

FMC를 사용하여 원격 지사에 FTD 구축

초판: 2020년 11월 2일

최종 변경: 2021년 2월 23일

FMC를 사용하여 원격 지사에 FTD 구축

이 문서에서는 원격 지사에서 FTD(Firepower Threat Defense)를 구축하는 방법을 설명합니다.

- 중앙 본사의 관리자가 FTD를 미리 구성한 다음 FTD를 원격 지사로 보냅니다.
- 지사 관리자가 FTD의 케이블을 연결하고 전원을 켭니다.
- 중앙 관리자가 FMC(Firepower Management Center)를 사용하여 FTD 구성을 완료합니다.



참고 이 기능을 사용하려면 Firepower 버전 6.7 이상이 필요합니다.

이 문서에서는 Firepower 1010, 1100, 2100, ASA 5508-X 및 5516-X 및 ISA 3000에 대해 설명합니다.



참고 Firepower 4100 및 9300의 경우 Firepower 4100 또는 9300 시작 가이드를 참조하십시오. Firepower 4100 및 9300에는 이 가이드에서 다루지 않는 추가 새시 설치 및 구성이 필요합니다.



참고 FTDv의 경우 FTDv 시작 가이드를 참조하십시오. FTDv에는 이 가이드의 범위를 벗어나는 추가 하이퍼 바이저 설치 및 구성이 필요합니다.

원격 관리 작동 방식

FMC에서 인터넷을 통해 FTD(를) 관리할 수 있도록 하려면 관리 인터페이스 대신 FMC 관리용 외부 인터페이스를 사용합니다. 대부분의 원격 지사에서는 단일 인터넷 연결만 가능하므로 외부 FMC 액세스를 통해 중앙 집중식 관리가 가능합니다.



참고 예를 들어 FMC 내부에 내부 인터페이스가 있는 경우 모든 데이터 인터페이스를 FMC 액세스에 사용할 수 있습니다. 그러나 이 가이드는 주로 원격 지사에 대한 시나리오이므로 외부 인터페이스 액세스를 다룹니다.

관리 인터페이스는 FTD 데이터 인터페이스와 별도로 구성된 특수 인터페이스이며 자체 네트워크 설정이 있습니다. 데이터 인터페이스에서 FMC 액세스를 활성화하더라도 관리 인터페이스 네트워크 설정은 계속 사용됩니다. 모든 관리 트래픽은 계속해서 관리 인터페이스에서 제공되거나 관리 인터페이스로 전송됩니다. 데이터 인터페이스에서 FMC 액세스를 활성화하면 FTD는 수신 인터페이스를 백플레인을 통해 관리 인터페이스로 전달합니다. 발신 관리 트래픽의 경우 관리 인터페이스는 백플레인을 통해 데이터 인터페이스로 트래픽을 전달합니다.

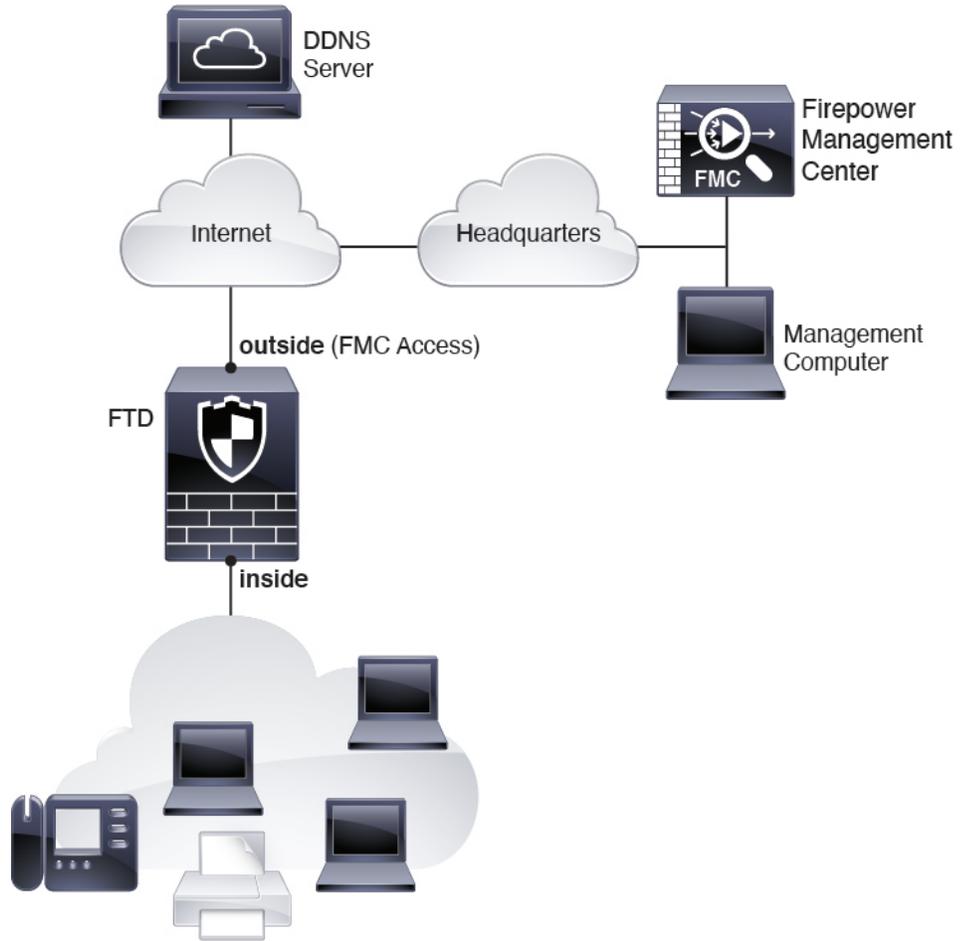
데이터 인터페이스에서의 FMC 액세스에는 다음과 같은 제한이 있습니다.

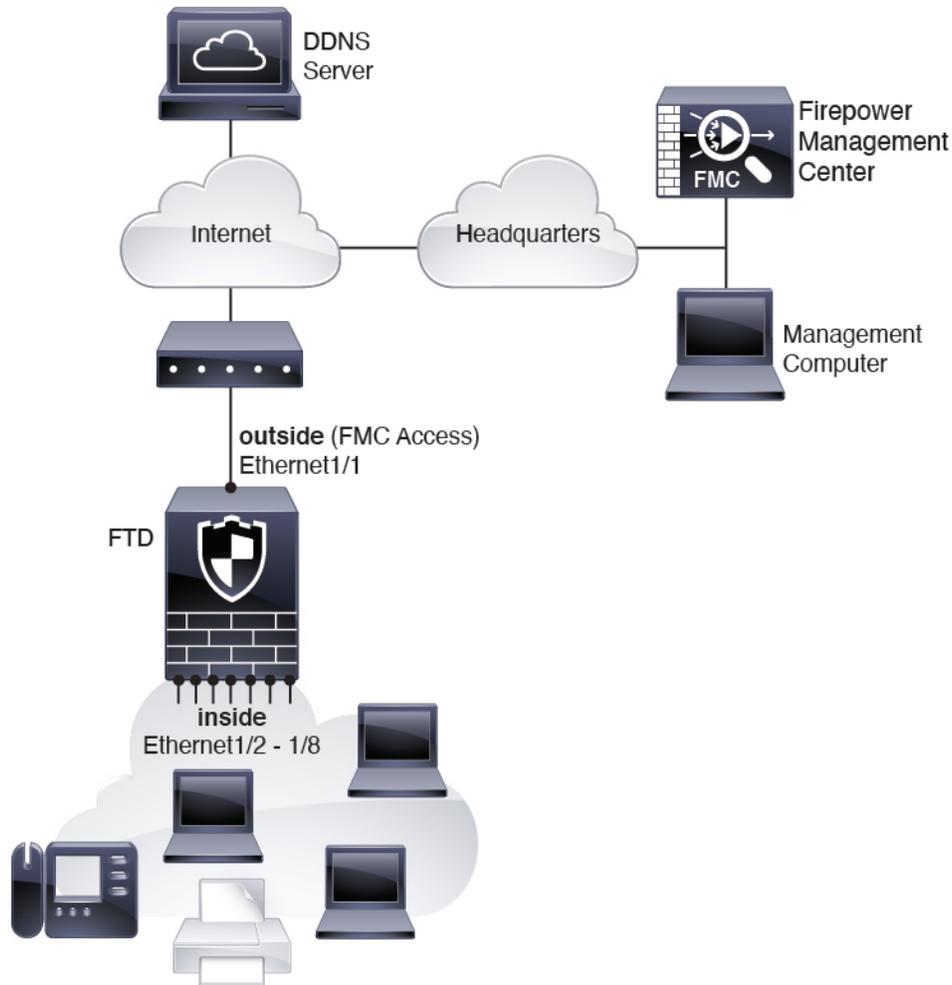
- 하나의 물리적 데이터 인터페이스에서만 FMC 액세스를 활성화할 수 있습니다. 하위 인터페이스 또는 EtherChannel은 사용할 수 없습니다.
- 이 인터페이스는 관리 전용일 수 없습니다.
- 라우팅 인터페이스를 사용하는 라우팅 방화벽 모드 전용입니다.
- 고가용성은 지원되지 않습니다. 이 경우에는 관리 인터페이스를 사용해야 합니다.
- PPPoE는 지원되지 않습니다. ISP에 PPPoE가 필요한 경우 FTD와 WAN 모뎀 간에 PPPoE를 지원하는 라우터를 설치해야 합니다.
- 인터페이스는 전역 VRF에만 있어야 합니다.
- 별도의 관리 및 이벤트 전용 인터페이스를 사용할 수 없습니다.
- SSH는 데이터 인터페이스에 대해 기본적으로 활성화되어 있지 않으므로 나중에 FMC를 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.

다음 그림에는 중앙 본사의 FMC 및 외부 인터페이스에 대한 FMC 액세스가 나와있는 FTD가 나와 있습니다.

FTD 또는 FMC는 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:





CLI를 사용한 중앙 관리자 사전 구성

초기 설정을 수행하려면 FTD CLI에 연결합니다. 초기 구성에 CLI를 사용하는 경우 관리 및 FMC 액세스 인터페이스 설정만 유지됩니다.

Before you begin

FMC의 초기 구성을 구축하고 실행합니다. [FMC 시작 가이드](#)를 참조하십시오. FTD를 설정하기 전에 FMC IP 주소 또는 호스트 이름을 알아야 합니다.

Procedure

단계 1 디바이스 전원을 켭니다.

단계 2 콘솔 포트에서 또는 관리 인터페이스에 대한 SSH를 사용하여 FTD CLI에 연결합니다. 이 인터페이스는 기본적으로 DHCP 서버에서 IP 주소를 가져옵니다. 이 절차를 수행하려면 관리 인터페이스 네트워크 설정을 변경해야 하므로 연결이 끊어지지 않도록 콘솔 포트를 사용하는 것이 좋습니다.

콘솔 포트는 FXOS CLI에 연결됩니다. SSH 세션은 FTD CLI에 직접 연결됩니다.

