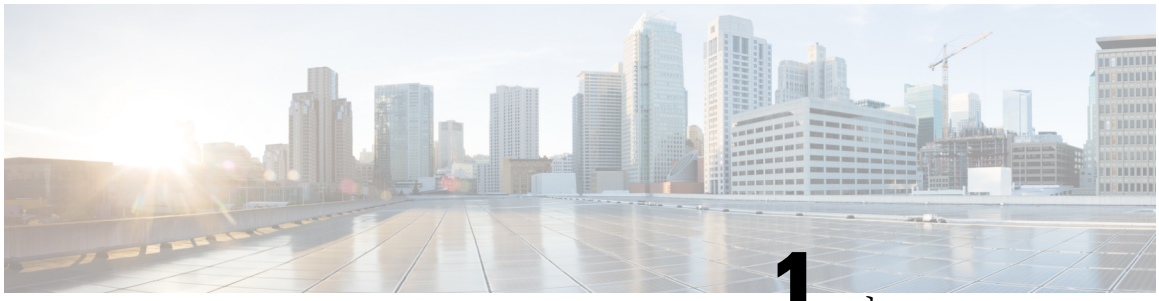
Google Cloud Platform용 Cisco Firepower Threat Defense Virtual 시작 가이드

초판: 2020년 10월 19일

최종 변경: 2020년 12월 11일

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



1 장

Firepower Threat Defense Virtual 및 Google Cloud Platform 시작하기

Firepower Threat Defense Virtual(FTDv)는 Cisco의 Firepower 차세대 방화벽 기능을 가상화된 환경으로 가져와 일관된 보안 정책으로 물리, 가상 및 클라우드 환경 전반 및 클라우드 간 워크로드를 준수하도록 합니다.

이 장에서는 기능 지원, 시스템 요구 사항, 지침, 제한 사항 등 Google Cloud Platform(GCP) 환경 내에서의 Firepower Threat Defense Virtual 기능에 대해 설명합니다. 이 장에서는 FTDv을(를) 관리하기 위한 옵션에 대해서도 설명합니다.

구축을 시작하기 전에 관리 옵션을 이해하는 것이 중요합니다. Firepower Management Center를 사용하여 FTDv을 관리하고 모니터링할 수 있습니다.

GCP에서 FTDv 구축

Firepower Threat Defense Virtual(FTDv)은 물리적 Cisco FTD와 동일한 소프트웨어를 실행하여 가상 폼 팩터에서 검증된 보안 기능을 제공합니다. FTDv은 퍼블릭 GCP에서 구축될 수 있습니다. 그러면 시간이 경과함에 따라 해당 위치를 확장, 축소 또는 이동하는 가상 및 물리적 데이터 센터 워크로드를 보호하기 위한 구성이 가능하게 됩니다.

GCP 시스템 유형 지원

FTDv 필요에 따라 Google 가상 머신 유형 및 크기를 선택합니다. 현재 FTDv은 컴퓨팅 최적화 및 범용 시스템(표준, 고용량 메모리 그리고 고 CPU 시스템 유형)을 모두 지원합니다.

참고 지원되는 시스템 유형은 예고 없이 변경될 수 있습니다.

표 *1:* 지원되는 컴퓨팅 최적화 시스템 유형

컴퓨팅 최적화 시스템 유형	속성	
	vCPUs	**RAM(GB)**
c2-standard-4	4	16GB
c2-standard-8	8	32GB
c2-standard-16	16	64GB

표 *2:* 지원되는 범용 시스템 유형

범용 시스템 유형	속성	
	vCPUs	**RAM(GB)**
n1-standard-4	4	15
n1-standard-8	8	30
n1-standard-16	16	60
n2-standard-4	4	16
n2-standard-8	8	32
n2-standard-16	16	64
n1-highcpu-8	8	7.2
n1-highcpu-16	16	14.4
n2-highcpu-8	8	8
n2-highmem-4	4	32
n2-highmem-8	8	64
n2-highmem-16	16	128

- FTDv에는 최소 4 개의 인터페이스가 필요합니다.
- 지원되는 최대 vCPU는 16개입니다.

GCP에서 계정을 생성하고, GCP Marketplace의 Cisco Firepower NGFW virtual firewall(NGFWv) 제품을 사용해서 VM 인스턴스를 실행한 다음 GCP 시스템 유형을 선택합니다.

FTDv 및 GCP의 사전 요건

- https://cloud.google.com에서 GCP 계정을 생성합니다.

- GCP 프로젝트를 생성합니다. Google 문서, 프로젝트 생성을 참조하십시오.
- Cisco Smart Account는 Cisco Software Central(https://software.cisco.com/)에서 생성할 수 있습니다.
- Firepower Threat Defense Virtual에 라이선스를 부여합니다.
  - Firepower Management Center의 보안 서비스에 대해 모든 라이선스 권한을 구성합니다.
  - 라이선스를 관리하는 방법에 대한 자세한 내용은 Firepower Management Center 구성 가이드의 *Firepower System* 라이선싱을 참조하십시오.
- 인터페이스 요구 사항:
  - 관리 인터페이스(2) - Firepower Threat Defense Virtual를 Firepower Management Center에 연결하는 데 사용되는 인터페이스, 진단에 사용되는 인터페이스는 통과 트래픽에는 사용할 수 없습니다.
  - 트래픽 인터페이스(2) - Firepower Threat Defense Virtual를 내부 호스트 및 공용 네트워크에 연결하는 데 사용됩니다.
- 통신 경로:
  - Firepower Threat Defense Virtual에 액세스하기 위한 공용 IP.
- FTDv 시스템 요구 사항은 Cisco FirePOWER 호환성 가이드를 참조하십시오.

FTDv 및 GCP의 지침 및 제한 사항

지원 기능

- GCP 컴퓨팅 엔진에서 구축
- 인스턴스당 최대 16개의 vCPU
- 라우팅 모드(기본값)
- 라이선싱 – BYOL만 지원됩니다.

