

Configuración, verificación y resolución de problemas del registro de dispositivos Firepower

Contenido

[Introducción](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Antecedentes](#)

[Opciones de diseño](#)

[¿Qué información se intercambia a través del sftunnel?](#)

[¿Qué protocolo/puerto utiliza el sftunnel?](#)

[¿Cómo se cambia el puerto TCP de Sftunnel en FTD?](#)

[¿Cuántas conexiones establece el sftunnel?](#)

[¿Qué dispositivo inicia cada canal?](#)

[Configurar](#)

[Fundamentos del registro](#)

[Escenario 1. Dirección IP estática FMC y FTD](#)

[Situación hipotética 2. Dirección IP DHCP FTD - Dirección IP estática FMC](#)

[Situación hipotética 3. Dirección IP estática FTD - Dirección IP DHCP FMC](#)

[Situación hipotética 4. Registro FTD en FMC HA](#)

[Situación hipotética 5. FTD HA](#)

[Situación hipotética 6. Clúster FTD](#)

[Solucionar problemas comunes](#)

[1. Sintaxis no válida en FTD CLI](#)

[2. Discordancia de clave de registro entre FTD - FMC](#)

[3. Problemas de conectividad entre FTD - FMC](#)

[4. SW incompatible entre FTD y FMC](#)

[5. Diferencia de tiempo entre FTD y FMC](#)

[6. Proceso sftunnel inactivo o inhabilitado](#)

[7. FTD pendiente de registro en el CSP secundario](#)

[8. El registro falla debido a la MTU de la ruta](#)

[9. El FTD deja de estar registrado después de un cambio de bootstrap desde la IU del administrador de chasis](#)

[10. El FTD pierde el acceso al FMC debido a los mensajes de redirección ICMP](#)

Introducción

Este documento describe los procedimientos de solución de problemas de la conexión entre Firepower Threat Defence (FTD) y Firepower Management Center (FMC).

Prerequisites

Requirements

No hay requisitos específicos para este documento.

Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- Software FTD 6.6.x y 6.5.x
- Software FMC 6.6.x

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Antecedentes

En este documento se describen los procedimientos de funcionamiento, verificación y solución de problemas de la conexión (sftunnel) entre un FTD gestionado y el FMC gestionado.

La información y los ejemplos se basan en el FTD, pero la mayoría de los conceptos también son totalmente aplicables a NGIPS (appliances de las series 7000/8000) o a un módulo FirePOWER en ASA55xx.

Un FTD admite dos modos de gestión principales:

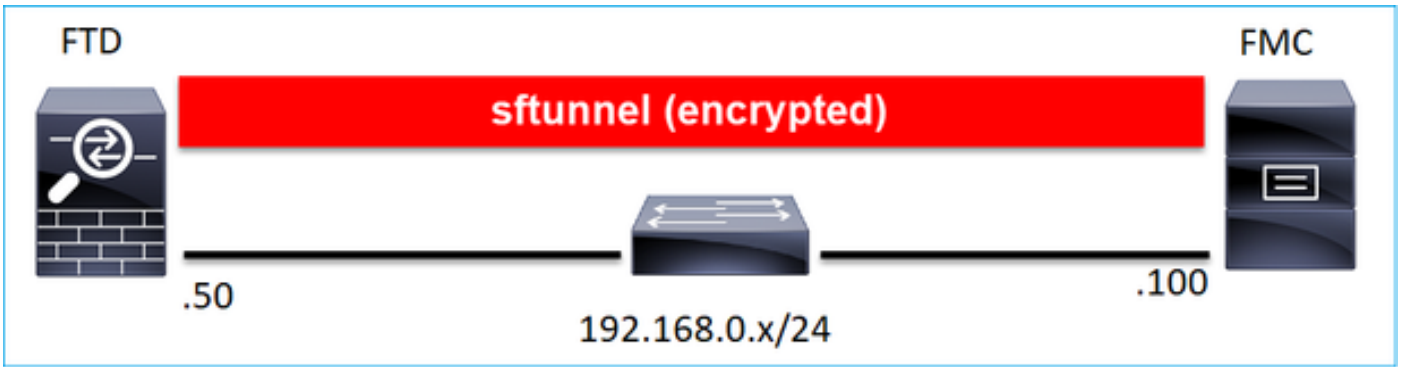
- Off-box a través de FMC, también conocido como gestión remota
- Integrado mediante Firepower Device Manager (FDM) o Cisco Defense Orchestrator (CDO), también conocido como gestión local

En el caso de la gestión remota, el FTD debe registrarse primero en el FMC que utilice un proceso conocido como registro de dispositivos.

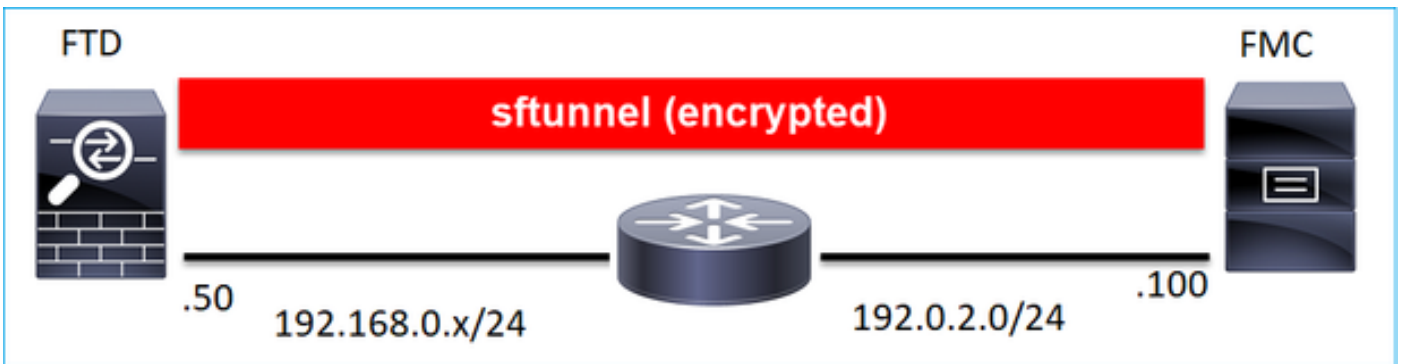
Una vez realizado el registro, el FTD y el FMC establecen un túnel seguro denominado sftunnel (el nombre deriva del túnel de Sourcefire).

Opciones de diseño


Desde el punto de vista del diseño, el FTD - FMC puede estar en la misma subred L3:

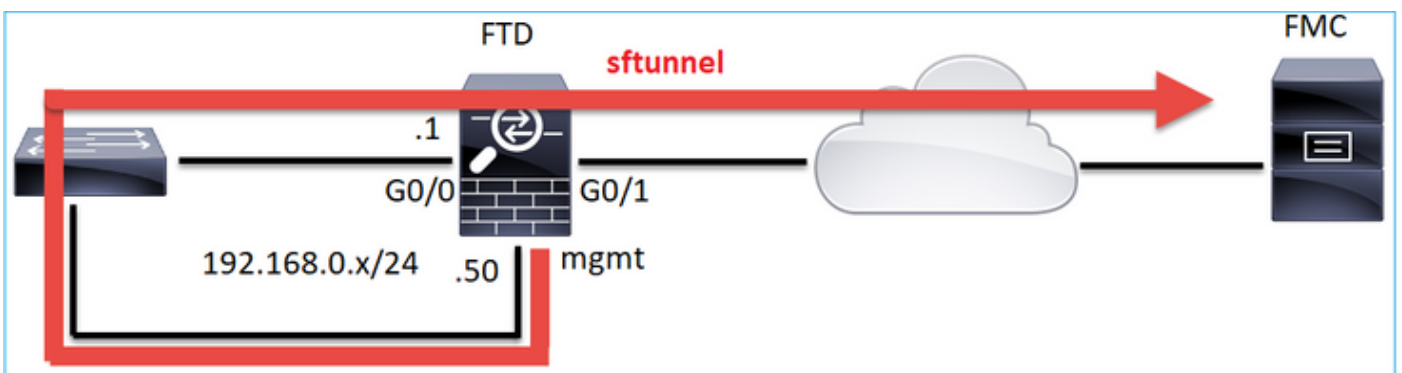


o estar separados por diferentes redes:



192.0.2.0

 Nota: El sftunnel también puede pasar a través del FTD. Este diseño no se recomienda. El motivo es que un problema de plano de datos del FTD puede interrumpir la comunicación entre el FTD y el FMC.