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

콘솔 포트에서 FXOS CLI에 연결합니다. FXOS에 처음 로그인하면 비밀번호를 변경하라는 메시지가 표시됩니다. 이 비밀번호는 SSH의 FTD 로그인에도 사용됩니다.

Note 비밀번호가 이미 변경되었거나 비밀번호를 모르는 경우 비밀번호를 기본값으로 재설정하려면 디바이스의 이미지를 재설치해야 합니다. [이미지 재설치 절차는 FXOS 문제 해결 설명서를 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 콘솔 포트에서 FXOS에 연결한 경우 FTD CLI에 연결합니다.

connect ftd

Example:

```
firepower# connect ftd
>
```

단계 5 FTD에 처음 로그인할 경우, 최종 사용자 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 FMC 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. [FTD 명령 참조](#)를 참조하십시오.

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

다음 지침을 참조하십시오.

- **Configure IPv4 via DHCP or manually?(DHCP를 통해 또는 수동으로 IPv4를 구성하시겠습니까?)**—**manual**(수동)을 선택합니다. 관리 인터페이스를 사용할 계획은 없지만 IP 주소(예: 개인 주소)를 설정해야 합니다. 이 IP 주소는 트래픽이 데이터 인터페이스로 전달될 때 NAT 처리됩니다. 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)**— 게이트웨이를 **data-interfaces**로 설정합니다. 이 설정은 관리 트래픽을 백플레인 을 통해 전달하므로 FMC 액세스 데이터 인터페이스를 통해 라우팅될 수 있습니다.
- **If your networking information has changed, you will need to reconnect(네트워킹 정보가 변경된 경우 다시 연결해야 합니다)**— SSH를 통해 연결되어 있는 경우 연결이 끊깁니다. 관리 컴퓨터가 관리 네트워크에 있는 경우 새 IP 주소 및 비밀번호로 다시 연결할 수 있습니다. 데이터 인터페이스를 통한 기본 경로 변경으로 인해 원격 네트워크에서 다시 연결할 수 없습니다. 콘솔 연결에는 영향을 미치지 않습니다.
- **Manage the device locally?(디바이스를 로컬로 관리하시겠습니까?)**—FMC을(를) 사용하려면 **no** 를 입력합니다. **yes**로 응답할 경우 그 대신 Firepower Device Manager를 사용하게 됩니다.
- **Configure firewall mode?(방화벽 모드를 구성하시겠습니까?)**—**routed**(라우팅)를 입력합니다. 외부의 FMC 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 change the password for 'admin' to continue.
Enter new password: *****
Confirm new password: *****
You must configure the network to continue.
You must configure at least one of IPv4 or IPv6.
Do you want to configure IPv4? (y/n) [y]:
Do you want to configure IPv6? (y/n) [n]:
Configure IPv4 via DHCP or manually? (dhcp/manual) [manual]:
Enter an IPv4 address for the management interface [192.168.45.45]: 10.10.10.15
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]: ftd-1.cisco.com
Enter a comma-separated list of DNS servers or 'none' [208.67.222.222,208.67.220.220]:
Enter a comma-separated list of search domains or 'none' []:
If your networking information has changed, you will need to reconnect.
For HTTP Proxy configuration, run 'configure network http-proxy'

Manage the device locally? (yes/no) [yes]: no
Configure firewall mode? (routed/transparent) [routed]:
Configuring firewall mode ...
```

```
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 FMC 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 지금 **configure network {ipv4 | ipv6} manual** 명령을 사용하여 설정할 수 있습니다. 관리 인터페이스 게이트웨이를 아직 **data-interfaces** 로 설정하지 않은 경우, 이 명령이 이제 설정합니다.
- FMC에 FTD를 추가하면 FMC는 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. FMC에서 나중에 FMC 액세스 인터페이스 컨피그레이션을 변경할 수 있지만, FTD 또는 FMC가 관리 연결을 재설정하지 못하게 할 수 있는 변경은 수행하지 않아야 합니다. 관리 연결이 중단되면 FTD에 이전 구축을 복구하는 **configure policy rollback** 명령이 포함됩니다.
- DDNS 서버 업데이트 URL을 설정하는 경우 FTD가 HTTPS 연결을 위해 DDNS 서버 인증서를 검증할 수 있도록 Cisco Trusted Root CA 번들에서 모든 주요 CA에 대한 인증서를 자동으로 추가합니다. FTD는 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.

FMC에서 이 FTD에 할당하는 플랫폼 설정 정책에서 데이터 인터페이스 DNS 서버가 설정됩니다. FMC에 FTD를 추가하면 로컬 설정이 유지되고 DNS 서버가 플랫폼 설정 정책에 추가되지 않

습니다. 그러나 나중에 DNS 컨피그레이션을 포함하는 FTD에 플랫폼 설정 정책을 할당하면 해당 컨피그레이션이 로컬 설정을 덮어씁니다. FMC와 FTD를 동기화하려면 이 설정과 일치하도록 DNS 플랫폼 설정을 적극적으로 구성하는 것이 좋습니다.

또한 로컬 DNS 서버는 초기 등록시 DNS 서버가 검색된 경우에만 FMC에 의해 유지됩니다. 예를 들어 관리 인터페이스를 사용하여 디바이스를 등록한 다음 나중에 **configure network management-data-interface** 명령을 사용하여 데이터 인터페이스를 구성하는 경우 FTD 컨피그레이션과 일치하도록 DNS 서버를 포함하여 FMC에서 이러한 모든 설정을 수동으로 구성해야 합니다.

- FTD를 FMC에 등록한 후 관리 인터페이스를 관리 인터페이스 또는 다른 데이터 인터페이스로 변경할 수 있습니다.
- 설정 마법사에서 설정한 FQDN이 이 인터페이스에 사용됩니다.
- 명령의 일부로 전체 디바이스 컨피그레이션을 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://deanwinchester: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 FMC access from any network, if you wish to change
the FMC 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 FMC access from any network, if you wish to change
the FMC 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 FMC에 대한 데이터 인터페이스 액세스를 제한합니다.

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

기본적으로 모든 네트워크가 허용됩니다.

단계 8 이 FTD를 관리할 FMC을(를) 식별합니다.

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

- **{hostname | IPv4_address | IPv6_address | DONTRESOLVE}**—FMC의 FQDN 또는 IP 주소를 지정합니다. FMC의 주소를 직접 지정할 수 없는 경우 **DONTRESOLVE**를 사용합니다. 하나 이상의 디바이스(FMC 또는 FTD)에는 두 디바이스 간 양방향 SSL 암호화 통신 채널을 설정하기 위한 연결 가능한 IP 주소가 있어야 합니다. 이 명령에서 **DONTRESOLVE**를 지정하는 경우 FTD에 연결할 수 있는 IP 주소 또는 호스트 이름이 있어야 합니다.
- **reg_key**—FTD 등록시 FMC에 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**—FMC에서 지정할 고유한 일회성 문자열을 지정합니다. 관리에 데이터 인터페이스를 사용하는 경우 등록을 위해 FTD 및 FMC 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 FMC에 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 FTD을(를) 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

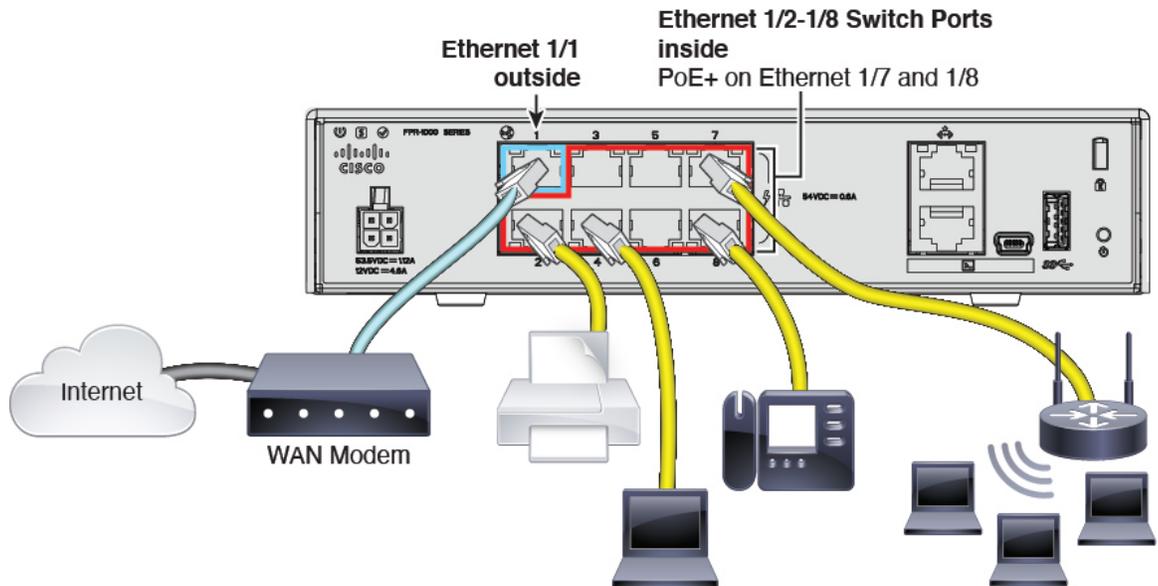
중앙 본사에서 FTD를 받은 후에는 외부 인터페이스에서 인터넷에 액세스할 수 있도록 방화벽에 케이블을 연결하고 전원을 켜면 됩니다. 그러면 중앙 관리자가 구성을 완료할 수 있습니다.

Firepower 1010 케이블 연결

FMC는 중앙 본사에 있으며 인터넷을 통해 FTD에 연결할 수 있습니다.

프로시저

단계 1 Firepower 1010 케이블을 연결합니다.



- 내부 엔드 포인트를 스위치 포트(이더넷 1/2 ~ 1/8)에 연결합니다.
- 이더넷 1/1을 외부 라우터에 연결합니다.

단계 2 디바이스 전원을 켭니다.

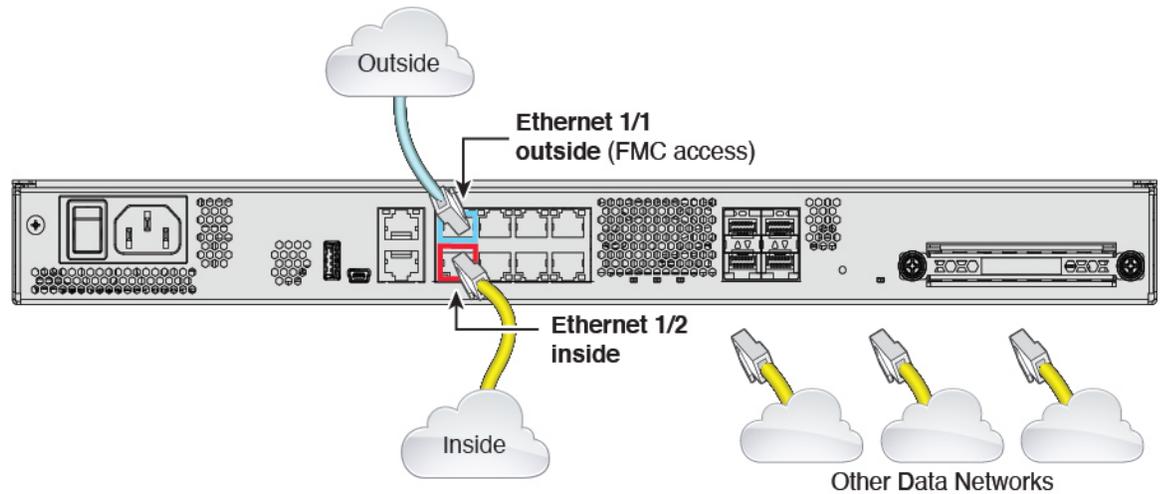
단계 3 디바이스가 작동 중이며 FMC에 등록할 준비가 되었음을 중앙 관리자에게 알립니다.

