# Firepower 디바이스 등록 구성, 확인 및 문제 해결

## 목차



## 소개

이 문서에서는 관리되는 FTD(Firepower Threat Defense)와 관리되는 FMC(Firepower Management Center) 간의 연결(sftunnel)에 대한 운영, 확인 및 트러블슈팅 절차에 대해 설명합니다. 정보 및 예는 FTD를 기반으로 하지만 대부분의 개념은 NGIPS(7000/8000 시리즈 어플라이언스) 또는 ASA55xx의 FirePOWER 모듈에도 완벽하게 적용됩니다.

## 사전 요구 사항

### 요구 사항

이 문서에 대한 특정 요건이 없습니다.

### 사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- FTD 소프트웨어 6.6.x 및 6.5.x
- FMC 소프트웨어 6.6.x

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 현재 네트워크가 작동 중인 경우 모든 명령의 잠재적인 영향을 미리 숙지하시기 바랍니다.

## 배경 정보

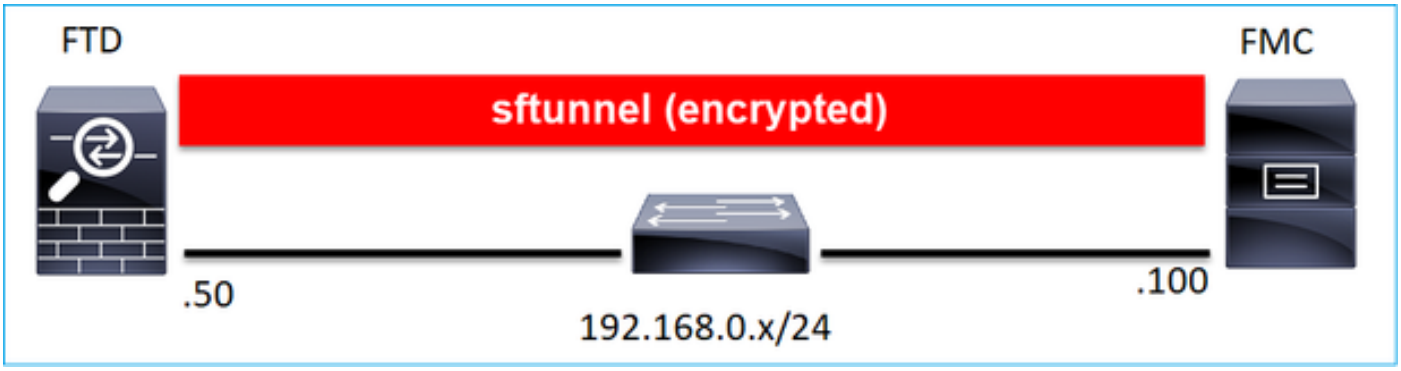
FTD는 2가지 기본 관리 모드를 지원합니다.

- FMC를 통한 오프박스(off-box) - 원격 관리라고도 함
- Firepower Device Manager(FDM) 및/또는 Cisco Defense Orchestrator(CDO)를 통한 온박스(로컬 관리라고도 함)

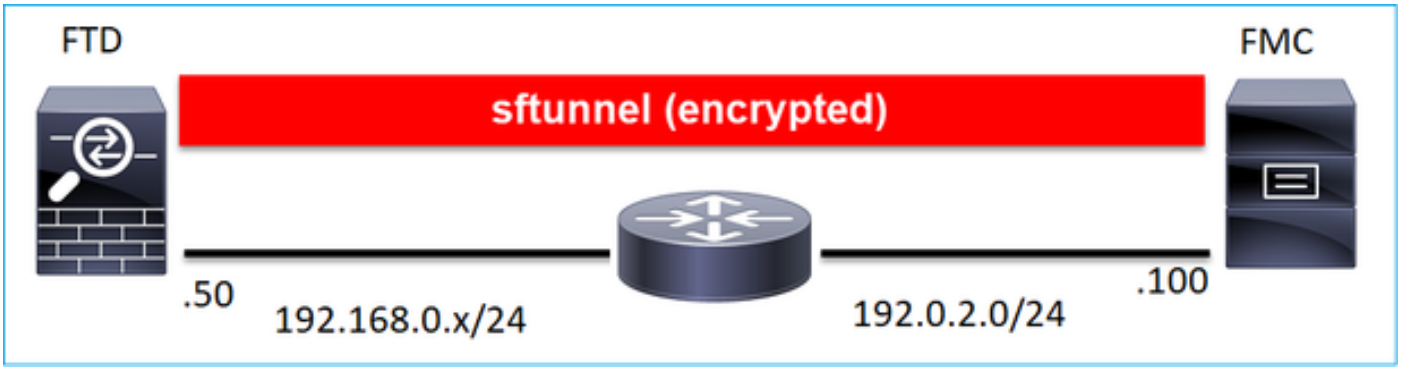
원격 관리의 경우 FTD는 먼저 디바이스 등록이라고 하는 프로세스를 사용하는 FMC에 등록해야 합니다. 등록이 완료되면 FTD 및 FMC는 sftunnel이라는 보안 터널을 설정합니다(이름은 Sourcefire 터널에서 파생됨).

### 설계 옵션

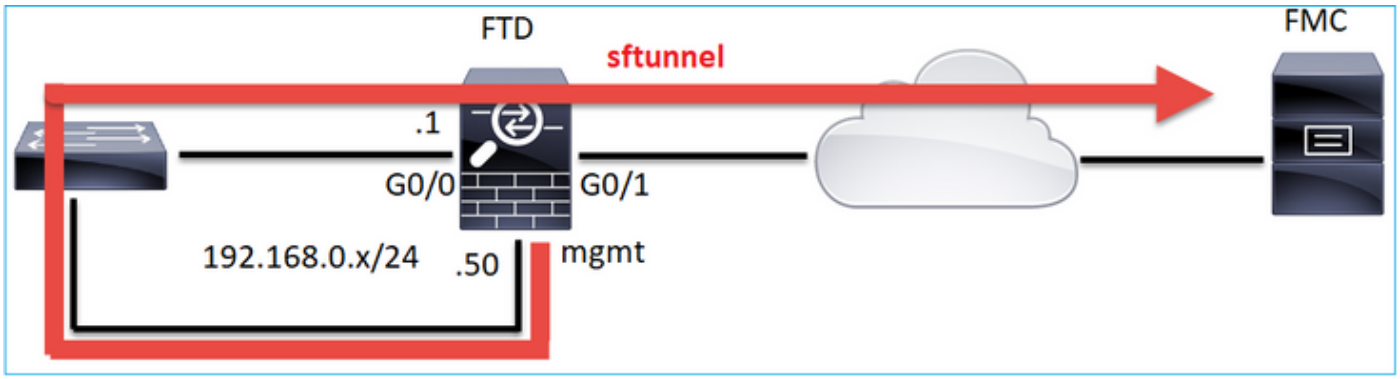
설계 관점에서 FTD - FMC는 동일한 L3 서브넷에 있을 수 있습니다.




또는 서로 다른 네트워크로 분리해야 합니다.




**참고:** sftunnel은 FTD 자체도 통과할 수 있습니다. 이 설계는 **권장하지 않습니다**. 그 이유는 FTD 데이터 플레인 문제가 FTD와 FMC 간의 통신을 방해할 수 있기 때문입니다.




## sftunnel을 통해 교환되는 정보는 무엇입니까?

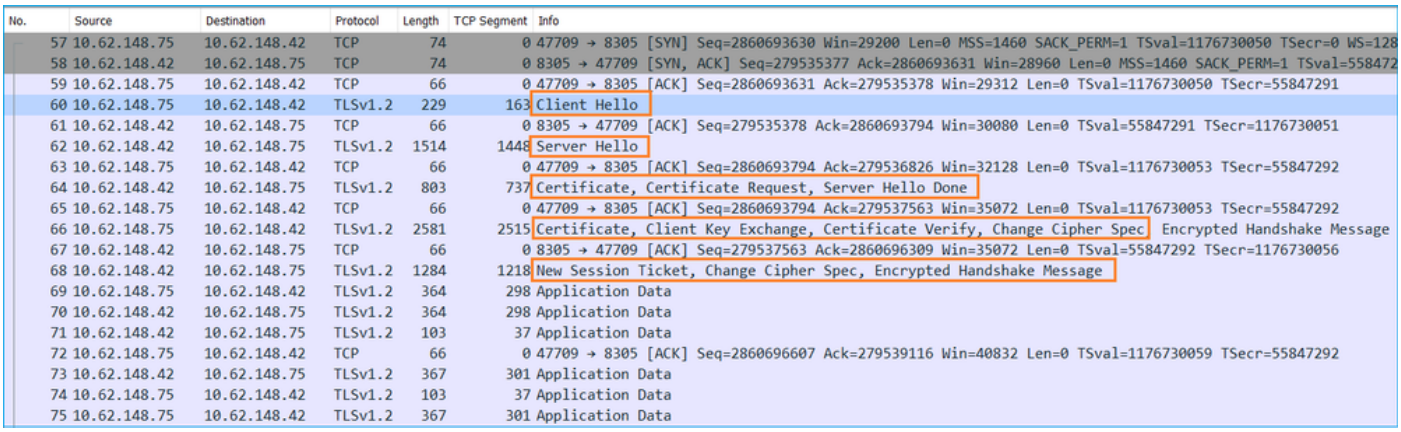
이 목록에는 sftunnel을 통해 전달되는 대부분의 정보가 포함되어 있습니다.

- 어플라이언스 하트비트(킵얼라이브)
- 시간 동기화(NTP)
- 이벤트(연결, 침입/IPS, 파일, SSL 등)
- 악성코드 조회
- 상태 이벤트/알림
- 사용자 및 그룹 정보(ID 정책용)
- FTD HA 상태 정보
- FTD 클러스터 상태 정보
- SI(Security Intelligent) 정보/이벤트
- TID(Threat Intelligence Director) 정보/이벤트
- 캡처된 파일
- 네트워크 검색 이벤트
- 정책 번들(정책 구축)
- 소프트웨어 업그레이드 번들
- 소프트웨어 패치 번들
- VDB

- SRU

## sftunnel에서 어떤 프로토콜/포트를 사용합니까?

sftunnel은 **TCP** 포트 8305**를 사용합니다**. 백엔드에서 TLS **터널입니다**.



