Firepowerデバイス登録の設定、確認、トラブルシューティング

内容

概要

このドキュメントでは、マネージドFirepower Threat Defense(FTD)とマネージドFirepower Management Center(FMC)間の接続(sftunnel)の操作、検証、およびトラブルシューティングの手順について説明します。 情報と例はFTDに基づいていますが、概念のほとんどはNGIPS（7000/8000シリーズアプライアンス）またはASA55xx上のFirePOWERモジュールにも完全に適用できます。

前提条件

要件

このドキュメントに特有の要件はありません。

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づいています。

- FTDソフトウェア6.6.xおよび6.5.x
- FMCソフトウェア6.6.x

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、初期（デフォルト）設定の状態から起動しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

背景説明

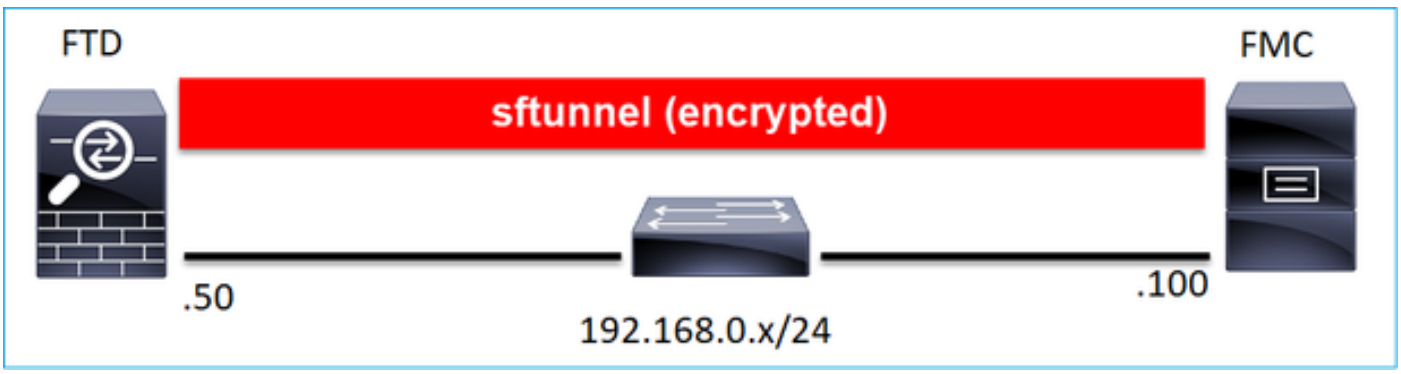
FTDは、次の2つの主要な管理モードをサポートしています。

- FMC経由のオフボックス：リモート管理とも呼ばれる
- Firepower Device Manager(FDM)またはCisco Defense Orchestrator(CDO)（ローカル管理とも呼ばれる）を介したオンボックス

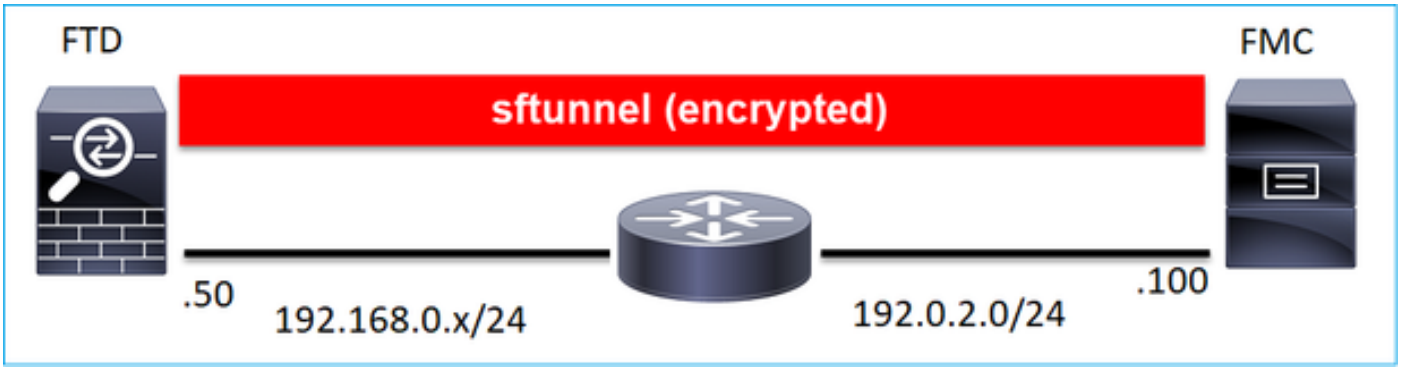
リモート管理の場合、FTDはまず、デバイス登録と呼ばれるプロセスを使用するFMCに登録する必要があります。登録が完了すると、FTDとFMCはsftunnelというセキュアなトンネルを確立します（この名前はSourcefireトンネルに由来します）。

設計オプション

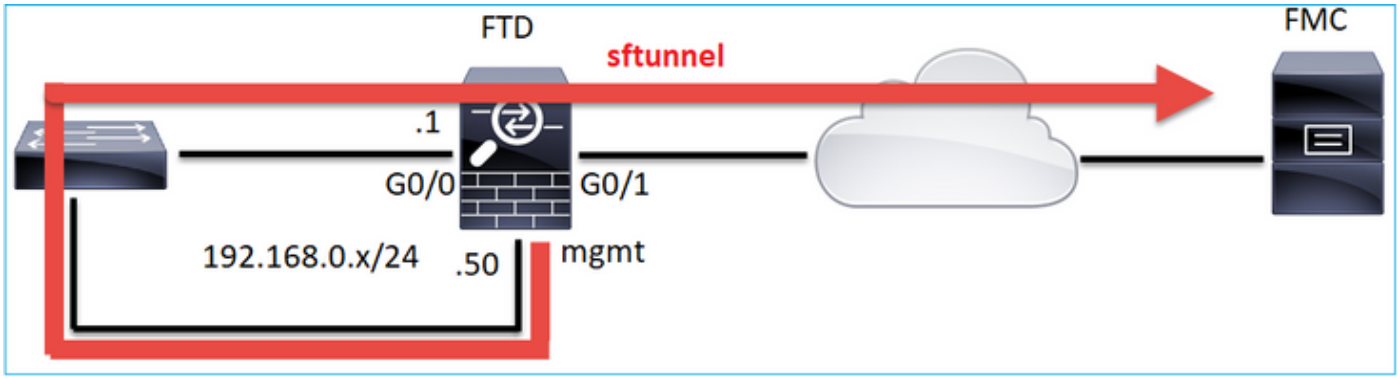
設計の観点からは、FTD - FMCは同じL3サブネットに存在できます。



または異なるネットワークによって分離されます。



注：sftunnelはFTD自体を通過することもできます。この設計は推奨**されません**。その理由は、FTDデータプレーンの問題により、FTDとFMC間の通信が中断される可能性があるためです。



sftunnelを介してどのような情報が交換されるか

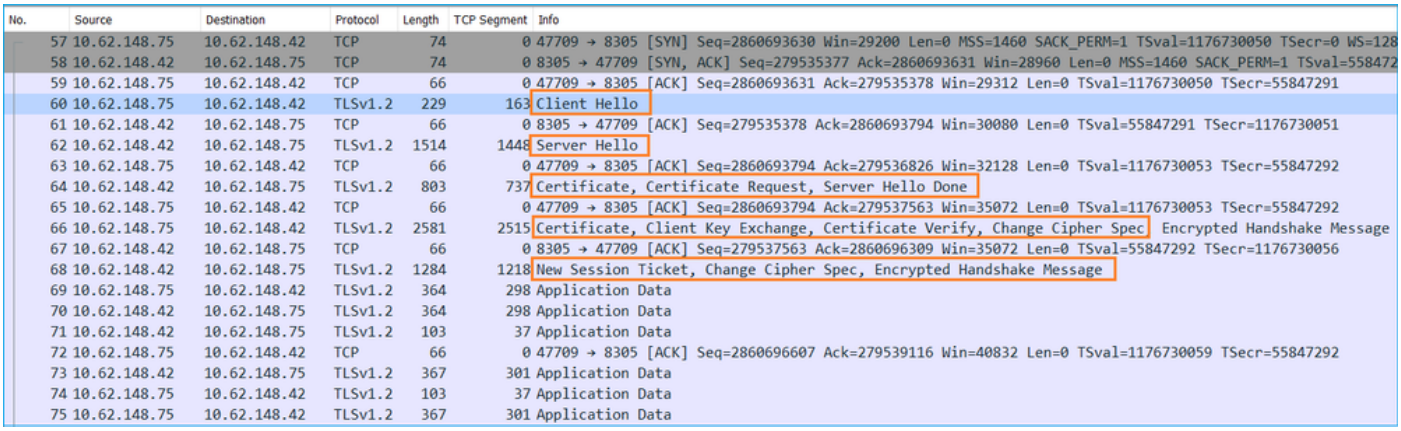
このリストには、sftunnelを介して伝送されるほとんどの情報が含まれています。

