

Secure FMCを使用したSecure FTDでのVXLANインターフェイスの設定

内容

[はじめに](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[背景説明](#)

[ネットワーク図](#)

[設定](#)

[VTEPピアグループの設定](#)

[VTEP送信元インターフェイスの設定](#)

[VTEP VNIインターフェイスの設定](#)

[確認](#)

[トラブルシューティング](#)

[関連情報](#)

はじめに

このドキュメントでは、Secure Firewall Management Center(FMC)を使用して、Secure Firewall Threat Defense(FTD)のVXLANインターフェイス(VXLAN)を設定する方法について説明します。

前提条件

要件

次の項目について理解しておくことをお勧めします。

- VLAN/VXLANの基本概念。
- ネットワークに関する基本的な知識
- Cisco Secure Management Centerの基本的なエクスペリエンス
- Cisco Secure Firewall Threat Defenseの基本的なエクスペリエンス

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づいています。

- 7.2.4リリースを実行しているCisco Secure Firewall Management Center(FMCv)Virtual VMware。
- 7.2.4リリースを実行しているCisco Secure Firewall Threat Defense(FTDv)仮想アプライア

ンス(VMware)

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、クリアな(デフォルト)設定で作業を開始しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

背景説明

仮想拡張VLAN(VXLAN)は、従来のVLANと同様にイーサネットレイヤ2ネットワークサービスを提供します。仮想環境ではVLANセグメントの需要が高いため、VXLANは拡張性と柔軟性に優れており、また、元のレイヤ2フレームにVXLANヘッダーが追加されてUDP-IPパケットに配置されるMAC-in-UDPカプセル化スキームも定義しています。このMAC-in-UDPカプセル化を使用して、VXLANはレイヤ3ネットワーク経由でレイヤ2ネットワークをトンネリングします。VXLANには次のような利点があります。

- マルチテナントセグメントにおけるVLANの柔軟性：
- より多くのレイヤ2(L2)セグメントに対応できる高い拡張性
- ネットワーク使用率の向上

Cisco Secure Firewall Threat Defense(FTD)は、2種類のVXLANカプセル化をサポートしています。

- VXLAN (すべてのセキュアファイアウォール脅威防御モデルに使用)
- Geneve (セキュアファイアウォール脅威対策の仮想アプライアンスに使用)

Geneveカプセル化は、アマゾンウェブサービス(AWS)ゲートウェイロードバランサーとアプライアンス間のパケットの透過的なルーティング、および追加情報の送信に必要です。

VXLANは、VXLANトンネルエンドポイント(VTEP)を使用して、テナントのエンドデバイスをVXLANセグメントにマッピングし、VXLANのカプセル化とカプセル化解除を実行します。各VTEPには2つのインターフェイスタイプがあります。1つ以上の仮想インターフェイスは、セキュリティポリシーを適用できるVXLANネットワーク識別子(VNI)インターフェイスと、VTEP間でVNIインターフェイスをトンネリングするVTEP送信元インターフェイスと呼ばれる標準インターフェイスです。VTEP送信元インターフェイスは、VTEP間の通信のためにトランスポートIPネットワークに接続されます。VNIインターフェイスはVLANインターフェイスと似ており、タギングを使用してネットワークトラフィックを特定の物理インターフェイス上で分離する仮想インターフェイスです。セキュリティポリシーは各VNIインターフェイスに適用されます。1つのVTEPインターフェイスを追加でき、すべてのVNIインターフェイスは同じVTEPインターフェイスに関連付けられます。AWSでの脅威防御仮想クラスタリングには例外があります。

