Configure, Verify, and Troubleshoot Firepower Device Registration

Contents

Introduction

Prerequisites

- Requirements
- Components Used

Background Information

- Design Options
- What Information is Exchanged Through the sftunnel?
- What Protocol/Port is Used by the sftunnel?
- How to Change the Sftunnel TCP Port on FTD?
- How Many Connections are Established by the sftunnel?
- Which Device Initiates Each Channel?

Configure

- Registration Basics
- Scenario 1. FMC and FTD Static IP Address
- Scenario 2. FTD DHCP IP Address - FMC Static IP Address
- Scenario 3. FTD Static IP Address - FMC DHCP IP Address
- Scenario 4. FTD Registration to FMC HA
- Scenario 5. FTD HA
- Scenario 6. FTD Cluster

Troubleshoot Common Issues

- 1. Invalid Syntax on FTD CLI
- 2. Registration Key Mismatch Between FTD - FMC
- 3. Connectivity Issues Between FTD - FMC
- 4. Incompatible SW Between FTD – FMC
- 5. Time Difference Between FTD and FMC
- 6. sftunnel Process Down or Disabled
- 7. FTD Pending registration on Secondary FMC
- 8. Registration Fails due to Path MTU
- 9. FTD Gets Unregistered After a Bootstrap Change From the Chassis Manager UI
- 10. FTD Loses Access to FMC due to ICMP Redirect Messages

Introduction

This document describes the troubleshoot procedures of the connection between Firepower Threat Defense (FTD) and Firepower Management Center (FMC).

Prerequisites

Requirements

There are no specific requirements for this document.

Components Used

The information in this document is based on these software and hardware versions:

- FTD software 6.6.x and 6.5.x
- FMC software 6.6.x

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command.

Background Information

This document describes the operation, verification, and troubleshoot procedures of the connection (sftunnel) between a managed FTD and the managed FMC.

The information and the examples are based on FTD, but most of the concepts are also fully applicable to NGIPS (7000/8000 series appliances) or a FirePOWER module on ASA55xx.

An FTD supports 2 main management modes:

- Off-box via FMC - also known as remote management
- On-box via Firepower Device Manager (FDM) and/or Cisco Defense Orchestrator (CDO) – also known as local management

In the case of remote management the FTD needs first to register to the FMC that uses a process known as device registration.

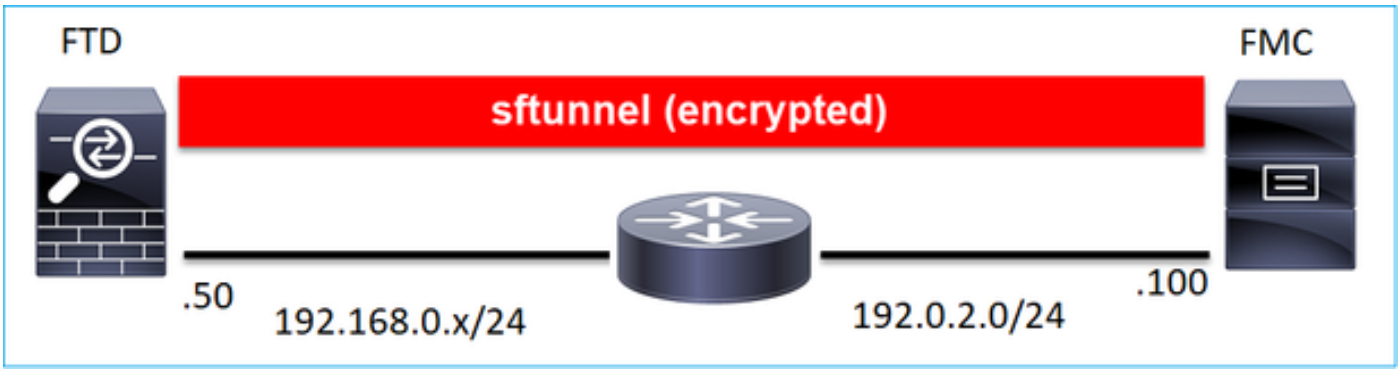
When the registration is done, the FTD and the FMC establish a secure tunnel called **sftunnel** (the name derives from the Sourcefire tunnel).

Design Options

From a design point of view, the FTD – FMC can be in the same L3 subnet:

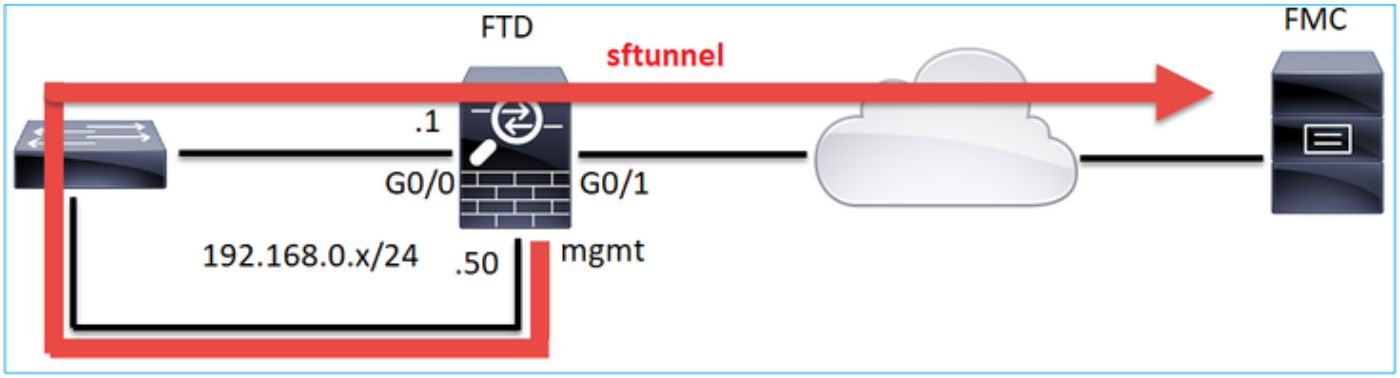


or be separated by different networks:



192.0.2.0

Note: The sftunnel can also go through the FTD itself. This design is **not recommended**. The reason is an FTD data-plane issue can disrupt the communication between FTD and FMC.



What Information is Exchanged Through the sftunnel?

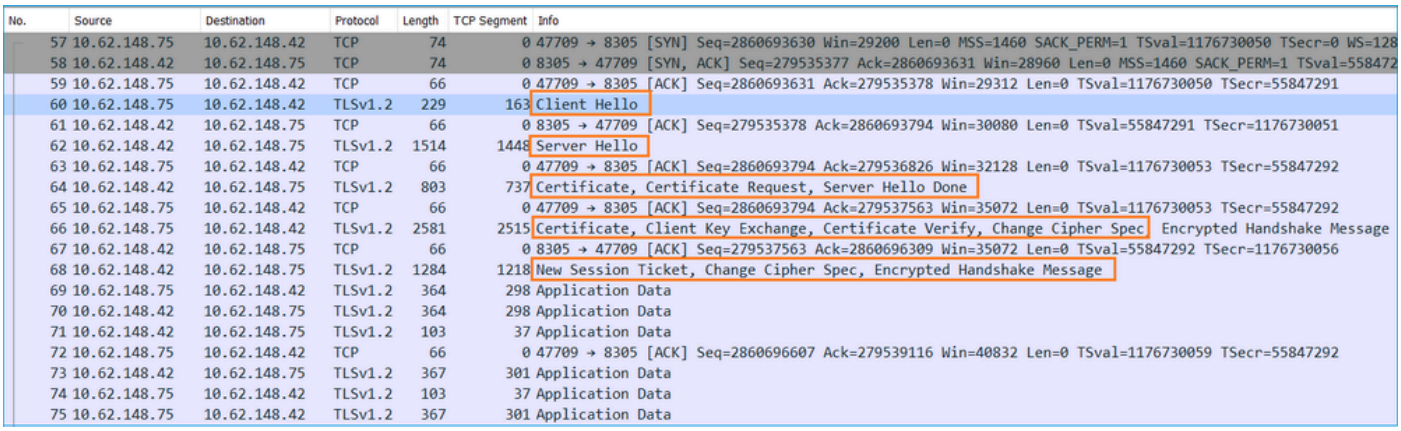
This list contains most of the information that is carried through the sftunnel:

- Appliance Heartbeat (keepalives)
- Time Synchronization (NTP)
- Events (Connection, Intrusion/IPS, File, SSL and so on)
- Malware Lookups
- Health Events/Alerts

- User and Group info (for Identity Policies)
- FTD HA state info
- FTD Cluster state info
- Security Intelligent (SI) info/events
- Threat Intelligence Director (TID) info/events
- Captured files
- Network Discovery Events
- Policy bundle (policy deployment)
- Software upgrade bundles
- Software patch bundles
- VDBs
- SRUs

What Protocol/Port is Used by the sftunnel?

