

Configureer Manager Access op FTD van beheer naar gegevensinterface

Inhoud

[Inleiding](#)

[Voorwaarden](#)

[Vereisten](#)

[Gebruikte componenten](#)

[Achtergrondinformatie](#)

[Configureren](#)

[Ga verder met interfacemigratie](#)

[SSH op platform-instellingen inschakelen](#)

[Verifiëren](#)

[Verifiëren via FMC Graphical User Interface \(GUI\)](#)

[Verifiëren vanaf FTD Command Line Interface \(CLI\)](#)

[Problemen oplossen](#)

[Beheerverbindingsstatus](#)

[Werkscenario](#)

[Niet-werkend scenario](#)

[De netwerkinformatie valideren](#)

[Valideren van de beheerderstaat](#)

[Netwerkconnectiviteit valideren](#)

[Het beheercentrum pingen](#)

[Interfacestatus, statistieken en pakketaantal controleren](#)

[Valideren van route op FTD naar FMC](#)

[Controleer de verbindingstatistieken en de subtunnelstatus](#)

[Gerelateerde informatie](#)

Inleiding

In dit document wordt beschreven hoe de Manager Access on the Firepower Threat Defence (FTD) kan worden gewijzigd van een beheer in een Data-interface.

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- Firepower Threat Defence
- Firepower Management Center

Gebruikte componenten

- Firepower Management Center Virtual 7.4.1
- Firepower Threat Defense Virtual 7.2.5

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

Elk apparaat beschikt over één specifieke beheerinterface voor communicatie met het VCC. U kunt het apparaat naar keuze configureren om een data-interface te gebruiken voor beheer in plaats van de speciale Management-interface. De FMC-toegang op een data-interface is handig als u de Firepower Threat Defence op afstand wilt beheren vanuit de buiteninterface, of als u geen afzonderlijk beheernetwerk hebt. Deze wijziging moet worden uitgevoerd in het Firepower Management Center (FMC) voor FTD die door het FMC wordt beheerd.

De FMC-toegang via een data-interface heeft de volgende beperkingen:

- U kunt alleen beheerderstoegang inschakelen op één fysieke gegevensinterface. U kunt geen subinterface of EtherChannel gebruiken.
- Routed firewall-modus alleen, met een routed interface.
- PPPoE wordt niet ondersteund. Als uw ISP PPPoE vereist, moet u een router met ondersteuning van PPPoE tussen de Firepower Threat Defence en de WAN-modem plaatsen.
- U kunt geen afzonderlijke beheer- en gebeurtenisinterfaces gebruiken.

Configureren

Ga verder met interfacemigratie

Opmerking: het is sterk aanbevolen om de laatste back-up van zowel FTD als FMC te hebben voordat u doorgaat met eventuele wijzigingen.

1. Navigeer naar de pagina Apparaten > Apparaatbeheer en klik op Bewerken voor het apparaat dat u wijzigt.

[Collapse All](#) [Download Device List Report](#)

<input type="checkbox"/>	Name	Model	Version	Chassis	Licenses	Access Control Policy	Auto RollBack	Group	
<input type="checkbox"/>	▼ FMT Test (1)								
<input type="checkbox"/>	FTD-Test Short 3 192.168.1.8 - Routed	FTDv for VMware	7.2.5	N/A	Essentials	Base-ACP	↺		Edit →

2. Ga naar het gedeelte Apparaat > Beheer en klik op de koppeling voor Manager Access Interface.

Management ✎ 🔴	
Remote Host Address:	192.168.1.8
Secondary Address:	
Status:	✔
Manager Access Interface:	 Management Interface

Het veld Toegang tot beheer toont de bestaande beheerinterface. Klik op de koppeling om het nieuwe interfacetype te selecteren. Dit is de optie Data Interface in de vervolgkeuzelijst Apparaat beheren en klik op Opslaan.

Manager Access Interface ?

i This is an advanced setting and need to be configured only if needed. See the [online help](#) for detailed steps.

