Firepower Device Registration configureren, controleren en problemen oplossen

Inhoud

Inleiding

In dit document worden de procedures beschreven voor de werking, verificatie en probleemoplossing van de verbinding (sftunnel) tussen een beheerde Firepower Threat Defence (FTD) en het beheerde Firepower Management Center (FMC). De informatie en de voorbeelden zijn gebaseerd op FTD, maar de meeste concepten zijn ook volledig van toepassing op NGIPS (7000/8000 Series toestellen) of een FirePOWER-module op ASA55xx.

Voorwaarden

Vereisten

Er zijn geen specifieke vereisten van toepassing op dit document.

Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

- FTD-software 6.6.x en 6.5.x
- FMC-software 6.6.x

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u zorgen dat u de potentiële impact van elke opdracht begrijpt.

Achtergrondinformatie

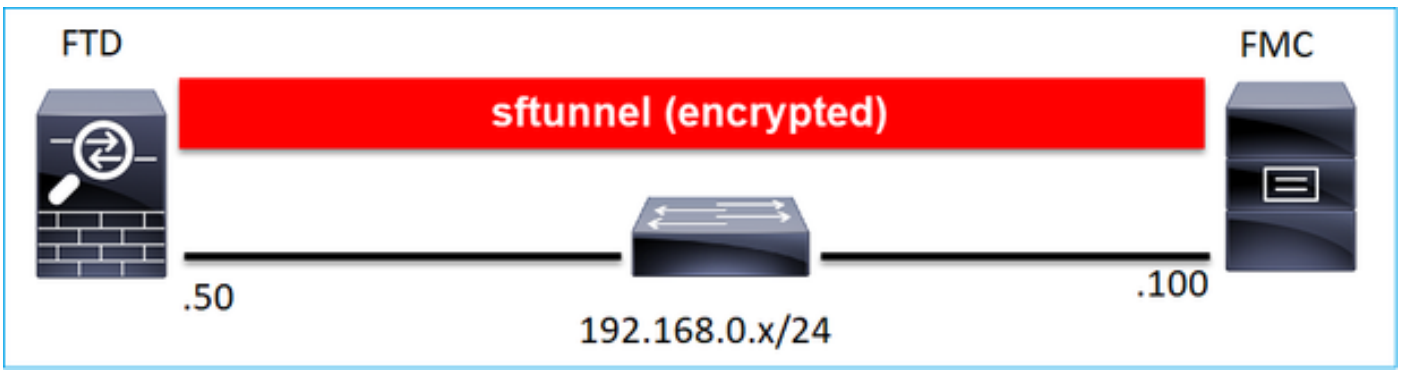
Een FTD ondersteunt twee hoofdbeheermodi:

- Off-box via FMC - ook bekend als remote management
- On-box via Firepower Device Manager (FDM) en/of Cisco Defense Orchestrator (CDO) - ook bekend als lokaal beheer

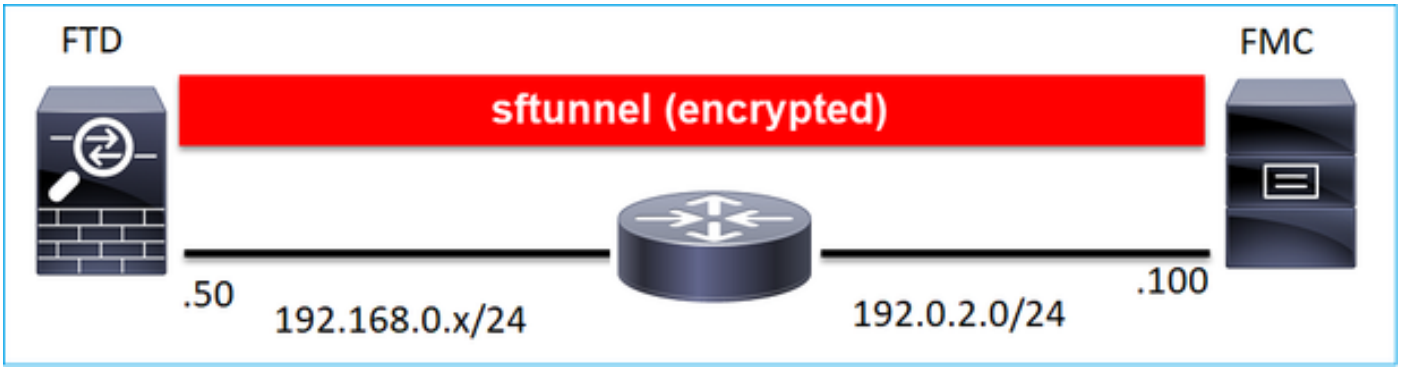
Bij beheer op afstand moet het FTD zich eerst registreren bij het VCC dat gebruikmaakt van een proces dat bekend staat als apparaatregistratie. Na de registratie zetten het FTD en het FMC een beveiligde tunnel op, de zogenaamde sftunnel (de naam komt van de Sourcefire-tunnel).

Ontwerpopties

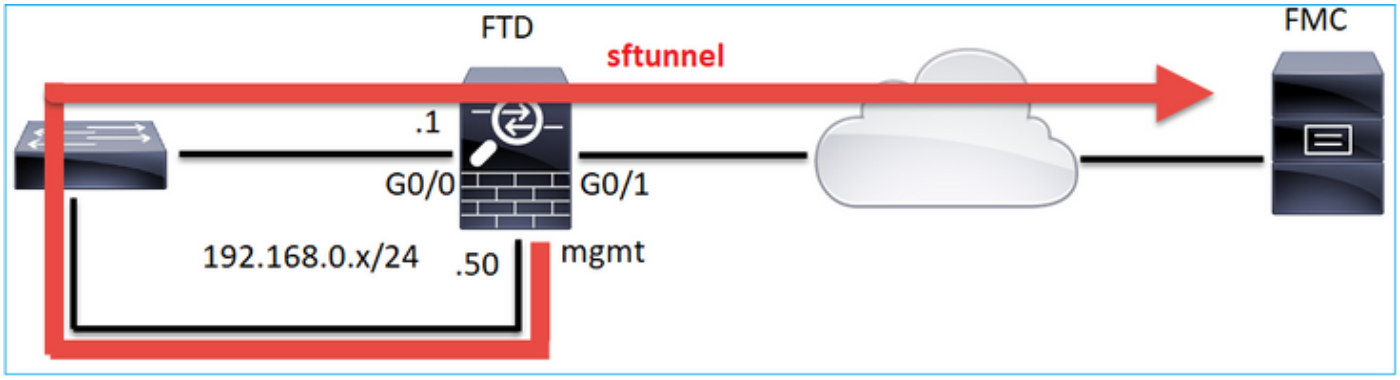
Vanuit ontwerpoogpunt kan het FTD - FMC in hetzelfde L3-subnet worden geplaatst:



of worden gescheiden door verschillende netwerken:



Opmerking: De sftunnel kan ook door de FTD zelf gaan. Dit ontwerp wordt **niet aanbevolen**. De reden hiervoor is dat een FTD dataplatform probleem de communicatie tussen FTD en FMC kan verstoren.



Welke informatie wordt uitgewisseld door de sftunnel?

Deze lijst bevat de meeste informatie die door de sftunnel wordt gedragen:

- Applicatie hartslag (keepalives)
- Tijdsynchronisatie (NTP)
- Gebeurtenissen (verbinding, inbraak/IPS, bestand, SSL enzovoort)
- Malware Lookups
- Gezondheid-evenementen/meldingen
- Informatie over gebruikers en groepen (voor identiteitsbeleid)
- FTD HA state info
- FTD Cluster status info
- Security Intelligent (SI) informatie/evenementen
- Informatie/evenementen over Threat Intelligence Director (TID)
- Opgenomen bestanden
- Detectie-evenementen voor netwerken
- Beleidsbundel (beleidsontwikkeling)
- Software-upgradebundels
- Software-patchbundels

- VDB's
- SRU

Welk protocol/poort wordt gebruikt door de sftunnel?

