



## **AWS Cloud용 Cisco Firepower Threat Defense Virtual 시작 가이드**

초판: 2018년 7월 31일

최종 변경: 2021년 4월 12일

### **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 AWS 시작하기

Amazon VPC(Amazon Virtual Private Cloud)를 통해 사용자가 정의한 가상 네트워크에서 AWS(Amazon Web Services) 리소스를 실행할 수 있습니다. 자체 데이터 센터에서 운영할 수 있는 기존 네트워크와 매우 유사한 이 가상 네트워크는 확장 가능한 AWS 인프라 사용 시의 이점도 제공합니다.

이 문서에서는 AWS에 Firepower Threat Defense Virtual을 구축하는 방법을 설명합니다.

- [FTDv 및 AWS 클라우드, 1 페이지](#)
- [Firepower 디바이스 관리 방법, 2 페이지](#)
- [AWS 솔루션 개요, 3 페이지](#)
- [Firepower Threat Defense Virtual 사전 요건, 3 페이지](#)
- [FTDv 및 AWS에 대한 지침과 제한 사항, 4 페이지](#)
- [AWS 환경 구성, 6 페이지](#)

### FTDv 및 AWS 클라우드

AWS는 퍼블릭 클라우드 환경입니다. Firepower Threat Defense Virtual은 다음 인스턴스 유형의 AWS 환경에서 게스트로 실행됩니다.



참고 Firepower 버전 6.6에서는 다음 표에 나와 있는 C5 인스턴스 유형에 대한 지원이 추가되었습니다. 인스턴스 유형이 클수록 AWS VM에 더 많은 CPU 리소스를 제공하여 성능을 높이고 일부는 더 많은 네트워크 인터페이스를 허용합니다.

표 1: FTDv에 대한 AWS 지원 인스턴스

인스턴스 유형	vCPU	메모리(RAM)	vNics
C5.xlarge	4	8GB	4
C5.2xlarge	8	16GB	4

인스턴스 유형	vCPU	메모리(RAM)	vNics
C5.xlarge	16	32GB	8
C4.xlarge	4	7.5GB	4
C3.xlarge	4	7.5GB	4

## Firepower 디바이스 관리 방법

두 가지 옵션을 통해 Firepower Threat Defense 디바이스를 관리할 수 있습니다.

### Firepower Device Manager

Firepower Device Manager(FDM) 온보드 통합 관리자.

FDM은(는) 일부 Firepower Threat Defense 디바이스에 포함된 웹 기반 구성 인터페이스입니다. FDM은(는) 소규모 네트워크에서 가장 흔히 사용되는 소프트웨어의 기본 기능을 구성하도록 합니다. Firepower Device Manager는 디바이스를 하나 또는 몇 개만 포함하는 네트워크 용도로 특별히 설계되어 고성능 다중 디바이스 관리자를 사용해 여러 Firepower Threat Defense 디바이스가 포함된 대규모 네트워크를 제어하기를 원하지 않을 경우에 유용합니다.



참고 FDM을 지원하는 Firepower Threat Defense 디바이스 목록은 [Firepower Device Manager용 Cisco Firepower Threat Defense 구성 가이드](#)를 참조하십시오.

### Firepower Management Center

Cisco Firepower Management Center(FMC)

다수의 디바이스를 관리하거나 Firepower Threat Defense에서 허용하는 더 복잡한 기능 및 구성을 사용하려는 경우에는 통합형 FDM 대신 FMC을(를) 사용하여 디바이스를 구성하십시오.



중요 Firepower 디바이스를 관리할 때 FDM와(과) FMC을(를) 동시에 사용할 수 없습니다. FDM 통합 관리가 활성화되면 로컬 관리를 사용하지 않도록 설정하고 FMC을(를) 사용하도록 재구성하기 전에는 FMC을(를) 사용해 Firepower 디바이스를 관리할 수 없습니다. 반면 FMC에 Firepower 디바이스를 등록하면 FDM 온보드 관리 서비스가 비활성화됩니다.



주의 현재 Cisco에는 FDM Firepower 구성을 FMC로, 또는 그 반대로 마이그레이션할 수 있는 옵션이 없습니다. Firepower 디바이스를 구성할 때는 이를 고려해 관리 유형을 선택해야 합니다.

## AWS 솔루션 개요

AWS는 클라우드 컴퓨팅 플랫폼을 구성하는 원격 컴퓨팅 서비스(웹 서비스라고도 함) 컬렉션으로 Amazon.com에서 제공합니다. 이러한 서비스는 전 세계 11개 지역에서 운영됩니다. Firepower Management Center Virtual 및 Firepower Threat Defense Virtual을 구축할 때는 일반적으로 다음의 AWS 서비스를 숙지해야 합니다.

- Amazon EC2(Elastic Compute Cloud) - Amazon의 데이터 센터에서 방화벽 등의 자체 애플리케이션 및 서비스를 실행하고 관리하기 위한 가상 컴퓨터를 임대할 수 있는 웹 서비스입니다.
- Amazon VPC(Virtual Private Cloud) - Amazon 퍼블릭 클라우드 내에 격리된 프라이빗 네트워크를 구성하는 데 사용할 수 있는 웹 서비스입니다. EC2 인스턴스는 VPC 내에서 실행할 수 있습니다.
- Amazon S3(Simple Storage Service) - 데이터 스토리지 인프라를 제공하는 웹 서비스입니다.

AWS에서 어카운트를 생성하고, AWS 마법사 또는 수동 컨피그레이션을 사용하여 VPC 및 EC2 구성 요소를 설정하고, AMI(Amazon Machine Image) 인스턴스를 선택합니다. AMI는 인스턴스 실행에 필요한 소프트웨어 컨피그레이션을 포함한 템플릿입니다.



참고 AMI 이미지는 AWS 환경이 아닌 곳에서 다운로드할 수 없습니다.

## Firepower Threat Defense Virtual 사전 요건

- Amazon 어카운트는 <http://aws.amazon.com/>에서 생성할 수 있습니다.
- FTDv 콘솔에 액세스하려면 SSH 클라이언트(예: Windows의 PuTTY 또는 Macintosh의 터미널)가 필요합니다.
- Cisco Smart Account는 Cisco Software Central에서 생성할 수 있습니다. <https://software.cisco.com/>
- Firepower Threat Defense Virtual 라이선스
  - Firepower Management Center의 보안 서비스에 대해 모든 라이선스 권한을 구성합니다.
  - 라이선스를 관리하는 방법에 대한 자세한 내용은 Firepower Management Center 컨피그레이션 가이드의 "Firepower System 라이선싱"을 참조하십시오.
- Firepower Threat Defense Virtual 인터페이스 요구 사항:
  - 관리 인터페이스(2 - 첫째는 Firepower Threat Defense Virtual을 Firepower Management Center에 연결하는 데 사용되고, 둘째는 진단용으로 사용되며, 통과 트래픽에는 사용할 수 없습니다).
  - 6.7 이상 버전에서는 선택적으로 관리 인터페이스 대신 FMC 관리용 데이터 인터페이스를 구성할 수 있습니다. 관리 인터페이스는 데이터 인터페이스 관리를 위한 전제 조건이므로 초기 설정에서 구성해야 합니다. 데이터 인터페이스에서의 FMC 액세스는 고 가용성 구축에

서 지원되지 않습니다. FMC 액세스를 위한 데이터 인터페이스 구성에 대한 자세한 내용은 [FTD command reference](#)에서 **configure network management-data-interface** 명령을 참조하십시오.

- 트래픽 인터페이스 (2) - Firepower Threat Defense Virtual을 내부 호스트 및 공용 네트워크에 연결하는 데 사용됩니다.

• 통신 경로:

- Firepower Threat Defense Virtual 액세스를 위한 Public/elastic IP

## FTDv 및 AWS에 대한 지침과 제한 사항

지원 기능

- VPC(Virtual Private Cloud)에서 구축
- 향상된 네트워킹(SR-IOV) - 사용 가능한 경우
- Amazon Marketplace에서 구축
- 인스턴스당 최대 4개의 vCPU
- L3 네트워크의 사용자 구축
- 라우팅 모드(기본값)
- ERSPAN을 통한 패시브 모드

**FTDv Smart Licensing**의 성능 계층

FTDv에서는 구축 요건에 따라 다양한 처리량 레벨 및 VPN 연결 제한을 제공하는 성능 계층 라이선싱을 지원합니다.

표 2: 자격 기준 **FTDv** 라이선스 기능 제한

성능 계층	디바이스 사양 (Core/RAM)	속도 제한	RA VPN 세션 제한
FTDv5, 100Mbps	4 코어/8GB	100Mbps	50
FTDv10, 1Gbps	4 코어/8GB	1Gbps	250
FTDv20, 3Gbps	4 코어/8GB	3Gbps	250
FTDv30, 5Gbps	8 코어/16GB	5Gbps	250
FTDv50, 10Gbps	12 코어/24GB	10Gbps	750

성능 계층	디바이스 사양 (Core/RAM)	속도 제한	RA VPN 세션 제한
FTDv100, 16Gbps	16 코어 / 34GB	16Gbps	10,000

- Cisco Smart License 계정을 사용하는 BYOL(Bring Your Own License)

FTDv 디바이스를 라이선싱할 때의 지침은 *Firepower Management Center* 구성의 "Firepower 시스템 라이선싱" 장을 참조하십시오.

### Firepower Threat Defense Virtual 제한 사항

- c4.xlarge가 권장되는 인스턴스입니다. c3.xlarge 인스턴스는 AWS 지역 전체에서 가용성이 제한됩니다.
- 시작하는 동안 2개의 관리 인터페이스를 구성해야 합니다.
- 시작하려면 트래픽 인터페이스 2개와 관리 인터페이스 2개, 즉 총 4개의 인터페이스가 있어야 합니다.



참고 Firepower Threat Defense Virtual은 4개의 인터페이스 없이는 실행되지 않습니다.

- AWS에서 트래픽 인터페이스를 구성할 때는 "Change Source / Dest. Check" 옵션을 선택해제해야 합니다.
- 모든 IP 주소 컨피그레이션(CLI 또는 Firepower Management Center의 컨피그레이션)은 AWS 콘솔에서 생성된 컨피그레이션과 일치해야 하며, 구축 중에 컨피그레이션 정보를 적어 두어야 합니다.
- Firepower Threat Defense Virtual을 등록한 후에는 인터페이스를 수정하여 Firepower Management Center에서 활성화해야 합니다. IP 주소는 AWS에서 구성한 인터페이스와 일치해야 합니다.
- IPv6은 현재 지원되지 않습니다.
- 투명 / 인라인 / 패시브 모드는 현재 지원되지 않습니다.
- 인터페이스를 수정하려면 AWS 콘솔에서 변경해야 합니다.
  - Firepower Management Center에서 등록 해제
  - AWS AMI 사용자 인터페이스를 통해 인스턴스를 중지합니다.
  - AWS AMI 사용자 인터페이스를 통해 변경하려는 인터페이스를 분리합니다.
  - 새 인터페이스를 연결합니다(시작하려면 트래픽 인터페이스 2개와 관리 인터페이스 2개가 있어야 합니다).
  - AWS AMI 사용자 인터페이스를 통해 인스턴스를 시작합니다.
  - Firepower Management Center에 재등록합니다.

- Firepower Management Center에서 디바이스 인터페이스를 수정하고 AWS 콘솔을 통해 변경한 내용과 일치하도록 IP 주소 및 기타 매개 변수를 수정합니다.
- 부팅 후에는 인터페이스를 추가할 수 없습니다.
- 복제/스냅샷은 현재 지원되지 않습니다.

## AWS 환경 구성

AWS에 Firepower Threat Defense Virtual을 구축하려면 구축 관련 요구 사항과 설정을 사용하여 Amazon VPC를 구성해야 합니다. 대부분의 상황에서는 설정 마법사가 설정 과정을 안내합니다. AWS는 소개 정보에서 고급 기능에 이르기까지 서비스와 관련된 여러 가지 유용한 정보를 찾을 수 있는 온라인 설명서를 제공합니다. 자세한 내용은 <https://aws.amazon.com/documentation/gettingstarted/>를 참조하십시오.

AWS 설정을 더 세부적으로 제어할 수 있도록 Firepower Threat Defense Virtual 인스턴스를 실행하기 전에 다음과 같은 섹션에서 VPC 및 EC2 구성을 안내합니다.

- [VPC 생성, 6 페이지](#)
- [인터넷 게이트웨이 추가, 7 페이지](#)
- [서브넷 추가, 8 페이지](#)
- [라우트 테이블 추가, 9 페이지](#)
- [보안 그룹 생성, 9 페이지](#)
- [네트워크 인터페이스 생성, 10 페이지](#)
- [탄력적 IP 생성, 11 페이지](#)

시작하기 전에

- AWS 어카운트를 생성합니다.
- Firepower Threat Defense Virtual 인스턴스에 AMI를 사용할 수 있는지 확인합니다.

## VPC 생성

VPC(Virtual Private Cloud)는 AWS 어카운트 전용 가상 네트워크이며, AWS Cloud의 다른 가상 네트워크와 논리적으로 격리되어 있습니다. Firepower Threat Defense Virtual 인스턴스 등의 AWS 리소스를 VPC에서 실행할 수 있습니다. VPC의 IP 주소 범위를 선택하고, 서브넷을 생성하고, 라우트 테이블, 네트워크 게이트웨이, 보안 설정을 구성하여 VPC를 구성할 수 있습니다.



## 프로시저

단계 1 <http://aws.amazon.com/>에 로그인하고 지역을 선택합니다.

AWS는 여러 지역으로 나뉘며, 이 지역은 상호 격리되어 있습니다. 화면의 우측 상단에 지역이 표시됩니다. 한 지역의 리소스가 다른 지역에는 나타나지 않습니다. 원하는 지역에 있는지 정기적으로 확인합니다.

단계 2 **Services**(서비스) > **VPC**를 클릭합니다.

단계 3 **VPC Dashboard**(VPC 대시보드) > 사용자 **VPC**를 클릭합니다.

단계 4 **Create VPC**(VPC 생성)를 클릭합니다.

단계 5 **Create VPC**(VPC 생성) 대화 상자에 다음 정보를 입력합니다.

- a) VPC를 식별하기 위한 사용자 정의 **Name tag**(이름 태그).
- b) IP 주소의 **CIDR block**(CIDR 블록). CIDR(Classless Inter-Domain Routing) 표기법은 IP 주소와 관련 라우팅 접두사를 축약한 표현입니다. 예를 들면 10.0.0.0/24와 같습니다.
- c) **Tenancy**(테넌시) 설정을 **Default**(기본값)로 설정하면 이 VPC에서 실행되는 인스턴스가 실행 시에 지정된 테넌시 특성을 사용합니다.

단계 6 VPC를 생성하려면 **Yes, Create**(예, 생성합니다)를 클릭합니다.

다음에 수행할 작업

다음 섹션의 설명에 따라 VPC에 인터넷 게이트웨이를 추가합니다.

## 인터넷 게이트웨이 추가

VPC를 인터넷에 연결하기 위해 인터넷 게이트웨이를 추가할 수 있습니다. VPC 외부의 IP 주소에 대한 트래픽을 인터넷 게이트웨이로 라우팅할 수 있습니다.

시작하기 전에

- Firepower Threat Defense Virtual 인스턴스용으로 VPC를 생성합니다.

## 프로시저

단계 1 **Services**(서비스) > **VPC**를 클릭합니다.

단계 2 **VPC Dashboard**(VPC 대시보드) > **Internet Gateways**(인터넷 게이트웨이)를 클릭하고 **Create Internet Gateway**(인터넷 게이트웨이 생성)를 클릭합니다.

