FTD Manager-Zugriffs-Datenschnittstelle ändern

Inhalt

Einleitung

In diesem Dokument werden die Schritte zum Ändern der Schnittstelle für den Manager Secure Firewall Threat Defense (FTD) beschrieben.

Voraussetzungen

Anforderungen

- Grundlegendes Produktwissen.
- Vertrautheit mit FTD-Management und -Management über Datenschnittstellen

Verwendete Komponenten

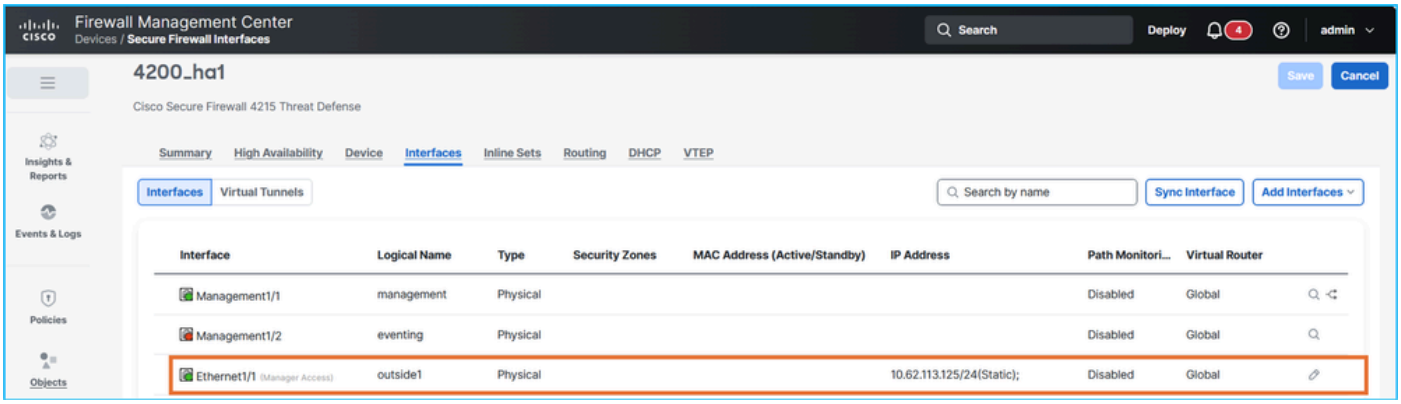
Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen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

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

- Sichere Firewall 4200
- Secure Firewall Threat Defense (FTD) 10.0.x, 7.6.4
- Secure Firewall Management Center (FMC) 10.0.x

Erstkonfiguration

1. Das FMC verwaltet FTD in Hochverfügbarkeit (HA) über die Datenschnittstelle Ethernet1/1 mit dem Namen outside1 unter Verwendung der aktiven und Standby-IP-Adressen 10.62.113.125 bzw. 10.62.113.126:



Überprüfung auf FTD CLISH:

<#root>

>

show network management-data-interface

Physical Interface Name of the Interface

Ethernet1/1 outside1

>

show network

```
===============[ System Information ]===============
Hostname                  : CSF4215-3
..
DNS from router           : enabled
Management port           : 8305
IPv4 Default route
  Gateway                 : data-interfaces
…
======[ System Information - Data Interfaces ]======
DNS Servers               : 192.0.2.100

Interfaces                : Ethernet1/1



==================[

Ethernet1/1

 ]===================

State                     : Enabled
Link                      : Up

Name                      : outside1


MTU                       : 1500
MAC Address               : 40:F4:9F:3D:5A:0E

----------------------[ IPv4 ]----------------------



Configuration             : Manual



Address                   : 10.62.113.125



Netmask                   : 255.255.255.0



Gateway                   : 10.62.113.1


…
```