- アプライアンスハートビート（キープアライブ）
- 時刻同期(NTP)
- イベント（接続、侵入/IPS、ファイル、SSLなど）
- マルウェアの検索
- ヘルスイベント/アラート
- ユーザおよびグループ情報（アイデンティティポリシー用）
- FTD HAステート情報
- FTDクラスタの状態情報
- セキュリティインテリジェント(SI)情報/イベント
- Threat Intelligence Director(TID)情報/イベント
- キャプチャされたファイル
- ネットワーク検出イベント
- ポリシーバンドル（ポリシー導入）
- ソフトウェアアップグレードバンドル
- ソフトウェアパッチバンドル

- VDB
- SRU

sftunnelによって使用されるプロトコル/ポートは何ですか。

sftunnelはTCPポート8305を使用します。バックエンドではTLSトンネルです。



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

FTDのSftunnel TCPポートを変更する方法

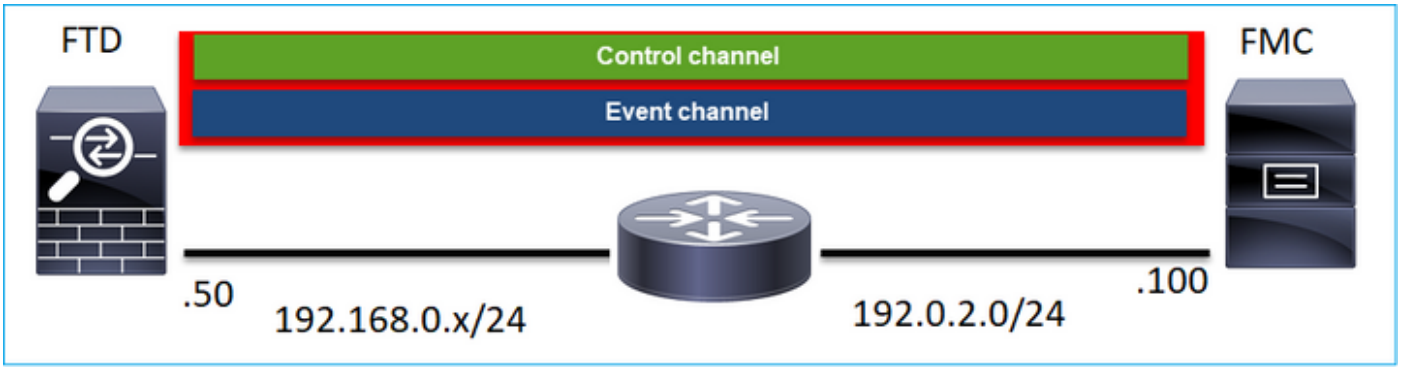
```
> configure network management-port 8306
Management port changed to 8306.
```

> **注**：この場合、FMCのポートも変更する必要があります([Configuration] > [Management Interfaces] > [Shared Settings])。 これは、同じFMCにすでに登録されている他のすべてのデバイスに影響します。リモート管理ポートはデフォルト設定のままにしておくことを強く推奨しますが、管理ポートがネットワーク上の他の通信と競合する場合は、別のポートを選択できます。管理ポートを変更する場合は、同時に通信する必要がある導入環境内のすべてのデバイスに対して管理ポートを変更する必要があります。

sftunnelによって確立される接続数

sftunnelは2つの接続（チャネル）を確立します。

- 制御チャネル
- イベントチャネル



各チャネルを開始するデバイスはどれか？

シナリオによって異なります。以降のドキュメントで説明されているシナリオを確認します。

設定

登録の基本

FTD CLI

FTDでは、デバイス登録の基本構文は次のとおりです。

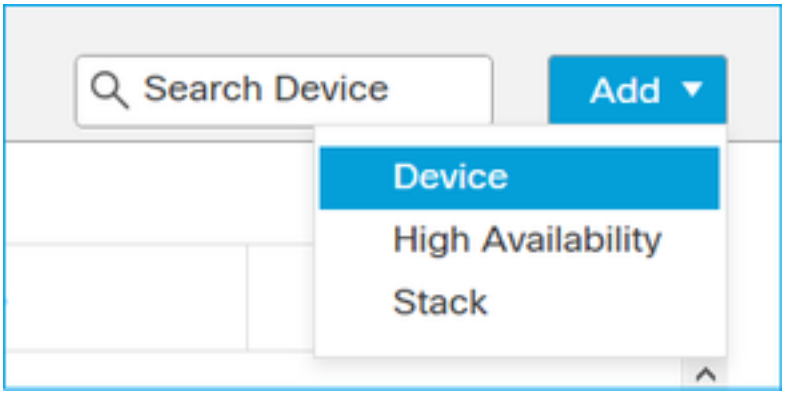
>configure manager add <FMC Host> <Registration Key> <NAT ID>

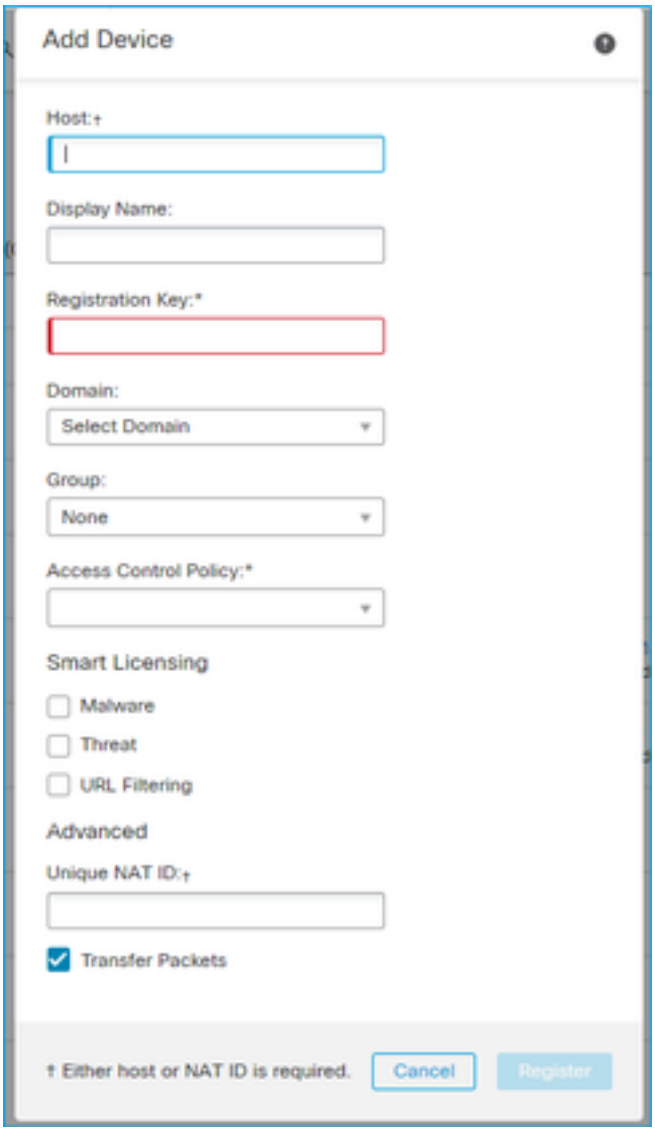
値	説明
FMCホスト	これは次のいずれかになります。 • [hostname] • ipv4アドレス • ipv6アドレス • DONTRESOLVE
登録キー	これは、デバイス登録に使用される共有秘密の英 文字列（2 ～ 36文字）です。英数字、ハイフン(- ンダースコア(_)、およびピリオド(.)のみ使用でき 。
NAT ID	一方の側でIPアドレスが指定されていない場合に FMCとデバイス間の登**録プロセス中に使用される 字の文字列**。FMCで同じNAT IDを指定します。