Firepower 1100 케이블 연결

FMC는 중앙 본사에 있으며 인터넷을 통해 FTD에 연결할 수 있습니다.

프로시저

단계 1 Firepower 1100 케이블을 연결합니다.



- 내부 인터페이스를 내부 네트워크에 연결합니다. 중앙 관리자가 다른 인터페이스를 사용하도록 지시하지 않는 한 내부에 이더넷 1/2 인터페이스를 사용합니다.
- 외부 인터페이스를 외부 라우터에 연결합니다. 중앙 관리자가 다른 인터페이스를 사용하도록 지시하지 않는 한 외부에 이더넷 1/1 인터페이스를 사용합니다.
- 중앙 관리자가 요청한 경우 나머지 인터페이스를 다른 네트워크에 연결합니다.

단계 2 디바이스 전원을 켭니다.

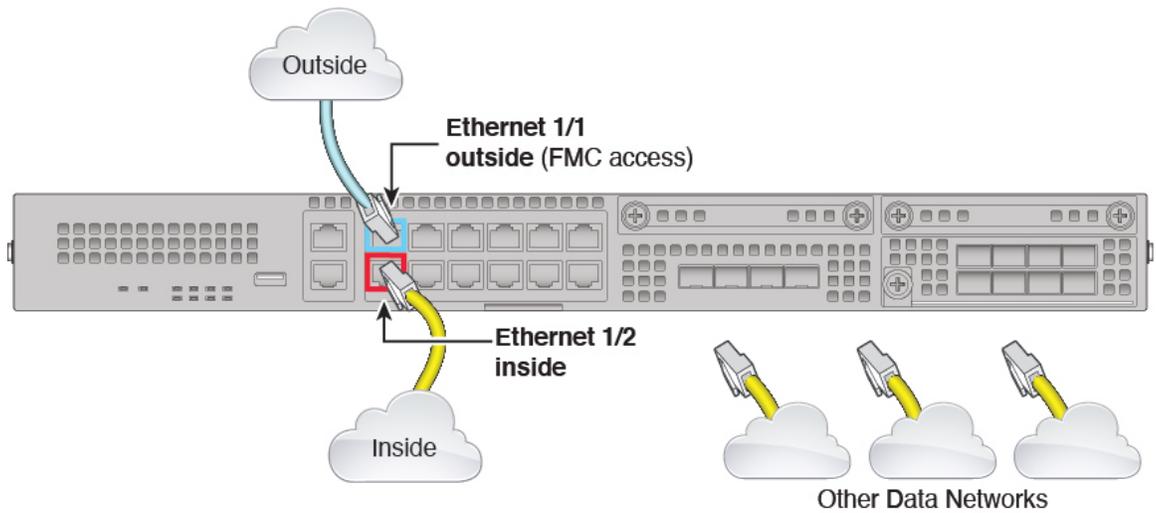
단계 3 디바이스가 작동 중이며 FMC에 등록할 준비가 되었음을 중앙 관리자에게 알립니다.

Firepower 2100 케이블 연결

FMC는 중앙 본사에 있으며 인터넷을 통해 FTD에 연결할 수 있습니다.

프로시저

단계 1 Firepower 2100 케이블을 연결합니다.



- 내부 인터페이스를 내부 네트워크에 연결합니다. 중앙 관리자가 다른 인터페이스를 사용하도록 지시하지 않는 한 내부에 이더넷 1/2 인터페이스를 사용합니다.
- 외부 인터페이스를 외부 라우터에 연결합니다. 중앙 관리자가 다른 인터페이스를 사용하도록 지시하지 않는 한 외부에 이더넷 1/1 인터페이스를 사용합니다.
- 중앙 관리자가 요청한 경우 나머지 인터페이스를 다른 네트워크에 연결합니다.

단계 2 디바이스 전원을 켭니다.

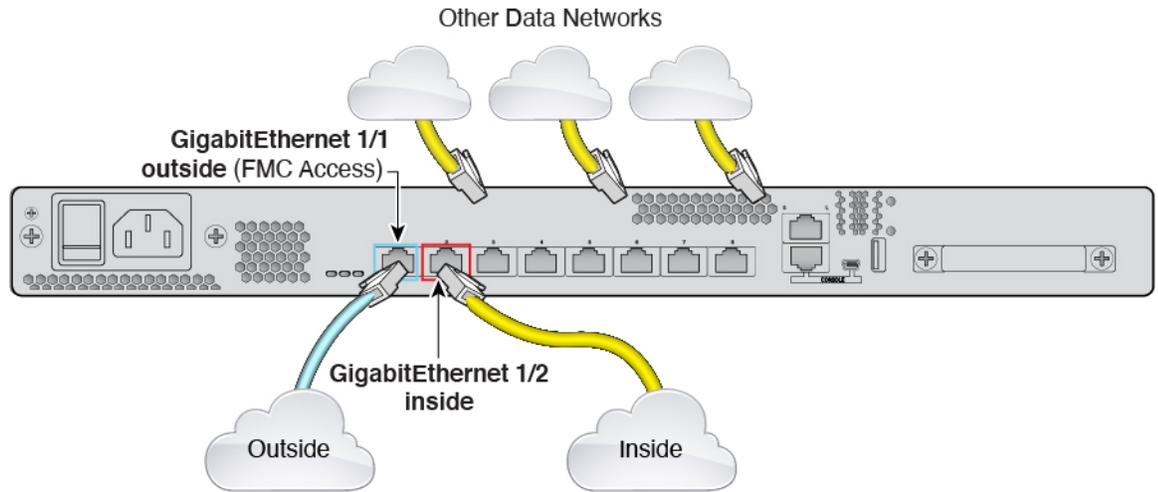
단계 3 디바이스가 작동 중이며 FMC에 등록할 준비가 되었음을 중앙 관리자에게 알립니다.

ASA 5508-X 또는 5516-X 케이블 연결

FMC는 중앙 본사에 있으며 인터넷을 통해 FTD에 연결할 수 있습니다.

프로시저

단계 1 ASA 5508-X 또는 5516-X 케이블을 연결합니다.



- 내부 인터페이스를 내부 네트워크에 연결합니다. 중앙 관리자가 다른 인터페이스를 사용하도록 지시하지 않는 한 내부에 GigabitEthernet 1/2 인터페이스를 사용합니다.
- 외부 인터페이스를 외부 라우터에 연결합니다. 중앙 관리자가 다른 인터페이스를 사용하도록 지시하지 않는 한 외부에 GigabitEthernet 1/1 인터페이스를 사용합니다.
- 중앙 관리자가 요청한 경우 나머지 인터페이스를 다른 네트워크에 연결합니다.

단계 2 디바이스 전원을 켭니다.

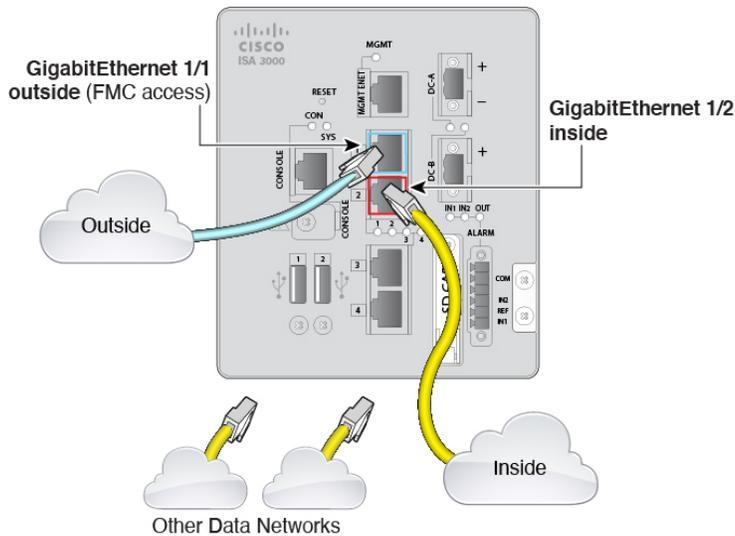
단계 3 디바이스가 작동 중이며 FMC에 등록할 준비가 되었음을 중앙 관리자에게 알립니다.

ISA 3000 케이블 연결

FMC는 중앙 본사에 있으며 인터넷을 통해 FTD에 연결할 수 있습니다.

프로시저

단계 1 ISA 3000 케이블을 연결합니다.



- 내부 인터페이스를 내부 네트워크에 연결합니다. 중앙 관리자가 다른 인터페이스를 사용하도록 지시하지 않는 한 내부에 GigabitEthernet 1/2 인터페이스를 사용합니다.
- 외부 인터페이스를 외부 라우터에 연결합니다. 중앙 관리자가 다른 인터페이스를 사용하도록 지시하지 않는 한 외부에 GigabitEthernet 1/1 인터페이스를 사용합니다.
- 중앙 관리자가 요청한 경우 나머지 인터페이스를 다른 네트워크에 연결합니다.

단계 2 디바이스 전원을 켭니다.

단계 3 디바이스가 작동 중이며 FMC에 등록할 준비가 되었음을 중앙 관리자에게 알립니다.

중앙 관리자 사후 구성

원격 지사 관리자가 외부 인터페이스에서 인터넷에 액세스할 수 있도록 FTD에 케이블을 연결하고 나면 FMC에 FTD을(를) 등록하고 디바이스의 구성을 완료할 수 있습니다.

에 로그인 Firepower Management Center

FMC를 사용해 FTD를 구성하고 모니터링합니다.

시작하기 전에

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

프로시저

단계 1 지원되는 브라우저를 사용해 다음 URL을 입력합니다.

https://fmc_ip_address

단계 2 사용자 이름 및 비밀번호를 입력합니다.

단계 3 **Log In**(로그인)을 클릭합니다.

Firepower Management Center 라이선스 얻기

모든 라이선스는 FMC를 통해 FTD에 제공됩니다. 다음 라이선스를 구매할 수 있습니다.