단계 3 게이트웨이 식별을 위한 사용자 정의 **Name tag**(이름 태그)를 입력한 후, 게이트웨이를 생성하려면 **Yes, Create**(예, 생성합니다)를 클릭합니다.

단계 4 이전 단계에서 생성한 게이트웨이를 선택합니다.

단계 5 **Attach to VPC**(VPC에 연결)를 클릭하고 이전에 생성한 VPC를 선택합니다.

단계 6 VPC에 게이트웨이를 연결하려면 **Yes, Attach**(예, 연결합니다)를 클릭합니다.

기본적으로 VPC에서 실행되는 인스턴스는 게이트웨이를 생성하여 VPC에 연결할 때까지 인터넷과 통신할 수 없습니다.

다음에 수행할 작업

다음 섹션의 설명에 따라 VPC에 서브넷을 추가합니다.

## 서브넷 추가

Firepower Threat Defense Virtual 인스턴스를 연결할 수 있는 VPC의 IP 주소 범위를 세그먼트로 지정할 수 있습니다. 보안 및 운영 요구 사항에 따라 서브넷을 생성하여 인스턴스를 그룹화할 수 있습니다. Firepower Threat Defense Virtual의 경우에는 트래픽용 서브넷과 관리용 서브넷을 모두 생성해야 합니다.

시작하기 전에

- Firepower Threat Defense Virtual 인스턴스용으로 VPC를 생성합니다.

프로시저

단계 1 **Services(서비스) > VPC**를 클릭합니다.

단계 2 **VPC Dashboard(VPC 대시보드) > Subnets(서브넷)**를 클릭하고 **Create Subnet(서브넷 생성)**을 클릭합니다.

단계 3 **Create Subnet(서브넷 생성)** 대화 상자에 다음 정보를 입력합니다.

- 서브넷을 식별하기 위한 사용자 정의 **Name tag(이름 태그)**.
- 이 서브넷에 사용할 **VPC**.
- 이 서브넷이 상주할 **Availability Zone(가용성 영역)**. Amazon이 해당 영역을 선택할 수 있게 하려면 **No Preference(환경 설정 없음)**를 선택합니다.
- IP 주소의 **CIDR block(CIDR 블록)**. 서브넷의 IP 주소 범위는 VPC의 IP 주소 범위의 하위 집합이어야 합니다. 블록 크기는 /16 네트워크 마스크와 /28 네트워크 마스크 사이여야 합니다. 서브넷의 크기는 VPC의 크기와 같아도 됩니다.

단계 4 서브넷을 생성하려면 **Yes, Create(예, 생성합니다)**를 클릭합니다.

단계 5 필요한 서브넷 수만큼 위의 단계를 반복합니다. 관리 트래픽용으로 별도의 서브넷을 생성하고, 데이터 트래픽용으로 필요한 수만큼의 서브넷을 생성합니다.

다음에 수행할 작업

다음 섹션의 설명에 따라 VPC에 라우트 테이블을 추가합니다.

## 라우트 테이블 추가

VPC용으로 구성된 게이트웨이에 라우트 테이블을 연결할 수 있습니다. 여러 서브넷을 단일 라우트 테이블과 연결할 수는 있지만, 각 서브넷은 한 번에 하나의 라우트 테이블에만 연결할 수 있습니다.

프로시저

- 
- 단계 1 **Services**(서비스) > **VPC**를 클릭합니다.
  - 단계 2 **VPC Dashboard**(VPC 대시보드) > **Route Tables**(라우트 테이블)를 클릭하고 **Create Route Tables**(라우트 테이블 생성)를 클릭합니다.
  - 단계 3 라우트 테이블 식별을 위한 사용자 정의 **Name tag**(이름 태그)를 입력합니다.
  - 단계 4 드롭다운 목록에서 이 라우트 테이블을 사용할 **VPC**를 선택합니다.
  - 단계 5 라우트 테이블을 생성하려면 **Yes, Create**(예, 생성합니다)를 클릭합니다.
  - 단계 6 방금 생성한 라우트 테이블을 선택합니다.
  - 단계 7 **Routes**(라우트) 탭을 클릭하여 상세 정보 창에 라우트 정보를 표시합니다.
  - 단계 8 **Edit**(수정), **Add another route**(다른 라우트 추가)를 차례로 클릭합니다.
    - a) **Destination**(대상) 열에 **0.0.0.0/0**을 입력합니다.
    - b) **Target**(대상) 열에서 게이트웨이를 선택합니다.
  - 단계 9 **Save**(저장)를 클릭합니다.
- 

다음에 수행할 작업

다음 섹션의 설명에 따라 보안 그룹을 생성합니다.

## 보안 그룹 생성

허용되는 프로토콜, 포트 및 소스 IP 범위를 지정하는 규칙을 사용하여 보안 그룹을 생성할 수 있습니다. 각 인스턴스에 할당할 수 있는 각기 다른 규칙을 사용해 여러 보안 그룹을 생성할 수 있습니다.

프로시저

- 
- 단계 1 **Services**(서비스) > **EC2**를 클릭합니다.
  - 단계 2 **EC2 Dashboard**(EC2 대시보드) > **Security Groups**(보안 그룹)를 클릭합니다.
  - 단계 3 **Create Security Group**(보안 그룹 생성)을 클릭합니다.
  - 단계 4 다음을 보안 그룹 생성 대화 상자에 입력합니다.
    - a) 보안 그룹 식별을 위한 사용자 정의 **Security group name**(보안 그룹 이름).
    - b) 이 보안 그룹에 대한 **Description**(설명).
    - c) 이 보안 그룹과 연결된 **VPC**.

단계 5 **Security group rules**(보안 그룹 규칙)를 구성합니다.

a) **Inbound**(인바운드) 탭을 클릭하고 **Add Rule**(규칙 추가)을 클릭합니다.

참고 외부 AWS에서 Firepower Management Center Virtual을 관리하려면 HTTPS 및 SSH 액세스가 필요합니다. 이에 따라 소스 IP 주소를 지정해야 합니다. 또한 AWS VPC 내에 Firepower Management Center Virtual과 Firepower Threat Defense Virtual을 모두 구성할 경우에는 개인 IP 관리 서브넷 액세스를 허용해야 합니다.

b) **Outbound**(아웃바운드) 탭을 클릭한 다음, **Add Rule**(규칙 추가)을 클릭하여 아웃바운드 트래픽용 규칙을 추가하거나, 기본값인 **All traffic**(모든 트래픽)(**Type**(유형)의 경우) 및 **Anywhere**(모든 위치)(**Destination**(대상)의 경우)를 그대로 유지합니다.

단계 6 보안 그룹을 생성하려면 **Create**(생성)를 클릭합니다.

다음에 수행할 작업

다음 섹션의 설명에 따라 네트워크 인터페이스를 생성합니다.

## 네트워크 인터페이스 생성

고정 IP 주소를 사용하여 Firepower Threat Defense Virtual용 네트워크 인터페이스를 생성할 수 있습니다. 특정 구축에 필요한 만큼 네트워크 인터페이스(외부 및 내부)를 생성합니다.

프로시저

단계 1 **Services**(서비스) > **EC2**를 클릭합니다.

단계 2 **EC2 Dashboard**(EC2 대시보드) > **Network Interfaces**(네트워크 인터페이스)를 클릭합니다.

단계 3 **Create Network Interface**(네트워크 인터페이스 생성)를 클릭합니다.

단계 4 **Create Network Interface**(네트워크 인터페이스 생성) 대화 상자에 다음 정보를 입력합니다.

- 네트워크 인터페이스에 대한 사용자 정의 **Description**(설명)(선택 사항)
- 드롭다운 목록에서 **Subnet**(서브넷)을 선택합니다. Firepower Threat Defense Virtual 인스턴스를 생성할 VPC의 서브넷을 선택해야 합니다.
- Private IP**(개인 IP) 주소를 입력합니다. **auto-assign**(자동 할당)보다는 고정 IP 주소를 사용하는 것이 좋습니다.
- 하나 이상의 **Security groups**(보안 그룹)를 선택합니다. 보안 그룹의 필수 포트가 모두 열려 있는지 확인합니다.

단계 5 네트워크 인터페이스를 생성하려면 **Yes, Create**(예, 생성합니다)를 클릭합니다.

단계 6 방금 생성한 네트워크 인터페이스를 선택합니다.

단계 7 마우스 오른쪽 버튼을 클릭하고 **Change Source/Dest. Check**(소스/대상 확인 변경)를 선택합니다.

단계 8 **Edit**(수정), **Add another route**(다른 라우트 추가)를 차례로 클릭합니다.

단계 9 **Disable**(비활성화)을 선택합니다. 생성하는 모든 네트워크 인터페이스에 대해 이 단계를 반복합니다.

다음에 수행할 작업

다음 섹션의 설명에 따라 탄력적 IP 주소를 생성합니다.

## 탄력적 IP 생성

인스턴스를 생성하면 공용 IP 주소가 인스턴스와 연결됩니다. 해당 공용 IP 주소는 인스턴스를 중지하고 시작할 때 자동으로 변경됩니다. 이 문제를 해결하려면 탄력적 IP 주소를 사용하여 인스턴스에 영구적 공용 IP 주소를 할당합니다. 탄력적 IP는 Firepower Threat Defense Virtual 및 기타 인스턴스의 원격 액세스에 사용되는 예약된 공용 IP입니다.



**참고** 최소한 Firepower Threat Defense Virtual 관리 및 진단 인터페이스용으로 탄력적 IP 주소를 생성할 수 있습니다.

프로시저

단계 1 **Services**(서비스) > **EC2**를 클릭합니다.

단계 2 **EC2 Dashboard**(EC2 대시보드) > **Elastic IPs**(탄력적 IP)를 클릭합니다.

단계 3 **Allocate New Address**(새 주소 할당)를 클릭합니다.

단계 4 필요한 수만큼의 탄력적/공용 IP에 대해 이 단계를 반복합니다.

단계 5 탄력적 IP를 생성하려면 **Yes, Allocate**(예, 할당합니다)를 클릭합니다.

단계 6 구축에 필요한 탄력적 IP 수만큼 위의 단계를 반복합니다.

다음에 수행할 작업

다음 섹션에 설명된 Firepower Threat Defense Virtual 구축





## 2 장

# Firepower Threat Defense Virtual 구축

이 장에서는 AWS 포털에서 Firepower Threat Defense Virtual을 구축하는 방법을 설명합니다.

- [Firepower Threat Defense Virtual 인스턴스 구축, 13 페이지](#)

## Firepower Threat Defense Virtual 인스턴스 구축

시작하기 전에

다음 작업을 수행하는 것이 좋습니다.

- [AWS 환경 구성, 6 페이지](#)의 설명에 따라 AWS VPC 및 EC2 요소를 구성합니다.
- Firepower Threat Defense Virtual 인스턴스에 AMI를 사용할 수 있는지 확인합니다.

프로시저

- 단계 1 <https://aws.amazon.com/marketplace>(Amazon Marketplace)로 이동하여 로그인합니다.
- 단계 2 Amazon Marketplace에 로그인한 후 Firepower Threat Defense Virtual(NGFWv (Cisco Firepower NGFW Virtual)-BYOL)에 대해 제공된 링크를 클릭합니다.  
참고 이전에 AWS를 사용했다면 로그아웃했다가 다시 로그인해야 링크가 작동합니다.
- 단계 3 **Continue**(계속)를 클릭하고 **Manual Launch**(수동 실행) 탭을 클릭합니다.
- 단계 4 **Accept Terms**(약관 동의)를 클릭합니다.
- 단계 5 원하는 지역에서 **Launch with EC2 Console**(EC2 콘솔로 실행)을 클릭합니다.
- 단계 6 Firepower Threat Defense Virtual에서 지원하는 **Instance Type**(인스턴스 유형)(c4.xlarge 권장)을 선택합니다.
- 단계 7 화면 하단의 **Next: Configure Instance Details**(다음: 인스턴스 상세 정보 구성) 버튼을 클릭합니다.
  - 이전에 생성한 VPC와 일치하도록 **Network**(네트워크)를 변경합니다.

- 이전에 생성한 관리 서브넷과 일치하도록 **Subnet**(서브넷)을 변경합니다. IP 주소를 지정하거나 자동 생성을 사용할 수 있습니다.
- 네트워크 인터페이스 아래에서 **Add Device**(디바이스 추가) 버튼을 클릭하여 eth1 네트워크 인터페이스를 추가합니다.
- eth0에 사용하기 위해서 이전에 생성한 관리 서브넷과 일치하도록 **Subnet**(서브넷)을 변경합니다.

참고 Firepower Threat Defense Virtual에는 2개의 관리 인터페이스가 필요합니다.

- **Advanced Details**(고급 상세 정보)에서 기본 로그인 정보를 추가합니다. 디바이스 이름과 비밀번호에 대한 요구 사항을 충족하도록 아래의 예시를 수정합니다.

주의:**Advanced Details**(고급 상세 정보) 필드에 데이터를 입력할 때는 일반 텍스트만 사용하십시오. 텍스트 편집기에서 이 정보를 복사하는 경우에는 일반 텍스트로만 복사해야 합니다. 유니코드 데이터(공백 포함)를 **Advanced Details**(고급 상세정보) 필드에 복사하는 경우, 인스턴스가 손상될 수 있으며 인스턴스를 종료하고 다시 생성해야 합니다.

Firepower Management Center를 사용하여 FTDv를 관리하기 위한 샘플 로그인 컨피그레이션:

```
#Sensor
{
    "AdminPassword": "<your_password>",
    "Hostname": "<your_hostname>",
    "ManageLocally": "No",
    "FmcIp": "<IP address of FMC>",
    "FmcRegKey": "<registration_passkey>",
    "FmcNatId": "<NAT_ID_if_required>"
}
```

Firepower Device Manager를 사용하여 FTDv를 관리하기 위한 샘플 로그인 컨피그레이션:

```
#Sensor
{
    "AdminPassword": "<your_password>",
    "Hostname": "<your_hostname>",
    "ManageLocally": "Yes"
}
```

단계 8 **Next: Add Storage**(다음: 스토리지 추가)를 클릭합니다.

기본값을 수락하거나 볼륨을 변경할 수 있습니다.

단계 9 **Next: Tag Instance**(다음: 인스턴스 태그 지정)를 클릭합니다.

태그는 대/소문자를 구별하는 키-값 쌍으로 구성됩니다. 예를 들어 **Key**(키)=Name, **Value**(값)=Firewall을 사용하여 태그를 정의할 수 있습니다.

단계 10 **Next: Configure Security Group**(다음: 보안 그룹 구성)을 선택합니다.



