使用安全FMC在安全FTD上設定VXLAN介面

目錄

簡介

本檔案介紹如何使用安全防火牆管理中心(FMC)設定安全防火牆威脅防禦(FTD)上的VXLAN介面

必要條件

需求

思科建議您瞭解以下主題：

- 基本VLAN/VXLAN概念。
- 基本網路知識。
- 基本Cisco Secure Management Center體驗。
- 基本思科安全防火牆威脅防禦體驗。

採用元件

本文中的資訊係根據以下軟體和硬體版本：

- 運行7.2.4版的Cisco Secure Firewall Management Center Virtual (FMCv) VMware。
- 運行7.2.4版本的思科安全防火牆威脅防禦虛擬裝置(FTDv) VMware。

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

背景資訊

虛擬可擴充VLAN (VXLAN)提供的乙太網路第2層網路服務與傳統VLAN相同。由於虛擬環境中對VLAN網段的需求很高，VXLAN提供了更高的擴展性和靈活性，並且還定義了MAC-in-UDP封裝方案，其中原始第2層幀增加了VXLAN報頭，然後將其置於UDP-IP資料包中。使用此UDP內MAC封裝，VXLAN會透過第3層網路透過第2層網路建立通道。VXLAN提供以下優勢：

- 多租戶網段中的VLAN靈活性：
- 更高的可擴充性，可解決更多的第2層(L2)網段。
- 提高網路利用率。

思科安全防火牆威脅防禦(FTD)支援兩種型別的VXLAN封裝。

- VXLAN（用於所有安全防火牆威脅防禦模型）
- 一般（用於安全防火牆威脅防禦虛擬裝置）

在Amazon Web Services (AWS)網關負載均衡器和裝置之間透明地路由資料包，以及傳送額外資訊需要通用封裝。

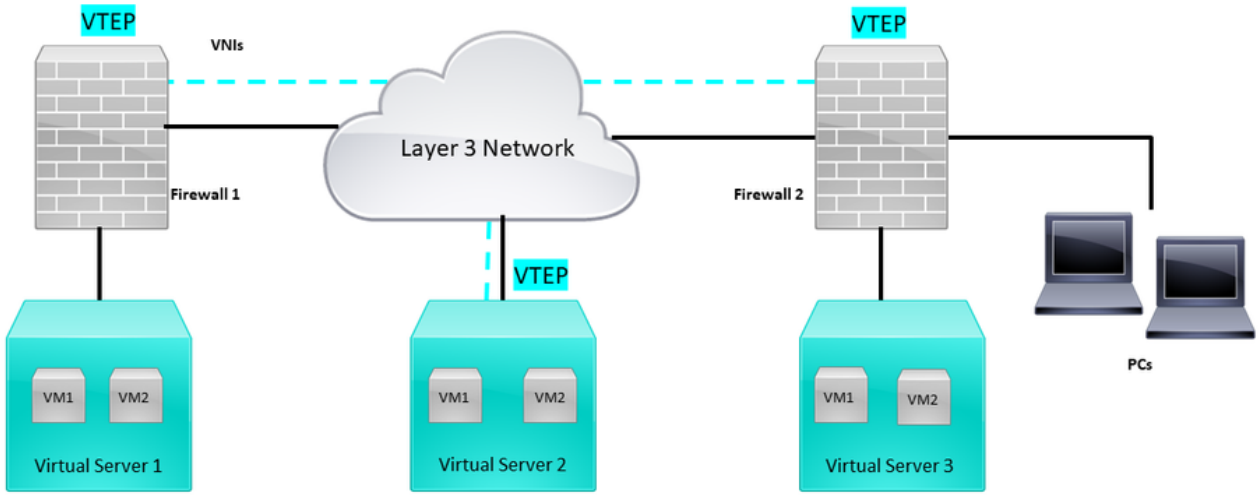
VXLAN使用VXLAN通道端點(VTEP)將租戶的終端裝置對應到VXLAN區段，並執行VXLAN封裝和解除封裝。每個VTEP有兩個介面型別：一個或多個稱為VXLAN網路辨識碼(VNI)介面（可套用安全原則），以及稱為VTEP來源介面的一般介面（VNI介面在VTEP之間以通道傳送）。VTEP源介面連線到傳輸IP網路以進行VTEP到VTEP通訊，VNI介面類似於VLAN介面：它們是虛擬介面，使用標籤在給定的物理介面上分隔網路流量。安全策略應用於每個VNI介面。可以增加一個VTEP介面，並且所有VNI介面與同一個VTEP介面關聯。AWS上的威脅防禦虛擬集群有一個例外。

威脅防禦透過三種方式進行封裝和解封：

- 可在威脅防禦上靜態配置單個對等VTEP IP地址。
- 可在威脅防禦上靜態配置一組對等VTEP IP地址。
- 可以在每個VNI介面上配置組播組。

本檔案將著重於靜態設定兩組對等式VTEP IP位址後，用於VXLAN封裝的VXLAN介面。如果需要配置通用介面，請檢視AWS中通用介面的正式文檔，或者使用單個對等體或組播組配置VTEP，請檢視VTEP介面與單個對等體或組播組配置指南。

