Firepower Management Center로 Firepower Threat Defense Virtual 관리

이 장에서는 FMC로 관리되는 독립형 FTDv 디바이스를 구축하는 방법을 설명합니다.

참고 이 문서에서는 최신 FTDv 버전의 기능 이전 버전의 소프트웨어를 사용할 경우에는 해당 버전에 대한 FMC 설정 가이드의 절차를 참조하십시오.

Firepower Management Center를 이용한 Firepower Threat Defense Virtual 관련 정보

Firepower Threat Defense Virtual(FTDv)은(는) Cisco NGFW 솔루션의 가상화된 구성 요소입니다. FTDv은 스테이트풀 방화벽, 라우팅, NGIPS(Next-Generation Intrusion Prevention System), AVC(Application Visibility and Control), URL 필터링, AMP(Advanced Malware Protection)와 같은 차세대 방화벽 서비스를 제공합니다.

전체 기능을 갖춘 별도 서버의 다중 디바이스 관리자인 Firepower Management Center(FMC)을 사용해 FTDv을 관리할 수 있습니다. FMC 설치에 대한 자세한 내용은 FMC시작 가이드를 참조하십시오.

FTDv은 FTDv 가상 머신에 할당한 관리 인터페이스의 FMC에 등록하고 통신합니다.

문제 해결을 위해 관리 인터페이스에서 SSH를 사용해 FTD CLI에 액세스하거나, Firepower CLI에서 FTD에 연결할 수 있습니다.

Firepower Management Center에 로그인

FMC을 사용해 FTD를 구성하고 모니터링합니다.

시작하기 전에

지원되는 브라우저에 대한 자세한 내용은 사용 중인 버전의 릴리스 노트를 참조하십시오 (https://www.cisco.com/go/firepower-notes 참조).

프로시저

단계 **1** 지원되는 브라우저를 사용해 다음 URL을 입력합니다.

https://*fmc_ip_address*

*fmc_ip_address*가 FMC의 IP 주소 또는 호스트 이름을 식별합니다.

단계 **2** 사용자 이름 및 비밀번호를 입력합니다.

단계 **3** **Log In(**로그인**)**을 클릭합니다.

Firepower Management Center로 디바이스 등록

시작하기 전에

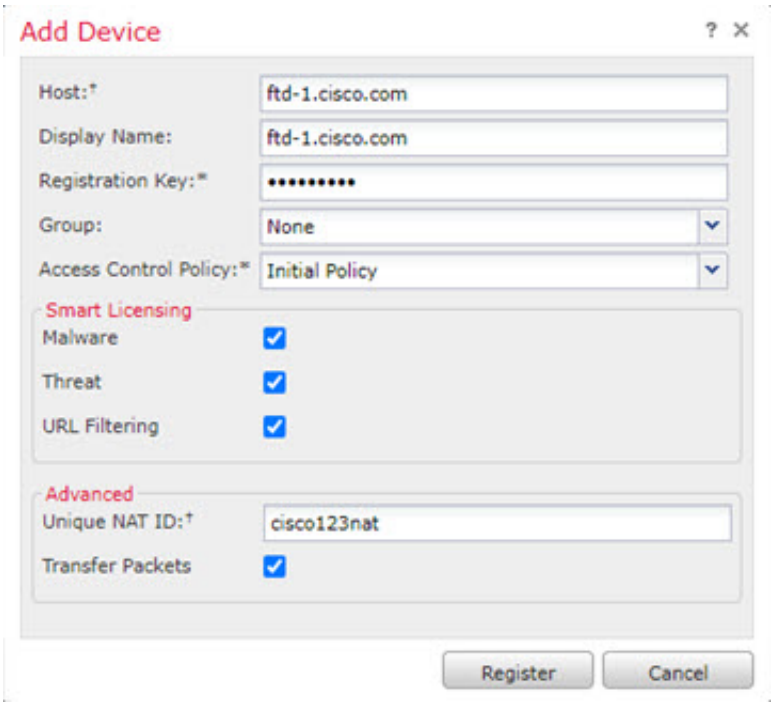
FTDv 가상 머신이 성공적으로 구축되었으며, 전원이 켜져 있고 첫 번째 부팅 절차를 완료했는지 확인하십시오.

참고 이 절차는 day0/부트스트랩을 통해서 FMC에 대한 등록 정보가 제공된 것으로 가정합니다. 그러나 이러한 모든 설정은 **configure network(**네트워크 구성**)** 명령을 사용하여 CLI에서 나중에 변경할 수 있습니다. FTD 명령 참조를 참조하십시오.

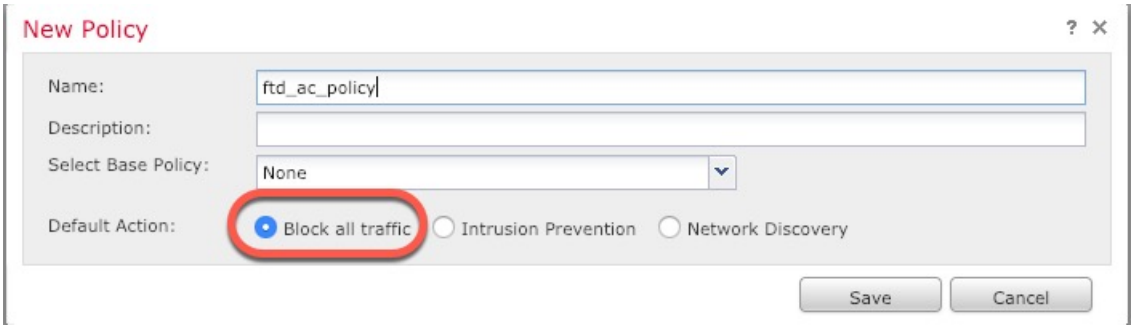
프로시저

단계 **1** **Devices(**디바이스**)** > **Device Management(**디바이스 관리**)**를 선택합니다.