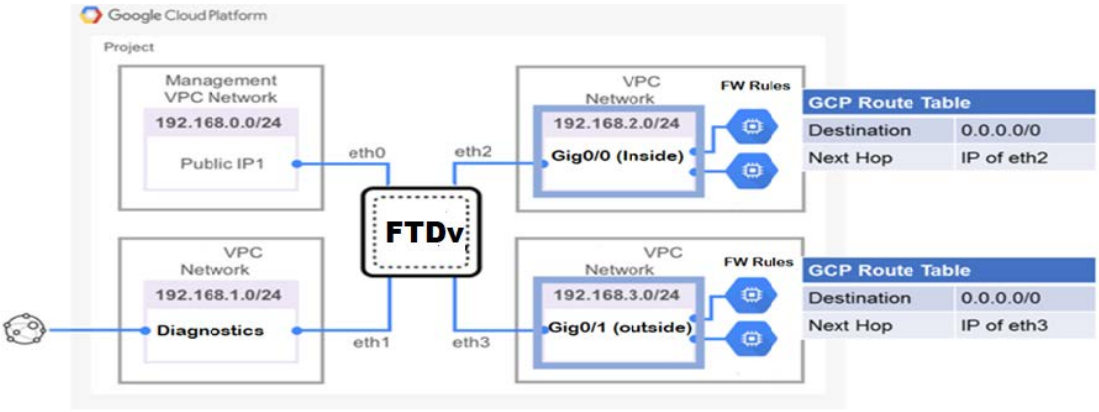
지원되지 않는 기능

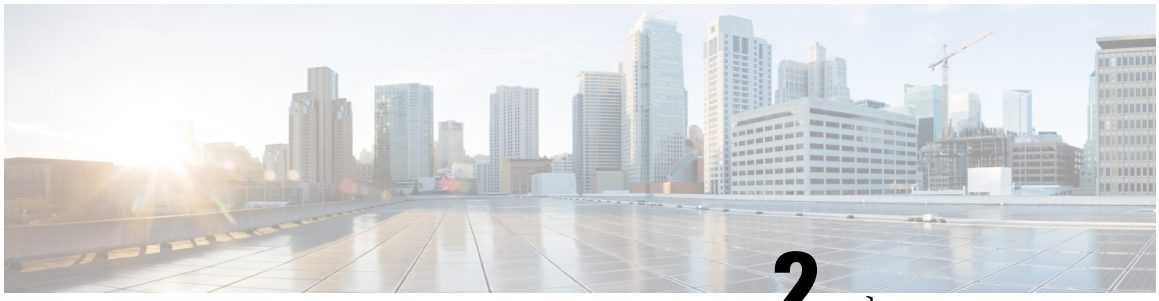
- IPv6
- FTDv 기본 HA
- 자동 확장
- 투명/인라인/패시브 모드
- 점보 프레임

GCP에서 FTDv를 위한 네트워크 토폴로지 샘플

다음 그림은 Routed Firewall Mode의 FTDv에 대한 권장 토폴로지와 FTDv에 대해서 GCP에 구성된 4개의 서브넷(관리, 진단, 내부 및 외부)을 보여줍니다.

그림 *1: GCP* 구축에 대한 *FTDv* 샘플





2 장

GCP에서 Firepower Threat Defense Virtual 구축

Google에서 제공하는 고 가용성 호스팅 환경에서 애플리케이션을 실행할 수 있는 퍼블릭 클라우드 컴퓨팅 서비스인 Google Cloud Platform(GCP)에 FTDv를 구축 할 수 있습니다.

GCP 콘솔 **Dashboard(**대시 보드**)**에 GCP 프로젝트 정보가 표시됩니다.

- 아직 선택하지 않은 경우 **Dashboard(**대시 보드**)**에서 GCP 프로젝트를 선택해야 합니다.
- Dashboard(대시 보드)에 액세스하려면 **Navigation(**탐색**)** 메뉴 > **Home(**홈**)** > **Dashboard(**대시 보드**)**를 클릭합니다.

GCP 콘솔에 로그인하여 GCP Marketplace에서 Cisco Firepower NGFW virtual firewall(NGFWv) 제품을 검색한 다음 FTDv 인스턴스를 시작합니다. 다음 절차에서는 GCP 환경을 준비하고 FTDv 인스턴스를 시작하여 FTDv를 구축하는 방법을 설명합니다.

- VPC 네트워크 생성, 5 페이지
- 방화벽 규칙 생성, 6 페이지
- GCP에서 FTDv 인스턴스 생성, 7 페이지

VPC 네트워크 생성

FTDv를 구축하려면 FTDv를 구축하기 전에 4개의 네트워크를 생성해야 합니다. 네트워크는 다음과 같습니다.

- 관리 서브넷의 관리 VPC
- 진단 VPC 또는 진단 서브넷
- 내부 서브넷의 내부 VPC
- 외부 서브넷의 외부 VPC

또한 FTDv로 트래픽 흐름을 허용하도록 경로 테이블 및 GCP 방화벽 규칙을 설정합니다. 경로 테이블 및 방화벽 규칙은 FTDv 자체에 구성된 규칙과 다릅니다. 연결된 네트워크 및 기능에 따라 GCP 경로 테이블 및 방화벽 규칙의 이름을 지정합니다. GCP에서 FTDv를 위한 네트워크 토폴로지 샘플을 지침으로 참고합니다.

프로시저

단계 **1** GCP 콘솔에서 **VPC networks(VPC** 네트워크**)**를 선택하고 **Create VPC Network(VPC** 네트워크 생성**)**를 클릭합니다.

단계 **2** **Name(**이름**)** 필드에 원하는 이름을 입력합니다.

단계 **3** **Subnet creation mode(**서브넷 생성 모드**)**에서 **Custom(**맞춤형**)**을 클릭합니다.

단계 **4** **New subnet(**새로운 서브넷**)** 아래의 **Name(**이름**)** 필드에 원하는 이름을 입력합니다.

단계 **5** **Region(**지역**)** 드롭 다운 목록에서 자신의 구축에 적합한 지역을 선택합니다. 네 개의 네트워크는 모두 같은 지역에 있어야 합니다.

단계 **6** **IP address range(IP** 주소 지역**)** 필드에 CIDR 포맷, 예를 들면 10.10.0.0/24의 형식으로 첫 번째 네트워크의 서브넷을 입력합니다.

단계 **7** 기타 모든 설정은 기본값으로 하고 **Create(**생성**)**를 클릭합니다.

단계 **8** 나머지 3 개의 VPC 네트워크를 생성하려면 1 ~ 7 단계를 반복합니다.

방화벽 규칙 생성

FTDv 인스턴스를 구축하는 동안 관리 인터페이스에 대한 방화벽 규칙을 적용합니다(SSH 및 SFTunnel이 FMC와 통신할 수 있도록). GCP에서 FTDv 인스턴스 생성, 7 페이지을 참조하십시오. 요구 사항에 따라 내부, 외부 및 진단 인터페이스에 대한 방화벽 규칙을 생성 할 수도 있습니다.

프로시저

단계 **1** GCP 콘솔에서 **Networking(**네트워킹**)** > **VPC network(VPC** 네트워크**)** > **Firewall(**방화벽**)**을 선택하고 **Create Firewall Rule(**방화벽 규칙 생성**)**을 클릭합니다.

단계 **2** **Name(**이름**)** 필드에 방화벽 규칙을 설명하는 이름(예: *vpc-asiasouth-inside-fwrule*)을 입력합니다.

단계 **3** **Network(**네트워크**)** 드롭 다운 목록에서 방화벽 규칙을 생성할 VPC 네트워크의 이름(예: *ftdv-south-inside*)을 선택합니다.

단계 **4** **Targets(**대상**)** 드롭 다운 목록에서 방화벽 규칙을 위해서 적용할 옵션(예: **All instances in the network**)을 선택합니다.

단계 **5** **Source IP(**소스 **IP)** 범위 필드에서 CIDR 형식(예: 0.0.0.0/0)으로 소스 IP 주소 범위를 입력합니다.

트래픽은 이들 IP 주소 범위 내의 소스로부터만 허용됩니다.

단계 **6** **Protocols and ports(**프로토콜 및 포트**)** 아래에서 **Specified protocols and ports(**명시된 프로토콜 및 포트**)**를 선택합니다.

단계 **7** 보안 규칙을 추가합니다.

단계 **8** **Create(**생성**)**를 클릭합니다.

