

使用安全FMC在安全FTD上配置VXLAN接口

目录

[简介](#)

[先决条件](#)

[要求](#)

[使用的组件](#)

[背景信息](#)

[网络图](#)

[配置](#)

[配置VTEP对等组](#)

[配置VTEP源接口](#)

[配置VTEP VNI接口](#)

[验证](#)

[故障排除](#)

[相关信息](#)

简介

本文档介绍如何使用安全防火墙管理中心(FMC)在安全防火墙威胁防御(FTD)上配置VXLAN接口

先决条件

要求

思科建议您了解以下主题：

- 基本VLAN/VXLAN概念。
- 基本的网络知识。
- 基本的Cisco Secure Management Center体验。
- 基本思科安全防火墙威胁防御体验。

使用的组件

本文档中的信息基于以下软件和硬件版本：

- 运行7.2.4版本的思科安全防火墙管理中心虚拟(FMCv) VMware。
- 运行7.2.4版本的思科安全防火墙威胁防御虚拟设备(FTDv) VMware。

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

背景信息

虚拟可扩展VLAN (VXLAN)像传统VLAN一样提供以太网第2层网络服务。由于虚拟环境中对VLAN网段的高需求，VXLAN提供了更大的可扩展性和灵活性，还定义了MAC-in-UDP封装方案，其中原始第2层帧添加了VXLAN报头，然后放入UDP-IP数据包中。使用此MAC-in-UDP封装，VXLAN通过隧道通过第3层网络连接第2层网络。VXLAN提供以下优势：

- 多租户网段中的VLAN灵活性：
- 更高的可扩展性，可满足更多第2层(L2)网段的要求。
- 提高网络利用率。

思科安全防火墙威胁防御(FTD)支持两种类型的VXLAN封装。

- VXLAN (用于所有安全防火墙威胁防御型号)
- 通用 (用于安全防火墙威胁防御虚拟设备)

在Amazon Web Services (AWS) Gateway Load Balancer和设备之间透明地路由数据包和发送额外信息需要通用封装。

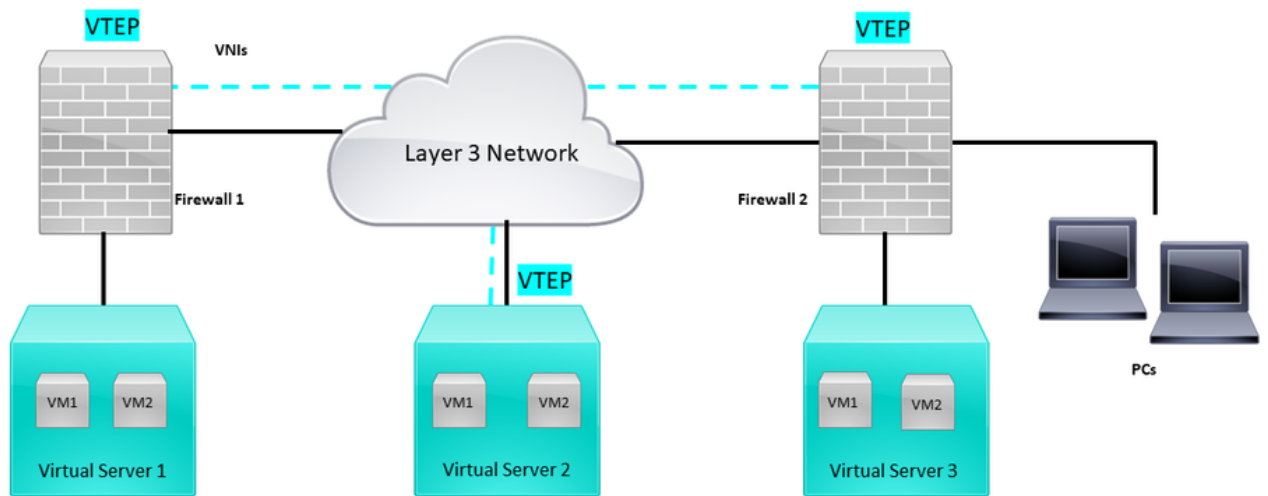
VXLAN使用VXLAN隧道终端(VTEP)将租户的终端设备映射到VXLAN网段，并执行VXLAN封装和解封。每个VTEP有两个接口类型：一个或多个称为VXLAN网络标识符(VNI)的虚拟接口，可以在其中应用安全策略；和一个称为VTEP源接口的常规接口，VNI接口在VTEP之间通过隧道传输。VTEP源接口连接到VTEP到VTEP通信的传输IP网络，VNI接口类似于VLAN接口：它们是虚拟接口，通过使用标记使网络流量在给定物理接口上分离。安全策略应用于每个VNI接口。可以添加一个VTEP接口，并且所有VNI接口与同一个VTEP接口相关联。AWS上的威胁防御虚拟集群有一个例外。

