Konfigurieren von VXLAN-Schnittstellen auf sicherem FTD mit sicherem FMC

Inhalt

Einleitung

In diesem Dokument wird beschrieben, wie Sie die VXLAN-Schnittstellen auf Secure Firewall Threat Defense (FTD) mit dem Secure Firewall Management Center (FMC) konfigurieren.

Voraussetzungen

Anforderungen

Cisco empfiehlt, dass Sie folgende Themen kennen:

- Grundlegende VLAN-/VXLAN-Konzepte.
- Grundlegende Netzwerkkenntnisse.
- Grundlegende Cisco Secure Management Center-Erfahrung.
- Grundlegende Cisco Secure Firewall Threat Defense-Erfahrung.

Verwendete Komponenten

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

- Cisco Secure Firewall Management Center Virtual (FMCv) VMware mit Version 7.2.4.
- Cisco Secure Firewall Threat Defense Virtual Appliance (FTDv) VMware mit Version 7.2.4.

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.

Hintergrundinformationen

Virtual Extensible VLAN (VXLAN) stellt Ethernet-Layer-2-Netzwerkdienste bereit, wie dies bei herkömmlichen VLANs der Fall ist. Aufgrund der hohen Nachfrage nach VLAN-Segmenten in virtuellen Umgebungen bietet VXLAN eine größere Erweiterbarkeit und Flexibilität und definiert außerdem ein MAC-in-UDP-Kapselungsschema, bei dem dem ursprünglichen Layer-2-Frame ein VXLAN-Header hinzugefügt und dann in einem UDP-IP-Paket platziert wird. Mit dieser MAC-in-UDP-Kapselung tunnelt VXLAN das Layer-2-Netzwerk über das Layer-3-Netzwerk. VXLAN bietet die folgenden Vorteile:

- VLAN-Flexibilität in Multi-Tenant-Segmenten:
- Höhere Skalierbarkeit für mehr Layer-2-Segmente (L2)
- Verbesserte Netzwerkauslastung.

Die Cisco Secure Firewall Threat Defense (FTD) unterstützt zwei Arten der VXLAN-Kapselung.

- VXLAN (für alle Modelle zum Schutz vor Bedrohungen von sicheren Firewalls)
- Geneve (für die virtuelle Appliance Secure Firewall Threat Defense)

Für die transparente Weiterleitung von Paketen zwischen dem Amazon Web Services (AWS) Gateway Load Balancer und Appliances sowie für die Übermittlung zusätzlicher Informationen ist eine Geneve-Kapselung erforderlich.

VXLAN verwendet den VXLAN Tunnel Endpoint (VTEP), um die Endgeräte von Tenants VXLAN-Segmenten zuzuordnen und VXLAN-Kapselung und -Entkapselung durchzuführen. Jeder VTEP verfügt über zwei Schnittstellentypen: eine oder mehrere virtuelle Schnittstellen, die als VXLAN Network Identifier (VNI)-Schnittstellen bezeichnet werden und auf die Sicherheitsrichtlinien angewendet werden können, und eine reguläre Schnittstelle, die als VTEP-Quellschnittstelle bezeichnet wird und über die VNI-Schnittstellen zwischen VTEPs getunnelt werden. Die VTEP-Quellschnittstelle ist mit dem Transport-IP-Netzwerk für die VTEP-zu-VTEP-Kommunikation verbunden. Die VNI-Schnittstellen ähneln den VLAN-Schnittstellen: Es handelt sich um virtuelle Schnittstellen, bei denen der Netzwerkverkehr auf einer bestimmten physischen Schnittstelle durch Tagging getrennt bleibt. Sicherheitsrichtlinien werden auf jede VNI-Schnittstelle angewendet. Eine VTEP-Schnittstelle kann hinzugefügt werden, und alle VNI-Schnittstellen sind derselben VTEP-Schnittstelle zugeordnet. Es gibt eine Ausnahme für das virtuelle Clustering zum Schutz vor Bedrohungen auf AWS.

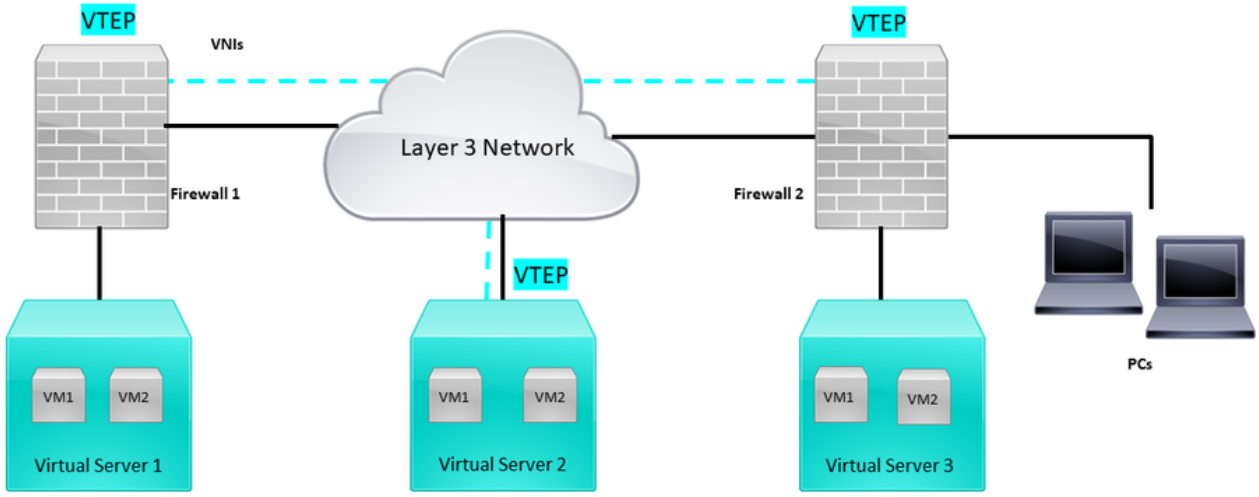
Es gibt drei Möglichkeiten, wie die Bedrohungsabwehr Kapselung und Entkapselung vornimmt:

- Eine einzelne Peer-VTEP-IP-Adresse kann statisch für die Bedrohungsabwehr konfiguriert werden.
- Eine Gruppe von Peer-VTEP-IP-Adressen kann statisch für die Bedrohungsabwehr

konfiguriert werden.
- Auf jeder VNI-Schnittstelle kann eine Multicast-Gruppe konfiguriert werden.

Dieses Dokument behandelt VXLAN-Schnittstellen zur VXLAN-Kapselung mit einer Gruppe von zwei statisch konfigurierten Peer-VTEP-IP-Adressen. Wenn Sie Geneve-Schnittstellen konfigurieren müssen, lesen Sie die offizielle Dokumentation zu Geneve-Schnittstellen in AWS, oder konfigurieren Sie VTEP mit einem einzelnen Peer oder einer Multicast-Gruppe. Überprüfen Sie die VTEP-Schnittstelle mit einem einzelnen Peer oder einer Konfigurationsanleitung für Multicast-Gruppen.

Netzwerkdiagramm



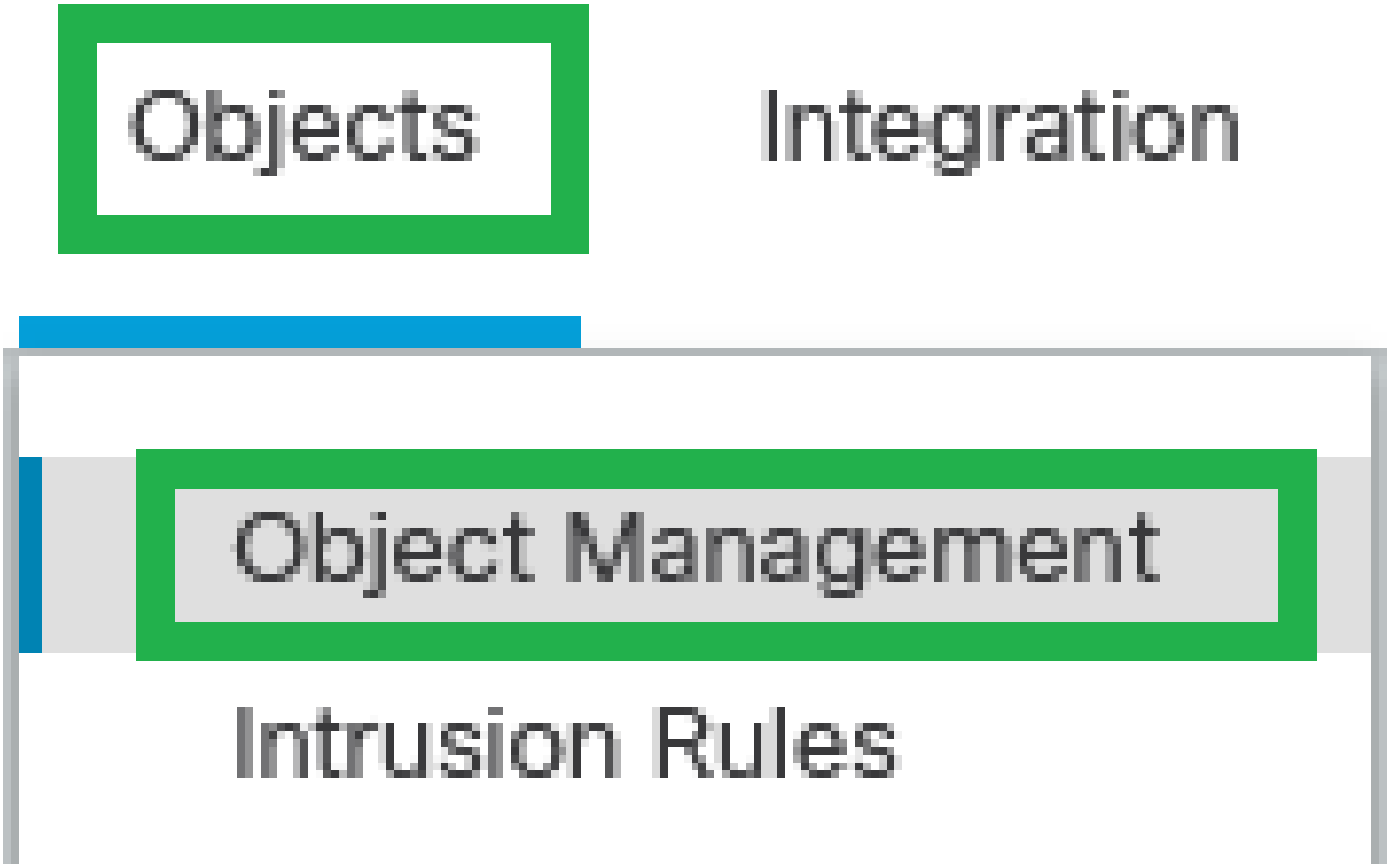
Netzwerktopologie

Im Abschnitt configure wird davon ausgegangen, dass das Underlay-Netzwerk bereits über das Secure Firewall Management Center für die Bedrohungsabwehr konfiguriert ist. Dieses Dokument behandelt hauptsächlich die Overlay-Netzwerkkonfiguration.