The sftunnel uses **TCP** port **8305**. In the backend it is a **TLS** tunnel:



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	10.62.148.75	10.62.148.42	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	10.62.148.42	10.62.148.75	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

How to Change the Sftunnel TCP Port on FTD?

<#root>

>

configure network management-port 8306

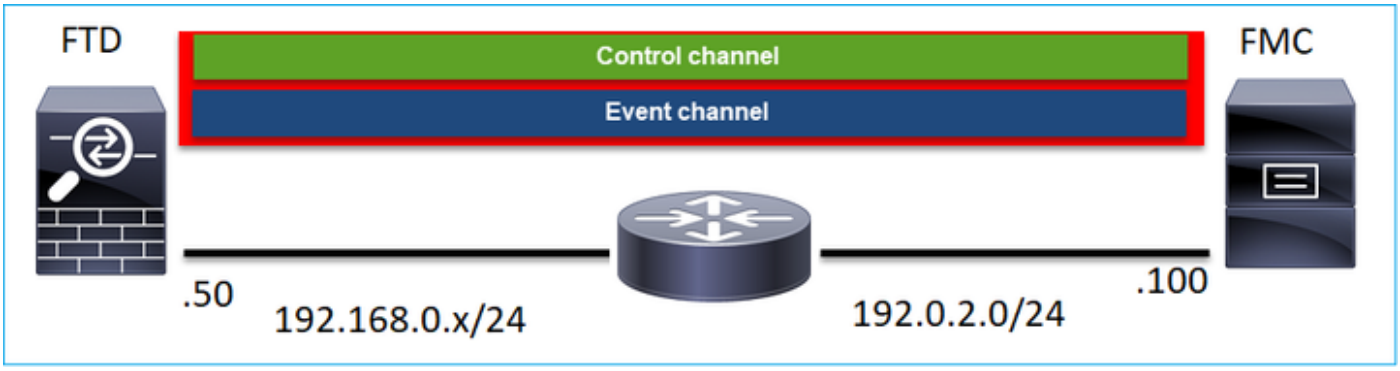
Management port changed to 8306.

Note: In this case you must also change the port on FMC (**Configuration > Management Interfaces > Shared Settings**). This affects all other devices that are already registered to the same FMC. Cisco strongly recommends that you keep the default settings for the remote management port, but if the management port conflicts with other communications on your network, you can choose a different port. If you change the management port, you must change it for all devices in your deployment that need to communicate together.

How Many Connections are Established by the sftunnel?

The sftunnel establishes 2 connections (channels):

- Control channel
- Event channel



Which Device Initiates Each Channel?

It depends on the scenario. Check the scenarios describes in the rest of the document.

Configure

Registration Basics

FTD CLI

On FTD the basic syntax for the device registration is:

> **configure manager add <FMC Host> <Registration Key> <NAT ID>**

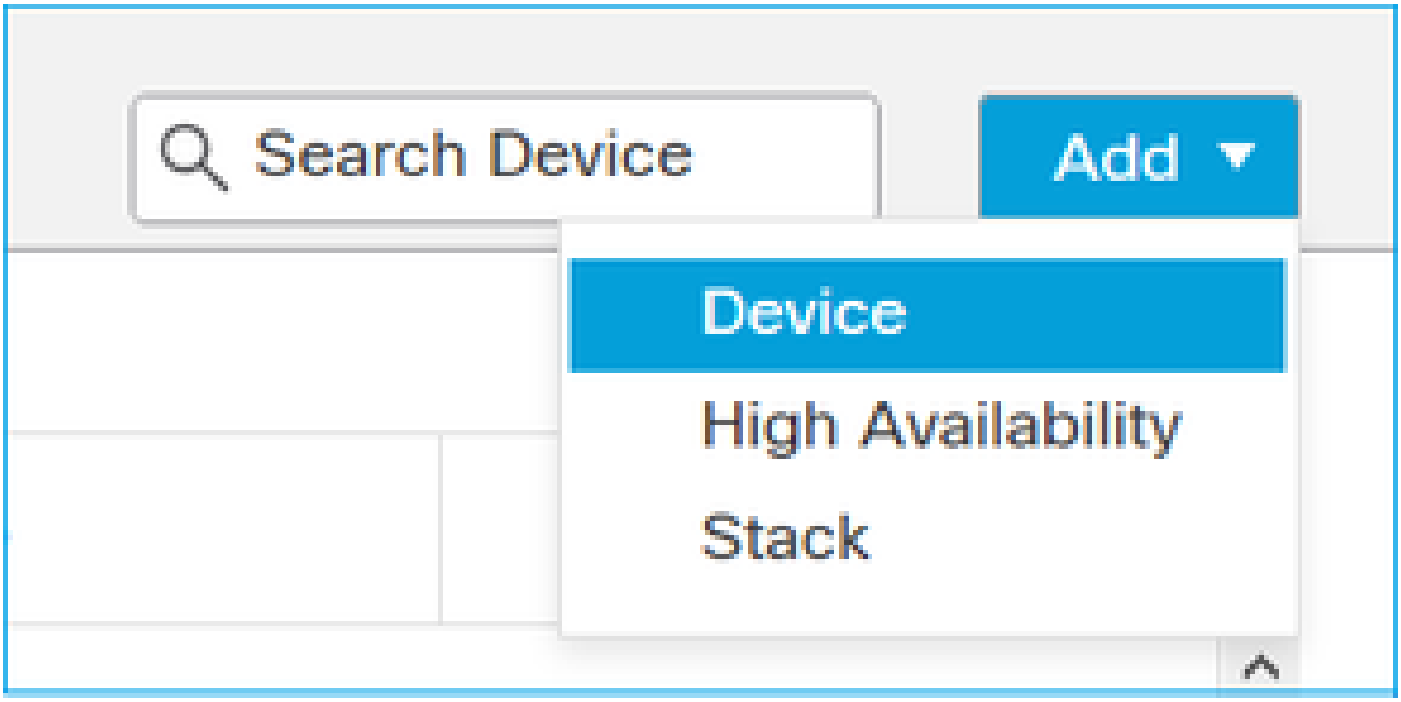
Value	**Description**
FMC Host	This can be either: • Hostname • ipv4 address • ipv6 address • DONTRESOLVE
Registration Key	This is a shared secret alphanumeric string (between 2 and 36 chars) used for the device registration. Only alphanumerics, hyphen (-), underscore (_) and period (.) are allowed.
NAT ID	An alphanumeric string used during the registration process between the FMC and the device **when one side does not specify an IP address**. Specify the

	same NAT ID on the FMC.