詳細については、『Cisco Firepower Threat Defenseコマンドリファレンス』を参照してください
。

FMC UI

FMCで、[Devices] > [Device Management] に移動します。**[Add] > [Device]** を選択します。





- [Host]でFTDのIPアドレスを指定します。
- [Display Name]で、必要な名前を指定します。
- 登録キーは、FTD CLIで指定されたものと一致する必要があります。
- 複数のドメインを使用する場合は、FTDを追加するドメインを指定します。
- [Group]で、FTDを追加するデバイスグループを指定します。
- [Access Control Policy]で、FTDに展開するセキュリティポリシーを指定します。
- Smart Licensing:設定された機能に必要なライセンスを指定します。
- NAT ID:このドキュメントで後述する特定のシナリオで必要です。

詳細については、『Firepower Management Center Configuration Guide』の「Add Devices to the Firepower Management Center

シナリオ1:FMCとFTDのスタティックIPアドレス

FTD CLI

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

以下に、いくつかの例を示します。

```
> 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.
```

背景情報

FTDコマンドを入力するとすぐに、FTDは20秒ごとにFMCへの接続を試行しますが、FMCはまだ設定されていないため、TCP RSTで応答します。

```
> 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
```

デバイス登録ステータス：

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

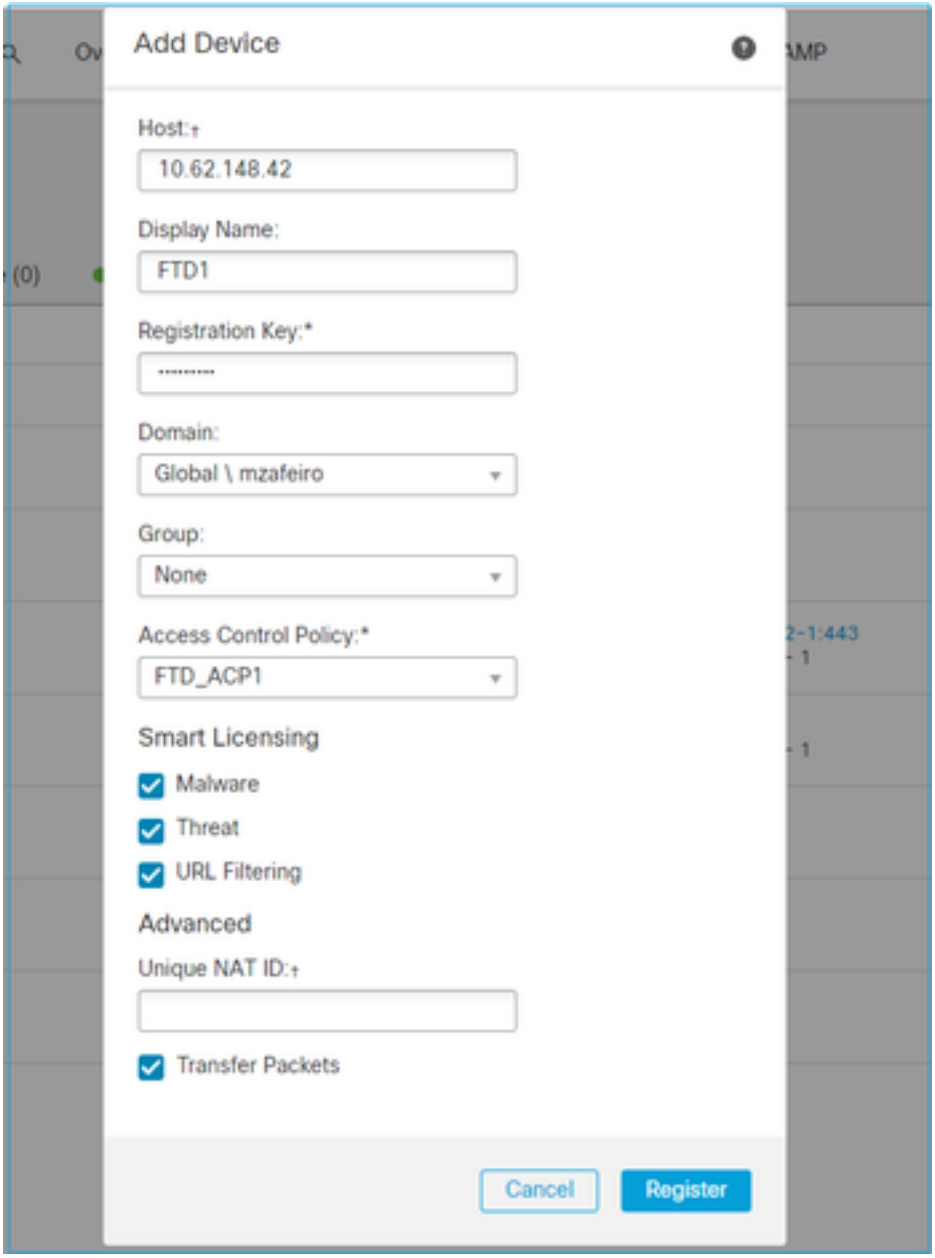
FTDはポートTCP 8305をリッスンします。

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

FMC UI

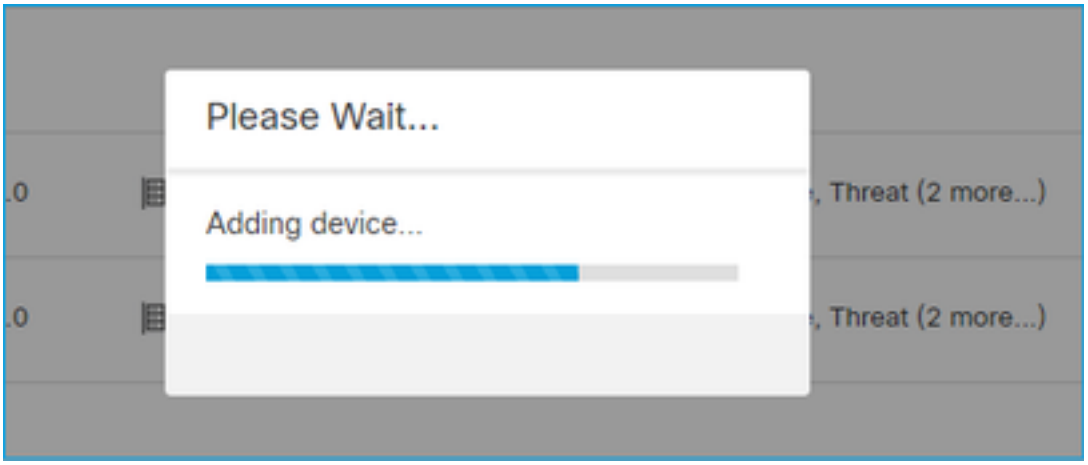
この場合は、次を指定します。

- ホスト（FTDのIPアドレス）
- 表示名
- 登録キー（FTDで設定されているものと一致する必要があります）
- アクセス コントロール ポリシー
- Domain
- スマートライセンス情報



[Register] を選択します。

登録プロセスが開始されます。



FMCがポートTCP 8305でリッスンを開始します。

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

バックグラウンドで、FMCはTCP接続を開始します。

```
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制御チャネルが確立されます。

```
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
```

数分後に、イベントチャネルが確立されます。イベントチャネルの発信側は**いずれかの**側にできます。この例では、FMCです。

