

VXLAN-interfaces op beveiligde FTD met beveiligde FMC configureren

Inhoud

[Inleiding](#)

[Voorwaarden](#)

[Vereisten](#)

[Gebruikte componenten](#)

[Achtergrondinformatie](#)

[Netwerkdigram](#)

[Configureren](#)

[De VTEP-peer groep configureren](#)

[De VTEP-broninterface configureren](#)

[De VTEP VLAN-interface configureren](#)

[Verifiëren](#)

[Problemen oplossen](#)

[Gerelateerde informatie](#)

Inleiding

Dit document beschrijft hoe u de VXLAN-interfaces op Secure Firewall Threat Defence (FTD) kunt configureren met het Secure Firewall Management Center (FMC)

Voorwaarden

Vereisten

Cisco raadt u aan deze onderwerpen te kennen:

- Basis VLAN/VXLAN-concepten.
- Basisnetwerkkennis.
- Basis Cisco Secure Management Center-ervaring.
- Basis ervaring met Cisco Secure Firewall Threat Defence.

Gebruikte componenten

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

- Cisco Secure Firewall Management Center Virtual (FMCv) VMware met 7.2.4 release.
- Cisco Secure Firewall Threat Defence Virtual Appliance (FTDv) voor VMware met 7.2.4 release.

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

Virtual Extensible VLAN (VXLAN) biedt Ethernet Layer 2-netwerkservices zoals traditioneel VLAN. Wegens de hoge vraag naar VLAN-segmenten in virtuele omgevingen biedt VXLAN grotere rekbaarheid, flexibiliteit en definieert ook een MAC-in-UDP-inkapselingsschema waarin het oorspronkelijke Layer 2-frame een VXLAN-header heeft toegevoegd en vervolgens in een UDP-IP-pakket wordt geplaatst. Met deze MAC-in-UDP insluiting, tunnelt VXLAN Layer 2 netwerk via Layer 3 netwerk. VXLAN biedt de volgende voordelen:

- VLAN-flexibiliteit in segmenten met meerdere deelnemers:
- Hogere schaalbaarheid voor meer Layer 2 (L2)-segmenten.
- Verbeterd netwerkgebruik.

De Cisco Secure Firewall Threat Defence (FTD) ondersteunt twee typen VXLAN-insluiting.

- VXLAN (gebruikt voor alle beveiligde firewall-bedreigingsverdedigingsmodellen)
- Geneve (gebruikt voor virtuele applicatie voor beveiligde firewall-bedreigingsverdediging)

Geneve inkapseling is vereist voor transparante routing van pakketten tussen Amazon Web Services (AWS) Gateway-taakverdeling en -apparaten, en voor het verzenden van extra informatie.

VXLAN gebruikt het VXLAN Tunnel Endpoint (VTEP) om eindapparaten van huurders aan VXLAN-segmenten in kaart te brengen en VXLAN-insluiting en -decapsulatie uit te voeren. Elke VTEP heeft twee interfacetypen: een of meer virtuele interfaces, VXLAN Network Identifier (VNI) interfaces waar beveiligingsbeleid kan worden toegepast, en een reguliere interface, VTEP source interface, waar VNI interfaces worden getunneld tussen VTEP's. De VTEP-broninterface is gekoppeld aan het IP-netwerk voor VTEP-naar-VTEP-communicatie. VNI-interfaces zijn vergelijkbaar met VLAN-interfaces: het zijn virtuele interfaces die netwerkverkeer op een bepaalde fysieke interface gescheiden houden door gebruik te maken van tagging. Beveiligingsbeleid wordt toegepast op elke VNI-interface. Er kan één VTEP-interface worden toegevoegd en alle VNI-interfaces zijn gekoppeld aan dezelfde VTEP-interface. Er is een uitzondering voor de virtuele clustering van bedreigingsverdediging op AWS.

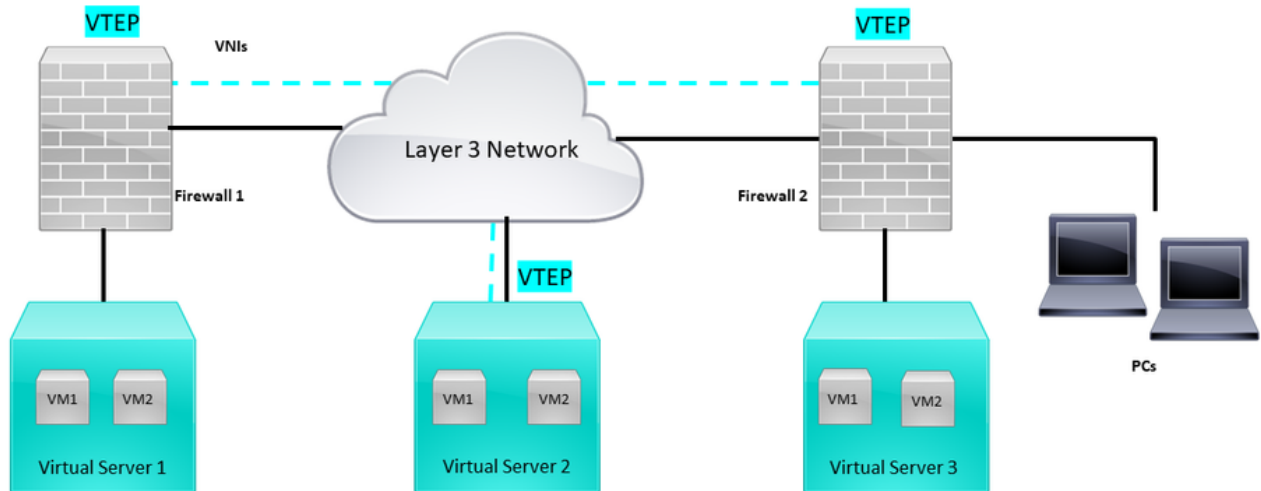
Er zijn drie manieren waarin de bedreigingsverdediging inkapselt en decapsuleert:

- Eén peer VTEP IP-adres kan statisch worden geconfigureerd voor de bescherming tegen bedreigingen.
- Een groep peer-VTEP IP-adressen kan op de bedreigingsverdediging statisch worden geconfigureerd.
- Op elke VNI-interface kan een multicast groep worden geconfigureerd.

Dit document is gericht op VXLAN-interfaces voor VXLAN-insluiting met een groep van twee

statische peer-VTEP IP-adressen. Als u Geneve interfaces moet configureren, controleer dan de Officiële documentatie voor [Geneve interfaces](#) in AWS of configureer VTEP met één peer of multicast groep, controleer dan de VTEP interface met [één peer of multicast](#) groepsconfiguratiegids.

Netwerkdigram



Netwerktopologie

In het gedeelte Configuration wordt ervan uitgegaan dat het onderliggenetwerk al is geconfigureerd voor bescherming tegen bedreigingen via het Secure Firewall Management Center. Dit document is gericht op overlay-netwerkconfiguratie.

Configureren

De VTEP-peer groep configureren

Stap 1: Ga naar Objecten > Objectbeheer.