GCP에서 FTDv 인스턴스 생성

아래 단계에 따라 GCP Marketplace에서 Cisco Firepower NGFW Virtual Firewall(NGFWv) 제품을 사용하여 FTDv 인스턴스를 구축할 수 있습니다.

프로시저

단계 **1** GCP 콘솔로 로그인합니다.

단계 **2** **Navigation(**탐색**)** 메뉴**(** > **Marketplace(**마켓플레이스**)**를 클릭합니다 .

단계 **3** Marketplace에서 "Cisco Firepower NGFW Virtual Firewall (NGFWv)"을 검색하고 제품을 선택합니다.

단계 **4** **Launch(**실행**)**를 클릭합니다.

a) **Deployment name(**구축 이름**)** — 인스턴스를 위한 고유한 이름을 지정합니다.

b) **Zone(**영역**)** — FTDv를 구축하고자 하는 영역을 선택합니다.

c) **Machine type(**시스템 유형**)** — GCP 시스템 유형 지원, 1 페이지에 따라 정확한 시스템 유형을 선택합니다.

d) **SSH key (SSH** 키**)(**선택**)** — SSH 키 쌍의 공용 키를 붙여넣기합니다.

키 쌍은 GCP가 저장하는 공용 키와 사용자가 저장하는 개인 키 파일로 구성됩니다. 이 두 키를 함께 사용하면 인스턴스에 안전하게 연결할 수 있습니다. 인스턴스에 연결할 때 필요한 만큼 키 쌍을 알고 있는 위치에 확실히 저장해야 합니다.

e) 이 인스턴스에 액세스하기 위해 프로젝트 전체 SSH 키를 허용할지 아니면 차단할지를 선택합니다. Google 문서 Allowing or blocking project-wide public SSH keys from a Linux instance를 참조하십시오.

f) 시작 스크립트 - 인스턴스가 부팅될 때마다 자동화된 작업을 수행하도록 FTDv 인스턴스에 대한 시작 스크립트를 생성할 수 있습니다.

다음 예는 시작 스크립트 필드에 복사하여 붙여 넣은 Day0 컨피그레이션의 샘플을 보여줍니다.

```
{
"AdminPassword": "Cisco@123123",
"Hostname": "ftdv-gcp",
"DNS1": "8.8.8.8",
"FirewallMode": "routed",
"IPv4Mode": "dhcp",
"ManageLocally": "No"
}
```

팁 실행 오류를 방지하려면 JSON 검사기를 사용하여 Day0 컨피그레이션을 검증해야 합니다.

g) 네트워크 인터페이스 - 인터페이스 구성: 1) 관리, 2) 진단, 3) 내부, 4) 외부.

참고 인터페이스를 생성한 후엔 거기에 인터페이스를 추가할 수 없습니다. 부적절한 인터페이스 컨피그레이션으로 인스턴스를 생성했을 경우 해당 인스턴스를 삭제하고 적절한 인터페이스 컨피그레이션으로 다시 생성해야 합니다.

1. **Network(**네트워크**)** 드롭 다운 목록에서 VPC 네트워크(예 : *vpc-asiasouth-mgmt*)를 선택합니다.
2. **External IP(**외부 **IP)** 드롭 다운 목록에서 적절한 옵션을 선택합니다.

   관리 인터페이스를 위해선 **External IP(**외부 **IP) - Ephemeral(**일회성**)**을 선택합니다. 이는 내부 및 외부 인터페이스의 경우 선택 사항입니다.
3. **Done(**완료**)**을 클릭합니다.

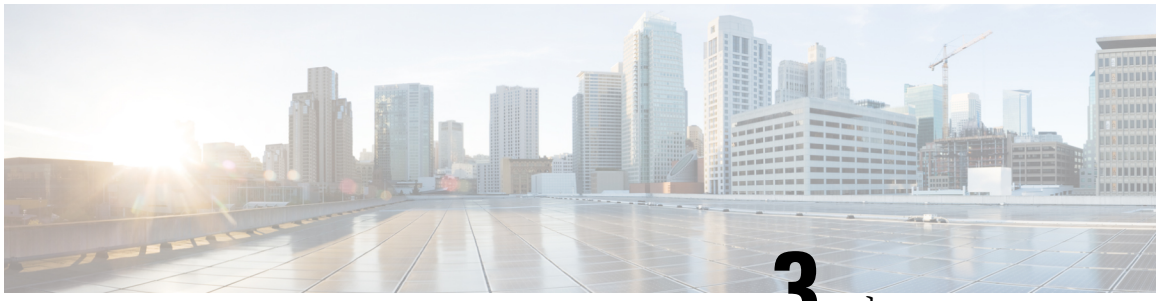
h) **Firewall(**방화벽**)**— 방화벽 규칙을 적용합니다.

- 인터넷의 **TCP** 포트 **22** 트래픽**(SSH** 액세스**)** 허용 확인란을 선택하여 SSH를 허용합니다.
- 인터넷의 **HTTPS** 트래픽**(FMC** 액세스**)** 허용 확인란을 선택하여 FMC를 허용하고 양방향, SSL 암호화 통신 채널(SFTunnel)을 사용하여 관리되는 디바이스가 통신할 수 있도록 합니다.

i) **More(**더 보기**)**를 클릭하여 보기를 확장하고 **IP Forwarding(IP** 전달**)**이 **On(**켜짐**)**으로 설정되어 있는지 확인합니다.

단계 **5** **Deploy(**구축**)**를 클릭합니다.

GCP 콘솔의 VM 인스턴스 페이지에서 인스턴스 상세 정보를 확인합니다. 내부 IP 주소, 외부 IP 주소 그리고 인스턴스를 시작하고 중지할 수 있는 제어 기능을 확인할 수 있습니다. 인스턴스를 수정해야 하는 경우 인스턴스를 중지해야 합니다.



3 장

GCP에서 Firepower Threat Defense Virtual 인스턴스 액세스

구축 중에 SSH(포트 22를 통한 TCP 연결)를 허용하는 방화벽 규칙을 이미 활성화했는지 확인합니다. 자세한 내용은 GCP에서 FTDv 인스턴스 생성, 7 페이지를 참조하십시오.

이 방화벽 규칙은 FTDv 인스턴스에 대한 액세스를 활성화하고 다음 방법을 사용하여 해당 인스턴스에 연결할 수 있도록 합니다.

- 외부 IP
  - 기타 SSH 클라이언트 또는 서드파티 도구
- 시리얼 콘솔
- Gcloud 명령줄

더 자세한 내용은 Google 문서 Connecting to instances를 참조하십시오.

참고 Day0 컨피그레이션을 추가하지 않을 경우 기본 자격 증명(사용자 이름: **admin**, 비밀번호: **Admin123**)을 사용하여 FTDv 인스턴스에 로그인할 수 있습니다. 최초 로그인 시에 프롬프트가 표시되어 비밀번호를 설정할 수 있습니다.

외부 IP를 사용해서 FTDv 인스턴스 연결

FTDv 인스턴스는 내부 IP와 외부 IP로 할당됩니다. 외부 IP를 사용해서 FTDv 인스턴스에 액세스할 수 있습니다.

프로시저

단계 1 GCP 콘솔에서 **Compute Engine(**컴퓨팅 엔진**)** > **VM instances(VM** 인스턴스**)**를 선택합니다.

