Configurar, verificar e solucionar problemas do registro de dispositivos do Firepower

Contents

Introdução

Este documento descreve os procedimentos de solução de problemas da conexão entre o Firepower Threat Defense (FTD) e o Firepower Management Center (FMC).

Pré-requisitos

Requisitos

Não existem requisitos específicos para este documento.

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

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

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Informações de Apoio

Este documento descreve os procedimentos de operação, verificação e resolução de problemas da conexão (sftunnel) entre um FTD gerido e o FMC gerido.

As informações e os exemplos são baseados no FTD, mas a maioria dos conceitos também se aplica totalmente ao NGIPS (dispositivos da série 7000/8000) ou a um módulo FirePOWER no ASA55xx.

Um DTF suporta dois modos principais de gestão:

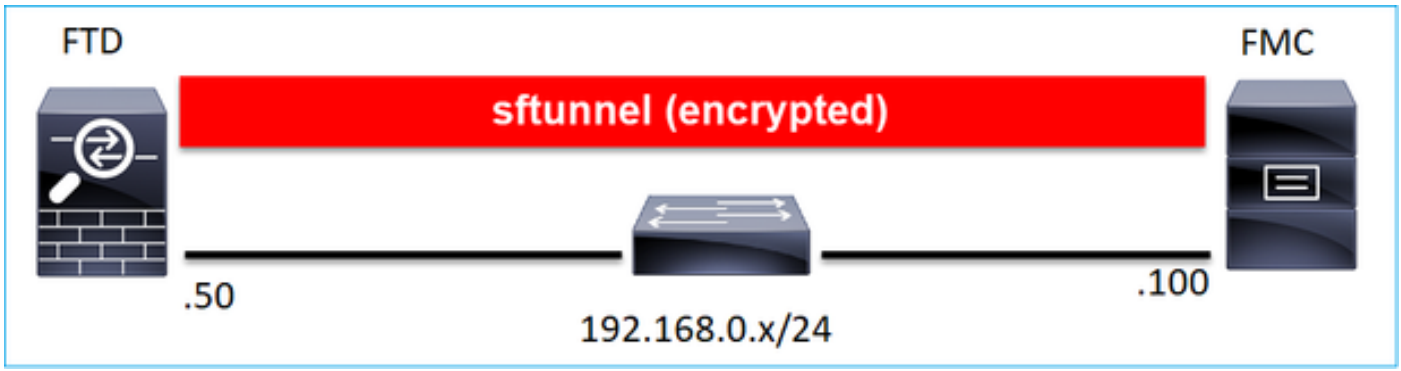
- Off-box via FMC - também conhecido como gerenciamento remoto
- On-box via Firepower Device Manager (FDM) e/ou Cisco Defense Orchestrator (CDO) - também conhecido como gerenciamento local

No caso da gestão à distância, o DTF deve, em primeiro lugar, registrar-se no CVP que utiliza um processo conhecido como registro de dispositivos.

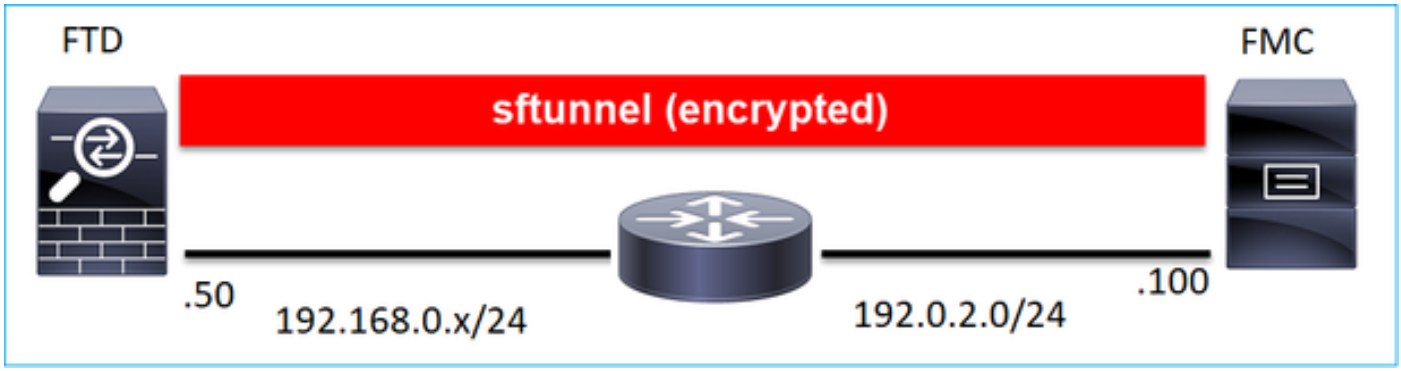
Quando o registro é feito, o FTD e o FMC estabelecem um túnel seguro chamado sftunnel (o nome deriva do túnel Sourcefire).

Opções de design

Do ponto de vista do projeto, o FTD - FMC pode estar na mesma sub-rede L3:

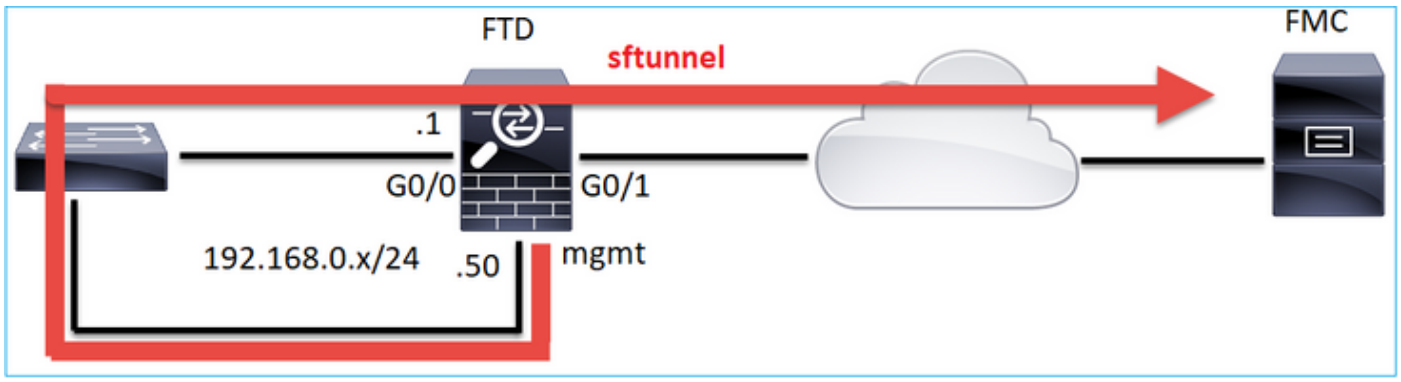


ou ser separados por redes diferentes:



192.0.2.0

Observação: o sftunnel também pode passar pelo próprio FTD. Este design não é recomendado. O motivo é que um problema de plano de dados do FTD pode interromper a comunicação entre o FTD e o FMC.



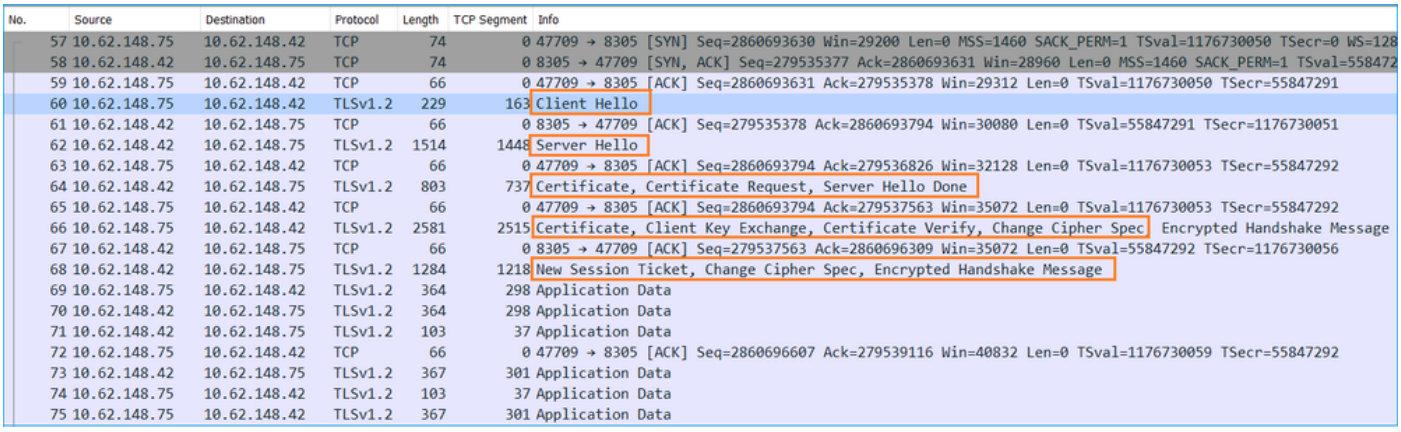
Que informações são trocadas através do túnel sf?

Esta lista contém a maioria das informações que são transportadas pelo túnel sf:

- Pulsação do dispositivo (keepalives)
- Sincronização de horário (NTP)
- Eventos (Conexão, Intrusão/IPS, Arquivo, SSL e assim por diante)
- Pesquisas de malware
- Eventos/alertas de integridade
- Informações de usuário e grupo (para Políticas de identidade)
- Informações sobre o estado HA do FTD
- Informações de estado do Cluster FTD
- Informações/eventos do Security Intelligent (SI)
- Informações/eventos do Threat Intelligence Diretor (TID)
- Arquivos capturados
- Eventos de Descoberta de Rede
- Pacote de políticas (implantação de políticas)
- Pacotes de atualização de software
- Pacotes de patches de software
- VDBs
- SRU

Que protocolo/porta é usado pelo sftunnel?

