

Configuration, vérification et dépannage de l'enregistrement des périphériques Firepower

Table des matières

[Introduction](#)

[Conditions préalables](#)

[Exigences](#)

[Composants utilisés](#)

[Informations générales](#)

[Options de conception](#)

[Quelles informations sont échangées via le sftunnel ?](#)

[Quel protocole/port est utilisé par le sftunnel ?](#)

[Comment modifier le port TCP Sftunnel sur FTD ?](#)

[Combien de connexions sont établies par le sftunnel ?](#)

[Quel Périphérique Lance Chaque Canal ?](#)

[Configurer](#)

[Notions de base](#)

[Scénario 1. Adresse IP statique FMC et FTD](#)

[Scénario 2. Adresse IP DHCP FTD - Adresse IP statique FMC](#)

[Scénario 3. Adresse IP statique FTD - Adresse IP DHCP FMC](#)

[Scénario 4 . Inscription FTD auprès de FMC HA](#)

[Scénario 5. FTD HA](#)

[Scénario 6. Cluster FTD](#)

[Dépannage des problèmes courants](#)

[1. Syntaxe incorrecte sur la CLI FTD](#)

[2. Incompatibilité de clé d'enregistrement entre FTD et FMC](#)

[3. Problèmes de connectivité entre FTD et FMC](#)

[4. Logiciel incompatible entre FTD et FMC](#)

[5. Différence de temps entre FTD et FMC](#)

[6. sftunnel Process Down ou Disabled](#)

[7. FTD Enregistrement en attente sur le FMC secondaire](#)

[8. Échec de l'enregistrement en raison de Path MTU](#)

[9. L'enregistrement du FTD est annulé après un changement de bootstrap de l'interface utilisateur du gestionnaire de châssis](#)

[10. Le FTD perd l'accès au FMC en raison des messages de redirection ICMP](#)

Introduction

Ce document décrit les procédures de dépannage de la connexion entre Firepower Threat Defense (FTD) et Firepower Management Center (FMC).

Conditions préalables

Exigences

Aucune exigence spécifique n'est associée à ce document.

Composants utilisés

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- Logiciels FTD 6.6.x et 6.5.x
- Logiciel FMC 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. Si votre réseau est en ligne, assurez-vous de bien comprendre l'incidence possible des commandes.

Informations générales

Ce document décrit les procédures de fonctionnement, de vérification et de dépannage de la connexion (sftunnel) entre un FTD géré et le FMC géré.

Les informations et les exemples sont basés sur le FTD, mais la plupart des concepts sont également pleinement applicables au NGIPS (appliances de la gamme 7000/8000) ou à un module FirePOWER sur ASA55xx.

Un FTD prend en charge 2 modes de gestion principaux :

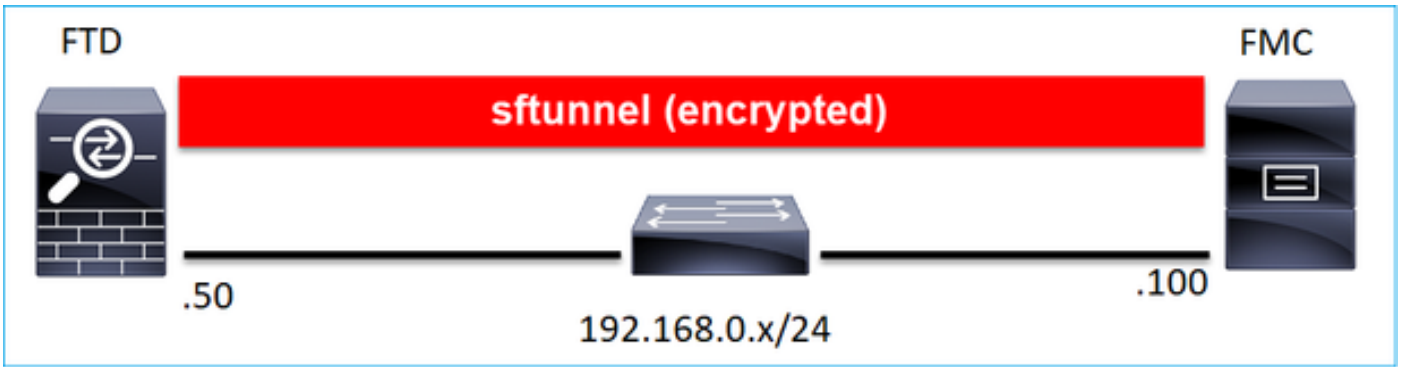
- Offbox via FMC, également appelé gestion à distance
- On-box via Firepower Device Manager (FDM) et/ou Cisco Defense Orchestrator (CDO), également appelé gestion locale

Dans le cas d'une gestion à distance, le FTD doit d'abord s'enregistrer auprès du FMC qui utilise un processus appelé enregistrement de périphérique.

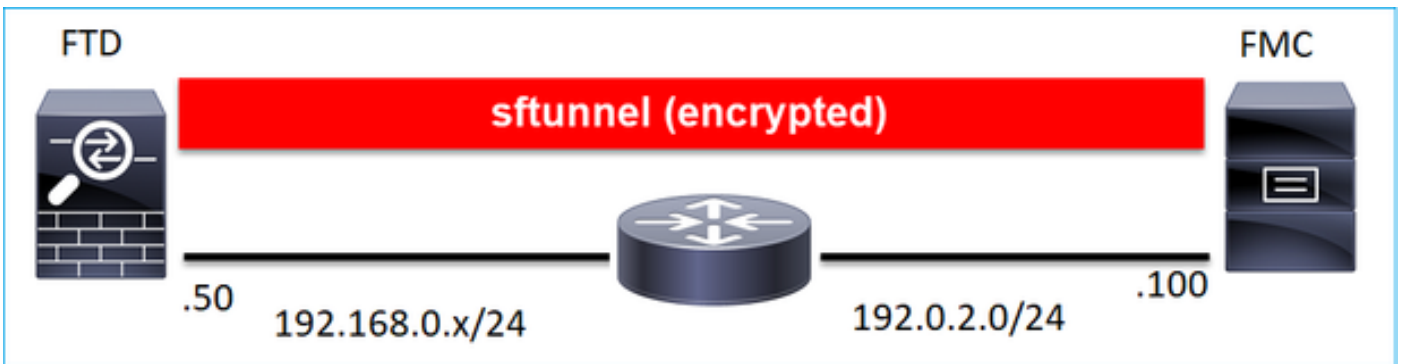
Lorsque l'enregistrement est fait, le FTD et le FMC établissent un tunnel sécurisé appelé sftunnel (le nom dérive du tunnel Sourcefire).

Options de conception


Du point de vue de la conception, le FTD - FMC peut se trouver dans le même sous-réseau L3 :

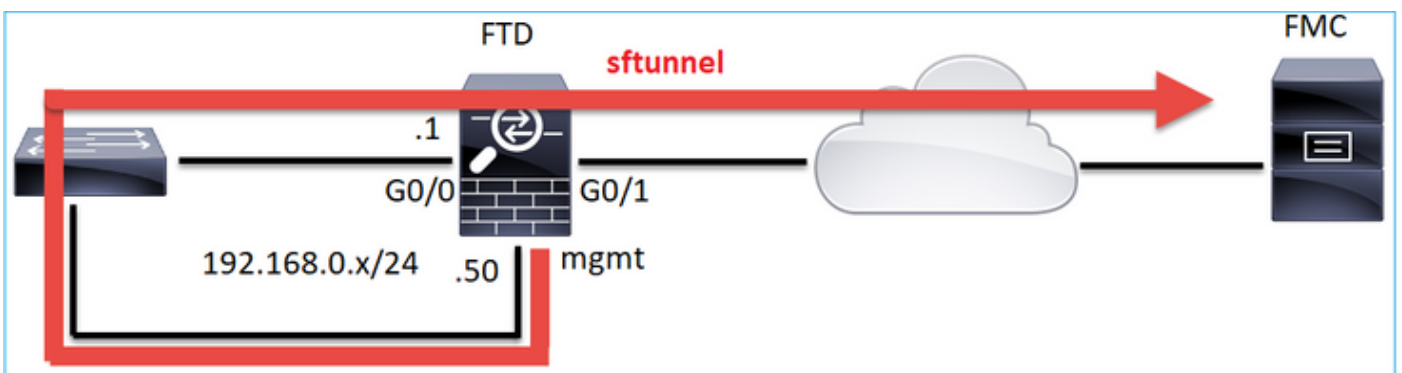


ou être séparés par des réseaux différents :



192.0.2.0

 Remarque : le sftunnel peut également passer par le FTD lui-même. Cette conception n'est pas recommandée. La raison en est qu'un problème de plan de données FTD peut interrompre la communication entre FTD et FMC.



Quelles informations sont échangées via le sftunnel ?

