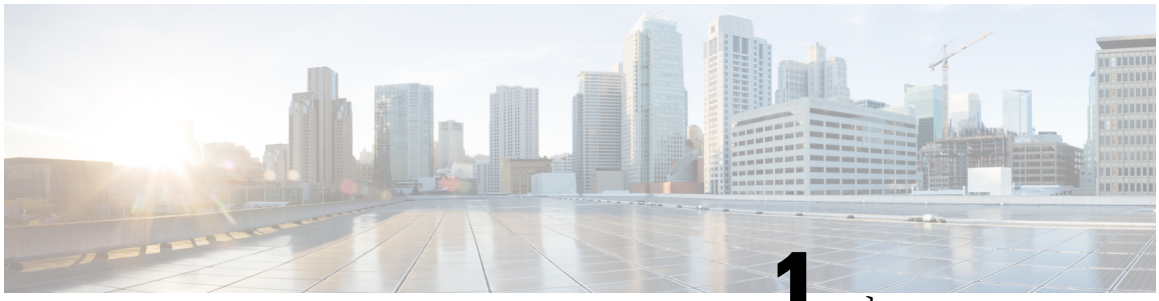
Secure Firewall 4200 Threat Defense 시작하기: Cloud-Delivered Firewall Management Center

최종 변경: 2026년 3월 25일

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

시작하기 전에

Secure Firewall 4200 시리즈는 대규모 기업, 데이터 센터, 통신 사업자의 보안 요구 사항을 충족하기 위한 고성능 방화벽입니다. 소형 1RU 폼 팩터 내에서 우수한 위협 방어 기능을 제공합니다. 주요 기능 및 이점:

- 암호화 가속 아키텍처의 SSL 및 VPN 해독으로 성능 유지
- 공간 절약형 1RU 폼 팩터
- 16노드 클러스터
- 추가 인터페이스 지원, 최대 400G 인터페이스 및 Fail-to-Wire 네트워크 모듈용 인터페이스 모듈 베이 2개
- 이벤트 스토리지 및 멀웨어 분석을 위한 SSD 2개
- 듀얼 관리 인터페이스를 통한 탄력성 향상
- SD-WAN 지원 기능으로, 온디맨드 터널 및 다중 WAN 인터페이스 간 동적 애플리케이션 경로 선택을 통해 간소화된 사이트 간 통신 구현
- Cisco의 네이티브 AI/ML 솔루션을 통해 이상 징후를 탐지하고 위협을 해결하며 정책을 최적화하여 최고 성능을 달성합니다.

브랜치 오피스에 방화을벽 설치하고 Security Cloud Control(이전 Cisco Defense Orchestrator)를 사용하여 외부 인터페이스에서 방화벽을 관리합니다.

참고 외부 관리는 클러스터링 또는 멀티인스턴스 클러스터링을 지원하지 않습니다. 이 경우, Security Cloud Control에 액세스하려면 관리 인터페이스를 사용하십시오.

이 가이드에서는 특히 외부 관리에 대해 설명하지만, 관리 인터페이스를 사용한 관리에 대해서는 *Cisco Security Cloud Control: Firewall Threat Defense*용 클라우드 제공 *Firewall Management Center*을 참조할 수 있습니다.

- 방화벽 켜기, 2 페이지
- Firewall Threat Defense와 ASA 중 어떤 애플리케이션이 설치되나요?, 3 페이지

방화벽 켜기

시스템 전원은 디바이스 뒷면에 있는 로커 전원 스위치로 제어됩니다. 로커 전원 스위치는 부드러운 알림 기능을 제공하여 시스템의 정상적인 종료 과정을 지원함으로써 시스템 소프트웨어 및 데이터 손상 위험을 줄입니다.

참고 방화벽을 처음 부팅할 때는 Firewall Threat Defense 초기화에 약 15~30분이 소요될 수 있습니다.

시작하기 전에

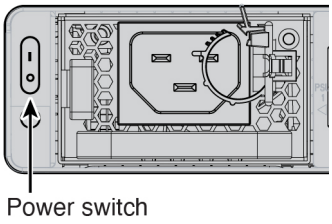
디바이스에 안정적인 전원을 제공하는 것이 중요합니다(예: UPS(Uninterruptable Power Supply) 사용). 먼저 셧다운하지 않고 전력이 손실되면 파일 시스템이 심각하게 손상될 수 있습니다. 항상 백그라운드에서 많은 프로세스가 실행되므로 전력이 손실되면 시스템이 정상적으로 종료되지 않습니다.

프로시저

단계 **1** 전원 케이블을 디바이스에 연결하고 전기 콘센트에 꽂습니다.

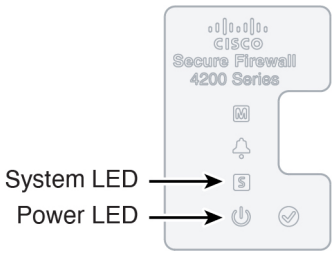
단계 **2** 전원 코드 옆에 위치한 섀시 후면의 로커 전원 스위치를 사용하여 전원을 켭니다.

그림 ***1:*** 전원 스위치



단계 **3** LED에서 현재 상태를 확인합니다.

그림 *2: LED*



- 전원 LED - 녹색으로 켜져 있으면 방화벽 전원이 켜져 있음을 의미합니다.
- 시스템 (S) LED - 다음 동작을 참조하십시오.

표 *1:* 시스템 *(S) LED* 동작

LED 동작	설명	디바이스 전원이 켜진 후의 시간**(**분**:** 초**)**
녹색으로 빠르게 깜박임	부팅	01:00
황색으로 빠르게 깜박임*(*오류 상태*)*	부팅 실패	01:00
녹색	애플리케이션 로드됨	15:00 - 30:00
황색 고정*(*오류 상태*)*	애플리케이션 로드 실패	15:00 - 30:00

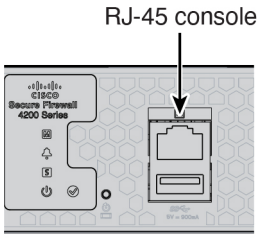
Firewall Threat Defense와 ASA 중 어떤 애플리케이션이 설치되나요?

애플리케이션 Firewall Threat Defense 또는 ASA 모두 하드웨어에서 지원됩니다. 콘솔 포트에 연결하고 공장에서 설치된 애플리케이션이 무엇인지 확인합니다.

프로시저

단계 **1** 콘솔 포트에 연결합니다.

그림 *3:* 콘솔 포트



단계 **2** CLI 프롬프트를 참조하여 방화벽 Firewall Threat Defense 또는 ASA를 실행 중인지 확인합니다.

Firewall Threat Defense

Firepower 로그인(FXOS) 프롬프트가 표시됩니다. 로그인하고 새 비밀번호 설정하지 않고 연결을 끊을 수 있습니다. 끝까지 로그인해야 하는 경우에는 Firewall Threat Defense CLI에 액세스, 4 페이지를 참조하십시오.

```
firepower login:
```

ASA

ASA 프롬프트가 표시됩니다.

```
ciscoasa>
```

단계 **3** 잘못된 애플리케이션을 실행 중인 경우 *Cisco Secure Firewall ASA 및 Secure Firewall Threat Defense 이미지 재설치 가이드*를 참조하십시오.

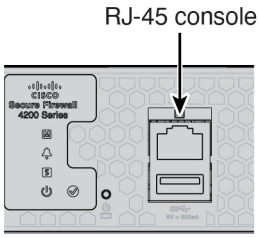
Firewall Threat Defense CLI에 액세스

구성 또는 문제 해결을 위해 CLI에 액세스해야 할 수 있습니다.

프로시저

단계 **1** 콘솔 포트에 연결합니다.

그림 *4:* 콘솔 포트



단계 **2** FXOS에 연결합니다. **admin** 사용자 이름 및 비밀번호(기본값은 **Admin123**)를 사용하여 CLI에 로그인합니다. 처음 로그인하면 비밀번호를 변경하라는 메시지가 표시됩니다.

```
firepower login: admin
Password: Admin123
Successful login attempts for user 'admin' : 1

[...]

Hello admin. You must change your password.
Enter new password: ********
Confirm new password: ********
Your password was updated successfully.

[...]

firepower#
```

단계 **3** Firewall Threat Defense CLI로 변경합니다.

connect ftd

Firewall Threat Defense CLI에 처음 연결할 때는 초기 구성을 완료하라는 프롬프트가 표시됩니다.

예제:

```
firepower# connect ftd
>
```

Firewall Threat DefenseCLI를 종료하려면 **exit** 또는 **logout** 명령을 입력합니다. 그러면 FXOS 프롬프트로 돌아갑니다.

예제:

```
> exit
firepower#
```

버전 확인 및 이미지 재설치

방화벽을 구성하기 전에 대상 버전을 설치하는 것이 좋습니다. 또는 가동을 시작한 후 업그레이드를 수행할 수 있지만, 구성을 유지하는 업그레이드는 이 절차를 사용하는 것보다 시간이 더 오래 걸릴 수 있습니다.

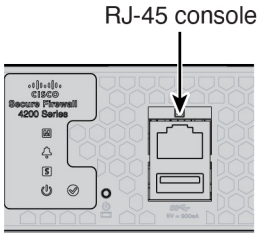
어떤 버전을 실행해야 하나요?