2. Sftunnel-Verbindungen werden zwischen der FTD HA-Einheit und dem FMC hergestellt:

```
<#root>

>

sftunnel-status-brief



PEER:fmc.example.org


        SFTunnel Status:-

                Channel A: Connected



                Channel B: Connected


        Peer channel Channel-A is valid  type (CONTROL), using 'tap_nlp', connected to '198.51.100.23' v
        Peer channel Channel-B is valid  type (EVENT), using 'tap_nlp', connected to '198.51.100.23' vi
        Registration: Completed.
        IPv4 Connection to peer 'fmc.example.org' Start Time: Fri Jul 17 08:22:31 2026 UTC
        Heartbeat Send Time:     Fri Jul 17 08:52:42 2026 UTC
        Heartbeat Received Time: Fri Jul 17 08:53:03 2026 UTC
        Last disconnect time   : Fri Jul 17 08:22:16 2026 UTC
        Last disconnect reason : Process shutdown due to stop request from PM
```

3. FTD setzt bei der Verbindung mit FMC auf die DNS-Auflösung. Die Konfiguration des Managers basiert auf dem vollqualifizierten Domänennamen (Fully Qualified Domain Name, FQDN):

```
<#root>

>

show managers


Type                      : Manager

Host                      : fmc.example.org
```

```
Display name              : fmc.example.org


Version                   : 10.0.1 (Build 1)
Identifier                : 6d86efc4-c095-11f0-9244-48f1a7894b18
Registration              : Completed
Management type           : Configuration and analytics

>

show network


===============[ System Information ]===============
Hostname                  : KSEC-FPR-4215-3

Domains                   : example.org



DNS Servers               : 192.0.2.100


DNS from router           : enabled
Management port           : 8305
IPv4 Default route
  Gateway                 : data-interfaces
…
```

Die DNS-Server sind über die Schnittstelle outside1 erreichbar.

4. Sftunnel-Verbindungen werden über die Lina-Engine hergestellt:

<#root>

```
>

show conn all port 8305


26 in use, 32 most used
Inspect Snort:
        preserve-connection: 0 enabled, 0 in effect, 0 most enabled, 0 most in effect


TCP nlp_int_tap  10.62.113.125(169.254.1.3):8305 outside1  198.51.100.23:45647, idle 0:00:03, bytes 2129
```

```
TCP nlp_int_tap  10.62.113.125(169.254.1.3):37141 outside1  198.51.100.23:8305, idle 0:00:04, bytes 1485
```

Konfigurationsschritte

Das Ziel besteht darin, den Manager-Zugriff von der aktuellen outside1-Schnittstelle auf die Ziel-outside2-Schnittstelle zu verschieben. Die IP-Adressen active und standby outside2 lauten 10.62.114.51/24 bzw. 10.62.114.52/24.

Beachten Sie, dass die FTD-Versionen 7.7.0 oder höher redundante Manager-Zugriffsdatenschnittstellen unterstützen, die die Konfiguration und Bereitstellung von mehr als einer Manager-Zugriffsschnittstelle ermöglichen. Diese Funktion wird in früheren Versionen als 7.7.0 nicht unterstützt.

Daher werden bestimmte Schritte übersprungen oder enthalten andere Aktionen.

⚠ Vorsicht: Trennen Sie die FTD-Registrierung bzw. -Löschung nicht von FMC.

1. Es wird empfohlen, Konsolenzugriff auf die FTDs zu haben:

- Bei Firepower 4100/9300 können Sie eine Verbindung mit dem Chassis über SSH herstellen und dann über den Befehl connect module x console eine Verbindung mit der nativen FTD-Konsole herstellen, wobei x die Steckplatz-/Sicherheitsmodul-ID ist.
- Wenn die Firepower 4100/9300 FTD im Multi-Instance (MI)-Modus ausführt, können Sie eine Verbindung zum Chassis über SSH herstellen und dann eine Verbindung zur nativen FTD-Konsole über den Befehl connect module x telnet herstellen, wobei x die Steckplatz-/Sicherheitsmodul-ID ist. Stellen Sie dann mit dem Befehl connect ftd <ftd_id> eine Verbindung zur FTD-Instanz her.
- Im Fall der Secure Firewall 3100/4200 im MI-Modus können Sie eine Verbindung mit dem Chassis über SSH herstellen und dann über den Befehl connect ftd <bezeichner> eine Verbindung mit der FTD-Konsole herstellen.