- 단계 11 **Select an existing Security Group**(기존 보안 그룹 선택)을 클릭하고 이전에 구성된 보안 그룹을 선택하거나 새 보안 그룹을 생성합니다. 보안 그룹 생성에 대한 자세한 내용은 AWS 설명서를 참조하십시오.
- 단계 12 **Review and Launch**(검토 및 실행)를 클릭합니다.
- 단계 13 **Launch**(실행)를 클릭합니다.
- 단계 14 기존 키 쌍을 선택하거나 새 키 쌍을 생성합니다.
- 참고 기존 키 쌍을 선택하거나 새 키 쌍을 생성할 수 있습니다. 키 쌍은 AWS가 저장하는 공개 키와 사용자가 저장하는 개인 키 파일로 구성됩니다. 이 두 키를 함께 사용하면 인스턴스에 안전하게 연결할 수 있습니다. 키 쌍은 인스턴스에 연결하는 데 필요할 수도 있으므로 확인된 위치에 저장해야 합니다.
- 단계 15 **Launch Instances**(인스턴스 실행)를 클릭합니다.
- 단계 16 **View Launch**(보기 실행)를 클릭하고 프롬프트를 따릅니다.
- 단계 17 **EC2 Dashboard**(EC2 대시보드) > **Network Interfaces**(네트워크 인터페이스)를 클릭합니다.
- 단계 18 **AWS 환경 구성, 6 페이지**에서 이전에 생성한 트래픽 인터페이스를 찾은 다음 **Attach**(연결)를 클릭합니다. 이는 Firepower Threat Defense Virtual 인스턴스에서 **eth2** 인터페이스가 됩니다.
- 단계 19 **AWS 환경 구성, 6 페이지**에서 이전에 생성한 트래픽 인터페이스를 찾은 다음 **Attach**(연결)를 클릭합니다. 이는 Firepower Threat Defense Virtual 인스턴스에서 **eth3** 인터페이스가 됩니다.
- 참고 4개의 인터페이스를 구성해야 합니다. 그렇지 않으면 Firepower Threat Defense Virtual에서 부팅 프로세스를 완료하지 않습니다.
- 단계 20 **EC2 Dashboard**(EC2 대시보드) > **Instances**(인스턴스)를 클릭합니다.
- 단계 21 상태를 보려면 인스턴스를 마우스 오른쪽 버튼으로 클릭하고 **Instance Settings**(인스턴스 설정) > **Get System Log**(인스턴스 시스템 로그)를 선택합니다.
- 참고 연결 문제에 대한 경고가 있을 수 있습니다. 이는 EULA가 완료될 때까지 eth0 인터페이스가 활성화되지 않기 때문입니다.
- 단계 22 20분 후에 Firepower Threat Defense Virtual을 Firepower Management Center에 등록할 수 있습니다.

다음에 수행할 작업

다음 단계는 선택한 관리 모드에 따라 달라집니다.

- **Enable Local Manager**(로컬 매니저 활성화)에 대해 **No**(아니요)를 선택한 경우 Firepower Management Center을 사용해 FTDv를 관리할 수 있습니다. [Firepower Management Center로 Firepower Threat Defense Virtual 관리, 39 페이지](#)를 참조하십시오.
- **Enable Local Manager**(로컬 매니저 활성화)에 대해 **Yes**(예)를 선택한 경우 Firepower Device Manager을 사용해 FTDv를 관리할 수 있습니다. [Firepower Device Manager를 이용한 Firepower Threat Defense Virtual 관리, 55 페이지](#)를 참조하십시오.

관리 옵션을 선택하는 방법에 대한 개요는 [Firepower 디바이스 관리 방법, 2 페이지](#)을 참조하십시오.





# 3 장

## Firepower Threat Defense Virtual Auto Scale for AWS 구축

이 문서에서는 AWS에서 FTDv Auto Scale Manager 용 서버리스 구성 요소를 구축하는 방법을 설명합니다.



**중요** 구축을 시작하기 전에 전체 문서를 읽어보십시오. 구축을 시작하기 전에 전체 조건이 충족되었는지 확인합니다.

- [AWS의 FTDv 용 Auto Scale 솔루션](#), 17 페이지
- [Auto Scale 솔루션 사전 요건](#), 21 페이지
- [Auto Scale 구축](#), 25 페이지
- [Auto Scale 유지 보수 작업](#), 34 페이지
- [Auto Scale 문제 해결 및 디버깅](#), 37 페이지

## AWS의 FTDv 용 Auto Scale 솔루션

다음 섹션에서는 AWS에서 Auto Scale 솔루션의 구성 요소가 FTDv에서 작동하는 방식을 설명합니다.

### Auto Scale 솔루션

Cisco는 램다, 자동 확장 그룹, ELB(Elastic Load Balancing), Amazon S3 버킷, SNS 및 CloudWatch를 비롯한 여러 AWS 서비스를 사용하여 FTDv 방화벽의 자동 확장 그룹을 구축하기 위한 CloudFormation 템플릿 및 스크립트를 제공합니다.

FTDv AWS의 Auto Scale은 완전한 서버리스 방식으로 구현되는 만큼(즉, 이 기능의 자동화와 관련된 헬퍼 VM 없음) AWS 환경의 FTDv 인스턴스에 수평 자동 확장 기능을 추가합니다.

FTDv Auto Scale 솔루션은 다음을 제공하는 CloudFormation 템플릿 기반 구축입니다.

- 완전 자동화된 FTDv 인스턴스 등록 및 FMC 등록 취소
- 확장된 FTDv 인스턴스에 자동으로 적용되는 NAT 정책, 액세스 정책 및 경로

- 로드 밸런서 및 다중 가용성 영역 지원
- Auto Scale 기능 활성화 및 비활성화 지원
- FMC에서만 작동합니다. Firepower Device Manager는 지원되지 않습니다.

### Auto Scale(버전 6.7) 개선 사항

- Custom Metric Publisher(맞춤형 메트릭 게시자)-새로운 램다 함수가 Auto Scale 그룹에 있는 모든 FTDv 인스턴스의 메모리 사용량에 대해 2분마다 FMC를 폴링한 다음 해당 값을 CloudWatch Metric에 게시합니다. 자세한 내용은 [입력 매개변수, 25 페이지](#)를 참조하십시오.
- 메모리 소비를 기반으로 하는 새로운 확장 정책을 사용할 수 있습니다.
- SSH 및 FMC에 대한 보안 터널용 FTDv 개인 IP 연결
- FMC 컨피그레이션 검증
- ELB에서 추가 수신 대기 포트 열기 지원
- 단일 스택 구축으로 수정되었습니다. 모든 램다 함수 및 AWS 리소스는 간소화된 구축을 위해 단일 스택에서 구축됩니다.

### 지원되는 소프트웨어 플랫폼

FTDv Auto Scale 솔루션은 FMC에서 관리하는 FTDv에 적용 가능하며 소프트웨어 버전과 무관합니다. [Cisco Firepower Compatibility Guide](#)는 운영 체제 및 호스팅 환경 요구 사항을 포함해서 Cisco Firepower 소프트웨어 및 하드웨어 호환성에 대한 내용을 제공합니다.

- [Firepower Management Centers: Virtual](#) 표는 Firepower 호환성 그리고 AWS의 FMCv에 대한 가상 호스팅 환경 요건을 제시합니다.
- [Firepower Threat Defense Virtual Compatibility](#) 표는 Firepower 호환성 그리고 AWS의 FTDv에 대한 가상 호스팅 환경 요건을 제시합니다.



참고 AWS Auto Scale 솔루션 구축을 위해 AWS에서 FTDv에 대해 지원되는 최소 Firepower 버전은 버전 6.4입니다. 메모리 기반 확장을 사용하려면 FMC에서 버전 6.6 이상을 실행해야 합니다.

## Auto Scale 사용 사례

이 FTDv AWS Auto Scale 솔루션의 사용 사례는 [그림 1: FTDv Auto Scale 사용 사례 다이어그램, 19 페이지](#)에 제시되어 있습니다. AWS 로드 밸런서는 인바운드 시작 연결만 허용하므로 외부에서 생성된 트래픽만 Cisco FTDv 방화벽을 통해 내부로 전달할 수 있습니다.



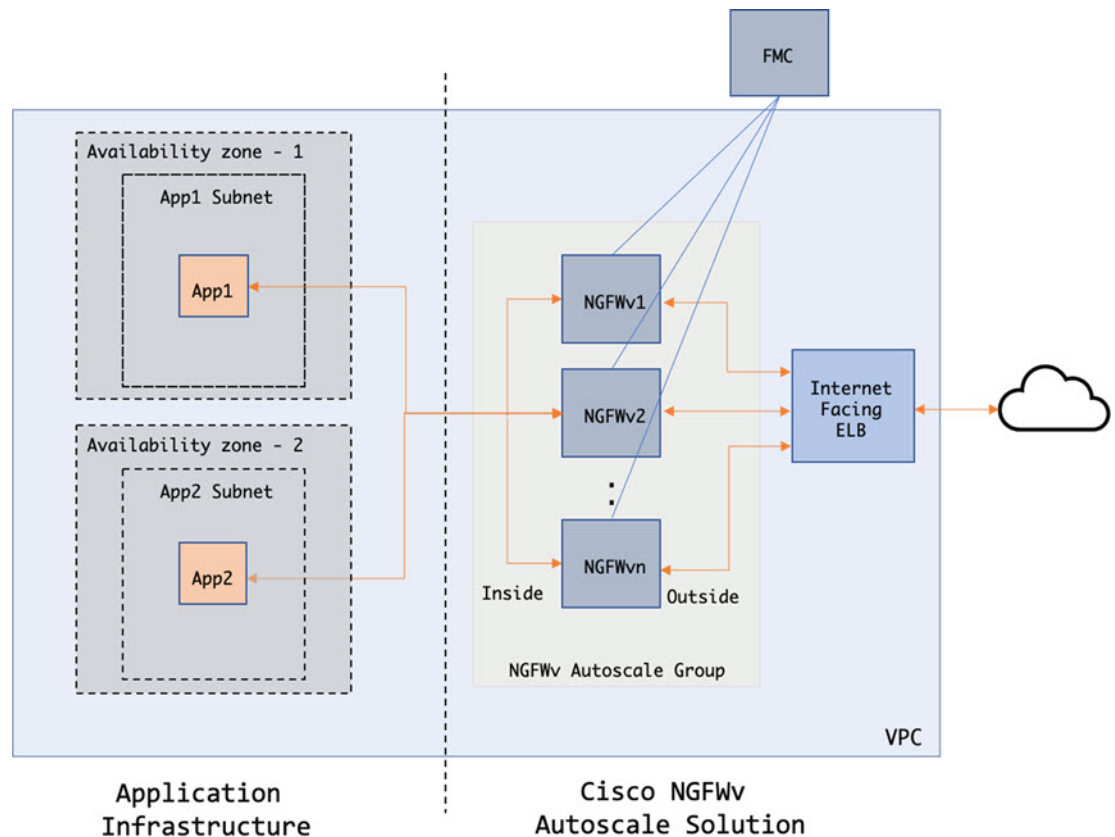
참고 보안 포트에는 [SSL 서버 인증서, 24 페이지](#) 전제 조건에 설명된 대로 SSL/TLS 인증서가 필요합니다.

인터넷 연결 로드 밸런서는 Network Load Balancer 또는 Application Load Balancer일 수 있습니다. 두 경우 모두 모든 AWS 요건 및 조건이 적용됩니다. 사용 사례 다이어그램에 나와 있는 것처럼 점선의 오른쪽은 FTDv 템플릿을 통해 구축됩니다. 왼쪽은 완전히 사용자 정의된 것입니다.



참고 애플리케이션 시작 아웃 바운드 트래픽은 FTDv를 통과하지 않습니다.

그림 1: FTDv Auto Scale 사용 사례 다이어그램



트래픽에 대한 포트 기반 분기가 가능합니다. 이는 NAT 규칙을 통해 수행할 수 있습니다. [FMC에서 개체, 디바이스 그룹, NAT 규칙, 액세스 정책의 구성, 31 페이지](#)를 참조하십시오. 예를 들어 인터넷 연결 LB DNS, 포트 80의 트래픽은 Application-1로 라우팅될 수 있습니다. 포트: 88 트래픽을 애플리케이션-2로 라우팅할 수 있습니다.

## Auto Scale 솔루션 작동 방식

FTDv 인스턴스를 확장 및 축소하기 위해 Auto Scale Manager라는 외부 엔터티가 메트릭을 모니터링하고, FTDv 인스턴스를 추가 또는 삭제하도록 자동 확장 그룹에 명령하고, 관리 FMC에 FTDv 디바이스를 등록 및 등록 취소하고, FTDv 인스턴스를 구성합니다.

Auto Scale Manager는 AWS 서버리스 아키텍처를 사용하여 구현되며 AWS 리소스, FTDv, FMC . Cisco는 Auto Scale Manager 구성 요소의 구축을 자동화하기 위해 CloudFormation 템플릿을 제공합니다. 이 템플릿은 전체 솔루션이 작동하는 데 필요한 기타 리소스도 구축합니다.



**참고** 서버리스 Auto Scale 스크립트는 CloudWatch 이벤트에서만 호출되므로 인스턴스가 시작될 때만 실행됩니다.

## Auto Scale 솔루션 구성 요소

다음 구성 요소가 Auto Scale 솔루션을 구성합니다.

### CloudFormation 템플릿

CloudFormation 템플릿은 AWS의 Auto Scale 솔루션에 필요한 리소스를 구축하는 데 사용됩니다. 템플릿은 다음으로 구성됩니다.

- 자동 확장 그룹, 로드 밸런서, 보안 그룹 및 기타 기타 구성 요소
- 템플릿은 사용자 입력에 따라 구축을 맞춤화합니다.



**참고** 템플릿에는 사용자 입력을 검증하는 데 제한이 있으므로 구축 중에 입력을 검증하는 것은 사용자의 책임입니다.

### 람다 함수

Auto Scale은 Python으로 개발한 람다 함수의 집합으로서 라이프사이클 후크, SNS, CloudWatch 이벤트/경보 이벤트에서 트리거됩니다. 기본 기능은 다음과 같습니다.

- 인스턴스에 Diag, Gig0/0 및 Gig 0/1 인터페이스를 추가/제거합니다.
- 로드 밸런서의 대상 그룹에 Gig0/1 인터페이스를 등록합니다.
- FMC에 새 FTDv를 등록합니다.
- FMC를 통해 새 FTDv를 구성하고 구축합니다.
- FMC에서 확장된 FTDv를 등록취소(제거)합니다.
- FMC에서 메모리 메트릭을 게시합니다.

람다 함수는 Python 패키지 형식으로 고객에게 제공됩니다.

#### 라이프 사이클 후크

- 라이프 사이클 후크는 인스턴스에 대한 라이프 사이클 변경 알림을 가져오는 데 사용됩니다.
- 인스턴스 시작의 경우 라이프 사이클 후크를 사용하여 FTDv 인스턴스에 인터페이스를 추가하고 대상 그룹에 외부 인터페이스 IP를 등록할 수 있는 람다 함수를 트리거합니다.
- 인스턴스가 종료되는 경우, 라이프 사이클 후크를 사용하여 대상 그룹에서 FTDv 인스턴스의 등록을 취소하는 람다 함수를 트리거합니다.

#### 간편 알림 서비스(SNS)

- AWS의 SNS(Simple Notification Service)를 사용하여 이벤트를 생성합니다.
- AWS에는 서버리스 람다 함수에 적합한 오케스트레이터가 없다는 제한 때문에, 솔루션은 SNS를 일종의 기능 체인으로 사용하여 이벤트를 기반으로 람다 함수를 오케스트레이션합니다.

## Auto Scale 솔루션 사전 요건

### 구축 파일 다운로드

FTDv Auto Scale for AWS 솔루션을 시작하는 데 필요한 파일을 다운로드합니다. Firepower 버전의 구축 스크립트 및 템플릿은 GitHub 리포지토리에서 제공됩니다.

- <https://github.com/CiscoDevNet/cisco-ftdv/tree/master/autoscale/aws>



주의 Cisco에서 제공하는 자동 확장용 구축 스크립트 및 템플릿은 오픈 소스 예시로 제공되며 일반적인 Cisco TAC 지원 범위에서는 다루지 않습니다. GitHub에서 정기적으로 업데이트 및 ReadMe 지침을 확인하십시오.

