



OpenStack용 Cisco Secure Firewall Threat Defense Virtual 시작 가이드

초판: 2021년 5월 28일

최종 변경: 2022년 5월 31일

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

Secure Firewall Threat Defense Virtual 및 OpenStack으로 시작하기

OpenStack 환경의 컴퓨팅 노드에서 실행 중인 KVM(Kernel-based Virtual Machine) 하이퍼바이저에 Secure Firewall Threat Defense Virtual(이전 Firepower Threat Defense Virtual)을 구축할 수 있습니다.

- [OpenStack에서의 Threat Defense Virtual 구축 정보, 1 페이지](#)
- [End-to-End Procedure, on page 2](#)
- [Prerequisites for the Threat Defense Virtual and OpenStack, on page 2](#)
- [Threat Defense Virtual 및 OpenStack에 대한 지침 및 제한 사항, 3 페이지](#)
- [구축을 위한 OpenStack 요구 사항, 5 페이지](#)
- [OpenStack의 Threat Defense Virtual에 대한 네트워크 토폴로지 예, 6 페이지](#)

OpenStack에서의 Threat Defense Virtual 구축 정보

이 가이드에서는 OpenStack 환경에서 threat defense virtual을 구축하는 방법을 설명합니다. OpenStack은 무료 개방형 표준 클라우드 컴퓨팅 플랫폼으로, 가상 서버 및 기타 리소스가 사용자에게 제공되는 퍼블릭 및 프라이빗 클라우드 모두에서 대부분 IaaS(infrastructure-as-a-service)로 구축됩니다.

이 구축에서는 KVM 하이퍼바이저를 사용하여 가상 리소스를 관리합니다. KVM은 가상화 확장 프로그램(예: Intel VT)이 포함된 x86 하드웨어의 Linux용 전체 가상화 솔루션입니다. KVM은 로드 가능한 커널 모듈인 kvm.ko로 구성되어 있으며, 코어 가상화 인프라 및 kvm-intel.ko와 같은 프로세서별 모듈을 제공합니다.

KVM을 사용하여 수정되지 않은 OS 이미지를 실행하는 여러 가상 머신을 실행할 수 있습니다. 각 가상 머신에는 네트워크 카드, 디스크, 그래픽 어댑터 등의 개인 가상화 하드웨어가 있습니다.

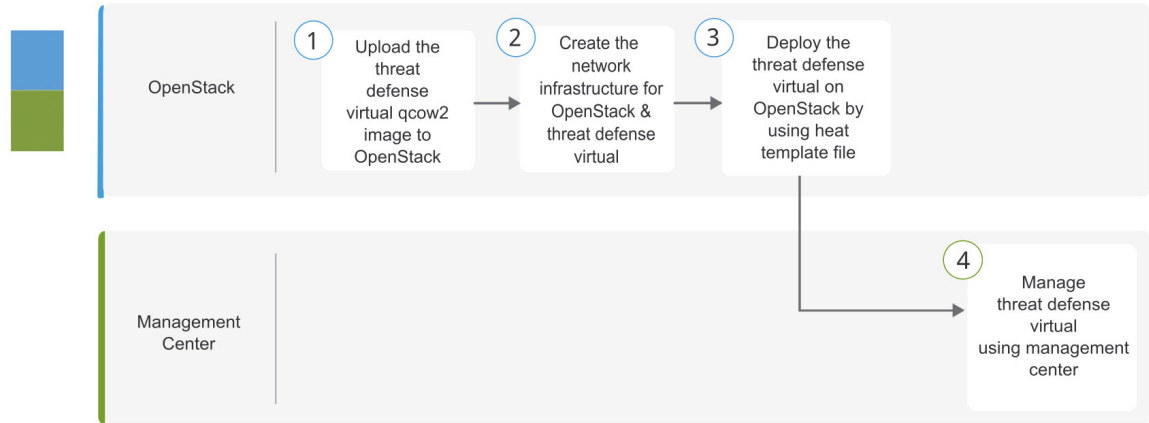
디바이스는 KVM 하이퍼바이저에서 이미 지원되므로 OpenStack 지원을 활성화하는 데 추가 커널 패키지 또는 드라이버가 필요하지 않습니다.



참고 OpenStack의 Threat Defense Virtual은 모든 최적화된 다중 노드 환경에 설치할 수 있습니다.

End-to-End Procedure

The following flowchart illustrates the workflow for deploying threat defense Virtual on OpenStack.



	Workspace	Steps
①	OpenStack	OpenStack에 Threat Defense Virtual 이미지 업로드: Upload the threat defense virtual image to OpenStack.
②	OpenStack	OpenStack 및 Threat Defense Virtual의 네트워크 인프라 생성: Create the network infrastructure for OpenStack and threat defense virtual.
③	OpenStack	OpenStack에 Threat Defense Virtual 구축: Deploy the threat defense virtual on OpenStack by using threat defense virtual heat template file.
④	Management Center	Manage threat defense Virtual: <ul style="list-style-type: none"> • Using Management Center

Prerequisites for the Threat Defense Virtual and OpenStack

- Get the qcow2 threat defense virtual image from software.cisco.com.
- Threat Defense Virtual supports deployment on opensource OpenStack environment and Cisco VIM managed OpenStack environment.

Set up the OpenStack environment according to the OpenStack guidelines.

- See the opensource OpenStack document:

Stein Release - <https://docs.openstack.org/project-deploy-guide/openstack-ansible/stein/overview.html>

Queens Release - <https://docs.openstack.org/project-deploy-guide/openstack-ansible/queens/overview.html>

- See the Cisco Virtualized Infrastructure Manager (VIM) OpenStack document: [Cisco Virtualized Infrastructure Manager Documentation, 3.4.3 to 3.4.5](#)
- A Cisco Smart Account. You can create one at [Cisco Software Central](#).
- License the threat defense virtual.
 - Configure all license entitlements for the security services from the management center.
 - See “Licensing” in the *Secure Firewall Management Center Admin Guide* for more information about how to manage licenses.
- Interface requirements:
 - Management interfaces (2) — One used to connect the threat defense virtual to the management center, second used for diagnostics; cannot be used for through traffic.
 - Inside and outside interfaces — Used to connect the threat defense virtual to inside hosts and to the public network.
- Communications paths:
 - Floating IPs for access into the threat defense virtual.
- Minimum supported the threat defense virtual version:
 - Version 7.0
- For OpenStack requirements, see [구축을 위한 OpenStack 요구 사항, on page 5](#).
- For threat defense virtual system requirements, see [Cisco Firepower Compatibility](#).

