FTD Manager Access Data Interface wijzigen

Inhoud

Inleiding

In dit document worden de stappen beschreven voor het wijzigen van de FTD-beheerdersinterface (Secure Firewall Threat Defense).

Voorwaarden

Vereisten

- Basisproductkennis.
- Bekendheid met FTD-beheer en -beheer via gegevensinterfaces.

Gebruikte componenten

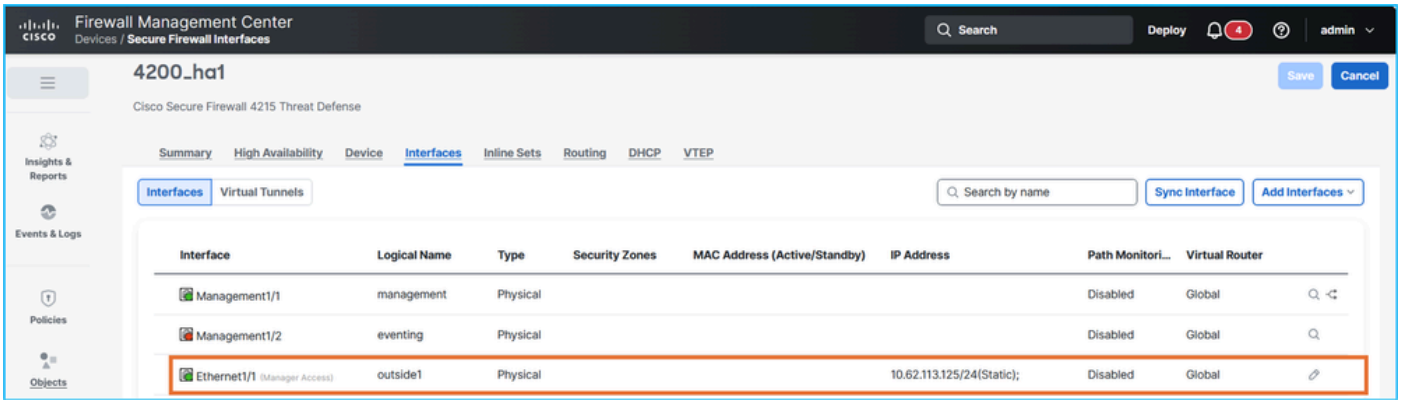
De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u zorgen dat u de potentiële impact van elke opdracht begrijpt.

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

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

initiële configuratie

1. Het VCC beheert FTD in hoge beschikbaarheid (HA) via de data-interface Ethernet1/1 met de naam if outside1, met respectievelijk actieve en stand-by IP-adressen 10.62.113.125 en 10.62.113.126:



Verificatie op 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. Er worden sftunnelverbindingen tot stand gebracht tussen de FTD HA-eenheid en het VCC:

```
<#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 vertrouwt op DNS-resolutie om verbinding te maken met FMC. De beheerconfiguratie is gebaseerd op de volledig gekwalificeerde domeinnaam (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
…
```

De DNS-servers zijn bereikbaar via de outside1-interface.

4. via de Lina-motor worden tunnelverbindingen tot stand gebracht:

<#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
```

Configuratiestappen

Het doel is om de beheerderstoegang van de huidige outside1 naar de target outside2-interface te verplaatsen. De actieve en standby outside2 IP-adressen zijn respectievelijk 10.62.114.51/24 en 10.62.114.52/24.

FTD-versies 7.7.0 of hoger ondersteunen redundante beheerderstoegangsgegevensinterfaces, waarmee meer dan één beheerderstoegangsinterfaces kunnen worden geconfigureerd en geïmplementeerd. Deze functie wordt niet ondersteund in versies eerder dan 7.7.0.

Hierdoor worden specifieke stappen overgeslagen of bevatten ze verschillende acties.

⚠ Let op: verwijder FTD's bij geen enkele stap uit het FMC.

1. Het wordt aanbevolen om consoletoegang tot de FTD's te hebben:

- In het geval van Firepower 4100/9300 kunt u verbinding maken met het chassis met behulp van SSH en vervolgens verbinding maken met de standaard FTD-console met behulp van de opdracht module x-console aansluiten, waarbij x de ID van de sleuf/beveiligingsmodule is.
- In het geval van Firepower 4100/9300 met FTD in de modus voor meerdere instanties (MI), kunt u verbinding maken met het chassis met SSH en vervolgens verbinding maken met de standaard FTD-console met behulp van de opdracht verbindingsmodule x telnet, waarbij x de ID van de sleuf/beveiligingsmodule is. Maak vervolgens verbinding met de FTD-instantie met de opdracht connect ftd <ftd_id>.