¿Qué información se intercambia a través del sftunnel?

Esta lista contiene la mayor parte de la información que se transporta a través del sftunnel:

- Latido del dispositivo (keepalives)
- Sincronización horaria (NTP)
- Eventos (conexión, intrusión/IPS, archivo, SSL, etc.)
- Búsquedas de malware
- Alertas/eventos de estado
- Información de usuario y grupo (para políticas de identidad)
- información de estado de FTD HA
- Información de estado de clúster de FTD
- Información/eventos de inteligencia de seguridad (SI)
- Información/eventos de Threat Intelligence Director (TID)
- Archivos capturados
- Eventos de descubrimiento de red
- Paquete de políticas (implementación de políticas)
- Paquetes de actualización de software
- Paquetes de parches de software
- VDB
- SRU

¿Qué protocolo/puerto utiliza el sftunnel?

El sftunnel utiliza el puerto TCP 8305. En el backend es un túnel 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	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


¿Cómo se cambia el puerto TCP de Sftunnel en FTD?

```
<#root>
```

```
>
```

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

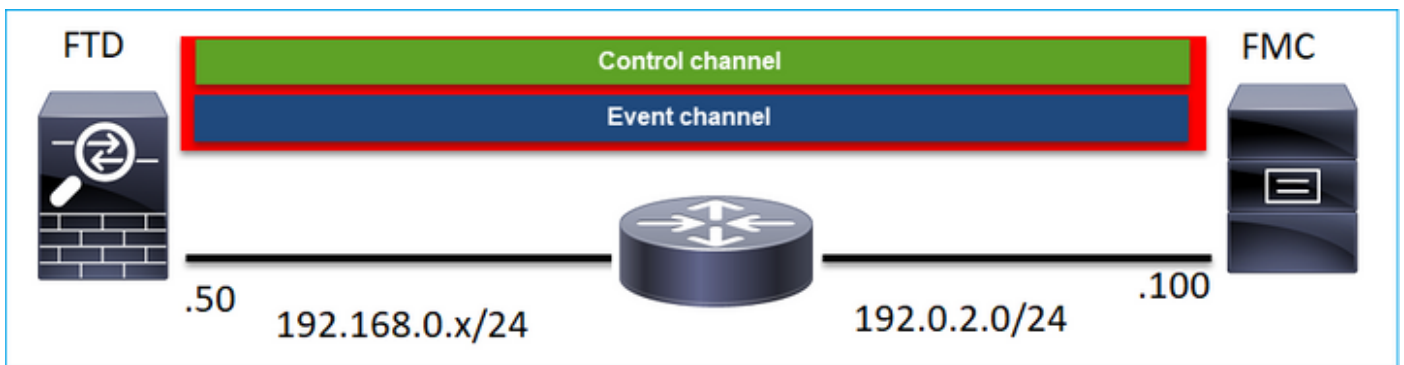
```
Management port changed to 8306.
```

 Nota: En este caso, también debe cambiar el puerto en FMC (Configuración > Interfaces de gestión > Configuración compartida). Esto afecta a todos los demás dispositivos que ya están registrados en el mismo FMC. Cisco recomienda encarecidamente mantener los parámetros predeterminados del puerto de administración remota, pero si el puerto de administración entra en conflicto con otras comunicaciones de la red, puede elegir un puerto diferente. Si cambia el puerto de gestión, debe cambiarlo para todos los dispositivos de la implementación que necesiten comunicarse entre sí.

¿Cuántas conexiones establece el sftunnel?

El sftunnel establece 2 conexiones (canales):

- Canal de control
- Canal de eventos



¿Qué dispositivo inicia cada canal?

Depende del escenario. Compruebe los escenarios descritos en el resto del documento.

Configurar

Fundamentos del registro

CLI FTD

En FTD, la sintaxis básica para el registro de dispositivos es:

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

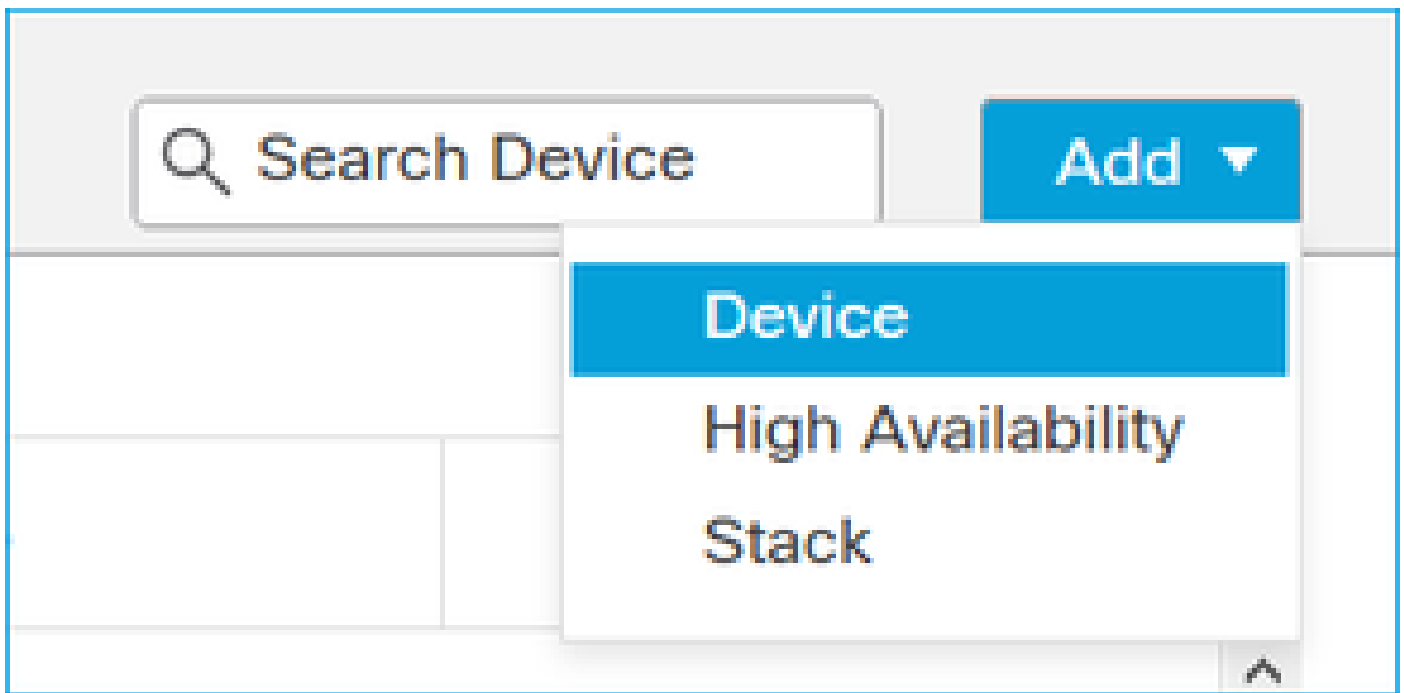
Valor	Descripción
-------	-------------

Host FMC	<p>Puede ser:</p> <ul style="list-style-type: none"> • Hostname • dirección ipv4 • dirección ipv6 • DONTRESOLVE
Clave de registro	<p>Se trata de una cadena alfanumérica secreta compartida (entre 2 y 36 caracteres) que se utiliza para el registro del dispositivo. Sólo se permiten caracteres alfanuméricos, guiones (-), guiones bajos (_) y puntos (.).</p>
ID de NAT	<p>Cadena alfanumérica utilizada durante el proceso de registro entre el CSP y el dispositivo cuando un lado no especifica una dirección IP. Especifique el mismo ID de NAT en el FMC.</p>

