기본 정책 구성

다음 설정으로 기본 보안 정책을 구성:

- 내부 및 외부 인터페이스 - 내부 인터페이스에 고정 IP 주소를 할당하고, 외부 인터페이스에 DHCP를 사용합니다.
- DHCP Server(DHCP 서버) - 클라이언트용 내부 인터페이스에서 DHCP 서버를 사용합니다.
- Default route(기본 경로) - 외부 인터페이스를 통해 기본 경로를 추가합니다.
- NAT - 외부 인터페이스에서 인터페이스 PAT를 사용합니다.
- Access control(액세스 제어) - 내부에서 외부로 향하는 트래픽을 허용합니다.

보안 정책을 사용자 지정하여 더 고급 검사를 포함시킬 수도 있습니다.

클라우드 제공 **Firewall Management Center**로 이동

클라우드 제공 Firewall Management Center는 Security Cloud Control의 자체 탭에서 실행됩니다.

프로시저

단계 **1** **Administration(**관리**)** > **Integration(**통합**)** > **Firewall Management Center**를 선택합니다.

단계 **2** 클라우드 제공 **FMC**를 선택하고 **Actions(**작업**)**, **Management(**관리**)**또는 **Settings(**설정**)** 창 링크를 클릭하여 새 탭에서 클라우드 제공 Firewall Management Center을 엽니다.

팁
클라우드 제공 Firewall Management Center에서 Security Cloud Control로 다시 이동하려면 **Home(홈)**를 클릭합니다.

인터페이스 구성

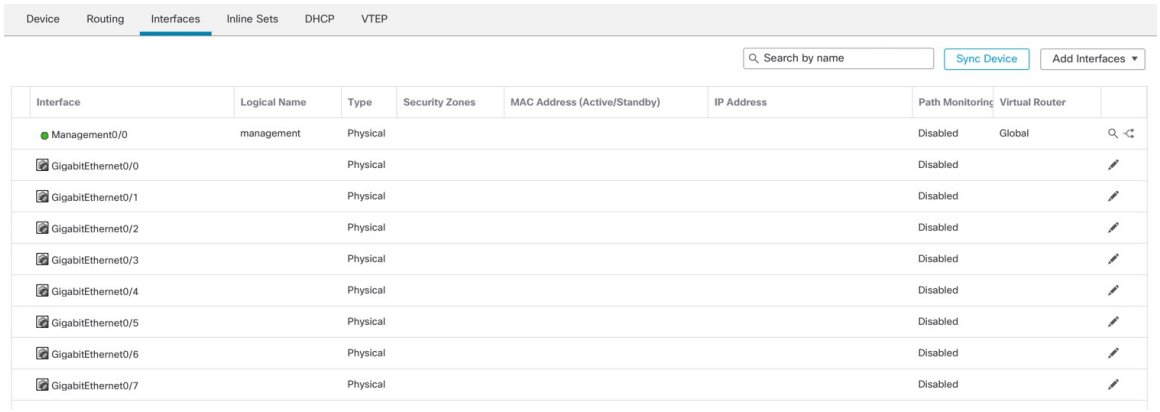
다음 예에서는 DHCP를 사용하는 외부 인터페이스에서 고정 주소 및 라우팅 모드를 사용하여 인터페이스 내부에 라우팅 모드를 구성합니다. 또한 내부 웹 서버용 DMZ 인터페이스를 추가합니다.

프로시저

단계 **1** **Devices(**디바이스**)** > **Device Management(**디바이스 관리**)**를 선택하고 방화벽에 대해 편집( )를 클릭합니다.

단계 **2** **Interfaces(**인터페이스**)**를 클릭합니다.

그림 ***1: Interfaces***

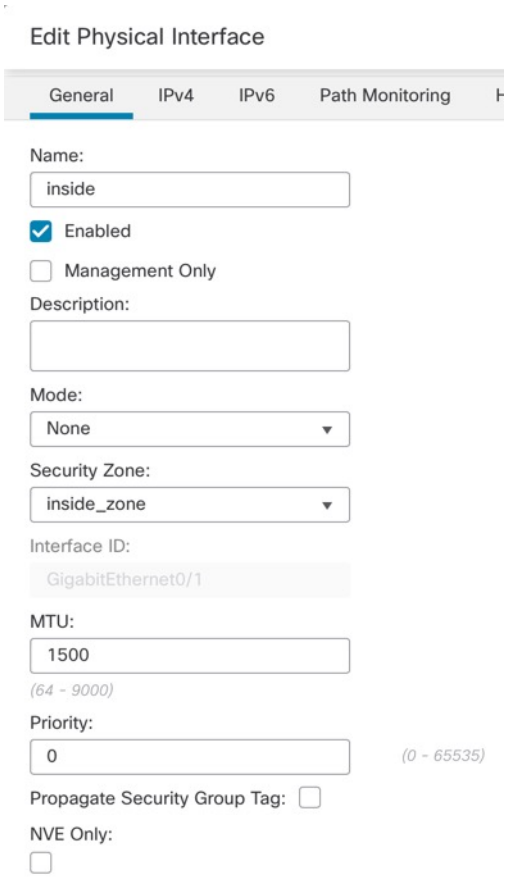


단계 **3** 40Gb 이상의 인터페이스에서 브레이크아웃 포트를 생성하려면 해당 인터페이스의 **Break** 아이콘을 클릭합니다.

구성에서 이미 전체 인터페이스를 사용한 경우 분할을 계속 진행하기 전에 구성을 제거해야 합니다.

단계 **4** 내부에 사용할 인터페이스의 편집( )를 클릭합니다.

그림 *2:* 일반 탭



a) **Security Zone(**보안 영역**)** 드롭다운 목록에서 기존의 내부 보안 영역을 선택하거나 **New(**새로 만들기**)**를 클릭하여 새 보안 영역을 추가합니다.

   예를 들어 **inside_zone**이라는 영역을 추가합니다. 영역 또는 그룹을 기준으로 보안 정책을 적용합니다. 예를 들어, 트래픽이 내부 영역에서 외부 영역으로는 이동하되 외부에서 내부로는 이동할 수 없도록 액세스 제어 정책을 구성할 수 있습니다.

   내부 인터페이스가 사전 구성된 경우, 나머지 필드는 선택 사항입니다.

b) **Name(**이름**)** 필드에 이름을 48자 이내로 입력합니다.