Objects

Integration

Object Management

Intrusion Rules

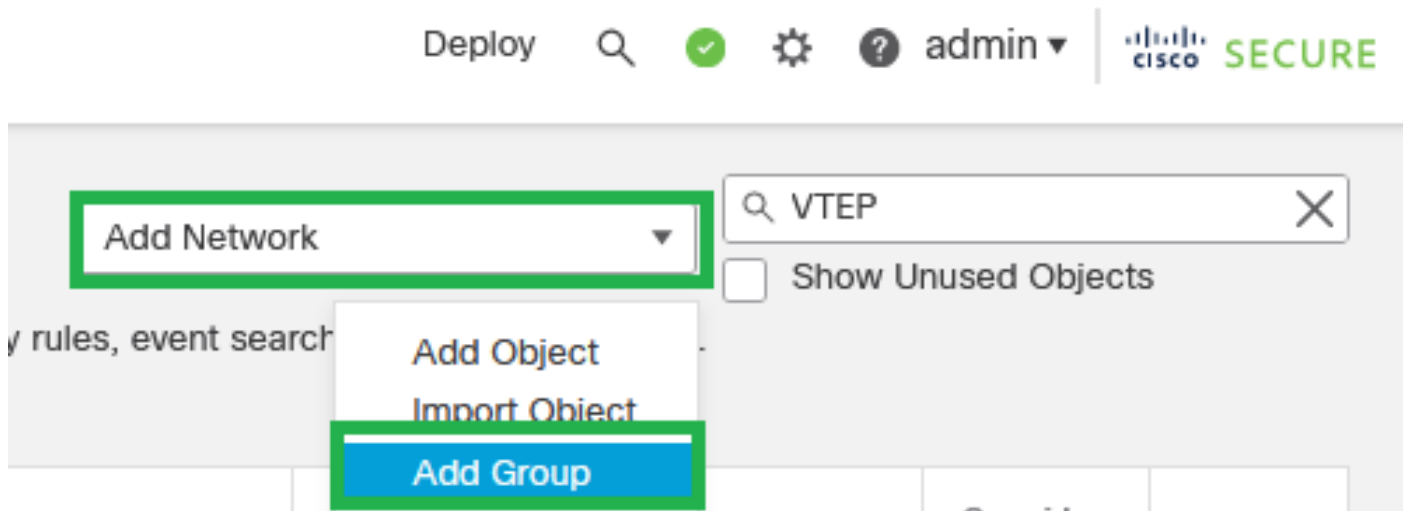
Objecten - Objectbeheer

Stap 2: Klik op Network in het linkermenu.

- > AAA Server
- > Access List
- > Address Pools
- Application Filters
- AS Path
- Cipher Suite List
- > Community List
- > Distinguished Name
- DNS Server Group
- > External Attributes
- File List
- > FlexConfig

: configureer meer host-netwerkobjecten voor elk VTEP peer IP-adres dat u hebt. Er zijn twee objecten in deze configuratiehandleiding.

Stap 5: Maak een objectgroep, klik op Add Network > Add Group.



Netwerk toevoegen - Groep toevoegen

Stap 6: Maak de netwerkobjectgroep met alle VTEP peer IP-adressen. Stel een naam voor de netwerkgroep in en selecteer de gewenste netwerkobjectgroepen. Klik vervolgens op Opslaan.

New Network Group



Name
FPR1-VTEP-Group-Object

Description
This is a network group with VTEP group peer IP addresses

Allow Overrides

Available Networks

Search

- 3-VTEP-172.16.207.1
- FPR1-GW-172.16.203.3
- FPR1-VTEP-Group-Object
- FPR2-GW-172.16.205.3
- FPR2-VTEP-172.16.205.1**
- FTD1-GW1-172.16.203.2

Selected Networks

Search by name

- 3-VTEP-172.16.207.1
- FPR2-VTEP-172.16.205.1

Cancel **Save**

Netwerkgroep maken

Stap 7: Bevestig het netwerkobject en de netwerkgroep vanuit het netwerkobjectfilter.

Network Add Network

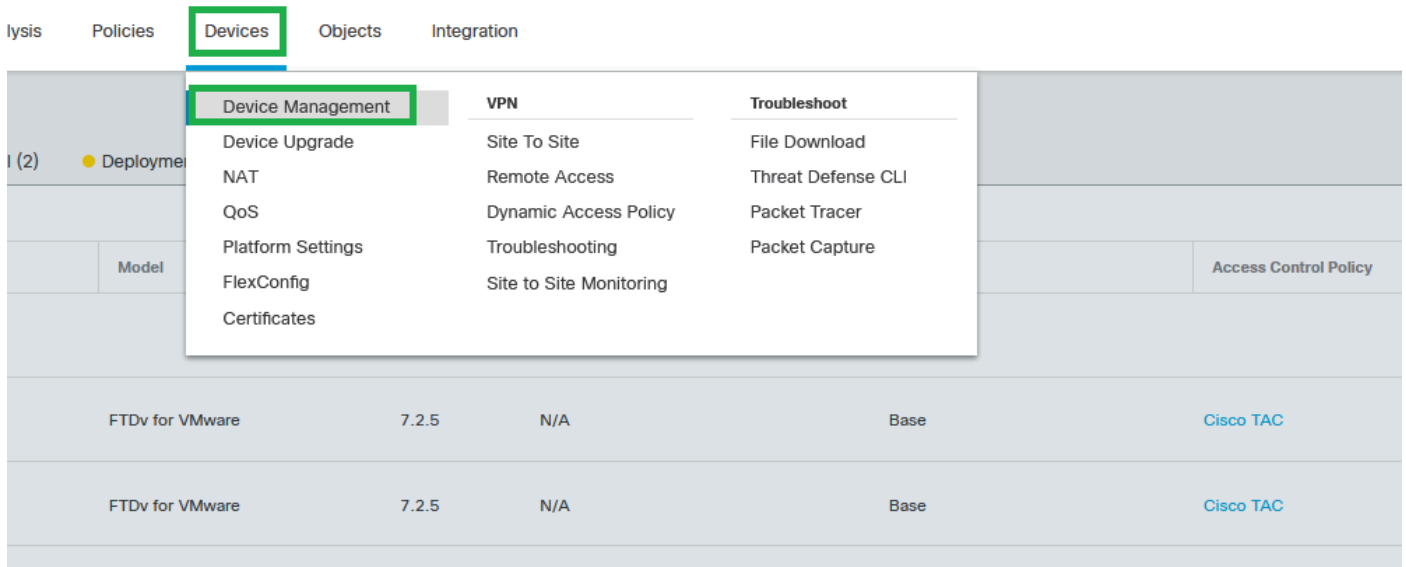
A network object represents one or more IP addresses. Network objects are used in various places, including access control policies, network variables, intrusion rules, identity rules, network discovery rules, event searches, reports, and so on.