Para obtener más información, consulte la [Referencia de comandos de Cisco Firepower Threat Defence](#)

IU de FMC

En FMC, vaya a Devices > Device Management . Seleccione Agregar > Dispositivo



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 <FMC Static IP> <Registration Key>

Por ejemplo:

```
<#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.
```

Información de fondo

Tan pronto como ingrese el comando FTD, el FTD intenta conectarse al FMC cada 20 segundos, pero dado que el FMC aún no está configurado, responde con 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
```

Estado de registro del dispositivo:

```
<#root>
```

```
>
```

```
show managers
```

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

El FTD escucha en el puerto TCP 8305:

```
<#root>
```

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

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

```
tcp        0      0 10.62.148.42:
```

```
8305
```

```
0.0.0.0:*
```

```
LISTEN
```

IU de FMC

En este caso, especifique lo siguiente:

- Host (dirección IP del FTD)
- Mostrar nombre:
- Clave de registro (debe coincidir con la configurada en FTD)
- Política de control de acceso
- Dominio
- Información de Smart Licensing

Add Device

Host:†

Display Name:

Registration Key:*

Domain:

Group:

Access Control Policy:*

Smart Licensing

- Malware
- Threat
- URL Filtering

Advanced

Unique NAT ID:†

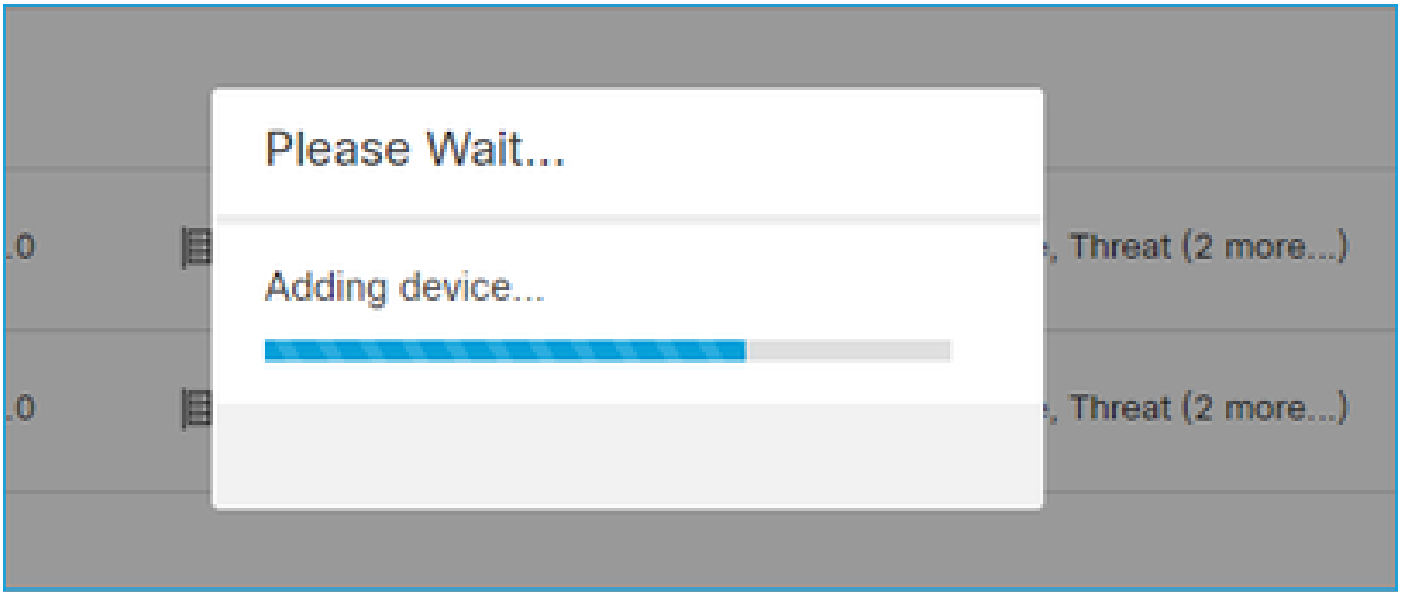
- Transfer Packets

Cancel

Register

Seleccione Registrar

Se inicia el proceso de registro:



El FMC comienza a escuchar en el puerto TCP 8305:

```
<#root>
```

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

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

```
tcp        0      0 10.62.148.75:
```

```
8305
```

```
0.0.0.0:*
```

```
LISTEN
```

En segundo plano, el FMC inicia una conexión 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, optio
20:16:08.342953 IP 10.62.148.42.8305 > 10.62.148.75.50693: Flags [.]
```

Se establece el canal de control sftunnel:

```
<#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

Después de unos minutos se establece el canal de eventos. El iniciador del canal de eventos puede ser cualquiera de los lados. En este ejemplo, fue el CSP:

<#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

El puerto de origen aleatorio denota el iniciador de la conexión:

<#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
```

En caso de que el canal de eventos haya sido iniciado por el FTD, el resultado es:

```
<#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
```

Desde el lado del 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

>

Situación hipotética 2. Dirección IP DHCP FTD - Dirección IP estática FMC

En este escenario, la interfaz de administración de FTD obtuvo su dirección IP de un servidor DHCP:



CLI FTD

Debe especificar el ID de NAT:

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

Por ejemplo:

```
<#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.

```
>
```

Estado de registro de FTD:

```
<#root>
```

```
>
```

```
show managers
```

```
Host : 10.62.148.75
```

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

```
Registration : pending
```

```
RPC Status :
```

```
Type : Manager
```

```
Host : 10.62.148.75
```

```
Registration : Pending
```

IU de FMC

En este caso, especifique lo siguiente:

- Mostrar nombre:
- Clave de registro (debe coincidir con la configurada en FTD)
- Política de control de acceso
- Dominio
- Información de Smart Licensing
- ID de NAT (obligatorio cuando no se especifica Host). Debe coincidir con el configurado en 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

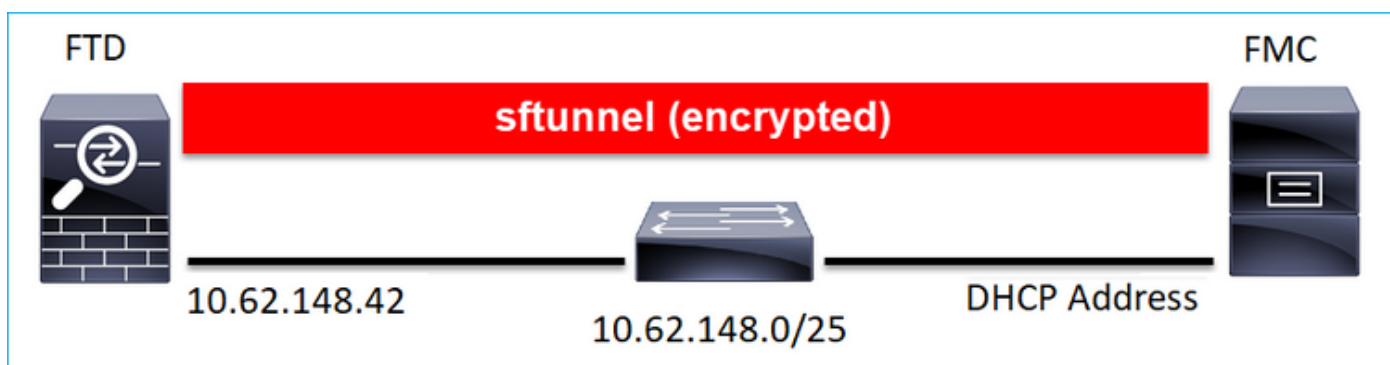
- Transfer Packets

¿Quién inicia el sftunnel en este caso?

El FTD inicia ambas conexiones 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
```