網路圖表



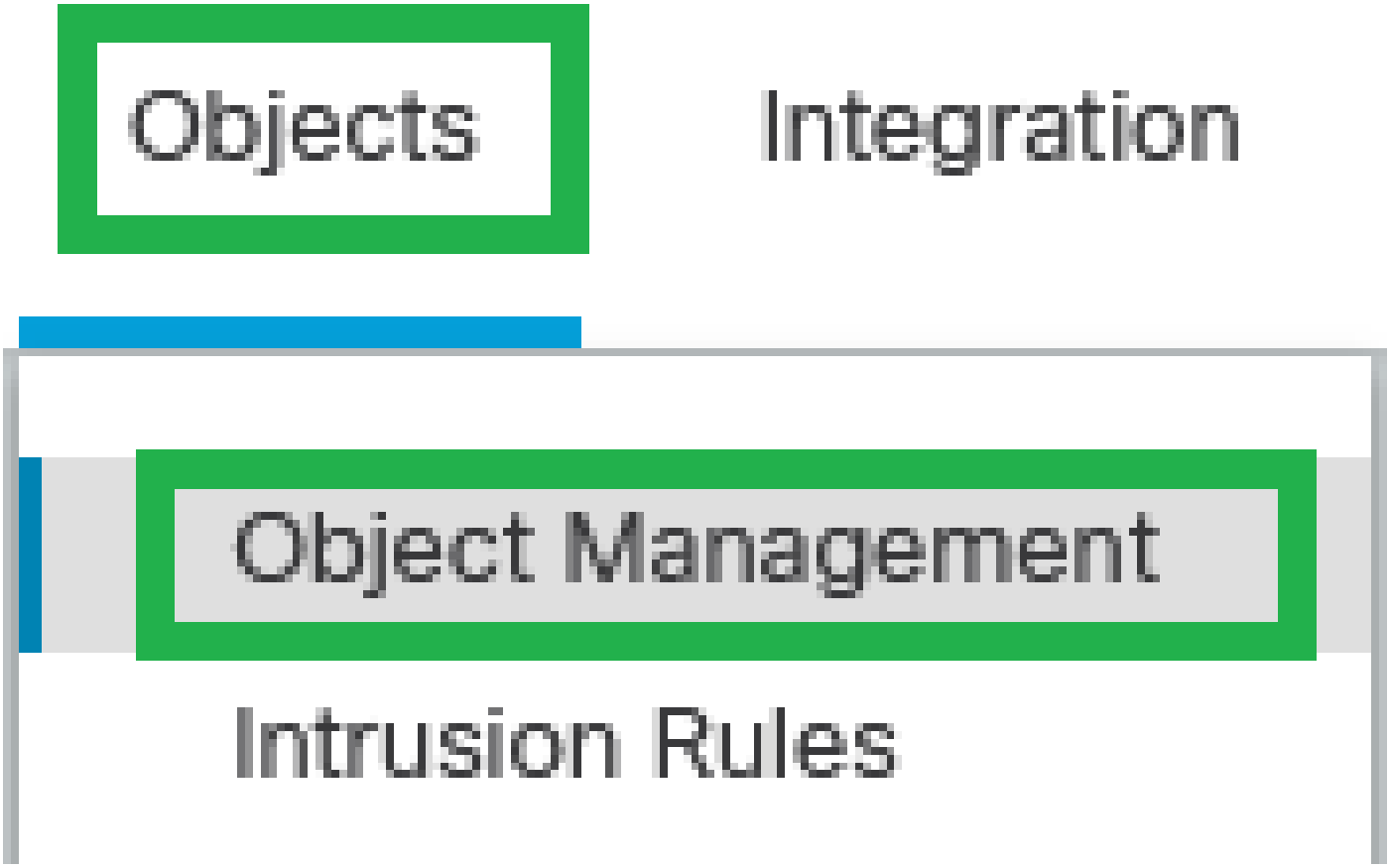
網路拓撲

配置部分假設底層網路已透過安全防火牆管理中心進行威脅防禦。本文檔重點介紹重疊網路配置。

設定

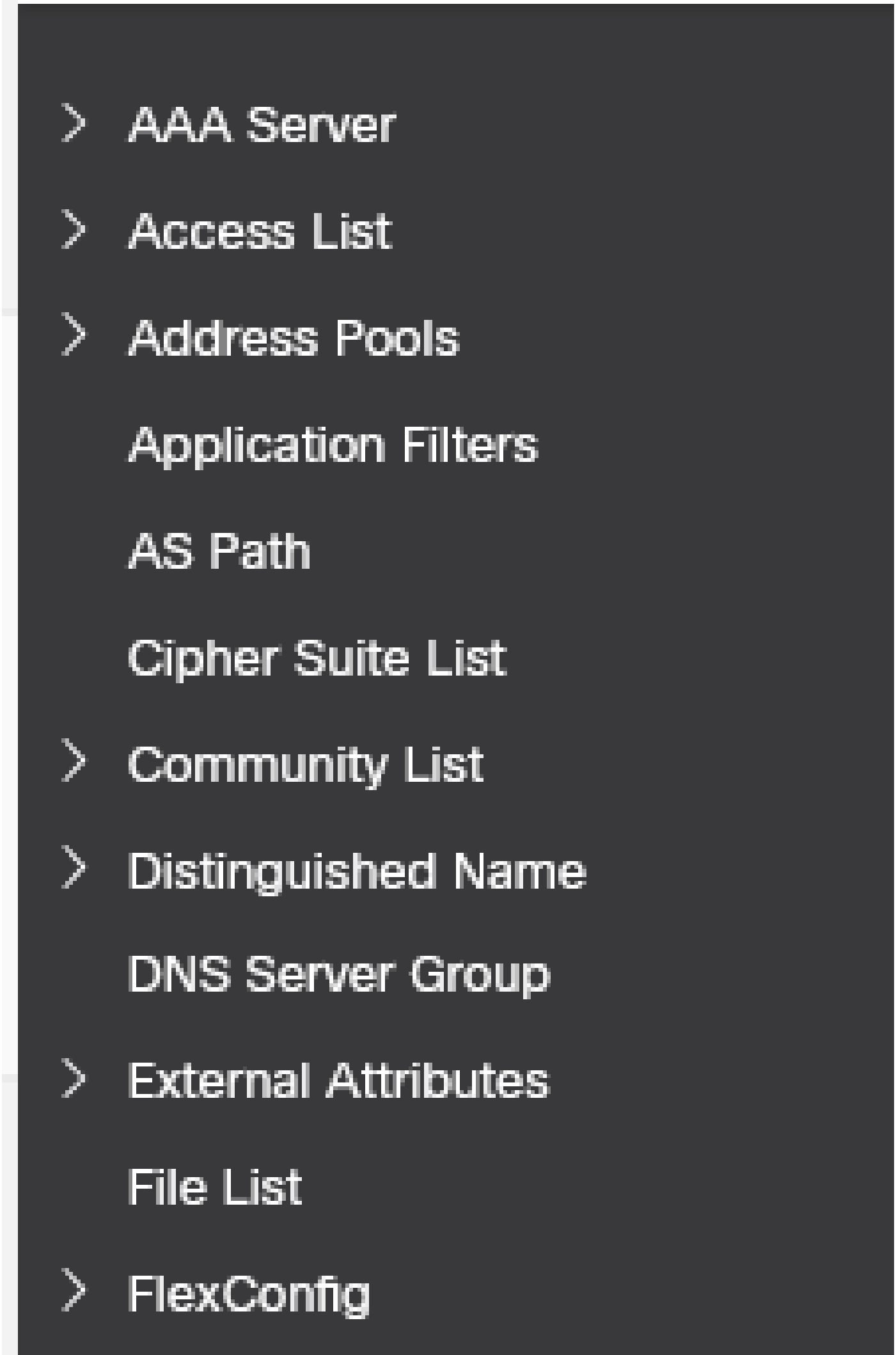
配置VTEP對等組

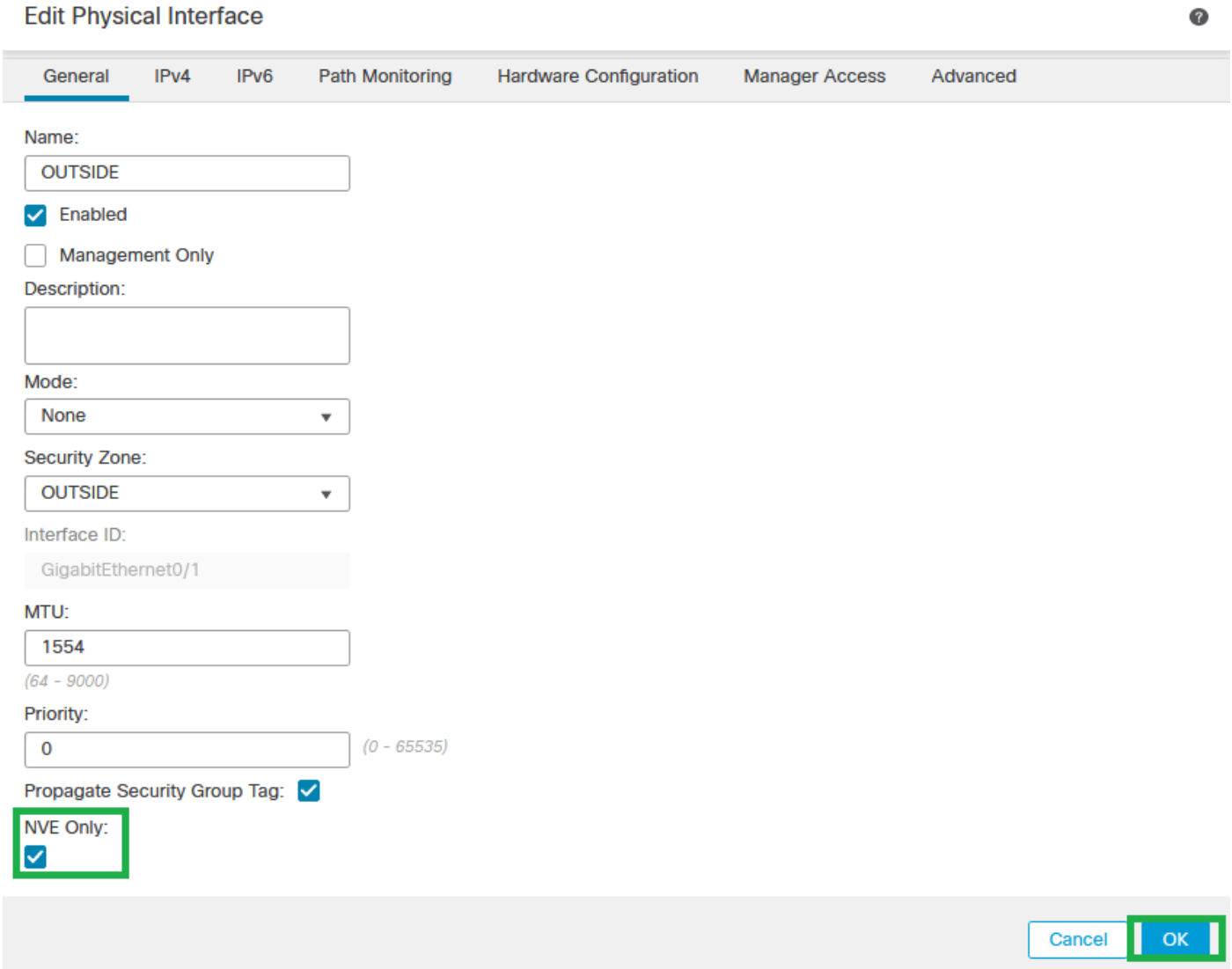
第1步：導航到對象>對象管理。



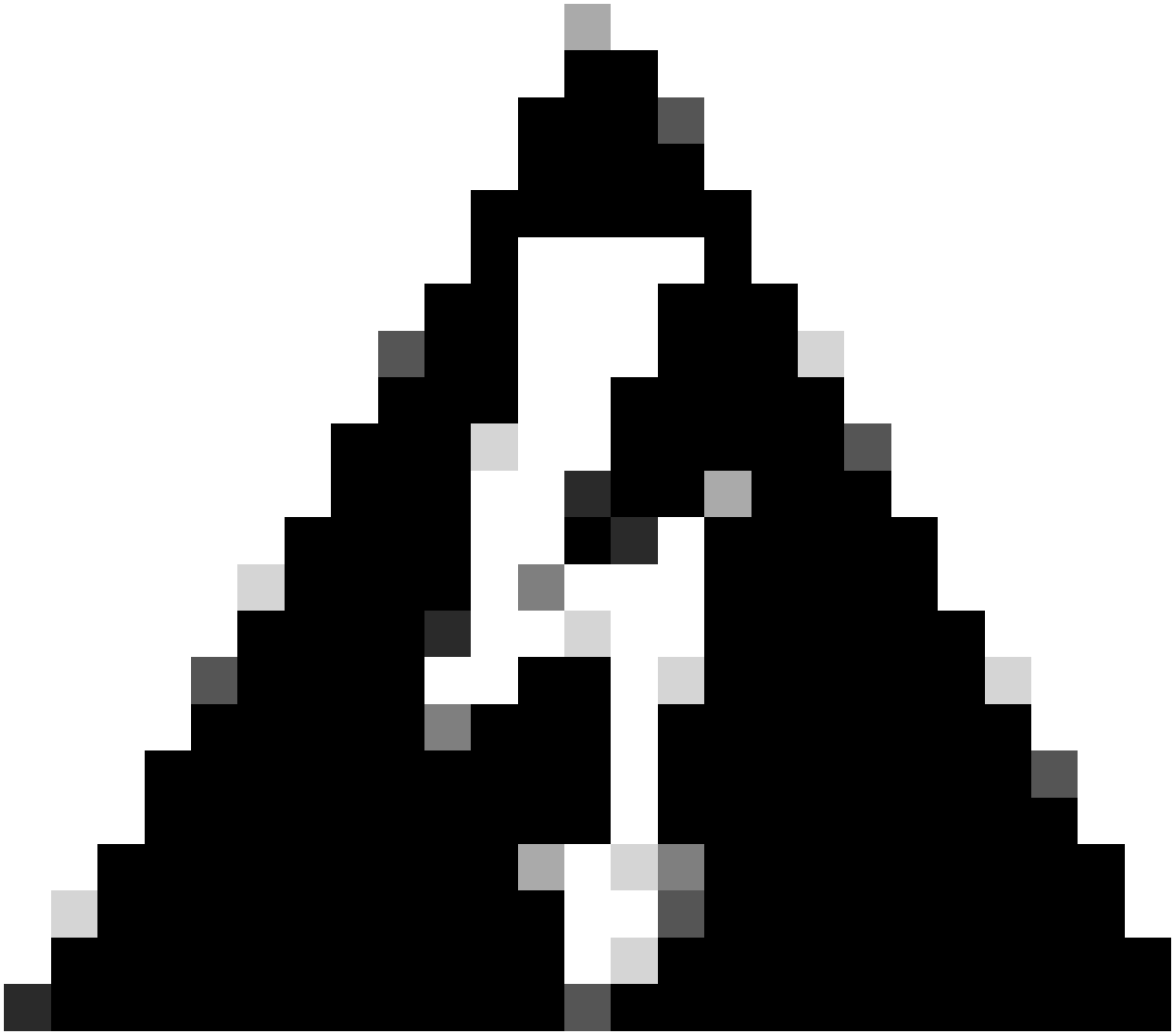