Name	Value	Type	Override	
3-VTEP-172.16.207.1	172.16.207.1	Host		
FPR1-VTEP-Group-Object	3-VTEP-172.16.207.1 FPR2-VTEP-172.16.205.1	Group		
FPR2-VTEP-172.16.205.1	172.16.205.1	Host		

De VTEP-objectgroep valideren

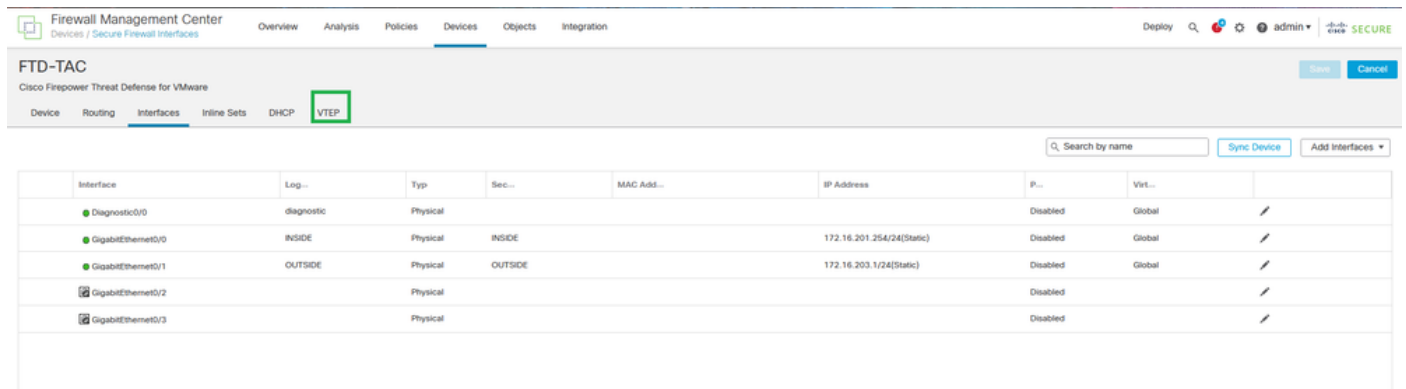
De VTEP-broninterface configureren

Stap 1: Navigeer naar Apparaten > Apparaatbeheer en bewerk de beveiliging tegen bedreigingen.



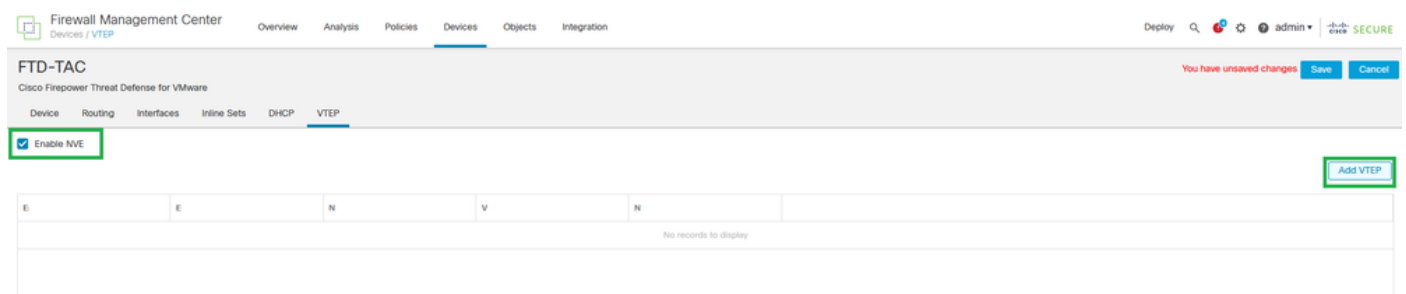
Apparaten - Apparaatbeheer

Stap 2: Navigeer naar de VTEP-sectie.



VTEP-sectie

Stap 3: Selecteer het aanvinkvakje Enable VNE en klik op Add VTEP.



NVE inschakelen en VTEP toevoegen

Stap 4: Kies VxLAN als insluitingstype, voer de waarde voor insluitingshaven in en kies de interface die voor VTEP-bron wordt gebruikt bij deze bedreigingsverdediging (buiteninterface voor

deze configuratiegids)

Add VTEP



Encapsulation type

VxLAN

Encapsulation port*

4789

(1024 - 65535)

NVE number

1



VTEP Source Interface

OUTSIDE


Neighbor Address

None Peer VTEP  Peer Group Default Multicast

Cancel

OK

VTEP toevoegen

 **Opmerking:** VxLAN-insluiting is de standaardinsluiting. Voor AWS kunt u kiezen tussen VxLAN en Geneve. De standaardwaarde is 4789, elke insluitingspoort kan worden gekozen tussen 1024 - 65535 bereik volgens ontwerp.

Stap 5: Selecteer Peer Group en kies de netwerkobjectgroep die in de vorige configuratiesectie is gemaakt. Klik vervolgens op OK.

Add VTEP



Encapsulation type

VxLAN

Encapsulation port*

4789

(1024 - 65535)

NVE number

1

VTEP Source Interface

OUTSIDE

Neighbor Address

None Peer VTEP Peer Group Default Multicast

Network Group*

FPR1-VTEP-Group-Object

Cancel

OK

Peer Group - netwerkgroep

Stap 6: Sla de wijzigingen op.



Waarschuwing: nadat de wijzigingen zijn opgeslagen, verschijnt er een bericht over de wijziging van het jumboframe, wordt MTU gewijzigd op de interface die als VTEP is toegewezen aan 1554, zodat dezelfde MTU op het onderliggenetwerk wordt gebruikt.

Stap 7: Klik op Interfaces en bewerk de interface die wordt gebruikt voor de VTEP-broninterface. (Buiten interface op deze configuratiehandleiding)

FTD-TAC
Cisco Firepower Threat Defense for VMware

Device Routing **Interfaces** Inline Sets DHCP VTEP

Search by name Sync Device Add Interfaces

Interface	Log...	Typ	Sec...	MAC Add...	IP Address	P...	Virt...	
Diagnostic0/0	diagnostic	Physical				Disabled	Global	/
GigabitEthernet0/0	INSIDE	Physical	INSIDE		172.16.201.254/24(Static)	Disabled	Global	/
GigabitEthernet0/1	OUTSIDE	Physical	OUTSIDE		172.16.203.1/24(Static)	Disabled	Global	/
GigabitEthernet0/2		Physical				Disabled		/
GigabitEthernet0/3		Physical				Disabled		/

Buiten als VTEP-broninterface

Stap 8 (optioneel): Schakel op de pagina Algemeen het aankruisvakje Alleen NVE in, en klik vervolgens op OK.