- **Threat**—보안 인텔리전스 및 Cisco Firepower Next-Generation IPS
- **Malware**—네트워크용 Advanced Malware Protection(AMP)
- **URL**—URL 필터링
- **RA VPN**—AnyConnect Plus, AnyConnect Apex 또는 AnyConnect VPN 전용

시작하기 전에

- [Cisco Smart Software Manager](#)에서 마스터 계정을 만듭니다.
아직 어카운트가 없는 경우 [새 어카운트 설정](#) 링크를 클릭합니다. Smart Software Manager에서 조직의 마스터 계정을 만들 수 있습니다.
- Cisco Smart Software Licensing 계정은 일부 기능(export-compliance 플래그를 사용하여 활성화됨)을 사용하려면 강력한 암호화(3DES/AES) 라이선스 자격을 얻어야 합니다.

프로시저

단계 1 Smart Licensing 계정에서 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 **Find Products and Solutions**(제품 및 솔루션 찾기) 검색 필드를 사용합니다. 다음 라이선스 PID를 검색합니다.

그림 2: 라이선스 검색



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

- Threat, Malware, URL 라이선스 조합:
 - L-FPR1010T-TMC =

- L-FPR1120T-TMC =
- L-FPR1140T-TMC =
- L-FPR1150T-TMC =
- L-FPR2110T-TMC=
- L-FPR2120T-TMC=
- L-FPR2130T-TMC=
- L-FPR2140T-TMC=
- L-ASA5508T-TMC=
- L-ASA5516T-TMC=
- L-ISA3000T-TMC=

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

- FPR1010T-TMC-1Y
- L-FPR1010T-TMC-3Y
- L-FPR1010T-TMC-5Y
- L-FPR1120T-TMC-1Y
- L-FPR1120T-TMC-3Y
- L-FPR1120T-TMC-5Y
- L-FPR1140T-TMC-1Y
- L-FPR1140T-TMC-3Y
- L-FPR1140T-TMC-5Y
- L-FPR1150T-TMC-1Y
- L-FPR1150T-TMC-3Y
- L-FPR1150T-TMC-5Y
- FPR2110T-TMC-1Y
- L-FPR2110T-TMC-3Y
- L-FPR2110T-TMC-5Y
- L-FPR2120T-TMC-1Y

- L-FPR2120T-TMC-3Y
- L-FPR2120T-TMC-5Y
- L-FPR2130T-TMC-1Y
- L-FPR2130T-TMC-3Y
- L-FPR2130T-TMC-5Y
- L-FPR2140T-TMC-1Y
- L-FPR2140T-TMC-3Y
- L-FPR2140T-TMC-5Y

- L-ASA5508T-TMC-1Y
- L-ASA5508T-TMC-3Y
- L-ASA5508T-TMC-5Y
- L-ASA5516T-TMC-1Y
- L-ASA5516T-TMC-3Y
- L-ASA5516T-TMC-5Y

- L-ISA3000T-TMC-1Y
- L-ISA3000T-TMC-3Y
- L-ISA3000T-TMC-5Y

- RA VPN—[Cisco AnyConnect 주문 가이드](#)를 참조하십시오.

단계 2 아직 등록하지 않은 경우 FMC을 Smart Licensing 서버에 등록합니다.

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

FTD을 FMC에 등록합니다.

FTD를 FMC에 수동으로 등록합니다.

시작하기 전에

- FTD 초기 구성
 - FTD 관리 IP 주소 또는 호스트 이름 및 NAT ID
 - FMC 등록 키

프로시저

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

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

The screenshot shows the 'Add Device' configuration window. It contains the following fields and options:

- Host:** Input field containing 'ftd-1.cisco.com'.
- Display Name:** Input field containing 'ftd-1.cisco.com'.
- Registration Key:*** Input field containing '....'.
- Group:** Dropdown menu set to 'None'.
- Access Control Policy:*** Dropdown menu set to 'inside-outside'.
- Smart Licensing:**
 - Malware
 - Threat
 - URL Filtering
- Advanced:**
 - Unique NAT ID:†** Input field containing 'natid56'.
 - Transfer Packets

At the bottom, there are two buttons: 'Cancel' and 'Register'.

다음 매개변수를 설정합니다.

- **Host(호스트)**—추가하려는 FTD의 IP 주소 또는 호스트 이름을 입력합니다. FTD 초기 구성에서 FMC IP 주소와 NAT ID를 모두 지정한 경우 이 필드를 비워둘 수 있습니다.
- **Display Name(표시 이름)**—FMC에서 표시하려는 FTD의 이름을 입력합니다.
- **Registration key(등록 키)**—FTD 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 정책 이미 있는 경우가 아니라면 **Create new policy(새 정책 생성)**, **Block all traffic(모든 트래픽 차**

단)을 선택합니다. 나중에 트래픽을 허용하도록 변경할 수 있습니다. [내부에서 외부로 트래픽을 허용합니다.](#), 33 페이지를 참조하십시오.

그림 3: **New Policy**

The screenshot shows the 'New Policy' configuration interface. It includes 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' (which is selected and highlighted with a red box), 'Intrusion Prevention', and 'Network Discovery'.
- Buttons:** 'Cancel' and 'Save' buttons at the bottom right.

- **Smart license** (스마트 라이선싱) - 구축하려는 기능에 필요한 스마트 라이선스(AMP 약성코드 검사를 사용하려는 경우 **Malware**(악성코드), 침입 방지를 사용하려는 경우 **Threat**(위협), 카테고리 기반 URL 필터링을 구현하려는 경우 **URL**)를 할당합니다. 참고: 디바이스를 추가한 후 **System**(시스템) > **Licenses**(라이선스) > **Smart Licenses**(스마트 라이선스) 페이지에서 AnyConnect Remote Access VPN 라이선스를 적용할 수 있습니다.
- **Unique NAT ID**(고유 NAT ID)—FTD 초기 구성에서 지정한 NAT ID를 지정합니다.
- **Transfer Packets**(패킷 전송) - 디바이스가 FMC에 패킷을 전송하도록 허용합니다. 이 옵션이 활성화되어 IPS 또는 Snort 같은 이벤트가 트리거되면 디바이스는 검사를 위해 이벤트 메타데이터 정보 및 패킷 데이터를 FMC에 전송합니다. 비활성화하면 FMC에 이벤트 정보만 전송하고 패킷 데이터는 전송하지 않습니다.

단계 3 **Register**(등록)를 클릭하여 등록을 확인합니다.

등록에 성공하면 디바이스가 목록에 추가됩니다. 오류가 발생하면 오류 메시지가 표시됩니다. FTD 등록에 실패하면 다음 항목을 확인하십시오.

- **Ping**—다음 명령을 사용해 FTD CLI에 액세스하고 FMC IP 주소에 Ping을 보냅니다.

ping system ip_address

Ping이 실패하는 경우 **show network** 명령을 사용해 네트워크 설정을 확인합니다. FTD 관리 IP 주소를 변경해야 하는 경우 **configure network {ipv4 | ipv6} manual** 명령을 사용합니다. FMC 액세스를 위해 데이터 인터페이스를 구성한 경우 **configure network management-data-interface** 명령을 사용합니다.

- 등록 키, NAT ID 및 FMC IP 주소 - 두 디바이스에서 동일한 등록 키 및 NAT ID가 사용되고 있는지 확인합니다. **configure manager add** 명령을 사용해 FTD에서 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 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.

기본 보안 정책을 구성하려면 다음 작업을 완료합니다.

①	인터페이스 구성(6.5 이상), 20 페이지 인터페이스 구성(6.4), 24 페이지.
②	DHCP 서버 구성, 28 페이지.
③	기본 경로 추가, 29 페이지.
④	NAT 구성, 30 페이지.
⑤	내부에서 외부로 트래픽을 허용합니다., 33 페이지.
⑥	구성 구축, 34 페이지.

인터페이스 구성(6.5 이상)

스위치 포트에 대한 VLAN1 인터페이스를 추가하거나 스위치 포트를 방화벽 인터페이스로 변환하고 인터페이스를 보안 영역에 할당하거나, 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. 기본적으로 Ethernet1/1은 외부용으로 사용할 수 있는 일반 방화벽 인터페이스이며, 나머지 인터페이스는 VLAN 1의 스위치 포트입니다. VLAN1 인터페이스를 추가한 후에는 이를 내부

인터페이스로 지정할 수 있습니다. 또는 다른 VLAN에 스위치 포트를 할당하거나 스위치 포트를 방화벽 인터페이스로 변환할 수 있습니다.

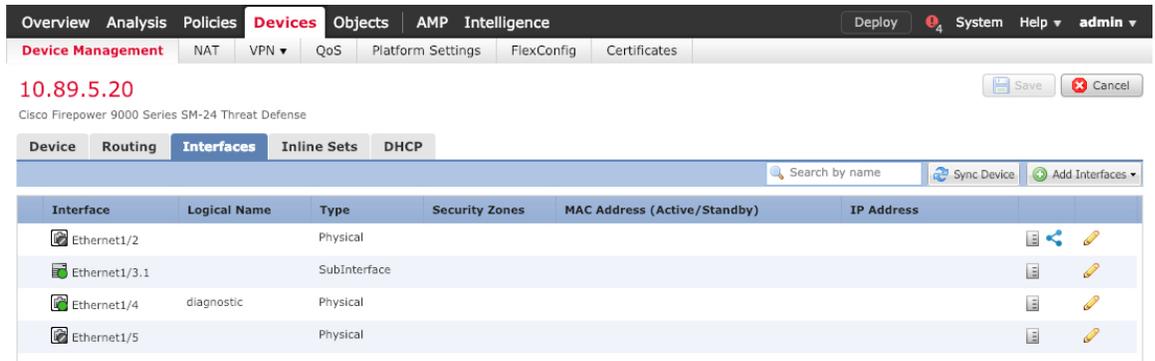
일반적인 에지 라우팅 상황의 경우, 내부 인터페이스에서 정적 주소를 정의하는 반면 ISP에서 온 DHCP를 통해 외부 인터페이스 주소를 가져옵니다.

다음 예에서는 DHCP를 사용하는 외부 인터페이스(Ethernet1/1)에서 고정 주소 및 라우팅 모드를 사용하여 내부 인터페이스(VLAN1)에 라우팅 모드를 구성합니다.

프로시저

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

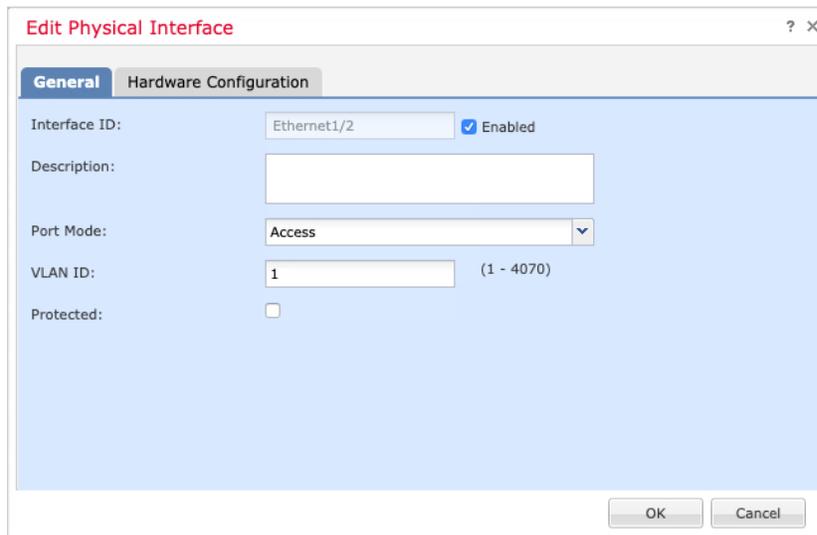
단계 2 **Interfaces**(인터페이스)를 클릭합니다.