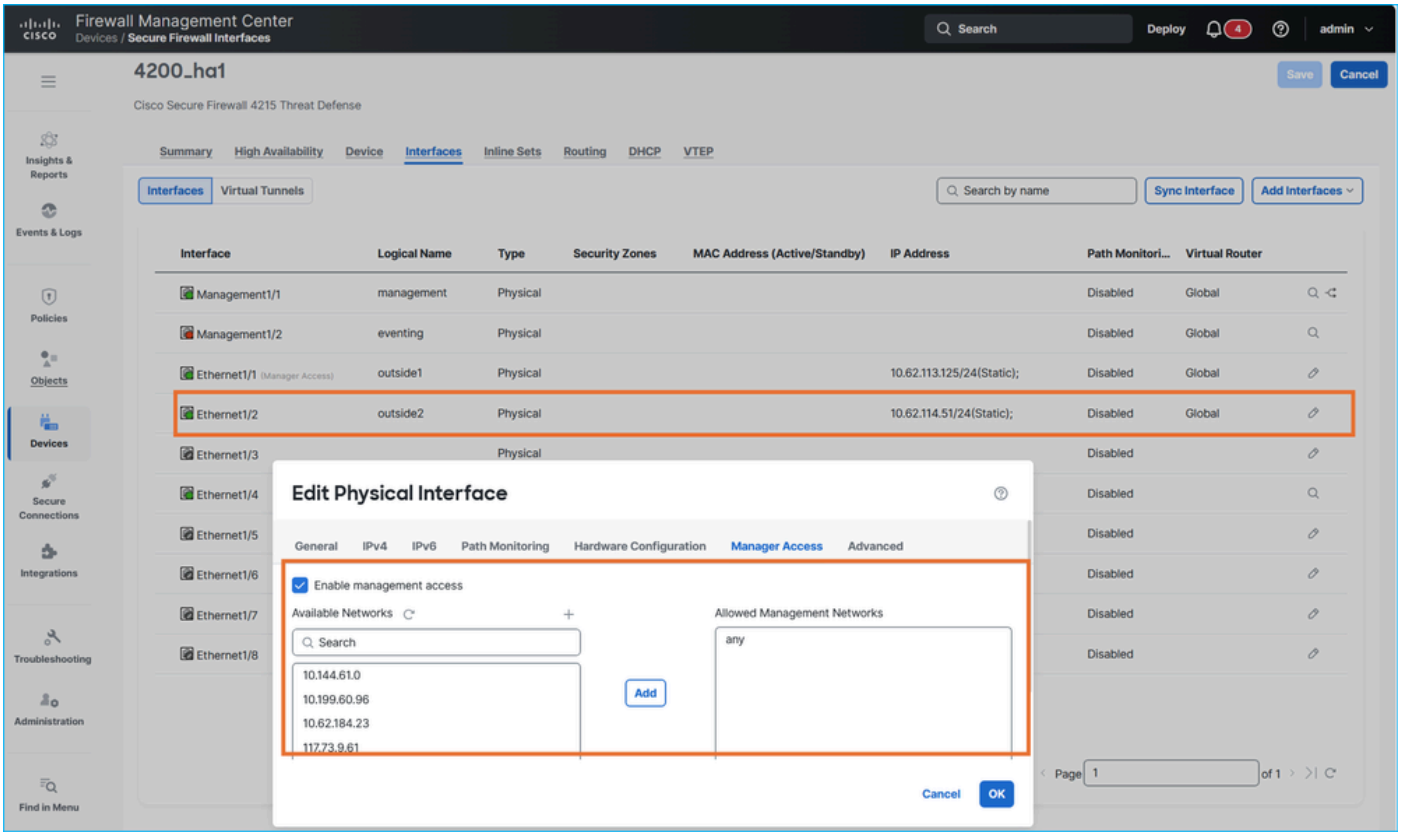
2. Bereitstellen ausstehender Richtlinien

3. Es wird dringend empfohlen, FTD- und FMC-Backups zu erstellen. Im Fall von FTD HA sollten Sie die Sicherung beider Einheiten durchführen.