Edit Physical Interface



General	IPv4	IPv6	Path Monitoring	Hardware Configuration	Manager Access	Advanced
<p>Name: <input type="text" value="OUTSIDE"/></p> <p><input checked="" type="checkbox"/> Enabled <input type="checkbox"/> Management Only</p> <p>Description: <input type="text"/></p> <p>Mode: <input type="text" value="None"/></p> <p>Security Zone: <input type="text" value="OUTSIDE"/></p> <p>Interface ID: <input type="text" value="GigabitEthernet0/1"/></p> <p>MTU: <input type="text" value="1554"/> <small>(64 - 9000)</small></p> <p>Priority: <input type="text" value="0"/> <small>(0 - 65535)</small></p> <p>Propagate Security Group Tag: <input checked="" type="checkbox"/></p> <p>NVE Only: <input checked="" type="checkbox"/></p>						
						<input type="button" value="Cancel"/> <input checked="" type="button" value="OK"/>

Configuratie alleen NVE

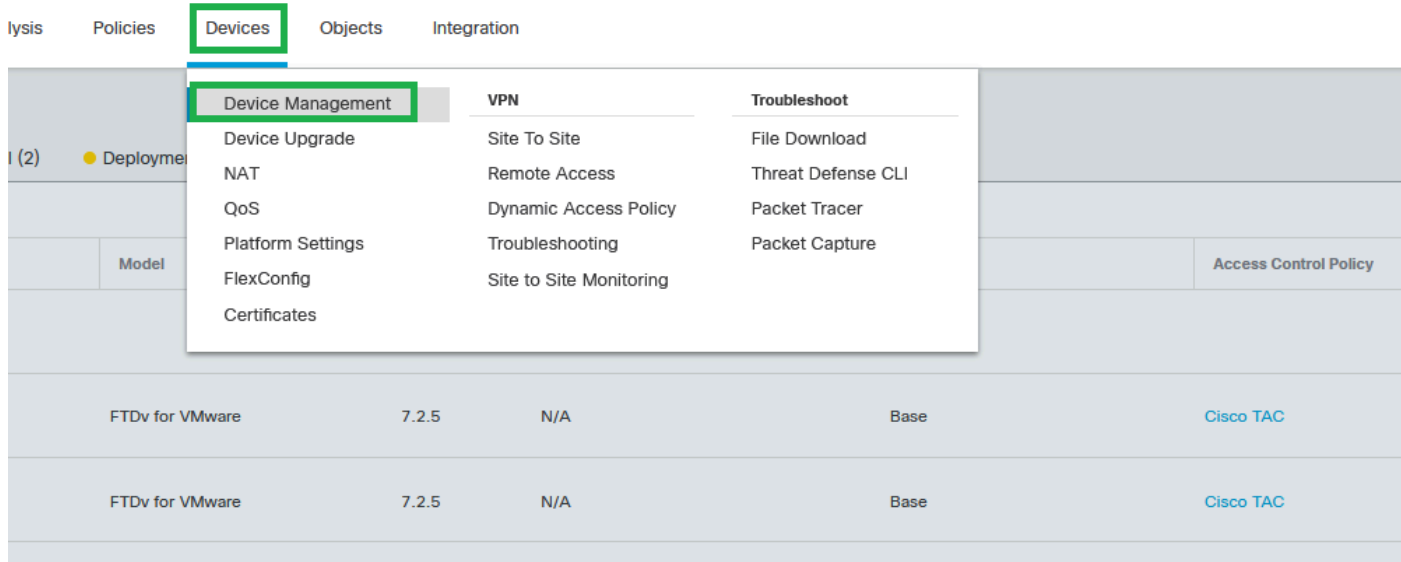


Waarschuwing: deze instelling is optioneel voor Routed Mode, waarbij deze instelling verkeer beperkt tot VXLAN en gemeenschappelijk beheerverkeer, alleen op deze interface. Deze instelling wordt automatisch ingeschakeld voor de transparante firewallmodus.

Stap 9: Sla de wijzigingen op.

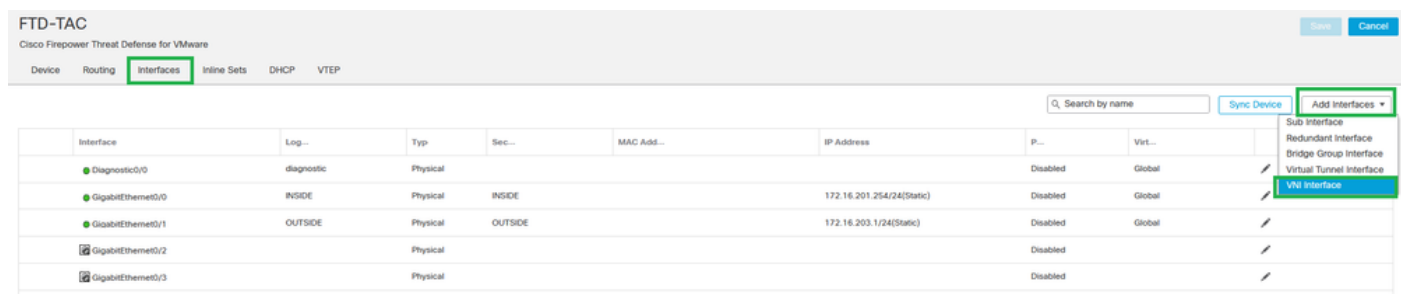
De VTEP VLAN-interface configureren

Stap 1: Navigeer Apparaten > Apparaatbeheer, en bewerk de bedreigingsverdediging.



Apparaten - Apparaatbeheer

Stap 2: Klik onder het gedeelte Interfaces op Interfaces toevoegen > VNI-interfaces.



Interfaces - Interfaces toevoegen - VNI-interfaces

Stap 3: Stel onder de sectie Algemeen de VNI-interface in met naam, beschrijving, Security Zone, VNI-id en VNI-segment-id.

Add VNI Interface



General

IPv4

IPv6

Advanced

Name:

VNI-1

Enabled

Description:

Security Zone:

VNI-1

Priority:

0

(0 - 65535)

VNI ID*:

100

(1 - 10000)

VNI Segment ID:

10001

(1 - 10777215)

Multicast Group IP

Address:

NVE Mapped to

VTEP Interface:

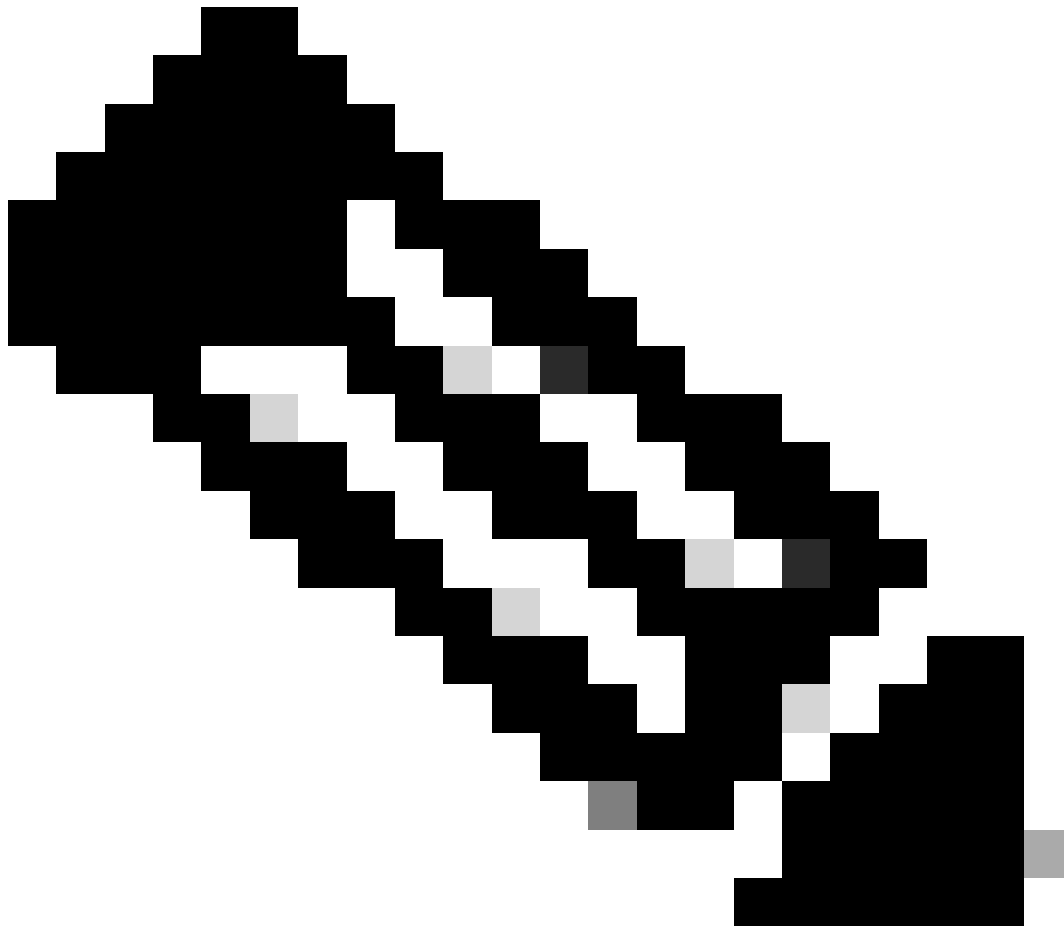
NVE Number:

1

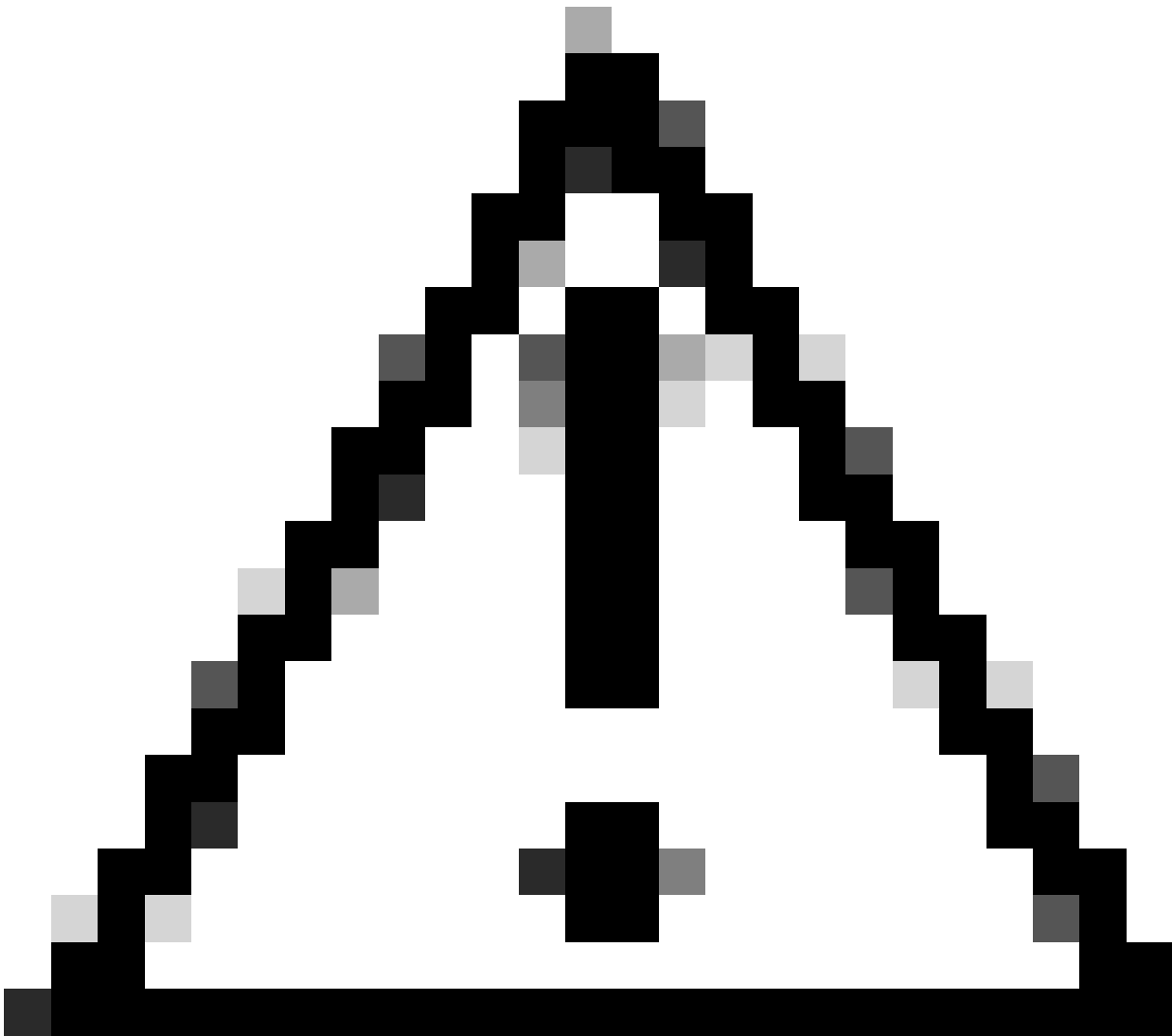
Cancel

OK

VNI-interface toevoegen



Opmerking: de VNI-id is ingesteld tussen 1 en 10000 en de VNI-segment-ID is ingesteld tussen 1 en 16777215 (de segment-id wordt gebruikt voor VXLAN-codering).



Waarschuwing: als de multicast groep niet is geconfigureerd op de VNI-interface, wordt de standaardgroep uit de configuratie van de VTEP-broninterface gebruikt als deze beschikbaar is. Als u handmatig een VTEP peer IP instelt voor de VTEP-broninterface, kunt u geen multicast groep voor de VNI-interface specificeren.

Stap 3: Selecteer het selectievakje NVE toegewezen aan VTEP-interface en klik op OK.

Add VNI Interface



General

IPv4

IPv6

Advanced

Name:

VNI-1

Enabled

Description:

Security Zone:

VNI-1

Priority:

0

(0 - 65535)

VNI ID*:

100

(1 - 10000)

VNI Segment ID:

10001

(1 - 16777215)

Multicast Group IP

Address:

NVE Mapped to
VTEP Interface:



NVE Number:

Cancel

OK

NVE toegewezen aan VTEP-interface

Stap 4: Configureer een statische route om de doelnetwerken voor VXLAN te adverteren naar de VNI peer interface. Navigeer routing > Statische route.

