



VXLAN インターフェイス

この章では、仮想拡張 LAN (VXLAN) インターフェイスを設定する方法について説明します。VXLAN は、レイヤ 2 ネットワークを拡張するためにレイヤ 3 物理ネットワーク上のレイヤ 2 仮想ネットワークとして機能します。

- [VXLAN インターフェイスの概要 \(1 ページ\)](#)
- [VXLAN インターフェイスのガイドライン \(7 ページ\)](#)
- [VXLAN インターフェイスのデフォルト設定 \(8 ページ\)](#)
- [VXLAN インターフェイスの設定 \(8 ページ\)](#)
- [VXLAN インターフェイスのモニタリング \(12 ページ\)](#)
- [VXLAN インターフェイスの例 \(15 ページ\)](#)
- [VXLAN インターフェイスの履歴 \(19 ページ\)](#)

VXLAN インターフェイスの概要

VXLAN は、VLAN の場合と同じ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が、より優れた拡張性と柔軟性を備えています。VLAN と比較して、VXLAN には次の利点があります。

- データセンター全体でのマルチテナントセグメントの柔軟な配置。
- より多くのレイヤ 2 セグメント (最大 1600 万の VXLAN セグメント) に対応するための高度なスケーラビリティ。

ここでは、VXLAN の動作について説明します。VXLAN の詳細については、RFC 7348 を参照してください。

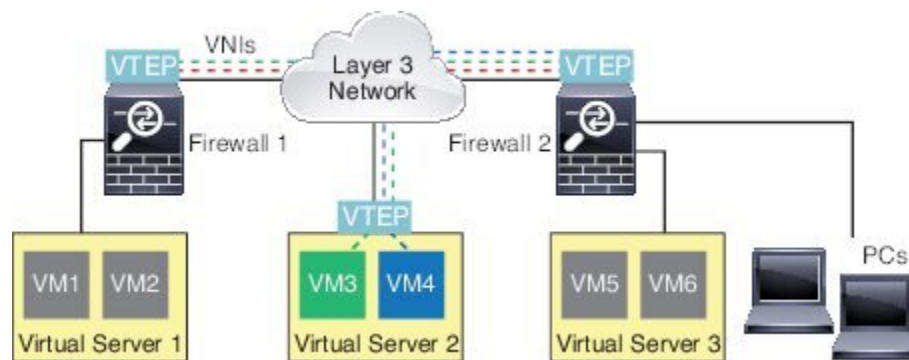
VXLAN カプセル化

VXLAN は、レイヤ 3 ネットワーク上のレイヤ 2 オーバーレイ方式です。VXLAN は、MAC Address-in-User Datagram Protocol (MAC-in-UDP) のカプセル化を使用します。元のレイヤ 2 フレームに VXLAN ヘッダーが追加され、UDP-IP パケットに置かれます。

VXLAN トンネルエンドポイント

VXLAN トンネルエンドポイント (VTEP) デバイスは、VXLAN のカプセル化および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 (セキュリティ ポリシーを適用する VXLAN Network Identifier (VNI) インターフェイスと呼ばれる 1 つ以上の仮想インターフェイスと、VTEP 間に VNI 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通常のインターフェイス) があります。VTEP 送信元インターフェイスは、VTEP 間通信のトランスポート IP ネットワークに接続されます。

次の図に、レイヤ 3 ネットワークで VTEP として機能し、サイト間の VNI 1、2、3 を拡張する 2 つの ASA と仮想サーバ 2 を示します。ASA は、VXLAN と VXLAN 以外のネットワークの間のブリッジまたはゲートウェイとして機能します。



VTEP 間の基盤となる IP ネットワークは、VXLAN オーバーレイに依存しません。カプセル化されたパケットは、発信元 IP アドレスとして開始 VTEP を持ち、宛先 IP アドレスとして終端 VTEP を持っており、外部 IP アドレス ヘッダーに基づいてルーティングされます。宛先 IP アドレスは、リモート VTEP が不明な場合、マルチキャストグループにすることができます。デフォルトでは、宛先ポートは UDP ポート 4789 です (ユーザ設定可能)。

VTEP 送信元インターフェイス

VTEP 送信元インターフェイスは、すべての VNI インターフェイスに関連付けられる予定の標準の ASA インターフェイス (物理、冗長、EtherChannel、または VLAN) です。ASA/セキュリティ コンテキストごとに 1 つの VTEP 送信元インターフェイスを設定できます。

VTEP 送信元インターフェイスは、VXLAN トラフィック専用にすることができますが、その使用に制限されません。必要に応じて、インターフェイスを通常のトラフィックに使用し、そのトラフィックのインターフェイスにセキュリティポリシーを適用できます。ただし、VXLAN トラフィックの場合は、すべてのセキュリティポリシーを VNI インターフェイスに適用する必要があります。VTEP インターフェイスは、物理ポートとしてのみ機能します。