단계 **2** **Add(**추가**)** 드롭다운 목록에서 **Add device(**디바이스 추가**)**를 선택하고 다음 매개변수를 입력합니다.



- **Host(**호스트**)**—추가하고자 하는 디바이스의 IP 주소를 입력합니다.
- **Display Name(**표시 이름**)**—FMC에 표시하고자 하는 디바이스 이름을 입력합니다.
- **Registration key(**등록 키**)** - FTDv 부트스트랩 구성에서 지정한 것과 동일한 등록 키를 입력합니다.
- **Domain(**도메인**)** - 멀티 도메인 환경이 있는 경우 리프 도메인에 디바이스를 할당합니다.
- **Group(**그룹**)** - 그룹을 사용하는 경우 디바이스 그룹에 할당합니다.
- **Access Control Policy(**액세스 제어 정책**)** - 초기 정책을 선택합니다. 사용해야 하는 맞춤형 정책이 이미 있는 경우가 아니라면 **Create new policy(**새 정책 생성**)**, **Block all traffic(**모든 트래픽 차단**)**을 선택합니다. 나중에 트래픽을 허용하도록 변경할 수 있습니다. 액세스 제어 구성, 14 페이지을 참조하십시오.



- **Smart license (**스마트 라이선싱**)** - 구축하려는 기능에 필요한 스마트 라이선스(AMP 악성코드 검사를 사용하려는 경우 **Malware(**악성코드**)**, 침입 방지를 사용하려는 경우 **Threat(**위협**)** , 카테고리 기반 URL 필터링을 구현하려는 경우 **URL**)를 할당합니다.
- **Unique NAT ID(**고유 **NAT ID)** - FTDv 부트스트랩 구성에서 지정한 NAT ID를 지정합니다.
- **Transfer Packets(**패킷 전송**)** - 디바이스가 FMC에 패킷을 전송하도록 허용합니다. 이 옵션이 활성화되어 IPS 또는 Snort 같은 이벤트가 트리거되면 디바이스는 검사를 위해 이벤트 메타데이터 정보 및 패킷 데이터를 FMC에 전송합니다. 비활성화하면 FMC에 이벤트 정보만 전송하고 패킷 데이터는 전송하지 않습니다.

단계 **3** **Register(**등록**)**를 클릭하여 성공적인 등록을 확인합니다.

등록에 성공하면 디바이스가 목록에 추가됩니다. 오류가 발생하면 오류 메시지가 표시됩니다. FTDv 등록에 실패하면 다음 항목을 확인하십시오.

- Ping - 다음 명령을 사용해 FTD CLI(Firepower Threat Defense CLI 액세스, 16 페이지)에 액세스하고 FMC IP 주소에 Ping을 보냅니다.

  ping system *ip_address*

  Ping이 실패하는 경우 **show network** 명령을 사용해 네트워크 설정을 확인합니다. FTD IP 주소를 변경해야 하는 경우 **configure network** {**ipv4** | **ipv6**} **manual** 명령을 사용합니다.
- NTP - NTP 서버가 **System(**시스템**)** > **Configuration(**설정**)** > **Time Synchronization(**시간 동기화**)** 페이지에서 설정한 FMC 서버와 일치하는지 확인합니다.
- 등록 키, NAT ID 및 FMC IP 주소 - 두 디바이스에서 동일한 등록 키 및 NAT ID가 사용되고 있는지 확인합니다. **configure manager add** 명령을 사용해 FTDv에서 등록 키 및 NAT ID를 설정할 수 있습니다. 이 명령을 사용해 FMC IP 주소를 변경할 수도 있습니다.

기본 보안 정책 구성

이 섹션에서는 다음 설정을 사용해 기본 보안 정책을 구성하는 방법에 대해 설명합니다.

- 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.

프로시저

인터페이스 구성

FTDv 인터페이스를 활성화하고, 보안 영역에 이를 할당하며, IP 주소를 설정합니다. 일반적으로 시스템이 의미 있는 트래픽을 전달하도록 최소 2개 이상의 인터페이스를 구성해야 합니다. 일반적으로 업스트림 라우터 또는 인터넷과 만나는 외부 인터페이스와 조직 네트워크에서 사용하는 하나 이상의 내부 인터페이스를 사용합니다. 이런 인터페이스의 일부는 웹 서버와 같이 공개적으로 액세스할 수 있는 에셋을 배치하는 '비무장지대(DMZ)'로 사용하게 됩니다.

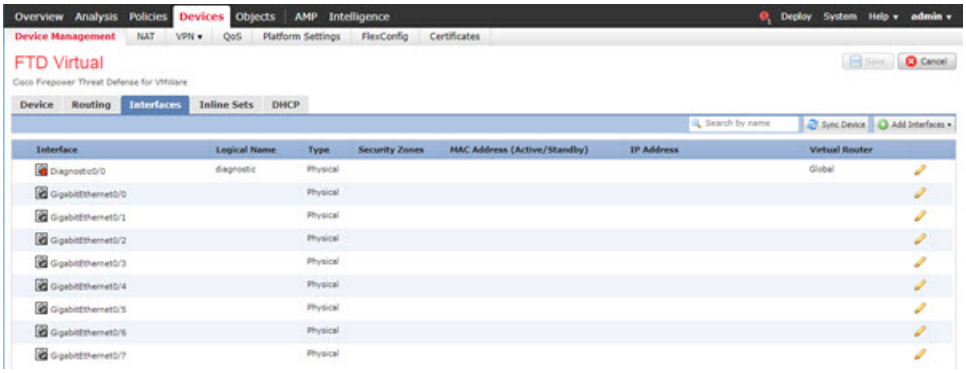
일반적인 에지 라우팅 상황의 경우, 내부 인터페이스에서 정적 주소를 정의하는 반면 ISP에서 온 DHCP를 통해 외부 인터페이스 주소를 가져옵니다.

