내부 인터페이스가 하나이든 여러 개이든 프로세스는 동일합니다.

참고 이 예에서는 IPv4만 사용한다고 가정합니다. VPN에 IPv6 네트워크도 포함되어 있으면 IPv6용 병렬 규칙을 생성합니다. IPv6 인터페이스 PAT를 구현할 수는 없으므로 PAT에 사용할 고유 IPv6 주소가 포함된 호스트 개체를 생성해야 합니다.

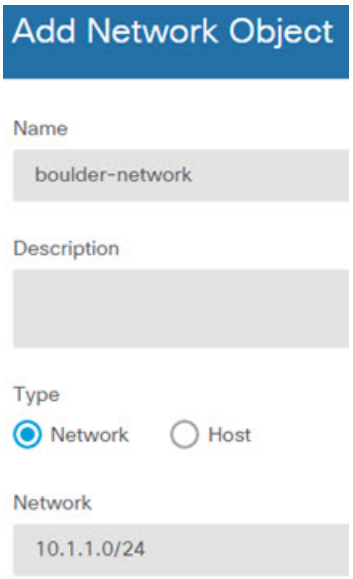
절차

단계 **1** 여러 네트워크를 정의하기 위한 개체를 생성합니다.

a) **Objects(**개체**)**를 선택합니다.

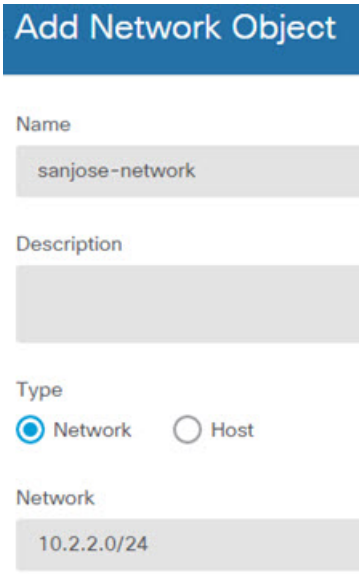
b) 목차에서 **Network(**네트워크**)**를 선택하고 +를 클릭합니다.

c) 볼더 내부 네트워크를 확인합니다.
네트워크 개체의 이름을 boulder-network와 같이 지정하고 **Network(**네트워크**)**를 선택한 후에 네트워크 주소 10.1.1.0/24를 입력합니다.



d) **OK(**확인**)**를 클릭합니다.

e) +를 클릭하여 내부 산호세 네트워크를 정의합니다.
네트워크 개체의 이름을 sanjose-network와 같이 지정하고 **Network(**네트워크**)**를 선택한 후에 네트워크 주소 10.2.2.0/24를 입력합니다.



f) **OK(**확인**)**를 클릭합니다.

단계 **2** 방화벽1(볼더)에서 VPN을 통해 산호세로 이동할 때 볼더 네트워크용 수동 ID NAT를 구성합니다.

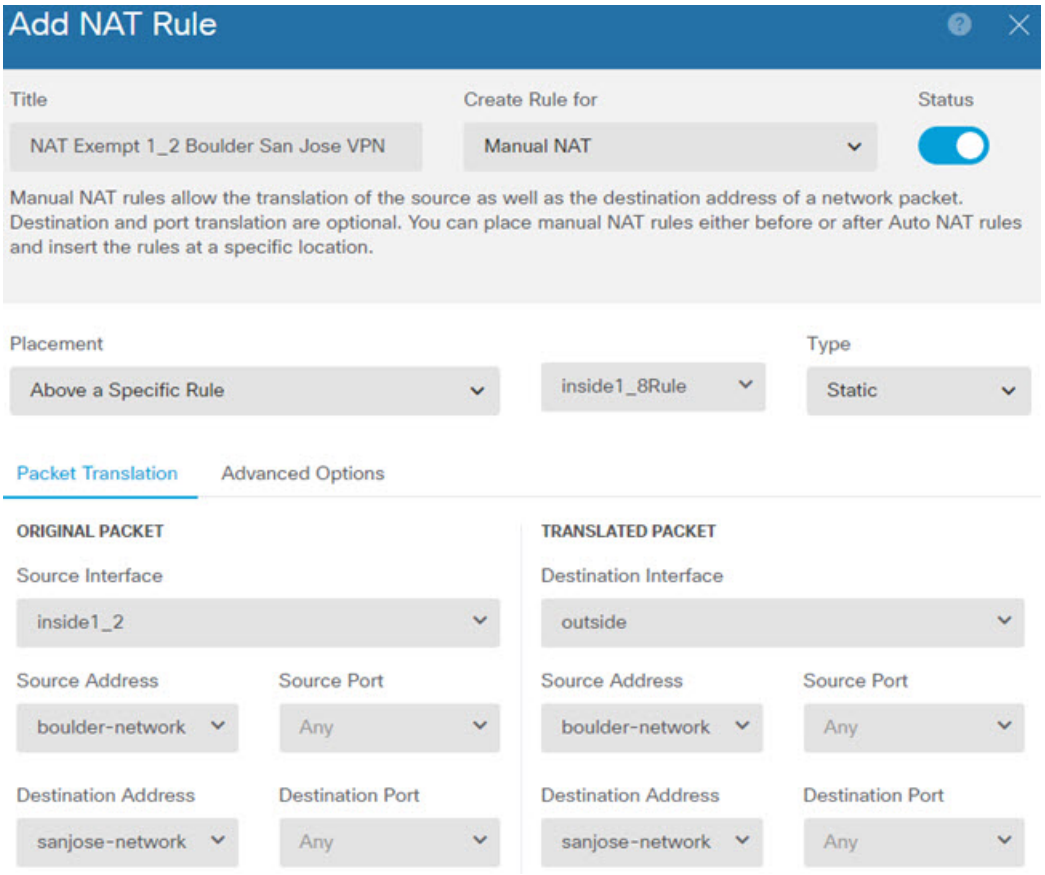
a) **Policies(**정책**)** > **NAT**를 선택합니다.

b) + 버튼을 클릭합니다.

c) 다음 속성을 구성합니다.

- 제목 = NAT Exempt 1_2 Boulder San Jose VPN 또는 원하는 다른 이름
- 규칙 생성 = 수동 NAT
- 배치 = 특정 규칙 위를 선택하고 자동 NAT 앞의 수동 NAT 섹션에서 첫 번째 규칙을 선택합니다. 대상 인터페이스의 모든 일반 인터페이스 PAT 규칙 앞에 이 규칙을 배치해야 합니다. 그렇지 않으면 규칙이 적절한 트래픽에 적용되지 않을 수 있습니다.
- 유형 = 고정
- 소스 인터페이스 = inside1_2
- 대상 인터페이스 = outside
- 원본 소스 주소 = boulder-network 네트워크 개체
- 변환된 소스 주소 = boulder-network 네트워크 개체
- 원본 대상 주소 = sanjose-network 네트워크 개체
- 변환된 대상 주소 = sanjose-network 네트워크 개체

  참고 대상 주소를 변환하지 않을 것이기 때문에 원본 주소 및 변환된 대상 주소에 대해 동일한 주소를 지정하여 대상 주소에 대한 ID NAT를 구성해야 합니다. 포트 필드는 모두 비워 둡니다. 이 규칙은 소스 및 대상 둘 다에 대해 ID NAT를 구성합니다.



d) **Advanced(**고급**)** 탭에서 **Do not proxy ARP on Destination interface(**대상 인터페이스에서 **ARP** 프록시 설정 안 함**)**를 선택합니다.

e) **OK(**확인**)**를 클릭합니다.

f) 이 프로세스를 반복하여 각각의 기타 내부 인터페이스에 대해 동일 규칙을 생성합니다.

단계 **3** 방화벽1(볼더)에서 내부 볼더 네트워크에 대해 인터넷으로 이동할 때 수동 동적 인터페이스 PAT를 구성합니다.

참고 모든 IPv4 트래픽에 적용되는 내부 인터페이스용 동적 인터페이스 PAT 규칙은 이미 있을 수 있습니다. 이러한 규칙은 초기 컨피그레이션 중에 기본적으로 생성되기 때문입니다. 그러나 여기서는 완전한 설명을 위해 컨피그레이션을 제공합니다. 이러한 단계를 완료하기 전에 내부 인터페이스와 네트워크에 적용되는 규칙이 이미 있는지 확인하고 해당 규칙이 있으면 이 단계를 건너뜁니다.

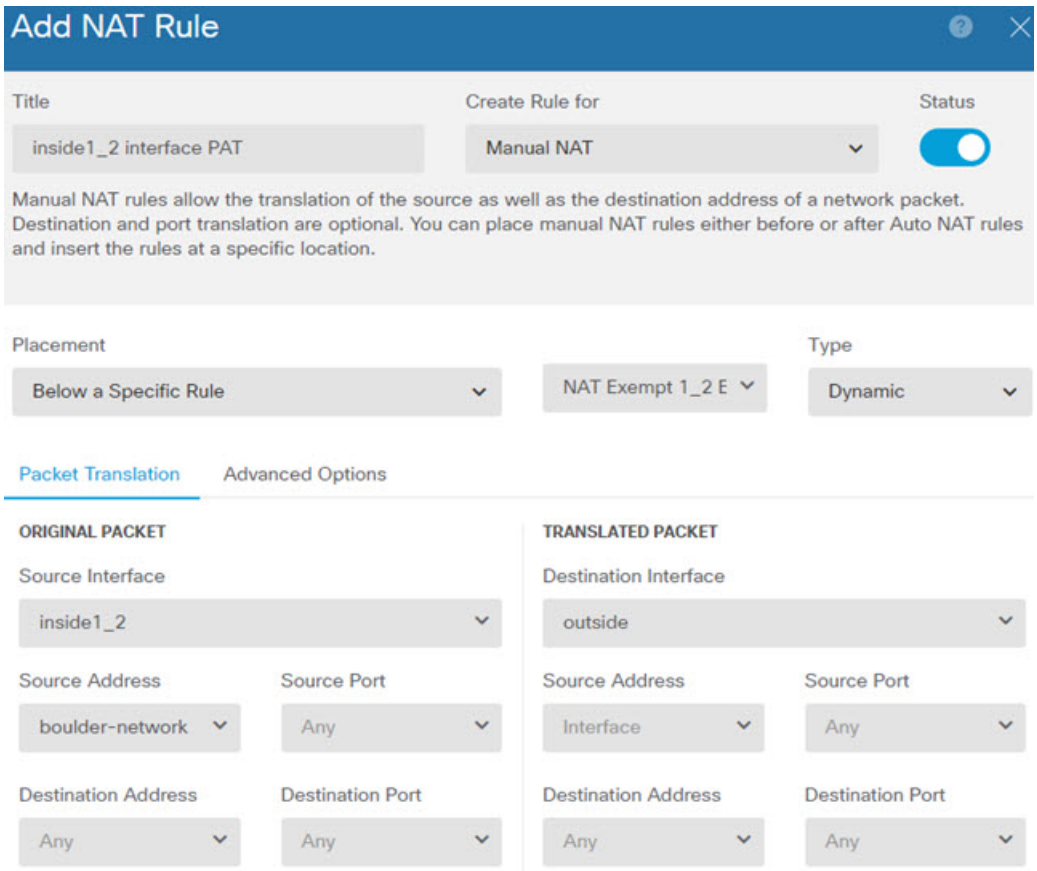
a) + 버튼을 클릭합니다.

b) 다음 속성을 구성합니다.

- 제목 = inside1_2 interface PAT 또는 원하는 다른 이름
- 규칙 생성 = 수동 NAT
- 배치 = 특정 규칙 아래를 선택하고 자동 NAT 앞의 수동 NAT 섹션에서 이 인터페이스용으로 생성한 규칙을 선택합니다. 이 규칙은 모든 대상 주소에 적용되므로 sanjose-network를 대상

으로 사용하는 규칙이 이 규칙 앞에 와야 합니다. 그렇지 않으면 sanjose-network 규칙은 어떤 주소와도 일치하지 않게 됩니다. 기본적으로는 "자동 NAT 앞의 NAT 규칙" 섹션 끝에 새 수동 NAT 규칙을 배치합니다. 이 기본 배치를 사용해도 충분합니다.

- 유형 = 동적
- 소스 인터페이스 = inside1_2
- 대상 인터페이스 = outside
- 원본 소스 주소 = boulder-network 네트워크 개체
- 변환된 소스 주소 = **Interface** 이 옵션은 대상 인터페이스를 사용하여 인터페이스 PAT를 구성합니다.
- 원본 대상 주소 = 임의
- 변환된 대상 주소 = 임의



c) **OK**(확인)를 클릭합니다.

d) 이 프로세스를 반복하여 각각의 기타 내부 인터페이스에 대해 동일 규칙을 생성합니다.

단계 **4** 방화벽2(산호세)도 관리하는 경우 해당 디바이스에 대해 비슷한 규칙을 구성할 수 있습니다.

- 대상이 boulder-network일 때는 sanjose-network용 수동 ID NAT 규칙을 구성합니다. 방화벽2 내부 및 외부 네트워크용으로 새 인터페이스 개체를 생성합니다.
- 대상이 "임의"일 때는 sanjose-network용 수동 동적 인터페이스 PAT 규칙을 생성합니다.

사이트 대 사이트 VPN 연결 확인

사이트 대 사이트 VPN 연결을 구성하고 디바이스에 컨피그레이션을 구축한 후에는 시스템이 원격 디바이스와 보안 연결을 설정했는지 확인합니다.

연결을 설정할 수 없는 경우, 디바이스 CLI에서 **ping interface***interface_nameremote_ip_address* 명령을 사용하여 VPN 인터페이스를 통해 원격 디바이스로 전달되는 경로를 확보합니다. 구성된 인터페이스를 통과하는 연결이 없을 경우, **interface***interface_name* 키워드를 중단하고, 연결이 다른 인터페이스를 통과하는지 확인합니다. 연결에 잘못된 인터페이스를 연결했을 가능성이 있습니다. 보호되는 네트워크를 향한 네트워크가 아닌, 원격 디바이스를 향하는 인터페이스를 선택해야 합니다.