威胁防御封装和解封的方式有三种：

- 可以在威胁防御上静态配置单个对等体VTEP IP地址。
- 可在威胁防御上静态配置一组对等VTEP IP地址。
- 可以在每个VNI接口上配置组播组。

本文档重点介绍一组静态配置的2个对等VTEP IP地址用于VXLAN封装的VXLAN接口。如果需要配置通用接口，请查看AWS中[通用接口](#)的官方文档或使用单个对等体或组播组配置VTEP，然后使用[单个对等体或组播组](#)配置指南检查VTEP接口。

网络图



网络拓扑

“配置”部分假设底层网络已通过安全防火墙管理中心进行威胁防御配置。本文档重点介绍重叠网络配置。

配置

配置VTEP对等组

第1步：导航到对象>对象管理。



Objects

Integration



Object Management

Intrusion Rules

对象-对象管理

第2步：点击左侧菜单中的网络。

- > 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

Edit Physical Interface



General

IPv4

IPv6

Path Monitoring

Hardware Configuration

Manager Access

Advanced

Name:

OUTSIDE

Enabled

Management Only

Description:

Mode:

None

Security Zone:

OUTSIDE

Interface ID:

GigabitEthernet0/1

MTU:

1554

(64 - 9000)

Priority:

0

(0 - 65535)

Propagate Security Group Tag:

NVE Only:



Cancel

OK

仅NVE配置

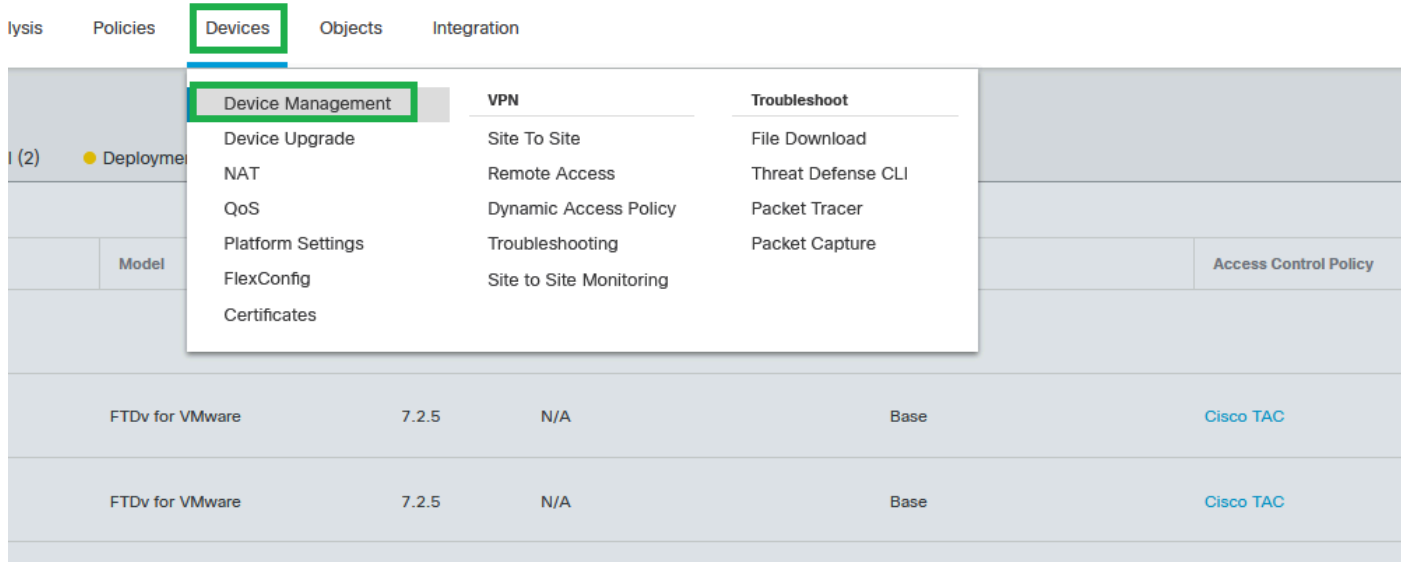


警告：对于此设置限制到VXLAN的流量和仅在此接口上限制通用管理流量的路由模式，此设置是可选的。此设置会自动在透明防火墙模式下启用。

第9步：保存更改。

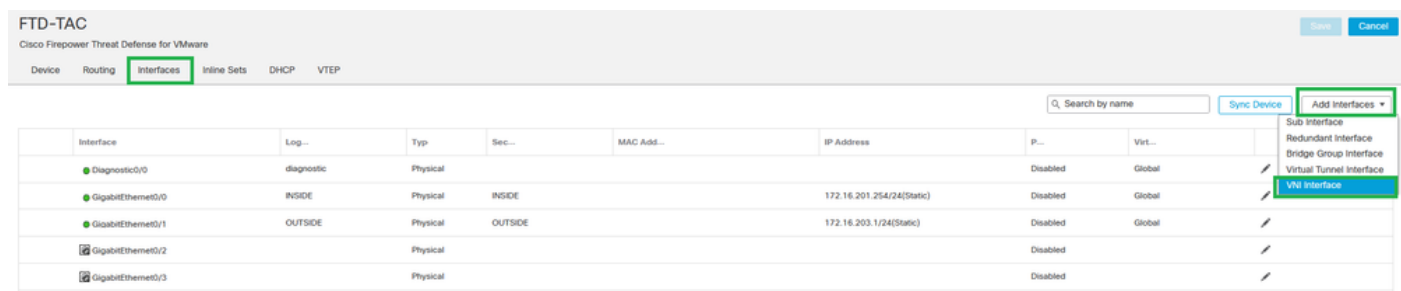
配置VTEP VNI接口

第1步：导航到设备>设备管理，然后编辑威胁防御。



设备-设备管理

第2步：在接口部分下，单击添加接口> VNI接口。



接口-添加接口- VNI接口

第3步：在常规部分下，使用名称、说明、安全区域、VNI ID和VNI网段ID设置VNI接口。

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:

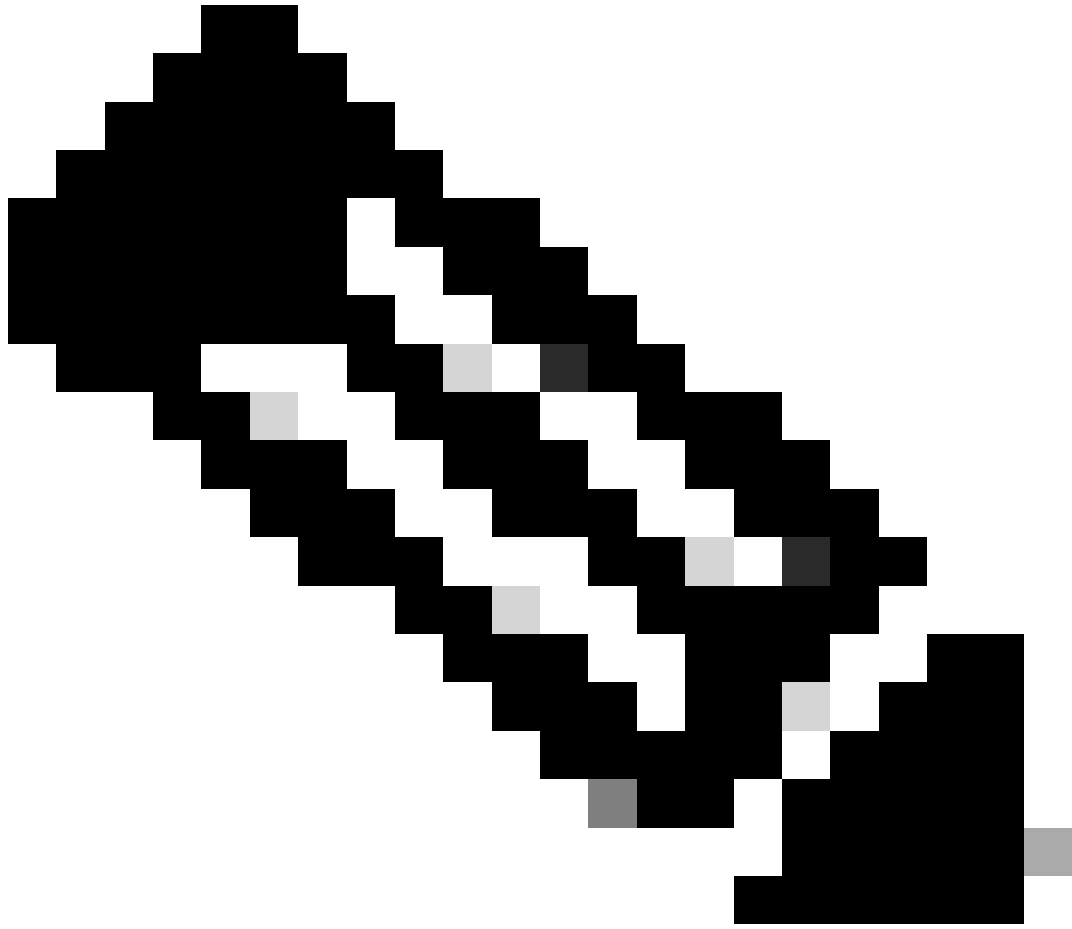
NVE Number:

1

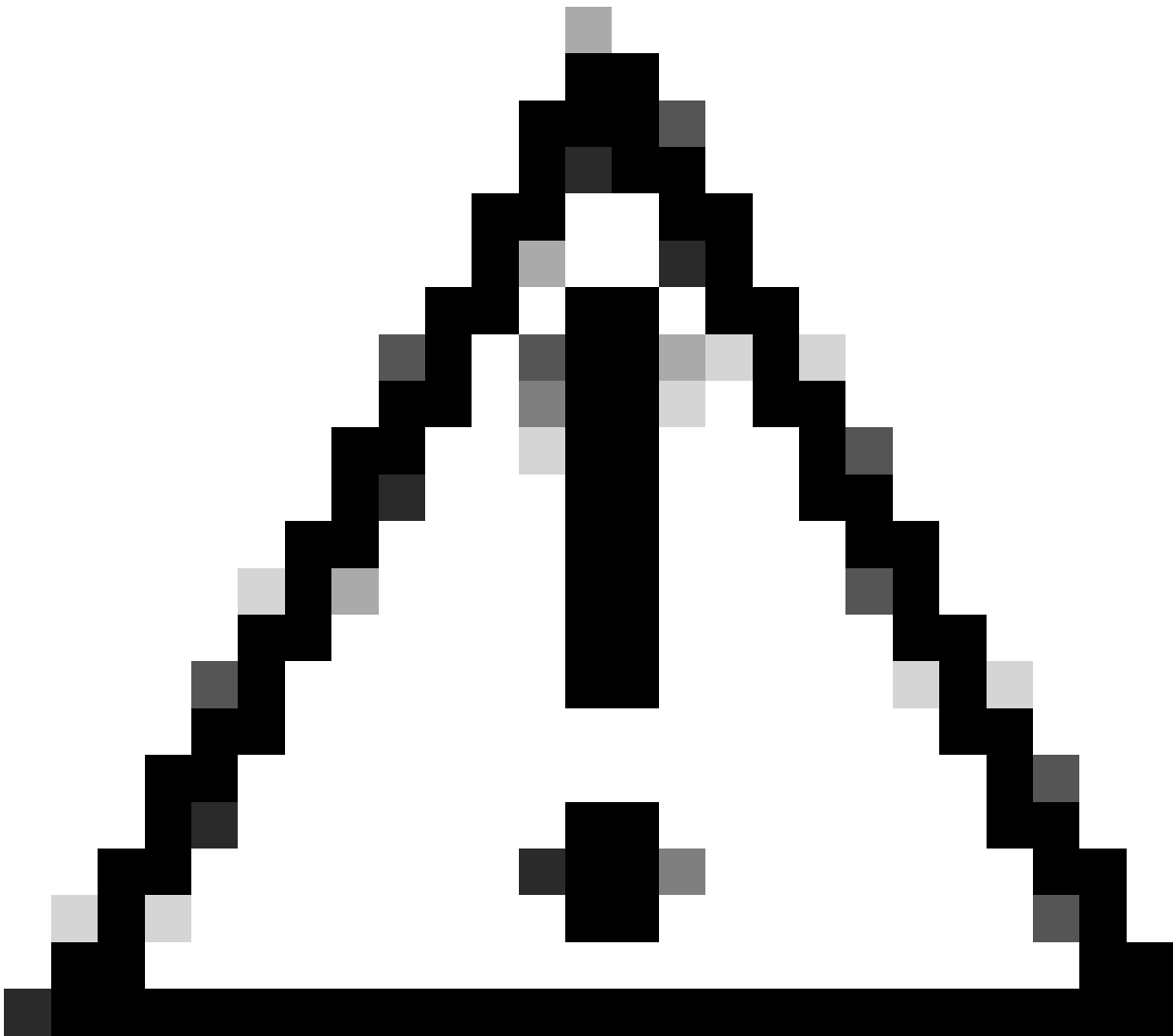
Cancel

OK

添加VNI接口



注意：VNI ID配置在1和10000之间，VNI网段ID配置在1和16777215之间（网段ID用于VXLAN标记）。



注意：如果未在VNI接口上配置组播组，则使用VTEP源接口配置中的默认组（如果可用）。如果手动设置VTEP源接口的VTEP对等体IP，则无法为VNI接口指定组播组。

第3步：选中NVE Mapped to VTEP Interface复选框并单击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映射到VTEP接口

第4步：配置静态路由以将VXLAN的目标网络通告给VNI对等接口。导航到Routing > Static 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