- In het geval van Secure Firewall 3100/4200 in MI-modus kunt u verbinding maken met het chassis met SSH en vervolgens verbinding maken met de FTD-console met behulp van de opdracht ftd <identifier> verbinden.

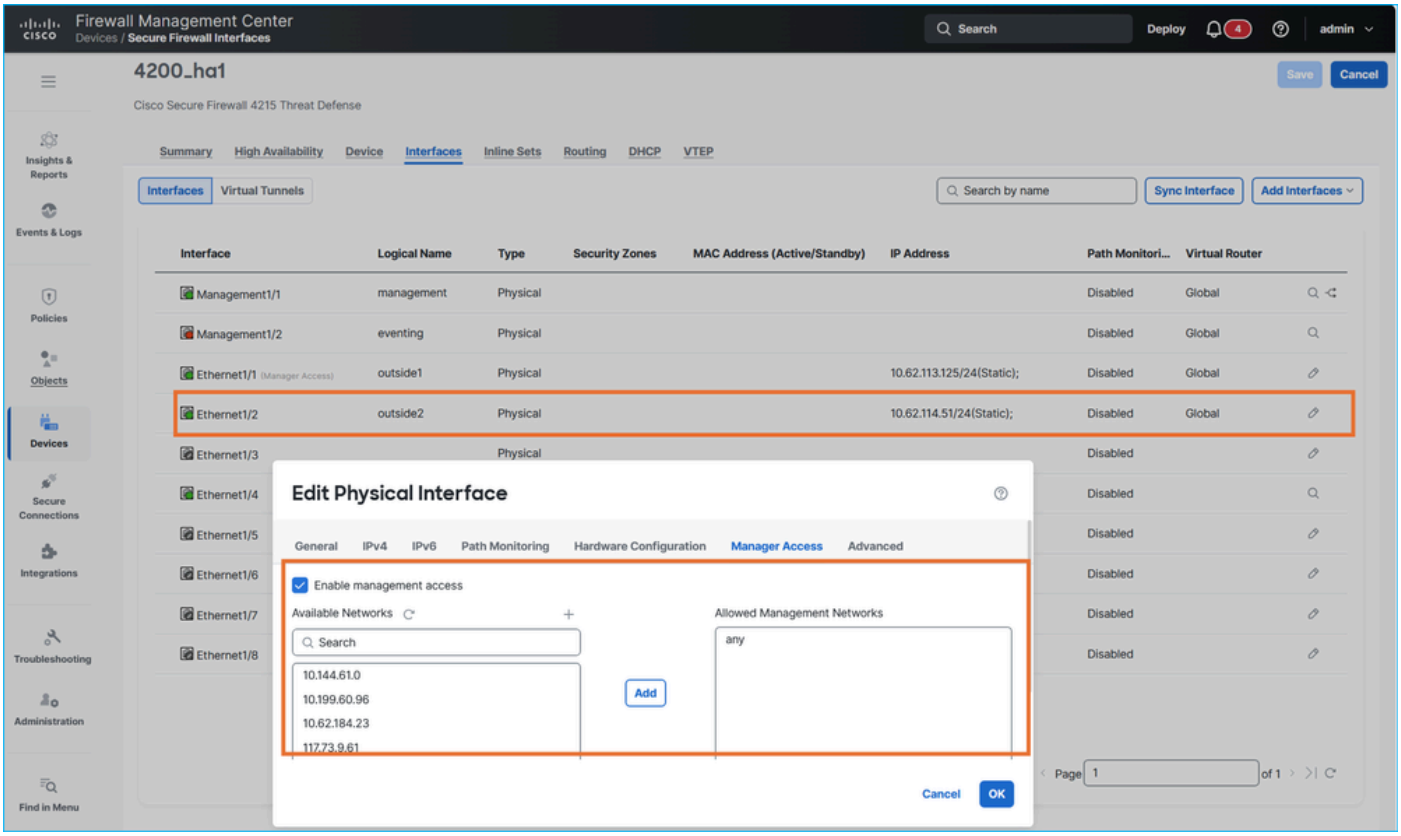
2. Bezig met implementeren van beleid.

3. Het wordt sterk aanbevolen om FTD- en FMC-back-ups te maken. In het geval van FTD HA, neem de back-up van beide eenheden.

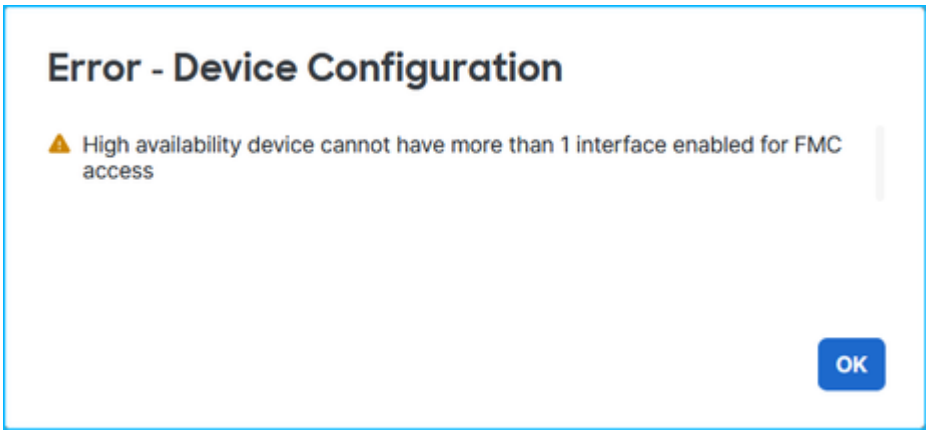
4. Configureer, indien van toepassing, de naam van de doelinterface, het IP-adres, de beveiligingszone en andere interface-gerelateerde instellingen.

5. Configureer het IP-adres van de doelinterface in stand-by.

6. Als de FTD-softwareversie 7.7.0 of hoger is, schakelt u de beheerderstoegang in op de doelinterface en past u de beheertoegangsnetwerken naar behoefte aan:



FTD-versies ouder dan 7.7.0 ondersteunen geen redundante beheerderstoegangsgegevensinterfaces. Als u probeert de toegangsinterface van het tweede beheerprogramma te configureren, wordt de volgende foutmelding weergegeven:



Zorg ervoor dat u stap 7 en 8 voor FTD-versies eerder dan 7.7.0 overslaat.

7. Implementeer het beleid en verifieer de instellingen op de FTD CLISH. In dit voorbeeld heeft de Ethernet1/2-interface met name if outside2 IP-adressen 10.62.114.51 en 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
```

