



Threat Defense 원격으로 구축 Management Center

이 장의 설명이 유용합니까?

사용 가능한 모든 애플리케이션 및 관리자를 보려면 [귀하에게 적합한 애플리케이션 및 관리자는 무엇입니까?](#)의 내용을 참조하십시오. 이 장은 management center Threat Defense 에 적용됩니다.

이 장에서는 Threat Defense 를 중앙 본사에 있는 management center를 사용하여 관리하는 방법을 설명합니다. 로컬 관리 네트워크에서 management center가 상주하는 로컬 구축의 경우, [Management Center 로 Threat Defense 구축](#)의 내용을 참조하십시오.

방화벽 정보

하드웨어는 ASA 소프트웨어 또는 threat defense 소프트웨어를 실행할 수 있습니다. ASA와 threat defense 간 전환하려면 디바이스에 이미지를 재설치해야 합니다. 현재 설치된 것과 다른 소프트웨어 버전이 필요한 경우에도 이미지를 재설치해야 합니다. [Cisco Secure Firewall ASA 및 Secure Firewall Threat Defense 이미지 재설치 가이드](#)의 내용을 참조하십시오.

방화벽은 Secure Firewall eXtensible Operating System(FXOS)라는 기본 운영 체제를 실행합니다. 방화벽은 FXOS Secure Firewall 새시 관리자를 지원하지 않습니다. 문제 해결을 위해 제한된 CLI만 지원됩니다. 자세한 내용은 [Cisco Firepower 1000/2100 및 Firepower Threat Defense 기능이 있는 Threat Defense 3100/4200용 Cisco FXOS 문제 해결 가이드](#)을 참조하십시오.

Privacy Collection Statement(개인정보 수집 선언)—방화벽은 개인 식별 정보를 요구하거나 적극적으로 수집하지 않습니다. 그러나 구성에서 개인 식별이 가능한 정보(예: 사용자 이름)를 사용할 수 있습니다. 이 경우 관리자는 해당 설정으로 작업하거나 SNMP를 사용할 때 이 정보를 확인할 수도 있습니다.

- [원격 관리 작동 방식, 2 페이지](#)
- [시작하기 전에, 4 페이지](#)
- [엔드 투 엔드 작업, 4 페이지](#)
- [중앙 관리자 사전 구성, 6 페이지](#)
- [지사 설치, 13 페이지](#)
- [중앙 관리자 사후 구성, 15 페이지](#)

원격 관리 작동 방식

management center에서 인터넷을 통해 threat defense를 관리할 수 있도록 하려면 관리 인터페이스 대신 management center 관리 액세스용 외부 인터페이스를 사용합니다. 대부분의 원격 브랜치 오피스에서는 단일 인터넷 연결만 가능하므로 외부 관리자 액세스를 통해 중앙 집중식 관리가 가능합니다.



참고 관리 연결은 자신과 디바이스 사이의 보안 TLS-1.3 암호화 통신 채널입니다. 보안을 위해 사이트 간 VPN과 같은 추가 암호화 터널을 통해 이 트래픽을 실행할 필요가 없습니다. 예를 들어 VPN이 다운되면 관리 연결이 끊어지므로 간단한 관리 경로를 사용하는 것이 좋습니다.

1. CLI에서 threat defense를 사전 구성한 다음 threat defense를 브랜치 오피스로 보냅니다.
2. 브랜치 오피스에서 Threat Defense 의 케이블을 연결하고 전원을 켭니다.
3. management center를 사용하여 Threat Defense 등록을 완료합니다.

Threat Defense 관리자 액세스 인터페이스

이 설명서는 원격 브랜치 오피스에 대한 시나리오이므로 외부 인터페이스 액세스를 다룹니다. 관리자 액세스는 외부 인터페이스에서 발생하지만 여전히 전용 관리 인터페이스와 관련이 있습니다. 관리 인터페이스는 threat defense 데이터 인터페이스와 별도로 구성된 특수 인터페이스이며 자체 네트워크 설정이 있습니다.

- 데이터 인터페이스에서 관리자 액세스를 활성화하더라도 관리 인터페이스 네트워크 설정은 계속 사용됩니다.
- 모든 관리 트래픽은 계속해서 관리 인터페이스에서 제공되거나 관리 인터페이스로 전송됩니다.
- 데이터 인터페이스에서 관리자 액세스를 활성화하면 threat defense는 수신 인터페이스를 백플레인을 통해 관리 인터페이스로 전달합니다.
- 발신 관리 트래픽의 경우 관리 인터페이스는 백플레인을 통해 데이터 인터페이스로 트래픽을 전달합니다.

관리자 액세스 요구 사항

데이터 인터페이스에서의 관리자 액세스에는 다음과 같은 제한이 있습니다.

- 물리적 데이터 인터페이스에서만 관리자 액세스를 활성화할 수 있습니다. 하위 인터페이스 또는 EtherChannel은 사용할 수 없습니다. 또한 management center를 사용하여 리던던시(redundancy)를 위해 단일 보조 인터페이스에서 관리자 액세스를 활성화할 수 있습니다.
- 이 인터페이스는 관리 전용일 수 없습니다.
- 라우팅 인터페이스를 사용하는 라우팅 방화벽 모드 전용입니다.

- PPPoE는 지원되지 않습니다. ISP에 PPPoE가 필요한 경우 threat defense와 WAN 모듈 간에 PPPoE를 지원하는 라우터를 설치해야 합니다.
- 인터페이스는 전역 VRF에만 있어야 합니다.
- SSH는 데이터 인터페이스에 대해 기본적으로 활성화되어 있지 않으므로 나중에 management center를 사용하여 SSH를 활성화해야 합니다. 관리 인터페이스 게이트웨이가 데이터 인터페이스로 변경되므로, **configure network static-routes** 명령을 사용하여 관리 인터페이스에 대한 고정 경로를 추가하지 않는 한 원격 네트워크에서 관리 인터페이스로 SSH 연결할 수도 없습니다.
- 별도의 관리 및 이벤트 전용 인터페이스를 사용할 수 없습니다.
- 클러스터링은 지원되지 않습니다. 이 경우에는 관리 인터페이스를 사용해야 합니다.

고가용성 요구 사항

디바이스 고가용성이 있는 데이터 인터페이스를 사용하는 경우 다음 요구 사항을 참조하십시오.

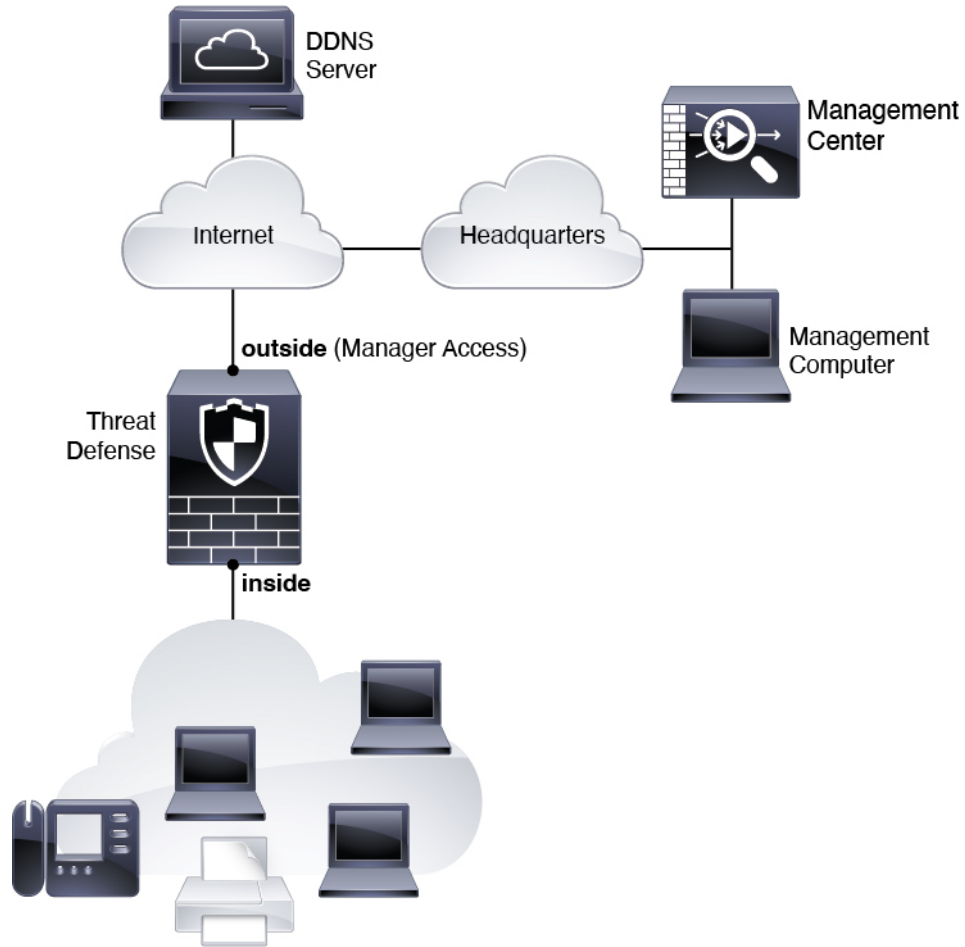
- 관리자 액세스를 위해 두 디바이스에서 동일한 데이터 인터페이스를 사용합니다.
- 이중화 관리자 액세스 데이터 인터페이스는 지원되지 않습니다.
- DHCP를 사용할 수 없습니다. 정적 IP 주소만 지원됩니다. DDNS 및 제로 터치 프로비저닝을 포함하여 DHCP에 의존하는 기능은 사용할 수 없습니다.
- 동일한 서브넷에 서로 다른 고정 IP 주소가 있어야 합니다.
- IPv4 또는 IPv6을 사용하십시오. 둘 다 설정할 수 없습니다.
- 동일한 관리자 구성(**configure manager add** 명령)을 사용하여 연결이 동일한지 확인하십시오.
- 장애 조치 또는 상태 링크로 데이터 인터페이스를 사용할 수 없습니다.