Cette liste contient la plupart des informations qui sont transportées par le sftunnel :

- Pulsation de l'appliance (keepalives)
- Synchronisation temporelle (NTP)
- Événements (connexion, intrusion/IPS, fichier, SSL, etc.)
- Recherches de programmes malveillants
- Événements/alertes de santé
- Informations sur l'utilisateur et le groupe (pour les politiques d'identité)
- Informations d'état FTD HA
- Informations d'état du cluster FTD
- Informations/événements de sécurité intelligente (SI)
- Informations/événements sur Threat Intelligence Director (TID)
- Fichiers capturés
- Événements de découverte de réseau
- Ensemble de politiques (déploiement de politiques)
- Ensembles de mise à niveau logicielle
- Ensembles de correctifs logiciels
- VDB
- SRU

Quel protocole/port est utilisé par le sftunnel ?

Le sftunnel utilise le port TCP 8305. Dans le back-end, il s'agit d'un tunnel TLS :

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=55847292
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	1218	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


Comment modifier le port TCP Sftunnel sur FTD ?

```
<#root>
```

```
>
```

```
configure network management-port 8306
```

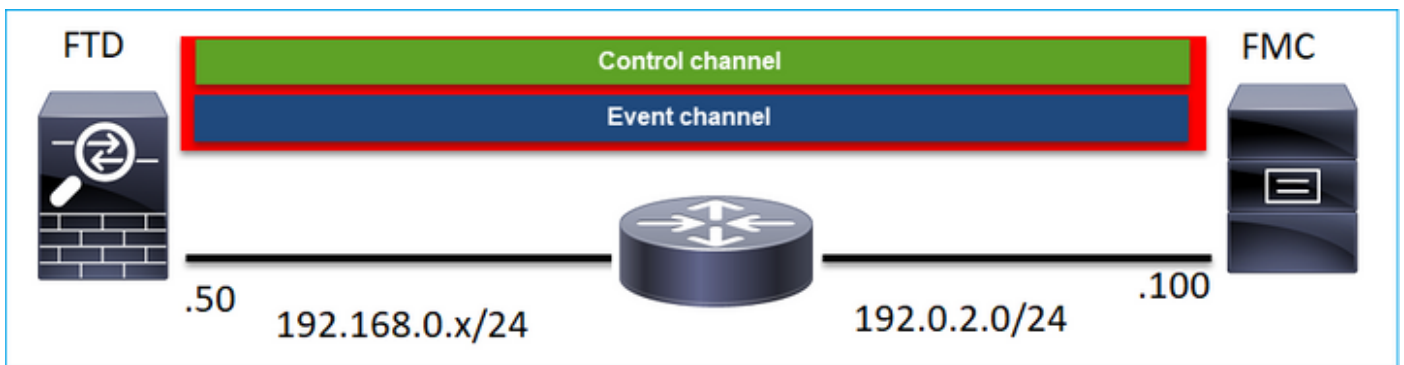
```
Management port changed to 8306.
```

 Remarque : dans ce cas, vous devez également modifier le port sur FMC (Configuration > Management Interfaces > Shared Settings). Cela affecte tous les autres périphériques qui sont déjà enregistrés sur le même FMC. Cisco vous recommande vivement de conserver les paramètres par défaut du port de gestion à distance, mais si ce dernier est en conflit avec d'autres communications de votre réseau, vous pouvez choisir un autre port. Si vous modifiez le port de gestion, vous devez le modifier pour tous les périphériques de votre déploiement qui doivent communiquer entre eux.

Combien de connexions sont établies par le sftunnel ?

Le sftunnel établit 2 connexions (canaux) :

- Canal de contrôle
- Canal Événement



Quel Périphérique Lance Chaque Canal ?

Cela dépend du scénario. Vérifiez les scénarios décrits dans le reste du document.

Configurer

Notions de base

CLI FTD

Sur FTD, la syntaxe de base pour l'enregistrement du périphérique est la suivante :

> configure manager add <Hôte FMC> <Clé d'enregistrement> <ID NAT>

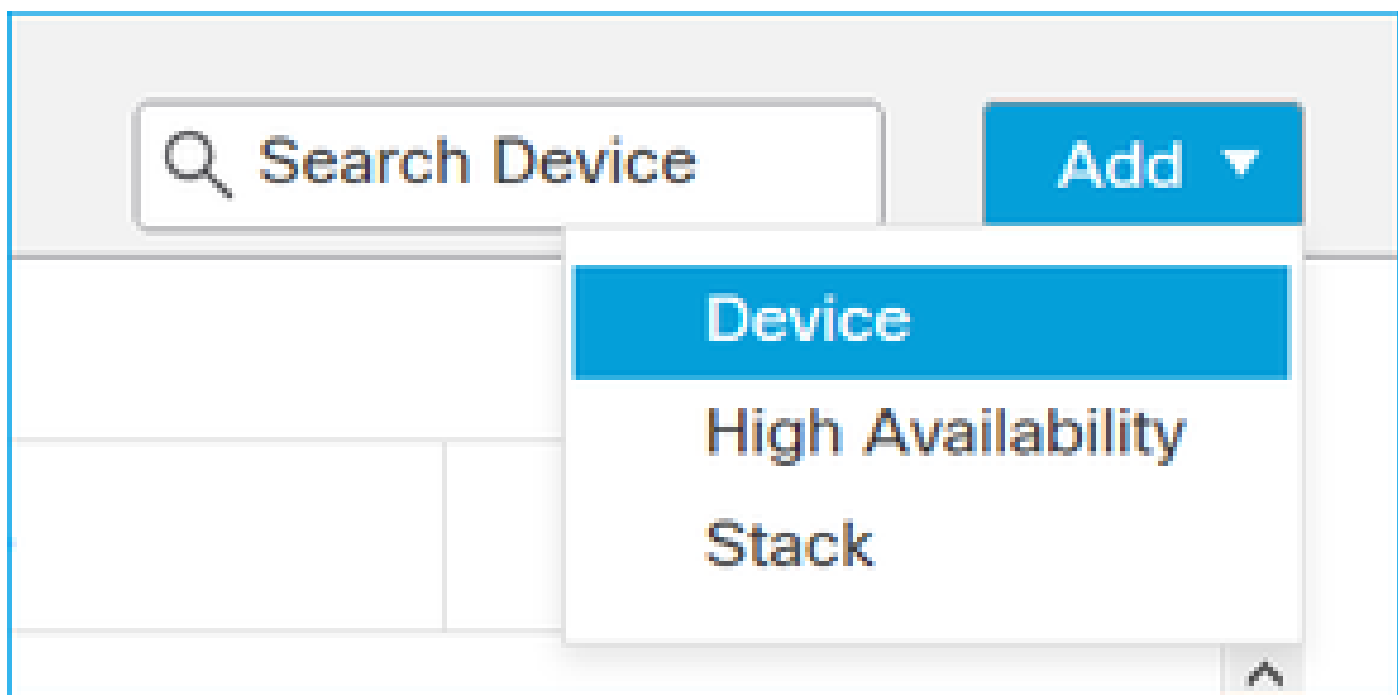
Valeur	Description
--------	-------------

Hôte FMC	<p>Il peut s'agir :</p> <ul style="list-style-type: none"> • Nom de l'hôte • adresse ipv4 • adresse ipv6 • DONTRÉSOLU
Clé d'enregistrement	<p>Il s'agit d'une chaîne alphanumérique secrète partagée (entre 2 et 36 caractères) utilisée pour l'enregistrement du périphérique. Seuls les caractères alphanumériques, le tiret (-), le trait de soulignement (_) et le point (.) sont autorisés.</p>
ID NAT	<p>Chaîne alphanumérique utilisée lors du processus d'enregistrement entre le FMC et le périphérique lorsqu'un côté ne spécifie pas d'adresse IP. Spécifiez le même ID NAT sur le FMC.</p>

Pour plus d'informations, consultez le document [Cisco Firepower Threat Defense Command Reference](#)

Interface utilisateur FMC

Sur FMC, accédez à Devices > Device Management. Sélectionnez Add > Device



Add Device



Host:

Display Name:

Registration Key:*

Domain:

Group:

Access Control Policy:*

Smart Licensing

- Malware
- Threat
- URL Filtering

Advanced

Unique NAT ID:†

Transfer Packets

CLI FTD

> configure manager add <IP statique FMC> <Clé d'enregistrement>

Exemple :

<#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.