네트워크 경로가 있을 경우, 두 엔드포인트에서 지원하는 IKE 버전 및 키를 확인하고 필요한 경우 VPN 연결을 조정합니다. 액세스 제어 또는 NAT 규칙이 연결을 차단하고 있지 않은지 확인합니다.

절차

단계 **1** CLI(Command Line Interface) 로그인, 7 페이지에 설명된 대로 디바이스 CLI에 로그인합니다.

단계 **2** **show ipsec sa** 명령을 사용하여 IPSec 보안 연결이 설정되었는지 확인합니다.
디바이스(**local addr**)와 원격 피어(**current_peer**) 사이에 VPN 연결이 설정되었는지 확인해야 합니다. 연결을 통해 트래픽을 전송할 때 패킷(pkts) 수가 증가해야 합니다. 액세스 목록에는 연결의 로컬 및 원격 네트워크가 표시되어야 합니다.

예를 들어 다음 출력은 IKEv2 연결을 표시합니다.

```
> show ipsec sa
interface: site-a-outside
    Crypto map tag: s2sCryptoMap, seq num: 1, local addr: 192.168.2.15

      access-list |s2sAcl|0730e31c-1e5f-11e7-899f-27f6e1030344
extended permit ip 192.168.1.0 255.255.255.0 192.168.3.0 255.255.255.0
      local ident (addr/mask/prot/port): (192.168.1.0/255.255.255.0/0/0)
      remote ident (addr/mask/prot/port): (192.168.3.0/255.255.255.0/0/0)
      current_peer: 192.168.4.6


      #pkts encaps: 69, #pkts encrypt: 69, #pkts digest: 69
      #pkts decaps: 69, #pkts decrypt: 69, #pkts verify: 69
      #pkts compressed: 0, #pkts decompressed: 0
      #pkts not compressed: 69, #pkts comp failed: 0, #pkts decomp failed: 0
      #pre-frag successes: 0, #pre-frag failures: 0, #fragments created: 0
      #PMTUs sent: 0, #PMTUs rcvd: 0, #decapsulated frgs needing reassembly: 0
```

```
      #TFC rcvd: 0, #TFC sent: 0
      #Valid ICMP Errors rcvd: 0, #Invalid ICMP Errors rcvd: 0
      #send errors: 0, #recv errors: 0

      local crypto endpt.: 192.168.2.15/500, remote crypto endpt.: 192.168.4.6/500
      path mtu 1500, ipsec overhead 55(36), media mtu 1500
      PMTU time remaining (sec): 0, DF policy: copy-df
      ICMP error validation: disabled, TFC packets: disabled
      current outbound spi: CD22739C
      current inbound spi : 52D2F1E4

    inbound esp sas:
      spi: 0x52D2F1E4 (1389556196)
         SA State: active
         transform: esp-aes-gcm-256 esp-null-hmac no compression
         in use settings ={L2L, Tunnel, PFS Group 19, IKEv2, }
         slot: 0, conn_id: 62738432, crypto-map: s2sCryptoMap
         sa timing: remaining key lifetime (kB/sec): (4285434/28730)
         IV size: 8 bytes
         replay detection support: Y
         Anti replay bitmap:
          0xFFFFFFFF 0xFFFFFFFF
    outbound esp sas:
      spi: 0xCD22739C (3441587100)
         SA State: active
         transform: esp-aes-gcm-256 esp-null-hmac no compression
         in use settings ={L2L, Tunnel, PFS Group 19, IKEv2, }
         slot: 0, conn_id: 62738432, crypto-map: s2sCryptoMap
         sa timing: remaining key lifetime (kB/sec): (4055034/28730)
         IV size: 8 bytes
         replay detection support: Y
         Anti replay bitmap:
          0x00000000 0x00000001
```

다음 출력은 IKEv1 연결을 표시합니다.

```
> show ipsec sa
interface: site-a-outside
    Crypto map tag: s2sCryptoMap, seq num: 1, local addr: 192.168.2.15

      access-list |s2sAcl|0730e31c-1e5f-11e7-899f-27f6e1030344
extended permit ip 192.168.1.0 255.255.255.0 192.168.3.0 255.255.255.0
      local ident (addr/mask/prot/port): (192.168.1.0/255.255.255.0/0/0)
      remote ident (addr/mask/prot/port): (192.168.3.0/255.255.255.0/0/0)
      current_peer: 192.168.4.6


      #pkts encaps: 10, #pkts encrypt: 10, #pkts digest: 10
      #pkts decaps: 10, #pkts decrypt: 10, #pkts verify: 10
      #pkts compressed: 0, #pkts decompressed: 0
      #pkts not compressed: 10, #pkts comp failed: 0, #pkts decomp failed: 0
      #pre-frag successes: 0, #pre-frag failures: 0, #fragments created: 0
      #PMTUs sent: 0, #PMTUs rcvd: 0, #decapsulated frgs needing reassembly: 0
      #TFC rcvd: 0, #TFC sent: 0
```

```
    #Valid ICMP Errors rcvd: 0, #Invalid ICMP Errors rcvd: 0
    #send errors: 0, #recv errors: 0

    local crypto endpt.: 192.168.2.15/0, remote crypto endpt.: 192.168.4.6/0
    path mtu 1500, ipsec overhead 74(44), media mtu 1500
    PMTU time remaining (sec): 0, DF policy: copy-df
    ICMP error validation: disabled, TFC packets: disabled
    current outbound spi: 077D72C9
    current inbound spi : AC146DEC

  inbound esp sas:
    spi: 0xAC146DEC (2887020012)
       SA State: active
       transform: esp-aes-256 esp-sha-hmac no compression
       in use settings ={L2L, Tunnel, PFS Group 5, IKEv1, }
       slot: 0, conn_id: 143065088, crypto-map: s2sCryptoMap
       sa timing: remaining key lifetime (kB/sec): (3914999/28567)
       IV size: 16 bytes
       replay detection support: Y
       Anti replay bitmap:
        0x00000000 0x000007FF
  outbound esp sas:
    spi: 0x077D72C9 (125661897)
       SA State: active
       transform: esp-aes-256 esp-sha-hmac no compression
       in use settings ={L2L, Tunnel, PFS Group 5, IKEv1, }
       slot: 0, conn_id: 143065088, crypto-map: s2sCryptoMap
       sa timing: remaining key lifetime (kB/sec): (3914999/28567)
       IV size: 16 bytes
       replay detection support: Y
       Anti replay bitmap:
        0x00000000 0x00000001
```

단계 **3** **show isakmp sa** 명령을 사용하여 IKE 보안 연결을 확인합니다.
sa 키워드 없이 명령을 사용하거나, **stats** 키워드를 대신 사용하여 IKE 통계를 볼 수 있습니다.

예를 들어 다음 출력은 IKEv2 보안 연결을 표시합니다.

```
> show isakmp sa

There are no IKEv1 SAs

IKEv2 SAs:

Session-id:15317, Status:UP-ACTIVE, IKE count:1, CHILD count:1

Tunnel-id Local             Remote            Status   Role
592216161 192.168.2.15/500  192.168.4.6/500   READY    INITIATOR
      Encr: AES-GCM, keysize: 256, Hash: N/A, DH Grp:21, Auth sign: PSK, Auth verify: PSK
      Life/Active Time: 86400/12 sec
Child sa: local selector  192.168.1.0/0 - 192.168.1.255/65535
          remote selector 192.168.3.0/0 - 192.168.3.255/65535
          ESP spi in/out: 0x52d2f1e4/0xcd22739c
```

다음 출력은 IKEv1 보안 연결을 표시합니다.

```
> show isakmp sa

IKEv1 SAs:

   Active SA: 1
    Rekey SA: 0 (A tunnel will report 1 Active and 1 Rekey SA during rekey)
Total IKE SA: 1

1   IKE Peer: 192.168.4.6
    Type    : L2L             Role    : initiator
    Rekey   : no              State   : MM_ACTIVE

There are no IKEv2 SAs
```

사이트 대 사이트 VPN 모니터링

사이트 대 사이트 VPN 연결을 모니터링하고 트러블슈팅을 수행하려면 디바이스 CLI에 로그인하여 다음 명령을 사용합니다.

- **show ipsec sa**에는 VPN 세션(보안 연결)이 표시됩니다. **clear ipsec sa counters** 명령을 사용하여 이러한 통계를 재설정할 수 있습니다.
- **show ipsec**키워드는 IPsec 운영 데이터 및 통계를 표시합니다. 사용 가능한 키워드를 보려면 **show ipsec ?**를 입력합니다.
- **show isakmp**는 ISAKMP 운영 데이터 및 통계를 표시합니다.

IV 부

시스템 관리

12 장

시스템 설치

다음 주제에서는 시스템 설정 페이지에서 함께 그룹화되어 있는 여러 시스템 설정을 구성하는 방법을 설명합니다. 이러한 설정에는 전반적인 시스템 기능이 포함됩니다.

관리 액세스 목록 구성

기본적으로는 모든 IP 주소에서 관리 주소의 디바이스 Firepower Device Manager 웹 또는 CLI 인터페이스에 연결할 수 있습니다. 시스템 액세스는 사용자/비밀번호를 통해서만 보호됩니다. 그러나 특정 IP 주소 또는 서브넷으로부터의 연결만 허용하도록 액세스 목록을 구성하여 보호 레벨을 추가로 제공할 수 있습니다.

데이터 인터페이스를 열어 Firepower Device Manager 또는 SSH의 CLI 연결을 허용할 수도 있습니다. 그러면 관리 주소를 사용하지 않고도 디바이스를 관리할 수 있습니다. 예를 들어 디바이스를 원격으로 구성하기 위해 외부 인터페이스에 대한 관리 액세스를 허용할 수 있습니다. 사용자 이름/비밀번호를 통해 원치 않는 연결로부터 디바이스를 보호할 수 있습니다. 기본적으로 데이터 인터페이스에 대한 HTTPS 관리 액세스는 내부 인터페이스에서는 활성화되지만 외부 인터페이스에서는 비활성화됩니다. 즉, 기본 "내부" 브리지 그룹이 있는 디바이스 모델의 경우 브리지 그룹 내에 있는 모든 데이터 인터페이스를 통해 브리지 그룹 IP 주소(기본값: 192.168.1.1)에 대한 Firepower Device Manager 연결

을 설정할 수 있습니다. 디바이스에 진입하는 데 사용하는 인터페이스에서만 관리 연결을 열 수 있습니다.

주의 특정 주소에 대한 액세스를 제한하면 시스템이 잠겨 사용이 차단되기 쉽습니다. 현재 사용 중인 IP 주소에 대한 액세스 권한을 삭제하여 "모든" 주소에 대한 항목이 없으면 정책 배포 시 시스템에 액세스할 수 없게 됩니다. 따라서 액세스 목록을 구성하려는 경우 각별히 주의해야 합니다.

절차

단계 **1** 디바이스을 클릭한 다음 **System Settings(**시스템 설정**)** > **Management Access List(**관리 액세스 목록**)** 링크를 클릭합니다.
System Settings(시스템 설정) 페이지가 이미 열려 있는 경우 목차에서 **Management Access List(**관리 액세스 목록**)**를 클릭하면 됩니다.

규칙 목록에 따라 지정된 포트 액세스가 허용되는 주소가 정의됩니다. 이 포트는 Firepower Device Manager의 경우 443(HTTPS 웹 인터페이스)이고 SSH CLI의 경우 22입니다.

규칙은 순서가 지정된 목록이 아닙니다. IP 주소가 요청된 포트에 대한 어떤 규칙에든 일치하는 경우 사용자의 디바이스 로그인 시도는 허용됩니다.

참고 규칙을 삭제하려면 해당 규칙의 휴지통 아이콘( )을 클릭합니다.

단계 **2** 관리 주소에 대한 규칙을 생성하려면 다음을 수행합니다.

a) **Management Interface(**관리 인터페이스**)** 탭을 선택합니다.

b) +를 클릭하고 다음 옵션에 내용을 입력합니다.

- 프로토콜 - 규칙이 HTTPS(포트 443)용인지 아니면 SSH(포트 22)용인지를 선택합니다.
- **IP** 주소 - 시스템에 액세스할 수 있어야 하는 IPv4 또는 IPv6 네트워크나 호스트를 정의하는 네트워크 개체를 선택합니다. "임의" 주소를 지정하려면 **any-ipv4**(0.0.0.0/0) 및 **any-ipv6**(::/0)를 선택합니다.

c) **OK(**확인**)**를 클릭합니다.

단계 **3** 데이터 인터페이스에 대한 규칙을 생성하려면 다음을 수행합니다.

a) **Data Interfaces(**데이터 인터페이스**)** 탭을 선택합니다.

b) +를 클릭하고 다음 옵션에 내용을 입력합니다.

- 인터페이스 - 관리 액세스를 허용할 인터페이스를 선택합니다.
- 프로토콜 - 규칙이 HTTPS(포트 443)용인지, SSH(포트 22)용인지 아니면 둘 다에 사용할 수 있는지를 선택합니다.
- 허용된 네트워크 - 시스템에 액세스할 수 있어야 하는 IPv4 또는 IPv6 네트워크나 호스트를 정의하는 네트워크 개체를 선택합니다. "임의" 주소를 지정하려면 **any-ipv4**(0.0.0.0/0) 및 **any-ipv6**(::/0)를 선택합니다.

c) **OK(**확인**)**를 클릭합니다.

진단 로깅 구성

진단 로깅은 연결과 관련이 없는 이벤트에 대한 syslog 메시지를 제공합니다. 개별 액세스 제어 규칙 내에서 연결 로깅을 구성합니다. 다음 절차에서는 진단 메시지 로깅을 구성하는 방법을 설명합니다.

절차

단계 **1** 디바이스을 클릭한 다음 **System Settings(**시스템 설정**)** > **Logging Settings(**로깅 설정**)** 링크를 클릭합니다.
시스템 설정 페이지가 이미 열려 있는 경우 목차에서 로깅 설정을 클릭하면 됩니다.

단계 **2** **Diagnostic Log Settings(**진단 로그 설정**)** > **On(**켜기**)**을 클릭합니다.
이 페이지에서 나머지 필드를 구성하더라도 이 설정을 켜지 않으면 진단 로그 메시지는 생성되지 않습니다.