단계 3 (선택 사항) **SwitchPort**(스위치포트) 열의 슬라이더를 클릭하여 비활성화(☒)로 표시되면 스위치 포트(Ethernet1/2~1/8)의 스위치 포트를 비활성화합니다.

단계 4 스위치 포트를 활성화합니다.

a) 스위치 포트에 대해 수정(✎)를 클릭합니다.



- b) **Enabled**(활성화됨) 체크 박스를 선택하여 인터페이스를 활성화합니다.
- c) (선택 사항) VLAN ID를 변경합니다. 기본값은 1입니다. 그런 다음 이 ID와 일치하는 VLAN 인터페이스를 추가합니다.
- d) **OK**(확인)를 클릭합니다.

단계 5 *Inside*(내부) VLAN 인터페이스를 추가합니다.

- a) **Add Interfaces**(인터페이스 추가) > **VLAN Interface**(VLAN 인터페이스)를 클릭합니다.

General(일반) 탭이 표시됩니다.

The screenshot shows the 'Add VLAN Interface' dialog box with the following configuration:

- Name:** inside (with an 'Enabled' checkbox checked)
- Description:** (empty text box)
- Mode:** None (dropdown menu)
- Security Zone:** inside_zone (dropdown menu)
- MTU:** 1500 (range: 64 - 9198)
- VLAN ID *:** 1 (range: 1 - 4070)
- Disable Forwarding on Interface Vlan:** None (dropdown menu)

The 'Associated Interface' table is currently empty, displaying 'No records to display'. The 'OK' and 'Cancel' buttons are located at the bottom right of the dialog.

- 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) **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.

f) **VLAN ID**를 **1**로 설정합니다.

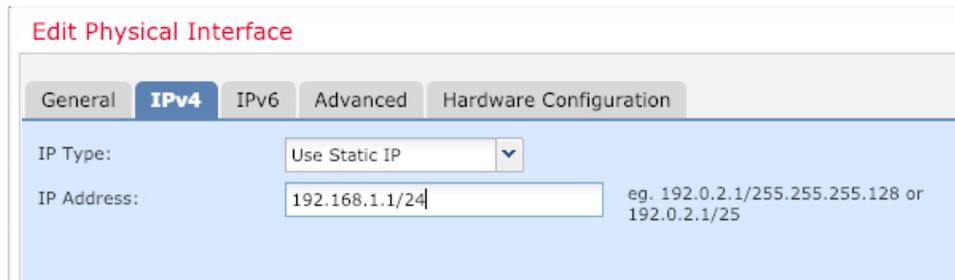
기본적으로 모든 스위치 포트는 VLAN 1로 설정됩니다. 여기서 다른 VLAN ID를 선택하는 경우에는 각 스위치 포트를 새 VLAN ID에 맞게 수정해야 합니다.

인터페이스를 저장한 후에는 VLAN ID를 변경할 수 없습니다. VLAN ID는 사용된 VLAN 태그이자 구성의 인터페이스 ID입니다.

g) **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.

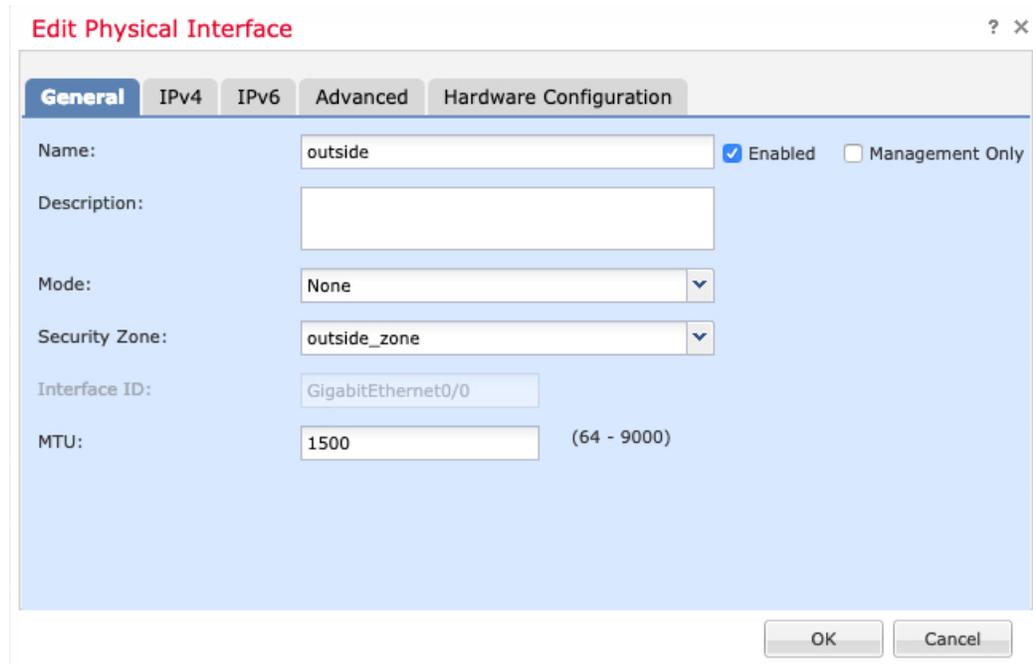


- **IPv6** - 상태 비저장 자동 구성을 하려면 **Autoconfiguration**(자동 구성) 확인란을 선택합니다.

h) **OK**(확인)를 클릭합니다.

단계 6 *Outside*(외부)로 사용하려는 Ethernet1/1에 수정(✎)를 클릭합니다.

General(일반) 탭이 표시됩니다.



참고 FMC 액세스 관리를 위해 이 인터페이스를 미리 구성한 경우 인터페이스의 이름이 이미 지정되고 활성화되어 있으며 주소가 지정됩니다. 이러한 기본 설정을 변경하면 FMC 관리 연결이 중단되므로 이 설정을 변경하면 안됩니다. 트래픽 정책을 통해 이 화면에서 보안 영역을 구성할 수 있습니다.

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.

- **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', with a range of '(1 - 255)' indicated to the right.

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

f) **OK(확인)**를 클릭합니다.

단계 7 **Save(저장)**를 클릭합니다.

인터페이스 구성(6.4)

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

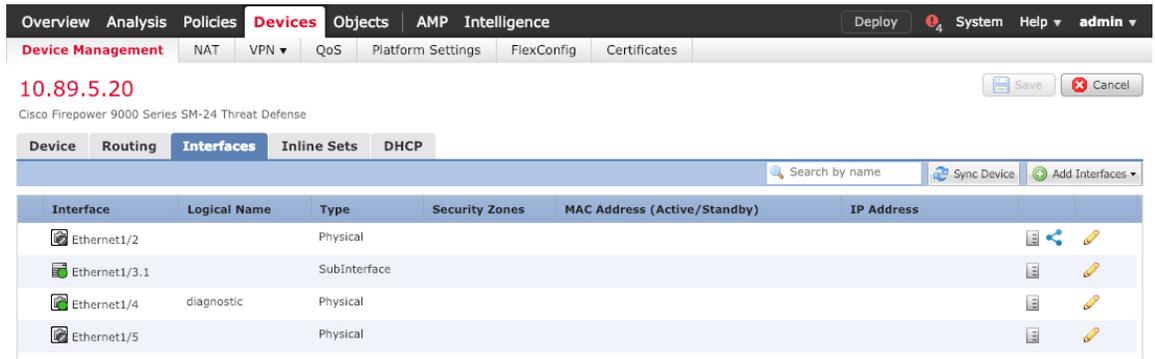
일반적인 에지 라우팅 상황의 경우, 내부 인터페이스에서 정적 주소를 정의하는 반면 ISP에서 온 DHCP를 통해 외부 인터페이스 주소를 가져옵니다.

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

프로시저

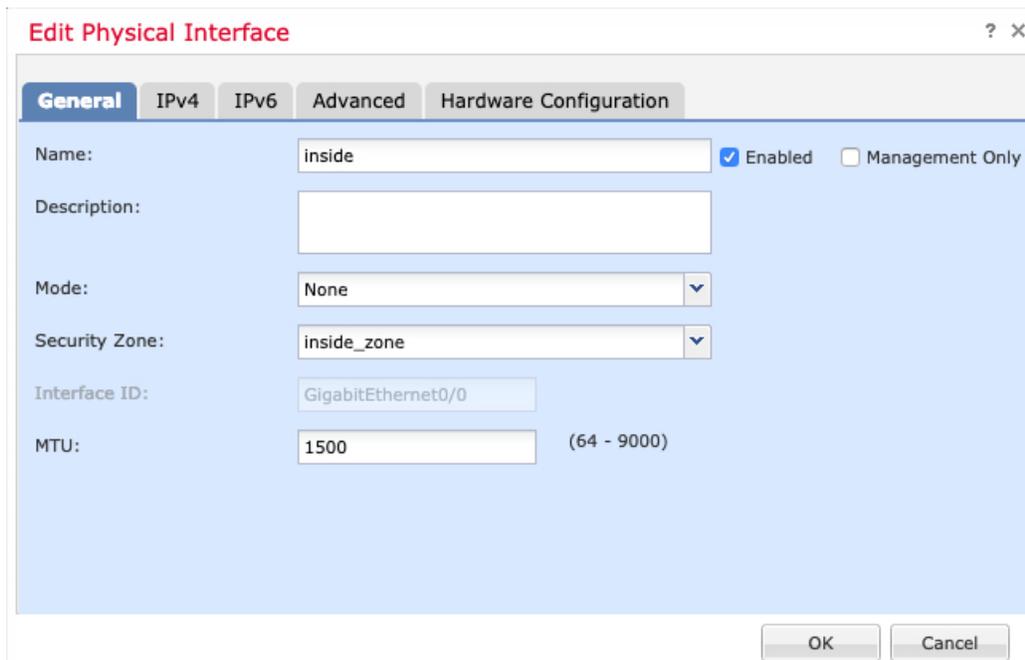
단계 1 **Devices(디바이스) > Device Management(디바이스 관리)**를 선택하고 방화벽에 대해 수정(✎)를 클릭합니다.

단계 2 **Interfaces(인터페이스)**를 클릭합니다.



단계 3 내부에 사용할 인터페이스의 수정(✎)를 클릭합니다.

General(일반) 탭이 표시됩니다.



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

예를 들어 인터페이스에 **inside**라는 이름을 지정합니다.

- b) **Enable(활성화)** 확인란을 선택합니다.
- c) **Mode(모드)**는 **None(없음)** 상태로 남겨둡니다.
- d) **Security Zone(보안 영역)** 드롭다운 목록에서 기존의 내부 보안 영역을 선택하거나 **New(새로 만들기)**를 클릭하여 새 보안 영역을 추가합니다.

