配置、验证Firepower设备注册并对其进行故障排除

目录

简介

本文档介绍Firepower威胁防御(FTD)和Firepower管理中心(FMC)之间连接的故障排除过程。

先决条件

要求

本文档没有任何特定的要求。

使用的组件

本文档中的信息基于以下软件和硬件版本：

- FTD软件6.6.x和6.5.x
- FMC软件6.6.x

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

背景信息

本文档介绍托管FTD和托管FMC之间的连接(sftunnel)的操作、验证和故障排除过程。

信息和示例基于FTD，但大多数概念也完全适用于NGIPS（7000/8000系列设备）或ASA55xx上的FirePOWER模块。

FTD支持两种主要管理模式：

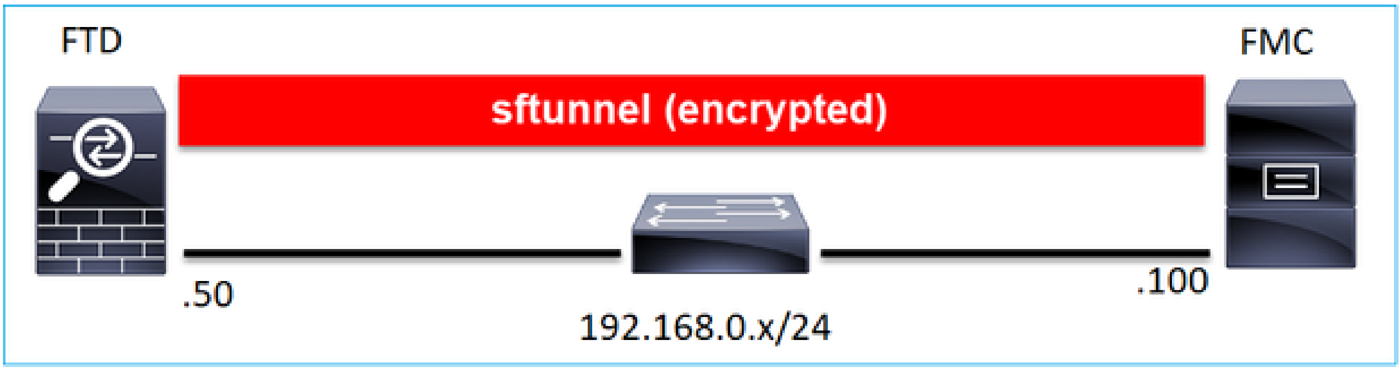
- 通过FMC进行机外 — 也称为远程管理
- 通过Firepower设备管理器(FDM)和/或Cisco Defense Orchestrator(CDO)（也称为本地管理）进行机上部署

在远程管理的情况下，FTD需要首先注册到使用称为设备注册的进程的FMC。

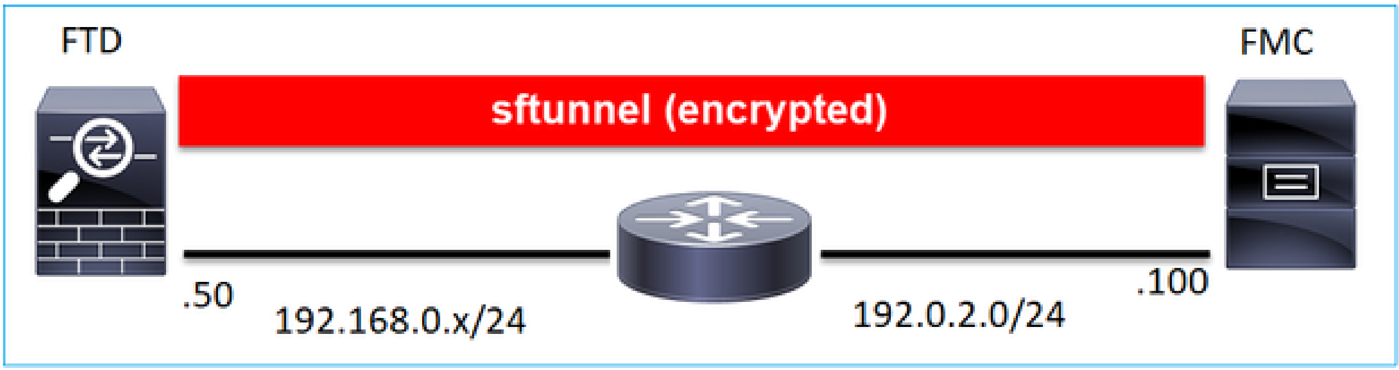
完成注册后，FTD和FMC会建立名为sftunnel（名称源自Sourcefire隧道）的安全隧道。

设计选项

从设计的角度来看，FTD - FMC可以处于同一个L3子网中：

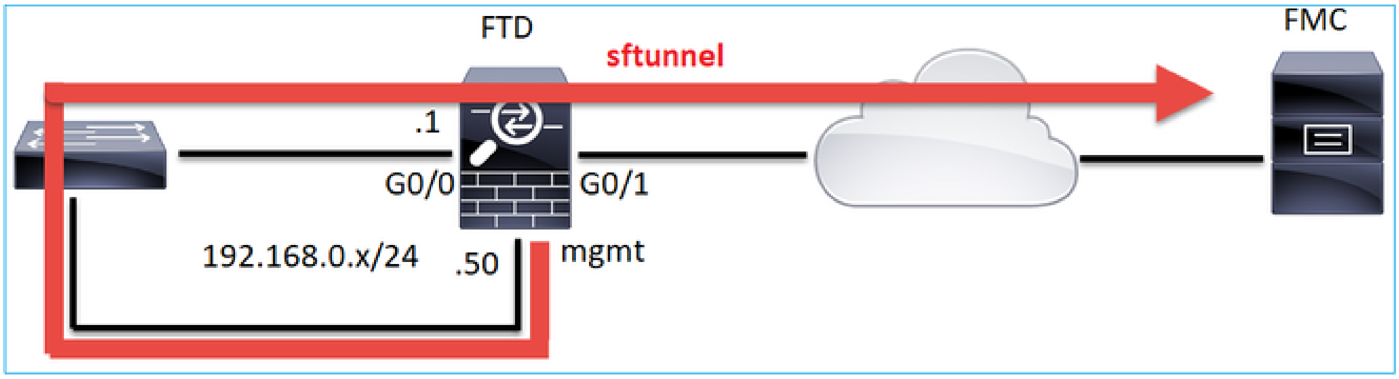


或由不同的网络分隔：



192.0.2.0

注:sftunnel也可以通过FTD本身。不建议使用此设计。原因是FTD数据平面问题可能会中断FTD和FMC之间的通信。



通过sftunnel交换什么信息？

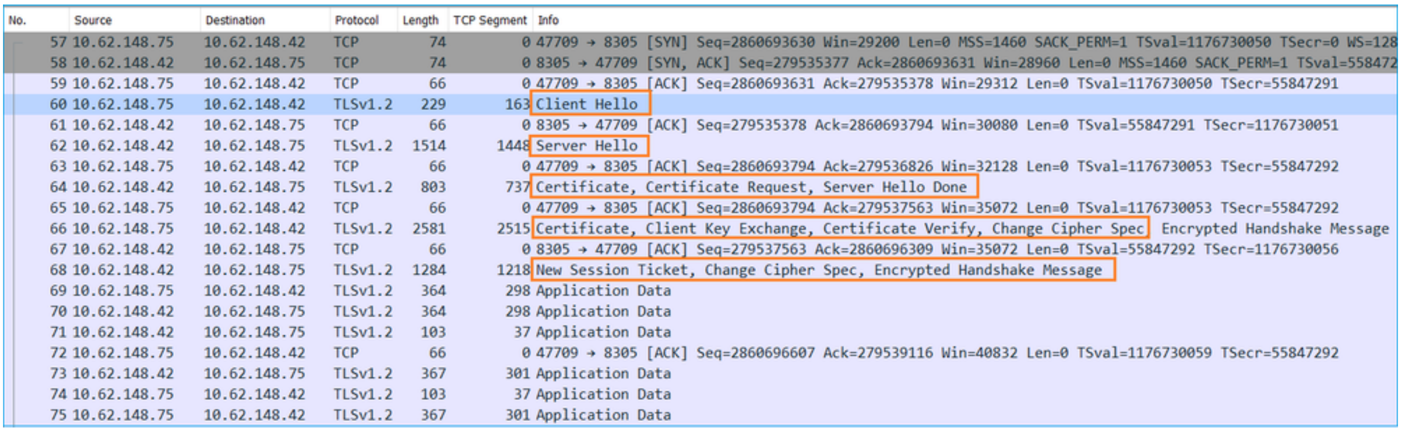
此列表包含通过sftunnel传输的大部分信息：

- 设备心跳(keepalive)
- 时间同步(NTP)
- 事件（连接、入侵/IPS、文件、SSL等）

- 恶意软件查找
- 运行状况事件/警报
- 用户和组信息（用于身份策略）
- FTD高可用性状态信息
- FTD集群状态信息
- 安全智能(SI)信息/事件
- Threat Intelligence Director(TID)信息/事件
- 捕获的文件
- 网络发现事件
- 策略捆绑包（策略部署）
- 软件升级捆绑包
- 软件补丁捆绑包
- VDB
- SRU

sftunnel使用什么协议/端口？

sftunnel使用TCP端口8305。在后端是TLS隧道：



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	10.62.148.75	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

如何更改FTD上的Sftunnel TCP端口？

```
<#root>

>

configure network management-port 8306

Management port changed to 8306.
```

