在 Secure FTD 上使用 Secure FMC 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)配置安全防火墙威胁防御(FTD)上的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。
- 基本网络知识。
- 基本的Cisco安全管理中心体验。
- 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)提供与传统VLAN相同的以太网第2层网络服务。由于虚拟环境中对VLAN网段的高需求，VXLAN提供了更高的扩展性和灵活性，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，然后放置在UDP-IP数据包中。使用此MAC-in-UDP封装，VXLAN在第3层网络上通过隧道传输第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，以满足更多第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模型）
- Geneve（用于安全防火墙威胁防御虚拟设备）

在Amazon Web Services(AWS)网关负载均衡器和设备之间透明地路由数据包，以及发送额外信息需要通用封装。

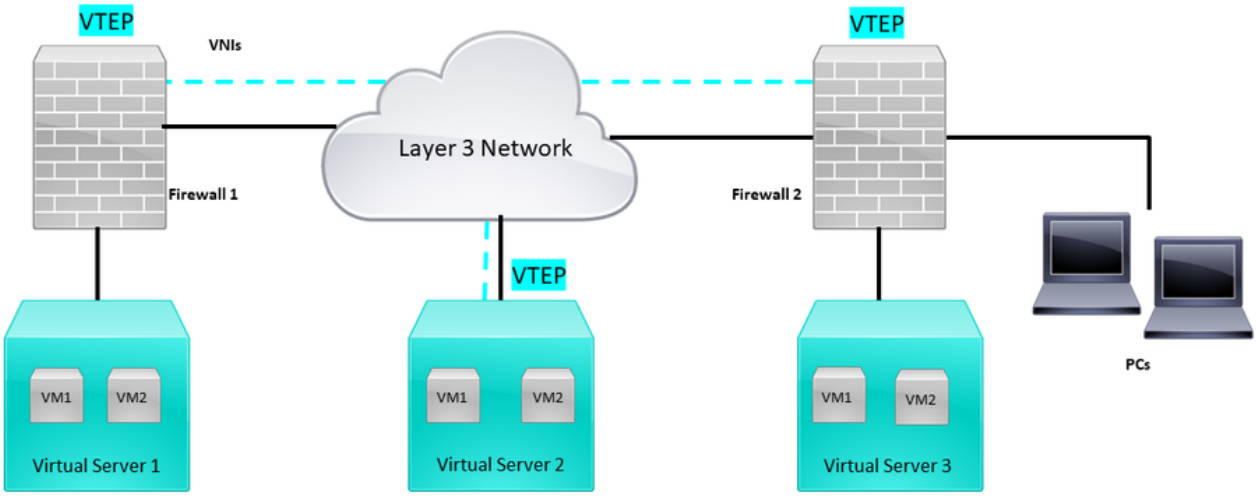
VXLAN使用VXLAN隧道终端(VTEP)将租户的终端设备映射到VXLAN网段，并执行VXLAN封装和解封。每个VTEP具有两种接口类型：一个或多个称为VXLAN网络标识符(VNI)的虚拟接口，其中可以应用安全策略；以及称为VTEP源接口的常规接口，其中VNI接口在VTEP之间通过隧道传输。VTEP源接口连接到传输IP网络以进行VTEP到VTEP通信，VNI接口类似于VLAN接口：它们是虚拟接口，使用标记在给定物理接口上分隔网络流量。安全策略应用于每个VNI接口。可以添加一个VTEP接口，并且所有VNI接口与同一VTEP接口关联。AWS上的威胁防御虚拟集群有一个例外。

威胁防御可通过三种方式封装和解封：

- 可以在威胁防御上静态配置单个对等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。

本文档重点介绍静态配置了2个对等VTEP IP地址组的VXLAN接口用于VXLAN封装。如果您需要配置Geneve接口，请查看AWS中Geneve接口的官方文档，或者使用单个对等体或组播组配置VTEP，请查看VTEP接口与单个对等体或组播组配置指南。