단계 2 FTDv 인스턴스 이름을 클릭하여 **VM** 인스턴스 세부 정보 페이지를 엽니다.

단계 3 **Details(**상세정보**)** 탭 아래에서 **SSH** 필드를 위한 드롭 다운 메뉴를 엽니다.

단계 4 **SSH** 드롭 다운 메뉴에서 원하는 옵션을 선택합니다.

다음 방법을 사용해서 FTDv 인스턴스에 연결할 수 있습니다.

- 기타 SSH 클라이언트 또는 서드파티 도구 - 더 자세한 내용은 Google 문서 Connecting using third-party tools을 참조하십시오.

SSH를 사용해서 FTDv 인스턴스 연결

Unix 스타일 시스템에서 인스턴스에 연결하려면 SSH를 사용하여 FTDv 인스턴스에 로그인합니다.

프로시저

단계 1 다음 명령을 사용해서 파일 권한을 설정해서 본인만 파일을 읽을 수 있도록 합니다.

```
$ chmod 400 <private_key>
```

여기서 각 항목은 다음을 나타냅니다.

<private_key>는 액세스하고자 하는 인스턴스에 연결된 개인 키를 포함하고 있는 파일의 전체 경로와 이름입니다.

단계 2 다음 SSH 명령을 사용해서 인스턴스에 액세스합니다.

```
$ ssh -i <private_key> <username>@<public-ip-address>
```

여기서 각 항목은 다음을 나타냅니다.

<private_key>는 액세스하고자 하는 인스턴스에 연결된 개인 키를 포함하고 있는 파일의 전체 경로와 이름입니다.

<username>은 FTDv 인스턴스를 위한 사용자 이름입니다.

<public-ip-address>는 콘솔에서 가져온 인스턴스 IP 주소입니다.

시리얼 콘솔을 사용하여 FTDv 인스턴스에 연결

프로시저

단계 1 GCP 콘솔에서 **Compute Engine(**컴퓨팅 엔진**)** > **VM instances(VM** 인스턴스**)**를 선택합니다.
단계 2 FTDv 인스턴스 이름을 클릭하여 **VM** 인스턴스 세부 정보 페이지를 엽니다.
단계 3 **Details(**세부 사항**)** 탭에서 **Connect to serial console(**시리얼 콘솔에 연결**)**을 클릭합니다.

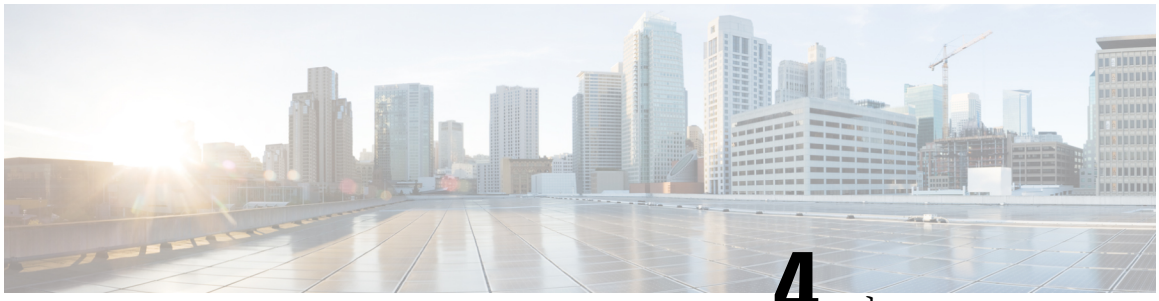
자세한 내용은 Google 문서 Interacting with the serial console을 참조하십시오.

Gcloud를 사용하여 FTDv 인스턴스에 연결

프로시저

단계 1 GCP 콘솔에서 **Compute Engine(**컴퓨팅 엔진**)** > **VM instances(VM** 인스턴스**)**를 선택합니다.
단계 2 FTDv 인스턴스 이름을 클릭하여 **VM** 인스턴스 세부 정보 페이지를 엽니다.
단계 3 Details (세부 사항) 탭에서 SSH 필드의 드롭 다운 메뉴를 클릭합니다.
단계 4 **View gcloud command(gcloud** 명령 보기**)** > **Run in Cloud Shell(**클라우드 셸에서 구동**)**을 클릭합니다.

클라우드 셸 터미널 창이 열립니다. 더 자세한 내용은 Google 문서 gcloud command-line tool overview 그리고 gcloud compute ssh를 참조하십시오.



4 장

Firepower Management Center로 Firepower Threat Defense Virtual 관리

이 장에서는 FMC로 관리되는 독립형 FTDv 디바이스를 구축하는 방법을 설명합니다.

참고 이 문서에서는 최신 FTDv 버전의 기능에 대해 설명합니다. 기능 변경에 대한 자세한 내용은 Firepower Management를 이용한 Firepower Threat Defense Virtual 관리 기록 , 28 페이지를 참조하십시오. 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

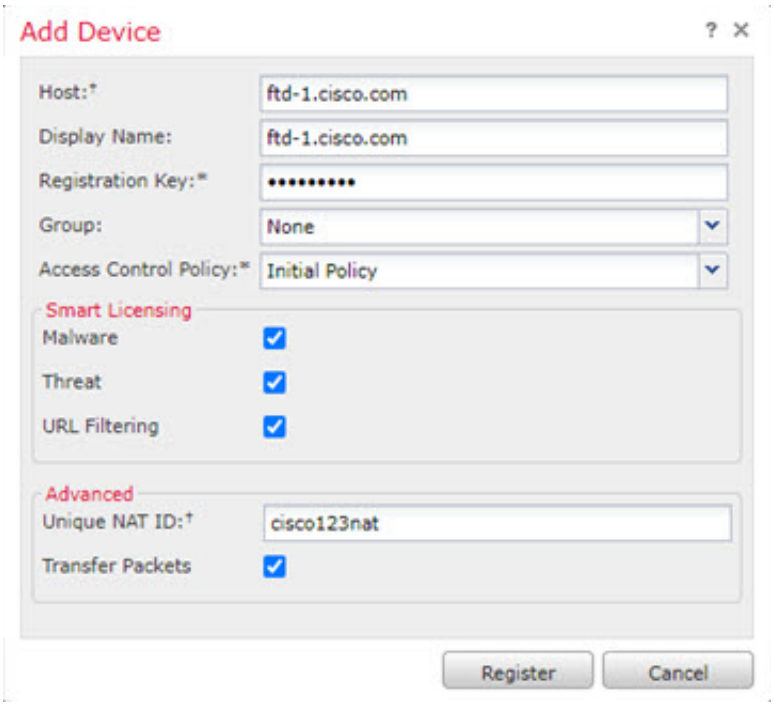
FTDv 가상 머신이 성공적으로 구축되었으며, 전원이 켜져 있고 첫 번째 부팅 절차를 완료했는지 확인하십시오.

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.