Threat Defense Virtual 및 OpenStack에 대한 지침 및 제한 사항

지원 기능

OpenStack의 threat defense virtual는 다음 기능을 지원합니다.

- OpenStack 환경의 컴퓨팅 노드에서 실행 중인 KVM 하이퍼바이저의 threat defense virtual 구축.
- OpenStack CLI
- Heat 템플릿 기반 구축
- OpenStack Horizon 대시보드
- 라우팅 모드(기본값)
- 라이선싱 - BYOL만 지원됩니다.

- management center를 사용해 Threat Defense Virtual 관리
- 드라이버 - virtIO, VPP 및 SR-IOV

Threat Defense Virtual 스마트 라이선싱의 성능 계층

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

표 1: 자격 기준 **Threat Defense Virtual** 라이선스 기능 제한

성능 계층	디바이스 사양 (Core/RAM)	속도 제한	RA VPN 세션 제한
FTDv5	4 코어/8GB	100Mbps	50
FTDv10	4 코어/8GB	1Gbps	250
FTDv20	4 코어/8GB	3Gbps	250
FTDv30	8 코어/16GB	5Gbps	250
FTDv50	12 코어/24GB	10Gbps	750
FTDv100	16 코어/32GB	16Gbps	10,000

threat defense virtual 디바이스 라이선싱에 대한 지침은 *Secure Firewall Management Center* 관리자 가이드의 "라이선싱" 장을 참조하십시오.

성능 최적화

threat defense virtual에서 최상의 성능을 얻으려면 VM과 호스트를 모두 조정할 수 있습니다. 자세한 내용은 [OpenStack의 가상화 조정 및 최적화](#)를 참조하십시오.

Receive Side Scaling— threat defense virtual은 RSS(Receive Side Scaling)를 지원합니다. RSS는 네트워크 수신 트래픽을 여러 프로세서 코어로 분산하기 위해 네트워크 어댑터에서 활용하는 기술입니다. 버전 7.0 이상에서 지원됩니다. 자세한 내용은 [RSS\(Receive Side Scaling\)를 위한 다중 RX 대기열](#)을 참조하십시오.

Snort

- Snort를 종료하는 데 시간이 오래 걸리거나, VM이 일반적으로 느려지거나, 특정 프로세스가 실행되는 등의 비정상적인 동작이 관찰되는 경우 threat defense virtual 및 VM 호스트에서 로그를 수집합니다. 전체 CPU 사용량, 메모리, I/O 사용량 및 읽기/쓰기 속도 로그를 수집하면 문제를 해결하는 데 도움이 됩니다.
- Snort가 종료될 때 높은 CPU 및 I/O 사용량이 관찰됩니다. 메모리가 충분하지 않고 전용 CPU가 없는 단일 호스트에서 여러 threat defense virtual 인스턴스가 생성된 경우 Snort가 종료되는 데 시간이 오래 걸리므로 Snort 코어가 생성됩니다.

지원되지 않는 기능

OpenStack의 threat defense virtual은 다음을 지원하지 않습니다.

- 자동 확장
- OpenStack Stein 및 Queens 릴리스 이외의 OpenStack 릴리스
- Ubuntu 18.04 버전 및 RHEL(Red Hat Enterprise Linux) 7.6 이외의 운영 체제

구축을 위한 OpenStack 요구 사항

OpenStack 환경은 다음의 지원되는 하드웨어 및 소프트웨어 요구 사항을 준수해야 합니다.

표 2: 하드웨어 및 소프트웨어 요건

카테고리	지원되는 버전	Notes(참고)
서버 하드웨어	UCS C240 M5	os-controller 및 os-compute 노드에 대해 각각 하나씩, 2개의 UCS 서버가 권장됩니다.
동인	VIRTIO, IXGBE, I40E	다음은 지원되는 드라이버입니다.
운영 체제	Ubuntu Server 18.04	이는 UCS 서버의 권장 OS입니다.
OpenStack 버전	스타인 릴리스	다양한 OpenStack 릴리스에 대한 세부 정보는 다음에서 확인할 수 있습니다. https://releases.openstack.org/

표 3: Cisco VIM Managed OpenStack의 하드웨어 및 소프트웨어 요구 사항

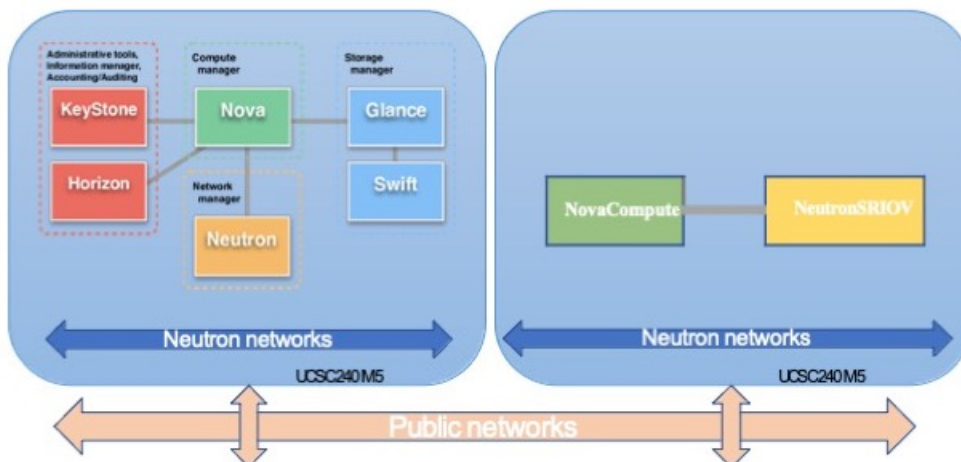
카테고리	지원되는 버전	Notes(참고)
서버 하드웨어	UCS C220-M5/UCS C240-M4	5개의 UCS 서버를 사용하는 것이 좋습니다. os-controller에는 각각 3개, os-compute 노드에는 2개 이상입니다.
동인	VIRTIO, SRIOV 및 VPP	다음은 지원되는 드라이버입니다.
운영 체제	Red Hat Enterprise Linux 7.6	권장되는 OS입니다.