Informations de fond

Dès que vous entrez la commande FTD, le FTD tente de se connecter au FMC toutes les 20 secondes, mais comme le FMC n'est pas encore configuré, il répond avec 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
```

État d'enregistrement du périphérique :

```
<#root>
```

```
>
```

```
show managers
```

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

Le FTD écoute sur le port TCP 8305 :

```
<#root>
```

```
admin@vFTD66:~$
```

```
netstat -na | grep 8305
```

```
tcp        0      0 10.62.148.42:8305
```

```
LISTEN
```

```
0.0.0.0:*
```

```
LISTEN
```

Interface utilisateur FMC

Dans ce cas, spécifiez les éléments suivants :

- Hôte (adresse IP du FTD)
- Nom d'affichage
- Clé d'enregistrement (elle doit correspondre à celle configurée sur le FTD)
- Politique de contrôle d'accès
- Domaine
- Informations sur les licences Smart

Add Device

Host:†

Display Name:

Registration Key:*

Domain:

Group:

Access Control Policy:*

Smart Licensing

- Malware
- Threat
- URL Filtering

Advanced

Unique NAT ID:†

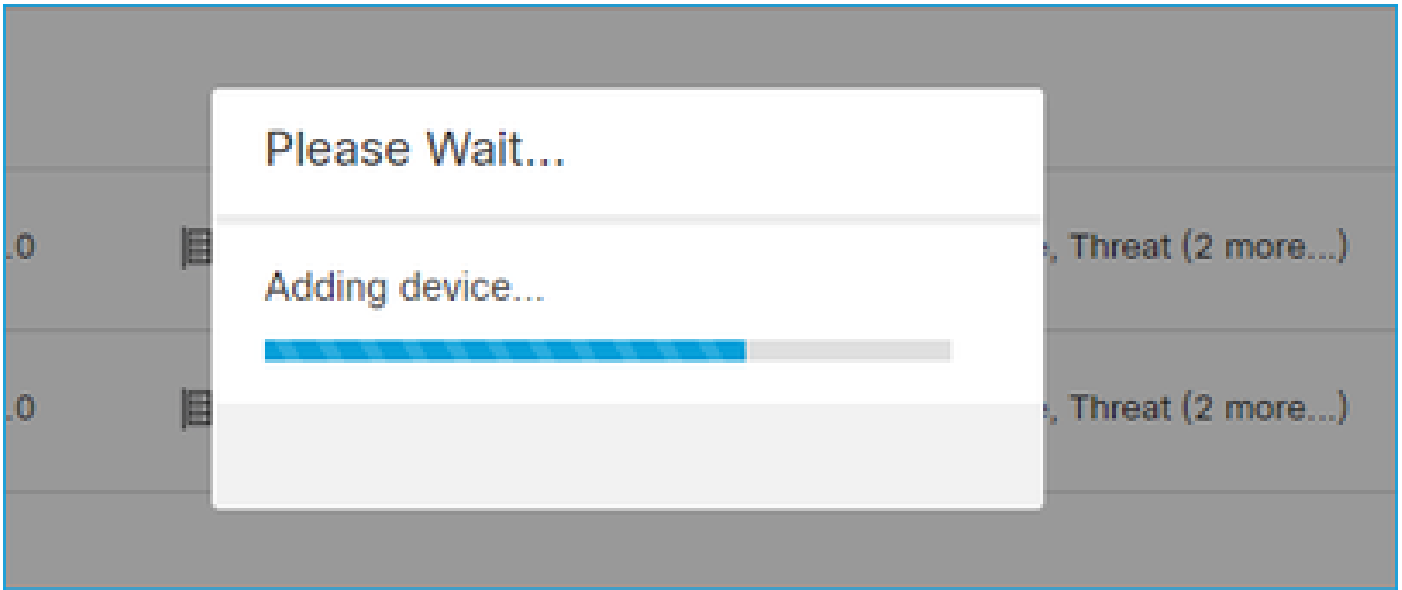
- Transfer Packets

Cancel

Register

Sélectionner le registre

La procédure d'enregistrement commence :



Le FMC commence à écouter sur le port TCP 8305 :

```
<#root>
```

```
admin@FMC2000-2:~$
```

```
netstat -na | grep 8305
```

```
tcp        0      0 10.62.148.75:
```

```
8305
```

```
0.0.0.0:*
```

```
LISTEN
```

En arrière-plan, le FMC initie une connexion TCP :

```
<#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, option
20:16:08.342953 IP 10.62.148.42.8305 > 10.62.148.75.50693: Flags [.] , ack 164, win 235, options [nop,nop,
```

Le canal de contrôle sftunnel est établi :

```
<#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 '10.62.148.75'

Peer channel Channel-B is not valid

Après quelques minutes, le canal Event est établi. L'initiateur du canal d'événement peut être de chaque côté. Dans cet exemple, il s'agissait du 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, option

Le port source aléatoire indique l'initiateur de la connexion :

<#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
```

Dans le cas où le canal Event a été initié par le FTD, le résultat est :

<#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
```

Du côté du FTD :

<#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 '10.62.148.75'
Peer channel Channel-B is valid type (EVENT), using 'eth0', connected to '10.62.148.75' via '10.62.148.75'

<#root>

>

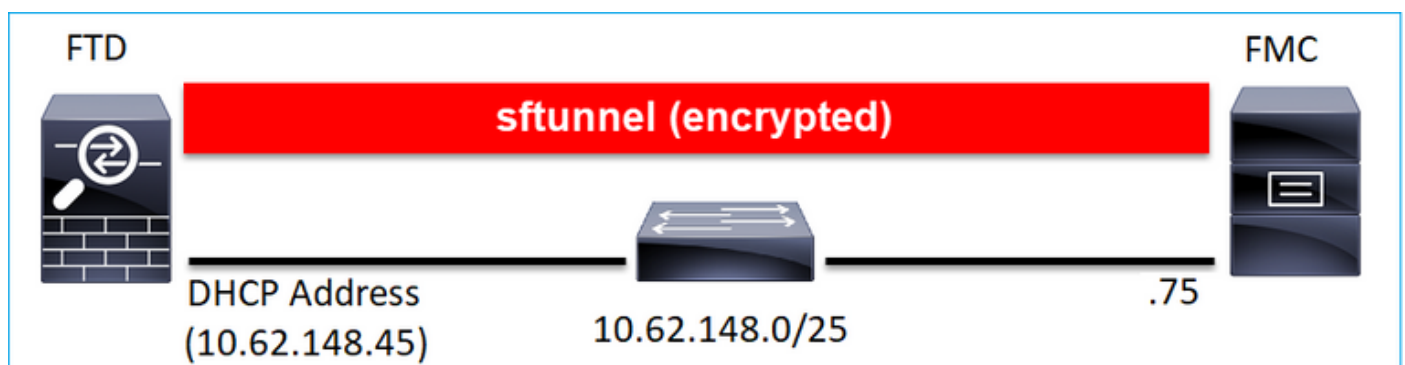
show managers

Type : Manager
Host : 10.62.148.75
Registration : Completed

>

Scénario 2. Adresse IP DHCP FTD - Adresse IP statique FMC

Dans ce scénario, l'interface de gestion FTD a obtenu son adresse IP d'un serveur DHCP :



CLI FTD

Vous devez spécifier l'ID NAT :

> configure manager add <IP statique FMC> <Clé d'enregistrement> <ID NAT>

Exemple :


```
<#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.

```
>
```

État de l'enregistrement FTD :

```
<#root>
```

```
>
```

```
show managers
```

```
Host : 10.62.148.75
```

```
Registration Key : ****
```

```
Registration : pending
```

```
RPC Status :
```

```
Type : Manager
```

```
Host : 10.62.148.75
```

```
Registration : Pending
```

Interface utilisateur FMC

Dans ce cas, spécifiez les éléments suivants :

- Nom d'affichage
- Clé d'enregistrement (elle doit correspondre à celle configurée sur le FTD)
- Politique de contrôle d'accès
- Domaine
- Informations sur les licences Smart
- ID NAT (requis lorsque Host n'est pas spécifié. Il doit correspondre à celui configuré sur FTD)

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

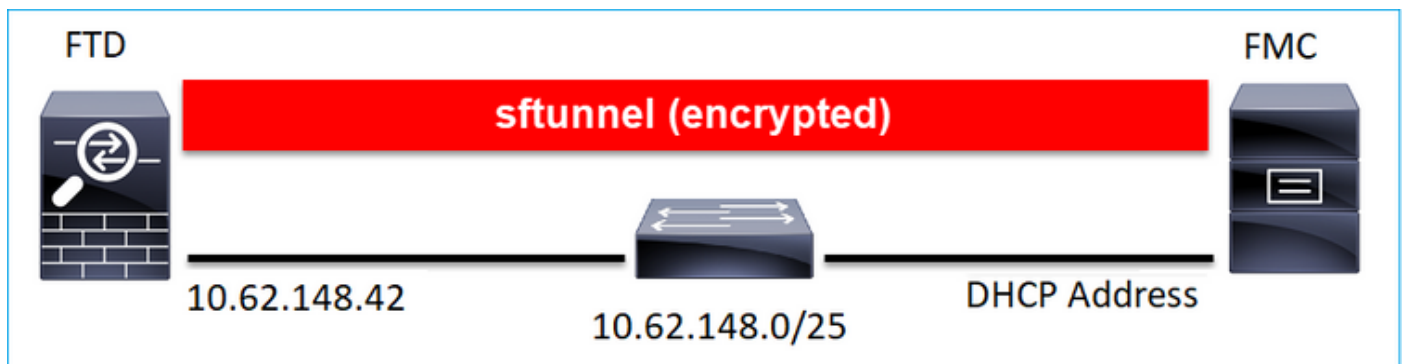
Transfer Packets

Qui initie le sftunnel dans ce cas ?

Le FTD initie les deux connexions de canal :