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配置了威胁防御。本文档重点介绍重叠网络配置。

配置

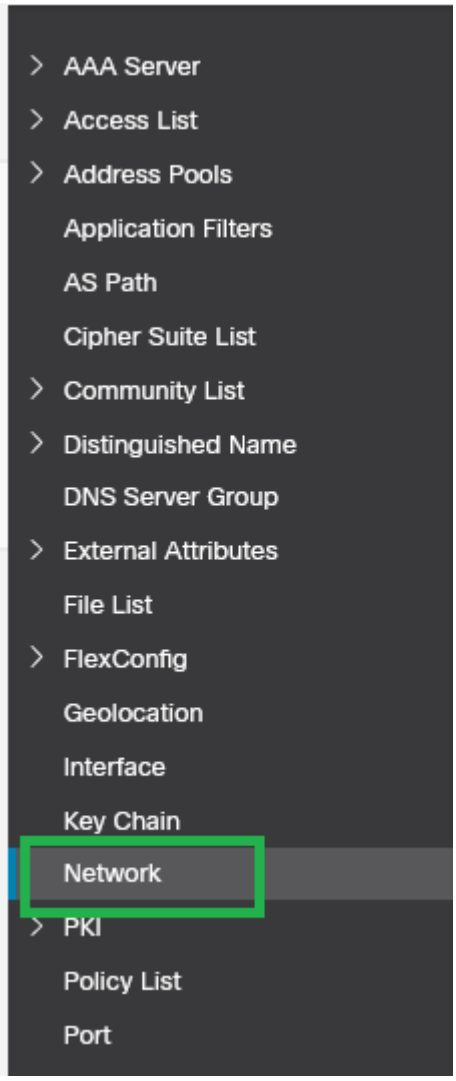
配置VTEP对等组

步骤 1：导航到对象>对象管理。



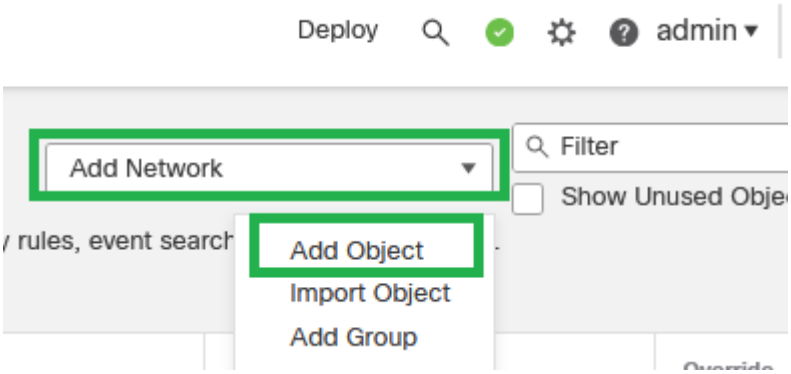
对象 — 对象管理

步骤 2： 单击左侧菜单中的Network。



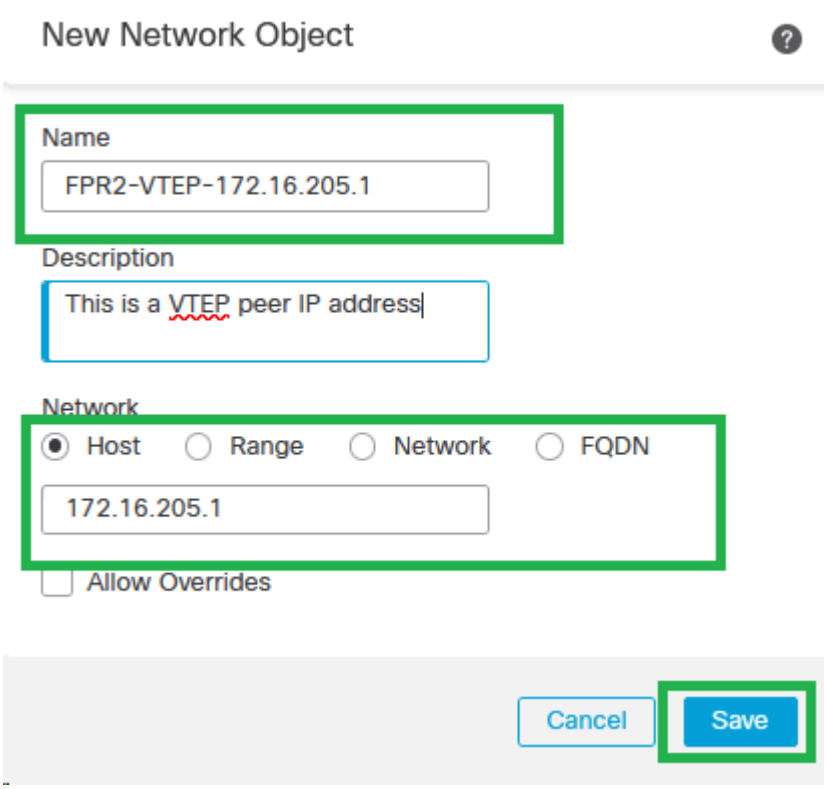