| No. | Source | Destination | Protocol | Length | TCP Segment | Info |
|---|---|---|---|---|---|---|
| 57 | 10.62.148.75 | 10.62.148.42 | TCP | 74 | 0 | 47709 → 8305 [SYN] Seq=2860693630 Win=29200 Len=0 MSS=1460 SACK_PERM=1 TSval=1176730050 TSecr=0 WS=128 |
| 58 | 10.62.148.42 | 10.62.148.75 | TCP | 74 | 0 | 8305 → 47709 [SYN, ACK] Seq=279535377 Ack=2860693631 Win=28960 Len=0 MSS=1460 SACK_PERM=1 TSval=558472 |
| 59 | 10.62.148.75 | 10.62.148.42 | TCP | 66 | 0 | 47709 → 8305 [ACK] Seq=2860693631 Ack=279535378 Win=29312 Len=0 TSval=1176730050 TSecr=55847291 |
| 60 | 10.62.148.75 | 10.62.148.42 | TLSv1.2 | 229 | 163 | Client Hello |
| 61 | 10.62.148.42 | 10.62.148.75 | TCP | 66 | 0 | 8305 → 47709 [ACK] Seq=279535378 Ack=2860693794 Win=30080 Len=0 TSval=55847291 TSecr=1176730051 |
| 62 | 10.62.148.42 | 10.62.148.75 | TLSv1.2 | 1514 | 1448 | Server Hello |
| 63 | 10.62.148.42 | 10.62.148.75 | TCP | 66 | 0 | 47709 → 8305 [ACK] Seq=2860693794 Ack=279536826 Win=32128 Len=0 TSval=1176730053 TSecr=55847292 |
| 64 | 10.62.148.42 | 10.62.148.75 | TLSv1.2 | 803 | 737 | Certificate, Certificate Request, Server Hello Done |
| 65 | 10.62.148.75 | 10.62.148.42 | TCP | 66 | 0 | 47709 → 8305 [ACK] Seq=2860693794 Ack=279537563 Win=35072 Len=0 TSval=1176730053 TSecr=55847292 |
| 66 | 10.62.148.75 | 10.62.148.42 | TLSv1.2 | 2581 | 2515 | Certificate, Client Key Exchange, Certificate Verify, Change Cipher Spec Encrypted Handshake Message |
| 67 | 10.62.148.42 | 10.62.148.75 | TCP | 66 | 0 | 8305 → 47709 [ACK] Seq=279537563 Ack=2860696309 Win=35072 Len=0 TSval=55847292 TSecr=1176730056 |
| 68 | 10.62.148.42 | 10.62.148.75 | TLSv1.2 | 1284 | 1218 | New Session Ticket, Change Cipher Spec, Encrypted Handshake Message |
| 69 | 10.62.148.75 | 10.62.148.42 | TLSv1.2 | 364 | 298 | Application Data |
| 70 | 10.62.148.42 | 10.62.148.75 | TLSv1.2 | 364 | 298 | Application Data |
| 71 | 10.62.148.42 | 10.62.148.75 | TLSv1.2 | 103 | 37 | Application Data |
| 72 | 10.62.148.75 | 10.62.148.42 | TCP | 66 | 0 | 47709 → 8305 [ACK] Seq=2860696607 Ack=279539116 Win=40832 Len=0 TSval=1176730059 TSecr=55847292 |
| 73 | 10.62.148.42 | 10.62.148.75 | TLSv1.2 | 367 | 301 | Application Data |
| 74 | 10.62.148.75 | 10.62.148.42 | TLSv1.2 | 103 | 37 | Application Data |
| 75 | 10.62.148.75 | 10.62.148.42 | TLSv1.2 | 367 | 301 | Application Data |

## FTD에서 Sftunnel TCP 포트를 변경하는 방법?

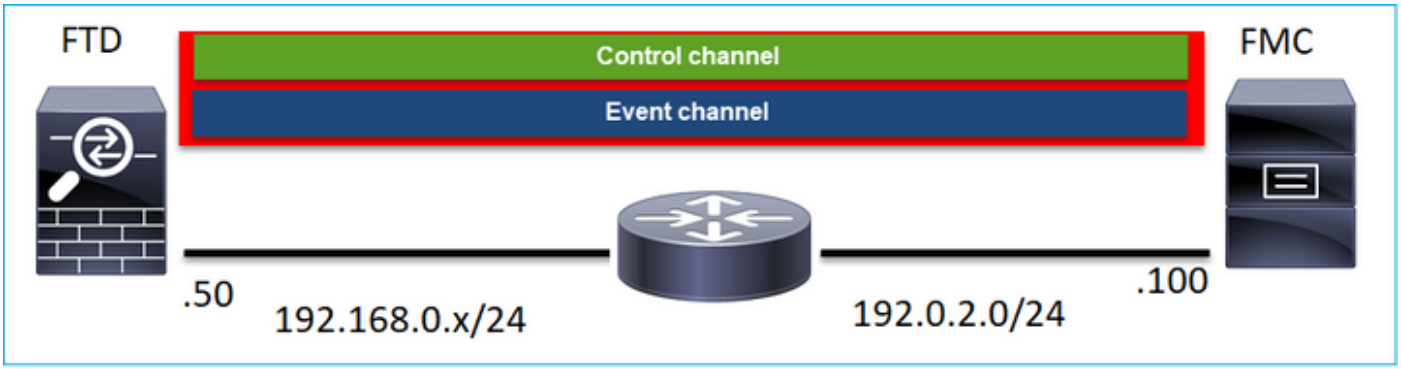
```
> configure network management-port 8306
Management port changed to 8306.
```

> **참고:** 이 경우 FMC의 포트도 변경해야 합니다(**Configuration > Management Interfaces > Shared Settings**). 이는 동일한 FMC에 이미 등록된 다른 모든 디바이스에 영향을 미칩니다. Cisco에서는 원격 관리 포트의 기본 설정을 유지하는 것을 적극 권장하지만 관리 포트가 네트워크의 다른 통신과 충돌할 경우 다른 포트를 선택할 수 있습니다. 관리 포트를 변경할 경우, 함께 통신해야 하는 구축의 모든 디바이스에 대해 변경해야 합니다.

## sftunnel에 의해 설정되는 연결 수는 몇 개입니까?

sftunnel은 2개의 연결(채널)을 설정합니다.

- 제어 채널
- 이벤트 채널



### 어떤 디바이스가 각 채널을 시작합니까?

시나리오에 따라 다릅니다. 문서의 나머지 부분에 설명된 시나리오를 확인하십시오.

# 구성

## 등록 기본 사항

FTD CLI

FTD에서 디바이스 등록을 위한 기본 구문은 다음과 같습니다.

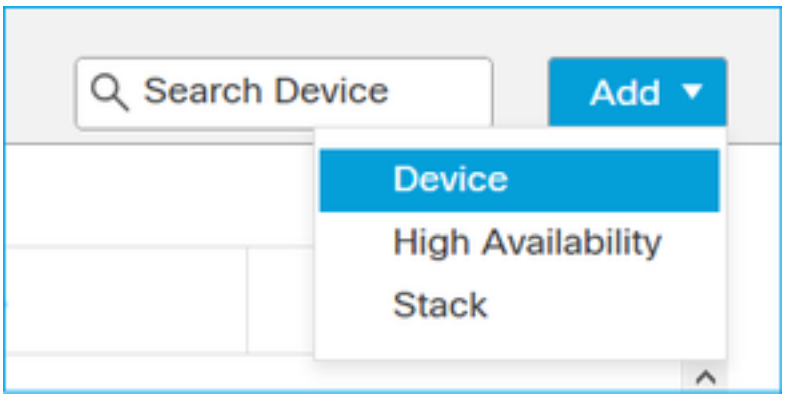
**>관리자를 추가 구성 <FMC 호스트> <등록 키> <NAT ID>**

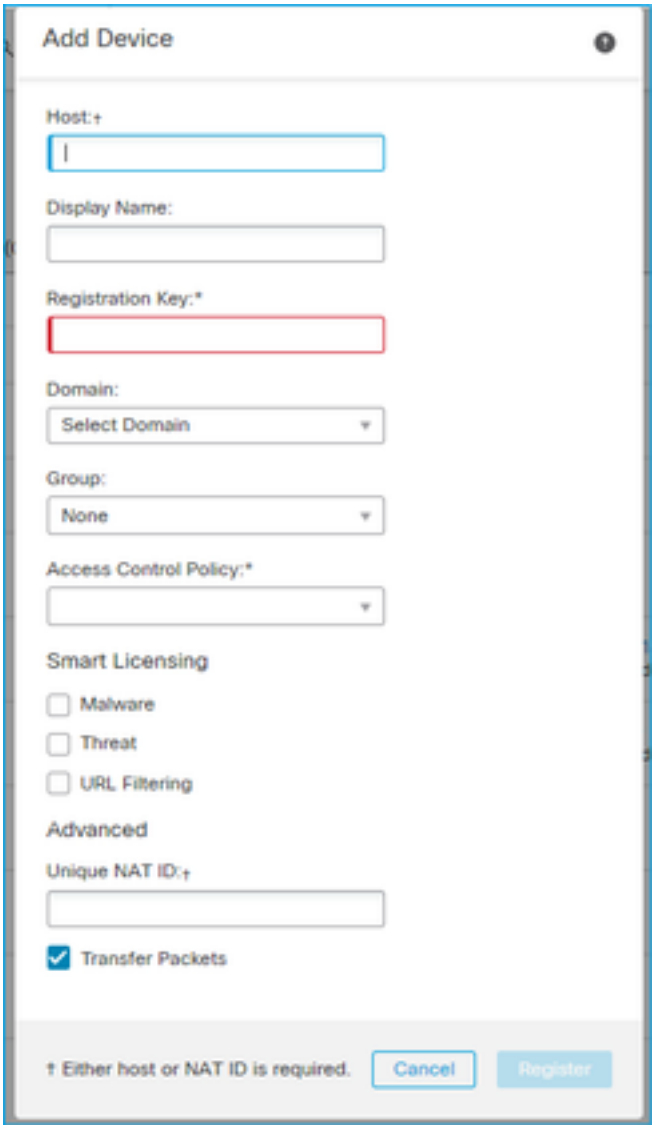
| 가치 | 설명 |
| --- | --- |
| FMC 호스트 | 다음 중 하나일 수 있습니다.<br>• 호스트 이름<br>• ipv4 주소<br>• ipv6 주소<br>• 돈트리졸브 |
| 등록 키 | 디바이스 등록에 사용되는 공유 암호 영숫자 문자<br>(2~36자)입니다. 영숫자, 하이픈(-), 밑줄(_) 및 마침<br>(.)만 사용할 수 있습니다. |
| NAT ID | 한쪽에서 **IP** 주소를 지정하지 **않을 때** FMC와 디바<br>간의 등록 프로세스 **중에 사용되는 영숫자 문자열**<br>**다**. FMC에서 동일한 NAT ID를 지정합니다. |

자세한 내용은 Cisco Firepower Threat Defense 명령 참조를 확인하십시오

FMC UI

FMC에서 Devices(디바이스) **> Device Management(디바이스 관리)로 이동합니다.** Add(추가) **> Device(디바이스)를 선택합니다**

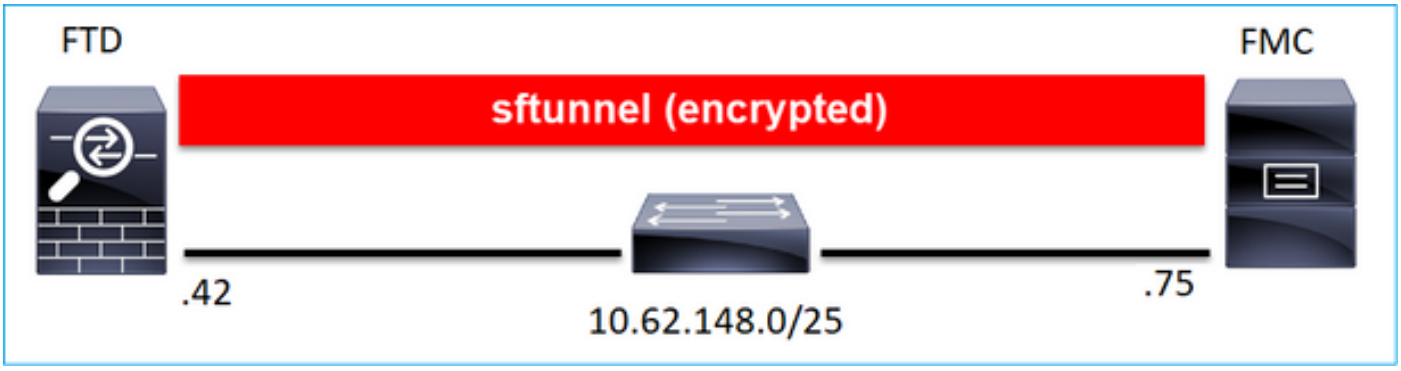





- 호스트에서 FTD IP 주소를 지정합니다.
- 표시 이름에서 원하는 것을 지정합니다.
- 등록 키는 FTD CLI에 지정된 것과 일치해야 합니다.
- 여러 도메인을 사용하는 경우 FTD를 추가할 도메인을 지정합니다.
- Group(그룹)에서 FTD를 추가할 Device Group(디바이스 그룹)을 지정합니다.
- 액세스 제어 정책에서 FTD에 구축할 보안 정책을 지정합니다.
- 스마트 라이선싱: 구성된 기능에 필요한 라이센스를 지정합니다.
- NAT ID: 이 문서의 뒷부분에 설명된 특정 시나리오에 필요합니다.