Firewall Management Center
Devices / Secure Firewall Routing

Overview Analysis Policies **Devices** Objects Integration

Deploy 🔍 ⚙️ admin 🔒 **SECURE**

FTD-TAC

Cisco Firepower Threat Defense for VMware





Device **Routing** Interfaces Inline Sets DHCP VTEP

Manage Virtual Routers + Add Route

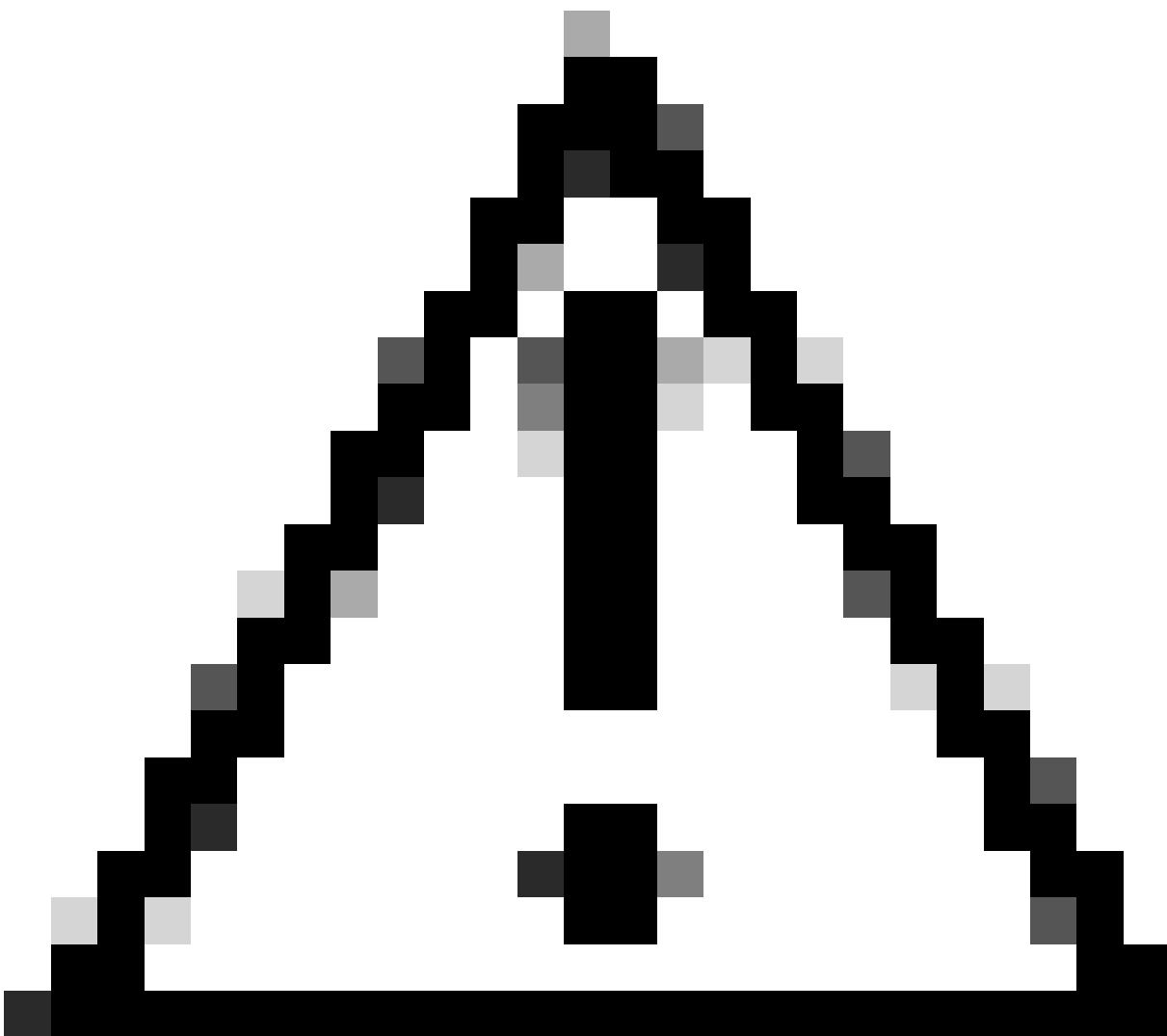
Global

Virtual Router Properties

- ECMP
- OSPF
- OSPFV3
- EIGRP
- RIP
- Policy Based Routing
- BGP
 - IPv4
 - IPv6
- Static Route

Network	Interface	Leaked from Virtual Router	Gateway	Tunneled	Metric	Tracked
IPv4 Routes						
FPR2-INSIDE-172.16.212.0-24	VNI-1	Global	FPR2-VNI-IP-172.16.209.2	false	1	 
any-ipv4	OUTSIDE	Global	FPR1-GW-172.16.203.3	false	10	 
IPv6 Routes						

Statische routeconfiguratie



Waarschuwing: doelnetwerken voor VXLAN moeten worden verzonden via de peer-VNI-interface. Alle VNI-interfaces moeten zich op hetzelfde uitzenddomein bevinden (logisch segment).

Stap 5: Opslaan en implementeren van de wijzigingen.



Waarschuwing: validatiewaarschuwingen kunnen worden gezien vóór de implementatie, om ervoor te zorgen dat de VTEP peer IP-adressen bereikbaar zijn vanuit de fysieke VTEP-broninterface.

Verifiëren

Controleer de NVE configuratie.

```
firepower# show running-config nve
nve 1
encapsulation vxlan
source-interface OUTSIDE
peer-group FPR1-VTEP-Group-Object
```

```
firepower# show nve 1
nve 1, source-interface "OUTSIDE" is up (nve-only cluster is OFF)
IP address 172.16.203.1, subnet mask 255.255.255.0
Encapsulation: vxlan
Encapsulated traffic statistics:
1309 packets input, 128170 bytes
2009 packets output, 230006 bytes
142 packets dropped
Number of configured static peer VTEPs: 0
Configured static peer group: FPR1-VTEP-Group-Object
Configured static peer group VTEPs:
IP address 172.16.205.1 MAC address 0050.56b3.c30a (learned)
IP address 172.16.207.1 MAC address 0050.56b3.c30a (learned)
Number of discovered peer VTEPs: 1
Discovered peer VTEPs:
IP address 172.16.205.1
IP address 172.16.207.1
Number of VNIs attached to nve 1: 1
VNIs attached:
vni 100: proxy off, segment-id 10001, mcast-group none
NVE proxy single-arm channel is off.
```

```
firepower# show nve 1 summary
nve 1, source-interface "OUTSIDE" is up (nve-only cluster is OFF)
Encapsulation: vxlan
Number of configured static peer VTEPs: 0
Configured static peer group: FPR1-VTEP-Group-Object
Number of discovered peer VTEPs: 2
Number of VNIs attached to nve 1: 1
NVE proxy single-arm channel is off.
```

Controleer de configuratie van de VNI-interface.

```
firepower# show run interface
interface vni100
segment-id 10001
nameif VNI-1
security-level 0
ip address 172.16.209.1 255.255.255.0
vtep-nve 1
```