O sftunnel usa a porta TCP 8305. No back-end, é um 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=558472
59	10.62.148.75	10.62.148.42	TCP	66	0	47709 → 8305 [ACK] Seq=2860693631 Ack=279535378 Win=29312 Len=0 TSval=1176730050 TSecr=55847291
60	10.62.148.75	10.62.148.42	TLSv1.2	229	163	Client Hello
61	10.62.148.42	10.62.148.75	TCP	66	0	8305 → 47709 [ACK] Seq=279535378 Ack=2860693794 Win=30080 Len=0 TSval=55847291 TSecr=1176730051
62	10.62.148.42	10.62.148.75	TLSv1.2	1514	1448	Server Hello
63	10.62.148.75	10.62.148.42	TCP	66	0	47709 → 8305 [ACK] Seq=2860693794 Ack=279536826 Win=32128 Len=0 TSval=1176730053 TSecr=55847292
64	10.62.148.42	10.62.148.75	TLSv1.2	803	737	Certificate, Certificate Request, Server Hello Done
65	10.62.148.75	10.62.148.42	TCP	66	0	47709 → 8305 [ACK] Seq=2860693794 Ack=279537563 Win=35072 Len=0 TSval=1176730053 TSecr=55847292
66	10.62.148.75	10.62.148.42	TLSv1.2	2581	2515	Certificate, Client Key Exchange, Certificate Verify, Change Cipher Spec Encrypted Handshake Message
67	10.62.148.42	10.62.148.75	TCP	66	0	8305 → 47709 [ACK] Seq=279537563 Ack=2860696309 Win=35072 Len=0 TSval=55847292 TSecr=1176730056
68	10.62.148.42	10.62.148.75	TLSv1.2	1284	1218	New Session Ticket, Change Cipher Spec, Encrypted Handshake Message
69	10.62.148.75	10.62.148.42	TLSv1.2	364	298	Application Data
70	10.62.148.42	10.62.148.75	TLSv1.2	364	298	Application Data
71	10.62.148.42	10.62.148.75	TLSv1.2	103	37	Application Data
72	10.62.148.42	10.62.148.75	TCP	66	0	47709 → 8305 [ACK] Seq=2860696607 Ack=279539116 Win=40832 Len=0 TSval=1176730059 TSecr=55847292
73	10.62.148.42	10.62.148.75	TLSv1.2	367	301	Application Data
74	10.62.148.75	10.62.148.42	TLSv1.2	103	37	Application Data
75	10.62.148.75	10.62.148.42	TLSv1.2	367	301	Application Data

Como alterar a porta TCP Sftunnel no FTD?

<#root>

>

configure network management-port 8306

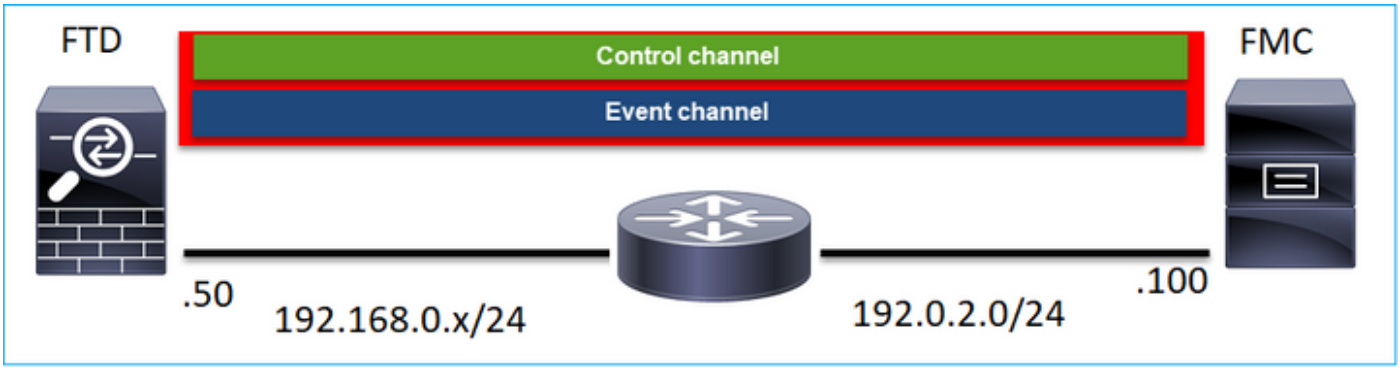
Management port changed to 8306.

Observação: nesse caso, você também deve alterar a porta no FMC (Configuração > Interfaces de gerenciamento > Configurações compartilhadas). Isso afeta todos os outros dispositivos que já estão registrados no mesmo FMC. A Cisco recomenda que você mantenha as configurações padrão para a porta de gerenciamento remoto, mas se a porta de gerenciamento entrar em conflito com outras comunicações em sua rede, você poderá escolher uma porta diferente. Se você alterar a porta de gerenciamento, deverá alterá-la para todos os dispositivos em sua implantação que precisam se comunicar juntos.

Quantas conexões são estabelecidas pelo túnel sf?

O sftunnel estabelece 2 conexões (canais):

- Canal de controle
- Canal do evento



Que dispositivo inicia cada canal?

Depende do cenário. Verifique os cenários descritos no restante do documento.

Configurar

Conceitos Básicos de Registro

CLI de FTD

No FTD, a sintaxe básica para o registro do dispositivo é:

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

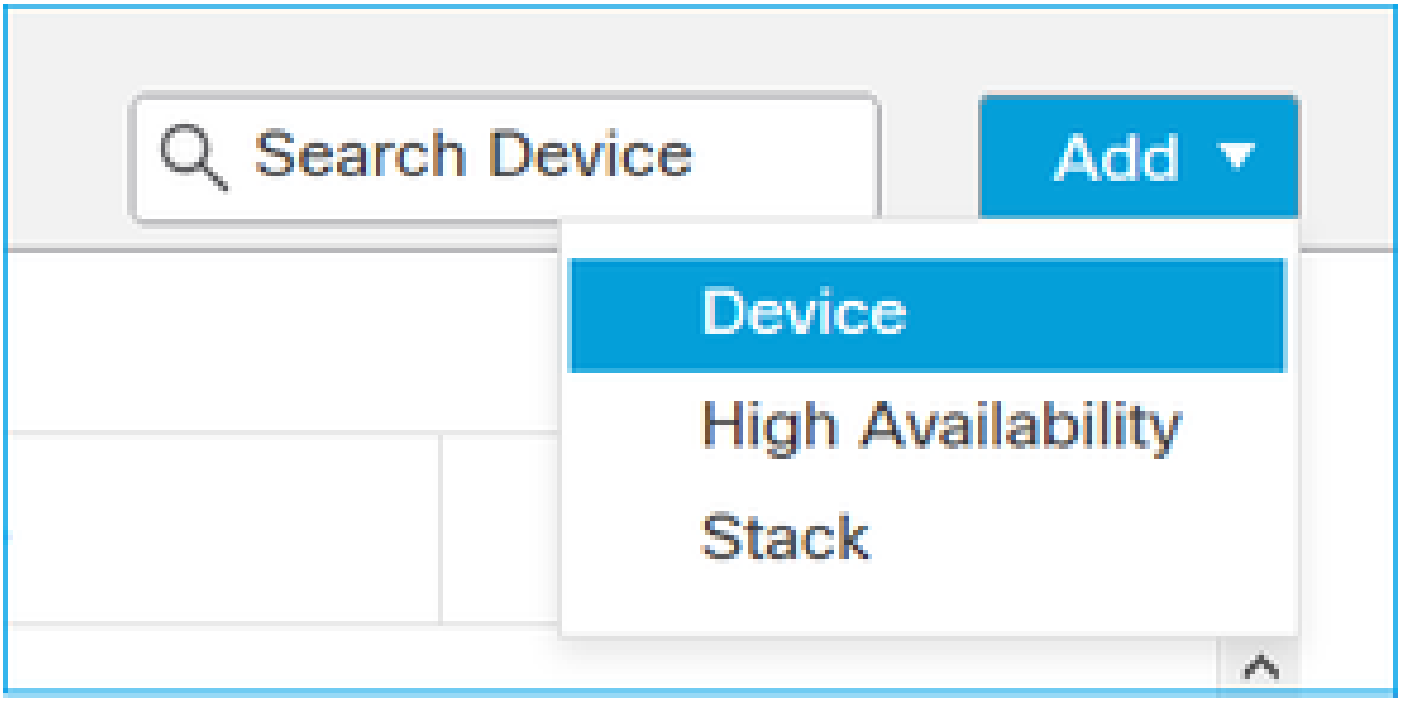
Valor	Descrição

Host FMC	Isso pode ser: • Hostname • endereço ipv4 • endereço ipv6 • DONTRESOLVE
Chave de registro	Trata-se de uma sequência alfanumérica secreta compartilhada (entre 2 e 36 caracteres) usada para o registro do dispositivo. Apenas alfanuméricos, hífen (-), sublinhado (_) e ponto (.) são permitidos.
ID NAT	Uma sequência alfanumérica utilizada durante o processo de registro entre o FMC e o dispositivo, quando um dos lados não especifica um endereço IP. Especifique a mesma ID de NAT no FMC.

Para obter mais detalhes, consulte a Referência de Comandos do Cisco Firepower Threat Defense

IU do FMC

No FMC, navegue até Devices > Device Management. Selecione Add > Device



Add Device

Host:*

Display Name:

Registration Key:*

Domain:

Select Domain

Group:

None

Access Control Policy:*

Smart Licensing

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

Advanced

Unique NAT ID:*

- [x] Transfer Packets

CLI de FTD

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

Por exemplo:

<#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.