Cisco는 소프트웨어 다운로드 페이지에서 릴리스 번호 옆에 금색 별표로 표시된 Gold Star 릴리스를 실행할 것을 권장합니다. https://www.cisco.com/c/en/us/products/collateral/security/firewalls/bulletin-c25-743178.html에 설명된 릴리스 전략을 참조할 수도 있습니다.

프로시저

단계 **1** 콘솔 포트에 연결합니다.

그림 ***5:*** 콘솔 포트



단계 **2** FXOS CLI에서 실행 중인 버전을 표시합니다.

scope ssa

show app-instance

예제:

```
Firepower# scope ssa
Firepower /ssa # show app-instance

Application Name Slot ID Admin State Operational State Running Version Startup Version Cluster Oper State
---------------- ------- ----------- ----------------- --------------- --------------- -------------------
ftd              1       Enabled     Online            7.6.0.65        7.6.0.65        Not Applicable
```

단계 **3** 새 버전을 설치하려면 다음 단계를 수행합니다.

a) 기본적으로 관리 인터페이스는 DHCP를 사용합니다. 관리 인터페이스에 대한 고정 IP 주소를 설정해야 하는 경우 다음 명령을 입력합니다.

scope fabric-interconnect a

set out-of-band static ip *ip* **netmask** 넷마스크 **gw** 게이트웨이

commit-buffer

b) 이미지 재설치 절차는 FXOS 문제 해결 설명서를 참조하십시오.

관리 인터페이스에서 액세스할 수 있는 서버에서 새 이미지를 다운로드해야 합니다.

방화벽이 재부팅된 후 FXOS CLI에 다시 연결됩니다

c) FXOS CLI에서 관리자 비밀번호를 다시 설정하라는 메시지가 표시됩니다.

d) 방화벽을 종료합니다. (필요한 경우) 방화벽 전원 끄기, 8 페이지의 내용을 참조하십시오.

라이선스 얻기

Cisco 또는 리셀러에서 디바이스를 구매한 경우 라이선스는 Smart Software License 어카운트에 연결되어 있어야 합니다. 아직 Smart Software Manager에 어카운트가 없는 경우 새 어카운트 설정 링크를 클릭합니다.

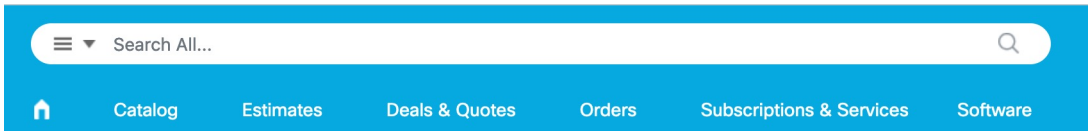
아직 등록하지 않은 경우 Security Cloud Control를 Smart Software Manager에 등록합니다. 등록하려면 Smart Software Manager에서 등록 토큰을 생성해야 합니다.자세한 지침은 Security Cloud Control 설명서를 참조하십시오.

Firewall Threat Defense에는 다음 라이선스가 있습니다.

- Essentials—필수
- IPS
- 악성코드 방어
- URL 필터링
- Cisco Secure Client
- Carrier—배율, GTP/GPRS, M3UA, SCTP

1. 라이선스를 직접 추가해야 하는 경우 Cisco Commerce Workspace로 이동하여 **Search All(**모두 검색**)** 필드를 사용합니다.

   그림 *6:* 라이선스 검색



2. 다음 라이선스 PID를 검색합니다.

참고 PID를 찾을 수 없는 경우 주문에 수동으로 PID를 추가할 수 있습니다.

- Essentials
  - 자동 포함
- IPS, 악성코드 방어 및 URL 조합:
  - L-FPR4215T-TMC =
  - L-FPR4225T-TMC =
  - L-FPR4245T-TMC =

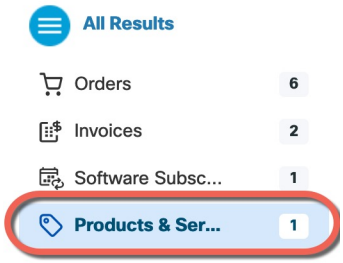
위의 PID 중 하나를 주문에 추가하면 다음 PID 중 하나에 해당하는 기간별 구독을 선택할 수 있습니다.

- L-FPR4215T-TMC-1Y
- L-FPR4215T-TMC-3Y
- L-FPR4215T-TMC-5Y
- L-FPR4225T-TMC-1Y
- L-FPR4225T-TMC-3Y
- L-FPR4225T-TMC-5Y
- L-FPR4245T-TMC-1Y
- L-FPR4245T-TMC-3Y
- L-FPR4245T-TMC-5Y

- 캐리어:
  - L-FPR4200-FTD-CAR=
- Cisco Secure 클라이언트—Cisco Secure Client 주문 가이드를 참조하십시오.

3. 결과에서 **Products & Services(**제품 및 서비스**)**를 선택합니다.

그림 *7:* 결과



(필요한 경우) 방화벽 전원 끄기

시스템을 올바르게 종료하는 것이 중요합니다. 단순히 전원을 분리하거나 전원 스위치를 누르는 경우 파일 시스템이 심각하게 손상될 수 있습니다. 항상 백그라운드에서 많은 프로세스가 실행되므로 전원을 분리하거나 종료하면 방화벽 시스템이 정상적으로 종료되지 않습니다.

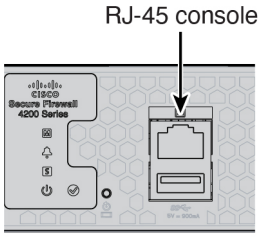
CLI에서 방화벽 전원 끄기

FXOS를 사용하여 시스템을 안전하게 종료하고 Firewall의 전원을 끌 수 있습니다.

프로시저

단계 **1** 콘솔 포트에 연결합니다.

그림 ***8:*** 콘솔 포트



단계 **2** FXOS CLI 에서 local-mgmt에 연결합니다.

Firepower # **connect local-mgmt**

단계 **3** 시스템을 종료합니다.

firepower(local-mgmt) # **shutdown**

예제**:**

```
firepower(local-mgmt)# shutdown
This command will shutdown the system.  Continue?
Please enter 'YES' or 'NO': yes
INIT: Stopping Cisco Threat Defense......ok
```

단계 **4** 방화벽이 종료될 때 시스템 프롬프트를 모니터링합니다. 종료가 완료되면 다음 프롬프트가 표시됩니다.

```
System is stopped.
It is safe to power off now.
Do you want to reboot instead? [y/N]
```

단계 **5** 새시가 성공적으로 꺼진 후에 필요한 경우 새시에서 전원을 분리하여 물리적으로 제거할 수 있습니다.

Management Center를 사용하여 Firewall 전원 끄기

Firewall Management Center를 사용하여 시스템을 올바르게 종료할 수 있습니다.

프로시저

단계 **1** 방화벽을 종료합니다.

a) **Devices(**디바이스**)** > **Device Management(**디바이스 관리**)**를 선택합니다.
b) 다시 시작할 디바이스 옆의 편집( )을 클릭합니다.
c) **Device(**디바이스**)** 탭을 클릭합니다.

d) **System(**시스템**)** 섹션에서 디바이스 종료()을 클릭합니다.

e) 메시지가 표시되면 디바이스 종료를 확인합니다.

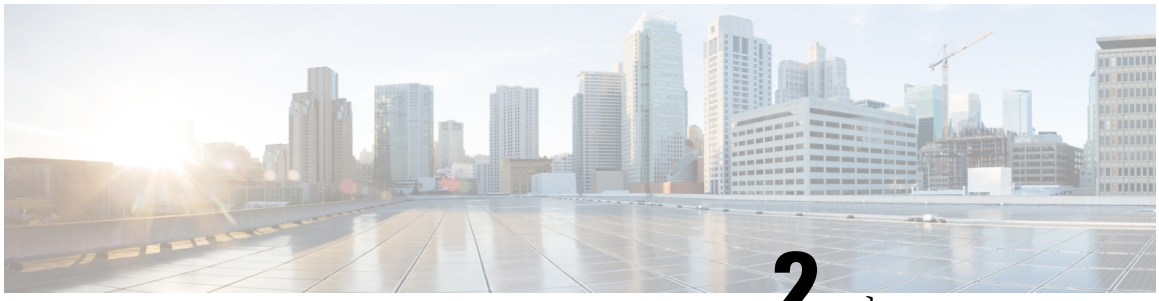
단계 **2** 방화벽에 대한 콘솔 연결이 있는 경우 방화벽이 종료될 때 시스템 프롬프트를 모니터링합니다. 셧다운이 완료되면 다음 프롬프트가 표시됩니다.

```
System is stopped.
It is safe to power off now.

Do you want to reboot instead? [y/N]
```

콘솔에 연결되지 않은 경우 시스템이 종료될 때까지 약 3분 동안 기다리십시오.

단계 **3** 섀시가 성공적으로 꺼진 후에 필요한 경우 섀시에서 전원을 분리하여 물리적으로 제거할 수 있습니다.