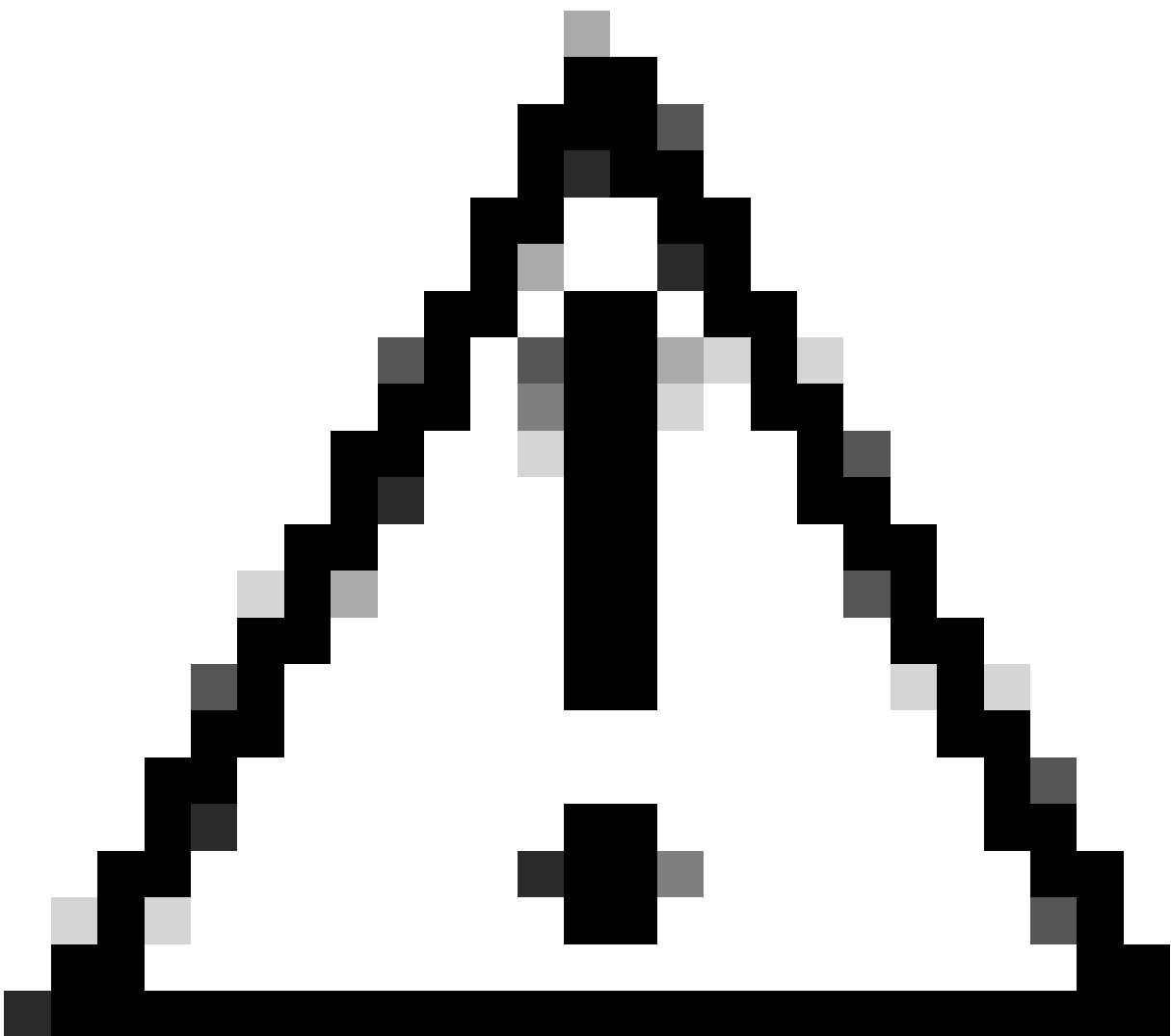
Global

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						

静态路由配置



注意：VXLAN的目标网络必须通过对等体VNI接口发送。所有VNI接口必须位于同一广播域（逻辑网段）中。

第5步：保存并部署更改。



警告：在部署之前可以看到验证警告，请确保可以从物理VTEP源接口访问VTEP对等体IP地址。

验证

检验NVE配置。

```
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.
```

检验VNI接口配置。

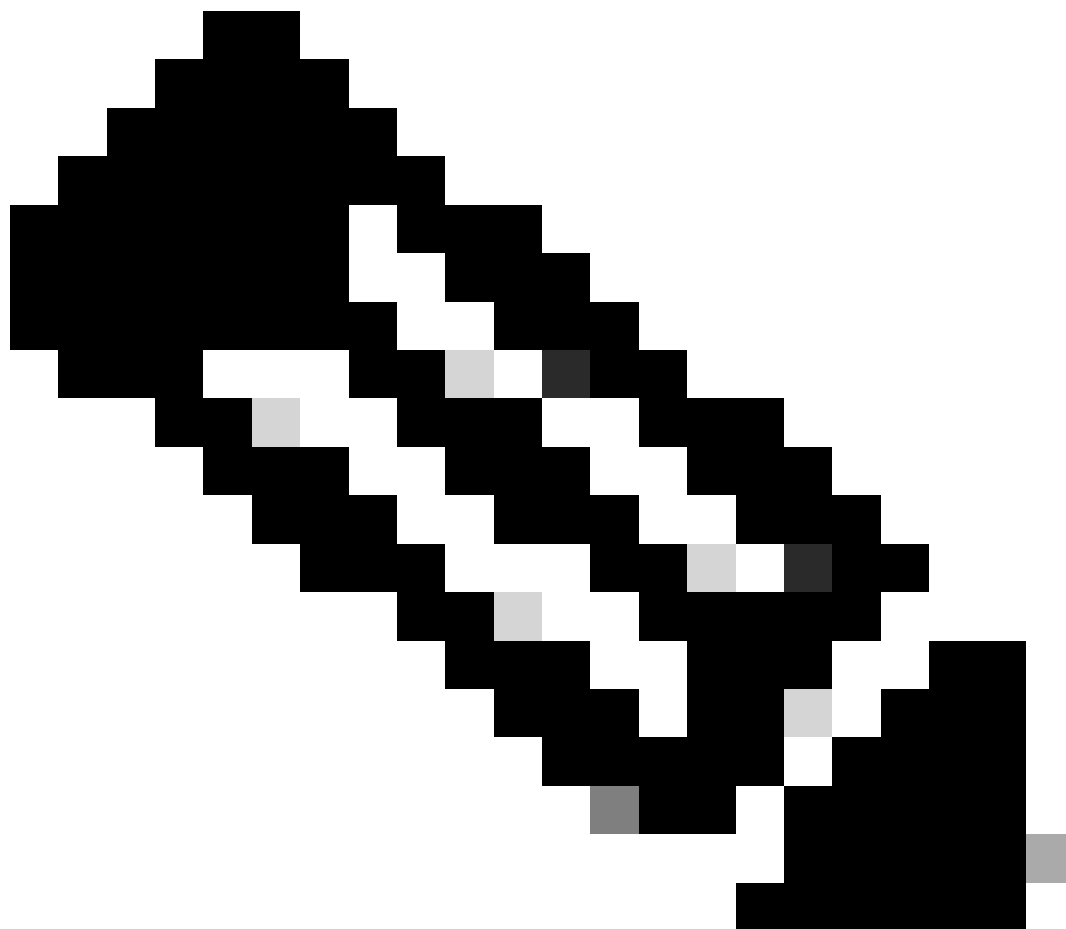
```
firepower# show run interface
interface vni100
segment-id 10001
nameif VNI-1
security-level 0
ip address 172.16.209.1 255.255.255.0
vtep-nve 1
```

检验VTEP接口上的MTU配置。

```
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]
```

验证目的网络的静态路由配置。

```
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
```



注意：验证所有对等体上的VNI接口是否配置在同一个广播域中。

故障排除

检查与VTEP对等体的连接。

对等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
```

对等体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
```



注意：VTEP对等连接问题可能会在安全FMC上生成部署故障。确保与所有VTEP对等配置保持连接。

检查与VNI对等体的连接。

对等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
```

对等体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
```

有时，错误的静态路由可能会生成ARP不完整的输出。在VTEP接口上为VXLAN数据包配置捕获并下载pcap格式，任何数据包分析器工具都可以帮助确认路由是否存在任何问题。确保使用VNI对等IP地址作为网关。