For additional details check the Cisco Firepower Threat Defense Command Reference

FMC UI

On FMC navigate to **Devices > Device Management.** Select **Add > Device**



Add Device

Host:*

Display Name:

Registration Key:*

Domain:

Select Domain

Group:

None

Access Control Policy:*

Smart Licensing

- [ ] Malware
- [ ] Threat
- [ ] URL Filtering

Advanced

Unique NAT ID:*

- [x] Transfer Packets

FTD CLI

> **configure manager add <FMC Static IP> <Registration Key>**

For example:

```
<#root>

>

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.
```

Background Info

As soon as you enter the FTD command the FTD tries to connect to the FMC every 20 seconds, but since the FMC is not yet configured it replies with TCP RST:

```
<#root>

>

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

The device registration status:

<#root>

>

show managers

Host   : 10.62.148.75
Registration Key   : ****
Registration   : pending
RPC Status   :
Type   : Manager
Host   : 10.62.148.75
Registration   : Pending

The FTD listens on port TCP 8305:

<#root>

admin@vFTD66:~$

netstat -na | grep 8305

tcp   0   0 10.62.148.42:

8305

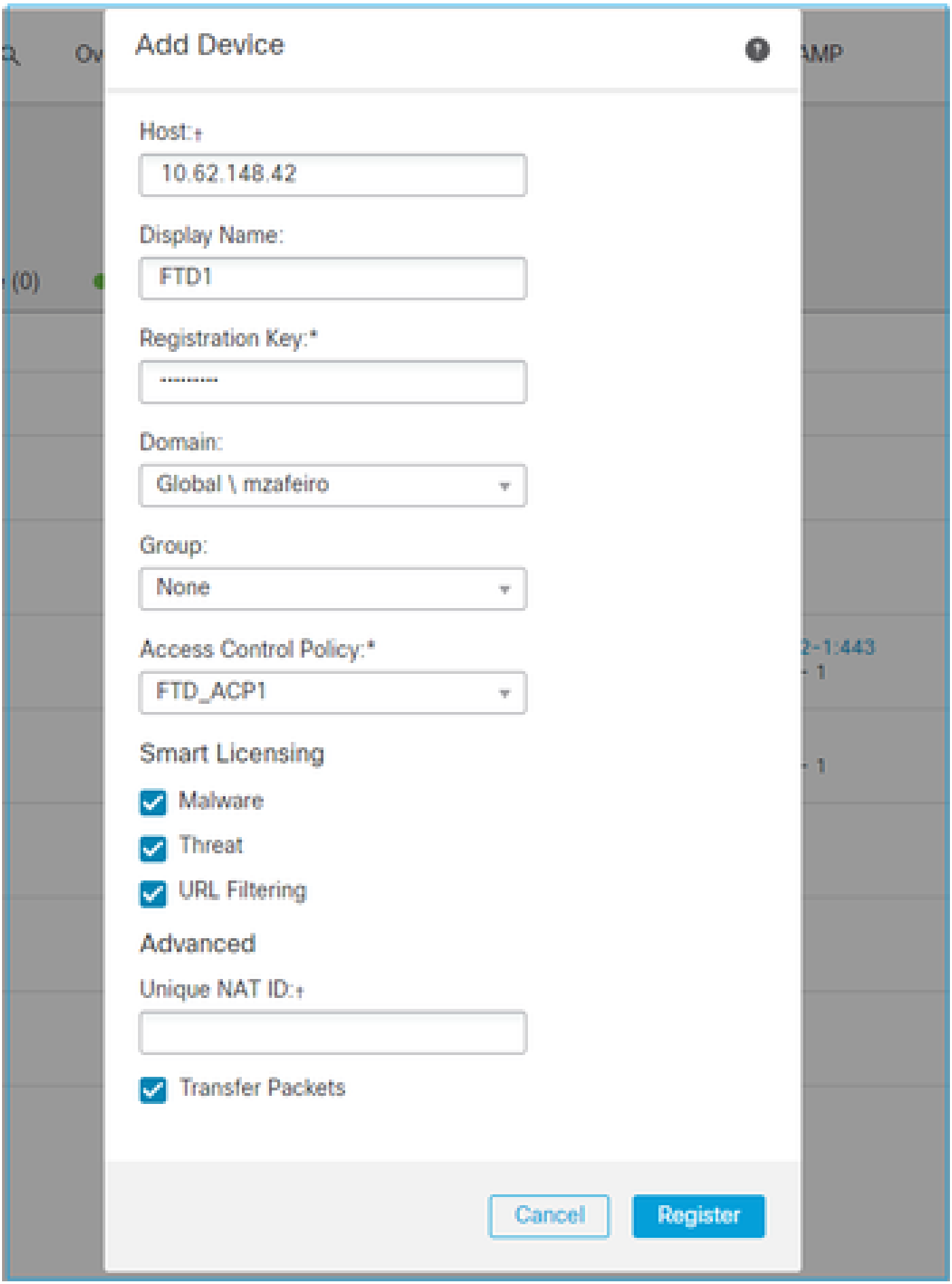
       0.0.0.0:*

LISTEN

FMC UI

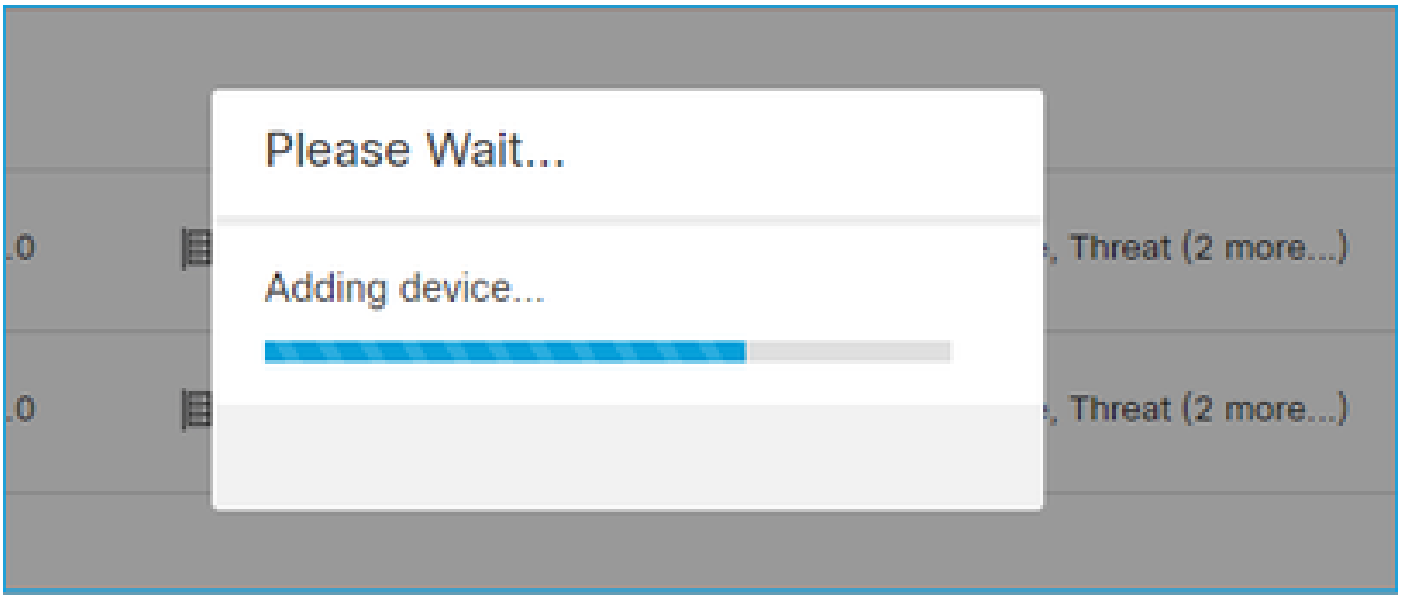
In this case, specify the:

- Host (IP address of the FTD)
- Display Name
- Registration Key (this must match the one configured on FTD)
- Access Control Policy
- Domain
- Smart Licensing info


Add Device
Host:*
10.62.148.42
Display Name:
FTD1
Registration Key:*
Domain:
Global \ mzafeiro
Group:
None
Access Control Policy:*
FTD_ACP1
Smart Licensing
Malware
Threat
URL Filtering
Advanced
Unique NAT ID:*
Transfer Packets
Cancel
Register

Select **Register**

The registration process starts:



The FMC starts to listen on port TCP 8305:

<#root>

admin@FMC2000-2:~$

netstat -na | grep 8305

tcp 0 0 10.62.148.75:

8305

0.0.0.0:*

LISTEN

In the background the FMC initiates a TCP connection:

<#root>

```
20:15:55.437434 IP 10.62.148.42.49396 > 10.62.148.75.8305: Flags [S], seq 655146775, win 29200, options
20:15:55.437685 IP 10.62.148.75.8305 > 10.62.148.42.49396: Flags [R.], seq 0, ack 655146776, win 0, len
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, optio
20:16:08.342953 IP 10.62.148.42.8305 > 10.62.148.75.50693: Flags [.], ack 164, win 235, options [nop,no

The sftunnel Control channel is established:

<#root>

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

<#root>

>

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 '10.62.14

Peer channel Channel-B is not valid

After a few minutes the Event channel is established. The initiator of the Event channel can be **either side**.
In this example, it was the FMC:

<#root>

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, optio

The random source port denotes the connection initiator:

<#root>

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

In case the Event channel was initiated by the FTD the output is:

```
<#root>

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
```

From the FTD side:

```
<#root>

>

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 '10.62.1
       Peer channel Channel-B is valid  type (EVENT), using 'eth0', connected to '10.62.148.75' via '10
```

<#root>

>

show managers

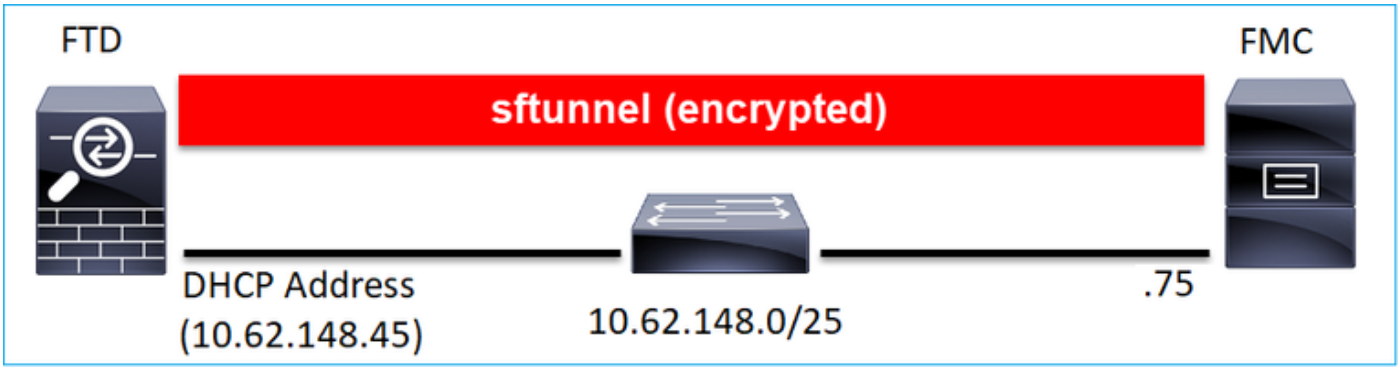
Type : Manager
Host : 10.62.148.75

Registration : Completed

>

Scenario 2. FTD DHCP IP Address - FMC Static IP Address

In this scenario, the FTD management interface got his IP address from a DHCP server:



FTD CLI

You must specify the NAT ID:

> **configure manager add <FMC Static IP> <Registration Key> <NAT ID>**

For example:

<#root>

>

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.

>

The FTD registration status:

```
<#root>

>

show managers

Host                    : 10.62.148.75
Registration Key        : ****

Registration            : pending

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

FMC UI

In this case, specify the:

- Display Name
- Registration Key (this must match the one configured on FTD)
- Access Control Policy
- Domain
- Smart Licensing info
- NAT ID (this is **required** when **Host is not specified**. It must match the one configured on FTD)

Add Device

Host:*

empty

Display Name:

FTD1

Registration Key:*

Domain:

Global \ mzafeiro

Group:

None

Access Control Policy:*

FTD_ACP1

Smart Licensing

- [x] Malware
- [x] Threat
- [x] URL Filtering

Advanced

Unique NAT ID:*

nat123

- [x] Transfer Packets

Who initiates the sftunnel in this case?

The FTD initiates both channel connections:

```
<#root>

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
```

Scenario 3. FTD Static IP Address - FMC DHCP IP Address




```
<#root>

>

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.

>
```

Note: With DONTRESOLVE the NAT ID is required.

FMC UI

In this case specify the:

- **FTD IP address**
- Display Name
- Registration Key (this must match the one configured on FTD)
- Access Control Policy
- Domain
- Smart Licensing info
- **NAT ID (It must match the one configured on FTD)**

Add Device

Host:*

10.62.148.42

Display Name:

FTD1

Registration Key:*

.....

Domain:

Global \ mzafeiro

Group:

None

Access Control Policy:*

FTD_ACP1

Smart Licensing

- [x] Malware
- [x] Threat
- [x] URL Filtering

Advanced

Unique NAT ID:*

nat123

- [x] Transfer Packets

- The FMC initiates the Control channel.
- The Event channel can be initiated by either side.

<#root>

```
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
```

Scenario 4. FTD Registration to FMC HA

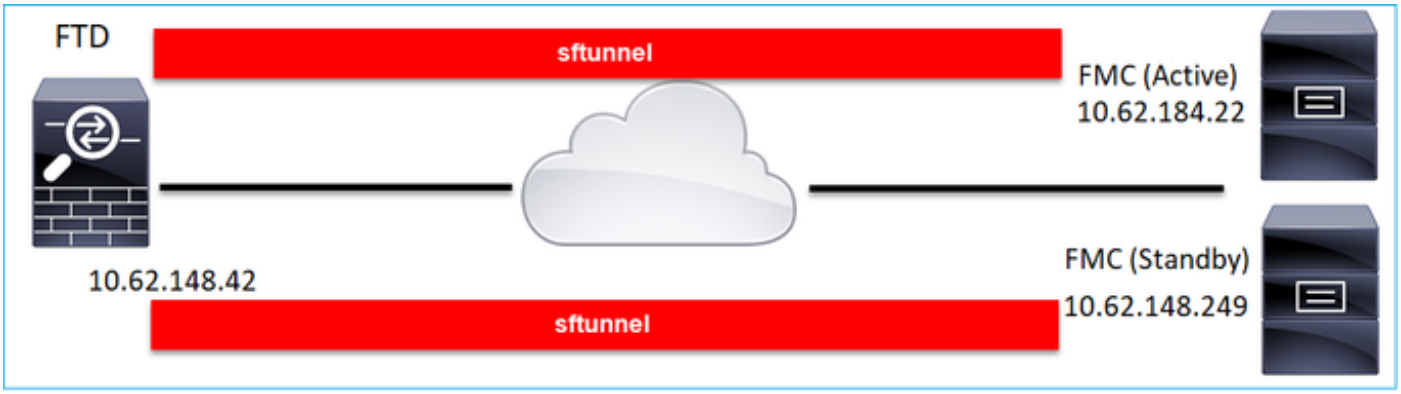
On FTD configure only the Active FMC:

<#root>

```
>

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.
```



Note: Ensure that TCP port 8305 traffic is allowed from the FTD to both FMCs.

First, the sftunnel to the Active FMC is established:

```
<#root>

>

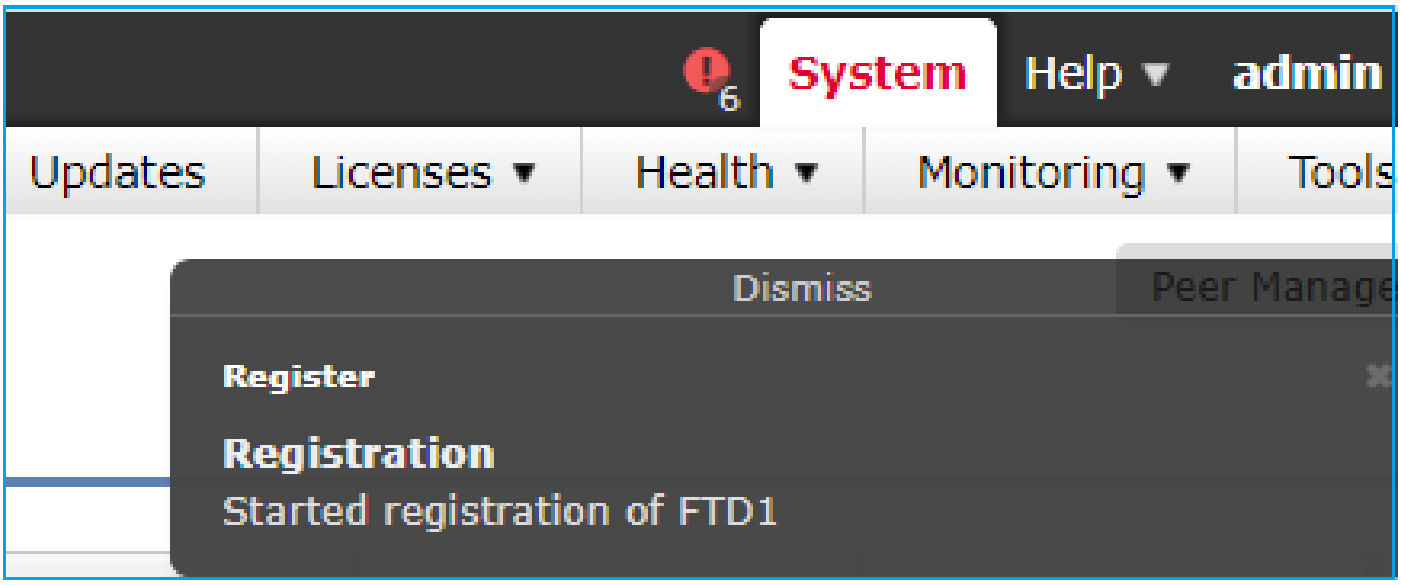
show managers

Type                    : Manager
Host                    :