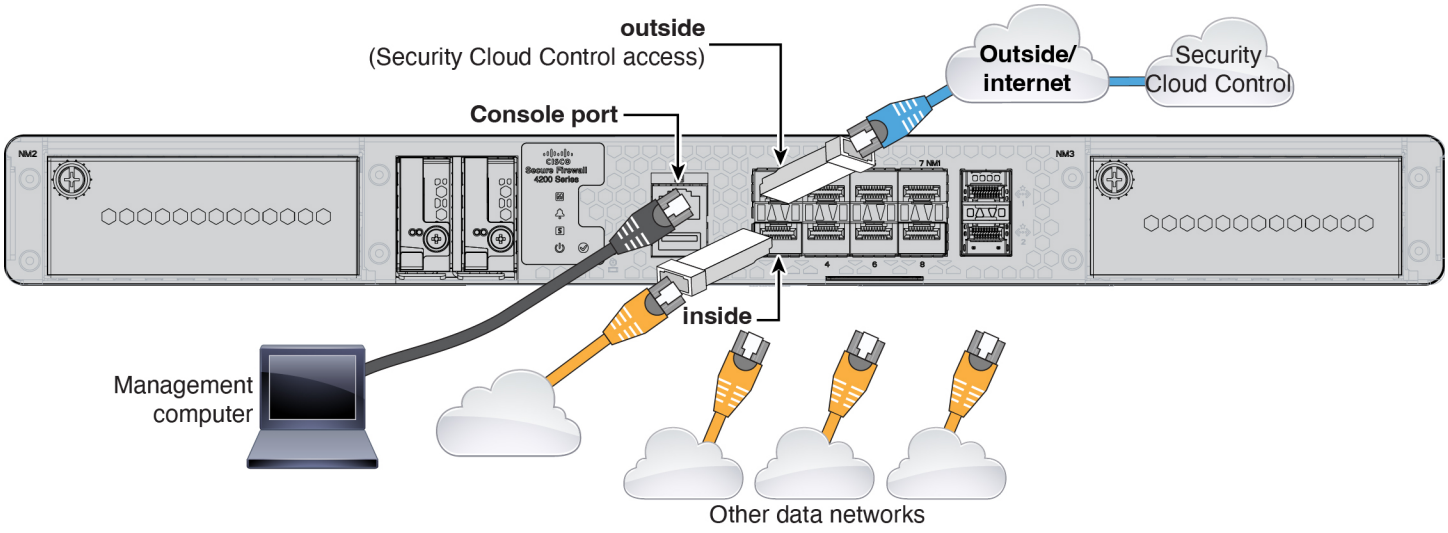
2 장

방화벽 케이블 연결 및 온보딩

Security Cloud Control에 방화벽을 케이블로 연결하고 온보딩합니다.

방화벽 케이블 연결

- 콘솔 케이블 준비 - 방화벽은 기본적으로 콘솔 케이블과 함께 제공되지 않으므로 예를 들어 타사 USB-RJ-45 직렬 케이블을 구매해야 합니다.
- 데이터 인터페이스 포트에 SFP 설치 - 기본 제공 포트는 SFP 모듈이 필요한 1/10/25-Gbps SFP 포트입니다.
- 자세한 내용은 하드웨어 설치 가이드를 참조하십시오.



방화벽 온보딩

CLI 등록 키를 사용하여 방화벽을 본보딩합니다.

프로시저

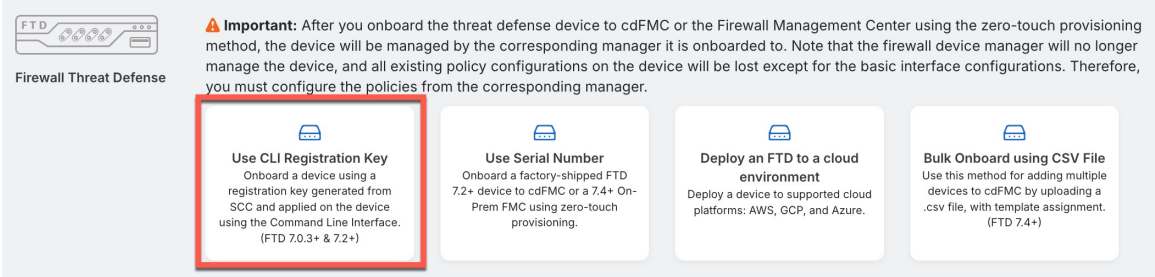
단계 **1** Security Cloud Control 탐색 메뉴에서 보안 디바이스를 클릭한 다음 파란색 더하기 버튼(+)을 클릭하여 디바이스를 온보딩합니다.

단계 **2** **FTD tile(**타일**)**을 클릭합니다.

단계 **3** **Management Mode(**관리 모드**)**에서 **FTD**가 선택되어 있는지 확인합니다.

단계 **4** 온보딩 방법으로 **Use CLI Registration Key(CLI** 등록 키 사용**)**를 선택합니다.

그림 ***9: CLI*** 등록 키 사용

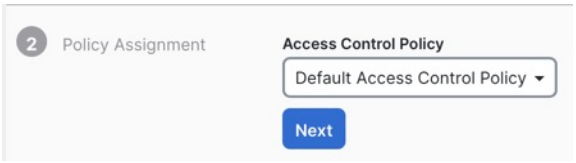


단계 **5** **Device Name(**디바이스 이름**)**을 입력하고 **Next(**다음**)**를 클릭합니다.

그림 ***10: Device Name(***디바이스 이름***)***

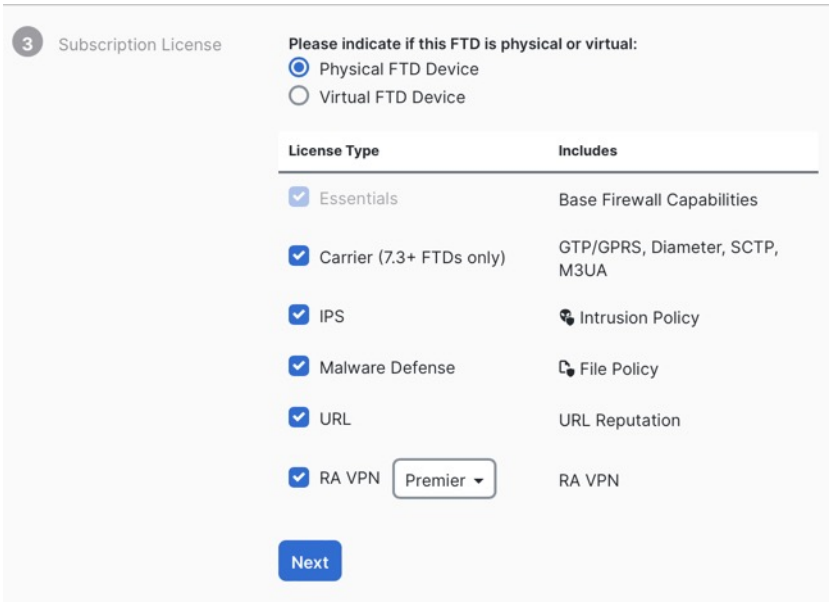
단계 **6** **Policy Assignment(**정책 할당**)**에서 드롭다운 메뉴를 사용하여 디바이스에 대한 액세스 제어 정책을 선택합니다. 구성된 정책이 없는 경우 **Default Access Control Policy(**기본 액세스 제어 정책**)**를 선택합니다.

그림 ***11:*** 액세스 제어 정책



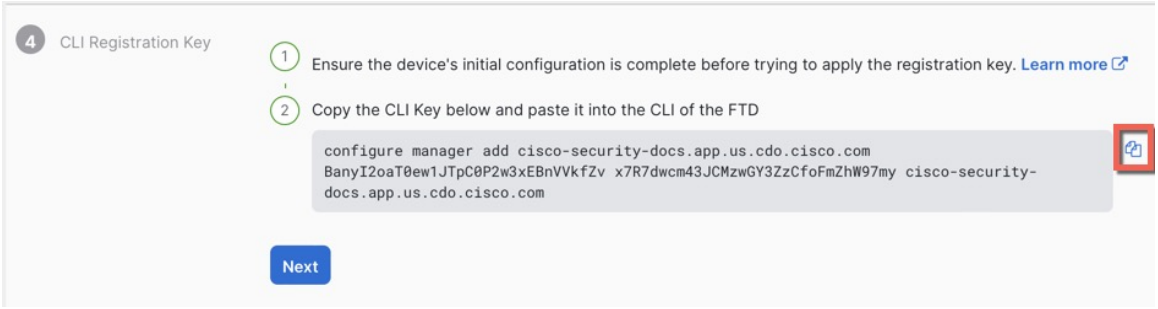
단계 **7** 구독 라이선스의 경우, **Physical FTD Device(**물리적 **FTD** 디바이스**)** 라디오 버튼을 클릭한 다음 활성화하려는 각 기능 라이선스를 선택합니다. **Next(**다음**)**를 클릭합니다.

그림 *12:* 구독 라이선스



단계 **8** **CLI** 등록 키의 경우 Security Cloud Control는 등록 키 및 기타 매개 변수를 사용하여 명령을 생성합니다. 이 명령을 복사하여 Firewall Threat Defense의 초기 구성에서 사용해야 합니다.

그림 *13: CLI* 등록 키



configure manager add Security Cloud Control_*hostname registration_key nat_id display_name*

시작 스크립트를 완료한 후 Firewall Threat Defense CLI에서 이 명령을 복사합니다. 초기 구성 수행, 14 페이지의 내용을 참조하십시오.