物件-物件管理

第2步：按一下左側選單中的Network。


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

僅NVE配置

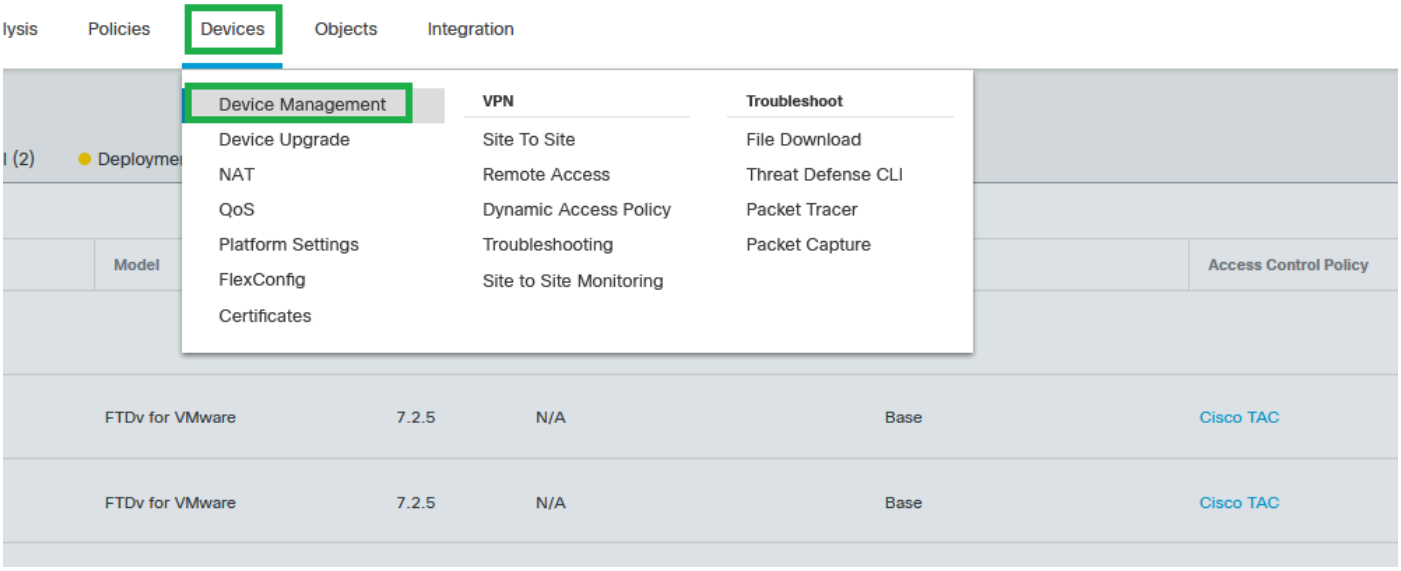


警告：對於此設定將流量限制為VXLAN並且僅在此介面上限制公共行政流量的路由模式，此設定是可選的。此設定會自動為透明防火牆模式啟用。

第9步：儲存更改。