Situación hipotética 3. Dirección IP estática FTD - Dirección 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.
```

```
>
```

 Nota: Con DONTRESOLVE se requiere el ID de NAT.

IU de FMC

En este caso, especifique lo siguiente:

- Dirección IP de FTD
- Mostrar nombre:
- Clave de registro (debe coincidir con la configurada en FTD)
- Política de control de acceso
- Dominio
- Información de Smart Licensing
- ID de NAT (debe coincidir con el configurado en 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

- El CSP inicia el canal de control.
- El canal de eventos puede ser iniciado por cualquiera de los lados.

<#root>

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

```
netstat -an | grep 148.42
```

```
tcp        0      0 10.62.148.75:50465
```

```
50465
```

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

```
tcp        0      0 10.62.148.75:48445
```

```
48445
```

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

Situación hipotética 4. Registro FTD en FMC HA

En FTD, configure solo el FMC activo:

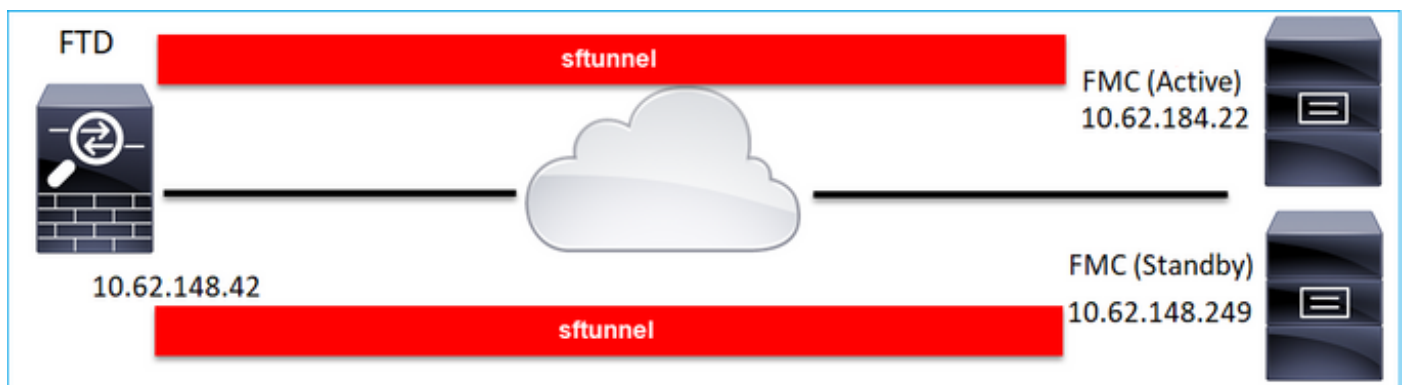
<#root>


>

```
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.



 Nota: Asegúrese de que el tráfico del puerto TCP 8305 esté permitido desde el FTD a ambos FMC.

En primer lugar, se establece el sftunnel al FMC activo:

```
<#root>
```

```
>
```

```
show managers
```

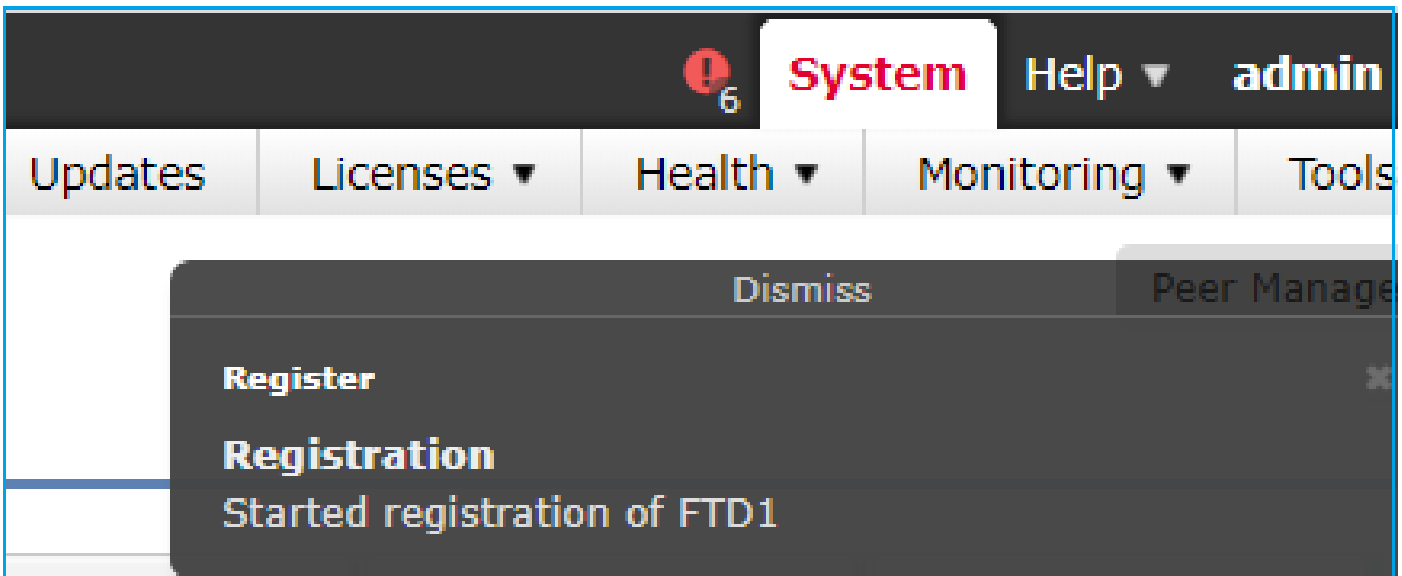
```
Type : Manager
```

```
Host :
```

```
10.62.184.22
```

```
Registration : Completed
```

Transcurridos unos minutos, el FTD inicia el registro en el CSP en espera:



```
<#root>
```

```
>
```

```
show managers
```

```
Type : Manager
```

```
Host :
```

```
10.62.184.22
```

```
Registration : Completed
```

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

En el backend del FTD, se establecen 2 canales de control (uno para cada FMC) y 2 canales de eventos (uno para cada FMC):

```
<#root>
```

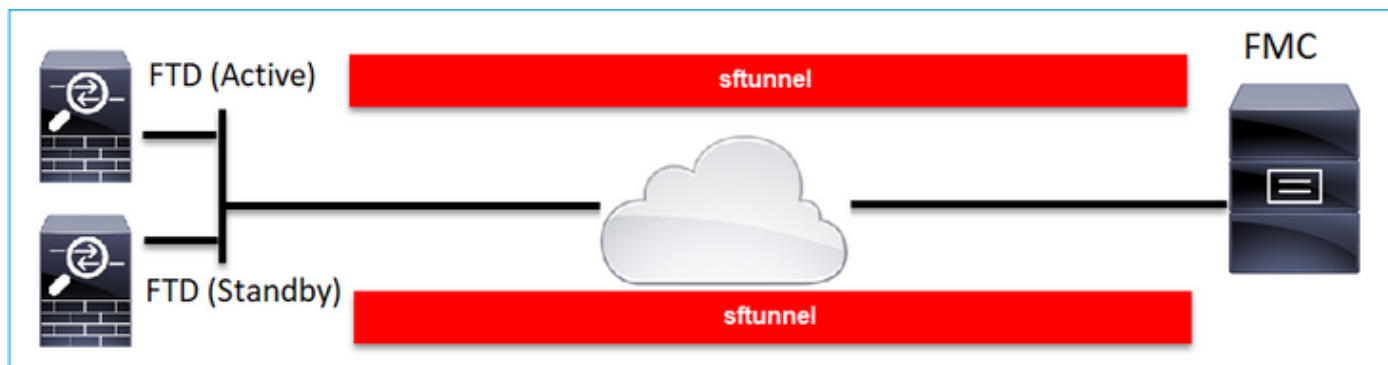
```
ftd1:/home/admin#
```

```
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
```