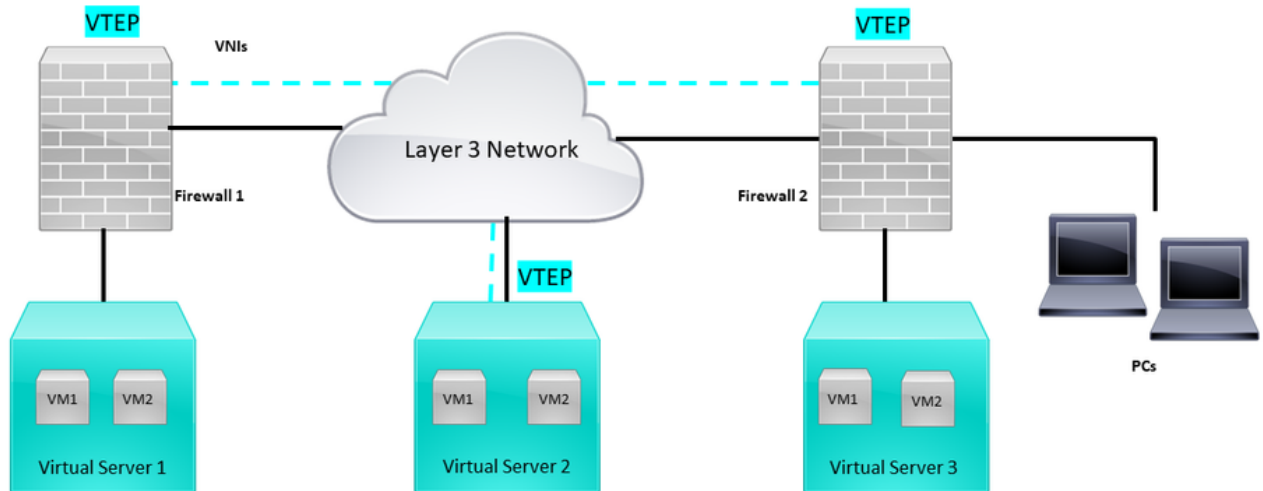
脅威対策では、3つの方法でカプセル化とカプセル化解除を行います。

- 単一ピアのVTEP IPアドレスは、脅威対策に静的に設定できます。
- ピアVTEP IPアドレスのグループは、脅威対策に静的に設定できます。
- マルチキャストグループは、各VNIインターフェイスで設定できます。

このドキュメントでは、2つのピアVTEP IPアドレスのグループが静的に設定されたVXLANカプ

セル化のVXLANインターフェイスに焦点を当てています。Geneveインターフェイスを設定する必要がある場合は、AWSの[Geneveインターフェイス](#)に関する公式ドキュメントを参照するか、[単一のピアまたはマルチキャストグループ](#)でVTEPを設定するか、[単一のピアまたはマルチキャストグループ](#)でVTEPインターフェイスを確認してください。

ネットワーク図



Network Topology

「設定」セクションでは、アンダーレイネットワークがSecure Firewall Management Centerを介して脅威対策にすでに設定されていることを前提としています。このドキュメントでは、オーバーレイネットワーク設定を中心に説明します。