Konfigurieren

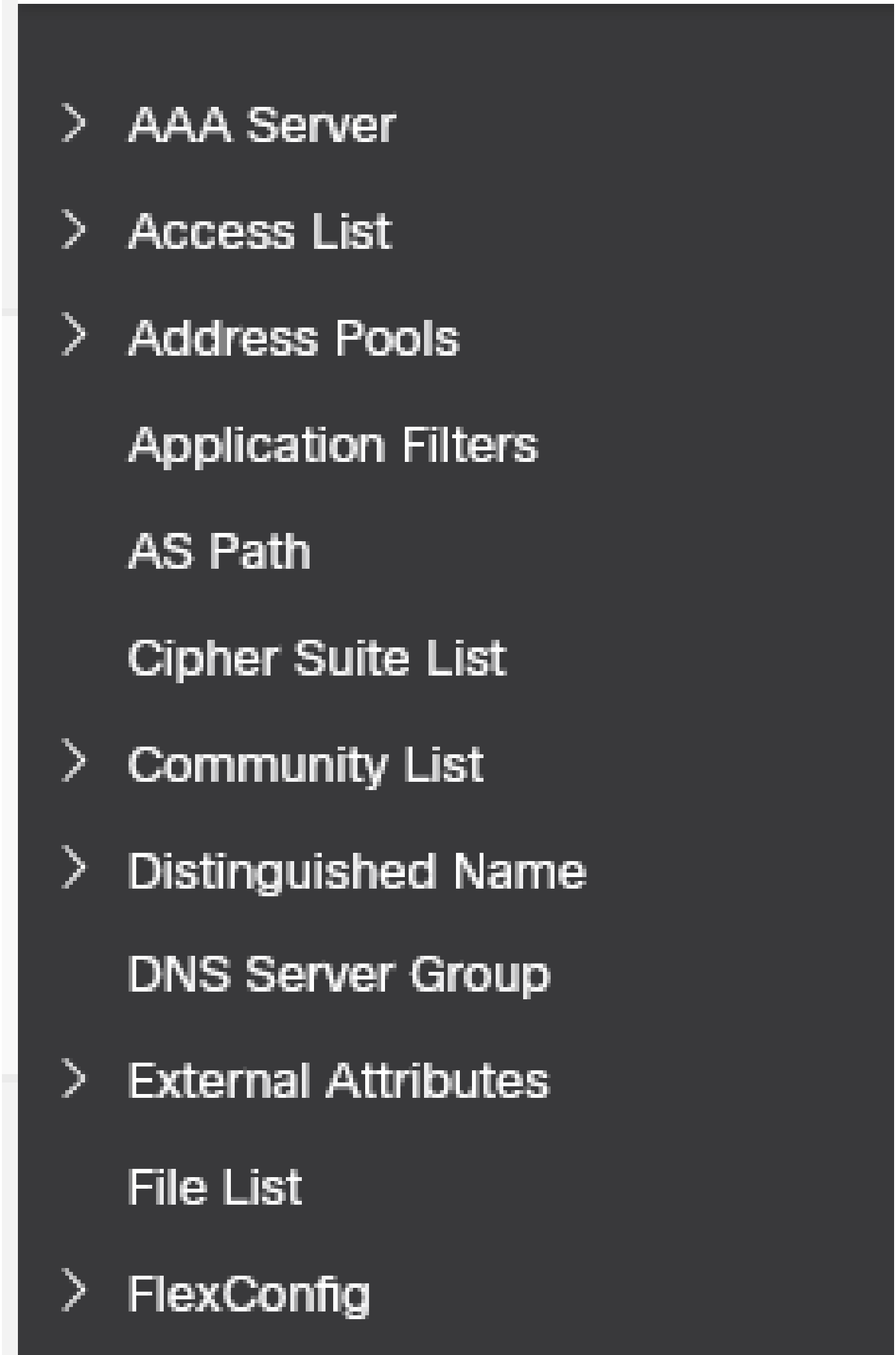
Konfigurieren der VTEP-Peer-Gruppe

Schritt 1: Navigieren Sie zu Objekte > Objektverwaltung.



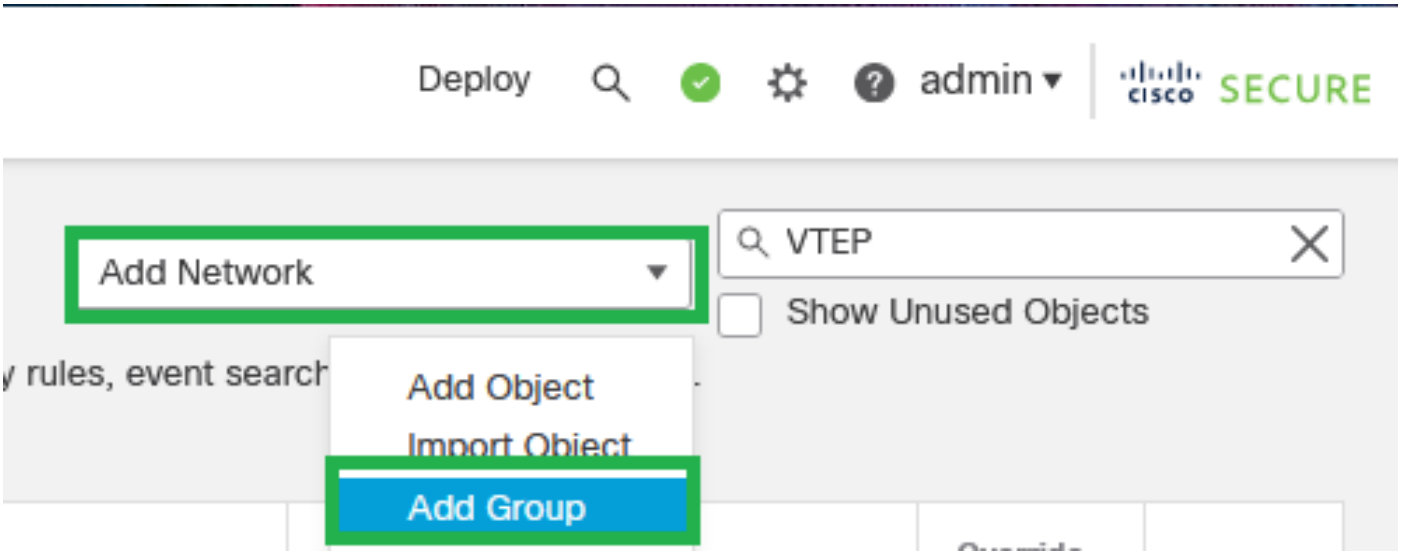
Objekte - Objektmanagement

Schritt 2: Klicken Sie auf Netzwerk im linken Menü.


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

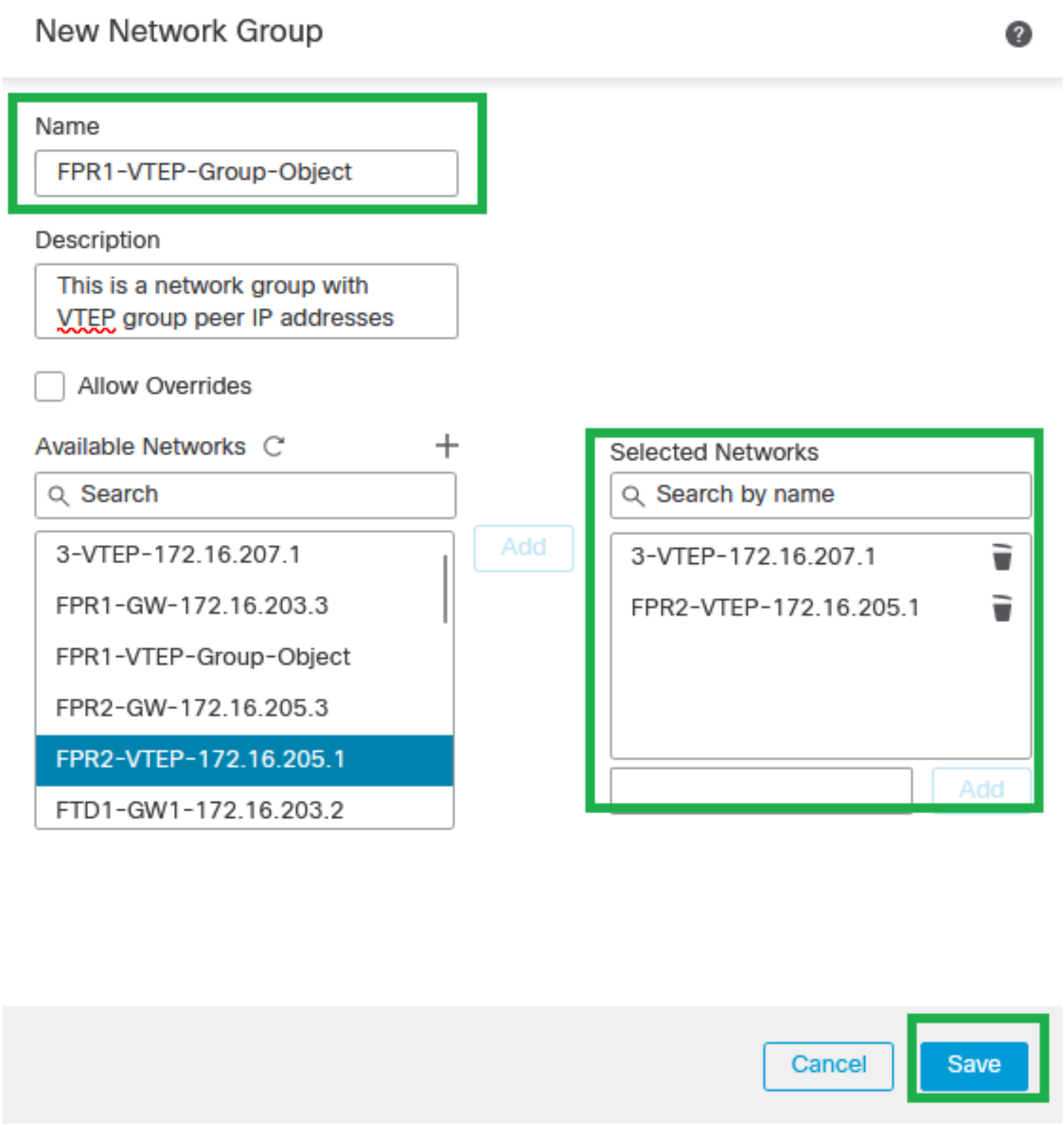
: Konfigurieren Sie mehr Hostnetzwerkobjekte für jede VTEP-Peer-IP-Adresse, die Sie haben. Dieser Konfigurationsleitfaden enthält zwei Objekte.

Schritt 5: Erstellen Sie die Objektgruppe, klicken Sie auf Netzwerk hinzufügen > Gruppe hinzufügen.



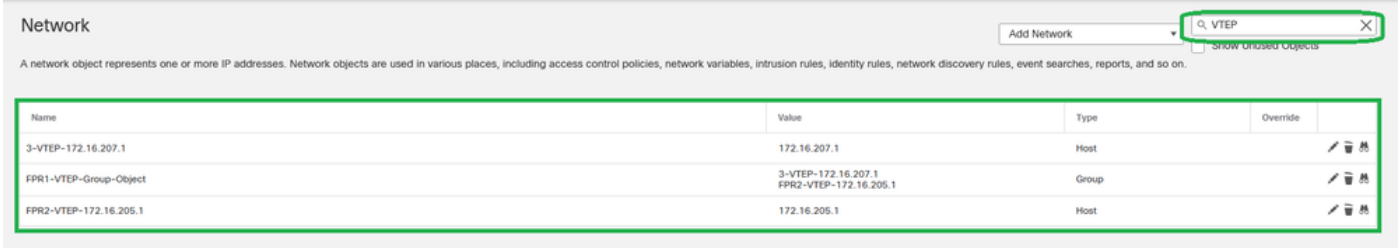
Netzwerk hinzufügen - Gruppe hinzufügen

Schritt 6: Erstellen Sie die Netzwerkobjektgruppe mit allen VTEP-Peer-IP-Adressen. Richten Sie einen Netzwerkgruppennamen ein, und wählen Sie die erforderlichen Netzwerkobjektgruppen aus. Klicken Sie anschließend auf Speichern.