De sftunnel maakt gebruik van **TCP**-poort **8305**. In de backend is het een **TLS**-tunnel:

No.	Source	Destination	Protocol	Length	TCP Segment	Info
57	10.62.148.75	10.62.148.42	TCP	74	0	47709 → 8305 [SYN] Seq=2860693630 Win=29200 Len=0 MSS=1460 SACK_PERM=1 TSval=1176730050 TSecr=0 WS=128
58	10.62.148.42	10.62.148.75	TCP	74	0	8305 → 47709 [SYN, ACK] Seq=279535377 Ack=2860693631 Win=28960 Len=0 MSS=1460 SACK_PERM=1 TSval=558472
59	10.62.148.75	10.62.148.42	TCP	66	0	47709 → 8305 [ACK] Seq=2860693631 Ack=279535378 Win=29312 Len=0 TSval=1176730050 TSecr=55847291
60	10.62.148.75	10.62.148.42	TLSv1.2	229	163	Client Hello
61	10.62.148.42	10.62.148.75	TCP	66	0	8305 → 47709 [ACK] Seq=279535378 Ack=2860693794 Win=30080 Len=0 TSval=55847291 TSecr=1176730051
62	10.62.148.42	10.62.148.75	TLSv1.2	1514	1448	Server Hello
63	10.62.148.75	10.62.148.42	TCP	66	0	47709 → 8305 [ACK] Seq=2860693794 Ack=279536826 Win=32128 Len=0 TSval=1176730053 TSecr=55847292
64	10.62.148.42	10.62.148.75	TLSv1.2	803	737	Certificate, Certificate Request, Server Hello Done
65	10.62.148.75	10.62.148.42	TCP	66	0	47709 → 8305 [ACK] Seq=2860693794 Ack=279537563 Win=35072 Len=0 TSval=1176730053 TSecr=55847292
66	10.62.148.75	10.62.148.42	TLSv1.2	2581	2515	Certificate, Client Key Exchange, Certificate Verify, Change Cipher Spec Encrypted Handshake Message
67	10.62.148.42	10.62.148.75	TCP	66	0	8305 → 47709 [ACK] Seq=279537563 Ack=2860696309 Win=35072 Len=0 TSval=55847292 TSecr=1176730056
68	10.62.148.42	10.62.148.75	TLSv1.2	1284	1218	New Session Ticket, Change Cipher Spec, Encrypted Handshake Message
69	10.62.148.75	10.62.148.42	TLSv1.2	364	298	Application Data
70	10.62.148.42	10.62.148.75	TLSv1.2	364	298	Application Data
71	10.62.148.42	10.62.148.75	TLSv1.2	103	37	Application Data
72	10.62.148.75	10.62.148.42	TCP	66	0	47709 → 8305 [ACK] Seq=2860696607 Ack=279539116 Win=40832 Len=0 TSval=1176730059 TSecr=55847292
73	10.62.148.42	10.62.148.75	TLSv1.2	367	301	Application Data
74	10.62.148.75	10.62.148.42	TLSv1.2	103	37	Application Data
75	10.62.148.75	10.62.148.42	TLSv1.2	367	301	Application Data

Hoe de Sftunnel TCP-poort op FTD te wijzigen?

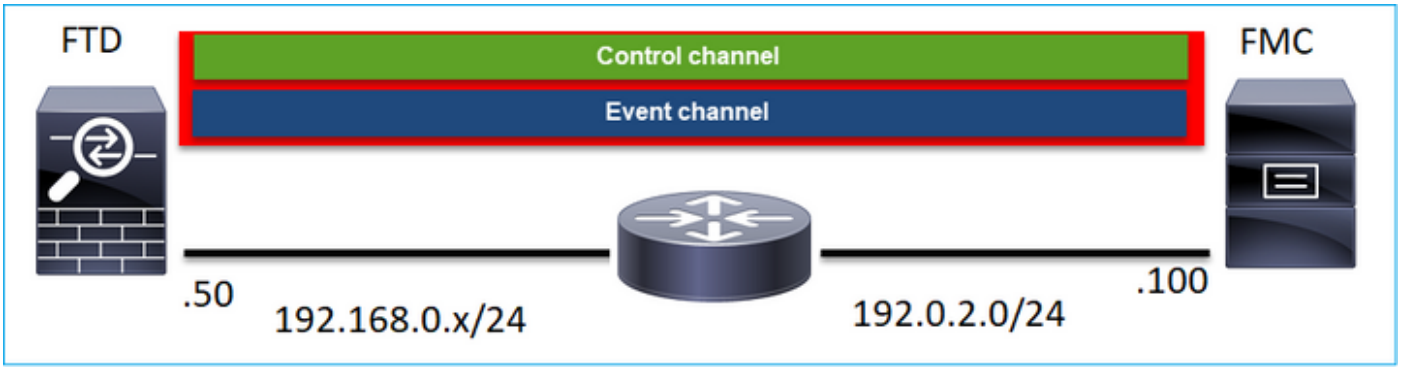
```
> configure network management-port 8306
Management port changed to 8306.
```

> **Opmerking:** In dit geval moet u ook de poort wijzigen op FMC (**Configuration > Management Interfaces > Gedeelde instellingen**). Dit heeft betrekking op alle andere hulpmiddelen die reeds bij hetzelfde VCC zijn geregistreerd. Cisco raadt u ten zeerste aan de standaardinstellingen voor de externe beheerpoort te bewaren, maar als de beheerpoort conflicten heeft met andere communicatie in uw netwerk, kunt u een andere poort kiezen. Als u de beheerpoort wijzigt, moet u deze wijzigen voor alle apparaten in uw implementatie die moeten communiceren.

Hoeveel verbindingen zijn er tot stand gebracht door de sftunnel?

De sftunnel creëert 2 verbindingen (kanalen):

- Controlekanaal
- Gebeurteniskanaal



Welk apparaat initieert elk kanaal?

Dat hangt af van het scenario. Controleer de scenario's die in de rest van het document worden beschreven.

Configureren

Registratiebeginselen

FTD CLI

Op FTD is de basissyntaxis voor de apparaatregistratie:

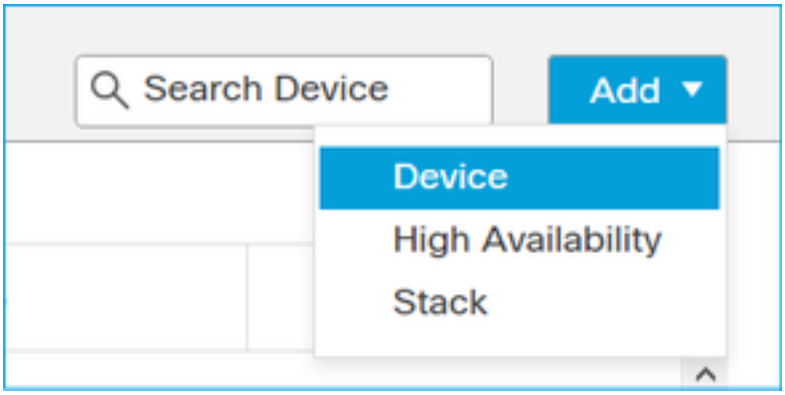
>Manager configureren Voeg <FMC Host> <Registratiesleutel> <NAT ID> toe

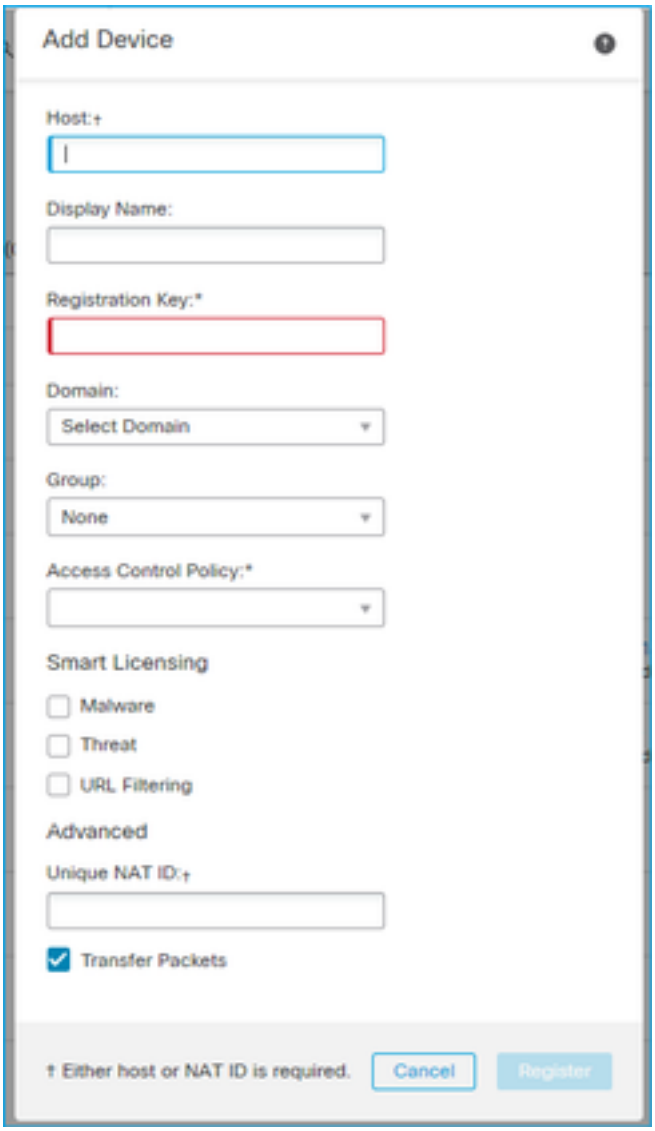
Waarde	Beschrijving
FMC-host	Dit kan zijn: • Hostname • IPv4-adres • IPv6-adres • ONTBINDEN
Registratiesleutel	Dit is een gedeelde geheime alfanumerieke string (tussen 2 en 36 tekens) gebruikt voor de apparaatregistratie. Alleen alfanumeriek, koppelte (-), onderstrepingsteken (_) en punt (.) zijn toeges
NAT-id	Een alfanumerieke tekenreeks die wordt gebruikt tijdens het registratieproces tussen het VCC en h apparaat **wanneer geen van de partijen een IP-ad opgeeft**. Geef dezelfde NAT-ID op het VCC op.