De outside2 interface wordt toegevoegd aan de sftunnelconfiguratie:

```
<#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
```

Hoewel er aanvullende regels zijn geïnstalleerd in de NAT-tabel (Network Address Translation), worden de regels met de outside1-interface gebruikt:

```
<#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. Controleer de hoge beschikbaarheidsstatus en de interfacemonitoring:

<#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. Als u van plan bent de FTD's via de externe2-interface te beheren, moet u ervoor zorgen dat toegang in het gedeelte SSH-toegang van de platforminstellingen is toegestaan.

10. Breng de nodige wijzigingen aan om verbinding via de doelinterface met domeinnaamservers (DNS) en FMC mogelijk te maken:

- Als DNS (Domain Name Resolution) vereist is voor connectiviteit tussen FMC en FTD's, moet u ervoor zorgen dat de FTD's bereikbaar zijn via de doelinterface naar de volgende

hop die wordt gebruikt om de DNS-servers te bereiken. DNS-resolutie moet ook worden toegestaan in het transitpad.
- Zorg ervoor dat FTD's bereikbaar zijn via de doelinterface naar de volgende hop die moet worden gebruikt om de FMC te bereiken.
- Zorg ervoor dat bidirectionele connectiviteit tussen FMC en FTD's via TCP-poort 8305 is toegestaan in het transitpad via de doelinterface. De verbinding moet in beide richtingen worden toegestaan.

In dit geval moet IP 10.62.114.1 worden gebruikt als de standaard gateway over de doelinterface. Het volgende hop IP-adres is bereikbaar via Internet Control Message Protocol (ICMP):

```
<#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
```

Als ICMP administratief is geblokkeerd in het doorvoerpad of de volgende hop, controleert u of het MAC-adres (Media Access Control) van de volgende hop zichtbaar is in de uitvoer van de opdracht show arp en geldig is:

```
<#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. Voer de volgende stappen uit, afhankelijk van de FTD-versie:

- Versie 7.7.0 of hoger: schakel op FMC de beheerderstoegang uit via de broninterface (buiten 1), pas de routering aan, inclusief routering naar DNS-servers (als DNS wordt gebruikt om toegang te krijgen tot FMC) en FMC via de doelinterface (buiten 2). Configureer bijvoorbeeld specifieke statische routes of configureer de standaardgateway via de doelinterface.
- Versie eerder dan 7.7.0: schakel op FMC de toegang van de beheerder via de broninterface uit (buiten1), schakel de toegang van de beheerder via de doelinterface in (buiten2), pas de routering aan, inclusief routering naar DNS-servers (als DNS wordt gebruikt om toegang te krijgen tot FMC) en FMC via de doelinterface (buiten2). Configureer bijvoorbeeld specifieke statische routes of configureer de standaardgateway via de doelinterface.