Netzwerkobjektgruppe erstellen

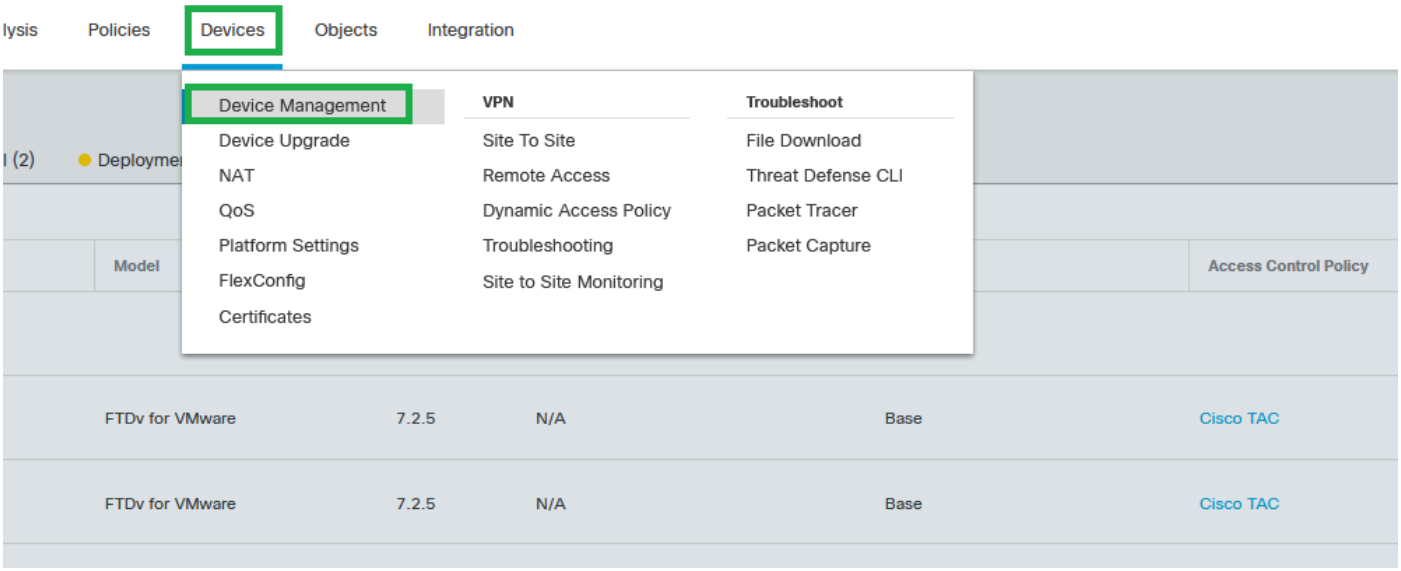
Schritt 7: Validieren Sie das Netzwerkobjekt und die Netzwerkobjektgruppe über den Netzwerkobjektfilter.



Validierung der VTEP-Objektgruppe

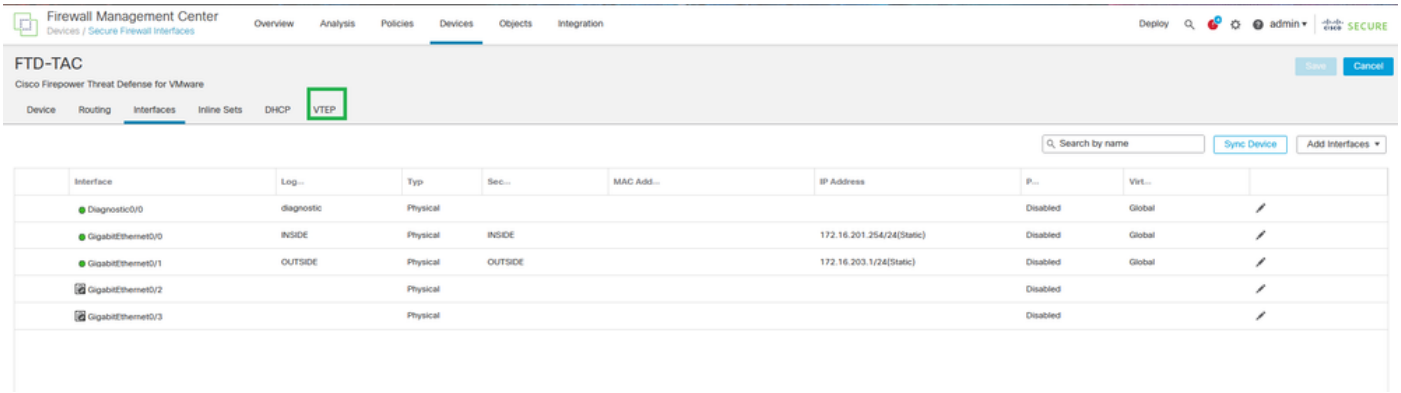
Konfigurieren der VTEP-Quellschnittstelle

Schritt 1: Navigieren Sie zu Geräte > Geräteverwaltung, und bearbeiten Sie die Bedrohungsabwehr.



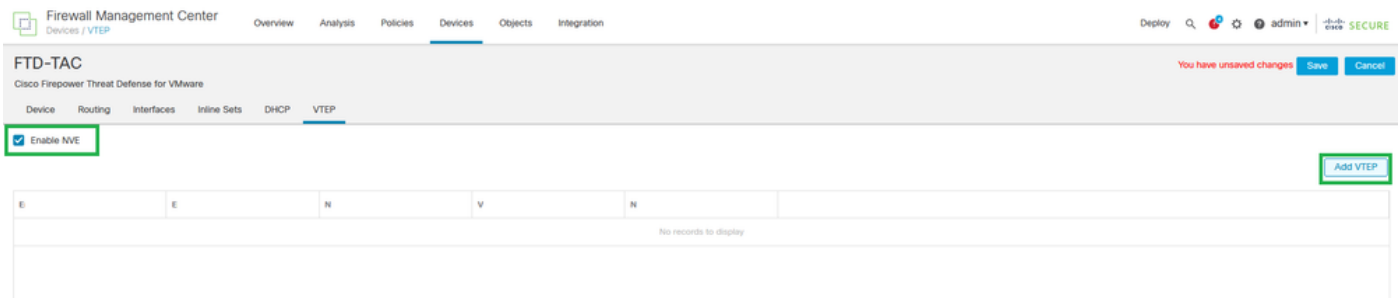
Geräte - Gerätemanagement

Schritt 2: Navigieren Sie zum Abschnitt VTEP.

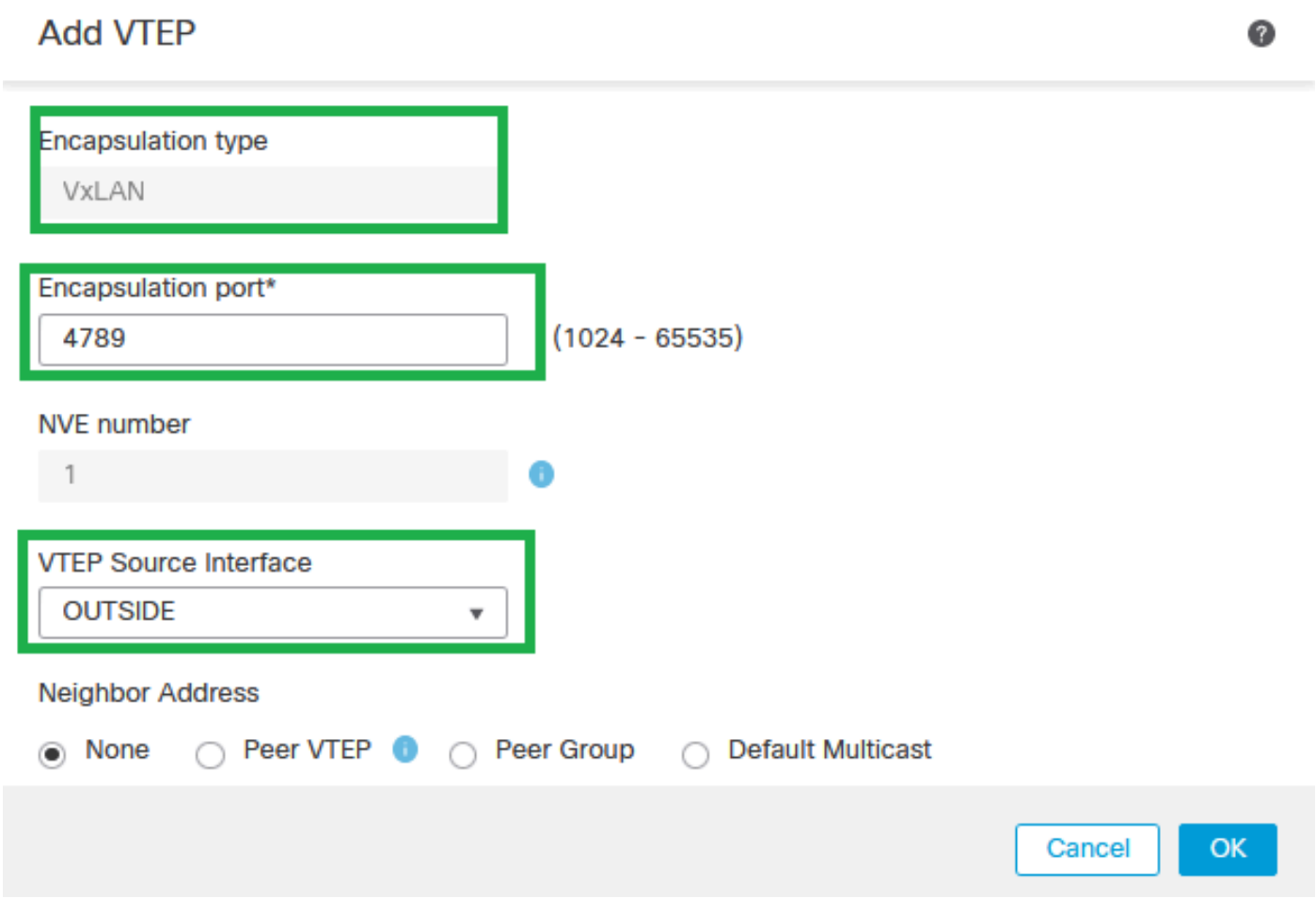


VTEP-Abschnitt

Schritt 3: Aktivieren Sie das Kontrollkästchen "VNE aktivieren", und klicken Sie auf "VTEP hinzufügen".