Controleer voor meer informatie de referentie van de Cisco Firepower Threat Defence Command

FMC UI

Ga in het VCC naar **Apparaten > Apparaatbeheer.** Selecteer **Toevoegen > Apparaat**





- Specificeer in de Host het FTD IP-adres.
- Specificeer in de weergavenaam wat u wilt.
- De registratiesleutel moet overeenkomen met de in de FTD CLI gespecificeerde sleutel.
- Indien u meerdere domeinen gebruikt, geef dan het domein op waaronder u het FTD wilt toevoegen.
- Specificeer in de groep Apparaatgroep waaronder u het FTD wilt toevoegen.
- Specificeer in het Toegangsbeheerbeleid het beveiligingsbeleid dat u op FTD wilt implementeren.
- Smart Licensing: Specificeer de licenties die nodig zijn voor de geconfigureerde functies.
- NAT-id: Nodig in specifieke scenario's die later in dit document worden beschreven.

Raadpleeg de configuratiehandleiding van Firepower Management Center voor aanvullende

informatie. Apparaten toevoegen aan het Firepower Management Center

Scenario 1. Statisch IP-adres van het VCC en de FTD

FTD CLI

>configureer beheerder en voeg <FMC Static IP> <Registratiesleutel> toe

Voorbeeld:

```
> 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.
```

Achtergrondinformatie

Zodra u de opdracht FTD invoert, probeert de FTD elke 20 seconden verbinding te maken met het FMC, maar aangezien het FMC nog niet is geconfigureerd, reageert het met TCP RST:

```
> 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
```

De registratiestatus van het apparaat:

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

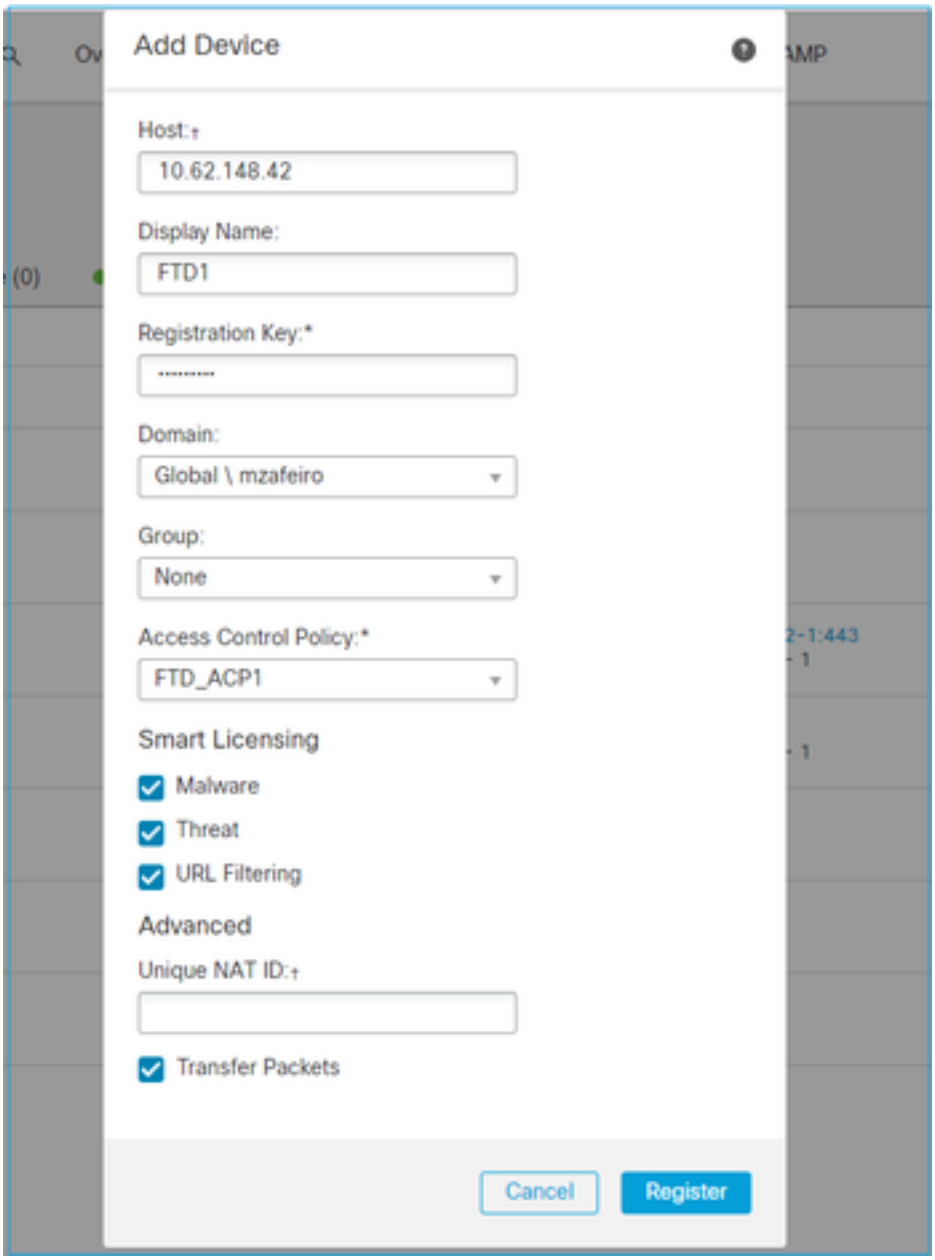
De FTD luistert op poort TCP 8305:

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

FMC UI

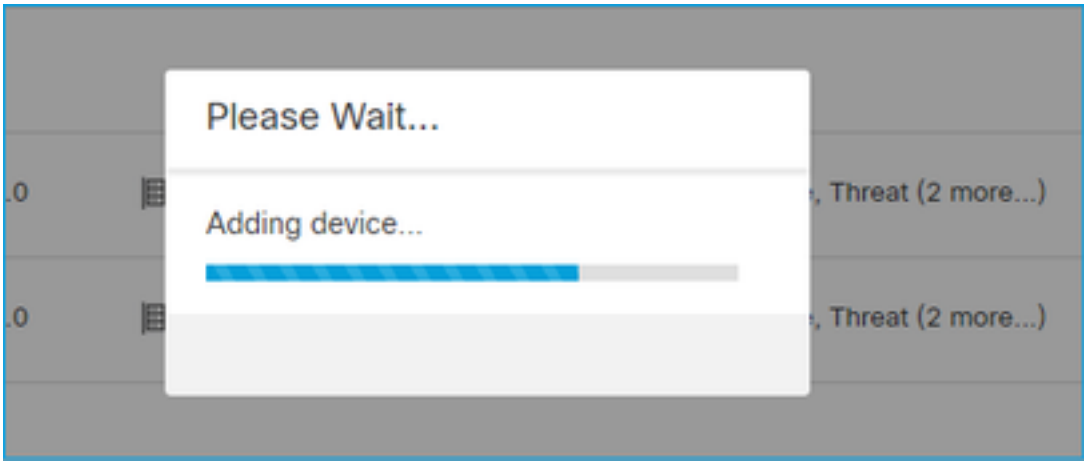
Specificeer in dat geval het volgende:

- Host (IP-adres van de FTD)
- Display naam
- Registratiesleutel (deze moet overeenkomen met de toets die op FTD is geconfigureerd)
- Toegangsbeheerbeleid
- domein
- Smart Licensing-informatie



Selecteer **Registreren**

Het registratieproces wordt gestart:



Het VCC begint te luisteren op poort TCP 8305:

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

Op de achtergrond start het VCC een TCP-verbinding:

```
20:15:55.437434 IP 10.62.148.42.49396 > 10.62.148.75.8305: Flags [S], seq 655146775, win 29200,
options [mss 1460,sackOK,TS val 56302505 ecr 0,nop,wscale 7], length 0
20:15:55.437685 IP 10.62.148.75.8305 > 10.62.148.42.49396: Flags [R.], seq 0, ack 655146776, win
0, length 0
20:16:00.463637 ARP, Request who-has 10.62.148.42 tell 10.62.148.75, length 46
20:16:00.463655 ARP, Reply 10.62.148.42 is-at 00:50:56:85:7b:1f, length 28
20:16:08.342057 IP 10.62.148.75.50693 > 10.62.148.42.8305: Flags [S], seq 2704366385, win 29200,
options [mss 1460,sackOK,TS val 1181294721 ecr 0,nop,wscale 7], length 0
20:16:08.342144 IP 10.62.148.42.8305 > 10.62.148.75.50693: Flags [S.], seq 1829769842, ack
2704366386, win 28960, options [mss 1460,sackOK,TS val 56303795 ecr 1181294721,nop,wscale 7],
length 0
20:16:08.342322 IP 10.62.148.75.50693 > 10.62.148.42.8305: Flags [.], ack 1, win 229, options
[nop,nop,TS val 1181294722 ecr 56303795], length 0
20:16:08.342919 IP 10.62.148.75.50693 > 10.62.148.42.8305: Flags [P.], seq 1:164, ack 1, win
229, options [nop,nop,TS val 1181294722 ecr 56303795], length 163
20:16:08.342953 IP 10.62.148.42.8305 > 10.62.148.75.50693: Flags [.], ack 164, win 235, options
[nop,nop,TS val 56303795 ecr 1181294722], length 0
```

Het sftunnelcontrolekanaal wordt ingesteld:

```
admin@FMC2000-2:~$ netstat -na | grep 8305
tcp        0      0 10.62.148.75:8305       0.0.0.0:*               LISTEN
tcp        0      0 10.62.148.75:50693      10.62.148.42:8305       ESTABLISHED


> sftunnel-status

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

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

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

**RUN STATUS****ksec-fs2k-2-mgmt.cisco.com************
        Cipher used = AES256-GCM-SHA384 (strength:256 bits)
        ChannelA Connected: Yes, Interface eth0
        ChannelB Connected: No
        Registration: Completed.
        IPv4 Connection to peer '10.62.148.75' Start Time: Sat Apr 18 20:16:08 2020


PEER INFO:
        sw_version 6.6.0
        sw_build 90
        Management Interfaces: 1
        eth0 (control events) 10.62.148.75,
        Peer channel Channel-A is valid  type (CONTROL), using 'eth0', connected to
```

```
'10.62.148.75' via '10.62.148.42'
        Peer channel Channel-B is not valid
```