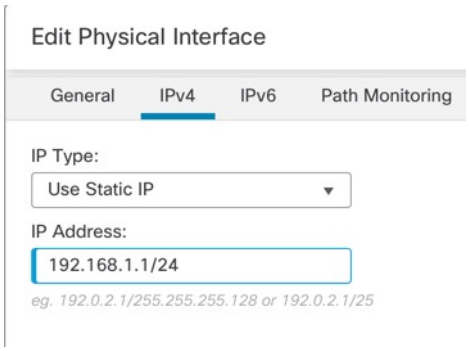
   예를 들어 인터페이스에 **inside**라는 이름을 지정합니다.

c) **Enable(**활성화**)** 확인란을 선택합니다.
d) **Mode(**모드**)**는 **None(**없음**)** 상태로 남겨둡니다.
e) **IPv4** 및/또는 **IPv6** 탭을 클릭 합니다.

   - **IPv4** - 드롭다운 목록에서 **Use Static IP(**고정 **IP** 사용**)**를 선택하고 슬래시(/) 표기로 IP 주소와 서브넷 마스크를 입력합니다.

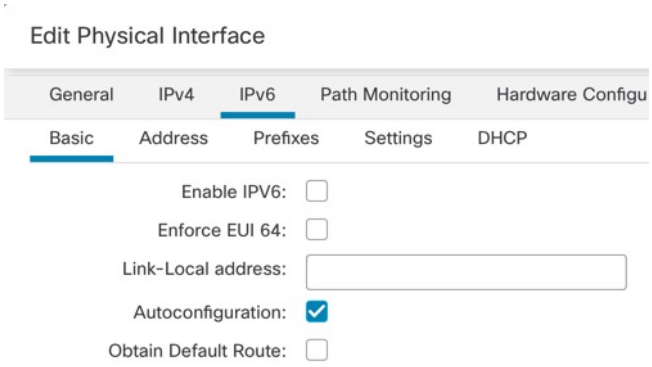
     예를 들어 **192.168.1.1/24** 를 입력합니다.

그림 ***3: IPv4*** 탭



- **IPv6** - 상태 비저장 자동 구성을 하려면 **Autoconfiguration(**자동 구성**)** 확인란을 선택합니다.

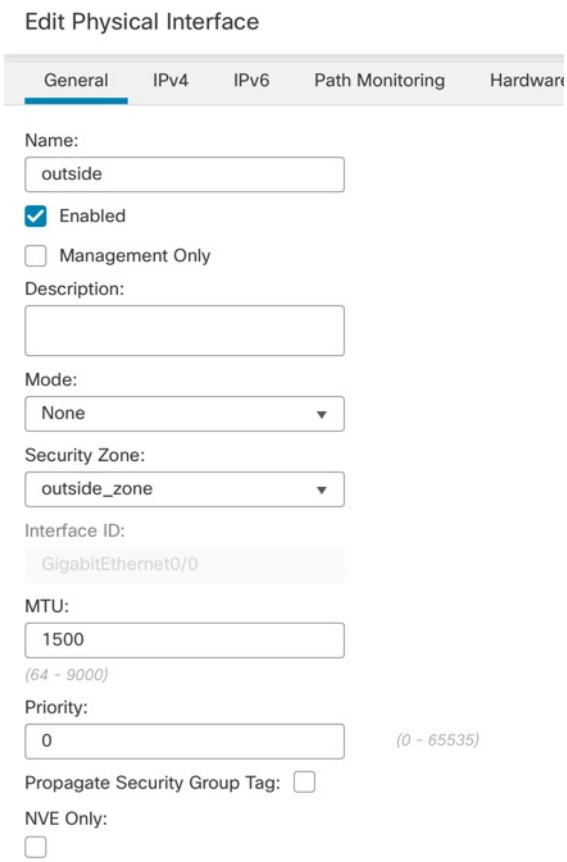
  그림 ***4: IPv6*** 탭



f) **OK(**확인**)**를 클릭합니다.

단계 **5** 외부에서 사용하려는 인터페이스의 편집( )를 클릭합니다.

그림 *5:* 일반 탭



a) **Security Zone(**보안 영역**)** 드롭다운 목록에서 기존의 외부 보안 영역을 선택하거나 **New(**새로 만들기**)**를 클릭하여 새 보안 영역을 추가합니다.

예를 들어 **outside_zone**이라는 영역을 추가합니다.

이러한 기본 설정을 변경하면 Firewall Management Center 관리 연결이 중단되므로 다른 기본 설정을 변경하면 안됩니다.

b) **OK(**확인**)**를 클릭합니다.

단계 **6** 예를 들어 웹 서버를 호스팅하기 위해 DMZ 인터페이스를 구성합니다.

a) 사용하려는 인터페이스의 편집( )를 클릭합니다.

b) **Security Zone(**보안 영역**)** 드롭다운 목록에서 기존의 DMZ 보안 영역을 선택하거나 **New(**새로 만들기**)**를 클릭하여 새 보안 영역을 추가합니다.

예를 들어 **dmz_zone**이라는 영역을 추가합니다.

c) **Name(**이름**)** 필드에 이름을 48자 이내로 입력합니다.

예를 들어 인터페이스 이름을 **dmz**로 지정합니다.

d) **Enable(**활성화**)** 확인란을 선택합니다.

e) **Mode(**모드**)**는 **None(**없음**)** 상태로 남겨둡니다.
f) **IPv4** 탭 및/또는 **IPv6** 탭을 클릭하고 원하는 IP 주소를 구성합니다.
g) **OK(**확인**)**를 클릭합니다.

단계 **7** **Save(**저장**)**를 클릭합니다.