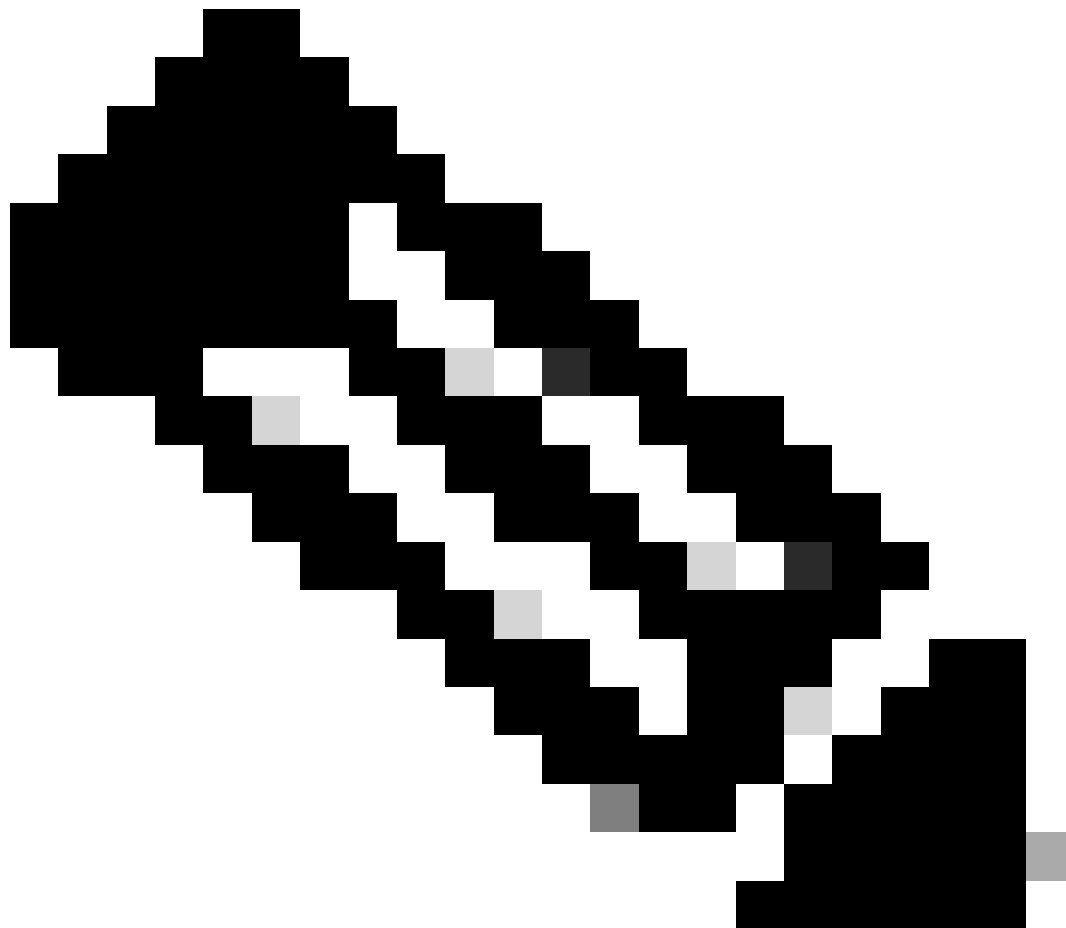
Controleer de MTU-configuratie op de VTEP-interface.

```
firepower# show interface GigabitEthernet0/1
Interface GigabitEthernet0/1 "OUTSIDE", is up, line protocol is up
Hardware is net_vmxnet3, BW 10000 Mbps, DLY 10 usec
Auto-Duplex(Full-duplex), Auto-Speed(10000 Mbps)
Input flow control is unsupported, output flow control is unsupported
MAC address 0050.56b3.26b8, MTU 1554
IP address 172.16.203.1, subnet mask 255.255.255.0
```

[Output omitted]

Controleer de statische routeconfiguratie voor doelnetwerken.

```
firepower# show run route  
route OUTSIDE 0.0.0.0 0.0.0.0 172.16.203.3 10  
route VNI-1 172.16.212.0 255.255.255.0 172.16.209.2 1  
route VNI-1 172.16.215.0 255.255.255.0 172.16.209.3 1
```



Opmerking: valideren van de VNI-interfaces op alle peers zijn geconfigureerd op hetzelfde broadcast-domein.

Problemen oplossen

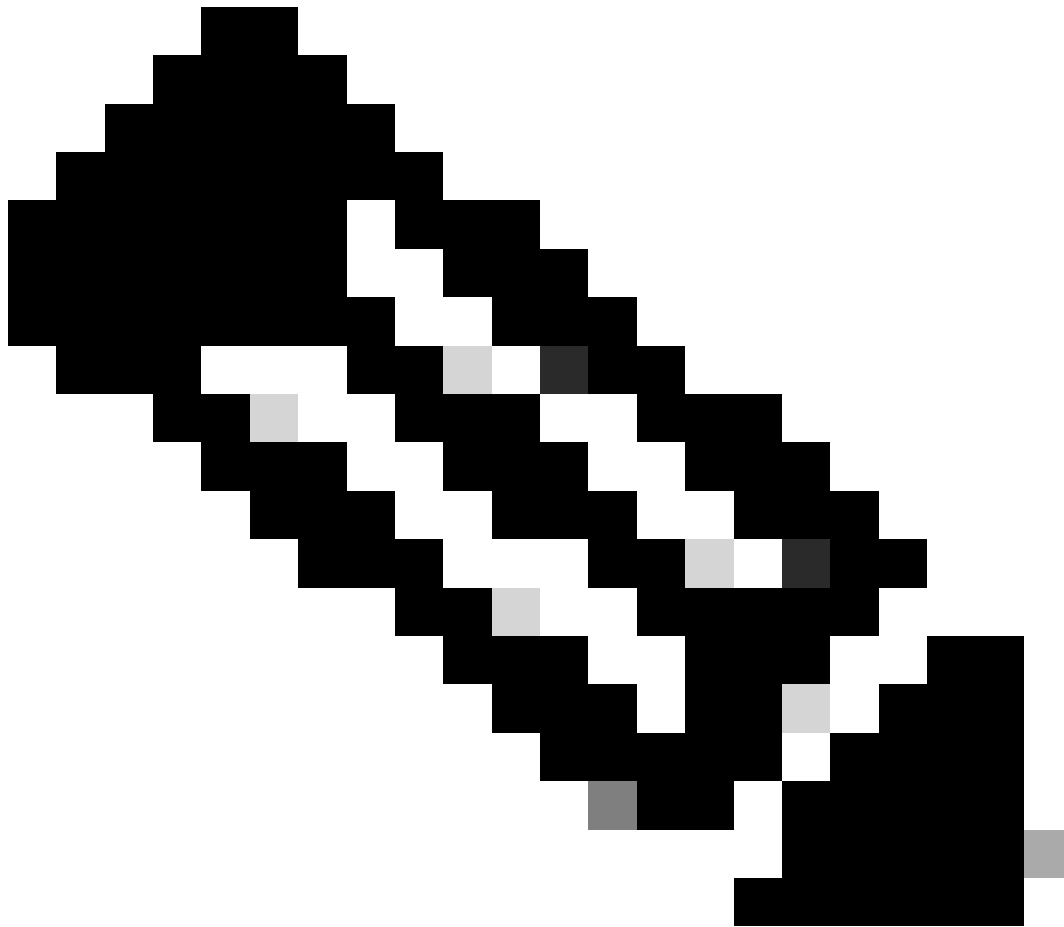
Controleer de connectiviteit met VTEP-peers.