Na een paar minuten is het Event kanaal opgericht. De initiator van het kanaal van de Gebeurtenis kan **aan beide kanten** zijn. In dit voorbeeld was het FMC:

```
20:21:15.347587 IP 10.62.148.75.43957 > 10.62.148.42.8305: Flags [S], seq 3414498581, win 29200,
options [mss 1460,sackOK,TS val 1181601702 ecr 0,nop,wscale 7], length 0
20:21:15.347660 IP 10.62.148.42.8305 > 10.62.148.75.43957: Flags [S.], seq 2735864611, ack
3414498582, win 28960, options [mss 1460,sackOK,TS val 56334496 ecr 1181601702,nop,wscale 7],
length 0
20:21:15.347825 IP 10.62.148.75.43957 > 10.62.148.42.8305: Flags [.], ack 1, win 229, options
[nop,nop,TS val 1181601703 ecr 56334496], length 0
20:21:15.348415 IP 10.62.148.75.43957 > 10.62.148.42.8305: Flags [P.], seq 1:164, ack 1, win
229, options [nop,nop,TS val 1181601703 ecr 56334496], length 163
```

De willekeurige bronpoort duidt de aansluitingsinitiator aan:

```
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
```

Indien het Event-kanaal door de FTD is geïnitieerd, is de output:

```
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
```

Van FTD-zijde:

```
> sftunnel-status

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

        Both IPv4 and IPv6 connectivity is supported
        Broadcast count = 6
        Reserved SSL connections: 0
        Management Interfaces: 1
        eth0 (control events) 10.62.148.42,

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

**RUN STATUS****ksec-fs2k-2-mgmt.cisco.com*************
        Cipher used = AES256-GCM-SHA384 (strength:256 bits)
        ChannelA Connected: Yes, Interface eth0
        Cipher used = AES256-GCM-SHA384 (strength:256 bits)
        ChannelB Connected: Yes, Interface eth0
        Registration: Completed.
        IPv4 Connection to peer '10.62.148.75' Start Time: Sat Apr 18 20:16:08 2020


PEER INFO:
        sw_version 6.6.0
        sw_build 90
        Management Interfaces: 1
```

```
        eth0 (control events) 10.62.148.75,
        Peer channel Channel-A is valid  type (CONTROL), using 'eth0', connected to
'10.62.148.75' via '10.62.148.42'
        Peer channel Channel-B is valid  type (EVENT), using 'eth0', connected to '10.62.148.75'
via '10.62.148.42'


> show managers
Type                      : Manager
Host                      : 10.62.148.75
Registration              : Completed

>
```

Scenario 2. FTD DHCP IP-adres - Statisch IP-adres van FMC

In dit scenario kreeg de FTD management interface zijn IP adres van een DHCP server:

FTD CLI

U moet de NAT-id opgeven:

>Manager configureren - <FMC Static IP> <Registratiesleutel> <NAT-id>

Voorbeeld:

```
> 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.

>
```

De FTD-registratiestatus:

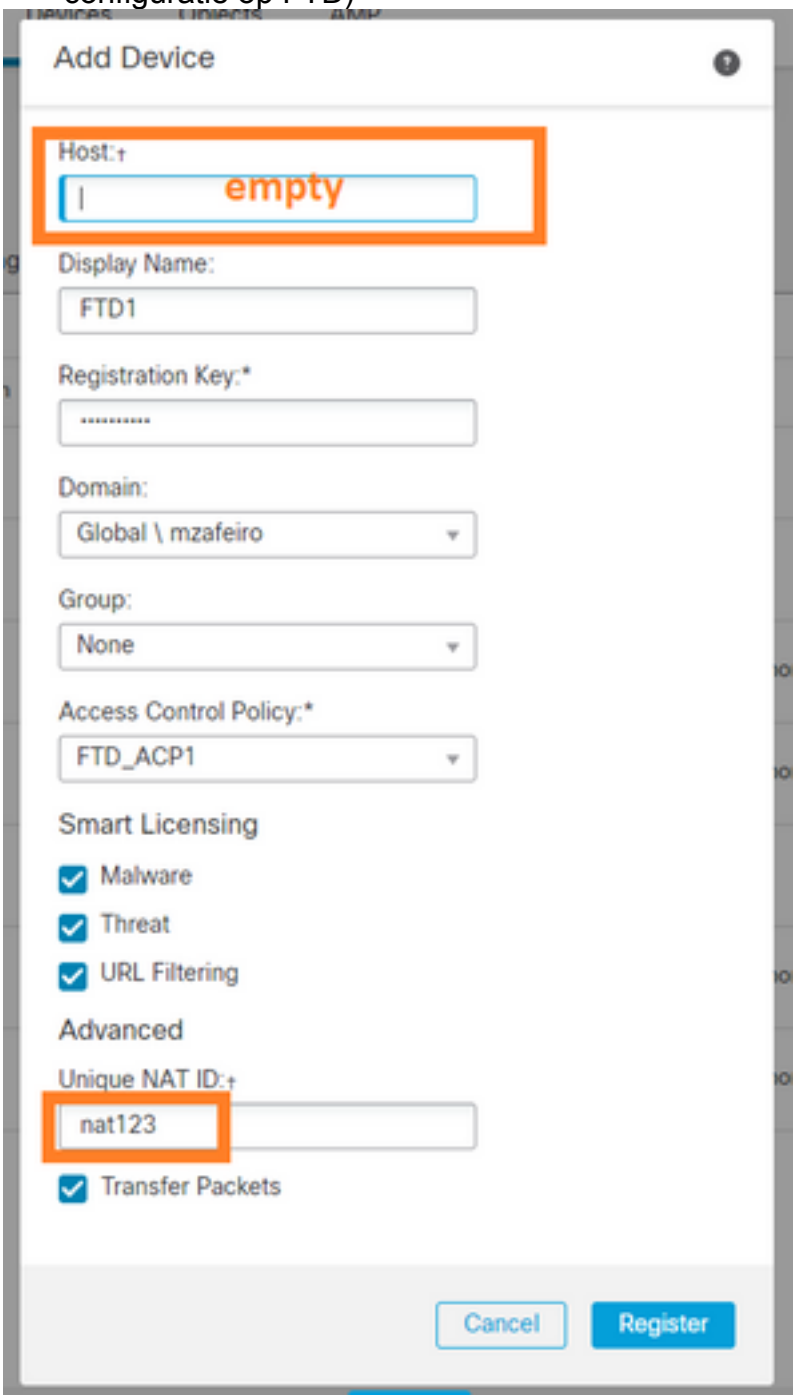
```
> show managers
Host                      : 10.62.148.75
Registration Key          : ****
Registration              : pending
RPC Status                :
```

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

FMC UI

Specificeer in dat geval het volgende:

- Display naam
- Registratiesleutel (deze moet overeenkomen met de toets die op FTD is geconfigureerd)
- Toegangsbeheerbeleid
- domein
- Smart Licensing-informatie
- NAT-id (dit is **vereist** wanneer **Host niet is opgegeven**. Het moet overeenkomen met de configuratie op FTD)

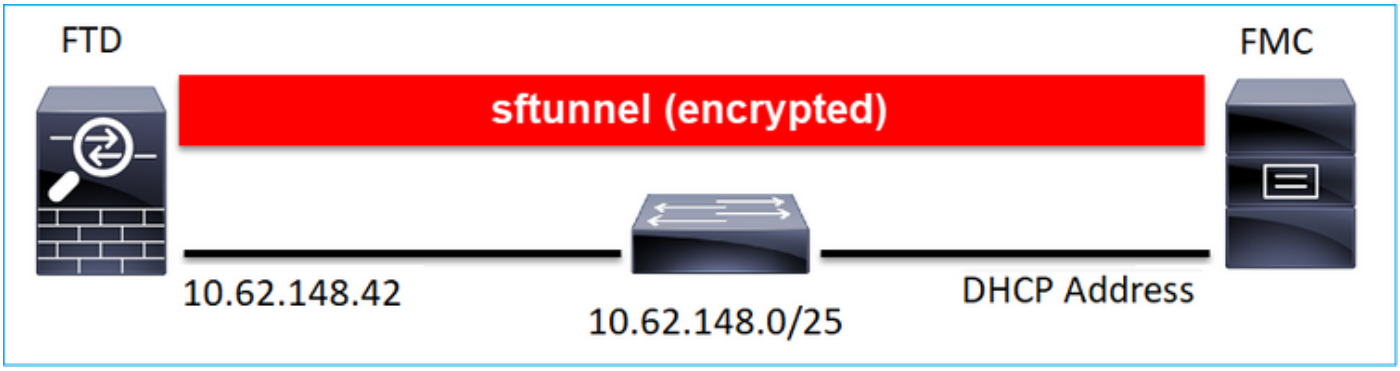


Wie initieert in dit geval de sftunnel?