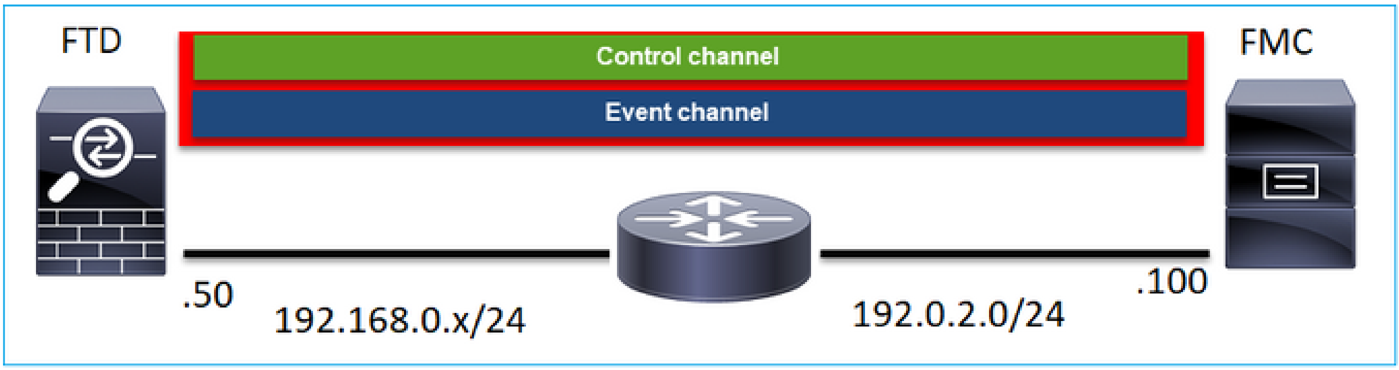
注意：在这种情况下，您还必须更改FMC上的端口(Configuration > Management Interfaces > Shared Settings)。这会影响已注册到同一FMC的所有其他设备。思科强烈建议您保留远程管理端口的默认设置，但如果管理端口与网络上的其他通信冲突，您可以选择其他端口。如果更

改管理端口，则必须为部署中需要相互通信的所有设备更改管理端口。

sftunnel建立了多少个连接？

sftunnel建立2个连接（通道）：

- 控制信道
- 事件通道



哪台设备会启动每个通道？

这取决于具体场景。检查文档其余部分中描述的场景。

配置

注册基础知识

FTD CLI

在FTD上，设备注册的基本语法为：

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

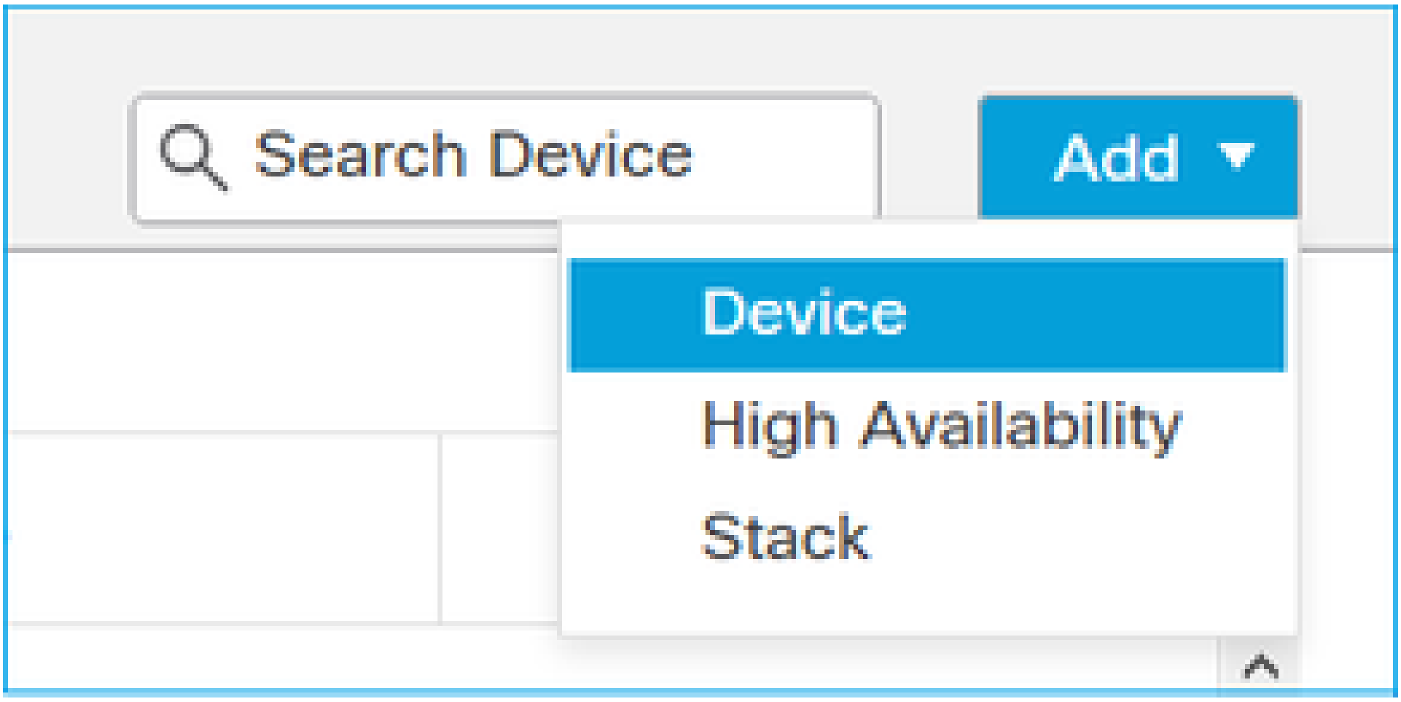
价值	描述
FMC主机	这可以是： • 主机名 • ipv4地址 • ipv6 address • DONTRESOLVE

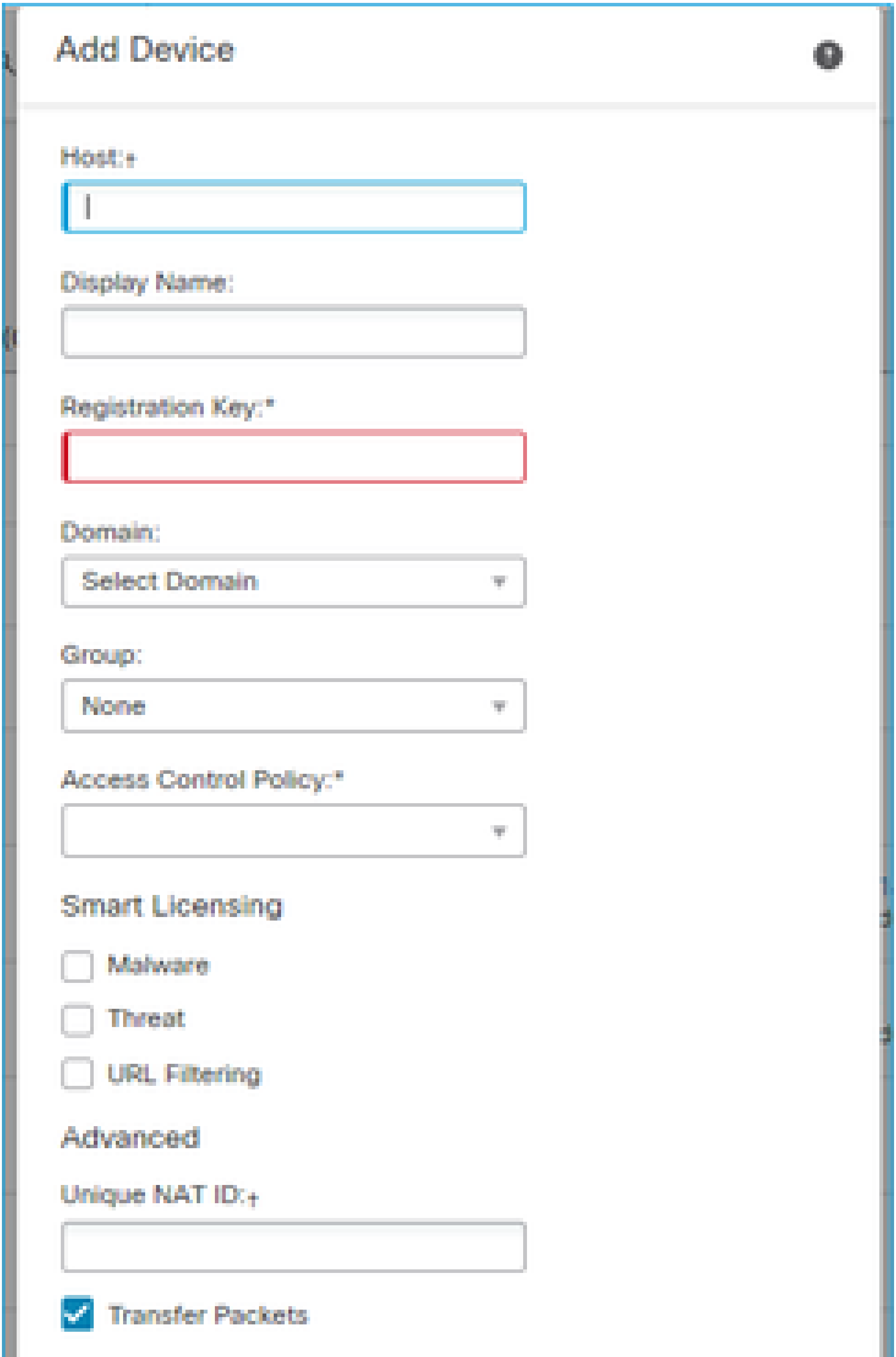
注册密钥	这是用于设备注册的共享密钥字母数字字符串（2到36个字符）。仅允许使用字母数字、连字符(-)、下划线(_)和句点(.)。
NAT ID	当一端未指定IP地址时，在FMC和设备之间的注册过程中使用的字母数字字符串。在FMC上指定相同的NAT ID。

有关其他详细信息，请查看Cisco Firepower威胁防御命令参考

FMC用户界面

在FMC上，导航到Devices > Device Management。选择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:+

☑ Transfer Packets

FTD CLI

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

例如：

```
<#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.
```

背景信息

输入FTD命令后，FTD会每20秒尝试连接到FMC，但由于尚未配置FMC，因此它会回复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
```

设备注册状态：

<#root>

```
>

show managers

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

FTD侦听端口TCP 8305:

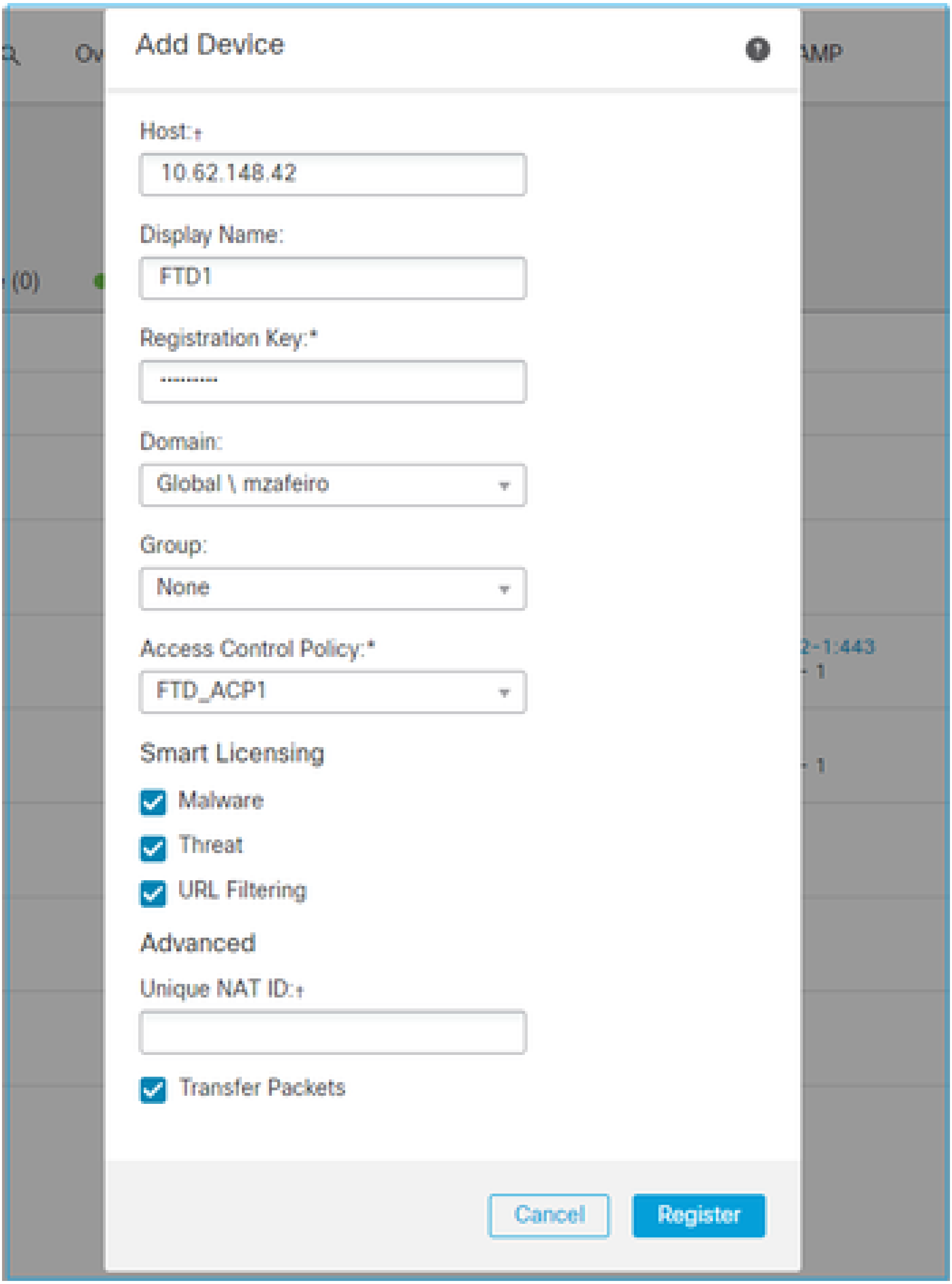
<#root>

```
admin@vFTD66:~$

netstat -na | grep 8305

tcp        0      0 10.62.148.42:

8305

       0.0.0.0:*

LISTEN
```

FMC用户界面

在这种情况下，请指定：

- 主机（FTD的IP地址）
- 显示名称
- 注册密钥（必须与FTD上配置的密钥匹配）
- 访问控制策略
- 域
- 智能许可信息



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

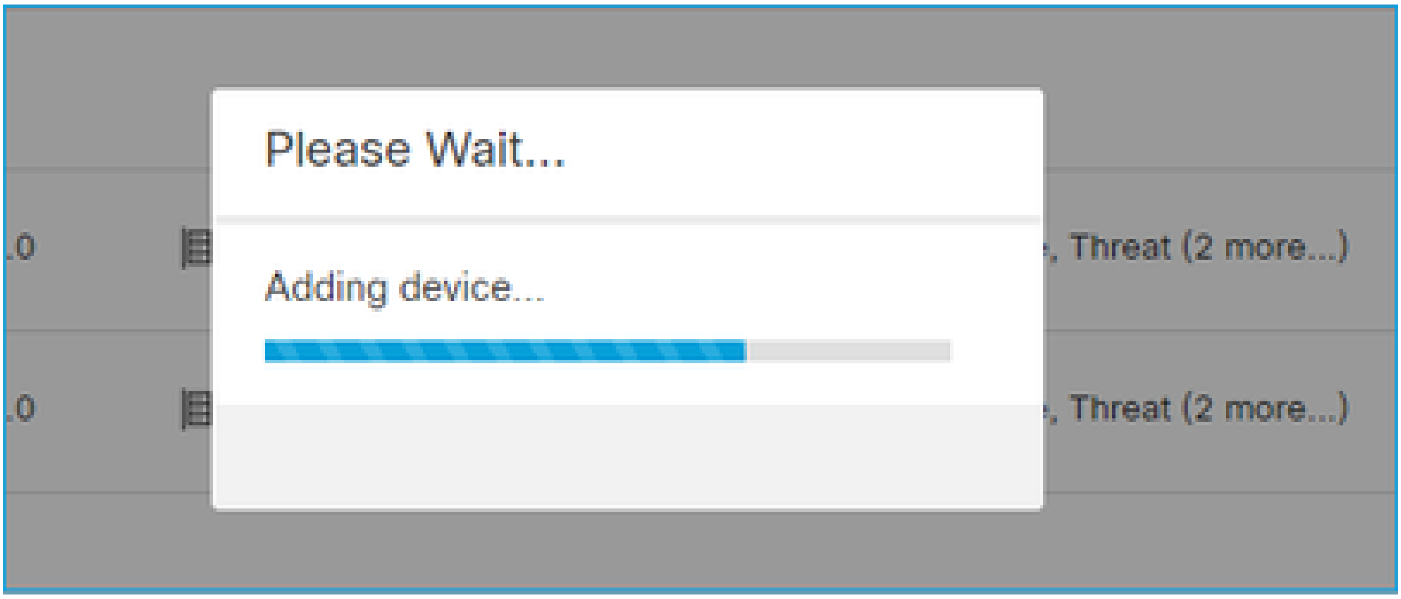
Advanced

Unique NAT ID:+

☑ Transfer Packets

选择Register

注册过程开始：


Please Wait...

Adding device...

FMC开始侦听端口TCP 8305:

<#root>

```
admin@FMC2000-2:~$

netstat -na | grep 8305

tcp        0      0 10.62.148.75:

8305

       0.0.0.0:*

LISTEN
```

FMC在后台启动TCP连接：

<#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,nop
```

已建立sftunnel控制通道：

<#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
```

几分钟后，事件通道建立。事件通道的发起者可以是两端。在本例中，它是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
```

随机源端口表示连接发起方：

<#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
```

如果Event channel由FTD启动，则输出为：

<#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
```

从FTD端：

<#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
```

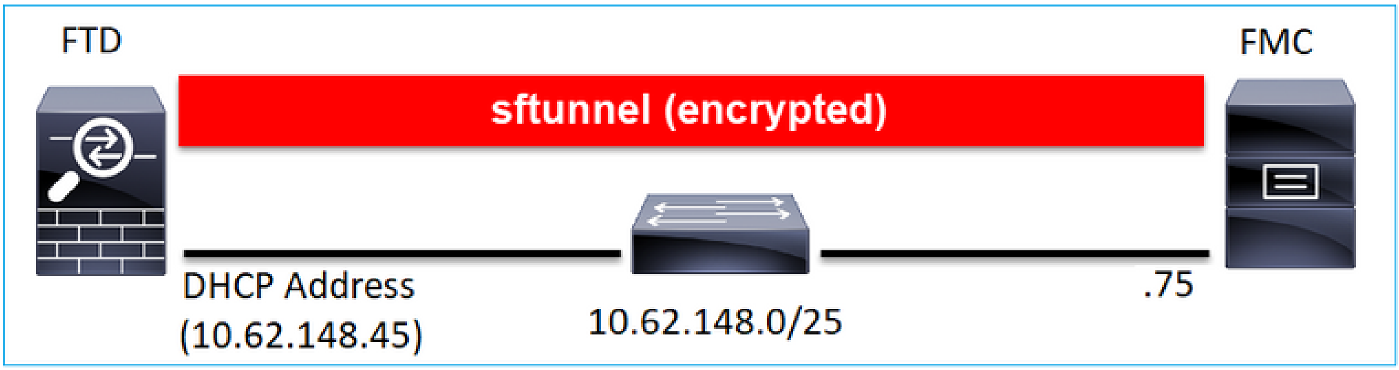
```
PEER INFO:
        sw_version 6.6.0
        sw_build 90
        Management Interfaces: 1
        eth0 (control events) 10.62.148.75,


 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


>
```

场景 2：FTD DHCP IP地址 — FMC静态IP地址

在此场景中，FTD管理接口从DHCP服务器获取其IP地址：



FTD CLI

必须指定NAT ID:

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

例如：

<#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.