카테고리	지원되는 버전	Notes(참고)
OpenStack 버전	OpenStack 13.0(Queens 릴리스)	다양한 OpenStack 릴리스에 대한 세부 정보는 다음에서 확인할 수 있습니다. https://releases.openstack.org/
Cisco VIM 버전	Cisco VIM 3.4.4	Cisco VIM OpenStack 문서를 참고하십시오.

OpenStack 플랫폼 토폴로지

다음 그림에는 2개의 UCS 서버를 사용하여 OpenStack에서 구축을 지원하기 위한 권장 토폴로지가 나와 있습니다.

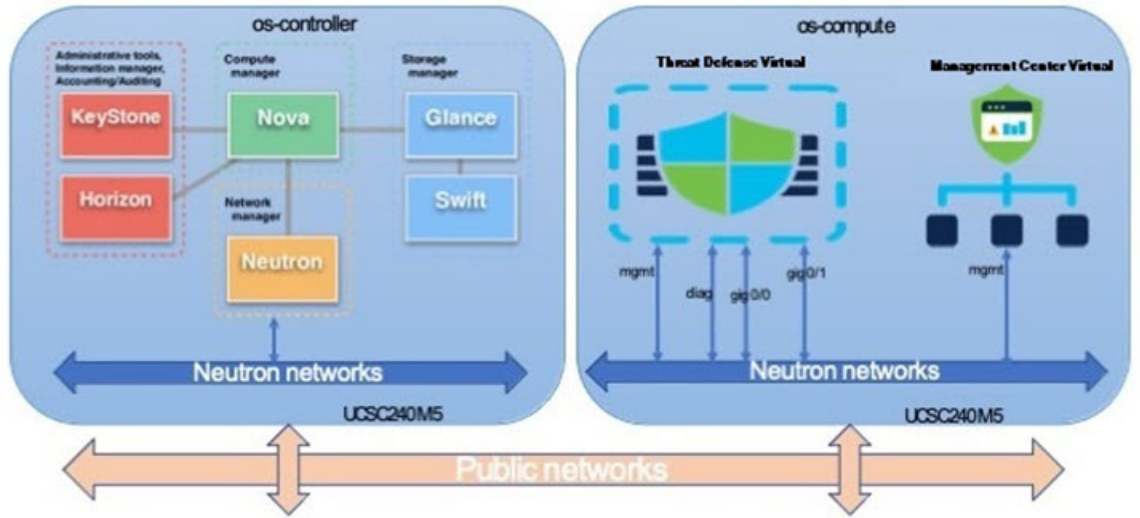
그림 1: OpenStack 플랫폼 토폴로지



OpenStack의 Threat Defense Virtual에 대한 네트워크 토폴로지 예

다음 그림은 Routed Firewall Mode의 threat defense virtual에 대한 예시 네트워크 토폴로지와 threat defense virtual에 대해서 OpenStack에 구성된 4개의 서브넷(관리, 진단, 내부 및 외부)을 보여줍니다.

그림 2: Threat Defense Virtual 및 OpenStack의 Management Center Virtual에 대한 토폴로지 예





2 장

OpenStack에 Threat Defense Virtual 구축

- 구축 개요, 9 페이지
- OpenStack에 Threat Defense Virtual 이미지 업로드, 10 페이지
- OpenStack 및 Threat Defense Virtual의 네트워크 인프라 생성, 10 페이지
- OpenStack에 Threat Defense Virtual 구축, 11 페이지

구축 개요

Cisco는 threat defense virtual 구축을 위한 샘플 히트 템플릿을 제공합니다. OpenStack 인프라 리소스를 생성하는 단계는 히트 템플릿(`deploy_os_infra.yaml`) 파일에 포함되어 네트워크, 서버넷 및 라우터 인터페이스를 생성합니다. threat defense virtual 구축 단계는 개략적으로 다음 섹션으로 분류됩니다.

- OpenStack Glance 서비스에 threat defense virtual qcow2 이미지를 업로드합니다.
- 네트워크 인프라 생성:
 - 네트워크
 - 서버넷
 - 라우터 인터페이스
- threat defense virtual 인스턴스 생성:
 - Flavor
 - 보안 그룹
 - 부동 IP
 - Instance

다음 단계를 사용하여 OpenStack에서 threat defense virtual을 구축할 수 있습니다.

OpenStack에 Threat Defense Virtual 이미지 업로드

threat defense virtual qcow2 이미지를 OpenStack 컨트롤러 노드에 복사한 다음 OpenStack Glance 서비스에 이미지를 업로드합니다.

시작하기 전에

Cisco.com에서 threat defense virtual qcow2 파일을 다운로드하고 이를 Linux 호스트에 넣습니다.

<https://software.cisco.com/download/navigator.html>



참고 Cisco.com 로그인 및 Cisco 서비스 계약이 필요합니다.

단계 1 qcow2 이미지 파일을 OpenStack 컨트롤러 노드에 복사합니다.

단계 2 OpenStack Glance 서비스에 threat defense virtual 이미지를 업로드합니다.

```
root@ucs-os-controller:~$ openstack image create <image_name> --public --disk-format qcow2 --container-format bare --file ./<ftdv_qcow2_file>
```

단계 3 threat defense virtual 이미지 업로드에 성공했는지 확인합니다.

```
root@ucs-os-controller:~$ openstack image list
```

예제:

```
root@ucs-os-controller:~$ openstack image list
list+-----+
| ID | Name | Status |
+-----+-----+-----+
| 06dd7975-0b6e-45b8-810a-4ff98546a39d | ftdv-7-0-image | active |
+-----+-----+-----+
```

업로드된 이미지 및 해당 상태가 표시됩니다.

다음에 수행할 작업

deploy_os_infra.yaml 템플릿을 사용하여 네트워크 인프라를 생성합니다.

OpenStack 및 Threat Defense Virtual의 네트워크 인프라 생성

시작하기 전에

Heat 템플릿 파일은 네트워크 인프라 및 threat defense virtual에 대한 필수 구성 요소(예: 버전, 네트워크, 서버넷, 라우터 인터페이스 및 보안 그룹 규칙)를 생성하는 데 필요합니다.

- `deploy_os_infra.yaml`
- `env.yaml`

사용 중인 threat defense virtual 버전의 템플릿은 [FTDv OpenStack 히트 템플릿](#)의 GitHub 리포지토리에서 사용할 수 있습니다.