예를 들어 **inside_zone**이라는 영역을 추가합니다. 각 인터페이스는 보안 영역 및/또는 인터페이스 그룹에 할당되어야 합니다. 인터페이스는 하나의 보안 영역에만 속할 수 있지만, 여러 인터페이스 그룹에 속할 수도 있습니다. 영역 또는 그룹을 기준으로 보안 정책을 적용합니다. 예를 들어 내부 인터페이스는 내부 영역에, 외부 인터페이스는 외부 영역에 할당할 수 있습니다. 트래픽이 내부에서 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.

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

- f) **OK(확인)**를 클릭합니다.

단계 4 외부에서 사용하려는 인터페이스의 수정(✎)를 클릭합니다.

General(일반) 탭이 표시됩니다.

Edit Physical Interface ? x

General IPv4 IPv6 Advanced Hardware Configuration

Name: Enabled Management Only

Description:

Mode: ▼

Security Zone: ▼

Interface ID:

MTU: (64 - 9000)

OK Cancel

참고 FMC 액세스 관리를 위해 이 인터페이스를 미리 구성한 경우 인터페이스의 이름이 이미 지정되고 활성화되어 있으며 주소가 지정됩니다. 이러한 기본 설정을 변경하면 FMC 관리 연결이 중단되므로 이 설정을 변경하면 안됩니다. 트래픽 정책을 통해 이 화면에서 보안 영역을 구성할 수 있습니다.

- 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.
 - **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.

Edit Physical Interface

General **IPv4** IPv6 Advanced Hardware Configuration

IP Type: Use DHCP

Obtain default route using DHCP:

DHCP route metric: 1 (1 - 255)

- **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

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

프로시저

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

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

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

Add Server ? X

Interface* inside

Address Pool* 10.9.7.9-10.9.7.25 (2.2.2.10-2.2.2.20)

Enable DHCP Server

OK Cancel

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

단계 4 **OK**(확인)를 클릭합니다.

단계 5 **Save(저장)**를 클릭합니다.

기본 경로 추가

기본 경로는 일반적으로 외부 인터페이스에서 접근 가능한 업스트림 라우터를 가리킵니다. 외부 인터페이스에 DHCP를 사용하는 경우 디바이스가 이미 기본 경로를 수신했을 수 있습니다. 수동으로 경로를 추가해야 하는 경우 이 절차를 완료합니다. DHCP 서버에서 기본 경로를 수신한 경우, **Devices(디바이스) > Device Management(디바이스 관리) > Routing(라우팅) > Static Route(정적 경로)** 페이지의 **IPv4 Routes(IPv4 경로)** 또는 **IPv6 Routes(IPv6 경로)** 테이블에 표시됩니다.

프로시저

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

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

- **Type(유형)** - 추가하려는 정적 경로 유형에 따라 **IPv4** 또는 **IPv6** 라디오 버튼을 클릭합니다.
- **Interface(인터페이스)** - 이그레스 인터페이스를 선택합니다. 일반적으로 외부 인터페이스입니다.
- **Available Network(사용 가능한 네트워크)**—IPv4 기본 경로에 대해 **any-ipv4**를 선택하거나 IPv6 기본 경로에 대해 **any-ipv6**을 선택하고 추가를 클릭하여 선택된 네트워크 목록으로 이동합니다.

- **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.

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

단계 4 **Save**(저장)를 클릭합니다.

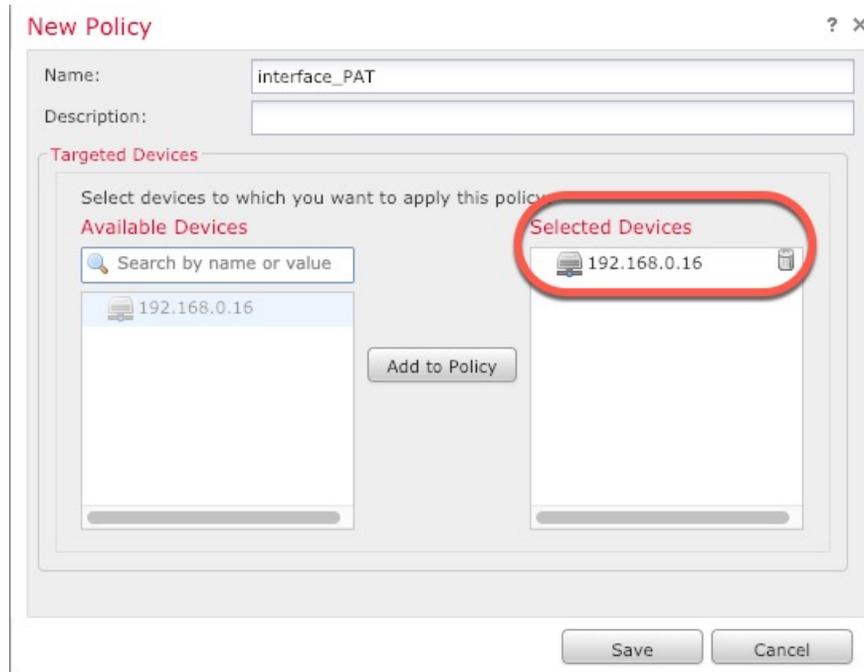
NAT 구성

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

프로시저

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

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

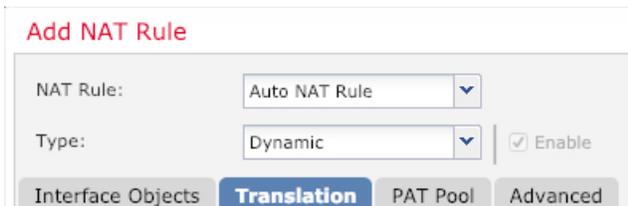


정책이 FMC를 추가합니다. 계속해서 정책에 규칙을 추가해야 합니다.

단계 3 **Add Rule**(규칙 추가)을 클릭합니다.

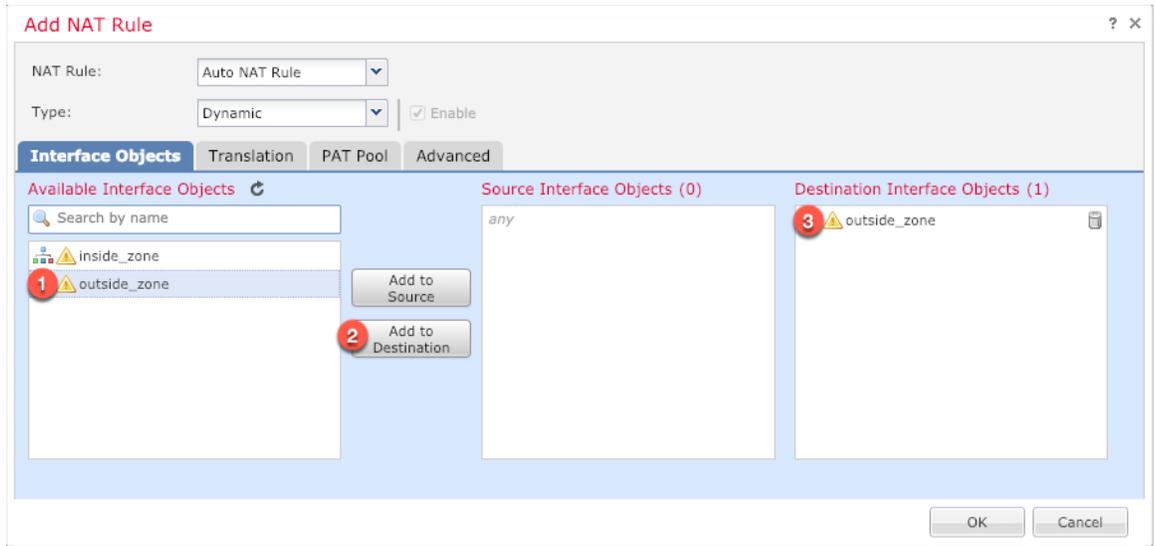
Add NAT Rule(NAT 규칙 추가) 대화 상자가 나타납니다.

단계 4 기본 규칙 옵션을 구성합니다.

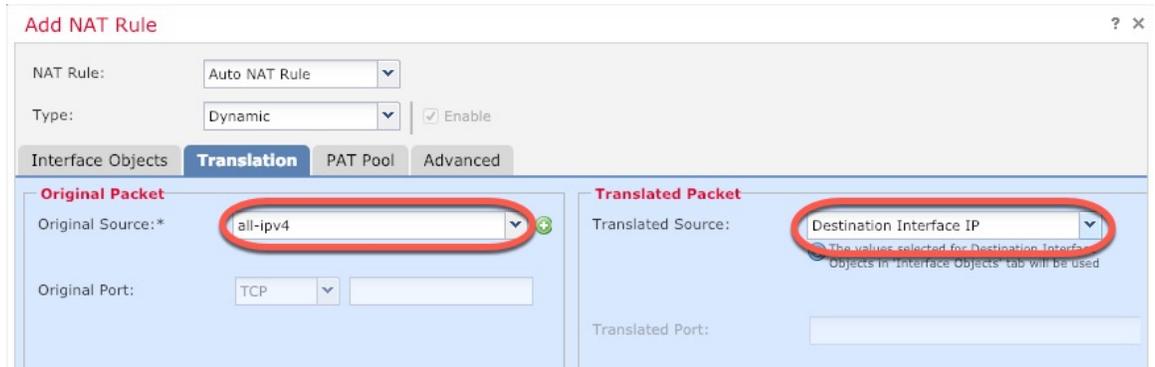


- **NAT Rule**(NAT 규칙) - **Auto NAT Rule**(자동 NAT 규칙)을 선택합니다.
- **Type**(유형) - **Dynamic**(동적)을 선택합니다.

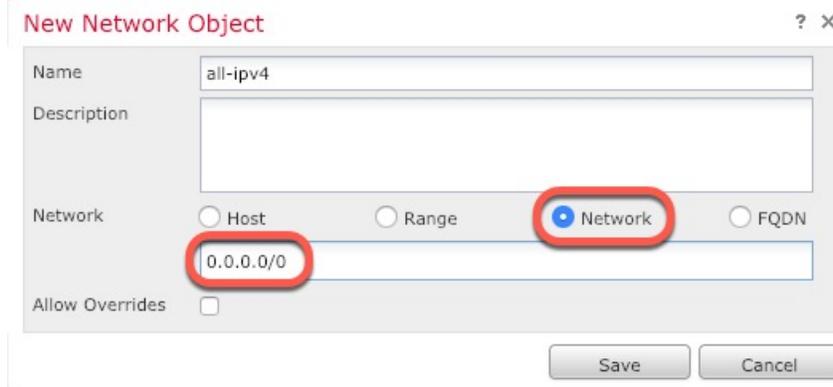
단계 5 **Interface Objects**(인터페이스 개체) 페이지에서 **Available Interface Objects**(사용 가능한 인터페이스 개체) 영역의 외부 영역을 **Destination Interface objects**(대상 인터페이스 개체) 영역에 추가합니다.