网络

步骤 3：为VTEP对等IP地址创建网络主机对象。单击Add Network > Add Object。



添加网络 — 添加对象

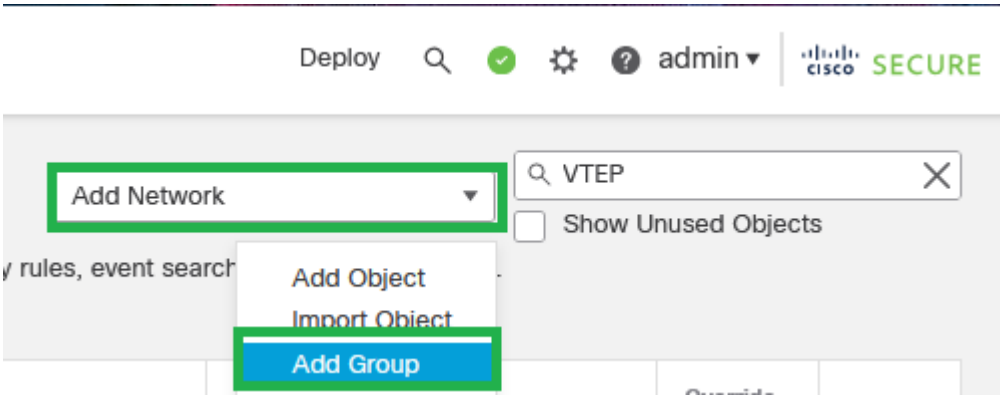
步骤 4：为VTEP对等体创建新的主机网络对象。设置对象名称和IP地址，然后单击Save。



新建网络对象

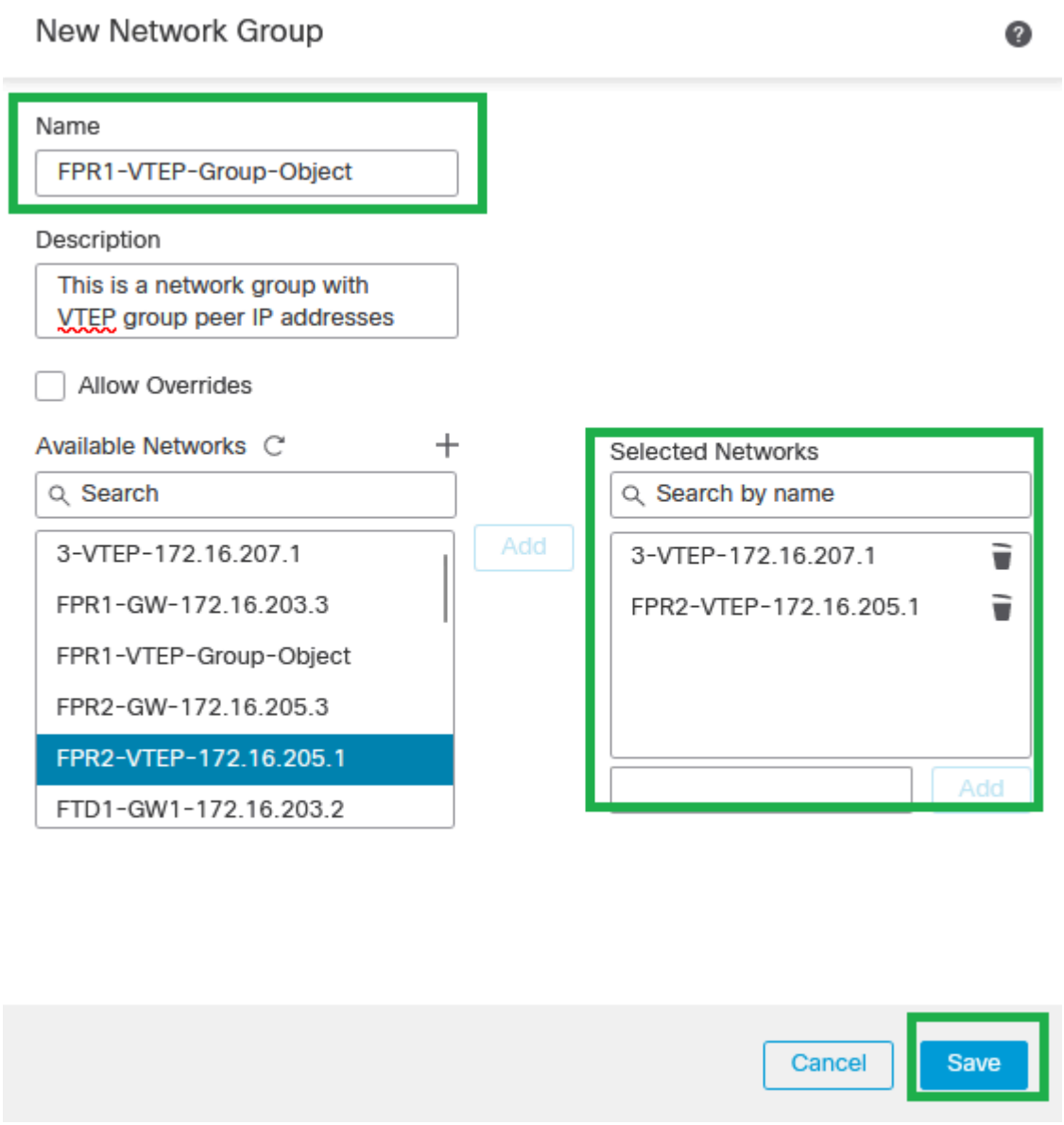
注意：为您拥有的每个VTEP对等IP地址配置更多主机网络对象。本配置指南中有两个对象。