단계 **3** 진단 로그 메시지를 확인하려는 각 위치에 대해 슬라이더를 **On(**켜기**)**으로 이동하고 최소 심각도 레벨을 선택합니다.
다음 위치에서 메시지를 로깅할 수 있습니다.

- 콘솔 - 콘솔 포트에서 CLI에 로그인하면 이러한 메시지가 표시됩니다. **show console-output** 명령을 사용하면 다른 인터페이스에 대한 SSH 세션에서도 이러한 로그를 확인할 수 있습니다(관리 주소 포함).
- **Syslog** - 이러한 메시지는 지정한 외부 syslog 서버로 전송됩니다. +를 클릭하고 syslog 서버 개체를 선택한 다음 팝업 대화 상자에서 **OK(**확인**)**를 클릭합니다. 서버의 개체가 아직 없으면 **Syslog** 서버 추가를 클릭하여 개체를 생성합니다.

단계 **4** **Save(**저장**)**를 클릭합니다.

Severity Levels(심각도 레벨)

다음 표에서는 syslog 메시지 심각도 레벨을 보여줍니다.

표 ***5: Syslog*** 메시지 심각도 레벨

레벨 번호	심각도 수준	설명
0	**emergencies(**비상**)**	시스템을 사용할 수 없습니다.
1	**Alert(**긴급 경고**)**	즉각적인 행동이 필요합니다.

레벨 번호	심각도 수준	설명
2	**critical(**심각**)**	심각한 상태입니다.
3	**error(**오류**)**	오류 상태입니다.
4	**warning(**경고**)**	경고 상태입니다.
5	**notification(**알림**)**	일반적이지만 중요한 상태입니다.
6	**informational(**정보**)**	정보 메시지만 해당됩니다.
7	**debugging(**디버깅**)**	디버깅 메시지만 해당됩니다.

참고 Firepower Threat Defense에서는 심각도 레벨이 0(응급)인 syslog 메시지를 생성하지 않습니다.

DHCP 서버 구성

DHCP 서버는 IP 주소와 같은 네트워크 컨피그레이션 파라미터를 DHCP 클라이언트에 제공합니다. 연결된 네트워크의 DHCP 클라이언트에 컨피그레이션 파라미터를 제공하기 위해 인터페이스에서 DHCP 서버를 구성할 수 있습니다.

IPv4 DHCP 클라이언트는 서버와 연결하는 데 멀티캐스트 주소가 아닌 브로드캐스트를 사용합니다. DHCP 클라이언트는 UDP 포트 68에서 메시지를 수신합니다. DHCP 서버는 UDP 포트 67에서 메시지를 수신합니다. DHCP 서버는 BOOTP 요청을 지원하지 않습니다.

DHCP 클라이언트는 서버를 사용하는 인터페이스와 같은 네트워크에 있어야 합니다. 즉, 서버와 클라이언트 사이에 스위치는 있을 수 있지만 개입하는 라우터가 있어서는 안 됩니다.

참고 이미 DHCP 서버가 작동 중인 네트워크에서는 DHCP 서버를 구성하지 마십시오. 이렇게 하면 두 서버가 충돌하여 예측할 수 없는 결과가 발생합니다.

절차

단계 **1** **Device(**디바이스**)**를 클릭한 다음 **System Settings(**시스템 설정**)** > **DHCP Server(DHCP** 서버**)** 링크를 클릭합니다.
시스템 설정 페이지가 이미 열려 있는 경우 목차에서 **DHCP Server(DHCP** 서버**)**를 클릭하면 됩니다.

이 페이지에는 2개의 탭이 있습니다. 먼저 **Configuration(**컨피그레이션**)** 탭에는 글로벌 파라미터가 표시됩니다.

DHCP Servers(DHCP 서버**)** 탭에는 DHCP 서버를 구성한 인터페이스, 서버 사용 여부 및 서버의 주소 풀이 표시됩니다.

단계 **2** **Configuration(**컨피그레이션**)** 탭에서 자동 컨피그레이션 및 글로벌 설정을 구성합니다.
DHCP 자동 컨피그레이션은 DHCP 서버가 지정된 인터페이스에서 실행 중인 어떤 DHCP 클라이언트로부터 얻은 DNS 서버, 도메인 이름, WINS 서버 정보를 DHCP 클라이언트에 제공할 수 있게 합니다. 일반적으로는 외부 인터페이스의 DHCP를 사용하여 주소를 가져오는 경우 자동 컨피그레이션을 사용하지만, DHCP를 통해 주소를 가져오는 모든 인터페이스를 선택할 수 있습니다. 자동 컨피그레이션을 사용할 수 없는 경우에는 필요한 옵션을 수동으로 정의할 수 있습니다.

a) 자동 컨피그레이션을 사용하려면 **Enable Auto Configuration(**자동 컨피그레이션 사용**)** > **On(**켜기**)**을 클릭(슬라이더가 오른쪽에 있어야 함)한 다음 인터페이스에서에서 DHCP를 통해 주소를 가져오는 인터페이스를 선택합니다.

b) 자동 컨피그레이션을 사용하지 않거나 자동으로 구성된 설정을 재정의하려는 경우 다음의 글로벌 옵션을 구성합니다. 이러한 설정은 DHCP 서버를 호스팅하는 모든 인터페이스의 DHCP 클라이언트에 전송됩니다.

- **1**차 **WINS IP** 주소, **2**차 **WINS IP** 주소 - 클라이언트가 NetBIOS 이름 확인에 사용해야 하는 WINS(Windows 인터넷 이름 서비스) 서버의 주소입니다.
- **1**차 **DNS IP** 주소, **2**차 **DNs IP** 주소 - 클라이언트가 도메인 이름 확인에 사용해야 하는 DNS(Domain Name System) 서버의 주소입니다. OpenDNS 공개 DNS 서버를 구성하려면 **OpenDNS** 사용을 클릭합니다. 버튼을 클릭하면 필드에 적절한 IP 주소가 로드됩니다.

c) **Save(**저장**)**를 클릭합니다.

단계 **3** **DHCP Servers(DHCP** 서버**)** 탭을 클릭하고 서버를 구성합니다.

a) 다음 중 하나를 수행합니다.

- 이미 나열되어 있지 않은 인터페이스에 대해 DHCP 서버를 구성하려면 +를 클릭합니다.
- 기존 DHCP 서버를 수정하려면 해당 서버의 수정 아이콘( )을 클릭합니다.

서버를 삭제하려면 해당 서버의 휴지통 아이콘( )을 클릭합니다.

b) 서버 속성을 구성합니다.

- **DHCP** 서버 사용 - 서버를 사용할지를 선택합니다. 서버를 구성하되 사용할 준비가 될 때까지 비활성화해 둘 수 있습니다.
- 인터페이스 - 클라이언트에 DHCP 주소를 제공할 인터페이스를 선택합니다. 이 인터페이스에는 고정 IP 주소가 있어야 합니다. 인터페이스에서 DHCP 서버를 실행하려는 경우 DHCP를 사용하여 인터페이스 주소를 가져올 수는 없습니다. 브리지 그룹의 경우 구성원 인터페이스가 아닌 BVI(브리지 가상 인터페이스)에서 DHCP 서버를 구성합니다. 그러면 서버가 모든 구성원 인터페이스에서 작동합니다.

  진단 인터페이스에서는 DHCP 서버를 구성할 수 없습니다. 대신 **Device(**디바이스**)** > **System Settings(**시스템 설정**)** > **Management Interface(**관리 인터페이스**)** 페이지를 통해 관리 인터페이스에서 DHCP 서버를 구성합니다.

- 주소 풀 - 서버가 주소를 요청하는 클라이언트에 제공할 수 있는 IP 주소의 범위(최저 범위에서 최고 범위 순서)입니다. 이 IP 주소 범위는 선택된 인터페이스와 동일한 서브넷에 있어야 하며, 인터페이스 자체의 IP 주소, 브로드캐스트 주소 또는 서브넷 네트워크 주소는 포함할 수 없습니다. 풀의 시작 주소와 끝 주소를 하이픈으로 구분하여 지정합니다. 예를 들면 10.100.10.12-10.100.10.250과 같이 지정합니다.

c) **OK(**확인**)**를 클릭합니다.

DNS 구성

DNS(Domain Name System) 서버는 호스트 이름을 IP 주소로 확인하는 데 사용됩니다. 이러한 서버는 관리 인터페이스에서 사용됩니다. DNS 서버는 초기 시스템 설정 시 구성하지만 다음 절차를 통해 변경할 수 있습니다.

configure network dns servers 및 **configure network dns searchdomains** 명령을 사용하여 CLI에서 DNS 컨피그레이션을 변경할 수도 있습니다.

절차

단계 **1** 디바이스을 클릭한 다음 **System Settings(**시스템 설정**)** > **DNS Server(DNS** 서버**)** 링크를 클릭합니다.
시스템 설정 페이지가 이미 열려 있는 경우 목차에서 **DNS Server(DNS** 서버**)**를 클릭하면 됩니다.

단계 **2** **1**차**, 2**차**, 3**차 **DNS IP** 주소에 최대 3개 DNS 서버의 IP 주소를 선호하는 순서대로 입력합니다.
연결할 수 없는 경우를 제외하면 1차 DNS 서버가 사용됩니다. 이 서버에 연결할 수 없으면 2차 서버에 연결을 시도하며, 마지막으로 3차 서버에 연결을 시도합니다.

OpenDNS 공개 DNS 서버를 구성하려면 **Use OpenDNS(OpenDNS** 사용**)**를 클릭합니다. 버튼을 클릭하면 필드에 적절한 IP 주소가 로드됩니다.

단계 **3** 도메인 검색 이름에서 example.com과 같은 네트워크의 도메인 이름을 입력합니다.
이 도메인은 정규화되지 않은 호스트 이름(예: serverA.example.com이 아닌 serverA)에 추가됩니다.

단계 **4** **Save(**저장**)**를 클릭합니다.

관리 인터페이스 구성

관리 인터페이스는 물리적 관리 포트에 연결된 가상 인터페이스입니다. 물리적 포트는 이름이 진단 인터페이스이며, 다른 물리적 포트와 함께 인터페이스 페이지에서 구성할 수 있습니다.

관리 인터페이스는 다음과 같은 두 가지 용도로 사용됩니다.

- IP 주소에 대한 웹 및 SSH 연결을 열고 인터페이스를 통해 디바이스를 구성할 수 있습니다.

- 시스템은 이 IP 주소를 통해 스마트 라이선싱 및 데이터베이스 업데이트를 가져옵니다.

CLI 설정 마법사를 사용하는 경우 초기 시스템 컨피그레이션 중에 디바이스의 관리 주소 및 게이트웨이를 구성합니다. Firepower Device Manager 설정 마법사를 사용하는 경우에는 관리 주소와 게이트웨이가 기본값으로 유지됩니다.

필요한 경우 Firepower Device Manager를 통해 이러한 주소를 변경할 수 있습니다. **configure network ipv4 manual** 및 **configure network ipv6 manual** 명령을 사용하여 CLI에서 관리 주소 및 게이트웨이를 변경할 수도 있습니다.

고정 주소를 정의할 수도 있고, 관리 네트워크의 다른 디바이스가 DHCP 서버로 작동하는 경우에는 DHCP를 통해 주소를 가져올 수 있습니다. 기본적으로, 관리 주소는 고정 주소이며 DHCP 서버는 포트에서 실행됩니다. 따라서 관리 포트에 디바이스를 직접 연결하여 워크스테이션의 DHCP 주소를 가져올 수 있습니다. 이렇게 하면 디바이스를 쉽게 연결하고 구성할 수 있습니다.

주의 현재 연결된 주소를 변경할 경우 변경 사항을 저장하면 즉시 적용되므로 Firepower Device Manager 또는 CLI에 액세스할 수 없게 됩니다. 디바이스와 다시 연결해야 합니다. 관리 네트워크에서 새 주소가 유효하며 사용 가능한지 확인합니다.

절차

단계 **1** **Device(**디바이스**)**를 클릭한 후 **System Settings(**시스템 설정**)** > **Management Interface(**관리 인터페이스**)** 링크를 클릭합니다.
시스템 설정 페이지가 이미 열려 있는 경우 목차에서 **Management Interface(**관리 인터페이스**)**를 클릭하면 됩니다.

단계 **2** 관리 게이트웨이를 정의할 방법을 선택합니다.
게이트웨이는 시스템에서 스마트 라이선스 및 데이터베이스 업데이트(VDB, 규칙, 지리위치, URL 등)를 받고 관리 DNS 및 NTP 서버에 접속하기 위해 인터넷에 연결할 수 있는 방법을 결정합니다. 다음 옵션 중에서 선택합니다.

- 데이터 인터페이스를 게이트웨이로 사용합니다**.** - 별도의 관리 네트워크가 물리적 관리 인터페이스에 연결되지 않은 경우 이 옵션을 선택합니다. 라우팅 테이블에 따라 트래픽이 인터넷에 라우팅되며, 대개 외부 인터페이스를 거칩니다. 이것이 기본 옵션입니다.
- 관리 인터페이스에 고유 게이트웨이를 사용합니다**.** - 별도의 관리 네트워크가 관리 인터페이스에 연결된 경우 IPv4 및 IPv6를 위한 고유 게이트웨이(아래)를 지정합니다.

단계 **3** IPv4, IPv6 중 하나 또는 둘 다의 관리 주소, 서브넷 마스크 또는 IPv6 접두사 및 게이트웨이(필요한 경우)를 구성합니다.
속성 집합을 하나 이상 구성해야 합니다. 특정 집합의 주소 지정 방법을 비활성화하려면 해당 집합을 비워 둡니다.

Type(유형**)** > **DHCP**를 선택하여 DHCP 또는 IPv6 자동 컨피그레이션을 통해 주소와 게이트웨이를 가져옵니다. 그러나 데이터 인터페이스를 게이트웨이로 사용하는 경우에는 DHCP를 사용할 수 없습니다. 이 경우에는 고정 주소를 사용해야 합니다.