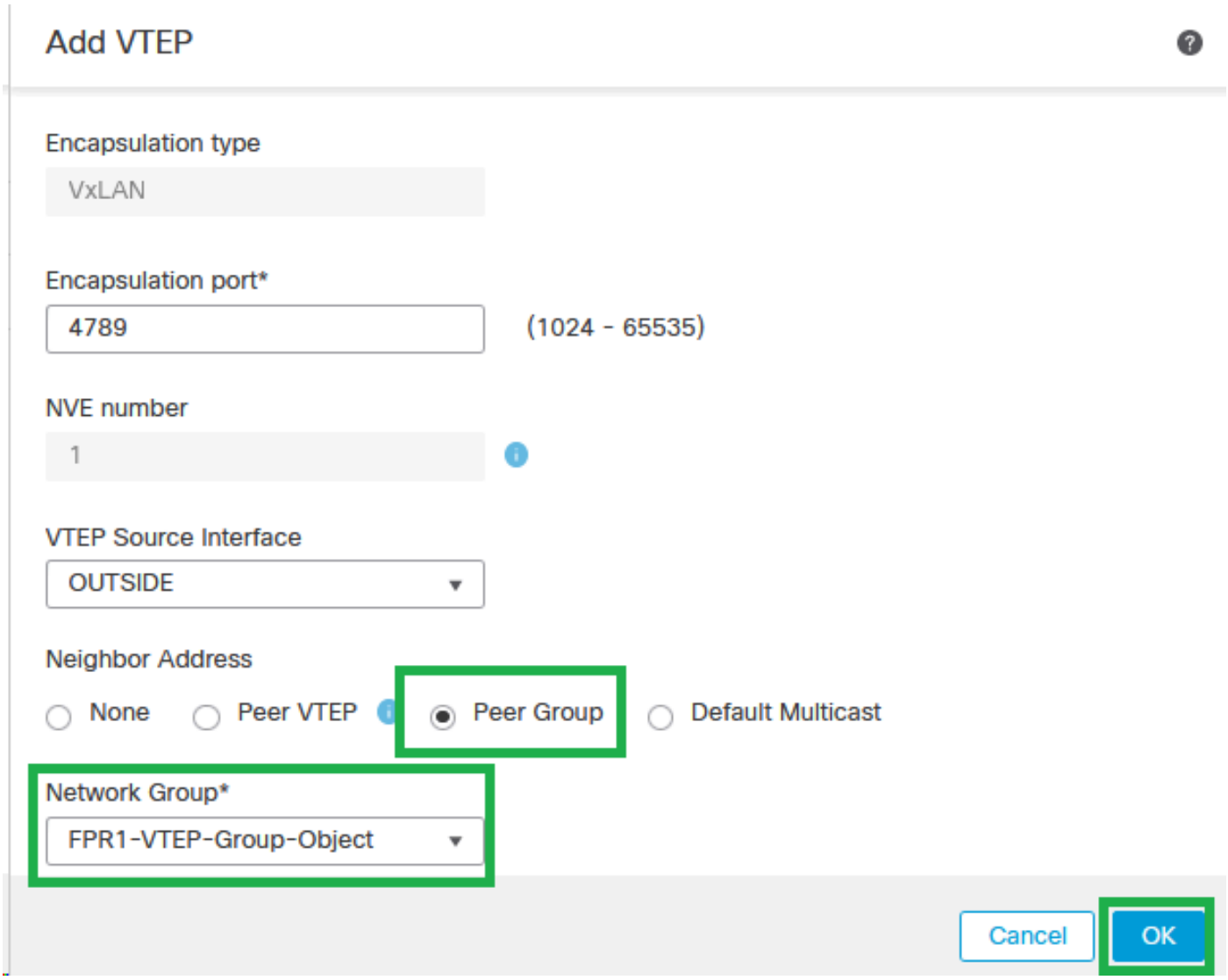
Schritt 4: Wählen Sie VxLAN als Kapselungstyp aus, geben Sie den Wert für den Kapselungsport ein, und wählen Sie die Schnittstelle aus, die für die VTEP-Quelle in diesem Bedrohungsschutz verwendet wird (externe Schnittstelle für diesen Konfigurationsleitfaden).



VTEP hinzufügen

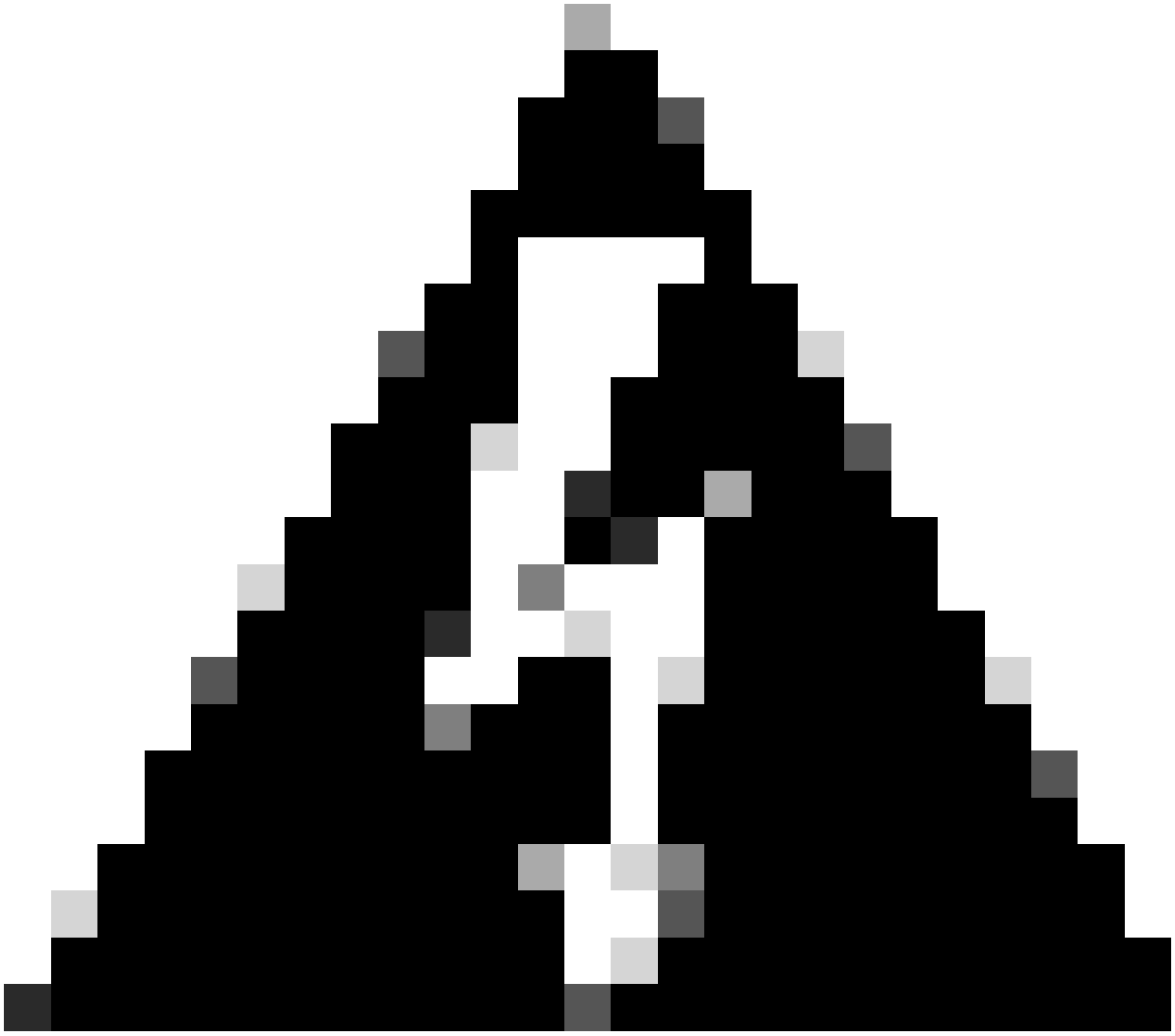
Hinweis: Die VxLAN-Kapselung ist die Standardeinstellung. Für AWS können Sie zwischen VxLAN und Geneve wählen. Der Standardwert ist 4789. Ein beliebiger Kapselungsport kann je nach Design zwischen 1024 und 65535 gewählt werden.

Schritt 5: Wählen Sie Peer Group (Peergruppe) aus, wählen Sie die im vorherigen Konfigurationsabschnitt erstellte Netzwerkobjektgruppe aus, und klicken Sie dann auf OK.



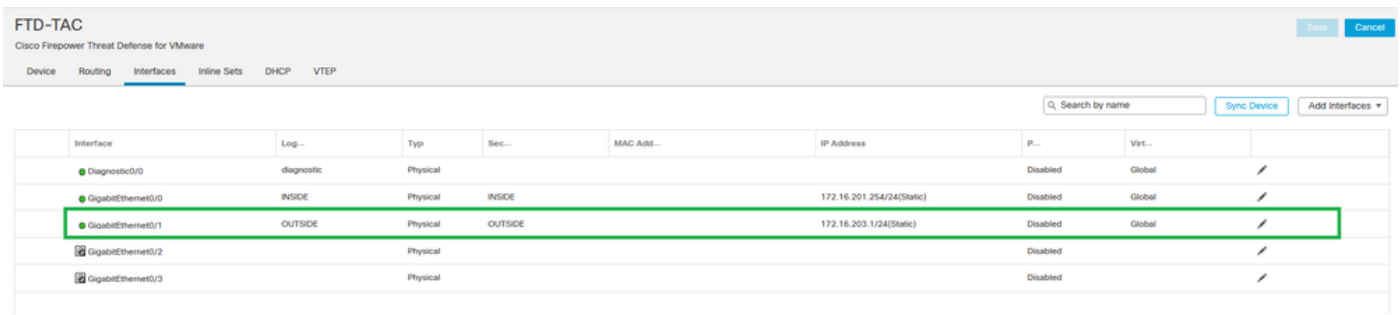
Peer-Gruppe - Netzwerkobjektgruppe

Schritt 6: Speichern der Änderungen

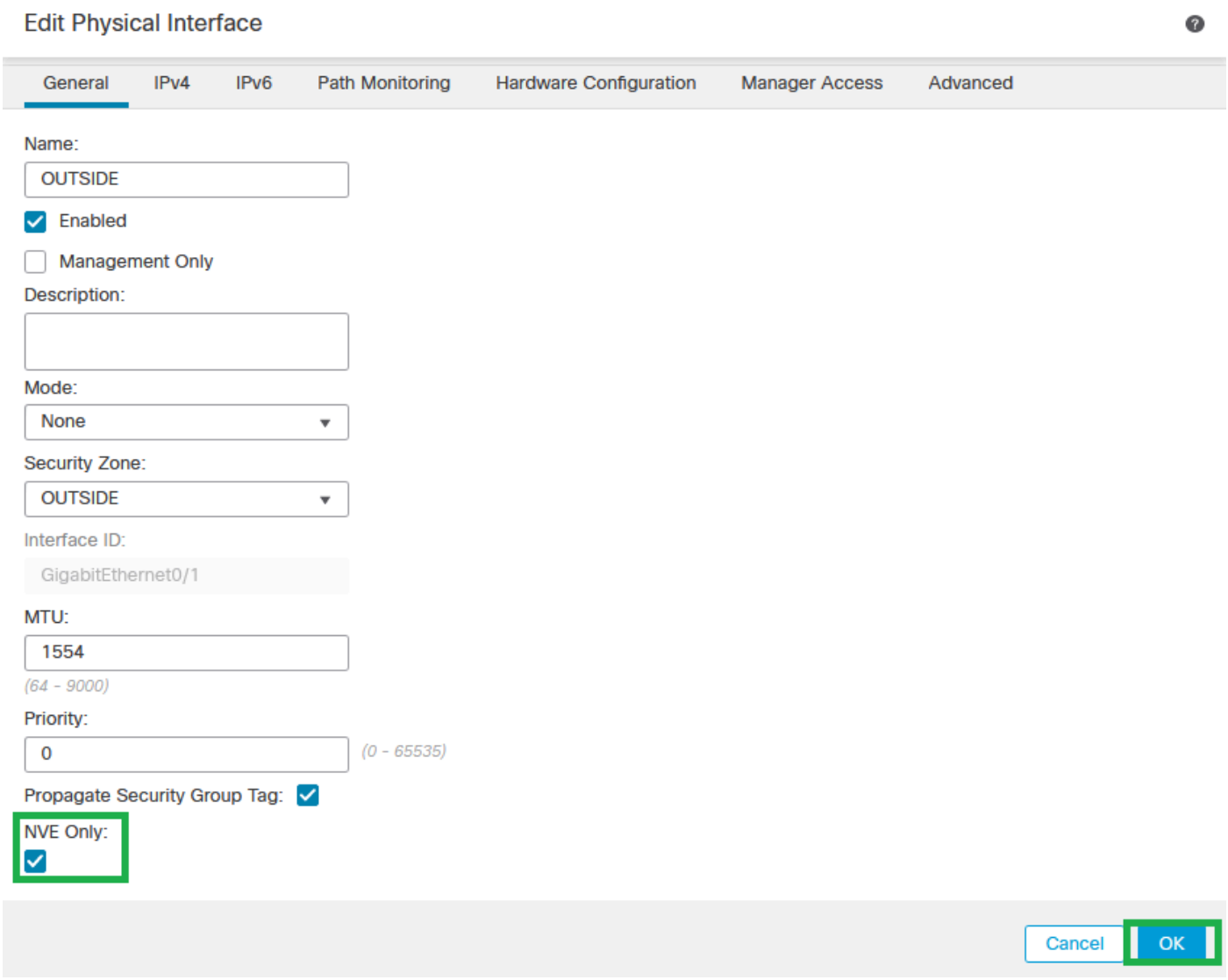


Warnung: Nach dem Speichern der Änderungen wird eine Jumbo Frame-Änderungsmeldung angezeigt. Die MTU wird auf der Schnittstelle geändert, die als VTEP 1554 zugewiesen ist. Achten Sie darauf, dass dieselbe MTU auf dem Underlay-Netzwerk verwendet wird.