步骤 5：创建对象组，单击Add Network > Add Group。



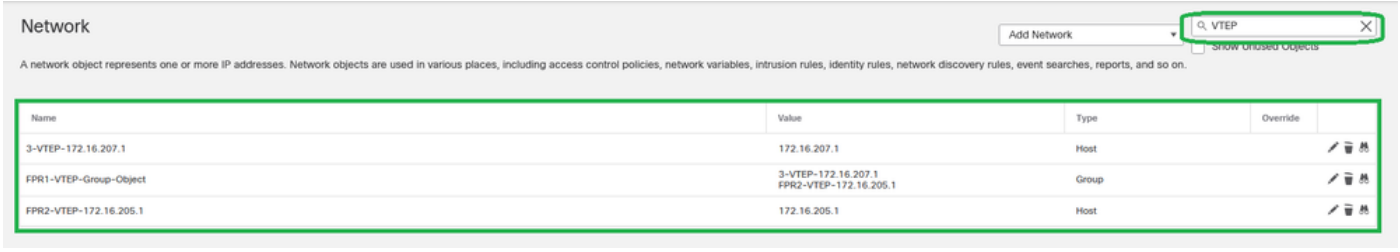
添加网络 — 添加组

第6步：使用所有VTEP对等IP地址创建网络对象组。设置网络组名称并选择所需的网络对象组，然后单击Save。



创建网络对象组

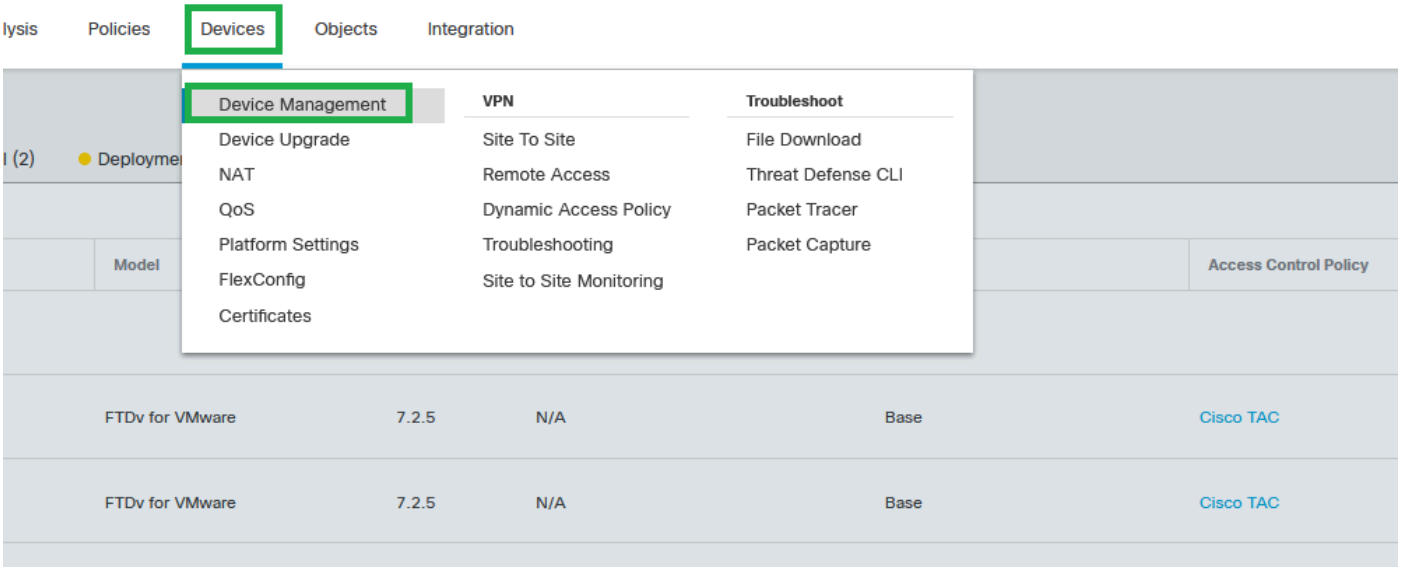
步骤 7：从网络对象过滤器验证网络对象和网络对象组。



验证VTEP对象组

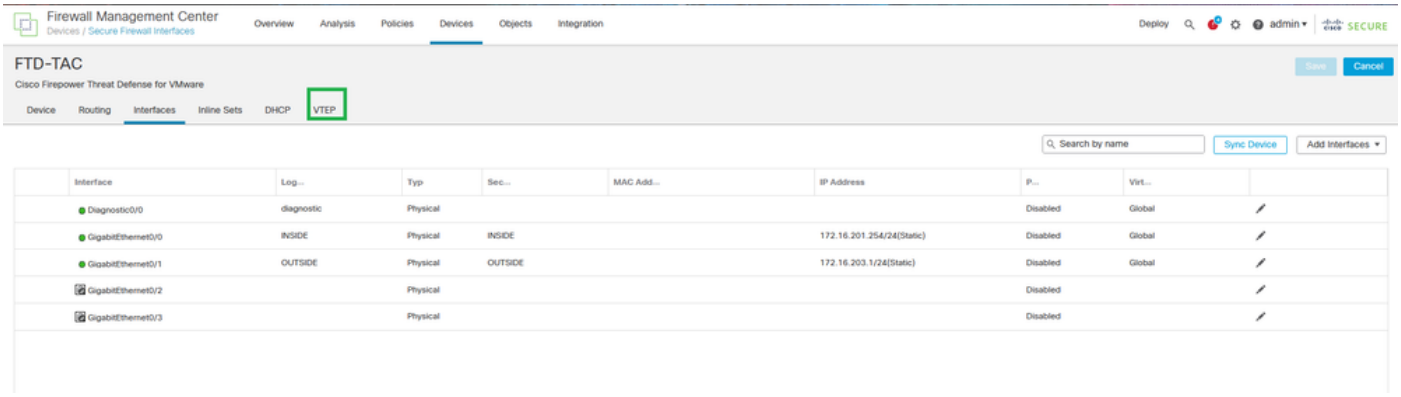
配置VTEP源接口

步骤 1：导航到设备>设备管理，然后编辑威胁防御。



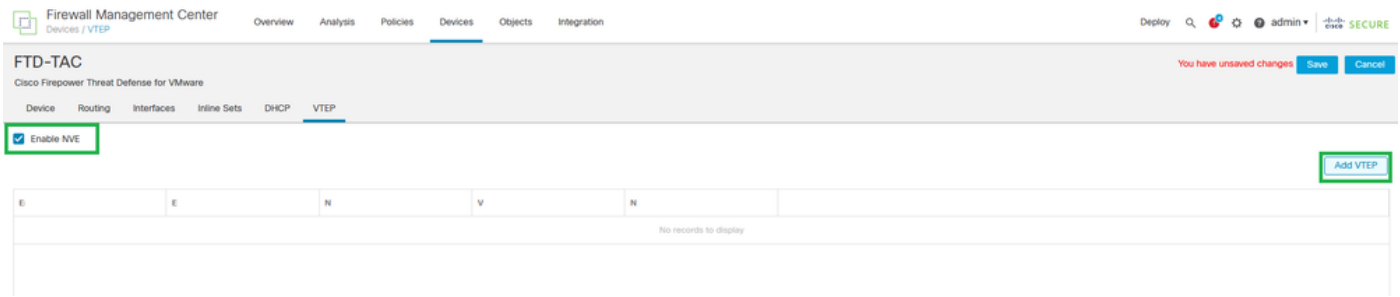