Manage device by

Management Interface ▼

Management Interface

Data Interface

Close Save

3. U moet nu verdergaan om beheerstoegang op een data-interface in te schakelen, naar Apparaten > Apparaatbeheer > Interfaces > Fysieke interface bewerken > Manager toegang.

Edit Physical Interface



- General
- IPv4
- IPv6
- Path Monitoring
- Hardware Configuration
- Manager Access**
- Advanced

Enable management access

Available Networks: +

-
- 10.201.204.129
 - 192.168.1.0_24
 - any-ipv4
 - any-ipv6
 - CSM
 - Data_Store

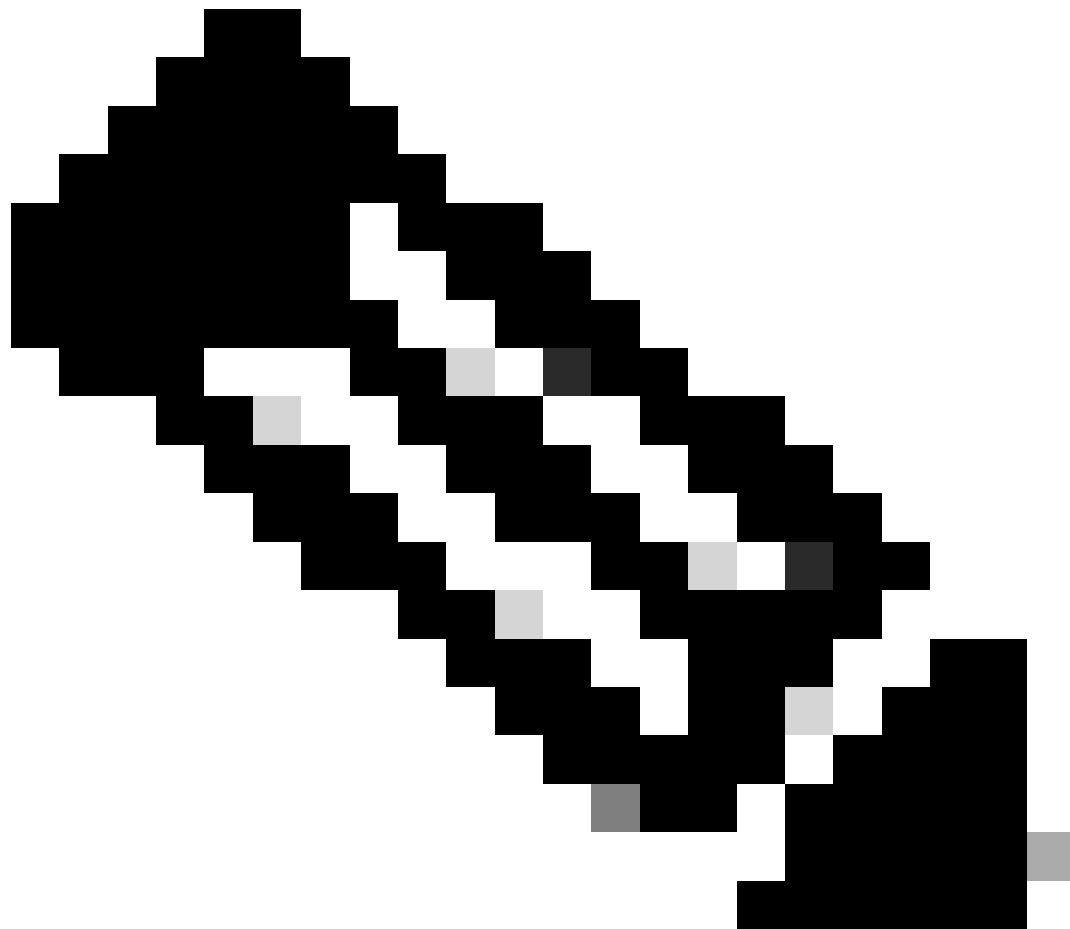
Add

Allowed Management Networks

- any

Cancel

OK



Opmerking: (optioneel) Als u een secundaire interface voor redundantie gebruikt, schakelt u beheertoegang in op de interface die voor redundantiedoeleinden wordt gebruikt.