トランスペアレントファイアウォールモードでは、VTEP 送信元インターフェイスは、BVI の一部ではないため、その IP アドレスを設定しません。このインターフェイスは、管理インターフェイスが処理される方法に似ています。

VNI インターフェイス

VNI インターフェイスは VLAN インターフェイスに似ています。VNI インターフェイスは、タグgingを使用して特定の物理インターフェイスでのネットワークトラフィックの分割を維持する仮想インターフェイスです。各VNI インターフェイスにセキュリティポリシーを直接適用します。

追加できる VTEP インターフェイスは1つだけで、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。

VXLAN パケット処理

VTEP 送信元インターフェイスを出入りするトラフィックは、VXLAN 処理、特にカプセル化または非カプセル化の対象となります。

カプセル化処理には、次のタスクが含まれます。

- VTEP 送信元インターフェイスにより、VXLAN ヘッダーが含まれている内部 MAC フレームがカプセル化されます。
- UDP チェックサム フィールドがゼロに設定されます。
- 外部フレームの送信元 IP が VTEP インターフェイスの IP に設定されます。
- 外部フレームの宛先 IP がリモート VTEP IP ルックアップによって決定されます。

カプセル化解除については、次の場合に ASA によって VXLAN パケットのみがカプセル化解除されます。

- これが、宛先ポートが 4789 に設定された UDP パケットである場合（この値はユーザー設定可能です）。
- 入力インターフェイスが VTEP 送信元インターフェイスである場合。
- 入力インターフェイスの IP アドレスが宛先 IP アドレスと同じになります。
- VXLAN パケット形式が標準に準拠します。

ピア VTEP

ASA がピア VTEP の背後にあるデバイスにパケットを送信する場合、ASA には次の 2 つの重要な情報が必要です。

- リモート デバイスの宛先 MAC アドレス
- ピア VTEP の宛先 IP アドレス

ASA は VNI インターフェイスのリモート VTEP IP アドレスに対する宛先 MAC アドレスのマッピングを維持します。

ASA がこの情報を検出するには 2 つの方法があります。

- 単一のピア VTEP IP アドレスを ASA に静的に設定できます。

手動で複数のピアを定義することはできません。

ASA が VXLAN カプセル化 ARP ブロードキャストを VTEP に送信し、エンドノードの MAC アドレスを取得します。

- マルチキャストグループは、VNI インターフェイスごとに（または VTEP 全体に）設定できます。

ASA は、IP マルチキャストパケット内の VXLAN カプセル化 ARP ブロードキャストパケットを VTEP 送信元インターフェイスを経由して送信します。この ARP 要求への応答により、ASA はリモート VTEP の IP アドレスと、リモートエンドノードの宛先 MAC アドレスの両方を取得することができます。