De FTD initieert beide kanaalverbindingen:

```
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
```

Scenario 3. Statisch IP-adres FTD - DHCP IP-adres van FMC




```
> 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.

>
```

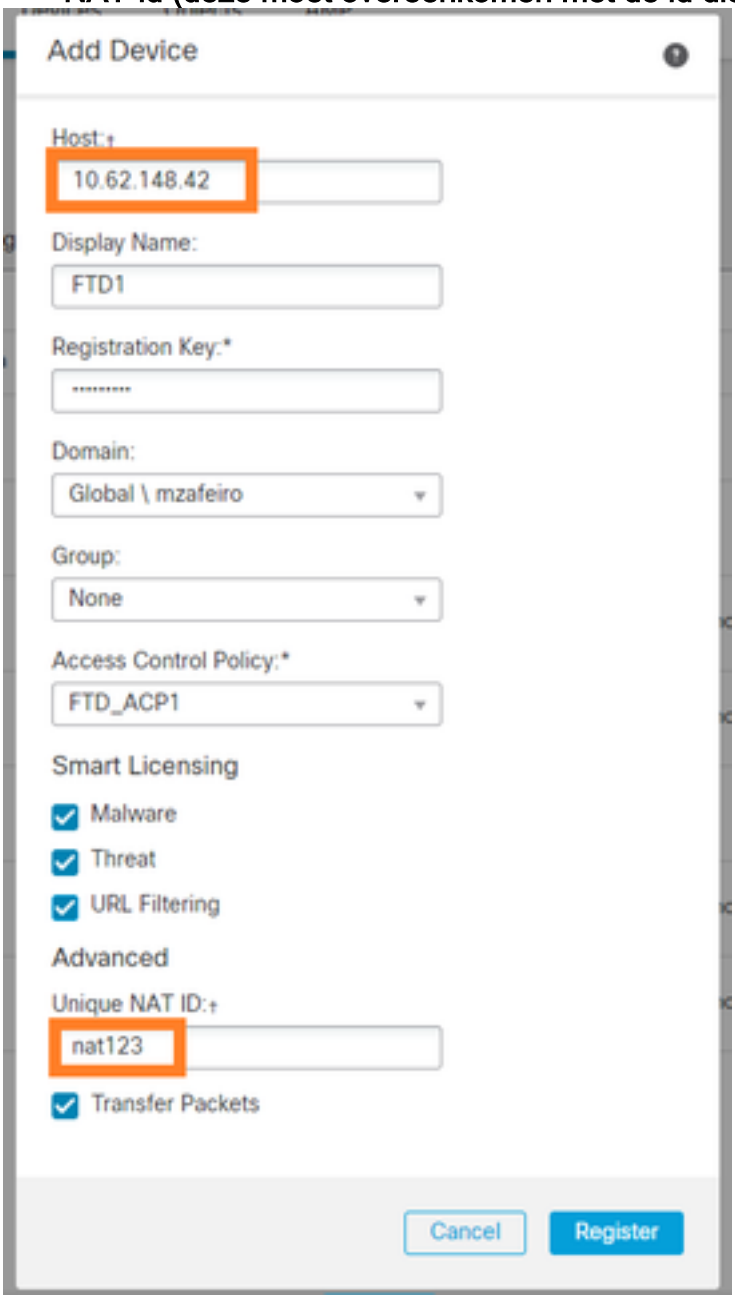
Opmerking: Bij DONTResolution is de NAT-id vereist.

FMC UI

Specificeer in dat geval:

- **FTD IP-adres**
- Display naam
- Registratiesleutel (deze moet overeenkomen met de toets die op FTD is geconfigureerd)
- Toegangsbeheerbeleid
- domein
- Smart Licensing-informatie

- NAT-id (deze moet overeenkomen met de id die op FTD is geconfigureerd)



Het FTD na de registratie:

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

Wie initieert in dit geval de sftunnel?

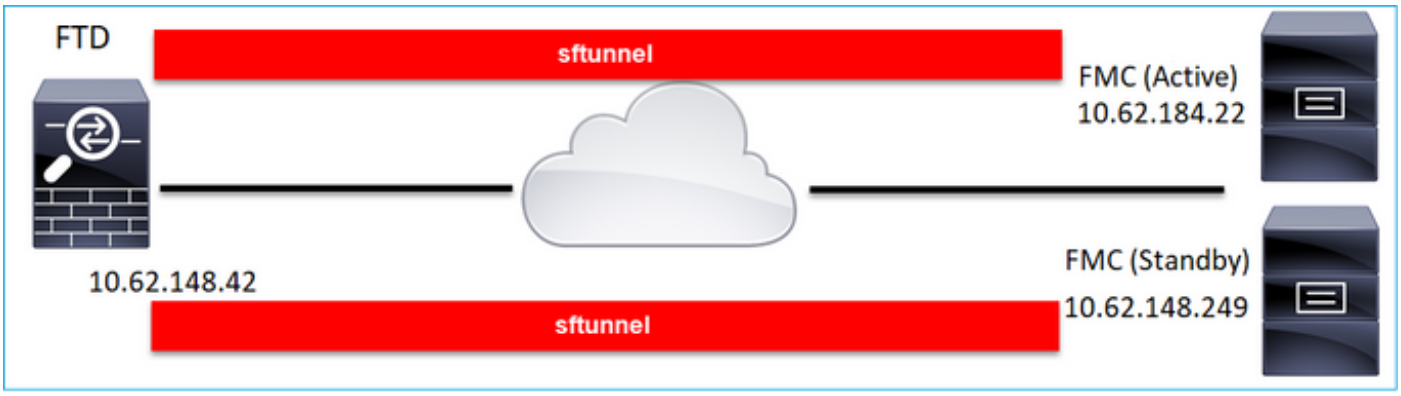
- Het VCC start het controlekanaal.
- Het Event kanaal kan door beide kanten worden geïnitieerd.

```
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
```

Scenario 4. FTD-registratie bij FMC HA

Configureer in FTD alleen het actieve VCC:

```
> 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.
```

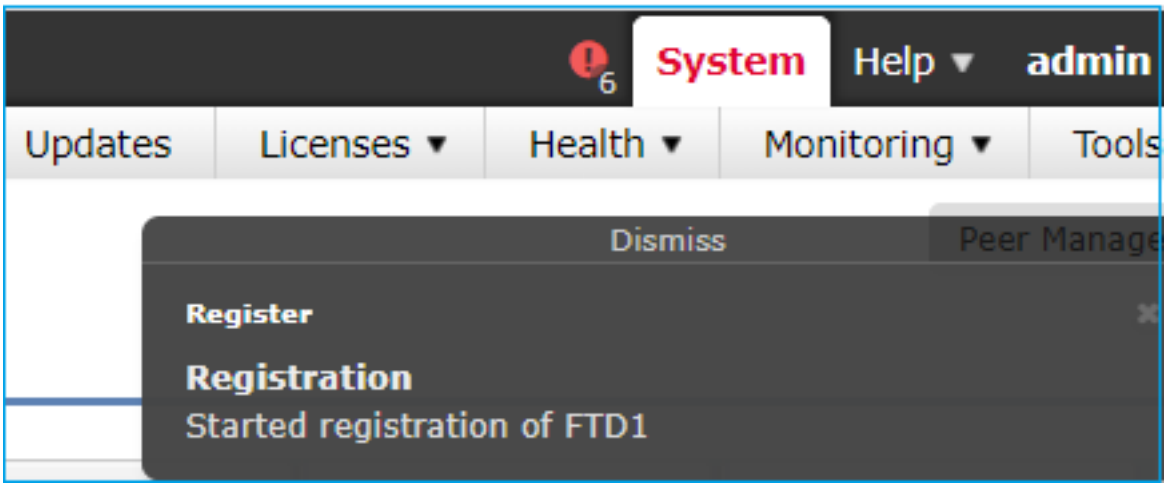


> **Opmerking:** Zorg ervoor dat TCP-poort 8305 verkeer is toegestaan van de FTD naar beide FMC's.

Ten eerste wordt de tunnel naar het actieve VCC ingesteld:

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

Na enkele minuten begint de FTD met de registratie bij het Standby-VCC:



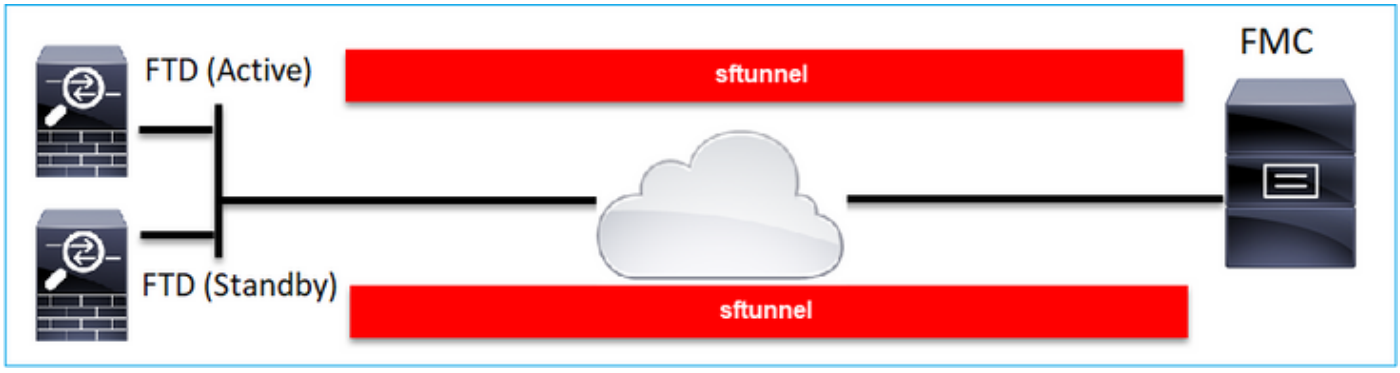

```
> show managers
Type                    : Manager
Host                    : 10.62.184.22
Registration            : Completed

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

In de FTD-backend worden 2 controlekanalen (één naar elk FMC) en 2 evenementkanalen (één naar elk FMC) opgezet:

```
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
```

Scenario 5. FTD HA

In het geval van FTD HA heeft elke eenheid een afzonderlijke tunnel voor het FMC:

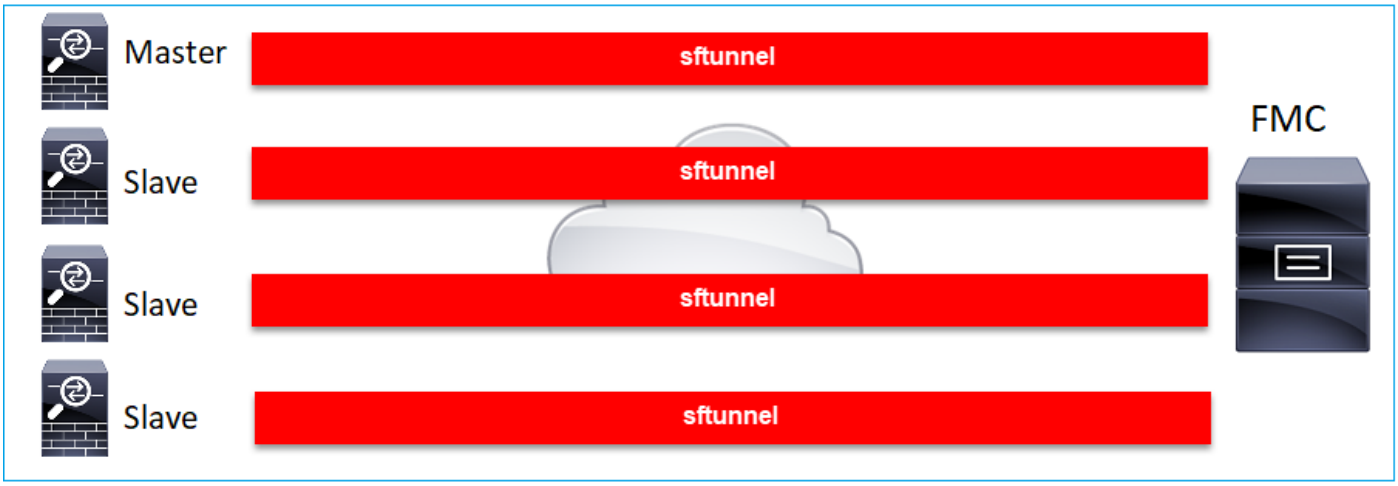


U registreert beide FTDs onafhankelijk en dan van FMC vormt u de FTD HA. Voor meer details:

- Hoge beschikbaarheid van FTD op Firepower-applicaties configureren
- Hoge beschikbaarheid voor Firepower Threat Defence

Scenario 6. FTD-cluster

In het geval van FTD Cluster heeft elke eenheid een afzonderlijke tunnel voor het VCC. Vanaf 6.3 FMC release hoeft u alleen de FTD Master te registreren bij FMC. Vervolgens zorgt het VCC voor de rest van de eenheden en registreert ze automatisch.

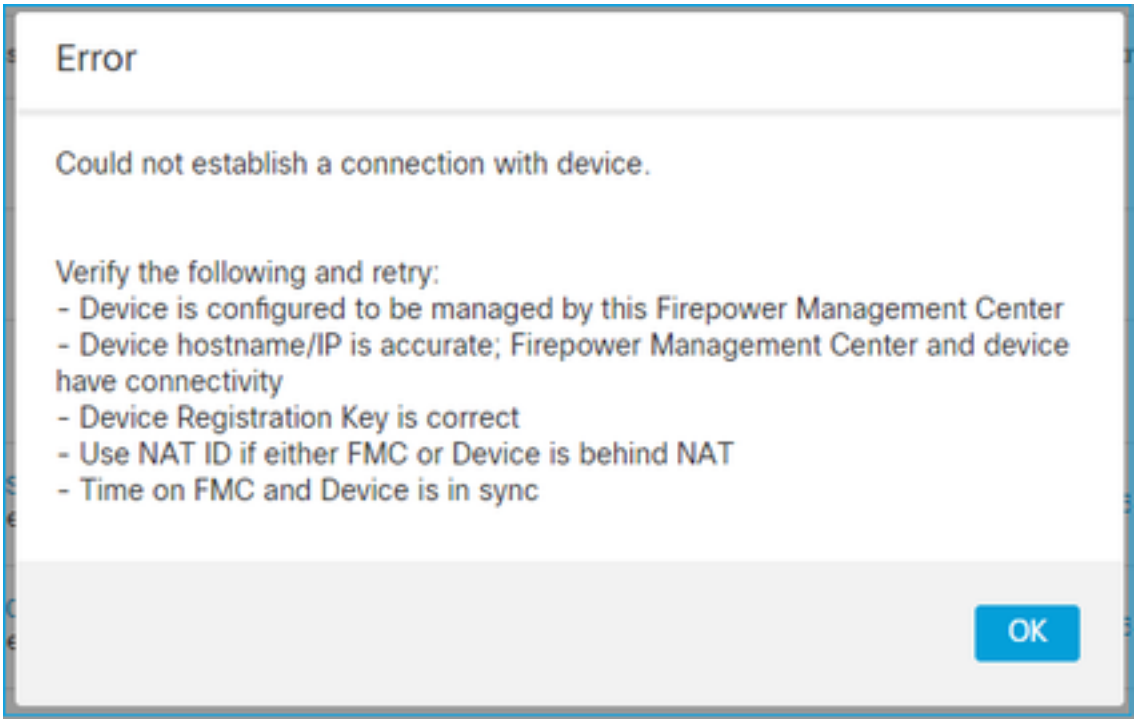


> **Opmerking:** We raden aan om de hoofdeenheid toe te voegen voor de beste prestaties, maar u kunt elke eenheid van het cluster toevoegen. Voor aanvullende details: Een FirePOWER Threat Defense Cluster maken

Gemeenschappelijke problemen oplossen

1. Ongeldige syntaxis op FTD CLI

In het geval van een ongeldige syntaxis op FTD en een mislukte registratiepoging laat de FMC UI een vrij algemene foutmelding zien:



In deze opdracht is de **sleutelwoordsleutel** de registratiesleutel terwijl **cisco123** de NAT-id is. Het is vrij gebruikelijk om de sleutelwoordsleutel toe te voegen terwijl er technisch geen dergelijk sleutelwoord is:

```
> 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.
```

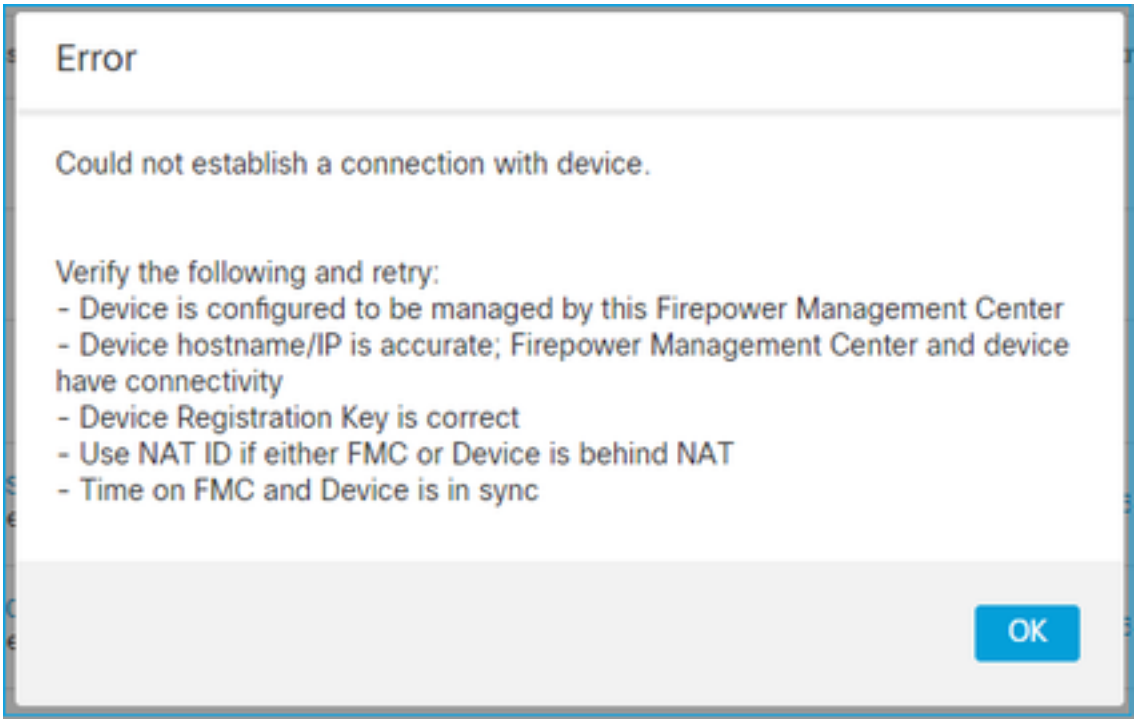
Aanbevolen actie

Gebruik de juiste syntaxis en gebruik geen trefwoorden die niet bestaan.