예제**:**

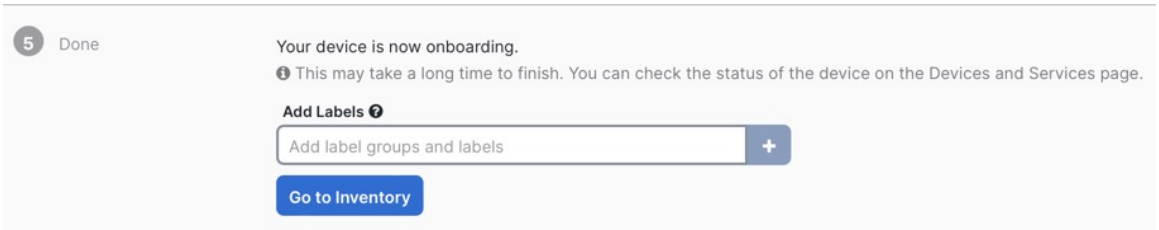
CLI 설정을 위한 샘플 명령:

```
configure manager add account1.app.us.scc.cisco.com KPOOP0rgWzaHrnj1V5ha2q5Rf8pKFX9E
Lzm1HOynhVUWhXYWz2swmkj2ZWsN3Lb account1.app.us.scc.cisco.com
```

단계 **9** 온보딩 마법사에서 **Next(**다음**)**를 클릭하여 디바이스 등록을 시작합니다.

단계 **10** (선택 사항) **Security Devices(**보안 디바이스**)** 페이지를 정렬하고 필터링하는 데 도움이 되도록 디바이스에 레이블을 추가합니다. 레이블을 입력하고 파란색 더하기 버튼( )을 선택합니다. 레이블은 Security Cloud Control에 온보딩된 후 디바이스에 적용됩니다.

그림 ***14:*** 완료



초기 구성 수행

CLI 설정 스크립트를 사용하여 전용 관리 IP 주소, 게이트웨이 및 기타 기본 네트워킹 설정을 설정합니다.

프로시저

단계 **1** Firewall Threat Defense 및 ASA CLI에 액세스하기 위해 콘솔 포트에 연결 Firewall Threat Defense CLI에 액세스, 4 페이지을 참조하십시오.

단계 **2** 그러면 관리 인터페이스 설정을 위한 CLI 설정 스크립트가 표시됩니다.

참고
이미지 재설치 등을 통해 구성을 지우지 않으면 CLI 설정 스크립트를 반복할 수 없습니다. 그러나 이러한 모든 설정은 **configure network(**네트워크 구성**)** 명령을 사용하여 CLI에서 나중에 변경할 수 있습니다. *Cisco Secure Firewall Threat Defense* 명령 참조의 내용을 참조하십시오.

```
You must accept the EULA to continue.
Press <ENTER> to display the EULA:
Cisco General Terms
[...]

Please enter 'YES' or press <ENTER> to AGREE to the EULA:

System initialization in progress.  Please stand by.
You must configure the network to continue.
Configure at least one of IPv4 or IPv6 unless managing via data interfaces.
Do you want to configure IPv4? (y/n) [y]:
Do you want to configure IPv6? (y/n) [y]: n
```

지침**:** 다음 주소 유형 중 하나 이상에 대해 **y**를 입력합니다.관리 인터페이스를 사용할 계획은 없지만 IP 주소(예: 개인 주소)를 설정해야 합니다.

```
Configure IPv4 via DHCP or manually? (dhcp/manual) [manual]:
```

지침: **manual(**수동**)**을 선택합니다. 관리자 액세스용 외부 인터페이스를 사용할 때는 DHCP가 지원되지 않습니다. 라우팅 문제를 방지하기 위해 이 인터페이스가 관리자 액세스 인터페이스와 다른 서브넷에 있는지 확인하십시오.

```
Enter an IPv4 address for the management interface [192.168.45.61]: 10.89.5.17
Enter an IPv4 netmask for the management interface [255.255.255.0]: 255.255.255.192
Enter the IPv4 default gateway for the management interface [data-interfaces]:
```

지침: 게이트웨이를 **data-interfaces**로 설정합니다. 이 설정은 관리 트래픽을 백플레인을 통해 포워딩하므로 외부 인터페이스를 통해 라우팅될 수 있습니다.

```
Enter a fully qualified hostname for this system [firepower]: 1010-3
Enter a comma-separated list of DNS servers or 'none' [208.67.222.222,208.67.220.220,2620:119:35::35]:
Enter a comma-separated list of search domains or 'none' []: cisco.com
If your networking information has changed, you will need to reconnect.
Disabling IPv6 configuration: management0
Setting DNS servers: 208.67.222.222,208.67.220.220,2620:119:35::35
Setting DNS domains:cisco.com
```

지침: 관리 인터페이스 DNS 서버를 설정합니다. 외부 인터페이스에서 액세스하므로 나중에 설정하는 외부 인터페이스 DNS 서버와 일치할 수 있습니다.

```
Setting hostname as 1010-3
Setting static IPv4: 10.89.5.17 netmask: 255.255.255.192 gateway: data on management0
Updating routing tables, please wait...
All configurations applied to the system. Took 3 Seconds.
Saving a copy of running network configuration to local disk.
For HTTP Proxy configuration, run 'configure network http-proxy'
```

```
Setting hostname as 1010-3
Setting static IPv4: 10.89.5.17 netmask: 255.255.255.192 gateway: data on management0
Updating routing tables, please wait...
All configurations applied to the system. Took 3 Seconds.
Saving a copy of running network configuration to local disk.
For HTTP Proxy configuration, run 'configure network http-proxy'
```

지침: **routed**를 입력합니다. 외부 관리자 액세스는 라우팅 방화벽 모드에서만 지원됩니다.

```
Configuring firewall mode ...


Device is in OffBox mode - disabling/removing port 443 from iptables.
Update policy deployment information
    - add device configuration
    - add network discovery
    - add system policy

You can register the sensor to a Firepower Management Center and use the
Firepower Management Center to manage it. Note that registering the sensor
to a Firepower Management Center disables on-sensor Firepower Services
management capabilities.

When registering the sensor to a Firepower Management Center, a unique
alphanumeric registration key is always required.  In most cases, to register
a sensor to a Firepower Management Center, you must provide the hostname or
the IP address along with the registration key.
'configure manager add [hostname | ip address ] [registration key ]'

However, if the sensor and the Firepower Management Center are separated by a
NAT device, you must enter a unique NAT ID, along with the unique registration
key.
'configure manager add DONTRESOLVE [registration key ] [ NAT ID ]'

Later, using the web interface on the Firepower Management Center, you must
```

```
use the same registration key and, if necessary, the same NAT ID when you add
this sensor to the Firepower Management Center.
>
```

단계 **3** 관리자 액세스를 위한 외부 인터페이스를 구성합니다.

configure network management-data-interface

Enter를 누르면 외부 인터페이스에 대한 기본 네트워크 설정을 구성하라는 메시지가 표시됩니다.

수동 **IP** 주소

```
> configure network management-data-interface
Data interface to use for management: ethernet1/1
Specify a name for the interface [outside]: internet
IP address (manual / dhcp) [dhcp]: manual
IPv4/IPv6 address: 10.10.6.7
Netmask/IPv6 Prefix: 255.255.255.0
Default Gateway: 10.10.6.1
Comma-separated list of DNS servers [none]: 208.67.222.222,208.67.220.220
```

지침**:** 등록 후 외부 DNS 서버를 유지하려면 Firewall Management Center에서 DNS 플랫폼 설정을 다시 구성해야 합니다.

```
DDNS server update URL [none]:
Do you wish to clear all the device configuration before applying ? (y/n) [n]:

Configuration done with option to allow manager access from any network, if you wish to change the manager
 access network
use the 'client' option in the command 'configure network management-data-interface'.

Setting IPv4 network configuration.
Network settings changed.

>
```

DHCP로부터 할당된 **IP** 주소

```
> configure network management-data-interface
Data interface to use for management: ethernet1/1
Specify a name for the interface [outside]:
IP address (manual / dhcp) [dhcp]:
DDNS server update URL [none]:
https://dwinchester:pa$$w0rd17@domains.example.com/nic/update?hostname=<h>&myip=<a>
Do you wish to clear all the device configuration before applying ? (y/n) [n]:

Configuration done with option to allow manager access from any network, if you wish to change the manager
 access network
use the 'client' option in the command 'configure network management-data-interface'.

Setting IPv4 network configuration.
Network settings changed.

>
```

단계 **4** Security Cloud Control에서 생성한 **configure manager add** 명령을 사용하여 이 Firewall Threat Defense를 관리할 Security Cloud Control를 식별합니다. 명령을 생성하려면 방화벽 온보딩, 12 페이지의 내용을 참조하십시오.

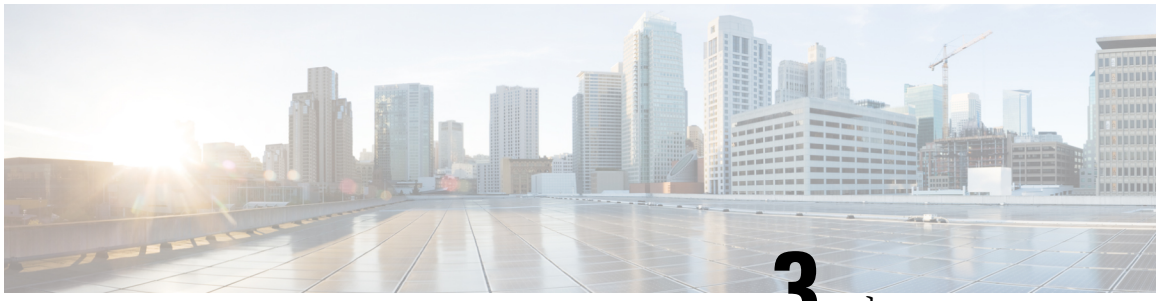
예제**:**

```
> configure manager add account1.app.us.cdo.cisco.com KPOOP0rgWzaHrnj1V5ha2q5Rf8pKFX9E
Lzm1HOynhVUWhXYWz2swmkj2ZWsN3Lb account1.app.us.cdo.cisco.com
Manager successfully configured.
```

단계 **5** 원격 지사로 디바이스를 전송할 수 있도록 Firewall Threat Defense를 종료합니다.