Situación hipotética 5. FTD HA

En el caso del FTD HA, cada unidad tiene un túnel separado al CSP:

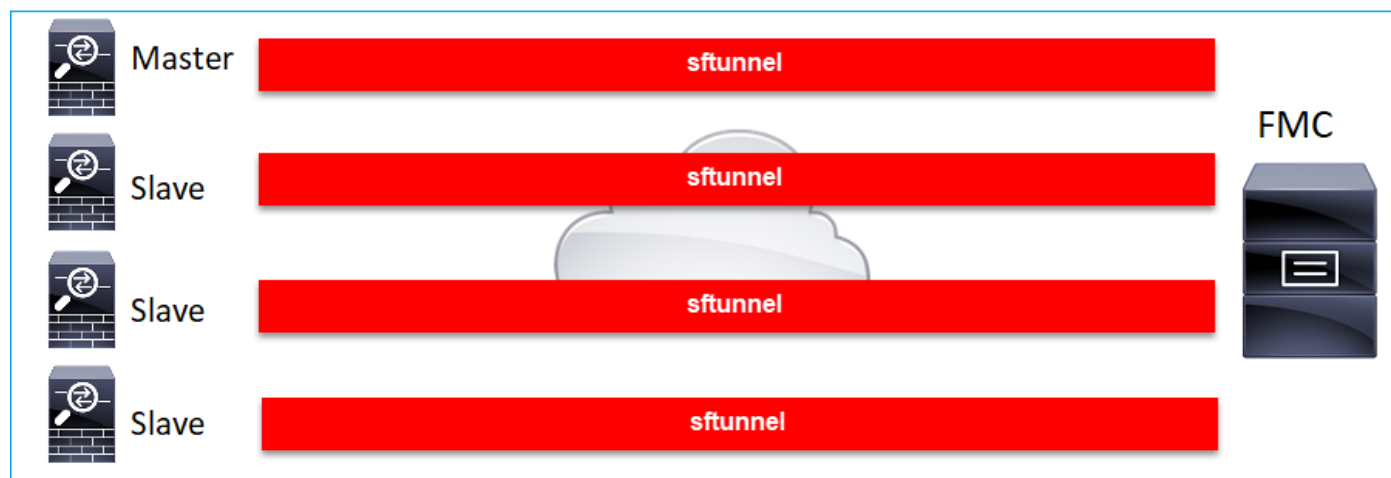



Los dos FTD se registran de forma independiente y, a partir del FMC, se forma el FTD HA. Para obtener más información, consulte:

- [Configuración de alta disponibilidad de FTD en dispositivos Firepower](#)
- [Alta disponibilidad para Firepower Threat Defence](#)

Situación hipotética 6. Clúster FTD

En el caso del clúster FTD, cada unidad tiene un túnel independiente al FMC. A partir de la versión 6.3 del FMC, sólo tendrá que registrar la unidad de control FTD en el FMC. A continuación, el FMC se encarga del resto de las unidades y las descubre automáticamente y las registra.

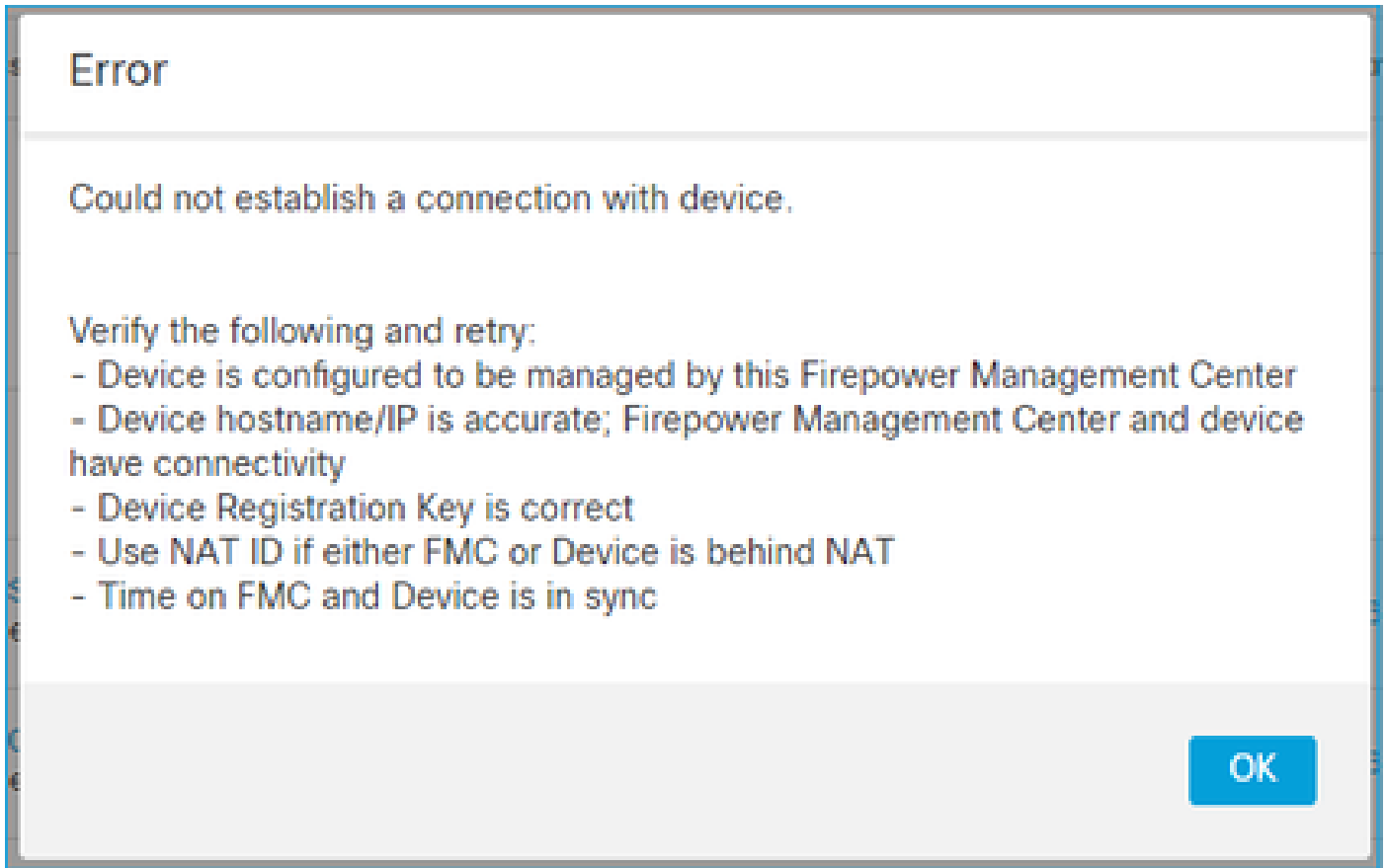


 Nota: Se recomienda agregar la unidad de control para obtener el mejor rendimiento, pero puede agregar cualquier unidad del clúster. Para obtener más información, consulte: [Creación de un clúster de Firepower Threat Defence](#)

Solucionar problemas comunes

1. Sintaxis no válida en FTD CLI

En caso de sintaxis no válida en FTD y de un intento de registro fallido, la interfaz de usuario de FMC muestra un mensaje de error bastante genérico:



En este comando, la palabra clave key es la clave de registro, mientras que cisco123 es el ID de NAT. Es bastante común agregar la clave de la palabra clave mientras que técnicamente no existe tal palabra clave:

```
<#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.
```