### 인프라 구성

복제/다운로드된 GitHub 리포지토리의 **infrastructure.yaml** 파일은 템플릿 폴더에 있습니다. 이 CFT는 버킷 정책을 통해 VPC, 서브넷, 경로, ACL, 보안 그룹, VPC 엔드 포인트 및 S3 버킷을 구축하는 데 사용할 수 있습니다. 이 CFT는 요구 사항에 맞게 수정할 수 있습니다.

다음 섹션에서는 이러한 리소스 및 해당 리소스가 Auto Scale에서 사용되는 방법에 대해 자세히 설명합니다. 이러한 리소스를 수동으로 구축하고 Auto Scale에서도 사용할 수 있습니다.



참고 **infrastructure.yaml** 템플릿은 VPC, 서브넷, ACL, 보안 그룹, S3 버킷 및 VPC 엔드 포인트만 구축합니다. SSL 인증서, 람다 레이어 또는 KMS 키 리소스는 생성하지 않습니다.

## VPC

애플리케이션 요구 사항에 따라 VPC를 생성해야 합니다. VPC에는 인터넷에 대한 경로가 연결된 하나 이상의 서브넷이 있는 인터넷 게이트웨이가 있어야 합니다. 보안 그룹, 서브넷 등에 대한 요구 사항은 해당 섹션을 참조하십시오.

## 서브넷

필요할 경우 애플리케이션 요구 사항에 따라 서브넷을 생성할 수 있습니다. FTDv VM에는 사용 사례에 나와 있는 것처럼 작동하기 위해 3개의 서브넷이 필요합니다.



참고 다중 가용성 영역 지원이 필요한 경우 서브넷은 AWS 클라우드 내의 영역 속성이므로 각 영역에서 서브넷이 필요합니다.

### 외부 서브넷

외부 서브넷에는 인터넷 게이트웨이에 대한 기본 경로가 '0.0.0.0/0'이어야 합니다. 여기에는 FTDv의 외부 인터페이스가 포함되며 인터넷 연결 NLB도 이 서브넷에 포함됩니다.

### 내부 서브넷

이는 NAT/인터넷 게이트웨이가 있거나 없는 애플리케이션 서브넷과 유사할 수 있습니다. FTDv 상태 프로브의 경우 포트 80을 통해 AWS 메타 데이터 서버(169.254.169.254)에 연결할 수 있어야 합니다.



참고 이 AutoScale 솔루션에서 로드 밸런서 상태 프로브는 `inside/Gig0/0` 인터페이스를 통해 AWS 메타 데이터 서버로 리디렉션됩니다. 그러나 로드 밸런서에서 FTDv로 전송되는 상태 프로브 연결을 제공하는 고유한 애플리케이션을 사용하여 이를 변경할 수 있습니다. 이 경우 상태 프로브 응답을 제공하려면 AWS Metadata Server 개체를 해당 애플리케이션 IP 주소로 교체해야 합니다.

### 관리 서브넷

이 서브넷에는 FTDv 관리 인터페이스가 포함되어 있습니다. 이 서브넷에서 FMC를 사용하는 경우 FTDv에 EIP(Elastic IP Address)를 할당하는 것은 선택 사항입니다. 진단 인터페이스도 이 서브넷에 있습니다.



### 람다 서브넷

AWS 람다 함수를 사용하려면 NAT 게이트웨이가 기본 게이트웨이인 두 개의 서브넷이 필요합니다. 이렇게 하면 VPC 전용의 람다 함수가 생성됩니다. 람다 서브넷은 다른 서브넷만큼 넓을 필요는 없습니다. 람다 서브넷에 대한 모범 사례는 AWS 설명서를 참조하십시오.

### 애플리케이션 서브넷

Auto Scale 솔루션에서 이 서브넷에 적용되는 제한은 없지만, 애플리케이션이 VPC 외부에서 아웃 바운드 연결을 필요로 하는 경우 서브넷에 각각의 경로가 구성되어 있어야 합니다. 이는 아웃 바운드에서 시작된 트래픽이 로드 밸런서를 통과하지 않기 때문입니다. AWS [Elastic Load Balancing User Guide](#)를 참조하십시오.

## 보안 그룹

제공된 Auto Scale 그룹 템플릿에서 모든 연결이 허용됩니다. Auto Scale 솔루션이 작동하려면 다음 연결만 필요합니다.

표 3: 필수 포트

포트	사용	서브넷
8305	FMC-FTDv 보안 터널 연결	관리 서브넷
상태 프로브 포트 (기본값: 8080)	인터넷 연결 로드 밸런서 상태 프로브	외부, 내부 서브넷
애플리케이션 포트	애플리케이션 데이터 트래픽	외부, 내부 서브넷

### FMC 인스턴스의 보안 그룹 또는 ACL

람다 함수와 FMC 간의 HTTPS 연결을 허용합니다. 람다 함수는 NAT 게이트웨이를 기본 경로로 사용하는 람다 서브넷에서 유지되므로 FMC는 NAT 게이트웨이 IP 주소에서 인바운드 HTTPS 연결을 가질 수 있어야 합니다.

## Amazon S3 버킷

Amazon Simple Storage Service(Amazon S3)는 업계 최고의 확장성, 데이터 가용성, 보안 및 성능을 제공하는 개체 스토리지 서비스입니다. 방화벽 템플릿 및 애플리케이션 템플릿 모두에 필요한 모든 작업을 S3 버킷에 담을 수 있습니다.

템플릿이 구축되면 S3 버킷의 Zip 파일을 참조하는 람다 함수가 생성됩니다. 따라서 사용자 계정에서 S3 버킷에 액세스할 수 있어야 합니다.

## SSL 서버 인증서

인터넷 연결 로드 밸런서가 TLS / SSL을 지원해야 하는 경우 인증서 ARN이 필요합니다. 자세한 내용은 다음 링크를 참조하십시오.

- [서버 인증서 작업](#)
- [테스트를 위한 개인 키 및 자체 서명 인증서 생성](#)
- [자체 서명 SSL 인증서로 AWS ELB 생성](#)(서드 파티 링크)

ARN의 예: `arn:aws:iam::[AWS 계정]:server-certificate/[인증서 이름]`

## 람다 레이어

`autoscale_layer.zip`은 Linux 환경(예: Python 3.6이 설치된 Ubuntu 18.04)에서 생성 할 수 있습니다.

```
#!/bin/bash
mkdir -p layer
virtualenv -p /usr/bin/python3.6 ./layer/
source ./layer/bin/activate
pip3 install pycrypto==2.6.1
pip3 install paramiko==2.7.1
pip3 install requests==2.23.0
pip3 install scp==0.13.2
pip3 install jsonschema==3.2.0
echo "Copy from ./layer directory to ./python\"
mkdir -p ./python/.libs_cffi_backend/
cp -r ./layer/lib/python3.6/site-packages/* ./python/
cp -r ./layer/lib/python3.6/site-packages/.libs_cffi_backend/* ./python/.libs_cffi_backend/
zip -r autoscale_layer.zip ./python
```

결과 `autoscale_layer.zip` 파일을 `lambda-python-files` 폴더에 복사해야 합니다.

## KMS 마스터 키

이는 FMC 및 FTDv 비밀번호가 암호화된 형식인 경우 필요합니다. 그렇지 않으면 이 구성 요소가 필요하지 않습니다. 비밀번호는 여기에 제공된 KMS만 사용하여 암호화해야 합니다. KMS ARN이 CFT에 입력된 경우 비밀번호를 암호화해야 합니다. 그렇지 않으면 비밀번호는 일반 텍스트여야 합니다.

마스터 키 및 암호화에 대한 자세한 내용은 AWS 문서 [Creating keys](#) 및 [the AWS CLI Command Reference](#)에서 비밀번호 암호화 및 KMS에 대한 내용을 참조하십시오.

예:

```
$ aws kms encrypt --key-id <KMS-ARN> --plaintext 'MyC0mplIc@tedProtect1oN'
{
  "KeyId": "KMS-ARN",
  "CiphertextBlob":
  "AQICAHgcQFAGtz/hvaxMtJvY/x/rfHnKI3clFPpSXUU7HQrnCAFwfXhXHJAHl8tcVmDqurALAAAaJBoBgkqhki
  G9w0BBwagWzBZAgEAMFQGCsqGSIB3DQEhATAeBglghkgBZQMEAS4weEQM45AIkTqjSekX2mniAgEQgCcOav6Hhol
  +wpxWRtXY4y1Z1d0z1P4fx0jTdosfCbPnUExmNJ4zdx8="
```

```
}
$
```

*CiphertextBlob* 키의 값을 비밀번호로 사용해야 합니다.

## Python 3 환경

*make.py* 파일은 복제된 리포지토리의 최상위 디렉토리에 있습니다. 이렇게하면 *python* 파일을 Zip 파일로 압축하고 대상 폴더에 복사합니다. 이러한 작업을 수행하려면 Python 3 환경을 사용할 수 있어야 합니다.

## Auto Scale 구축

### 준비

애플리케이션이 구축되었거나 구축 계획을 사용할 수 있어야 합니다.

### 입력 매개변수

다음 입력 매개 변수는 구축 전에 수집해야 합니다.

표 4: *Auto Scale* 입력 매개 변수

파라미터	허용되는 값 / 유형	설명
PodNumber	문자열 허용되는 패턴: '\d{1,3}\$'	Pod 번호입니다. 이는 Auto Scale 그룹 이름 (FTDv-Group-Name)의 접미사입니다. 예를 들어 이 값이 '1'인 경우 그룹 이름은 <i>FTDv-Group-Name-1</i> 이 됩니다.  숫자는 한 자릿수 이상 세 자릿수 이하여야 합니다. 기본값: 1
AutoscaleGrpNamePrefix	문자열	Auto Scale 그룹 이름 접두사입니다. Pod 번호는 접미사로 추가됩니다.  최대 문자수: 18자  예: Cisco-FTDv-1
NotifyEmailID	문자열	Auto Scale 이벤트가 이 이메일 주소로 전송됩니다. 구독 이메일 요청을 수락해야 합니다.  예: admin@company.com

파라미터	허용되는 값 / 유형	설명
VpcId	문자열	디바이스를 구축해야 하는 VPC ID입니다. 이는 AWS 요건에 따라 구성해야 합니다.  유형: AWS::EC2::VPC::Id  "infrastructure.yaml" 파일을 사용하여 인프라를 구축하는 경우 스택의 출력 섹션에 이 값이 지정됩니다. 해당 값을 사용하십시오.
LambdaSubnets	목록	람다 함수가 구축될 서브넷  유형: List<AWS::EC2::Subnet::Id>  "infrastructure.yaml" 파일을 사용하여 인프라를 구축하는 경우 스택의 출력 섹션에 이 값이 지정됩니다. 해당 값을 사용하십시오.
LambdaSG	목록	람다 함수의 보안 그룹  유형: List<AWS::EC2::SecurityGroup::Id>  "infrastructure.yaml" 파일을 사용하여 인프라를 구축하는 경우 스택의 출력 섹션에 이 값이 지정됩니다. 해당 값을 사용하십시오.
S3BktName	문자열	파일의 S3 버킷 이름입니다. 이는 AWS 요건에 따라 사용자 계정에서 구성해야 합니다.  "infrastructure.yaml" 파일을 사용하여 인프라를 구축하는 경우 스택의 출력 섹션에 이 값이 지정됩니다. 해당 값을 사용하십시오.
LoadBlancerType	문자열	인터넷 연결 로드 밸런서의 유형("애플리케이션" 또는 "네트워크")입니다.  예: application
LoadBlancerSG	문자열	로드 밸런서의 보안 그룹 네트워크 로드 밸런서의 경우에는 사용되지 않습니다. 그러나 보안 그룹 ID를 제공해야 합니다.  유형: List<AWS::EC2::SecurityGroup::Id>  "infrastructure.yaml" 파일을 사용하여 인프라를 구축하는 경우 스택의 출력 섹션에 이 값이 지정됩니다. 해당 값을 사용하십시오.

파라미터	허용되는 값 / 유형	설명
LoadBlancerPort	정수	로드 밸런서 포트 이 포트는 선택한 로드 밸런서 유형에 따라 프로토콜로 HTTP / HTTPS 또는 TCP / TLS를 사용하여 LB에서 열립니다.  포트가 유효한 TCP 포트인지 확인합니다. 이 포트는 로드 밸런서 리스너를 생성하는 데 사용됩니다.  기본값: 80
SSL인증서	문자열	보안 포트 연결을 위한 SSL 인증서의 ARN입니다. 지정하지 않으면 로드 밸런서에서 열린 포트는 TCP / HTTP가 됩니다. 지정된 경우 로드 밸런서에서 열린 포트는 TLS / HTTPS입니다.
TgHealthPort	정수	이 포트는 상태 프로브의 대상 그룹에서 사용됩니다. FTDv에서 이 포트에 도착하는 상태 프로브는 AWS 메타 데이터 서버로 라우팅되며 트래픽에 사용해서는 안 됩니다. 유효한 TCP 포트여야 합니다.  애플리케이션 자체가 상태 프로브에 응답하도록 하려면 FTDv에 따라 NAT 규칙을 변경할 수 있습니다. 이 경우 애플리케이션이 응답하지 않으면 FTDv가 비정상 상태로 표시되고 비정상 인스턴스 임계 값 알람으로 인해 삭제됩니다.  예: 8080
AssignPublicIP	부울	"true"로 선택된 경우 공용 IP가 할당됩니다. BYOL 유형 FTDv의 경우 <a href="https://tools.cisco.com">https://tools.cisco.com</a> 에 연결해야 합니다.  예: true
인스턴스 유형	문자열	AMI(Amazon Machine Image)는 인스턴스의 크기와 필요한 메모리 양을 결정하는 다양한 인스턴스 유형을 지원합니다.  FTDv을 지원하는 AMI 인스턴스 유형만 사용해야 합니다. <a href="#">Firepower 릴리스 노트</a> 를 참조하십시오.  예: c4.2xlarge
LicenseType	문자열	FTDv 라이선스 유형(BYOL 또는 PAYG) 관련 AMI ID가 동일한 라이선싱 유형인지 확인합니다.  예: BYOL

파라미터	허용되는 값 / 유형	설명
AmiId	문자열	FTDv AMI ID(유효한 Cisco FTDv AMI ID) 유형: AWS::EC2::Image::Id 영역 및 원하는 이미지 버전에 따라 올바른 AMI ID를 선택하십시오. Auto Scale 기능은 Firepower 버전 6.4 이상, BYOL / PAYG 이미지를 지원합니다. 두 경우 모두 AWS 마켓플레이스에서 라이선스를 수락해야 합니다. BYOL의 경우 컨피그레이션 JSON의 'licenseCaps' 키를 'BASE', 'MALWARE', 'THREAT', 'URLFilter' 등의 기능으로 업데이트하십시오.
NoOfAZs	정수	FTDv가 1~3의 범위에 걸쳐 있어야 하는 가용성 영역의 수입니다. ALB 구축의 경우 AWS에 필요한 최소값은 2입니다. 예: 2
ListOfAZs	쉼표로 구분된 문자열	쉼표로 구분된 영역의 목록(순서대로) 참고 나열되는 순서가 중요합니다. 서브넷 목록은 동일한 순서로 제공되어야 합니다. "infrastructure.yaml" 파일을 사용하여 인프라를 구축하는 경우 스택의 출력 섹션에 이 값이 지정됩니다. 해당 값을 사용하십시오. 예: us-east-1a, us-east-1b, us-east-1c
MgmtInterfaceSG	문자열	FTDv 관리 인터페이스의 보안 그룹입니다. 유형: List<AWS::EC2::SecurityGroup::Id> "infrastructure.yaml" 파일을 사용하여 인프라를 구축하는 경우 스택의 출력 섹션에 이 값이 지정됩니다. 해당 값을 사용하십시오.
InsideInterfaceSG	문자열	FTDv 내부 인터페이스의 보안 그룹입니다. 유형: AWS::EC2::SecurityGroup::Id "infrastructure.yaml" 파일을 사용하여 인프라를 구축하는 경우 스택의 출력 섹션에 이 값이 지정됩니다. 해당 값을 사용하십시오.