자세한 내용은 Firepower Management Center 컨피그레이션 가이드를 참조하여 Firepower Management Center에 디바이스 추가

## 시나리오 1. FMC 및 FTD 고정 IP 주소




FTD CLI

**>관리자를 추가 구성 <FMC 고정 IP> <등록 키>**

예를 들면 다음과 같습니다.

```
> configure manager add 10.62.148.75 Cisco-123
Manager successfully configured.
Please make note of reg_key as this will be required while adding Device in FMC.
```

**배경 정보**

FTD 명령을 입력하는 즉시 FTD는 20초마다 FMC에 연결을 시도하지만 FMC가 아직 구성되지 않았으므로 TCP RST로 응답합니다.

```
> capture-traffic

Please choose domain to capture traffic from:
  0 - eth0
  1 - Global

Selection? 0

Please specify tcpdump options desired.
(or enter '?' for a list of supported options)
Options: -n host 10.62.148.75
HS_PACKET_BUFFER_SIZE is set to 4.
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on eth0, link-type EN10MB (Ethernet), capture size 262144 bytes
18:53:33.365513 IP 10.62.148.42.46946 > 10.62.148.75.8305: Flags [S], seq 2274592861, win 29200,
options [mss 1460,sackOK,TS val 55808298 ecr 0,nop,wscale 7], length 0
18:53:33.365698 IP 10.62.148.75.8305 > 10.62.148.42.46946: Flags [R.], seq 0, ack 2274592862,
win 0, length 0
18:53:53.365973 IP 10.62.148.42.57607 > 10.62.148.75.8305: Flags [S], seq 1267517632, win 29200,
options [mss 1460,sackOK,TS val 55810298 ecr 0,nop,wscale 7], length 0
18:53:53.366193 IP 10.62.148.75.8305 > 10.62.148.42.57607: Flags [R.], seq 0, ack 1267517633,
win 0, length 0
18:54:13.366383 IP 10.62.148.42.55484 > 10.62.148.75.8305: Flags [S], seq 4285875151, win 29200,
options [mss 1460,sackOK,TS val 55812298 ecr 0,nop,wscale 7], length 0
18:54:13.368805 IP 10.62.148.75.8305 > 10.62.148.42.55484: Flags [R.], seq 0, ack 4285875152,
win 0, length 0
```

디바이스 등록 상태:

```
> show managers
Host                        : 10.62.148.75
Registration Key            : ****
Registration                : pending
RPC Status                  :
Type                        : Manager
Host                        : 10.62.148.75
Registration                : Pending
```

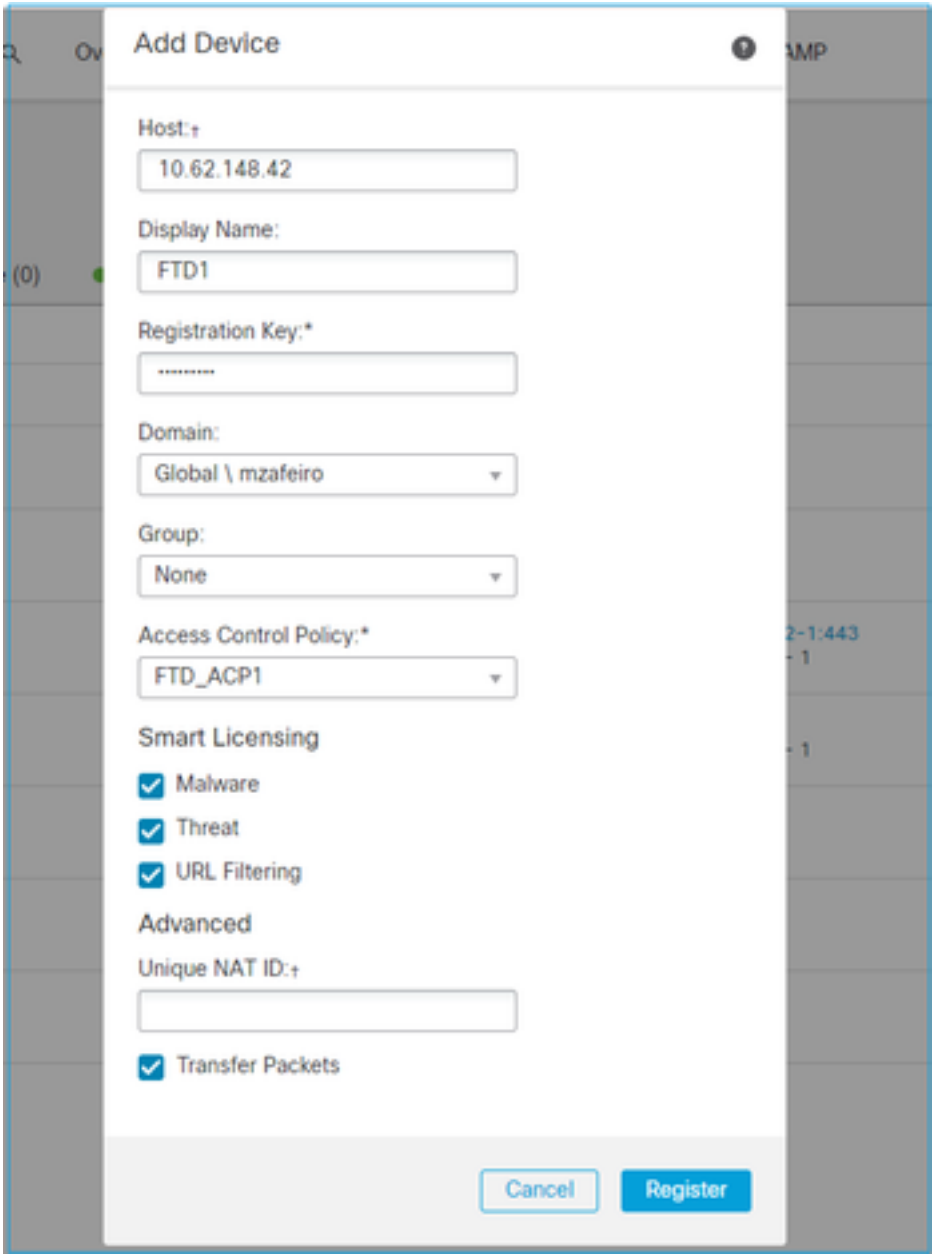
FTD는 포트 TCP 8305에서 수신합니다.

```
admin@vFTD66:~$ netstat -na | grep 8305
tcp        0      0 10.62.148.42:8305       0.0.0.0:*               LISTEN
```

FMC UI

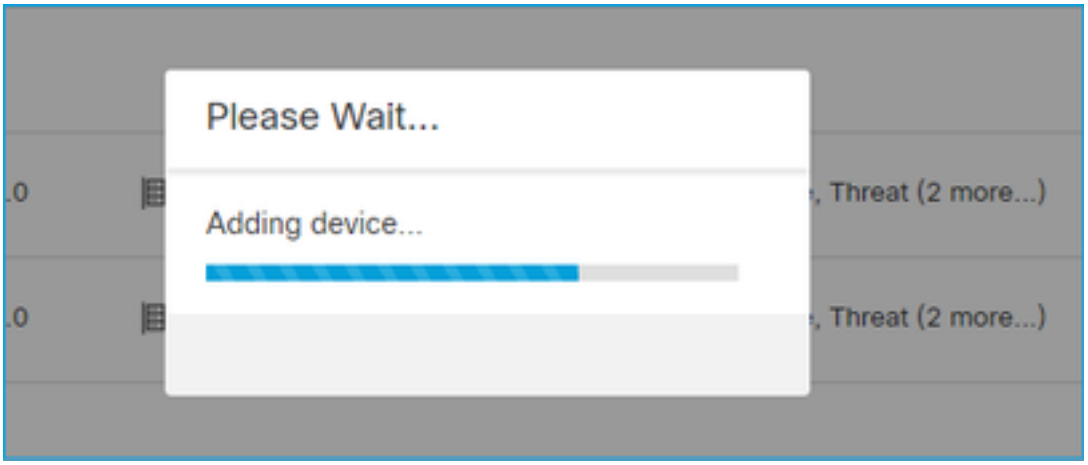
이 경우 다음을 지정합니다.

- 호스트(FTD의 IP 주소)
- 표시 이름
- 등록 키(FTD에 구성된 것과 일치해야 함)
- 액세스 제어 정책
- 도메인
- Smart Licensing 정보




**등록** 선택

등록 프로세스가 시작됩니다.



FMC는 포트 TCP 8305에서 수신 대기를 시작합니다.

```
admin@FMC2000-2:~$ netstat -na | grep 8305
tcp        0      0 10.62.148.75:8305       0.0.0.0:*               LISTEN
```

백그라운드에서 FMC는 TCP 연결을 시작합니다.

```
20:15:55.437434 IP 10.62.148.42.49396 > 10.62.148.75.8305: Flags [S], seq 655146775, win 29200,
options [mss 1460,sackOK,TS val 56302505 ecr 0,nop,wscale 7], length 0
20:15:55.437685 IP 10.62.148.75.8305 > 10.62.148.42.49396: Flags [R.], seq 0, ack 655146776, win
0, length 0
20:16:00.463637 ARP, Request who-has 10.62.148.42 tell 10.62.148.75, length 46
20:16:00.463655 ARP, Reply 10.62.148.42 is-at 00:50:56:85:7b:1f, length 28
20:16:08.342057 IP 10.62.148.75.50693 > 10.62.148.42.8305: Flags [S], seq 2704366385, win 29200,
options [mss 1460,sackOK,TS val 1181294721 ecr 0,nop,wscale 7], length 0
20:16:08.342144 IP 10.62.148.42.8305 > 10.62.148.75.50693: Flags [S.], seq 1829769842, ack
2704366386, win 28960, options [mss 1460,sackOK,TS val 56303795 ecr 1181294721,nop,wscale 7],
length 0
20:16:08.342322 IP 10.62.148.75.50693 > 10.62.148.42.8305: Flags [.], ack 1, win 229, options
[nop,nop,TS val 1181294722 ecr 56303795], length 0
20:16:08.342919 IP 10.62.148.75.50693 > 10.62.148.42.8305: Flags [P.], seq 1:164, ack 1, win
229, options [nop,nop,TS val 1181294722 ecr 56303795], length 163
20:16:08.342953 IP 10.62.148.42.8305 > 10.62.148.75.50693: Flags [.], ack 164, win 235, options
[nop,nop,TS val 56303795 ecr 1181294722], length 0
```

sftunnel 제어 채널이 설정됩니다.

```
admin@FMC2000-2:~$ netstat -na | grep 8305
tcp        0      0 10.62.148.75:8305       0.0.0.0:*               LISTEN
tcp        0      0 10.62.148.75:50693      10.62.148.42:8305       ESTABLISHED


> sftunnel-status

SFTUNNEL Start Time: Sat Apr 18 20:14:20 2020

        Both IPv4 and IPv6 connectivity is supported
        Broadcast count = 4
        Reserved SSL connections: 0
        Management Interfaces: 1
        eth0 (control events) 10.62.148.42,

**********************

**RUN STATUS****ksec-fs2k-2-mgmt.cisco.com************
        Cipher used = AES256-GCM-SHA384 (strength:256 bits)
        ChannelA Connected: Yes, Interface eth0
        ChannelB Connected: No
        Registration: Completed.
        IPv4 Connection to peer '10.62.148.75' Start Time: Sat Apr 18 20:16:08 2020


PEER INFO:
        sw_version 6.6.0
        sw_build 90
        Management Interfaces: 1
        eth0 (control events) 10.62.148.75,
        Peer channel Channel-A is valid  type (CONTROL), using 'eth0', connected to
```

```
'10.62.148.75' via '10.62.148.42'
        Peer channel Channel-B is not valid
```