DHCP 서버 구성

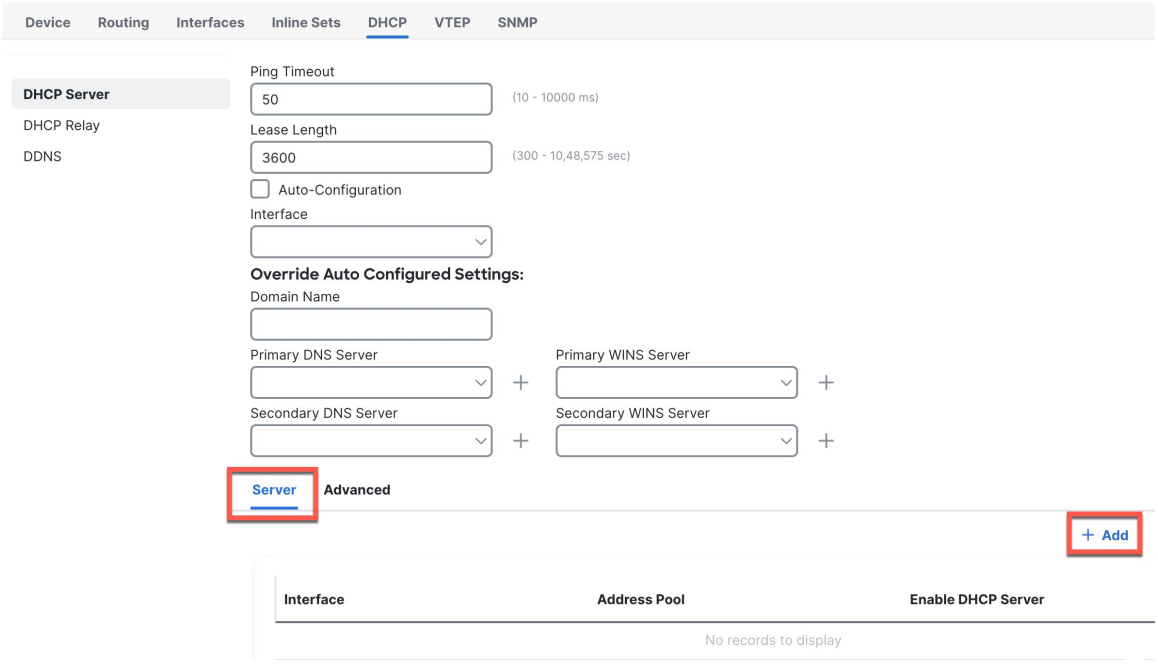
클라이언트가 DHCP를 사용하여 방화벽에서 IP 주소를 가져오게 하려면 DHCP 서버를 활성화합니다.

프로시저

단계 **1** **Devices(**디바이스**)** > **Device Management(**디바이스 관리**)**를 선택하고 디바이스의 편집( )을 클릭합니다.

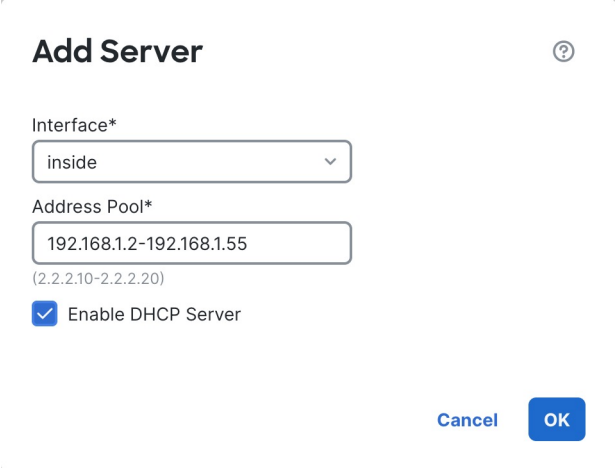
단계 **2** **DHCP** > **DHCP Server(DHCP** 서버**)**를 선택합니다.

그림 ***6: DHCP*** 서버



단계 **3** **Server(**서버**)** 페이지에서 **Add(**추가**)**를 클릭하고 다음 옵션을 구성합니다.

그림 *7:* 서버 추가



- **Interface(**인터페이스**)** - 드롭다운 목록에서 인터페이스를 선택합니다.
- **Address Pool(**주소 풀**)**- IP 주소의 범위를 설정합니다. 이 IP 주소는 선택된 인터페이스와 동일한 서브넷에 있어야 하며, 인터페이스 자체의 IP 주소는 포함할 수 없습니다.
- **Enable DHCP Server(DHCP** 서버 활성화**)** - 선택한 인터페이스에서 DHCP 서버를 활성화합니다.

단계 **4** **OK(**확인**)**를 클릭합니다.

단계 **5** **Save(**저장**)**를 클릭합니다.

NAT 구성

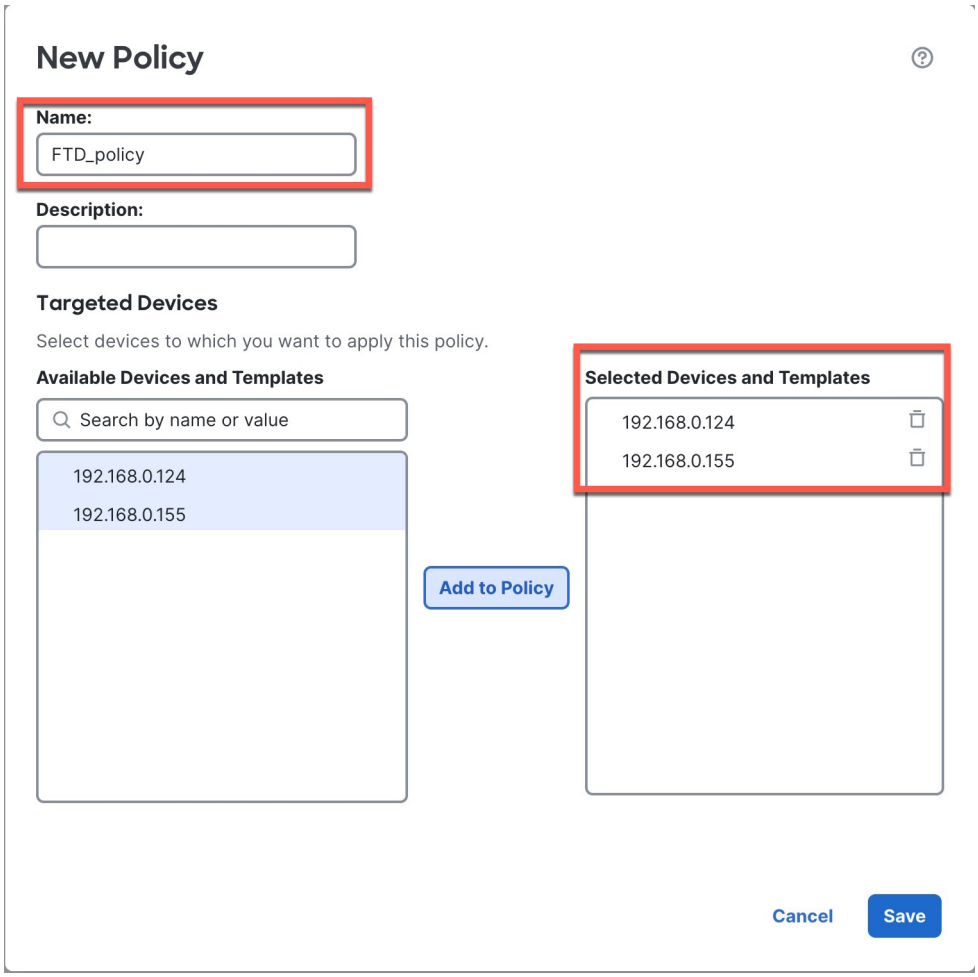
이 절차는 내부 클라이언트가 내부 주소를 외부 인터페이스 IP 주소의 포트로 변환하도록 하는 NAT 규칙을 생성합니다. 이러한 유형의 NAT 규칙을 인터페이스 포트 주소 변환*(PAT)*이라고 합니다.