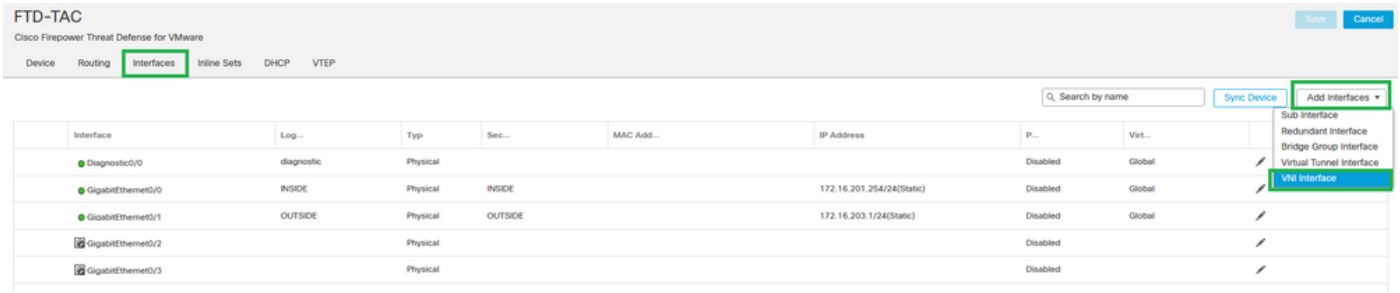
配置VTEP VNI介面

第1步：導航到裝置>裝置管理，然後編輯威脅防禦。



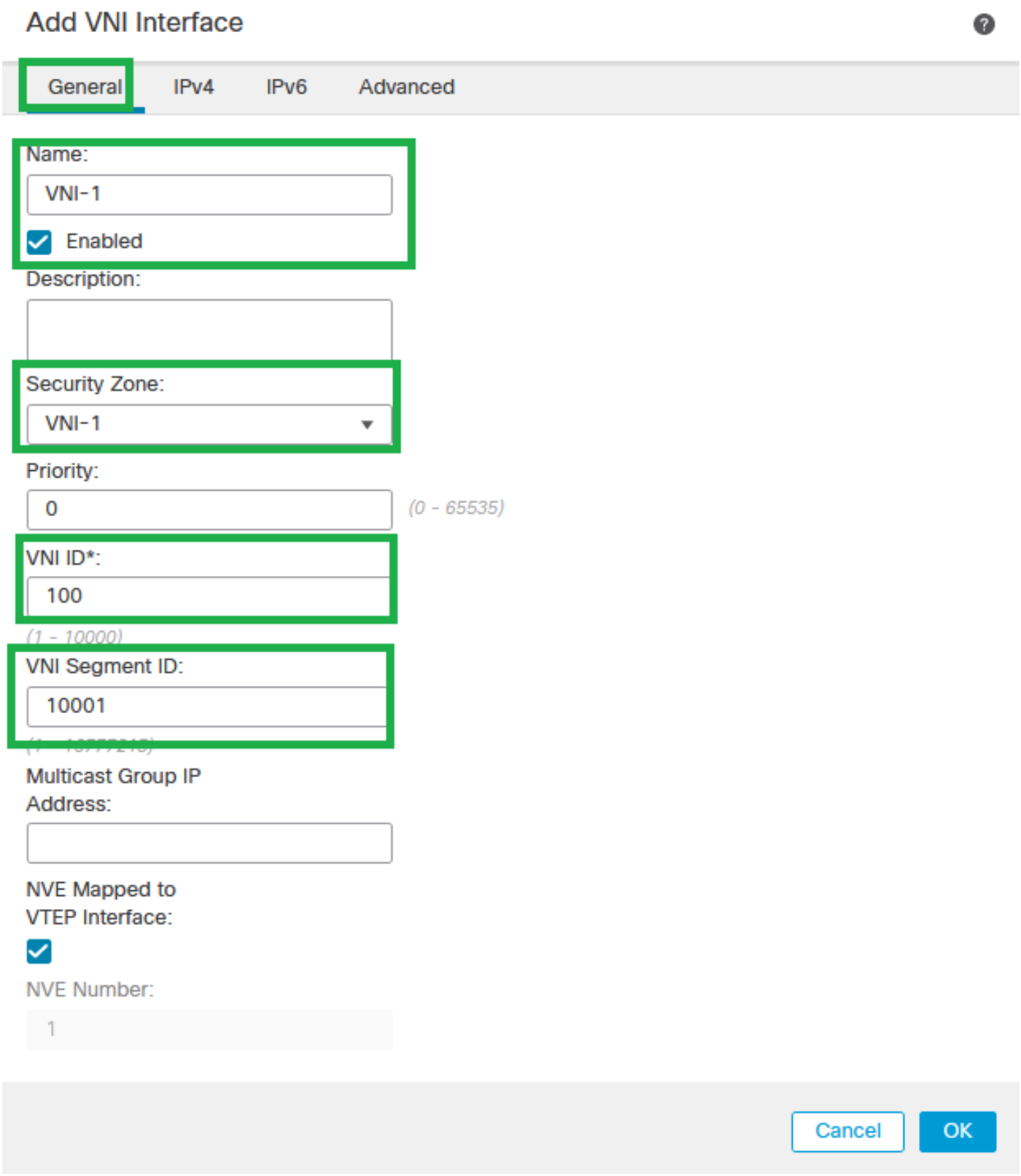
裝置-裝置管理

第2步：在Interfaces 部分下，點選Add Interfaces > VNI Interfaces。

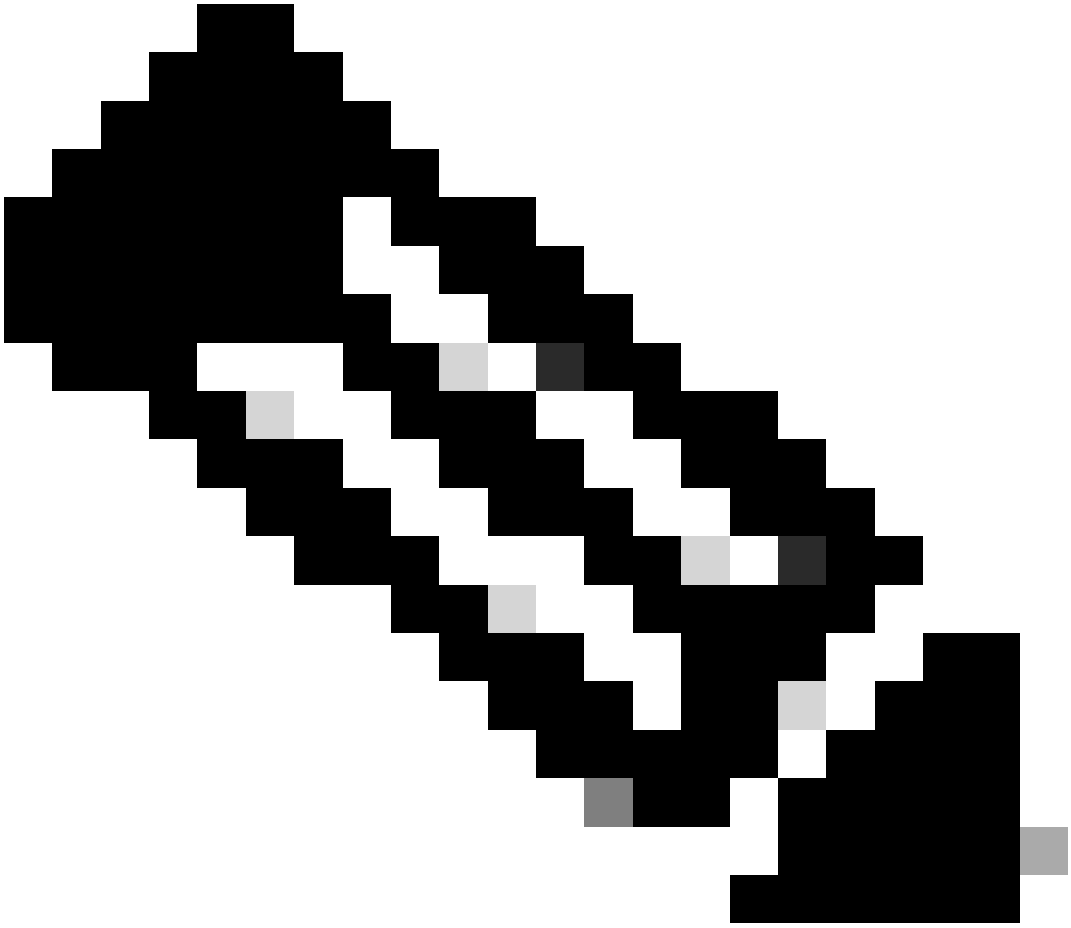