Informações de fundo

Assim que você inserir o comando FTD, o FTD tentará se conectar ao FMC a cada 20 segundos, mas como o FMC ainda não está configurado, ele responde com 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
```

O status de registro do dispositivo:

```
<#root>

>

show managers

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

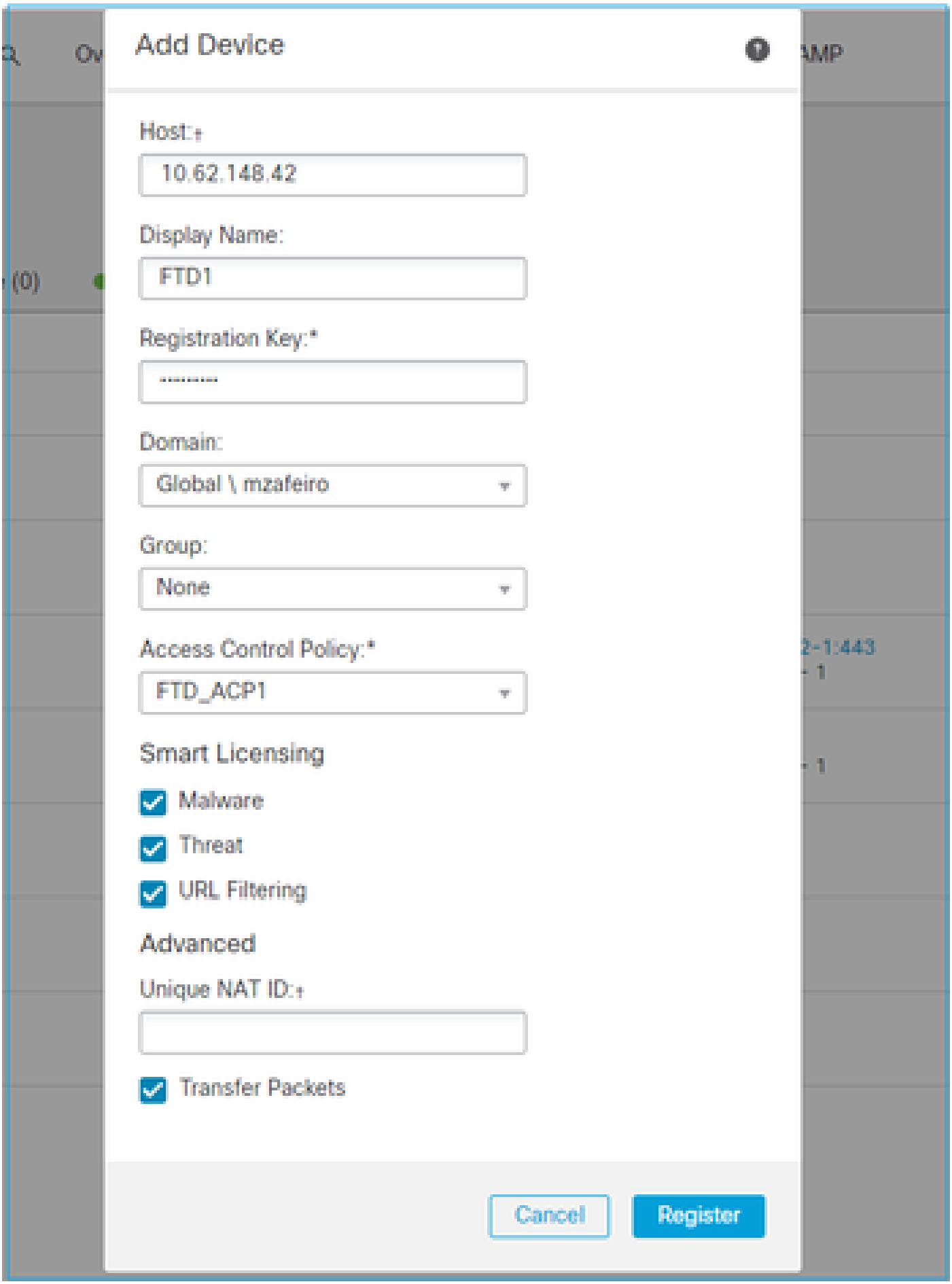
O FTD escuta na porta TCP 8305:

```
<#root>

admin@vFTD66:~$

netstat -na | grep 8305

tcp        0      0 10.62.148.42:

8305

       0.0.0.0:*

LISTEN
```

IU do FMC

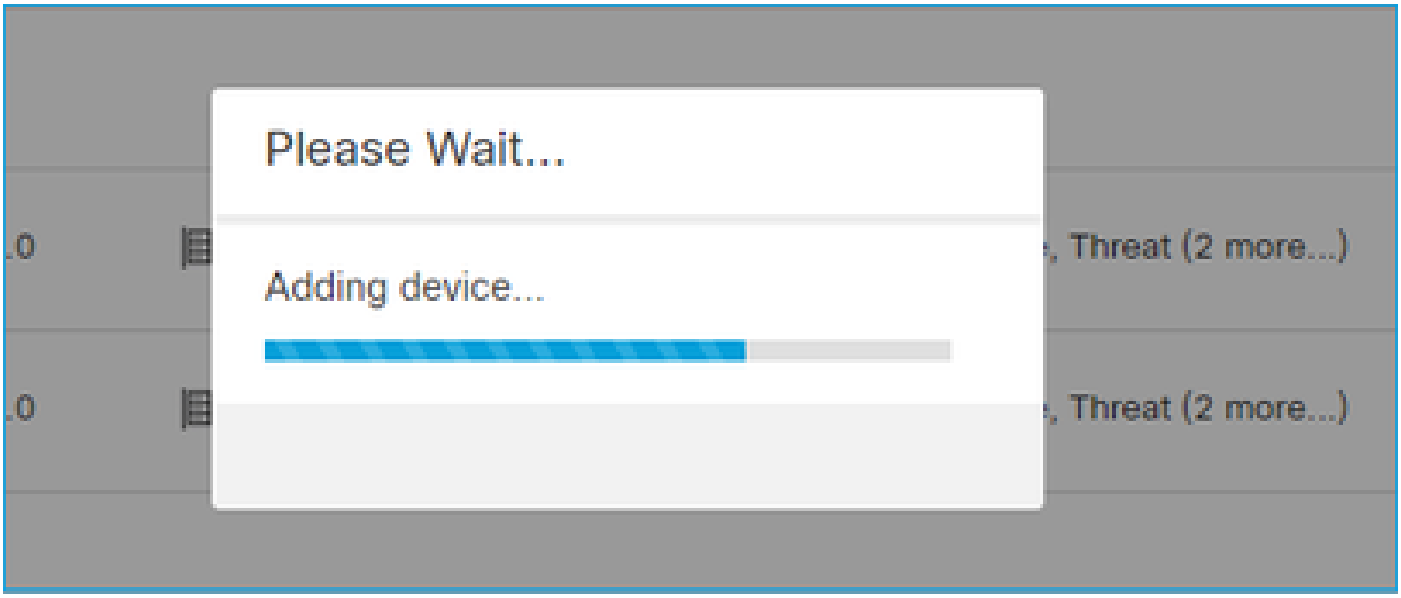
Nesse caso, especifique:

- Host (endereço IP do FTD)
- Nome de exibição
- Chave de registro (deve corresponder àquela configurada no FTD)
- Política de controle de acesso
- domínio
- Informações do Smart Licensing


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

Selecione Registrar

O processo de registro é iniciado:



O FMC começa a escutar na porta TCP 8305:

<#root>

admin@FMC2000-2:~$

netstat -na | grep 8305

tcp 0 0 10.62.148.75:

8305

0.0.0.0:*

LISTEN

Em segundo plano, o FMC inicia uma conexão 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 [.], ack 164, win 235, options [nop,no
```

O canal de controle sftunnel é estabelecido:

<#root>

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

netstat -na | grep 8305

```
tcp        0      0 10.62.148.75:8305       0.0.0.0:*               LISTEN
tcp        0      0
```

10.62.148.75:50693   10.62.148.42:8305

ESTABLISHED

<#root>

```
>
```

sftunnel-status

```
SFTUNNEL Start Time: Sat Apr 18 20:14:20 2020

        Both IPv4 and IPv6 connectivity is supported
        Broadcast count = 4
        Reserved SSL connections: 0
        Management Interfaces: 1
        eth0 (control events) 10.62.148.42,

**********************

**RUN STATUS****ksec-fs2k-2-mgmt.cisco.com*************
        Cipher used = AES256-GCM-SHA384 (strength:256 bits)
```

ChannelA Connected: Yes, Interface eth0

```
ChannelB Connected: No

        Registration: Completed.
        IPv4 Connection to peer '10.62.148.75' Start Time: Sat Apr 18 20:16:08 2020


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

Peer channel Channel-A is valid  type (CONTROL), using 'eth0', connected to '10.62.148.75' via '10.62.14


Peer channel Channel-B is not valid
```

Depois de alguns minutos, o canal de Evento é estabelecido. O iniciador do canal de Evento pode estar em ambos os lados. Neste exemplo, era o FMC:

```
<#root>

20:21:15.347587 IP 10.62.148.75.43957 > 10.62.148.42.8305: Flags

[S]

, seq 3414498581, win 29200, options [mss 1460,sackOK,TS val 1181601702 ecr 0,nop,wscale 7], length 0
20:21:15.347660 IP 10.62.148.42.8305 > 10.62.148.75.43957: Flags

[S.]