>
```

FTD注册状态：

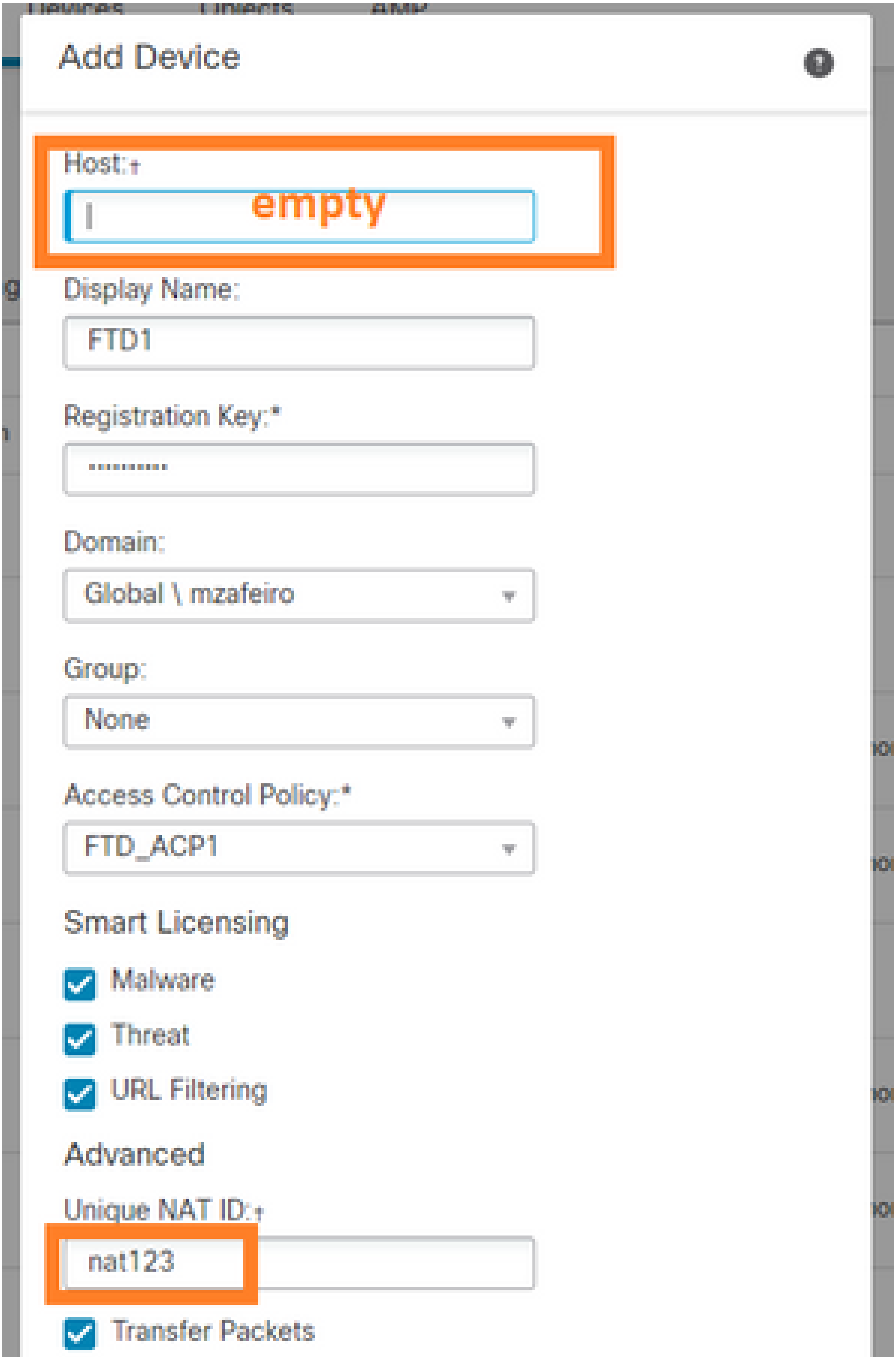
<#root>

```
>

show managers

Host                      : 10.62.148.75
Registration Key          : ****

Registration              : pending

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

FMC用户界面

在这种情况下，请指定：

- 显示名称
- 注册密钥（必须与FTD上配置的密钥匹配）
- 访问控制策略
- 域
- 智能许可信息
- NAT ID(如果未指定Host，则需要此ID。它必须与FTD上配置的相匹配)



Add Device

Host:†

empty

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:† nat123

☑ Transfer Packets

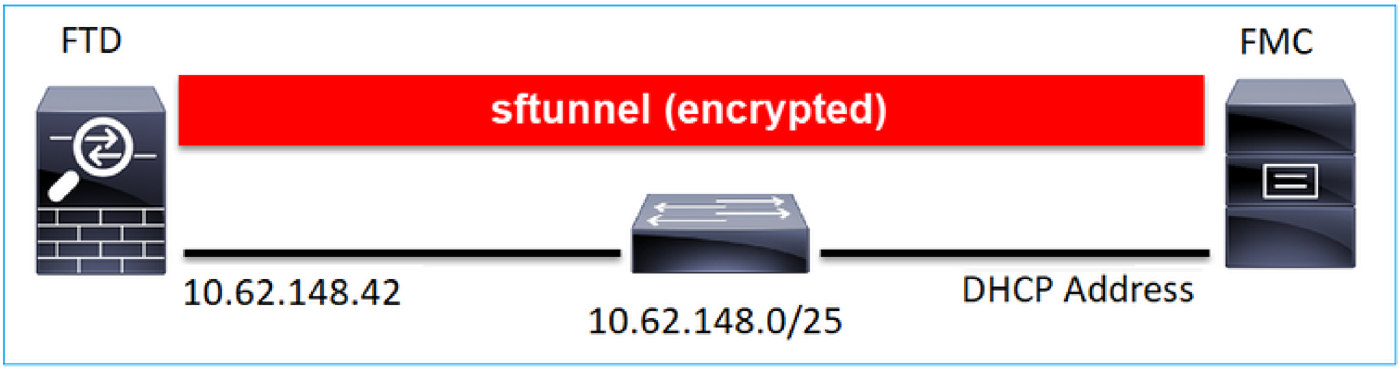
在这种情况下，由谁启动sftunnel?

FTD启动两个通道连接：

<#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
```

场景 3：FTD静态IP地址 — FMC DHCP IP地址



<#root>

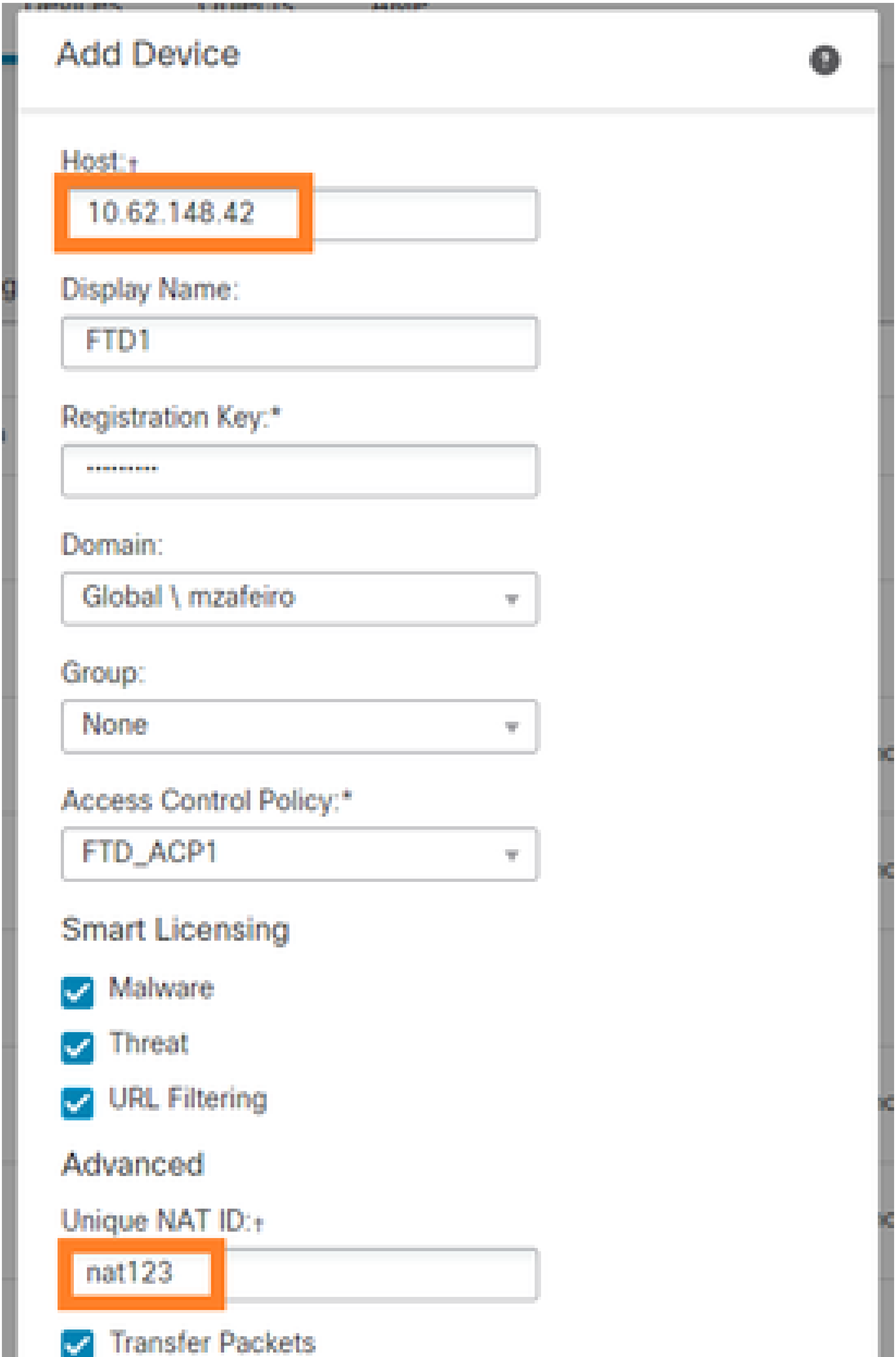
```
>

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.