Acción Recomendada

Utilice una sintaxis correcta y no utilice palabras clave que no existan.

```
<#root>
```

```
>
```

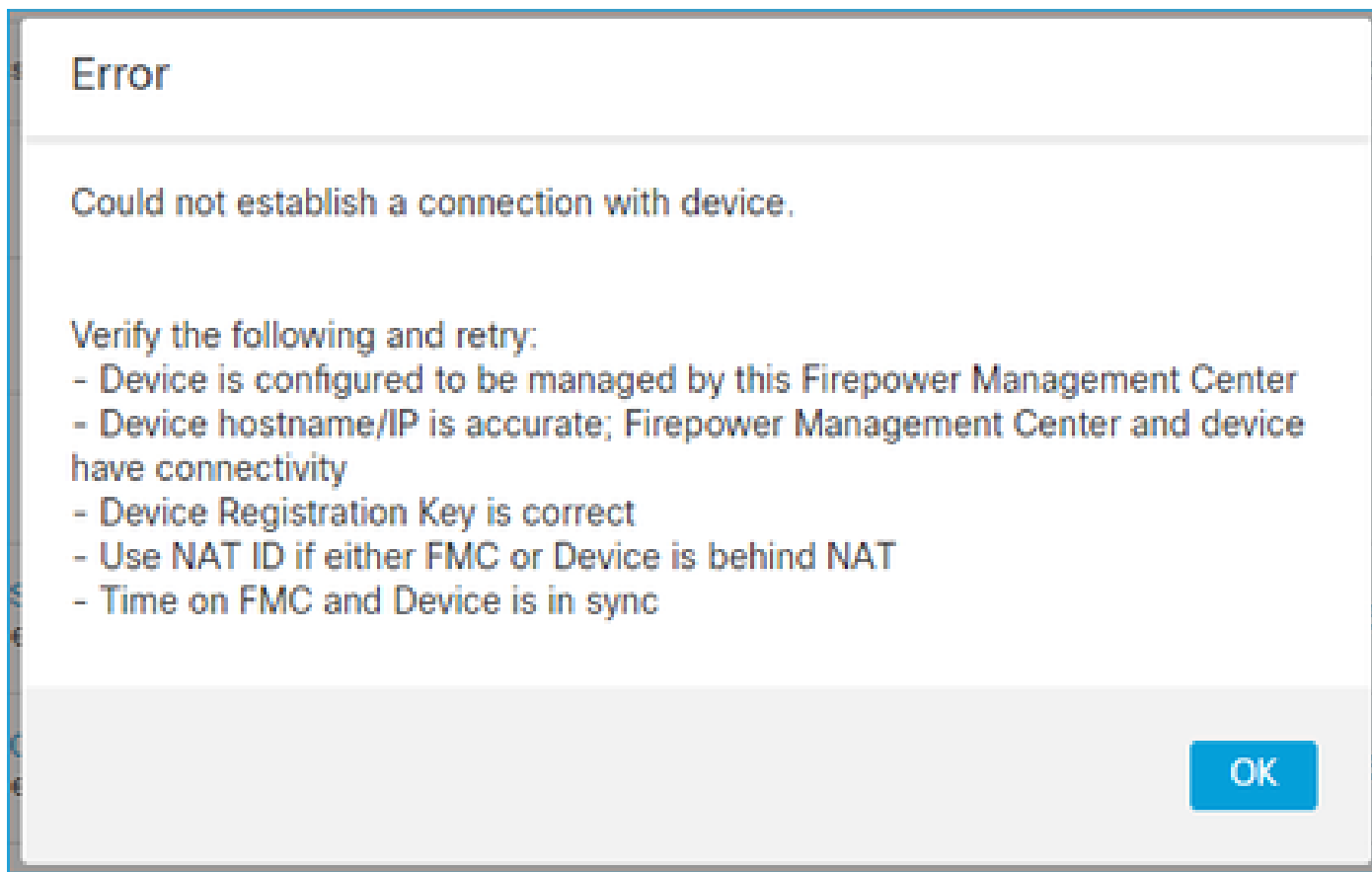
```
configure manager add 10.62.148.75 cisco123
```

```
Manager successfully configured.
```

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

2. Discordancia de clave de registro entre FTD - FMC

La interfaz de usuario de FMC muestra:



Acción Recomendada

En FTD, verifique los problemas de autenticación en el archivo `/ngfw/var/log/messages`.

Camino 1 - Comprobar los registros anteriores

```
<#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
```

Camino 2 - Comprobar los registros en vivo

```
<#root>
```

```
>
```

```
expert  
ftd1:~$
```

```
sudo su
```

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

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

En FTD, compruebe el contenido del archivo `/etc/sf/sftunnel.conf` para asegurarse de que la clave de registro es correcta:

```
<#root>
```

```
ftd1:~$
```

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

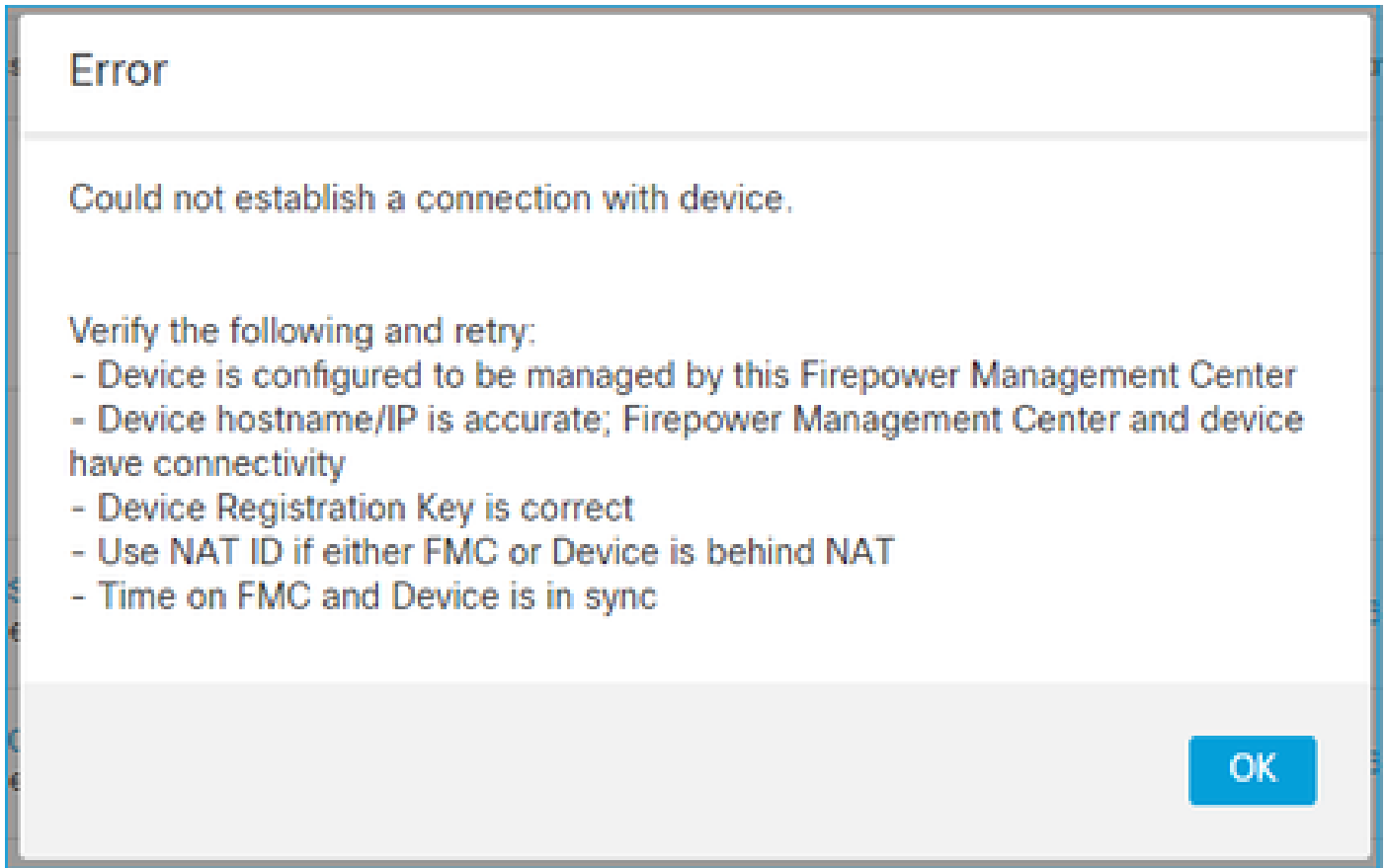
```
    reg_key
```

```
cisco-123
```

```
;
```