```
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
```

ランダムな送信元ポートは接続イニシエータを示します。

```
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
```

イベントチャネルがFTDによって開始された場合、出力は次のようになります。

```
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側から：

```
> 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

>
```

シナリオ2:FTD DHCP IPアドレス – FMC固定IPアドレス

このシナリオでは、FTD管理インターフェイスはDHCPサーバからIPアドレスを取得しました。

FTD CLI

NAT IDを指定する必要があります。

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

以下に、いくつかの例を示します。

```
> 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登録ステータスは次のとおりです。

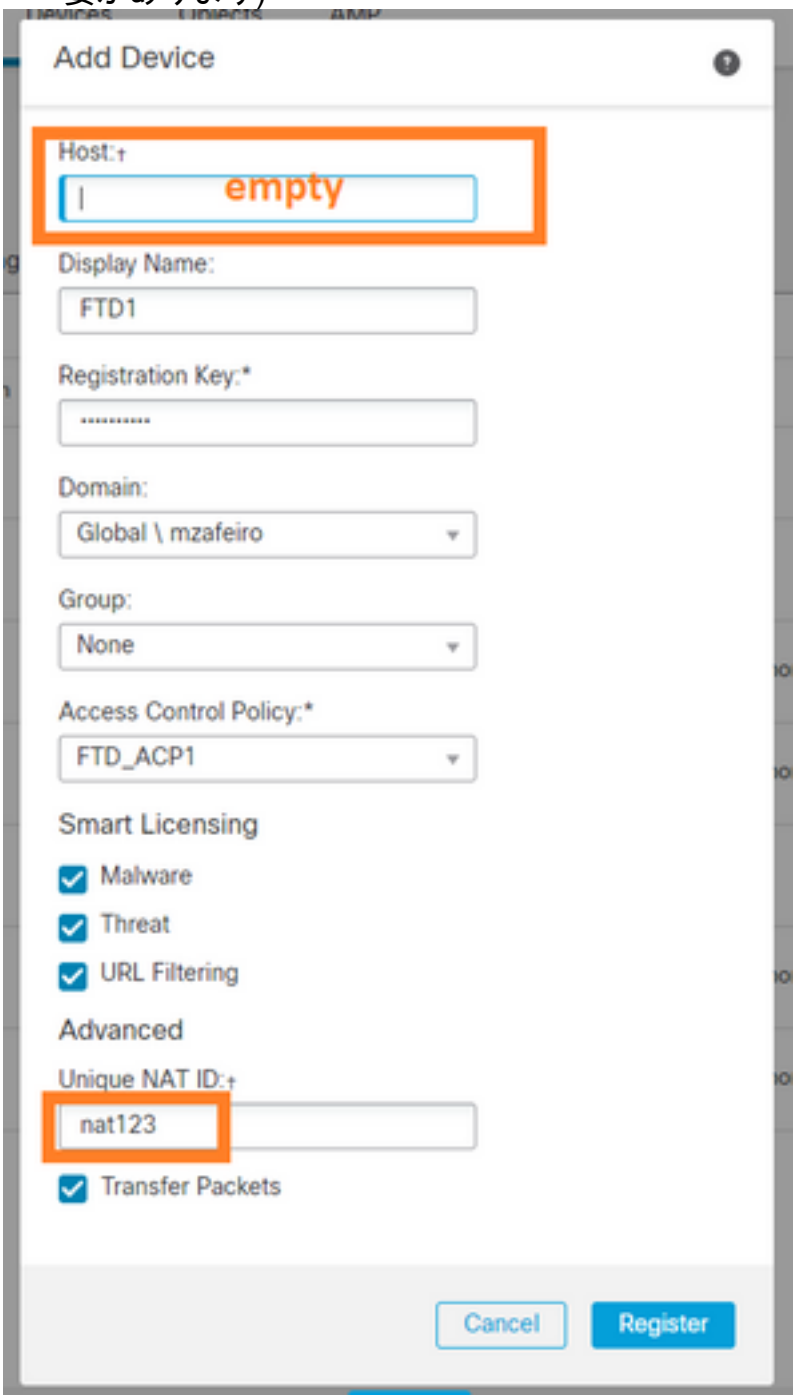
```
> show managers
Host                      : 10.62.148.75
Registration Key          : ****
Registration              : pending
RPC Status                :
```

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

FMC UI

この場合は、次を指定します。

- 表示名
- 登録キー（FTDで設定されているものと一致する必要があります）
- アクセス コントロール ポリシー
- Domain
- スマートライセンス情報
- NAT ID(**ホストが指定されていない場合は必須**)FTDで設定されているものと一致している必要があります)

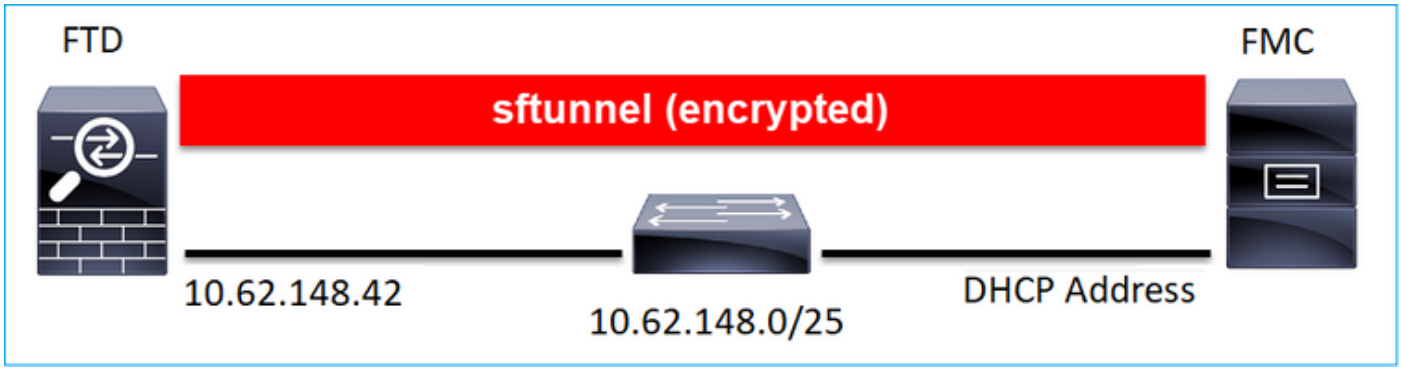


この場合、誰がsftunnelを開始しますか。

FTDが両方のチャネル接続を開始します。

```
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
```

シナリオ3:FTDスタティックIPアドレス – FMC DHCP IPアドレス




```
> 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.