원격 브랜치 네트워크

다음 그림에는 다음과 같은 방화벽에 대한 일반적인 네트워크 구축이 나와 있습니다.

- management center는 중앙 본사에 있습니다.
- threat defense는 관리자 액세스를 위한 외부 인터페이스를 사용합니다.
- threat defense 또는 management center는 인바운드 관리 연결을 허용하기 위해 또는 공용 IP 주소 또는 호스트 이름이 필요하며 초기 설정을 위해 이 IP 주소를 알아야 합니다. 변경 사항에 따라 DHCP IP 할당을 수용하도록 외부 인터페이스에 대해 DDNS(Dynamic DNS)를 선택적으로 구성할 수도 있습니다.

그림 1:



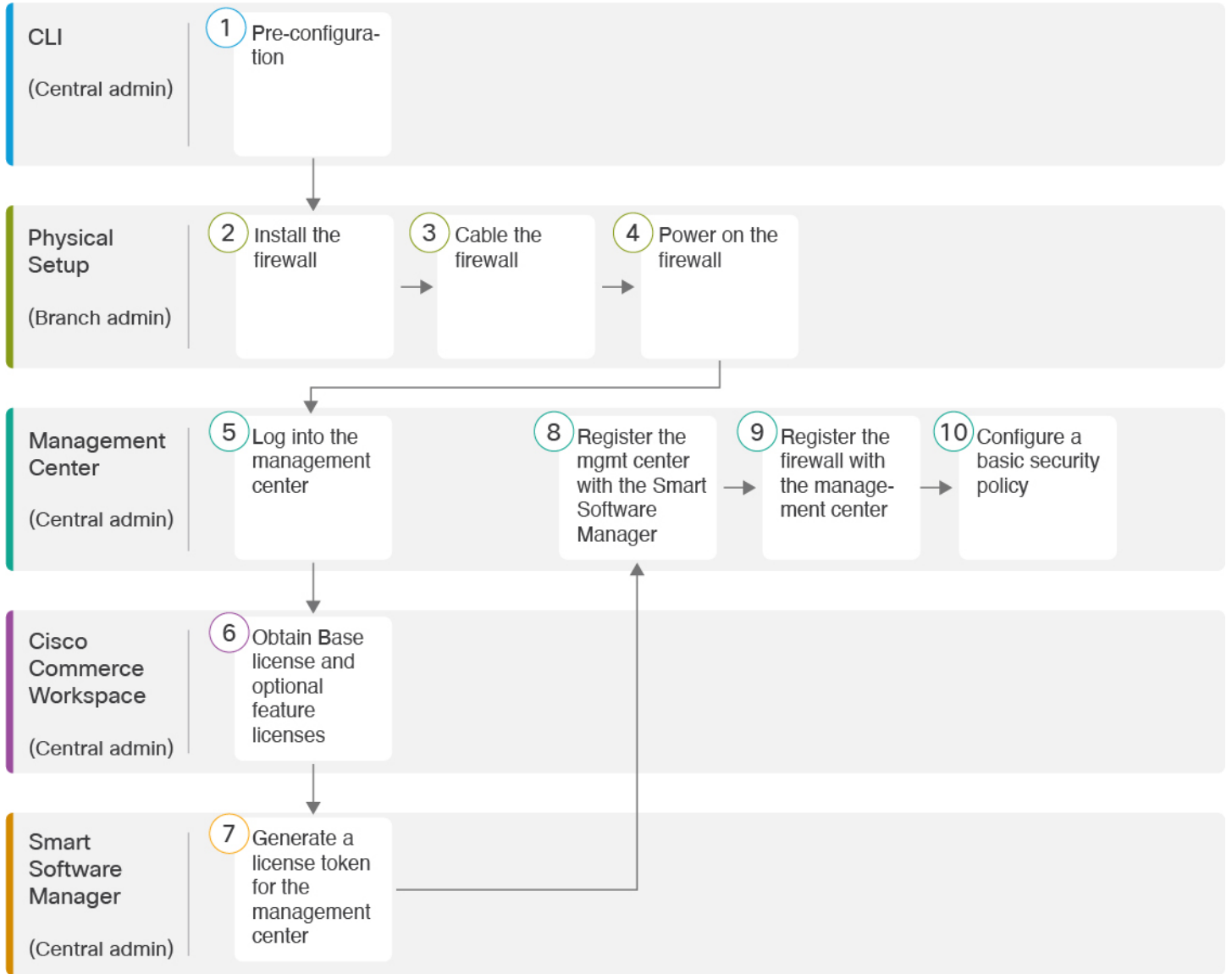
시작하기 전에

management center의 초기 구성을 구축하고 실행합니다. 사용자 모델의 시작 가이드를 참조하십시오.

엔드 투 엔드 작업

management center와 함께 threat defense을 구축하려면 다음 작업을 참조하십시오.

그림 2: 엔드 투 엔드 작업



①	CLI (중앙 관리자)	<ul style="list-style-type: none"> • (선택 사항) 소프트웨어 확인 및 새 버전 설치, 6 페이지 • CLI를 사용한 사전 구성, 8 페이지.
②	물리적 설정 (브랜치 관리자)	방화벽을 설치합니다. 하드웨어 설치 가이드를 참조하십시오.
③	물리적 설정 (브랜치 관리자)	방화벽 케이블 연결, 13 페이지.

4	물리적 설정 (브랜치 관리자)	Firewall 켜기, 14 페이지
5	Management Center (중양 관리자)	Management Center에 로그인에 전달하는 고성능 고속 어플라이언스입니다.
6	Cisco Commerce Workspace (중양 관리자)	기본 라이선스 및 선택적 기능 라이선스를 구매합니다(Management Center 라이선스 얻기, 15 페이지).
7	Smart Software Manager (중양 관리자)	management center에 대한 라이선스 토큰을 생성합니다(Management Center 라이선스 얻기, 15 페이지).
8	Management Center (중양 관리자)	스마트 라이선싱 서버에 management center를 등록합니다(Management Center 라이선스 얻기, 15 페이지).
9	Management Center (중양 관리자)	Management Center에 디바이스 추가, 18 페이지.
10	Management Center (중양 관리자)	기본 보안 정책 구성, 21 페이지.

중양 관리자 사전 구성

브랜치 오피스에 전송 하기 전에 수동으로 threat defense 사전 구성을 해야 할 수 있습니다.

(선택 사항) 소프트웨어 확인 및 새 버전 설치

소프트웨어 버전을 확인하고 필요한 경우 다른 버전을 설치하려면 다음 단계를 수행합니다. 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 합니까?

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.html>에 설명된 릴리스 전략을 참조할 수도 있습니다. 예를 들어, 이 게시판에서는 단기 릴리스 번호 지정(최신 기능 포함), 장기 릴리스 번호 지정(장기간 유지 보수 릴리스 및 패치) 또는 추가 장기 릴리스 번호 지정(가장 긴 기간, 정부 인증) 등이 있습니다.