단계 **4** (선택 사항). 고정 IPv4 주소를 구성하는 경우 포트에서 DHCP 서버를 구성합니다.
관리 포트에서 DHCP 서버를 구성하는 경우 직접 연결된 클라이언트 또는 관리 네트워크의 클라이언트가 DHCP 풀에서 주소를 가져올 수 있습니다.

a) **Enable DHCP Server(DHCP** 서버 활성화**)** > **On(**켜기**)**을 클릭합니다.
b) 서버의 주소 풀을 입력합니다.
주소 풀은 서버가 주소를 요청하는 클라이언트에 제공할 수 있는 IP 주소의 범위(최저 범위에서 최고 범위 순서)입니다. 이 IP 주소 범위는 관리 주소와 동일한 서브넷에 있어야 하며, 인터페이스 자체의 IP 주소, 브로드캐스트 주소 또는 서브넷 네트워크 주소는 포함할 수 없습니다. 풀의 시작 주소와 끝 주소를 하이픈으로 구분하여 지정합니다. 예를 들면 192.168.45.46-192.168.45.254와 같이 지정합니다.

단계 **5** **Save(**저장**)**를 클릭하고 경고를 확인한 후에 **OK(**확인**)**를 클릭합니다.

디바이스 호스트 이름 구성

디바이스 호스트 이름을 변경할 수 있습니다.

또한, **configure network hostname** 명령을 사용하여 CLI에서 호스트 이름을 변경할 수도 있습니다.

⚠

주의 호스트 이름을 사용하여 시스템에 연결할 때 호스트 이름을 변경하는 경우 변경 사항을 저장하면 즉시 적용되므로 Firepower Device Manager에 액세스할 수 없게 됩니다. 디바이스와 다시 연결해야 합니다.

절차

단계 **1** 디바이스을 클릭한 다음 **System Settings(**시스템 설정**)** > **Hostname(**호스트 이름**)** 링크를 클릭합니다.
시스템 설정 페이지가 이미 열려 있는 경우 목차에서 호스트 이름을 클릭하면 됩니다.

단계 **2** 새 호스트 이름을 입력합니다.

단계 **3** **Save(**저장**)**를 클릭하고 경고를 확인한 후에 **Proceed(**진행**)**를 클릭합니다.

NTP(Network Time Protocol) 구성

시스템에서 시간을 정의하려면 NTP(Network Time Protocol) 서버를 구성해야 합니다. NTP 서버는 초기 시스템 설정 시 구성하지만, 다음 절차를 통해 변경할 수 있습니다. NTP 연결에 문제가 있는 경우, NTP 트러블슈팅, 312 페이지를 참조하십시오.

절차

단계 **1** 디바이스을 클릭한 다음 **System Settings(**시스템 설정**)** > **NTP** 링크를 클릭합니다.
시스템 설정 페이지가 이미 열려 있는 경우 목차에서 **NTP**를 클릭하면 됩니다.

단계 **2** **NTP** 시간 서버에서 자체(수동) 시간 서버를 사용할지 아니면 Cisco 시간 서버를 사용할지를 선택합니다.

- 기본 **NTP** 시간 서버 - 이 옵션을 선택하는 경우 서버 목록에는 NTP에 사용되는 서버 이름이 표시됩니다.
- 수동 입력 - 이 옵션을 선택하는 경우 사용하려는 NTP 서버의 IP 주소 또는 FQDN(Fully-Qualified Domain Name)을 입력합니다. 예를 들어 ntp1.example.com 또는 10.100.10.10을 입력합니다. NTP 서버가 둘 이상인 경우 다른 **NTP** 시간 서버 추가를 클릭하고 주소를 입력합니다.

단계 **3** **Save(**저장**)**를 클릭합니다.

Cisco CSI용 URL 필터링 환경 설정 구성

시스템은 평판, 위험 및 위협 인텔리전스에 Cisco CSI(Collective Security Intelligence)를 사용합니다.

URL 필터링 및 AMP for Firepower에 필요한 라이선스(악성코드 파일 정책에 사용됨)가 있는 경우 시스템은 해당 기능을 자동으로 활성화하며 Cisco CSI에서 필요한 정보를 검색하기 위한 통신을 활성화합니다. 그러나 통신을 제어하기 위해 몇 가지 옵션을 구성할 수 있습니다.

절차

단계 **1** 디바이스을 클릭한 다음 **System Settings(**시스템 설정**)** > **URL Filtering Preferences(URL** 필터링 환경 설정**)** 링크를 클릭합니다
시스템 설정 페이지가 이미 열려 있는 경우 목차에서 **URL** 필터링 기본 설정을 클릭하면 됩니다.

단계 **2** 다음 옵션을 구성합니다.

- 자동 업데이트 사용 - 시스템이 업데이트된 URL 데이터를 자동으로 확인하고 다운로드할 수 있도록 합니다. 이 데이터에는 범주 및 평판 정보가 포함됩니다. 시스템은 30분마다 업데이트를 확인하지만, 데이터는 대개 매일 한 번씩 업데이트됩니다. 기본적으로는 업데이트가 활성화됩니다. 이 옵션을 선택 취소하는 경우 범주 및 평판 필터링을 사용 중이라면 자동 업데이트를 주기적으로 사용하여 새 URL 데이터를 가져옵니다.
- **Cisco CSI**에서 알 수 없는 **URL** 쿼리 - 로컬 URL 필터링 데이터베이스에 범주 및 평판 데이터가 없는 URL에 대해 Cisco CSI에 업데이트된 정보를 확인할지를 선택합니다. 조회에서 적절한 시

간제한 이내에 이 정보가 반환되면 URL 조건을 기준으로 액세스 규칙을 선택할 때 해당 정보가 사용됩니다. 그렇지 않으면 URL은 미분류 범주와 일치합니다.

단계 **3** **Save(**저장**)**를 클릭합니다.

클라우드 관리 구성

Cisco Defense Orchestrator 클라우드 기반 포털을 사용하여 디바이스를 관리할 수 있습니다. Cisco Defense Orchestrator를 사용하면 다음 기술을 통해 디바이스 관리에 접근할 수 있습니다.

- 초기 컨피그레이션 다운로드 - 이 방식을 사용하는 경우 Cisco Defense Orchestrator에서 초기 디바이스 컨피그레이션을 다운로드하지만 그 후에는 Firepower Device Manager를 사용하여 로컬로 디바이스를 구성합니다.

  참고 Firepower Device Manager를 사용하여 디바이스를 구성한 후 대신 클라우드를 통해 디바이스를 관리하려는 경우에는 클라우드 기반 컨피그레이션에서 로컬 변경 사항을 복제해야 합니다.

- 클라우드를 통해 원격 컨피그레이션 관리 - 이 방식을 사용하는 경우에는 Cisco Defense Orchestrator를 사용하여 디바이스 컨피그레이션을 생성하고 업데이트합니다. 이 방식을 사용할 때는 컨피그레이션을 로컬에서 변경하지 마십시오. 각 클라우드 구축에서는 클라우드에 정의된 컨피그레이션이 디바이스의 로컬 컨피그레이션을 대체하기 때문입니다. 로컬 변경을 수행하는 경우 변경 사항을 보존하려면 클라우드 기반 컨피그레이션에서도 컨피그레이션을 반복해야 합니다.

클라우드 관리 방식에 대한 자세한 내용을 확인하려면 Cisco Defense Orchestrator 포털(http://www.cisco.com/go/cdo)을 참조하거나 서비스를 받고 있는 리셀러 또는 파트너에게 문의하십시오.

시작하기 전에

Cisco Defense Orchestrator용 등록 키를 받습니다.

디바이스에 인터넷으로 연결되는 경로가 있는지도 확인합니다.

절차

단계 **1** **Device(**디바이스**)**를 클릭한 다음 **System Settings(**시스템 설정**)** > **Cloud Management(**클라우드 관리**)** 링크를 클릭합니다.
시스템 설정 페이지가 이미 열려 있는 경우 목차에서 **Cloud Management(**클라우드 관리**)**를 클릭하면 됩니다.

단계 **2** **Get Started(**시작하기**)**를 클릭합니다.

단계 **3** **Registration Key(**등록 키**)**에 키를 붙여넣고 **Connect(**연결**)**를 클릭합니다.

등록 요청이 클라우드 포털로 전송됩니다. 키가 유효하며 인터넷으로 연결되는 경로가 있으면 디바이스가 포털에 정상적으로 등록됩니다. 그러면 포털을 사용하여 디바이스 관리를 시작할 수 있습니다.

클라우드 관리를 더 이상 사용하지 않으려는 경우 기어 드롭다운 목록에서 **Unregister(**등록 취소**)**를 선택하면 됩니다.

13 장

시스템 관리

다음 주제에서는 시스템 데이터베이스 업데이트, 시스템 백업 및 복원 등의 시스템 관리 작업을 수행하는 방법을 설명합니다.

소프트웨어 업데이트 설치

시스템 데이터베이스 및 시스템 소프트웨어에 업데이트를 설치할 수 있습니다. 다음 주제에서는 이러한 업데이트를 설치하는 방법을 설명합니다.

시스템 데이터베이스 업데이트

시스템은 여러 가지 데이터베이스 를 사용하여 고급 서비스를 제공합니다. Cisco에서는 보안 정책에서 최신 정보를 사용할 수 있도록 이러한 데이터베이스 에 대한 업데이트를 제공합니다.

시스템 데이터베이스 업데이트 개요

Firepower Threat Defense는 다음 데이터베이스 를 사용하여 고급 서비스를 제공합니다.

침입 규칙

새로운 취약점이 확인되면 Cisco Talos(Talos Security Intelligence and Research Group)에서는 가져올 수 있는 침입 규칙 업데이트를 제공합니다. 이러한 업데이트는 침입 규칙, 전처리기 규칙 및 규칙을 사용하는 정책에 영향을 줍니다.

침입 규칙은 업데이트된 새로운 침입 규칙과 전처리기 규칙, 기존 규칙의 수정된 상태, 수정된 기본 침입 정책 설정을 제공합니다. 규칙 업데이트는 또한 규칙을 삭제하고, 새로운 규칙 카테고리와 기본 변수를 제공하며, 기본 변수 값을 변경할 수 있습니다.

침입 규칙 업데이트를 통해 수행된 변경 사항을 적용하려면 컨피그레이션을 재구축해야 합니다.

침입 규칙 업데이트는 규모가 클 수 있으므로 네트워크 이용률이 낮은 시간 동안 규칙을 가져오십시오.

GeoDB(지리위치 데이터베이스**)**

Cisco GeoDB(Geolocation Database, 지리위치 데이터베이스)는 라우팅 가능한 IP 주소와 관련된 지리 데이터(국가, 도시, 좌표 등) 및 연결 관련 데이터(인터넷 서비스 공급자, 도메인 이름, 연결 유형 등)의 데이터베이스입니다.

GeoDB 업데이트는 물리적 위치, 연결 유형 등의 업데이트된 정보를 제공하여 시스템이 라우팅 가능한 탐지된 IP 주소에 연결할 수 있습니다. 위치 정보 데이터를 액세스 제어 규칙의 조건으로 사용할 수 있습니다.

GeoDB 업데이트에 필요한 시간은 어플라이언스에 따라 다릅니다. 설치하는 데 일반적으로 30~40분이 소요됩니다. GeoDB 업데이트가 다른 시스템 기능(위치 정보의 지속적 수집을 포함하는)을 중단하지 않지만, 업데이트를 완료하는 동안 시스템 리소스를 소모합니다. 업데이트를 예약하는 경우 이를 고려하십시오.

VDB(Vulnerability Database)

Cisco VDB(Vulnerability Database)는 호스트가 영향을 받기 쉬운 알려진 취약점의 데이터베이스인 동시에 운영 체제, 클라이언트 및 애플리케이션의 지문이기도 합니다. Firepower System은 지문과 취약점의 상관관계를 지정하므로, 특정 호스트가 네트워크 보안 침해 위험을 증가시키는지를 쉽게 확인할 수 있습니다. Cisco Talos(Security Intelligence and Research Group)는 VDB 정기 업데이트를 제공합니다.

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.

VDB를 업데이트한 후에는 컨피그레이션을 재구축해야 업데이트된 애플리케이션 탐지기 및 운영 체제 지문을 적용할 수 있습니다.

시스템 데이터베이스 업데이트

편의상 시스템 데이터베이스 업데이트를 수동으로 검색하여 적용할 수 있습니다. Cisco 지원 사이트에서 업데이트를 검색합니다. 따라서 시스템 관리 주소에서 인터넷으로 이동하는 경로가 있어야 합니다.

데이터베이스 업데이트를 검색하고 적용하는 정기적인 일정을 설정할 수도 있습니다. 이러한 업데이트는 크기가 클 수 있으므로 네트워크 활동이 적은 시간에 예약합니다.

참고 데이터베이스 업데이트가 진행 중인 동안에는 사용자 인터페이스가 작업에 응답하는 속도가 느려질 수 있습니다.

시작하기 전에

보류 중인 변경 사항에 영향을 줄 가능성을 방지하려면 이러한 데이터베이스를 수동으로 업데이트하기 전에 컨피그레이션을 디바이스에 구축합니다.

절차

단계 **1** 디바이스을 클릭한 다음 업데이트 Updates(업데이트) 요약에서 **View Configuration(**컨피그레이션 보기**)**을 클릭합니다.
그러면 업데이트 페이지가 열립니다. 페이지의 정보에는 각 데이터베이스의 현재 버전과 각 데이터베이스가 업데이트된 마지막 날짜 및 시간이 표시됩니다.

단계 **2** 수동으로 데이터베이스를 업데이트하려면 해당 데이터베이스의 섹션에서 **Update Now(**지금 업데이트**)**를 클릭합니다.
업데이트를 다운로드 및 적용하고 나면 시스템이 업데이트된 정보를 사용할 수 있도록 정책이 디바이스에 자동으로 재구축됩니다.

단계 **3** (선택 사항) 정기적인 데이터베이스 업데이트 일정을 설정하려면 다음을 수행합니다.

a) 원하는 데이터베이스의 섹션에서 **Configure(**구성**)** 링크를 클릭합니다. 일정이 이미 있는 경우 **Edit(**수정**)**을 클릭합니다.
데이터베이스의 업데이트 일정은 별개이므로 별도로 일정을 정의해야 합니다.

b) 업데이트 시작 시간을 설정합니다.