>
```

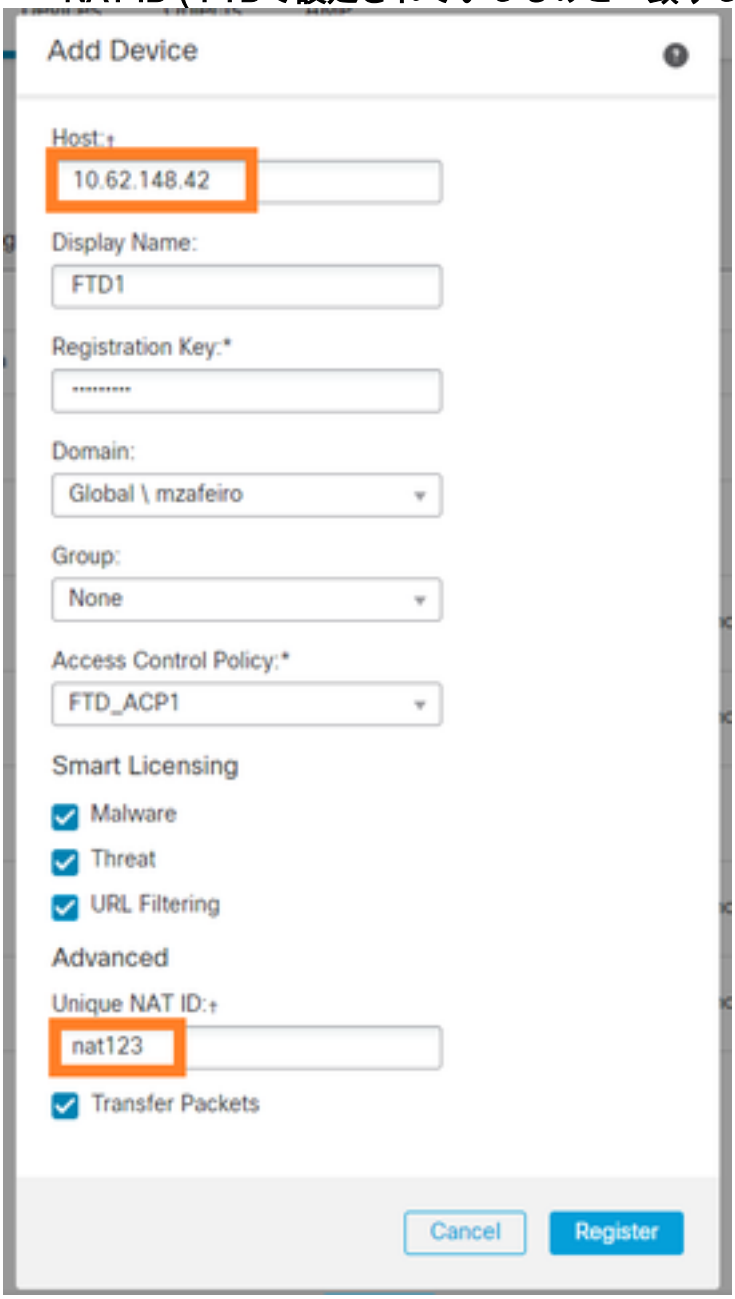
注：DONTRESOLVEでは、NAT IDが必要です。

FMC UI

この場合は、次のように指定します。

- **FTDのIPアドレス**
- 表示名
- 登録キー（FTDで設定されているものと一致する必要があります）
- アクセス コントロール ポリシー
- Domain
- スマートライセンス情報

- **NAT ID（FTDで設定されているものと一致する必要がある）**



登録後のFTD:

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

この場合、誰がsftunnelを開始しますか。

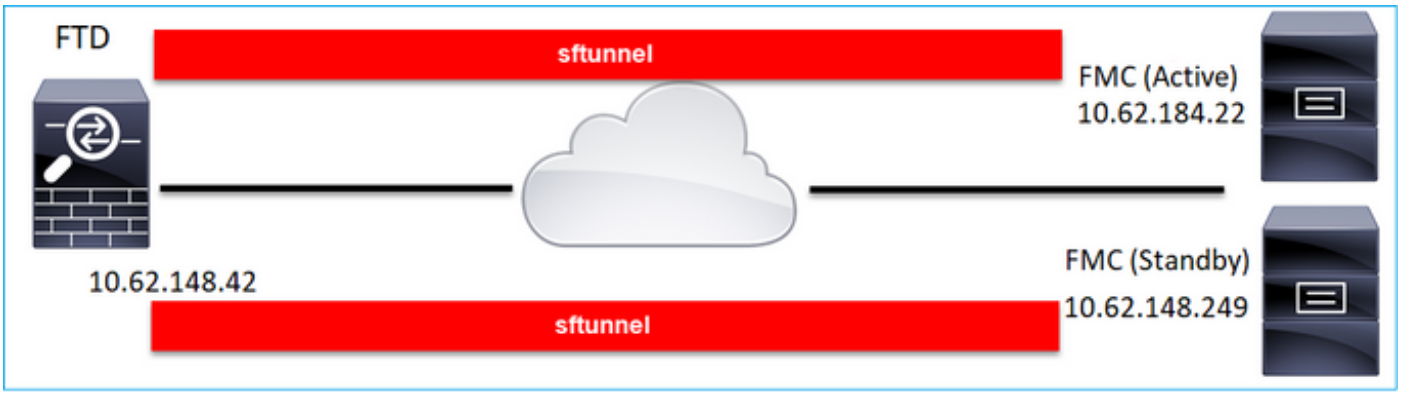
- FMCが制御チャネルを開始します。
- イベントチャネルはどちらの側からも開始できます。

```
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
```

シナリオ4:FMC HAへのFTDの登録

FTDでは、アクティブFMCのみを設定します。

```
> 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.
```

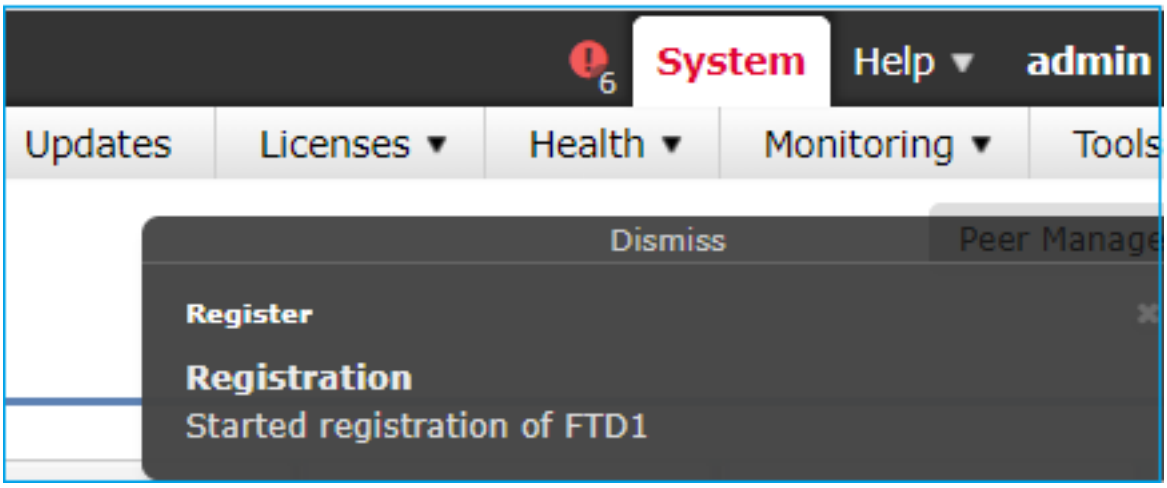


> **注**：FTDから両方のFMCへのTCPポート8305トラフィックが許可されていることを確認します。

まず、アクティブFMCへのsftunnelが確立されます。

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

数分後、FTDはスタンバイFMCへの登録を開始します。



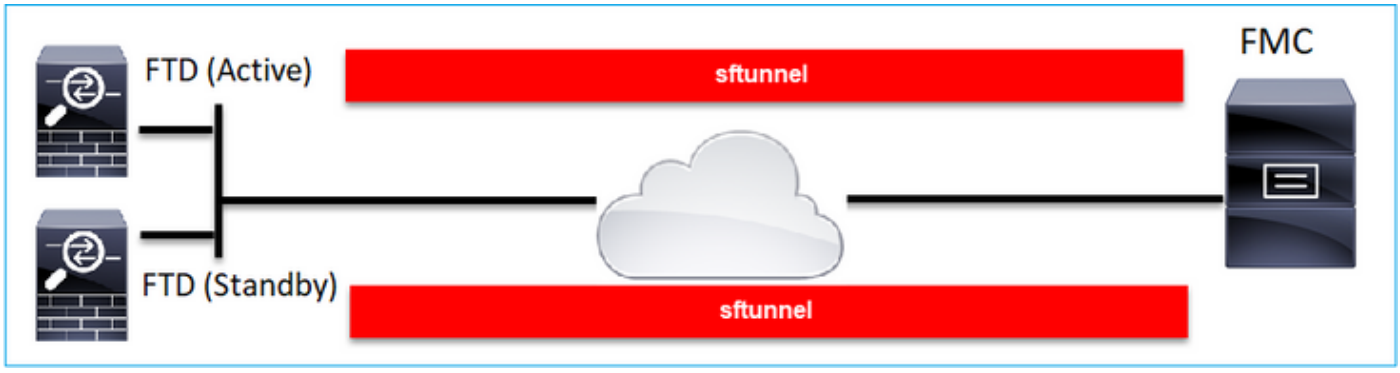