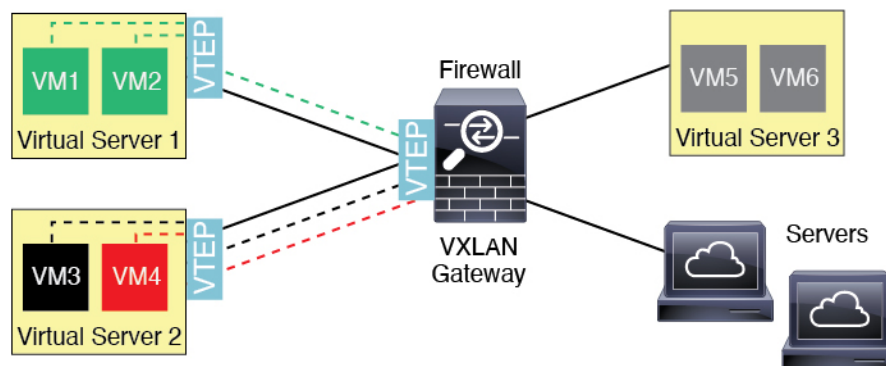
VXLAN 使用例

ここでは、ASA 上への VXLAN の実装事例について説明します。

VXLAN ブリッジまたはゲートウェイの概要

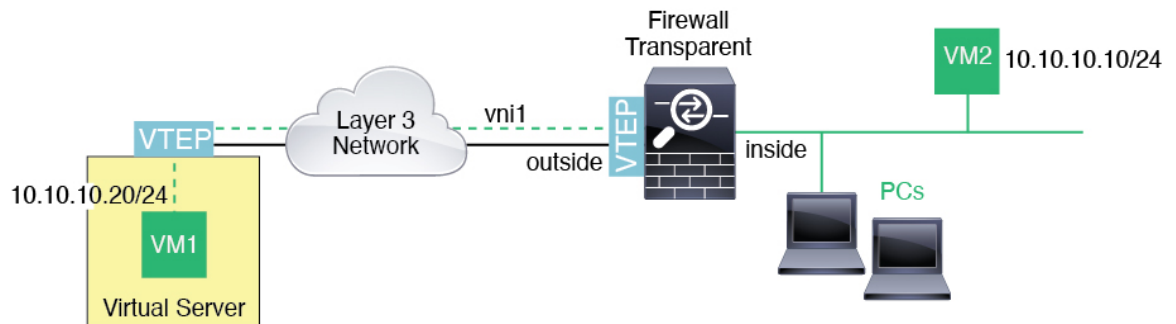
各 ASA の VTEP は、VM、サーバ、PC、VXLAN のオーバーレイ ネットワークなどのエンドノード間のブリッジまたはゲートウェイとして機能します。VTEP 送信元インターフェイスを介して VXLAN カプセル化で受信した受信フレームの場合、ASA は VXLAN ヘッダーを除去して、内部イーサネットフレームの宛先 MAC アドレスに基づいて非 VXLAN ネットワークに接続されている物理インターフェイスに転送します。

ASA は、常に VXLAN パケットを処理します。つまり、他の 2 つの VTEP 間で VXLAN パケットをそのまま転送する訳ではありません。



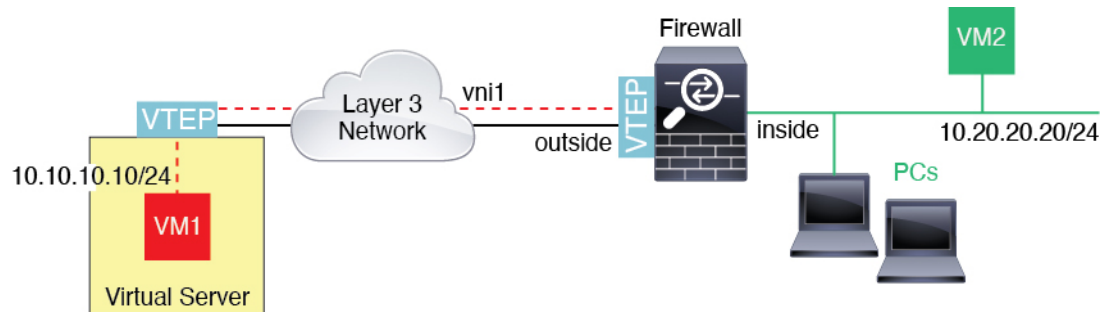
VXLAN ブリッジ

ブリッジグループ（トランスペアレント ファイアウォール モードまたは任意ルーテッドモード）を使用する場合、ASAは、同じネットワークに存在する（リモート）VXLANセグメントとローカルセグメント間のVXLANブリッジとして機能できます。この場合、ブリッジグループのメンバーは通常インターフェイス1つのメンバーが通常のインターフェイスで、もう1つのメンバーがVNIインターフェイスです。