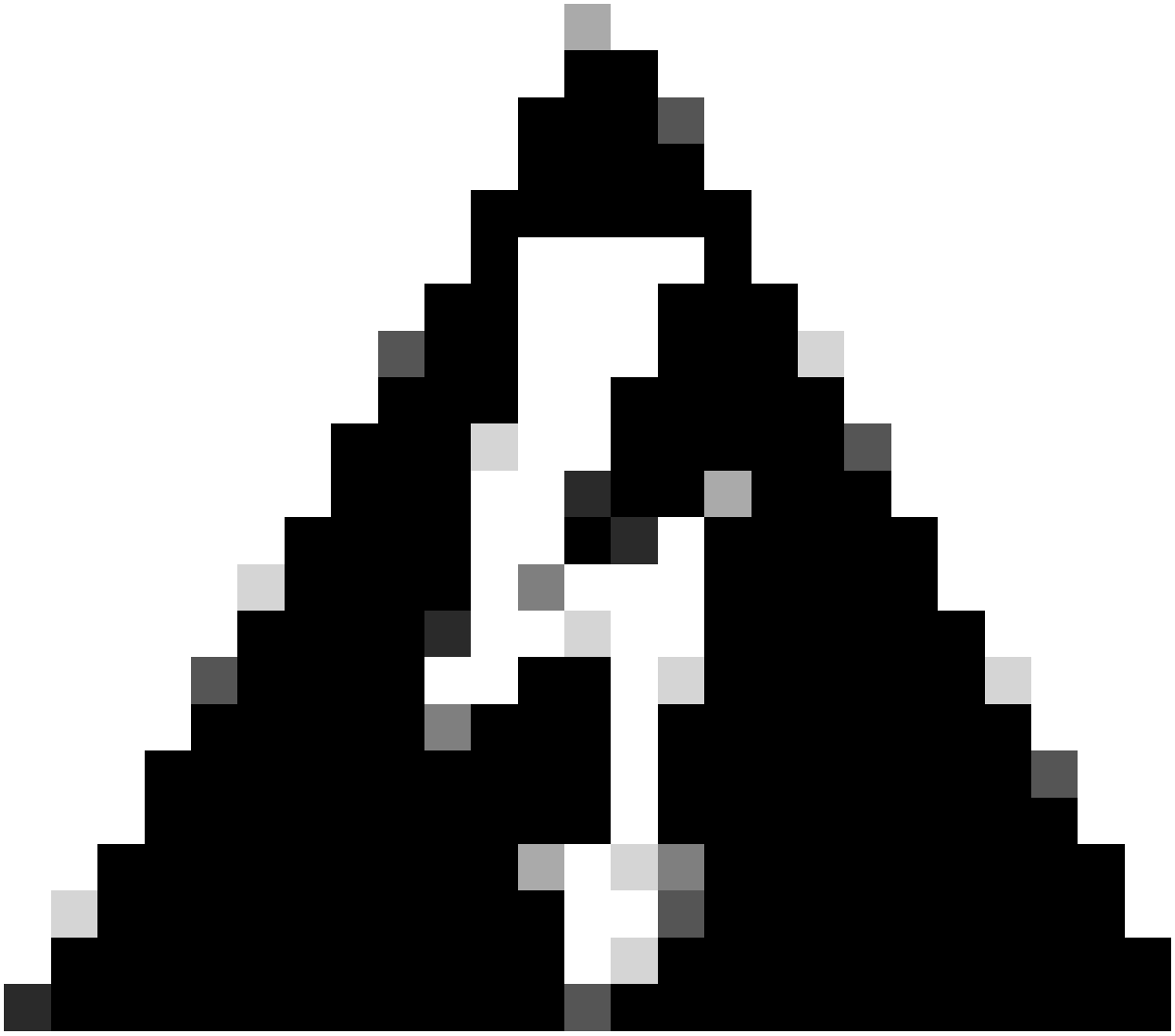
Schritt 7:Klicken Sie auf Interfaces (Schnittstellen), und bearbeiten Sie die für die VTEP-Quellschnittstelle verwendete Schnittstelle. (Externe Schnittstelle in dieser Konfigurationsanleitung)



Schritt 8 (Optional): Aktivieren Sie auf der Seite Allgemein das Kontrollkästchen NVE Only (Nur NVE), und klicken Sie dann auf OK.



NVE Only-Konfiguration

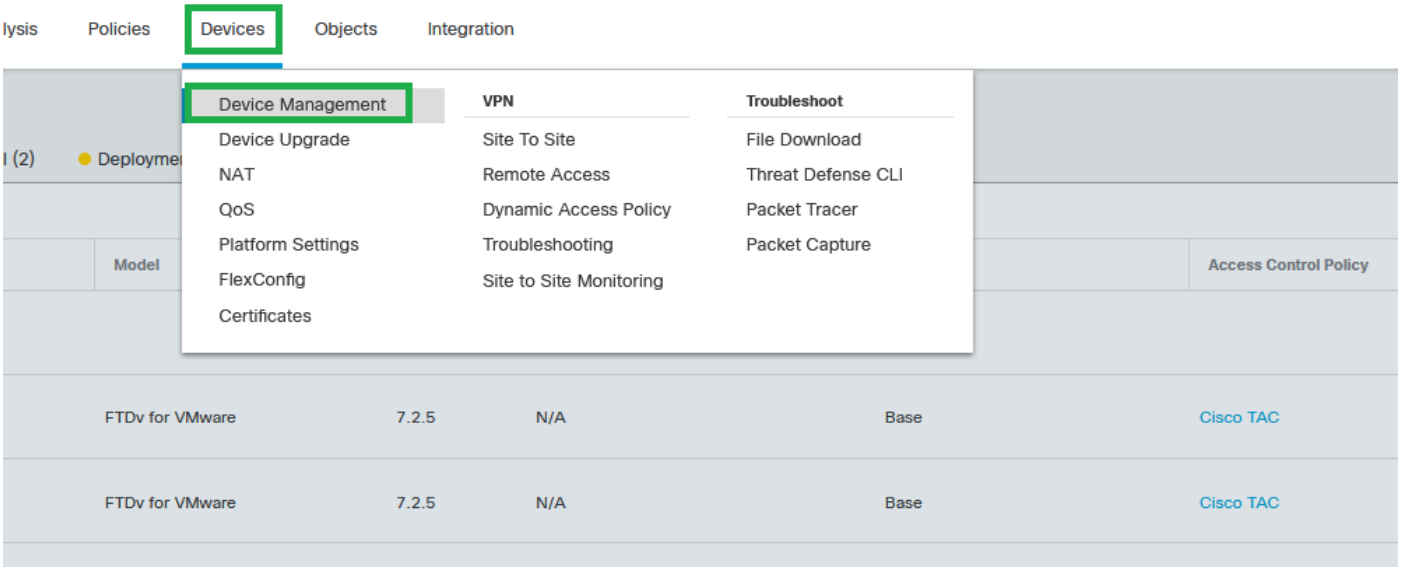


Warnung: Diese Einstellung ist für den Routing-Modus optional, bei dem durch diese Einstellung der Datenverkehr auf VXLAN und der allgemeine Verwaltungsdatenverkehr nur auf dieser Schnittstelle beschränkt wird. Diese Einstellung wird automatisch für den transparenten Firewall-Modus aktiviert.

Schritt 9: Speichern Sie die Änderungen.

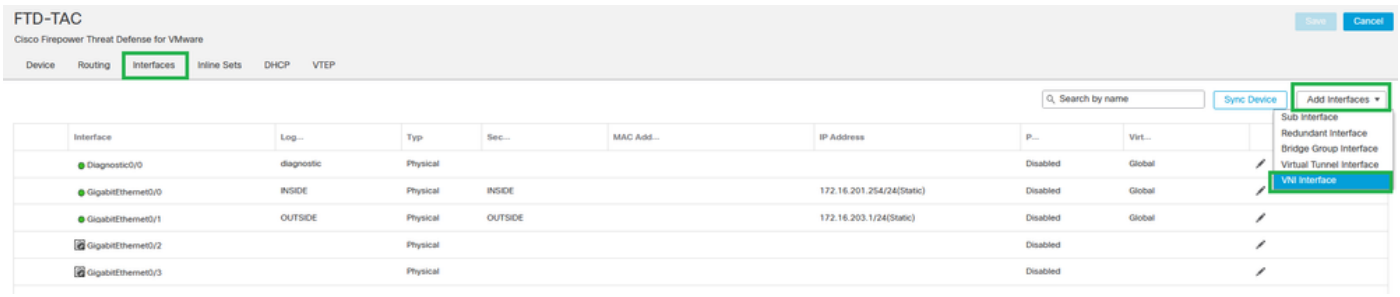
Konfigurieren der VTEP VNI-Schnittstelle

Schritt 1: Navigieren Sie zu Geräte > Gerätemanagement, und bearbeiten Sie die Bedrohungsabwehr.



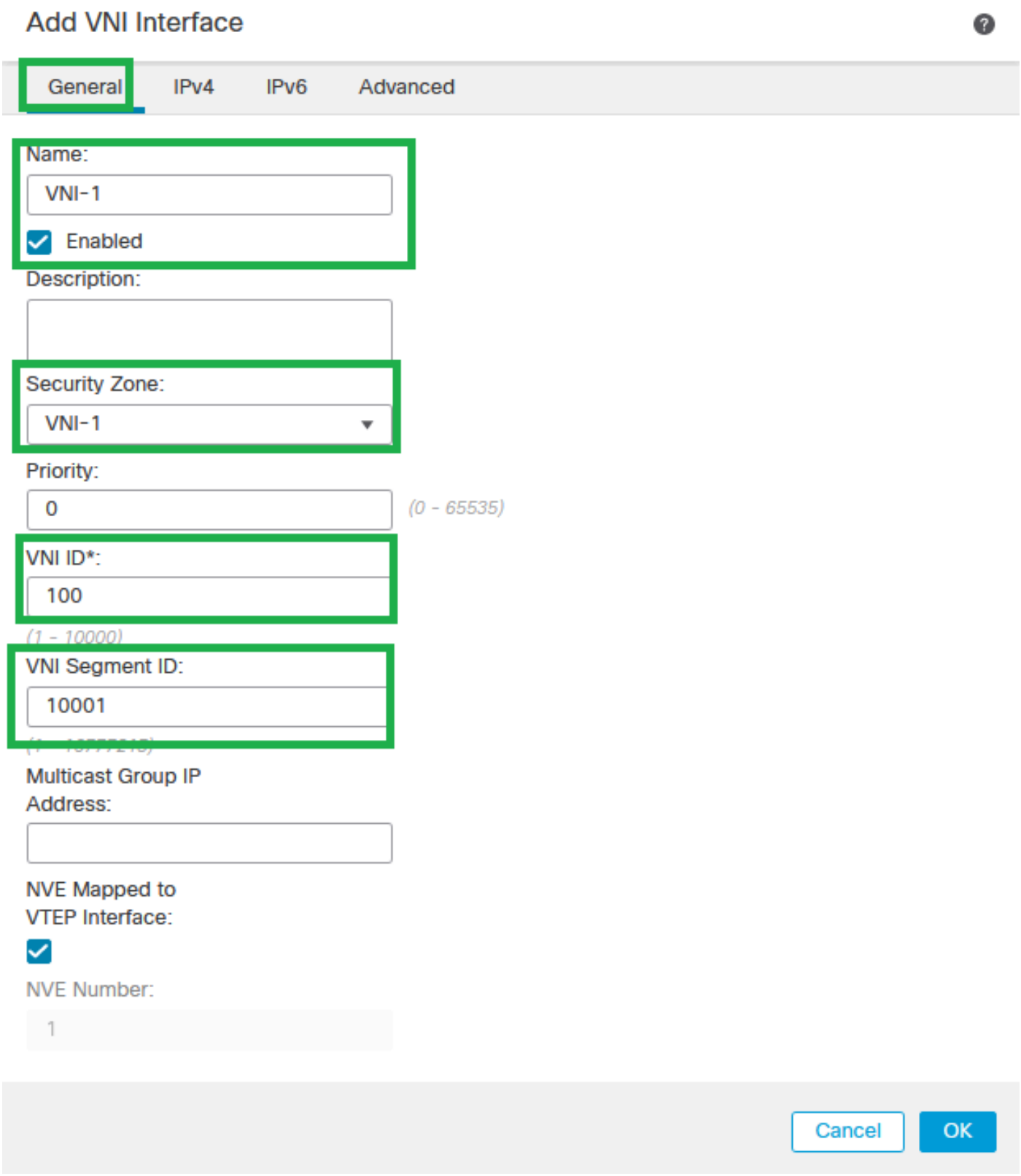
Geräte - Gerätemanagement

Schritt 2: Klicken Sie im Abschnitt "Interfaces" (Schnittstellen) auf Add Interfaces > VNI Interfaces (Schnittstellen hinzufügen > VNI-Schnittstellen).