设备 — 设备管理

步骤 2：导航到VTEP部分。



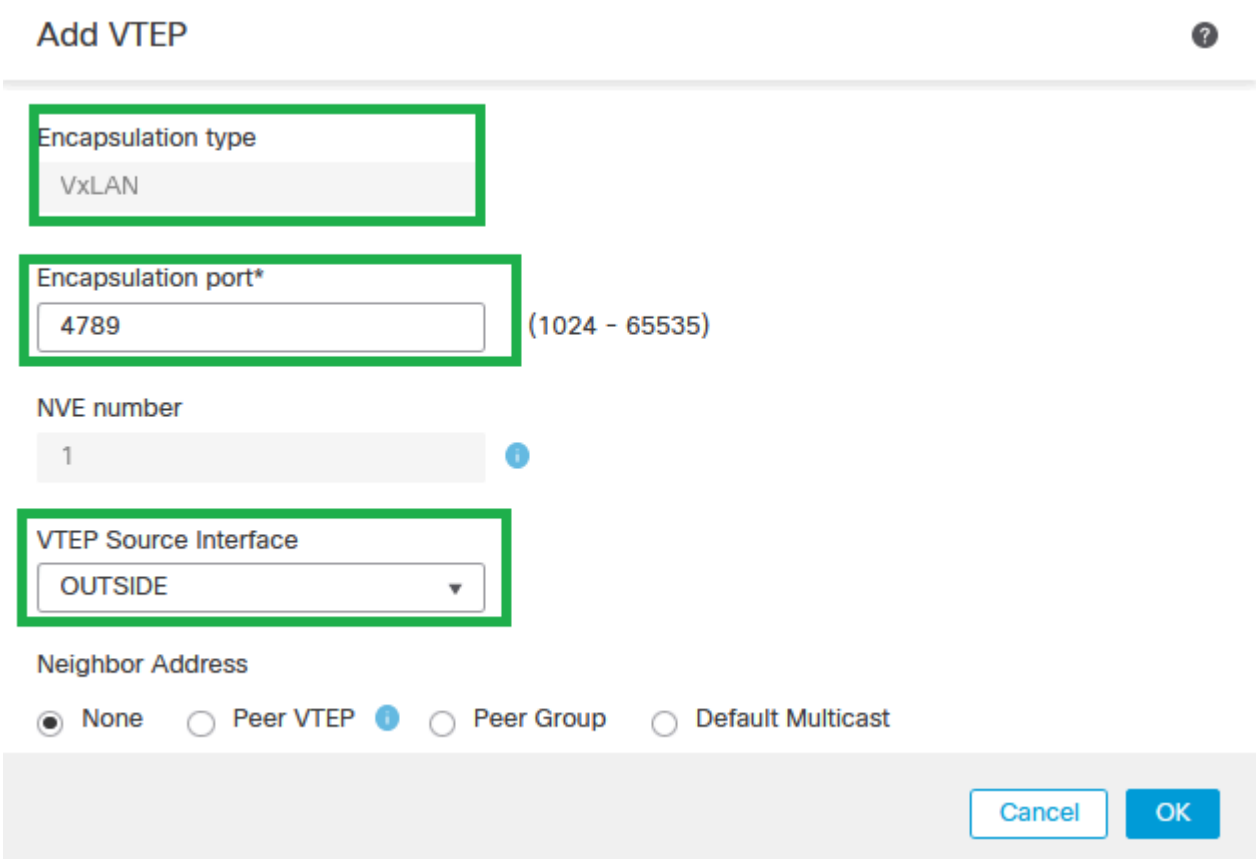
VTEP部分

步骤 3：选中Enable VNE复选框，然后单击Add VTEP。



启用NVE并添加VTEP

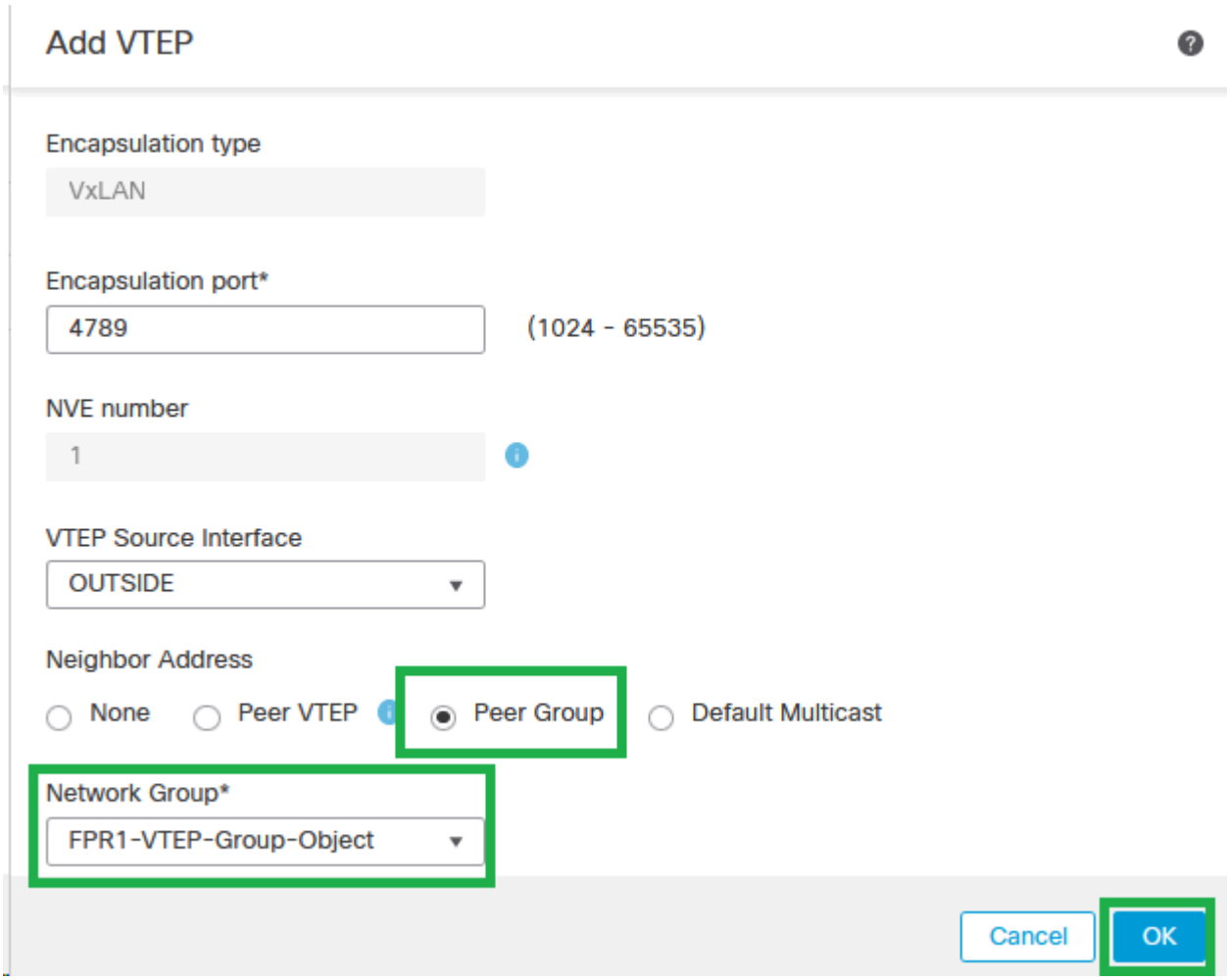
步骤 4：选择VxLAN作为Encapsulation类型，输入Encapsulation Port值，然后选择用于此威胁防御的VTEP源的接口（本配置指南为Outside interface）



添加VTEP

注意：VxLAN封装是默认封装。对于AWS，您可以在VxLAN和Geneve之间进行选择。默认值为4789，任何封装端口都可以根据设计在1024 - 65535范围之间选择。