, seq 2735864611,

ack

 3414498582, win 28960, options [mss 1460,sackOK,TS val 56334496 ecr 1181601702,nop,wscale 7], length 0
20:21:15.347825 IP 10.62.148.75.43957 > 10.62.148.42.8305: Flags [.],

ack

 1, win 229, options [nop,nop,TS val 1181601703 ecr 56334496], length 0
20:21:15.348415 IP 10.62.148.75.43957 > 10.62.148.42.8305: Flags [P.], seq 1:164, ack 1, win 229, optio
```

A porta origem aleatória denota o iniciador da conexão:

```
<#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
```

Caso o canal de Evento tenha sido iniciado pelo FTD, a saída será:

<#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
```

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

<#root>

>

show managers

Type : Manager
Host : 10.62.148.75

Registration : Completed

>

Cenário 2. Endereço IP DHCP do FTD - Endereço IP estático do FMC

Neste cenário, a interface de gerenciamento FTD obteve seu endereço IP de um servidor DHCP:

CLI de FTD

Você deve especificar a ID do NAT:

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

Por exemplo:

```
<#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.

>
```

O status de registro do 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 do FMC

Nesse caso, especifique:

- Nome de exibição
- Chave de registro (deve corresponder àquela configurada no FTD)
- Política de controle de acesso
- domínio
- Informações do Smart Licensing
- ID de NAT (necessária quando Host não está especificado. Ele deve corresponder ao configurado no FTD)

Add Device

Host:*

empty

Display Name:

FTD1

Registration Key:*

Domain:

Global \ mzafeiro

Group:

None

Access Control Policy:*

FTD_ACP1

Smart Licensing

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

Advanced

Unique NAT ID:*

nat123

- [x] Transfer Packets

Quem inicia o sftunnel nesse caso?

O FTD inicia ambas as conexões 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
```

Cenário 3. Endereço IP estático do FTD - Endereço IP DHCP do 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.

>
```

Observação: com DONTRESOLVE, a ID de NAT é necessária.

IU do FMC

Nesse caso, especifique:

- Endereço IP do FTD
- Nome de exibição
- Chave de registro (deve corresponder àquela configurada no FTD)
- Política de controle de acesso
- domínio
- Informações do Smart Licensing
- ID de NAT (deve corresponder ao configurado no FTD)

Add Device

Host:*

10.62.148.42

Display Name:

FTD1

Registration Key:*

.....

Domain:

Global \ mzafeiro

Group:

None

Access Control Policy:*

FTD_ACP1

Smart Licensing

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

Advanced

Unique NAT ID:*

nat123

- [x] Transfer Packets

- O FMC inicia o canal de controle.
- O canal de Evento pode ser iniciado por ambos os lados.

<#root>

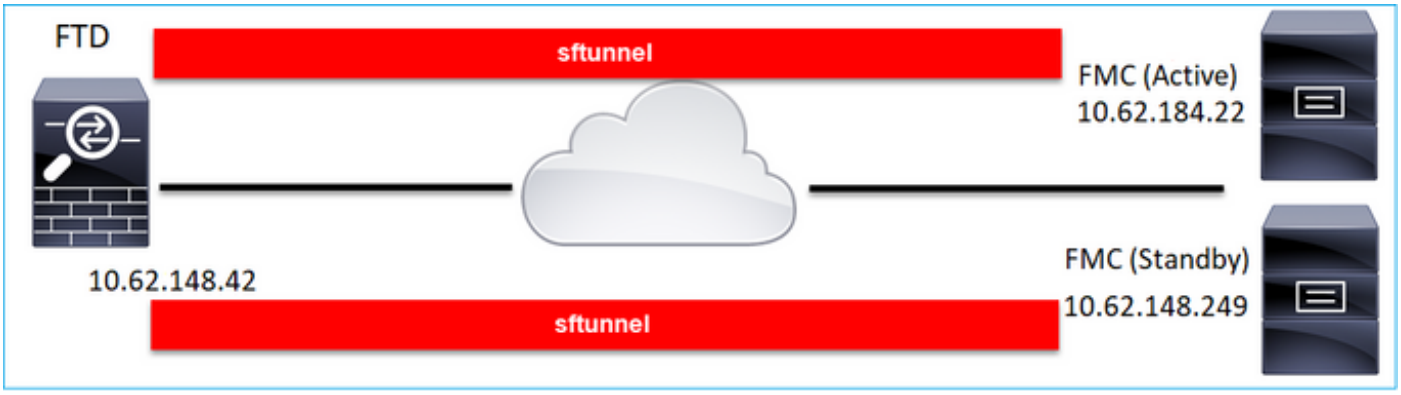
```
root@FMC2000-2:/Volume/home/admin#

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
```

Cenário 4. Registro do FTD no FMC HA

No FTD, configure somente o FMC Ativo:

<#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.
```

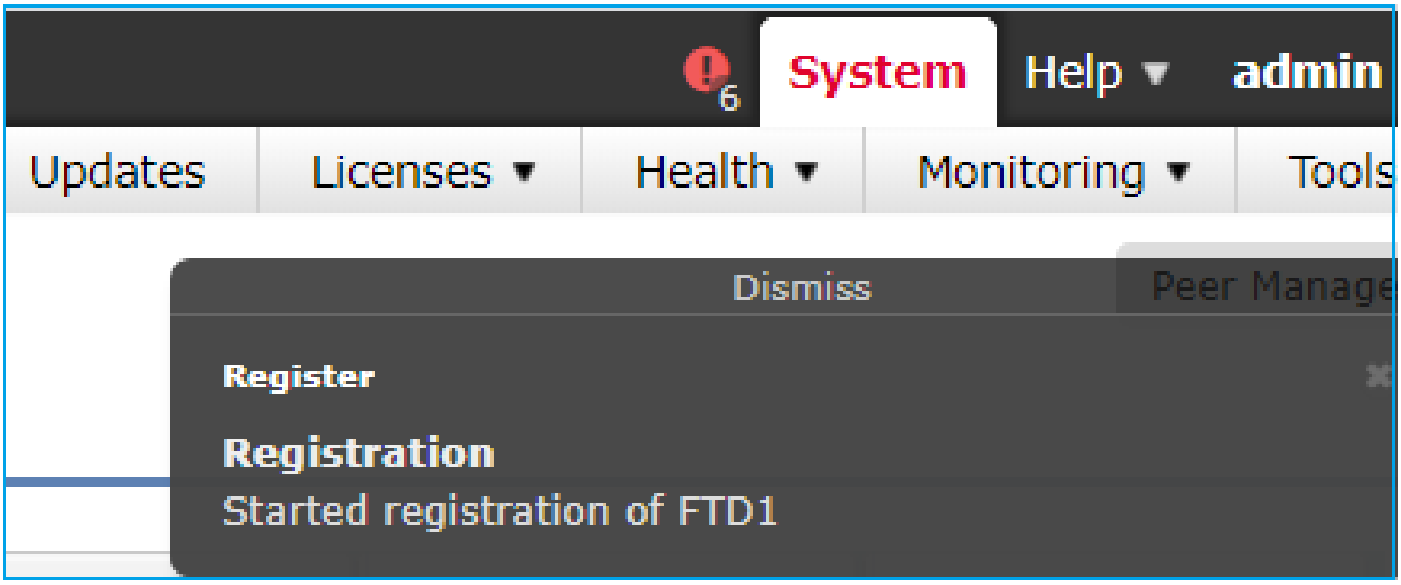


Observação: verifique se o tráfego da porta TCP 8305 é permitido do FTD para ambos os FMCs.

Em primeiro lugar, o túnel sfpara o CVP ativo é estabelecido:

```
<#root>

>

show managers

Type                    : Manager
Host                    :

10.62.184.22

Registration            : Completed
```

Após alguns minutos, o FTD inicia o registro no CVP de vigília:




```
<#root>

>

show managers

Type                    : Manager
Host                    :

10.62.184.22

Registration            : Completed
```

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

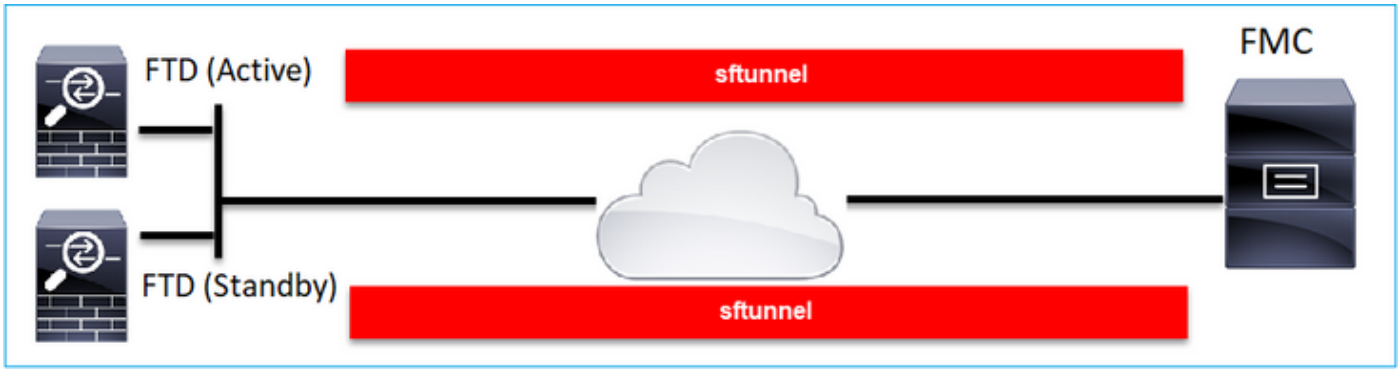
Na infraestrutura do FTD, são estabelecidos 2 canais de controlo (um para cada CVP) e 2 canais de eventos (um para cada CVP):

<#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
```

Cenário 5. HA FTD

No caso do FTD HA, cada unidade tem um túnel separado para o CVP:

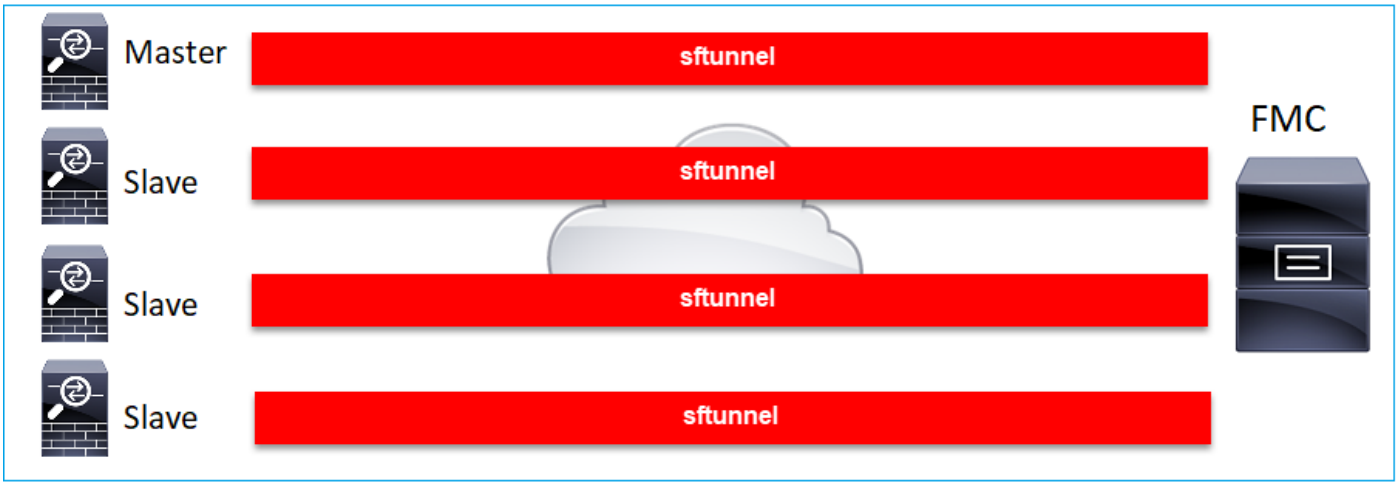


Você registra ambos os FTDs de forma independente e, em seguida, do FMC, forma o FTD HA. Para obter mais detalhes, verifique:

- Configurar a alta disponibilidade do FTD em dispositivos Firepower
- Alta disponibilidade do Firepower Threat Defense

Cenário 6. Cluster FTD

No caso do cluster FTD, cada unidade tem um túnel separado para o CVP. A partir da versão 6.3 do FMC, só é necessário registrar a unidade de controlo do FTD no FMC. Em seguida, o FMC cuida do restante das unidades e as autodescobre e registra.

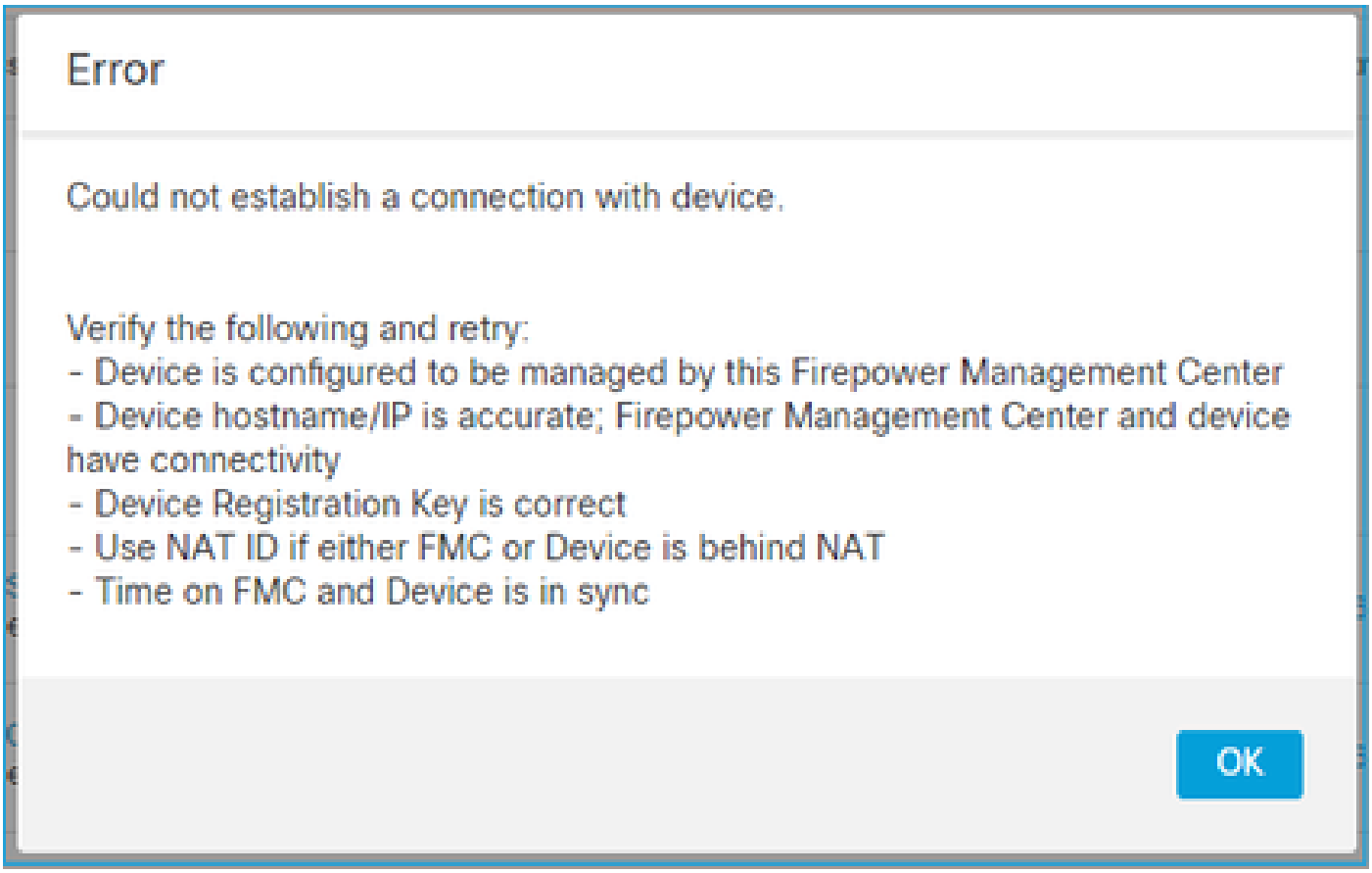


Observação: recomendamos adicionar a unidade de Controle para obter o melhor desempenho, mas você pode adicionar qualquer unidade do cluster. Para obter mais detalhes, verifique: Criar um cluster do Firepower Threat Defense

Solucionar problemas comuns

1. Sintaxe inválida na CLI do FTD

Em caso de sintaxe inválida no FTD e falha na tentativa de registro, a interface do usuário do FMC mostra uma mensagem de erro bem genérica:



Nesse comando, a chave de palavra-chave é a chave de registro, enquanto o cisco123 é o ID de NAT. É muito comum adicionar a chave de palavra-chave enquanto tecnicamente não há tal palavra-chave:

```
<#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.
```

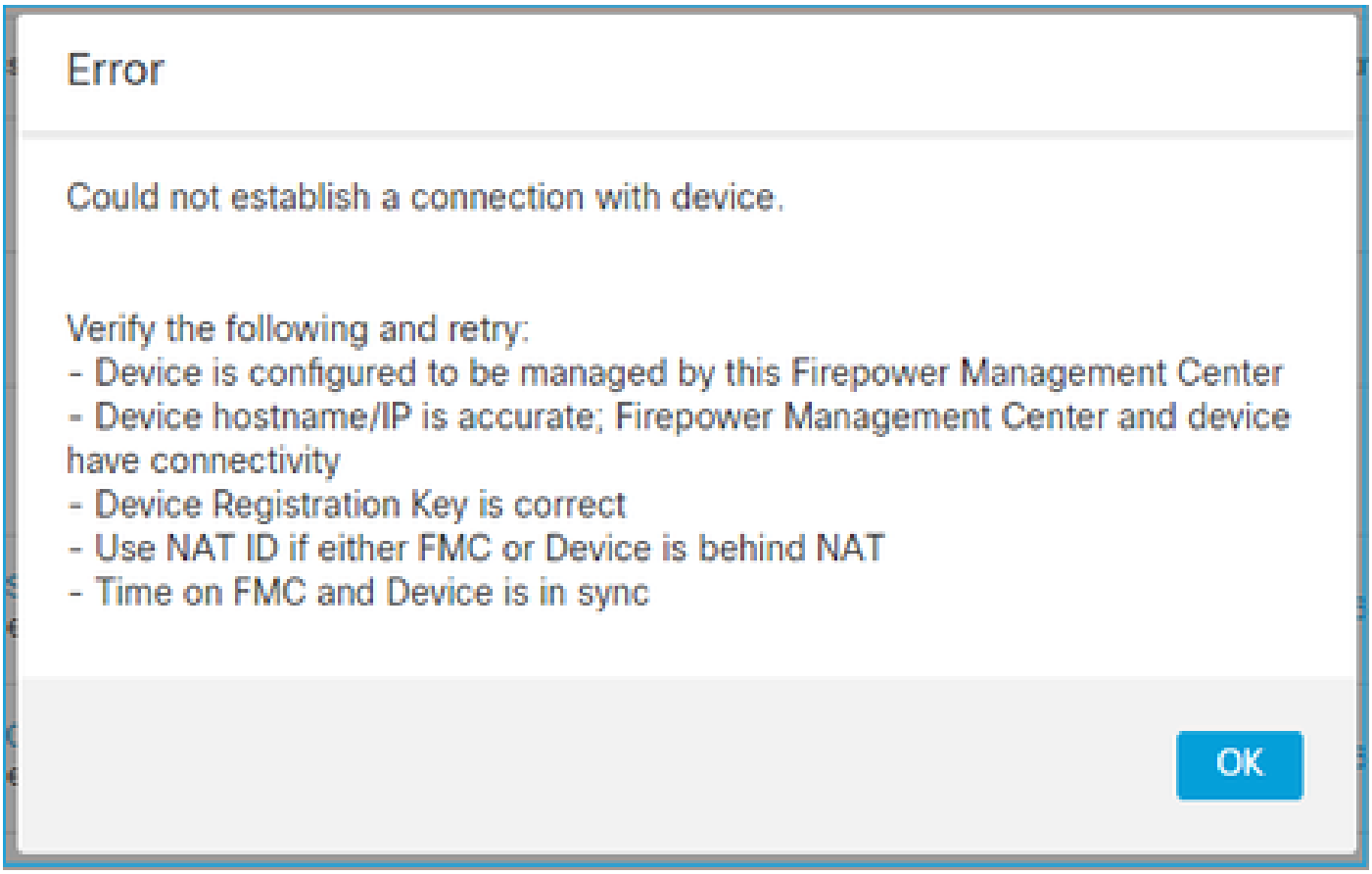
Ação recomendada

Use a sintaxe apropriada e não use palavras-chave que não existam.

```
<#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. Incompatibilidade da chave de registro entre o FTD e o FMC

A IU do FMC mostra:



Ação recomendada

No FTD, verifique se há problemas de autenticação no arquivo /ngfw/var/log/messages.

Caminho 1 - Verificar os logs 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] sftunneld:sf_ssl [WARN] Accept:
```