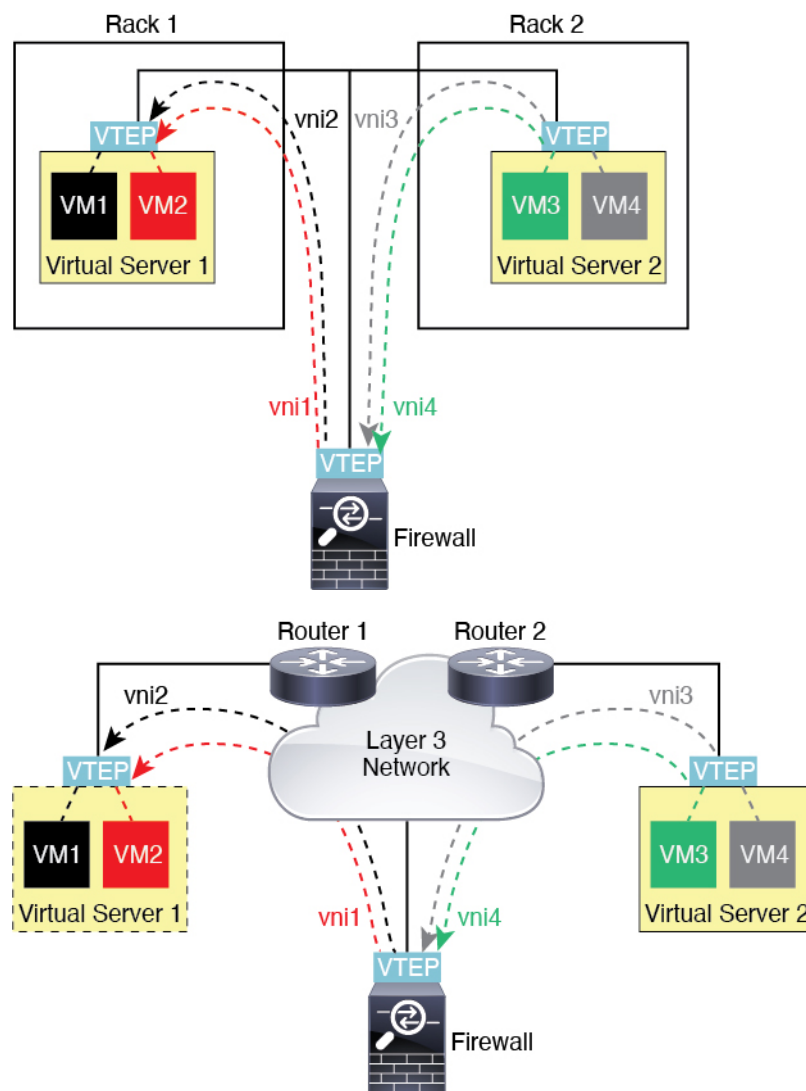
VXLAN ゲートウェイ（ルーテッドモード）

ASAは、VXLAN ドメインと非VXLAN ドメイン間のルータとして機能し、異なるネットワーク上のデバイスを接続します。



VXLAN ドメイン間のルータ

VXLAN 拡張レイヤ2ドメインを使用すると、VMは、ASAが同じラックにないとき、あるいはASAがレイヤ3ネットワーク上の離れた場所にあるときにゲートウェイとしてASAを指し示すことができます。



このシナリオに関する次の注意事項を参照してください。

1. VM3からVM1へのパケットでは、ASAがデフォルトゲートウェイであるため、宛先MACアドレスはASAのMACアドレスです。
2. 仮想サーバー2のVTEP送信元インターフェイスは、VM3からパケットを受信してから、VNI3のVXLANタグでパケットをカプセル化してASAに送信します。
3. ASAは、パケットを受信すると、そのパケットをカプセル化解除して内部フレームを取得します。
4. ASAは、ルートルックアップに内部フレームを使用して、宛先がVNI2上であることを認識します。VM1のマッピングがまだない場合、ASAは、VNI2カプセル化されたARPブロードキャストをVNI2のマルチキャストグループIPで送信します。



(注) このシナリオでは複数の VTEP ピアがあるため、ASA は、複数のダイナミック VTEP ピア ディスカバリを使用する必要があります。

5. ASA は、VNI 2 の VXLAN タグでパケットを再度カプセル化し、仮想サーバ 1 に送信します。カプセル化の前に、ASA は、内部フレームの宛先 MAC アドレスを変更して VM1 の MAC にします (ASA で VM1 の MAC アドレスを取得するためにマルチキャストカプセル化 ARP が必要な場合があります)。
6. 仮想サーバ 1 は、VXLAN パケットを受信すると、パケットをカプセル化解除して内部フレームを VM1 に配信します。

VXLAN インターフェイスのガイドライン

IPv6

- VNI インターフェイスでは、IPv6 トラフィックをサポートしますが、VTEP 送信元インターフェイス IP アドレスでは、IPv4 のみをサポートします。
- IPv6 OSPF インターフェイス設定はサポートされていません。

クラスタリング

- ASA クラスタリングでは、個別インターフェイスモードの VXLAN をサポートしません。Spanned EtherChannel モードでのみ VXLAN をサポートします。

Routing

- VNI インターフェイスでは、スタティック ルーティングまたはポリシー ベース ルーティングのみをサポートします。ダイナミック ルーティング プロトコルはサポートされません。

MTU

- 送信元インターフェイスの MTU が 1554 バイト未満の場合、ASA は自動的に MTU を 1554 バイトに増やします。この場合、イーサネット データグラム全体がカプセル化されるため、新しいパケットのサイズが大きくなるため、より大きな MTU が必要になります。他のデバイスが使用する MTU の方が大きい場合、送信元インターフェイス MTU を、ネットワーク MTU + 54 バイトに設定する必要があります。この MTU は、ジャンボフレーム予約を有効にする必要があります。[ジャンボフレームサポートの有効化 \(ASA モデルと ASAv および ISA 3000\)](#) を参照してください。

モデルのガイドライン

- Firepower 1010 スイッチポートおよび VLAN インターフェイスは、VTEP インターフェイスとしてサポートされていません。

VXLAN インターフェイスのデフォルト設定

デフォルトでは、VNI インターフェイスはイネーブルになっています。

VXLAN インターフェイスの設定

VXLAN を設定するには、次の手順を実行します。

手順

-
- ステップ 1 [VTEP 送信元インターフェイスの設定 \(8 ページ\)](#)。
 - ステップ 2 [VNI インターフェイスの設定 \(10 ページ\)](#)
 - ステップ 3 (オプション) [VXLAN UDP ポートの変更 \(12 ページ\)](#) を使用して無効にすることができます。
-