파라미터	허용되는 값 / 유형	설명
OutsideInterfaceSG	문자열	FTDv 외부 인터페이스의 보안 그룹입니다. 유형: AWS::EC2::SecurityGroup::Id "infrastructure.yaml" 파일을 사용하여 인프라를 구축하는 경우 스택의 출력 섹션에 이 값이 지정됩니다. 해당 값을 사용하십시오. 예: sg-0c190a824b22d52bb
MgmtSubnetId	섬표로 구분된 목록	섬표로 구분된 관리 서브넷 ID 목록입니다. 목록은 해당 가용 영역과 동일한 순서여야 합니다. 유형: List<AWS::EC2::SecurityGroup::Id> "infrastructure.yaml" 파일을 사용하여 인프라를 구축하는 경우 스택의 출력 섹션에 이 값이 지정됩니다. 해당 값을 사용하십시오.
InsideSubnetId	섬표로 구분된 목록	섬표로 구분된 inside/Gig0/0 ID 목록입니다. 목록은 해당 가용 영역과 동일한 순서여야 합니다. 유형: List<AWS::EC2::SecurityGroup::Id> "infrastructure.yaml" 파일을 사용하여 인프라를 구축하는 경우 스택의 출력 섹션에 이 값이 지정됩니다. 해당 값을 사용하십시오.
OutsideSubnetId	섬표로 구분된 목록	섬표로 구분된 outside/Gig0/1 ID 목록입니다. 목록은 해당 가용 영역과 동일한 순서여야 합니다. 유형: List<AWS::EC2::SecurityGroup::Id> "infrastructure.yaml" 파일을 사용하여 인프라를 구축하는 경우 스택의 출력 섹션에 이 값이 지정됩니다. 해당 값을 사용하십시오.
KmsArn	문자열	기존 KMS의 ARN(대기시 암호화 할 AWS KMS 키) 지정된 경우 FMC 및 FTDv 비밀번호를 암호화해야 합니다. 비밀번호 암호화는 지정된 ARN만 사용하여 수행해야 합니다. 암호화된 비밀번호 생성 예: "aws kmscrypt --key-id<KMS ARN> --plaintext<password> ". 표시된 대로 생성된 비밀번호를 사용하십시오. 예: arn:aws:kms:us-east-1:[AWS 계정]:key/7d586a25-5875-43b1-bb68-a452e2f6468e

파라미터	허용되는 값 / 유형	설명
ngfwPassword	문자열	모든 FTDv 인스턴스에는 기본 비밀번호가 표시되며, 이 비밀번호는 Launch Template(시작 템플릿)(Autoscale Group)의 <i>Userdata</i> (사용자 데이터) 필드에 입력됩니다.  이 입력은 FTDv에 액세스할 수 있게 되면 비밀번호를 새로 입력한 비밀번호로 변경합니다.  KMS ARN이 사용되지 않는 경우 일반 텍스트 비밀번호를 사용하십시오. KMS ARN을 사용하는 경우 암호화된 비밀번호를 사용해야 합니다.  예: Cisco123789! or AQIAgcQFAGtz/hvaxMtJvY/x/rfHnI3lPpSXU
fmcServer	숫자 문자열	람다 함수와 FTDv 관리 인터페이스 모두에 연결할 수 있는 관리 FMC의 IP 주소입니다.  예: 10.10.17.21
fmcOperationsUsername	문자열	관리 FMC에서 생성된 네트워크 관리자 이상의 권한이 있는 사용자. 자세한 내용은 <a href="#">Firepower Management Center Configuration Guide</a> 에서 사용자 및 역할 생성에 대한 내용을 참조하세요.  예: apiuser-1
fmcOperationsPassword	문자열	KMS ARN이 언급되지 않은 경우 일반 텍스트 비밀번호를 사용하십시오. 언급된 경우 암호화된 비밀번호를 사용해야 합니다.  예: Cisco123@ or AQICAHgcQAtz/hvaxMtJvY/x/mKI3clFPpSXUHQRnCAajB
fmcDeviceGrpName	문자열	FMC 디바이스 그룹 이름  예: AWS-Cisco-NGFW-VMs-1
fmcPublishMetrics	부울	"TRUE"로 설정된 경우, 제공된 디바이스 그룹에 등록된 FTDv 센서의 메모리 소비량을 가져 오기 위해 2분마다 한 번씩 실행되는 람다 함수가 생성됩니다.  허용되는 값: TRUE, FALSE  예: true



파라미터	허용되는 값 / 유형	설명
fmcMetricsUsername	문자열	AWS CloudWatch에 대한 메트릭 계정의 고유한 FMC 사용자 이름입니다. 자세한 내용은 <a href="#">Firepower Management Center Configuration Guide</a> 에서 사용자 및 역할 생성에 대한 내용을 참조하세요.  "fmcPublishMetrics"가 "FALSE"로 설정된 경우 이 입력을 제공할 필요가 없습니다.  예: publisher-1
fmcMetricsPassword	문자열	AWS CloudWatch에 메트릭 계정을 위한 FMC 비밀번호입니다. KMS ARN이 언급되지 않은 경우 일반 텍스트 비밀번호를 사용하십시오. 언급된 경우 암호화된 비밀번호를 사용해야 합니다.  "fmcPublishMetrics"가 "FALSE"로 설정된 경우 이 입력을 제공할 필요가 없습니다.  예: Cisco123789!
CpuThresholds	쉼표로 구분된 정수	CPU 하한 임계값 및 CPU 상한 임계값 최소값은 0이고 최대값은 99입니다.  기본값: 10, 70  하한 임계값은 상한 임계값보다 작아야 합니다.  예: 30, 70
MemoryThresholds	쉼표로 구분된 정수	하위 MEM 임계값 및 상위 MEM 임계값 최소값은 0이고 최대값은 99입니다.  기본값: 40, 70  하한 임계값은 상한 임계값보다 작아야 합니다.  "fmcPublishMetrics" 매개 변수가 "FALSE"이면 아무런 효과가 없습니다.  예: 40, 50

## FMC에서 개체, 디바이스 그룹, NAT 규칙, 액세스 정책의 구성

전체 기능을 갖춘 별도 서버의 다중 디바이스 관리자인 Firepower Management Center(FMC)를 사용해 FTDv를 관리할 수 있습니다. FTDv는 FDTv 가상 시스템에 할당된 관리 인터페이스의 FMC에 등록하고 통신합니다. 자세한 내용은 [Firepower Management Center를 이용한 Firepower Threat Defense Virtual 관련 정보, 39 페이지](#)를 참조하십시오.

FTDv 컨피그레이션에 사용되는 모든 개체는 사용자가 생성해야 합니다.



**중요** 디바이스 그룹을 생성하고 규칙을 적용해야 합니다. 디바이스 그룹에 적용된 모든 컨피그레이션은 FTDv 인스턴스로 푸시됩니다.

### 개체

다음 개체를 생성합니다.

표 5: FTDv 관리를 위한 FMC 컨피그레이션 개체

개체 유형	이름	값
Host(호스트)	aws-metadata-server	169.254.169.254
포트	health-check-port	8080 / 필요에 따라 다른 포트
Zone	내부 / 다른 이름	—
Zone	외부 / 다른 이름	—

### NAT 정책

일반적인 NAT 규칙은 내부 주소를 외부 인터페이스 IP 주소의 포트로 변환합니다. 이러한 유형의 NAT 규칙을 인터페이스 포트 주소 변환(PAT)이라고 합니다. NAT 정책에 대한 자세한 내용은 [Firepower Management Center](#)로 [Firepower Threat Defense Virtual](#) 관리, 39 페이지의 NAT 구성, 49 페이지를 참조하십시오.

NAT 정책에는 하나의 필수 규칙이 필요합니다.

- 소스 영역: 외부 영역
- 대상 영역: 내부 영역
- 원본 소스: any-ipv4
- 원본 소스 포트 - 원본/기본
- 원본 대상: 인터페이스
- 원본 대상 포트: 8080/ 또는 사용자가 구성한 상태 포트
- 변환된 소스: any-ipv4
- 변환된 소스 포트: 원본/기본
- 변환된 대상: aws-metadata-server
- 변환된 대상 포트: 80 / HTTP

마찬가지로 모든 데이터 트래픽 NAT 규칙을 추가할 수 있으므로 이 컨피그레이션이 FTDv 디바이스로 푸시됩니다.



**중요** 생성된 NAT 정책은 디바이스 그룹에 적용해야 합니다. 람다 함수의 FMC 검증에서 이를 확인합니다.

### 액세스 정책

액세스 제어를 내부에서 외부로 향하는 트래픽을 허용하도록 구성합니다. 모든 필수 정책이 포함된 액세스 정책을 생성할 수 있습니다. 이 포트의 트래픽에 도달할 수 있도록 상태 포트 개체를 허용해야 합니다. 액세스 정책에 대한 자세한 내용은 [Firepower Management Center로 Firepower Threat Defense Virtual 관리, 39 페이지의 액세스 제어 구성, 52 페이지를 참조하십시오.](#)

## 컨피그레이션 JSON 파일 업데이트

*Configuration.json* 파일은 [GitHub](#) 리포지토리에서 가져온 아카이브 Zip의 일부인 *lambda\_python\_files* 폴더에 있습니다. JSON 키는 변경할 수 없습니다. FTDv VM의 모든 고정 경로는 JSON 파일에서 구성해야 합니다.

고정 경로 컨피그레이션의 예는 다음을 참조하십시오.

```
{
  "interface": "inside",
  "network": "any-ipv4",
  "gateway": "",
  "metric": "1"
}
```

JSON 파일의 모든 값은 기본 FTDv 비밀번호를 제외하고 요구 사항에 따라 수정할 수 있습니다.

## Amazon Simple Storage Service(S3)로 파일 업로드

대상 디렉토리의 모든 파일을 Amazon S3 버킷에 업로드해야 합니다. 원할 경우 CLI를 사용하여 대상 디렉토리의 모든 파일을 Amazon S3 버킷에 업로드할 수 있습니다.

```
$ cd ./target
$ aws s3 cp . s3://<bucket-name> --recursive
```

## 스택 구축

구축을 위한 모든 전제 조건이 완료되면 AWS CloudFormation 스택을 생성할 수 있습니다.

대상 디렉토리의 *deploy\_ngfw\_autoscale.yaml* 파일을 사용합니다.

[입력 매개변수, 25 페이지](#)에 수집된 매개 변수를 제공합니다.

## 구축 검증

템플릿 구축이 완료되면, 람다 함수 및 CloudWatch 이벤트가 생성되었는지 검증해야 합니다. 기본적으로 Auto Scale 그룹에는 최소 및 최대 인스턴스 수가 0입니다. 원하는 인스턴스 수를 사용하여 AWS EC2 콘솔에서 Auto Scale 그룹을 편집해야 합니다. 그러면 새 FTDv 인스턴스가 트리거됩니다.

인스턴스를 하나만 실행하고 그 워크플로우를 확인하고 예상대로 작동하는지에 대한 동작을 검증하는 것이 좋습니다. FTDv의 실제 요구 사항을 구축한 후에는 동작에 대해 확인할 수도 있습니다. AWS Scaling 정책에서 FTDv 인스턴스가 제거되지 않도록 최소 인스턴스 수를 축소 보호로 표시 할 수 있습니다.

## Auto Scale 유지 보수 작업

### 확장 프로세스

이 항목에서는 Auto Scale 그룹에 대해 하나 이상의 확장 프로세스를 일시 중지한 다음 다시 시작하는 방법을 설명합니다.

확장 작업 시작 및 중지

스케일 아웃/인 작업을 시작하고 중지하려면 다음 단계를 수행합니다.

- AWS Dynamic Scaling의 경우 - 다음 링크를 참조하여 스케일 아웃 작업을 활성화하거나 비활성화할 수 있습니다.

[확장 프로세스 일시 중단 및 다시 시작](#)

### 상태 모니터

CloudWatch Cron 작업은 60분마다 Health Doctor 모듈의 Auto Scale Manager 램다를 트리거합니다.

- 유효한 FTDv VM에 속한 비정상적인 IP가 있는 경우 FTDv가 1시간 이상 경과하면 해당 인스턴스가 삭제됩니다.
- 해당 IP가 유효한 FTDv VM에 있지 않으면 대상 그룹에서 IP만 제거됩니다.

상태 모니터는 디바이스 그룹, 액세스 정책 및 NAT 규칙에 대한 FMC 컨피그레이션도 검증합니다. IP/인스턴스 상태가 비정상이거나 FMC 검증에 실패하면 상태 모니터가 사용자에게 이메일을 전송합니다.

상태 모니터 비활성화

상태 모니터를 비활성화하려면 `constant.py`에서 상수를 "True"로 지정합니다.

상태 모니터 활성화

상태 모니터를 활성화하려면 `consist.py`에서 상수를 "False"로 지정합니다.

### 라이프 사이클 후크 비활성화

라이프 사이클 후크를 비활성화해야 하는 경우는 드물지만 비활성화되면 인스턴스에 인터페이스를 추가하지 않습니다. 또한 일련의 FTDv 인스턴스 구축이 실패할 수 있습니다.

## Auto Scale Manager 비활성화

Auto Scale Manager를 비활성화하려면 각 CloudWatch 이벤트 "notify-instance-launch" 및 "notify-instance-terminate"를 비활성화해야 합니다. 이 기능을 비활성화하면 새 이벤트에 대해 램다가 트리거되지 않습니다. 그러나 이미 실행 중인 램다 작업은 계속 진행됩니다. Auto Scale Manager는 갑자기 중지되지 않습니다. 스택 삭제 또는 리소스 삭제로 인해 갑자기 중지하려고 시도하면 무한 상태가 발생할 수 있습니다.

## 로드 밸런서 대상

AWS 로드 밸런서는 둘 이상의 네트워크 인터페이스가 있는 인스턴스에 대해 인스턴스 유형 대상을 허용하지 않으므로 Gigabit0/1 인터페이스 IP는 대상 그룹에서 대상으로 구성됩니다. 그러나 현재 AWS Auto Scale 상태 확인은 IP가 아닌 인스턴스 유형 대상에 대해서만 작동합니다. 또한 이러한 IP는 대상 그룹에서 자동으로 추가되거나 제거되지 않습니다. 따라서 Auto Scale 솔루션은 이러한 두 작업을 모두 프로그래밍 방식으로 처리합니다. 그러나 유지 보수 또는 문제 해결의 경우에는 수동으로 수행해야 하는 상황이 있을 수 있습니다.

### 대상 그룹에 대상 등록

로드 밸런서에 FTDv 인스턴스를 등록하려면 Gigabit0/1 인스턴스 IP(외부 서브넷)를 대상 그룹의 대상으로 추가해야 합니다. [Register or Deregister Targets by IP Address](#)를 참조하십시오.

### 대상 그룹에서 대상 등록 취소

로드 밸런서에 FTDv 인스턴스를 등록 취소하려면 Gigabit0/1 인스턴스 IP(외부 서브넷)를 대상 그룹에서 삭제해야 합니다. [Register or Deregister Targets by IP Address](#)를 참조하십시오.