시스템을 올바르게 종료하는 것이 중요합니다. 단순히 전원을 분리하거나 전원 스위치를 누르는 경우 파일 시스템이 심각하게 손상될 수 있습니다. 항상 백그라운드에서 많은 프로세스가 실행되므로 전원을 분리하거나 종료하면 Firepower 시스템이 정상적으로 종료되지 않는다는 점에 유의하십시오.

a) **shutdown** 명령을 입력합니다.
b) 전원 LED 및 상태 LED를 관찰하여 섀시의 전원이 꺼져 있는지 확인합니다(LED 꺼짐).
c) 섀시가 성공적으로 꺼진 후에 필요한 경우 섀시에서 전원을 분리하여 물리적으로 제거할 수 있습니다.



3 장

기본 정책 구성

다음 설정으로 기본 보안 정책을 구성:

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

보안 정책을 사용자 지정하여 더 고급 검사를 포함시킬 수도 있습니다.

클라우드 제공 **Firewall Management Center**로 이동

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

프로시저

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

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

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

인터페이스 구성

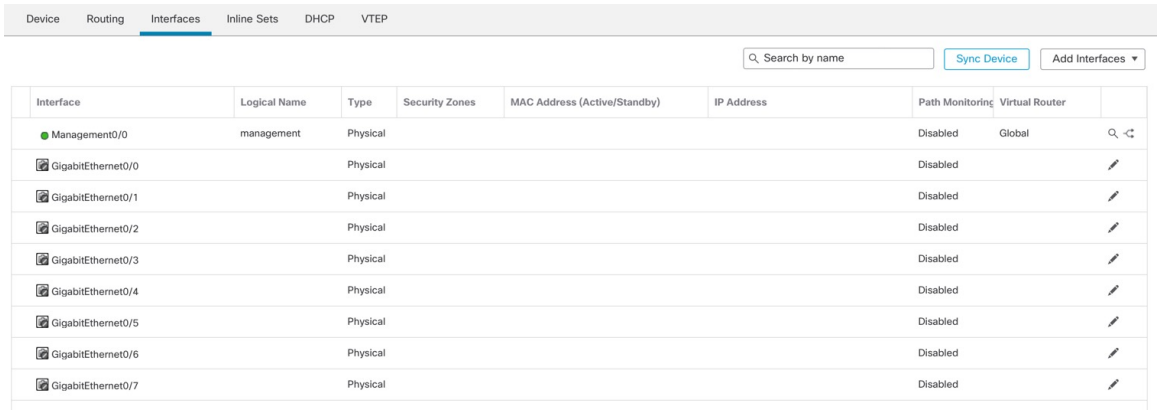
다음 예에서는 DHCP를 사용하는 외부 인터페이스에서 고정 주소 및 라우팅 모드를 사용하여 인터페이스 내부에 라우팅 모드를 구성합니다. 또한 내부 웹 서버용 DMZ 인터페이스를 추가합니다.

프로시저

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

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

그림 ***15: Interfaces***

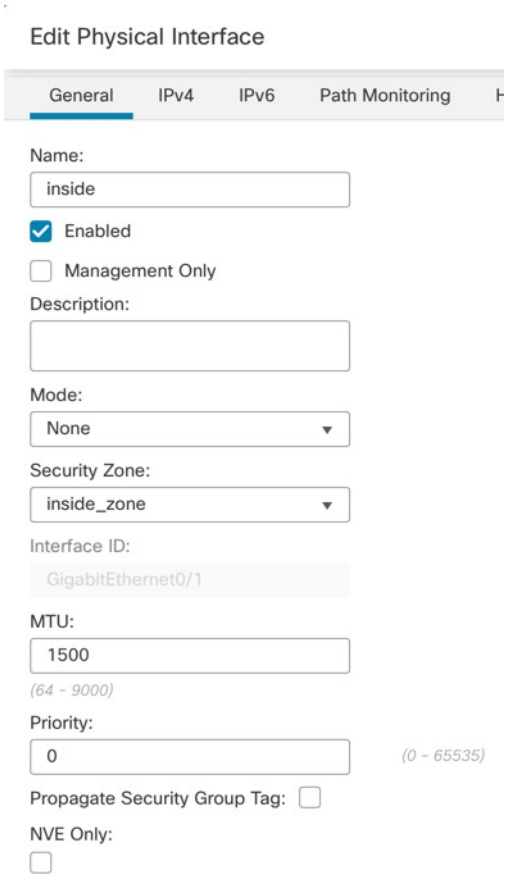


단계 **3** 40Gb 이상의 인터페이스에서 브레이크아웃 포트를 생성하려면 해당 인터페이스의 **Break** 아이콘을 클릭합니다.

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

단계 **4** 내부에 사용할 인터페이스의 편집( )를 클릭합니다.

그림 ***16:*** 일반 탭



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

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

   내부 인터페이스가 사전 구성된 경우, 나머지 필드는 선택 사항입니다.

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

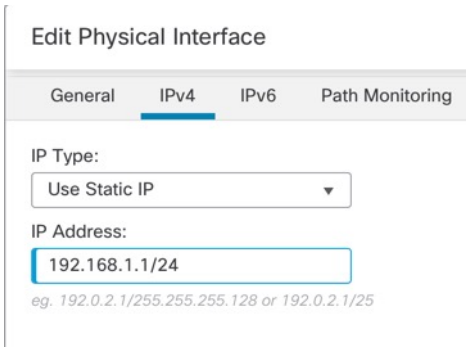
   예를 들어 인터페이스에 **inside**라는 이름을 지정합니다.

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

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

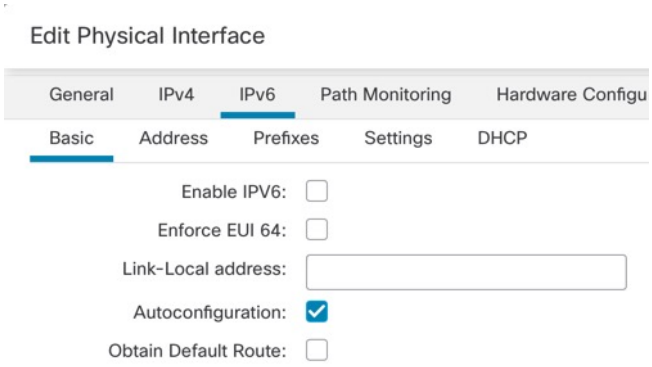
     예를 들어 **192.168.1.1/24** 를 입력합니다.

그림 ***17: IPv4*** 탭



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

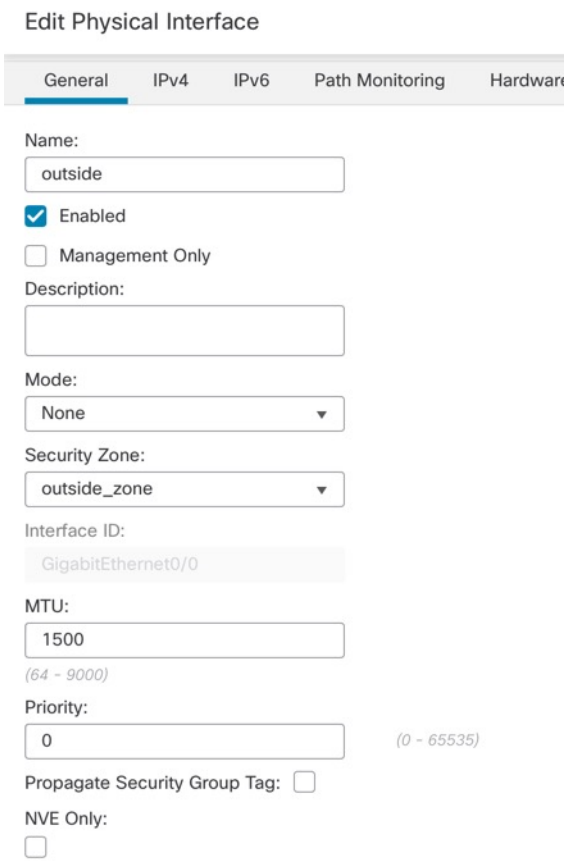
  그림 ***18: IPv6*** 탭



f) **OK(**확인**)**를 클릭합니다.

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

그림 ***19:*** 일반 탭



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

예를 들어 **outside_zone**이라는 영역을 추가합니다.

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

b) **OK(**확인**)**를 클릭합니다.

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

a) 사용하려는 인터페이스의 편집( )를 클릭합니다.

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

예를 들어 **dmz_zone**이라는 영역을 추가합니다.

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

예를 들어 인터페이스 이름을 **dmz**로 지정합니다.

d) **Enable(**활성화**)** 확인란을 선택합니다.