프로시저

단계 1 콘솔 포트에 연결합니다. 자세한 내용은 [Threat Defense 및 FXOS CLI 액세스](#), 35 페이지를 참조하십시오.

관리자 사용자(비밀번호: **Admin123**)로 로그인합니다.

FXOS CLI에 연결합니다. 처음 로그인하면 비밀번호를 변경하라는 메시지가 표시됩니다. 이 비밀번호는 SSH의 threat defense 로그인에도 사용됩니다.

참고 비밀번호가 이미 변경되었고 모르는 경우, 비밀번호를 기본값으로 재설정하려면 공장 설정 초기화를 수행해야 합니다. [공장 설정 초기화 절차](#)는 [FXOS 문제 해결 설명서](#)를 참조하십시오.

예제:

```
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 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) 관리 인터페이스에 대한 고정 IP 주소를 설정해야 하는 경우 [CLI를 사용한 사전 구성](#), 8 페이지를 참조하십시오. 기본적으로 관리 인터페이스는 DHCP를 사용합니다.

관리 인터페이스에서 액세스할 수 있는 서버에서 새 이미지를 다운로드해야 합니다.

b) [이미지 재설치 절차](#)는 [FXOS 문제 해결 설명서](#)를 참조하십시오.

방화벽이 재부팅된 후 FXOS CLI에 다시 연결됩니다.

- c) FXOS CLI에서 관리자 비밀번호를 다시 설정하라는 메시지가 표시됩니다.

제로 터치 프로비저닝의 경우 디바이스를 온보딩할 때 비밀번호를 이미 설정했으므로 **Password Reset**(비밀번호 재설정) 영역에서 **No...(아니요...)**를 선택해야 합니다.

- d) 디바이스를 종료합니다. **CLI에서 방화벽 전원 끄기, 37 페이지**의 내용을 참조하십시오.

CLI를 사용한 사전 구성

설정 마법사를 사용하여 관리 IP 주소, 게이트웨이 및 기타 기본 네트워킹 설정을 설정합니다.

Procedure

단계 1 Firewall의 전원을 켭니다.

Note threat defense를 처음 부팅할 때는 초기화에 약 15~30분이 소요될 수 있습니다.

단계 2 SSH 또는 콘솔 포트를 사용하여 threat defense CLI에 연결합니다.

콘솔 포트는 FXOS CLI에 연결됩니다.

단계 3 사용자 이름 **admin** 및 비밀번호 **Admin123**으로 로그인합니다.

FXOS에 처음 로그인하면 비밀번호를 변경하라는 메시지가 표시됩니다. 이 비밀번호는 SSH의 threat defense 로그인에도 사용됩니다.

Note 비밀번호가 이미 변경되었거나 비밀번호를 모르는 경우 비밀번호를 기본값으로 재설정하려면 디바이스의 이미지를 재설치해야 합니다. **이미지 재설치 절차는 FXOS 문제 해결 설명서**를 참조하십시오.

Example:

```
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 4 threat defense CLI에 연결합니다.

connect ftd**Example:**

```
firepower# connect ftd
>
```

단계 5 threat defense에 처음 로그인할 경우, 엔드 유저 라이선스 계약(EULA)에 동의하고 SSH 연결을 사용 중인 경우 관리자 비밀번호를 변경하라는 메시지가 표시됩니다. 그러면 관리 인터페이스 설정에 대한 CLI 설정 스크립트가 표시됩니다.

데이터 인터페이스에서 관리자 액세스를 활성화하더라도 관리 인터페이스 네트워크 설정은 계속 사용됩니다.

Note 이미지 재설치 등을 통해 컨피그레이션을 지우지 않으면 CLI 설정 마법사를 반복할 수 없습니다. 그러나 이러한 모든 설정은 **configure network**(네트워크 구성) 명령을 사용하여 CLI에서 나중에 변경할 수 있습니다. [Cisco Secure Firewall Threat Defense 명령 참조](#)의 내용을 참조하십시오.

기본값 또는 이전에 입력한 값이 괄호 안에 표시됩니다. 이전에 입력한 값을 승인하려면 **Enter**를 누릅니다.

다음 지침을 참조하십시오.

- **Do you want to configure IPv4?(IPv4를 구성하시겠습니까?)** 및/또는 **Do you want to configure IPv6?(IPv6를 구성하시겠습니까?)** - 이러한 주소 유형 중 하나 이상에 **y**를 입력합니다. 관리 인터페이스를 사용할 계획은 없지만 IP 주소(예: 개인 주소)를 설정해야 합니다.
- **Configure IPv4 via DHCP or manually?(DHCP를 통해 또는 수동으로 IPv4를 구성하시겠습니까?)** 및/또는 **Configure IPv6 via DHCP, router, or manually?(DHCP, 라우터를 통해 또는 수동으로 IPv6를 설정하시겠습니까?)**- **manual**(수동)을 선택합니다. 관리 인터페이스가 DHCP로 설정된 경우 관리를 위해 데이터 인터페이스를 설정할 수 없습니다. 데이터 인터페이스(데이터 인터페이스)여야 하는 기본 경로(다음 글머리 기호 참조)가 DHCP 서버에서 수신한 기본 경로를 덮어 쓸 수 있기 때문입니다.
- **Enter the IPv4 default gateway for the management interface(관리 인터페이스의 IPv4 기본 게이트웨이 입력)** 및/또는 **Enter the IPv6 gateway for the management interface(관리 인터페이스에 대한 IPv6 게이트웨이 입력)**— 게이트웨이를 **data-interfaces**로 설정합니다. 이 설정은 관리 트래픽을 백플레인을 통해 전달하므로 관리자 액세스 데이터 인터페이스를 통해 라우팅될 수 있습니다.
- **Configure firewall mode?(방화벽 모드를 구성하시겠습니까?)**—**routed**(라우팅)를 입력합니다. 외부 관리자 액세스는 라우팅 방화벽 모드에서만 지원됩니다.

Example:

```
You must accept the EULA to continue.
Press <ENTER> to display the EULA:
End User License Agreement
[...]
```

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

DHCP server is already disabled
DHCP Server Disabled
Configure firewall mode? (routed/transparent) [routed]:
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 6 관리자 액세스를 위한 외부 인터페이스를 구성합니다.

configure network management-data-interface

그러면 외부 인터페이스에 대한 기본 네트워크 설정을 구성하라는 메시지가 표시됩니다. 이 명령 사용에 대한 자세한 내용은 다음을 참조하십시오.

- 관리에 데이터 인터페이스를 사용하려는 경우 관리 인터페이스에서 DHCP를 사용할 수 없습니다. 초기 설정 중에 IP 주소를 수동으로 설정하지 않은 경우 사전에 **configure network {ipv4|ipv6} manual** 명령을 사용하여 설정할 수 있습니다. 관리 인터페이스 게이트웨이를 아직 **data-interfaces** 로 설정하지 않은 경우, 이 명령이 이제 설정합니다.
- management center에 threat defense를 추가하면 management center는 인터페이스 이름 및 IP 주소, 게이트웨이에 대한 고정 경로, DNS 서버 및 DDNS 서버를 포함한 인터페이스 컨피그레이션을 검색하고 유지 관리합니다. DNS 서버 설정에 관한 자세한 내용은 아래를 참조하십시오. management center에서 나중에 관리자 액세스 인터페이스 컨피그레이션을 변경할 수 있지만, threat defense 또는 management center가 관리 연결을 재설정하지 못하게 할 수 있는 변경은 수행하지 않아야 합니다. 관리 연결이 중단되면 threat defense에 이전 구축을 복구하는 **configure policy rollback** 명령이 포함됩니다.
- DDNS 서버 업데이트 URL을 설정하는 경우 threat defense가 HTTPS 연결을 위해 DDNS 서버 인증서를 검증할 수 있도록 threat defense가 Cisco Trusted Root CA 번들에서 모든 주요 CA에 대한 인증서를 자동으로 추가합니다. threat defense는 DynDNS 원격 API 사양 (<https://help.dyn.com/remote-access-api/>)을 사용하는 모든 DDNS 서버를 지원합니다.
- 이 명령은 데이터 인터페이스 DNS 서버를 설정합니다. 설정 스크립트로 설정하거나 **configure network dns servers** 명령을 사용하여 설정한 관리 DNS 서버는 관리 트래픽에 사용됩니다. 데이터 DNS 서버는 DDNS(설정된 경우) 또는 이 인터페이스에 적용된 보안 정책에 사용됩니다.
management center에서 이 threat defense에 할당하는 플랫폼 설정 정책에서 데이터 인터페이스 DNS 서버가 설정됩니다. management center에 threat defense를 추가하면 로컬 설정이 유지되고 DNS 서버가 플랫폼 설정 정책에 추가되지 않습니다. 그러나 나중에 DNS 컨피그레이션을 포함하는 threat defense에 플랫폼 설정 정책을 할당하면 해당 컨피그레이션이 로컬 설정을 덮어씁니다. management center와 threat defense를 동기화하려면 이 설정과 일치하도록 DNS 플랫폼 설정을 적극적으로 구성하는 것이 좋습니다.
또한 로컬 DNS 서버는 초기 등록시 DNS 서버가 검색된 경우에만 management center에 의해 유지됩니다. 예를 들어 관리 인터페이스를 사용하여 디바이스를 등록한 다음 나중에 **configure network management-data-interface** 명령을 사용하여 데이터 인터페이스를 구성하는 경우 threat defense 컨피그레이션과 일치하도록 DNS 서버를 포함하여 management center에서 이러한 모든 설정을 수동으로 구성해야 합니다.
- threat defense를 management center에 등록한 후 관리 인터페이스를 관리 인터페이스 또는 다른 데이터 인터페이스로 변경할 수 있습니다.
- 설정 마법사에서 설정한 FQDN이 이 인터페이스에 사용됩니다.
- 명령의 일부로 전체 디바이스 구성을 지울 수 있습니다. 복구 시나리오에서는 이 옵션을 사용할 수 있지만 초기 설정 또는 정상 작동에는 이 옵션을 사용하지 않는 것이 좋습니다.
- 데이터 관리를 비활성화하려면 **configure network management-data-interface disable** 명령을 입력합니다.