## 인스턴스 스탠바이

AWS는 Auto Scale 그룹에서 인스턴스 재부팅을 허용하지 않지만 사용자가 인스턴스를 스탠바이 상태로 설정하고 이러한 작업을 수행할 수 있도록 허용합니다. 그러나 이는 로드 밸런서 대상이 인스턴스 유형인 경우에 가장 적합합니다. 그러나 복수의 네트워크 인터페이스 때문에 FTDv VM은 인스턴스 유형 대상으로 구성할 수 없습니다.

### 인스턴스를 스탠바이 상태로 설정

인스턴스가 스탠바이 상태가 되면 대상 그룹의 해당 IP는 상태 프로브가 실패할 때까지 계속 동일한 상태로 유지됩니다. 따라서 인스턴스를 스탠바이 상태로 설정하기 전에 대상 그룹에서 각 IP를 등록 취소하는 것이 좋습니다. 자세한 내용은 [대상 그룹에서 대상 등록 취소, 35 페이지](#)를 참조하십시오.

IP가 제거되면 [Temporarily Removing Instances from Your Auto Scaling Group](#)을 참조하십시오.

### 스탠바이에서 인스턴스 제거

마찬가지로 인스턴스를 스탠바이 상태에서 실행 중 상태로 이동할 수 있습니다. 스탠바이 상태에서 제거한 후에는 인스턴스의 IP를 대상 그룹 대상에 등록해야 합니다. [대상 그룹에 대상 등록, 35 페이지](#)의 내용을 참조하십시오.

문제 해결 또는 유지 보수를 위해 인스턴스를 스탠바이 상태로 설정하는 방법에 대한 자세한 내용은 [AWS 뉴스 블로그](#)를 참조하십시오.

#### Auto Scale 그룹에서 인스턴스 제거/분리

Auto Scale 그룹에서 인스턴스를 제거하려면 먼저 스탠바이 상태로 이동해야 합니다. "Put Instances on Stand-by"를 참조하십시오. 인스턴스가 스탠바이 상태가 되면 제거하거나 분리할 수 있습니다. [Detach EC2 Instances from Your Auto Scaling Group](#)을 참조하십시오.

FMC 측에는 변경 사항이 없습니다. 필요한 변경은 수동으로 수행해야 합니다.

## 인스턴스 종료

인스턴스를 종료하려면 스탠바이 상태로 설정해야 합니다. [인스턴스 스탠바이, 35 페이지](#)을 참조하십시오. 인스턴스가 스탠바이 상태가 되면 종료를 진행할 수 있습니다.

## 인스턴스 축소 보호

Auto Scale 그룹에서 특정 인스턴스가 실수로 제거되는 것을 방지하기 위해 축소(scale in) 보호로 설정할 수 있습니다. 인스턴스가 축소(Scale-In) 보호 상태에 있을 경우 해당 인스턴스는 축소 이벤트로 인해 종료되지 않습니다.

인스턴스를 축소 보호 상태로 전환하려면 다음 링크를 참조하십시오.

<https://docs.aws.amazon.com/autoscaling/ec2/userguide/as-instance-termination.html>



**중요** 상태가 양호한 최소 인스턴스 수(대상 IP는 EC2 인스턴스가 아니라 정상이어야 함)를 축소 보호하는 것이 좋습니다.

## 자격 증명 및 등록 ID 변경

컨피그레이션의 변경 사항은 이미 실행 중인 인스턴스에 자동으로 반영되지 않습니다. 변경 사항은 향후 디바이스에만 반영됩니다. 이러한 변경 사항은 기존 디바이스에 수동으로 푸시해야 합니다.

#### FMC 사용자 이름 및 비밀번호 변경

FMC IP, 사용자 이름 또는 비밀번호를 변경하는 경우, 각각의 변경은 Auto Scale Manager 람다 함수 및 맞춤형 메트릭 게시자 람다 함수 환경 변수에서 수행해야 합니다. [Using AWS Lambda Environment Variables](#)을 확인하십시오.

다음 번에 람다가 실행되면 변경된 환경 변수를 참조합니다.



**참고** 환경 변수는 람다 함수에 직접 제공됩니다. 여기에는 비밀번호 복잡성 확인이 없습니다.

### FTDv 관리자 비밀번호 변경

FTDv 비밀번호를 변경하려면 사용자가 실행 중인 인스턴스에 대해 각 디바이스에서 비밀번호를 수동으로 변경해야 합니다. 새 FTDv 디바이스를 온보딩할 경우, FTDv 비밀번호는 람다 환경 변수에서 가져옵니다. [Using AWS Lambda Environment Variables](#)을 확인하십시오.

### 등록 및 NAT ID 변경

새 FTDv 디바이스를 다른 등록 및 NAT ID로 온보딩하려면 FMC 등록을 위해 이 정보를 Configuration.json 파일에서 변경해야 합니다. Configuration.json 파일은 람다 리소스 페이지에 있습니다.

## 액세스 정책 및 NAT 정책 변경

액세스 정책 또는 NAT 정책에 대한 모든 변경 사항은 디바이스 그룹 할당을 통해 향후 인스턴스에 자동으로 적용됩니다. 그러나 기존 FTDv 인스턴스를 업데이트하려면 컨피그레이션 변경 사항을 수동으로 푸시하고 FMC에서 구축해야 합니다.

## AWS 리소스 변경

Auto Post Group, Launch Configuration(컨피그레이션 시작), CloudWatch 이벤트, 확장 정책 등 AWS 사후 구축에서 여러 가지 사항을 변경할 수 있습니다. 리소스를 CloudFormation 스택으로 가져 오거나 기존 리소스에서 새 스택을 생성할 수 있습니다.

AWS 리소스에서 수행되는 변경 사항을 관리하는 방법에 대한 자세한 내용은 [Bringing Existing Resources Into CloudFormation Management](#)를 참조하십시오.

## CloudWatch 로그 수집 및 분석

CloudWatch 로그를 내보내려면 [Export Log Data to Amazon S3 Using the AWS CLI](#)를 참조하십시오.

## Auto Scale 문제 해결 및 디버깅

### AWS CloudFormation 콘솔

AWS CloudFormation 콘솔에서 CloudFormation 스택에 대한 입력 매개 변수를 확인할 수 있습니다. 그러면 웹 브라우저에서 직접 스택을 생성, 모니터링, 업데이트 및 삭제할 수 있습니다.

필요한 스택으로 이동하여 매개 변수 탭을 확인합니다. 또한 람다 함수 환경 변수 탭에서 람다 함수에 대한 입력을 확인할 수도 있습니다. `configuration.json` 파일은 Auto Scale Manager 람다 함수 자체에서도 볼 수 있습니다.

AWS CloudFormation 콘솔에 대한 자세한 내용은 [AWS CloudFormation User Guide](#)를 참조하십시오.



### Amazon Cloudwatch 로그

개별적인 램다 함수의 로그를 볼 수 있습니다. AWS 램다는 사용자를 대신하여 램다 함수를 자동으로 모니터링하며 Amazon CloudWatch를 통해 메트릭을 보고합니다. 함수에서 장애를 해결하는 데 도움이 되도록 램다 함수에서 처리한 모든 요청을 기록하고, 코드에서 생성된 로그를 Amazon CloudWatch Logs를 통해 자동으로 저장합니다.

램다 콘솔, CloudWatch 콘솔, AWS CLI 또는 CloudWatch API를 사용하여 램다에 대한 로그를 볼 수 있습니다. CloudWatch 콘솔을 통해 로그 그룹에 액세스하고 액세스하는 방법에 대한 자세한 내용은 *Amazon CloudWatch User Guide*의 모니터링 시스템, 애플리케이션 및 맞춤형 로그 파일을 참조하십시오.

### 로드 밸런서 상태 확인 실패

로드 밸런서 상태 확인에는 프로토콜, ping 포트, ping 경로, 응답 시간 초과, 상태 확인 간격 등의 정보가 포함됩니다. 상태 확인 간격 내에 200 응답 코드를 반환하는 인스턴스는 정상 상태로 간주됩니다.

일부 또는 모든 인스턴스의 현재 상태가 `OutOfService`이고 설명 필드에 인스턴스가 최소한 비정상 상태 임계 횟수 이상 실패했다는 메시지가 표시되면 인스턴스가 로드 밸런서 상태 검사에 실패한 것입니다.

FMC 컨피그레이션에서 상태 프로브 NAT 규칙을 확인해야 합니다. 자세한 내용은 [Troubleshoot a Classic Load Balancer: Health checks](#)를 참조하십시오.

### 트래픽 문제

FTDv 인스턴스의 트래픽 문제를 해결하려면 로드 밸런서 규칙, NAT 규칙 및 FTDv 인스턴스에 구성된 고정 경로를 확인해야 합니다.

또한 보안 그룹 규칙 등 구축 템플릿에 제공된 AWS 가상 네트워크 / 서브넷 / 게이트웨이 세부 정보도 확인해야 합니다. [Troubleshooting EC2 instances](#)와 같은 AWS 설명서를 참조할 수도 있습니다.

### FMC 연결에 실패함

관리 연결이 중단된 경우 FMC 컨피그레이션 및 자격 증명을 확인해야 합니다. *Firepower Management Center Configuration Guide*의 "디바이스 관리 요구 사항 및 사전 요구 사항"을 참조하십시오.

### 디바이스 등록 실패 FMC

디바이스가 FMC에 등록하지 못하면 FMC 컨피그레이션에 결함이 있는지/ 연결할 수 없는지 또는 FMC에 새 디바이스를 수용할 수 있는 용량이 있는지 확인해야 합니다. *Firepower Management Center Configuration Guide*에서 "FMC에 디바이스 추가"를 참조하십시오.

### SSH 실패 FTDv

SSH를 FTDv로 연결할 수 없는 경우 템플릿을 통해 복잡한 비밀번호가 FTDv에 전달되었는지 확인합니다.





## 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 기능 이전 버전의 소프트웨어를 사용할 경우에는 해당 버전에 대한 FMC 설정 가이드의 절차를 참조하십시오.

- [Firepower Management Center를 이용한 Firepower Threat Defense Virtual 관련 정보, 39 페이지](#)
- [Firepower Management Center에 로그인, 40 페이지](#)
- [Firepower Management Center로 디바이스 등록, 40 페이지](#)
- [기본 보안 정책 구성, 42 페이지](#)
- [Firepower Threat Defense CLI 액세스, 54 페이지](#)

## 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 가이드](#)를 참조하십시오.

FTDv은 FTDv 가상 머신에 할당된 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

FMC를 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 참조](#)를 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.

**Add Device** ? X

Host:†

Display Name:

Registration Key:™

Group:  ▼

Access Control Policy:™  ▼

**Smart Licensing**

Malware

Threat

URL Filtering

**Advanced**

Unique NAT ID:†

Transfer Packets

- **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, 52 페이지](#)를 참조하십시오.

**New Policy** ? X

Name:

Description:

Select Base Policy:  ▼

Default Action:  Block all traffic  Intrusion Prevention  Network Discovery

- **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, 54 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

- 단계 1 인터페이스 구성, 43 페이지
- 단계 2 DHCP 서버 구성, 46 페이지
- 단계 3 기본 경로 추가, 47 페이지
- 단계 4 NAT 구성, 49 페이지
- 단계 5 액세스 제어 구성, 52 페이지
- 단계 6 구성 구축, 53 페이지

## 인터페이스 구성

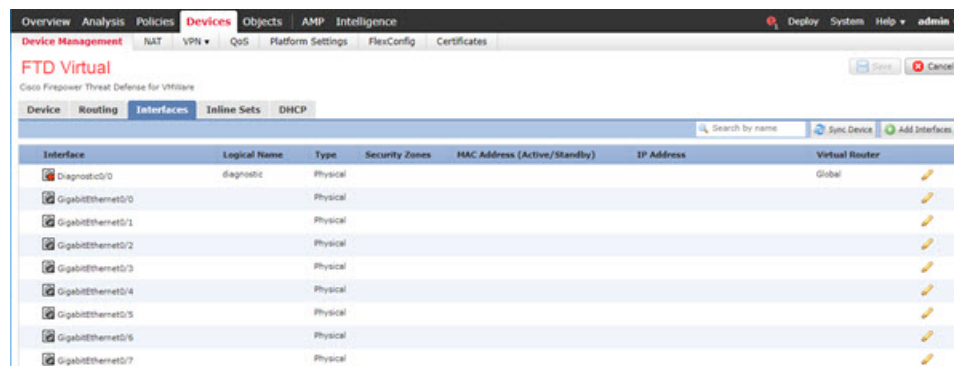
FTDv 인터페이스를 활성화하고, 보안 영역에 이를 할당하며, IP 주소를 설정합니다. 일반적으로 시스템이 의미 있는 트래픽을 전달하도록 최소 2개 이상의 인터페이스를 구성해야 합니다. 일반적으로 업스트림 라우터 또는 인터넷과 만나는 외부 인터페이스와 조직 네트워크에서 사용하는 하나 이상의 내부 인터페이스를 사용합니다. 이런 인터페이스의 일부는 웹 서버와 같이 공개적으로 액세스할 수 있는 에셋을 배치하는 '비무장지대(DMZ)'로 사용하게 됩니다.

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(✎)을 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 외부로 이동하지만 외부에서 내부로 이동할 수 없도록 액세스 제어 정책을 구성할 수 있습니다. 대부분의 정책은 보안 영역만 지원됩니다. 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.

The screenshot shows the 'Edit Physical Interface' dialog box with the 'IPv4' tab selected. The 'IP Type' dropdown is set to 'Use DHCP'. Below it, the checkbox 'Obtain default route using DHCP' is checked. The 'DHCP route metric' is set to '1' in a text input field, with a range '(1 - 255)' indicated to the right.

- **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 뛴니다.

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.

The screenshot shows the 'Add Server' dialog box. The 'Interface\*' dropdown is set to 'inside'. The 'Address Pool\*' text box contains '10.9.7.9-10.9.7.25' and '(2.2.2.10-2.2.2.20)' is shown to the right. The 'Enable DHCP Server' checkbox is checked. At the bottom, there are 'OK' and 'Cancel' buttons.



- 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.

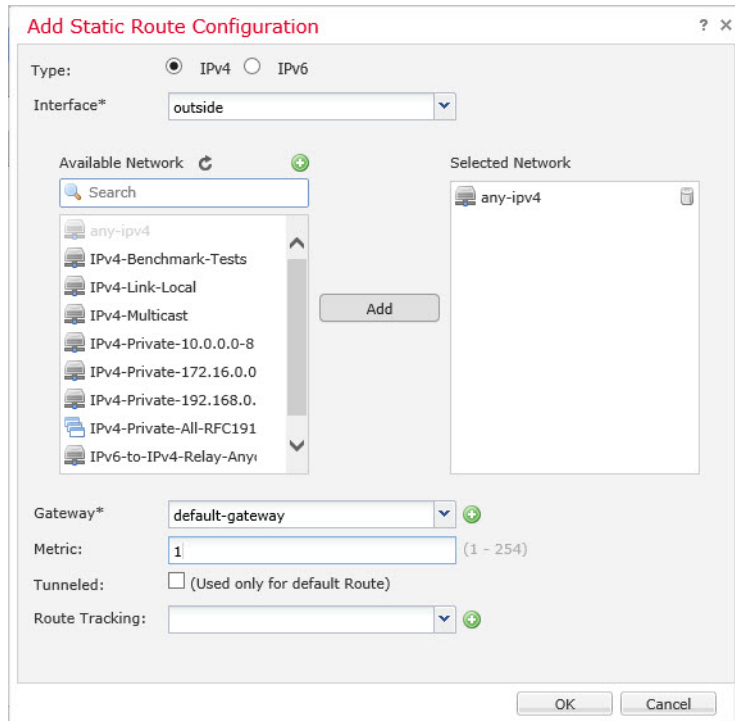
## 기본 경로 추가

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.