```
> 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. Onjuiste registratie-sleutel tussen FTD - FMC

De FMC UI toont:



Aanbevolen actie

Controleer op FTD het bestand /ngfw/var/log/message op authenticatieproblemen.

Weg 1 - Controleer de oude logboeken

```
> system support view-files
Type a sub-dir name to list its contents: s

Type the name of the file to view ([b] to go back, [Ctrl+C] to exit)
> messages
Apr 19 04:02:05 vFTD66 syslog-ng[1440]: Configuration reload request received, reloading
configuration;
Apr 19 04:02:07 vFTD66 SF-IMS[3116]: [3116] pm:control [INFO] ControlHandler auditing message-
>type 0x9017, from '', cmd '/ngf
w/usr/bin/perl /ngfw/usr/local/sf/bin/run_hm.pl --persistent', pid 19455 (uid 0, gid 0)
/authenticate

Apr 19 20:17:14 vFTD66 SF-IMS[18974]: [19131] sftunneld:sf_ssl [WARN] Accept: Failed to
authenticate peer '10.62.148.75' <- The problem
```

Weg 2 - Controleer de live logs

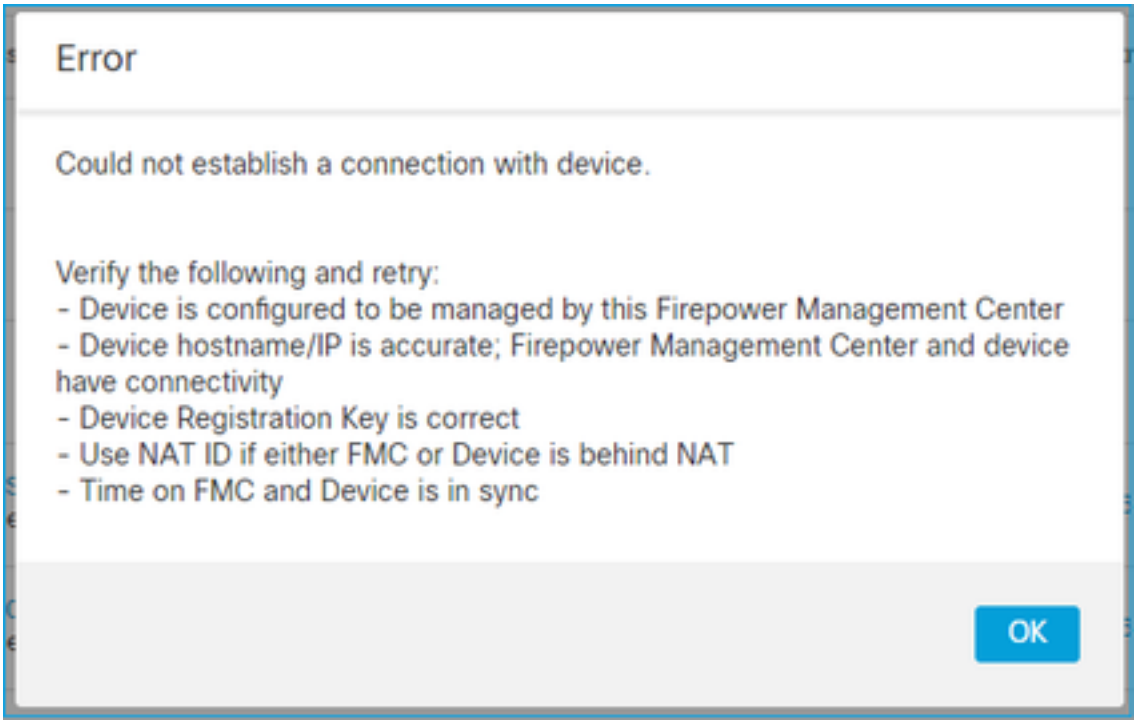
```
> expert
ftd1:~$ sudo su
Password:
ftd1::/home/admin# tail -f /ngfw/var/log/messages
```

Controleer op FTD de inhoud van het /etc/sf/sftunnel.conf bestand om er zeker van te zijn dat de registratiesleutel correct is:

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

3. Connectiviteitsproblemen tussen het FTD en het FMC

De FMC UI toont:



Aanbevolen acties

- Zorg ervoor dat er geen apparaat in het pad is (bijvoorbeeld een firewall) dat het verkeer blokkeert (TCP 8305). In het geval van FMC HA, ervoor zorgen dat verkeer naar TCP-poort 8305 naar beide FMC's is toegestaan.
- Opname nemen om bidirectionele communicatie te verifiëren. Gebruik op FTD de opdracht **Capture-Traffic**. Zorg ervoor dat er een TCP 3-weg handdruk en geen TCP FIN of RST pakketten.

```
> 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
```

Evenzo moet het VCC worden geïnventariseerd om te zorgen voor bidirectionele communicatie:

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

Het wordt ook aanbevolen om de opname in pcap-indeling te exporteren en de pakketinhoud te controleren:

```
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
```

Mogelijke oorzaken:

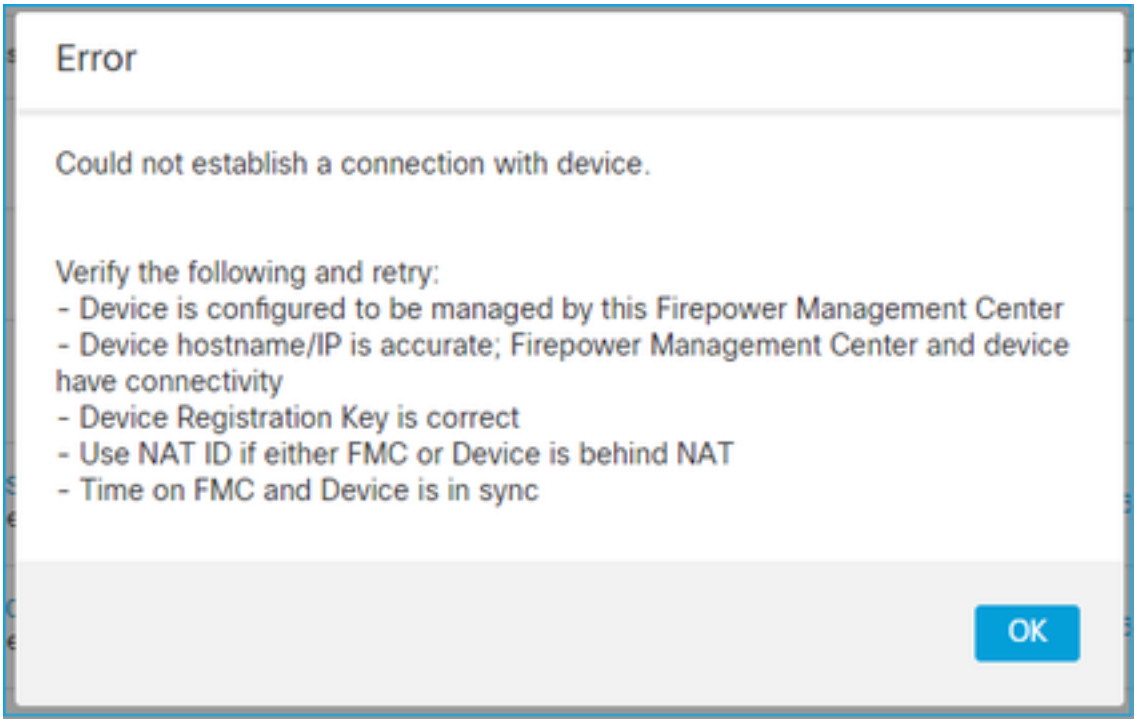
- Het FMC is niet voorzien van het FTD-apparaat.
- Een apparaat in het pad (bijvoorbeeld firewall) blokkeert of wijzigt het verkeer.
- De pakketten worden niet goed op het pad gerouteerd.
- Het Sftunnelproces op FTD of FMC is niet aan de gang (zie scenario 6)
- Er is een MTU probleem in het pad (check scenario).