프로시저

단계 **1** **Devices(**디바이스**)** > **NAT**를 선택하고, **New Policy(**새 정책**)**를 클릭합니다.

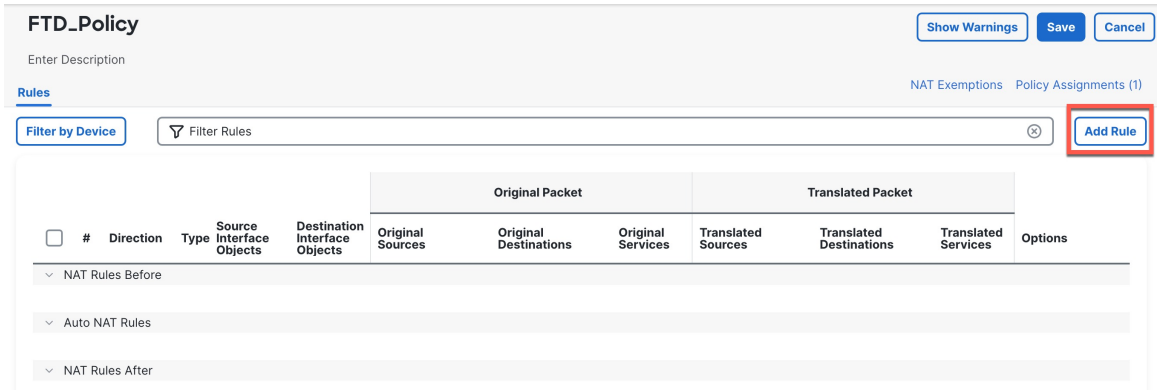
단계 **2** 정책 이름을 지정하고, 정책을 사용할 디바이스를 선택한 뒤 **Save(**저장**)**를 클릭합니다.

그림 *8:* 새 정책



정책이 Firewall Management Center을 추가합니다. 계속해서 정책에 규칙을 추가해야 합니다.

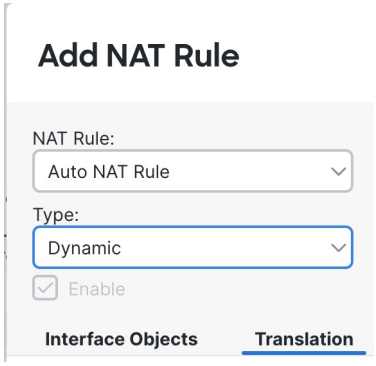
그림 *9: NAT* 정책



단계 **3** **Add Rule(**규칙 추가**)**을 클릭합니다.

단계 **4** 기본 규칙 옵션을 구성합니다.

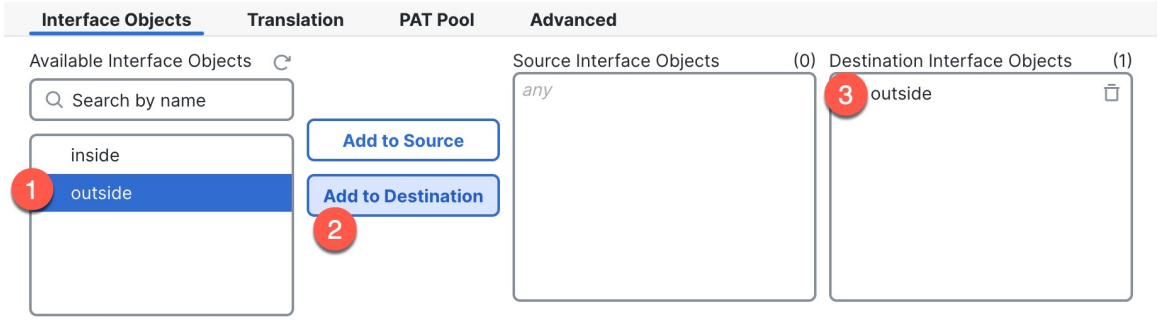
그림 ***10:*** 기본 규칙 옵션



- **NAT Rule(NAT** 규칙**) - Auto NAT Rule(**자동 **NAT** 규칙**)**을 선택합니다.
- **Type(**유형**) - Dynamic(**동적**)**을 선택합니다.

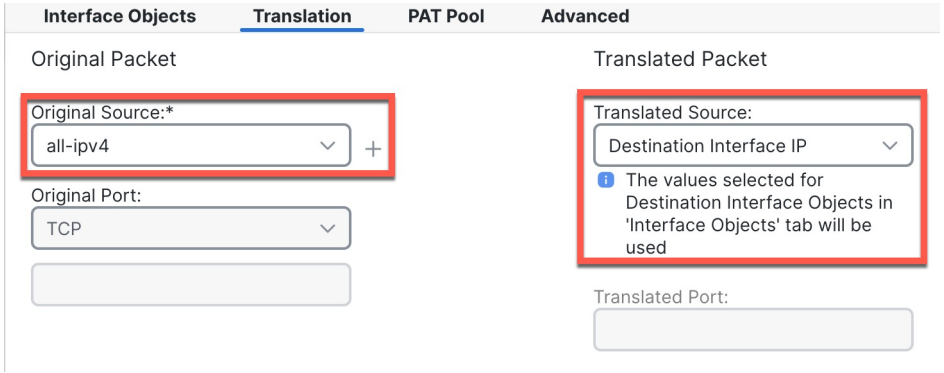
단계 **5** **Interface Objects(**인터페이스 개체**)** 페이지에서 **Available Interface Objects(**사용 가능한 인터페이스 개체**)** 영역의 외부 영역을 **Destination Interface objects(**대상 인터페이스 개체**)** 영역에 추가합니다.