단계 6 Translation(변환) 페이지에서 다음 옵션을 설정합니다.



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

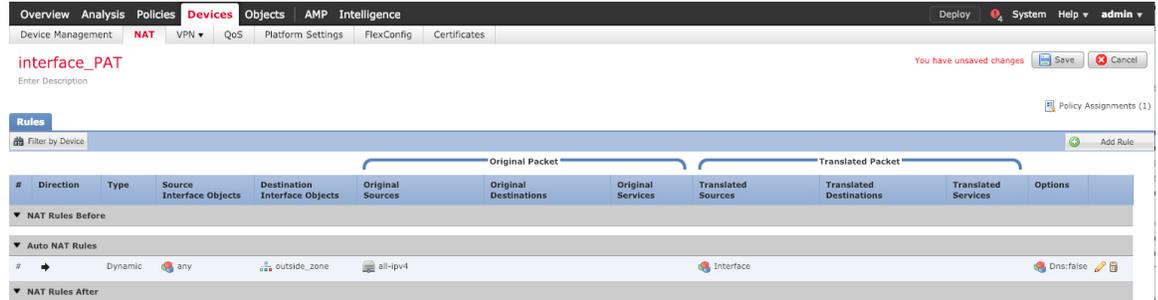


참고 자동 NAT 규칙은 개체 정의의 일부로 NAT를 추가하고 시스템 정의의 개체를 수정할 수 없기 때문에 시스템에서 정의된 **any-ipv4** 개체를 사용할 수 없습니다.

- **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.

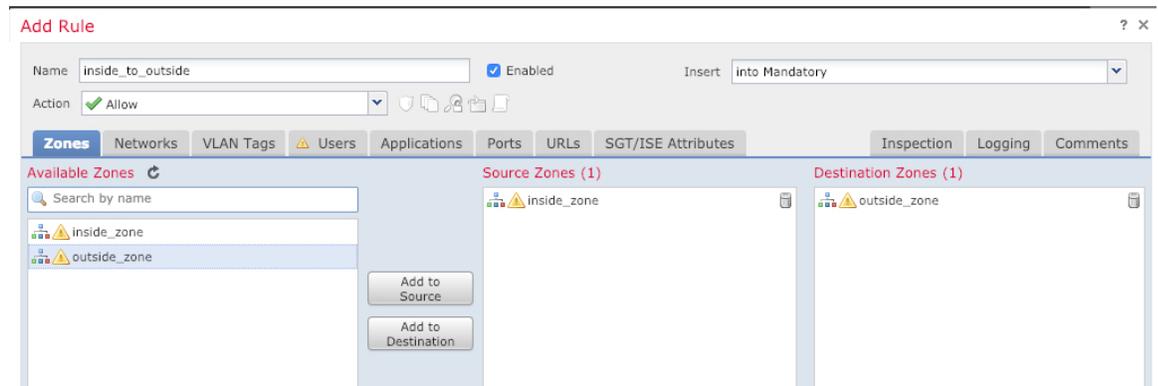
FMC를 사용해 FTD를 등록할 때 기본 액세스 컨트롤 정책인 **Block all traffic(모든 트래픽 차단)**을 생성했다면, 디바이스에 트래픽을 허용하기 위해 정책에 규칙을 추가해야 합니다. 다음 절차에서는 내부 영역에서 외부 영역으로 향하는 트래픽을 허용하는 규칙을 추가합니다. 다른 영역이 있는 경우에는 적절한 네트워크에 대한 트래픽을 허용하는 규칙을 추가해야 합니다.

고급 보안 설정 및 규칙을 구성하려면 [FMC구성 가이드](#)를 참조하십시오.

프로시저

단계 1 **Policy(정책) > Access Policy(액세스 정책) > Access Policy(액세스 정책)**을 선택하고 FTD에 할당된 액세스 컨트롤 정책에 대해 수정(✎)를 클릭합니다.

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



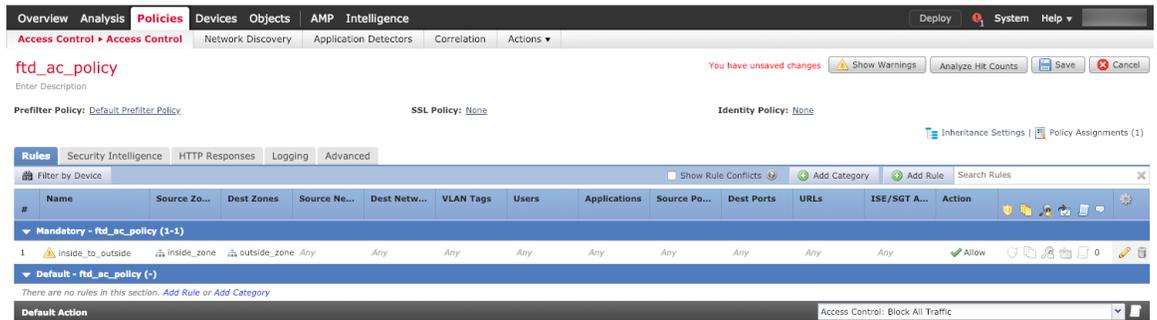
- **Name(이름)** - 예를 들어 이 규칙의 이름을 **inside_to_outside**로 지정합니다.

- **Source Zones(원본 영역) - Available Zones(사용 가능한 영역)**에서 내부 영역을 선택하고 **Add to Source(원본에 추가)**를 클릭합니다.
- **Destination Zones(대상 영역) - Available Zones(사용 가능한 영역)**에서 외부 영역을 선택하고 **Add to Destination(대상에 추가)**를 클릭합니다.

기타 설정은 변경하지 않습니다.

단계 3 **Add(추가)**를 클릭합니다.

규칙이 **Rules(규칙)** 테이블에 추가됩니다.



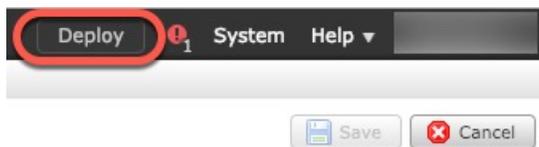
단계 4 **Save(저장)**를 클릭합니다.

구성 구축

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

프로시저

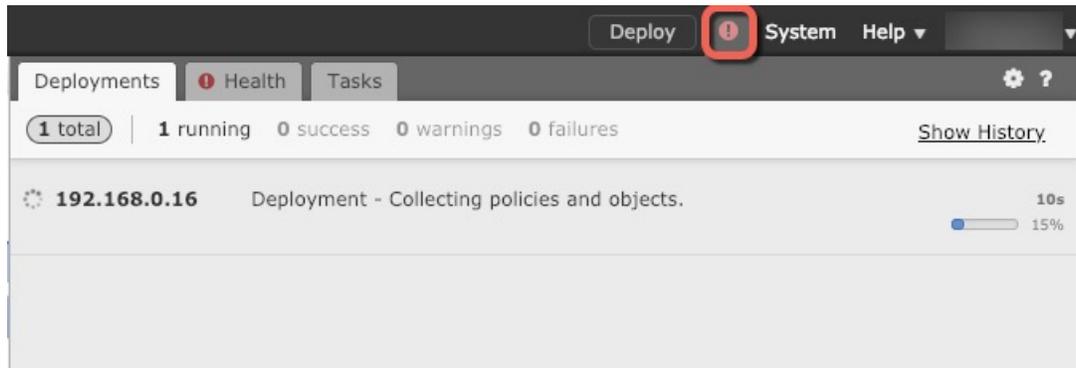
단계 1 우측 상단에서 **Deploy(구축)**를 클릭합니다.



단계 2 **Deploy policy(정책 구축)** 대화 상자에서 디바이스를 선택한 다음 **Deploy(구축)**를 클릭합니다.



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



데이터 인터페이스에서 관리 연결성 문제 해결

모델 지원—FTD

전용 관리 인터페이스를 사용하는 대신 FMC 관리용 데이터 인터페이스를 사용하는 경우, FMC에서 FTD에 대한 인터페이스 및 네트워크 설정을 변경할 때 연결이 중단되지 않도록 주의해야 합니다. FMC에 FTD를 추가한 후 관리 인터페이스 유형을 데이터에서 관리로 또는 관리에서 데이터로 변경하는 경우, 인터페이스 및 네트워크 설정이 올바르게 설정되지 않으면 관리 연결이 끊어질 수 있습니다.

이 주제는 관리 연결 끊김 문제를 해결하는 데 도움이 됩니다.

관리 연결 상태 보기

FMC의 **Devices(디바이스) > Device Management(디바이스 관리) > Device(디바이스) > Management(관리) > FMC Access Details(FMC 액세스 디테일) > Connection Status(연결 상태)** 페이지에서 관리 연결 상태를 확인합니다.

FTD CLI에서 관리 연결 상태를 확인하는 **sftunnel-status-brief** 명령을 입력합니다. **sftunnel-status** 명령을 사용하여 전체 정보를 볼 수도 있습니다.

작동 중지된 연결에 대해서는 다음 샘플 출력을 참조하십시오. 다음과 같은 피어 채널이나 하트비트 정보가 "연결"되지 않았습니다.

```
> sftunnel-status-brief
PEER:10.10.17.202
Registration: Completed.
Connection to peer '10.10.17.202' Attempted at Mon Jun 15 09:21:57 2020 UTC
Last disconnect time : Mon Jun 15 09:19:09 2020 UTC
Last disconnect reason : Both control and event channel connections with peer went down
```

피어 채널 및 하트비트 정보가 표시되는 작동 중인 연결에 대한 다음 샘플 출력을 참조하십시오.

```
> sftunnel-status-brief
PEER:10.10.17.202
```

```
Peer channel Channel-A is valid type (CONTROL), using 'eth0', connected to '10.10.17.202'
via '10.10.17.222'
Peer channel Channel-B is valid type (EVENT), using 'eth0', connected to '10.10.17.202'
via '10.10.17.222'
Registration: Completed.
IPv4 Connection to peer '10.10.17.202' Start Time: Wed Jun 10 14:27:12 2020 UTC
Heartbeat Send Time: Mon Jun 15 09:02:08 2020 UTC
Heartbeat Received Time: Mon Jun 15 09:02:16 2020 UTC
```

FTD 네트워크 정보 보기

FTD CLI에서 관리 및 FMC 액세스 데이터 인터페이스 네트워크 설정을 확인합니다.

show network

```
> show network
===== [ System Information ] =====
Hostname                : 5516X-4
DNS Servers             : 208.67.220.220,208.67.222.222
Management port        : 8305
IPv4 Default route
  Gateway               : data-interfaces
IPv6 Default route
  Gateway               : data-interfaces

===== [ br1 ] =====
State                   : Enabled
Link                    : Up
Channels                : Management & Events
Mode                    : Non-Autonegotiation
MDI/MDIX                : Auto/MDIX
MTU                     : 1500
MAC Address             : 28:6F:7F:D3:CB:8D
----- [ IPv4 ] -----
Configuration          : Manual
Address                 : 10.99.10.4
Netmask                 : 255.255.255.0
Gateway                 : 10.99.10.1
----- [ IPv6 ] -----
Configuration          : Disabled

===== [ Proxy Information ] =====
State                   : Disabled
Authentication         : Disabled

===== [ System Information - Data Interfaces ] =====
DNS Servers             :
Interfaces              : GigabitEthernet1/1

===== [ GigabitEthernet1/1 ] =====
State                   : Enabled
Link                    : Up
Name                    : outside
MTU                     : 1500
MAC Address             : 28:6F:7F:D3:CB:8F
----- [ IPv4 ] -----
Configuration          : Manual
Address                 : 10.89.5.29
Netmask                 : 255.255.255.192
Gateway                 : 10.89.5.1
----- [ IPv6 ] -----
Configuration          : Disabled
```

FTD가 FMC에 등록되었는지 확인합니다.