介面-增加介面- VNI介面

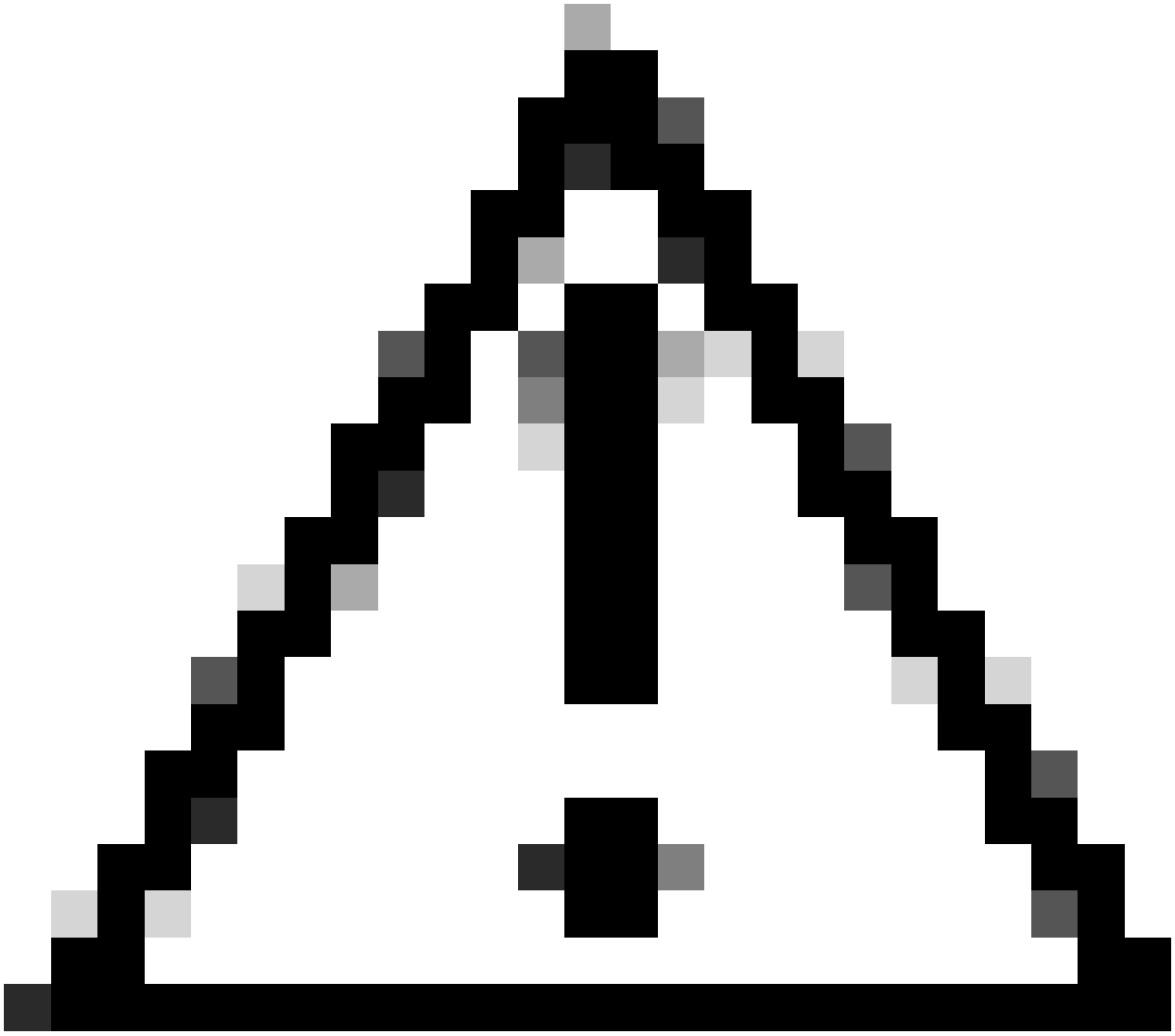
第3步：在常規部分下，使用名稱、說明、安全區域、VNI ID和VNI分段ID設定VNI介面。


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
Multicast Group IP Address:
NVE Mapped to VTEP Interface:
NVE Number:
1
Cancel
OK