그림 ***11:*** 인터페이스 개체



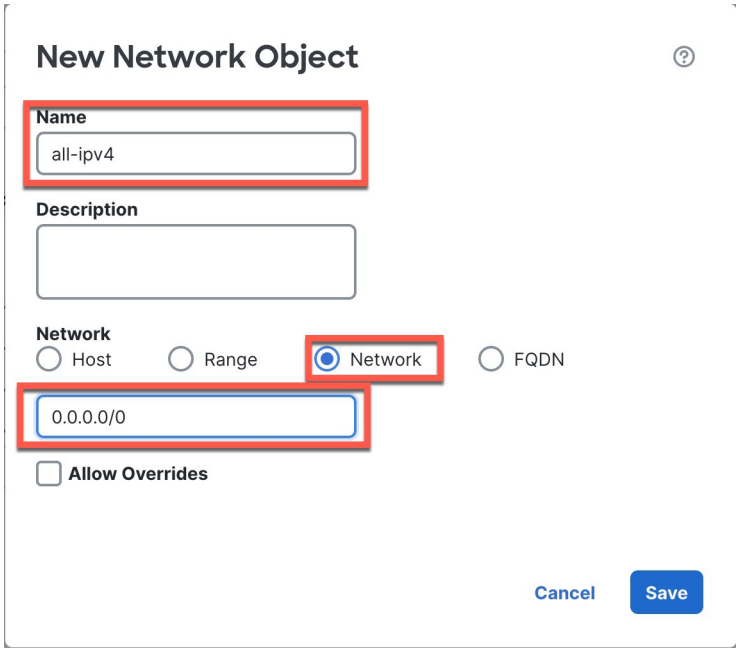
단계 **6** **Translation(**변환**)** 페이지에서 다음 옵션을 설정합니다.

그림 ***12:*** 변환



- **Original Source(**원본 소스**)**- 모든 IPv4 트래픽(**0.0.0.0/0**)에 대한 네트워크 개체를 추가하려면 **Add(**추가**)** (+)를 클릭합니다.

그림 ***13:*** 새 네트워크 개체



참고
자동 NAT 규칙은 개체 정의의 일부로 NAT를 추가하고 시스템 정의 개체를 수정할 수 없기 때문에 시스템에서 정의된 **any-ipv4** 개체를 사용할 수 없습니다.

- **Translated Source(**변환된 소스**) - Destination Interface IP(**대상 인터페이스 **IP)**를 선택합니다.

단계 **7** **Save(**저장**)**를 클릭하여 규칙을 저장하십시오.

규칙이 **Rules(**규칙**)** 테이블에 저장됩니다.

단계 **8** 변경 사항을 저장하려면 **NAT** 페이지에서 **Save(**저장**)**를 클릭합니다.

액세스 제어 규칙을 구성합니다.

디바이스를 등록할 때 기본 액세스 컨트롤 정책인 **Block all traffic(**모든 트래픽 차단**)**을 생성했다면, 디바이스에 트래픽을 허용하기 위해 정책에 규칙을 추가해야 합니다. 액세스 제어 정책은 순서대로 평가되는 여러 규칙을 포함할 수 있습니다.

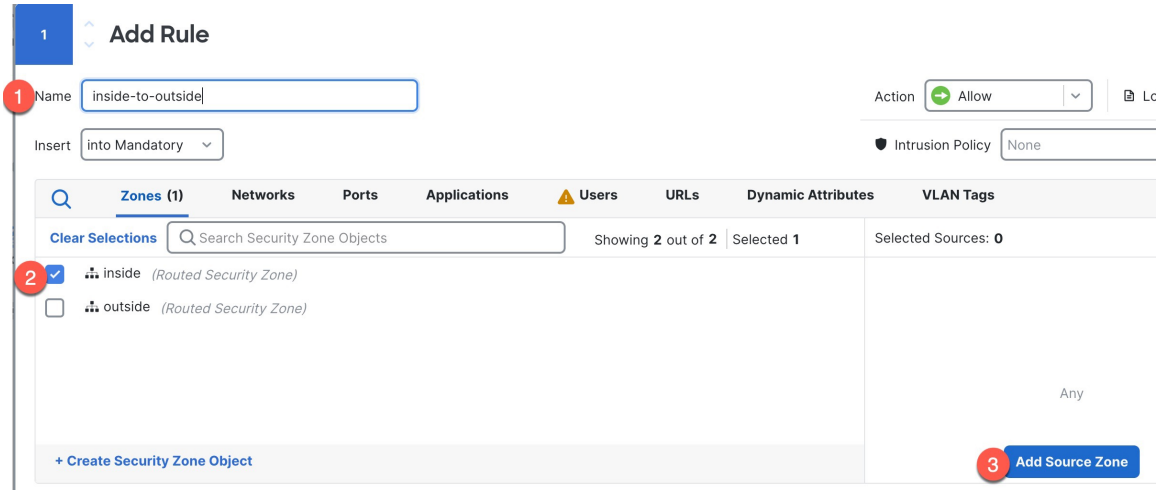
이 절차는 내부 영역에서 외부 영역으로의 모든 트래픽을 허용하는 액세스 제어 규칙을 생성합니다.

프로시저

단계 **1** **Policies(**정책**)** > **Security policies(**보안 정책**)** > **Access Control(**액세스 제어**)**을 선택하고 편집( )에 할당된 액세스 컨트롤 정책에 대해 디바이스를 클릭합니다.

단계 **2** **Add Rule(**규칙 추가**)**을 클릭하고 다음 매개변수를 설정합니다.