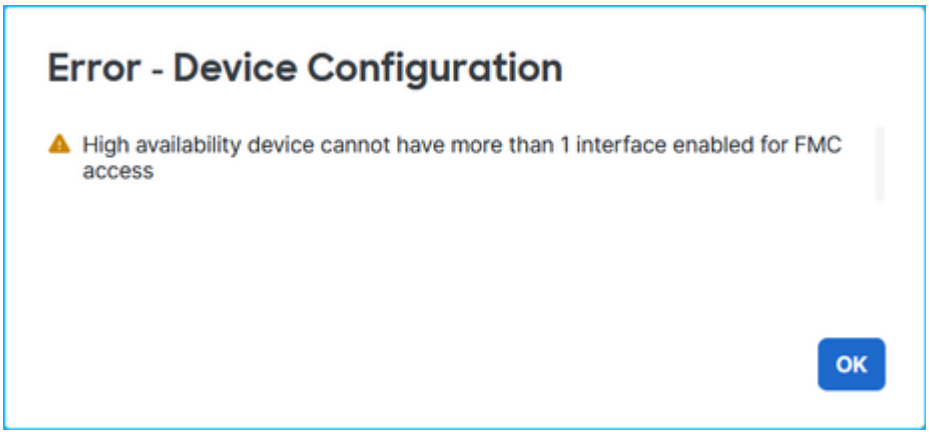
4. Konfigurieren Sie den Namen der Zielschnittstelle, die IP-Adresse, die Sicherheitszone und ggf. andere schnittstellenbezogene Einstellungen.

5. Konfigurieren Sie die Standby-IP-Adresse der Zielschnittstelle.

6. Wenn die FTD-Softwareversion 7.7.0 oder höher ist, aktivieren Sie den Manager-Zugriff auf die Zielschnittstelle, und passen Sie die Managementzugriffsnetzwerke nach Bedarf an:



Beachten Sie, dass FTD-Versionen vor 7.7.0 keine redundanten Manager-Zugriffsdatenschnittstellen unterstützen. Der Versuch, die zweite Manager-Zugriffsschnittstelle zu konfigurieren, führt zu folgender Fehlermeldung:



Überspringen Sie die Schritte 7 und 8 für FTD-Versionen vor 7.7.0.

7. Stellen Sie die Richtlinien bereit, und überprüfen Sie die Einstellungen auf der FTD CLISH. In diesem Beispiel hat die Ethernet1/2-Schnittstelle mit dem Namen eif outside2 die IP-Adressen 10.62.114.51 und 10.62.114.52:

```
<#root>

>

show ip


System IP Addresses:
Interface                Name                IP address      Subnet mask     Method
Ethernet1/1              outside1            10.62.113.125   255.255.255.0   manual <- source interf

Ethernet1/2              outside2            10.62.114.51    255.255.255.0   manual

<- target interface
Ethernet1/4              fover               10.9.0.21       255.255.255.0   unset
```

Die outside2-Schnittstelle wird der Sftunnel-Konfiguration hinzugefügt:

```
<#root>

>

show running-config sftunnel


sftunnel interface outside2
```

```
<- target interface

sftunnel interface outside1

<- source interface
sftunnel port 8305
sftunnel route-map FMC_GEN_19283746_RBD_DUAL_WAN_RMAP_91827346
```