(Optioneel) Als u DHCP voor de interface gebruikt, schakelt u de DDNS-methode van het webtype in op het dialoogvenster Apparaten > Apparaatbeheer > DHCP > DDNS.

(Facultatief) vorm DNS in een beleid van de Instellingen van het Platform, en pas het op dit apparaat bij Apparaten > de Montages van het Platform > DNS toe.

4. Zorg ervoor dat de bedreigingsverdediging naar het beheercentrum kan routeren via de data-interface; voeg indien nodig een statische route toe op Apparaten > Apparaatbeheer > Routing > Statische route.

1. Klik op IPv4 of IPv6 afhankelijk van het type statische route dat u toevoegt.
2. Kies de interface waarop deze statische route van toepassing is.
3. Kies in de lijst Beschikbare netwerken het doelnetwerk.
4. Voer in het veld Gateway of IPv6 Gateway de gatewayrouter in of kies die de volgende hop voor deze route is.

(Optioneel) Om de beschikbaarheid van de route te bewaken, voert u de naam in van een monitorobject Service Level Agreement (SLA) dat het monitoringbeleid definieert, in het veld Route Tracking.

Add Static Route Configuration



Type: IPv4 IPv6

Interface*



(Interface starting with this icon  signifies it is available for route leak)

Available Network  +

Add

Selected Network



10.201.204.129
192.168.1.0_24
any-ipv4
CSM
Data_Store
FDM

Gateway*

+



Metric:

(1 - 254)

Tunneled: (Used only for default Route)

Route Tracking:

+

Cancel

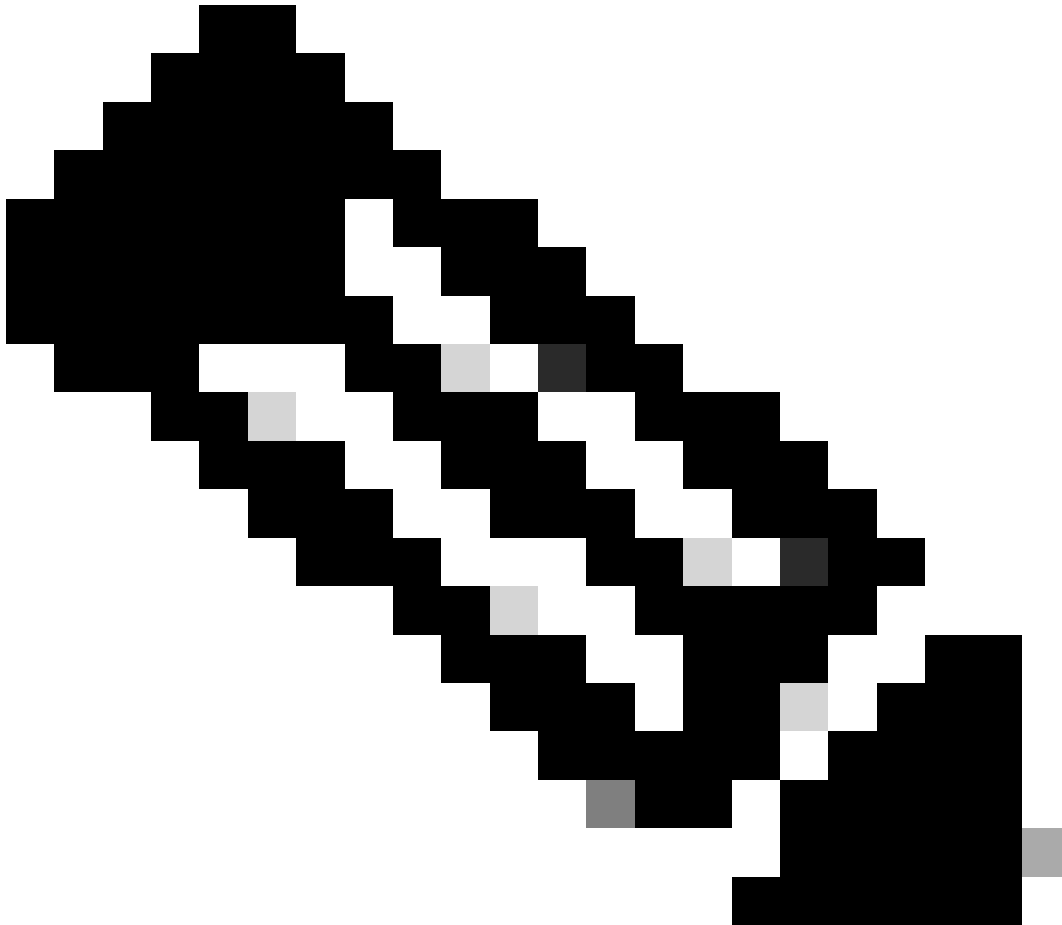
OK

5. Implementeer configuratiewijzigingen. De configuratiewijzigingen worden nu via de huidige beheerinterface geïmplementeerd.

6. Stel in de FTD CLI de beheerinterface in op een statisch IP-adres en stel de gateway in als data-interfaces.

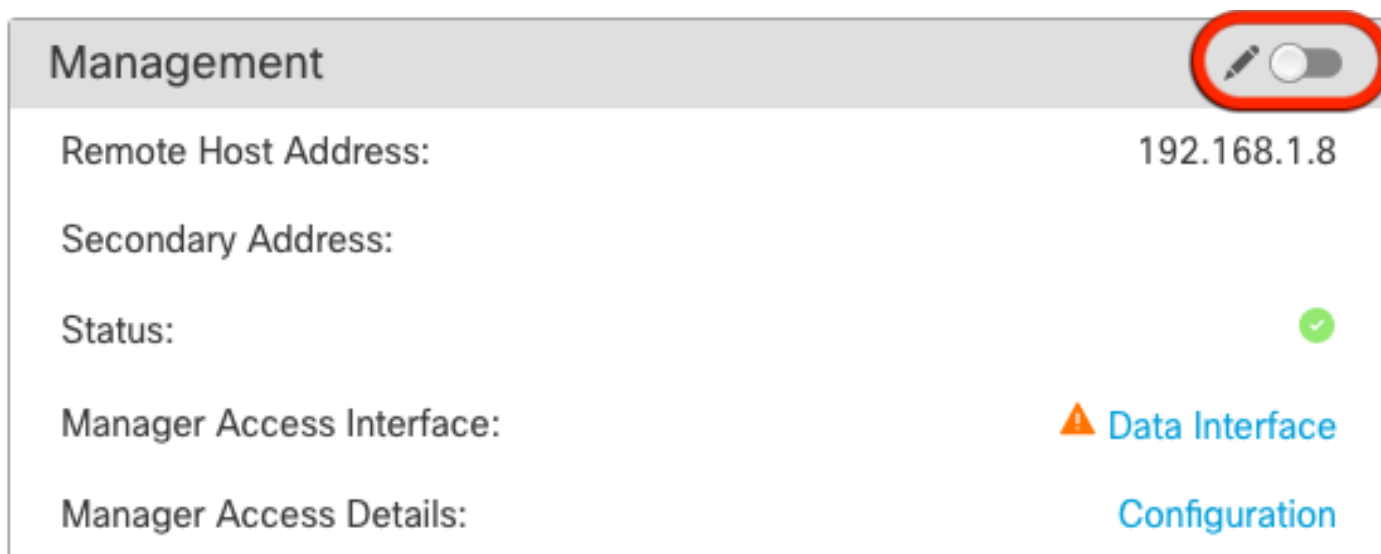
- `configure network {ipv4 | ipv6} manual ip_address netmask data-interfaces`


```
>
>
> configure network ipv4 manual IP_ADDRESS192.168.1.8 NETMASK255.255.255.0 GATEWAYdata-interfaces
Setting IPv4 network configuration...
Interface eth0 speed is set to '10000baseT/Full'
Network settings changed.
```



Opmerking: hoewel u niet van plan bent de beheerinterface te gebruiken, moet u een statisch IP-adres instellen. Bijvoorbeeld, een privé adres zodat u de gateway aan **gegeven-interfaces** kunt plaatsen. Dit beheer wordt gebruikt om het beheerverkeer door te sturen naar data-interface met behulp van tap_nlp interface.