Controleer voor de opnameanalyse dit document:

Vastleggingen van de Firepower-firewall analyseren om netwerkproblemen effectief te troubleshooten

4. Incompatibele SW tussen FTD en het FMC

De FMC UI toont:



Aanbevolen actie

Controleer het bestand FTD/ngfw/var/log/message:

```
Apr 19 22:08:09 mzafeiro_vFTD66 SF-IMS[12730]: [12830] sftunneld:sf_connections [INFO] Need to
send SW version and Published Services to 10.62.148.247
Apr 19 22:08:09 mzafeiro_vFTD66 SF-IMS[12730]: [12830] sftunneld:sf_channel [INFO] >>
ChannelState do_dataio_for_heartbeat peer 10.62.148.247 / channelA / CONTROL [ msgSock &
ssl_context ] <<
Apr 19 22:08:09 mzafeiro_vFTD66 SF-IMS[12730]: [12830] sftunneld:sf_heartbeat [INFO] Saved SW
VERSION from peer 10.62.148.247 (10.10.0.4)
Apr 19 22:08:09 mzafeiro_vFTD66 SF-IMS[12730]: [12830] sftunneld:ssl_mac [WARN] FMC(manager)
10.62.148.247 send unsupported version 10.10.0.4
Apr 19 22:08:09 mzafeiro_vFTD66 SF-IMS[12730]: [12830] sftunneld:sf_connections [INFO]
<<<<<<<<<<<<<<<<<<<< ShutDownPeer 10.62.148.247 >>>>>>>>>>>>>>>>>>>>
Apr 19 22:08:09 mzafeiro_vFTD66 SF-IMS[12730]: [12830] sftunneld:stream_file [INFO] Stream CTX
destroyed for 10.62.148.247
Apr 19 22:08:09 mzafeiro_vFTD66 SF-IMS[12730]: [12830] sftunneld:sf_channel [INFO] >>
ChannelState ShutDownPeer peer 10.62.148.247 / channelA / CONTROL [ msgSock & ssl_context ] <<
```

Controleer de Firepower Compatibility matrix:

Cisco Firepower Compatibility Guide

5. Tijdverschil tussen FTD en FMC

De FTD-FMC-communicatie is gevoelig voor tijdsverschillen tussen de twee apparaten. Het is een ontwerpvereiste om FTD en FMC te laten synchroniseren door dezelfde NTP-server.

Met name wanneer de FTD op een platform als 41xx of 93xx wordt geïnstalleerd, neemt het zijn

tijdsinstellingen vanaf het moederchassis (FXOS).

Aanbevolen actie

Zorg ervoor dat de chassisbeheerder (FCM) en het VCC dezelfde tijdbron gebruiken (NTP-server)

6. Sftunnelproces omlaag of uitgeschakeld

Op FTD wordt het registratieproces verwerkt in het **sftunnelproces**. Dit is de status van het proces vóór de beheerderconfiguratie:

```
> 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
```

De registratiestatus:

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

Configureer de beheerder:

```
> 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.
```

Nu is het proces UP:

```
> 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)
```

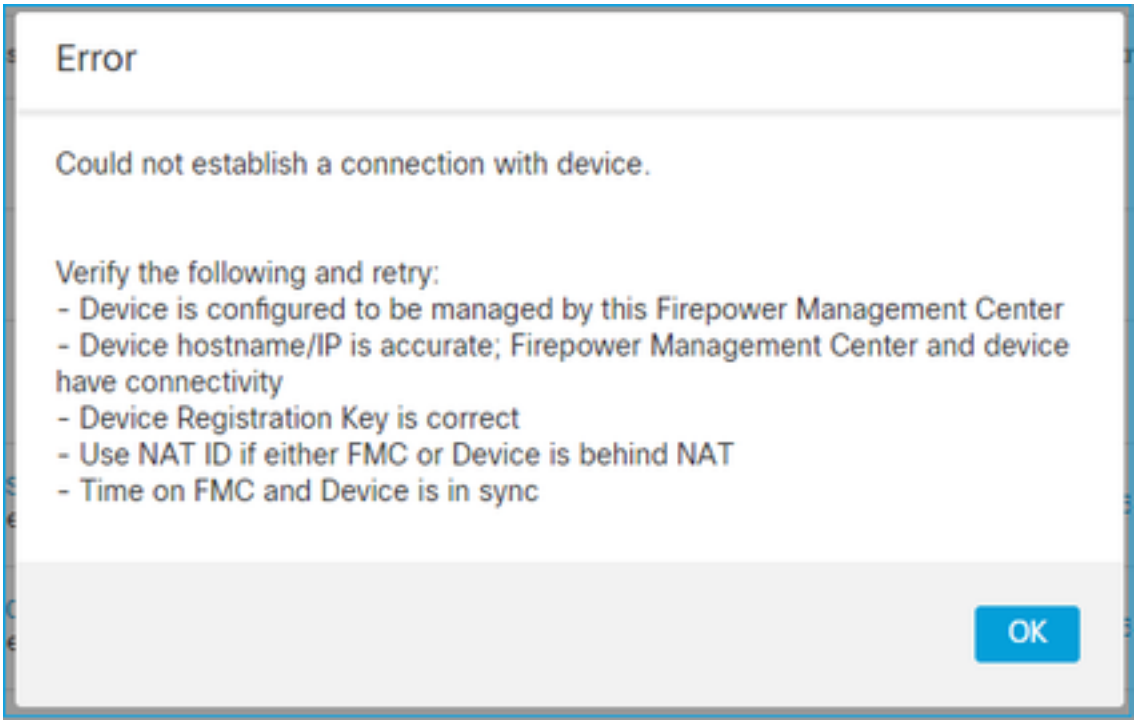
In enkele zeldzame gevallen kan het proces worden uitgeschakeld of uitgeschakeld:

```
> 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
```

De manager status ziet er normaal uit:

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

De registratie van het apparaat is daarentegen mislukt:



Op de FTD worden geen gerelateerde berichten gezien in **/ngfw/var/log/message**

Aanbevolen actie

Verzamel het FTD-probleemoplossingsbestand en neem contact op met Cisco TAC

7. FTD In afwachting van registratie bij secundair FMC

Er zijn scenario's waarin het FTD-apparaat na de initiële FTD-registratie bij een instelling voor FMC HA niet wordt toegevoegd aan het secundaire FMC.

Aanbevolen actie

Volg de in dit document beschreven procedure:

[CLI gebruiken om apparaatregistratie op te lossen in Firepower Management Center hoge beschikbaarheid]

> **Waarschuwing**: Deze procedure is opdringerig aangezien het een apparaat bevat unregistration. Dit beïnvloedt de configuratie van het FTD-apparaat (het wordt verwijderd). Het wordt aanbevolen deze procedure alleen te gebruiken tijdens de eerste FTD-registratie en -instelling. Verzamel in andere gevallen FTD- en FMC-probleemoplossingsbestanden en neem contact op met Cisco TAC.

8. Registratie mislukt vanwege pad MTU

Er zijn scenario's die in Cisco TAC worden gezien waar het sftunnelverkeer een verbinding moet oversteken die kleine MTU heeft. De sftunnelpakketten hebben de **Don't fragment** bit **Set** en fragmentatie is dus niet toegestaan:

	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

Bovendien, in de /ngfw/var/log/message bestanden kunt u een bericht als dit zien:

MNG: 10-09 14:41:11 ftd1 SF-IMS[7428]: [6612] sftunneld:sf_sl [ERROR] **Connect:SSL-handdruk mislukt**

Aanbevolen actie

Om te verifiëren of er pakketverlies door fragmentatie optreedt, neemt u opnamen op FTD, FMC en, idealiter, op apparaten op het pad. Controleer of je pakketten ziet die aan beide uiteinden aankomen.

Op FTD lager de MTU op de FTD-beheerinterface. De standaardwaarde is 1500 bytes. MAX is 1500 voor de Management Interface en 9000 voor de Event Interface. Het commando werd toegevoegd in FTD 6.6 release.

[Referentie van opdracht voor Cisco Firepower Threat Defence]

Voorbeeld

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

Verificatie

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

Om het pad MTU vanaf de FTD te verifiëren kunt u deze opdracht gebruiken:

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

Met de optie **do wordt** het **niet-fragmentatiebit** in ICMP-pakketten ingesteld

Op FMC verlaagt u de MTU-waarde op de FMC-beheerinterface zoals beschreven in dit

document:

Firepower Management Center beheerinterfaces configureren

9. FTD wordt niet geregistreerd na een bootstrap verandering van Chassis Manager UI

Dit is van toepassing op FP41xx- en FP93xx-platforms en gedocumenteerd in Cisco bug-id CSCvn45138 .

In het algemeen, moet u laarzentrekveranderingen van de chassismanager (FCM) niet doen tenzij u een rampenherstel doet.

Aanbevolen actie

Indien u een bootstrap-wijziging hebt uitgevoerd en u aan de voorwaarde voldeed (de FTD-FMC-communicatie is verbroken terwijl de FTD na de bootstrap-wijziging omhoog komt) moet u de FTD verwijderen en opnieuw registreren in FMC.

10. FTD verliest toegang tot het VCC vanwege ICMP-omleidingsberichten

Dit probleem kan van invloed zijn op het registratieproces of de communicatie tussen het FTD en het FMC verstoren na de registratie.

Het probleem in dit geval is een netwerkapparaat dat **ICMP Redirect-**berichten naar de FTD-beheerinterface en de FTD-FMC-communicatie met zwarte gaten verstuurt.

Hoe dit probleem te identificeren

In dit geval is 10.100.1.1 het IP-adres van het VCC. Op FTD is er een gecachede route toe te schrijven aan ICMP redirect bericht dat door FTD op de beheersinterface werd ontvangen:

```
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
```

Aanbevolen actie

Stap 1

Schakel de ICMP-omleiding uit op het apparaat dat de ICMP verstuurt (bijvoorbeeld upstream L3-switch, router enzovoort).

Stap 2

Schakel de FTD route cache uit de FTD CLI:

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

Als het niet wordt omgeleid ziet het er zo uit:

```
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
```

Referenties

- ICMP-omleidingsberichten begrijpen
- Cisco bug-id CSCvm53282 FTD: Routing-tabellen toegevoegd door ICMP-omleidingen blijft voor altijd vast zitten in het routing-tafelcachegeheugen

Gerelateerde informatie

- NGFW-configuratiehandleidingen

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.