>
```

注：使用DONTRESOLVE时，需要NAT ID。

FMC用户界面

在这种情况下，请指定：

- FTD IP地址
- 显示名称
- 注册密钥（必须与FTD上配置的密钥匹配）
- 访问控制策略
- 域
- 智能许可信息
- NAT ID（必须与FTD上配置的相同）



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:†

nat123

☑ Transfer Packets

- FMC启动控制信道。
- 事件通道可以由任一端发起。

<#root>

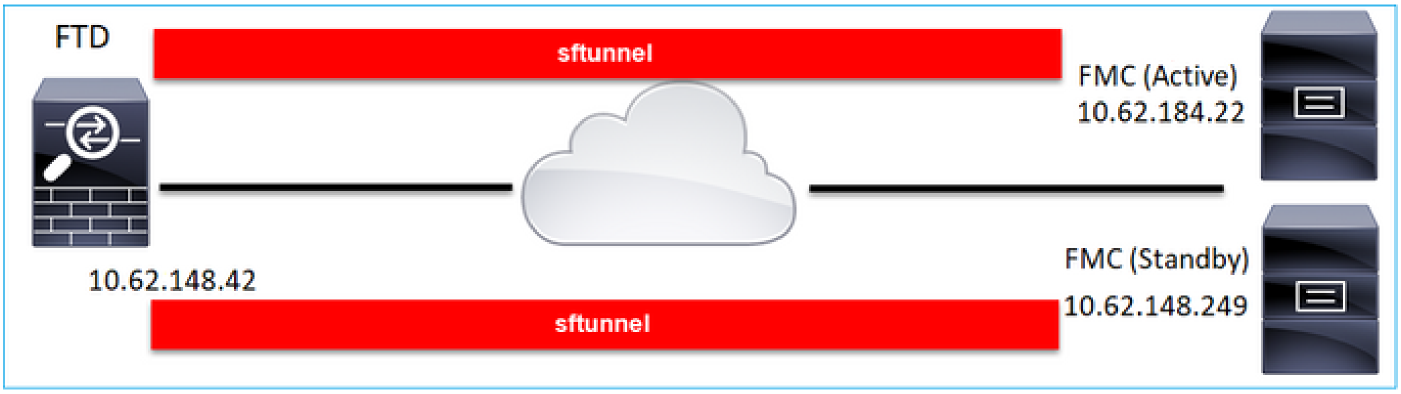
```
root@FMC2000-2:/Volume/home/admin#

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
```

场景 4.FTD注册到FMC高可用性

在FTD上仅配置活动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.
```

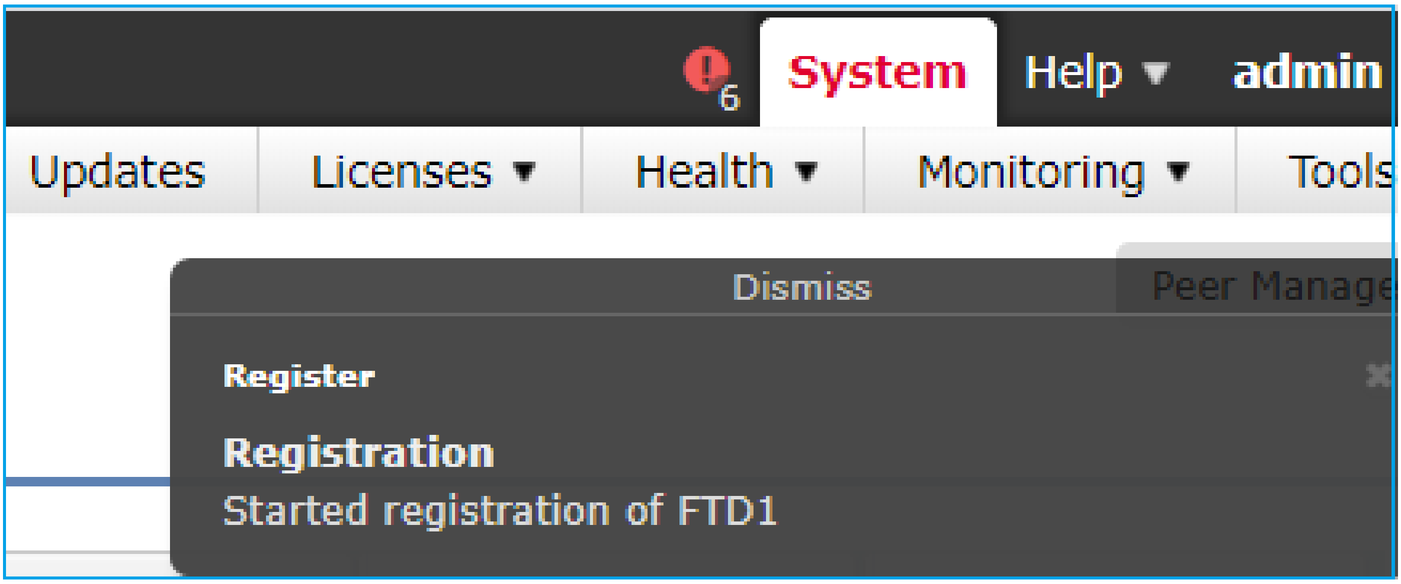


注意：确保允许TCP端口8305流量从FTD传输到两个FMC。

首先，建立到活动FMC的sftunnel:

```
<#root>

>

show managers

Type                      : Manager
Host                      :

10.62.184.22

Registration              : Completed
```

几分钟后，FTD开始注册到备用FMC:



Register

Registration

Started registration of FTD1

```
<#root>

>

show managers

Type                      : Manager
Host                      :

10.62.184.22

Registration              : Completed


Type                      : Manager
```

```
Host                      :
10.62.148.249
Registration              : Completed
```

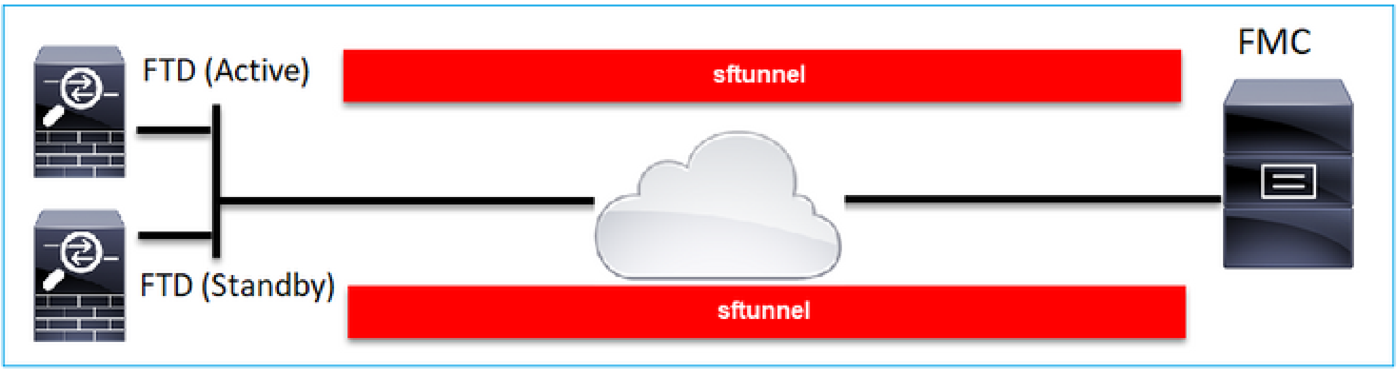
在FTD后端中，建立了2个控制通道（每个FMC一个）和2个事件通道（每个FMC一个）：