7. Schakel het beheer in het Management Center uit, klik op Bewerken en update het **IP-adres van het Remote Host Address (optioneel)** voor de beveiliging tegen bedreigingen in de sectie Apparaten > **Apparaatbeheer** > **Apparaat** > **Beheer en schakel de verbinding in**.




Management 

Remote Host Address: 192.168.1.8

Secondary Address:

Status: 

Manager Access Interface:  [Data Interface](#)

Manager Access Details: [Configuration](#)

SSH op platform-instellingen inschakelen

Schakel SSH voor de data-interface in in Platform Instellingen beleid, en pas het toe op dit apparaat op Apparaten > **Platform-instellingen** > **SSH Access**. Klik op **Add** .

- De hosts of netwerken waarmee u SSH-verbindingen kunt maken.
- Voeg de zones toe die de interfaces bevatten waaraan SSH-verbindingen kunnen worden toegestaan. Voor interfaces niet in een zone, kunt u de **interfacenaam** in het veld **Geselecteerde zones/interfaces** typen en op **Toevoegen** klikken.
- Klik op **OK**. **Breng** de veranderingen aan

Add Secure Shell Configuration



IP Address* +



Available Zones/Interfaces C

Q Search

DMZ

Inside

outside

Add



Selected Zones/Interfaces

Interface Name

Add

Cancel

OK



Opmerking: SSH is standaard niet ingeschakeld op de data-interfaces, dus als u de bedreigingsverdediging met SSH wilt beheren, moet u dit expliciet toestaan.

Verifiëren

Zorg ervoor dat de beheerverbinding via de Data-interface tot stand is gebracht.

Verifiëren via FMC Graphical User Interface (GUI)

Controleer in het beheercentrum de status van de beheerverbinding op de **pagina** Apparaten > **Apparaatbeheer** > **Apparaat** > **Beheer** > **Manager Access - Configuration Details** > **Verbindingsstatus**.

Management

Remote Host Address:	192.168.1.30
Secondary Address:	
Status:	Connected
Manager Access Interface:	Data Interface
Manager Access Details:	Configuration

Verifiëren vanaf FTD Command Line Interface (CLI)

Bij de bedreiging defenceCLI, ga **heftunnel-status-brief**commando in om de status van de beheersverbinding te bekijken.

```
>
> sftunnel-status-brief
PEER:192.168.1.2
Peer channel Channel-A is valid type (CONTROL), using 'tap_nlp', connected to '192.168.1.2' via '169.254.1.2'
Peer channel Channel-B is valid type (EVENT), using 'tap_nlp', connected to '192.168.1.2' via '169.254.1.2'
Registration: Completed.
IPv4 Connection to peer '192.168.1.2' Start Time: Tue Jul 16 22:23:54 2024 UTC
Heartbeat Send Time: Tue Jul 16 22:39:52 2024 UTC
Heartbeat Received Time: Tue Jul 16 22:39:52 2024 UTC
Last disconnect time : Tue Jul 16 22:17:42 2024 UTC
Last disconnect reason : Both control and event channel connections with peer went down
```

De status toont een succesvolle verbinding voor een data-interface, die de interne tap_nlp interface toont.

Problemen oplossen

Controleer in het beheercentrum de status van de beheersverbinding op de **pagina** Apparaten > **Apparaatbeheer** > **Apparaat** > **Beheer** > **Manager Access - Configuration Details** > **Verbindingsstatus**.

Bij de bedreiging defenceCLI, ga **heftunnel-status-brief**commando in om de status van de beheersverbinding te bekijken. U kunt ook **ftunnel-status** gebruiken om meer volledige informatie te bekijken.