```
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
```

路由问题

在任何防火墙丢弃的情况下，在安全FTD上配置ASP丢弃捕获，使用show asp drop命令检查ASP丢弃计数器。联系思科TAC进行分析。

确保将访问控制策略规则配置为允许VNI/VTEP接口上的VXLAN UDP流量。

有时VXLAN数据包可以分段，请确保在底层网络上将MTU更改为巨型帧以避免分段。

在Ingress/VTEP接口上配置捕获，并下载.pcap格式的捕获以供分析。数据包必须包含VTEP接口上的VXLAN报头，

```
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)
```

使用VXLAN报头捕获的Ping

```
> Frame 8: 148 bytes on wire (1184 bits), 148 bytes captured (1184 bits)
> Ethernet II, Src: Whare_b3:ba:6a (00:50:56:b3:ba:6a), Dst: Whare_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
v Virtual extensible Local Area Network
  > Flags: 0x0000, VXLAN Network ID (VNI)
  > Group Policy ID: 0
  > VXLAN Network Identifier (VNI): 10001
  > Reserved: 0
v Ethernet II, Src: Whare_b3:ba:6a (00:50:56:b3:ba:6a), Dst: Whare_b3:26:b8 (00:50:56:b3:26:b8)
  > Destination: Whare_b3:26:b8 (00:50:56:b3:26:b8)
  > Source: Whare_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
```

VXLAN报头

相关信息

- [配置VXLAN接口](#)
- [VXLAN使用案例](#)

- [VXLAN数据包处理](#)
- [配置VTEP源接口](#)
- [配置VNI接口](#)
- [思科技术支持和下载](#)

关于此翻译

思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。