

Konfiguration, Überprüfung und Fehlerbehebung bei der Registrierung von FirePOWER-Geräten

Inhalt

[Einleitung](#)

[Voraussetzungen](#)

[Anforderungen](#)

[Verwendete Komponenten](#)

[Hintergrundinformationen](#)

[Designoptionen](#)

[Welche Informationen werden über den sftunnel ausgetauscht?](#)

[Welches Protokoll/welchen Port verwendet der Sftunnel?](#)

[Wie ändere ich den Sftunnel TCP Port auf FTD?](#)

[Wie viele Verbindungen werden durch den Sftunnel hergestellt?](#)

[Welches Gerät initiiert die einzelnen Kanäle?](#)

[Konfigurieren](#)

[Grundlagen der Registrierung](#)

[Szenario 1. Statische IP-Adresse von FMC und FTD](#)

[Szenario 2: FTD DHCP-IP-Adresse - Statische FMC-IP-Adresse](#)

[Szenario 3. Statische FTD-IP-Adresse - FMC DHCP-IP-Adresse](#)

[Szenario 4. FTD-Registrierung bei FMC HA](#)

[Szenario 5. FTD HA](#)

[Szenario 6. FTD-Cluster](#)

[Fehlerbehebung bei gängigen Problemen](#)

[1. Ungültige Syntax in FTD CLI](#)

[2. Nichtübereinstimmung des Registrierungsschlüssels zwischen FTD und FMC](#)

[3. Verbindungsprobleme zwischen FTD - FMC](#)

[4. Inkompatible SW zwischen FTD - FMC](#)

[5. Zeitdifferenz zwischen FTD und FMC](#)

[6. sftunnel-Prozess deaktiviert oder deaktiviert](#)

[7. FTD Ausstehende Registrierung auf sekundärem FMC](#)

[8. Registrierung schlägt aufgrund von Pfad-MTU fehl](#)

[9. FTD wird nach einem Bootstrap-Wechsel von der Chassis-Manager-Benutzeroberfläche abgemeldet](#)

[10. FTD verliert Zugriff auf FMC aufgrund von ICMP-Umleitungsnachrichten](#)

Einleitung

In diesem Dokument werden der Betrieb, die Verifizierung und die Fehlerbehebung für die Verbindung (Sftunnel) zwischen einer verwalteten Firepower Threat Defense (FTD) und dem verwalteten Firepower Management Center (FMC) beschrieben. Die Informationen und Beispiele basieren auf FTD, die meisten Konzepte sind jedoch auch vollständig auf NGIPS (Appliances der Serien 7000/8000) oder ein FirePOWER-Modul auf ASA55xx anwendbar.

Voraussetzungen

Anforderungen

Es gibt keine spezifischen Anforderungen für dieses Dokument.

Verwendete Komponenten

Die Informationen in diesem Dokument basierend auf folgenden Software- und Hardware-Versionen:

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

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle verstehen.

Hintergrundinformationen

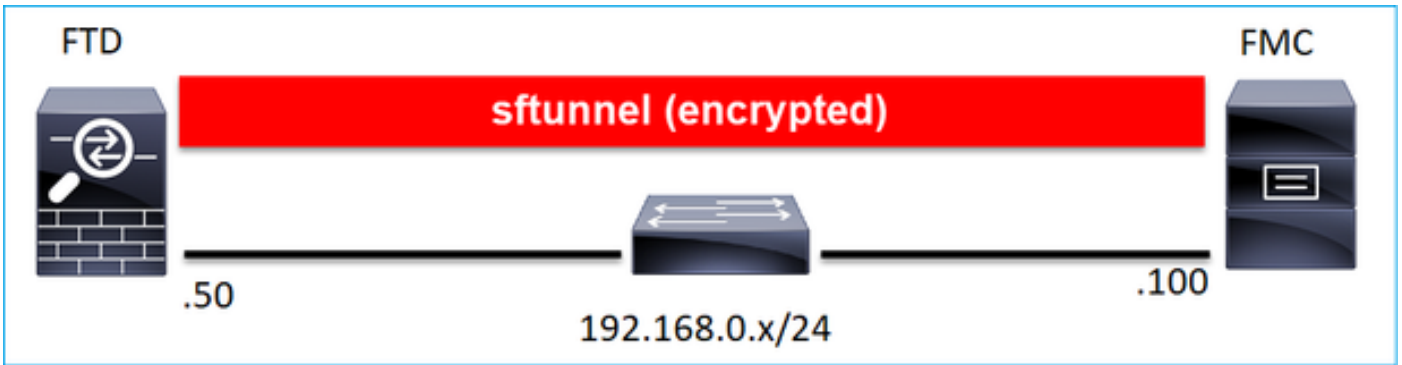
Ein FTD unterstützt zwei Hauptverwaltungsmodi:

- Offbox über FMC - auch bekannt als Remote-Management
- On-Box über FirePOWER Device Manager (FDM) und/oder Cisco Defense Orchestrator (CDO) - auch bekannt als lokales Management

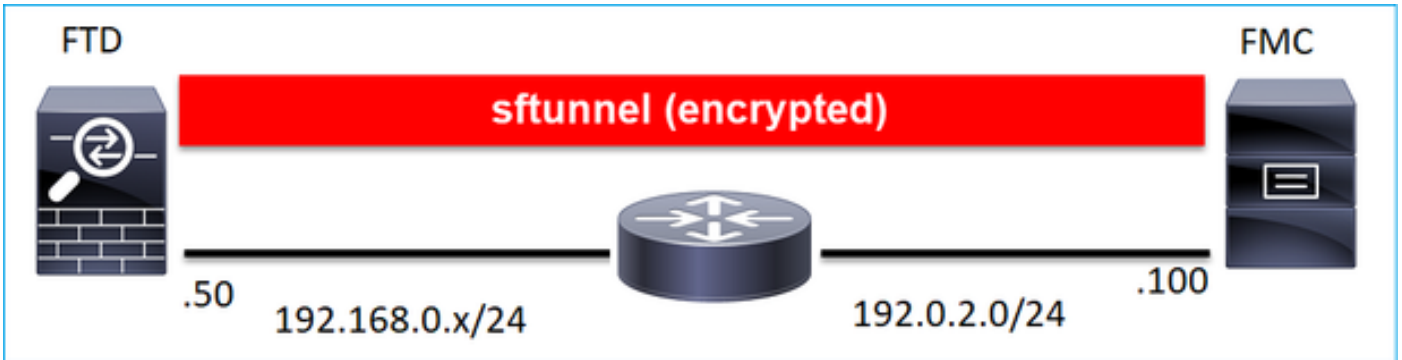
Im Fall der Remote-Verwaltung muss sich die FTD zunächst beim FMC registrieren, das einen Prozess verwendet, der als Geräteregistrierung bezeichnet wird. Nach Abschluss der Registrierung richten die FTD und das FMC einen sicheren Tunnel mit der Bezeichnung "sftunnel" ein (der Name leitet sich vom Sourcefire Tunnel ab).