Beheersverbindingstatus

Werkscenario

> sftunnel-status-brief

PEER:192.168.1.2

```
Peer channel Channel-A is valid type (CONTROL), using 'eth0', connected to '192.168.1.2' via '192.168.1.8'
Peer channel Channel-B is valid type (EVENT), using 'tap_nlp', connected to '192.168.1.2' via '169.254.1.2'
Registration: Completed.
IPv4 Connection to peer '192.168.1.2' Start Time: Wed Jul 17 06:21:15 2024 UTC
Heartbeat Send Time: Wed Jul 17 17:15:20 2024 UTC
Heartbeat Received Time: Wed Jul 17 17:16:55 2024 UTC
Last disconnect time : Wed Jul 17 06:21:12 2024 UTC
Last disconnect reason : Process shutdown due to stop request from PM
```

Niet-werkend scenario

> sftunnel-status-brief

PEER:192.168.1.2

```
Registration: Completed.
Connection to peer '192.168.1.2' Attempted at Wed Jul 17 17:20:26 2024 UTC
Last disconnect time : Wed Jul 17 17:20:26 2024 UTC
Last disconnect reason : Both control and event channel connections with peer went down
```

De netwerkinformatie valideren

Bij de bedreigingsdefensie CLI, bekijk de netwerkinstellingen van de interface van toegangsgegevens voor beheer en beheer:

> **netwerk weergeven**

```
> show network
===== [ System Information ] =====
Hostname                : ftdcdo.breakstuff.com
Domains                 : breakstuff.com
DNS Servers             : 192.168.1.103
DNS from router        : enabled
Management port        : 8305
IPv4 Default route
  Gateway               : data-interfaces
IPv6 Default route
  Gateway               : data-interfaces

===== [ eth0 ] =====
State                   : Enabled
Link                   : Up
Channels               : Management & Events
Mode                   : Non-Autonegotiation
MDI/MDIX               : Auto/MDIX
MTU                    : 1500
MAC Address            : 00:0C:29:54:D4:47
----- [ IPv4 ] -----
Configuration          : Manual
Address                : 192.168.1.8
Netmask                : 255.255.255.0
Gateway                : 192.168.1.1
----- [ IPv6 ] -----
Configuration          : Disabled

===== [ Proxy Information ] =====
State                   : Disabled
Authentication         : Disabled

===== [ System Information - Data Interfaces ] =====
DNS Servers            :
Interfaces             : GigabitEthernet0/0

===== [ GigabitEthernet0/0 ] =====
State                   : Enabled
Link                   : Up
Name                   : Outside
MTU                    : 1500
MAC Address            : 00:0C:29:54:D4:5B
```

Opmerking: deze opdracht geeft de huidige status van de beheerverbinding niet weer.

Netwerkconnectiviteit valideren

Het beheercentrum pingen

Gebruik bij de bedreigingsverdedigingCLI de opdracht om het beheercentrum van de gegevensinterfaces te pingen:

> fmc_ip pingen

```
> ping 192.168.1.2
Please use 'CTRL+C' to cancel/abort...
Sending 5, 100-byte ICMP Echos to 192.168.1.2, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms
```

Gebruik bij de bedreigingsverdedigingCLI de opdracht om het beheercentrum te pingelen van de beheerinterface, die via de backplane naar de gegevensinterfaces routeert:

> systeem pingen fmc_ip

```
> ping system 192.168.1.2
PING 192.168.1.2 (192.168.1.2) 56(84) bytes of data.
64 bytes from 192.168.1.2: icmp_seq=1 ttl=64 time=0.340 ms
64 bytes from 192.168.1.2: icmp_seq=2 ttl=64 time=0.291 ms
64 bytes from 192.168.1.2: icmp_seq=3 ttl=64 time=0.333 ms
64 bytes from 192.168.1.2: icmp_seq=4 ttl=64 time=0.282 ms
^C
--- 192.168.1.2 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 132ms
rtt min/avg/max/mdev = 0.282/0.311/0.340/0.030 ms
```