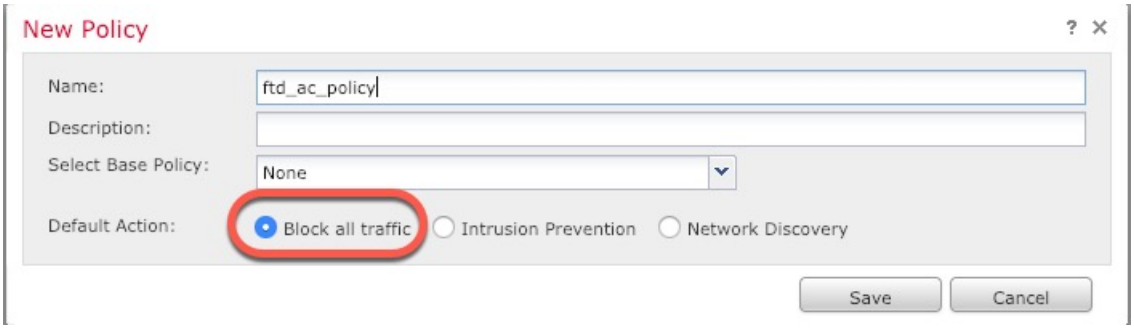
프로시저

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, 26 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, 28 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.

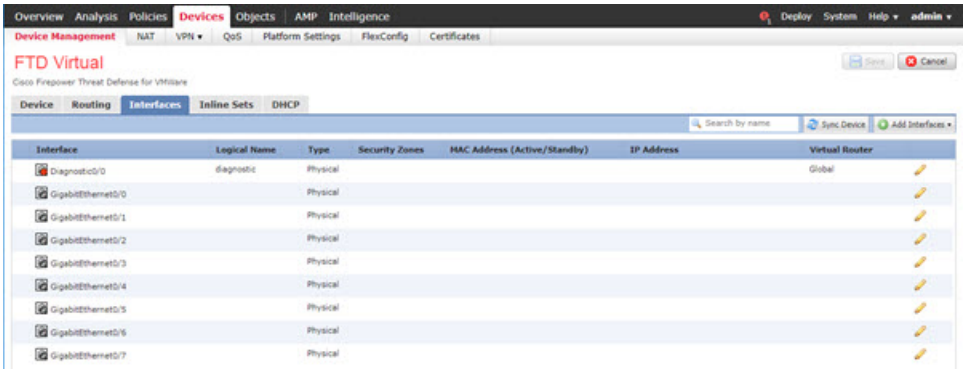
일반적인 에지 라우팅 상황의 경우, 내부 인터페이스에서 정적 주소를 정의하는 반면 ISP에서 온 DHCP를 통해 외부 인터페이스 주소를 가져옵니다.

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

프로시저

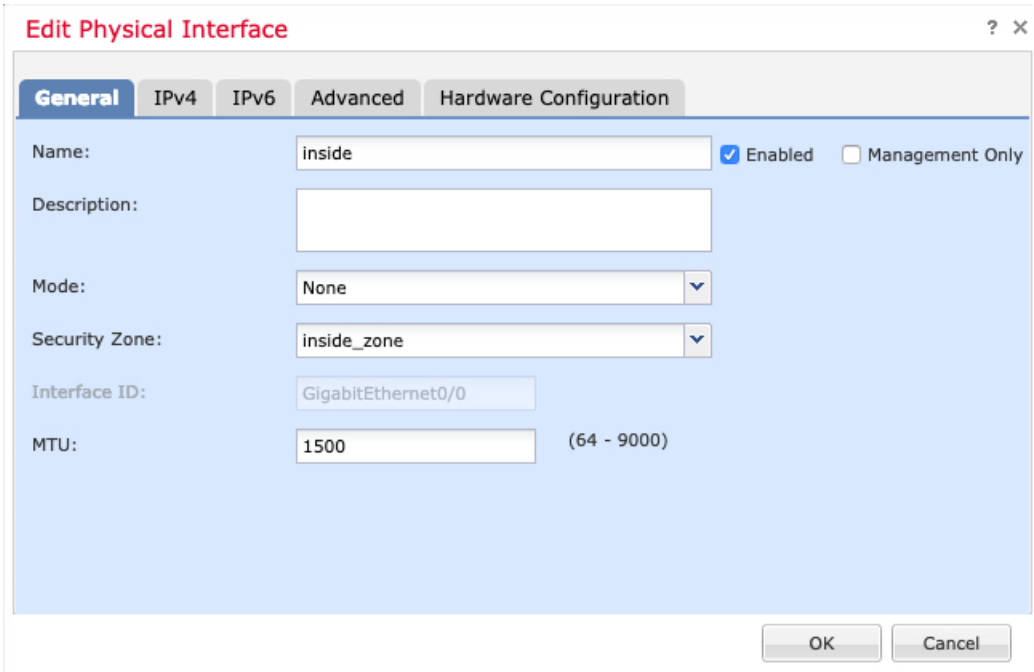
단계 1 **Devices(**디바이스**)** > **Device Management(**디바이스 관리**)**를 선택하고 디바이스의 수정( )을(를) 클릭합니다.

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.

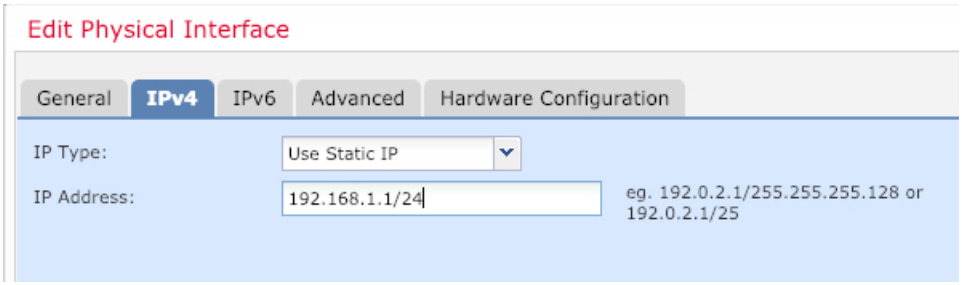
예를 들어 **inside_zone**이라는 영역을 추가합니다. 각 인터페이스는 보안 영역 및/또는 인터페이스 그룹에 할당되어야 합니다. 인터페이스는 하나의 보안 영역에만 속할 수 있지만, 여러 인터페이스 그룹에 속할 수도 있습니다. 영역 또는 그룹을 기준으로 보안 정책을 적용합니다. 예를 들어 내부 인터페이스는 내부 영역에, 외부 인터페이스는 외부 영역에 할당할 수 있습니다. 트래픽이 내부에서 외부로는 이동하지만 외부에서 내부로는 이동할 수 없도록 액세스 제어 정책을 구성할 수 있습니다. 대부분의 정책은 보안 영역만 지원합니다. NAT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