3. Problemas de conectividad entre FTD - FMC

La interfaz de usuario de FMC muestra:



Acciones recomendadas

- Asegúrese de que no haya ningún dispositivo en la ruta (por ejemplo, un firewall) que bloquee el tráfico (TCP 8305). En el caso de FMC HA, asegúrese de que el tráfico al puerto TCP 8305 esté permitido hacia ambos FMC.
- Tome capturas para verificar la comunicación bidireccional. En FTD, utilice el comando `capture-traffic`. Asegúrese de que haya un protocolo de enlace de 3 vías TCP y de que no haya paquetes TCP FIN o 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
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
```

Del mismo modo, tome una captura de FMC para garantizar la comunicación bidireccional:

```
<#root>

root@FMC2000-2:/var/common#

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

También se recomienda exportar la captura en formato pcap y verificar el contenido del paquete:

```
<#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
```

Posibles Causas:

- El CSP no tiene agregado el dispositivo FTD.
- Un dispositivo de la ruta (por ejemplo, un firewall) bloquea o modifica el tráfico.
- Los paquetes no se rutean correctamente en el trayecto.
- El proceso sftunnel en FTD o FMC está inactivo (comprobar el escenario 6)
- Hay un problema de MTU en la trayectoria (escenario de verificación).

Para el análisis de capturas, consulte este documento:

[Análisis de las capturas de firewall de Firepower para solucionar problemas de red de manera eficaz](#)

5. Diferencia de tiempo entre FTD y FMC

La comunicación FTD-FMC es sensible a las diferencias horarias entre los 2 dispositivos. Es un requisito de diseño tener FTD y FMC sincronizados por el mismo servidor NTP.

En concreto, cuando el FTD se instala en una plataforma como 41xx o 93xx, los ajustes de tiempo se toman del chasis principal (FXOS).

Acción Recomendada

Asegúrese de que el administrador del chasis (FCM) y el FMC utilizan la misma fuente de tiempo (servidor NTP)

6. Proceso sftunnel inactivo o inhabilitado

En FTD, el proceso sftunnel maneja el proceso de registro. Este es el estado del proceso antes de la configuración del administrador:

```
<#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,sfiproxy
```

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

Estado de registro:


```
<#root>
```

```
>
```

```
show managers
```

```
No managers configured.
```

Configuración del jefe:

```
<#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.
```

Ahora el proceso está ACTIVO:

```
<#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)
```

En algunos casos raros, el proceso puede estar inactivo o desactivado:

```
<#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
```

El estado del jefe parece normal:

```
<#root>
```

```
>
```

```
show managers
```

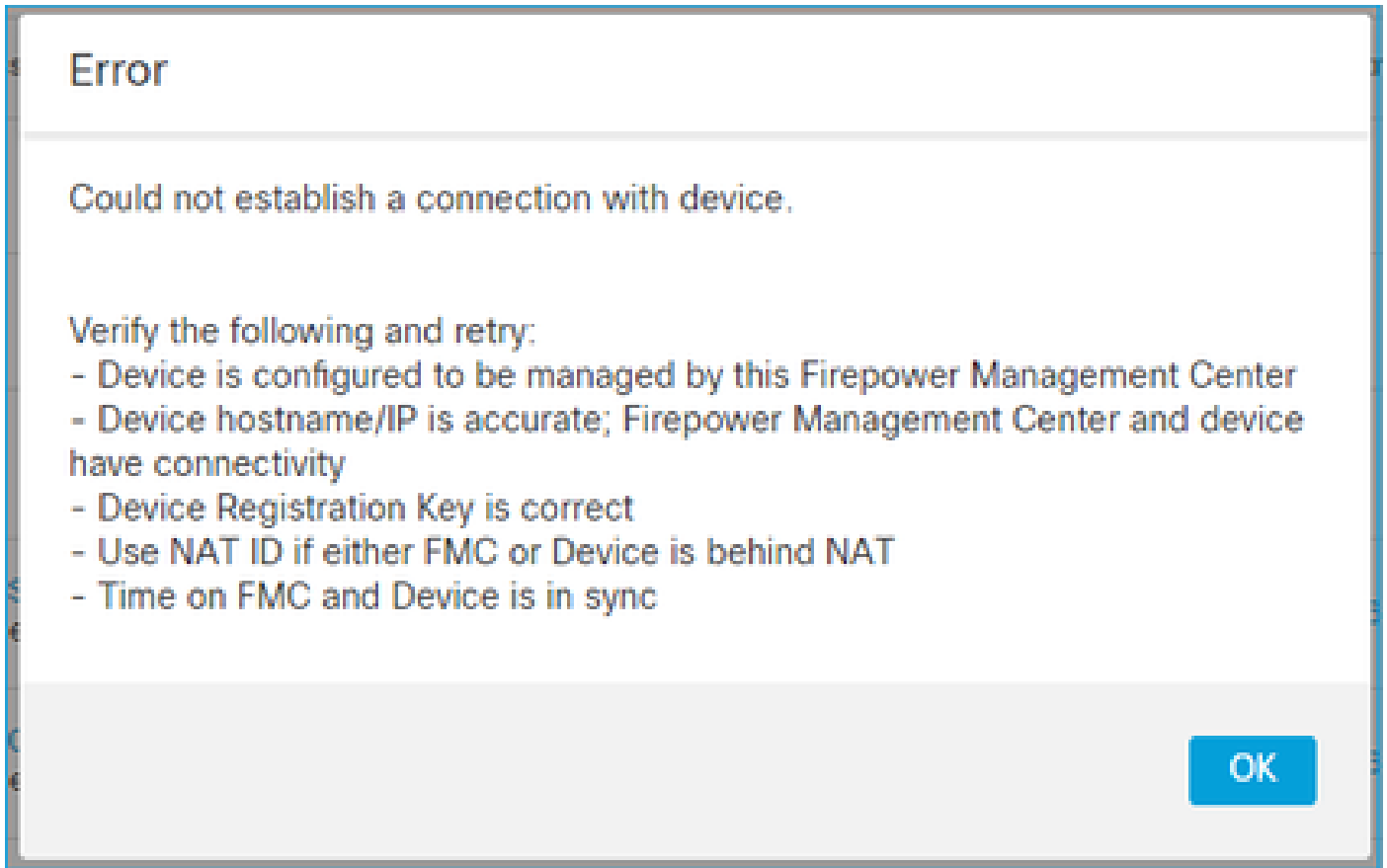
```
Host : 10.62.148.75
```

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

```
Registration : pending
```

```
RPC Status :
```

Por otro lado, el registro del dispositivo falla:



En FTD no se ven mensajes relacionados en `/ngfw/var/log/messages`

Acción Recomendada

Recopile el archivo de solución de problemas de FTD y póngase en contacto con Cisco TAC


7. FTD pendiente de registro en el CSP secundario

Existen situaciones en las que, tras el registro inicial del FTD en una configuración de FMC HA, el dispositivo FTD no se añade al FMC secundario.