步骤 5：选择Peer Group，然后选择在上一个配置部分中创建的网络对象组，然后单击OK。

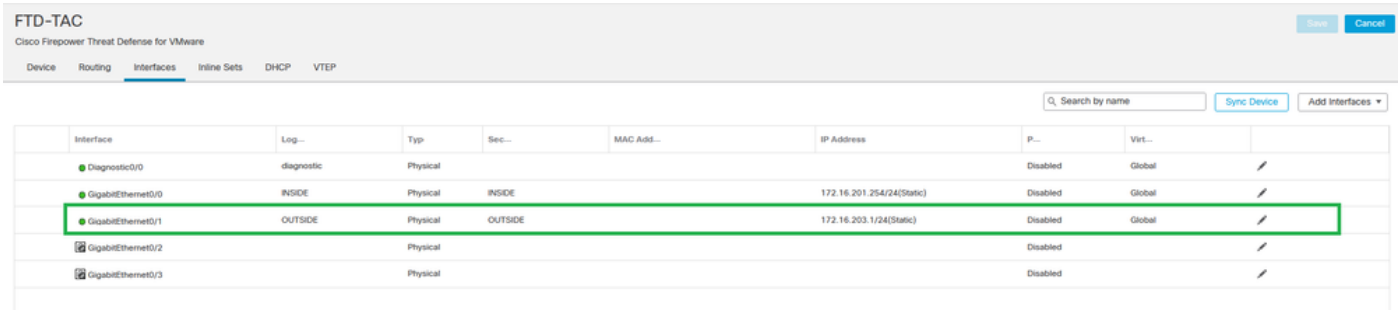


对等组 — 网络对象组

步骤 6：保存更改。

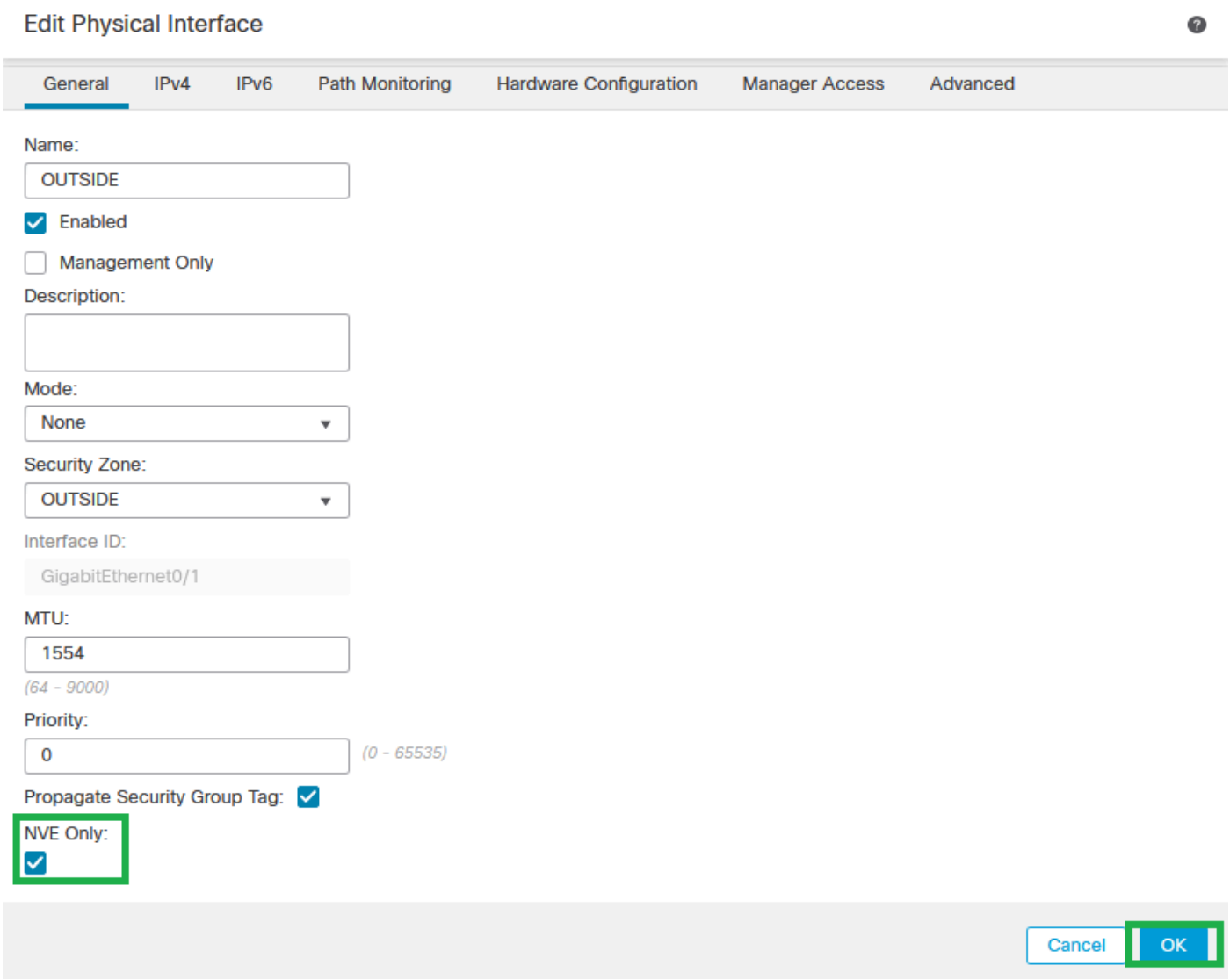
警告：保存更改后，系统会显示巨帧更改消息，将分配为VTEP的接口上的MTU更改为1554，确保底层网络上使用相同的MTU。