10.62.184.22

Registration            : Completed
```

After a few minutes the FTD starts the registration to the Standby FMC:




```
<#root>

>

show managers

Type                    : Manager
Host                    :

10.62.184.22

Registration            : Completed


Type                    : Manager
Host                    :

10.62.148.249

Registration            : Completed
```

In the FTD backend, 2 Control channels (one to each FMC) and 2 Event channels (one to each FMC) are established:

<#root>

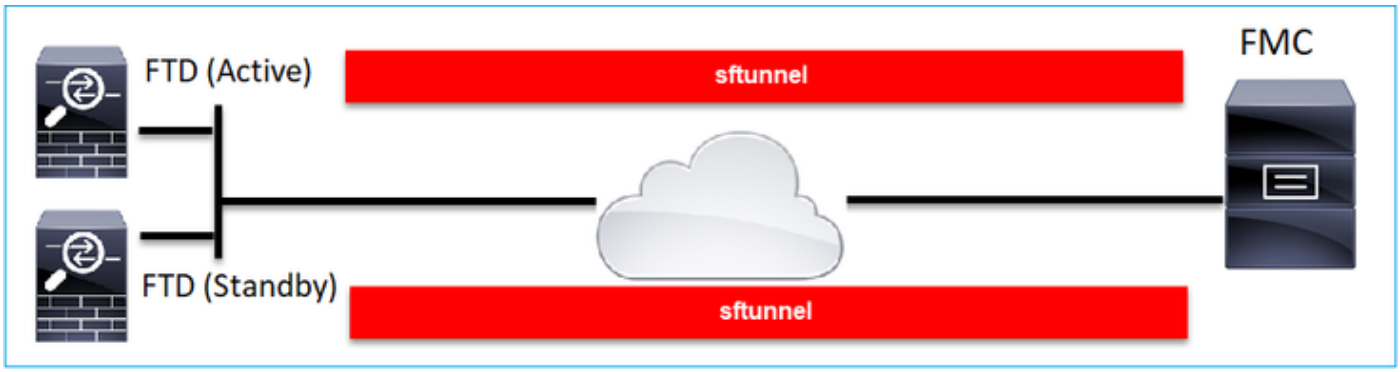
```
ftd1:/home/admin#

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
```

Scenario 5. FTD HA

In the case of FTD HA each unit has a separate tunnel to the FMC:

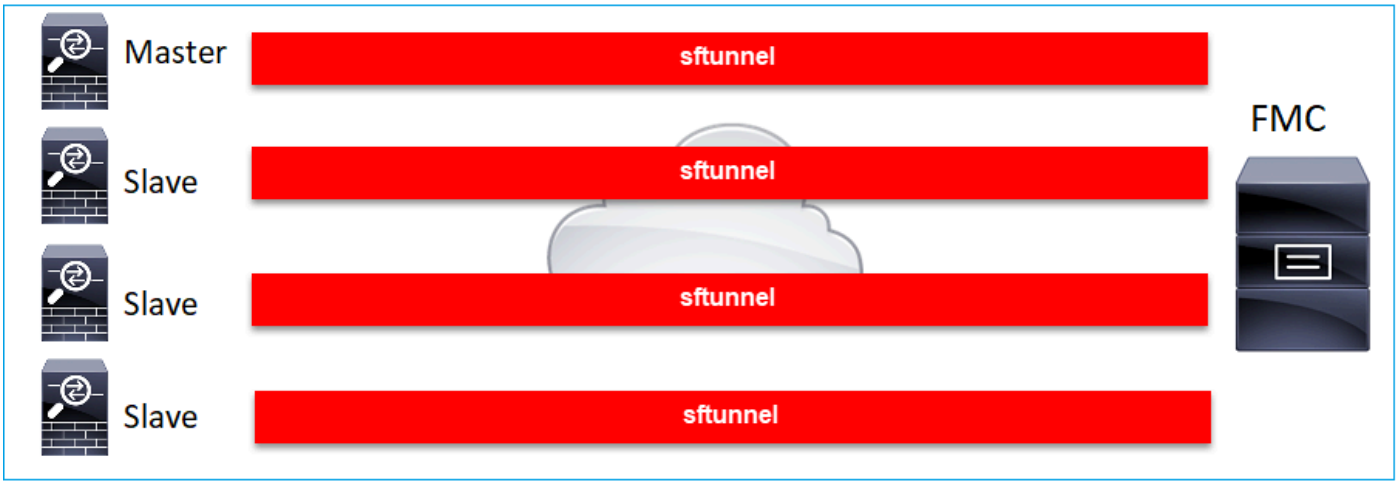


You register both FTDs independently and then from FMC you form the FTD HA. For more details check:

- Configure FTD High Availability on Firepower Appliances
- High Availability for Firepower Threat Defense

Scenario 6. FTD Cluster

In the case of FTD Cluster each unit has a separate tunnel to the FMC. As from 6.3 FMC release you need to only register the FTD Control unit to FMC. Then the FMC takes care of the rest of the units and auto-discovers + registers them.

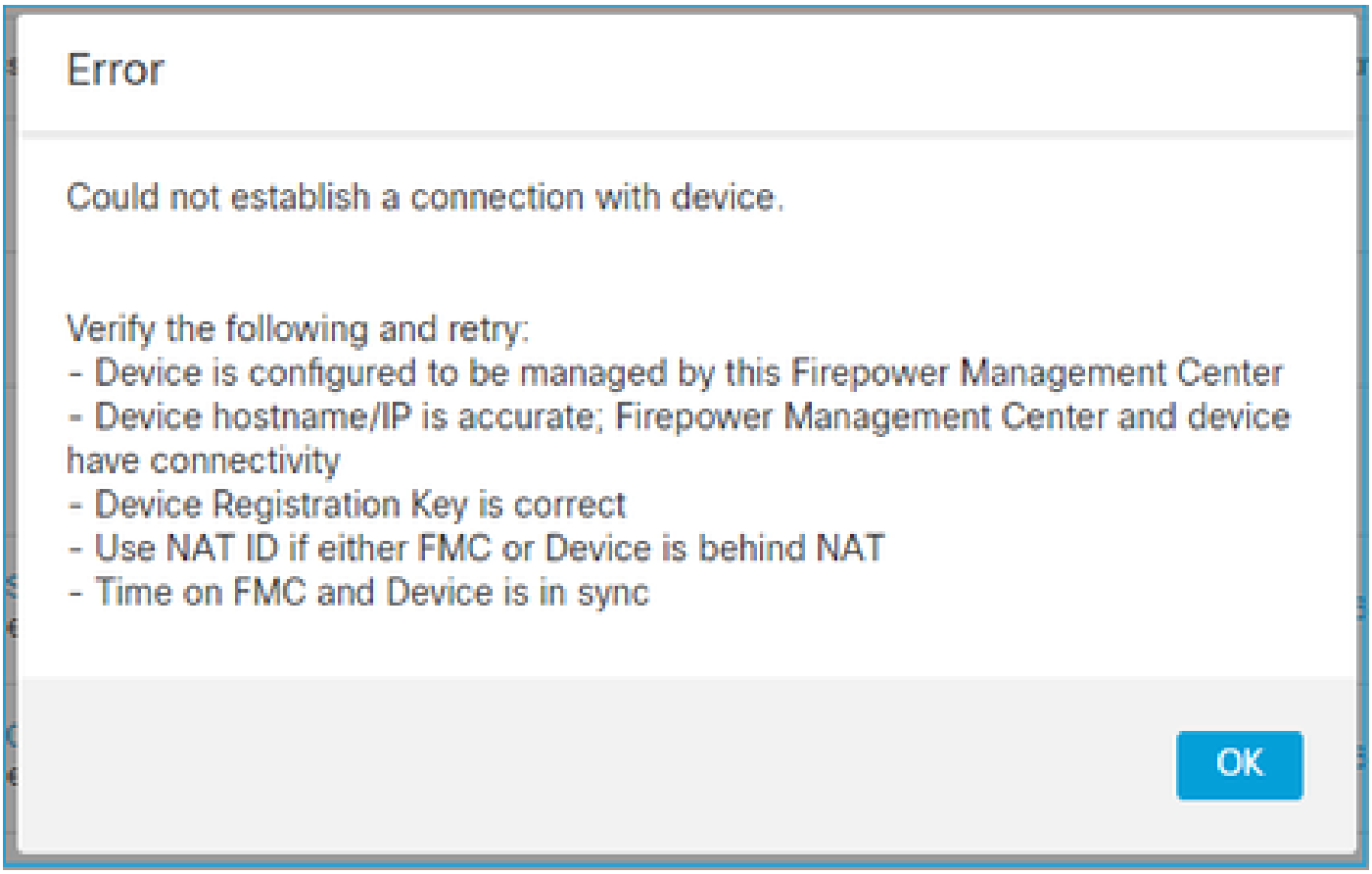


Note: We recommend to add the Control unit for the best performance, but you can add any unit of the cluster. For additional details check: Create a Firepower Threat Defense Cluster

Troubleshoot Common Issues

1. Invalid Syntax on FTD CLI

In case of invalid syntax on FTD and a failed registration attempt the FMC UI shows a quite generic Error message:



In this command the keyword **key** is the registration key while the **cisco123** is the NAT ID. It is quite common to add the keyword key while technically there is no such keyword:

```
<#root>

>

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.
```

Recommended Action

Use proper syntax and do not use keywords that do not exist.

```
<#root>

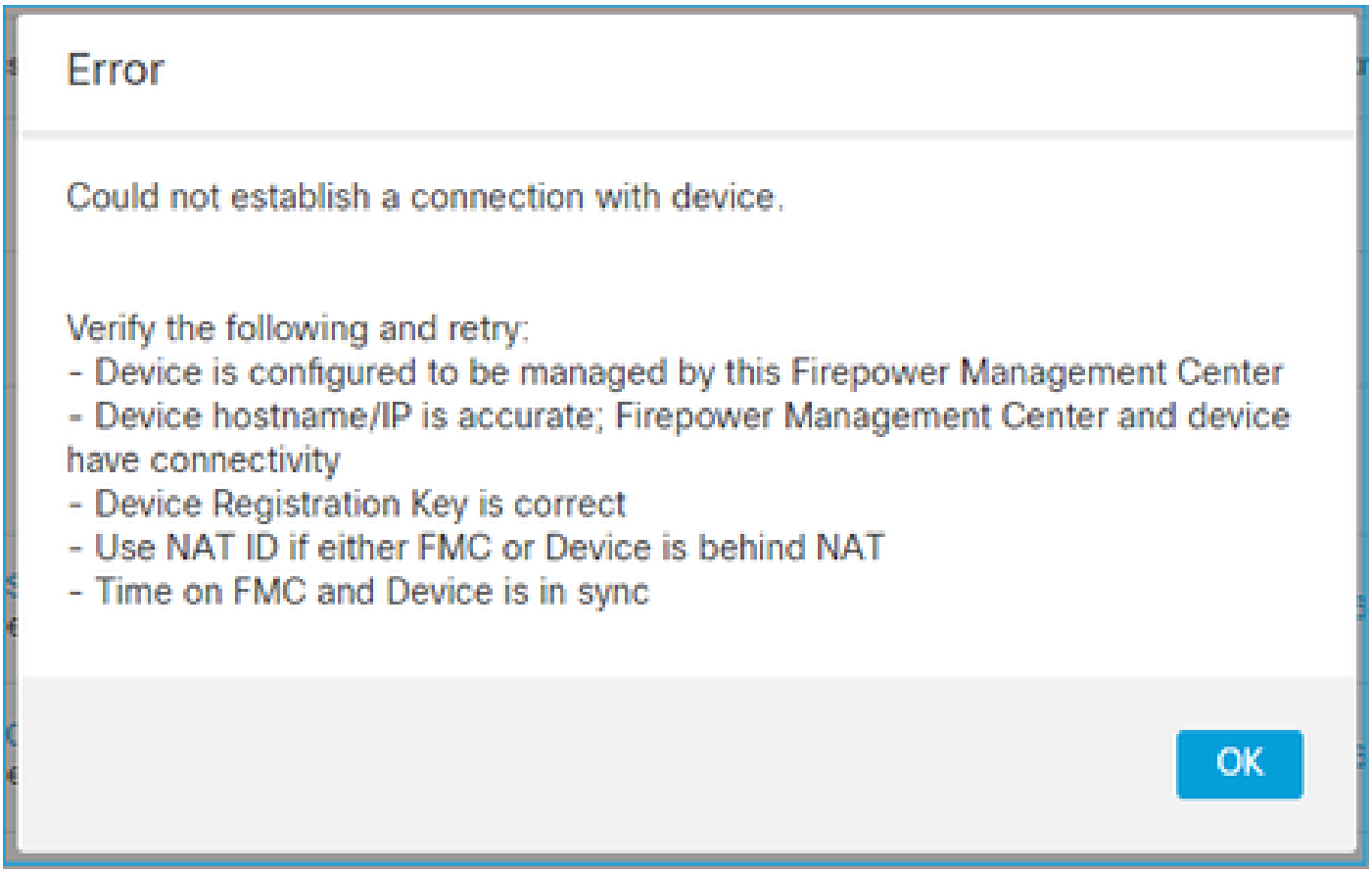
>

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. Registration Key Mismatch Between FTD - FMC

The FMC UI shows:



Recommended Action

On FTD check the /ngfw/var/log/messages file for authentication issues.

Way 1 – Check the past logs

<#root>

>

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 0x9
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 – Check the live logs

```
<#root>
>
expert
ftd1:~$

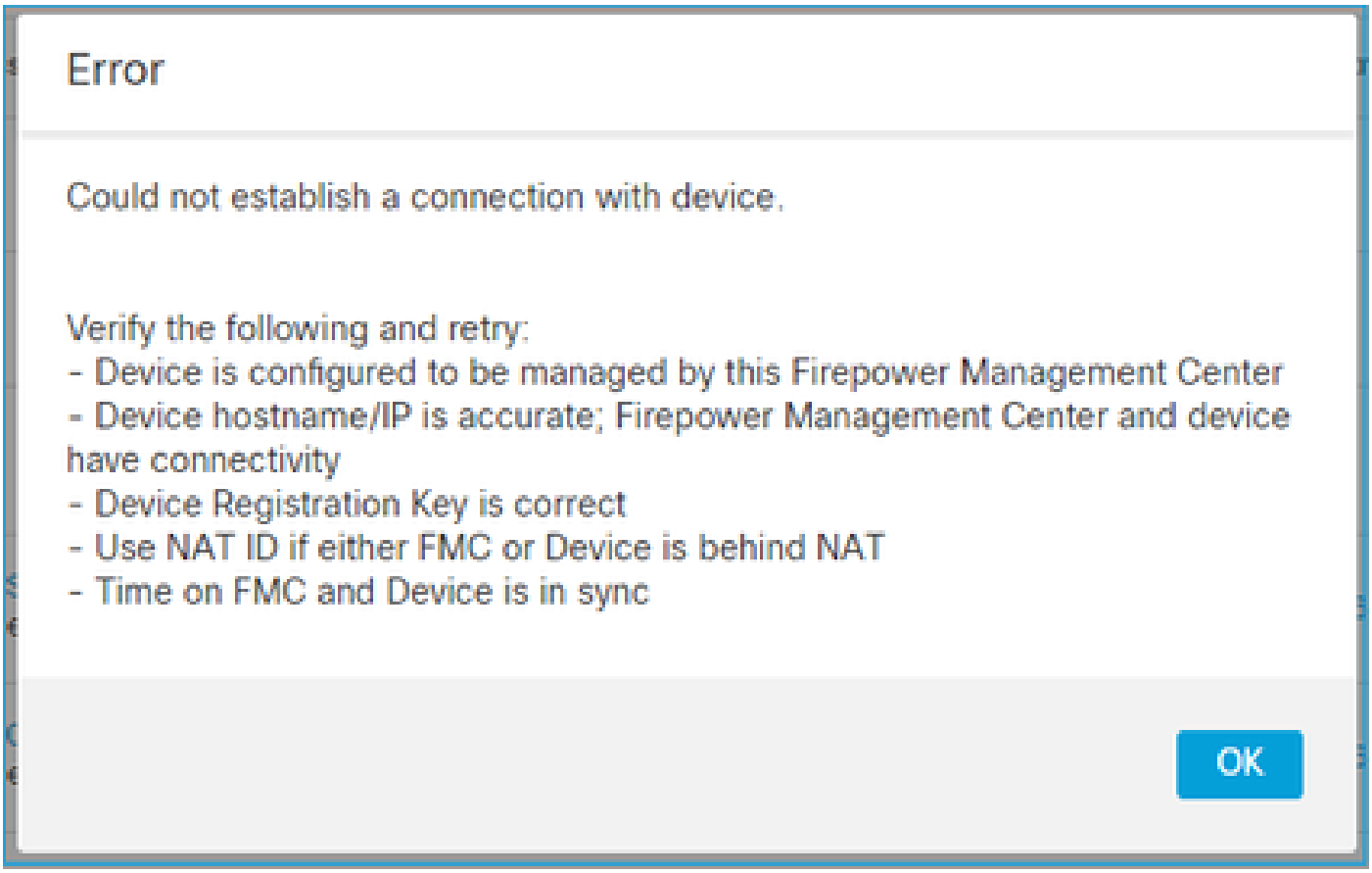
sudo su
Password:
ftd1::/home/admin#
tail -f /ngfw/var/log/messages
```