Failed to authenticate peer '10.62.148.75' <- The problem

Caminho 2 - Verificar os registros em tempo real

<#root>

>

expert
ftd1:~$

sudo su

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

tail -f /ngfw/var/log/messages

No FTD, verifique o conteúdo do arquivo /etc/sf/sftunnel.conf para garantir que a chave de registro esteja correta:

<#root>

```
ftd1:~$
```

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

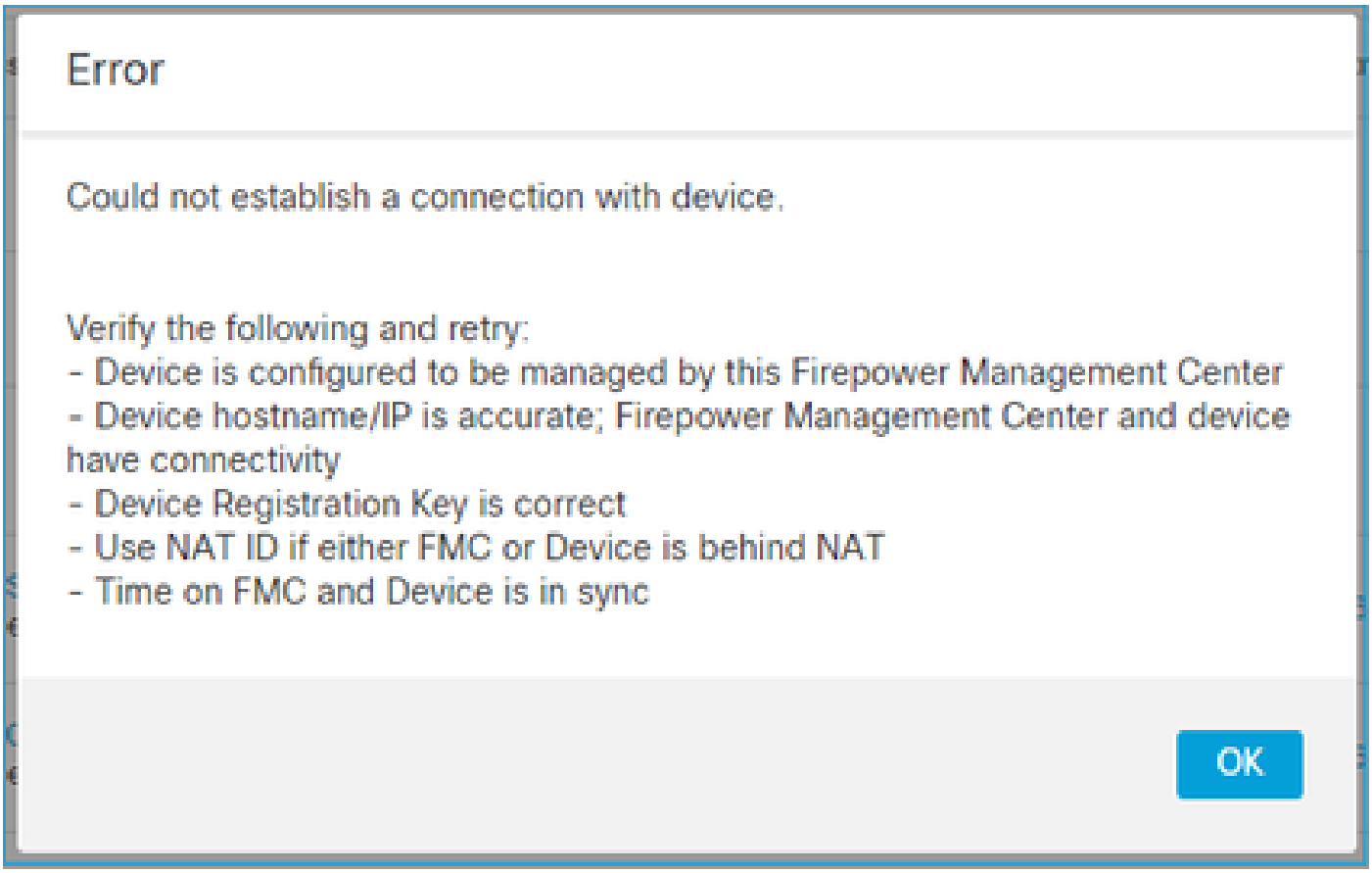
```
        reg_key
```

cisco-123

;

3. Problemas de conectividade entre o FTD e o FMC

A IU do FMC mostra:



Ações recomendadas

- Verifique se não há nenhum dispositivo no caminho (por exemplo, um firewall) que bloqueie o tráfego (TCP 8305). No caso do FMC HA, assegure-se de que o tráfego para a porta TCP 8305 seja permitido para ambos os FMCs.
- Faça capturas para verificar a comunicação bidirecional. No FTD, use o comando capture-traffic. Verifique se há um handshake triplo TCP e se não há pacotes TCP FIN ou 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
```

Do mesmo modo, efetuar uma captura no CVP para assegurar a comunicação bidirecional:

<#root>

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

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

Também é recomendável exportar a captura no formato pcap e verificar o conteúdo do pacote:

<#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
```

Possíveis causas:

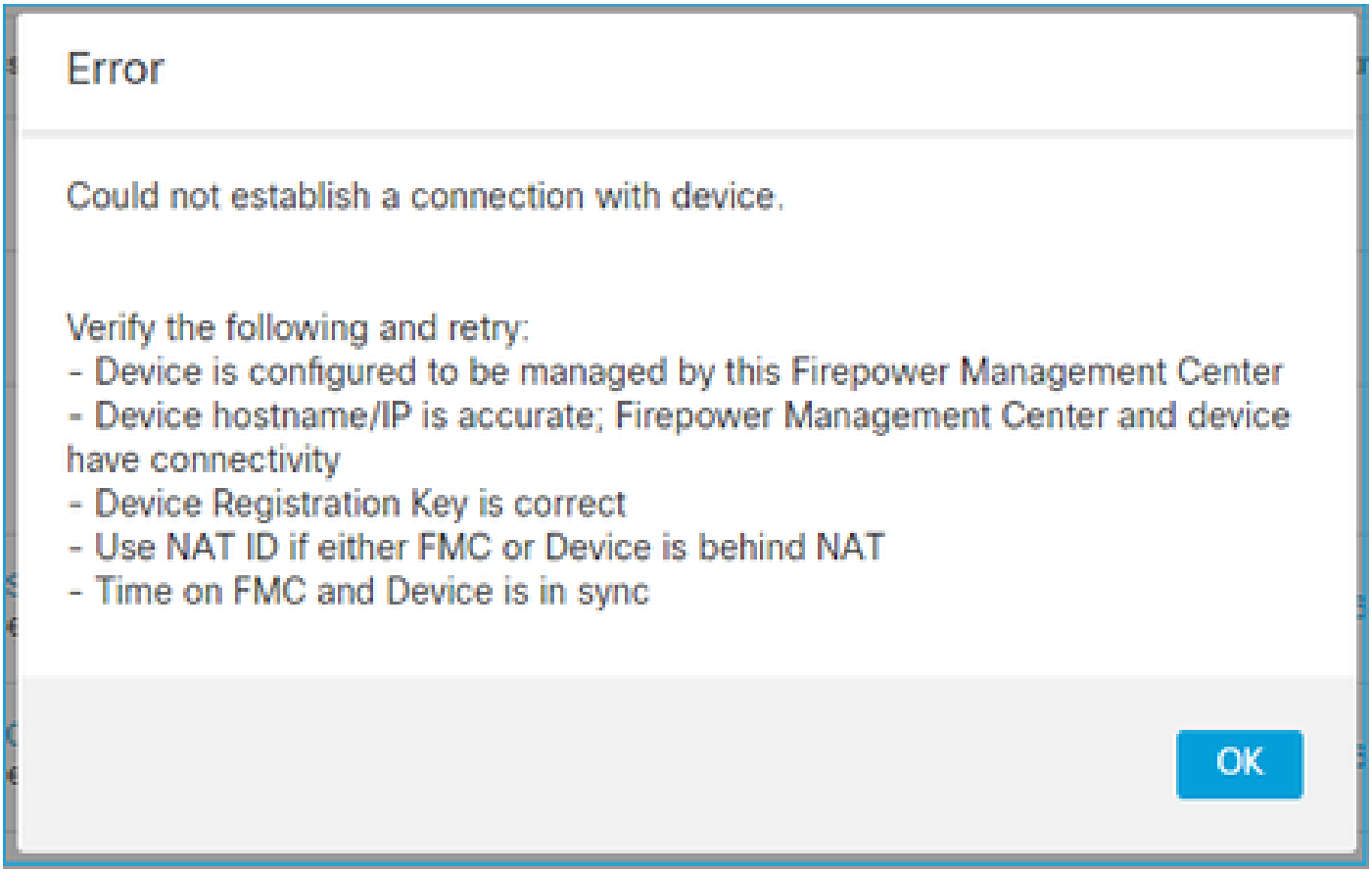
- O FMC não tem o dispositivo FTD adicionado.
- Um dispositivo no caminho (por exemplo, firewall) bloqueia ou modifica o tráfego.
- Os pacotes não são roteados corretamente no caminho.
- O processo sftunnel no FTD ou no FMC está inoperante (verificar cenário 6)
- Há um problema de MTU no caminho (verifique o cenário).