```
<#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
```

Scénario 3. Adresse IP statique FTD - Adresse IP DHCP FMC



```
<#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.
```

```
>
```

 Remarque : avec DONTRESOLVE, l'ID NAT est requis.

Interface utilisateur FMC

Dans ce cas, spécifiez les éléments suivants :

- Adresse IP FTD
- Nom d'affichage
- Clé d'enregistrement (elle doit correspondre à celle configurée sur le FTD)
- Politique de contrôle d'accès
- Domaine
- Informations sur les licences Smart
- ID NAT (il doit correspondre à celui configuré sur 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

Malware

Threat

URL Filtering

Advanced

Unique NAT ID:†

nat123

Transfer Packets

- Le FMC lance le canal de contrôle.
- Le canal d'événement peut être initié par l'un ou l'autre côté.

<#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

```

Scénario 4 . Inscription FTD auprès de FMC HA

Sur FTD, configurez uniquement le FMC actif :

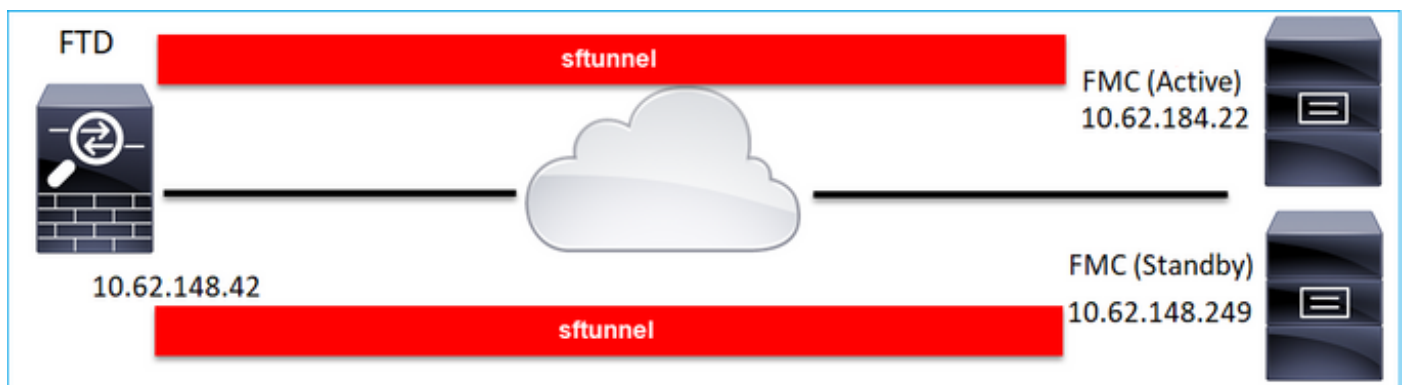
<#root>


>

```
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.



 Remarque : assurez-vous que le trafic du port TCP 8305 est autorisé du FTD vers les deux FMC.

Tout d'abord, le sftunnel vers le FMC actif est établi :

```
<#root>
```

```
>
```

```
show managers
```

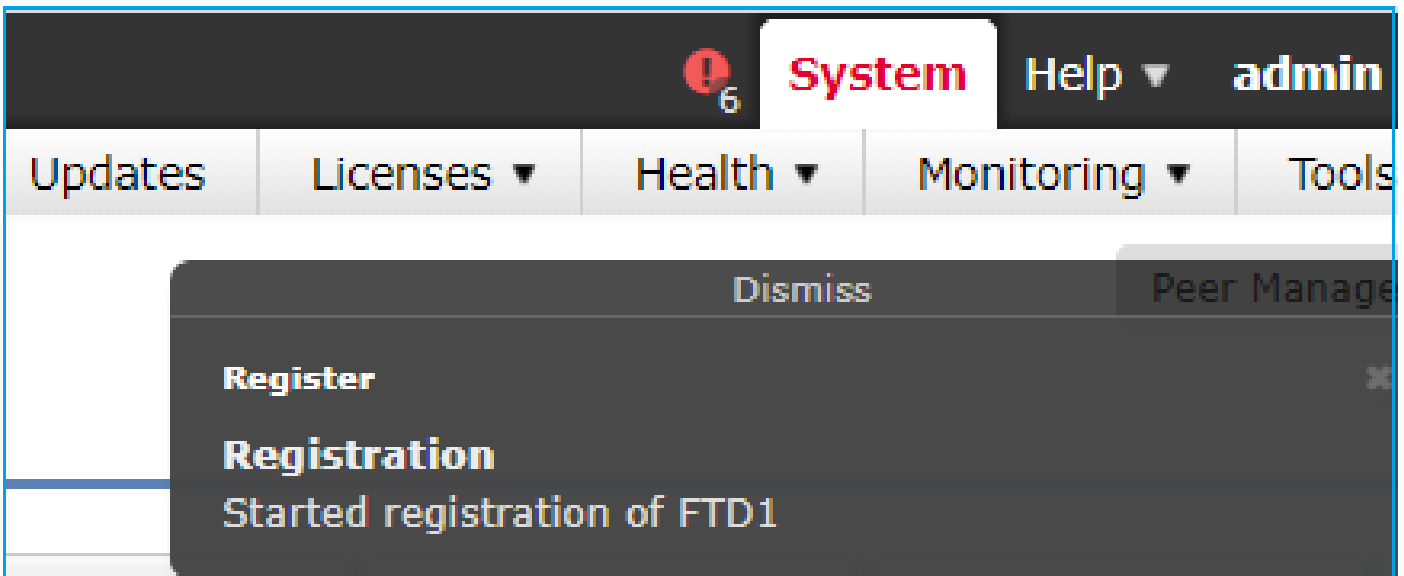
```
Type : Manager
```

```
Host :
```

```
10.62.184.22
```

```
Registration : Completed
```

Après quelques minutes, le FTD commence l'enregistrement auprès du FMC de secours :