```
> show managers
Type                    : Manager
Host                    : 10.62.184.22
Registration            : Completed

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

FTDバックエンドでは、2つの制御チャネル（各FMCに1つ）と2つのイベントチャネル（各FMCに1つ）が確立されます。

```
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
```

シナリオ5:FTD HA

FTD HAの場合、各ユニットにはFMCへの個別のトンネルがあります。



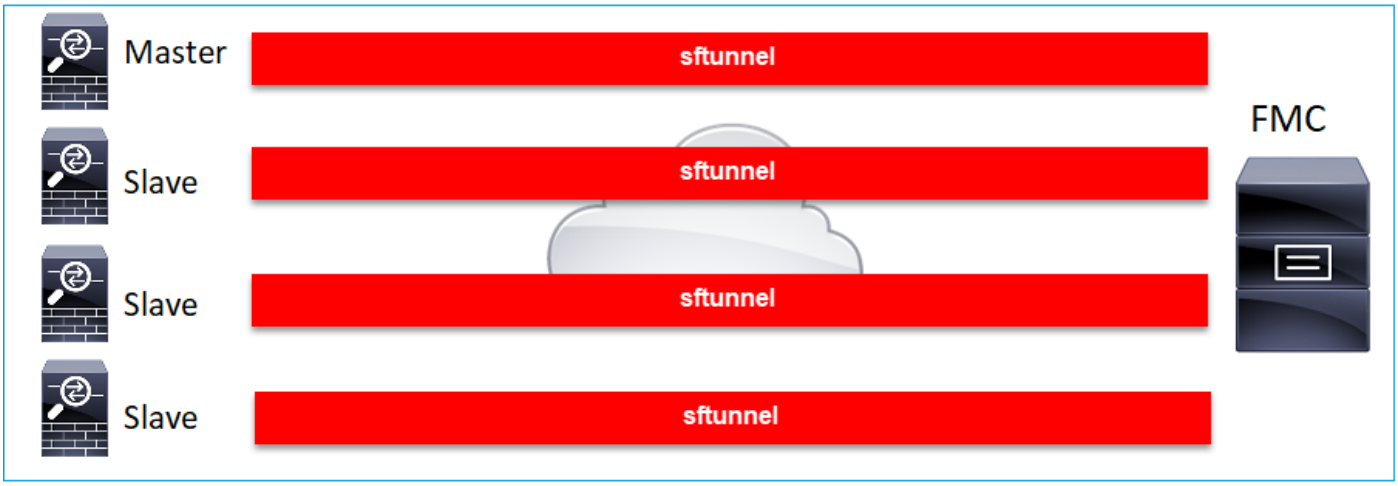
両方のFTDを個別に登録し、FMCからFTD HAを形成します。詳細については、次を確認してく

ださい。

- Firepower アプライアンスでの FTD 高可用性の設定
- Firepower Threat Defenseの高可用性

シナリオ6:FTDクラスタ

FTDクラスタの場合、各ユニットにはFMCへの個別のトンネルがあります。6.3 FMCリリース以降では、FTDマスターをFMCに登録するだけで済みます。その後、残りのユニットはFMCが処理し、自動検出+登録します。

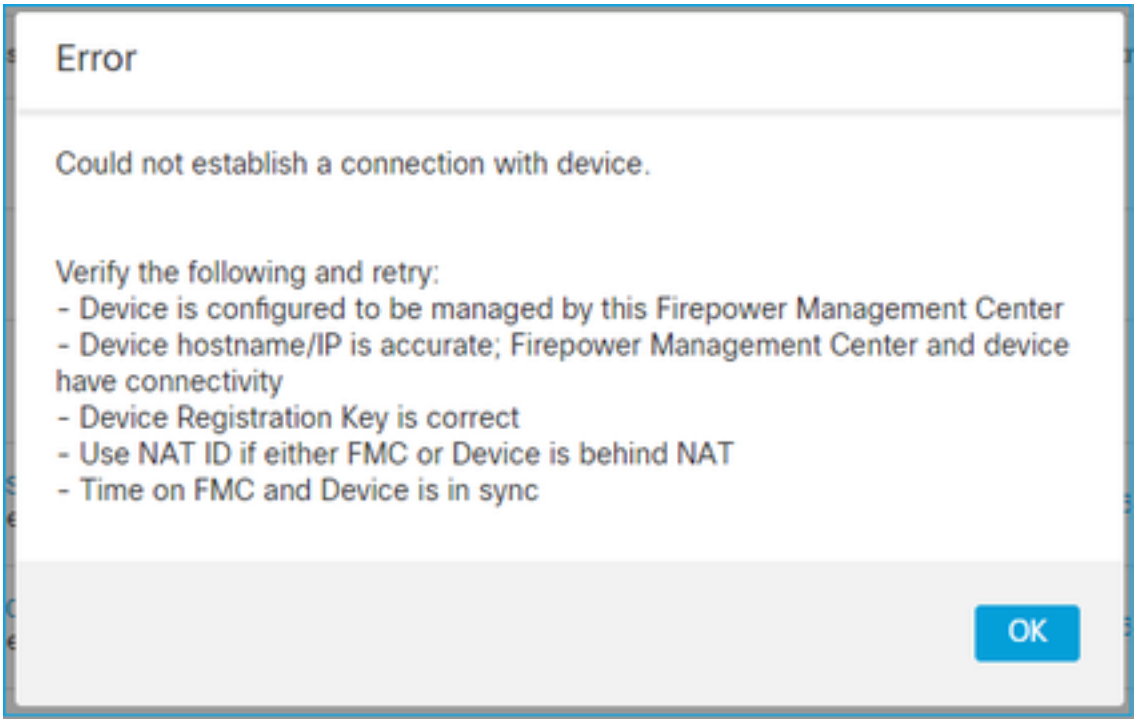


注：最適なパフォーマンスを得るためにマスターユニットを追加することをお勧めしますが、クラスタの任意のユニットを追加できます。詳細については、次の項目を確認してください。Firepower Threat Defenseクラスタの作成

一般的な問題のトラブルシューティング

1. FTD CLIの無効な構文

FTDの構文が無効で、登録の試行に失敗した場合、FMC UIに非常に一般的なエラーメッセージが表示されます。



このコマンドでは、キーワードkeyが登録キーで、cisco123がNAT IDです。技術的にはそのようなキーワードはありませんが、キーワードキーを追加することはかなり一般的です。

```
> 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.
```