다음 예에서는 DHCP를 사용하는 외부 인터페이스에서 고정 주소 및 라우팅 모드를 사용하여 인터페이스 내부에 라우팅 모드를 구성합니다.

프로시저

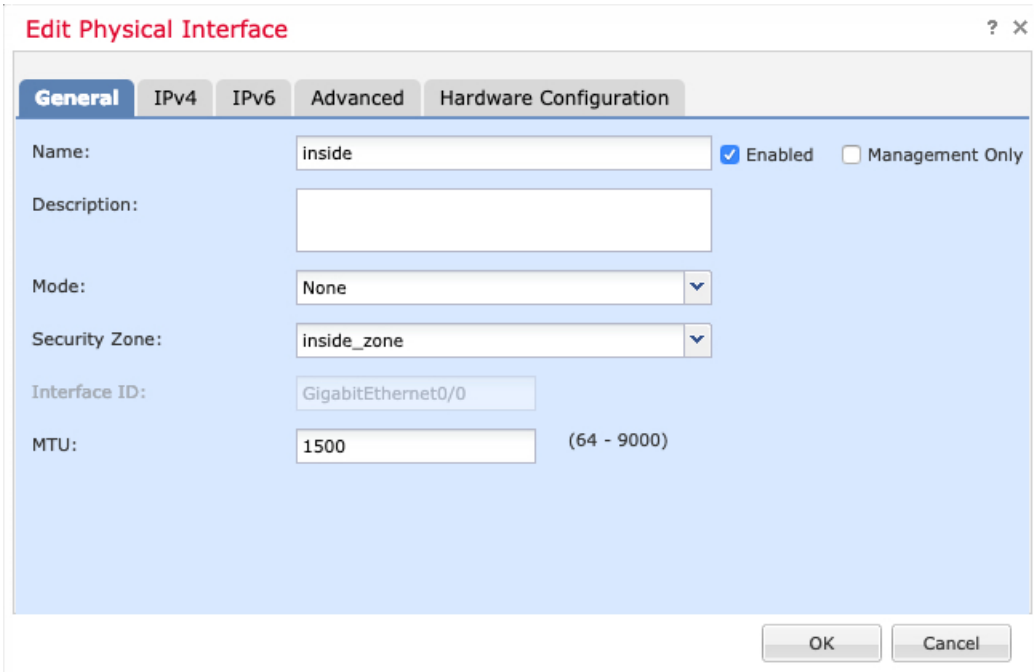
단계 1 **Devices(**디바이스**)** > **Device Management(**디바이스 관리**)**를 선택하고 디바이스의 수정( )을(를) 클릭합니다.

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



단계 3 내부에 사용할 인터페이스의 수정( )를 클릭합니다.

General(일반**)** 탭이 표시됩니다.



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

예를 들어 인터페이스에 **inside**라는 이름을 지정합니다.

b) **Enable(**활성화**)** 확인란을 선택합니다.

c) **Mode(**모드**)**는 **None(**없음**)** 상태로 남겨둡니다.

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

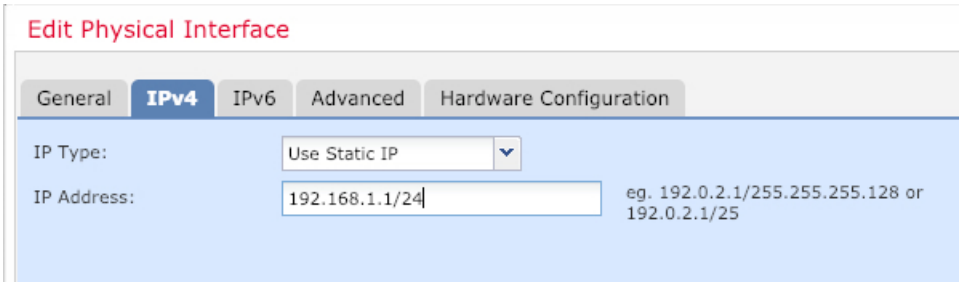
예를 들어 **inside_zone**이라는 영역을 추가합니다. 각 인터페이스는 보안 영역 및/또는 인터페이스 그룹에 할당되어야 합니다. 인터페이스는 하나의 보안 영역에만 속할 수 있지만, 여러 인터페이스 그룹에 속할 수도 있습니다. 영역 또는 그룹을 기준으로 보안 정책을 적용합니다. 예를 들어 내부 인터페이스는 내부 영역에, 외부 인터페이스는 외부 영역에 할당할 수 있습니다. 트래픽이 내부에서 외부로는 이동하지만 외부에서 내부로는 이동할 수 없도록 액세스 제어 정책을 구성할 수 있습니다. 대부분의 정책은 보안 영역만 지원합니다. NAT 정책, 사전 필터 정책, QoS 정책에서 영역이나 인터페이스 그룹을 사용할 수 있습니다.

e) **IPv4** 및/또는 **IPv6** 탭을 클릭 합니다.