- 업데이트 빈도(매일, 매주, 매월)
- 매주 또는 매월의 경우 업데이트를 수행할 요일이나 날짜
- 업데이트를 시작할 시간

c) **Save(**저장**)**를 클릭합니다.

참고 반복 예약을 제거하려면 **Edit(**수정**)** 링크를 클릭하여 예약 대화 상자를 연 다음 **Remove(**제거**)** 버튼을 클릭합니다.

Firepower Threat Defense 소프트웨어 업그레이드

Firepower Threat Defense 소프트웨어 업그레이드는 사용 가능해지면 설치할 수 있습니다. 다음 절차에서는 시스템이 Firepower Threat Defense 버전 6.2.0 이상을 이미 실행 중이며 정상적으로 작동 중이라고 가정합니다.

업그레이드에는 핫픽스, 간단한 업그레이드 및 주요 업그레이드의 세 가지 유형이 있습니다. 핫픽스 업그레이드 시에는 시스템 재부팅이 필요하지 않을 수도 있지만 간단한 업그레이드 및 주요 버전 업그레이드 시에는 재부팅이 필요합니다. 재부팅이 필요하면 설치 후에 시스템이 자동으로 재부팅됩니다. 업데이트를 설치할 때는 트래픽이 중단될 수 있으므로 시스템 사용량이 적을 때 설치를 수행하십시오.

이 절차를 통해 디바이스를 재이미징하거나 ASA 소프트웨어에서 Firepower Threat Defense 소프트웨어로 마이그레이션할 수는 없습니다.

참고 업데이트를 설치하기 전에 보류 중인 모든 변경 사항을 구축해야 합니다. 또한 백업을 실행하고 백업 복사본을 다운로드해야 합니다.

시작하기 전에

Cisco.com에 로그인하여 업그레이드 이미지를 다운로드합니다.

- 파일 유형이 .sh인 적절한 업그레이드 파일을 다운로드해야 합니다. 시스템 소프트웨어 패키지 또는 부트 이미지를 다운로드하지 마십시오.
- 업그레이드에 필요한 베이스라인 이미지를 실행 중인지 확인합니다. 호환성 정보는 *Cisco Firepower* 호환성 가이드 http://www.cisco.com/c/en/us/td/docs/security/firepower/compatibility/firepower-compatibility.html을 참조하십시오.
- 새 버전의 릴리스 노트를 확인합니다. 릴리스 노트는 http://www.cisco.com/c/en/us/support/security/firepower-ngfw/products-release-notes-list.html에서 확인할 수 있습니다.

절차

단계 **1** **Device(**디바이스**)**를 선택한 다음 업데이트 요약에서 **View Configuration(**컨피그레이션 보기**)**을 클릭합니다.
시스템 업그레이드 섹션에는 현재 실행 중인 소프트웨어 버전과 이미 업로드한 업데이트가 표시됩니다.

단계 **2** 업그레이드 파일을 업로드합니다.

- 업그레이드 파일을 아직 업로드하지 않은 경우 **Browse(**찾아보기**)**를 클릭하고 파일을 선택합니다.
- 업로드한 파일이 이미 있지만 다른 파일을 업로드하려는 경우에는 **Upload Another File(**다른 파일 업로드**)** 링크를 클릭합니다. 파일은 하나만 업로드할 수 있습니다. 새 파일을 업로드하면 이전 파일이 교체됩니다.

- 파일을 제거하려면 삭제 아이콘( )을 클릭합니다.

단계 **3** **Install**(설치)을 클릭하여 설치 프로세스를 시작합니다.
아이콘 옆의 정보는 디바이스가 설치 중에 재부팅되는지 여부를 나타냅니다. 디바이스가 재부팅되면 시스템에서 자동으로 로그아웃됩니다. 설치에는 30분 이상 소요될 수 있습니다.

이 시간 동안 기다렸다가 시스템에 다시 로그인하십시오. 디바이스 요약 또는 시스템 모니터링 대시보드에 새 버전이 표시됩니다.

문제가 발생하면 설치 로그를 확인할 수 있습니다. 로그 파일은 /var/log/업그레이드 파일 이름 폴더에 보관됩니다. 여기서 폴더 이름은 빌드 번호가 없는 업그레이드 파일 이름입니다. 확인하면 가장 유용한 로그 파일은 **main_upgrade_script.log**입니다. 로그를 확인하려면 디바이스 CLI에서 **system support view-logs** 명령을 사용합니다. 설치 시에 장애가 발생하여 업그레이드를 다시 설치해도 문제를 해결할 수 없으면 Cisco 기술 지원에 문의하십시오.

단계 **4** (선택 사항). 시스템 데이터베이스를 업데이트합니다.
지리위치, 규칙 및 VDB(Vulnerability Database)에 대해 자동 업데이트 작업을 구성하지 않으면 지금 이러한 항목을 업데이트하는 것이 좋습니다.

디바이스 재이미징

디바이스를 재이미징할 때는 디바이스 컨피그레이션을 없애고 새 소프트웨어 이미지를 설치합니다. 재이미징은 공장 기본 컨피그레이션을 사용하여 소프트웨어를 새로 설치하기 위한 작업입니다.

다음과 같은 상황에서 디바이스를 재이미징합니다.

- 시스템을 ASA 소프트웨어에서 Firepower Threat Defense 소프트웨어로 변환하려는 경우. ASA 이미지를 실행하는 디바이스를 Firepower Threat Defense 이미지를 실행하는 디바이스로 업그레이드할 수는 없습니다.
- 디바이스에서 6.1.0 이전 이미지를 실행 중이며 Firepower Device Manager를 사용하여 6.1 이상 이미지로 업그레이드하고 디바이스를 구성하려는 경우. Firepower Management Center를 사용하여 6.1 이전 디바이스를 업그레이드한 다음 로컬 관리로 전환할 수는 없습니다.
- 디바이스가 정상적으로 작동하지 않으며 모든 컨피그레이션을 수정하려는 시도에 실패한 경우

디바이스를 재이미징하는 방법에 대한 자세한 내용은 사용 중인 디바이스 모델의 *Cisco ASA* 또는 *Firepower Threat Defense* 디바이스 재이미징 또는 *Firepower Threat Defense* 빠른 시작 가이드를 참조하십시오. 이러한 가이드는 http://www.cisco.com/c/en/us/support/security/firepower-ngfw/products-installation-guides-list.html에서 확인할 수 있습니다.

시스템 백업 및 복원

잘못된 후속 컨피그레이션 또는 물리적 사고로 인해 컨피그레이션이 손상되는 경우 디바이스를 복원할 수 있도록 시스템 컨피그레이션을 백업할 수 있습니다.

두 디바이스가 동일한 모델이며 소프트웨어의 동일한 버전을 실행하는 경우에만 교체 디바이스에 백업을 복원할 수 있습니다. 백업 및 복원 프로세스를 사용하여 어플라이언스 간에 컨피그레이션을 복사하지 마십시오. 백업 파일은 어플라이언스를 고유하게 식별하는 정보를 포함하므로 이러한 방식을 통해 공유할 수 없습니다.

참고 백업에는 관리 IP 주소 컨피그레이션이 포함되지 않습니다. 따라서 백업 파일을 복원할 때는 관리 주소가 백업 복사본에서 대체되지 않습니다. 이로 인해 주소에 대해 수행하는 변경 사항이 유지되며, 다른 네트워크 세그먼트의 다른 디바이스에서도 컨피그레이션을 복원할 수도 있습니다.

백업은 컨피그레이션만 포함하며 시스템 소프트웨어는 포함하지 않습니다. 디바이스를 재이미징해야 하는 경우에는 소프트웨어를 다시 설치해야 하며, 그 이후에 백업을 업로드하고 컨피그레이션을 복구할 수 있습니다.

컨피그레이션 데이터베이스는 백업하는 동안 잠겨 있습니다. 백업 중에는 정책, 대시보드 등을 볼 수는 있지만 컨피그레이션을 변경할 수는 없습니다. 복원 중에는 시스템을 완전히 사용할 수 없게 됩니다.

백업 및 복원 페이지의 표에는 시스템에서 사용 가능한 모든 기존 백업 복사본과 백업의 파일 이름, 백업이 생성된 날짜와 시간 및 파일 크기가 나열됩니다. 백업의 유형(수동, 예약, 반복)은 해당 백업 복사본을 생성하도록 시스템에 명령한 방법을 기준으로 합니다.

팁 백업 복사본은 시스템 자체에 생성됩니다. 수동으로 백업 복사본을 다운로드하여 안전한 서버에 저장해야 재해 복구에 필요한 백업 복사본을 사용할 수 있습니다.

다음 항목에서는 백업 및 복원 작업을 관리하는 방법을 설명합니다.

시스템 즉시 백업

언제든지 원할 때 백업을 시작할 수 있습니다.

절차

단계 **1** 디바이스을 클릭한 다음 Backup and Restore(백업 및 복원) 요약에서 **View Configuration(**컨피그레이션 보기**)**을 클릭합니다.
그러면 백업 및 복원 페이지가 열립니다. 테이블에는 시스템에서 사용 가능한 모든 기존 백업 복사본이 나열됩니다.

단계 **2** **Manual Backup(**수동 백업**)** > **Back Up Now(**지금 백업**)**를 클릭합니다.

단계 **3** 백업의 이름과 설명(선택 사항)을 입력합니다.
백업을 즉시 수행하지 않고 나중에 수행하려는 경우에는 **Schedule(**일정**)**을 대신 클릭하면 됩니다.

단계 **4** **Back Up Now(**지금 백업**)**를 클릭합니다.
시스템에서 백업 프로세스를 시작합니다. 백업이 완료되면 백업 파일이 테이블에 표시됩니다. 그러면 백업 복사본을 시스템에 다운로드하고 원하는 경우 다른 위치에 저장할 수 있습니다.

백업을 시작한 후에는 백업 및 복원 페이지에서 나가도 됩니다.

예약한 시간에 시스템 백업

예약 백업을 설정하여 향후의 특정 날짜와 시간에 시스템을 백업할 수 있습니다. 예약 백업은 한 번만 수행됩니다. 정기적으로 백업을 생성하는 백업 일정을 생성하려면 예약 백업 대신 반복 백업을 구성합니다.

참고 이후 백업 일정을 삭제하려면 일정을 수정하고 **Remove(**제거**)**를 클릭합니다.

절차

단계 **1** 디바이스을 클릭한 다음 Backup and Restore(백업 및 복원) 요약에서 **View Configuration(**컨피그레이션 보기**)**을 클릭합니다.

단계 **2** **Scheduled Backup(**예약 백업**)** > **Schedule a Backup(**백업 예약**)**을 클릭합니다.
이미 예약한 백업이 있는 경우 **Scheduled Backup(**예약 백업**)** > **Edit(**수정**)**을 클릭합니다.

단계 **3** 백업의 이름과 설명(선택 사항)을 입력합니다.

단계 **4** 백업의 날짜와 시간을 선택합니다.

단계 **5** **Schedule(**예약**)**을 클릭합니다.
선택한 날짜와 시간이 되면 시스템이 백업을 수행합니다. 백업이 완료되면 백업 복사본이 백업 테이블에 나열됩니다.

반복 백업 일정 설정

반복 백업을 설정하여 정기적인 일정으로 시스템을 백업할 수 있습니다. 예를 들어 매주 금요일 자정에 백업을 만들 수 있습니다. 반복 백업 일정을 사용하는 경우 항상 최신 백업 집합을 적용할 수 있습니다.

참고 반복 일정을 삭제하려면 일정을 수정하고 **Remove(**제거**)**를 클릭합니다.

절차

단계 **1** 디바이스을 클릭한 다음 Backup and Restore(백업 및 복원) 요약에서 **View Configuration(**컨피그레이션 보기**)**을 클릭합니다.

단계 **2** **Recurring Backup(**반복 백업**)** > **Configure(**구성**)**를 클릭합니다.
이미 반복 백업을 구성한 경우 **Recurring Backup(**반복 백업**)** > **Edit(**수정**)**을 클릭합니다.

단계 **3** 백업의 이름과 설명(선택 사항)을 입력합니다.

단계 **4** 빈도 및 관련 일정을 선택합니다.

- 매일 - 시간을 선택합니다. 이 경우 매일 예약된 시간에 백업을 만듭니다.
- 매주 - 요일과 시간을 선택합니다. 이 경우 매 날짜의 예약된 시간에 백업을 만듭니다. 예를 들어 매주 월요일, 수요일, 금요일 23:00(오후 11시)에 백업을 예약할 수 있습니다.
- 매월 - 날짜와 시간을 선택합니다. 이 경우 매 날짜의 예약된 시간에 백업을 만듭니다. 예를 들어 매월 1일, 15일, 28일 23:00(오후 11시)에 백업을 예약할 수 있습니다.

단계 **5** **Save(**저장**)**를 클릭합니다.
선택한 날짜와 시간이 되면 시스템에서 백업을 만듭니다. 백업이 완료되면 백업 복사본이 백업 테이블에 나열됩니다.

반복 일정을 변경하거나 제거할 때까지 해당 일정에 따라 백업이 계속 만들어집니다.

백업 복원

필요에 따라 백업을 복원할 수 있습니다. 복원하려는 백업 복사본이 디바이스에 아직 없으면 복원 전에 백업을 먼저 업로드해야 합니다.

복원 중에는 시스템을 완전히 사용할 수 없게 됩니다.

참고 백업에는 관리 IP 주소 컨피그레이션이 포함되지 않습니다. 따라서 백업 파일을 복원할 때는 관리 주소가 백업 복사본에서 대체되지 않습니다. 이로 인해 주소에 대해 수행하는 변경 사항이 유지되며, 다른 네트워크 세그먼트의 다른 디바이스에서도 컨피그레이션을 복원할 수도 있습니다.

절차

단계 **1** 디바이스을 클릭한 다음 Backup and Restore(백업 및 복원) 요약에서 **View Configuration(**컨피그레이션 보기**)**을 클릭합니다.
그러면 백업 및 복원 페이지가 열립니다. 테이블에는 시스템에서 사용 가능한 모든 기존 백업 복사본이 나열됩니다.

단계 **2** 복원하려는 백업 복사본이 사용 가능한 백업 목록에 없으면 **Upload(**업로드**)** > **Browse(**찾아보기**)**를 클릭하여 백업 복사본을 업로드합니다.