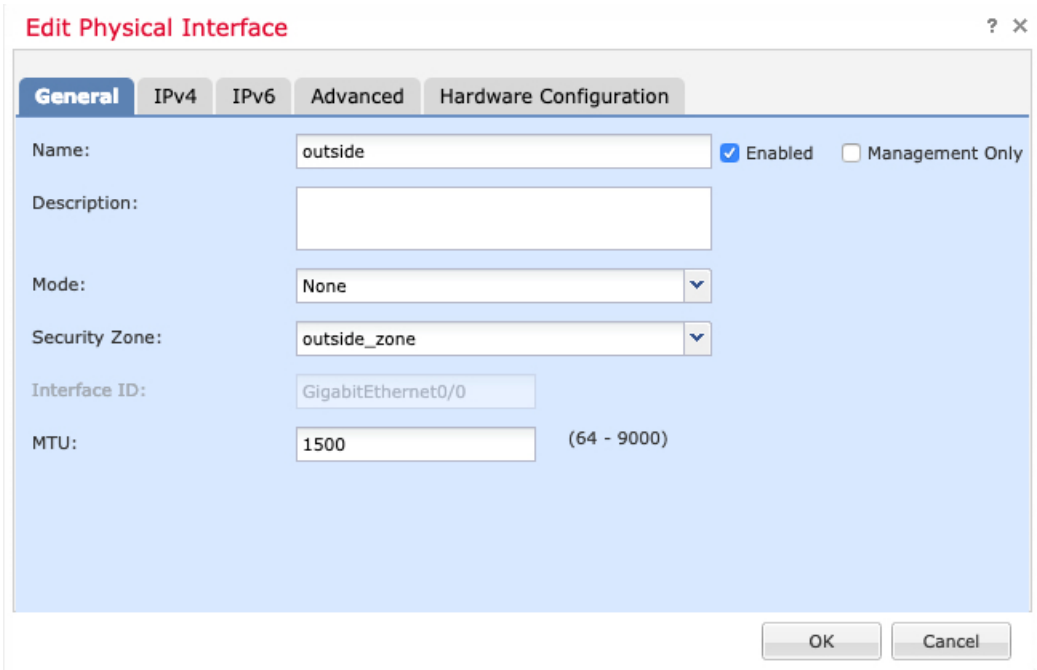


- **IPv6** - 상태 비저장 자동 구성을 하려면 **Autoconfiguration(**자동 구성**)** 확인란을 선택합니다.

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.

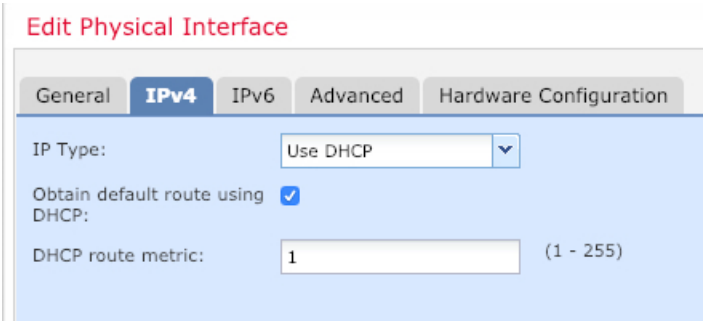
d) **Security Zone(**보안 영역**)** 드롭다운 목록에서 기존의 외부 보안 영역을 선택하거나 **New(**새로 만들기**)**를 클릭하여 새 보안 영역을 추가합니다.

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.

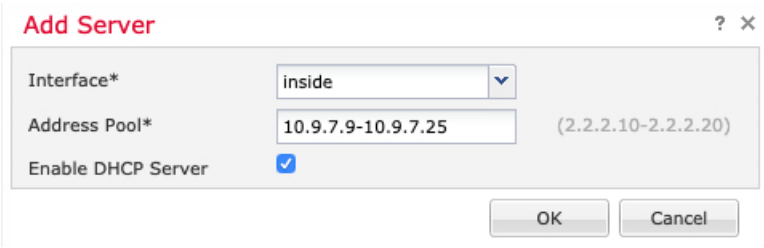
클라이언트가 DHCP를 사용하여 FTDv에서 IP 주소를 가져오게 하려면 DHCP 서버를 활성화합니다.

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.

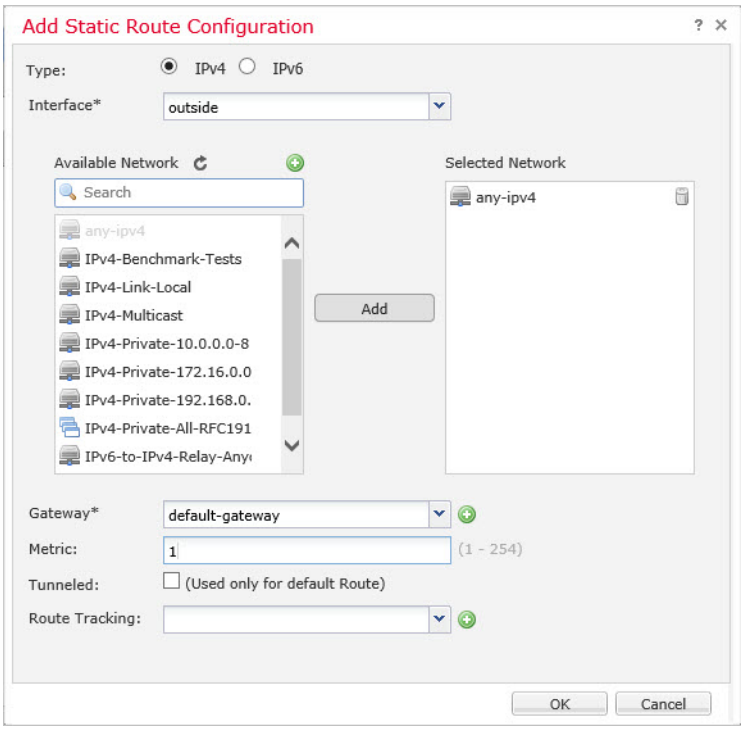
기본 경로 추가

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.

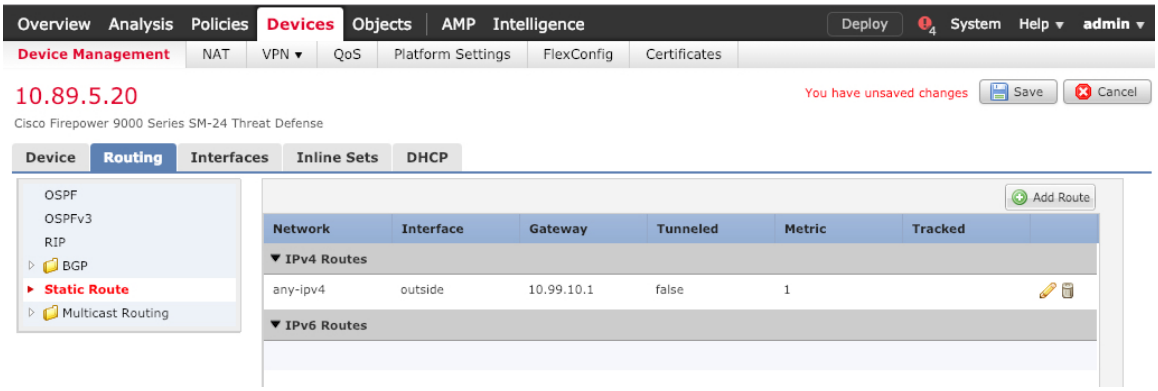
단계 **2** **Routing(**라우팅**)** > **Static Route(**정적 경로**)**를 선택하고 **Add Route(**경로 추가**)**를 클릭해 다음을 설정합니다.



- **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.