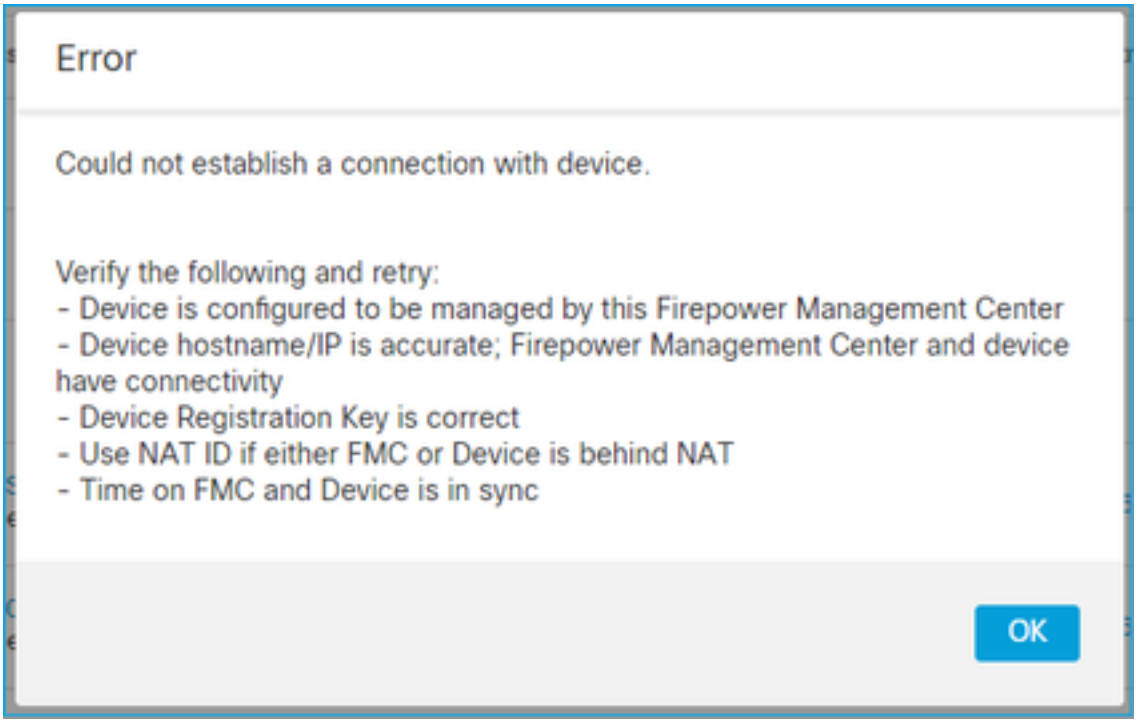
推奨処置

正しい構文を使用し、存在しないキーワードは使用しないでください。

```
> 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とFMC間の登録キーの不一致

FMC UIには次のように表示されます。



推奨処置

FTDで/ngfw/var/log/messagesファイルをチェックして、認証の問題を確認します。

方法1：過去のログを確認する

```
> 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
```

方法2：ライブログの確認

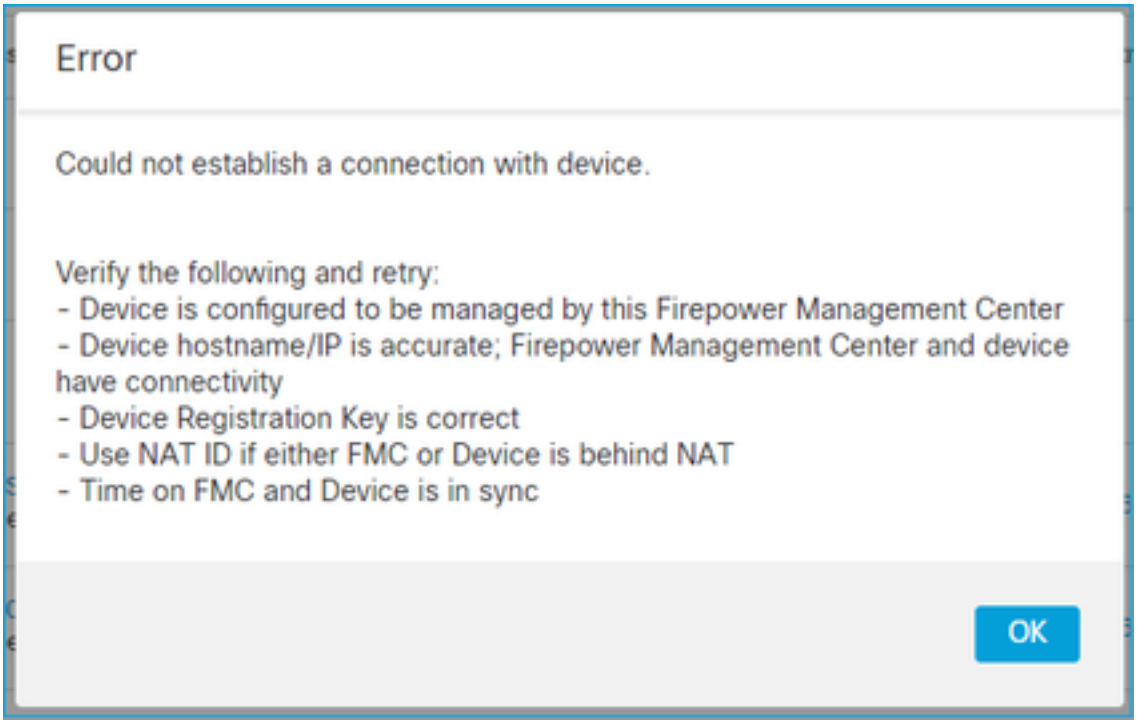
```
> expert
ftd1:~$ sudo su
Password:
ftd1::/home/admin# tail -f /ngfw/var/log/messages
```

FTDで/etc/sf/sftunnel.confファイルの内容をチェックし、登録キーが正しいことを確認します。

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

3. FTDとFMC間の接続の問題

FMC UIには次のように表示されます。



推奨処置

- パス (ファイアウォールなど) にトラフィックをブロックするデバイス(TCP 8305)がないことを確認します。 FMC HAの場合は、TCPポート8305へのトラフィックが両方のFMCに対して許可されていることを確認します。
- キャプチャを取得して、双方向通信を確認します。FTDで**capture-traffic**コマンドを使用します。TCP 3ウェイハンドシェイクがあり、TCP FINまたはRSTパケットがないことを確認します。

```
> 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
```

同様に、FMCでキャプチャを取得して、双方向通信を確保します。

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

また、キャプチャをpcap形式でエクスポートし、パケットの内容を確認することをお勧めします。

```
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
```

考えられる原因：

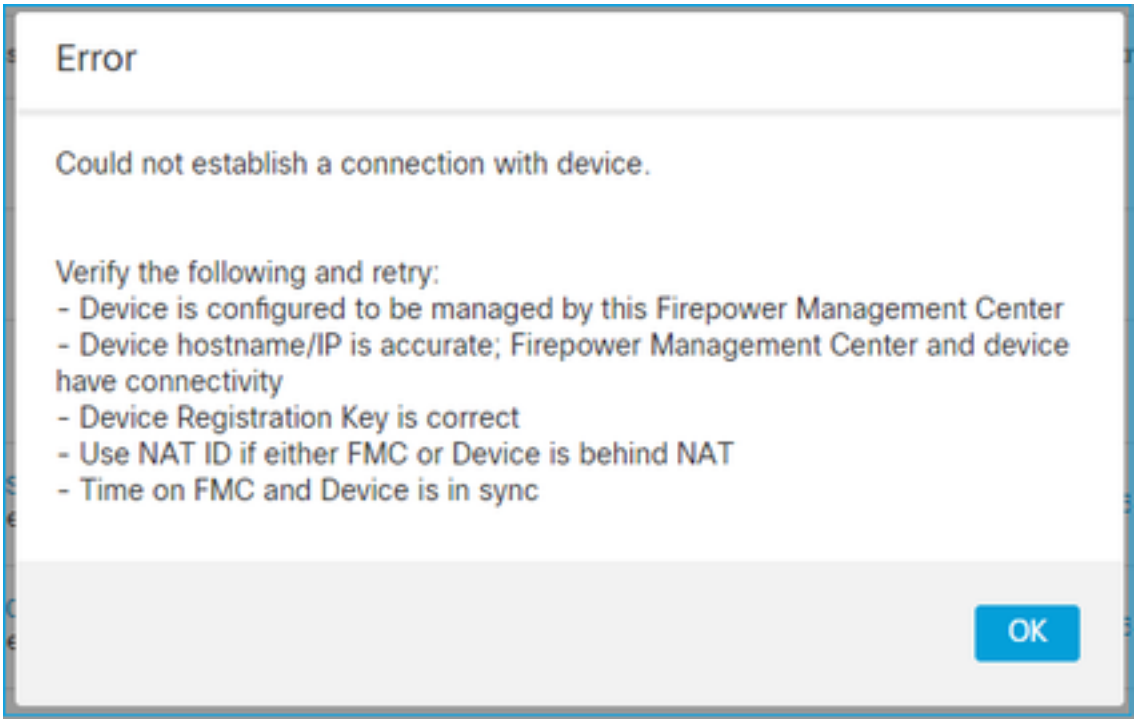
- FMCにFTDデバイスが追加されていません。
- パス内のデバイス（ファイアウォールなど）は、トラフィックをブロックまたは変更します。
- パケットがパスで正しくルーティングされない。
- FTDまたはFMCのsftunnelプロセスがダウンしている（シナリオ6を確認）
- パスにMTUの問題がある（シナリオを確認）。

キャプチャ分析については、次のドキュメントを確認してください。

ネットワークの問題を効果的にトラブルシューティングするための Firepower ファイアウォール キャプチャの分析

4. FTDとFMCの間で互換性のないソフトウェア

FMC UIには次のように表示されます。



推奨処置

FTD /ngfw/var/log/messagesファイルを確認します。