```
<#root>
```

```
>
```

```
show managers
```

```
Type : Manager
```

```
Host :
```

```
10.62.184.22
```

```
Registration : Completed
```

Type : Manager
Host :
10.62.148.249
Registration : Completed

Dans le back-end FTD, 2 canaux de contrôle (un pour chaque FMC) et 2 canaux d'événements (un pour chaque FMC) sont établis :

<#root>

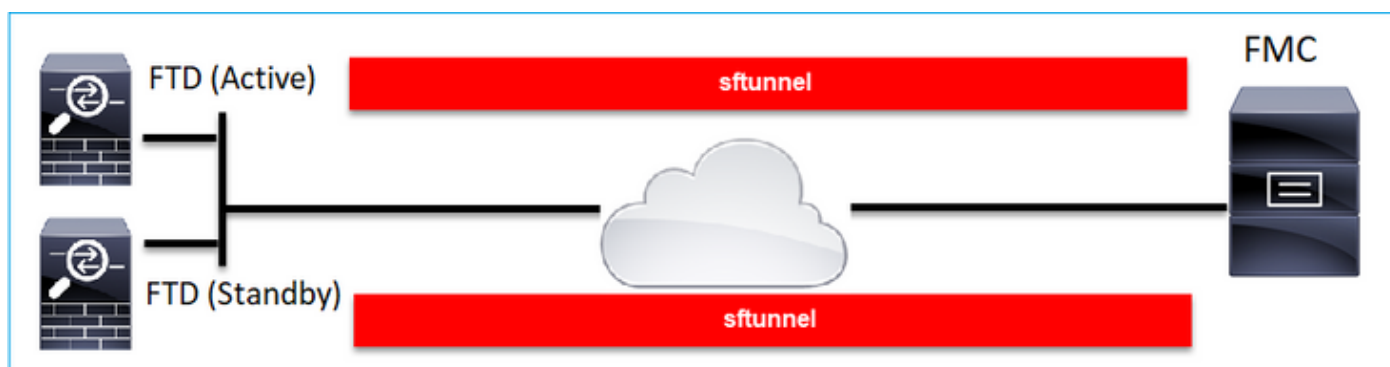
ftd1:/home/admin#

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

Scénario 5. FTD HA

Dans le cas de la haute disponibilité du FTD, chaque unité dispose d'un tunnel distinct vers le FMC :

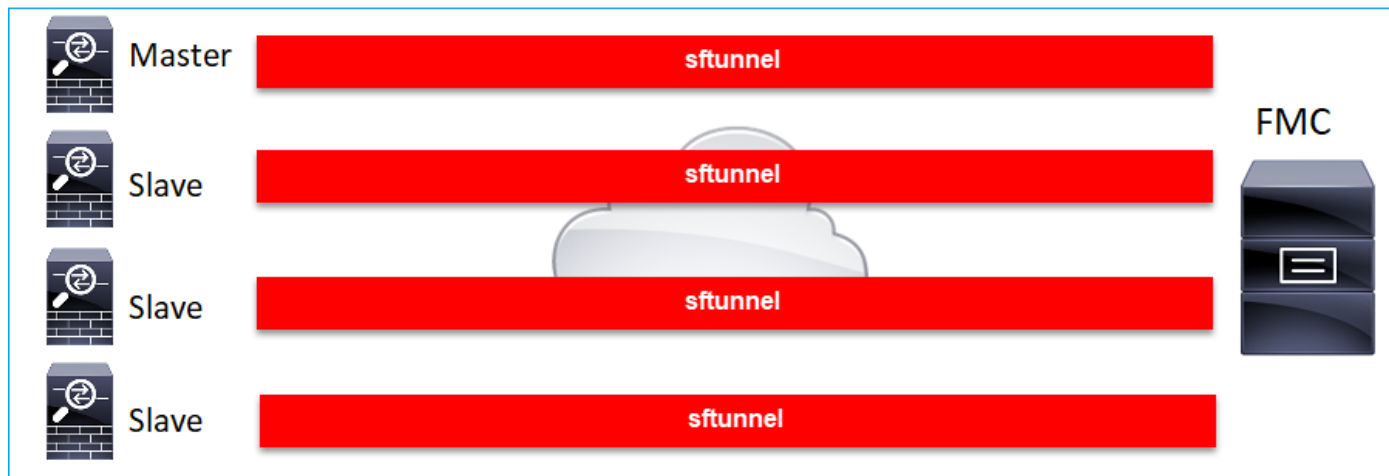



Vous enregistrez les deux FTD indépendamment, puis à partir du FMC, vous formez la FTD HA. Pour plus de détails, consultez :

- [Configurer la haute disponibilité FTD sur les appareils Firepower](#)
- [Haute disponibilité pour Firepower Threat Defense](#)

Scénario 6. Cluster FTD

Dans le cas du cluster FTD, chaque unité possède un tunnel distinct vers le FMC. À partir de la version 6.3 de FMC, vous devez uniquement enregistrer l'unité de contrôle FTD auprès de FMC. Ensuite, le FMC s'occupe du reste des unités et les détecte et les enregistre automatiquement.

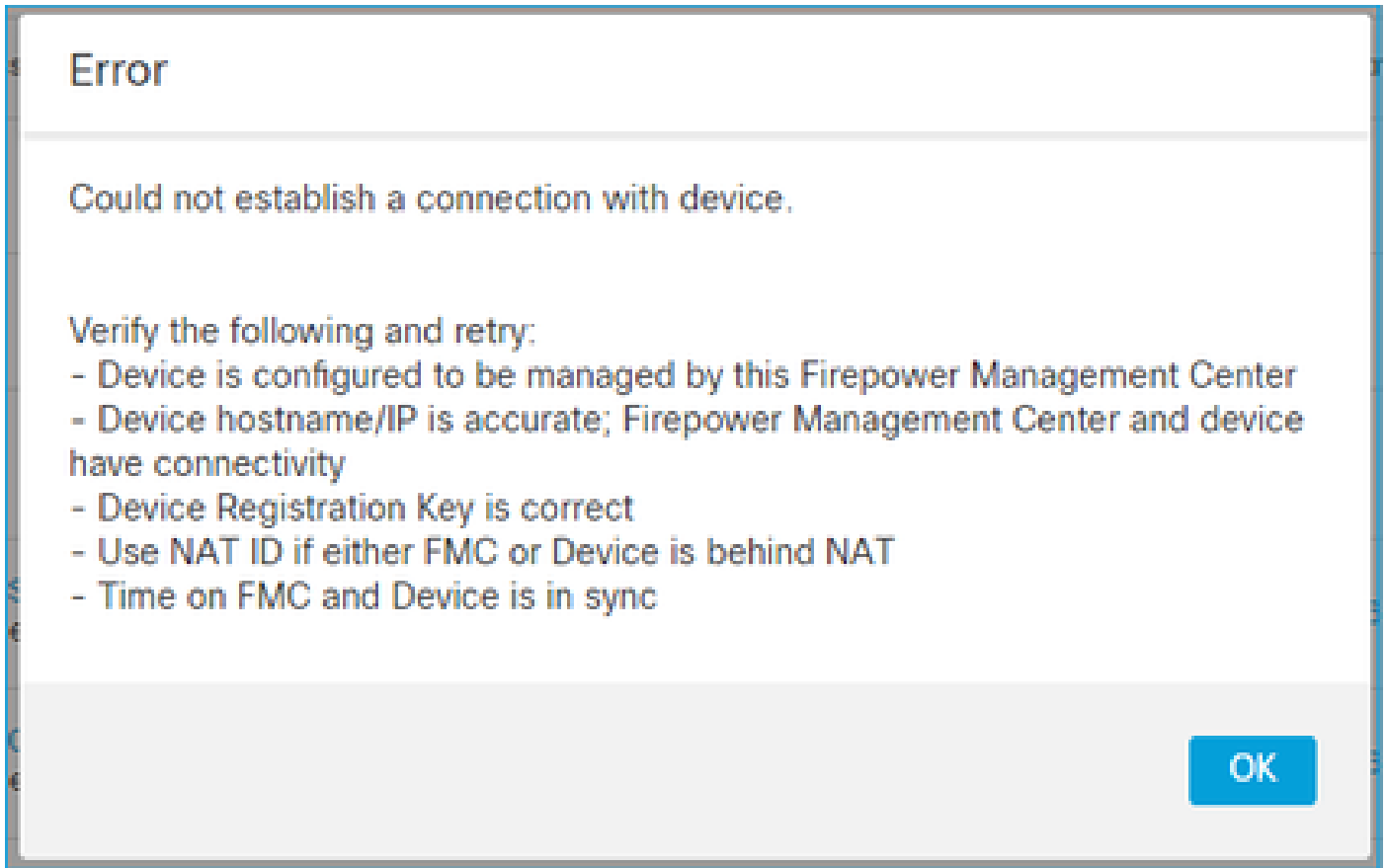


 Remarque : nous vous recommandons d'ajouter l'unité de contrôle pour obtenir les meilleures performances, mais vous pouvez ajouter n'importe quelle unité du cluster. Pour plus d'informations, consultez [Créer un cluster de défense contre les menaces Firepower](#)

Dépannage des problèmes courants

1. Syntaxe incorrecte sur la CLI FTD

En cas de syntaxe incorrecte sur FTD et d'échec de la tentative d'enregistrement, l'interface utilisateur FMC affiche un message d'erreur assez générique :



Dans cette commande, le mot clé key est la clé d'enregistrement tandis que le cisco123 est l'ID NAT. Il est assez courant d'ajouter le mot clé alors que techniquement il n'y a pas de mot clé de ce type :

```
<#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.
```

Action recommandée

Utilisez une syntaxe correcte et n'utilisez pas de mots clés qui n'existent pas.