참고 Google Cloud Platform의 VPC 네트워크는 IPv6를 지원하지 않습니다.

- **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.

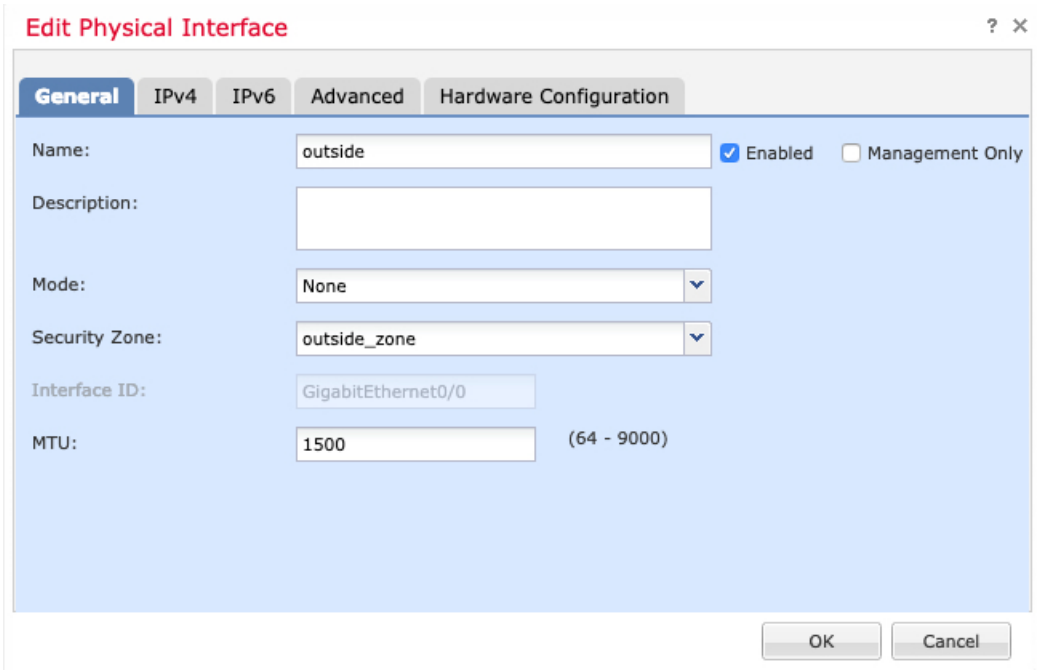


- **IPv6** - 상태 비저장 자동 구성을 하려면 **Autoconfiguration(**자동 구성**)** 확인란을 선택합니다.

f) **OK(**확인**)**를 클릭합니다.

단계 **4** 외부에서 사용하려는 인터페이스의 수정( )를 클릭합니다.

General(일반**)** 탭이 표시됩니다.



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

예를 들어, 인터페이스에 **outside**라는 이름을 지정합니다.

b) **Enable(**활성화**)** 확인란을 선택합니다.

c) **Mode(**모드**)**는 **None(**없음**)** 상태로 남겨둡니다.

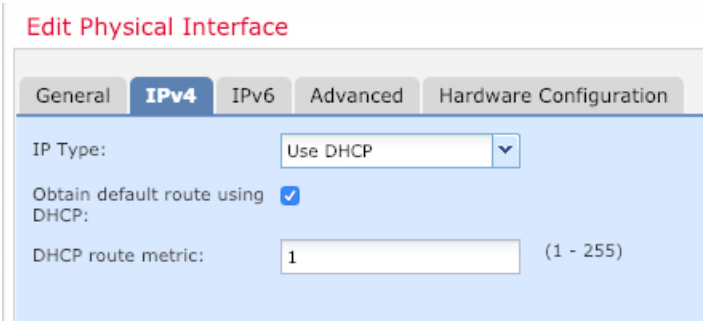
d) **Security Zone(**보안 영역**)** 드롭다운 목록에서 기존의 외부 보안 영역을 선택하거나 **New(**새로 만들기**)**를 클릭하여 새 보안 영역을 추가합니다.

예를 들어 **outside_zone**이라는 영역을 추가합니다.

e) **IPv4** 및/또는 **IPv6** 탭을 클릭 합니다.

참고 Google Cloud Platform의 VPC 네트워크는 IPv6를 지원하지 않습니다.

- **IPv4 - Use DHCP(DHCP** 사용**)**를 선택하여 다음 옵션 매개변수를 구성합니다.
  - **DHCP**에서 기본 경로 가져오기 - DHCP 서버에서 기본 경로를 가져옵니다.
  - **DHCP** 경로 메트릭 - 파악된 경로에 대해 1과 255 사이의 관리 거리를 할당합니다. 파악된 경로의 기본 관리 거리는 1입니다.



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

f) **OK(**확인**)**를 클릭합니다.

단계 **5** **Save(**저장**)**를 클릭합니다.

DHCP 서버 구성

참고 AWS, Azure, GCP, OCI 등의 퍼블릭 클라우드 환경에 구축하는 경우 이 절차를 건너 뜁니다.

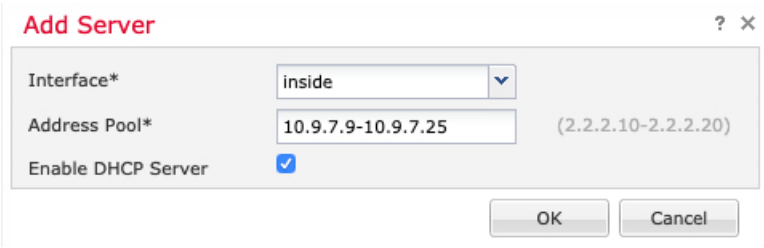
클라이언트가 DHCP를 사용하여 FTDv에서 IP 주소를 가져오게 하려면 DHCP 서버를 활성화합니다.