몇 분 후에 이벤트 채널이 설정됩니다. 이벤트 채널의 개시자는 **어느** 쪽이든 될 수 **있습니다**. 이 예에서는 FMC였습니다.

```
20:21:15.347587 IP 10.62.148.75.43957 > 10.62.148.42.8305: Flags [S], seq 3414498581, win 29200,
options [mss 1460,sackOK,TS val 1181601702 ecr 0,nop,wscale 7], length 0
20:21:15.347660 IP 10.62.148.42.8305 > 10.62.148.75.43957: Flags [S.], seq 2735864611, ack
3414498582, win 28960, options [mss 1460,sackOK,TS val 56334496 ecr 1181601702,nop,wscale 7],
length 0
20:21:15.347825 IP 10.62.148.75.43957 > 10.62.148.42.8305: Flags [.], ack 1, win 229, options
[nop,nop,TS val 1181601703 ecr 56334496], length 0
20:21:15.348415 IP 10.62.148.75.43957 > 10.62.148.42.8305: Flags [P.], seq 1:164, ack 1, win
229, options [nop,nop,TS val 1181601703 ecr 56334496], length 163
```

임의 소스 포트는 연결 개시자를 나타냅니다.

```
admin@FMC2000-2:~$ netstat -na | grep 10.62.148.42
tcp        0      0 10.62.148.75:50693      10.62.148.42:8305       ESTABLISHED
tcp        0      0 10.62.148.75:43957      10.62.148.42:8305       ESTABLISHED
```

이벤트 채널이 FTD에 의해 시작된 경우 출력은 다음과 같습니다.

```
admin@FMC2000-2:~$ netstat -na | grep 10.62.148.42
tcp        0      0 10.62.148.75:58409      10.62.148.42:8305       ESTABLISHED
tcp        0      0 10.62.148.75:8305       10.62.148.42:46167      ESTABLISHED
```

FTD 측에서

```
> sftunnel-status

SFTUNNEL Start Time: Sat Apr 18 20:14:20 2020

        Both IPv4 and IPv6 connectivity is supported
        Broadcast count = 6
        Reserved SSL connections: 0
        Management Interfaces: 1
        eth0 (control events) 10.62.148.42,

**********************

**RUN STATUS****ksec-fs2k-2-mgmt.cisco.com*************
        Cipher used = AES256-GCM-SHA384 (strength:256 bits)
        ChannelA Connected: Yes, Interface eth0
        Cipher used = AES256-GCM-SHA384 (strength:256 bits)
        ChannelB Connected: Yes, Interface eth0
        Registration: Completed.
        IPv4 Connection to peer '10.62.148.75' Start Time: Sat Apr 18 20:16:08 2020


PEER INFO:
        sw_version 6.6.0
        sw_build 90
        Management Interfaces: 1
```

```
        eth0 (control events) 10.62.148.75,
        Peer channel Channel-A is valid  type (CONTROL), using 'eth0', connected to
'10.62.148.75' via '10.62.148.42'
        Peer channel Channel-B is valid  type (EVENT), using 'eth0', connected to '10.62.148.75'
via '10.62.148.42'


> show managers
Type                      : Manager
Host                      : 10.62.148.75
Registration              : Completed

>
```

## 시나리오 2. FTD DHCP IP 주소 - FMC 고정 IP 주소

이 시나리오에서 FTD 관리 인터페이스는 DHCP 서버에서 IP 주소를 받았습니다.


FTD CLI

NAT ID를 지정해야 합니다.

**>관리자를 추가 구성 <FMC 고정 IP> <등록 키> <NAT ID>**

예를 들면 다음과 같습니다.

```
> configure manager add 10.62.148.75 Cisco-123 nat123
Manager successfully configured.
Please make note of reg_key as this will be required while adding Device in FMC.

>
```

FTD 등록 상태:

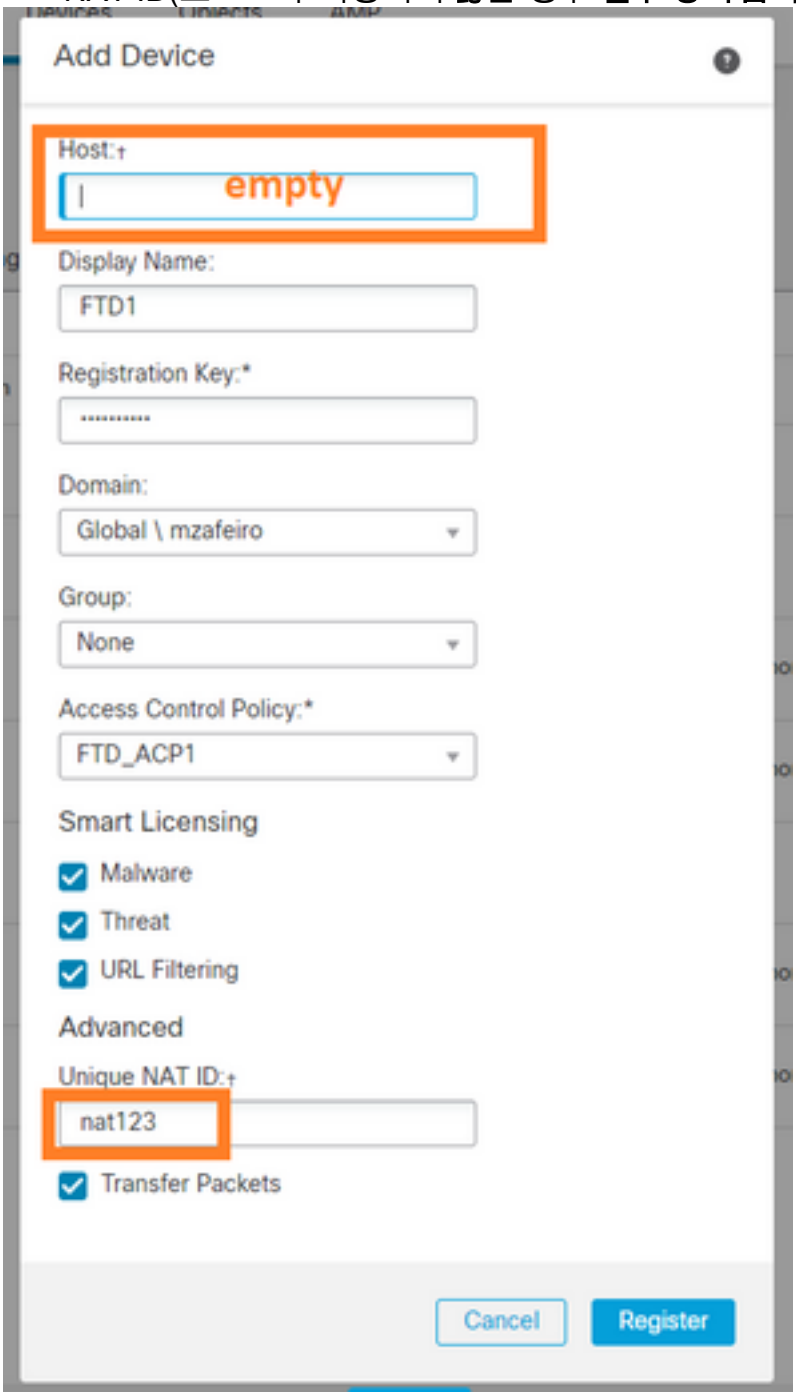
```
> show managers
Host                      : 10.62.148.75
Registration Key          : ****
Registration              : pending
RPC Status                :
```

```
Type                    : Manager
Host                    : 10.62.148.75
Registration            : Pending
```

FMC UI

이 경우 다음을 지정합니다.

- 표시 이름
- 등록 키(FTD에 구성된 것과 일치해야 함)
- 액세스 제어 정책
- 도메인
- Smart Licensing 정보
- NAT ID(호스트가 지정되지 **않은** 경우 **필수 항목입니다**. FTD에 구성된 것과 일치해야 합니다.)

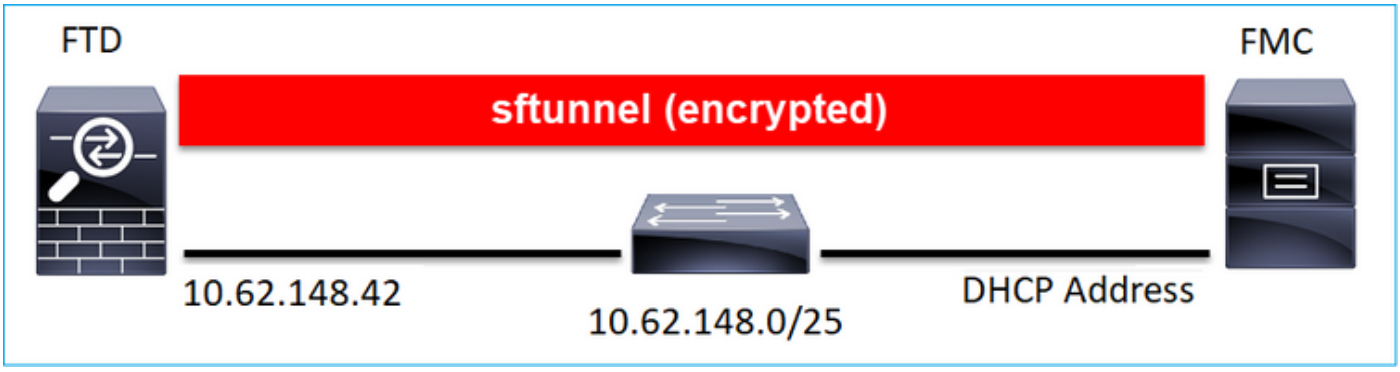


**이 경우 sftunnel을 시작하는 사람은 누구입니까?**

FTD는 두 채널 연결을 모두 시작합니다.

```
ftd1:/home/admin# netstat -an | grep 148.75
tcp        0      0 10.62.148.45:40273      10.62.148.75:8305       ESTABLISHED
tcp        0      0 10.62.148.45:39673      10.62.148.75:8305       ESTABLISHED
```