設定

VTEPピアグループの設定

ステップ1: Objects > Object Managementの順に移動します。

Objects

Integration

Object Management

Intrusion Rules

オブジェクト - オブジェクト管理

ステップ2 : 左側のメニューでNetworkをクリックします。

- > 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

NVEのみの設定

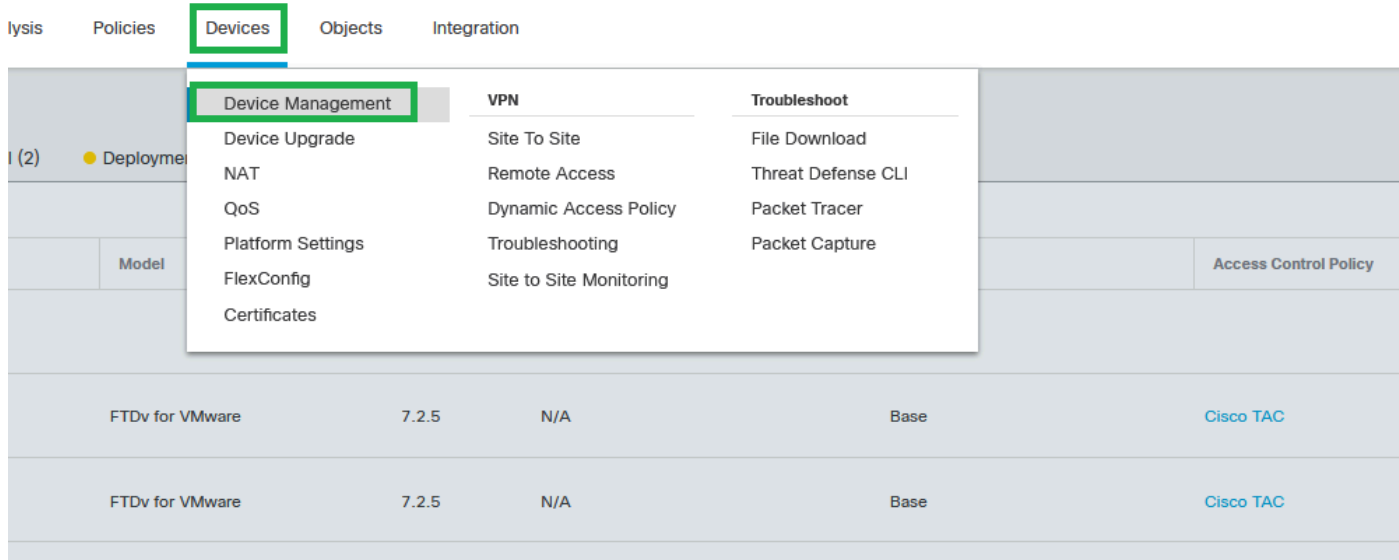


警告：この設定は、このインターフェイスでのみトラフィックをVXLANおよび共通管理トラフィックに制限するルーテッドモードのオプションです。この設定は、トランスペアレントファイアウォールモードに対して自動的に有効になります。