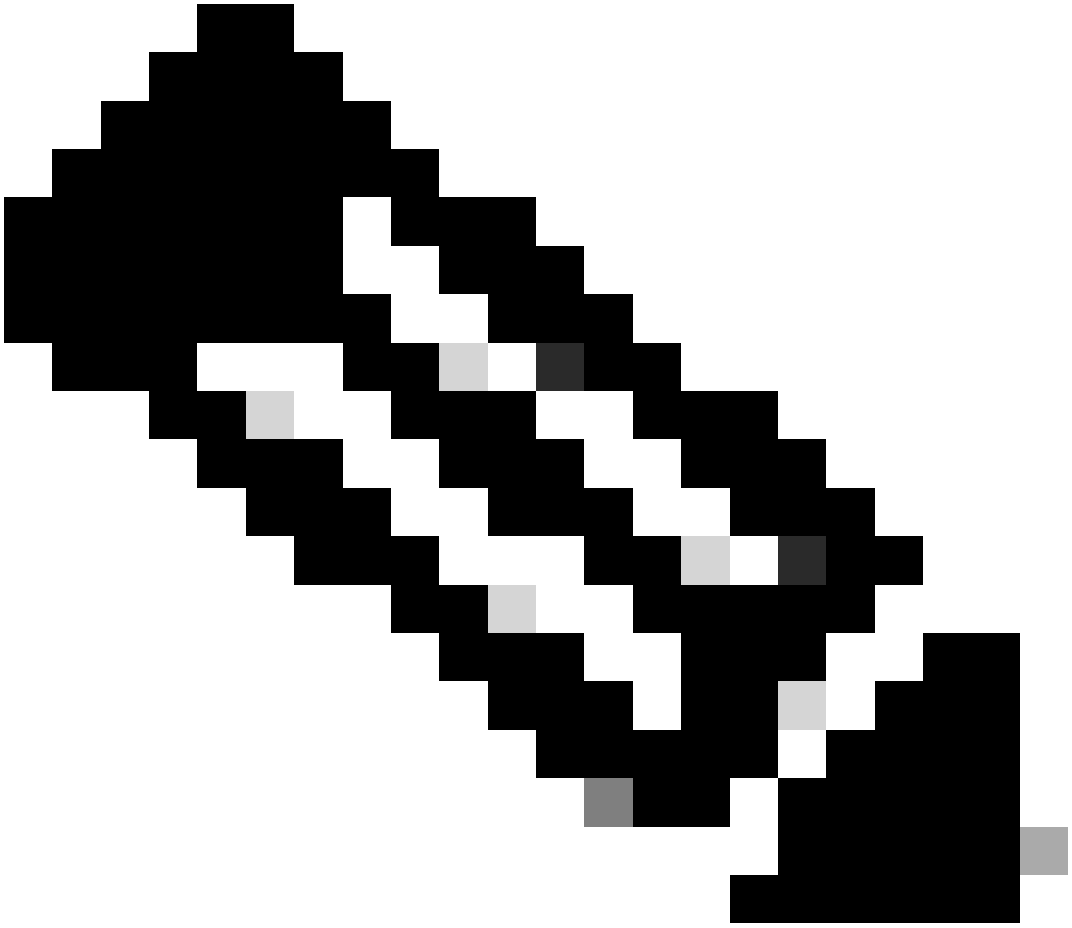


Schnittstellen - Hinzufügen von Schnittstellen - VNI-Schnittstellen

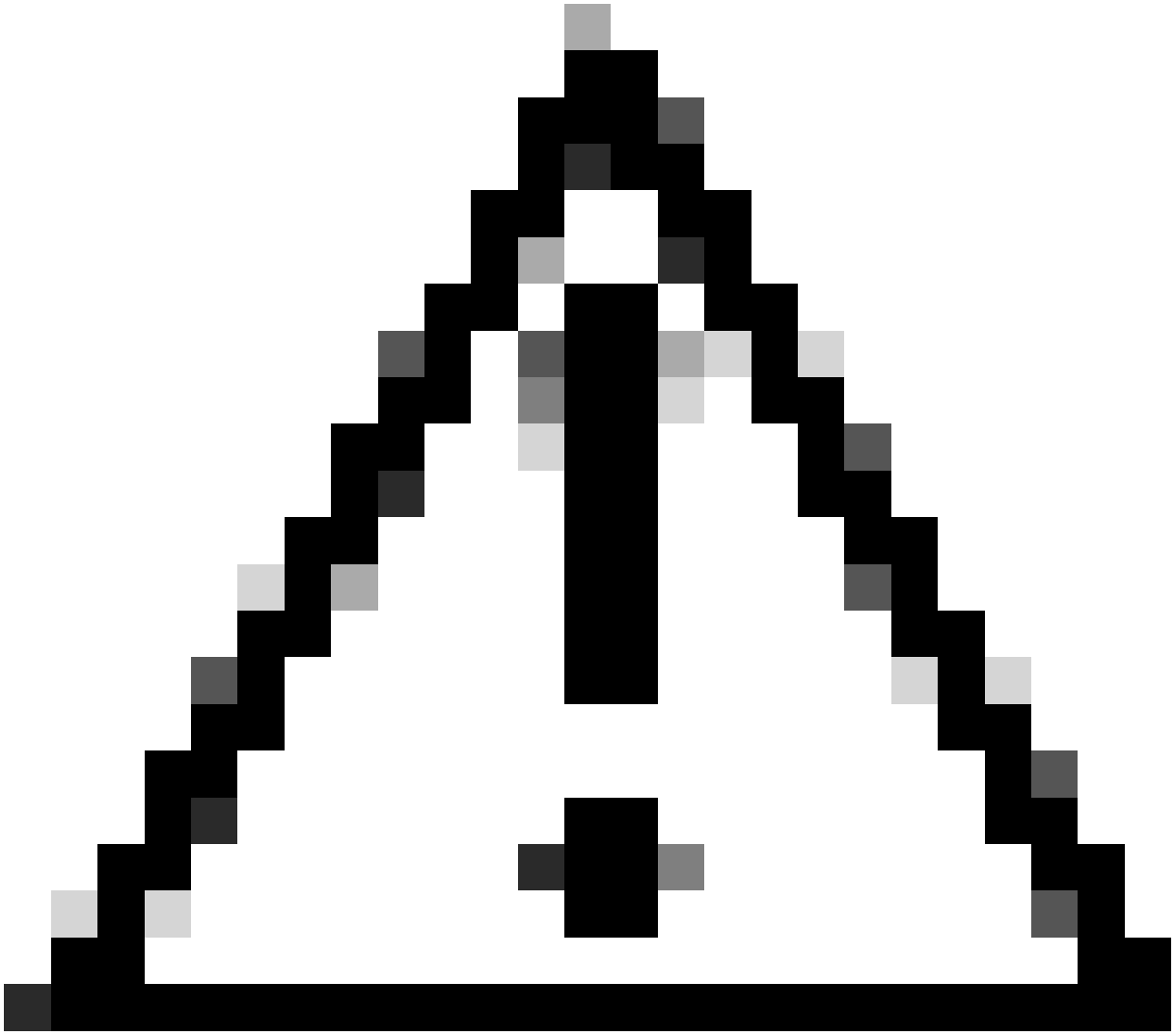
Schritt 3: Richten Sie im Abschnitt "Allgemein" die VNI-Schnittstelle mit Name, Beschreibung, Sicherheitszone, VNI-ID und VNI-Segment-ID ein.



VNI-Schnittstelle hinzufügen

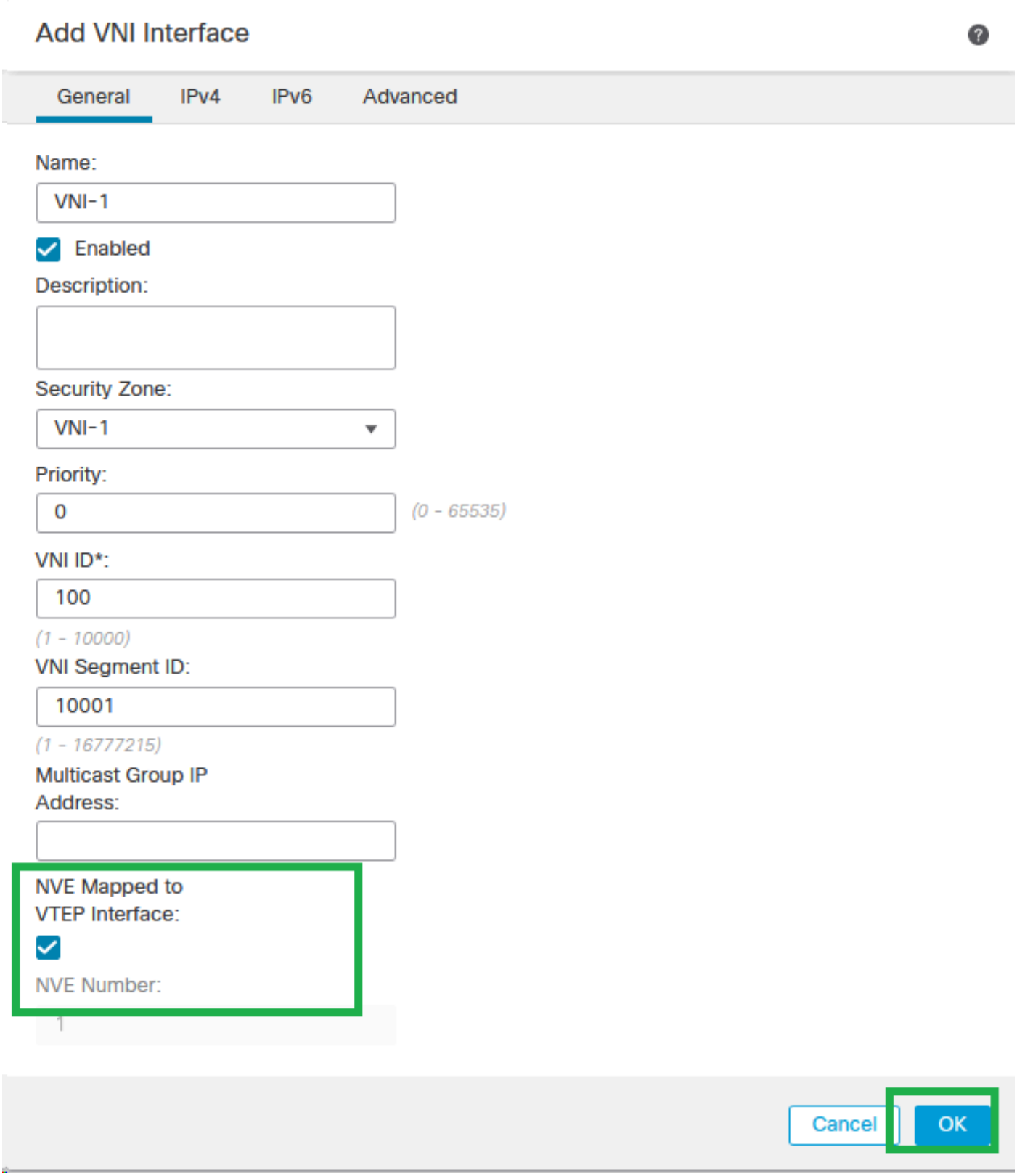


Hinweis: Die VNI-ID ist zwischen 1 und 10000 konfiguriert, die VNI-Segment-ID zwischen 1 und 16777215 (die Segment-ID wird für das VXLAN-Tagging verwendet).