## 시나리오 3. FTD 고정 IP 주소 - FMC DHCP IP 주소



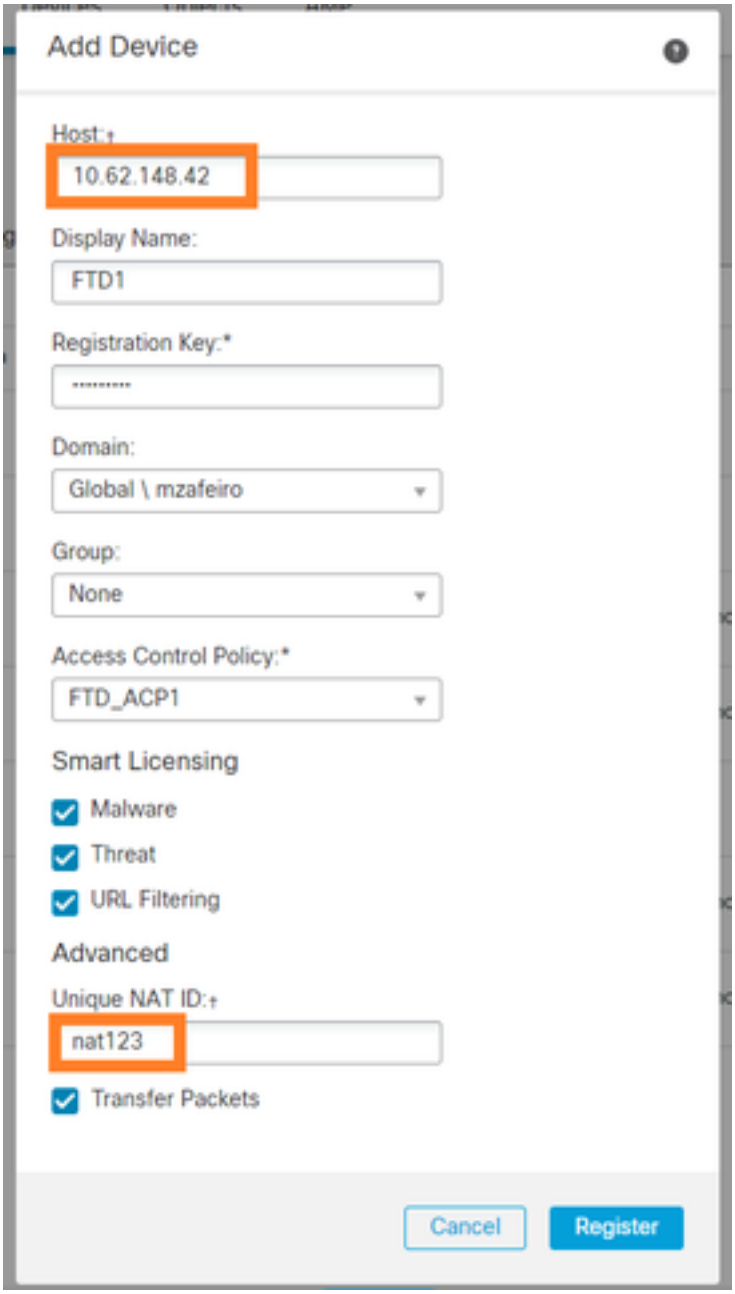

```
> configure manager add DONTRESOLVE Cisco-123 nat123
Manager successfully configured.
Please make note of reg_key as this will be required while adding Device in FMC.

>
```

**참고:** DONTRESOLVE를 사용하는 경우 NAT ID가 필요합니다.

FMC UI

이 경우 다음을 지정합니다.

- **FTD IP 주소**
- 표시 이름
- 등록 키(FTD에 구성된 것과 일치해야 함)
- 액세스 제어 정책
- 도메인
- Smart Licensing 정보
- **NAT ID(FTD에 구성된 것과 일치해야 함)**




등록 후 FTD:

```
> show managers
Type                    : Manager
Host                    : 5a8454ea-8273-11ea-a7d3-d07d71db8f19DONTRESOLVE
Registration            : Completed
```

### 이 경우 sftunnel을 시작하는 사람은 누구입니까?

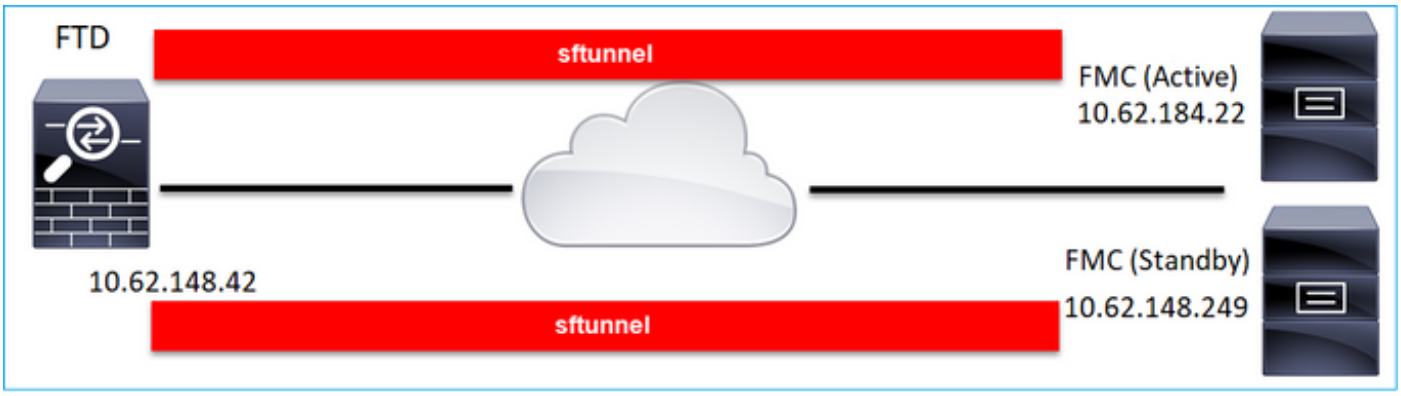
- FMC가 제어 채널을 시작합니다.
- 이벤트 채널은 양쪽에서 시작할 수 있습니다.

```
root@FMC2000-2:/Volume/home/admin# netstat -an | grep 148.42
tcp        0      0 10.62.148.75:50465      10.62.148.42:8305       ESTABLISHED
tcp        0      0 10.62.148.75:48445      10.62.148.42:8305       ESTABLISHED
```

## 시나리오 4. FMC HA에 대한 FTD 등록

FTD에서는 활성 FMC만 구성합니다.

```
> configure manager add 10.62.184.22 cisco123
Manager successfully configured.
Please make note of reg_key as this will be required while adding Device in FMC.
```

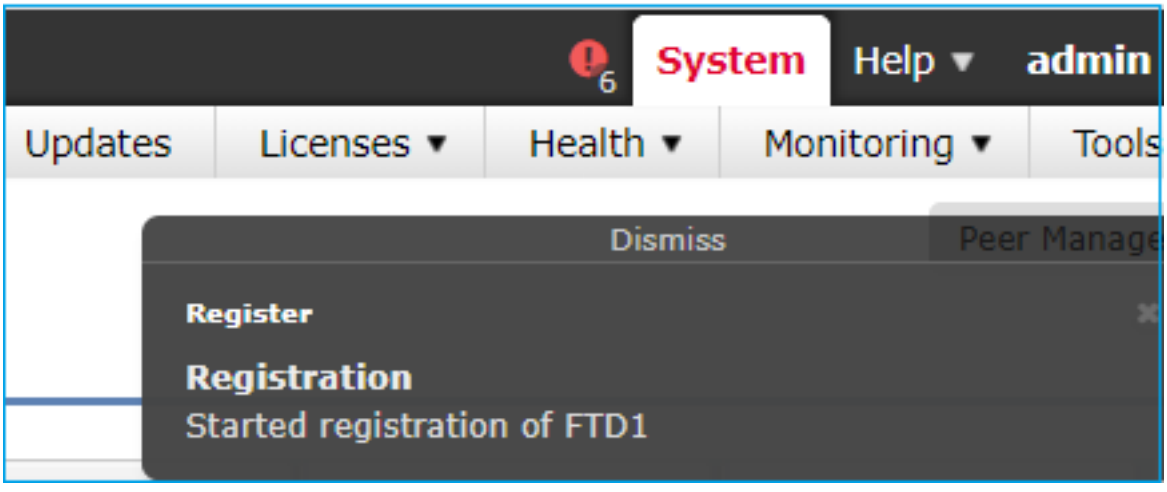



**참고:** TCP 포트 8305 트래픽이 FTD에서 두 FMC 모두로 허용되는지 확인합니다.

먼저 액티브 FMC에 대한 sftunnel이 설정됩니다.

```
> show managers
Type                    : Manager
Host                    : 10.62.184.22
Registration            : Completed
```

몇 분 후 FTD가 대기 FMC에 등록을 시작합니다.



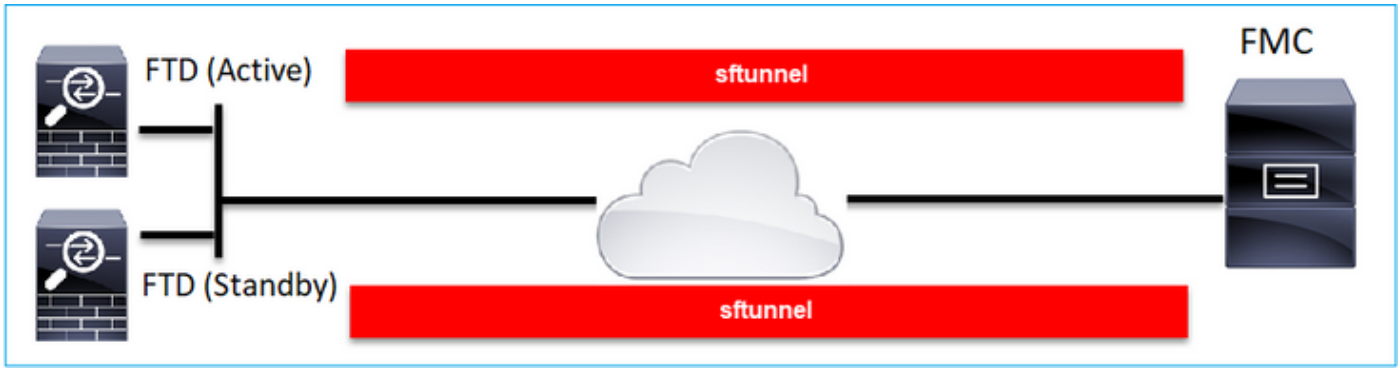
```
> show managers
Type                    : Manager
Host                    : 10.62.184.22
Registration            : Completed

Type                    : Manager
Host                    : 10.62.148.249
Registration            : Completed
```

FTD 백엔드에서 제어 채널 2개(각 FMC에 하나씩) 및 이벤트 채널 2개(각 FMC에 하나씩)가 설정됩니다.

```
ftd1:/home/admin# netstat -an | grep 8305
tcp        0      0 10.62.148.42:8305       10.62.184.22:36975      ESTABLISHED
tcp        0      0 10.62.148.42:42197      10.62.184.22:8305       ESTABLISHED
tcp        0      0 10.62.148.42:8305       10.62.148.249:45373     ESTABLISHED
tcp        0      0 10.62.148.42:8305       10.62.148.249:51893     ESTABLISHED
```

## 시나리오 5. FTD HA

FTD HA의 경우 각 유닛에는 FMC에 대한 별도의 터널이 있습니다.