프로시저

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

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

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



- 인터페이스 - 드롭다운 목록에서 인터페이스를 선택합니다.
- **Address Pool(**주소 풀**)** - DHCP 서버에서 사용되는 최소 및 최대 IP 주소 범위를 설정합니다. 이 IP 주소 범위는 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.

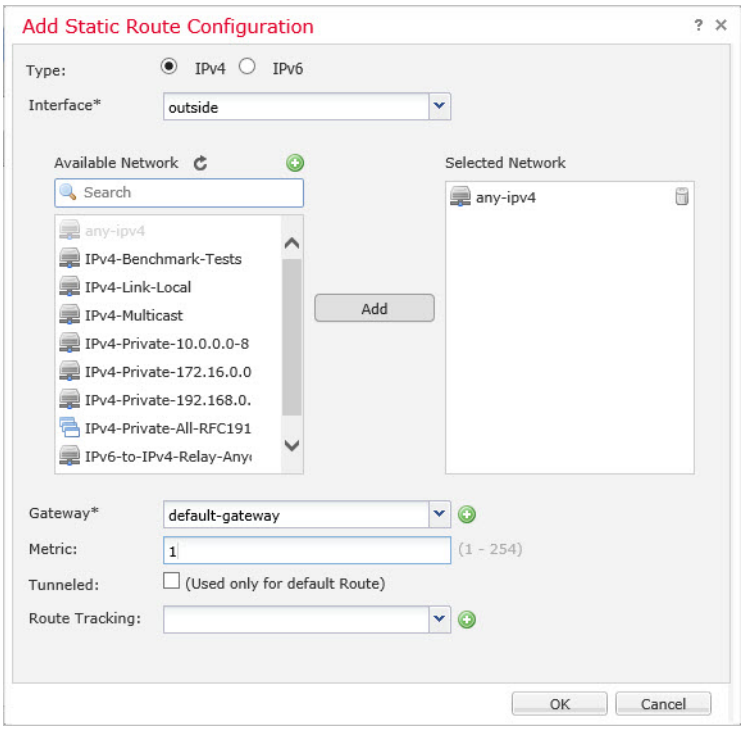
기본 경로 추가

기본 경로는 일반적으로 외부 인터페이스에서 접근 가능한 업스트림 라우터를 가리킵니다. 외부 인터페이스에 DHCP를 사용하는 경우 디바이스가 이미 기본 경로를 수신했을 수 있습니다. 수동으로 경로를 추가해야 하는 경우 이 절차를 완료합니다. DHCP 서버에서 기본 경로를 수신한 경우, **Devices(**디바이스**)** > **Device Management(**디바이스 관리**)** > **Routing(**라우팅**)** > **Static Route(**정적 경로**)** 페이지의 **IPv4 Routes(IPv4** 경로**)** 또는 **IPv6 Routes(IPv6** 경로**)** 테이블에 표시됩니다.

프로시저

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

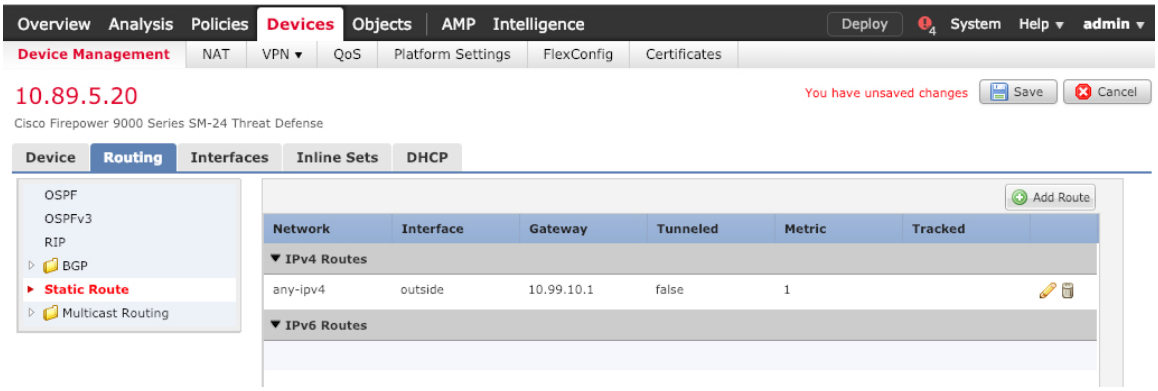
단계 **2** **Routing(**라우팅**)** > **Static Route(**정적 경로**)**를 선택하고 **Add Route(**경로 추가**)**를 클릭해 다음을 설정합니다.



- **Type(**유형**)** - 추가하려는 정적 경로 유형에 따라 **IPv4** 또는 **IPv6** 라디오 버튼을 클릭합니다.
- **Interface(**인터페이스**)** - 이그레스 인터페이스를 선택합니다. 일반적으로 외부 인터페이스입니다.
- **Available Network(**사용 가능한 네트워크**)** - IPv4 기본 경로에 대해 **any-ipv4**를 선택하거나, IPv6 기본 경로에 대해 **any-ipv6**를 선택합니다.
- **Gateway(**게이트웨이**)** 또는 **IPv6 Gateway(IPv6** 게이트웨이**)** - 이 경로의 다음 홉인 게이트웨이 라우터를 입력 또는 선택합니다. IP 주소 또는 네트워크/호스트 개체를 제공할 수 있습니다.
- **Metric(**메트릭**)** - 대상 네트워크 홉 수를 입력합니다. 유효한 범위는 1~255이고 기본값은 1입니다.