중요 Cisco에서 제공하는 템플릿은 오픈 소스 예시로 제공되며 일반적인 Cisco TAC 지원 범위에서는 다루지 않습니다. GitHub에서 정기적으로 업데이트 및 ReadMe 지침을 확인하십시오.

단계 1 인프라 히트 템플릿 파일을 구축합니다.

```
root@ucs-os-controller:~$ openstack stack create<stack-name> -e<environment files name> -t<deployment file name>
```

예제:

```
root@ucs-os-controller:~$ openstack stack create infra-stack -e env.yaml -t deploy_os_infra.yaml
```

단계 2 인프라 스택이 성공적으로 생성되었는지 확인합니다.

```
root@ucs-os-controller:~$ openstack stack list
```

다음에 수행할 작업

OpenStack에서 threat defense virtual 인스턴스를 생성합니다.

OpenStack에 Threat Defense Virtual 구축

샘플 threat defense virtual 히트 템플릿을 사용하여 OpenStack에 threat defense virtual를 구축합니다.

시작하기 전에

OpenStack에 threat defense virtual를 구축하려면 히트 템플릿이 필요합니다.

- `deploy_ftdv.yaml`

사용 중인 threat defense virtual 버전의 템플릿은 [FTDv OpenStack 히트 템플릿](#)의 GitHub 리포지토리에서 사용할 수 있습니다.



중요 Cisco에서 제공하는 템플릿은 오픈 소스 예시로 제공되며 일반적인 Cisco TAC 지원 범위에서는 다루지 않습니다. GitHub에서 정기적으로 업데이트 및 ReadMe 지침을 확인하십시오.

단계 1 threat defense virtual 히트 템플릿 파일(`deploy_ftdv.yaml`)을 구축하여 threat defense virtual 인스턴스를 생성합니다.

```
root@ucs-os-controller:~$ openstack stack create ftdv-stack -e env.yaml -t deploy_ftdv.yaml
```

예제:

```
+-----+-----+
| Field          | Value                               |
+-----+-----+
| id             | 14624af1-e5fa-4096-bd86-c453bc2928ae |
| stack_name     | ftdv-stack                          |
| description    | FTDvtemplate                         |
| creation_time  | 2020-12-07T14:55:05Z                |
| updated_time   | None                                  |
| stack_status   | CREATE_IN_PROGRESS                  |
| stack_status_reason | Stack CREATE started                |
+-----+-----+
```

단계 2 threat defense virtual 스택이 성공적으로 생성되었는지 확인합니다.

```
root@ucs-os-controller:~$ openstack stack list
```

예제:

```
+-----+-----+-----+-----+-----+-----+
| ID                               | Stack Name | Project                               | Stack Status |
| Creation Time | Updated Time |
+-----+-----+-----+-----+-----+-----+
| 14624af1-e5fa-4096-bd86-c453bc2928ae | ftdv-stack | 13206e49b48740fdafca83796c6f4ad5 | CREATE_COMPLETE |
| 2020-12-07T14:55:05Z | None |
| 198336cb-1186-45ab-858f-15ccd3b909c8 | infra-stack | 13206e49b48740fdafca83796c6f4ad5 | CREATE_COMPLETE |
| 2020-12-03T10:46:50Z | None |
+-----+-----+-----+-----+-----+-----+
```



3 장

Secure Firewall device manager로 Secure Firewall Threat Defense Virtual 관리

이 장에서는 device manager로 관리되는 독립형 threat defense virtual 디바이스를 구축하는 방법을 설명합니다. 고가용성 쌍을 구축하려면 [Cisco Secure Firewall Device Manager 구성 가이드](#) 설정 가이드를 참조하십시오.

- [Secure Firewall device manager를 사용하는 Secure Firewall Threat Defense Virtual 정보, 13 페이지](#)
- [초기 구성, 14 페이지](#)
- [Secure Firewall device manager에서 디바이스를 구성하는 방법, 16 페이지](#)

Secure Firewall device manager를 사용하는 Secure Firewall Threat Defense Virtual 정보

Secure Firewall Threat Defense Virtual은(는) Cisco NGFW 솔루션의 가상화된 구성 요소입니다. threat defense virtual은 스테이트풀 방화벽, 라우팅, NGIPS(Next-Generation Intrusion Prevention System), AVC(Application Visibility and Control), URL 필터링, 악성코드 디펜스와 같은 차세대 방화벽 서비스를 제공합니다.

일부 threat defense 모델에 포함된 웹 기반 디바이스 설정 마법사인 Secure Firewall device manager을 사용하여 threat defense virtual을 관리할 수 있습니다. device manager 사용을 통해 소규모 네트워크에서 가장 흔히 사용되는 소프트웨어의 기본 기능을 구성할 수 있습니다. Firepower Device Manager는 디바이스를 하나 또는 몇 개만 포함하는 네트워크 용도로 특별히 설계되어 고성능 다중 디바이스 관리자를 사용해 여러 threat defense 디바이스가 포함된 대규모 네트워크를 제어하기를 원하지 않을 경우에 유용합니다.

다수의 디바이스를 관리하거나 threat defense에서 허용하는 더 복잡한 기능 및 구성을 사용하려는 경우에는 통합형 device manager 대신 management center을(를) 사용하여 디바이스를 구성하십시오. 자세한 내용은 [Secure Firewall Management Center로 Secure Firewall Threat Defense Virtual 관리, 23 페이지](#)를 참조하십시오.

문제 해결을 위해 관리 인터페이스에서 SSH를 사용해 threat defense CLI에 액세스하거나, device manager CLI에서 threat defense에 연결할 수 있습니다.

기본 구성

threat defense virtual 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.

threat defense virtual은(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 threat defense virtual 기능이 네트워크에서 올바르게 작동하는 초기 구성을 완료해야 합니다. 다음 두 가지 방법 중 하나로 시스템의 초기 구성을 수행할 수 있습니다.

- device manager 웹 인터페이스(권장)를 사용합니다. Device Manager는 웹 브라우저에서 실행됩니다. 이 인터페이스를 사용하여 시스템을 구성, 관리 및 모니터링합니다.
- CLI(명령줄 인터페이스) 설정 마법사를 사용합니다(선택). 초기 구성에 device manager 대신 CLI 설정 마법사를 사용할 수 있으며, 문제 해결에도 CLI를 사용할 수 있습니다. device manager을(를) 사용해 여전히 시스템을 구성, 관리, 모니터링할 수 있습니다. (선택 사항) threat defense CLI 마법사 시작을 참조하십시오.