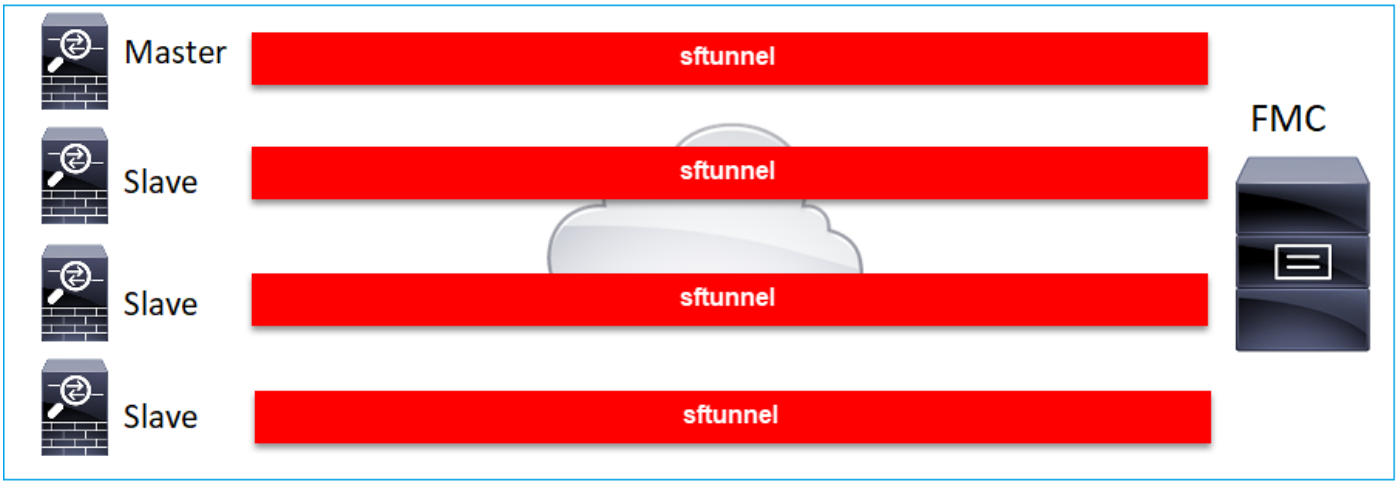



두 FTD를 독립적으로 등록한 다음 FMC에서 FTD HA를 구성합니다. 자세한 내용은 다음을 참조하십시오.

- Firepower 어플라이언스에서 FTD 고가용성 설정
- Firepower Threat Defense의 고가용성

## 시나리오 6. FTD 클러스터

FTD 클러스터의 경우 각 유닛에는 FMC에 대한 별도의 터널이 있습니다. 6.3 FMC 릴리스부터는 FTD 마스터만 FMC에 등록하면 됩니다. 그런 다음 FMC가 나머지 유닛을 처리하고 자동 검색 + 등록합니다.

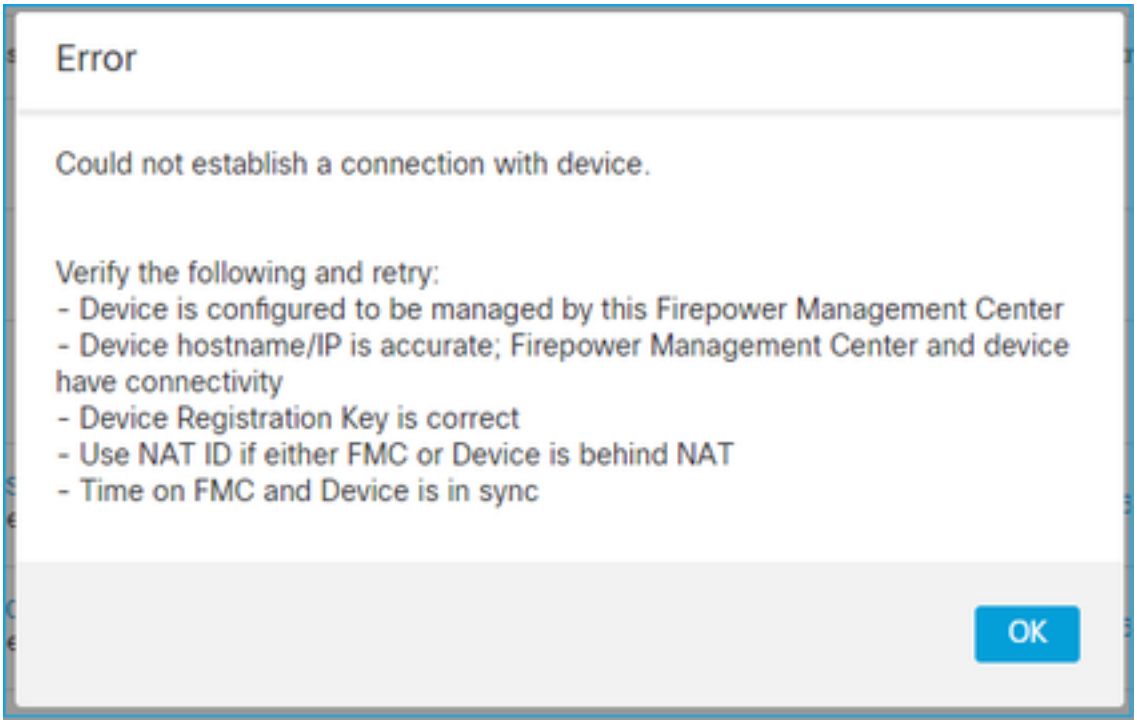



**참고:** 최상의 성능을 위해 마스터 유닛을 추가하는 것이 좋지만 클러스터의 모든 유닛을 추가할 수 있습니다. 자세한 내용은 다음을 참조하십시오. Firepower Threat Defense 클러스터 생성

# 일반적인 문제 해결

## 1. FTD CLI의 구문이 잘못되었습니다.

FTD에 잘못된 구문이 있고 등록이 실패한 경우 FMC UI는 일반적인 오류 메시지를 표시합니다.




이 명령에서 키워드 **키**는 등록 키이고 **cisco123**은 NAT ID입니다. 기술적으로 그러한 키워드가 없는 동안 키워드 키를 추가하는 것은 매우 일반적입니다.

```
> configure manager add 10.62.148.75 key cisco123
Manager successfully configured.
Please make note of reg_key as this will be required while adding Device in FMC.
```

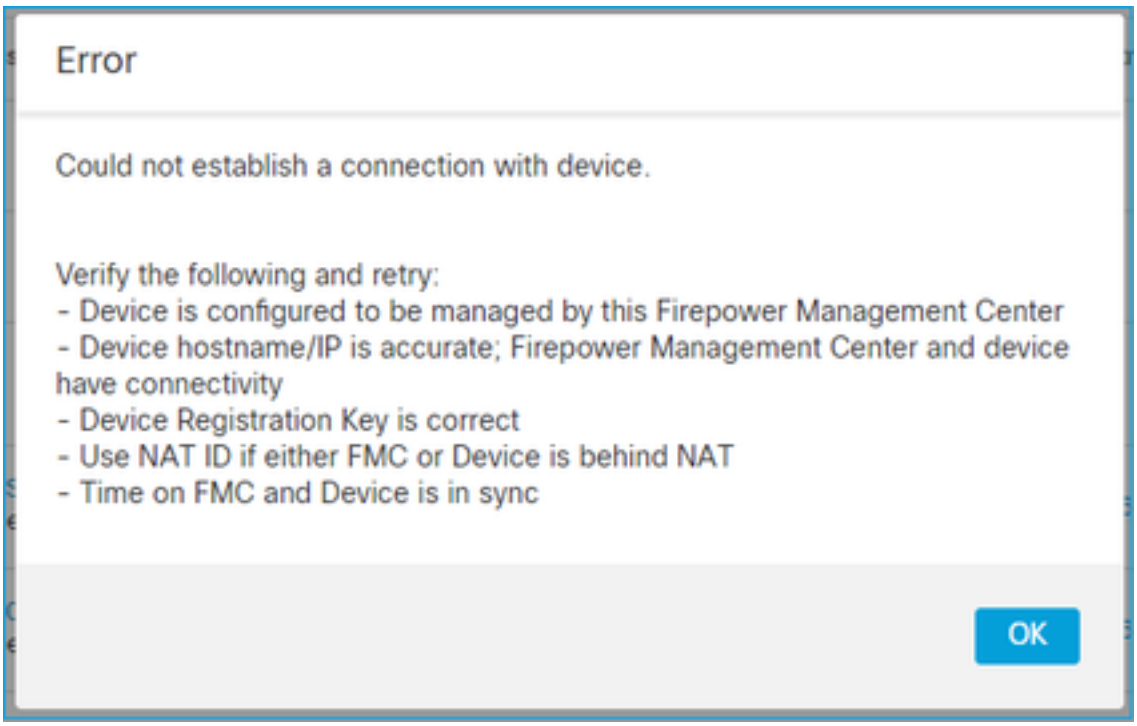
### 권장 조치

올바른 구문을 사용하고 존재하지 않는 키워드는 사용하지 마십시오.

```
> configure manager add 10.62.148.75 cisco123
Manager successfully configured.
Please make note of reg_key as this will be required while adding Device in FMC.
```

## 2. FTD - FMC 간의 등록 키 불일치

FMC UI에는 다음이 표시됩니다.




### 권장 조치

FTD에서 /ngfw/var/log/messages 파일에 인증 문제가 있는지 확인합니다.

Way 1 - 이전 로그 확인

```
> system support view-files
Type a sub-dir name to list its contents: s
```

```
Type the name of the file to view ([b] to go back, [Ctrl+C] to exit)
> messages
Apr 19 04:02:05 vFTD66 syslog-ng[1440]: Configuration reload request received, reloading
configuration;
Apr 19 04:02:07 vFTD66 SF-IMS[3116]: [3116] pm:control [INFO] ControlHandler auditing message-
>type 0x9017, from '', cmd '/ngf
w/usr/bin/perl /ngfw/usr/local/sf/bin/run_hm.pl --persistent', pid 19455 (uid 0, gid 0)
/authenticate

Apr 19 20:17:14 vFTD66 SF-IMS[18974]: [19131] sftunneld:sf_ssl [WARN] Accept: Failed to
authenticate peer '10.62.148.75' <- The problem
```

Way 2 - 라이브 로그 확인

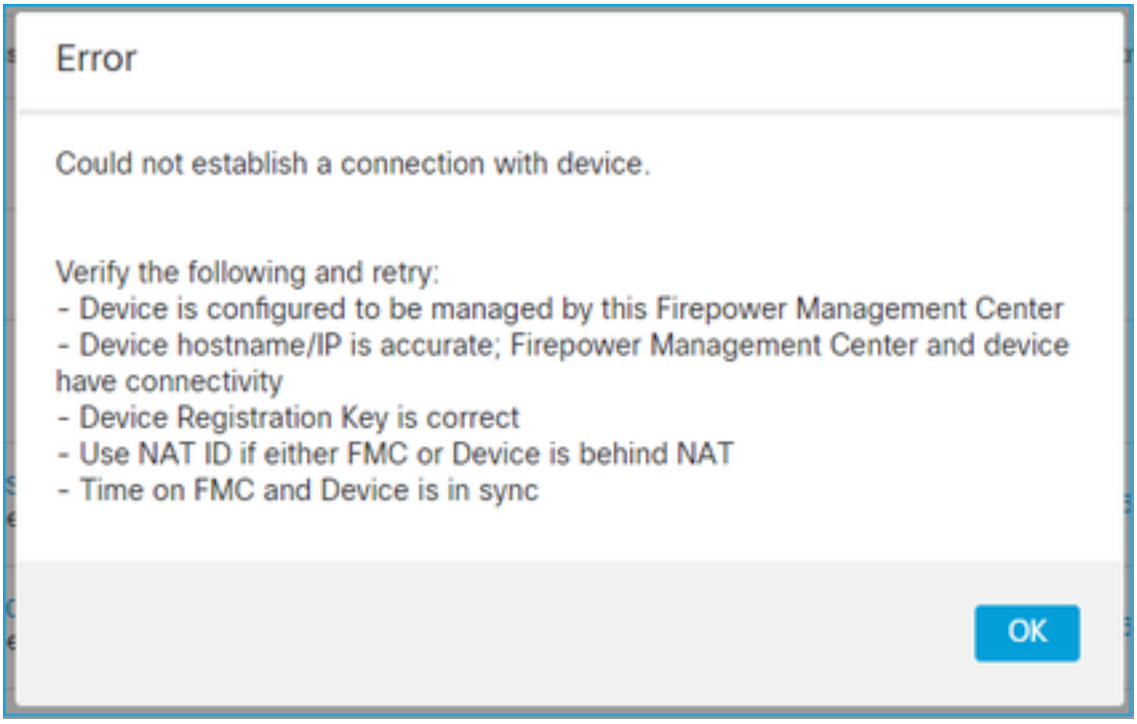
```
> expert
ftd1:~$ sudo su
Password:
ftd1::/home/admin# tail -f /ngfw/var/log/messages
```

FTD에서 /etc/sf/sftunnel.conf 파일의 내용을 확인하여 등록 키가 올바른지 확인합니다.

```
ftd1:~$ cat /etc/sf/sftunnel.conf | grep reg_key
        reg_key cisco-123;
```

## 3. FTD 간 연결 문제 - FMC

FMC UI에는 다음이 표시됩니다.