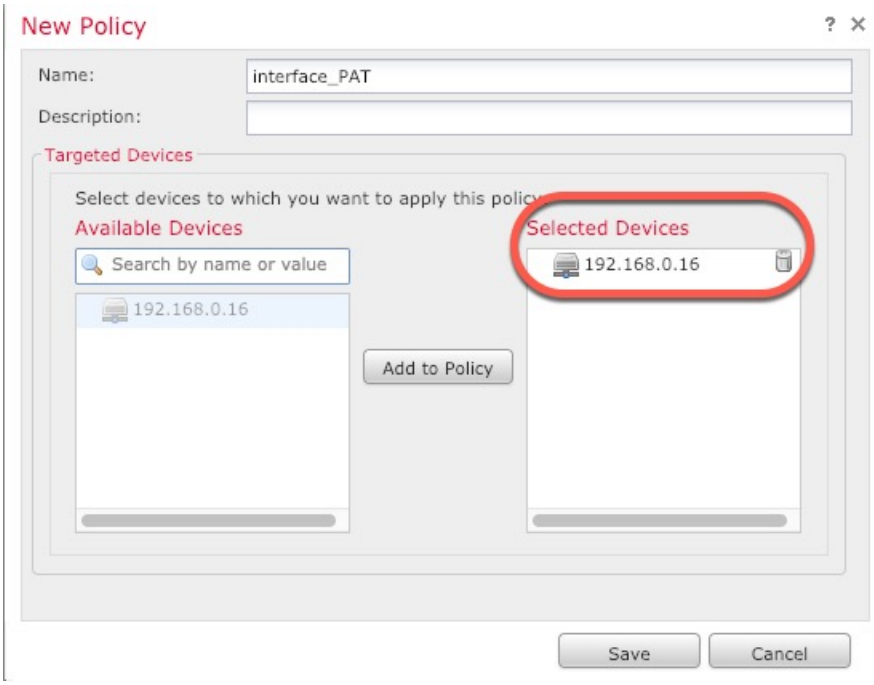
NAT 구성

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.

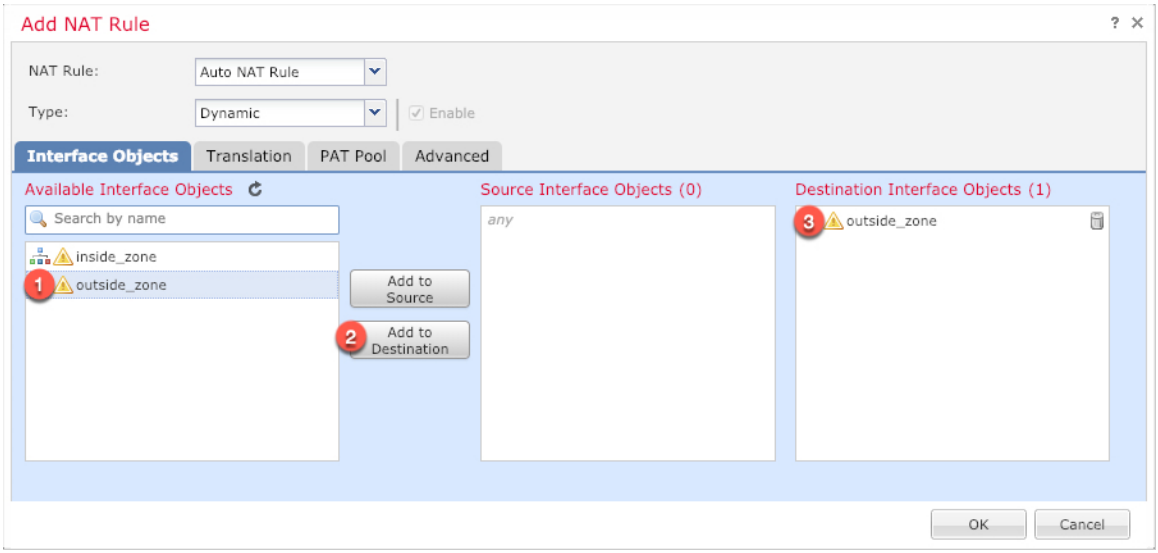
단계 **3** **Add Rule(**규칙 추가**)**을 클릭합니다.

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

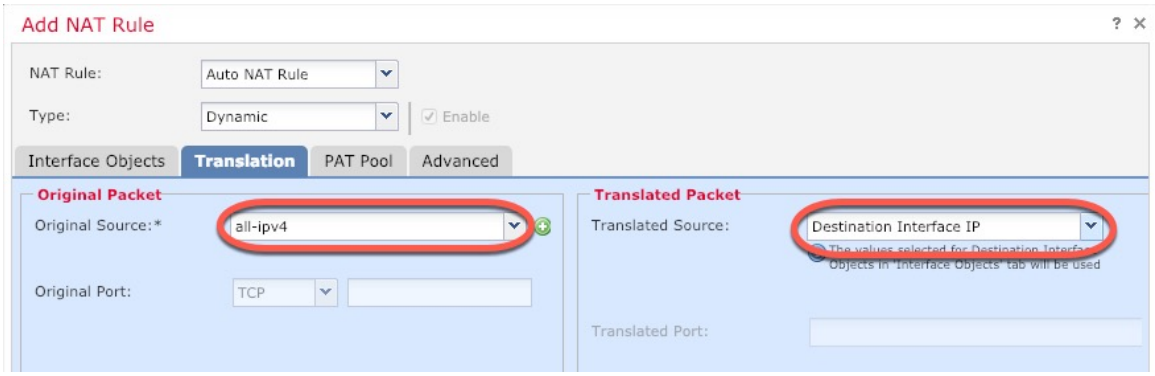
단계 **4** 기본 규칙 옵션을 구성합니다.

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

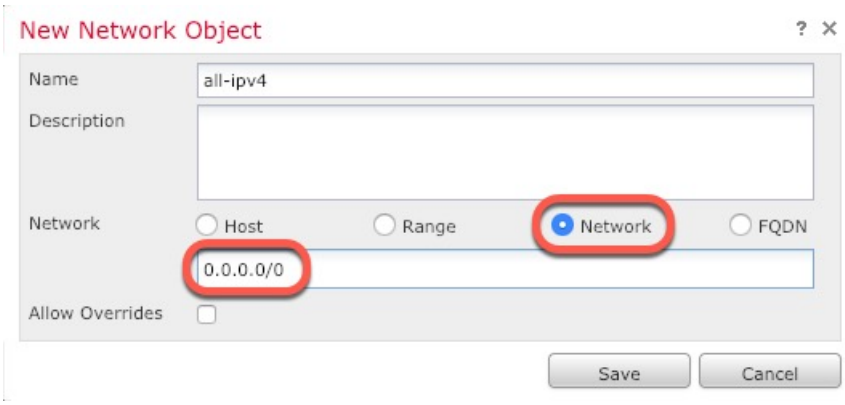
단계 **5** **Interface Objects(**인터페이스 개체**)** 페이지에서 **Available Interface Objects(**사용 가능한 인터페이스 개체**)** 영역의 외부 영역을 **Destination Interface objects(**대상 인터페이스 개체**)** 영역에 추가합니다.



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.