단계 **3** 파일의 복원 아이콘( )을 클릭합니다.
복원을 확인하라는 메시지가 나타납니다. 기본값으로, 복원 후에 백업 복사본이 삭제되지만, 복원을 계속하기 전에 복원 후 백업을 제거하면 안 됨을 선택하여 백업을 유지할 수 있습니다.

복원이 완료되고 나면 시스템이 재부팅됩니다.

참고 시스템은 재부팅된 후 VDB(Vulnerability Database), 지리위치 및 규칙 데이터베이스 업데이트를 자동으로 확인하여 필요한 경우 다운로드합니다. 또한 정책도 재구축합니다.

백업 파일 관리

새 백업을 생성할 때 백업 파일은 백업 및 복원 페이지에 나열됩니다. 백업 복사본은 무기한 보존되지 않으며, 디바이스의 디스크 공간 사용량이 최대 임계값에 도달하면 새 백업 복사본을 위한 공간 확보를 위해 이전 백업 복사본이 삭제됩니다. 따라서 가장 보관 필요성이 높은 특정 백업 복사본을 보관할 수 있도록 백업 파일을 정기적으로 관리해야 합니다.

다음 작업을 수행하여 백업 복사본을 관리할 수 있습니다.

- 보안 스토리지에 파일 다운로드 - 워크스테이션에 백업 파일을 다운로드하려면 해당 파일의 다운로드 아이콘( )을 클릭합니다. 그러면 보안 파일 스토리지로 파일을 이동할 수 있습니다.
- 시스템에 백업 파일 업로드 - 디바이스에서 더 이상 사용할 수 없는 백업 복사본을 복원하려면 **Upload(**업로드**)** > **Browse File(**파일 찾아보기**)**을 클릭하고 워크스테이션에서 해당 복사본을 업로드합니다. 그러면 백업을 복원할 수 있습니다.

  참고 업로드한 파일의 이름은 원본 파일 이름과 일치하도록 바꿀 수 있습니다. 또한, 시스템에 10개가 넘는 백업 복사본이 이미 있으면 업로드한 파일을 위한 공간 확보를 위해 가장 오래된 복사본이 삭제됩니다. 이전 소프트웨어 버전에서 생성한 파일은 업로드할 수 없습니다.

- 백업 복원 - 백업 복사본을 복원하려면 해당 파일의 복원 아이콘( )을 클릭합니다. 복원 중에는 시스템을 사용할 수 없으며 복원이 완료되면 시스템이 재부팅됩니다. 시스템이 가동 및 실행되고 나면 컨피그레이션을 구축해야 합니다.
- 백업 파일 삭제 - 특정 백업이 더 이상 필요하지 않으면 해당 파일의 삭제 아이콘( )을 클릭합니다. 그러면 삭제를 확인하라는 메시지가 나타납니다. 삭제한 백업 파일은 복구할 수 없습니다.

시스템 재부팅

시스템이 올바르게 작동하지 않으며 문제를 해결하기 위한 다른 작업에서 장애가 발생한 경우에는 디바이스를 재부팅할 수 있습니다. CLI를 통해 디바이스를 재부팅해야 하며 Firepower Device Manager를 통해 디바이스를 재부팅할 수는 없습니다.

절차

단계 **1** SSH 클라이언트를 사용하여 관리 IP 주소에 대한 연결을 열고 컨피그레이션 CLI 액세스 권한이 있는 사용자 이름으로 디바이스 CLI에 로그인합니다. 예를 들어 관리자 사용자 이름을 사용합니다.

단계 **2** **reboot** 명령을 입력합니다.

예제**:**

```
> reboot
```

시스템 문제해결

다음 항목에서는 일부 시스템 레벨 문제해결 작업과 기능에 관해 설명합니다. 액세스 제어와 같은 특정 기능의 문제해결에 대한 자세한 내용은 해당 기능 관련 장을 참조하십시오.

주소 **ping**을 통해 연결 테스트

ping은 특정 주소가 활성 상태이고 응답할 수 있는지 확인하는 간단한 명령입니다. 기본 연결이 작동 중인 것입니다. 그러나 디바이스에서 실행 중인 다른 정책 때문에 특정 트래픽 유형이 디바이스를 통과하지 못할 수도 있습니다. 디바이스 CLI에 로그인하면 ping을 사용할 수 있습니다.

참고 시스템에는 여러 인터페이스가 있으므로 주소 ping에 사용되는 인터페이스를 제어할 수 있습니다. 중요한 연결을 테스트할 수 있도록 적절한 명령을 사용해야 합니다. 예를 들어 시스템은 가상 관리 인터페이스를 통해 Cisco 라이선스 서버에 연결할 수 있어야 하므로, **ping system** 명령을 사용하여 연결을 테스트해야 합니다. **ping**을 사용하는 경우에는 데이터 인터페이스를 통해 특정 주소에 연결할 수 있는지를 테스트하게 되므로 결과가 달라질 수도 있습니다.

일반 ping은 ICMP 패킷을 사용하여 연결을 테스트합니다. 네트워크에서 ICMP를 금지하는 경우에는 TCP ping을 대신 사용할 수 있습니다(데이터 인터페이스 ping에만 해당함).

네트워크 주소 ping에 사용되는 주요 옵션은 다음과 같습니다.

가상 관리 인터페이스를 통해 주소 **ping**

ping system 명령을 사용합니다.

ping system*host*

호스트는 IP 주소일 수도 있고 www.example.com과 같은 FQDN(Fully-Qualified Domain Name)일 수도 있습니다. 데이터 인터페이스를 통해 수행하는 ping과는 달리 시스템 ping에는 기본 횟수가 없습니다. 즉, Ctrl+C를 사용하여 중지할 때까지 ping은 계속 실행됩니다. 예를 들면 다음과 같습니다.

```
> ping system www.cisco.com
PING origin-www.cisco.COM (72.163.4.161) 56(84) bytes of data.
64 bytes from www1.cisco.com (72.163.4.161): icmp_seq=1 ttl=242 time=10.6 ms
64 bytes from www1.cisco.com (72.163.4.161): icmp_seq=2 ttl=242 time=8.13 ms
64 bytes from www1.cisco.com (72.163.4.161): icmp_seq=3 ttl=242 time=8.51 ms
64 bytes from www1.cisco.com (72.163.4.161): icmp_seq=4 ttl=242 time=8.40 ms
^C
--- origin-www.cisco.COM ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3003ms
rtt min/avg/max/mdev = 8.139/8.927/10.650/1.003 ms
>
```

라우팅 테이블을 사용하여 데이터 인터페이스를 통해 주소 **ping**

ping 명령을 사용합니다. 이 경우 인터페이스를 지정하지 않고 시스템이 호스트에 대한 경로를 일반적으로 찾을 수 있는지를 테스트하게 됩니다. 시스템은 보통 이 방법을 통해 트래픽을 라우팅하므로 일반적으로 이 테스트를 수행하면 됩니다.

ping*host*

호스트의 IP 주소를 지정합니다. FQDN만 알고 있다면 **nslookup***fqdn-name* 명령을 사용하여 IP 주소를 확인합니다. 예를 들면 다음과 같습니다.

```
> ping 171.69.38.1
Sending 5, 100-byte ICMP Echos to 171.69.38.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/10 ms
```

참고 시간 초과, 반복 횟수, 패킷 크기 및 전송할 데이터 패턴을 지정할 수 있습니다. 사용 가능한 옵션을 확인하려면 CLI에서 도움말 표시기 ?를 사용합니다.

특정 데이터 인터페이스를 통해 주소 **ping**

특정 데이터 인터페이스를 통한 연결을 테스트하려는 경우 **pinginterface***if_name* 명령을 사용합니다. 이 명령을 사용하여 진단 인터페이스를 지정할 수도 있지만, 가상 관리 인터페이스는 지정할 수 없습니다.

pinginterface*if_namehost*

호스트의 IP 주소를 지정합니다. FQDN만 알고 있다면 **nslookup***fqdn-name* 명령을 사용하여 IP 주소를 확인합니다. 예를 들면 다음과 같습니다.

```
> ping interface inside 171.69.38.1
Sending 5, 100-byte ICMP Echos to 171.69.38.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/10 ms
```

TCP ping을 사용하여 데이터 인터페이스를 통해 주소 **ping**

ping tcp 명령을 사용합니다. TCP ping은 SYN 패킷을 전송하며, 목적지에서 SYN-ACK 패킷을 전송하는 경우 ping에 성공한 것으로 간주합니다.

ping tcp [**interface***if_name*] *hostport*

호스트 및 TCP 포트를 지정해야 합니다. FQDN만 알고 있다면 **nslookup***fqdn-name* 명령을 사용하여 IP 주소를 확인합니다.

원하는 경우 인터페이스(ping을 전송하는 데 사용할 인터페이스가 아닌 ping의 소스 인터페이스)를 지정할 수 있습니다. 이 ping 유형은 항상 라우팅 테이블을 사용합니다.

TCP ping은 SYN 패킷을 전송하며, 목적지에서 SYN-ACK 패킷을 전송하는 경우 ping에 성공한 것으로 간주합니다. 예를 들면 다음과 같습니다.

```
> ping tcp 10.0.0.1 21
Type escape sequence to abort.
No source specified. Pinging from identity interface.
Sending 5 TCP SYN requests to 10.0.0.1 port 21
from 10.0.0.10, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms
```

참고 TCP ping의 시간 초과, 반복 횟수 및 소스 주소를 지정할 수도 있습니다. 사용 가능한 옵션을 확인하려면 CLI에서 도움말 표시기 ?를 사용합니다.

호스트에 대한 경로 추적

어떤 IP 주소에 트래픽을 보내는 데 문제가 있을 경우 호스트까지의 경로를 추적하여 네트워크 경로에 문제가 있는지 확인할 수 있습니다. 경로 추적(traceroute)은 잘못된 포트의 UDP 패킷이나 ICMPv6 에코를 목적지로 전송하는 방식입니다. 이러한 패킷이나 에코를 목적지로 전송하는 과정에서 라우터는 ICMP 시간 초과 메시지로 응답하고 경로 추적에 해당 오류를 보고합니다. 각 노드는 3개의 패킷을 수신하므로 노드당 정보 결과를 가져올 수 있는 3번의 기회가 있습니다. 디바이스 CLI에 로그인하면 경로 추적을 사용할 수 있습니다.

참고 데이터 인터페이스 또는 가상 인터페이스를 통해 경로를 추적할 수 있는 별도의 명령이 있습니다(각각 **traceroute**, **traceroute system**). 경우에 따라 적절한 명령을 사용해야 합니다.

다음 표에는 출력에 표시될 수 있는 패킷별 결과에 대한 설명이 나와 있습니다.

출력 기호	설명
*	프로브에 대한 응답을 받지 못한 채 시간이 초과되었습니다.
nn msec	각 노드에서 지정된 수의 프로브가 왕복하는 데 걸린 시간(밀리초)입니다.
!N.	연결 불가한 ICMP 네트워크입니다.
!H	연결 불가한 ICMP 호스트입니다.
!P	ICMP 프로토콜에 연결할 수 없습니다.
!A	관리자가 ICMP를 금지했습니다.
?	알 수 없는 ICMP 오류입니다.

가상 관리 인터페이스를 통해 경로 추적

traceroute system 명령을 사용합니다.

traceroute system*destination*

호스트는 IPv4/IPv6 주소일 수도 있고 www.example.com과 같은 FQDN(Fully Qualified Domain Name)일 수도 있습니다. 예를 들면 다음과 같습니다.

```
> traceroute system www.example.com
traceroute to www.example.com (172.163.4.161), 30 hops max, 60 byte packets
 1  192.168.0.254 (192.168.0.254)  0.213 ms  0.310 ms  0.328 ms
 2  10.88.127.1 (10.88.127.1)  0.677 ms  0.739 ms  0.899 ms
 3  lab-gw1.example.com (10.89.128.25)  0.638 ms  0.856 ms  0.864 ms
 4  04-bb-gw1.example.com (10.152.240.65)  1.169 ms  1.355 ms  1.409 ms
 5  wan-gw1.example.com (10.152.240.33)  0.712 ms  0.722 ms  0.790 ms
 6  wag-gw1.example.com (10.152.240.73)  13.868 ms  10.760 ms  11.187 ms
 7  rbb-gw2.example.com (172.30.4.85)  7.202 ms  7.301 ms  7.101 ms
 8  rbb-gw1.example.com (172.30.4.77)  8.162 ms  8.225 ms  8.373 ms
 9  sbb-gw1.example.com (172.16.16.210)  7.396 ms  7.548 ms  7.653 ms
10  corp-gw2.example.com (172.16.16.58)  7.413 ms  7.310 ms  7.431 ms
11  dmzbb-gw2.example.com (172.16.0.78)  7.835 ms  7.705 ms  7.702 ms
12  dmzdcc-gw2.example.com (172.16.0.190)  8.126 ms  8.193 ms  11.559 ms
13  dcz05n-gw1.example.com (172.16.2.106)  11.729 ms  11.728 ms  11.939 ms
14  www1.example.com (172.16.4.161)  11.645 ms  7.958 ms  7.936 ms
```

데이터 인터페이스를 통해 경로 추적

traceroute 명령을 사용합니다.

traceroute*destination*

호스트의 IP 주소를 지정합니다. FQDN만 알고 있다면 **nslookup***fqdn-name* 명령을 사용하여 IP 주소를 확인합니다. 예를 들면 다음과 같습니다.

```
> traceroute 209.165.200.225
Tracing the route to 209.165.200.225
 1  10.83.194.1 0 msec 10 msec 0 msec
 2  10.83.193.65 0 msec 0 msec 0 msec
 3  10.88.193.101 0 msec 10 msec 0 msec
 4  10.88.193.97 0 msec 0 msec 10 msec
 5  10.88.239.9 0 msec 10 msec 0 msec
 6  10.88.238.65 10 msec 10 msec 0 msec
 7 172.16.7.221 70 msec 70 msec 80 msec
 8 209.165.200.225 70 msec 70 msec 70 msec
```

참고 시간 초과, TTL(Time to Live), 노드당 패킷 수 및 경로 추적의 출발지로 사용할 IP 주소나 인터페이스를 지정할 수 있습니다. 사용 가능한 옵션을 확인하려면 CLI에서 도움말 표시기 ?를 사용합니다.