第7步：点击Interfaces并编辑用于VTEP源接口的接口。（本配置指南中的外部接口）



外部作为VTEP源接口

第8步（可选）：在General页面上，选中NVE Only复选框，然后单击 OK。



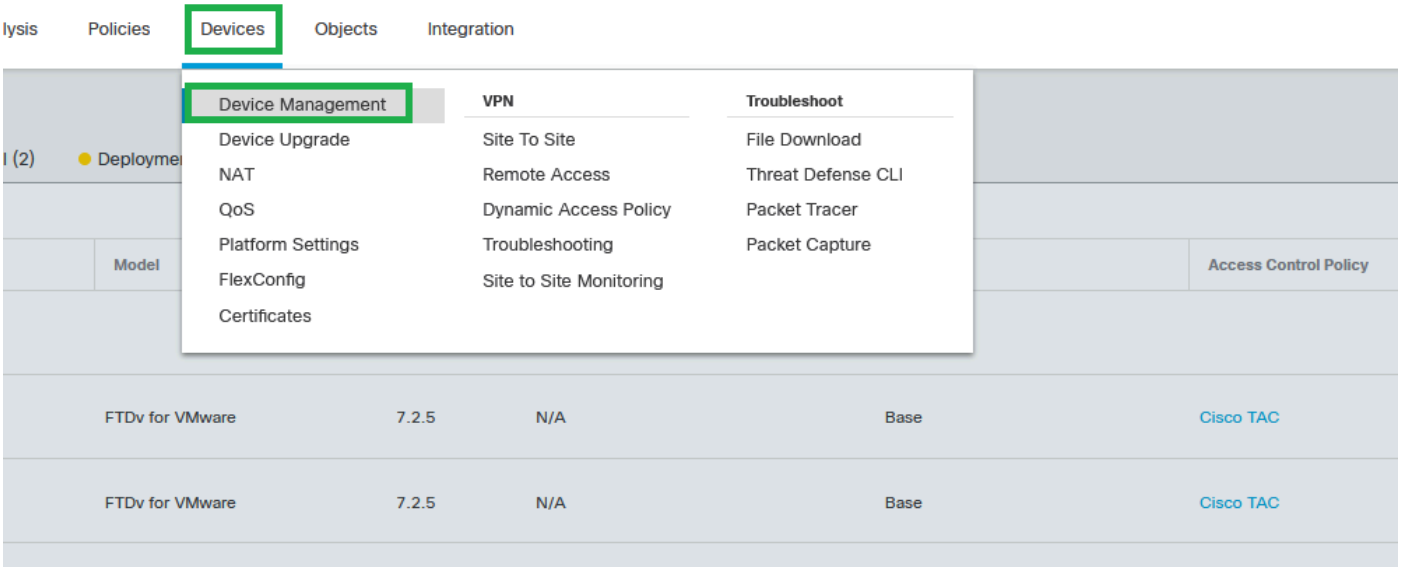
仅NVE配置

警告：此设置对于路由模式是可选的，在路由模式下，此设置将流量限制为VXLAN，并且仅在此接口上限制公共管理流量。此设置将自动在透明防火墙模式下启用。

步骤 9：保存更改。

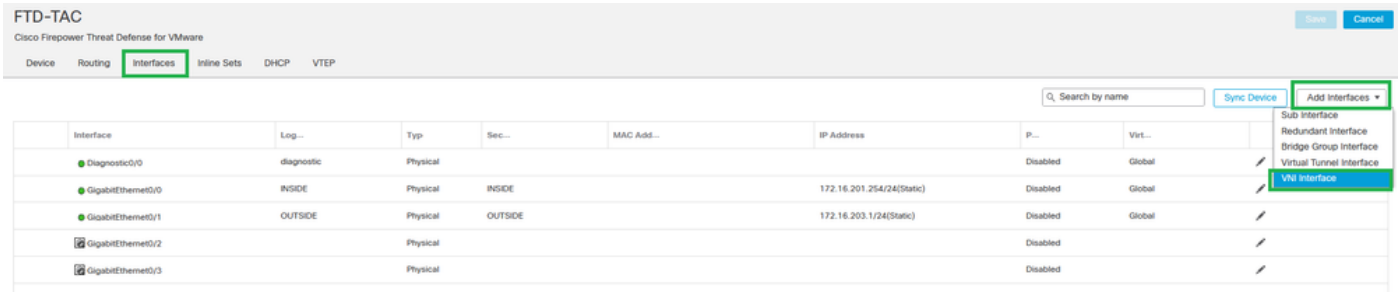
配置VTEP VNI接口

步骤 1：导航Devices > Device Management，然后编辑威胁防御。



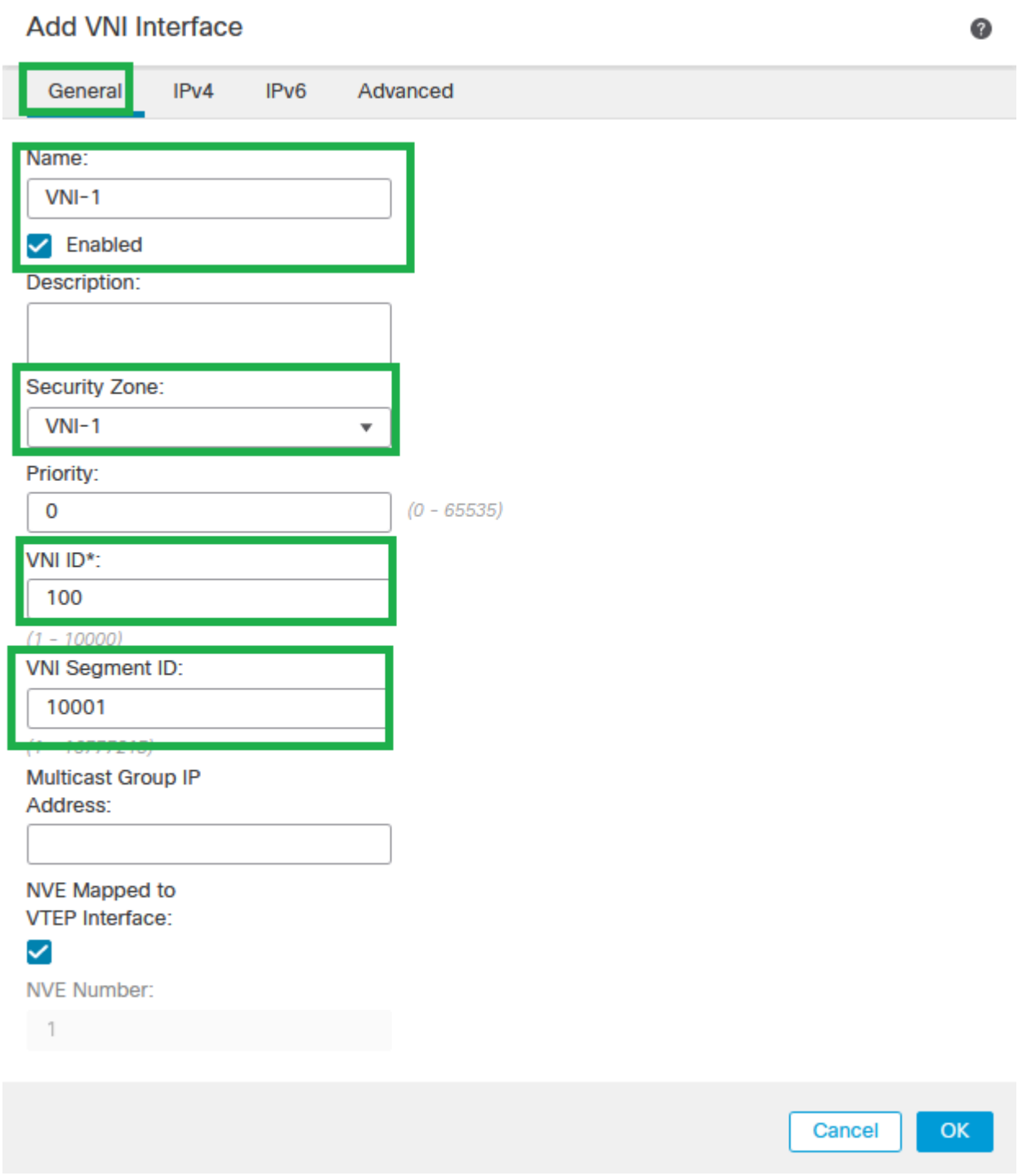
设备 — 设备管理

步骤 2：在Interfaces部分下，单击Add Interfaces > VNI Interfaces。



接口 — 添加接口 — VNI接口

步骤 3：在General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。

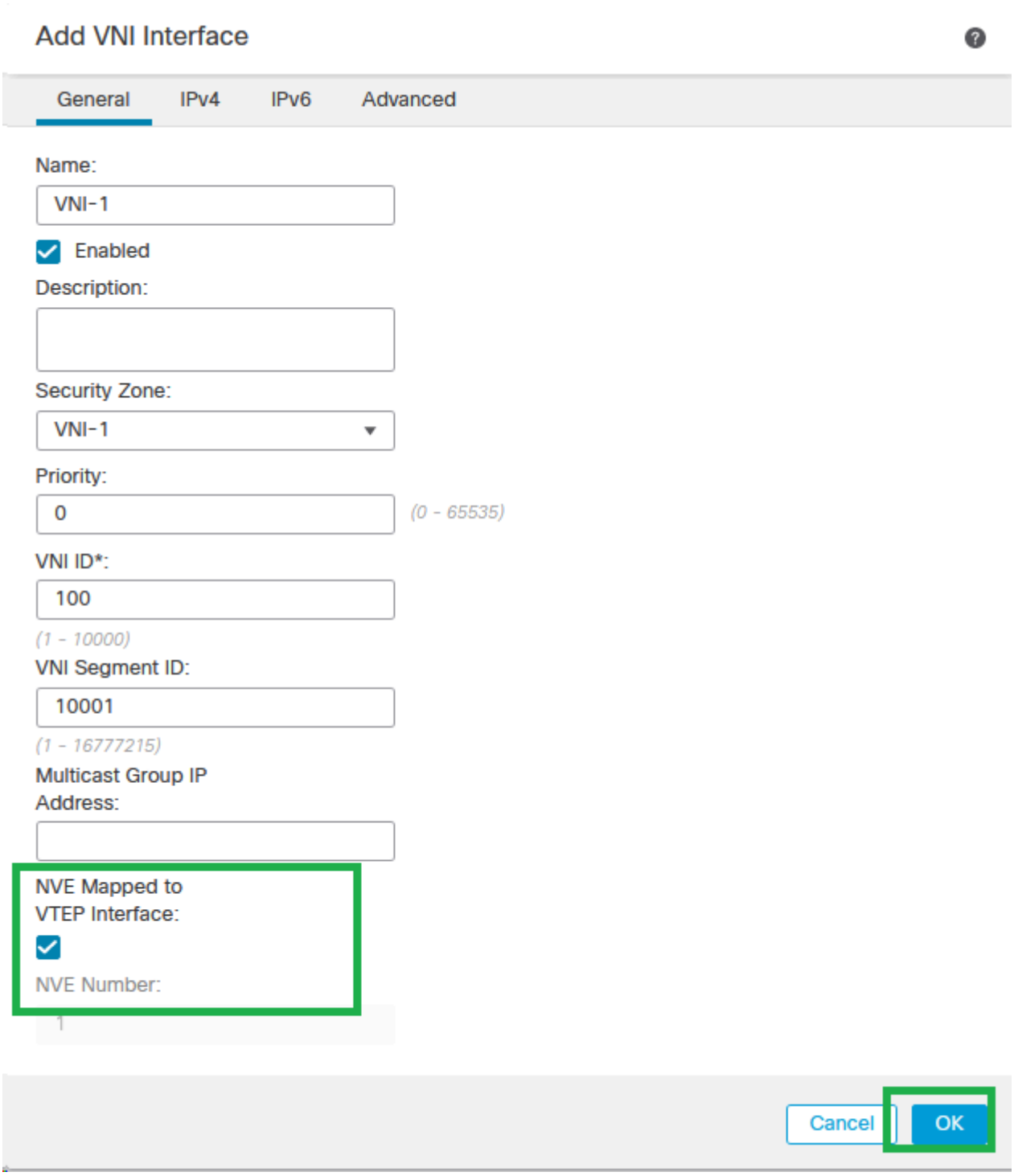


添加VNI接口

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

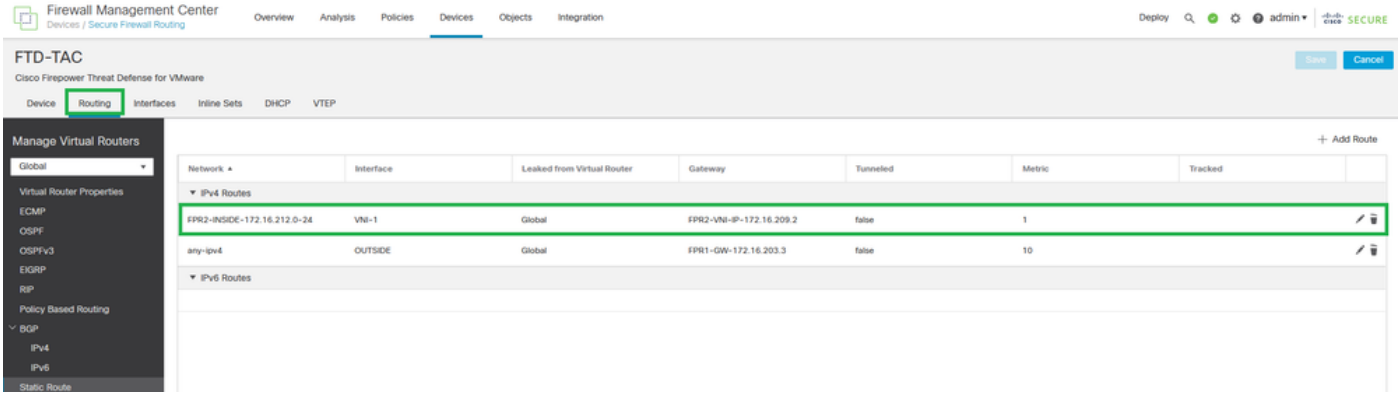
警告：如果未在VNI接口上配置组播组，则会使用VTEP源接口配置中的默认组（如果可用）。如果您为VTEP源接口手动设置VTEP对等IP，则不能为VNI接口指定组播组。

步骤 3：选中NVE Mapped to VTEP Interface复选框，然后单击OK。



NVE映射到VTEP接口

步骤 4：配置静态路由，将VXLAN的目的网络通告给VNI对等接口。导航路由>静态路由。



静态路由配置

警告：VXLAN的目的网络必须通过对等VNI接口发送。所有VNI接口必须位于同一个广播域（逻辑网段）中。

步骤 5：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]
---
```

检验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广播域中。

故障排除

检查与VTEP对等体的连接。