<#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
```

方案 5.FTD高可用性

对于FTD HA，每台设备都有到FMC的独立隧道：

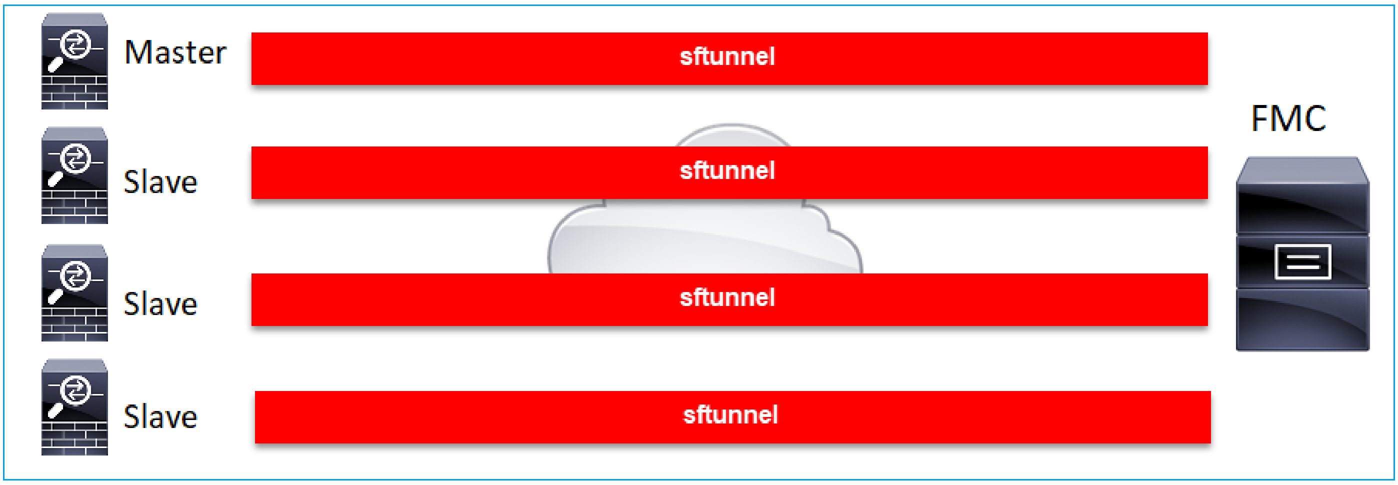


您独立注册两个FTD，然后从FMC形成FTD HA。有关更多详细信息，请查看：

- 在 Firepower 设备上配置 FTD 高可用性
- Firepower威胁防御的高可用性

方案 6.FTD集群

对于FTD集群，每台设备都有到FMC的独立隧道。从6.3 FMC版本开始，您只需将FTD控制单元注册到FMC。然后，FMC处理其余单元并自动发现+注册它们。

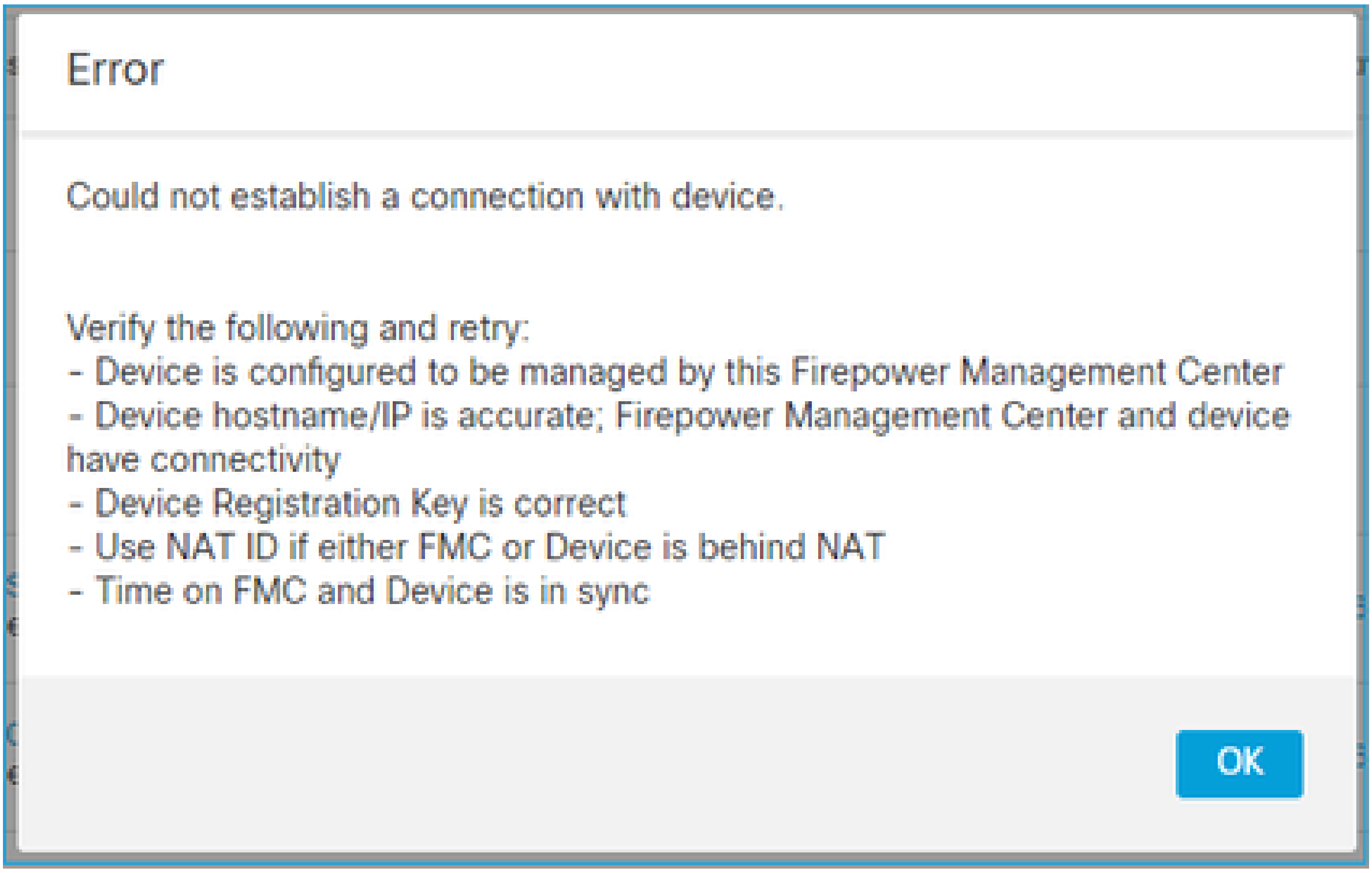


注意：我们建议添加控制单元以获得最佳性能，但您可以添加集群的任何单元。有关其他详细信息，请检查：创建Firepower威胁防御集群

排除常见问题

1. FTD CLI上的语法无效

如果FTD上的语法无效，并且注册尝试失败，则FMC UI会显示非常一般的错误消息：



Error

Could not establish a connection with device.

Verify the following and retry:
- Device is configured to be managed by this Firepower Management Center
- Device hostname/IP is accurate; Firepower Management Center and device have connectivity
- Device Registration Key is correct
- Use NAT ID if either FMC or Device is behind NAT
- Time on FMC and Device is in sync

在此命令中，关键字key是注册密钥，而cisco123是NAT ID。在技术上不存在关键字时，添加关键字键的情况很常见：

<#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.
```

建议操作

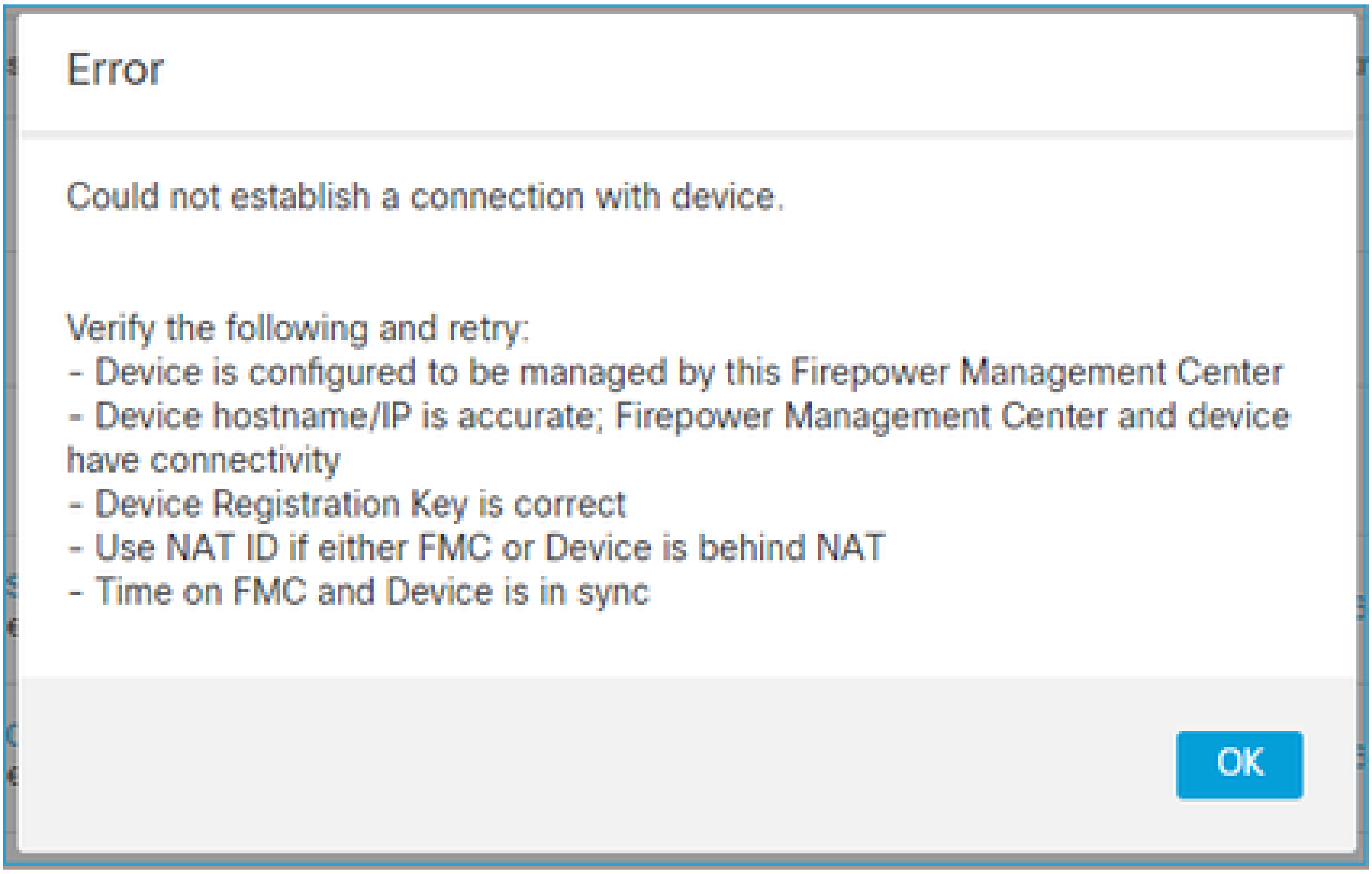
使用正确的语法，不要使用不存在的关键字。

<#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. FTD - FMC之间的注册密钥不匹配

FMC UI显示：



Error

Could not establish a connection with device.