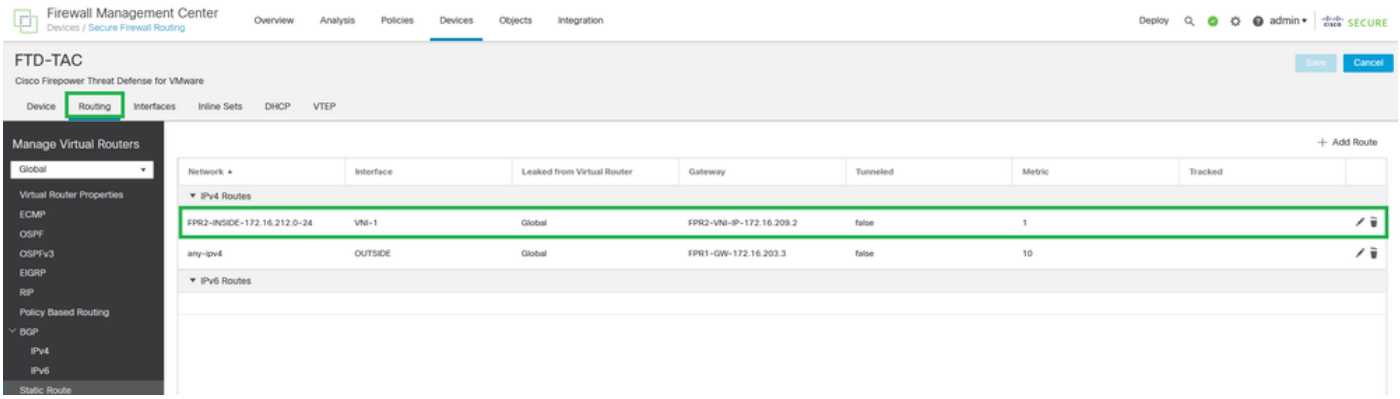
Achtung: Wenn die Multicast-Gruppe nicht für die VNI-Schnittstelle konfiguriert ist, wird die Standardgruppe aus der VTEP-Quellschnittstellenkonfiguration verwendet, sofern diese verfügbar ist. Wenn Sie eine VTEP-Peer-IP für die VTEP-Quellschnittstelle manuell festlegen, können Sie keine Multicast-Gruppe für die VNI-Schnittstelle angeben.

Schritt 3: Aktivieren Sie das Kontrollkästchen NVE Mapped to VTEP Interface (NVE der VTEP-Schnittstelle zugeordnet), und klicken Sie auf OK.

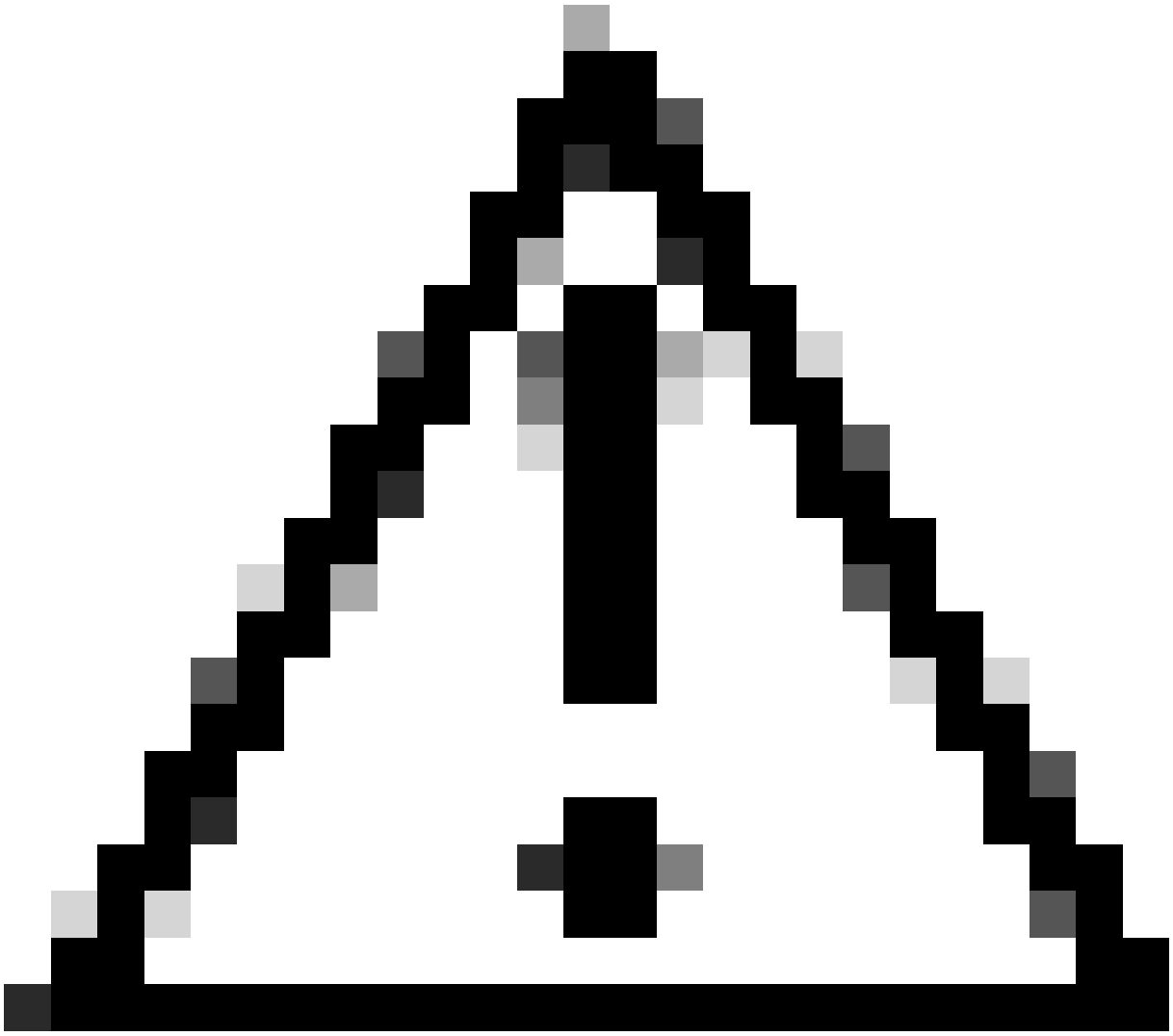


NVE wird VTEP-Schnittstelle zugeordnet

Schritt 4: Konfigurieren Sie eine statische Route, um der VNI-Peer-Schnittstelle die Zielnetzwerke für VXLAN anzukündigen. Navigieren Sie Routing > Statische Route.

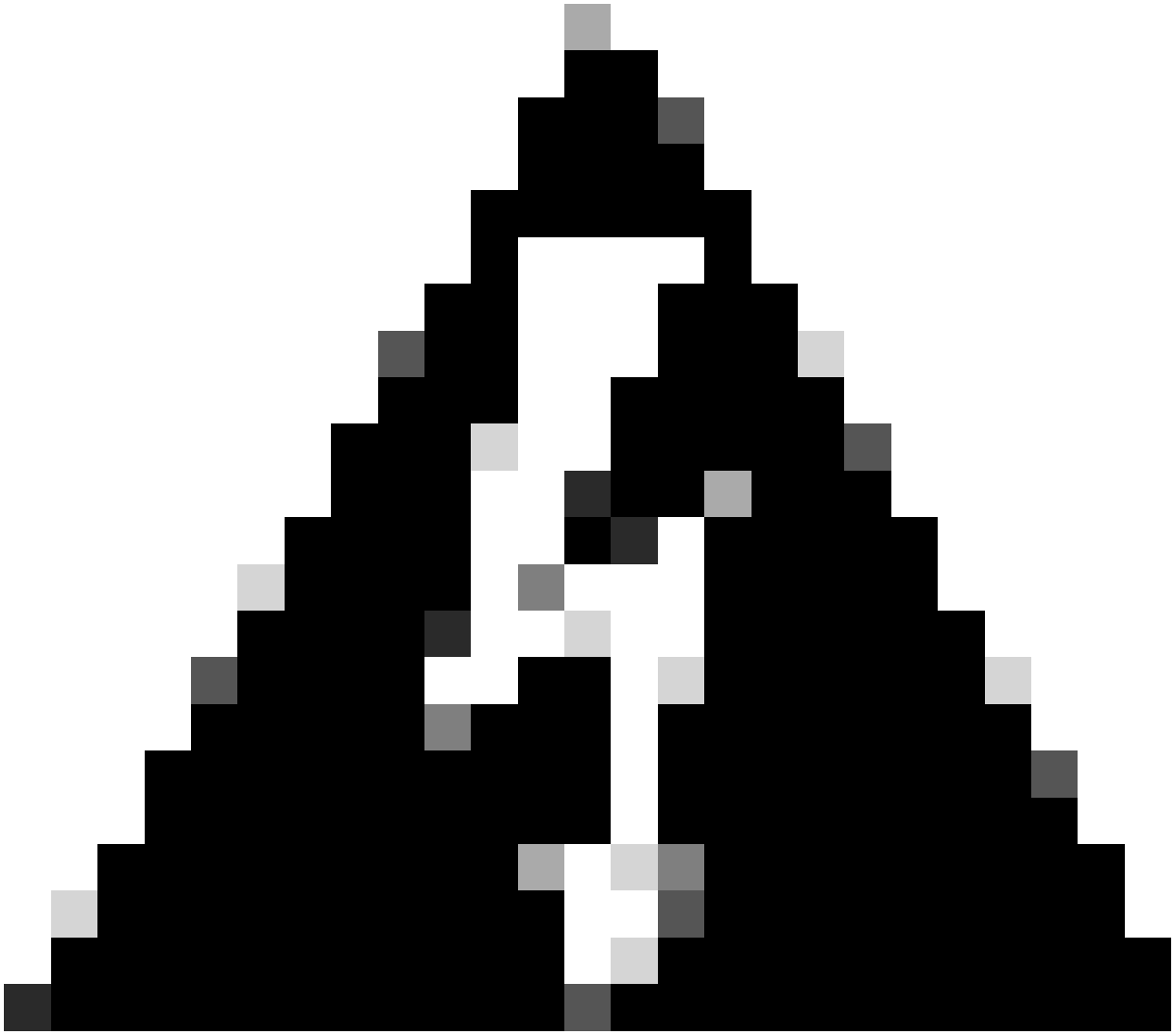


Statische Routenkonfiguration



Achtung: Zielnetzwerke für VXLAN müssen über die Peer-VNI-Schnittstelle gesendet werden. Alle VNI-Schnittstellen müssen sich in derselben Broadcast-Domäne befinden (logisches Segment).

Schritt 5: Speichern und Bereitstellen der Änderungen.