ステップ9：変更を保存します。

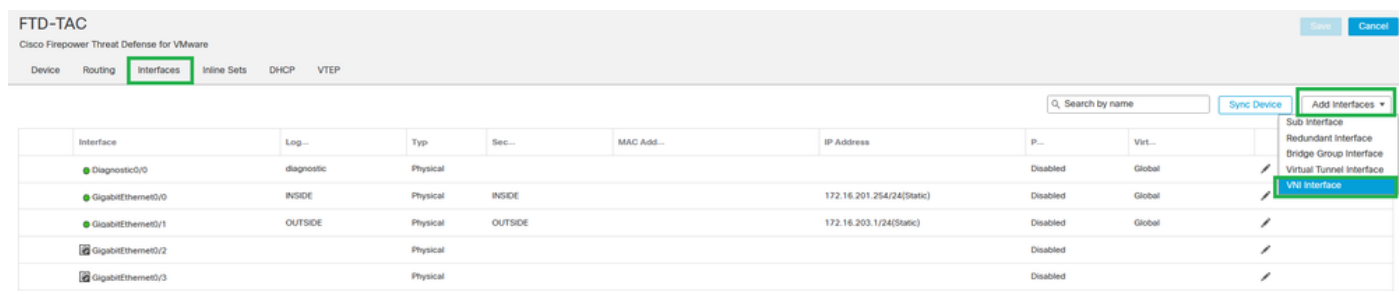
VTEP VNIインターフェイスの設定

ステップ1:Devices > Device Managementの順に移動し、脅威対策を編集します。



デバイス – デバイス管理

ステップ2: Interfacesセクションで、Add Interfaces > VNI Interfacesの順にクリックします。



インターフェイス – インターフェイスの追加 – VNIインターフェイス

ステップ3: Generalセクションで、VNIインターフェイスを名前、説明、セキュリティゾーン、VNI ID、およびVNIセグメントIDで設定します。

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

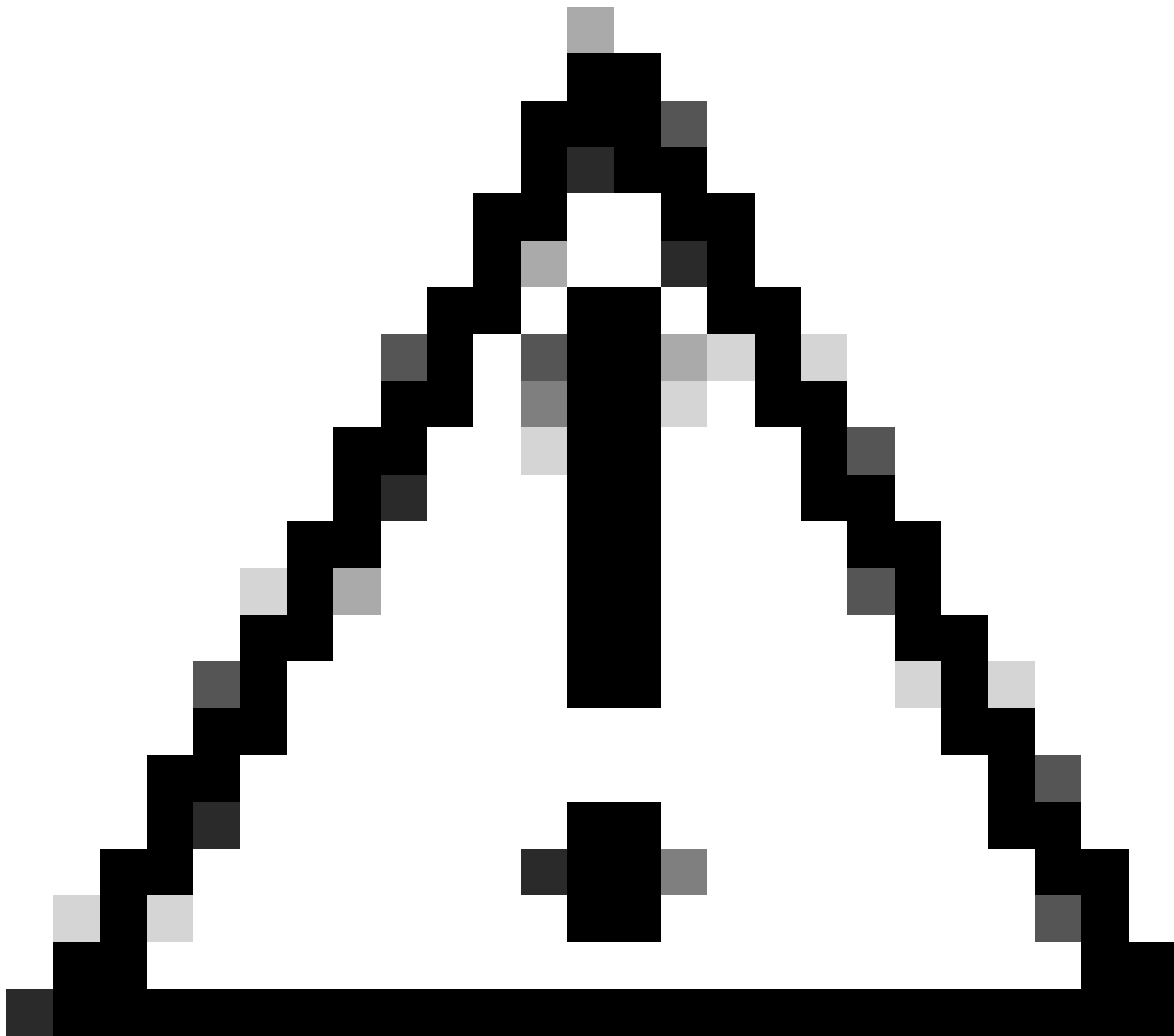
Cancel

OK

VNIインターフェイスの追加



注:VNI IDは1 ~ 10000に設定され、VNIセグメントIDは1 ~ 16777215に設定されます
(セグメントIDはVXLANタギングに使用されます)。