Example:

```
> 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.

>
```

Example:

```
> 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
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.

>
```

단계 7 (Optional) 특정 네트워크에서 management center에 대한 데이터 인터페이스 액세스를 제한합니다.

```
configure network management-data-interface client ip_address netmask
```

기본적으로 모든 네트워크가 허용됩니다.

단계 8 이 threat defense를 관리할 management center를 식별합니다.

```
configure manager add {hostname | IPv4_address | IPv6_address | DONTRESOLVE} reg_key [nat_id]
```

- **{hostname | IPv4_address | IPv6_address | DONTRESOLVE}**—management center의 FQDN 또는 IP 주소를 지정합니다. management center의 주소를 직접 지정할 수 없는 경우 **DONTRESOLVE**를 사용합니다. 하나 이상의 디바이스(management center 또는 threat defense)에는 두 디바이스 간 양방향 SSL 암호화 통신 채널을 설정하기 위한 연결 가능한 IP 주소가 있어야 합니다. 이 명령에서 **DONTRESOLVE**를 지정하는 경우 threat defense에 연결할 수 있는 IP 주소 또는 호스트 이름이 있어야 합니다.
- **reg_key**—threat defense 등록시 management center에 지정할 일회용 등록 키를 지정합니다. 이 등록 키는 37자를 초과해서는 안 됩니다. 영숫자(A~Z, a~z, 0~9)와 하이픈(-)을 사용할 수 있습니다.

- `nat_id` —management center에서 지정할 고유한 일회성 문자열을 지정합니다. 관리에 데이터 인터페이스를 사용하는 경우 등록을 위해 threat defense 및 management center 모두에서 NAT ID를 지정해야 합니다. NAT ID는 37자를 초과할 수 없습니다. 영숫자(A~Z, a~z, 0~9)와 하이픈(-)을 사용할 수 있습니다. 이 ID는 management center에 등록하는 다른 디바이스에 사용할 수 없습니다.

Example:

```
> configure manager add fmc-1.example.com regk3y78 natid56
Manager successfully configured.
```

단계 9 원격 지사로 디바이스를 전송할 수 있도록 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 새시의 전원이 꺼져 있는지 확인합니다(LED 꺼짐).
- c) 새시가 성공적으로 꺼진 후에 필요한 경우 새시에서 전원을 분리하여 물리적으로 제거할 수 있습니다.

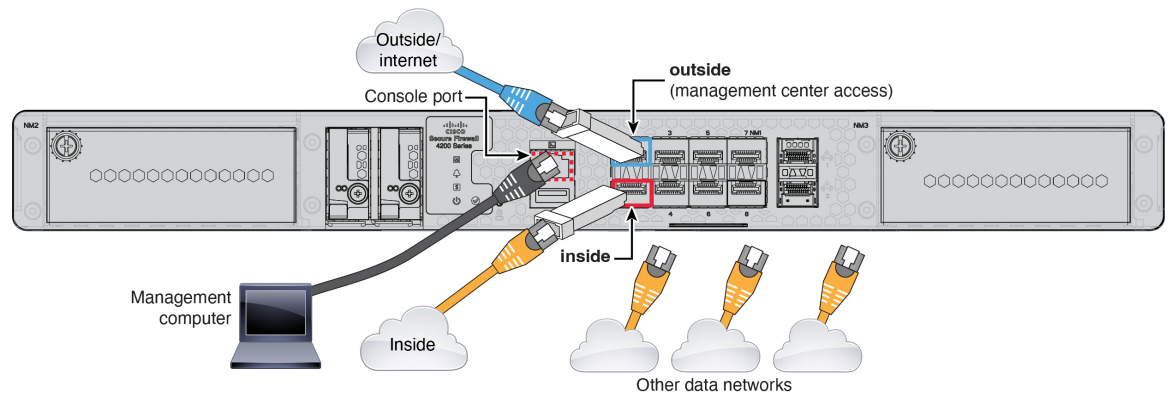
지사 설치

중앙 본사에서 threat defense를 받은 후에는 외부 인터페이스에서 인터넷에 액세스할 수 있도록 방화벽에 케이블을 연결하고 전원을 켜면 됩니다. 그러면 중앙 관리자가 구성을 완료할 수 있습니다.

방화벽 케이블 연결

management center 및 관리 컴퓨터는 원격 본사에 있으며 인터넷을 통해 threat defense에 연결할 수 있습니다. Secure Firewall 4200 케이블을 연결하려면 다음 단계를 참조하십시오.

그림 3: 원격 관리 구축 케이블 연결



시작하기 전에

- 데이터 인터페이스 포트에 SFP 설치 - 기본 제공 포트는 SFP 모듈이 필요한 1/10/25-Gb SFP 포트입니다.
- (선택 사항) 콘솔 케이블 얻기 - 방화벽은 기본적으로 콘솔 케이블과 함께 제공되지 않으므로 예를 들어 서드파티 USB-RJ-45 직렬 케이블을 구매해야 합니다.

프로시저

단계 1 새시를 설치합니다. [하드웨어 설치 가이드](#)를 참조하십시오.

단계 2 외부 인터페이스(예: Ethernet 1/1)를 외부 라우터에 연결합니다.

단계 3 내부 인터페이스(예: Ethernet 1/2)를 내부 스위치 또는 라우터에 연결합니다.

단계 4 나머지 인터페이스에 다른 네트워크를 연결합니다.

단계 5 (선택 사항) 관리 컴퓨터를 콘솔 포트에 연결합니다.

브랜치 오피스에서는 일상적인 사용에 콘솔 연결이 필요하지 않습니다. 그러나 문제 해결을 위해 필요할 수 있습니다.

Firewall 켜기

시스템 전원은 디바이스 뒷면에 있는 로커 전원 스위치로 제어됩니다. 전원 스위치는 정상적인 종료를 지원하는 소프트 알립 스위치로 구현되어 시스템 소프트웨어 및 데이터 손상의 위험을 줄여줍니다.



참고 처음 threat defense 부팅 시에는 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.

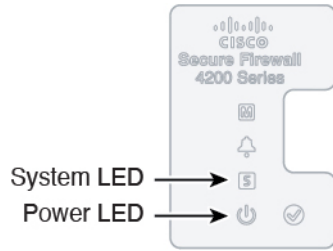
프로시저

단계 1 전원 케이블을 디바이스에 연결하고 전기 콘센트에 꽂습니다.

단계 2 전원 코드 옆 새시 후면에 있는 표준 로커 유형 전원 켜기/끄기 스위치를 사용하여 전원을 켭니다.

단계 3 방화벽 뒷면의 전원 LED를 확인합니다. 전원이 켜져 있으면 녹색으로 표시됩니다.

그림 4: 시스템 및 전원 LED



단계 4 방화벽 뒷면의 시스템 LED를 확인합니다. 시스템이 전원 켜기 진단을 통과하면 녹색으로 표시됩니다.