增加VNI介面

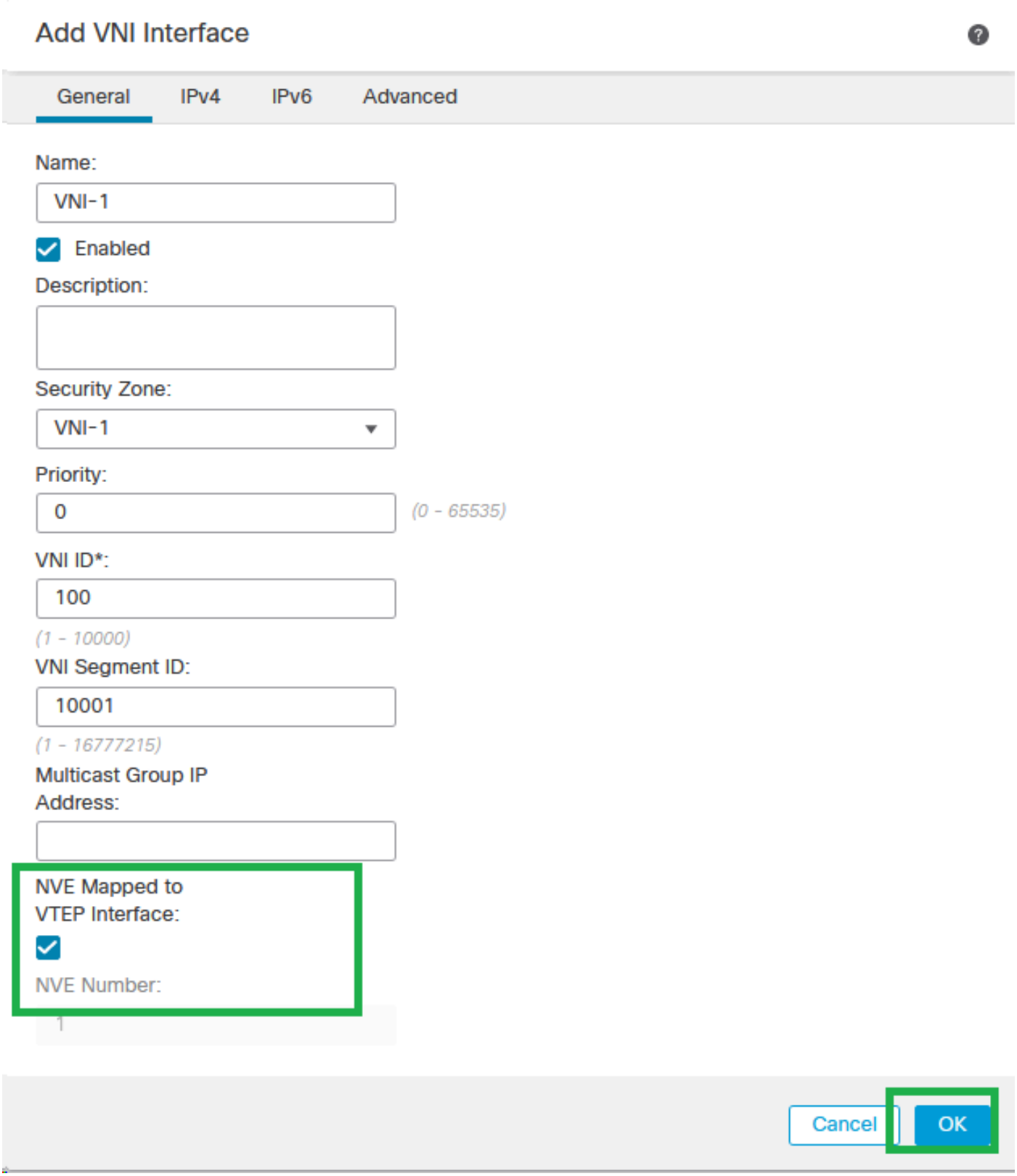


注意：VNI ID配置在1和10000之間，VNI段ID配置在1和16777215之間（段ID用於VXLAN標籤）。



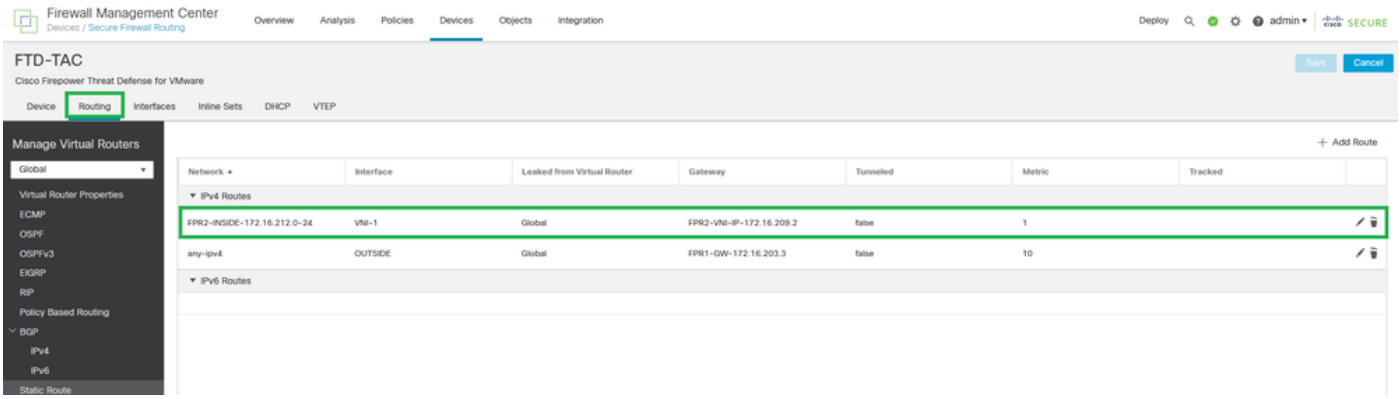
注意：如果未在VNI介面上配置多播組，則會使用VTEP源介面配置中的預設組（如果可用）。如果您手動為VTEP來源介面設定VTEP對等點IP，則無法為VNI介面指定多點傳送群組。