그림 ***14:*** 소스 영역

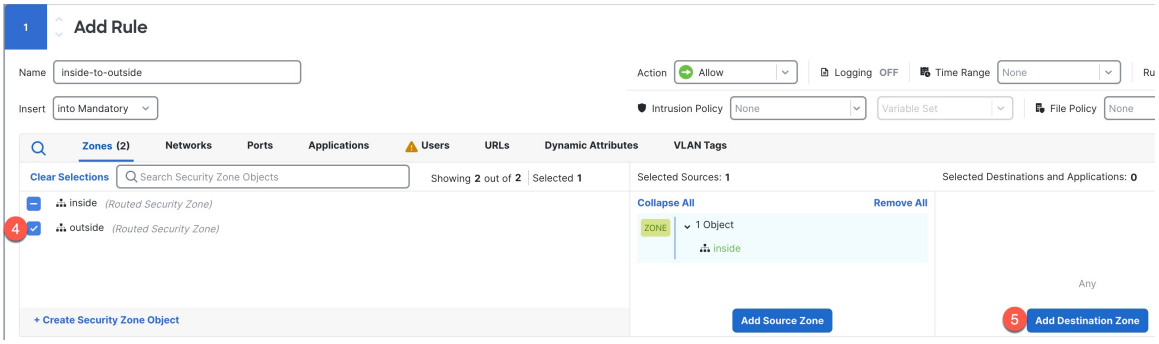


1. 예를 들어 이 규칙의 이름을 **inside-to-outside**로 지정합니다.

2. Zones(영역**)**에서 내부 영역을 선택합니다.

3. Add Source Zone(소스 영역 추가**)**을 클릭합니다.

그림 ***15:*** 대상 영역



4 . Zones(영역**)**에서 외부 영역을 선택합니다.

5. Add Destination Zone(대상 영역 추가**)**을 클릭합니다.

기타 설정은 변경하지 않습니다.

단계 **3** (선택 사항) 패킷 흐름 다이어그램에서 정책 유형을 클릭하여 연결된 정책을 사용자 지정합니다.

액세스 제어 규칙보다 사전 필터, 해독, Security Intelligence 및 ID 정책이 먼저 적용됩니다. 이러한 정책을 사용자 지정할 필요는 없지만, 네트워크의 요구 사항을 파악한 후에는 신뢰할 수 있는 트래픽을 단축 경로 지정(처리 우회)하거나 트래픽을 차단하여 추가 처리가 필요 없도록 함으로써 네트워크 성능을 개선할 수 있습니다.

그림 ***16:*** 액세스 제어 전에 적용된 정책

- 사전 필터 규칙 - 기본 사전 필터 정책은 모든 트래픽을 전달하여 다른 규칙이 조치(분석)를 취하도록하도록 합니다. 기본 정책에 대한 유일한 변경 사항은 터널 트래픽을 차단하는 것입니다. 그렇지 않으면 분석(전달), 단축 경로 지정(우회 확인 우회) 또는 차단을 수행할 수 있는 액세스 제어 정책과 연결할 새 사전 필터 정책을 생성할 수 있습니다.

  사전 필터를 사용하면 트래픽이 더 이상 발생하기 전에 차단하거나 단축 경로를 지정하여 성능을 개선할 수 있습니다. 새 정책에서 터널 규칙 및 사전 필터 규칙을 추가할 수 있습니다. 터널 규칙을 사용하면 평문(비암호화) 패스스루 터널을 단축경로 처리, 차단 또는 영역을 다시 지정할 수 있습니다. 사전 필터 규칙을 사용하면 IP 주소, 포트 및 프로토콜로 식별된 비터널 트래픽을 단축경로 처리하거나 차단할 수 있습니다.

  예를 들어 네트워크의 모든 FTP 트래픽을 차단하려고 하지만, 관리자 로부터의 단축경로 SSH 트래픽을 차단하려는 경우 새 사전 필터 정책을 추가할 수 있습니다.

- **Decryption(**해독**)** - 기본적으로 해독이 적용되지 않습니다. 해독은 네트워크 트래픽을 심층 검사에 노출하는 방법입니다. 대부분의 경우 트래픽은 해독을 원하지 않으며, 법적으로 허용되는 경우에만 가능합니다. 네트워크 보호를 극대화하려면 중요한 서버로 이동하거나 신뢰할 수 없는 네트워크 세그먼트에서 오는 트래픽 해독 정책을 사용하는 것이 좋습니다.

- **Security Intelligence**- (IPS 라이선스 필요) Security Intelligence는 기본적으로 활성화되어 있습니다. Security Intelligence는 추가 처리를 위해 액세스 제어 정책에 연결을 전달하기 전에 적용되는 악의적인 활동에 대한 또 다른 초기 방어 수단입니다. Security Intelligence는 평판 인텔리전스를 사용하여 시스코의 위협 인텔리전스 조직인 Talos에서 제공하는 IP 주소, URL 및 도메인 이름과의 연결을 신속하게 차단합니다. 원하는 경우 추가 IP 주소, URL 또는 도메인을 추가하거나 삭제할 수 있습니다.

  참고
  IPS 라이선스가 없는 경우 이 정책은 액세스 제어 정책에서 활성화된 것으로 표시되더라도 구축되지 않습니다.

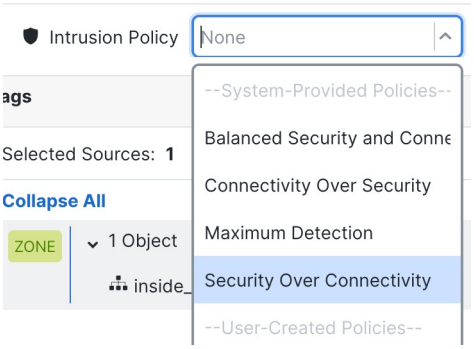
- **ID** - ID는 기본적으로 적용되지 않습니다. 액세스 제어 정책에 따라 트래픽을 처리하도록 허용하기 전에 사용자에게 인증을 요구할 수 있습니다.

단계 **4** (선택 사항) 액세스 제어 규칙 뒤에 적용되는 침입 정책을 추가합니다.

침입 정책은 보안 위반의 트래픽을 검사하는 침입 탐지 및 방지 설정의 정의된 집합입니다. Firewall Management Center에는 있는 그대로 활성화하거나 맞춤화할 수 있는 여러 시스템 제공 정책이 포함되어 있습니다. 이 단계에서는 시스템 제공 정책을 활성화합니다.

a) **Intrusion Policy(**침입 정책**)** 드롭다운 목록을 클릭합니다.