Para análise de captura, verifique este documento:

Analisar as capturas do Firepower Firewall para solucionar problemas de rede com eficiência

4. Software incompatível entre FTD e FMC

A IU do FMC mostra:



Ação recomendada

Verifique o arquivo FTD /ngfw/var/log/messages:

<#root>

```
Apr 19 22:08:09 mzafeiro_vFTD66 SF-IMS[12730]: [12830] sftunneld:sf_connections [INFO] Need to send SW
Apr 19 22:08:09 mzafeiro_vFTD66 SF-IMS[12730]: [12830] sftunneld:sf_channel [INFO] >> ChannelState do_d
Apr 19 22:08:09 mzafeiro_vFTD66 SF-IMS[12730]: [12830] sftunneld:sf_heartbeat [INFO] Saved SW VERSION f
Apr 19 22:08:09 mzafeiro_vFTD66 SF-IMS[12730]: [12830] sftunneld:ssl_mac [WARN]

FMC(manager) 10.62.148.247 send unsupported version 10.10.0.4

Apr 19 22:08:09 mzafeiro_vFTD66 SF-IMS[12730]: [12830] sftunneld:sf_connections [INFO] <<<<<<<<<<<<<<<<
Apr 19 22:08:09 mzafeiro_vFTD66 SF-IMS[12730]: [12830] sftunneld:stream_file [INFO] Stream CTX destroye
Apr 19 22:08:09 mzafeiro_vFTD66 SF-IMS[12730]: [12830] sftunneld:sf_channel [INFO] >> ChannelState Shut
```

Verifique a matriz de compatibilidade do Firepower:

Guia de compatibilidade do Cisco Firepower

5. Diferença temporal entre o FTD e o FMC

A comunicação FTD-FMC é sensível às diferenças de tempo entre os 2 dispositivos. É um requisito de projeto ter o FTD e o FMC sincronizados pelo mesmo servidor NTP.

Especificamente, quando o FTD é instalado em uma plataforma como 41xx ou 93xx, ele usa as configurações de tempo do chassi pai (FXOS).

Ação recomendada

Garantir que o gerenciador de chassis (FCM) e o FMC usem a mesma fonte de tempo (servidor NTP)

6. Processo de sftunnel Inativo ou Desativado

No FTD, o processo sftunnel processa o processo de registro. Este é o status do processo antes da configuração do gerenciador:

<#root>

>

pmtool status

…

sftunnel

(system) -

Waiting

Command:

/ngfw/usr/local/sf/bin/sftunnel -d -f /etc/sf/sftunnel.conf
PID File: /ngfw/var/sf/run/sftunnel.pid
Enable File: /ngfw/etc/sf/sftunnel.conf
CPU Affinity:
Priority: 0
Next start: Mon Apr 20 06:12:06 2020
Required by: sfmgr,sfmbservice,sfipproxy
CGroups: memory=System/ProcessHigh

O status do registro:

<#root>

>

show managers

No managers configured.

Configure o gerenciador:

<#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.

Agora o processo está ATIVADO:

<#root>

>

pmtool status
…
sftunnel

 (system) -

Running

 24386
Command: /ngfw/usr/local/sf/bin/sftunnel -d -f /etc/sf/sftunnel.conf
PID File: /ngfw/var/sf/run/sftunnel.pid
Enable File: /ngfw/etc/sf/sftunnel.conf
CPU Affinity:
Priority: 0
Next start: Mon Apr 20 07:12:35 2020
Required by: sfmgr,sfmbservice,sfipproxy
CGroups: memory=System/ProcessHigh(enrolled)

Em alguns casos raros, o processo pode ser desativado ou desativado:

<#root>

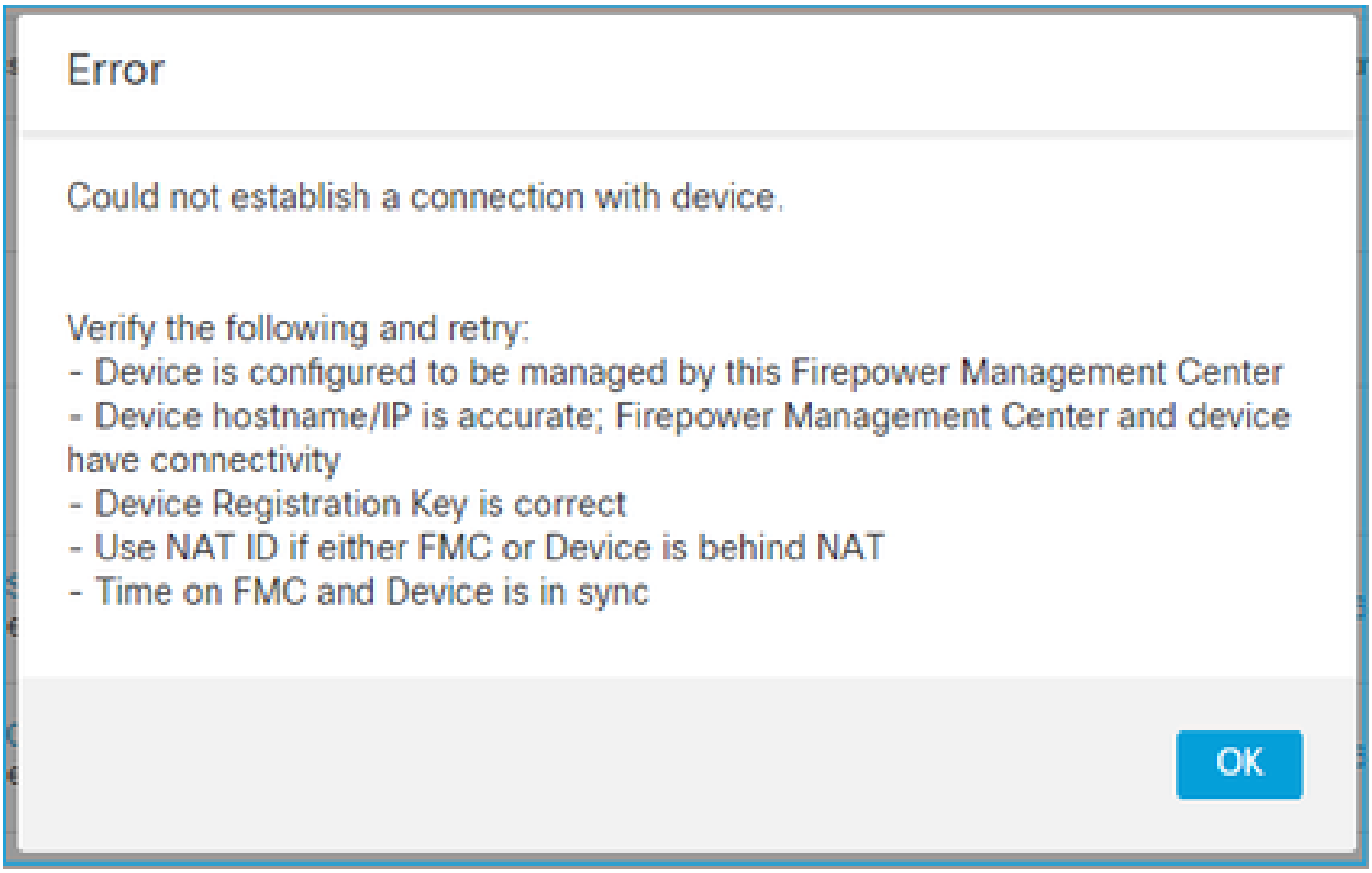
>

```
pmtool status
…
sftunnel

 (system) -

User Disabled

Command: /ngfw/usr/local/sf/bin/sftunnel -d -f /etc/sf/sftunnel.conf
PID File: /ngfw/var/sf/run/sftunnel.pid
Enable File: /ngfw/etc/sf/sftunnel.conf
CPU Affinity:
Priority: 0
Next start: Mon Apr 20 07:09:46 2020
Required by: sfmgr,sfmbservice,sfipproxy
CGroups: memory=System/ProcessHigh
```

O status do gerente parece normal:

```
<#root>

>

show managers

Host                      : 10.62.148.75
Registration Key          : ****

Registration              : pending

RPC Status                :
```

Por outro lado, o registro do dispositivo falha:



No FTD, não há mensagens relacionadas vistas em /ngfw/var/log/messages

Ação recomendada

Colete o arquivo de solução de problemas do FTD e entre em contato com o TAC da Cisco

7. FTD Registro pendente no CVP secundário

Existem cenários em que, após o registro inicial do FTD num CVP HA, o dispositivo de FTD não é adicionado ao CVP secundário.