Acción Recomendada

Utilice el procedimiento descrito en este documento:

[Utilizar CLI para resolver el registro de dispositivos en Firepower Management Center High Availability](#)

 Advertencia: este procedimiento es intrusivo, ya que contiene la anulación del registro de un dispositivo. Esto afecta a la configuración del dispositivo FTD (se elimina). Se recomienda utilizar este procedimiento solo durante el registro y la configuración iniciales del FTD. En otro caso, recopile los archivos de solución de problemas de FTD y FMC y póngase en

8. El registro falla debido a la MTU de la ruta

Existen situaciones en Cisco TAC en las que el tráfico sftunnel tiene que atravesar un link que tiene una MTU pequeña. Los paquetes sftunnel tienen el bit Don't fragment establecido, por lo que no se permite la fragmentación:

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

Además, en los archivos /ngfw/var/log/messages puede ver un mensaje como este:

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

Acción Recomendada

Para verificar si hay pérdida de paquetes debido a la fragmentación, realice capturas en FTD, FMC e idealmente en los dispositivos de la ruta. Verifique si ve los paquetes que llegan en ambos extremos.

En FTD, reduzca la MTU en la interfaz de administración de FTD. El valor predeterminado es 1500 bytes. MAX es 1500 para la interfaz de administración y 9000 para la interfaz de eventos. El comando fue agregado en la versión FTD 6.6.

[Referencia de comandos de Cisco Firepower Threat Defence](#)

Ejemplo:

```
<#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'
```

Verificación

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

Para verificar la MTU de trayectoria desde el FTD puede utilizar este comando:

```
<#root>
```

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

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

La opción do configura el bit don't fragment en los paquetes ICMP. Además, cuando se especifica 1472, el dispositivo envía 1500 bytes: (encabezado IP = 20 bytes) + (encabezado ICMP = 8 bytes) + (1472 bytes de datos ICMP)

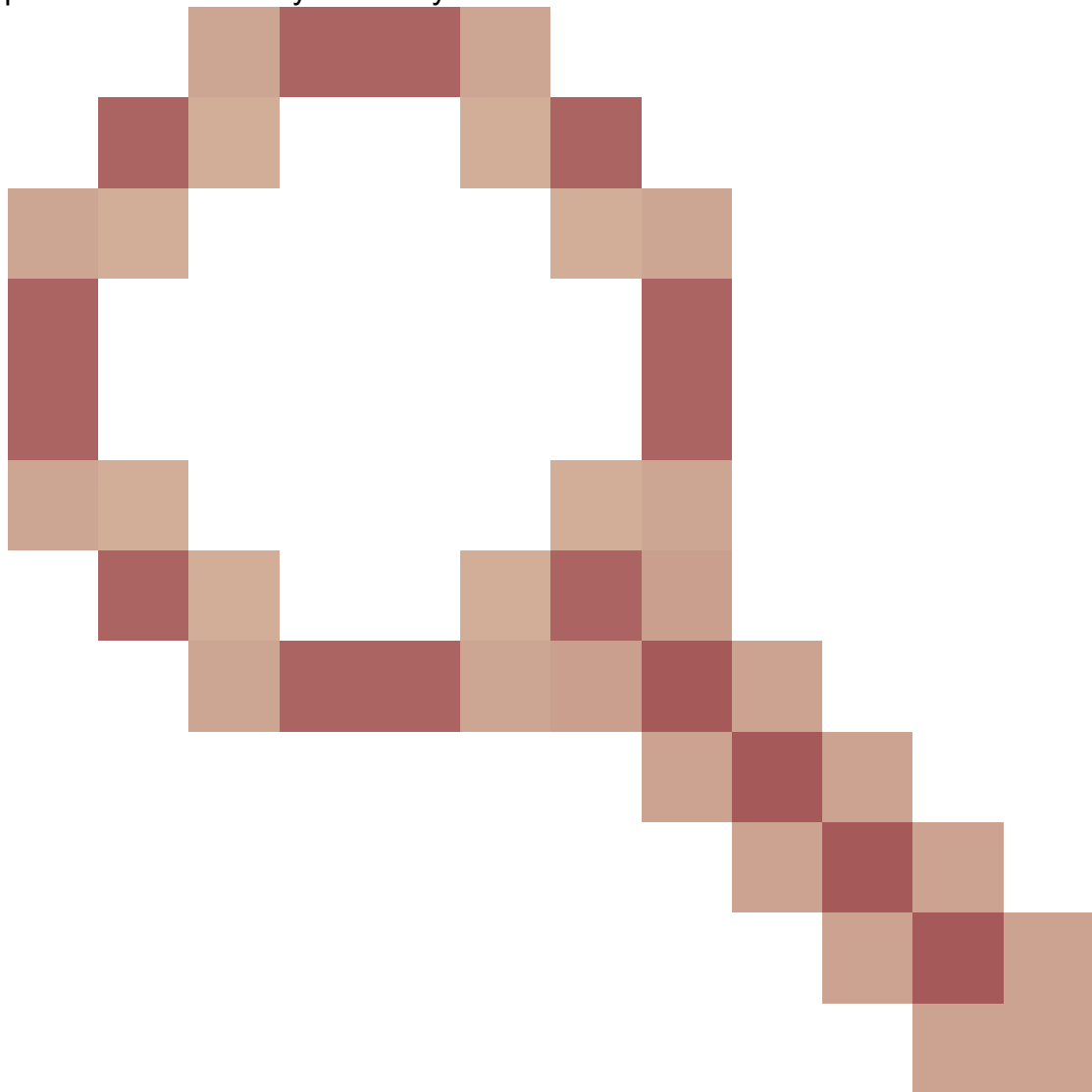
En el FMC, reduzca el valor de MTU en la interfaz de gestión del FMC como se describe en este

documento:

[Configurar interfaces de administración de Firepower Management Center](#)

9. El FTD deja de estar registrado después de un cambio de bootstrap desde la IU del administrador de chasis

Esto se aplica a las plataformas FP41xx y FP93xx y se documenta en la identificación de error de



Cisco [CSCvn45138](#)

En general, no debe realizar cambios de bootstrap desde el administrador de chasis (FCM) a menos que realice una recuperación ante desastres.

Acción Recomendada

En caso de que haya realizado un cambio de bootstrap y haya coincidido con la condición (la comunicación FTD-FMC se ha interrumpido mientras el FTD se activa después del cambio de bootstrap), debe eliminar y volver a registrar el FTD en FMC.

10. El FTD pierde el acceso al FMC debido a los mensajes de redirección ICMP

Este problema puede afectar al proceso de registro o interrumpir la comunicación FTD-FMC después del registro.

El problema en este caso es un dispositivo de red que envía mensajes ICMP Redirect a la interfaz de administración FTD y la comunicación FTD-FMC de agujeros negros.

Cómo identificar este problema

En este caso, 10.100.1.1 es la dirección IP de FMC. En el FTD hay una ruta en caché debido a un mensaje de redirección ICMP que fue recibido por el FTD en la interfaz de administración:

```
<#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
```

Acción Recomendada

Paso 1

Inhabilite el redireccionamiento ICMP en el dispositivo que lo envía (por ejemplo, switch ascendente L3, router, etc.).

Paso 2

Borre la memoria caché de rutas FTD de la CLI de FTD:

```
<#root>
```

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

```
ip route flush 10.100.1.1
```

Cuando no se redirige se ve así:

```
<#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
```

Referencias

- [Comprensión de los mensajes de redirección ICMP](#)
- ID de bug de Cisco [CSCvm53282](#) FTD: Las tablas de ruteo agregadas por redirecciones ICMP quedan atascadas en la memoria caché de la tabla de ruteo para siempre

Información Relacionada

- [Guías de configuración de NGFW](#)

Acerca de esta traducción

Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).