```
<#root>
```

```
>
```

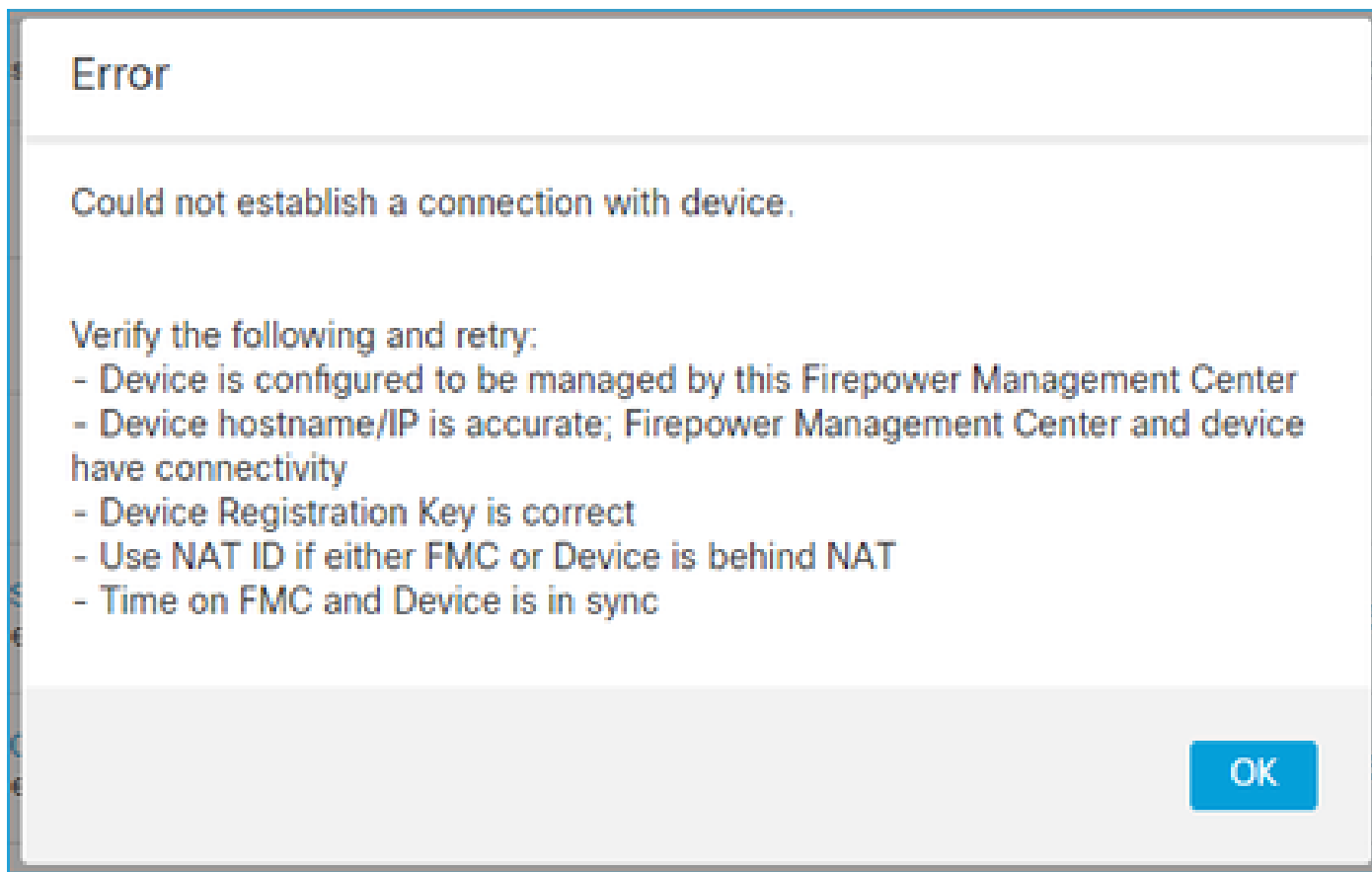
```
configure manager add 10.62.148.75 cisco123
```

```
Manager successfully configured.
```

```
Please make note of reg_key as this will be required while adding Device in FMC.
```

2. Incompatibilité de clé d'enregistrement entre FTD et FMC

L'interface utilisateur FMC affiche :



Action recommandée

Sur FTD, recherchez les problèmes d'authentification dans le fichier `/ngfw/var/log/messages`.

Méthode 1 - Vérifier les journaux précédents

```
<#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] sftunneId:sf_ssl [WARN] Accept:  
Failed to authenticate peer '10.62.148.75' <- The problem
```

Méthode 2 - Vérifier les journaux en direct

```
<#root>
```

```
>
```

```
expert  
ftd1:~$
```

```
sudo su
```

```
Password:  
ftd1:~/home/admin#
```

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

Sur FTD, vérifiez le contenu du fichier /etc/sf/sftunnel.conf pour vous assurer que la clé d'enregistrement est correcte :

```
<#root>
```

```
ftd1:~$
```

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

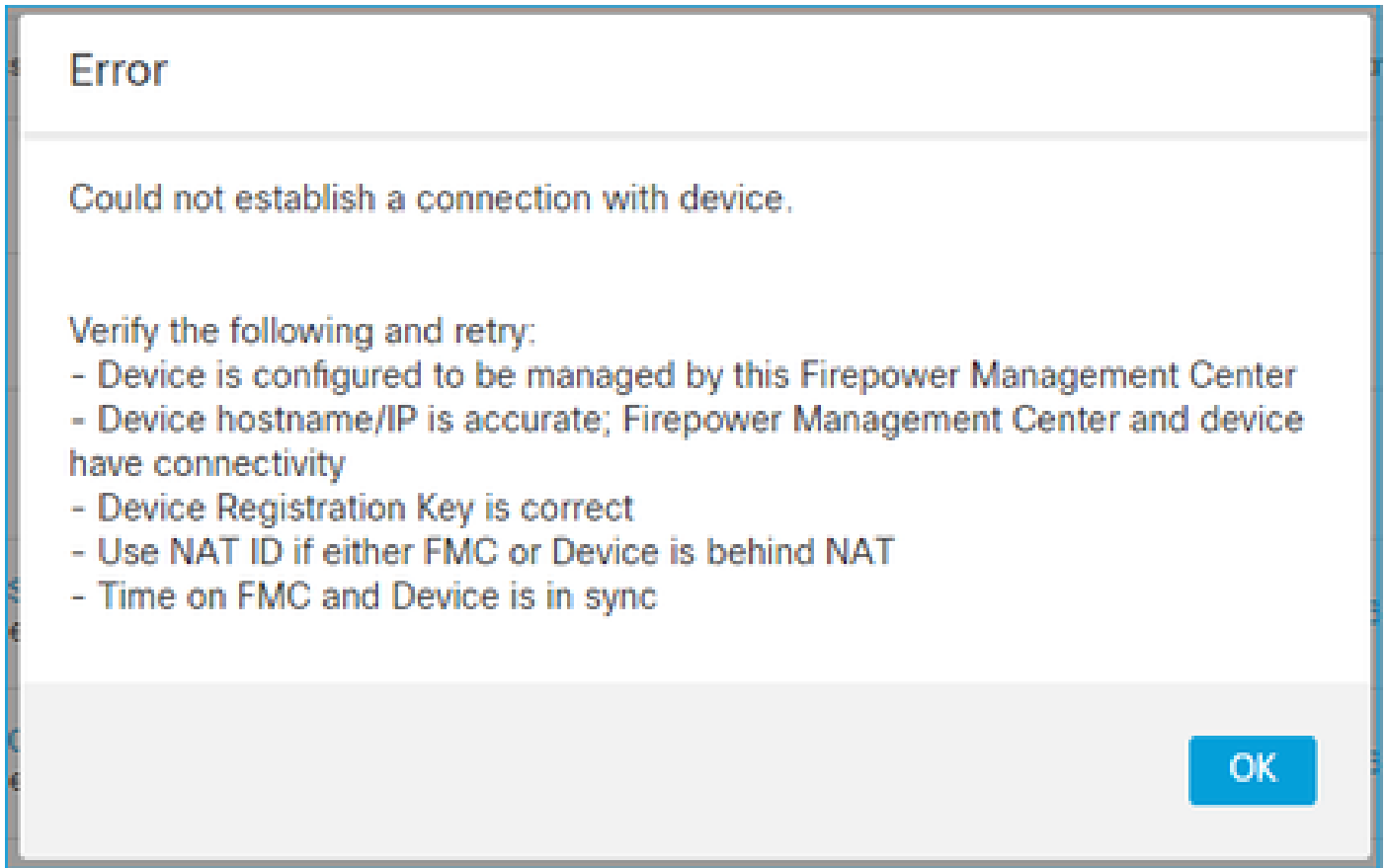
```
    reg_key
```

```
cisco-123
```

```
;
```

3. Problèmes de connectivité entre FTD et FMC

L'interface utilisateur FMC affiche :



Actions recommandées

- Assurez-vous qu'il n'y a aucun périphérique dans le chemin (par exemple, un pare-feu) qui bloque le trafic (TCP 8305). Dans le cas de FMC HA, assurez-vous que le trafic vers le port TCP 8305 est autorisé vers les deux FMC.
- Effectuez des captures pour vérifier la communication bidirectionnelle. Sur FTD, utilisez la commande capture-traffic. Assurez-vous qu'il existe une connexion TCP en trois étapes et qu'aucun paquet TCP FIN ou RST n'est envoyé.