```
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の互換性マトリクスを確認します。

Cisco Firepower 互換性ガイド

5. FTDとFMCの時間差

FTD-FMC通信は、2つのデバイス間の時間差に影響を受けます。FTDとFMCを同じNTPサーバで同期させる設計要件です。

具体的には、FTDが41xxや93xxなどのプラットフォームにインストールされている場合、親シャ

ーシ(FXOS)から時間設定を取得します。

推奨処置

シャーシマネージャ(FCM)とFMCが同じ時刻源（NTPサーバ）を使用していることを確認します

6.sftunnelプロセスのダウンまたは無効化

FTDでは、sftunnelプロセスが登録プロセスを処理します。これは、マネージャの設定前のプロセスのステータスです。

```
> 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
```

登録ステータス：

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

マネージャを設定します。

```
> 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.
```

これでプロセスはUPです。

```
> 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)
```

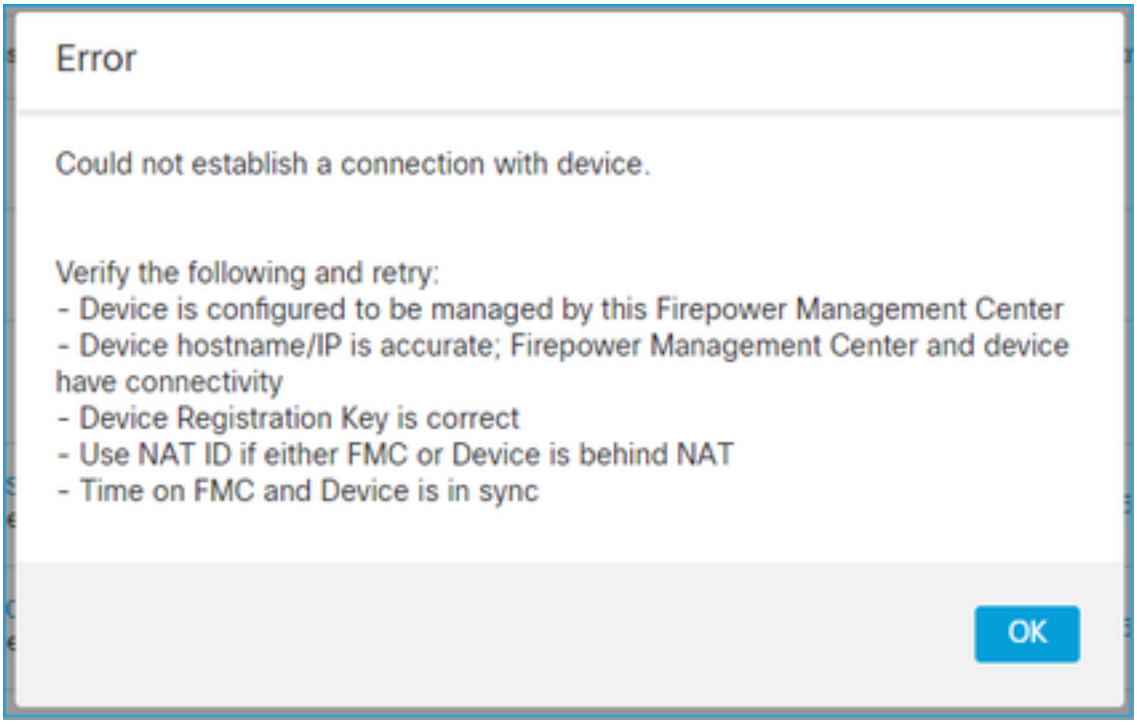
まれに、プロセスがダウンしたり無効になったりすることがあります。

```
> 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
```

マネージャステータスは正常です。

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

一方、デバイスの登録は失敗します。



FTDでは、/ngfw/var/log/messages

推奨処置

FTDトラブルシューティングファイルを収集し、Cisco TACに連絡する

7.セカンダリFMCでのFTD登録保留中

FMC HAセットアップへの最初のFTD登録後、FTDデバイスがセカンダリFMCに追加されないシナリオがあります。

推奨処置

このドキュメントで説明されている手順に従ってください。

CLIを使用したFirepower Management Centerハイアベイラビリティでのデバイス登録の解決

> **警告**：この手順にはデバイスの登録解除が含まれているため、この手順は煩わしい作業です。これは、FTDデバイスの設定に影響します（削除されます）。 この手順は、FTDの初期登録とセットアップの際にのみ使用することを推奨します。別のケースでは、FTDおよびFMCのトラブルシューティングファイルを収集し、Cisco TACに連絡してください。

8.パスMTUが原因で登録が失敗する

Cisco TACでは、Sftunnelトラフィックが小さなMTUのリンクを通過する必要があるシナリオがあります。sftunnelパケットには**Don't fragment**ビットが**設定**されているため、フラグメンテーションは許可されません。

	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

また、/ngfw/var/log/messagesファイルには、次のようなメッセージが表示されます。

MSGS:10-09 14:41:11 ftd1 SF-IMS[7428]:[6612] sftunneld:sf_ssl [ERROR] **Connect:SSLハンドシェイクが失敗しました**

推奨処置

フラグメンテーションによるパケット損失があるかどうかを確認するには、FTD、FMC、およびパス内のデバイスでキャプチャを取得します。両端に到着するパケットが表示されるかどうかを確認します。

FTDでは、FTD管理インターフェイスのMTUを小さくします。デフォルト値は1500バイトです。管理インターフェイスのMAXは1500、イベントインターフェイスのMAXは9000です。このコマンドは、FTD 6.6リリースで追加されました。

Cisco Firepower Threat Defenseコマンドリファレンス

例

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

確認

```
> 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 ]----------------------
```

FTDからのパスMTUを確認するには、次のコマンドを使用できます。

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

doオプションは、ICMPパケットのdon't fragmentビットを設定します

FMCでは、このドキュメントで説明されているように、FMC管理インターフェイスのMTU値を小さくします。

Firepower Management Center(FMC)管理インターフェイスの設定

9. FTDがChassis Manager UIからブートストラップ変更後に登録解除される

これはFP41xxおよびFP93xxプラットフォームに適用され、Cisco Bug ID CSCvn45138に記載されています .

一般に、ディザスタリカバリを行わない限り、Chassis Manager(FCM)からのブートストラップの変更は行わないでください。

推奨処置

ブートストラップの変更を行い、条件に一致した（ブートストラップの変更後にFTDが起動している間にFTD-FMC通信が切断された）場合は、FTDを削除し、FMCに再登録する必要があります。

10. ICMPリダイレクトメッセージが原因でFTDがFMCにアクセスできなくなる

この問題は、登録プロセスに影響を与えたり、登録後にFTD-FMCの通信を中断したりする可能性があります。

この場合の問題は、FTD管理インターフェイスに**ICMPリダイレクト**メッセージを送信し、FTD-FMC通信をブラックホール化するネットワークデバイスです。

この問題を特定する方法

この場合、10.100.1.1はFMCのIPアドレスです。FTDには、FTDが管理インターフェイスで受信したICMPリダイレクトメッセージによるキャッシュされたルートがあります。

```
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
```

推奨処置

手順 1

ICMPを送信するデバイス（たとえば、アップストリームL3スイッチ、ルータなど）でICMPリダイレクトを無効にします。

手順 2

FTD CLIからFTDルートキャッシュをクリアします。

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

リダイレクトされない場合は、次のようになります。

```
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
```

参考資料

- ICMP リダイレクトメッセージの理解
- Cisco Bug ID CSCvm53282 FTD:ICMPリダイレクトによって追加されたルーティングテーブルは、ルーティングテーブルキャッシュで永続的にスタックされます

関連情報

- NGFW設定ガイド

翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。