Verify the following and retry:
- Device is configured to be managed by this Firepower Management Center
- Device hostname/IP is accurate; Firepower Management Center and device have connectivity
- Device Registration Key is correct
- Use NAT ID if either FMC or Device is behind NAT
- Time on FMC and Device is in sync

建议操作

在FTD上，检查/ngfw/var/log/messages文件是否存在身份验证问题。

方法1 — 检查过去的日志

<#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
```

方法2 — 检查实时日志

<#root>

```
>

expert
ftd1:~$


sudo su

Password:
ftd1::/home/admin#

tail -f /ngfw/var/log/messages
```

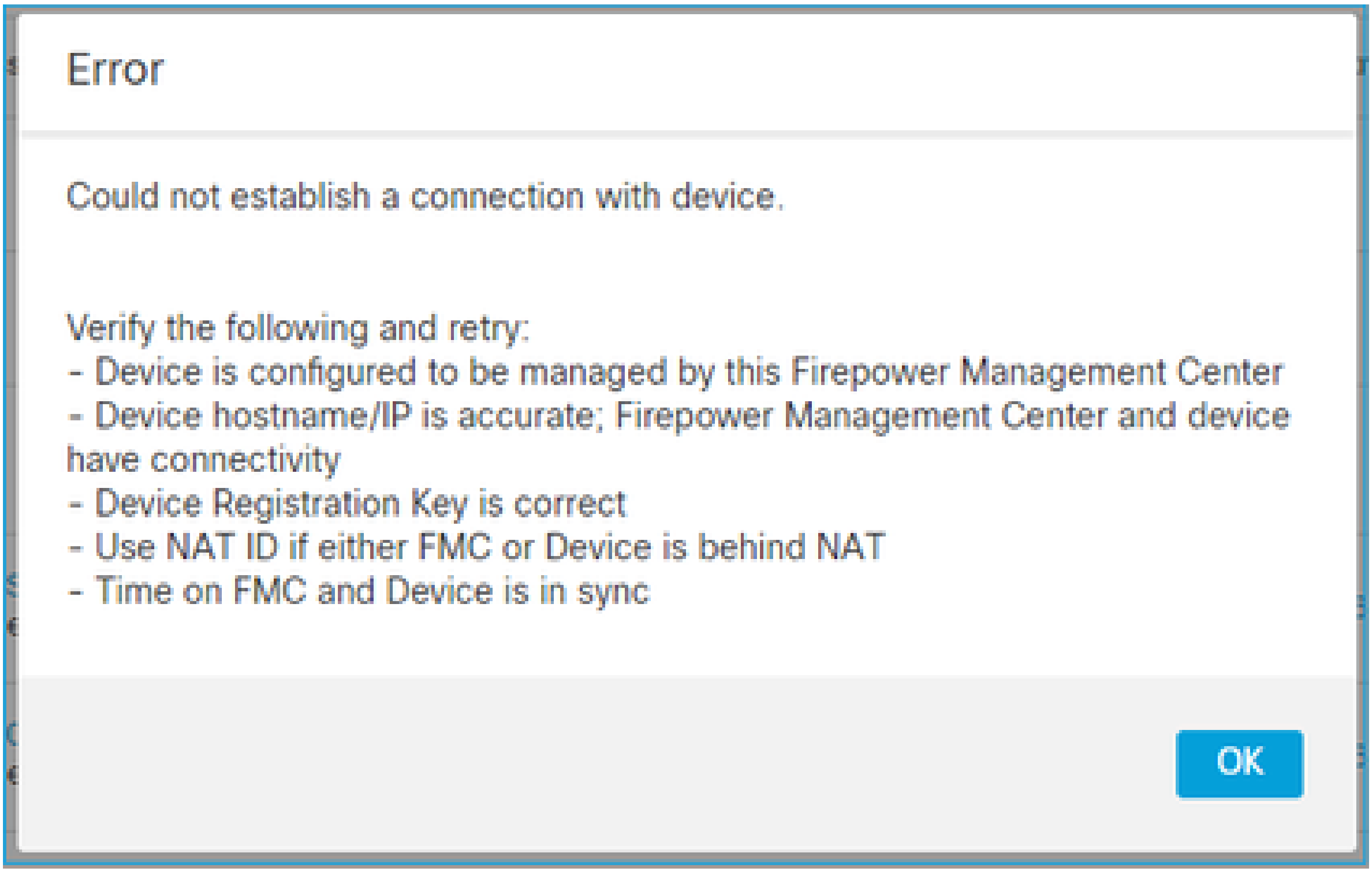
在FTD上，检查/etc/sf/sftunnel.conf文件的内容，以确保注册密钥正确：

<#root>

```
ftd1:~$

cat /etc/sf/sftunnel.conf | grep reg_key

        reg_key

cisco-123

;
```

3. FTD - FMC之间的连接问题

FMC UI显示：



Error

Could not establish a connection with device.

Verify the following and retry:
- Device is configured to be managed by this Firepower Management Center
- Device hostname/IP is accurate; Firepower Management Center and device have connectivity
- Device Registration Key is correct
- Use NAT ID if either FMC or Device is behind NAT
- Time on FMC and Device is in sync

推荐的操作

- 确保路径中没有阻止流量的设备（例如防火墙）(TCP 8305)。对于FMC HA，请确保允许到TCP端口8305的流量流向两个FMC。
- 捕获数据以检验双向通信。在FTD上，使用capture-traffic命令。确保存在TCP三次握手，且没有TCP FIN或RST数据包。

<#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
```

同样，在FMC上进行捕获以确保双向通信：

<#root>

```
root@FMC2000-2:/var/common#

tcpdump -i eth0 host 10.62.148.42 -n -w sftunnel.pcap
```

还建议以pcap格式导出捕获并检查数据包内容：

<#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
```

可能的原因:

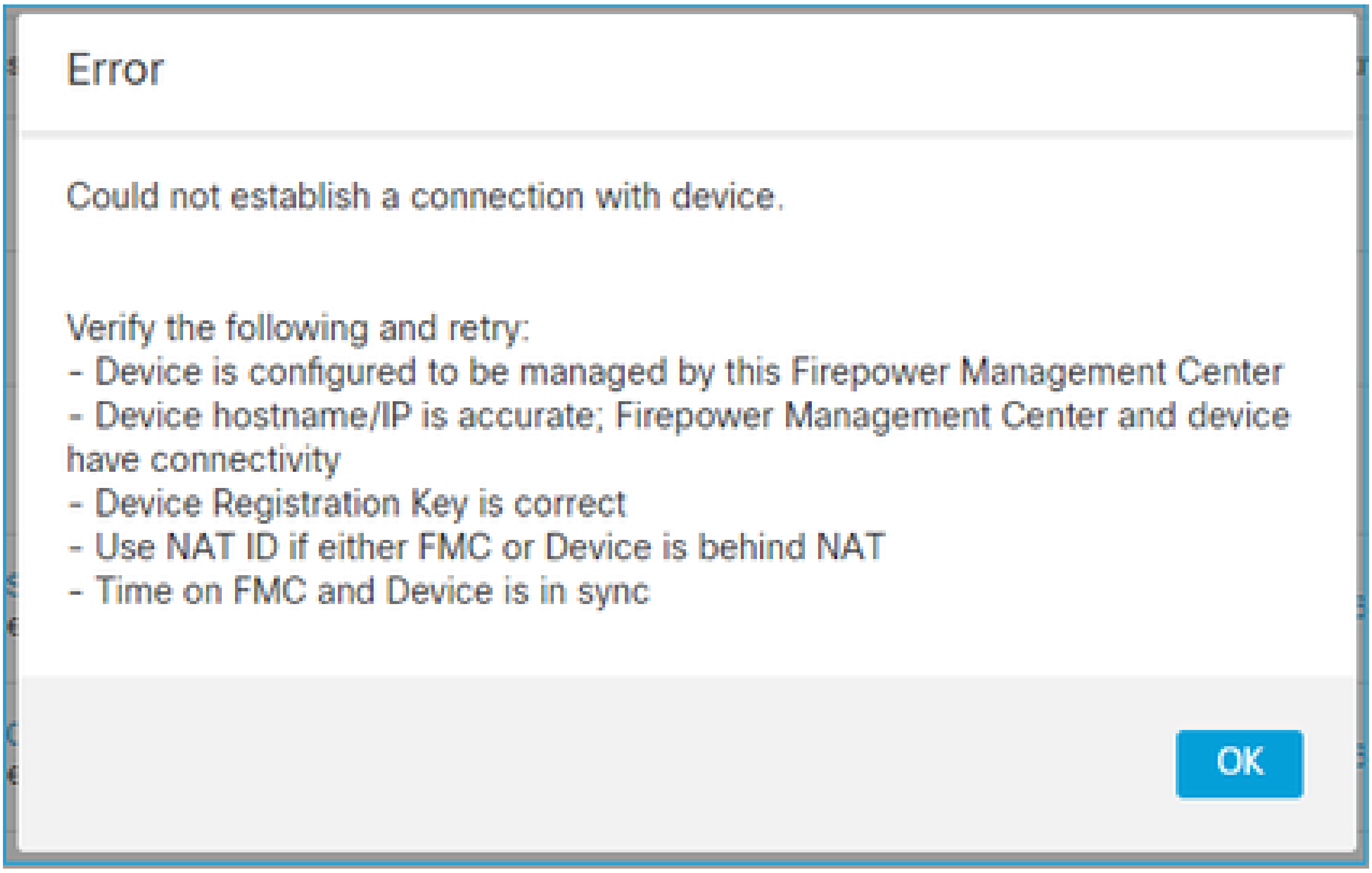
- FMC未添加FTD设备。
- 路径中的设备（例如防火墙）会阻止或修改流量。
- 数据包在路径中没有正确路由。
- FTD或FMC上的sftunnel进程已关闭（检查场景6）
- 路径中存在MTU问题（检查场景）。

对于捕获分析，请检查此文档：

分析 Firepower 防火墙捕获以有效排除网络问题

4. FTD - FMC之间的软件不兼容

FMC UI显示：



Error

Could not establish a connection with device.

Verify the following and retry:
- Device is configured to be managed by this Firepower Management Center
- Device hostname/IP is accurate; Firepower Management Center and device have connectivity
- Device Registration Key is correct
- Use NAT ID if either FMC or Device is behind NAT
- Time on FMC and Device is in sync

建议操作

检查FTD /ngfw/var/log/messages文件：

<#root>

```
Apr 19 22:08:09 mzafeiro_vFTD66 SF-IMS[12730]: [12830] sftunneld:sf_connections [INFO] Need to send SW v
Apr 19 22:08:09 mzafeiro_vFTD66 SF-IMS[12730]: [12830] sftunneld:sf_channel [INFO] >> ChannelState do_da
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
```

检查Firepower兼容性矩阵：

[Cisco Firepower兼容性指南]

5. FTD和FMC之间的时间差

FTD-FMC通信对两台设备之间的时间差非常敏感。FTD和FMC由同一NTP服务器同步是一项设计要求。

具体来说，当FTD安装在41xx或93xx等平台时，它从父机箱(FXOS)获取时间设置。

建议操作

确保机箱管理器(FCM)和FMC使用相同的时间源（NTP服务器）

6. sftunnel进程关闭或禁用

在FTD上，sftunnel进程处理注册过程。这是管理员配置前的流程状态：

<#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
```