VTEP 送信元インターフェイスの設定

ASA ごと、またはセキュリティ コンテキストごとに 1 つの VTEP 送信元インターフェイスを設定できます。VTEP は、ネットワーク仮想化エンドポイント (NVE) として定義されます。VXLAN VTEP が現時点でサポートされている唯一の NVE です。

始める前に

マルチ コンテキスト モードでは、この項のタスクをコンテキスト実行スペースで実行してください。設定したいコンテキストを変更するには、**changeto contextname** コマンドを入力します。

手順

-
- ステップ 1 (トランスペアレント モード) 送信元インターフェイスが NVE 専用であることを指定します。

interface id

nve-only

例 :


```
ciscoasa(config)# interface gigabitethernet 1/1
ciscoasa(config-if)# nve-only
```

この設定により、インターフェイスの IP アドレスを設定することができます。このコマンドは、この設定によってトラフィックがこのインターフェイスの VXLAN および共通の管理トラフィックのみに制限されるルーテッドモードではオプションです。

ステップ 2 送信元インターフェイス名と IPv4 アドレスを設定します。

例：

(ルーテッドモード)

```
ciscoasa(config)# interface gigabitethernet 1/1
ciscoasa(config-if)# nameif outside
ciscoasa(config-if)# ip address 10.1.1.1 255.255.255.0
```

例：

(トランスペアレントモード)

```
ciscoasa(config)# interface gigabitethernet 1/1
ciscoasa(config-if)# nve-only
ciscoasa(config-if)# nameif outside
ciscoasa(config-if)# ip address 10.1.1.1 255.255.255.0
```

ステップ 3 NVE インスタンスを指定します。

nve 1

ID 1 で NVE インスタンスを 1 つだけ指定できます。

例：

```
ciscoasa(config)# nve 1
ciscoasa(cfg-nve)#
```

ステップ 4 VXLAN カプセル化を指定します。

encapsulation vxlan

例：

```
ciscoasa(cfg-nve)# encapsulation vxlan
```

ステップ 5 ステップ 2 で設定した送信元インターフェイス名を指定します。

source-interface interface-name

例：

```
ciscoasa(cfg-nve)# source-interface outside
```

(注) 送信元インターフェイスの MTU が 1554 バイト未満の場合、ASA は自動的に MTU を 1554 バイトに増やします。

ステップ 6 (マルチ コンテキスト モード (シングル モードではオプション) 手動でピア VTEP の IP アドレスを指定します。

peer ip *ip_address*

例 :

```
ciscoasa(cfg-nve)# peer ip 10.1.1.2
```

ピア IP アドレスを指定した場合、マルチキャスト グループ ディスカバリは使用できません。マルチキャストは、マルチ コンテキスト モードではサポートされていないため、手動設定が唯一のオプションです。VTEP には 1 つのピアのみを指定できます。

ステップ 7 (オプション、シングルモードのみ) 関連付けられたすべての VNI インターフェイスにデフォルトのマルチキャスト グループを指定します。

default-mcast-group *mcast_ip*

例 :

```
ciscoasa(cfg-nve)# default-mcast-group 236.0.0.100
```

VNI インターフェイスごとにマルチキャスト グループを設定していない場合は、このグループが使用されます。その VNI インターフェイス レベルでグループを設定している場合は、そのグループがこの設定よりも優先されます。

VNI インターフェイスの設定

VNI インターフェイスを追加してそれを VTEP 送信元インターフェイスに関連付けて、基本インターフェイス パラメータを設定します。

手順

ステップ 1 VNI インターフェイスを作成します。

interface vni *vni_num*

例 :

```
ciscoasa(config)# interface vni 1
```

1 ~ 10000 の範囲で ID を設定します。この ID は内部インターフェイス識別子です。

ステップ 2 VXLAN セグメント ID を指定します。

segment-id *id*

例 :

```
ciscoasa(config-if)# segment-id 1000
```

1～16777215 の範囲で ID を設定します。セグメント ID は VXLAN タギングに使用されます。

- ステップ 3** (トランスペアレント モードの場合は必須) このインターフェイスを関連付けるブリッジグループを指定します。

bridge-group *number*

例 :

```
ciscoasa(config-if)# bridge-group 1
```

BVI インターフェイスを設定して通常のインターフェイスをこのブリッジグループに関連付けるには、[のブリッジグループ インターフェイスの設定](#)を参照してください。

- ステップ 4** このインターフェイスを VTEP 送信元インターフェイスに関連付けます。

vtep-nve **1**

- ステップ 5** インターフェイスの名前を指定します。

nameif *vni_interface_name*

例 :

```
ciscoasa(config-if)# nameif vxlan1000
```

name は最大 48 文字のテキスト文字列です。大文字と小文字は区別されません。名前を変更するには、このコマンドで新しい値を再入力します。その名前を参照するすべてのコマンドが削除されるため、**no** 形式は入力しないでください。