注意：マルチキャストグループがVNIインターフェイスで設定されていない場合、VTEP送信元インターフェイス設定のデフォルトグループが使用されます（使用可能な場合）。VTEP送信元インターフェイスのVTEPピアIPを手動で設定した場合、VNIインターフェイスのマルチキャストグループは指定できません。

ステップ3:NVE Mapped to VTEP Interfaceチェックボックスを選択して、OKをクリックします。

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

VTEPインターフェイスにマッピングされたNVE

手順4:VXLANの宛先ネットワークをVNIピアインターフェイスにアドバタイズするスタティックルートを設定します。Routing > Static Routeの順に選択します。

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

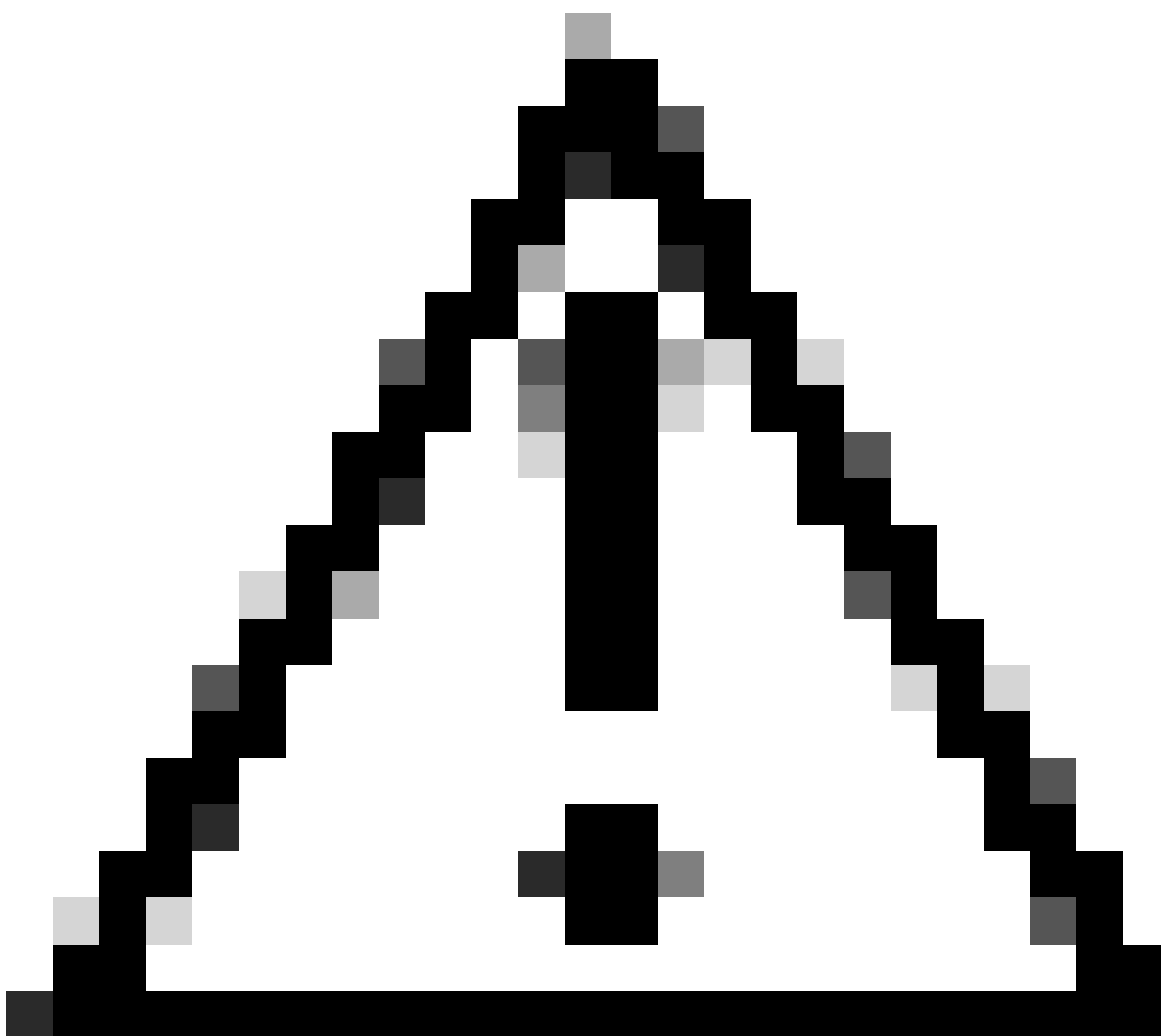
Global

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						