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

단계 **7** **Save(**저장**)**를 클릭합니다.

DHCP 서버 구성

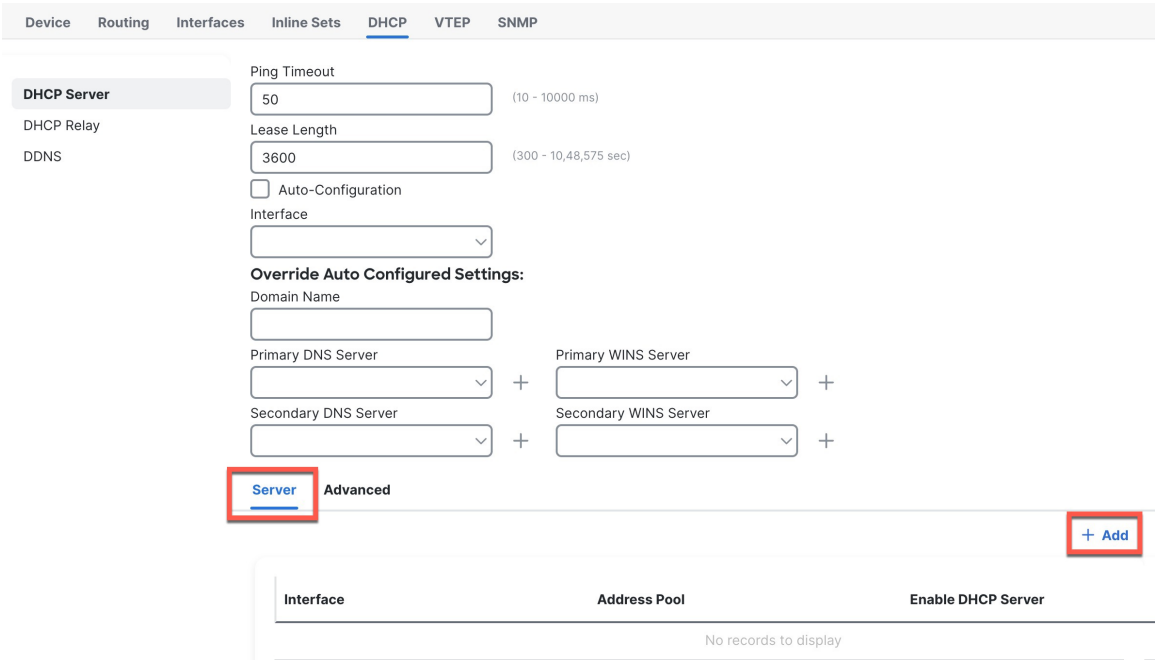
클라이언트가 DHCP를 사용하여 방화벽에서 IP 주소를 가져오게 하려면 DHCP 서버를 활성화합니다.

프로시저

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

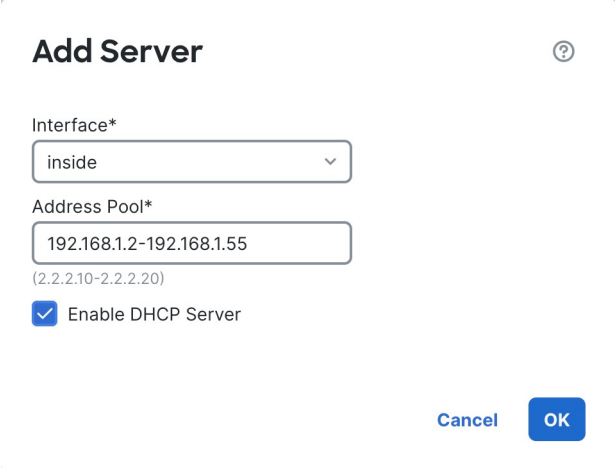
단계 **2** **DHCP** > **DHCP Server(DHCP** 서버**)**를 선택합니다.

그림 ***20: DHCP*** 서버



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

그림 *21:* 서버 추가



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

단계 **4** **OK(**확인**)**를 클릭합니다.

단계 **5** **Save(**저장**)**를 클릭합니다.

NAT 구성

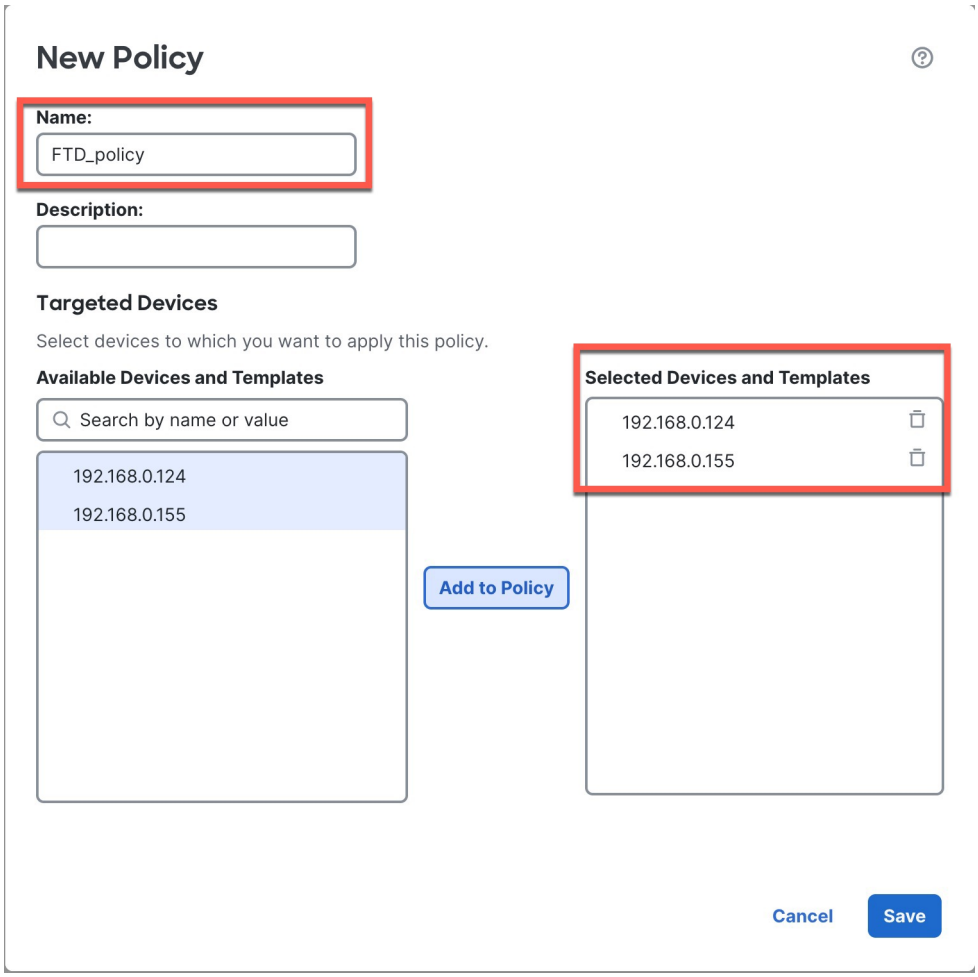
이 절차는 내부 클라이언트가 내부 주소를 외부 인터페이스 IP 주소의 포트로 변환하도록 하는 NAT 규칙을 생성합니다. 이러한 유형의 NAT 규칙을 인터페이스 포트 주소 변환*(PAT)*이라고 합니다.

프로시저

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

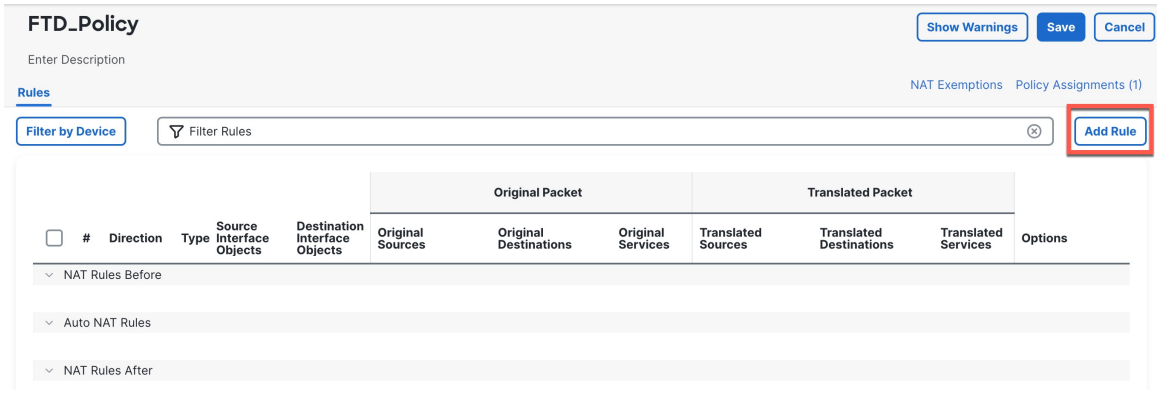
단계 **2** 정책 이름을 지정하고, 정책을 사용할 디바이스를 선택한 뒤 **Save(**저장**)**를 클릭합니다.