참고 스위치가 ON(켜짐)에서 OFF(꺼짐)로 토글된 경우 시스템에서 최종적으로 전원이 꺼지는 데 몇 초 정도가 걸릴 수 있습니다. 이 시간 동안 새시 전면에 있는 전원 LED가 녹색으로 깜박입니다. 전원 LED가 완전히 꺼질 때까지 전원을 제거하지 마십시오.

중앙 관리자 사후 구성

원격 지사 관리자가 외부 인터페이스에서 인터넷에 액세스할 수 있도록 threat defense에 케이블을 연결하고 나면 management center에 threat defense를 등록하고 디바이스의 구성을 완료할 수 있습니다.

Management Center에 로그인

management center을 사용해 threat defense를 구성하고 모니터링합니다.

프로시저

단계 1 지원되는 브라우저를 사용해 다음 URL을 입력합니다.

https://fmc_ip_address

단계 2 사용자 이름 및 비밀번호를 입력합니다.

단계 3 **Log In**(로그인)을 클릭합니다.

Management Center 라이선스 얻기

모든 라이선스는 management center를 통해 Threat Defense 에 제공됩니다. 선택적으로 다음 기능 라이선스를 구매할 수 있습니다.

- **Essentials**—(필수) Essentials 라이선스.

- **IPS**—보안 인텔리전스 및 Next-Generation IPS
- 악성코드 방어—악성코드 방어
- **URL 필터링** - URL 필터링
- **Cisco Secure Client**—Secure Client Advantage, Secure Client Premier 또는 Secure Client VPN 전용
- **Carrier**—배율, GTP/GPRS, M3UA, SCTP

시스코 라이선싱에 대한 자세한 내용은 cisco.com/go/licensingguide를 참조하세요.

시작하기 전에

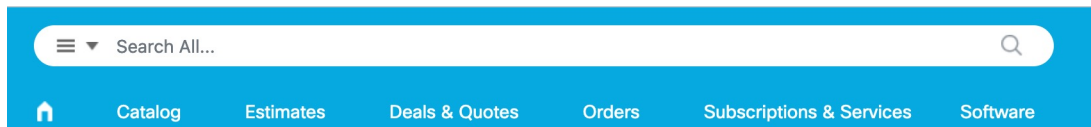
- **Smart Software Manager**에 어카운트가 있습니다.
아직 어카운트가 없는 경우 **새 어카운트 설정** 링크를 클릭합니다. Smart Software Manager를 사용하면 조직을 위한 어카운트를 생성할 수 있습니다.
- Smart Software Licensing 계정은 일부 기능(내보내기-컴플라이언스 플래그를 사용하여 활성화됨)을 사용하려면 강력한 암호화(3DES/AES) 라이선스 자격을 얻어야 합니다.

프로시저

단계 1 스마트 라이선싱 어카운트에서 필요한 라이선스가 사용 가능한지 확인합니다.

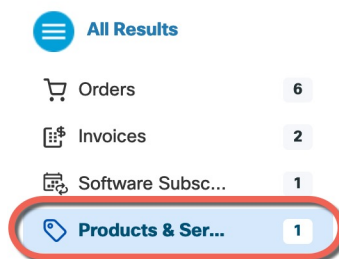
Cisco 또는 리셀러에서 디바이스를 구매한 경우 라이선스는 Smart Software License 계정에 연결되어 있어야 합니다. 그러나 라이선스를 직접 추가해야 하는 경우 **Cisco Commerce Workspace**에서 **Search All**(모두 검색) 필드를 사용합니다.

그림 5: 라이선스 검색



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

그림 6: 결과



다음 라이선스 PID를 검색합니다.

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

- Essentials 라이선스:
 - L-FPR4215-BSE=
 - L-FPR4225-BSE=
 - L-FPR4245-BSE=
- IPS, 악성코드 방어 및 URL 라이선스 조합:
 - L-FPR4215T-TMC =
 - L-FPR4225T-TMC =
 - L-FPR4245T-TMC =

위의 PID 중 하나를 주문에 추가하면 다음 PID 중 하나에 해당하는 기간별 서브스크립션을 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
- 통신 사업자 라이선스:
 - L-FPR4200-FTD-CAR=
- Cisco Secure Client— [Cisco Secure Client 주문 가이드](#)를 참조하십시오.

단계 2 아직 등록하지 않은 경우 management center를 Smart Software Manager에 등록합니다.

등록하려면 Smart Software Manager에서 등록 토큰을 생성해야 합니다. 자세한 지침은 [management center구성 가이드](#)를 참조하십시오.

Management Center에 디바이스 추가

디바이스 IP 주소 또는 호스트 이름과 등록 키를 사용하여 threat defense를 management center.

프로시저

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

단계 2 **Add**(추가) 드롭다운 메뉴에서 **Add Device**(디바이스 추가)를 선택합니다.

등록 키 방법이 기본적으로 선택됩니다.

그림 7: 등록 키를 사용하여 디바이스 추가

Add Device ?

Select the Provisioning Method:

Registration Key Serial Number

CDO Managed Device

Host:†

Display Name:

Registration Key:*

Group:

Access Control Policy:*

Smart Licensing

Note: All virtual Firewall Threat Defense devices 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 Firewall Threat Defense performance-tiered licensing. Until you choose a tier, your Firewall Threat Defense virtual defaults to the FTDv50 selection.

Performance Tier (only for Firewall Threat Defense virtual 7.0 and above):

Carrier

Malware Defense

IPS

URL

Advanced

Unique NAT ID:†

Transfer Packets

다음 매개변수를 설정합니다.

- **Host(호스트)**—추가하려는 threat defense의 IP 주소 또는 호스트 이름을 입력합니다. threat defense 초기 구성에서 management center IP 주소와 NAT ID를 모두 지정한 경우 이 필드를 비워둘 수 있습니다.

참고 HA 환경에서 management center 두 가지가 모두 NAT 뒤에 있는 경우 기본 management center에 호스트 IP 또는 이름 없이 threat defense 등록이 가능합니다. 그러나 보조 management center에 threat defense 등록을 하려면 threat defense에 대한 IP 주소 또는 호스트 이름을 제공해야 합니다.

- **Display Name**(표시 이름)—management center에서 표시하려는 threat defense의 이름을 입력합니다.
- **Registration key**(등록 키)—threat defense 초기 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. **내부에서 외부로 트래픽을 허용합니다.**을 참조하십시오.

그림 8: New Policy

New Policy

Name:
ftd-ac-policy

Description:

Select Base Policy:
None

Default Action:
 Block all traffic
 Intrusion Prevention
 Network Discovery

Cancel Save

- 스마트 라이선싱—구축하려는 기능에 필요한 스마트 라이선스를 할당합니다. 참고: 디바이스를 추가한 후 **System**(시스템) > **Licenses**(라이선스) > **Smart Licenses**(스마트 라이선스) 페이지에서 Secure Client 원격 액세스 VPN 라이선스를 적용할 수 있습니다.
- **Unique NAT ID**(고유 NAT ID)—threat defense 초기 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. 이벤트를 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 등록에 실패하면 다음 항목을 확인하십시오.

- Ping - 다음 명령을 사용해 threat defense CLI에 액세스하고 management center IP 주소에 Ping을 보냅니다.

ping system ip_address

Ping이 실패하는 경우 **show network** 명령을 사용해 네트워크 설정을 확인합니다. threat defense 관리 IP 주소를 변경해야 하는 경우 **configure network management-data-interface** 명령을 사용합니다.

- 등록 키, NAT ID 및 management center IP 주소 - 두 디바이스에서 동일한 등록 키 및 NAT ID가 사용되고 있는지 확인합니다. **configure manager add** 명령을 사용해 threat defense에서 등록 키 및 NAT ID를 설정할 수 있습니다.

자세한 문제 해결 정보는 <https://cisco.com/go/fmc-reg-error>를 참조하십시오.

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 할당합니다. 관리자 액세스 설정의 일부로 외부 인터페이스의 기본 설정을 구성했지만 보안 영역에 할당해야 합니다.
- DHCP Server(DHCP 서버) - 클라이언트용 내부 인터페이스에서 DHCP 서버를 사용합니다.
- NAT - 외부 인터페이스에서 인터페이스 PAT를 사용합니다.
- Access control(액세스 제어) - 내부에서 외부로 향하는 트래픽을 허용합니다.
- SSH - 관리자 액세스 인터페이스에서 SSH를 활성화합니다.