**권장 작업**

- 경로에 트래픽을 차단하는 디바이스(예: 방화벽)가 없는지 확인합니다(TCP 8305). FMC HA의 경우 TCP 포트 8305로의 트래픽이 두 FMC 모두에 허용되는지 확인합니다.
- 양방향 통신을 확인하기 위해 캡처를 사용합니다. FTD에서는 capture**-traffic 명령을** 사용합니다. TCP 3-way 핸드셰이크가 있고 TCP FIN 또는 RST 패킷이 없는지 확인합니다.

```
> capture-traffic

Please choose domain to capture traffic from:
  0 - eth0
  1 - Global

Selection? 0

Please specify tcpdump options desired.
(or enter '?' for a list of supported options)
Options: -n host 10.62.148.75
HS_PACKET_BUFFER_SIZE is set to 4.
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on eth0, link-type EN10MB (Ethernet), capture size 262144 bytes
20:56:09.393655 IP 10.62.148.42.53198 > 10.62.148.75.8305: Flags [S], seq 3349394953, win 29200,
options [mss 1460,sackOK,TS val 1033596 ecr 0,nop,wscale 7], length 0
20:56:09.393877 IP 10.62.148.75.8305 > 10.62.148.42.53198: Flags [R.], seq 0, ack 3349394954,
win 0, length 0
20:56:14.397412 ARP, Request who-has 10.62.148.75 tell 10.62.148.42, length 28
20:56:14.397602 ARP, Reply 10.62.148.75 is-at a4:6c:2a:9e:ea:10, length 46
```

마찬가지로 양방향 통신을 보장하기 위해 FMC에서 캡처합니다.

```
root@FMC2000-2:/var/common# tcpdump -i eth0 host 10.62.148.42 -n -w sftunnel.pcap
```

캡처를 pcap 형식으로 내보내고 패킷 내용을 확인하는 것도 좋습니다.

```
ftd1:/home/admin# tcpdump -i eth0 host 10.62.148.75 -n -w tunnel.pcap
HS_PACKET_BUFFER_SIZE is set to 4.
tcpdump: listening on eth0, link-type EN10MB (Ethernet), capture size 262144 bytes
```

가능한 원인:

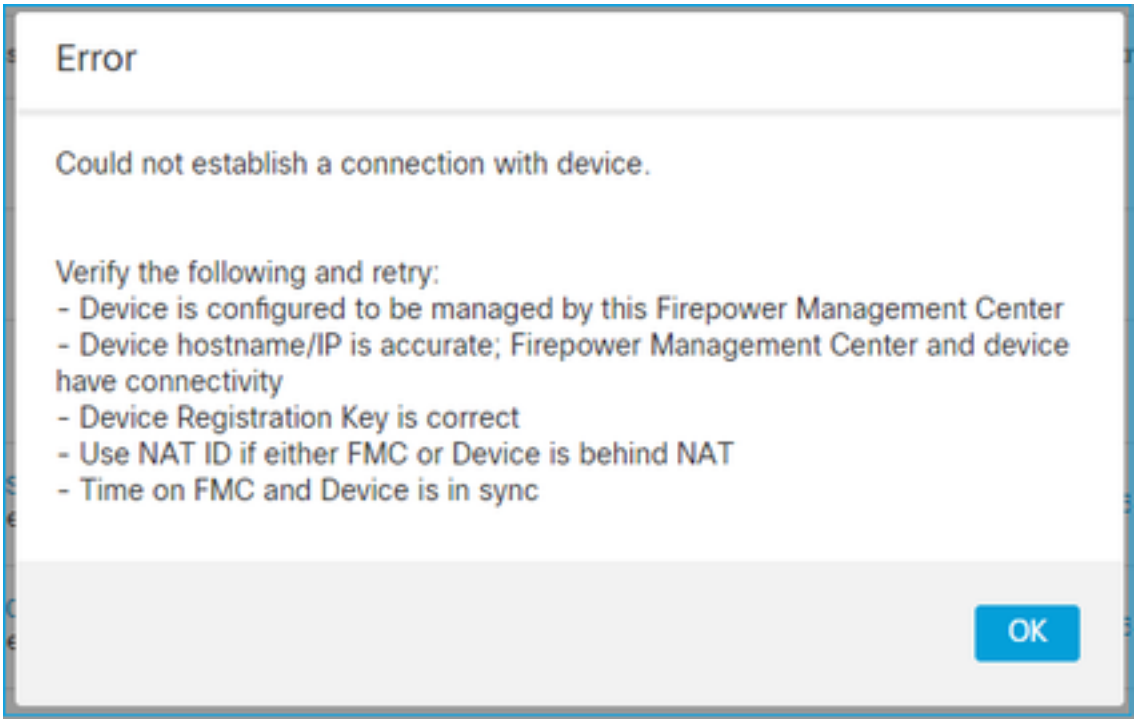
- FMC에 FTD 장치가 추가되어 있지 않습니다.
- 경로의 디바이스(예: 방화벽)는 트래픽을 차단하거나 수정합니다.
- 패킷이 경로에서 제대로 라우팅되지 않습니다.
- FTD 또는 FMC의 sftunnel 프로세스가 다운되었습니다(시나리오 6 확인).
- 경로에 MTU 문제가 있습니다(시나리오 확인).

캡처 분석을 위해 다음 문서를 확인하십시오.

Firepower 방화벽 캡처를 분석하여 네트워크 문제를 효과적으로 해결

## 4. FTD - FMC 간에 호환되지 않는 SW

FMC UI에는 다음이 표시됩니다.




**권장 조치**

FTD /ngfw/var/log/messages 파일을 확인합니다.

```
Apr 19 22:08:09 mzafeiro_vFTD66 SF-IMS[12730]: [12830] sftunneld:sf_connections [INFO] Need to
send SW version and Published Services to 10.62.148.247
Apr 19 22:08:09 mzafeiro_vFTD66 SF-IMS[12730]: [12830] sftunneld:sf_channel [INFO] >>
ChannelState do_dataio_for_heartbeat peer 10.62.148.247 / channelA / CONTROL [ msgSock &
ssl_context ] <<
Apr 19 22:08:09 mzafeiro_vFTD66 SF-IMS[12730]: [12830] sftunneld:sf_heartbeat [INFO] Saved SW
VERSION from peer 10.62.148.247 (10.10.0.4)
Apr 19 22:08:09 mzafeiro_vFTD66 SF-IMS[12730]: [12830] sftunneld:ssl_mac [WARN] FMC(manager)
10.62.148.247 send unsupported version 10.10.0.4
Apr 19 22:08:09 mzafeiro_vFTD66 SF-IMS[12730]: [12830] sftunneld:sf_connections [INFO]
<<<<<<<<<<<<<<<<<<<< ShutDownPeer 10.62.148.247 >>>>>>>>>>>>>>>>>>>>
Apr 19 22:08:09 mzafeiro_vFTD66 SF-IMS[12730]: [12830] sftunneld:stream_file [INFO] Stream CTX
destroyed for 10.62.148.247
Apr 19 22:08:09 mzafeiro_vFTD66 SF-IMS[12730]: [12830] sftunneld:sf_channel [INFO] >>
ChannelState ShutDownPeer peer 10.62.148.247 / channelA / CONTROL [ msgSock & ssl_context ] <<
```

Firepower 호환성 매트릭스를 확인합니다.

Cisco Firepower 호환성 가이드

## 5. FTD와 FMC의 시차

FTD-FMC 통신은 두 디바이스 간의 시간 차이에 민감합니다. FTD와 FMC를 동일한 NTP 서버에서 동기화하도록 설계해야 합니다.

특히 FTD를 41xx 또는 93xx와 같은 플랫폼에 설치할 경우 상위 섀시(FXOS)에서 시간 설정이 필요

합니다.

**권장 조치**

FCM(섀시 관리자) 및 FMC가 동일한 시간 소스(NTP 서버)를 사용하는지 확인합니다

## 6. sftunnel 프로세스 중단 또는 비활성화

FTD에서 sftunnel **프로세스**는 등록 프로세스를 처리합니다. 관리자 컨피그레이션 전의 프로세스 상태입니다.

```
> pmtool status
…
sftunnel (system) - Waiting
Command: /ngfw/usr/local/sf/bin/sftunnel -d -f /etc/sf/sftunnel.conf
PID File: /ngfw/var/sf/run/sftunnel.pid
Enable File: /ngfw/etc/sf/sftunnel.conf
CPU Affinity:
Priority: 0
Next start: Mon Apr 20 06:12:06 2020
Required by: sfmgr,sfmbservice,sfipproxy
CGroups: memory=System/ProcessHigh
```

등록 상태:

```
> show managers
No managers configured.
```

관리자를 구성합니다.

```
> configure manager add 10.62.148.75 cisco123
Manager successfully configured.
Please make note of reg_key as this will be required while adding Device in FMC.
```

이제 프로세스가 시작됩니다.

```
> pmtool status
…
sftunnel (system) - Running 24386
Command: /ngfw/usr/local/sf/bin/sftunnel -d -f /etc/sf/sftunnel.conf
```

```
PID File: /ngfw/var/sf/run/sftunnel.pid
Enable File: /ngfw/etc/sf/sftunnel.conf
CPU Affinity:
Priority: 0
Next start: Mon Apr 20 07:12:35 2020
Required by: sfmgr,sfmbservice,sfipproxy
CGroups: memory=System/ProcessHigh(enrolled)
```