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

실행 Device Manager

device manager에 처음 로그인할 때는 디바이스 설정 마법사로 이동해 초기 시스템 구성을 완료합니다.

단계 1 브라우저를 열고 device manager에 로그인합니다. CLI에서 초기 컨피그레이션을 수행하지 않았다고 가정하고 <https://FTDv> 공용 IPv4 주소 또는 [FTDv IPv6 공용 주소]에서 device manager를 엽니다.

단계 2 사용자 이름 **admin** 및 비밀번호 **Admin123**으로 로그인합니다.

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 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

- device manager를 사용해 디바이스 설정은 [Secure Firewall device manager에서 디바이스를 구성하는 방법, 16 페이지](#)를 참고하십시오.

Secure Firewall 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.

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

사용할 각 라이선스 옵션(IPS, 악성코드 방어, URL 필터링)에 대해 **Enable**(활성화)을 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 IPS 라이선스는 다음과 같이 표시됩니다.

그림 3: 활성화된 IPS 라이선스

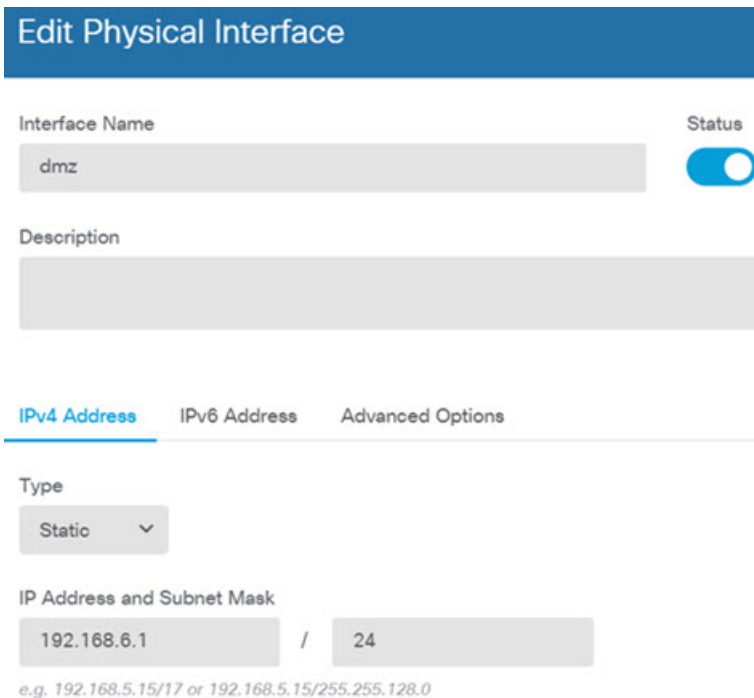


단계 2 다른 인터페이스를 구성한 경우 **Device**(디바이스)를 선택하고 **Interfaces**(인터페이스) 그룹에서 **View Configuration**(컨피그레이션 보기)를 클릭한 뒤 각 인터페이스를 구성합니다.

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 4: 인터페이스 수정



참고 IPv6 주소를 활성화하려면 IPv6 탭을 선택하고 고정 또는 DHCP를 사용하여 IPv6 주소를 구성합니다.

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.

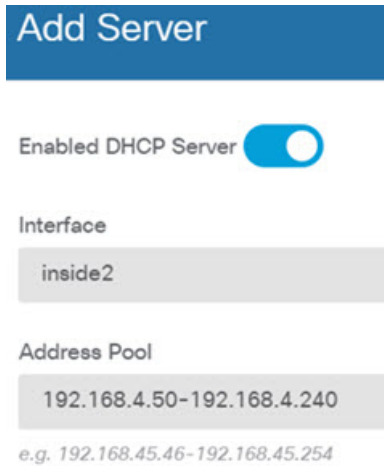
그림 5: 보안 영역 개체

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 6: 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) 드롭다운 목록의 아래쪽에서 **Create New Network**(새 네트워크 생성)를 클릭하여 생성할 수 있습니다.

그림 7: 기본 라우터

The screenshot shows the 'Add Static Route' configuration page. 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 '+' button and a text input field containing 'any-ipv4'.

참고 마찬가지로 IPv6 라디오 버튼을 선택하여 IPv6 경로를 구성할 수 있습니다.

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.

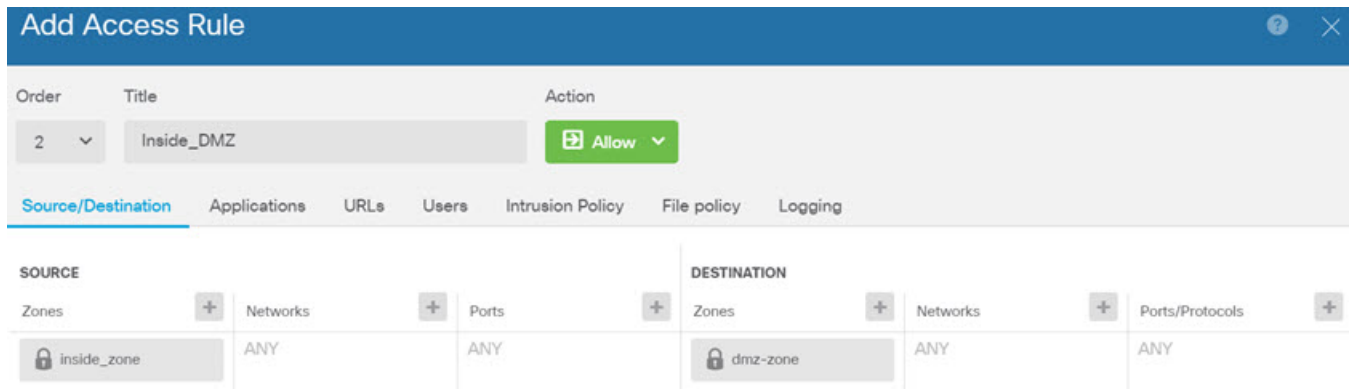
- **SSL Decryption(SSL 암호 해독)** — 침입, 악성코드 등에 대한 암호화된 연결(예: HTTPS)을 검사하려는 경우, 연결을 암호 해독해야 합니다. SSL 암호 해독 정책을 사용하여 어떤 연결을 암호 해독해야 할지 확인합니다. 시스템은 검사를 수행한 후에 연결을 다시 암호화합니다.
- **Identity(ID)** — 네트워크 활동과 개인 사용자의 상관관계를 분석하거나 사용자 또는 사용자 그룹 멤버십을 기반으로 네트워크 액세스를 제어하려면 ID 정책을 사용하여 지정된 소스 IP 주소와 연결된 사용자를 확인합니다.
- **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 업

데이트된 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 8: 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

device manager로 threat defense virtual을 관리하는 방법에 대한 자세한 내용은 [Firepower Device Manager 용 Cisco Firepower Threat Defense 구성 가이드](#) 또는 Secure Firewall device manager 온라인 도움말을 참조하십시오.