인터페이스 구성

threat defense 인터페이스를 활성화하고, 보안 영역에 이를 할당하며, IP 주소를 설정합니다. 또한 분할 인터페이스를 설정합니다.

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 방화벽에 대해 편집 (✎)를 클릭합니다.

단계 2 **Interfaces**(인터페이스)를 클릭합니다.

그림 9: 인터페이스

Interface	Logical Name	Type	Security Zones	MAC Address (Active/Standby)	IP Address	Path Monitoring	Virtual Router	
● Management0/0	management	Physical				Disabled	Global	🔍 ↶
☑ GigabitEthernet0/0		Physical				Disabled		✎
☑ GigabitEthernet0/1		Physical				Disabled		✎
☑ GigabitEthernet0/2		Physical				Disabled		✎
☑ GigabitEthernet0/3		Physical				Disabled		✎
☑ GigabitEthernet0/4		Physical				Disabled		✎
☑ GigabitEthernet0/5		Physical				Disabled		✎
☑ GigabitEthernet0/6		Physical				Disabled		✎
☑ GigabitEthernet0/7		Physical				Disabled		✎

단계 3 40Gb 인터페이스(일부 모델에서 사용 가능)에서 10Gb 분할 인터페이스 4개를 생성하려면 인터페이스의 분할 아이콘을 클릭합니다.

구성에서 이미 40Gb 인터페이스를 사용한 경우 분할을 계속 진행하기 전에 구성을 제거해야 합니다.

단계 4 내부에 사용할 인터페이스의 편집 (✎)를 클릭합니다.

General(일반) 탭이 표시됩니다.

그림 10: 일반 탭

Edit Physical Interface

General IPv4 IPv6 Path Monitoring

Name:

Enabled
 Management Only

Description:

Mode:

Security Zone:

Interface ID:

MTU:

(64 - 9000)

Priority:
 (0 - 65535)

Propagate Security Group Tag:

NVE Only:

- 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 지원합니다. 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(/) 표기로 IP 주소와 서브넷 마스크를 입력합니다.

예를 들어 **192.168.1.1/24** 를 입력합니다.

그림 11: IPv4 탭

Edit Physical Interface

General IPv4 IPv6 Path Monitoring

IP Type:
Use Static IP

IP Address:
192.168.1.1/24
eg. 192.0.2.1/255.255.255.128 or 192.0.2.1/25

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

그림 12: IPv6 탭

Edit Physical Interface

General IPv4 IPv6 Path Monitoring Hardware Configu

Basic Address Prefixes Settings DHCP

Enable IPV6:

Enforce EUI 64:

Link-Local address:

Autoconfiguration:

Obtain Default Route:

f) **OK**(확인)를 클릭합니다.

단계 5 외부에서 사용하려는 인터페이스의 편집 (✎)를 클릭합니다.

General(일반) 탭이 표시됩니다.

그림 13: 일반 탭

Edit Physical Interface

General IPv4 IPv6 Path Monitoring Hardware

Name:

Enabled
 Management Only

Description:

Mode:

Security Zone:

Interface ID:

MTU:

(64 - 9000)

Priority:
 (0 - 65535)

Propagate Security Group Tag:

NVE Only:

관리자 액세스를 위해 이 인터페이스를 미리 구성했으므로 인터페이스의 이름이 이미 지정되고 활성화되어 있으며 주소가 지정됩니다. 이러한 기본 설정을 변경하면 management center 관리 연결이 중단되므로 이 설정을 변경하면 안됩니다. 트래픽 정책을 통해 이 화면에서 보안 영역을 구성해야 합니다.

- 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.

- b) **OK**(확인)를 클릭합니다.

단계 6 **Save**(저장)를 클릭합니다.

DHCP 서버 구성

클라이언트가 DHCP를 사용하여 Threat Defense 에서 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 14: DHCP 서버

The screenshot shows the DHCP Server configuration interface. On the left, there is a sidebar with options: DHCP Server, DHCP Relay, and DDNS. The main area is divided into 'Server' and 'Advanced' tabs. The 'Server' tab is active, showing fields for Ping Timeout (50), Lease Length (3600), and an unchecked 'Auto-Configuration' checkbox. Below these are fields for Interface, Domain Name, Primary DNS Server, Secondary DNS Server, Primary WINS Server, and Secondary WINS Server. At the bottom right, a red box highlights the '+ Add' button. Below the configuration fields is a table with columns: Interface, Address Pool, and Enable DHCP Server. The table currently shows 'No records to display'.

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

그림 15: 서버 추가

The 'Add Server' dialog box is shown. It has a title bar with 'Add Server' and a help icon. The 'Interface*' field is a dropdown menu with 'inside' selected. The 'Address Pool*' field contains '10.9.7.9-10.9.7.25' with '(2.2.2.10-2.2.2.20)' below it. The 'Enable DHCP Server' checkbox is checked. At the bottom, there are 'Cancel' and 'OK' 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.

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.

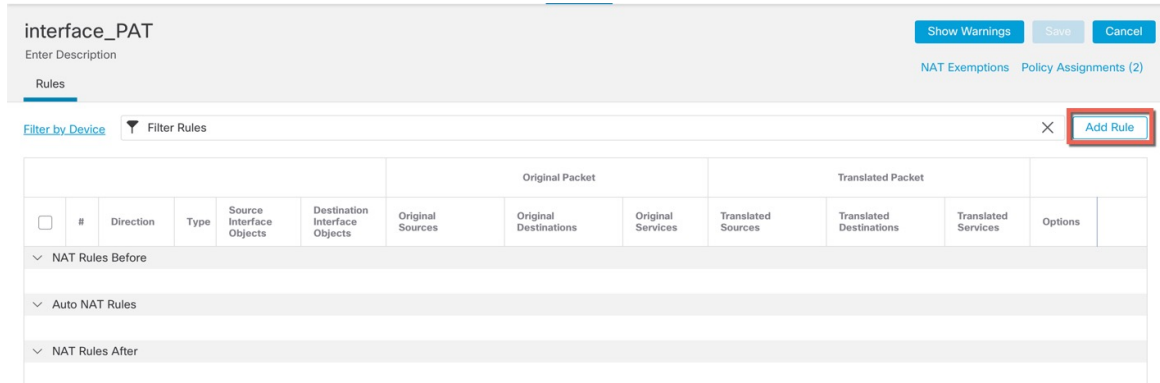
단계 2 정책 이름을 지정하고, 정책을 사용할 디바이스를 선택한 뒤 **Save**(저장)를 클릭합니다.

그림 16: *New Policy*

The screenshot shows the 'New Policy' configuration interface. It includes a search bar for 'Available Devices' and a list of selected devices. The 'Available Devices' list contains 10.10.0.6 and 10.10.0.7. The 'Selected Devices' list also contains 10.10.0.6 and 10.10.0.7. An 'Add to Policy' button is positioned between the two lists. At the bottom right, there are 'Cancel' and 'Save' buttons.

정책이 management center을 추가합니다. 계속해서 정책에 규칙을 추가해야 합니다.

그림 17: NAT 정책

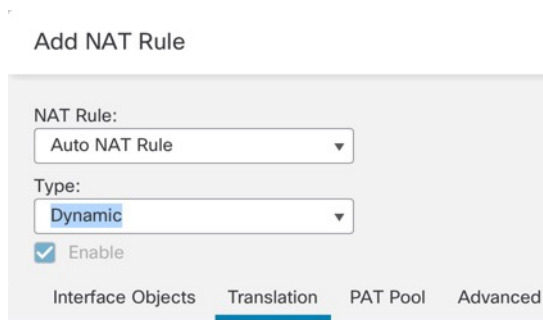


단계 3 **Add Rule**(규칙 추가)을 클릭합니다.

Add NAT Rule(NAT 규칙 추가) 대화 상자가 나타납니다.

단계 4 기본 규칙 옵션을 구성합니다.

그림 18: 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 19: 인터페이스 객체

Add NAT Rule

NAT Rule: Auto NAT Rule

Type: Dynamic

Enable

Interface Objects Translation PAT Pool Advanced

Available Interface Objects

- inside_zone
- outside_zone** (1)
- wfxAutomationZone

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

- any
- outside_zone** (3)

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

그림 20: 변환

Add NAT Rule

NAT Rule: Auto NAT Rule

Type: Dynamic

Enable

Interface Objects Translation PAT Pool Advanced

Original Packet

Original Source:* +

Original Port: TCP

Translated Packet

Translated Source:

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

Translated Port:

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

내부에서 외부로 트래픽을 허용합니다.