- ステップ 6** (ルーテッド モード) IPv4 アドレスと IPv6 アドレスの一方または両方を割り当てます。

ip address {*ip_address* [*mask*] [**standby** *ip_address*] | **dhcp** [**setroute**] | **pppoe** [**setroute**]}**ipv6 address** {**autoconfig** | *ipv6-address/prefix-length* [**standby** *ipv6-address*]}

例 :

```
ciscoasa(config-if)# ip address 192.168.1.1 255.255.255.0 standby 192.168.1.2
ciscoasa(config-if)# ipv6 address 2001:0DB8::BA98:0:3210/48
```

- ステップ 7** セキュリティ レベルを設定します。

security-level *level*

例 :

```
ciscoasa(config-if)# security-level 50
```

number には、0（最下位）～100（最上位）の整数を指定します。

ステップ 8 (シングルモード) マルチキャストグループアドレスを設定します。

mcast-group *multicast_ip*

例：

```
ciscoasa(config-if)# mcast-group 236.0.0.100
```

VNI インターフェイスに対してマルチキャストグループを設定しない場合は、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に対して手動でVTEP ピア IP を設定した場合、VNI インターフェイスに対してマルチキャストグループを指定することはできません。マルチキャストは、マルチコンテキストモードではサポートされていません。

(オプション) VXLAN UDP ポートの変更

デフォルトでは、VTEP 送信元インターフェイスは UDP ポート 4789 への VXLAN トラフィックを受け入れます。ネットワークで標準以外のポートを使用する場合は、それを変更できます。

始める前に

マルチコンテキストモードでは、システム実行スペースで次のタスクを実行します。コンテキストからシステム実行スペースに切り替えるには、**changeto system** コマンドを入力します。

手順

VXLAN UDP ポートを設定します。

vxlan *port number*

例：

```
ciscoasa(config)# vxlan port 5678
```

VXLAN インターフェイスのモニタリング

VTEP インターフェイスおよびVNI インターフェイスをモニターするには、次のコマンドを参照してください。

- **show nve** [*id*] [**summary**]

このコマンドは、NVE インターフェイスのパラメータ、ステータス、および統計情報とキャリア インターフェイス（送信元インターフェイス）のステータス、この NVE を VXLAN VTEP として使用する VNI、ならびにこの NVE インターフェイスに関連付けられているピア VTEP IP アドレスを表示します。**summary** オプションを指定すると、このコマンドは、the status of the NVE インターフェイスのステータス、NVE インターフェイスの背後にある VNI の数、検出された VTEP の数を表示します。

show nve 1 コマンドについては、次の出力を参照してください。

```
ciscoasa# show nve 1
ciscoasa(config-if)# show nve
nve 1, source-interface "inside" is up
IP address 15.1.2.1, subnet mask 255.255.255.0
Encapsulation: vxlan
Encapsulated traffic statistics:
6701004 packets input, 3196266002 bytes
6700897 packets output, 3437418084 bytes
1 packets dropped
Number of configured static peer VTEPs: 0
Number of discovered peer VTEPs: 1
Discovered peer VTEPs:
IP address 15.1.2.3
Number of VNIs attached to nve 1: 2
VNIs attached:
vni 2: segment-id 5002, mcast-group 239.1.2.3
vni 1: segment-id 5001, mcast-group 239.1.2.3
```

show nve 1 summary コマンドについては、次の出力を参照してください。

```
ciscoasa# show nve 1 summary
nve 1, source-interface "inside" is up
Encapsulation: vxlan
Number of configured static peer VTEPs: 0
Number of discovered peer VTEPs: 1
Default multicast group: 239.1.2.3
Number of VNIs attached to nve 1: 2
```

• **show interface vni id [summary]**

このコマンドは、VNI インターフェイスのパラメータ、ステータス、および統計情報と、ブリッジされているインターフェイス（設定されている場合）のステータス、ならびに関連付けられている NVE インターフェイスを表示します。**summary** オプションを指定すると、VNI インターフェイスのパラメータのみが表示されます。

show interface vni 1 コマンドについては、次の出力を参照してください。

```
ciscoasa# show interface vni 1
Interface vni1 "vni-inside", is up, line protocol is up
VTEP-NVE 1
Segment-id 5001
Tag-switching: disabled
MTU: 1500
MAC: aaaa.bbbb.1234
IP address 192.168.0.1, subnet mask 255.255.255.0
Multicast group 239.1.3.3
Traffic Statistics for "vni-inside":
```

```

235 packets input, 23606 bytes
524 packets output, 32364 bytes
14 packets dropped
1 minute input rate 0 pkts/sec, 0 bytes/sec
1 minute output rate 0 pkts/sec, 2 bytes/sec
1 minute drop rate, 0 pkts/sec
5 minute input rate 0 pkts/sec, 0 bytes/sec
5 minute output rate 0 pkts/sec, 0 bytes/sec
5 minute drop rate, 0 pkts/sec