Interfacestatus, statistieken en pakketaantal controleren

Bij de bedreigingsdefensieCLI, zie informatie over de interne backplane interface, nlp_int_tap:

> interfacedetails tonen

```
Interface Internal-Data0/1 "nlp_int_tap", is up, line protocol is up
Hardware is en_vtun rev00, BW Unknown Speed-Capability, DLY 1000 usec
(Full-duplex), (1000 Mbps)
Input flow control is unsupported, output flow control is unsupported
MAC address 0000.0100.0001, MTU 1500
IP address 169.254.1.1, subnet mask 255.255.255.248
311553 packets input, 41414494 bytes, 0 no buffer
Received 0 broadcasts, 0 runts, 0 giants
0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
0 pause input, 0 resume input
0 L2 decode drops
232599 packets output, 165049822 bytes, 0 underruns
0 pause output, 0 resume output
0 output errors, 0 collisions, 0 interface resets
0 late collisions, 0 deferred
0 input reset drops, 0 output reset drops
input queue (blocks free curr/low): hardware (0/0)
output queue (blocks free curr/low): hardware (0/0)
Traffic Statistics for "nlp_int_tap":
  311553 packets input, 37052752 bytes
  232599 packets output, 161793436 bytes
  167463 packets dropped
  1 minute input rate 0 pkts/sec, 3 bytes/sec
  1 minute output rate 0 pkts/sec, 0 bytes/sec
  1 minute drop rate, 0 pkts/sec
  5 minute input rate 0 pkts/sec, 3 bytes/sec
  5 minute output rate 0 pkts/sec, 0 bytes/sec
  5 minute drop rate, 0 pkts/sec
Control Point Interface States:
  Interface number is 14
  Interface config status is active
  Interface state is active
```

Valideren van route op FTD naar FMC

Controleer bij de bedreigingsverdediging CLI of de standaardroute (S*) is toegevoegd en of er interne NAT-regels bestaan voor de Management-interface (nlp_int_tap).

> route tonen


```
> show route
```

```
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP  
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area  
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2  
E1 - OSPF external type 1, E2 - OSPF external type 2, V - VPN  
i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2  
ia - IS-IS inter area, * - candidate default, U - per-user static route  
o - ODR, P - periodic downloaded static route, + - replicated route  
SI - Static InterVRF, BI - BGP InterVRF
```

```
Gateway of last resort is not set
```

```
C      192.168.1.0 255.255.255.0 is directly connected, Outside  
L      192.168.1.30 255.255.255.255 is directly connected, Outside
```

```
> NAT tonen
```

```
> show nat  
Manual NAT Policies Implicit (Section 0)  
1 (nlp_int_tap) to (Outside) source static nlp_server__sftunnel_0.0.0.0_intf3 interface destination static 0_0.0.0.0_5 0_0.0.0.0_5 service tcp 8305 8305  
   translate_hits = 5, untranslate_hits = 6  
2 (nlp_int_tap) to (Outside) source static nlp_server__sftunnel::_intf3 interface ipv6 destination static 0::_6 0::_6 service tcp 8305 8305  
   translate_hits = 0, untranslate_hits = 0  
3 (nlp_int_tap) to (Outside) source dynamic nlp_client_0_intf3 interface  
   translate_hits = 10, untranslate_hits = 0  
4 (nlp_int_tap) to (Outside) source dynamic nlp_client_0_ipv6_intf3 interface ipv6  
   translate_hits = 0, untranslate_hits = 0
```

Controleer de verbindingstatistieken en de subtunnelstatus

```
> tonen in werking stellen-configuratie sftunnel
```

```
> show running-config sftunnel  
sftunnel interface Outside  
sftunnel port 8305
```



Waarschuwing: tijdens het hele proces van wijziging van de toegang tot het FTD-bestand, moet u afzien van het verwijderen van de beheerder ervan of van het uitschrijven/forceren van het FTD uit het FMC.

Gerelateerde informatie

- [DNS over platform-instellingen configureren](#)
- [Configuratie van beheertoegang tot FTD \(HTTPS en SSH\) via FMC](#)

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.