그림 *22:* 새 정책



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

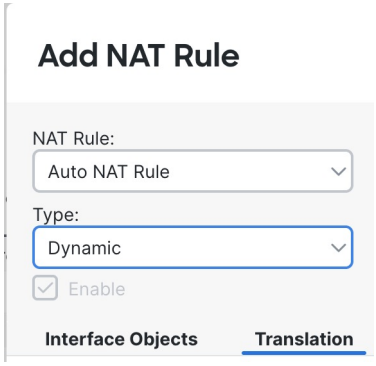
그림 *23: NAT* 정책



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

단계 **4** 기본 규칙 옵션을 구성합니다.

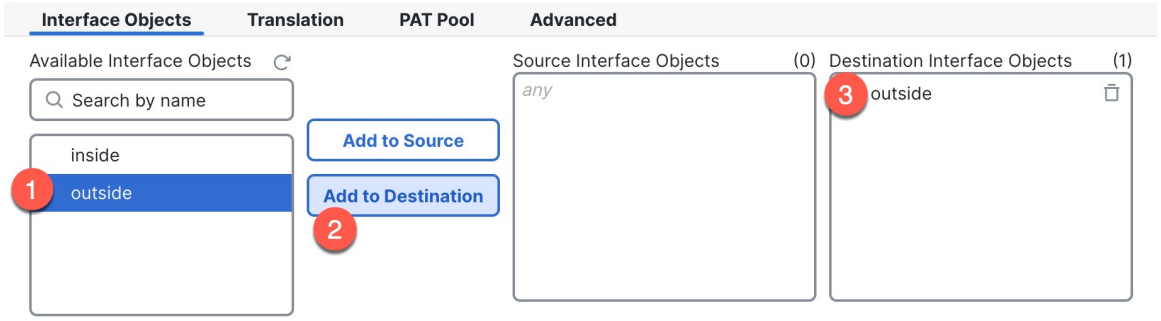
그림 ***24:*** 기본 규칙 옵션



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

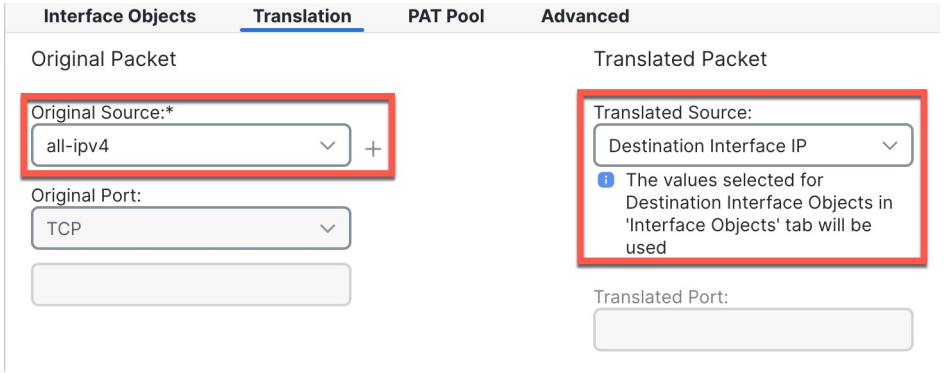
단계 **5** **Interface Objects(인터페이스 개체)** 페이지에서 **Available Interface Objects(사용 가능한 인터페이스 개체)** 영역의 외부 영역을 **Destination Interface objects(대상 인터페이스 개체)** 영역에 추가합니다.

그림 ***25:*** 인터페이스 개체



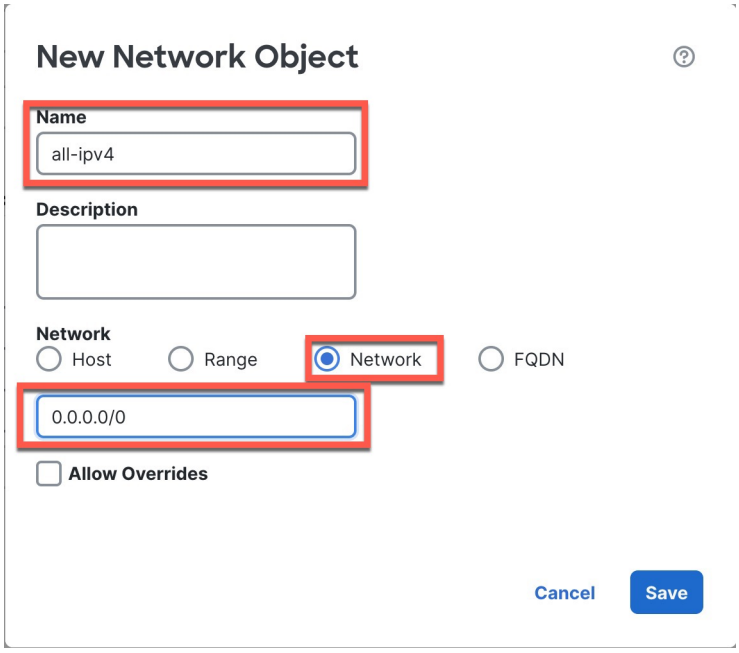
단계 **6** **Translation(변환)** 페이지에서 다음 옵션을 설정합니다.

그림 ***26:*** 변환



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

그림 ***27:*** 새 네트워크 개체



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

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

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

규칙이 **Rules(**규칙**)** 테이블에 저장됩니다.

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

액세스 제어 규칙을 구성합니다.

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

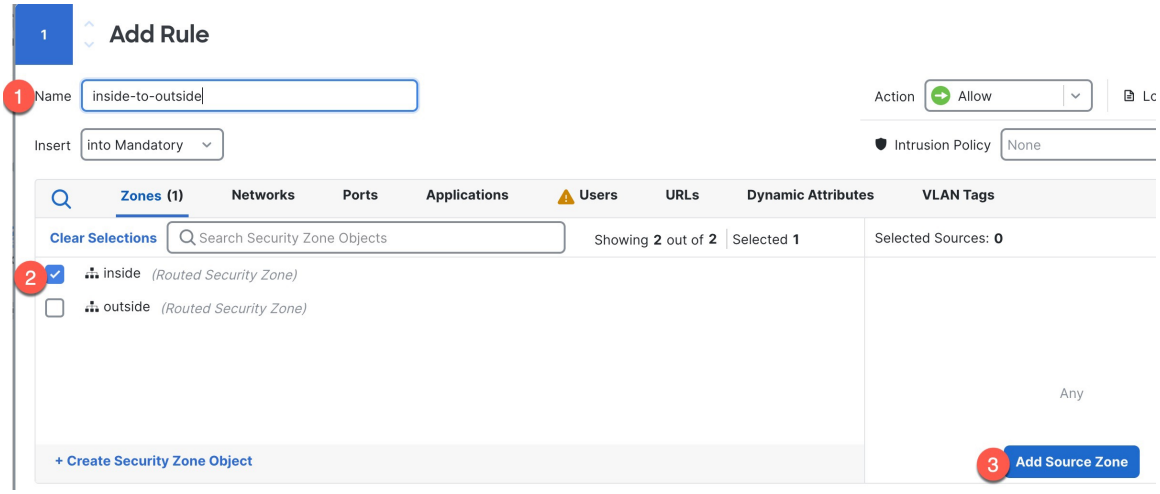
이 절차는 내부 영역에서 외부 영역으로의 모든 트래픽을 허용하는 액세스 제어 규칙을 생성합니다.

프로시저

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

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

그림 ***28:*** 소스 영역

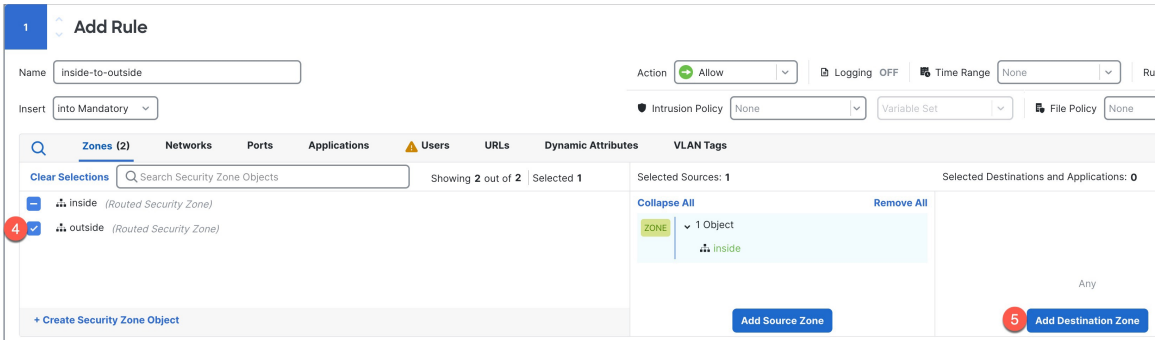


1. 예를 들어 이 규칙의 이름을 **inside-to-outside**로 지정합니다.

2. Zones(영역**)**에서 내부 영역을 선택합니다.

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

그림 ***29:*** 대상 영역



4 . Zones(영역**)**에서 외부 영역을 선택합니다.

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

기타 설정은 변경하지 않습니다.

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

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

그림 ***30:*** 액세스 제어 전에 적용된 정책

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

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

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

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

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

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

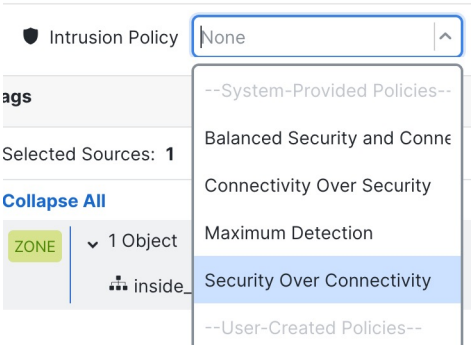
- **ID** - ID는 기본적으로 적용되지 않습니다. 액세스 제어 정책에 따라 트래픽을 처리하도록 허용하기 전에 사용자에게 인증을 요구할 수 있습니다.