그림 21: 새 네트워크 개체

참고 자동 NAT 규칙은 개체 정의의 일부로 NAT를 추가하고 시스템 정의의 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.

내부에서 외부로 트래픽을 허용합니다.

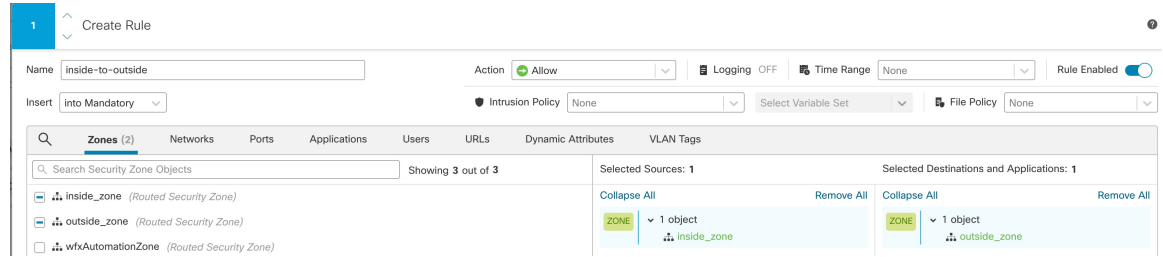
Threat Defense 를 등록할 때 기본 액세스 컨트롤 정책인 **Block all traffic**(모든 트래픽 차단)을 생성했다면, 디바이스에 트래픽을 허용하기 위해 정책에 규칙을 추가해야 합니다. 다음 절차에서는 내부 영역에서 외부 영역으로 향하는 트래픽을 허용하는 규칙을 추가합니다. 다른 영역이 있는 경우에는 적절한 네트워크에 대한 트래픽을 허용하는 규칙을 추가해야 합니다.

프로시저

단계 1 **Policy(정책) > Access Policy(액세스 정책) > Access Policy(액세스 정책)**을 선택하고 Threat Defense 에 할당된 액세스 컨트롤 정책에 대해 편집 (✎)를 클릭합니다.

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

그림 22: 규칙 추가



- **Name (이름)** - 예를 들어 이 규칙의 이름을 **inside-to-outside**로 지정합니다.
- **Selected Sources(선택한 원본)**—**Zones(영역)**에서 내부 영역을 선택하고 **Add Source Zone(원본 영역 추가)**을 클릭합니다.
- **Selected Destinations and Applications(선택한 대상 및 애플리케이션)**—**Zones(영역)**에서 외부 영역을 선택하고 **Add Destination Zone(대상 영역 추가)**을 클릭합니다.

기타 설정은 변경하지 않습니다.

단계 3 **Apply(적용)**를 클릭합니다.

규칙이 **Rules(규칙)** 테이블에 추가됩니다.

단계 4 **Save(저장)**를 클릭합니다.

관리자 액세스 데이터 인터페이스에서 SSH 구성

외부와 같은 데이터 인터페이스에서 management center 액세스를 활성화한 경우 이 절차를 사용하여 해당 인터페이스에서 SSH를 활성화해야 합니다. 이 섹션에서는 threat defense에서 하나 이상의 데이터 또는 진단 인터페이스에 대한 SSH 연결을 활성화하는 방법을 설명합니다.



참고 SSH는 관리 인터페이스에서 기본적으로 활성화됩니다. 하지만 이 화면은 관리 SSH 액세스에 영향을 미치지 않습니다.

관리 인터페이스는 디바이스에 있는 다른 인터페이스와 분리되어 있습니다. 이 인터페이스는 디바이스를 management center에 설치하고 등록하는 데 사용됩니다. 데이터 인터페이스용 SSH는 관리 인터페이스용 SSH로 내부 및 외부 사용자 목록을 공유합니다. 다른 설정은 별도로 구성됩니다. 데이터 인터페이스의 경우 이 화면을 사용하여 SSH 및 액세스 목록을 활성화합니다. 데이터 인터페이스용 SSH 트래픽은 일반 라우팅 구성을 사용하며 설치 또는 CLI에서 구성된 정적 경로는 사용하지 않습니다.

관리 인터페이스의 경우 SSH 액세스 목록을 구성하려면 [Cisco Secure Firewall Threat Defense 명령 참조](#)의 **configure ssh-access-list** 명령을 참조하십시오. 정적 경로를 구성하려면 **configure network static-routes** 명령을 참조하십시오. 기본적으로 초기 설정 시 관리 인터페이스를 통해 기본 경로를 구성합니다.

SSH를 사용하려면 호스트 IP 주소를 허용하는 액세스 규칙은 필요하지 않습니다. 이 섹션에 따라 SSH 액세스를 구성하면 됩니다.

연결할 수 있는 인터페이스에만 SSH를 사용할 수 있습니다. SSH 호스트가 외부 인터페이스에 있을 경우 외부 인터페이스와의 직접적인 관리 연결만 시작할 수 있습니다.

SSH는 다음과 같은 암호 및 키 교환을 지원합니다.

- 암호화—aes128-cbc, aes192-cbc, aes256-cbc, aes128-ctr, aes192-ctr, aes256-ctr
- 무결성—hmac-sha2-256
- 키 교환 — dh-group14-sha256



참고 3회 연속 SSH를 사용한 CLI 로그인에 실패한 경우, 디바이스가 SSH 연결을 종료합니다.

시작하기 전에

- **configure user add** 명령을 사용해 CLI에서 SSH 내부 사용자를 설정할 수 있습니다.의 내용을 참조하십시오. 기본적으로 초기 설정 중에 비밀번호를 구성한 관리자 사용자가 있습니다. 플랫폼 설정에서 **External Authentication**(외부 인증)을 구성하여 LDAP 또는 RADIUS에서 외부 사용자를 구성할 수도 있습니다.
- 디바이스에 SSH 연결을 허용할 호스트 또는 네트워크를 정의하는 네트워크 개체가 필요합니다. 이 절차의 일부로 개체를 추가할 수 있지만 개체 그룹을 사용하여 IP 주소 그룹을 식별하려면 규칙에 필요한 그룹이 이미 있는지 확인합니다. **Objects**(개체) > **Object Management**(개체 관리)를 선택하여 개체를 설정합니다.



참고 시스템에서 제공하는 **any** 네트워크 개체를 사용할 수 없습니다. 대신 **any-ipv4** 또는 **any-ipv6**를 사용합니다.

프로시저

단계 1 **Devices**(디바이스) > **Platform Settings**(플랫폼 설정)를 선택하고 threat defense 정책을 생성하거나 편집합니다.

단계 2 **SSH Access**(SSH 액세스)를 선택합니다.

단계 3 SSH 연결을 허용하는 인터페이스와 IP 주소를 확인합니다.

이 테이블을 사용하여 SSH 연결을 허용할 인터페이스와 이러한 연결을 허용할 수 있는 클라이언트의 IP 주소를 제한합니다. 개별 IP 주소가 아닌 네트워크 주소를 사용할 수 있습니다.

- 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(사용 가능한 영역/인터페이스)** - SSH 연결을 허용할 인터페이스가 포함된 영역을 추가합니다. 영역에 없는 인터페이스의 경우 **Selected Zones/Interface(선택한 영역/인터페이스)** 목록 아래의 필드에 인터페이스 이름을 입력하고 **Add(추가)**를 클릭할 수 있습니다. 루프백 인터페이스 및 가상 라우터 인식 인터페이스를 추가할 수도 있습니다. 이 규칙은 디바이스에 선택한 인터페이스 또는 영역이 포함되어 있는 경우에만 디바이스에 적용됩니다.

c) **OK(확인)**를 클릭합니다.

단계 4 **Save(저장)**를 클릭합니다.

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

구성 구축

Threat Defense 에 설정 변경 사항을 구축합니다. 구축하기 전에는 디바이스에서 변경 사항이 활성화 상태가 아닙니다.

프로시저

단계 1 우측 상단에서 **Deploy(구축)**를 클릭합니다.

그림 23: 구축



단계 2 빠르게 구축하려면 특정 디바이스를 선택한 다음 **Deploy(구축)**를 클릭하거나, 모든 디바이스에 구축하려면 **Deploy All(모두 구축)**을 클릭합니다. 그렇지 않으면 추가 구축 옵션에 대해 **Advanced Deploy(고급 구축)**를 클릭합니다.