Peer 1:

```
firepower# ping 172.16.205.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.16.205.1, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms
```

Peer 2:

```
firepower# ping 172.16.207.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.16.207.1, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms
```



Opmerking: een probleem met VTEP-peer-connectiviteit kan implementatiefouten genereren op Secure FMC. Zorg ervoor dat de connectiviteit met al uw VTEP-peer-configuraties behouden blijft.

Controleer de connectiviteit met VNI-peers.

.

Peer 1:

```
firepower# ping 172.16.209.2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.16.209.2, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/10 ms
```


Peer 2:

```
 firepower# ping 172.16.209.3
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.16.209.3, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/10 ms
```

Soms, kan een verkeerde statische route gevormd ARP onvolledige output produceren. Configureer een opname op de VTEP interface voor VXLAN-pakketten en download deze op een pcap-indeling. Elk pakketanalyzer-gereedschap helpt te bevestigen of er problemen zijn met de routes. Zorg ervoor dat u het VNI peer IP-adres als gateway gebruikt.

Broadcast	ARP	92 who has 172.16.209.3? Tell 172.16.209.1
Broadcast	ARP	92 who has 172.16.209.3? Tell 172.16.209.1
Broadcast	ARP	92 who has 172.16.209.3? Tell 172.16.209.1
Broadcast	ARP	92 who has 172.16.209.3? Tell 172.16.209.1
Broadcast	ARP	92 who has 172.16.209.3? Tell 172.16.209.1
Broadcast	ARP	92 who has 172.16.209.3? Tell 172.16.209.1
Broadcast	ARP	92 who has 172.16.209.3? Tell 172.16.209.1
Broadcast	ARP	92 who has 172.16.209.3? Tell 172.16.209.1
Broadcast	ARP	92 who has 172.16.209.3? Tell 172.16.209.1
Broadcast	ARP	92 who has 172.16.209.3? Tell 172.16.209.1

Probleem met routing

Configureer de ASP-drop-opnamen op beveiligde FTD in het geval van een Firewall-drop, controleer de ASP-drop-teller met de opdracht Snel drogen. Neem contact op met Cisco TAC voor analyse.

Zorg ervoor dat u toegangscontroleregels configureert om het VXLAN UDP-verkeer op de VNI/VTEP-interface toe te staan.

Soms kunnen de VXLAN-pakketten gefragmenteerd zijn en ervoor zorgen dat de MTU wordt gewijzigd in jumboframes op het onderlegnetwerk om fragmentatie te voorkomen.

Configureer de opname op de Ingress/VTEP-interface en download de opnamen op .pcap-formaat voor analyse. De pakketten moeten de VXLAN-header op de VTEP-interface bevatten.

1	2023-10-01 17:10:31.039823	172.16.201.1	172.16.212.2	ICMP	148 Echo (ping) request id=0x0032, seq=3285/54540, ttl=64 (reply in 2)
2	2023-10-01 17:10:31.041593	172.16.212.2	172.16.201.1	ICMP	148 Echo (ping) reply id=0x0032, seq=3285/54540, ttl=128 (request in 1)
3	2023-10-01 17:10:32.042127	172.16.201.1	172.16.212.2	ICMP	148 Echo (ping) request id=0x0032, seq=3286/54796, ttl=64 (reply in 4)
4	2023-10-01 17:10:32.043698	172.16.212.2	172.16.201.1	ICMP	148 Echo (ping) reply id=0x0032, seq=3286/54796, ttl=128 (request in 3)
5	2023-10-01 17:10:33.044171	172.16.201.1	172.16.212.2	ICMP	148 Echo (ping) request id=0x0032, seq=3287/55052, ttl=64 (reply in 6)
6	2023-10-01 17:10:33.046140	172.16.212.2	172.16.201.1	ICMP	148 Echo (ping) reply id=0x0032, seq=3287/55052, ttl=128 (request in 5)
7	2023-10-01 17:10:34.044797	172.16.201.1	172.16.212.2	ICMP	148 Echo (ping) request id=0x0032, seq=3288/55308, ttl=64 (reply in 8)
8	2023-10-01 17:10:34.046430	172.16.212.2	172.16.201.1	ICMP	148 Echo (ping) reply id=0x0032, seq=3288/55308, ttl=128 (request in 7)
9	2023-10-01 17:10:35.046903	172.16.201.1	172.16.212.2	ICMP	148 Echo (ping) request id=0x0032, seq=3289/55564, ttl=64 (reply in 10)
10	2023-10-01 17:10:35.049527	172.16.212.2	172.16.201.1	ICMP	148 Echo (ping) reply id=0x0032, seq=3289/55564, ttl=128 (request in 9)
11	2023-10-01 17:10:36.048352	172.16.201.1	172.16.212.2	ICMP	148 Echo (ping) request id=0x0032, seq=3290/55820, ttl=64 (reply in 12)
12	2023-10-01 17:10:36.049832	172.16.212.2	172.16.201.1	ICMP	148 Echo (ping) reply id=0x0032, seq=3290/55820, ttl=128 (request in 11)
13	2023-10-01 17:10:37.049786	172.16.201.1	172.16.212.2	ICMP	148 Echo (ping) request id=0x0032, seq=3291/56076, ttl=64 (reply in 14)
14	2023-10-01 17:10:37.051465	172.16.212.2	172.16.201.1	ICMP	148 Echo (ping) reply id=0x0032, seq=3291/56076, ttl=128 (request in 13)

Ping opgenomen met VXLAN-header

```
> Frame 8: 148 bytes on wire (1184 bits), 148 bytes captured (1184 bits)
> Ethernet II, Src: Vhuare_b3:ba:6a (00:50:56:b3:ba:6a), Dst: Vhuare_b3:6e:68 (00:50:56:b3:6e:68)
> Internet Protocol Version 4, Src: 172.16.209.1, Dst: 172.16.209.1
> User Datagram Protocol, Src Port: 61587, Dst Port: 4789
> Virtual eXtensible Local Area Network
  > Flags: 0x0000, VXLAN Network ID (VNI)
    Group Policy ID: 0
    VXLAN Network Identifier (VNI): 10001
    Reserved: 0
  > Ethernet II, Src: Vhuare_b3:ba:6a (00:50:56:b3:ba:6a), Dst: Vhuare_b3:26:b8 (00:50:56:b3:26:b8)
    > Destination: Vhuare_b3:26:b8 (00:50:56:b3:26:b8)
    > Source: Vhuare_b3:ba:6a (00:50:56:b3:ba:6a)
    > Type: IPv4 (0x0800)
  > Internet Protocol Version 4, Src: 172.16.212.2, Dst: 172.16.201.1
  > Internet Control Message Protocol
```

Gerelateerde informatie

- [VXLAN-interfaces configureren](#)
- [VXLAN-gebruikscases](#)
- [VXLAN-pakketverwerking](#)
- [De VTEP-broninterface configureren](#)
- [De VPN-interface configureren](#)
- [Cisco Technical Support en downloads](#)

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.