Warnung: Validierungswarnungen sind vor der Bereitstellung zu sehen. Stellen Sie sicher, dass die IP-Adressen der VTEP-Peers über die physische VTEP-Quellschnittstelle erreichbar sind.

Überprüfung

Überprüfen der NVE-Konfiguration

```
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.
```

Überprüfen der VNI-Schnittstellenkonfiguration

```
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
```

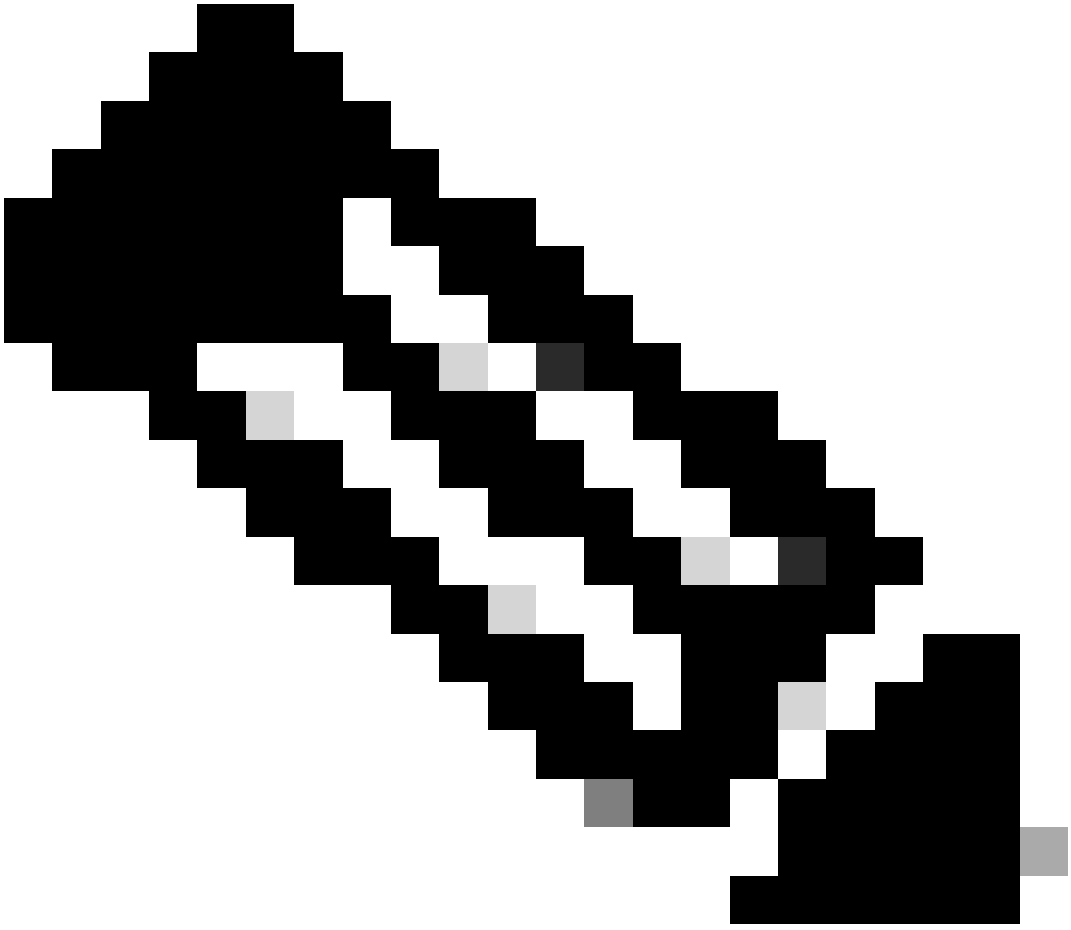
Überprüfen Sie die MTU-Konfiguration auf der VTEP-Schnittstelle.

```
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]
---
```

Überprüfen der Konfiguration der statischen Route für Zielnetzwerke

```
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
```



Hinweis: Überprüfen Sie, ob die VNI-Schnittstellen aller Peers in derselben Broadcast-Domäne konfiguriert sind.

Fehlerbehebung

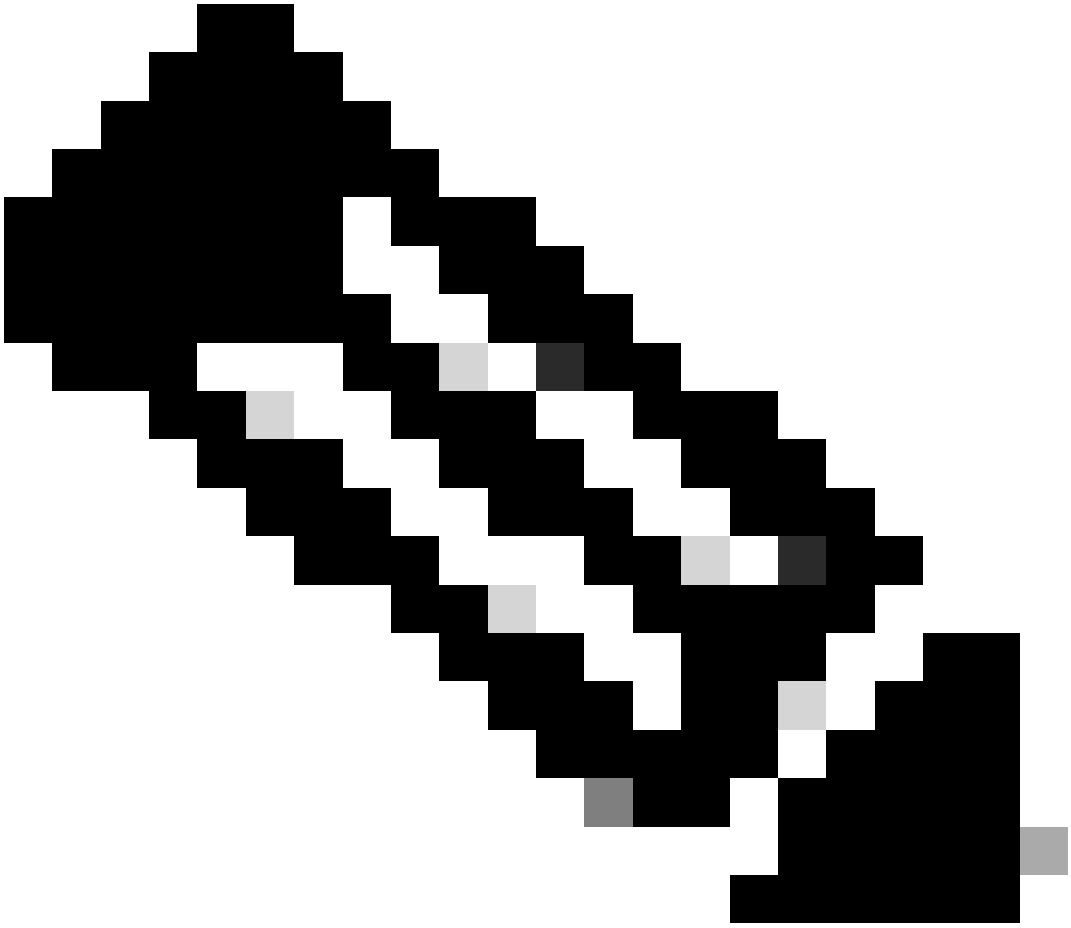
Überprüfen der Verbindung mit VTEP-Peers

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
```



Hinweis: Ein VTEP-Peer-Verbindungsproblem kann zu Bereitstellungsfehlern in Secure FMC führen. Stellen Sie sicher, dass die Verbindung zu allen VTEP-Peer-Konfigurationen erhalten bleibt.

Überprüfen Sie die Verbindungen mit VNI-Peers.

.

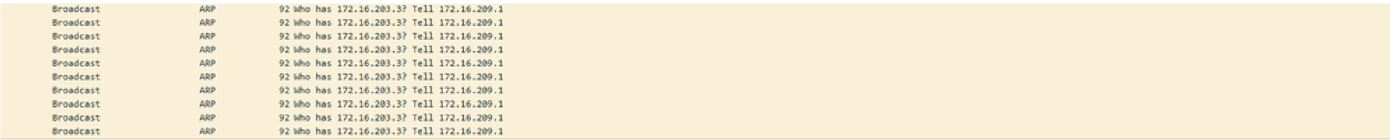
Peer 1:

```
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
```

Manchmal kann eine falsche statische Route unvollständige ARP-Ausgaben erzeugen. Konfigurieren Sie eine Erfassung auf der VTEP-Schnittstelle für VXLAN-Pakete, und laden Sie sie im pcap-Format herunter. Jedes Paketanalysetool hilft dabei, Probleme mit den Routen zu überprüfen. Stellen Sie sicher, dass Sie die VNI-Peer-IP-Adresse als Gateway verwenden.



Broadcast	ARP	92 Who has 172.16.203.3? Tell 172.16.209.1
Broadcast	ARP	92 Who has 172.16.203.3? Tell 172.16.209.1
Broadcast	ARP	92 Who has 172.16.203.3? Tell 172.16.209.1
Broadcast	ARP	92 Who has 172.16.203.3? Tell 172.16.209.1
Broadcast	ARP	92 Who has 172.16.203.3? Tell 172.16.209.1
Broadcast	ARP	92 Who has 172.16.203.3? Tell 172.16.209.1
Broadcast	ARP	92 Who has 172.16.203.3? Tell 172.16.209.1
Broadcast	ARP	92 Who has 172.16.203.3? Tell 172.16.209.1
Broadcast	ARP	92 Who has 172.16.203.3? Tell 172.16.209.1
Broadcast	ARP	92 Who has 172.16.203.3? Tell 172.16.209.1

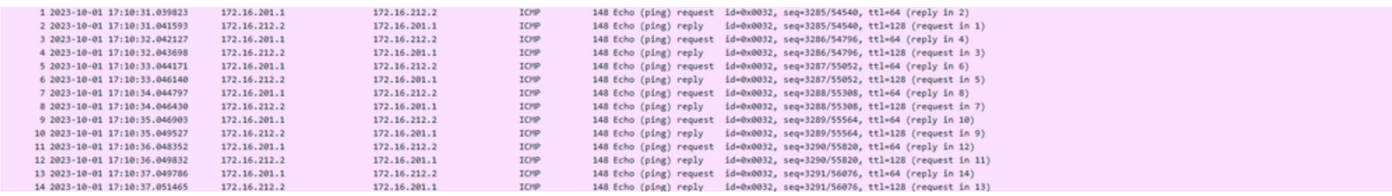
Routing-Problem

Konfigurieren Sie ASP-Drop-Captures in Secure FTD für den Fall eines Firewall-Drops. Überprüfen Sie den ASP-Drop-Zähler mit dem Befehl show asp drop. Wenden Sie sich zur Analyse an Cisco TAC.

Konfigurieren Sie Richtlinien für die Zugriffskontrolle so, dass der VXLAN-UDP-Datenverkehr an der VNI/VTEP-Schnittstelle zugelassen wird.

Manchmal können die VXLAN-Pakete fragmentiert werden. Stellen Sie sicher, dass die MTU im Underlay-Netzwerk in Jumbo Frames geändert wird, um eine Fragmentierung zu vermeiden.

Konfigurieren Sie die Erfassung auf der Eingangs-/VTEP-Schnittstelle, und laden Sie die Aufzeichnungen im .pcap-Format zur Analyse herunter. Die Pakete müssen den VXLAN-Header auf der VTEP-Schnittstelle enthalten.



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)

Mit VXLAN-Header erfasster Ping

VXLAN-Header

Zugehörige Informationen

- Konfigurieren von VXLAN-Schnittstellen
- VXLAN-Anwendungsfälle
- VXLAN-Paketverarbeitung
- Konfigurieren der VTEP-Quellschnittstelle
- Konfigurieren der VNI-Schnittstelle
- Technischer Support und Downloads von Cisco

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.