Obwohl zusätzliche Regeln in der NAT-Tabelle (Network Address Translation) installiert sind, werden die Regeln mit der Schnittstelle outside1 verwendet:

```
<#root>

>

show nat detail


Manual NAT Policies Implicit (Section 0)
1 (nlp_int_tap) to (outside1) source static nlp_server__sftunnel_0.0.0.0_intf5 interface  destination s
    translate_hits = 1448, untranslate_hits = 1448
    Source - Origin: 169.254.1.3/32, Translated: 10.62.113.125/24
    Destination - Origin: 0.0.0.0/0, Translated: 0.0.0.0/0
    Service - Protocol: tcp Real: 8305 Mapped: 8305

2 (nlp_int_tap) to (outside2) source static nlp_server__sftunnel_0.0.0.0_intf6 interface  destination st


    translate_hits = 0, untranslate_hits = 0
    Source - Origin: 169.254.1.3/32, Translated: 10.62.114.51/24
    Destination - Origin: 0.0.0.0/0, Translated: 0.0.0.0/0
    Service - Protocol: tcp Real: 8305 Mapped: 8305
3 (nlp_int_tap) to (outside1) source static nlp_server__sftunnel_::_intf5 interface ipv6  destination s
    translate_hits = 0, untranslate_hits = 0
    Source - Origin: fd00:0:0:1::3/128, Translated:
    Destination - Origin: ::/0, Translated: ::/0
    Service - Protocol: tcp Real: 8305 Mapped: 8305
4

(nlp_int_tap) to (outside2) source static nlp_server__sftunnel_::_intf6 interface ipv6  destination stat


    translate_hits = 0, untranslate_hits = 0
    Source - Origin: fd00:0:0:1::3/128, Translated:
    Destination - Origin: ::/0, Translated: ::/0
    Service - Protocol: tcp Real: 8305 Mapped: 8305
5 (nlp_int_tap) to (outside1) source dynamic nlp_client_0_intf5 interface
    translate_hits = 653, untranslate_hits = 0
    Source - Origin: 169.254.1.3/32, Translated: 10.62.113.125/24
6

(nlp_int_tap) to (outside2) source dynamic nlp_client_0_intf6 interface
```

```
    translate_hits = 0, untranslate_hits = 0
    Source - Origin: 169.254.1.3/32, Translated: 10.62.114.51/24
7 (nlp_int_tap) to (outside1) source dynamic nlp_client_0_ipv6_intf5 interface ipv6
    translate_hits = 0, untranslate_hits = 0
    Source - Origin: fd00:0:0:1::3/128, Translated:
8
```

(nlp_int_tap) to (outside2) source dynamic nlp_client_0_ipv6_intf6 interface ipv6

```
    translate_hits = 0, untranslate_hits = 0
    Source - Origin: fd00:0:0:1::3/128, Translated:
```

8. Überprüfen Sie den Hochverfügbarkeitsstatus und die Schnittstellenüberwachung:

<#root>

>

show monitor-interface

This host: Primary - Active

```
        Interface management (203.0.113.130): Normal (Monitored)
        Interface outside1 (10.62.113.125): Normal (Monitored)
        Interface outside2 (10.62.114.51): Normal (Monitored)
```

Other host: Secondary - Standby Ready

```
        Interface management (203.0.113.131): Normal (Monitored)
        Interface outside1 (10.62.113.126): Normal (Monitored)
        Interface outside2 (10.62.114.52): Normal (Monitored)
```

9. Wenn Sie die FTDs über die outside2-Schnittstelle verwalten möchten, stellen Sie sicher, dass der Zugriff im Abschnitt SSH-Zugriff der Plattformeinstellungen erlaubt ist.

10. Nehmen Sie die erforderlichen Änderungen vor, um die Verbindung über die Zielschnittstelle zu den Domänennamenservern (DNS) und zum FMC zu ermöglichen:

- Wenn für die Verbindung zwischen FMC und FTDs eine DNS (Domain Name Resolution)

erforderlich ist, stellen Sie sicher, dass die FTDs über die Zielschnittstelle zum nächsten Hop erreichbar sind, über den die DNS-Server erreicht werden. Die DNS-Auflösung muss auch im Übertragungspfad zugelassen werden.
- Stellen Sie sicher, dass FTDs über die Zielschnittstelle zum nächsten Hop erreichbar sind, der zum Erreichen von FMC verwendet wird.
- Stellen Sie sicher, dass bidirektionale Verbindungen zwischen FMC und FTDs über den TCP-Port 8305 im Transitpfad über die Zielschnittstelle zulässig sind. Die Verbindung muss in beide Richtungen zugelassen werden.