FTD CLI에서 FMC 등록이 완료되었는지 확인합니다. 이 명령은 관리 연결의 현재 상태를 표시하지 않습니다.

show managers

```
> show managers
Type                : Manager
Host                : 10.89.5.35
Registration        : Completed
>
```

FMC ping

FTD CLI에서 다음 명령을 사용하여 데이터 인터페이스에서 FMC를 ping합니다.

ping fmc_ip

FTD CLI에서 다음 명령을 사용하여 관리 인터페이스에서 FMC를 ping합니다. 이 인터페이스는 백플레인을 통해 데이터 인터페이스로 라우팅되어야 합니다.

ping system fmc_ip

FTD 내부 인터페이스에서 패킷 캡처

FTD CLI에서 내부 백플레인 인터페이스(nlp_int_tap)의 패킷을 캡처하여 관리 패킷이 전송되는지 확인합니다.

capture name interface nlp_int_tap trace detail match ip any any

show capture name trace detail

내부 인터페이스 상태, 통계 및 패킷 수 확인

FTD CLI에서 내부 백플레인 인터페이스, nlp_int_tap에 대한 정보를 참조하십시오.

show interace detail

```
> show interface detail
[...]
Interface Internal-Data0/1 "nlp_int_tap", is up, line protocol is up
  Hardware is en_vtun rev00, BW Unknown Speed-Capability, DLY 1000 usec
  (Full-duplex), (1000 Mbps)
  Input flow control is unsupported, output flow control is unsupported
  MAC address 0000.0100.0001, MTU 1500
  IP address 169.254.1.1, subnet mask 255.255.255.248
  37 packets input, 2822 bytes, 0 no buffer
  Received 0 broadcasts, 0 runts, 0 giants
  0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
  0 pause input, 0 resume input
  0 L2 decode drops
  5 packets output, 370 bytes, 0 underruns
  0 pause output, 0 resume output
  0 output errors, 0 collisions, 0 interface resets
  0 late collisions, 0 deferred
  0 input reset drops, 0 output reset drops
  input queue (blocks free curr/low): hardware (0/0)
  output queue (blocks free curr/low): hardware (0/0)
  Traffic Statistics for "nlp_int_tap":
```

```

37 packets input, 2304 bytes
5 packets output, 300 bytes
37 packets dropped
  1 minute input rate 0 pkts/sec,  0 bytes/sec
  1 minute output rate 0 pkts/sec,  0 bytes/sec
  1 minute drop rate, 0 pkts/sec
  5 minute input rate 0 pkts/sec,  0 bytes/sec
  5 minute output rate 0 pkts/sec,  0 bytes/sec
  5 minute drop rate, 0 pkts/sec
Control Point Interface States:
Interface number is 14
Interface config status is active
Interface state is active

```

라우팅 및 NAT 확인

FTD CLI에서 기본 경로(S*)가 추가되었고 관리 인터페이스(nlp_int_tap)에 대한 내부 NAT 규칙이 있는지 확인합니다.

show route

```

> show route

Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, V - VPN
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, + - replicated route
       SI - Static InterVRF
Gateway of last resort is 10.89.5.1 to network 0.0.0.0

S*      0.0.0.0 0.0.0.0 [1/0] via 10.89.5.1, outside
C       10.89.5.0 255.255.255.192 is directly connected, outside
L       10.89.5.29 255.255.255.255 is directly connected, outside
>

```

show nat

```

> show nat

Auto NAT Policies (Section 2)
1 (nlp_int_tap) to (outside) source static nlp_server_0_sftunnel_intf3 interface service
  tcp 8305 8305
  translate_hits = 0, untranslate_hits = 6
2 (nlp_int_tap) to (outside) source static nlp_server_0_ssh_intf3 interface service
  tcp ssh ssh
  translate_hits = 0, untranslate_hits = 73
3 (nlp_int_tap) to (outside) source static nlp_server_0_sftunnel_ipv6_intf3 interface
  ipv6 service tcp 8305 8305
  translate_hits = 0, untranslate_hits = 0
4 (nlp_int_tap) to (outside) source dynamic nlp_client_0_intf3 interface
  translate_hits = 174, untranslate_hits = 0
5 (nlp_int_tap) to (outside) source dynamic nlp_client_0_ipv6_intf3 interface ipv6
  translate_hits = 0, untranslate_hits = 0
>

```

다른 설정 확인

다른 모든 설정이 있는지 확인하려면 다음 명령을 참조하십시오. FMC의 **Devices(디바이스) > Device Management(디바이스 관리) > Device(디바이스) > Management(관리) > FMC Access Details(FMC 액세스 세부 사항) > CLI Output(CLI 출력)** 페이지에서 이러한 명령을 많이 볼 수 있습니다.

show running-config sftunnel

```
> show running-config sftunnel
sftunnel interface outside
sftunnel port 8305
```

show running-config ip-client

```
> show running-config ip-client
ip-client outside
```

show conn address fmc_ip

```
> show conn address 10.89.5.35
5 in use, 16 most used
Inspect Snort:
    preserve-connection: 0 enabled, 0 in effect, 0 most enabled, 0 most in effect

TCP nlp_int_tap 10.89.5.29(169.254.1.2):51231 outside 10.89.5.35:8305, idle 0:00:04,
bytes 86684, flags UxIO
TCP nlp_int_tap 10.89.5.29(169.254.1.2):8305 outside 10.89.5.35:52019, idle 0:00:02,
bytes 1630834, flags UIO
>
```

성공적인 DDNS 업데이트 확인

FTD CLI에서 DDNS 업데이트에 성공했는지 확인합니다.

debug ddns

```
> debug ddns
DDNS update request = /v3/update?hostname=domain.example.org&myip=209.165.200.225
Successfully updated the DDNS sever with current IP addresses
DDNS: Another update completed, outstanding = 0
DDNS: IDB SB total = 0
```

업데이트가 실패하면 **debug http** 및 **debug ssl** 명령을 사용합니다. 인증서 검증에 실패한 경우, 다음을 통해 루트 인증서가 디바이스에 설치되어 있는지 확인합니다.

show crypto ca certificates trustpoint_name

DDNS 작업을 확인하려면 다음 명령을 사용하십시오.

show ddns update interface fmc_access_ifc_name

```
> show ddns update interface outside

Dynamic DNS Update on outside:
  Update Method Name Update Destination
  RBD_DDNS not available

Last Update attempted on 04:11:58.083 UTC Thu Jun 11 2020
```

```
Status : Success
FQDN : domain.example.org
IP addresses : 209.165.200.225
```

FMC 로그 파일 확인

<https://cisco.com/go/fmc-reg-error>를 참조하십시오.

FMC가 연결을 상실할 경우 컨피그레이션을 롤백

FMC 관리를 위해 FTD에서 데이터 인터페이스를 사용하고 네트워크 연결에 영향을 주는 FMC에서 구성 변경 사항을 구축하는 경우 관리 연결을 복원할 수 있도록 FTD의 구성을 마지막으로 구축된 구성으로 롤백할 수 있습니다. 그런 다음 네트워크 연결이 유지되도록 FMC에서 구성 설정을 조정하고 다시 구축할 수 있습니다. 연결이 끊기지 않아도 롤백 기능을 사용할 수 있습니다. 이는 이 문제 해결 상황으로 제한되지 않습니다.

다음 지침을 참조하십시오.

- 이전 구축만 FTD에서 로컬로 사용할 수 있습니다. 이전 구축으로 롤백할 수 없습니다.
- 고가용성 또는 클러스터링 구축에서는 롤백이 지원되지 않습니다.
- 롤백은 FMC에서 설정할 수 있는 구성에만 영향을 미칩니다. 예를 들어 롤백은 FTD CLI에서만 구성할 수 있는 전용 관리 인터페이스와 관련된 로컬 구성에 영향을 주지 않습니다. **configure network management-data-interface** 명령을 사용하여 마지막 FMC 구축 후 데이터 인터페이스 설정을 변경한 다음 롤백 명령을 사용하면 해당 설정이 유지되지 않습니다. 마지막으로 구축된 FMC 설정으로 롤백됩니다.
- UCAPL/CC 모드는 롤백할 수 없습니다.
- 이전 구축 중에 업데이트된 OOB(Out of Band) SCEP 인증서 데이터는 롤백할 수 없습니다.
- 롤백 중에는 현재 구성이 지워지므로 연결이 삭제됩니다.

시작하기 전에

모델 지원—FTD

프로시저

단계 1 FTD CLI에서 이전 구성으로 롤백합니다.

configure policy rollback

롤백 후 FTD는 롤백이 성공적으로 완료되었음을 FMC에 알립니다. FMC에서 구축 화면에는 구성이 롤백되었음을 알리는 배너가 표시됩니다.

롤백에 실패한 경우, 일반적인 구축 문제에 대한 <https://www.cisco.com/c/en/us/support/docs/security/firepower-ngfw-virtual/215258-troubleshooting-firepower-threat-defense.html>의 내용을 참조하십시오. 경우에 따라 FMC 관리 액세스가 복원된 후 롤백이 실패할 수 있습니다. 이 경우 FMC 구성 문제를 해결하고 FMC에서 다시 구축할 수 있습니다.

예제:

```
> configure policy rollback

The last deployment to this FTD was on June 1, 2020 and its status was Successful.
Do you want to continue [Y/N]?

Y

Rolling back complete configuration on the FTD. This will take time.
.....
Policy rollback was successful on the FTD.
Configuration has been reverted back to transaction id:
Following is the rollback summary:
.....
.....
>
```

단계 2 관리 연결이 재설정되었는지 확인합니다.

FMC의 **Devices**(디바이스) > **Device Management**(디바이스 관리) > **Device**(디바이스) > **Management**(관리) > **FMC Access Details**(FMC 액세스 디테일) > **Connection Status**(연결 상태) 페이지에서 관리 연결 상태를 확인합니다.

FTD CLI에서 관리 연결 상태를 확인하는 **sftunnel-status-brief** 명령을 입력합니다.

연결을 다시 설정하는 데 10분 이상 걸릴 경우, 연결 문제를 해결해야 합니다. [데이터 인터페이스에서 관리 연결성 문제 해결, 35 페이지](#)의 내용을 참조하십시오.