```

show interface vni 1 summary コマンドについては、次の出力を参照してください。

```

ciscoasa# show interface vni 1 summary
Interface vni1 "vni-inside", is up, line protocol is up
VTEP-NVE 1
Segment-id 5001
Tag-switching: disabled
MTU: 1500
MAC: aaaa.bbbb.1234
IP address 192.168.0.1, subnet mask 255.255.255.0
Multicast group not configured

```

• show vni vlan-mapping

このコマンドは、VNIセグメントIDと、VLANインターフェイスまたは物理インターフェイス間のマッピングを表示します。このコマンドは、ルーテッドモードでは、VXLANとVLAN間のマッピングに表示する値を大量に含めることができるため、トランスペアレントファイアウォールモードでのみ有効です。

show vni vlan-mapping コマンドについては、次の出力を参照してください。

```

ciscoasa# show vni vlan-mapping
vni1: segment-id: 6000, interface: 'g0110', vlan 10, interface: 'g0111', vlan 11
vni2: segment_id: 5000, interface: 'g01100', vlan 1, interface: 'g111', vlan 3,
interface: 'g112', vlan 4

```

• show arp vtep-mapping

このコマンドは、リモートセグメントドメインにあるIPアドレスとリモートVTEP IPアドレス用のVNIインターフェイスにキャッシュされたMACアドレスを表示します。

show arp vtep-mapping コマンドについては、次の出力を参照してください。

```

ciscoasa# show arp vtep-mapping
vni-outside 192.168.1.4 0012.0100.0003 577 15.1.2.3
vni-inside 192.168.0.4 0014.0100.0003 577 15.1.2.3

```

• show mac-address-table vtep-mapping

このコマンドは、リモートVTEP IPアドレスが設定されたVNIインターフェイス上のレイヤ2転送テーブル（MACアドレステーブル）を表示します。

show mac-address-table vtep-mapping コマンドについては、次の出力を参照してください。

```

ciscoasa# show mac-address-table vtep-mapping

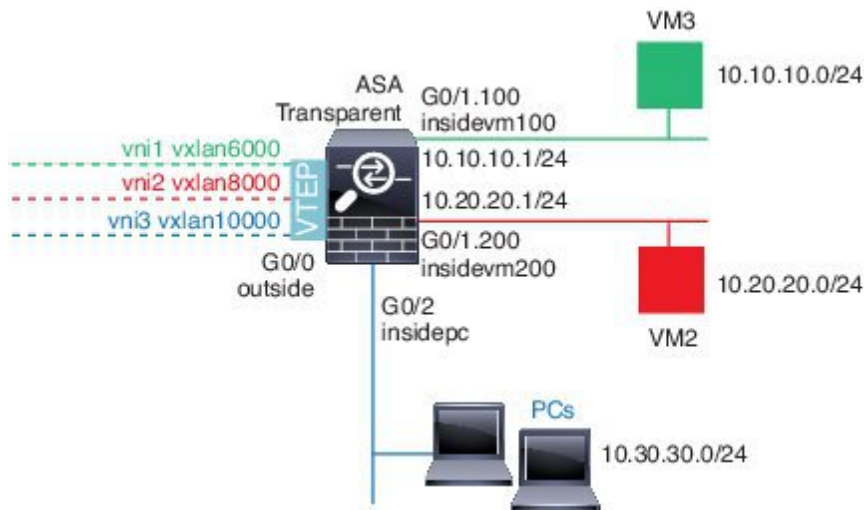
```

interface	mac address	type	Age (min)	bridge-group
VTEP				
vni-outside 10.9.1.3	00ff.9200.0000	dynamic	5	1
vni-inside	0041.9f00.0000	dynamic	5	1 10.9.1.3

VXLAN インターフェイスの例

次の VXLAN の設定例を参照してください。

トランスペアレント VXLAN ゲートウェイの例



この例の次の説明を参照してください。

- GigabitEthernet 0/0 の外部インターフェイスは、VTEP 送信元インターフェイスとして使用され、レイヤ 3 ネットワークに接続されます。
- GigabitEthernet 0/1.100 の insidevm100 VLAN サブインターフェイスは、VM3 が存在する 10.10.10.0/24 ネットワークに接続されます。VM3 が VM1 と通信する場合（表示されません。両方とも、10.10.10.0/24 の IP アドレスを持つ）、ASA は VXLAN タグ 6000 を使用します。
- GigabitEthernet 0/1.200 の insidevm200 VLAN サブインターフェイスは、VM2 が存在する 10.20.20.0/24 ネットワークに接続されます。VM2 が VM4 と通信する場合（表示されません。両方とも、10.20.20.0/24 の IP アドレスを持つ）、ASA は VXLAN タグ 8000 を使用します。
- GigabitEthernet 0/2 の insidepc インターフェイスは、数台の PC が存在する 10.30.30.0/24 ネットワークに接続されます。それらの PC が、同じネットワーク（すべて 10.30.30.0/24 の IP