NTP 트러블슈팅

시스템은 시스템이 올바르게 작동하고 이벤트 및 기타 데이터 포인트가 정확하게 처리되도록 정확하고 일관된 시간을 사용합니다. 시스템에서 항상 신뢰할 수 있는 시간 정보를 유지하려면 1개 이상의 NTP(Network Time Protocol) 서버(이상적으로는 3개)를 구성해야 합니다.

디바이스 요약 연결 다이어그램(기본 메뉴에서 **Device(**디바이스**)** 클릭)은 NTP 서버에 대한 연결 상태를 보여줍니다. 이 상태가 노란색 또는 주황색인 경우, 구성된 서버에 연결하는 데 문제가 있는 것입니다. 연결 문제가 지속될 경우(일시적인 문제가 아님), 다음을 수행하십시오.

- **Device(**디바이스**)** > **System Settings(**시스템 설정**)** > **NTP**에서 3개 이상의 NTP 서버를 구성합니다. 이것은 요건은 아니지만 3개 이상의 NTP 서버가 있는 경우 신뢰성이 매우 향상됩니다.
- **Device(**디바이스**)** > **System Settings(**시스템 설정**)** > **Management Interface(**관리 인터페이스**)**에 정의되어 있는 관리 인터페이스 IP 주소와 NTP 서버 간의 네트워크 경로가 있는지 확인합니다.
  - 관리 인터페이스 게이트웨이가 데이터 인터페이스인 경우, 기본 경로가 적절하지 않으면 **Device(**디바이스**)** > **Routing(**라우팅**)**에서 NTP 서버에 대한 고정 경로를 구성할 수 있습니다.
  - 명시적 관리 인터페이스 게이트웨이를 설정한 경우, 디바이스 CLI에 로그인하고 **ping system** 명령을 사용하여 각 NTP 서버에 대한 네트워크 경로가 있는지 테스트합니다.
- 디바이스 CLI에 로그인하고 다음 명령을 사용하여 NTP 서버의 상태를 확인합니다.
  - **show ntp** - 이 명령은 NTP 서버와 가용성에 대한 기본 정보를 표시합니다. 단, Firepower Device Manager의 연결 상태는 상태를 나타내는 추가 정보를 사용합니다. 따라서 이 명령

이 표시하는 항목과 연결 상태 다이어그램이 표시하는 항목 간에 불일치가 있을 수 있습니다.

◦ **system support ntp** - 이 명령은 **show ntp**의 출력과 함께 표준 NTP 명령인 **ntpq**의 출력(NTP 프로토콜에 문서화됨)도 포함합니다. NTP 동기화를 확인해야 하는 경우 이 명령을 사용합니다.

'ntpq -pn 결과' 섹션을 검색합니다. 예를 들면 다음과 같은 내용이 표시될 수 있습니다.

```
Results of 'ntpq -pn'
remote                    : +216.229.0.50
refid                     : 129.7.1.66
st                        : 2
t                         : u
when                      : 704
poll                      : 1024
reach                     : 377
delay                     : 90.455
offset                    : 2.954
jitter                    : 2.473
```

이 예에서 NTP 서버 주소 앞에 있는 +는 잠재적인 후보임을 나타냅니다. 여기에서 별표 * 는 현재 시간 소스 피어를 나타냅니다.

NTPD(NTP 데몬)는 각각의 피어에서 얻은 8개 샘플로 구성된 슬라이딩 윈도우를 사용하며, 하나의 샘플을 선택한 후 선택한 시계는 올바른 chimer와 잘못된 ticker를 확인합니다. 그런 다음 NTPD는 왕복 거리(후보의 오프셋은 왕복 지연의 1/2를 초과하지 않아야 함)를 확인합니다. 연결이 지연될 경우, 패킷이 손실되거나 서버 문제로 인해 하나 또는 모든 후보가 거부될 경우, 동기화에서 오랜 지연을 확인하게 됩니다. 조정 또한 매우 오랜 시간에 걸쳐 발생합니다. 시계 오프셋과 오실레이터 오류는 시계 규칙 알고리즘을 사용하여 해결해야 하며 이 작업에는 몇 시간이 걸릴 수 있습니다.

참고 refid가 .LOCL인 경우, 이는 피어가 규칙이 없는 로컬 시계임을 나타냅니다. 즉, 시간을 설정하기 위해 로컬 시계만 사용하는 것을 의미합니다. 선택한 피어가 .LOCL인 경우 Firepower Device Manager는 항상 동기화되지 않은 NTP 연결을 노란색으로 표시합니다. 일반적으로, NTP는 더 나은 후보를 사용할 수 있는 경우 .LOCL 후보를 선택하지 않으므로 3개 이상의 서버를 구성해야 합니다.

CPU 및 메모리 사용량 분석

CPU 및 메모리 사용량에 대한 시스템 레벨 정보를 보려면 **Monitoring(**모니터링**)** > **System(**시스템**)**을 선택하고 CPU 및 메모리 막대 그래프를 찾습니다. 이러한 그래프에는 **show cpu system** 및 **show memory system** 명령을 사용하여 CLI를 통해 수집한 정보가 표시됩니다.

CLI에 로그인하면 이러한 명령의 추가 버전을 사용하여 다른 정보를 확인할 수 있습니다. 일반적으로는 사용량과 관련하여 지속적인 문제가 발생하는 경우나 Cisco Technical Assistance Center(TAC)의 지침이 있는 경우에만 이 정보를 확인하면 됩니다. 자세한 정보는 대부분 복잡하므로 TAC의 해석이 필요합니다.

검사할 수 있는 몇 가지 주요 정보는 다음과 같습니다. 이러한 명령과 관련된 자세한 정보는 http://www.cisco.com/c/en/us/td/docs/security/firepower/command_ref/b_Command_Reference_for_Firepower_Threat_Defense.html의 *Firepower Threat Defence* 명령 참조에서 확인할 수 있습니다.

- **show cpu**는 데이터 플레인 CPU 사용률을 표시합니다.
- **show cpu core**는 각 CPU 코어의 사용량을 개별적으로 표시합니다.
- **show cpu detailed**는 코어당/전체 데이터 플레인 CPU 사용량을 추가로 표시합니다.
- **show memory**는 데이터 플레인 메모리 사용량을 표시합니다.

참고 위에 나와 있지 않은 일부 키워드의 경우 **cpu** 또는 **memory** 명령을 사용하여 프로파일링 또는 기타 기능을 먼저 설정해야 합니다. 이러한 기능은 TAC 지침에 따라 사용하십시오.

로그 보기

시스템은 다양한 작업에 대한 정보를 로깅합니다. **system support view-files** 명령을 사용하여 시스템 로그를 열 수 있습니다. Cisco TAC(Technical Assistance Center)와 작업할 때 이 명령을 사용하면 TAC에서 출력 해석을 지원할 수 있으며 확인해야 하는 적절한 로그를 선택할 수 있습니다.

이 명령을 실행하면 로그 선택을 위한 메뉴가 표시됩니다. 다음 명령을 사용하여 마법사를 탐색합니다.

- 하위 디렉터리로 변경하려면 디렉터리의 이름을 입력하고 Enter 키를 누릅니다.
- 보려는 파일을 선택하려면 프롬프트에서 **s**를 입력합니다. 그러면 파일 이름을 입력하라는 메시지가 표시됩니다. 대소문자를 구분하여 전체 이름을 입력해야 합니다. 파일 목록에는 로그의 크기가 표시됩니다. 매우 큰 로그의 경우 열기 전에 크기를 고려해야 합니다.
- --자세히--가 표시될 때 스페이스바를 누르면 다음 로그 항목 페이지가 표시되고 Enter 키를 누르면 다음 로그 항목만 표시됩니다. 로그의 끝에 도달하면 메인 메뉴로 이동됩니다. --자세히-- 줄에는 로그의 크기와 로그를 확인한 빈도가 표시됩니다. 전체 로그 페이지를 확인하지 않으려는 경우 **Ctrl+C**를 사용하여 로그를 닫고 명령을 종료합니다**.**
- 메뉴의 구조에서 한 레벨 위로 이동하려면 **b**를 입력합니다.

새로 추가되는 메시지를 확인할 수 있도록 로그를 열어 두려면 **system support view-files** 대신 **tail-logs** 명령을 사용합니다.

다음 예에서는 시스템 로그인 시도를 추적하는 cisco/audit.log 파일을 확인하는 방법을 보여줍니다. 파일 목록은 맨 위의 디렉터리에서 시작되며, 그 아래에는 현재 디렉터리의 파일 목록이 표시됩니다.

```
> system support view-files

===View Logs===

============================
Directory: /ngfw/var/log
----------sub-dirs----------
cisco
```

```
mojo
removed_packages
setup
seshat
connector
sf
scripts
packages
removed_scripts
httpd
-----------files------------
2016-10-14 18:12:04.514783 | 5371       | SMART_STATUS_sda.log
2016-10-14 18:12:04.524783 | 353        | SMART_STATUS_sdb.log
2016-10-11 21:32:23.848733 | 326517     | action_queue.log
2016-10-06 16:00:56.620019 | 1018       | br1.down.log

<list abbreviated>


([b] to go back or [s] to select a file to view, [Ctrl+C] to exit)
Type a sub-dir name to list its contents: cisco

============================
Directory: /ngfw/var/log/cisco
-----------files------------
2017-02-13 22:44:42.394907 | 472        | audit.log
2017-02-13 23:40:30.858198 | 903615     | ev_stats.log.0
2017-02-09 18:14:26.870361 | 0          | ev_stats.log.0.lck
2017-02-13 05:24:00.682601 | 1024338    | ev_stats.log.1
2017-02-12 08:41:00.478103 | 1024338    | ev_stats.log.2
2017-02-11 11:58:00.260805 | 1024218    | ev_stats.log.3
2017-02-09 18:12:13.828607 | 95848      | firstboot.ngfw-onbox.log
2017-02-13 23:40:00.240359 | 6523160    | ngfw-onbox.log

([b] to go back or [s] to select a file to view, [Ctrl+C] to exit)
Type a sub-dir name to list its contents: s

Type the name of the file to view ([b] to go back, [Ctrl+C] to exit)
> audit.log
2017-02-09 18:59:26 - SubSystem:LOGIN, User:admin, IP:10.24.42.205, Message:Login successful,

2017-02-13 17:59:28 - SubSystem:LOGIN, User:admin, IP:10.24.111.72, Message:Login successful,

2017-02-13 22:44:36 - SubSystem:LOGIN, User:admin, IP:10.24.111.72, Message:Login failed,
2017-02-13 22:44:42 - SubSystem:LOGIN, User:admin, IP:10.24.111.72, Message:Login successful,

2017-02-13 22:44:42 - SubSystem:LOGIN, User:admin, IP:10.24.111.72, Message:Unlocked account.,


<remaining log truncated>
```

문제해결 파일 생성

문제 보고서를 제출할 때는 Cisco TAC(Technical Assistance Center) 담당자가 시스템 로그 정보 제출을 요청할 수 있습니다. 담당자는 이 정보를 통해 문제를 보다 쉽게 진단할 수 있습니다. 별도의 요청이 없으면 진단 파일을 제출하지 않아도 됩니다.

다음 절차에서는 진단 파일을 생성하고 다운로드하는 방법을 설명합니다.

절차

단계 **1** 디바이스을 클릭합니다.

단계 **2** 트러블슈팅에서 파일 생성 요청 또는 파일 생성 재요청(이전에 파일 생성을 요청한 경우)을 클릭합니다.
시스템에서 진단 파일 생성이 시작됩니다. 다른 페이지로 이동했다가 돌아와서 상태를 확인할 수 있습니다. 파일이 준비되면 파일 생성 날짜와 시간이 다운로드 버튼과 함께 표시됩니다.

단계 **3** 파일이 준비되면 다운로드 버튼을 클릭합니다.
브라우저 표준 다운로드 방법을 통해 파일이 워크스테이션에 다운로드됩니다.

일반적이지 않은 관리 작업

다음 항목에서는 수행하더라도 자주 수행하지는 않는 작업에 관해 설명합니다. 이러한 모든 작업을 수행하면 디바이스 컨피그레이션이 지워집니다. 이러한 변경을 수행하기 전에 디바이스가 현재 프로덕션 네트워크에 중요한 서비스를 제공하고 있지 않은지 확인합니다.

로컬 및 원격 관리 간 전환

디바이스에서 직접 호스팅되거나 여러 Firepower Management Center는 디바이스 관리자를 사용하여 원격으로 호스팅되는 로컬 Firepower Device Manager를 통해 디바이스를 구성하고 관리할 수 있습니다. Firepower Device Manager에서 지원되지 않는 기능을 구성하려는 경우 또는 Firepower Management Center는에서 제공되는 전력 및 분석 기능이 필요한 경우 원격 관리자를 사용할 수 있습니다.

Transparent 방화벽 모드에서 디바이스를 실행하려는 경우에도 Firepower Management Center는를 사용해야 합니다.

소프트웨어를 다시 설치하지 않고도 로컬 및 원격 관리 간에 전환할 수 있습니다. 원격 관리에서 로컬 관리로 전환하기 전에 Firepower Device Manager가 모든 컨피그레이션 요건을 충족하는지 확인하십시오.

⚠

주의 관리자를 전환하면 디바이스 컨피그레이션이 지워지며 시스템이 기본 컨피그레이션으로 돌아갑니다. 그러나, 관리 IP 주소 및 호스트 이름은 유지됩니다.

시작하기 전에

디바이스를 등록한 경우, 특히 기능 라이선스를 사용하는 경우에는 원격 관리로 전환하기 전에 Firepower Device Manager를 통해 디바이스를 등록 취소해야 합니다. 디바이스 등록을 취소하면 기본 라이선스 및 모든 기능 라이선스가 해제됩니다. 디바이스를 등록 취소하지 않으면 해당 라이선스는 Cisco Smart Software Manager에서 디바이스에 할당된 상태로 유지됩니다. 디바이스 등록 취소, 69 페이지를 참조하십시오.