スタティックルートの設定



注意: VXLANの宛先ネットワークは、ピアVNIインターフェイス経由で送信する必要があります。すべてのVNIインターフェイスは、同じブロードキャストドメイン (論理セグメント) 上にある必要があります。

手順5: 変更を保存して展開します。



警告：展開の前に検証の警告が表示される可能性があります。VTEPピアのIPアドレスが物理VTEP送信元インターフェイスから到達可能であることを確認してください。

確認

NVE設定を確認します。

```
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.
```

VNIインターフェイスの設定を確認します。

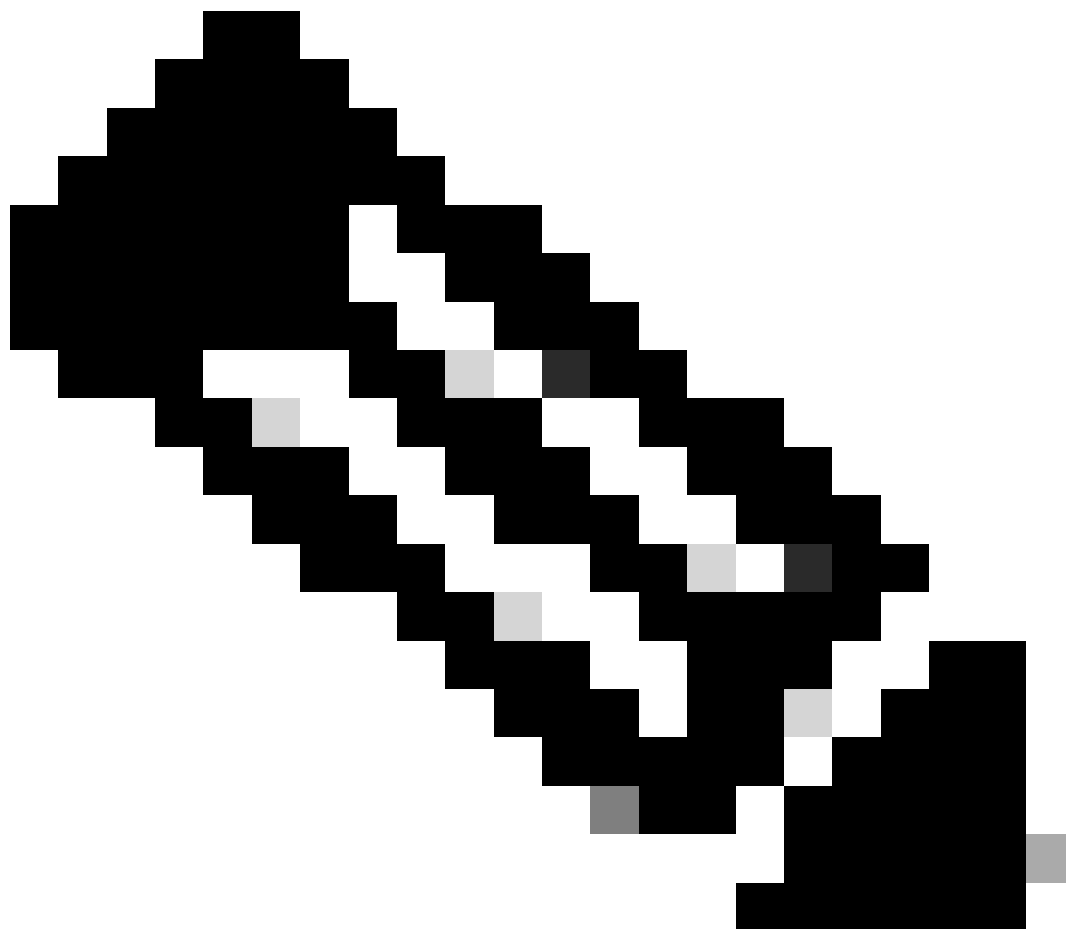
```
firepower# show run interface
interface vni100
segment-id 10001
nameif VNI-1
security-level 0
ip address 172.16.209.1 255.255.255.0
vtep-nve 1
```