그림 24: 모두 구축

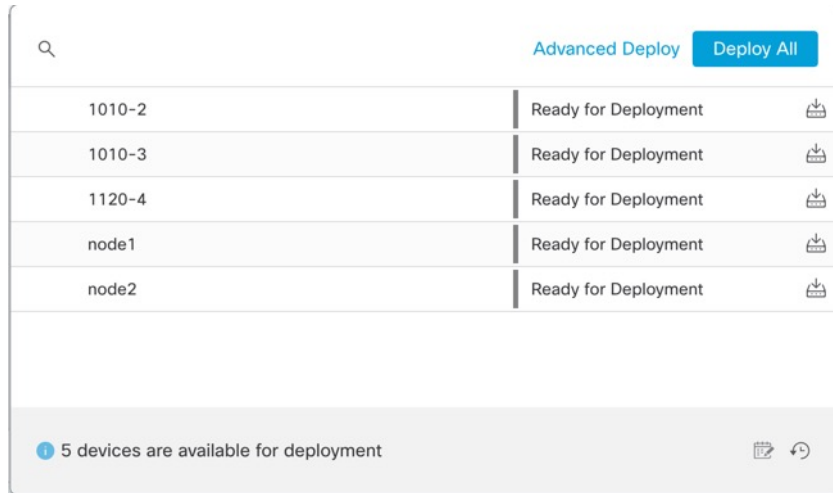
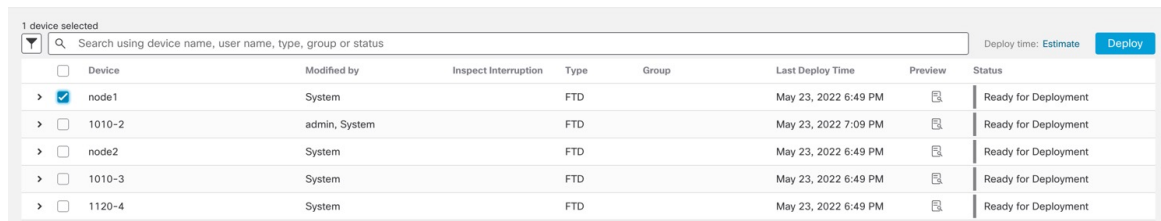
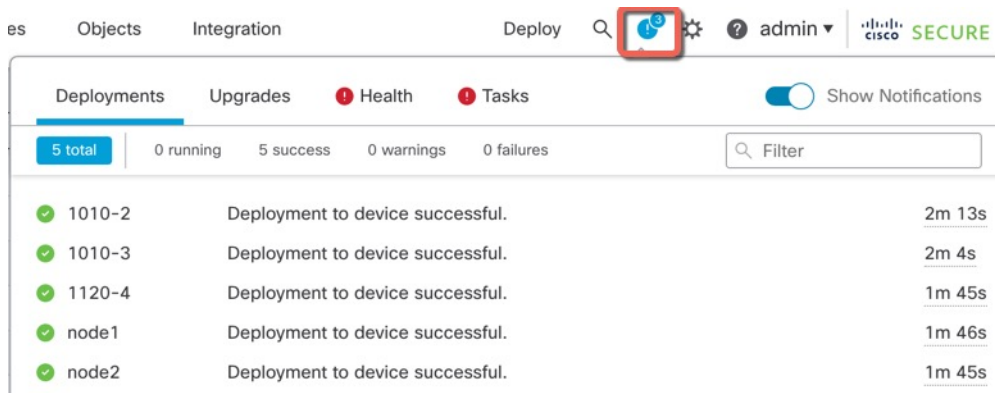


그림 25: 고급 구축



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

그림 26: 구축 상태



Threat Defense 및 FXOS CLI 액세스

CLI(Command Line Interface)를 사용하여 시스템을 설정하고 기본적인 시스템 트러블슈팅을 수행합니다. CLI 세션을 통해 정책을 구성할 수는 없습니다. 콘솔 포트에 연결하여 CLI에 액세스할 수 있습니다.

문제 해결을 위해 FXOS CLI에 액세스할 수 있습니다.



참고 아니면 SSH를 threat defense 디바이스의 관리 인터페이스로 할 수 있습니다. 콘솔 세션과 달리 SSH 세션은 기본적으로 threat defense CLI를 사용하며, **connect fxos** 명령을 사용하여 FXOS CLI에 연결할 수 있습니다. 이후 SSH 연결용 인터페이스를 여는 경우 데이터 인터페이스에 있는 주소에 연결할 수도 있습니다. 데이터 인터페이스에 대한 SSH 액세스는 기본값으로 사용 해제 상태입니다. 이 절차에서는 기본값이 FXOS CLI인 콘솔 포트 액세스에 대해 설명합니다.

프로시저

단계 1 CLI에 로그인하려면 관리 컴퓨터를 콘솔 포트에 연결합니다. Secure Firewall 4200은 기본적으로 콘솔 케이블과 함께 제공되지 않으므로, 예를 들어 서드파티 USB-RJ-45 직렬 케이블을 구매해야 합니다. 운영 체제에 필요한 모든 USB 시리얼 드라이버를 설치해야 합니다. 콘솔 포트의 기본값은 FXOS CLI입니다. 다음 시리얼 설정을 사용하십시오.

- 9600보드
- 8 데이터 비트
- 패리티 없음
- 1 스톱 비트

FXOS CLI에 연결합니다. 초기 설정 시 설정한 관리자 사용자 이름 및 비밀번호(기본값은 **Admin123**)를 사용하여 CLI에 로그인합니다.

예제:

```
firepower login: admin
Password:
Last login: Thu May 16 14:01:03 UTC 2019 on ttyS0
Successful login attempts for user 'admin' : 1
```

```
firepower#
```

단계 2 threat defense CLI에 액세스합니다.

connect ftd

예제:

```
firepower# connect ftd
```

>

로그인한 후 CLI에서 사용할 수 있는 명령에 대한 정보를 확인하려면 **help** 또는 **?**를 입력하십시오. 사용 정보는 [Cisco Secure Firewall Threat Defense 명령 참조](#)에서 참조하십시오.

단계 3 **threat defense** CLI를 종료하려면 **exit** 또는 **logout** 명령을 입력합니다.

그러면 FXOS CLI 프롬프트로 돌아갑니다. FXOS CLI에서 사용할 수 있는 명령에 대한 정보를 확인하려면 **?**를 입력하십시오.

예제:

```
> exit
firepower#
```

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 Firepower 시스템이 정상적으로 종료되지 않는다는 점에 유의하십시오.

디바이스 관리 페이지를 사용하여 management center 디바이스의 전원을 끄거나 FXOS CLI를 사용할 수 있습니다.

Management Center을 사용하여 Firewall 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 방화벽이 정상적으로 종료되지 않는다는 점에 유의하십시오.

management center를 사용하여 시스템을 올바르게 종료할 수 있습니다.

프로시저

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

단계 2 다시 시작할 디바이스 옆의 편집 (✎)을 클릭합니다.

단계 3 **Device**(디바이스) 탭을 클릭합니다.

단계 4 **System**(시스템) 섹션에서 **Shut Down Device**(디바이스 종료)(✕)을 클릭합니다.

단계 5 메시지가 표시되면 디바이스 종료를 확인합니다.

단계 6 방화벽에 대한 콘솔 연결이 있는 경우 방화벽이 종료될 때 시스템 프롬프트를 모니터링합니다. 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 7 새시가 성공적으로 꺼진 후에 필요한 경우 새시에서 전원을 분리하여 물리적으로 제거할 수 있습니다.

CLI에서 방화벽 전원 끄기

FXOS CLI를 사용하여 시스템을 안전하게 종료하고 디바이스의 전원을 끌 수 있습니다. 콘솔 포트에 연결하여 CLI에 액세스할 수 있습니다. [Threat Defense 및 FXOS CLI 액세스, 35 페이지](#) 참조.

프로시저

단계 1 FXOS CLI에서 local-mgmt에 연결합니다.

```
Firepower # connect local-mgmt
```

단계 2 **shutdown** 명령 실행:

```
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 3 방화벽이 종료될 때 시스템 프롬프트를 모니터링합니다. 다음 프롬프트가 표시됩니다.

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

단계 4 새시가 성공적으로 꺼진 후에 필요한 경우 새시에서 전원을 분리하여 물리적으로 제거할 수 있습니다.

다음 단계는 무엇입니까?

threat defense 설정을 계속하려면 [Cisco Secure Firewall Threat Defense 문서로 이동](#)에서 사용 중인 소프트웨어 버전에 해당하는 문서를 참조하십시오.

management center 사용과 관련된 내용은 [Cisco Secure Firewall Management Center 디바이스 구성 가이드](#)를 참조하십시오.

다음 단계는 무엇입니까?

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.