단계 **3** **OK(**확인**)**를 클릭합니다.

경로가 고정 경로 테이블에 추가됩니다.



단계 **4** **Save(**저장**)**를 클릭합니다.

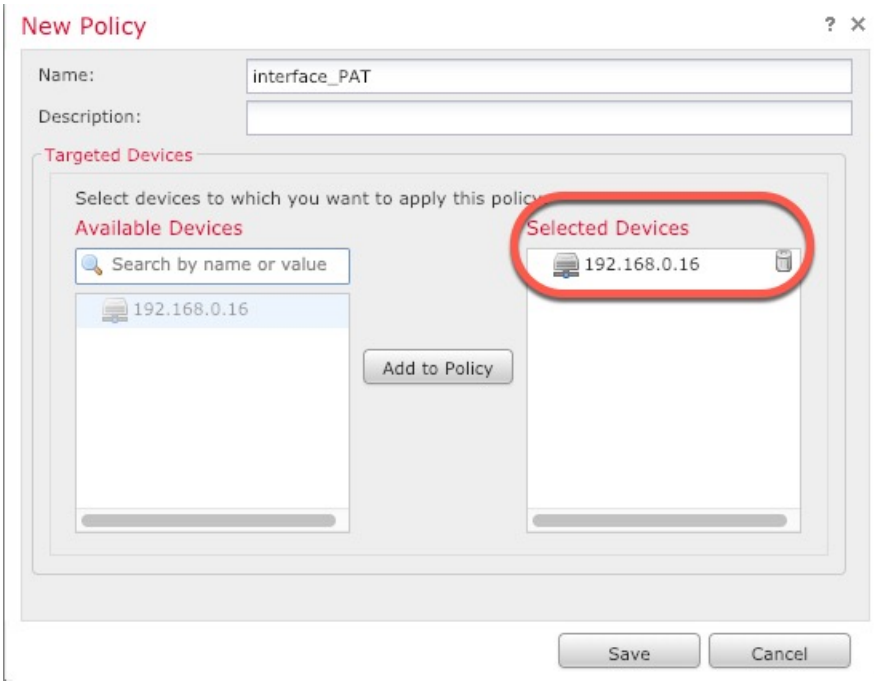
NAT 구성

일반적인 NAT 규칙은 내부 주소를 외부 인터페이스 IP 주소의 포트로 변환합니다. 이러한 유형의 NAT 규칙을 인터페이스 포트 주소 변환*(PAT)*이라고 합니다.

프로시저

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

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



정책이 FMC을 추가합니다. 계속해서 정책에 규칙을 추가해야 합니다.

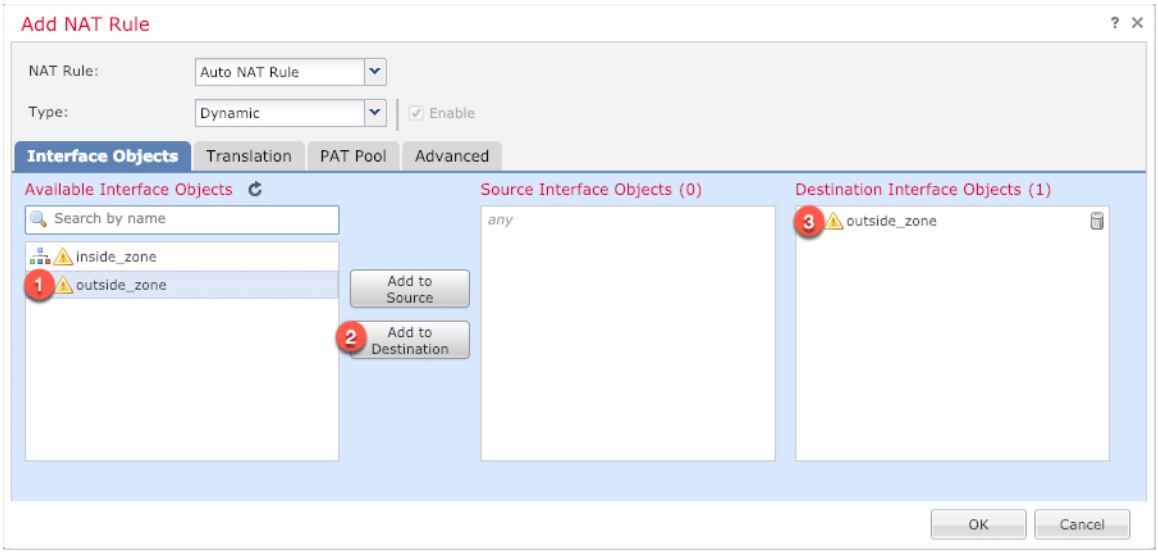
단계 **3** **Add Rule(**규칙 추가**)**을 클릭합니다.

Add NAT Rule(NAT 규칙 추가**)** 대화 상자가 나타납니다.