VTEPインターフェイスのMTU設定を確認します。

```
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]
```

宛先ネットワークのスタティックルート設定を確認します。

```
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：すべてのピアのVNIインターフェイスが同じブロードキャストドメイン上に設定されていることを確認します。

トラブルシューティング

VTEPピアとの接続をチェックします。

ピア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
```

ピア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:VTEPピア接続の問題により、Secure FMCで導入エラーが発生する可能性があります。すべてのVTEPピア設定への接続が維持されていることを確認します。

VNIピアとの接続をチェックします。

.

ピア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
```

ピア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

```

設定されているスタティックルートが正しくないと、ARPの不完全な出力が生成される場合があります。VXLANパケットのVTEPインターフェイスでキャプチャを設定し、pcap形式でダウンロードします。パケットアナライザツールは、ルートに問題があるかどうかを確認するのに役立ちます。VNIピアのIPアドレスをゲートウェイとして使用していることを確認します。

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
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
Broadcast	ARP	92 who has 172.16.209.3? Tell 172.16.209.1

ルーティング問題

Secure FTDでASPドロップキャプチャを設定する：ファイアウォールのドロップが発生した場合、show asp dropコマンドでASPドロップカウンタを確認します。分析については、Cisco TACにお問い合わせください。

VNI/VTEPインターフェイスでVXLAN UDPトラフィックを許可するようにアクセスコントロールポリシーを設定してください。

VXLANパケットがフラグメント化される可能性がある場合があります。フラグメント化を回避するために、アンダーレイネットワークでMTUをジャンボフレームに変更してください。

入力/VTEPインターフェイスでキャプチャを設定し、分析用に.pcap形式でキャプチャをダウンロードします。パケットには、VTEPインターフェイスのVXLANヘッダーが含まれている必要があります。

1	2023-10-01 17:10:31.039023	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)

VXLANヘッダーでキャプチャされたping

```

> Frame 8: 148 bytes on wire (1184 bits), 148 bytes captured (1184 bits)
> Ethernet II, Src: Vhware_b3:ba:6a (00:50:56:b3:ba:6a), Dst: Vhware_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
> 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: Vhware_b3:ba:6a (00:50:56:b3:ba:6a), Dst: Vhware_b3:26:b8 (00:50:56:b3:26:b8)
    > Destination: Vhware_b3:26:b8 (00:50:56:b3:26:b8)
    > Source: Vhware_b3:ba:6a (00:50:56:b3:ba:6a)
    Type: IPv4 (0x0000)
  > Internet Protocol Version 4, Src: 172.16.212.2, Dst: 172.16.201.1
  > Internet Control Message Protocol

```

VXLANヘッダー

関連情報

- [VXLANインターフェイスの設定](#)
- [VXLANの使用例](#)
- [VXLAN/パケット処理](#)
- [VTEP送信元インターフェイスの設定](#)
- [VNIインターフェイスの設定](#)
- [シスコのテクニカルサポートとダウンロード](#)

翻訳について

シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。