10.99.10.20

Device Management NAT VPN QoS Platform Settings FlexConfig Certificates

Overview Analysis Policies **Devices** Objects AMP Intelligence

Deploy System Help admin

Device Routing Interfaces Inline Sets DHCP

OSPF  
OSPFv3  
RIP  
BGP  
**Static Route**  
Multicast Routing

Network	Interface	Gateway	Tunneled	Metric	Tracked
▼ IPv4 Routes					
any-ipv4	outside	10.99.10.1	false	1	
▼ IPv6 Routes					

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.

New Policy

Name: interface\_PAT

Description:

Targeted Devices

Select devices to which you want to apply this policy

Available Devices

Search by name or value

192.168.0.16

Add to Policy

Selected Devices

192.168.0.16

Save Cancel

정책이 FMC를 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.

#	Direction	Type	Source Interface Objects	Destination Interface Objects	Original Sources	Original Destinations	Original Services	Translated Sources	Translated Destinations	Translated Services	Options
▼ NAT Rules Before											
▼ Auto NAT Rules											
#	→	Dynamic	any	outside_zone	all-ipv4			Interface			Dns:false
▼ NAT Rules After											

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

## 액세스 제어 구성

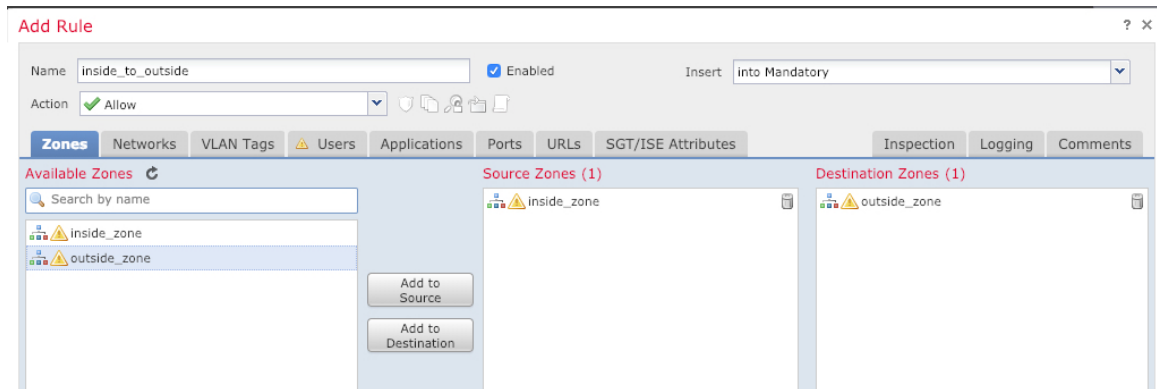
FMC를 사용해 FTDv를 등록할 때 기본 액세스 컨트롤 정책인 **Block all traffic**(모든 트래픽 차단)을 생성했다면, 디바이스에 트래픽을 허용하기 위해 정책에 규칙을 추가해야 합니다. 다음 절차에서는 내부 영역에서 외부 영역으로 향하는 트래픽을 허용하는 규칙을 추가합니다. 다른 영역이 있는 경우에는 적절한 네트워크에 대한 트래픽을 허용하는 규칙을 추가해야 합니다.

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.

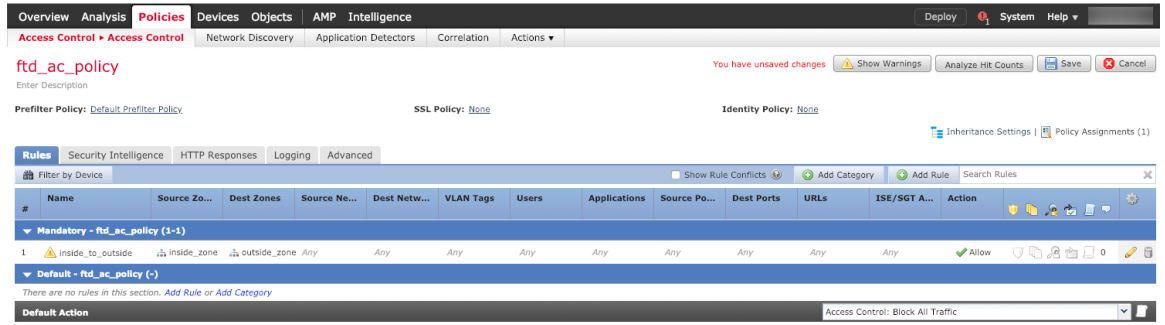


- **Name** (이름) - 예를 들어 이 규칙의 이름을 **inside\_to\_outside**로 지정합니다.
- **Source Zones**(원본 영역) - **Available Zones**(사용 가능한 영역)에서 내부 영역을 선택하고 **Add to Source**(원본에 추가)를 클릭합니다.
- **Destination Zones**(대상 영역) - **Available Zones**(사용 가능한 영역)에서 외부 영역을 선택하고 **Add to Destination**(대상에 추가)를 클릭합니다.

기타 설정은 변경하지 않습니다.

단계 3 **Add**(추가)를 클릭합니다.

규칙이 **Rules**(규칙) 테이블에 추가됩니다.



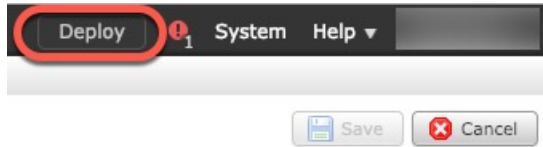
단계 4 **Save(저장)**를 클릭합니다.

## 구성 구축

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

프로시저

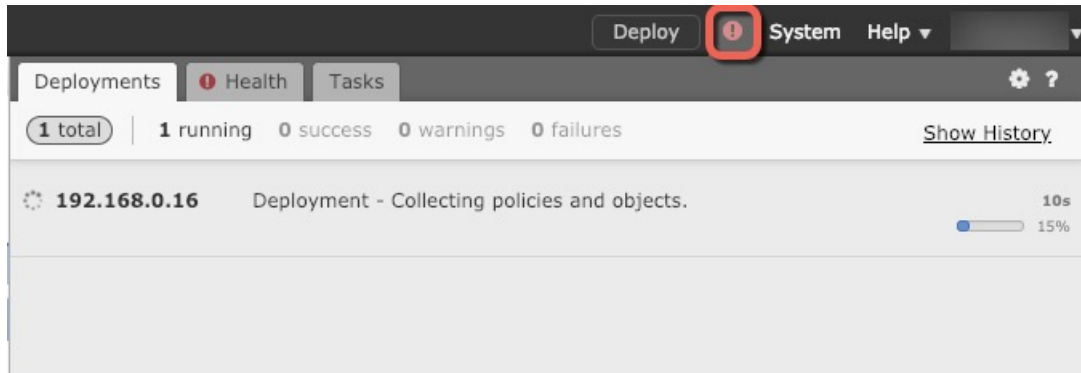
단계 1 우측 상단에서 **Deploy(구축)**를 클릭합니다.



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.





## 5 장

# Firepower Device Manager를 이용한 Firepower Threat Defense Virtual 관리

이 장에서는 FDM로 관리되는 독립형 FTDv 디바이스를 구축하는 방법을 설명합니다. 고가용성 쌍을 구축하려면 FDM 설정 가이드를 참조하십시오.

- [Firepower Device Manager를 이용하는 Firepower Threat Defense Virtual 관련 정보, 55 페이지](#)
- [초기 구성, 56 페이지](#)
- [Firepower Device Manager에서 디바이스를 구성하는 방법, 58 페이지](#)

## Firepower Device Manager를 이용하는 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.

일부 Firepower Threat Defense 모델이 포함된 웹 기반 디바이스 설정 마법사인 Firepower Device Manager(FDM)을(를) 사용해 FTDv을(를) 관리할 수 있습니다. FDM은(는) 소규모 네트워크에서 가장 흔히 사용되는 소프트웨어의 기본 기능을 구성하도록 합니다. Firepower Device Manager는 디바이스를 하나 또는 몇 개만 포함하는 네트워크 용도로 특별히 설계되어 고성능 다중 디바이스 관리자를 사용해 여러 Firepower Threat Defense 디바이스가 포함된 대규모 네트워크를 제어하기를 원하지 않을 경우에 유용합니다.

다수의 디바이스를 관리하거나 Firepower Threat Defense에서 허용하는 더 복잡한 기능 및 구성을 사용하려는 경우에는 통합형 Firepower Device Manager 대신 Firepower Management Center을(를) 사용하여 디바이스를 구성하십시오. 자세한 내용은 [Firepower Management Center로 Firepower Threat Defense Virtual 관리, 39 페이지](#)를 참조하십시오.

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

## 기본 구성

FTDv 기본 컨피그레이션에서는 관리 인터페이스와 내부 인터페이스를 동일한 서브넷에 배치합니다. 스마트 라이선싱을 사용하고 시스템 데이터베이스로 업데이트를 가져오려면 관리 인터페이스에서 인터넷에 연결할 수 있어야 합니다.

따라서 기본 컨피그레이션은 가상 스위치의 동일한 네트워크에 Management0-0 및 GigabitEthernet0-1(내부)을 둘 다 연결할 수 있도록 설계되어 있습니다. 기본 관리 주소는 내부 IP 주소를 게이트웨이로 사용합니다. 그러므로 관리 인터페이스는 인터넷에 연결하기 위해 내부 인터페이스와 외부 인터페이스를 차례로 통과하여 라우팅합니다.

인터넷에 액세스할 수 있는 네트워크를 사용한다면 내부 인터페이스에 사용하는 것과는 다른 서브넷에 Management0-0을 연결할 수도 있습니다. 이 경우 네트워크용으로 관리 인터페이스 IP 주소 및 게이트웨이를 적절하게 구성해야 합니다.

FTDv은(는) 전원이 공급되는 첫 부팅 시 최소 4개의 인터페이스를 사용해야 합니다.

- 가상 머신의 첫 번째 인터페이스는 관리 인터페이스(Management0-0)입니다.
- 가상 머신의 두 번째 인터페이스는 진단 인터페이스(Diagnostic0-0)입니다.
- 가상 머신의 세 번째 인터페이스(GigabitEthernet0-0)는 외부 인터페이스입니다.
- 가상 머신의 네 번째 인터페이스(GigabitEthernet0-1)는 내부 인터페이스입니다.

데이터 트래픽의 경우 최대 6개 이상의 인터페이스를 추가하여 총 8개의 데이터 인터페이스를 사용할 수 있습니다. 추가 데이터 인터페이스의 경우 소스 네트워크가 올바른 대상 네트워크에 매핑되는지, 또한 각 데이터 인터페이스가 고유한 서브넷 또는 VLAN에 매핑되는지 확인합니다. VMware 인터페이스 구성을 참조하십시오.

## 초기 구성

네트워크에 보안 어플라이언스를 삽입하고 인터넷 또는 기타 업스트림 라우터에 연결하는 데 필요한 주소 구성을 포함한 FTDv 기능이 네트워크에서 올바르게 작동하는 초기 구성을 완료해야 합니다. 다음 두 가지 방법 중 하나로 시스템의 초기 구성을 수행할 수 있습니다.

- FDM 웹 인터페이스(권장)를 사용합니다. FDM는 웹 브라우저에서 실행됩니다. 이 인터페이스를 사용하여 시스템을 구성, 관리 및 모니터링합니다.
- CLI(명령줄 인터페이스) 설정 마법사를 사용합니다(선택). 초기 구성에 FDM 대신 CLI 설정 마법사를 사용할 수 있으며, 문제 해결에도 CLI를 사용할 수 있습니다. FDM을(를) 사용해 여전히 시스템을 구성, 관리, 모니터링할 수 있습니다. (선택 사항) Firepower Threat Defense CLI 마법사 시작을 참조하십시오.

다음 주제에서는 이런 인터페이스를 사용해 시스템의 초기 구성을 수행하는 방법을 설명합니다.

## Firepower Device Manager 실행

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

아래 브라우저의 최신 버전인 Firefox, Chrome, Safari, Edge를 사용하십시오.



- 참고** 초기 구축 중에 사용자 데이터(**Advanced Details**(고급 세부 정보) > **User Data**(사용자 데이터))로 기본 비밀번호를 정의하지 않는 한 기본 관리자 비밀번호는 AWS 인스턴스 ID입니다.
- 잘못된 비밀번호를 입력하고 3회 연속하여 로그인 시도에 실패할 경우, 5분 동안 어카운트가 잠깁니다. 따라서 다시 로그인을 시도하기 전에 잠시 기다려야 합니다.

### 프로시저

- 단계 1** 브라우저를 사용하여 FDM에 로그인합니다. CLI에서 초기 컨피그레이션을 수행하지 않았다고 가정하겠습니다. <https://ip-address>에서 Firepower Device Manager를 엽니다. 여기서 주소는 다음 중 하나입니다.
- 관리 주소. 기본적으로 대부분의 플랫폼에서 관리 인터페이스는 DHCP 클라이언트이므로 IP 주소는 DHCP 서버에 따라 달라집니다.
  - FTDv가 Microsoft Azure 또는 Amazon Web Services와 같은 공용 클라우드 환경에 구축된 경우 공용 주소 풀에서 FTDv 인스턴스에 주소가 지정된 공용 IP가 자동으로 할당됩니다. 클라우드 대시보드에서 공용 IP 주소를 찾습니다.
- 단계 2** 사용자 이름 **admin** 및 기본 비밀번호로 로그인합니다.
- 버전 7.0 이상에서 초기 구축 중에 사용자 데이터(**Advanced Details**(고급 세부 정보) > **User Data**(사용자 데이터))로 기본 비밀번호를 정의하지 않는 한 기본 관리자 비밀번호는 AWS 인스턴스 ID입니다.
- 이전 릴리스에서 기본 관리자 비밀번호는 **Admin123**입니다.
- 단계 3** 시스템에 처음으로 로그인하며 CLI 설정 마법사를 사용하지 않은 경우에는 엔드 유저 라이선스 계약을 확인 및 동의하고 관리자 비밀번호를 변경하라는 메시지가 표시됩니다. 계속하려면 이러한 단계를 완료해야 합니다.
- 단계 4** 외부 및 관리 인터페이스에 대해 다음 옵션을 구성하고 **Next**(다음)를 클릭합니다.
- 참고** **Next**(다음)를 클릭하면 설정이 디바이스에 구축됩니다. 인터페이스는 이름이 "외부"로 지정되어 "outside\_zone" 보안 영역에 추가됩니다. 설정이 올바른지 확인합니다.
- a) **Outside Interface**(외부 인터페이스) - 게이트웨이 모드 또는 라우터에 연결한 데이터 포트입니다. 초기 디바이스 설정 중에는 대체 외부 인터페이스를 선택할 수 없습니다. 첫 번째 데이터 인터페이스가 기본 외부 인터페이스입니다.

**IPv4 구성** - 외부 인터페이스의 IPv4 주소를 구성합니다. DHCP를 사용하거나 수동으로 고정 IP 주소, 서브넷 마스크 및 게이트웨이를 입력할 수 있습니다. **끄기**를 선택하여 IPv4 주소를 구성하지 않을 수도 있습니다.

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

b) 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(OpenDNS 사용)**를 클릭하여 적절한 IP 주소를 필드에 다시 로드합니다.