4 장

Secure Firewall Management Center로 Secure Firewall Threat Defense Virtual 관리

이 장에서는 management center로 관리되는 독립형 threat defense virtual 디바이스를 구축하는 방법을 설명합니다.



참고 이 문서에서는 최신 threat defense virtual 버전의 기능 이전 버전의 소프트웨어를 사용할 경우에는 해당 버전에 대한 management center 설정 가이드의 절차를 참조하십시오.

- [Secure Firewall Management Center를 사용하는 Secure Firewall Threat Defense Virtual 정보, 23 페이지](#)
- [Secure Firewall Management Center에 로그인, 24 페이지](#)
- [디바이스를 Secure Firewall Management Center에 등록, 24 페이지](#)
- [기본 보안 정책 구성, 27 페이지](#)
- [Secure Firewall Threat Defense CLI에 액세스, 39 페이지](#)

Secure Firewall Management Center를 사용하는 Secure Firewall Threat Defense Virtual 정보

Secure Firewall Threat Defense Virtual은(는) Cisco NGFW 솔루션의 가상화된 구성 요소입니다. threat defense virtual은 스테이트풀 방화벽, 라우팅, NGIPS(Next-Generation Intrusion Prevention System), AVC(Application Visibility and Control), URL 필터링, 악성코드 디펜스와 같은 차세대 방화벽 서비스를 제공합니다.

전체 기능을 갖춘 별도 서버의 다중 디바이스 관리자인 management center를 사용해 threat defense virtual을 관리할 수 있습니다. management center 설치에 대한 자세한 내용은 [Cisco Firepower Management Center 1600, 2600 및 4600 하드웨어 설치 가이드](#)를 참조하십시오.

threat defense virtual은 threat defense virtual 장비에 할당된 관리 인터페이스의 management center로 등록 및 통신합니다.

문제 해결을 위해 관리 인터페이스에서 SSH를 사용해 threat defense CLI에 액세스하거나, management center CLI에서 threat defense에 연결할 수 있습니다.

Secure Firewall Management Center에 로그인

management center을 사용해 threat defense를 구성하고 모니터링합니다.

시작하기 전에

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

단계 1 지원되는 브라우저를 사용해 다음 URL을 입력합니다.

https://fmcv_ip_address

*fmc_ip_address*는 management center의 IP 주소 또는 호스트 이름을 식별합니다.

참고 [https://\[fmcv_ipv6_public_address\]](https://[fmcv_ipv6_public_address]) IPv6에 지정

단계 2 사용자 이름 및 비밀번호를 입력합니다.

단계 3 **Log In**(로그인)을 클릭합니다.

디바이스를 Secure Firewall Management Center에 등록

시작하기 전에

threat defense virtual 머신이 성공적으로 구축되었으며, 전원이 켜져 있고 첫 번째 부팅 절차를 완료했는지 확인하십시오.



참고 이 절차는 day0/부트스트랩을 통해서 management center에 대한 등록 정보가 제공된 것으로 가정합니다. 그러나 이러한 모든 설정은 **configure network**(네트워크 구성) 명령을 사용하여 CLI에서 나중에 변경할 수 있습니다. [Secure Firewall Threat Defense 명령 참조](#)를 참조하십시오.

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 ?

Host:†

Display Name:

Registration Key: *

Group:

Access Control Policy: *

Smart Licensing
 Note: All virtual FTDs require a performance tier license.
 Make sure your Smart Licensing account contains the available licenses you need.
 It's important to choose the tier that matches the license you have in your account.
 Click [here](#) for information about the FTD performance-tiered licensing.
 Until you choose a tier, your FTDv defaults to the FTDv50 selection.

Performance Tier (only for FTDv 7.0 and above):

Malware
 Threat
 URL Filtering

Advanced

Unique NAT ID: †

Transfer Packets

- **Host(호스트)**—추가할 디바이스의 IP 주소(IPv4 및 IPv6)를 입력합니다. IPv6 활성화 설정의 경우 호스트 이름에 Ipv4 또는 Ipv6을 포함할 수 있습니다.
- **Display Name(표시 이름)**—management center에 표시하고자 하는 디바이스 이름을 입력합니다.
- **Registration key(등록 키)** - threat defense virtual 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, 37 페이지](#)을 참조하십시오.

The screenshot shows the 'New Policy' configuration interface. It includes a search icon in the top right corner. The form contains the following elements:

- Name:** A text input field containing 'ftd-ac_policy'.
- Description:** An empty text input field.
- Select Base Policy:** A dropdown menu currently set to 'None'.
- Default Action:** Three radio button options: 'Block all traffic' (selected), 'Intrusion Prevention', and 'Network Discovery'.
- Targeted Devices:** A section with the instruction 'Select devices to which you want to apply this policy.' It features a search bar labeled 'Search by name or value' and a list of 'Available Devices' containing the IP address '192.168.0.12'. A blue 'Add to Policy' button is positioned next to the available device list, and an empty 'Selected Devices' list is on the right.

- **Smart license** (스마트 라이선싱) - 구축하려는 기능에 필요한 스마트 라이선스(악성코드 디펜스 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) - threat defense virtual 부트스트랩 구성에서 지정한 NAT ID를 지정합니다.
- **Transfer Packets**(패킷 전송) - 디바이스가 management center에 패킷을 전송하도록 허용합니다. 이 옵션이 활성화되어 IPS 또는 Snort 같은 이벤트가 트리거되면 디바이스는 검사를 위해 이벤트 메타데이터 정보 및 패킷 데이터를 management center에 전송합니다. 비활성화하면 management center에 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. threat defense virtual 등록에 실패하면 다음 항목을 확인하십시오.