Designoptionen

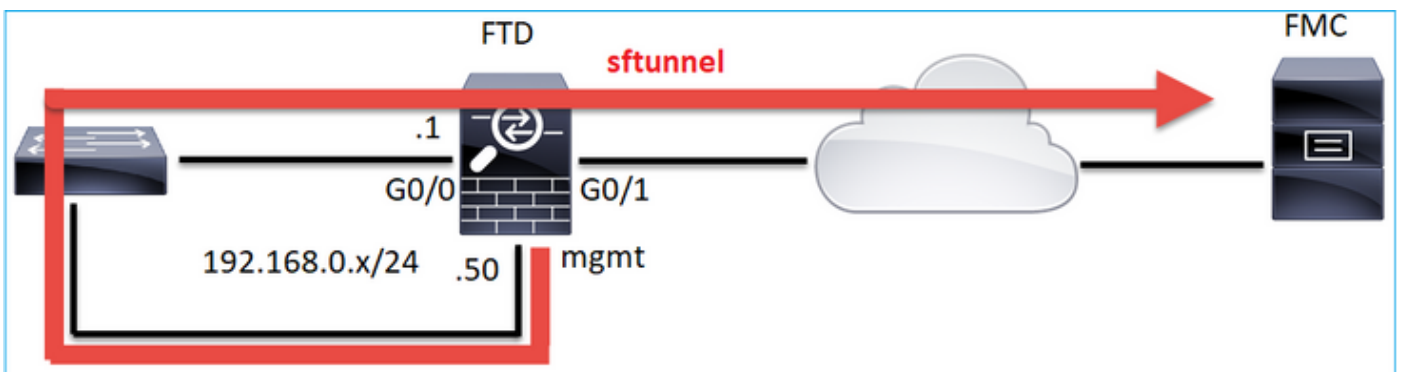
Aus Designsicht kann sich das FTD-FMC im gleichen L3-Subnetz befinden:



oder durch verschiedene Netzwerke getrennt werden:



Anmerkung: Der Sftunnel kann auch die FTD selbst durchlaufen. Dieses Design wird **nicht empfohlen**. Der Grund dafür ist, dass ein FTD-Datenebenenproblem die Kommunikation zwischen FTD und FMC stören kann.



Welche Informationen werden über den sftunnel ausgetauscht?

Diese Liste enthält die meisten Informationen, die über den sftunnel übertragen werden:

- Appliance-Heartbeat (Keepalive)
- Zeitsynchronisierung (NTP)
- Ereignisse (Verbindung, Intrusion/IPS, Datei, SSL usw.)
- Malware-Suchen

- Ereignisse/Warnmeldungen
- Benutzer- und Gruppeninformationen (für Identitätsrichtlinien)
- FTD HA-Statusinformationen
- FTD-Cluster-Statusinformationen
- Security Intelligent (SI) - Informationen/Ereignisse
- Threat Intelligence Director (TID) - Informationen/Ereignisse
- Erfasste Dateien
- Netzwerkerkennungsereignisse
- Richtlinienpaket (Richtlinienbereitstellung)
- Software-Upgrade-Pakete
- Software-Patchpakete
- VDBs
- SRU

Welches Protokoll/welchen Port verwendet der Sftunnel?

Der Sftunnel verwendet den TCP-Port **8305**. Im Backend ist es ein 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

Wie ändere ich den Sftunnel TCP Port auf FTD?

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

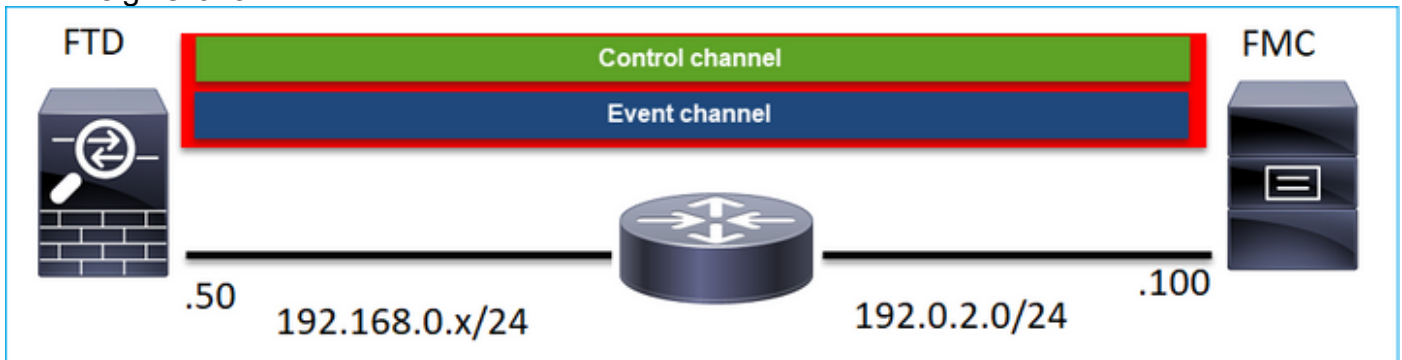
```
Management port changed to 8306.
```

Anmerkung: In diesem Fall müssen Sie auch den Port des FMC ändern (**Konfiguration > Verwaltungsschnittstellen > Gemeinsam genutzte Einstellungen**). Dies betrifft alle anderen Geräte, die bereits beim selben FMC registriert sind. Cisco empfiehlt nachdrücklich, die Standardeinstellungen für den Remote-Management-Port beizubehalten. Wenn der Management-Port jedoch mit anderen Kommunikationsverbindungen in Ihrem Netzwerk in Konflikt gerät, können Sie einen anderen Port auswählen. Wenn Sie den Management-Port ändern, müssen Sie ihn für alle Geräte in Ihrer Bereitstellung ändern, die miteinander kommunizieren müssen.

Wie viele Verbindungen werden durch den Sftunnel hergestellt?

Der Sftunnel stellt 2 Verbindungen (Kanäle) her:

- Steuerkanal
- Ereigniskanal



Welches Gerät initiiert die einzelnen Kanäle?

Das hängt vom Szenario ab. Überprüfen Sie die im restlichen Dokument beschriebenen Szenarien.

Konfigurieren

Grundlagen der Registrierung

FTD-CLI

Auf FTD lautet die grundlegende Syntax für die Geräteregistrierung:

```
>configure manager add <FMC Host> <Registrierungsschlüssel> <NAT-ID>
```