그림 *17:* 시스템 제공 침입 정책

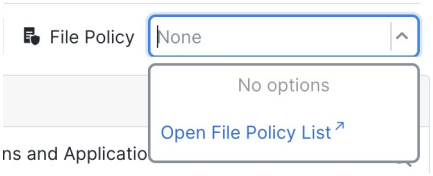


b) 목록에서 시스템 제공 정책 중 하나를 선택합니다.

단계 **5** (선택 사항) 액세스 제어 규칙 뒤에 적용되는 파일 정책을 추가합니다.

a) **File Policy(**파일 정책**)** 드롭다운 목록을 클릭하고 기존 정책을 선택하거나 **Open File Policy List(**파일 정책 목록 열기**)**를선택하여 정책을 추가합니다.

그림 *18:* 파일 정책



새 정책의 경우 **Policies(**정책**)** > **Security policies(**보안 정책**)** > **Malware & File(**멀웨어 및 파일**)** 페이지가 별도의 탭에 열립니다.

b) 정책 생성에 대한 자세한 내용은 *Cisco Secure Firewall Device Manager* 구성 가이드을 참조하십시오.

c) **Add Rule(**규칙 추가**)** 페이지로 돌아가 드롭다운 목록에서 새로 생성된 정책을 선택합니다.

단계 **6** **Apply(**적용**)**를 클릭합니다.

규칙이 **Rules(**규칙**)** 테이블에 추가됩니다.

단계 **7** **Save(**저장**)**를 클릭합니다.

외부 인터페이스에서 SSH 활성화

이 섹션에서는 외부 인터페이스에서 하나 이상의 데이터 또는 진단 인터페이스에 대한 SSH 연결을 활성화하는 방법을 설명합니다.

기본적으로 초기 설정 중에 비밀번호를 구성한 **admin** 사용자가 있습니다.

프로시저

단계 1 **Devices(**디바이스**)** > **Platform Settings(**플랫폼 설정**)**를 선택하고 Firewall Threat Defense 정책을 생성하거나 편집합니다.

단계 2 **Secure Shell(**보안 쉘**)**을 선택합니다.

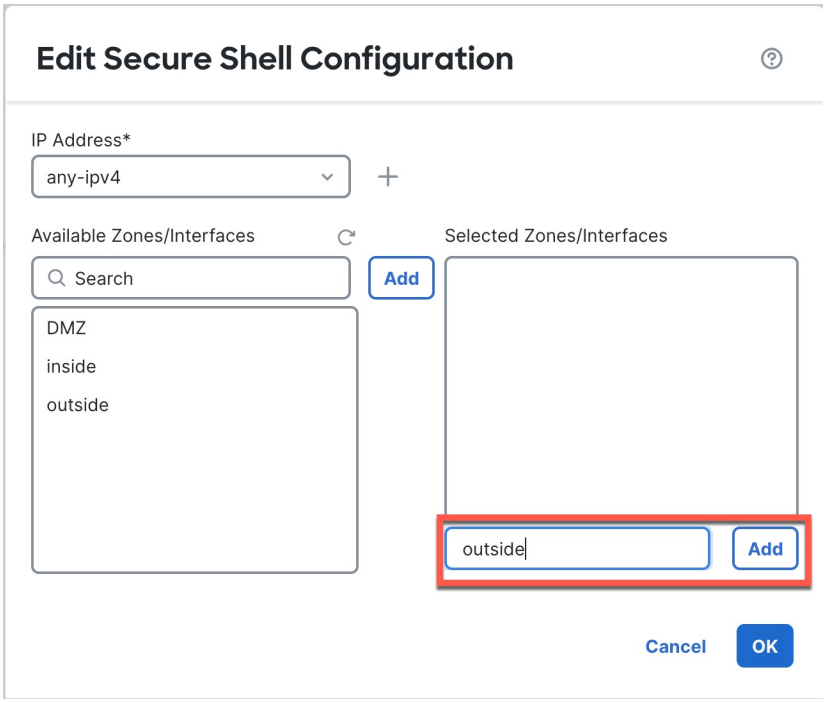
단계 3 SSH 연결을 허용하는 외부 인터페이스와 IP 주소를 확인합니다.

a) **Add(**추가**)**를 클릭해 새 규칙을 추가하거나, **Edit(**편집**)**을 클릭해 기존 규칙을 편집합니다.

b) 규칙 속성을 구성합니다.

- **IP Address(IP** 주소**)** - SSH 연결을 허용하는 호스트 또는 네트워크를 식별하는 네트워크 개체 또는 그룹입니다. 드롭다운 메뉴에서 개체를 선택하거나 +를 클릭하여 새 네트워크 개체를 추가합니다.
- **Available Zones/Interfaces(**사용할 수 있는 영역/인터페이스**) - Selected Zones/Interface(**선택한 영역/ 인터페이스**)** 목록 아래 필드에 외부 영역을 추가하거나 외부 인터페이스 이름을 입력한 후 **Add(**추가**)**를 클릭합니다.

그림 ***19:*** 외부 인터페이스에서 ***SSH*** 활성화



c) **OK(**확인**)**를 클릭합니다.

단계 4 **Save(**저장**)**를 클릭합니다.

이제 **Deploy(구축)** > **Deploy(구축)**로 이동하여 할당된 디바이스에 정책을 구축할 수 있습니다. 변경사항은 구축할 때까지 활성화되지 않습니다.

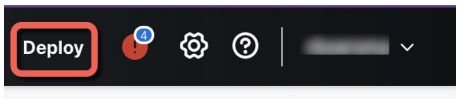
구성 구축

디바이스에 설정 변경 사항을 구축합니다. 구축하기 전에는 디바이스에서 변경 사항이 활성 상태가 아닙니다.