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

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

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

그림 *31:* 시스템 제공 침입 정책

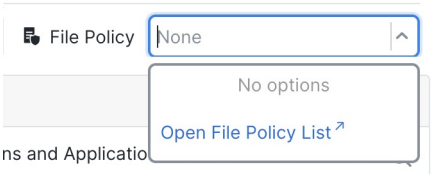


b) 목록에서 시스템 제공 정책 중 하나를 선택합니다.

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

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

그림 *32:* 파일 정책



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

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

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

단계 **6** **Apply(**적용**)**를 클릭합니다.

규칙이 **Rules(**규칙**)** 테이블에 추가됩니다.

단계 **7** **Save(**저장**)**를 클릭합니다.

외부 인터페이스에서 SSH 활성화

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

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

프로시저

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

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

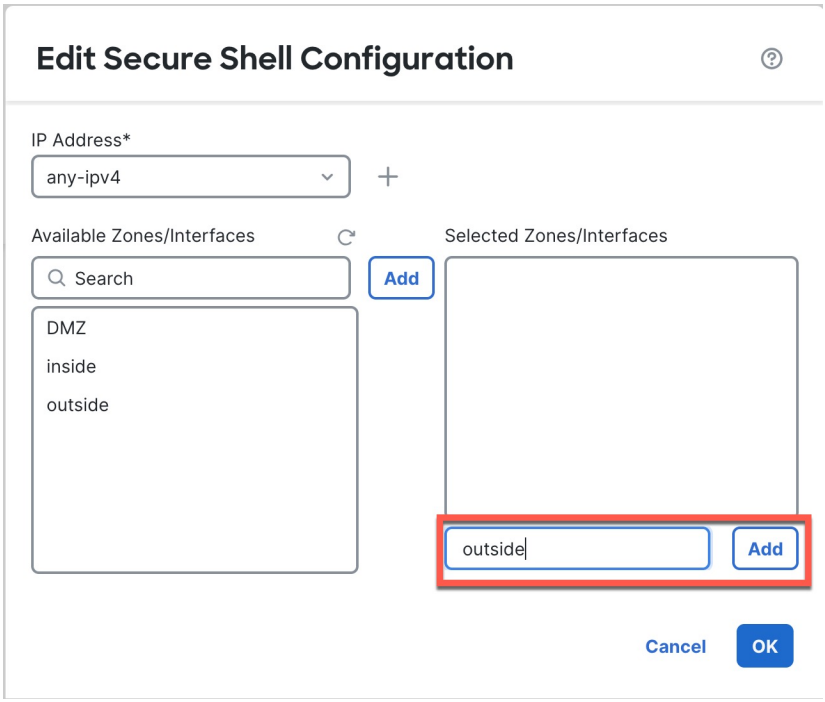
단계 3 SSH 연결을 허용하는 외부 인터페이스와 IP 주소를 확인합니다.

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

b) 규칙 속성을 구성합니다.

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

그림 ***33:*** 외부 인터페이스에서 ***SSH*** 활성화



c) **OK(**확인**)**를 클릭합니다.

단계 4 **Save(**저장**)**를 클릭합니다.

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

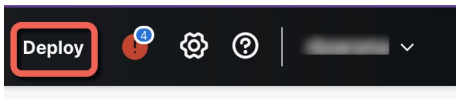
구성 구축

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

프로시저

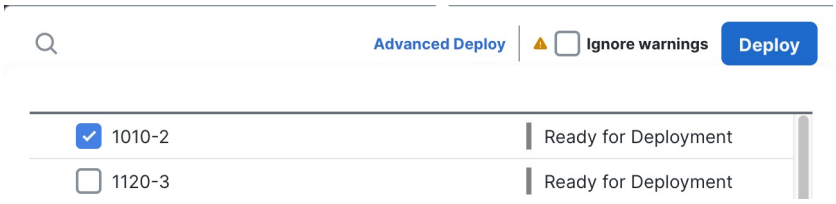
단계 **1** 우측 상단에서 **Deploy(구축)**를 클릭합니다.

그림 ***34:*** 구축



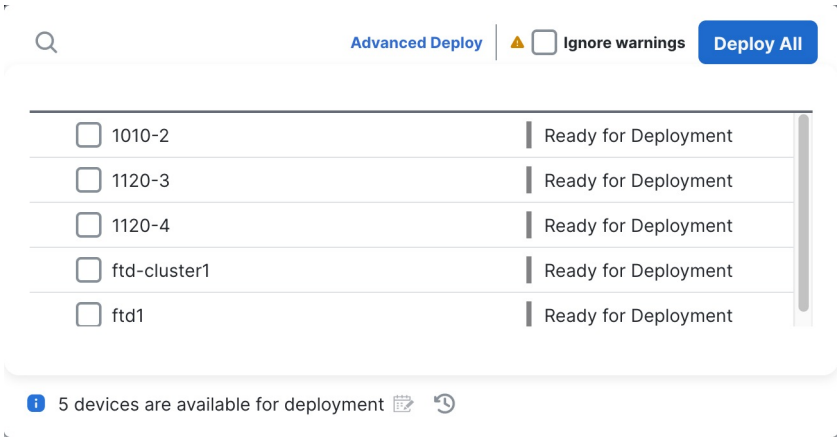
단계 **2** 빠르게 구축하려면 특정 디바이스를 선택한 다음 **Deploy(구축)**를 클릭합니다.

그림 ***35:*** 선택 항목 구축



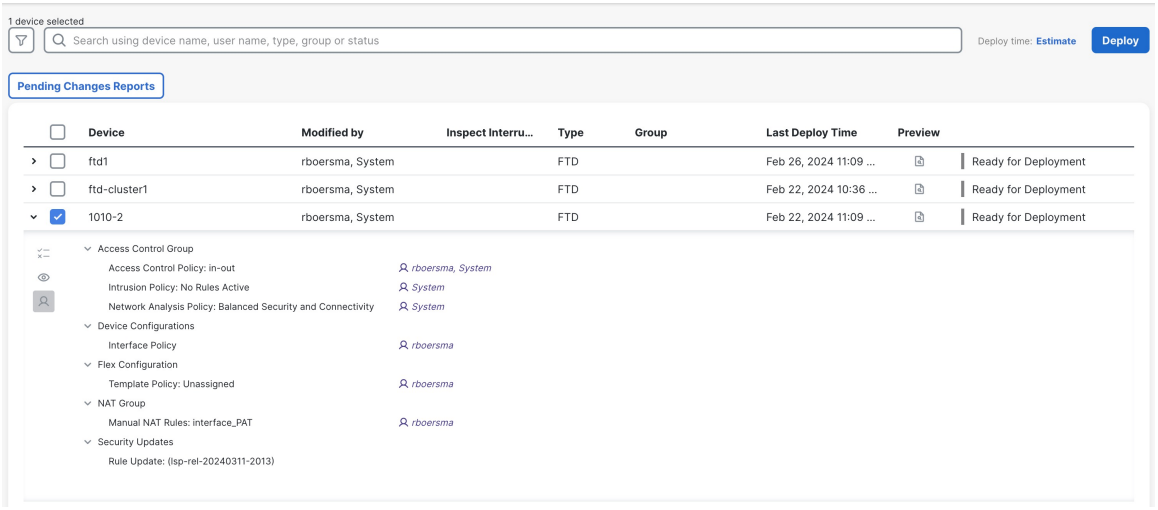
또는 **Deploy All(모두 구축)**을 클릭하여 모든 디바이스에 구축합니다.

그림 ***36:*** 모두 구축



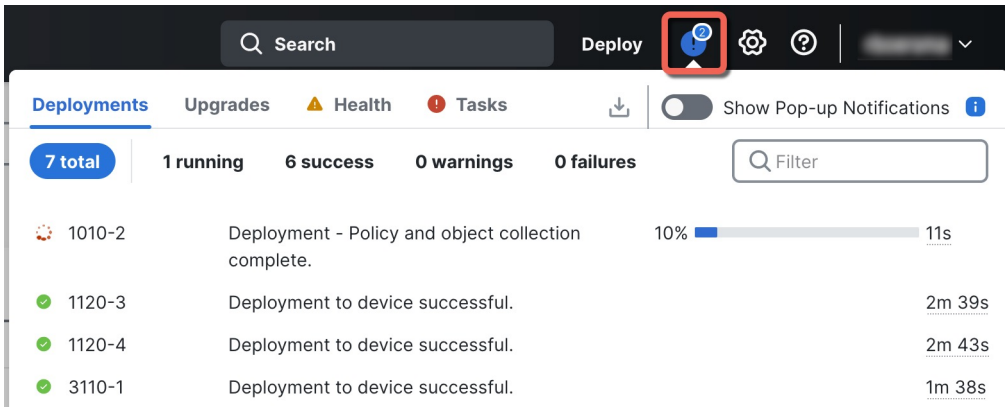
그렇지 않으면 추가 구축 옵션에 대해 Advanced Deploy(고급 구축)를 클릭합니다.

그림 ***37:*** 고급 구축



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

그림 ***38:*** 구축 상태



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