Wert

FMC-Host

Registrierungsschlüssel

NAT-ID

Beschreibung

Dies kann entweder

- Hostname
- IPv4-Adresse
- IPv6-Adresse
- DONTRESOLVE

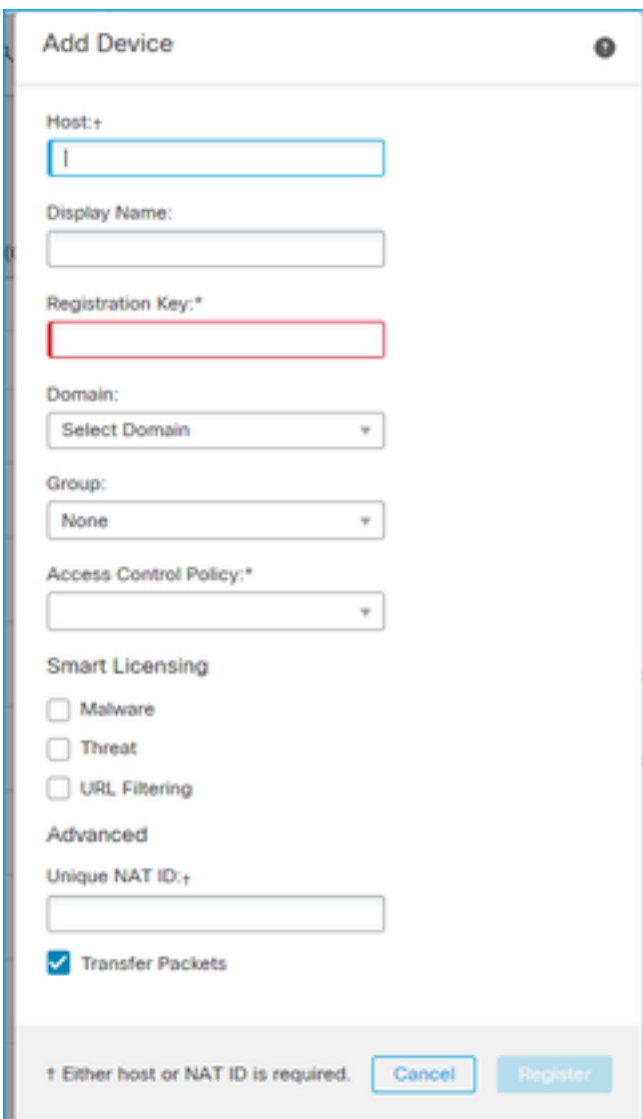
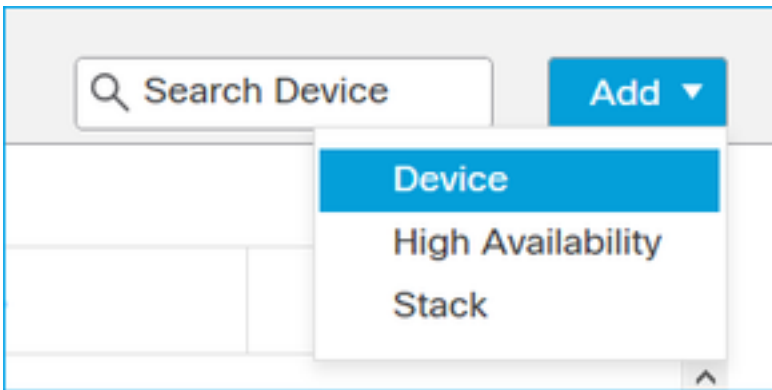
Hierbei handelt es sich um eine alphanumerische Zeichenfolge mit gemeinsamem geheimen Schlüssel (zwischen 2 und 36 Zeichen), die für die Geräteregistrierung verwendet wird. Nur alphanumerische Zeichen, Bindestrich (-), Unterstrich (_) und Punkt (.) sind zulässig.

Eine alphanumerische Zeichenfolge, die bei der Registrierung zwischen dem FMC und dem Gerät verwendet wird, **wenn auf einer Seite keine IP-Adresse angegeben ist**. Geben Sie dieselbe NAT-ID auf dem FMC an.

Weitere Informationen finden Sie in der [Cisco Firepower Threat Defense Command Reference](#)

FMC-Benutzeroberfläche

Navigieren Sie auf FMC zu **Devices (Geräte) > Device Management (Geräteverwaltung)**. Wählen Sie **Hinzufügen > Gerät** aus.

A screenshot of the 'Add Device' form in the FMC interface. The form is titled 'Add Device' and contains several fields and sections. The 'Host:' field is a text input with a cursor. Below it is the 'Display Name:' field. The 'Registration Key:*' field is a text input with a red border. Below that is the 'Domain:' dropdown menu with 'Select Domain' as the current selection. The 'Group:' dropdown menu is set to 'None'. The 'Access Control Policy:*' dropdown menu is empty. The 'Smart Licensing' section has three checkboxes: 'Malware', 'Threat', and 'URL Filtering', all of which are unchecked. The 'Advanced' section has a 'Unique NAT ID:†' text input field. At the bottom, there is a checked checkbox for 'Transfer Packets'. At the very bottom, there is a note: '† Either host or NAT ID is required.' and two buttons: 'Cancel' and 'Register'.

- Geben Sie auf dem Host die FTD-IP-Adresse an.
- Geben Sie im Feld Anzeigename den gewünschten Namen an.

- Der Registrierungsschlüssel muss mit dem in der FTD-CLI angegebenen Schlüssel übereinstimmen.
- Wenn Sie mehrere Domänen verwenden, geben Sie die Domäne an, unter der Sie das FTD hinzufügen möchten.
- Geben Sie in Group (Gruppe) die Gerätegruppe an, der Sie den FTD hinzufügen möchten.
- Geben Sie in der Zugriffskontrollrichtlinie die Sicherheitsrichtlinie an, die Sie auf FTD bereitstellen möchten.
- Smart Licensing: Geben Sie die erforderlichen Lizenzen für die konfigurierten Funktionen an.
- NAT-ID: Erforderlich in spezifischen Szenarien, die weiter unten in diesem Dokument beschrieben werden.

Weitere Informationen finden Sie im Firepower Management Center Configuration Guide, [Add Devices to the Firepower Management Center](#).

Szenario 1. Statische IP-Adresse von FMC und FTD



FTD-CLI

```
>configure manager add <FMC Static IP> <Registrierungsschlüssel>
```

Beispiele:

```
> 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.
```

Hintergrundinformationen

Sobald Sie den FTD-Befehl eingeben, versucht die FTD, alle 20 Sekunden eine Verbindung zum FMC herzustellen. Da das FMC jedoch noch nicht konfiguriert ist, antwortet es mit 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

Registrierungsstatus des Geräts:

> **show managers**

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

Der FTD hört den Port TCP 8305:

```
admin@vFTD66:~$ netstat -na | grep 8305
```

```
tcp        0      0 10.62.148.42:8305      0.0.0.0:*          LISTEN
```

FMC-Benutzeroberfläche

Geben Sie in diesem Fall Folgendes an:

- Host (IP-Adresse des FTD)
- Anzeigename
- Registrierungsschlüssel (dieser muss mit dem auf FTD konfigurierten Schlüssel übereinstimmen)
- Zugriffskontrollrichtlinie
- Domäne

- Smart Licensing-Informationen

Add Device

Host:

Display Name:

Registration Key:

Domain:

Group:

Access Control Policy:

Smart Licensing

- Malware
- Threat
- URL Filtering

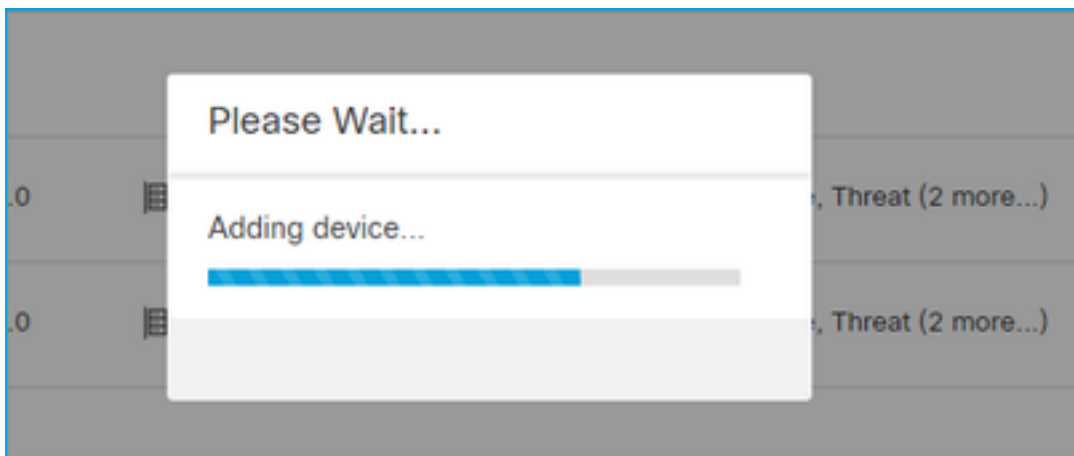
Advanced

Unique NAT ID:

- Transfer Packets

Registrieren auswählen

Der Registrierungsvorgang wird gestartet:



Das FMC beginnt, den Port TCP 8305 abzuhören:

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

Im Hintergrund initiiert das FMC eine TCP-Verbindung:

```
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
```

Der sftunnel-Steuerungskanal wird eingerichtet:

```
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
```

Nach wenigen Minuten ist der Event-Kanal eingerichtet. Der Initiator des Event-Kanals kann auf **beiden Seiten** stehen. In diesem Beispiel war es das 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
```

Der Port der zufälligen Quelle gibt den Verbindungsinitiator an:

```
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
```

Falls der Ereigniskanal von der FTD initiiert wurde, lautet die Ausgabe:

```
admin@FMC2000-2:~$ netstat -na | grep 10.62.148.42
tcp        0      0 10.62.148.75:58409   10.62.148.42:8305    ESTABLISHED
tcp        0      0 10.62.148.75:8305    10.62.148.42:46167   ESTABLISHED
```

FTD-Seite:

```
> 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'

```

```

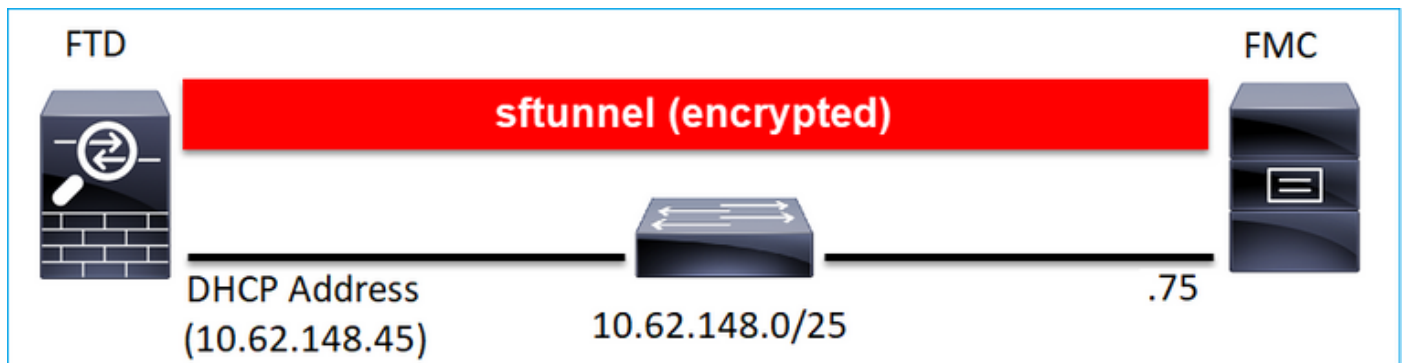
> show managers
Type           : Manager
Host           : 10.62.148.75
Registration   : Completed

```

```
>
```

Szenario 2: FTD DHCP-IP-Adresse - Statische FMC-IP-Adresse

In diesem Szenario hat die FTD-Verwaltungsschnittstelle seine IP-Adresse von einem DHCP-Server erhalten:



FTD-CLI

Sie müssen die NAT-ID angeben:

```
>configure manager add <FMC Static IP> <Registrierungsschlüssel> <NAT-ID>
```

Beispiele:

```

> configure manager add 10.62.148.75 Cisco-123 nat123
Manager successfully configured.
Please make note of reg_key as this will be required while adding Device in FMC.

```

```
>
```

FTD-Registrierungsstatus:

```
> show managers
```

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

FMC-Benutzeroberfläche

Geben Sie in diesem Fall Folgendes an:

- Anzeigename
- Registrierungsschlüssel (dieser muss mit dem auf FTD konfigurierten Schlüssel übereinstimmen)
- Zugriffskontrollrichtlinie
- Domäne
- Smart Licensing-Informationen
- NAT-ID (dies ist **erforderlich**, wenn **Host nicht angegeben ist**. Sie muss mit der FTD-Konfiguration übereinstimmen.)

Add Device

Host:

Display Name:

Registration Key:

Domain:

Group:

Access Control Policy:

Smart Licensing

- Malware
- Threat
- URL Filtering

Advanced

Unique NAT ID:

- Transfer Packets

Wer initiiert in diesem Fall den sftunnel?

Die FTD initiiert beide Kanalverbindungen:

```
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
```

Szenario 3. Statische FTD-IP-Adresse - FMC DHCP-IP-Adresse



```
> 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.

```
>
```

Anmerkung: Bei DONTRESOLVE ist die NAT-ID erforderlich.

FMC-Benutzeroberfläche

Geben Sie in diesem Fall Folgendes an:

- **FTD-IP-Adresse**
- Anzeigename
- Registrierungsschlüssel (dieser muss mit dem auf FTD konfigurierten Schlüssel übereinstimmen)
- Zugriffskontrollrichtlinie
- Domäne
- Smart Licensing-Informationen
- **NAT-ID (muss mit der auf FTD konfigurierten ID übereinstimmen)**

Die FTD nach Abschluss der Registrierung ist:

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

Wer initiiert in diesem Fall den sftunnel?

- Das FMC initiiert den Steuerungskanal.
- Der Event-Kanal kann von beiden Seiten initiiert werden.

```
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
```