第3步：選中NVE Mapped to VTEP Interface覈取方塊並按一下OK。

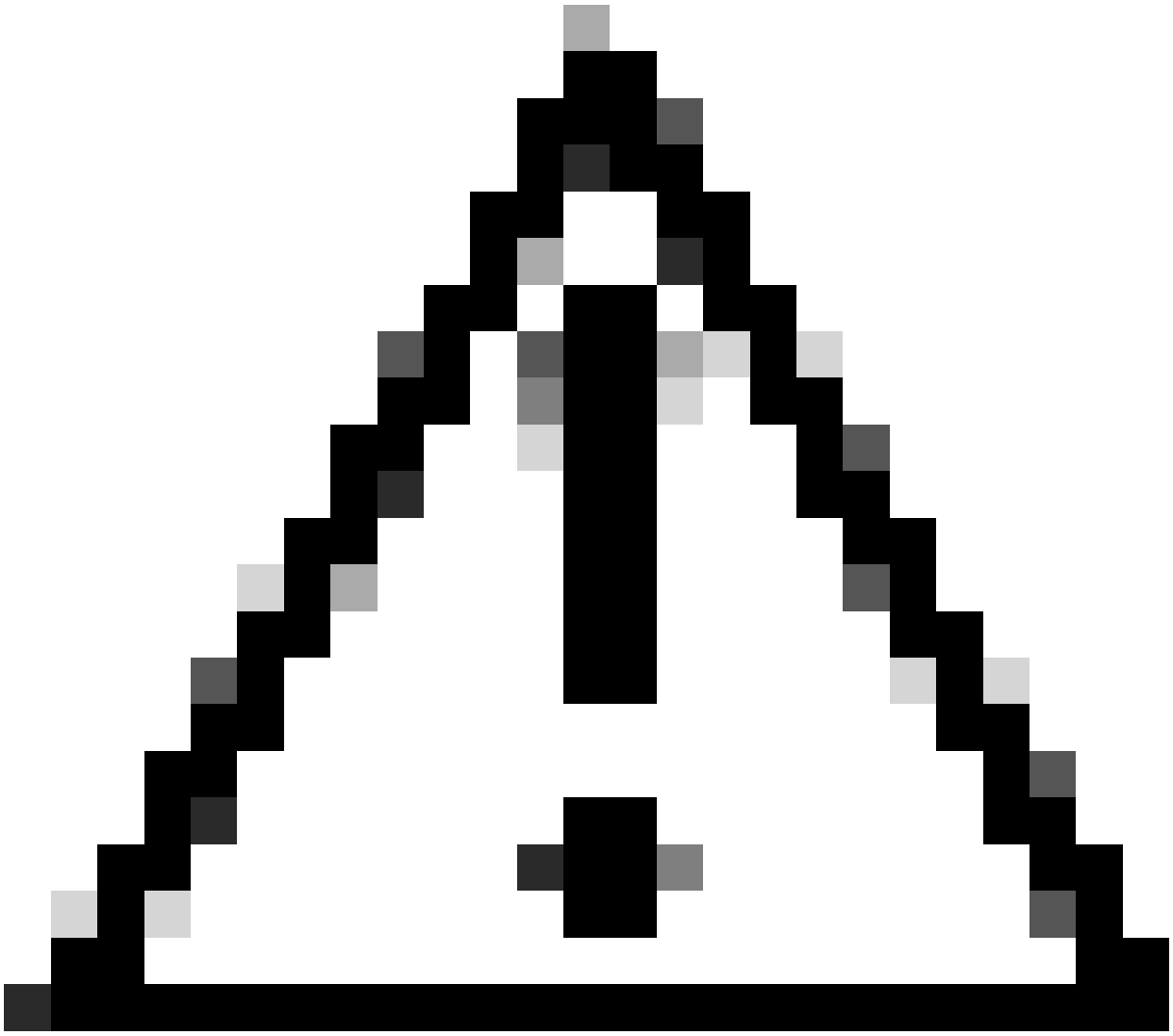


NVE對應到VTEP介面

第4步：配置靜態路由，將VXLAN的目標網路通告給VNI對等介面。導航到Routing > Static Route。

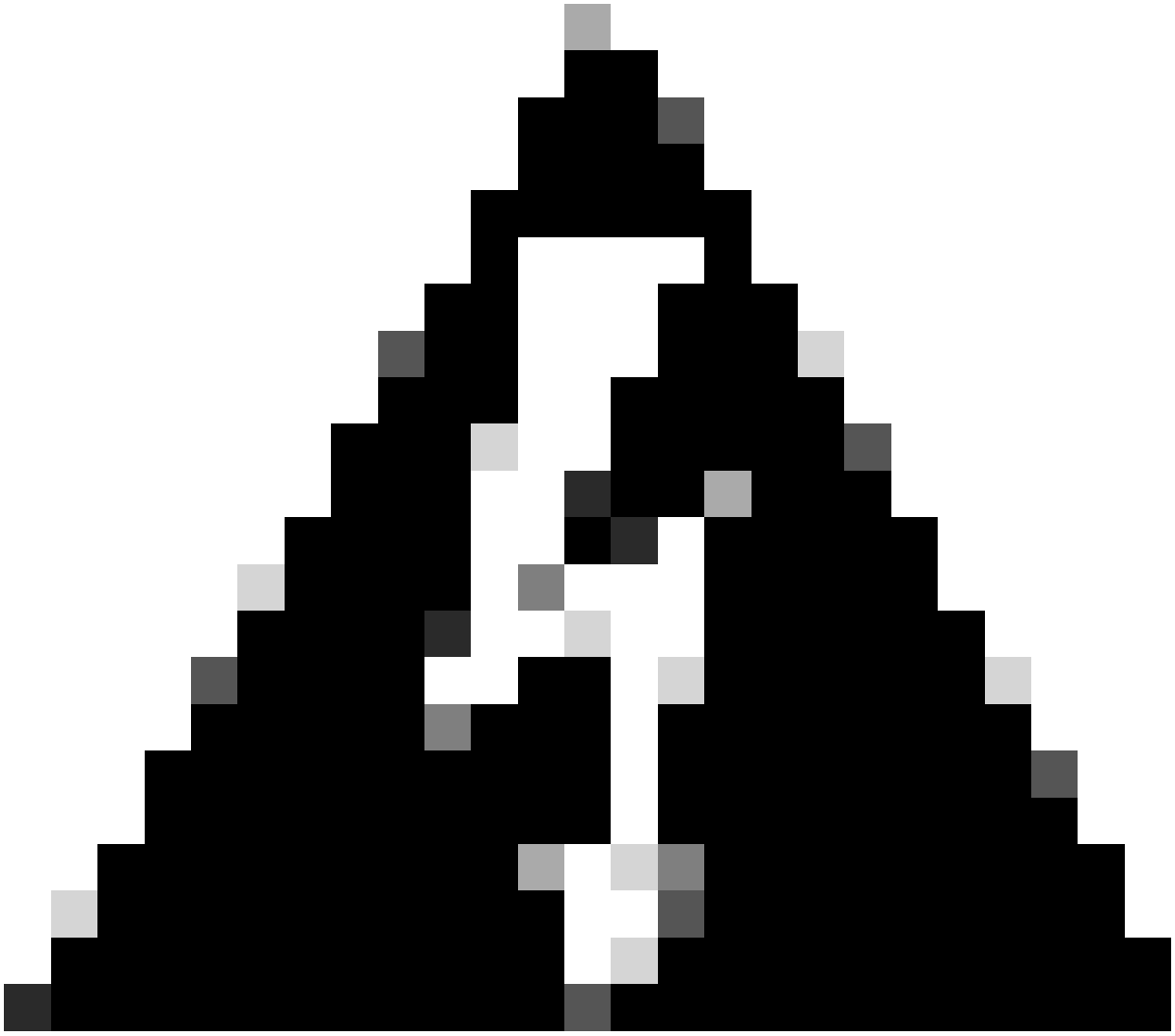


靜態路由配置



注意：VXLAN的目標網路必須透過對等VNI介面傳送。所有VNI介面必須位於同一個廣播域（邏輯網段）上。

第5步：儲存並部署更改。



警告：在部署之前可以看到驗證警告，請確保可以從物理VTEP源介面訪問VTEP對等體IP地址。

驗證

驗證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.
```

檢驗VNI介面配置。

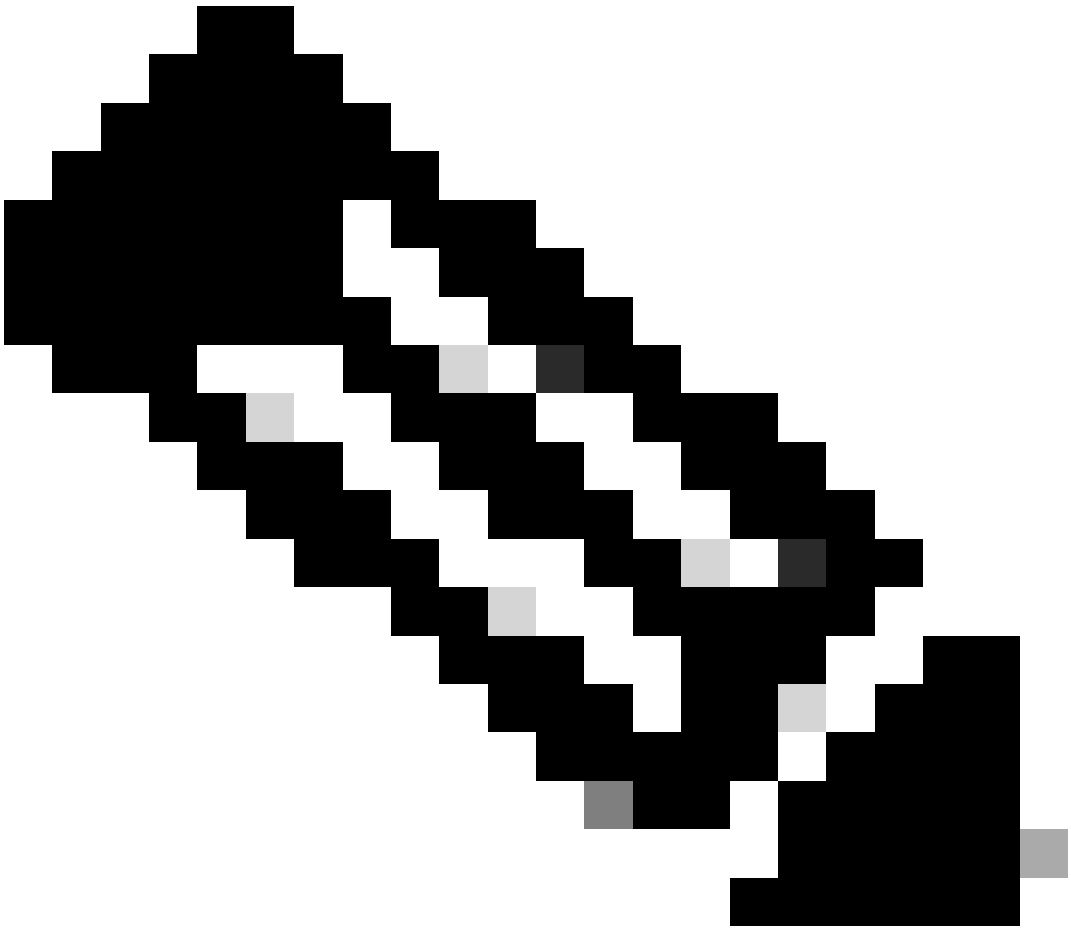
```
firepower# show run interface
interface vni100
segment-id 10001
nameif VNI-1
security-level 0
ip address 172.16.209.1 255.255.255.0
vtep-nve 1
```

驗證VTEP介面上的MTU組態。