- **Ping** - 다음 명령을 사용해 threat defense CLI([Secure Firewall Threat Defense CLI에 액세스, 39 페이지](#))에 액세스하고 management center IP 주소에 Ping을 보냅니다.

ping system ip_address

Ping이 실패하는 경우 **show network** 명령을 사용해 네트워크 설정을 확인합니다. threat defense IP 주소를 변경해야 하는 경우 **configure network {ipv4 | ipv6} manual or DHCP** 명령을 사용합니다.

- **NTP** - NTP 서버가 **System**(시스템) > **Configuration**(설정) > **Time Synchronization**(시간 동기화) 페이지에서 설정한 management center 서버와 일치하는지 확인합니다.
- 등록 키, NAT ID 및 management center IP 주소 - 두 디바이스에서 동일한 등록 키 및 NAT ID가 사용되고 있는지 확인합니다. **configure manager add DONTRESOLVE<registrationkey> <NATID>** 명령을 사용해 threat

defense virtual에서 등록 키 및 NAT ID를 설정할 수 있습니다. 이 명령을 사용해 management center 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.

단계 1 인터페이스 구성, 27 페이지

단계 2 DHCP 서버 구성, 31 페이지

단계 3 기본 경로 추가, 32 페이지

단계 4 NAT 구성, 34 페이지

단계 5 액세스 제어 구성, 37 페이지

단계 6 구성 구축, 38 페이지

인터페이스 구성

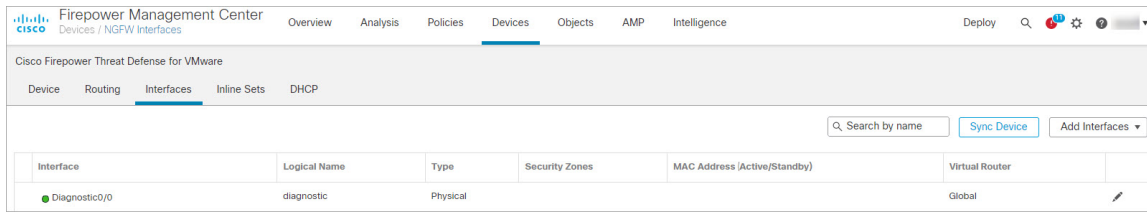
threat defense virtual 인터페이스를 활성화하고, 보안 영역에 이를 할당하며, IP 주소를 설정합니다. 일반적으로 시스템이 의미 있는 트래픽을 전달하도록 최소 2개 이상의 인터페이스를 구성해야 합니다. 일반적으로 업스트림 라우터 또는 인터넷과 만나는 외부 인터페이스와 조직 네트워크에서 사용하는 하나 이상의 내부 인터페이스를 사용합니다. 이런 인터페이스의 일부는 웹 서버와 같이 공개적으로 액세스할 수 있는 에셋을 배치하는 '비무장지대(DMZ)'로 사용하게 됩니다.

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.

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.

Edit Physical Interface

General | IPv4 | IPv6 | Advanced | Hardware Configuration | FMC Access

Name:

Enabled
 Management Only

Description:

Mode:

Security Zone:

Interface ID:

MTU:
(64 - 9000)

Priority:
(0 - 65535)

Propagate Security Group Tag:

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.

- **IPv4**—드롭다운 목록에서 **Use Static IP**(고정 IP 사용)를 선택하고 슬래시(/) 표기 또는 DHCP 옵션으로 IP 주소와 서브넷 마스크를 입력합니다.

예를 들어 **192.168.1.1/24** 를 입력합니다.

The screenshot shows the 'Edit Physical Interface' configuration window. The 'IPv4' tab is active. Under 'IP Type', 'Use Static IP' is selected. The 'IP Address' field contains '192.168.1.1/24'. A note below the field reads 'eg. 192.0.2.1/255.255.255.128 or 192.0.2.1/25'.

- **IPv6**—상태 비저장 자동 구성 및 IPv6 DHCP 또는 정적 구성의 경우 **Autoconfiguration**(자동 구성) 확인란을 선택하여 인터페이스를 활성화합니다.

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' configuration window with the 'IPv4' tab selected. The 'IP Type' dropdown menu is set to 'Use DHCP'. Below it, the 'Obtain default route using DHCP' checkbox is checked. The 'DHCP route metric' is set to '1' in a text input field. At the bottom left of the input field, '(1 - 255)' is displayed.

- **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 threat defense virtual에서 IP 주소를 가져오게 하려면 DHCP 서버를 활성화합니다.

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.

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.

Add Static Route Configuration

Type: IPv4 IPv6

Interface*
 Outside

(Interface starting with this icon signifies it is available for route leak)

Available Network + Selected Network

Search Add

- any-ipv4
- any-IPv4-10.0.0.1
- IPv4-Benchmark-Tests
- IPv4-Link-Local
- IPv4-Multicast
- IPv4-Private-10.0.0.0-8

any-ipv4

Ensure that egress virtualrouter has route to that destination

Gateway
 any-IPv4-10.0.0.1 +

Metric:
 1
 (1 - 254)

Tunneled: (Used only for default Route)

Route Tracking:
 +

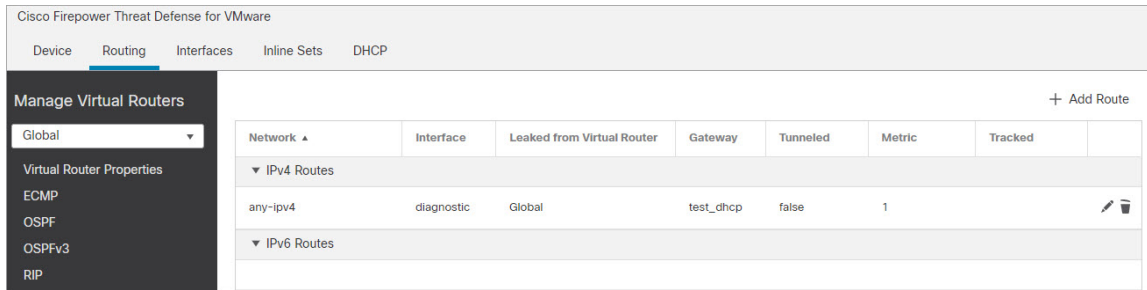
Cancel OK

- **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.