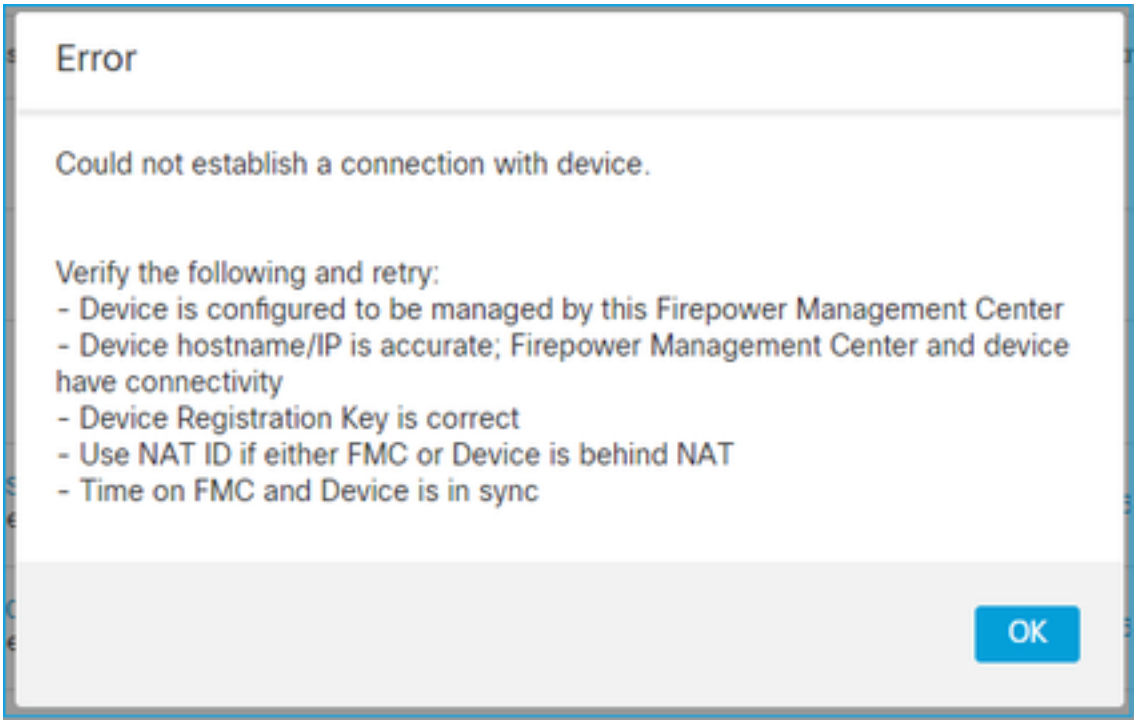
드물게 프로세스가 다운되거나 비활성화될 수 있습니다.

```
> pmtool status
…
sftunnel (system) - User Disabled
Command: /ngfw/usr/local/sf/bin/sftunnel -d -f /etc/sf/sftunnel.conf
PID File: /ngfw/var/sf/run/sftunnel.pid
Enable File: /ngfw/etc/sf/sftunnel.conf
CPU Affinity:
Priority: 0
Next start: Mon Apr 20 07:09:46 2020
Required by: sfmgr,sfmbservice,sfipproxy
CGroups: memory=System/ProcessHigh
```

관리자 상태는 정상으로 보입니다.

```
> show managers
Host                    : 10.62.148.75
Registration Key        : ****
Registration            : pending
RPC Status              :
```

반면 디바이스 등록은 실패합니다.




FTD에서 /ngfw/var/log/messages에 관련 **메시지가 표시되지 않습니다.**

**권장 조치**

FTD 문제 해결 파일 수집 및 Cisco TAC에 문의

## 7. 보조 FMC에 대한 FTD 등록 보류 중

초기 FTD가 FMC HA 설정에 등록된 후 FTD 디바이스가 보조 FMC에 추가되지 않는 경우가 있습니다.

**권장 조치**

이 문서에 설명된 절차를 수행합니다.

CLI를 사용하여 Firepower Management Center 고가용성의 디바이스 등록 확인

> **경고:** 이 절차에는 디바이스 등록 취소가 포함되어 있으므로 번거롭습니다. 이는 FTD 디바이스 컨피그레이션에 영향을 줍니다(삭제됨). 초기 FTD 등록 및 설정 시에만 이 절차를 사용하는 것이 좋습니다. 경우에 따라 FTD 및 FMC 문제 해결 파일을 수집하고 Cisco TAC에 문의하십시오.

## 8. 경로 MTU로 인해 등록 실패

Cisco TAC에서는 sftunnel 트래픽이 작은 MTU를 갖는 링크를 통과해야 하는 시나리오가 있습니다. sftunnel 패킷에는 **Don't fragment** bit **Set가** 있으므로 단편화가 허용되지 않습니다.

| | Source | Destination | Protocol | Length | TCP Segment | Don't fragment | Info |
|---|---|---|---|---|---|---|---|
| 57 | 10.62.148.75 | 10.62.148.42 | TCP | 74 | 0 | Set | 47709 → 8305 [SYN] Seq=2860693630 Win=29200 Len=0 MS |
| 58 | 10.62.148.42 | 10.62.148.75 | TCP | 74 | 0 | Set | 8305 → 47709 [SYN, ACK] Seq=279535377 Ack=2860693631 |
| 59 | 10.62.148.75 | 10.62.148.42 | TCP | 66 | 0 | Set | 47709 → 8305 [ACK] Seq=2860693631 Ack=279535378 Win= |
| 60 | 10.62.148.75 | 10.62.148.42 | TLSv1.2 | 229 | 163 | Set | Client Hello |
| 61 | 10.62.148.42 | 10.62.148.75 | TCP | 66 | 0 | Set | 8305 → 47709 [ACK] Seq=279535378 Ack=2860693794 Win= |
| 62 | 10.62.148.42 | 10.62.148.75 | TLSv1.2 | 1514 | 1448 | Set | Server Hello |
| 63 | 10.62.148.75 | 10.62.148.42 | TCP | 66 | 0 | Set | 47709 → 8305 [ACK] Seq=2860693794 Ack=279536826 Win= |
| 64 | 10.62.148.42 | 10.62.148.75 | TLSv1.2 | 803 | 737 | Set | Certificate, Certificate Request, Server Hello Done |
| 65 | 10.62.148.75 | 10.62.148.42 | TCP | 66 | 0 | Set | 47709 → 8305 [ACK] Seq=2860693794 Ack=279537563 Win= |
| 66 | 10.62.148.75 | 10.62.148.42 | TLSv1.2 | 2581 | 2515 | Set | Certificate, Client Key Exchange, Certificate Verify |
| 67 | 10.62.148.42 | 10.62.148.75 | TCP | 66 | 0 | Set | 8305 → 47709 [ACK] Seq=279537563 Ack=2860696309 Win= |
| 68 | 10.62.148.42 | 10.62.148.75 | TLSv1.2 | 1284 | 1218 | Set | New Session Ticket, Change Cipher Spec, Encrypted Ha |
| 69 | 10.62.148.75 | 10.62.148.42 | TLSv1.2 | 364 | 298 | Set | Application Data |
| 70 | 10.62.148.42 | 10.62.148.75 | TLSv1.2 | 364 | 298 | Set | Application Data |

또한 /ngfw/var/log/messages 파일에 다음과 같은 메시지가 표시됩니다.

MSGS: 10-09 14:41:11 ftd1 SF-IMS[7428]: [6612] sftunneld:sf_ssl [ERROR] **Connect:SSL 핸드셰이크 실패**

**권장 조치**

프래그먼트화로 인한 패킷 손실이 있는지 확인하려면 FTD, FMC 및 경로의 디바이스에 대한 캡처를 수행합니다. 양 끝에 도착하는 패킷이 표시되는지 확인합니다.

FTD에서 FTD 관리 인터페이스의 MTU를 낮춥니다. 기본값은 1500바이트입니다. MAX는 관리 인터페이스의 경우 1500이고 이벤트 인터페이스의 경우 9000입니다. 이 명령은 FTD 6.6 릴리스에 추가되었습니다.

Cisco Firepower Threat Defense 명령 참조

예

```
> configure network mtu 1300
MTU set successfully to 1300 from 1500 for eth0
Refreshing Network Config...
Interface eth0 speed is set to '10000baseT/Full'
```

확인

```
> show network
===============[ System Information ]===============
Hostname                  : ksec-sfvm-kali-3.cisco.com
DNS Servers               : 192.168.200.100
Management port           : 8305
IPv4 Default route
  Gateway                 : 10.62.148.1
  Netmask                 : 0.0.0.0


======================[ eth0 ]======================
State                     : Enabled
Link                      : Up
Channels                  : Management & Events
Mode                      : Non-Autonegotiation
MDI/MDIX                  : Auto/MDIX
MTU                       : 1300
MAC Address               : 00:50:56:85:7B:1F
----------------------[ IPv4 ]----------------------
Configuration             : Manual
Address                   : 10.62.148.42
Netmask                   : 255.255.255.128
Gateway                   : 10.62.148.1
----------------------[ IPv6 ]----------------------
```

FTD에서 경로 MTU를 확인하려면 다음 명령을 사용할 수 있습니다.

```
root@firepower:/home/admin# ping -M do -s 1500 10.62.148.75
```

do **옵션**은 ICMP **패킷**에서 **don't fragment** 비트를 설정합니다

FMC에서는 이 문서에 설명된 대로 FMC 관리 인터페이스의 MTU 값을 낮춥니다.

Firepower Management Center 관리 인터페이스 구성

## 9. Chassis Manager UI에서 부트스트랩 변경 후 FTD가 등록 취소됩니다.

이는 FP41xx 및 FP93xx 플랫폼에 적용되며 Cisco 버그 ID CSCvn에 문서화되었습니다45138 .

일반적으로 재해 복구를 수행하지 않는 한 FCM(섀시 관리자)에서 부트스트랩 변경을 수행하지 않아야 합니다.

### 권장 조치

부트스트랩 변경을 수행했고 조건을 일치시킨 경우(부트스트랩 변경 후 FTD가 가동되는 동안 FTD-FMC 통신이 끊어짐) FTD를 삭제하고 FMC에 다시 등록해야 합니다.

## 10. FTD는 ICMP 리디렉션 메시지로 인해 FMC에 대한 액세스 권한을 상실합니다.

이 문제는 등록 프로세스에 영향을 주거나 등록 후 FTD-FMC 통신을 중단할 수 있습니다.

이 경우 문제는 FTD 관리 인터페이스 및 블랙홀 FTD-FMC 통신에 **ICMP** 리디렉션 메시지를 전송하는 네트워크 디바이스입니다.

### 이 문제를 확인하는 방법

이 경우 10.100.1.1은 FMC IP 주소입니다. FTD에는 관리 인터페이스의 FTD에서 수신한 ICMP 리디렉션 메시지로 인한 캐시된 경로가 있습니다.

```
ftd1:/ngfw/var/common# ip route get 10.100.1.1
10.100.1.1 via 10.10.1.1 dev br1  src 10.10.1.23
    cache
```

### 권장 조치

#### 1단계

ICMP를 전송하는 디바이스(예: 업스트림 L3 스위치, 라우터 등)에서 ICMP 리디렉션을 비활성화합니다.

#### 2단계

FTD CLI에서 FTD 경로 캐시를 지웁니다.

```
ftd1:/ngfw/var/common# ip route flush 10.100.1.1
```

리디렉션되지 않으면 다음과 같이 표시됩니다.

```
ftd1:/ngfw/var/common# ip route get 10.100.1.1
10.100.1.1 via 10.62.148.1 dev eth0  src 10.10.1.23
    cache  mtu 1500 advmss 1460 hoplimit 64
```

## 참조

- ICMP 리디렉션 메시지 이해
- Cisco 버그 ID CSCvm53282 FTD: ICMP 리디렉션에 의해 추가된 라우팅 테이블은 라우팅 테이블 캐시에서 영원히 중단됩니다.

## 관련 정보

- NGFW 컨피그레이션 가이드

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.