12. Implementeer beleid.

13. Controleer op 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

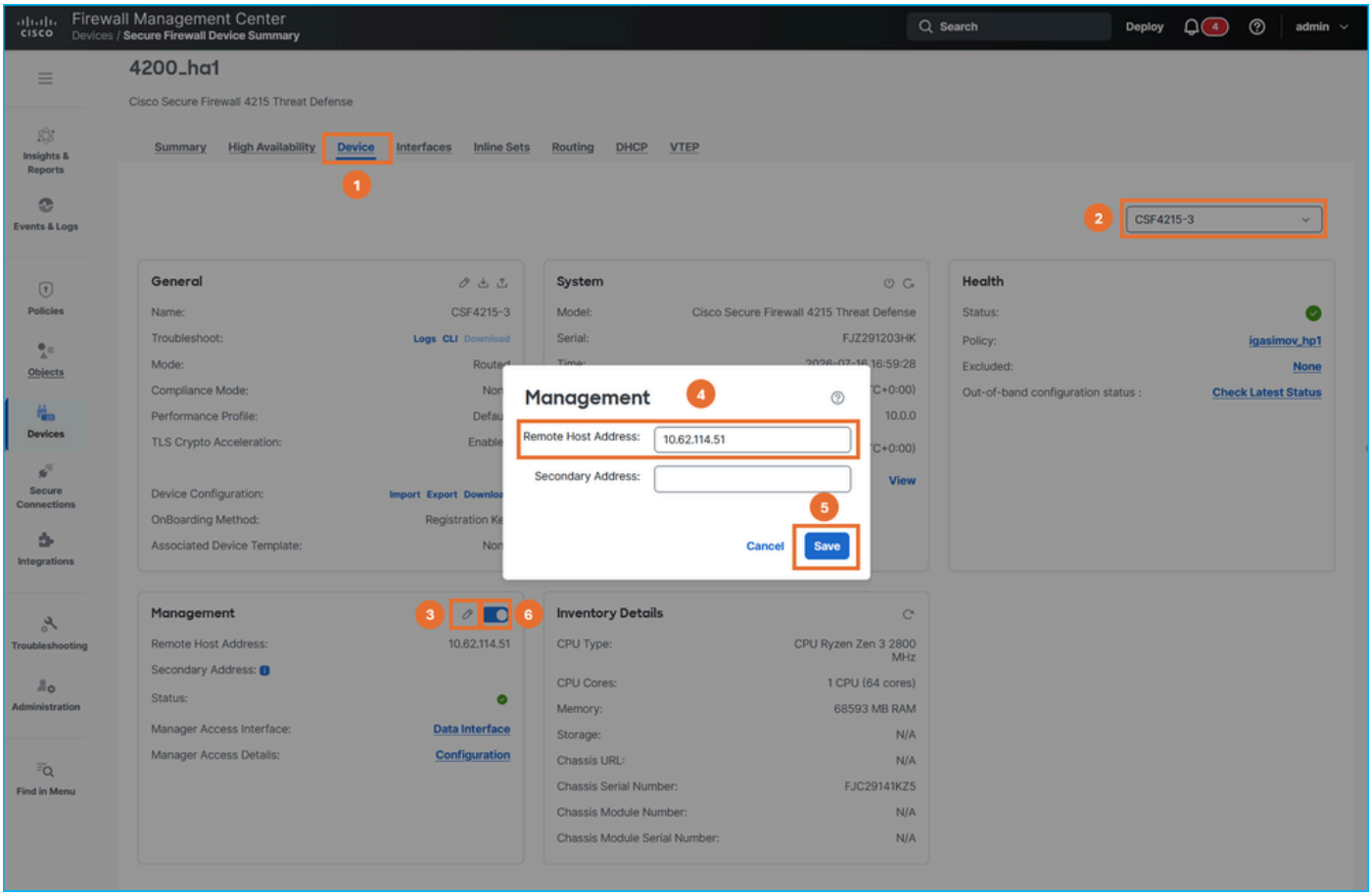
14. Als de DNS-servers in de uitvoer van de CLISH-opdracht 'Netwerk weergeven' moeten worden gewijzigd, configureert u de nieuwe DNS-servers:

<#root>

>

configure network dns servers 192.0.2.184

15. Wijzig op FMC het IP-adres van het FTD-beheer in het externe2-IP-adres en schakel vervolgens de verbinding uit en schakel deze opnieuw in met behulp van de schuifregelaar. Herhaal deze stap voor beide eenheden in HA:



16. Controleer de stetunnelconnectiviteit op alle FTD's:

<#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. Als DNS-servers in platforminstellingen moeten worden gewijzigd, voert u de juiste configuratiewijzigingen en implementatiebeleid uit.

Verbinding voor probleemoplossing

Gebruik deze opdrachten voor verificaties:

1. Toon netwerk – toont configuratie van beheerinterface.

2. sftunnel-status-brief – toont de status van de sftunnel-connectiviteit.
3. show run sftunnel – toont sftunnel configuratie in de firewall engine (Lina).
4. toon conn alle poort 8305 – toont sftunnelverbindingen via de Lina-motor.

Als u problemen met beheerverbindingen wilt oplossen, raadpleegt u het gedeelte Problemen oplossen in de sectie Verbinding beheren in de officiële handleiding.

Referenties

1. Cisco Secure Firewall Management Center Device Configuration Guide, 10.x
2. De toegangsinterface van Manager wijzigen
3. Problemen met de beheerverbinding oplossen

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.