NAT 구성



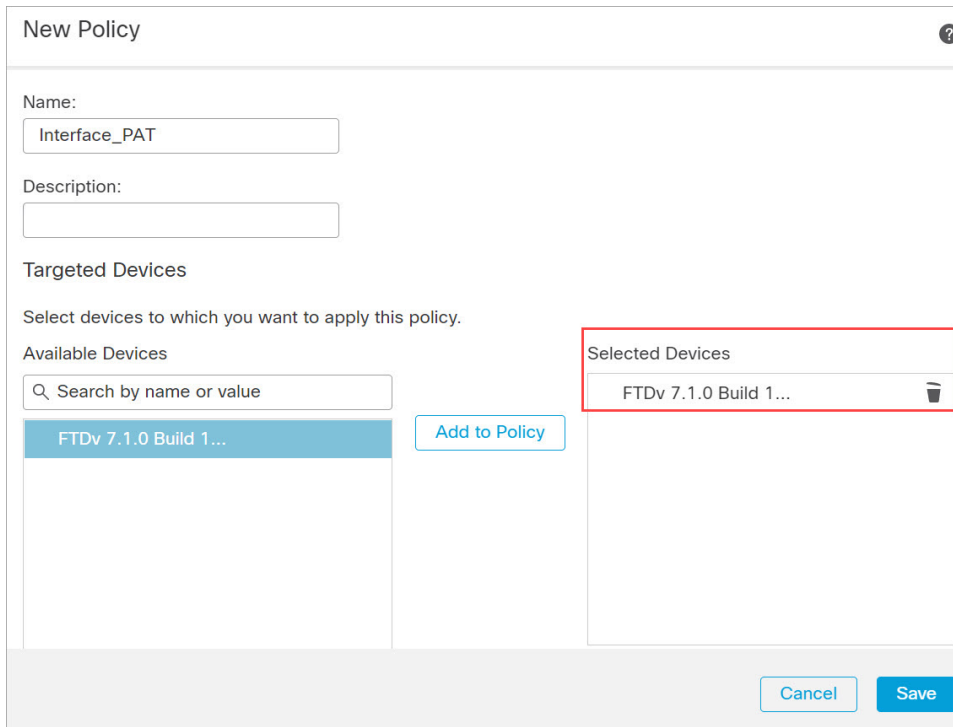
단계 4 **Save**(저장)를 클릭합니다.

NAT 구성

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

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 management center을 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.

Add NAT Rule

NAT Rule:
Auto NAT Rule

Type:
Dynamic

Enable

Interface Objects Translation PAT Pool Advanced

- **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.

Add NAT Rule

NAT Rule:
Auto NAT Rule

Type:
Dynamic

Enable

Interface Objects Translation PAT Pool Advanced

Available Interface Objects Source Interface Objects (0) Destination Interface Objects (1)

Q Search by name

outside-zone Add to Source

any

outside-zone

Add to Destination

Cancel OK

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

Add NAT Rule

NAT Rule:

Type:

Enable

Interface Objects **Translation** PAT Pool Advanced

Original Packet	Translated Packet
Original Source:* <input type="text" value="any-IPv4-10.0.0.1"/> +	Translated Source: <input type="text" value="Destination Interface IP"/>
Original Port: <input type="text" value="TCP"/>	Translated Port: <input type="text"/>

The values selected for Destination Interface Objects in 'Interface Objects' tab will be used

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

New Network Object

Name

Description

Network
 Host Range **Network** FQDN

Allow Overrides

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

마찬가지로, 모든 IPv6 트래픽에 대해 기본 호스트 네트워크 [::/0]를 사용하여 NAT 정책을 생성할 수 있습니다.

- **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

management center을 사용해 threat defense virtual를 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 [Firepower Management Center 구성 가이드](#) 구성 가이드를 참조하십시오.

단계 1 **Policy(정책) > Access Policy(액세스 정책) > Access Policy(액세스 정책)**을 선택하고 threat defense에 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.

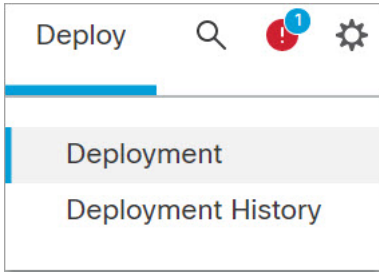
#	Name	Source Zones	Dest Zones	Source Netw...	Dest Netw...	VLAN Tags	Users	Appli...	Source Ports	Dest Ports	URLs	Source Dyna... Attrl...	Desti... Dyna... Attrl...	Act...	Icons
1	inside_to_outside	inside-zone	outside-zone	Any	Any	Any	Any	Any	Any	Any	Any	Any	Any	Allow	Icons

단계 4 **Save(저장)**를 클릭합니다.

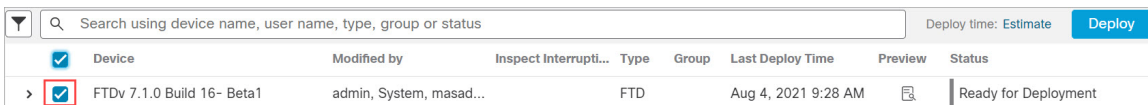
구성 구축

threat defense virtual에 설정 변경 사항을 구축합니다. 구축하기 전에는 디바이스에서 변경 사항이 활성 상태가 아닙니다.

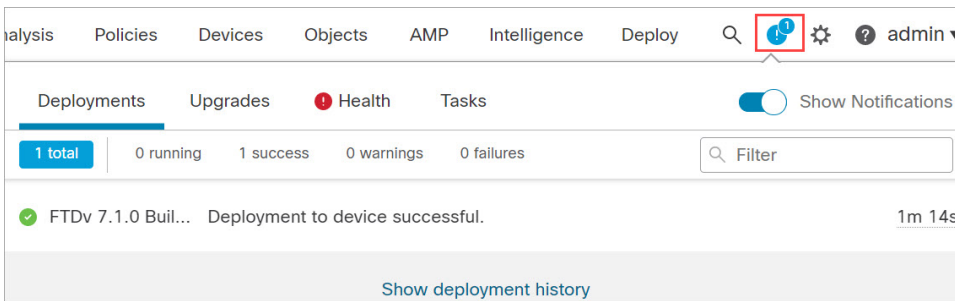
단계 1 우측 상단에서 **Deploy**(구축)를 클릭합니다.



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.



Secure Firewall Threat Defense CLI에 액세스

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

단계 1 (옵션 1) threat defense virtual 관리 인터페이스 IP 주소로 직접 SSH.

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

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

번역에 관하여

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