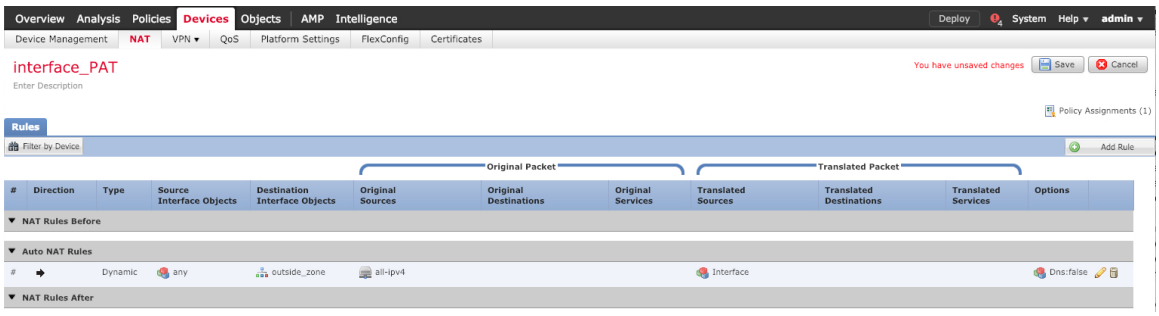


참고 자동 NAT 규칙은 개체 정의의 일부로 NAT를 추가하고 시스템 정의 개체를 수정할 수 없기 때문에 시스템에서 정의된 **any-ipv4** 개체를 사용할 수 없습니다.

- **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

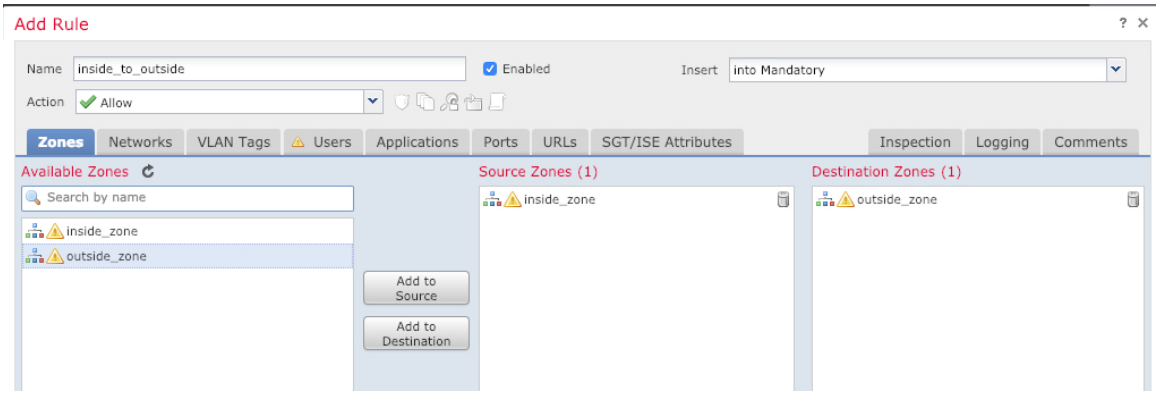
FMC을 사용해 FTDv를 등록할 때 기본 액세스 컨트롤 정책인 **Block all traffic(**모든 트래픽 차단**)**을 생성했다면, 디바이스에 트래픽을 허용하기 위해 정책에 규칙을 추가해야 합니다. 다음 절차에서는 내부 영역에서 외부 영역으로 향하는 트래픽을 허용하는 규칙을 추가합니다. 다른 영역이 있는 경우에는 적절한 네트워크에 대한 트래픽을 허용하는 규칙을 추가해야 합니다.

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.

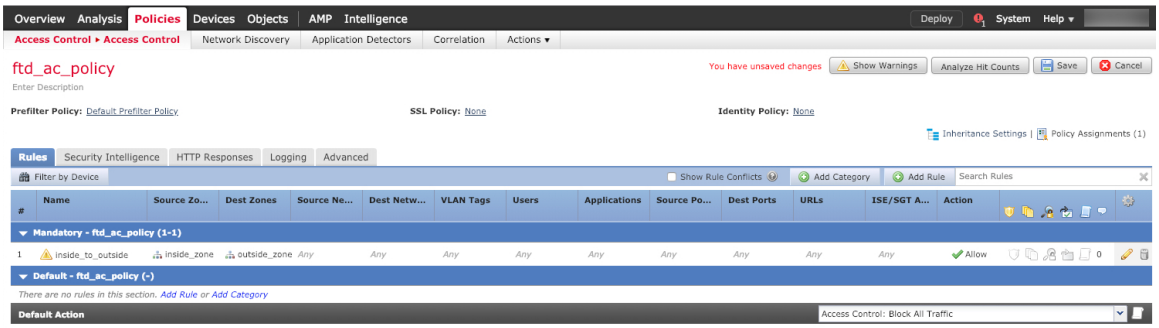


- **Name (**이름**)** - 예를 들어 이 규칙의 이름을 **inside_to_outside**로 지정합니다.
- **Source Zones(**원본 영역**)** - **Available Zones(**사용 가능한 영역**)**에서 내부 영역을 선택하고 **Add to Source(**원본에 추가**)**를 클릭합니다.
- **Destination Zones(**대상 영역**)** - **Available Zones(**사용 가능한 영역**)**에서 외부 영역을 선택하고 **Add to Destination(**대상에 추가**)**를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

기타 설정은 변경하지 않습니다.

단계 **3** **Add(**추가**)**를 클릭합니다.

규칙이 **Rules(**규칙**)** 테이블에 추가됩니다.



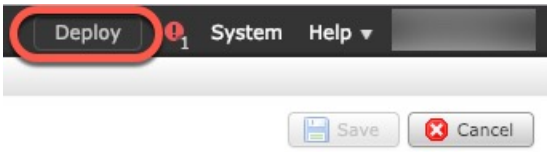
단계 **4** **Save(**저장**)**를 클릭합니다.

구성 구축

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

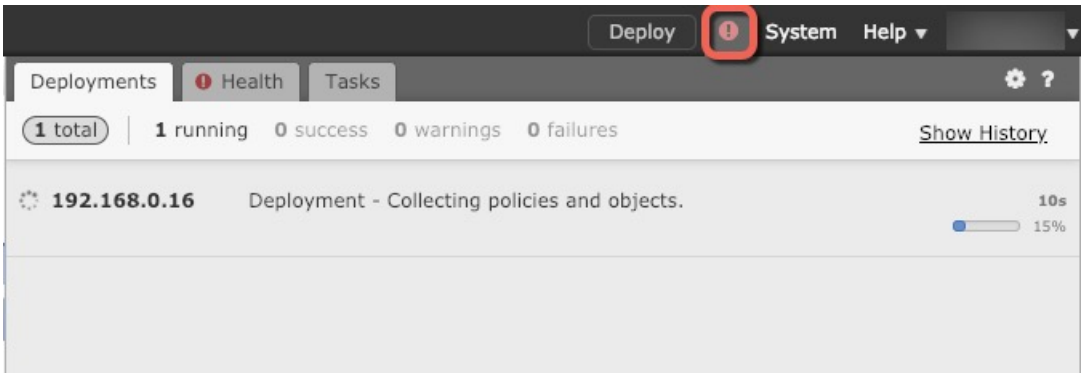
프로시저

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.

Firepower Management를 이용한 Firepower Threat Defense Virtual 관리 기록

기능 이름	플랫폼 릴리스	기능 정보
FMC 관리	6.0	초기 지원.