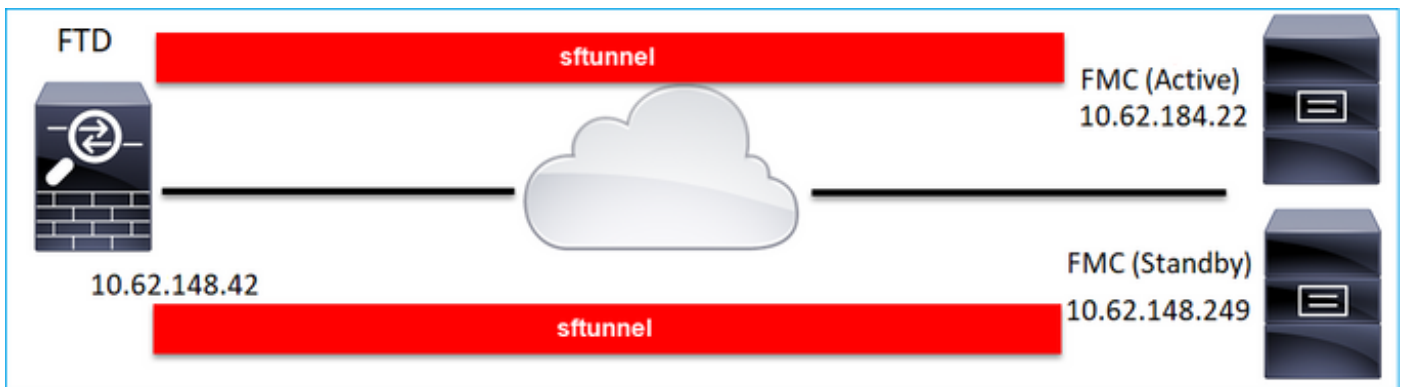

Szenario 4. FTD-Registrierung bei FMC HA

Konfigurieren Sie auf FTD nur das aktive FMC:

```
> 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.



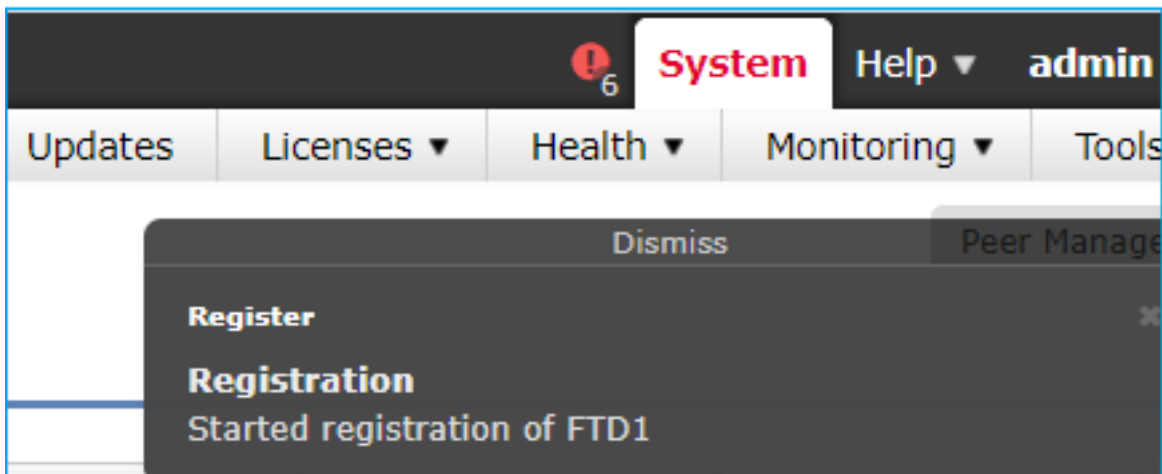
Anmerkung: Stellen Sie sicher, dass Datenverkehr vom TCP-Port 8305 vom FTD zu beiden FMCs zulässig ist.

Zunächst wird der Sftunnel zum aktiven FMC eingerichtet:

```
> show managers
```

```
Type           : Manager
Host           : 10.62.184.22
Registration    : Completed
```

Nach wenigen Minuten beginnt die FTD-Registrierung beim Standby-FMC:



> **show managers**

Type : Manager
Host : **10.62.184.22**
Registration : Completed

Type : Manager
Host : **10.62.148.249**
Registration : Completed

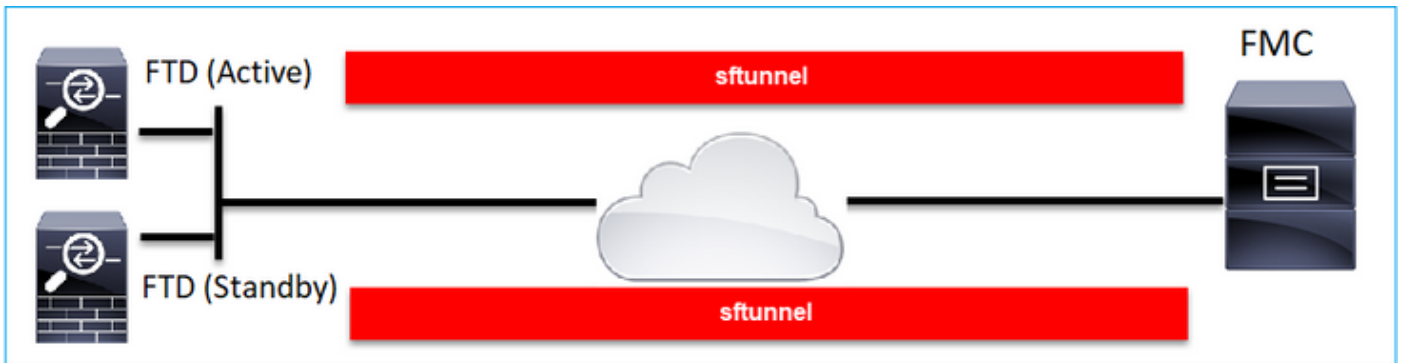
Im FTD-Backend werden 2 Steuerungskanäle (einer zu jedem FMC) und 2 Ereigniskanäle (einer zu jedem FMC) eingerichtet:

```
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
```

Szenario 5. FTD HA

Bei FTD HA verfügt jede Einheit über einen separaten Tunnel zum FMC:

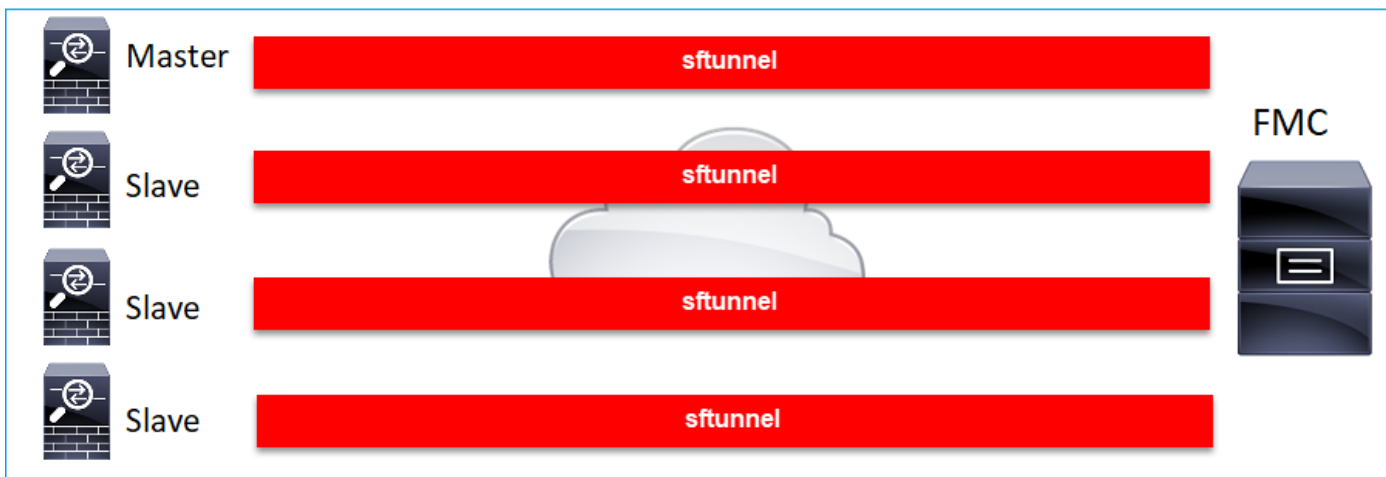


Sie registrieren beide FTDs unabhängig voneinander und bilden dann von FMC aus das FTD HA. Weitere Informationen finden Sie unter:

- [Konfigurieren von FTD-Hochverfügbarkeit auf Firepower-Appliances](#)
- [Hohe Verfügbarkeit für Firepower Threat Defense](#)

Szenario 6. FTD-Cluster

Bei einem FTD-Cluster verfügt jede Einheit über einen separaten Tunnel zum FMC. Ab Version 6.3 des FMC müssen Sie nur noch den FTD Master für FMC registrieren. Dann kümmert sich das FMC um die restlichen Einheiten und erfasst sie automatisch.

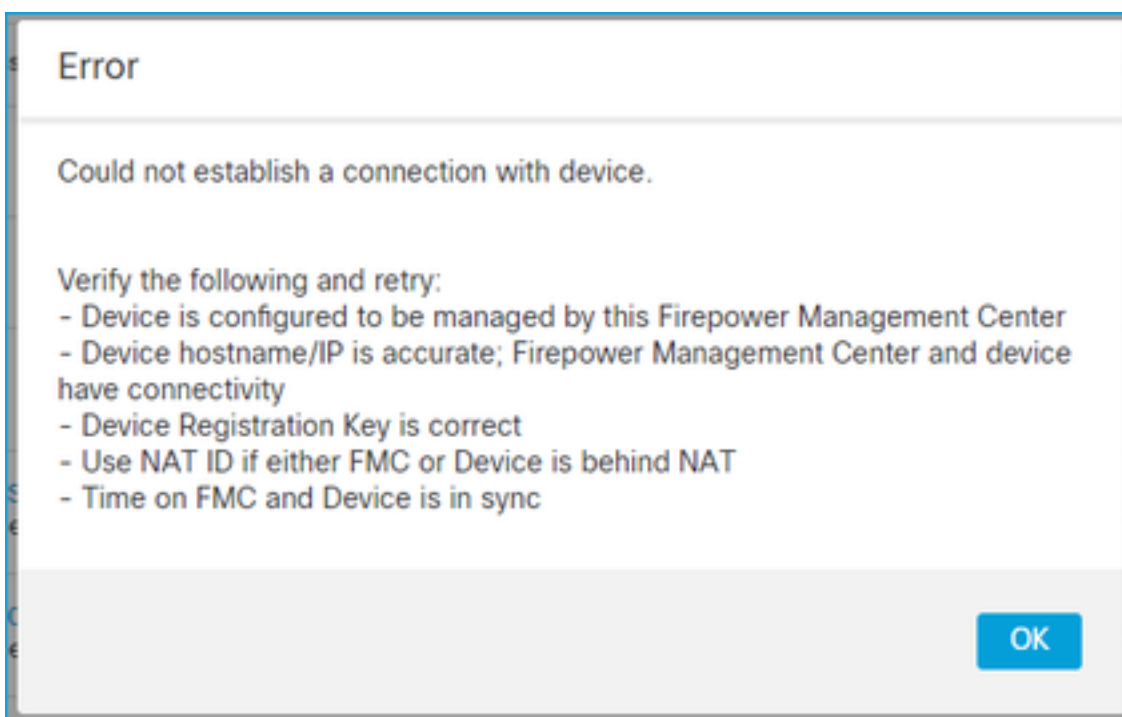


Anmerkung: Wir empfehlen, die Master-Einheit für die beste Leistung hinzuzufügen. Sie können jedoch jede Einheit des Clusters hinzuzufügen. Weitere Informationen finden Sie unter: [Erstellen eines Firepower Threat Defense-Clusters](#)

Fehlerbehebung bei gängigen Problemen

1. Ungültige Syntax in FTD CLI

Bei einer ungültigen Syntax auf FTD und einem fehlgeschlagenen Registrierungsversuch zeigt die FMC-Benutzeroberfläche eine ziemlich allgemeine Fehlermeldung an:



In diesem Befehl ist das Schlüsselwort **key** der Registrierungsschlüssel, während **cisco123** die NAT-ID ist. Es ist durchaus üblich, das Schlüsselwort hinzuzufügen, obwohl es technisch gesehen kein solches Schlüsselwort gibt:

```
> 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.

Empfohlene Aktion

Verwenden Sie die richtige Syntax und keine nicht vorhandenen Schlüsselwörter.

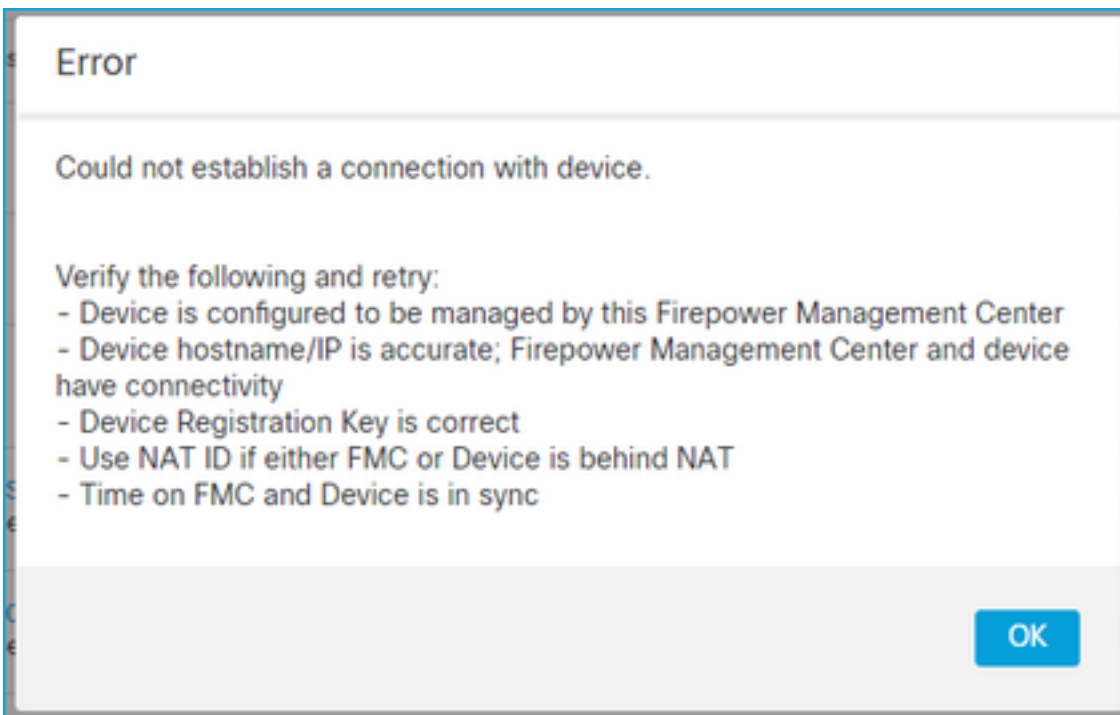
```
> configure manager add 10.62.148.75 cisco123
```

Manager successfully configured.