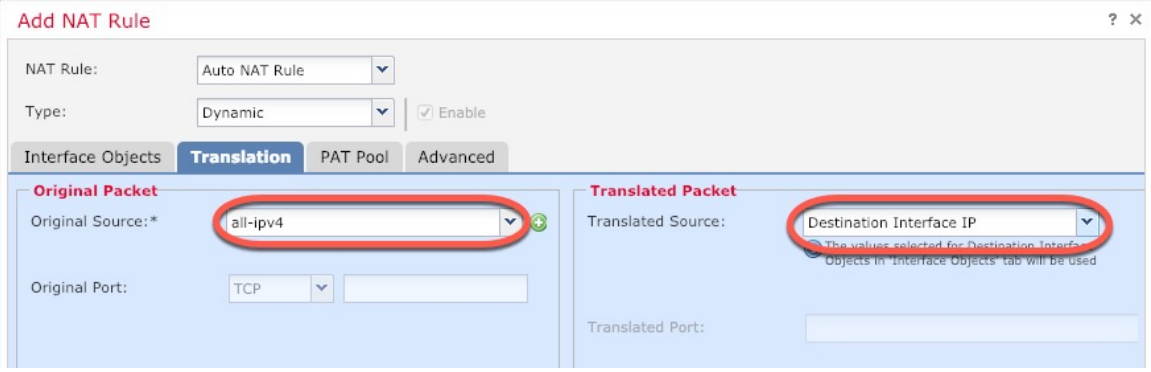
단계 **4** 기본 규칙 옵션을 구성합니다.

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

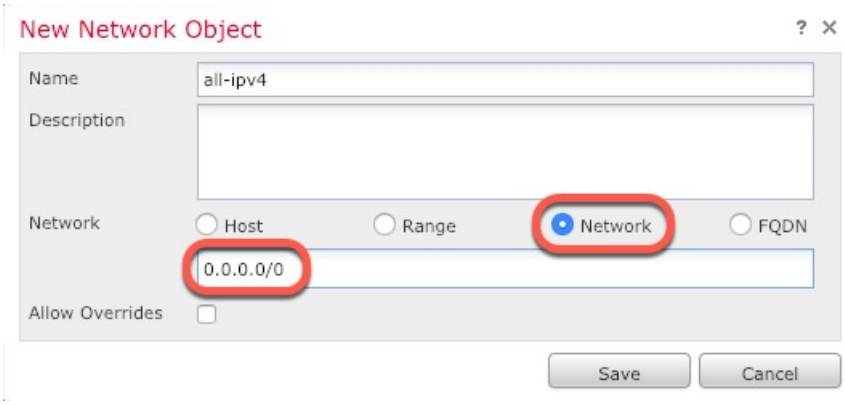
단계 **5** **Interface Objects(**인터페이스 개체**)** 페이지에서 **Available Interface Objects(**사용 가능한 인터페이스 개체**)** 영역의 외부 영역을 **Destination Interface objects(**대상 인터페이스 개체**)** 영역에 추가합니다.



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



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

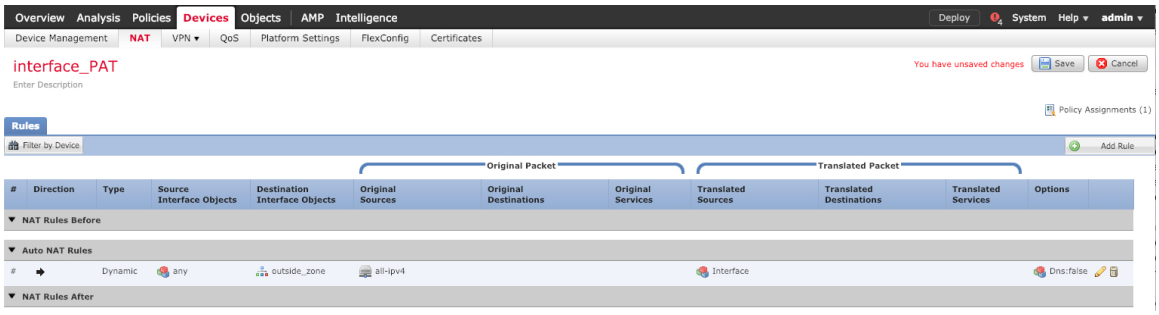


참고 자동 NAT 규칙은 개체 정의의 일부로 NAT를 추가하고 시스템 정의 개체를 수정할 수 없기 때문에 시스템에서 정의된 **any-ipv4** 개체를 사용할 수 없습니다.

- **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 구성

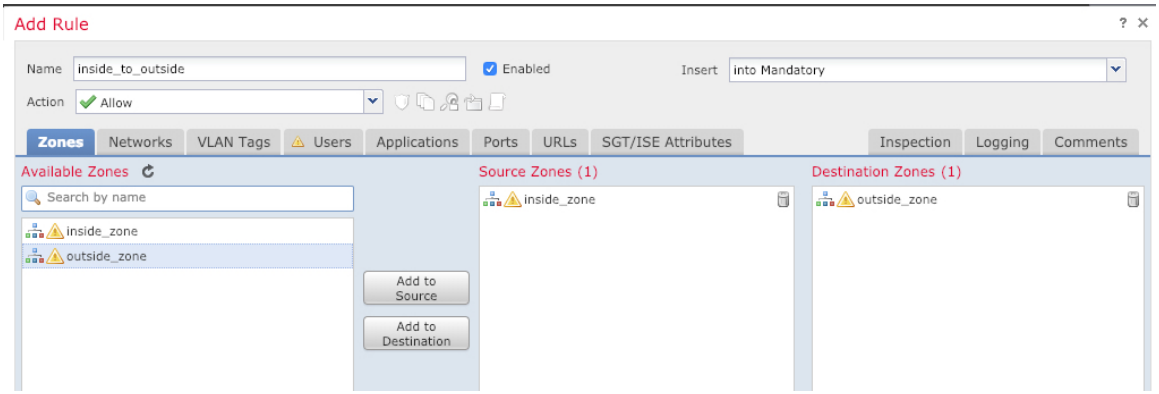
FMC을 사용해 FTDv를 등록할 때 기본 액세스 컨트롤 정책인 **Block all traffic(**모든 트래픽 차단**)**을 생성했다면, 디바이스에 트래픽을 허용하기 위해 정책에 규칙을 추가해야 합니다. 다음 절차에서는 내부 영역에서 외부 영역으로 향하는 트래픽을 허용하는 규칙을 추가합니다. 다른 영역이 있는 경우에는 적절한 네트워크에 대한 트래픽을 허용하는 규칙을 추가해야 합니다.