프로시저

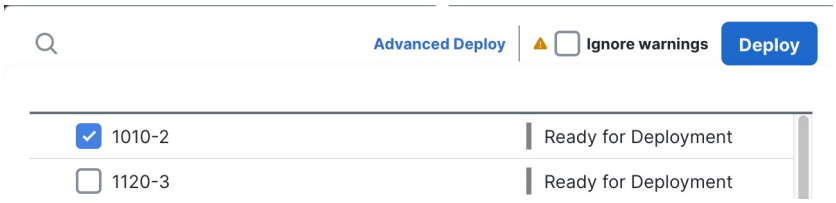
단계 **1** 우측 상단에서 **Deploy(구축)**를 클릭합니다.

그림 ***20:*** 구축



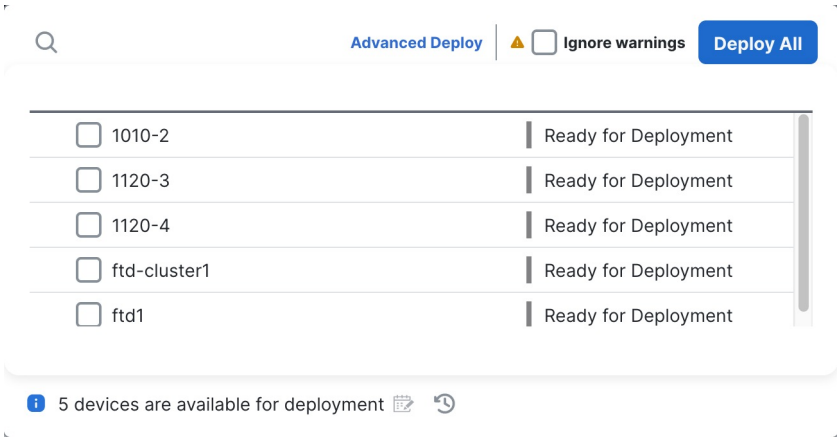
단계 **2** 빠르게 구축하려면 특정 디바이스를 선택한 다음 **Deploy(구축)**를 클릭합니다.

그림 ***21:*** 선택 항목 구축



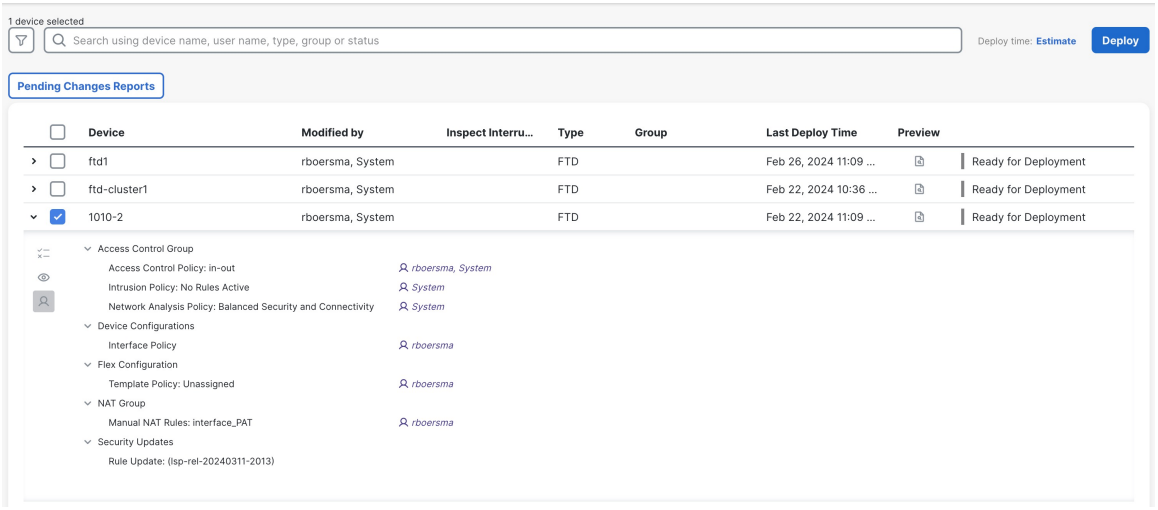
또는 **Deploy All(모두 구축)**을 클릭하여 모든 디바이스에 구축합니다.

그림 ***22:*** 모두 구축



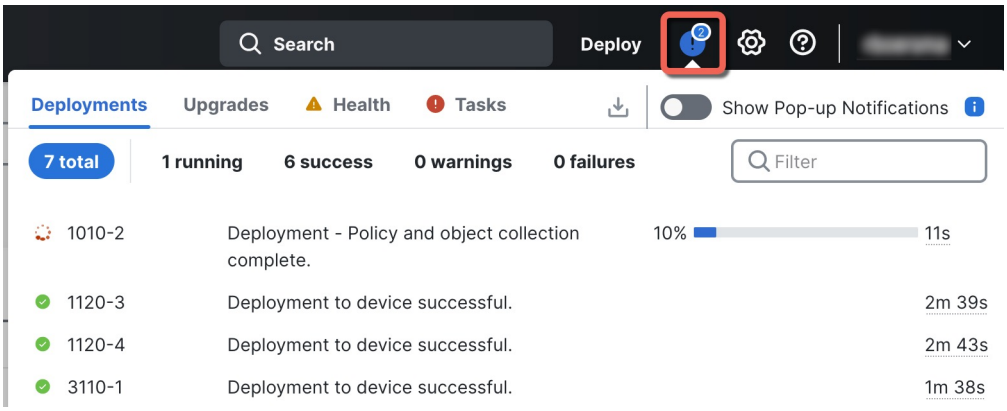
그렇지 않으면 추가 구축 옵션에 대해 Advanced Deploy(고급 구축)를 클릭합니다.

그림 ***23:*** 고급 구축



단계 **3** 구축이 성공하는지 확인합니다. 메뉴 모음의 **Deploy(구축)** 버튼 오른쪽에 있는 아이콘을 클릭하여 구축 상태를 확인합니다.

그림 ***24:*** 구축 상태



번역에 관하여
Cisco는 일부 지역에서 본 콘텐츠의 현지 언어 번역을 제공할 수 있습니다. 이러한 번역은 정보 제공의 목적으로만 제공되며, 불일치가 있는 경우 본 콘텐츠의 영어 버전이 우선합니다.

번역에 관하여
Cisco는 일부 지역에서 본 콘텐츠의 현지 언어 번역을 제공할 수 있습니다. 이러한 번역은 정보 제공의 목적으로만 제공되며, 불일치가 있는 경우 본 콘텐츠의 영어 버전이 우선합니다.