**방화벽 호스트 이름** - 시스템 관리 주소용 호스트 이름을 지정합니다.

**참고** 디바이스 설정 마법사를 사용해 Firepower Threat Defense 디바이스를 구성할 때 시스템은 아웃바운드 및 인바운드 트래픽에 대해 두 가지 기본 액세스 규칙을 제공합니다. 초기 설정 후에 다시 돌아가 이 액세스 규칙을 편집할 수 있습니다.

**단계 5** 시스템 시간 설정을 구성하고 **Next(다음)**를 클릭합니다.

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

**단계 6** 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 **90일** 평가 기간 시작을 선택합니다. 나중에 디바이스를 등록하고 스마트 라이선스를 가져오려면 메뉴의 디바이스 이름을 클릭한 다음 **Device Dashboard(디바이스 대시보드)**로 이동해 **Smart Licenses(스마트 라이선스)** 그룹에서 링크를 클릭합니다.

**단계 7** **Finish(마침)**를 클릭합니다.

다음에 수행할 작업

- Firepower Device Manager에서 디바이스를 구성하려면 [Firepower Device Manager에서 디바이스를 구성하는 방법, 58 페이지](#)를 참조하십시오.

## Firepower Device Manager에서 디바이스를 구성하는 방법

설치 마법사를 완료하고 나면 작동 중인 디바이스에 몇 가지 기본 정책이 갖추어져 있어야 합니다.

- 내부 및 외부 인터페이스용 보안 영역
- 내부에서 외부로 이동하는 모든 트래픽을 신뢰하는 액세스 규칙
- 내부에서 외부로 이동하는 모든 트래픽을 외부 인터페이스의 IP 주소에 있는 고유한 포트로 변환하는 인터페이스 NAT 규칙입니다.
- 내부 인터페이스 또는 브리지 그룹에서 실행 중인 DHCP 서버

다음 단계에서는 구성하려는 추가적인 기능에 대한 개요가 제공됩니다. 각 단계에 대한 자세한 내용을 보려면 페이지에서 도움말 버튼(?)을 클릭하십시오.

프로시저

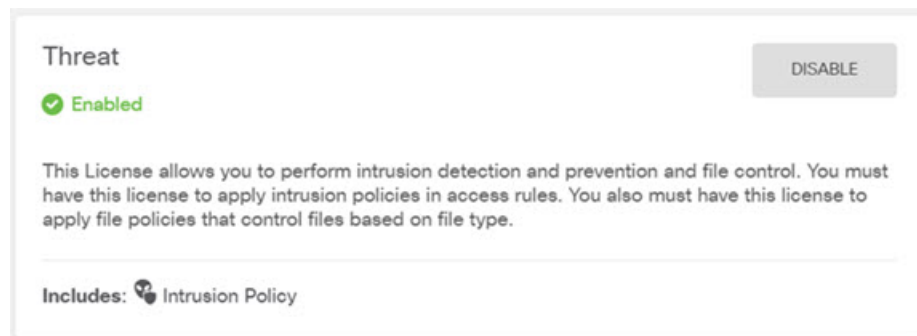
**단계 1 Device(디바이스)를 선택한 다음 Smart License(스마트 라이선스) 그룹에서 View Configuration(컨피그레이션 보기)를 클릭합니다.**

사용할 각 라이선스 옵션(Threat(위협), Malware(악성코드), URL)에 대해 **Enable(활성화)**를 클릭합니다. 설치 시 디바이스를 등록한 경우, 원하는 RA VPN 라이선스를 활성화할 수도 있습니다. 필요 여부가 확실하지 않은 경우 각 라이선스에 대한 설명을 읽어보십시오.

등록하지 않은 경우에는 이 페이지에서 등록할 수 있습니다. **Request Register(등록 요청)**를 클릭하고 지침을 따릅니다. 평가 라이선스가 만료되기 전에 등록하십시오.

예를 들어, 활성화된 위협 라이선스는 다음과 같이 표시됩니다.

그림 2: 활성화된 위협 라이선스



**단계 2** 다른 인터페이스를 구성한 경우 **Device(디바이스)를 선택하고 Interfaces(인터페이스) 그룹에서 View Configuration(컨피그레이션 보기)를 클릭한 뒤 각 인터페이스를 구성합니다.**

다른 인터페이스용 브리지 그룹을 생성하거나, 별도의 네트워크를 구성하거나 이 두 방법을 조합해 사용할 수 있습니다. 각 인터페이스의 편집 아이콘(🔗)을 클릭하여 IP 주소 및 기타 설정을 정의합니다.

다음 예에서는 인터페이스를 웹 서버와 같이 공개적으로 액세스할 수 있는 자산을 배치하는 DMZ("Demilitarized Zone(비무장지대)")로 사용되도록 구성합니다. 완료되면 **Save(저장)**를 클릭합니다.

그림 3: 인터페이스 수정

**Edit Physical Interface**

Interface Name:  Status:

Description:

IPv4 Address | IPv6 Address | Advanced Options

Type:

IP Address and Subnet Mask:  /

e.g. 192.168.5.15/17 or 192.168.5.15/255.255.128.0

단계 3 새로운 인터페이스를 구성한 경우 목차에서 **Objects(개체)**를 선택한 다음 **Security Zones(보안 영역)**를 선택합니다.

새로운 영역을 적절히 편집하거나 생성합니다. 정책은 인터페이스가 아니라 보안 영역을 기반으로 구성하기 때문에 각 인터페이스는 하나의 영역에 속해 있어야 합니다. 인터페이스를 구성할 때는 영역에 인터페이스를 배치할 수 없으므로 새 인터페이스를 생성하거나 기존 인터페이스의 용도를 변경한 후에는 항상 영역 개체를 편집해야 합니다.

다음 예에는 dmz 인터페이스에서 새 dmz-zone을 생성하는 방법이 나와 있습니다.

그림 4: 보안 영역 개체

단계 4 내부 클라이언트가 DHCP를 사용해 디바이스에서 IP 주소를 가져오도록 하려면 **Device**(디바이스) > **System Settings**(시스템 설정) > **DHCP Server**(DHCP 서버)을 선택하고 **DHCP Servers**(DHCP 서버) 탭을 선택합니다.

내부 인터페이스에 이미 DHCP 서버가 구성되어 있지만 주소 풀을 편집하거나 삭제할 수도 있습니다. 다른 내부 인터페이스를 구성한 경우, 이러한 인터페이스에서 DHCP 서버를 설정하는 것은 매우 일반적입니다. +를 클릭하여 각 내부 인터페이스에 서버 및 주소 풀을 구성합니다.

또한 **Configuration**(컨피그레이션) 탭에서 클라이언트에게 제공된 WINS 및 DNS 목록을 조정할 수 있습니다. 다음 예에는 주소 풀이 192.168.4.50-192.168.4.240인 inside2 인터페이스에서 DHCP 서버를 설정하는 방법이 나와 있습니다.

그림 5: DHCP 서버

단계 5 **Device**(디바이스)를 선택한 후 **Routing**(라우팅) 그룹에서 **View Configuration**(컨피그레이션 보기)(또는 **Create First Static Route**(첫 번째 정적 경로 생성))을 클릭하고 기본 경로를 컨피그레이션합니다.

기본 경로는 일반적으로 외부 인터페이스 외에 있는 업스트림 또는 ISP 라우터를 가리킵니다. 기본 IPv4 경로는 any-ipv4(0.0.0.0/0)용인 반면, 기본 IPv6 경로는 any-ipv6(::0/0)용입니다. 사용하는 각 IP 버전에 대해 경로를 생성합니다. DHCP를 사용하여 외부 인터페이스에 대한 주소를 얻으려는 경우, 필요한 기본 경로가 이미 있을 수도 있습니다.

참고 이 페이지에서 정의하는 경로는 데이터 인터페이스 전용입니다. 이러한 경로는 관리 인터페이스에 영향을 주지 않습니다. **Device**(디바이스) > **System Settings**(시스템 설정) > **Management Interface**(관리 인터페이스)에서 관리 게이트웨이를 설정합니다.

다음 예에는 IPv4의 기본 경로가 나와 있습니다. 이 예에서 isp-gateway는 ISP 게이트웨이의 IP 주소 (ISP에서 주소를 획득해야 함)를 식별하는 네트워크 개체입니다. 이 개체는 **Gateway**(게이트웨이) 그룹다운 목록의 아래쪽에서 **Create New Network**(새 네트워크 생성)를 클릭하여 생성할 수 있습니다.

그림 6: 기본 라우터

The screenshot shows the 'Add Static Route' configuration interface. It includes the following fields and options:

- Protocol:** Radio buttons for IPv4 (selected) and IPv6.
- Gateway:** A text input field containing 'isp-gateway'.
- Interface:** A text input field containing 'outside'.
- Metric:** A text input field containing '1'.
- Networks:** A section with a '+' button and a list containing 'any-ipv4'.

단계 6 **Policies**(정책)를 선택하고 네트워크의 보안 정책을 구성합니다.

디바이스 설치 마법사를 사용하면 외부 인터페이스로 이동할 때 모든 인터페이스에 대한 inside-zone, outside-zone 및 인터페이스 NAT 간의 트래픽 플로우가 가능합니다. 새 인터페이스를 구성하는 경우에도 inside-zone 개체에 이러한 인터페이스를 추가하면 이러한 인터페이스에 액세스 제어 규칙이 자동으로 적용됩니다.

그러나 내부 인터페이스가 여러 개 있는 경우, inside-zone 간의 트래픽 플로우를 허용하기 위해 액세스 제어 규칙이 필요합니다. 다른 보안 영역을 추가하는 경우, 이러한 영역을 오고 가는 트래픽을 허용하는 규칙이 필요합니다. 이렇게 해야 변경 사항이 가장 적습니다.

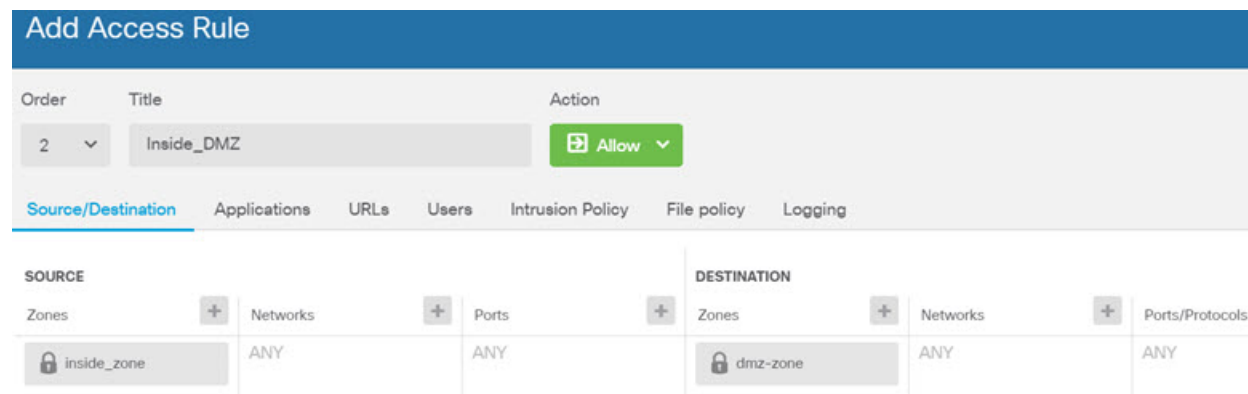
또한, 다른 정책을 구성하여 추가 서비스를 제공할 수 있으며 NAT 및 액세스 규칙을 조정하여 조직에 필요한 결과를 얻을 수 있습니다. 다음과 같은 정책을 구성할 수 있습니다.



- **SSL Decryption(SSL 암호 해독)** — 침입, 악성코드 등에 대한 암호화된 연결(예: HTTPS)을 검사하려는 경우, 연결을 암호 해독해야 합니다. SSL 암호 해독 정책을 사용하여 어떤 연결을 암호 해독해야 할지 확인합니다. 시스템은 검사를 수행한 후에 연결을 다시 암호화합니다.
- **Identity(ID)** — 네트워크 활동과 개인 사용자의 상관관계를 분석하거나 사용자 또는 사용자 그룹 멤버십을 기반으로 네트워크 액세스를 제어하려면 ID 정책을 사용하여 지정된 소스 IP 주소와 연결된 사용자를 확인합니다.
- **Security Intelligence(보안 인텔리전스)** — 보안 인텔리전스 정책을 사용하여 블랙리스트에 추가된 IP 주소 또는 URL을 오가는 연결을 신속하게 삭제합니다. 알려진 유해 사이트를 블랙리스트에 추가함으로써 해당 사이트를 액세스 제어 정책에서 고려할 필요가 없습니다. Cisco는 알려진 유해 주소 및 URL에 대해 정기적으로 업데이트된 피드를 제공하므로 보안 인텔리전스 블랙리스트가 동적으로 업데이트됩니다. 피드를 사용하는 경우에는 블랙리스트에서 항목을 추가하거나 제거하기 위해 정책을 편집할 필요가 없습니다.
- **NAT(Network Address Translation)** - NAT 정책을 사용하여 내부 IP 주소를 외부에서 라우팅 가능한 주소로 변환합니다.
- **Access Control(액세스 제어)** — 액세스 제어 정책을 사용하여 네트워크에서 어떤 연결이 허용되는지 확인합니다. 보안 영역, IP 주소, 프로토콜, 포트, 애플리케이션, URL, 사용자 또는 사용자 그룹을 기준으로 필터링할 수 있습니다. 액세스 제어 규칙을 사용하여 침입 및 파일(악성코드) 정책을 적용할 수도 있습니다. 이 정책을 사용하여 URL 필터링을 구현할 수 있습니다.
- **Intrusion(침입)** — 침입 정책을 사용하여 알려진 위협을 검사합니다. 액세스 제어 규칙을 사용하여 침입 정책을 적용하는 경우에도 침입 정책을 편집하여 특정 침입 규칙을 선택적으로 활성화 또는 비활성화할 수 있습니다.


다음 예에는 액세스 제어 정책에서 inside-zone 및 dmz-zone 간의 트래픽을 허용하는 방법이 나와 있습니다. 이 예에서는 **Logging(로깅)(At End of Connection(연결 종료 시))**이 선택된 경우)을 제외하고는 다른 어떤 탭에도 옵션이 설정되어 있지 않습니다.

그림 7: 액세스 제어 정책



단계 7 **Device(디바이스)**를 선택한 다음 **Updates(업데이트)** 그룹에서 **View Configuration(구성 보기)**를 클릭하고 시스템 데이터베이스에 대한 업데이트 일정을 구성합니다.

침입 정책을 사용하는 경우 규칙 및 VDB 데이터베이스에 대한 정기 업데이트를 설정합니다. 보안 인텔리전스 피드를 사용하는 경우 피드의 업데이트 일정을 설정합니다. 모든 보안 정책의 일치 기준으로 지리적 위치를 사용하는 경우 해당 데이터베이스에 대한 업데이트 일정을 설정합니다.

단계 8 메뉴에서 **Deploy**(구축) 버튼을 클릭한 다음 지금 구축 버튼()을 클릭하여 디바이스에 변경 사항을 구축합니다.

변경 사항은 구축할 때까지 디바이스에서 활성화되지 않습니다.

---

다음에 수행할 작업

Firepower Device Manager로 Firepower Threat Defense Virtual을 관리하는 방법에 대한 자세한 내용은 [Firepower Device Manager용 Cisco Firepower Threat Defense 구성 가이드](#) 또는 Firepower Device Manager 온라인 도움말을 참조하십시오.