On FTD check the contents of the /etc/sf/sftunnel.conf file to ensure that the registration key is correct:

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

3. Connectivity Issues Between FTD - FMC

The FMC UI shows:



Recommended Actions

- Ensure there is no device in the path (for example, a firewall) that blocks the traffic (TCP 8305). In the case of FMC HA, ensure that traffic to TCP port 8305 is allowed towards both FMCs.
- Take captures to verify bidirectional communication. On FTD use the **capture-traffic** command. Ensure that there is a TCP 3-way handshake and no TCP FIN or RST packets.

```
<#root>

>

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
```

Similarly, take a capture on FMC to ensure bidirectional communication:

<#root>

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

It is also recommended to export the capture in pcap format and check the packet contents:

<#root>

```
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
```

Possible Causes:

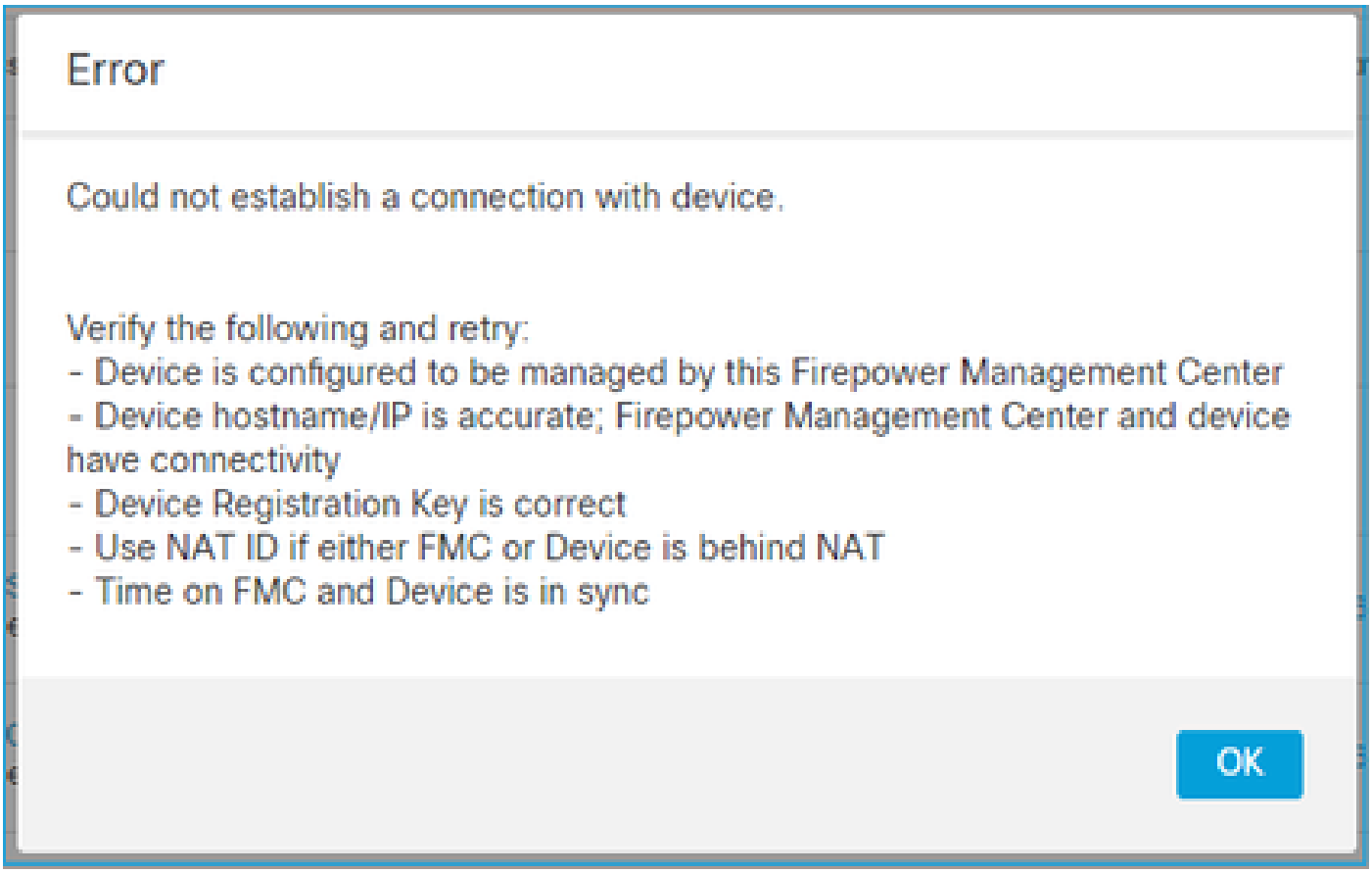
- The FMC does not have the FTD device added.
- A device in the path (for example, firewall) blocks or modifies the traffic.
- The packets are not routed properly in the path.
- The sftunnel process on FTD or FMC is down (check scenario 6)
- There is an MTU issue in the path (check scenario).

For capture analysis check this document:

Analyze Firepower Firewall Captures to Effectively Troubleshoot Network Issues

4. Incompatible SW Between FTD – FMC

The FMC UI shows:



Recommended Action

Check the FTD /ngfw/var/log/messages file:

<#root>

```
Apr 19 22:08:09 mzafeiro_vFTD66 SF-IMS[12730]: [12830] sftunneld:sf_connections [INFO] Need to send SW
Apr 19 22:08:09 mzafeiro_vFTD66 SF-IMS[12730]: [12830] sftunneld:sf_channel [INFO] >> ChannelState do_d
Apr 19 22:08:09 mzafeiro_vFTD66 SF-IMS[12730]: [12830] sftunneld:sf_heartbeat [INFO] Saved SW VERSION f
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] <<<<<<<<<<<<<<<<
Apr 19 22:08:09 mzafeiro_vFTD66 SF-IMS[12730]: [12830] sftunneld:stream_file [INFO] Stream CTX destroye
Apr 19 22:08:09 mzafeiro_vFTD66 SF-IMS[12730]: [12830] sftunneld:sf_channel [INFO] >> ChannelState Shut
```

Check the Firepower Compatibility matrix:

Cisco Firepower Compatibility Guide

5. Time Difference Between FTD and FMC

The FTD-FMC communication is sensitive to time differences between the 2 devices. It is a design

requirement to have FTD and FMC synchronized by the same NTP server.