In diesem Fall muss IP 10.62.114.1 als Standard-Gateway für die Zielschnittstelle verwendet werden. Die nächste Hop-IP-Adresse ist über das Internet Control Message Protocol (ICMP) erreichbar:

```
<#root>

>

ping 10.62.114.1


Please use 'CTRL+C' to cancel/abort...

Sending 5, 100-byte ICMP Echos to 10.62.114.1, timeout is 2 seconds:



!!!!!


Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/10 ms
```

Wenn ICMP administrativ im Transitpfad oder im nächsten Hop blockiert wird, stellen Sie sicher, dass die MAC-Adresse (Media Access Control) des nächsten Hop in der Ausgabe des Befehls show arp sichtbar und gültig ist:

```
<#root>

>

show arp


        fover 10.9.0.22 4c01.f7e9.e111 13275
        outside1 10.62.113.1 c02c.1782.2cbf 1
        outside1 10.62.113.126 4c01.f7e9.e10e 5453
```

outside2 10.62.114.1 c02c.1782.2cbf 0

```
        outside2 10.62.114.52 4c01.f7e9.e10f 5453
```

11. Führen Sie je nach FTD-Version die folgenden Schritte aus:

- Version 7.7.0 oder höher: auf FMC: Deaktivieren des Manager-Zugriffs über die Quellschnittstelle (outside1), Anpassen des Routings, einschließlich des Routings zu DNS-Servern (wenn DNS für den Zugriff auf FMC verwendet wird) und des FMC über die Zielschnittstelle (outside2). Konfigurieren Sie z. B. spezifische statische Routen oder das Standard-Gateway über die Zielschnittstelle.
- Version vor 7.7.0: auf FMC: Deaktivieren des Manager-Zugriffs über die Quellschnittstelle (outside1), Aktivieren des Manager-Zugriffs über die Zielschnittstelle (outside2), Anpassen des Routings, einschließlich des Routings zu DNS-Servern (wenn DNS für den Zugriff auf FMC verwendet wird) und des FMC über die Zielschnittstelle (outside2). Konfigurieren Sie z. B. bestimmte statische Routen oder das Standard-Gateway über die Zielschnittstelle.

12. Bereitstellen von Richtlinien

13. Überprüfen Sie auf FTD CLISH:

<#root>

```
>
```

show route 0.0.0.0

```
Routing entry for 0.0.0.0 0.0.0.0, supernet
  Known via "static", distance 1, metric 0, candidate default path
  Routing Descriptor Blocks:

  * 10.62.114.1, via outside2

<- default route over outside2
      Route metric is 0, traffic share count is 1

>
```

show running-config sftunnel

sftunnel interface outside2

<- sftunnel is enabled only over outside2
sftunnel port 8305

>

show nat detail

Manual NAT Policies Implicit (Section 0)

1 (nlp_int_tap) to (outside2) source static nlp_server__sftunnel_0.0.0.0_intf6 interface destination st

translate_hits = 3, untranslate_hits = 3

Source - Origin: 169.254.1.3/32, Translated: 10.62.114.51/24
Destination - Origin: 0.0.0.0/0, Translated: 0.0.0.0/0
Service - Protocol: tcp Real: 8305 Mapped: 8305
2 (nlp_int_tap) to (outside2) source static nlp_server__sftunnel_::_intf6 interface ipv6 destination s
translate_hits = 0, untranslate_hits = 0
Source - Origin: fd00:0:0:1::3/128, Translated:
Destination - Origin: ::/0, Translated: ::/0
Service - Protocol: tcp Real: 8305 Mapped: 8305
3 (nlp_int_tap) to (outside2) source dynamic nlp_client_0_intf6 interface
translate_hits = 407, untranslate_hits = 0
Source - Origin: 169.254.1.3/32, Translated: 10.62.114.51/24
4 (nlp_int_tap) to (outside2) source dynamic nlp_client_0_ipv6_intf6 interface ipv6
translate_hits = 0, untranslate_hits = 0
Source - Origin: fd00:0:0:1::3/128, Translated:

>

show conn all port 8305

31 in use, 42 most used
Inspect Snort:
preserve-connection: 0 enabled, 0 in effect, 0 most enabled, 0 most in effect

TCP nlp_int_tap 10.62.114.51(169.254.1.3):56853 outside2 198.51.100.23:8305, idle 0:00:06, bytes 33008

<- connectivity over outside2

TCP nlp_int_tap 10.62.114.51(169.254.1.3):32905 outside2 198.51.100.23:8305, idle 0:00:00, bytes 15959

<- connectivity over outside2

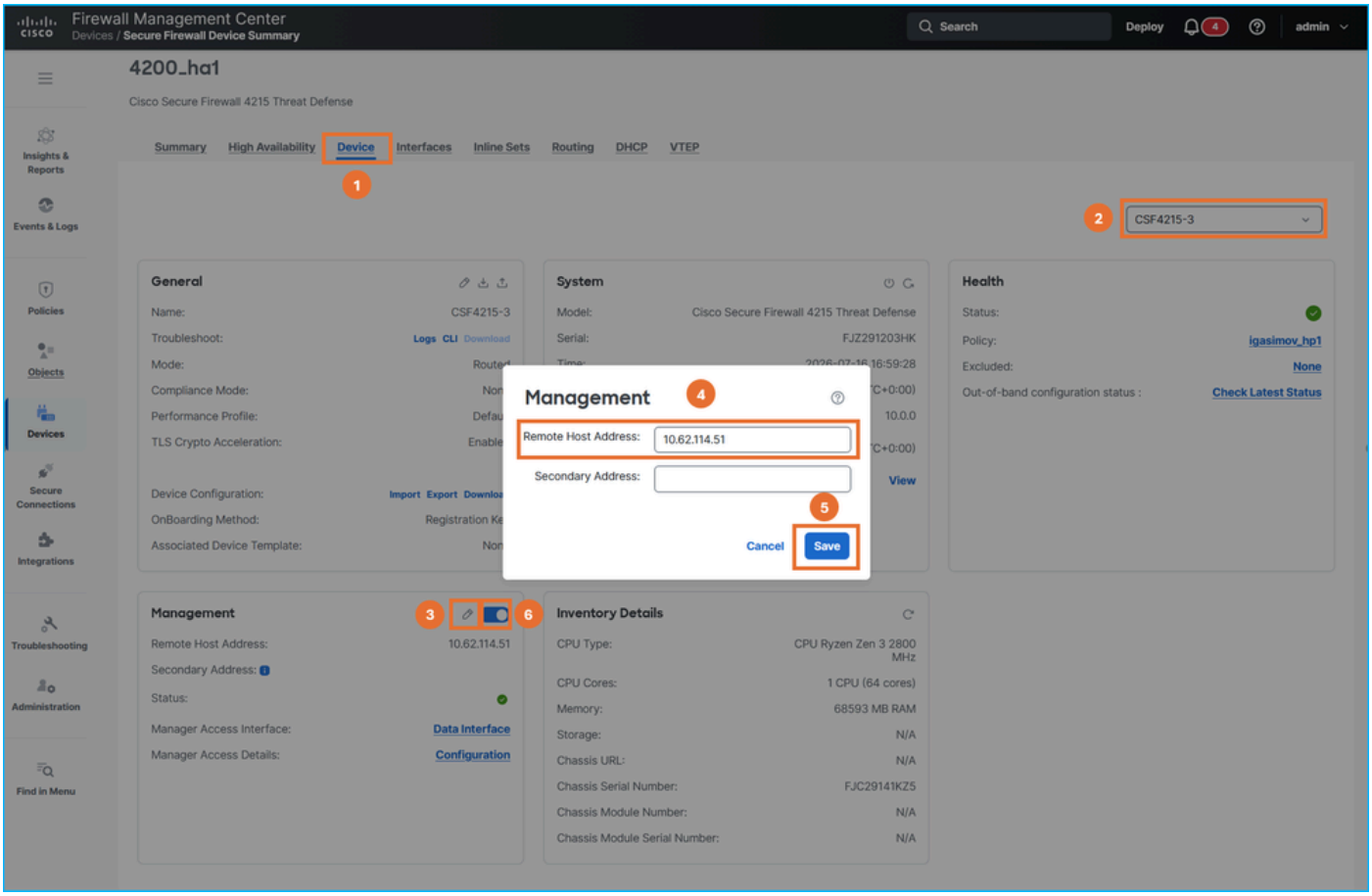
14. Wenn die DNS-Server in der Ausgabe des CLISH-Befehls "show network" geändert werden müssen, konfigurieren Sie die neuen DNS-Server:

<#root>

>

configure network dns servers 192.0.2.184

15. Auf FMC ändern FTD-Management-IP-Adresse auf die externe IP-Adresse2, dann deaktivieren und wieder aktivieren Sie die Verbindung mit dem Schieberegler. Wiederholen Sie diesen Schritt für beide Einheiten in HA:



16. Überprüfen Sie die Sftunnel-Konnektivität auf allen FTDs:

<#root>

>

sftunnel-status-brief

```
PEER:198.51.100.23
        SFTunnel Status:-
```

Channel A: Connected

Channel B: Connected

```
        Peer channel Channel-A is valid  type (CONTROL), using 'tap_nlp', connected to '198.51.100.23' v
        Peer channel Channel-B is valid  type (EVENT), using 'tap_nlp', connected to '198.51.100.23' vi
        Registration: Completed.
        IPv4 Connection to peer '198.51.100.23' Start Time: Thu Jul 16 16:37:14 2026 UTC
        Heartbeat Send Time:     Thu Jul 16 16:38:13 2026 UTC
        Heartbeat Received Time: Thu Jul 16 16:39:13 2026 UTC
        Last disconnect time   : Thu Jul 16 16:37:11 2026 UTC
        Last disconnect reason : Both control and event channel connections with peer went down

>
```

show conn all port 8305

```
32 in use, 42 most used
Inspect Snort:
        preserve-connection: 0 enabled, 0 in effect, 0 most enabled, 0 most in effect
```

TCP nlp_int_tap 10.62.114.51(169.254.1.3):8305 outside2 198.51.100.23:36383, idle 0:00:00, bytes 23575

```
<- new connection over different source port
```

TCP nlp_int_tap 10.62.114.51(169.254.1.3):8305 outside2 198.51.100.23:50963, idle 0:00:01, bytes 12319

```
<- new connection over different source port
```

17. Wenn DNS-Server in den Plattformeinstellungen geändert werden müssen, nehmen Sie die entsprechenden Konfigurationsänderungen vor, und stellen Sie Richtlinien bereit.

Fehlerbehebung bei Managementverbindung

Verwenden Sie diese Befehle für die Verifizierung:

1. show network: Zeigt die Konfiguration der Verwaltungsschnittstelle.
2. sftunnel-status-brief - Zeigt den Status der Sftunnel-Verbindung an.
3. show run sftunnel - Zeigt die Sftunnel-Konfiguration in der Firewall-Engine (Lina) an.
4. show conn all port 8305 - Zeigt die Sftunnel-Verbindungen über die Lina-Engine an.

Informationen zur Behebung von Verbindungsproblemen bei der Verwaltung finden Sie im Abschnitt Fehlerbehebung bei Management-Verbindungen im offiziellen Handbuch.

Referenzen

1. Konfigurationsanleitung für Cisco Secure Firewall Management Center-Geräte, 10.x
2. Ändern der Manager-Zugriffsschnittstelle
3. Fehlerbehebung bei der Management-Verbindung

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.