对等体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。

.

对等体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，配置错误的静态路由可能会生成ARP不完整输出。在VTEP接口上为VXLAN数据包配置捕获并以pcap格式下载该捕获，任何数据包分析器工具都可以帮助确认路由是否有任何问题。确保使用VNI对等IP地址作为网关。

```
Broadcast    ARP    92 Who has 172.16.203.3? 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
```

路由问题

在安全FTD上配置ASP丢弃捕获，以防发生任何防火墙丢弃，请使用show asp drop命令检查ASP丢弃计数器。联系思科TAC进行分析。

确保配置访问控制策略规则以允许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: VMware_b3:ba:6a (00:50:56:b3:ba:6a), Dst: VMware_b3:6e:68 (00:50:56:b3:6e:68)
> Internet Protocol Version 4, Src: 172.16.205.1, Dst: 172.16.203.1
> User Datagram Protocol, Src Port: 61587, Dst Port: 4789
v Virtual eXtensible Local Area Network
  > Flags: 0x0800, VXLAN Network ID (VNI)
    Group Policy ID: 0
    VXLAN Network Identifier (VNI): 10001
    Reserved: 0
v Ethernet II, Src: VMware_b3:ba:6a (00:50:56:b3:ba:6a), Dst: VMware_b3:26:b8 (00:50:56:b3:26:b8)
  > Destination: VMware_b3:26:b8 (00:50:56:b3:26:b8)
  > Source: VMware_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）。

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）。