```
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]
```

驗證目的網路的靜態路由配置。

```
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：驗證所有對等體上的VNI介面是否配置在同一個廣播域中。

疑難排解

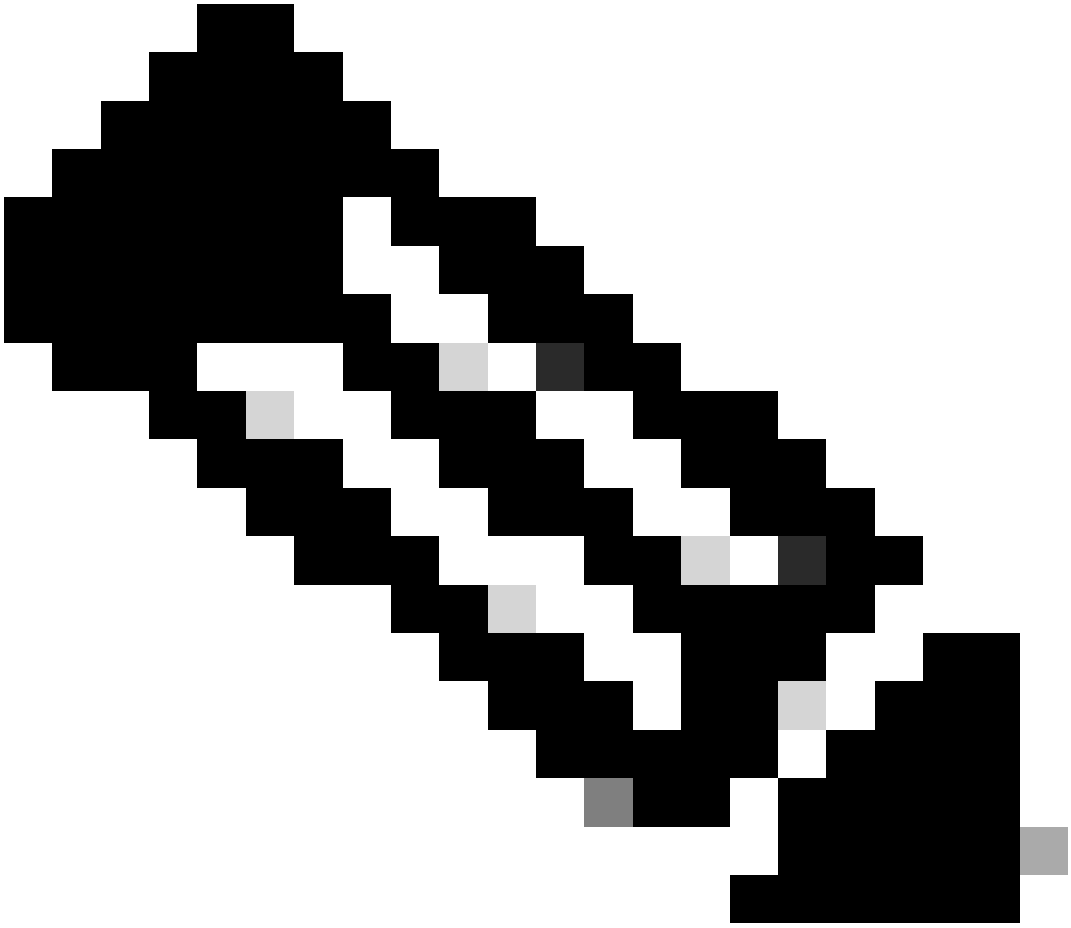
檢查與VTEP對等點的連線。

對等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
```

對等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對等連線問題可能會在安全FMC上生成部署故障。確保與所有VTEP對等配置保持連線。

檢查與VNI對等點的連線。

.

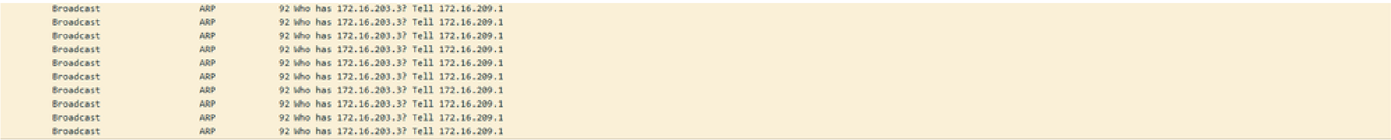
對等1：

```
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
```

對等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
```

有時，配置錯誤的靜態路由可能會生成ARP不完整的輸出。在VTEP介面上為VXLAN資料包配置捕獲並以pcap格式下載，任何資料包分析器工具都可以幫助確認路由是否存在任何問題。確保使用VNI對等體IP地址作為網關。



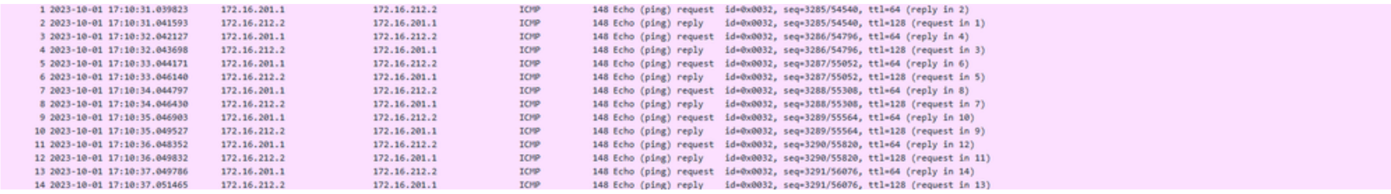
路由問題

在安全FTD上配置ASP丟棄捕獲，以防發生任何防火牆丟棄，請使用show asp drop命令檢查ASP丟棄計數器。聯絡思科TAC進行分析。

確保配置訪問控制策略規則以允許VNI/VTEP介面上的VXLAN UDP流量。

有時VXLAN封包可以分段，請確保在底層網路上將MTU變更為巨型架構以避免分段。

在輸入/VTEP介面上設定擷取，並下載.pcap格式的擷取以供分析。封包必須包括VTEP介面上的VXLAN標頭，



使用VXLAN標頭捕獲的Ping

VXLAN標頭

相關資訊

- [配置VXLAN介面]
- [VXLAN使用案例]

- VXLAN封包處理
- 設定VTEP來源介面
- 配置VNI介面
- 思科技術支援與下載

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。