```
<#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
```

De même, effectuez une capture sur FMC pour assurer une communication bidirectionnelle :

```
<#root>
```

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

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

Il est également recommandé d'exporter la capture au format pcap et de vérifier le contenu du paquet :

```
<#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
```

Causes possibles:

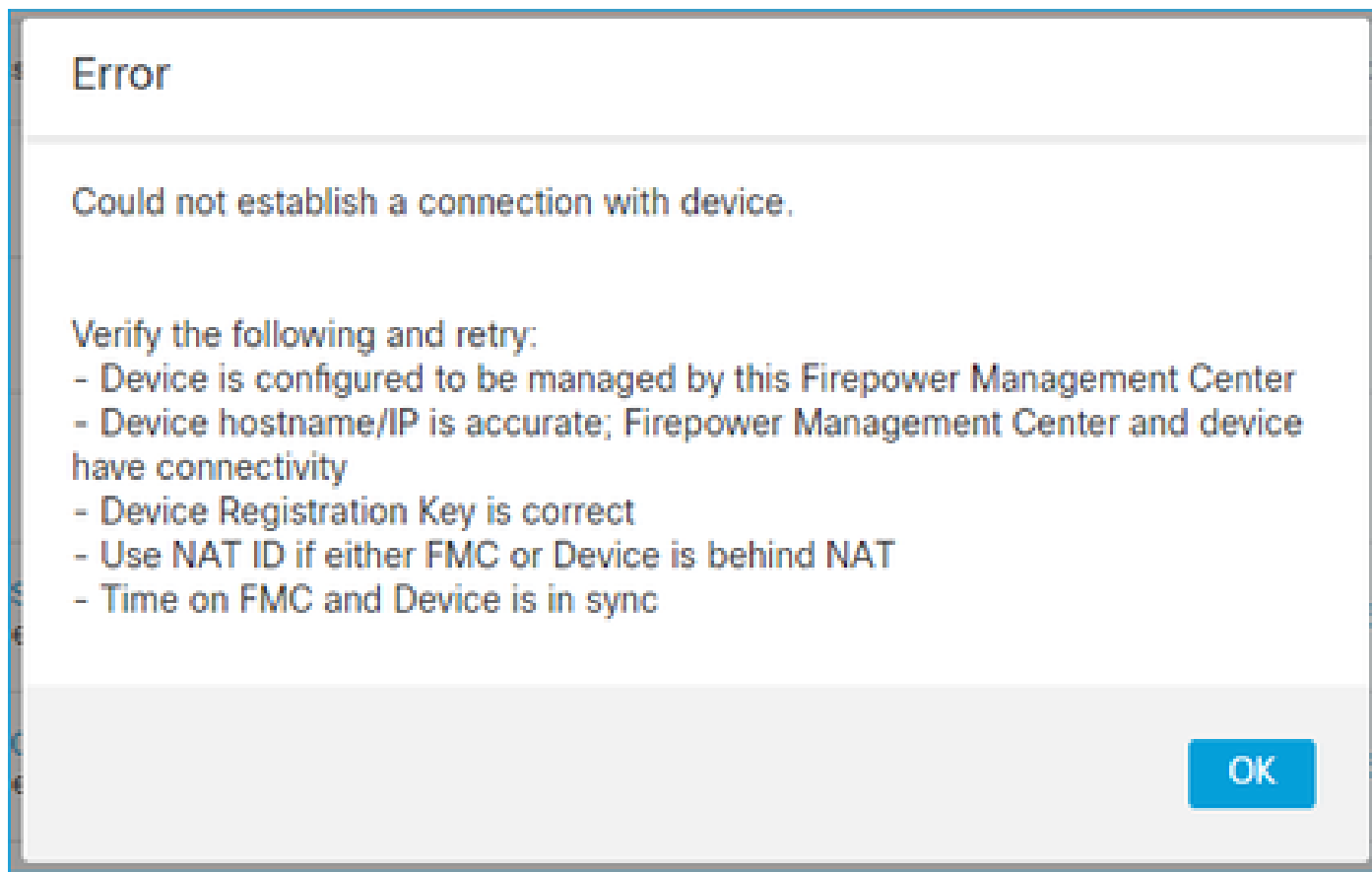
- Le périphérique FTD n'est pas ajouté au FMC.
- Un périphérique dans le chemin (par exemple, un pare-feu) bloque ou modifie le trafic.
- Les paquets ne sont pas acheminés correctement sur le chemin.
- Le processus sftunnel sur FTD ou FMC est arrêté (vérifiez le scénario 6)
- Il y a un problème de MTU dans le chemin (scénario de vérification).

Pour l'analyse de capture, consultez ce document :

[Analysez les captures de pare-feu Firepower pour résoudre efficacement les problèmes de réseau](#)

4. Logiciel incompatible entre FTD et FMC

L'interface utilisateur FMC affiche :



Action recommandée

Vérifiez le fichier FTD /ngfw/var/log/messages :

<#root>

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

Consultez la matrice de compatibilité Firepower :

[Guide de compatibilité Cisco Firepower](#)

5. Différence de temps entre FTD et FMC

La communication FTD-FMC est sensible aux différences de temps entre les deux périphériques. Il est impératif de synchroniser FTD et FMC par le même serveur NTP.

Plus précisément, lorsque le FTD est installé sur une plate-forme telle que 41xx ou 93xx, il prend ses paramètres de temps du châssis parent (FXOS).

Action recommandée

Assurez-vous que le gestionnaire de châssis (FCM) et le FMC utilisent la même source de temps (serveur NTP)

6. sftunnel Process Down ou Disabled

Sur FTD, le processus sftunnel gère le processus d'enregistrement. Il s'agit de l'état du processus avant la configuration du gestionnaire :

```
<#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,sfmbsevice,sfipproxy  
CGroups: memory=System/ProcessHigh
```

État de l'inscription :


```
<#root>
```

```
>
```

```
show managers
```

```
No managers configured.
```

Configurez le gestionnaire :

```
<#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.
```

Maintenant, le processus est 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,sfmbsservice,sfiproxy
```

```
CGroups: memory=System/ProcessHigh(enrolled)
```

Dans de rares cas, le processus peut être arrêté ou désactivé :

```
<#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,sfmbsservice,sfiproxy
```

```
CGroups: memory=System/ProcessHigh
```

L'état du manager semble normal :

```
<#root>
```

```
>
```

```
show managers
```

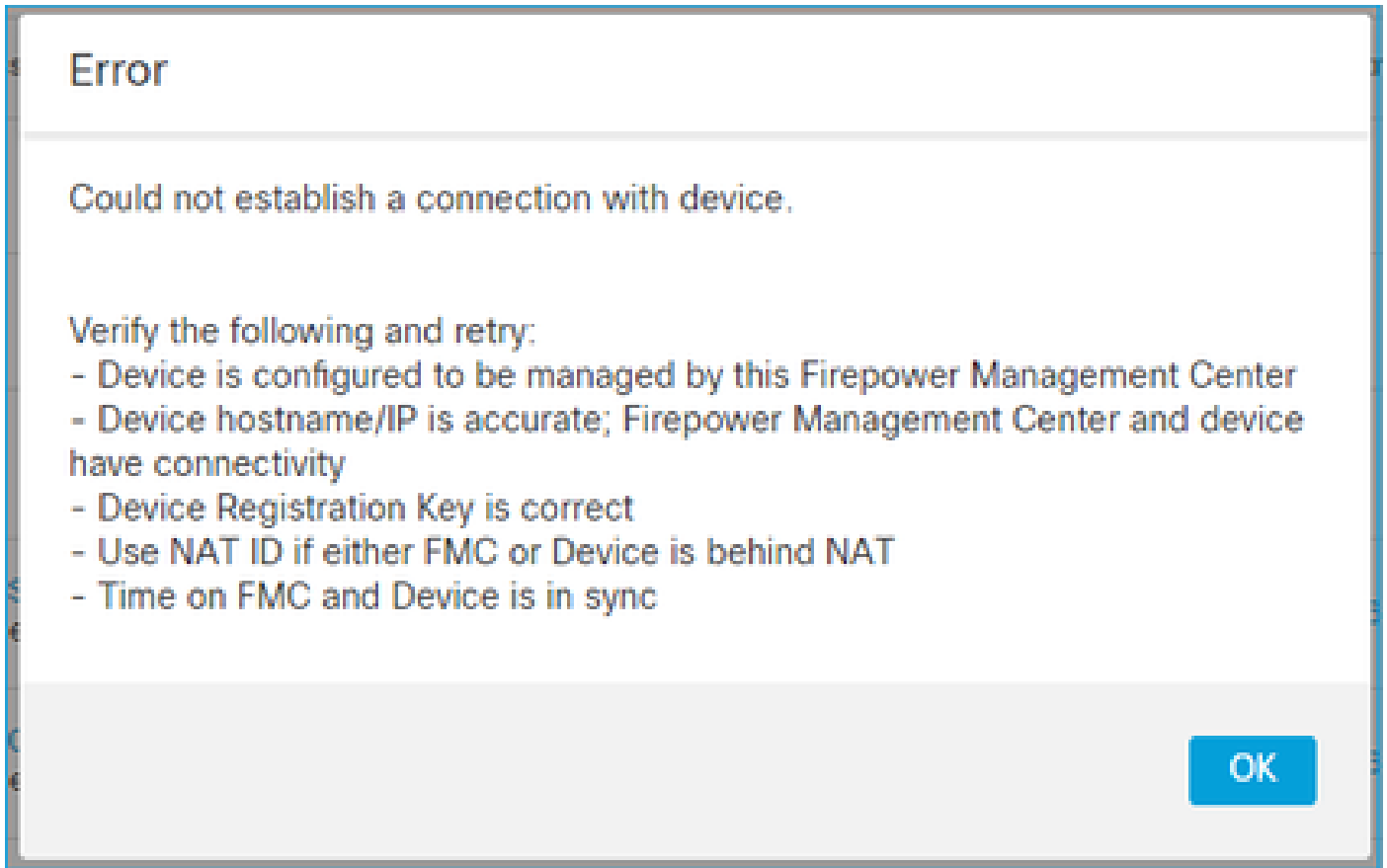
```
Host : 10.62.148.75
```

```
Registration Key : ****
```

```
Registration : pending
```

```
RPC Status :
```

D'un autre côté, l'enregistrement du périphérique échoue :



Sur FTD, aucun message associé n'est affiché dans `/ngfw/var/log/messages`

Action recommandée

Collecter le fichier de dépannage FTD et contacter le TAC Cisco


7. FTD Enregistrement en attente sur le FMC secondaire

Dans certains cas, après l'enregistrement FTD initial dans une configuration FMC HA, le périphérique FTD n'est pas ajouté au FMC secondaire.