고급 보안 설정 및 규칙을 구성하려면 FMC 구성 가이드를 참조하십시오.

프로시저

단계 **1** **Policy(**정책**)** > **Access Policy(**액세스 정책**)** > **Access Policy(**액세스 정책**)**을 선택하고 FTD에 할당된 액세스 컨트롤 정책에 대해 수정( )를 클릭합니다.

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

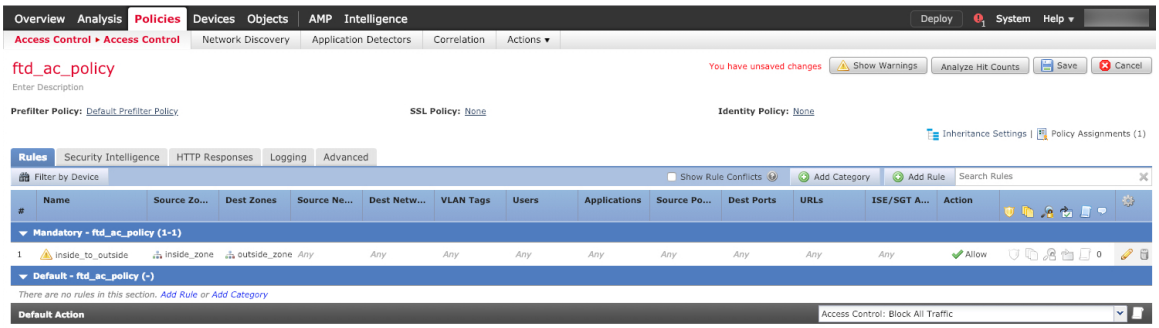


- **Name (**이름**)** - 예를 들어 이 규칙의 이름을 **inside_to_outside**로 지정합니다.
- **Source Zones(**원본 영역**)** - **Available Zones(**사용 가능한 영역**)**에서 내부 영역을 선택하고 **Add to Source(**원본에 추가**)**를 클릭합니다.
- **Destination Zones(**대상 영역**)** - **Available Zones(**사용 가능한 영역**)**에서 외부 영역을 선택하고 **Add to Destination(**대상에 추가**)**를 클릭합니다.

기타 설정은 변경하지 않습니다.

단계 **3** **Add(**추가**)**를 클릭합니다.

규칙이 **Rules(**규칙**)** 테이블에 추가됩니다.



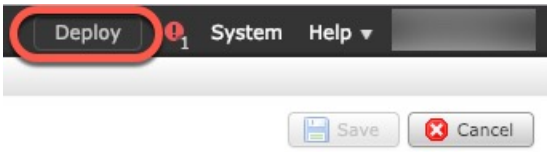
단계 **4** **Save(**저장**)**를 클릭합니다.

구성 구축

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

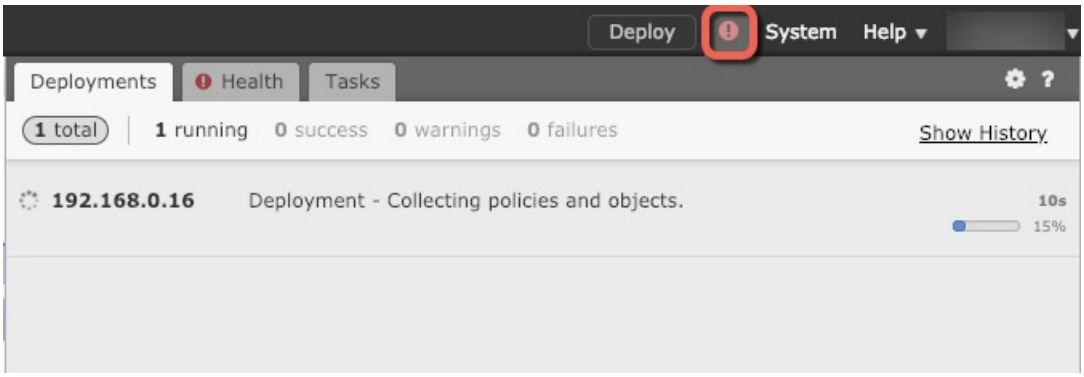
프로시저

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



단계 **2** **Deploy policy(**정책 구축**)** 대화 상자에서 디바이스를 선택한 다음 **Deploy(**구축**)**를 클릭합니다.

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



Firepower Threat Defense CLI 액세스

FTDv CLI를 사용하여 관리 인터페이스 매개변수를 변경하고 문제를 해결할 수 있습니다. SSH를 사용하여 관리 인터페이스에 액세스하거나 VMware 콘솔에서 연결하여 CLI에 액세스할 수 있습니다.

프로시저

단계 **1** (옵션 1) FTDv 관리 인터페이스 IP 주소로 직접 SSH.

가상 머신을 구축할 때 관리 IP 주소를 설정합니다. 초기 구축 시 **admin** 계정 및 비밀번호를 사용해 FTDv에 로그인합니다.

단계 **2** (옵션 2) VMware 콘솔을 열고 초기 구축 과정에 설정한 **admin** 계정의 기본 이름과 비밀번호를 사용해 로그인합니다.