Ação recomendada

Use o procedimento descrito neste documento:

Use a CLI para resolver o registro de dispositivos no Firepower Management Center High Availability

---

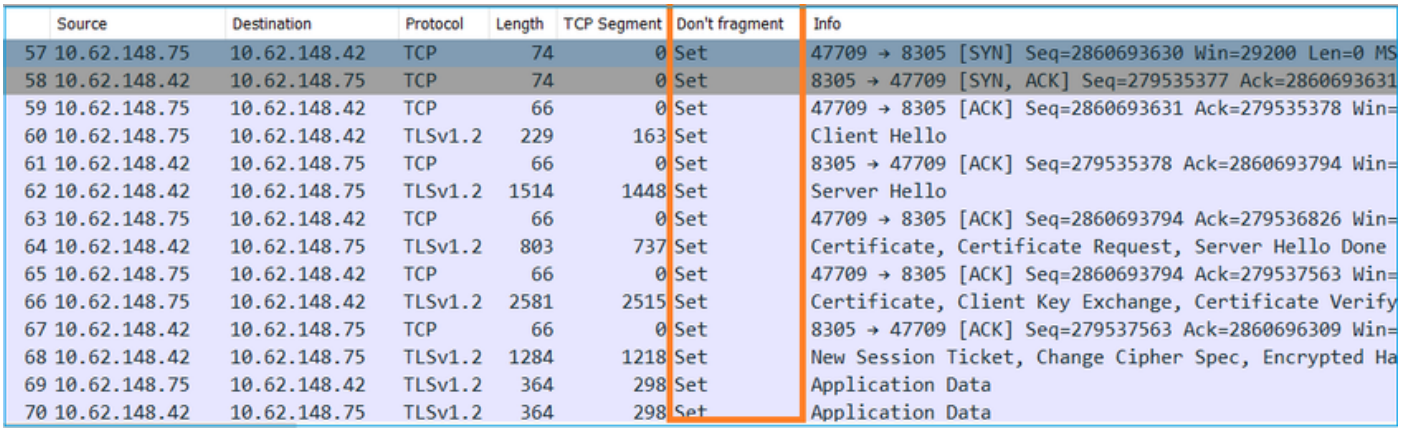
Aviso: este procedimento é intrusivo, pois contém um cancelamento de registro de dispositivo. Isso afeta a configuração do dispositivo FTD (ele é excluído). Recomenda-se usar esse procedimento somente durante o registro e a configuração iniciais do FTD. Em casos diferentes, colete os arquivos de solução de problemas do FTD e do FMC e entre em

---

contato com o TAC da Cisco.

8. Falha no registro devido ao MTU do Caminho

Há cenários vistos no Cisco TAC em que o tráfego de sftunnel tem que atravessar um link que tem uma MTU pequena. Os pacotes sftunnel têm o Conjunto de bits Não fragmentar e, portanto, a fragmentação não é permitida:



	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

Além disso, nos arquivos /ngfw/var/log/messages você pode ver uma mensagem como esta:

MSGS: 10-09 14:41:11 ftd1 SF-IMS[7428]: [6612] sftunneld:sf_ssl [ERRO] Falha no handshake Connect:SSL

Ação recomendada

Para verificar se há perda de pacotes devido à fragmentação, faça capturas no FTD, no FMC e, de preferência, nos dispositivos no caminho. Verifique se você vê pacotes que chegam em ambas as extremidades.

No FTD, diminua o MTU na interface de gerenciamento do FTD. O valor padrão é 1500 bytes. MAX é 1500 para a interface de gerenciamento e 9000 para a interface de eventos. O comando foi adicionado na versão 6.6 do FTD.

Referência de comandos do Cisco Firepower Threat Defense

Exemplo

<#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'
```

Verificação

<#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 o caminho MTU do FTD, você pode usar este comando:

<#root>

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

ping -M do -s 1472 10.62.148.75

A opção do define o bit don't fragment nos pacotes ICMP. Além disso, quando você especifica 1472, o dispositivo envia 1500 Bytes: (cabeçalho IP = 20 Bytes) + (cabeçalho ICMP = 8 Bytes) + (dados ICMP de 1472 Bytes)

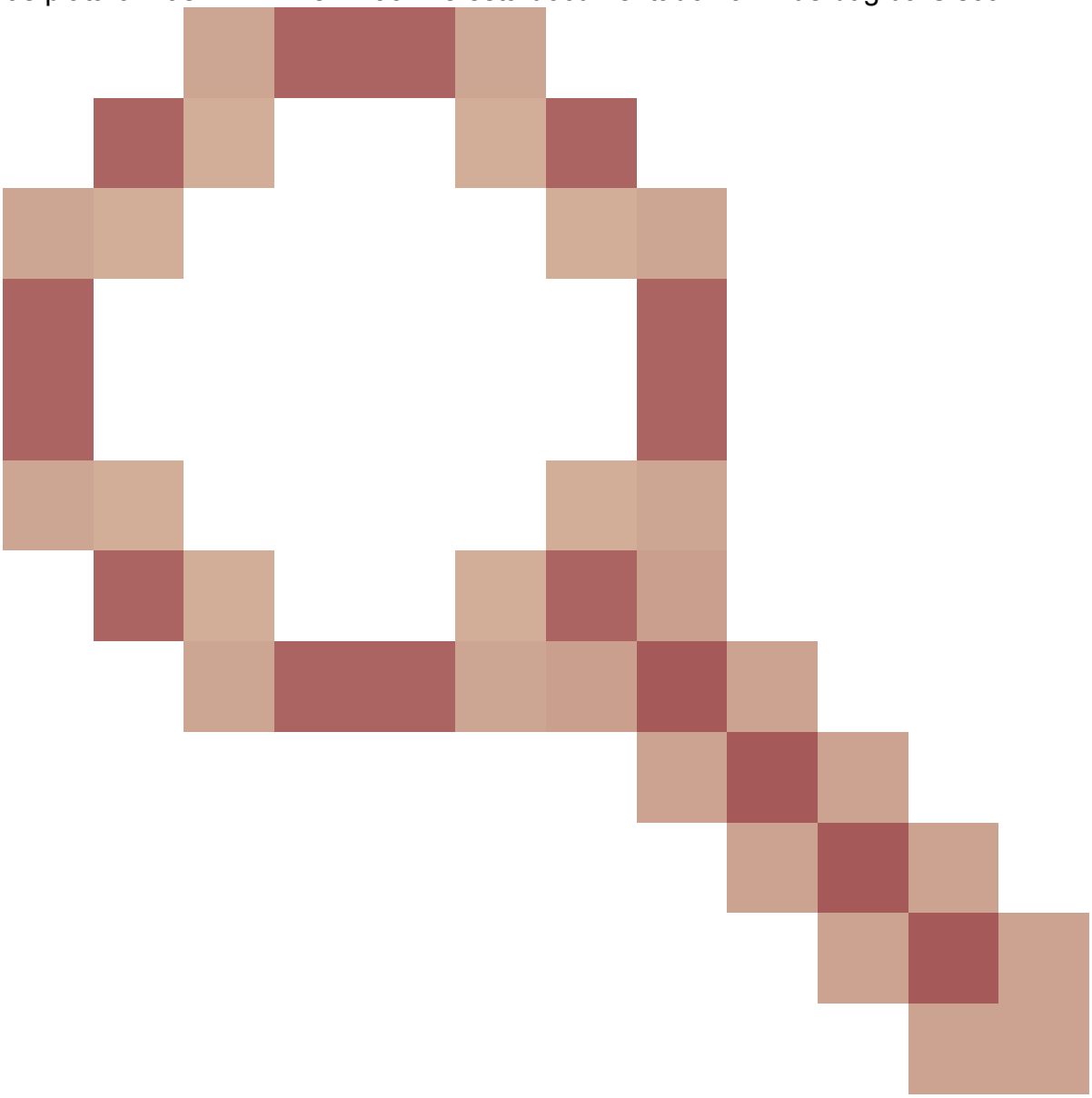
No FMC, reduza o valor de MTU na interface de gerenciamento do FMC, conforme descrito neste

documento:

[Configurar as interfaces de gerenciamento do Firepower Management Center]

9. O FTD perde o registro após uma alteração de bootstrap na interface do usuário do Gerenciador de Chassi

Isso se aplica às plataformas FP41xx e FP93xx e está documentado na ID de bug da Cisco



[CSCvn45138]

.

Em geral, você não deve fazer alterações de bootstrap no gerenciador de chassis (FCM), a menos que faça uma recuperação de desastre.

Ação recomendada

Caso você tenha feito uma alteração de bootstrap e correspondeu à condição (a comunicação FTD-FMC é interrompida enquanto o FTD é ativado após a alteração de bootstrap), você deverá excluir e registrar novamente o FTD no FMC.

10. O FTD perde o acesso ao FMC devido a mensagens de redirecionamento ICMP

Este problema pode afetar o processo de registro ou interromper a comunicação FTD-FMC após o registro.

O problema, nesse caso, é um dispositivo de rede que envia mensagens de redirecionamento ICMP para a interface de gerenciamento do FTD e comunicações FTD-FMC black holes.

Como identificar esse problema

Nesse caso, 10.100.1.1 é o endereço IP do FMC. No FTD, há uma rota armazenada em cache devido à mensagem de redirecionamento ICMP recebida pelo FTD na interface de gerenciamento:

<#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
```

Ação recomendada

Passo 1

Desative o redirecionamento ICMP no dispositivo que o envia (por exemplo, switch L3 upstream, roteador e assim por diante).

Passo 2

Limpe o cache da rota de FTD da CLI de FTD:

<#root>

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

ip route flush 10.100.1.1

Quando não é redirecionado, ele se parece com:

<#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
```

Referências

- Entender mensagens de redirecionamento ICMP
- ID de bug Cisco CSCvm53282 FTD: Tabelas de roteamento adicionadas por redirecionamentos de ICMP ficam presas no cache de tabela de roteamento para sempre

Informações Relacionadas

- Guias de configuração do NGFW

Sobre esta tradução
A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.