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

2. Nichtübereinstimmung des Registrierungsschlüssels zwischen FTD und FMC

Die Benutzeroberfläche des FMC zeigt Folgendes an:



Empfohlene Aktion

Überprüfen Sie auf FTD die Datei /ngfw/var/log/messages auf Authentifizierungsprobleme.

Weg 1 - Überprüfen der vergangenen Protokolle

```
> 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 '/ngfw/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] sftunnel:sf_ssl [WARN] Accept: Failed to authenticate peer '10.62.148.75' <- The problem
```

Weg 2 - Überprüfung der Live-Protokolle

> **expert**

```
ftd1:~$ sudo su
```

Password:

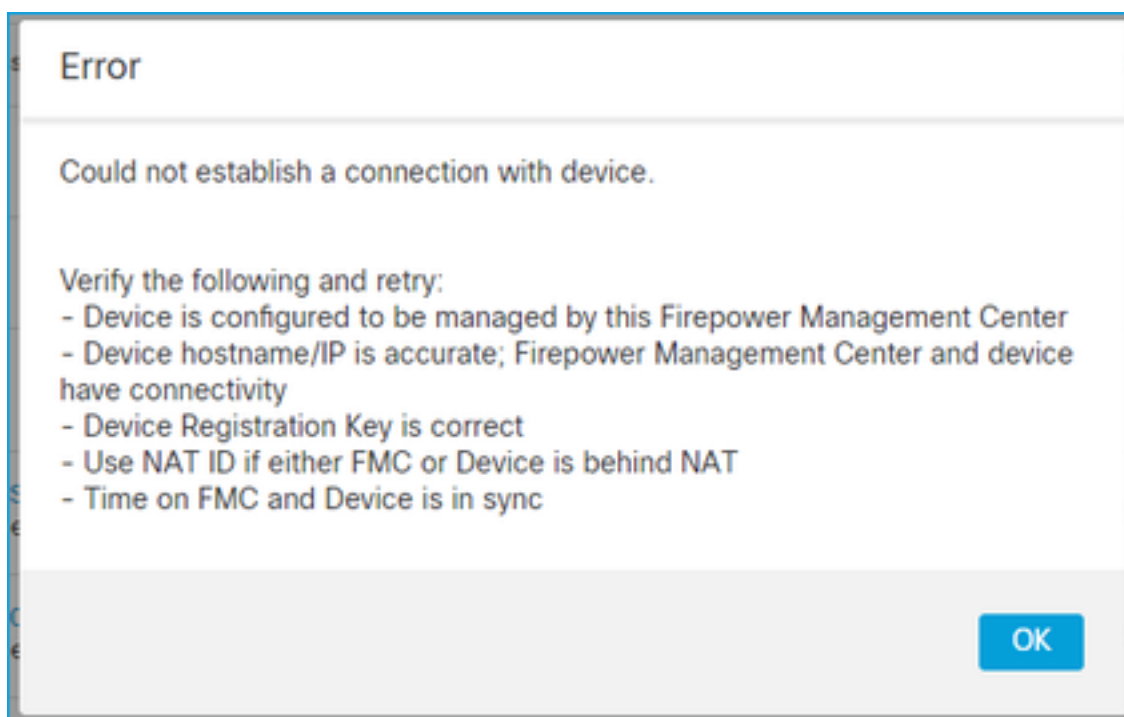
```
ftd1:~/home/admin# tail -f /ngfw/var/log/messages
```

Überprüfen Sie auf FTD den Inhalt der Datei /etc/sf/sftunnel.conf, um sicherzustellen, dass der Registrierungsschlüssel korrekt ist:

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

3. Verbindungsprobleme zwischen FTD - FMC

Die Benutzeroberfläche des FMC zeigt Folgendes an:



Empfohlene Maßnahmen

- Stellen Sie sicher, dass sich kein Gerät im Pfad (z. B. eine Firewall) befindet, das den Datenverkehr blockiert (TCP 8305). Bei FMC HA stellen Sie sicher, dass der Datenverkehr zu TCP-Port 8305 zu beiden FMCs zugelassen wird.
- Aufnahmen zur Verifizierung der bidirektionalen Kommunikation Verwenden Sie auf FTD den Befehl **capture-traffic**. Stellen Sie sicher, dass ein TCP 3-Wege-Handshake stattfindet und keine TCP FIN- oder RST-Pakete.

```
> 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
```

Auf ähnliche Weise sollten Sie eine Erfassung auf dem FMC durchführen, um eine bidirektionale Kommunikation sicherzustellen:

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

Es wird außerdem empfohlen, die Erfassung im pcap-Format zu exportieren und den Paketinhalt zu überprüfen:

```
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
```

Mögliche Ursachen:

- Dem FMC wurde das FTD-Gerät nicht hinzugefügt.
- Ein Gerät im Pfad (z. B. die Firewall) blockiert oder ändert den Datenverkehr.
- Die Pakete werden im Pfad nicht richtig geroutet.
- Der Sftunnel-Prozess auf FTD oder FMC ist ausgefallen (Szenario 6 prüfen)
- Es liegt ein MTU-Problem im Pfad vor (Prüfszenario).

Für die Erfassungsanalyse lesen Sie dieses Dokument:

[Analyse der FirePOWER-Firewall-Erfassung zur effektiven Behebung von Netzwerkproblemen](#)

5. Zeitdifferenz zwischen FTD und FMC

Bei der FTD-FMC-Kommunikation werden Zeitunterschiede zwischen den beiden Geräten berücksichtigt. Es ist eine Designanforderung, dass FTD und FMC vom gleichen NTP-Server synchronisiert werden.

Wenn der FTD auf einer Plattform wie 41xx oder 93xx installiert wird, werden die Zeiteinstellungen vom übergeordneten Chassis (FXOS) übernommen.

Empfohlene Aktion

Stellen Sie sicher, dass der Gehäusemanager (FCM) und das FMC dieselbe Zeitquelle (NTP-Server) verwenden.

6. sftunnel-Prozess deaktiviert oder deaktiviert

Auf FTD übernimmt der **sftunnel**-Prozess den Registrierungsprozess. Dies ist der Status des Prozesses vor der Manager-Konfiguration:

```
> 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,sfiproxy
CGroups: memory=System/ProcessHigh
```

Registrierungsstatus:

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

Konfigurieren Sie den Manager:

```
> 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.

Der Prozess ist jetzt aktiv:

```
> 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)
```

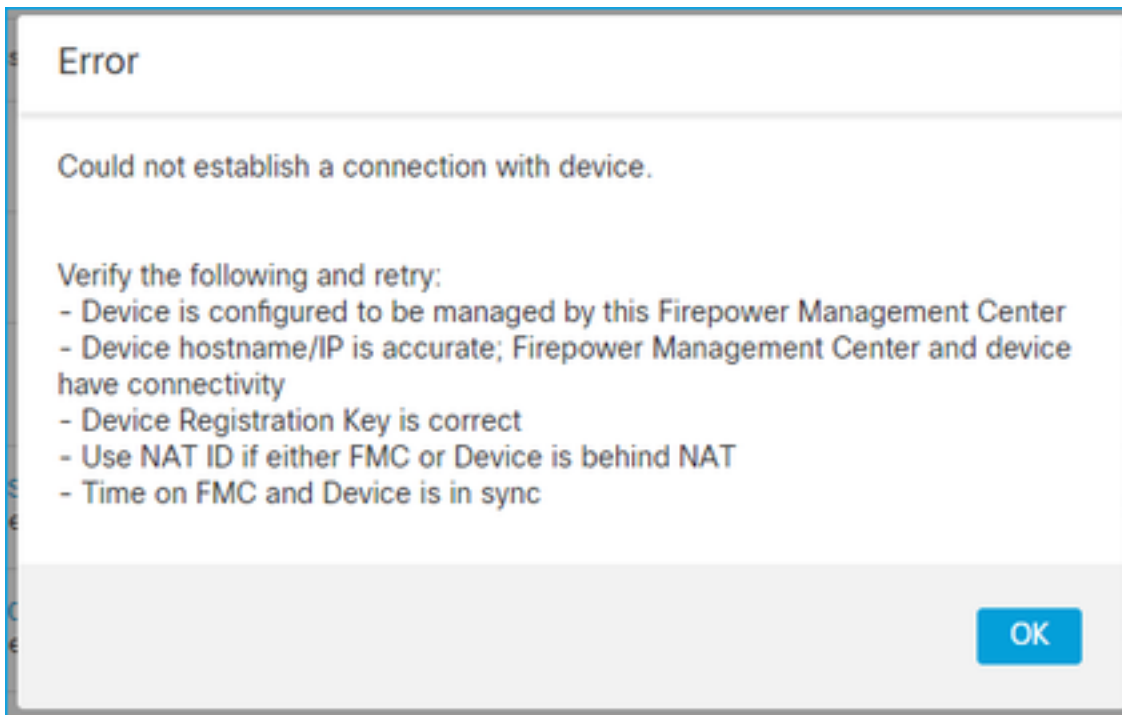
In seltenen Fällen kann der Prozess heruntergefahren oder deaktiviert werden:

```
> 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
```

Der Manager-Status sieht normal aus:

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

Andererseits schlägt die Geräteregistrierung fehl:



Auf FTD werden keine verwandten Meldungen in `/ngfw/var/log/messages` angezeigt.

Empfohlene Aktion

Sammeln Sie die FTD-Problembearbeitungsdatei, und wenden Sie sich an das Cisco TAC.

7. FTD Ausstehende Registrierung auf sekundärem FMC

Es gibt Szenarien, in denen das FTD-Gerät nach der ersten FTD-Registrierung beim FMC HA-Setup nicht zum sekundären FMC hinzugefügt wird.

Empfohlene Aktion

Befolgen Sie die in diesem Dokument beschriebenen Schritte:

[Auflösen der Geräteregistrierung in FirePOWER Management Center High Availability über CLI](#)

Warnung: Dieses Verfahren ist aufdringlich, da es die Aufhebung der Geräteregistrierung beinhaltet. Dies wirkt sich auf die FTD-Gerätekonfiguration aus (sie wird gelöscht). Es wird empfohlen, dieses Verfahren nur bei der FTD-Registrierung und -Einrichtung anzuwenden. Sammeln Sie in anderen Fällen FTD- und FMC-Problembearbeitungsdateien, und wenden Sie sich an Cisco TAC.

8. Registrierung schlägt aufgrund von Pfad-MTU fehl

Im Cisco TAC gibt es Szenarien, bei denen der Sftunnel-Datenverkehr eine Verbindung mit geringer MTU durchqueren muss. Die Sftunnel-Pakete haben den **Don't fragment** bit **Set**, daher ist

eine Fragmentierung nicht zulässig:

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

Zusätzlich können Sie in den Dateien /ngfw/var/log/messages eine Meldung wie diese sehen:

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

Empfohlene Aktion

Um zu überprüfen, ob aufgrund einer Fragmentierung Paketverluste auftreten, führen Sie Erfassungen auf FTD, FMC und idealerweise auf Geräten im Pfad durch. Überprüfen Sie, ob Pakete auf beiden Seiten eintreffen.

Reduzieren Sie auf FTD die MTU auf der FTD-Management-Schnittstelle. Der Standardwert ist 1500 Byte. MAX ist 1500 für die Management-Schnittstelle und 9000 für die Eventing-Schnittstelle. Der Befehl wurde in FTD 6.6 hinzugefügt.

[Cisco FirePOWER Threat Defense-Befehlsreferenz](#)

Beispiel

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

Verifizierung

```
> show network
===== [ System Information ] =====
Hostname           : ksec-sfvn-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 ]-----
```

Um die Pfad-MTU vom FTD zu überprüfen, können Sie folgenden Befehl verwenden:

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

Mit der **do**-Option wird das Bit **nicht fragmentieren** in den ICMP-Paketen festgelegt.

Verringern Sie bei FMC den MTU-Wert auf der FMC-Management-Schnittstelle, wie in diesem Dokument beschrieben:

[Konfigurieren der Management-Schnittstellen von FirePOWER Management Center](#)

9. FTD wird nach einem Bootstrap-Wechsel von der Chassis-Manager-Benutzeroberfläche abgemeldet

Dies gilt für die Plattformen FP41xx und FP93xx und ist in Cisco Bug-ID [CSCvn45138](#) dokumentiert. .

Im Allgemeinen dürfen Sie Bootstrap-Änderungen über den Chassis-Manager (FCM) nur vornehmen, wenn Sie eine Notfallwiederherstellung durchführen.

Empfohlene Aktion

Falls Sie einen Bootstrap-Wechsel durchgeführt haben und die Bedingung erfüllt haben (die FTD-FMC-Kommunikation ist unterbrochen, während der FTD nach dem Bootstrap-Wechsel hochgefahren wird), müssen Sie den FTD-FMC löschen und erneut registrieren.

10. FTD verliert Zugriff auf FMC aufgrund von ICMP-Umleitungsnachrichten

Dieses Problem kann den Registrierungsprozess beeinträchtigen oder die FTD-FMC-Kommunikation nach der Registrierung unterbrechen.

Problematisch ist in diesem Fall ein Netzwerkgerät, das **ICMP Redirect** Meldungen an die FTD-Management-Schnittstelle und Black-Holes FTD-FMC Kommunikation sendet.

So erkennen Sie dieses Problem

In diesem Fall ist 10.100.1.1 die IP-Adresse des FMC. Auf FTD gibt es eine zwischengespeicherte Route aufgrund einer ICMP-Umleitungsnachricht, die von der FTD an der Verwaltungsschnittstelle empfangen wurde:

```
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
```

Empfohlene Aktion

Schritt 1

Deaktivieren Sie die ICMP-Umleitung auf dem Gerät, das sie sendet (z. B. Upstream-L3-Switch, Router usw.).

Schritt 2

Löschen Sie den FTD-Routen-Cache aus der FTD-CLI:

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

Wenn er nicht umgeleitet wird, sieht er wie folgt aus:

```
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
```

Referenzen

- [Grundlegendes zu ICMP-Umleitungsnachrichten](#)
- [Cisco Bug-ID CSCvm53282 FTD: Routingtabellen, die von ICMP-Umleitungen hinzugefügt werden, bleiben für immer im Routingtabellen-Cache stecken.](#)

Zugehörige Informationen

- [NGFW-Konfigurationsleitfäden](#)

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.