Specifically, when the FTD is installed on a platform like 41xx or 93xx it takes its time settings from the parent chassis (FXOS).

Recommended Action

Ensure that the chassis manager (FCM) and the FMC use the same time source (NTP server)

6. sftunnel Process Down or Disabled

On FTD the **sftunnel** process handles the registration process. This is the status of the process before the manager configuration:

```
<#root>

>

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
```

The registration status:

```
<#root>

>

show managers

No managers configured.
```

Configure the manager:

<#root>

>

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.

Now the process is UP:

<#root>

>

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)

In some rare cases the process can be down or disabled:

<#root>

>

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
```

The manager status looks normal:

<#root>

>

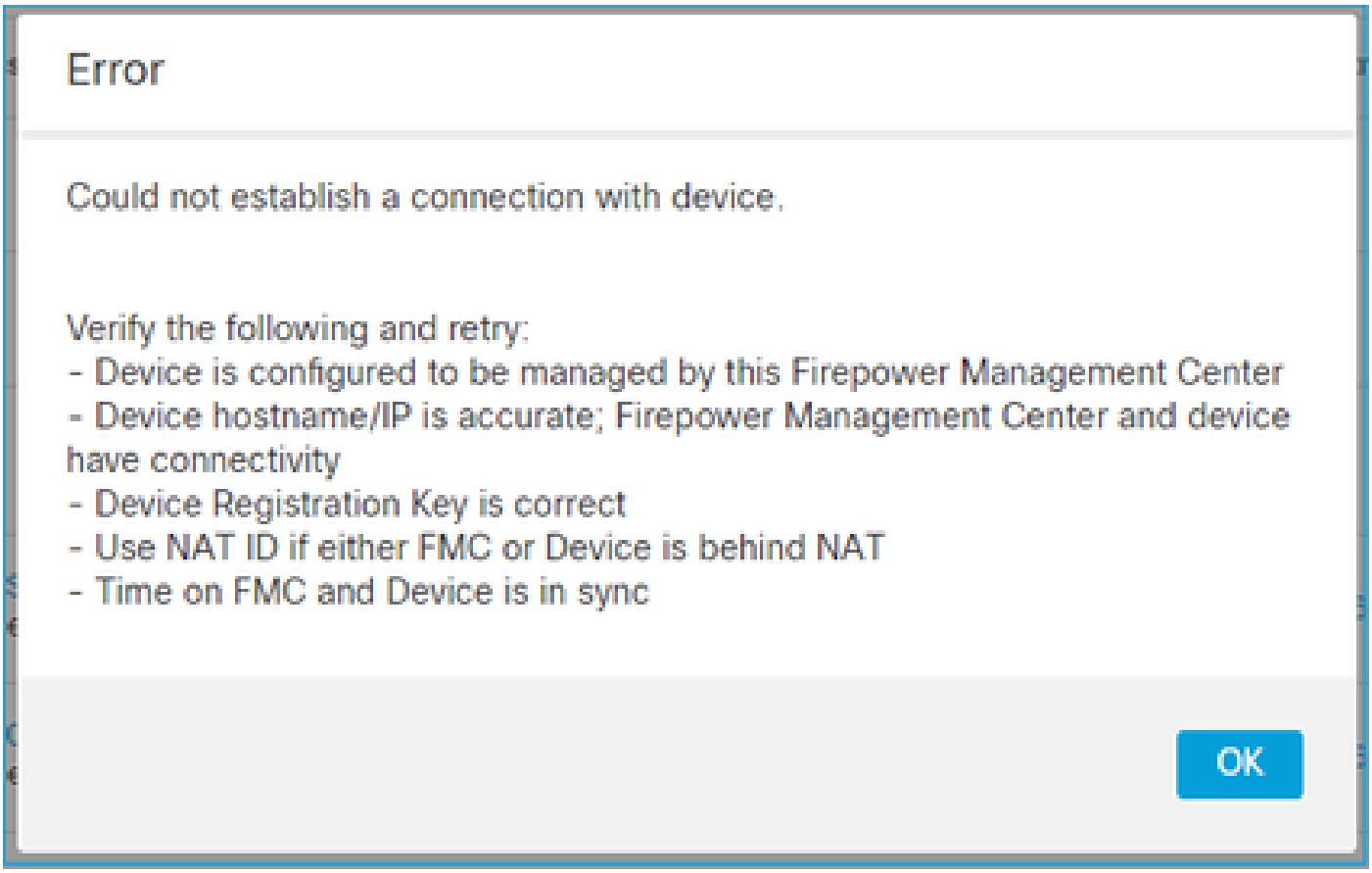
show managers

```
Host                    : 10.62.148.75
Registration Key        : ****
```

Registration **: pending**

```
RPC Status              :
```

On the other hand, the device registration fails:



On FTD there are no related messages seen in **/ngfw/var/log/messages**

Recommended Action

Collect the FTD Troubleshoot File and contact Cisco TAC

7. FTD Pending registration on Secondary FMC

There are scenarios where after the initial FTD registration to an FMC HA setup the FTD device is not added to the Secondary FMC.

Recommended Action

Use the procedure described in this document:

Use CLI to Resolve Device Registration in Firepower Management Center High Availability

---

Warning: This procedure is intrusive since it contains a device unregistration. This affects the FTD device configuration (it is deleted). It is recommended to use this procedure only during the initial FTD registration and setup. In different case collect FTD and FMC Troubleshoot Files and contact Cisco TAC.

---

8. Registration Fails due to Path MTU

There are scenarios seen in Cisco TAC where the sftunnel traffic has to traverse a link that has small MTU. The sftunnel packets have the **Don't fragment** bit **Set** thus fragmentation is not allowed:

	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

Additionally, in the /ngfw/var/log/messages files you can see a message like this:

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

Recommended Action

To verify if there is packet loss due to fragmentation take captures on FTD, FMC, and ideally on devices in the path. Check if you see packets that arrive on both ends.

On FTD lower the MTU on the FTD management interface. The default value is 1500 Bytes. MAX is 1500 for the Management Interface and 9000 for the Eventing Interface. The command was added in FTD 6.6

release.

[Cisco Firepower Threat Defense Command Reference]

Example

```
<#root>

>

configure network mtu 1300

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

Verification

```
<#root>

>

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 ]----------------------
```

To verify the path MTU from the FTD you can use this command:

```
<#root>

root@firepower:/home/admin#
```

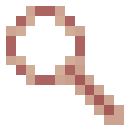
```
ping -M do -s 1472 10.62.148.75
```

The **do** option sets the **don't fragment** bit in the ICMP packets. Additionally, when you specify 1472, the device sends 1500 Bytes: (IP header = 20 Bytes) + (ICMP header = 8 Bytes) + (1472 Bytes ICMP data)

On FMC lower the MTU value on the FMC management interface as described in this document:

Configure Firepower Management Center Management Interfaces

9. FTD Gets Unregistered After a Bootstrap Change From the Chassis Manager UI



This is applicable to FP41xx and FP93xx platforms and documented in Cisco bug ID CSCvn45138
.

In general, you must not do bootstrap changes from the chassis manager (FCM) unless you do a disaster recovery.

Recommended Action

In case you did a bootstrap change and you matched the condition (the FTD-FMC communication is broken while the FTD comes UP after the bootstrap change) you must delete and register again the FTD to FMC.

10. FTD Loses Access to FMC due to ICMP Redirect Messages

This issue can affect the registration process or break FTD-FMC communication after the registration.

The problem in this case is a network device that sends **ICMP Redirect** messages to the FTD management interface and black-holes FTD-FMC communication.

How to identify this problem

In this case, the 10.100.1.1 is the FMC IP address. On FTD there is a cached route due to ICMP redirect message that was received by the FTD on the management interface:

<#root>

```
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 <redirected>
```

Recommended Action

Step 1

Disable the ICMP redirect on the device that sends it (for example, upstream L3 switch, router, and so on).

Step 2

Clear the FTD route cache from the FTD CLI:

<#root>

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

When it is not redirected it looks like this:

<#root>

```
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
```

References

- Understand ICMP Redirect Messages
- Cisco bug ID CSCvm53282 FTD: Routing tables added by ICMP redirects gets stuck in routing table cache forever

Related Information

- NGFW Configuration Guides