절차

단계 **1** SSH 클라이언트를 사용하여 관리 **IP** 주소에 대한 연결을 열고 컨피그레이션 CLI 액세스 권한이 있는 사용자 이름으로 디바이스 CLI에 로그인합니다. 예를 들어 관리자 사용자 이름을 사용합니다.
관리 IP 주소에 연결되어 있는 동안에는 이 프로세스를 따라야 합니다. Firepower Device Manager를 사용할 때는 데이터 인터페이스의 IP 주소를 통해 디바이스를 관리할 수 있습니다. 그러나 디바이스를 원격으로 관리하려면 관리 물리적 포트 및 관리 IP 주소를 사용해야 합니다.

관리 IP 주소에 연결할 수 없는 경우에는 다음 작업을 수행합니다.

- 관리 물리적 포트가 작동하는 네트워크에 유선 연결되어 있는지 확인합니다.
- 관리 네트워크에 대해 관리 IP 주소 및 게이트웨이가 구성되어 있는지 확인합니다. Firepower Device Manager의 **Device(**디바이스**)** > **System Settings(**시스템 설정**)** > **Management Interface(**관리 인터페이스**)**에서 주소와 게이트웨이를 구성합니다. CLI에서는 **configure network ipv4/ipv6 manual** 명령을 사용합니다.

  참고 관리 IP 주소에 대해 외부 게이트웨이를 사용하고 있는지 확인합니다. 원격 관리자를 사용할 때는 데이터 인터페이스를 게이트웨이로 사용할 수 없습니다.

단계 **2** 로컬 관리에서 원격 관리로 전환하려면 다음을 수행합니다.

a) 현재 로컬 관리 모드 상태인지 확인합니다.

```
> show managers
Managed locally.
```

b) 원격 관리자를 구성합니다.
configure manager add {*hostname* | *IPv4_address* | *IPv6_address* | **DONTRESOLVE**} *regkey* [*nat_id*]

여기서 각 항목은 다음을 나타냅니다.

- {*hostname* | *IPv4_address* | *IPv6_address* | **DONTRESOLVE**}는 이 디바이스를 관리하는 Firepower Management Center는의 DNS 호스트 이름이나 IP 주소(IPv4 또는 IPv6)를 지정합니다. Firepower Management Center는의 주소를 직접 지정할 수 없으면 **DONTRESOLVE**를 사용합니다. **DONTRESOLVE**를 사용하는 경우 *nat_id*가 필요합니다.
- *regkey*는 디바이스를 Firepower Management Center는에 등록하기 위해 필요한 고유한 영숫자 등록 키입니다.
- *nat_id*는 Firepower Management Center는와 디바이스 간의 등록 프로세스 동안 사용되는 선택적인 영숫자 문자열입니다. 호스트 이름을 DONTRESOLVE로 설정하는 경우 반드시 필요합니다.

예를 들어 등록 키 **secret**을 사용하여 192.168.0.123에서 관리자를 사용하려면 다음을 입력합니다.

```
> configure manager add 192.168.0.123 secret
If you enabled any feature licenses, you must disable them in
Firepower Device Manager before switching to remote management.
Otherwise, those licenses remain assigned to the device in Cisco
```

```
Smart Software Manager.
Do you want to continue  [yes/no] yes
Manager successfully configured.
Please make note of reg_key as this will be required while adding
Device in FMC.

> show managers
Host                      : 192.168.0.123
Registration Key          : ****
Registration              : pending
RPC Status                :
```

참고 등록이 아직 보류 중인 상태에서 **configure manager delete**를 사용하여 등록을 취소한 다음 **configure manager local**을 사용하여 로컬 관리로 돌아갈 수 있습니다.

c) Firepower Management Center는에 로그인하여 디바이스를 추가합니다.
자세한 내용은 Firepower Management Center는 온라인 도움말을 참조하십시오.

단계 **3** 원격 관리에서 로컬 관리로 전환하려면 다음을 수행합니다.

a) 현재 원격 관리 모드 상태인지 확인합니다.

```
> show managers
Host                      : 192.168.0.123
Registration Key          : ****
Registration              : pending
RPC Status                :
```

b) 원격 관리자를 삭제하고 관리자 없음 모드를 설정합니다.
원격 관리에서 로컬 관리로 직접 이동할 수는 없습니다. **configure manager delete** 명령을 사용하여 관리자를 제거합니다.

```
> configure manager delete
Deleting task list
Manager successfully deleted.

>
> show managers
No managers configured.
```

c) 로컬 관리자를 구성합니다.
configure manager local

예를 들면 다음과 같습니다.

```
> configure manager local
Deleting task list

> show managers
Managed locally.
```

이제 웹 브라우저를 사용하여 **https://***management-IP-address*에서 로컬 관리자를 열 수 있습니다.

방화벽 모드 변경

Firepower Threat Defense 방화벽은 라우팅 모드 또는 Transparent 모드에서 실행될 수 있습니다. 라우팅 모드 방화벽은 라우팅 홉이며, 해당 스크린드 서브넷 중 하나에 연결되는 호스트의 기본 게이트웨이 역할을 수행합니다. 이와 반대로 Transparent 방화벽은 "비활성 엔드포인트(bump in the wire)" 또는 "은폐형 방화벽(stealth firewall)" 같은 역할을 수행하는 레이어 2 방화벽이며, 연결된 디바이스에 대한 라우터 홉으로 표시되지 않습니다.

로컬 Firepower Device Manager는 라우팅 모드만 지원합니다. 그러나 Transparent 모드에서 상자를 실행해야 하는 경우에는 방화벽 모드를 변경하고 Firepower Management Center는를 사용하여 디바이스 관리를 시작할 수 있습니다. 반면 Transparent 모드 디바이스는 라우팅 모드로 변환할 수 있으며, 그 후에는 로컬 관리자를 사용하여 해당 디바이스를 구성할 수 있습니다. Firepower Management Center는를 사용하여 라우팅 모드 디바이스를 관리할 수도 있습니다.

로컬 또는 원격 관리와 관계없이 모드를 변경하려면 디바이스 CLI를 사용해야 합니다.

다음 절차에서는 로컬 관리자를 사용 중이거나 사용하려는 경우 모드를 변경하는 방법을 설명합니다.

주의 방화벽 모드를 변경하면 디바이스 컨피그레이션이 지워지며 시스템이 기본 컨피그레이션으로 돌아갑니다. 그러나, 관리 IP 주소 및 호스트 이름은 유지됩니다.

시작하기 전에

Transparent 모드로 변환하는 경우 방화벽 모드를 변경하기 전에 Firepower Management Center는를 설치합니다.

기능 라이선스를 활성화한 경우에는 로컬 관리자를 삭제하고 원격 관리로 전환하기 전에 Firepower Device Manager에서 해당 라이선스를 비활성화해야 합니다. 이렇게 하지 않으면 해당 라이선스는 Cisco Smart Software Manager에서 디바이스에 할당된 상태로 유지됩니다. 선택 가능한 라이선스 활성화 또는 비활성화, 67 페이지를 참조하십시오.

절차

단계 **1** SSH 클라이언트를 사용하여 관리 **IP** 주소에 대한 연결을 열고 컨피그레이션 CLI 액세스 권한이 있는 사용자 이름으로 디바이스 CLI에 로그인합니다. 예를 들어 관리자 사용자 이름을 사용합니다.
관리 IP 주소에 연결되어 있는 동안에는 이 프로세스를 따라야 합니다. Firepower Device Manager를 사용할 때는 데이터 인터페이스의 IP 주소를 통해 디바이스를 관리할 수 있습니다. 그러나 디바이스를 원격으로 관리하려면 관리 물리적 포트 및 관리 IP 주소를 사용해야 합니다.

관리 IP 주소에 연결할 수 없는 경우에는 다음 작업을 수행합니다.

- 관리 물리적 포트가 작동하는 네트워크에 유선 연결되어 있는지 확인합니다.
- 관리 네트워크에 대해 관리 IP 주소 및 게이트웨이가 구성되어 있는지 확인합니다. Firepower Device Manager의 **Device(**디바이스**)** > **System Settings(**시스템 설정**)** > **Management Interface(**관

리 인터페이스)에서 주소와 게이트웨이를 구성합니다. CLI에서는 **configure network ipv4/ipv6 manual** 명령을 사용합니다.

참고 관리 IP 주소에 대해 외부 게이트웨이를 사용하고 있는지 확인합니다. 원격 관리자를 사용할 때는 데이터 인터페이스를 게이트웨이로 사용할 수 없습니다.

단계 **2** 라우팅 모드에서 Transparent 모드로 변경하고 원격 관리를 사용하려면 다음을 수행합니다.

a) 로컬 관리를 비활성화하고 관리자 모드로 진입하지 않습니다.
활성 관리자가 있으면 방화벽 모드를 변경할 수 없습니다. **configure manager delete** 명령을 사용하여 관리자를 제거합니다.

```
> configure manager delete
If you enabled any feature licenses, you must disable them in
Firepower Device Manager before deleting the local manager.
Otherwise, those licenses remain assigned to the device in
Cisco Smart Software Manager.
Do you want to continue[yes/no] yes
Deleting task list
Manager successfully deleted.

>
> show managers
No managers configured.
```

b) 방화벽 모드를 Transparent로 변경합니다.
configure firewalltransparent

예제:

```
> configure firewall transparent
This will destroy the current interface configurations,
are you sure that you want to proceed? [y/N] y
The firewall mode was changed successfully.
```

c) 원격 관리자를 구성합니다.
configure manager add {*hostname* | *IPv4_address* | *IPv6_address* | **DONTRESOLVE**} *regkey* [*nat_id*]

여기서 각 항목은 다음을 나타냅니다.

- {*hostname* | *IPv4_address* | *IPv6_address* | **DONTRESOLVE**}는 이 디바이스를 관리하는 Firepower Management Center는의 DNS 호스트 이름이나 IP 주소(IPv4 또는 IPv6)를 지정합니다. Firepower Management Center는의 주소를 직접 지정할 수 없으면 **DONTRESOLVE**를 사용합니다. **DONTRESOLVE**를 사용하는 경우 *nat_id*가 필요합니다.
- *regkey*는 디바이스를 Firepower Management Center는에 등록하기 위해 필요한 고유한 영숫자 등록 키입니다.
- *nat_id*는 Firepower Management Center는와 디바이스 간의 등록 프로세스 동안 사용되는 선택적인 영숫자 문자열입니다. 호스트 이름을 DONTRESOLVE로 설정하는 경우 반드시 필요합니다.

예를 들어 등록 키 **secret**을 사용하여 192.168.0.123에서 관리자를 사용하려면 다음을 입력합니다.

```
> configure manager add 192.168.0.123 secret
Manager successfully configured.
Please make note of reg_key as this will be required while adding
Device in FMC.

> show managers
Host                      : 192.168.0.123
Registration Key          : ****
Registration              : pending
RPC Status                :
```

d) Firepower Management Center는에 로그인하여 디바이스를 추가합니다.
자세한 내용은 Firepower Management Center는 온라인 도움말을 참조하십시오.

단계 **3** Transparent 모드에서 라우팅 모드로 변경하고 로컬 관리로 변환하려면 다음을 수행합니다.

a) Management Center에서 디바이스를 등록 취소합니다.

b) Firepower Threat Defense 디바이스 CLI에 액세스합니다. 콘솔 포트에서 액세스하는 것이 좋습니다.
모드를 변경하면 컨피그레이션이 지워지므로 관리 IP 주소는 기본값으로 되돌아갑니다. 따라서 모드를 변경한 후에는 관리 IP 주소에 대한 SSH 연결이 끊길 수 있습니다.

c) 방화벽 모드를 라우팅으로 변경합니다.
configure firewallrouted

예제:

```
> configure firewall routed
This will destroy the current interface configurations,
are you sure that you want to proceed? [y/N] y
The firewall mode was changed successfully.
```

d) 로컬 관리자를 활성화합니다.
configure manager local

예를 들면 다음과 같습니다.

```
> configure manager local
Deleting task list

> show managers
Managed locally.
```

이제 웹 브라우저를 사용하여 **https://***management-IP-address*에서 로컬 관리자를 열 수 있습니다.

컨피그레이션 재설정

컨피그레이션을 처음부터 다시 시작하려는 경우 시스템 컨피그레이션을 공장 기본값으로 재설정할 수 있습니다. 컨피그레이션을 직접 재설정할 수는 없지만 관리자를 삭제했다가 추가하면 컨피그레이션이 지워집니다.

컨피그레이션을 지우고 백업을 복구하려는 경우에는 복원할 백업 복사본을 이미 다운로드한 상태여야 합니다. 시스템을 재설정한 후에 백업을 복원할 수 있도록 해당 복사본을 업로드해야 합니다.

시작하기 전에

기능 라이선스를 활성화한 경우에는 로컬 관리자를 삭제하기 전에 Firepower Device Manager에서 해당 라이선스를 비활성화해야 합니다. 이렇게 하지 않으면 해당 라이선스는 Cisco Smart Software Manager에서 디바이스에 할당된 상태로 유지됩니다. 선택 가능한 라이선스 활성화 또는 비활성화, 67 페이지를 참조하십시오.

절차

단계 **1** SSH 클라이언트를 사용하여 관리 IP 주소에 대한 연결을 열고 컨피그레이션 CLI 액세스 권한이 있는 사용자 이름으로 디바이스 CLI에 로그인합니다. 예를 들어 관리자 사용자 이름을 사용합니다.

단계 **2** **configure manager delete** 명령을 사용하여 관리자를 제거합니다.

```
> configure manager delete
If you enabled any feature licenses, you must disable them in
Firepower Device Manager before deleting the local manager.
Otherwise, those licenses remain assigned to the device in Cisco
Smart Software Manager.
Do you want to continue[yes/no] yes
Deleting task list
Manager successfully deleted.

>
> show managers
No managers configured.
```

단계 **3** 로컬 관리자를 구성합니다.
configure manager local

예를 들면 다음과 같습니다.

```
> configure manager local
Deleting task list

> show managers
Managed locally.
```

이제 웹 브라우저를 사용하여 **https://***management-IP-address*에서 로컬 관리자를 열 수 있습니다. 컨피그레이션을 지우면 디바이스 설정 마법사를 완료하라는 메시지가 표시됩니다.