Action recommandée

Suivez la procédure décrite dans ce document :

[Utiliser l'interface CLI pour résoudre l'enregistrement des périphériques dans Firepower Management Center High Availability](#)

 **Avertissement** : cette procédure est intrusive car elle contient une annulation de l'enregistrement d'un périphérique. Cela affecte la configuration du périphérique FTD (il est supprimé). Il est recommandé d'utiliser cette procédure uniquement pendant l'enregistrement et la configuration initiaux du FTD. Dans d'autres cas, collectez les fichiers

 de dépannage FTD et FMC et contactez le TAC Cisco.

8. Échec de l'enregistrement en raison de Path MTU

Il existe des scénarios dans Cisco TAC où le trafic sftunnel doit traverser une liaison qui a un petit MTU. Les paquets sftunnel ont le bit Don't fragment Set ainsi la fragmentation n'est pas autorisée :

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

De plus, dans les fichiers /ngfw/var/log/messages, vous pouvez voir un message comme ceci :

```
MSGs: 10-09 14:41:11 ftd1 SF-IMS[7428]: [6612] sftunneld:sf_ssl [ERREUR] Connect:échec de la connexion SSL
```

Action recommandée

Pour vérifier s'il y a une perte de paquets due à la fragmentation, effectuez des captures sur FTD, FMC et, idéalement, sur les périphériques sur le chemin. Vérifiez si vous voyez des paquets qui arrivent aux deux extrémités.

Sur FTD, diminuez la MTU sur l'interface de gestion FTD. La valeur par défaut est 1 500 octets. MAX est 1500 pour l'interface de gestion et 9000 pour l'interface d'évènements. La commande a été ajoutée dans la version FTD 6.6.

[Référence des commandes Cisco Firepower Threat Defense](#)

Exemple

```
<#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'
```

Vérification

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

Pour vérifier le MTU du chemin à partir du FTD, vous pouvez utiliser cette commande :

```
<#root>
```

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

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

L'option do définit le bit don't fragment dans les paquets ICMP. En outre, lorsque vous spécifiez 1472, le périphérique envoie 1 500 octets : (en-tête IP = 20 octets) + (en-tête ICMP = 8 octets) + (données ICMP de 1 472 octets)

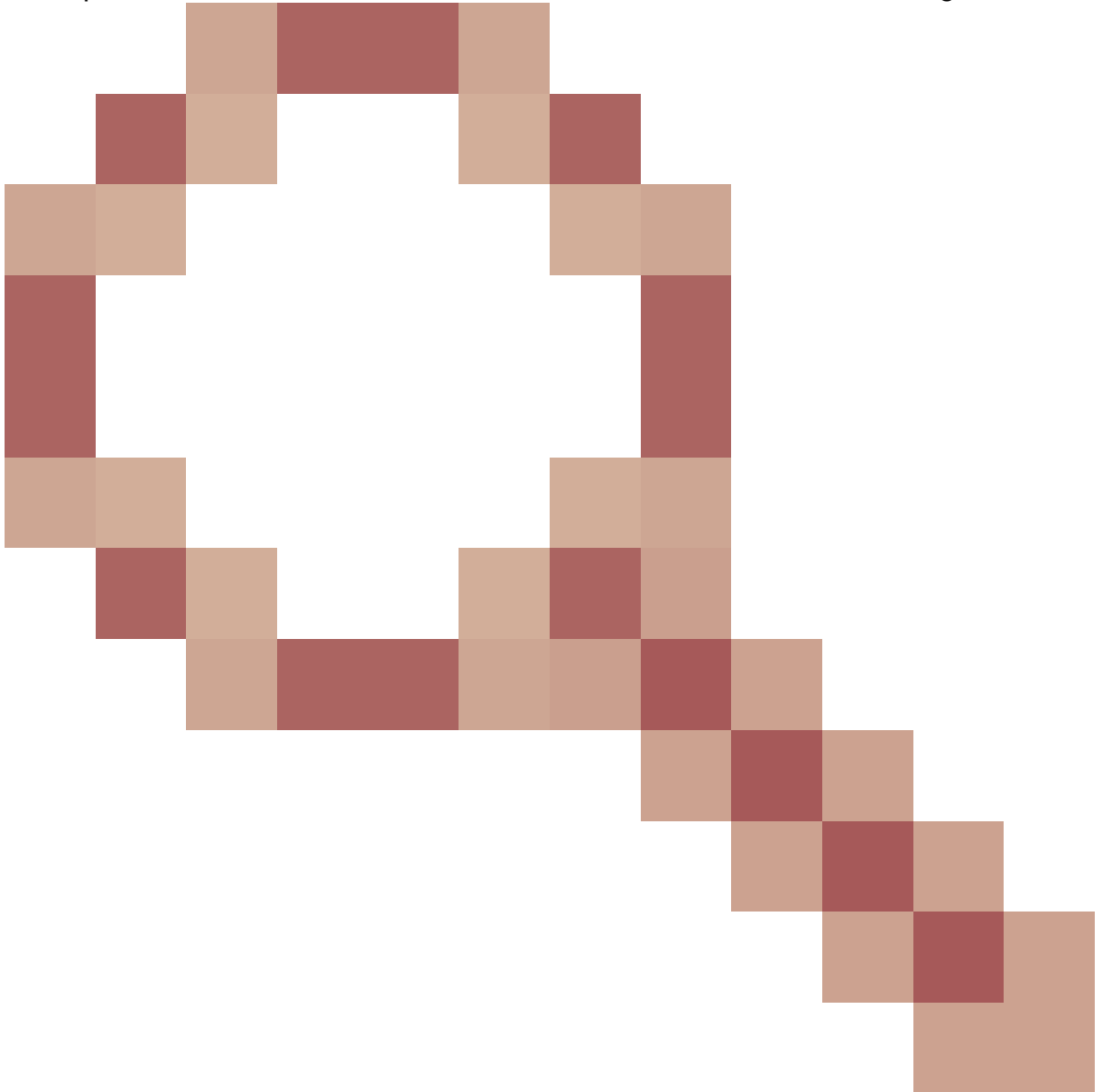
Sur FMC, abaissez la valeur MTU sur l'interface de gestion FMC comme décrit dans ce document

:

[Configuration des interfaces de gestion Firepower Management Center](#)

9. L'enregistrement du FTD est annulé après un changement de bootstrap de l'interface utilisateur du gestionnaire de châssis

Ceci s'applique aux plates-formes FP41xx et FP93xx et est documenté dans l'ID de bogue Cisco



[CSCvn45138](#)

En règle générale, vous ne devez pas effectuer de modifications de bootstrap à partir du gestionnaire de châssis (FCM), sauf si vous effectuez une reprise après sinistre.

Action recommandée

Si vous avez effectué une modification de bootstrap et que vous avez répondu à la condition (la communication FTD-FMC est interrompue pendant que le FTD est activé après la modification de bootstrap), vous devez supprimer et enregistrer à nouveau le FTD dans FMC.

10. Le FTD perd l'accès au FMC en raison des messages de redirection ICMP

Ce problème peut affecter le processus d'enregistrement ou interrompre la communication FTD-FMC après l'enregistrement.

Le problème dans ce cas est un périphérique réseau qui envoie des messages ICMP Redirect à l'interface de gestion FTD et la communication FTD-FMC trous noirs.

Comment identifier ce problème ?

Dans ce cas, l'adresse 10.100.1.1 est l'adresse IP FMC. Sur FTD, il y a une route mise en cache en raison du message de redirection ICMP qui a été reçu par le FTD sur l'interface de gestion :

```
<#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
```

Action recommandée

Étape 1

Désactivez la redirection ICMP sur le périphérique qui l'envoie (par exemple, commutateur L3 en

amont, routeur, etc.).

Étape 2

Effacez le cache de routage FTD de l'interface de ligne de commande FTD :

```
<#root>
```

```
ftd1:/ngfw/var/common#
```

```
ip route flush 10.100.1.1
```

Lorsqu'il n'est pas redirigé, il ressemble à ceci :

```
<#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
```

Références

- [Comprendre les messages de redirection ICMP](#)
- ID de bogue Cisco [CSCvm53282](#) FTD : les tables de routage ajoutées par les redirections ICMP sont bloquées définitivement dans le cache de la table de routage

Informations connexes

- [Guides de configuration du pare-feu](#)

À propos de cette traduction

Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.