注册状态：

<#root>

```
>

show managers
```

```
No managers configured.
```

配置管理器：

```
<#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.
```

现在该过程已启动：

```
<#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)
```

在某些情况下，进程可能会关闭或禁用：

```
<#root>

>

pmtool status
…
sftunnel

 (system) -
```

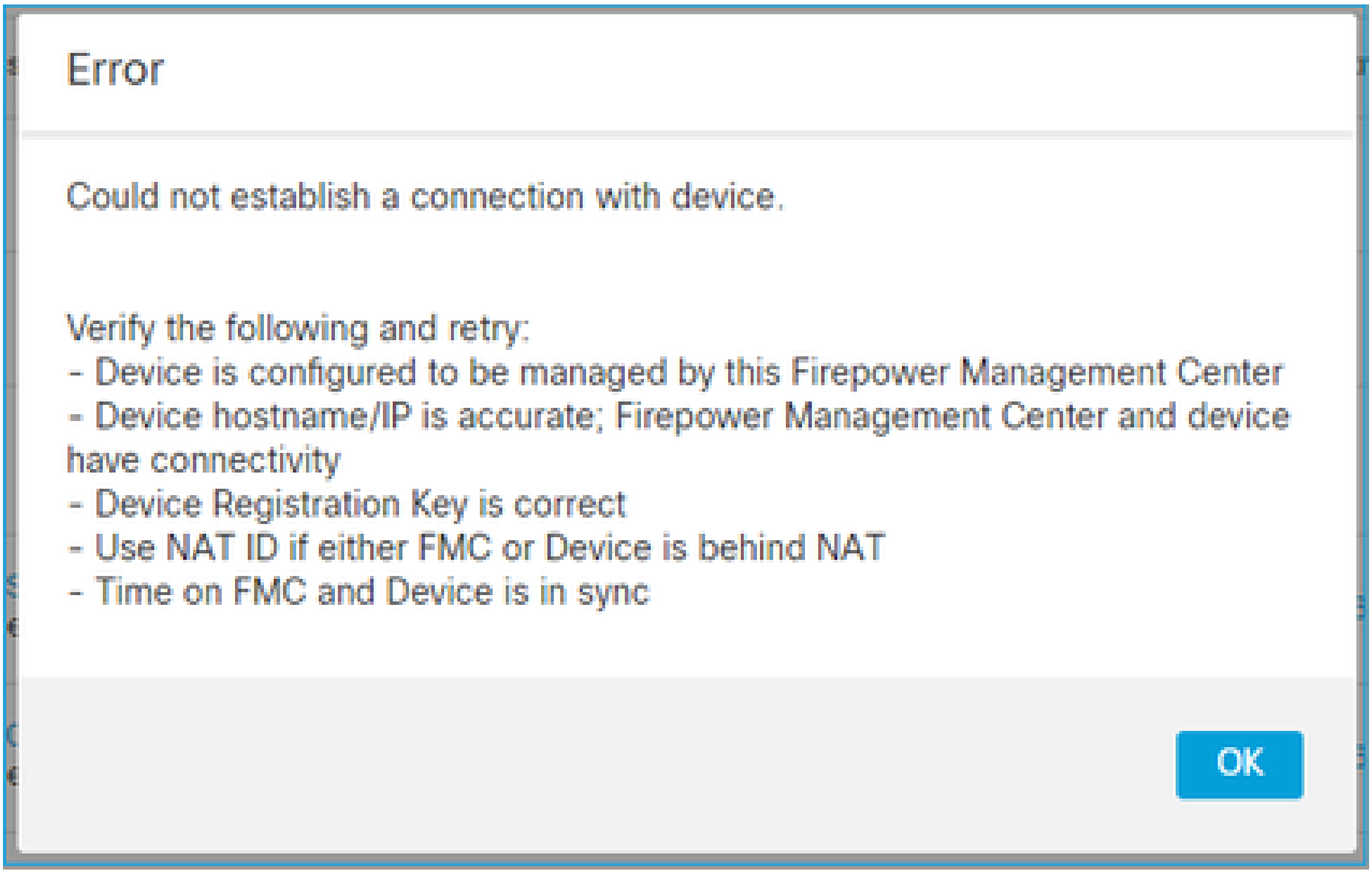
```
User Disabled

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
```

管理器状态看起来正常：

<#root>

```
>

show managers

Host                          : 10.62.148.75
Registration Key              : ****

Registration                  : pending

RPC Status                    :
```

另一方面，设备注册失败：



Error

Could not establish a connection with device.

Verify the following and retry:
- Device is configured to be managed by this Firepower Management Center
- Device hostname/IP is accurate; Firepower Management Center and device have connectivity
- Device Registration Key is correct
- Use NAT ID if either FMC or Device is behind NAT
- Time on FMC and Device is in sync

在FTD上，/ngfw/var/log/messages中未显示相关消息

建议操作

收集FTD故障排除文件并联系思科TAC

7. FTD等待在辅助FMC上注册

在某些情况下，初始FTD注册到FMC HA设置后，FTD设备不会添加到辅助FMC。

建议操作

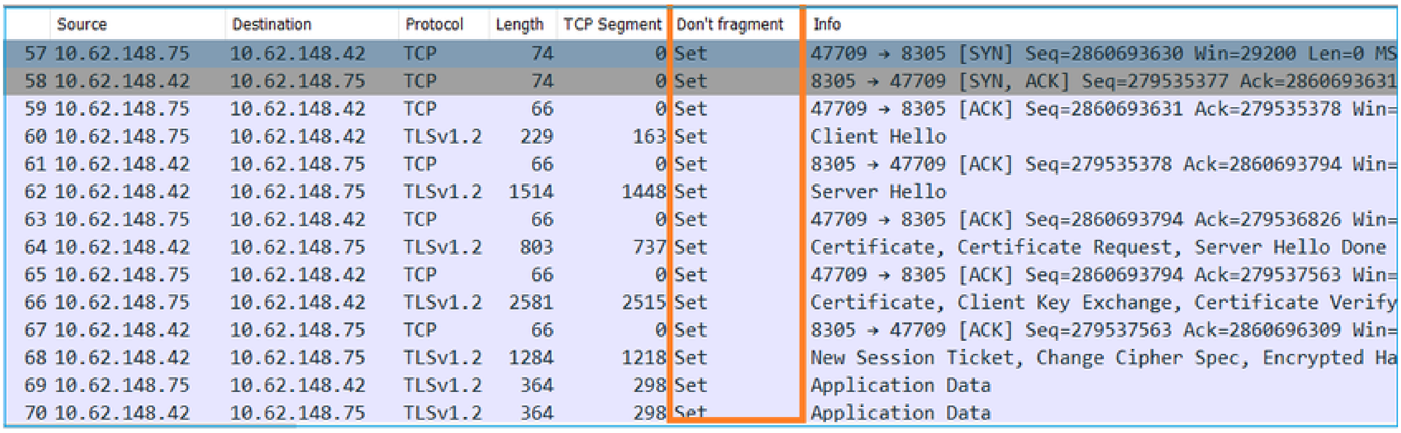
使用本文档中介绍的步骤：

使用CLI解决Firepower管理中心高可用性中的设备注册

⚠ 警告：此过程具有侵入性，因为它包含设备取消注册。这会影响FTD设备配置（它将被删除）。建议仅在初始FTD注册和设置期间使用此过程。在不同情况下，收集FTD和FMC故障排除文件并联系思科TAC。

8.由于路径MTU，注册失败

在Cisco TAC中可以看到，sftunnel流量必须经过具有小MTU的链路的情况。sftunnel数据包具有Don't fragment bit Set，因此不允许分段：



	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

此外，在/ngfw/var/log/messages文件中，您可以看到如下消息：

MSGS: 10-09 14:41:11 ftd1 SF-IMS[7428]: [6612] sftunneld:sf_ssl [ERROR] Connect:SSL握手失败

建议操作

要验证是否由于分段而丢失数据包，请捕获FTD、FMC上的数据包，最好捕获路径中的设备。检查是否看到两端都到达的数据包。

在FTD上，降低FTD管理接口上的MTU。默认值为 1500 字节。管理接口的最大值为1500，事件接口的最大值为9000。该命令在FTD 6.6版本中添加。

[Cisco Firepower威胁防御命令参考](#)

示例

<#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'
```

确认

<#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 ]----------------------
```

要从FTD验证路径MTU，您可以使用以下命令：

```
<#root>
root@firepower:/home/admin#
ping -M do -s 1472 10.62.148.75
```

do选项设置ICMP数据包中的don’t fragment位。此外，当您指定1472时，设备发送1500字节：（IP报头= 20字节）+（ICMP报头= 8字节）+（1472字节ICMP数据）

在FMC上，按本文档所述降低FMC管理接口上的MTU值：

配置Firepower管理中心管理接口

9. FTD在机箱管理器UI中的引导程序更改后注销

这适用于FP41xx和FP93xx平台，记录在Cisco Bug ID CSCvn45138中
.

一般来说，除非执行灾难恢复，否则不能从机箱管理器(FCM)进行引导程序更改。

建议操作

如果执行了引导程序更改并且匹配了条件（FTD-FMC通信中断，而FTD在引导程序更改后启动），则必须删除并重新向FMC注册FTD。

10. FTD由于ICMP重定向消息而失去对FMC的访问权限

此问题可能影响注册过程或在注册后中断FTD-FMC通信。

在这种情况下，问题在于网络设备会将ICMP重定向消息发送到FTD管理接口和黑洞FTD-FMC通信。

如何确定此问题

在本例中，10.100.1.1是FMC IP地址。在FTD上，由于FTD在管理接口上收到的ICMP重定向消息，存在缓存路由：

```
<#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
```

建议操作

第 1 步

在发送它的设备（例如，上游L3交换机、路由器等）上禁用ICMP重定向。

步骤 2

从FTD CLI清除FTD路由缓存：

```
<#root>

ftd1:/ngfw/var/common#

ip route flush 10.100.1.1
```

如果未重定向，则如下所示：

<#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
```

参考

- 了解ICMP重定向消息
- Cisco Bug ID CSCvm53282 FTD：由ICMP重定向添加的路由表将永远滞留在路由表缓存中

相关信息

- NGFW配置指南

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。