アドレスを持つ) に属するリモート VTEP の裏の VMs/PCs (表示されません) と通信する場合、ASA は VXLAN タグ 10000 を使用します。

ASA の設定

```
firewall transparent
vxlan port 8427
!
interface gigabitethernet0/0
  nve-only
  nameif outside
  ip address 192.168.1.30 255.255.255.0
  no shutdown
!
nve 1
  encapsulation vxlan
  source-interface outside
!
interface vni1
  segment-id 6000
  nameif vxlan6000
  security-level 0
  bridge-group 1
  vtep-nve 1
  mcast-group 235.0.0.100
!
interface vni2
  segment-id 8000
  nameif vxlan8000
  security-level 0
  bridge-group 2
  vtep-nve 1
  mcast-group 236.0.0.100
!
interface vni3
  segment-id 10000
  nameif vxlan10000
  security-level 0
  bridge-group 3
  vtep-nve 1
  mcast-group 236.0.0.100
!
interface gigabitethernet0/1.100
  nameif insidevm100
  security-level 100
  bridge-group 1
!
interface gigabitethernet0/1.200
  nameif insidevm200
  security-level 100
  bridge-group 2
!
interface gigabitethernet0/2
  nameif insidepc
  security-level 100
  bridge-group 3
!
interface bvi 1
  ip address 10.10.10.1 255.255.255.0
!
interface bvi 2
```



```

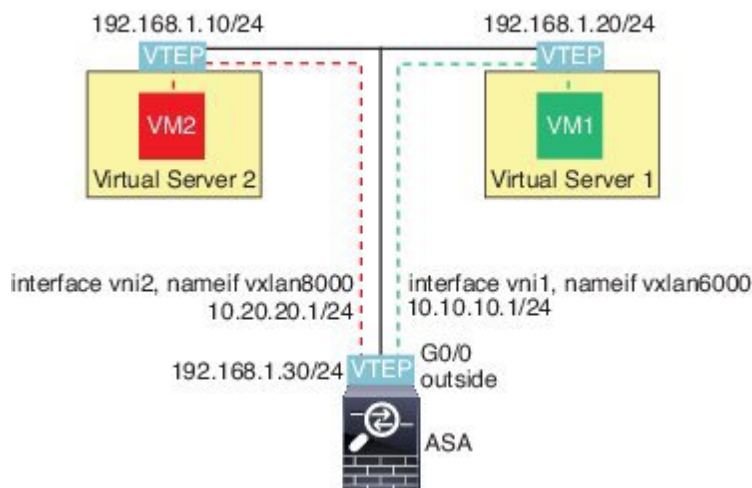
ip address 10.20.20.1 255.255.255.0
!
interface bvi 3
ip address 10.30.30.1 255.255.255.0

```

注意

- VNI インタフェース `vni1` と `vni2` の場合、カプセル化時に内部 VLAN タグが削除されま
す。
- VNI インタフェース `vni2` と `vni3` は、マルチキャストでカプセル化された ARP に対し
て同じマルチキャスト IP アドレスを共有します。この共有は許可されます。
- ASA は、上記の BVI とブリッジグループ設定に基づいて VXLAN トラフィックを非 VXLAN
でサポートされているインターフェイスにブリッジします。拡張されたレイヤ 2 ネット
ワークの各セグメント (10.10.10.0/24、10.20.20.0/24、10.30.30.0/24) の場合、ASA はブ
リッジとして機能します。
- 複数の VNI または複数の通常のインターフェイス (VLAN または単に物理インターフェ
イス) をブリッジグループに設定できます。VXLAN セグメント ID から VLAN ID (物理
インターフェイス) の転送または関連付けは、宛先 MAC アドレスによって決定され、ど
ちらかのインターフェイスが宛先に接続されます。
- VTEP 送信元インターフェイスは、インターフェイス設定で `nve-only` によって示されるト
ランスペアレントファイアウォールモードのレイヤ 3 インターフェイスです。VTEP 送信
元インターフェイスは、BVI インターフェイスまたは管理インターフェイスではありません
が、IP アドレスがあり、ルーティングテーブルを使用します。

VXLAN ルーティングの例



この例の次の説明を参照してください。

- VM1 (10.10.10.10) は仮想サーバー 1 にホストされ、VM2 (10.20.20.20) は仮想サーバー 2 にホストされます。
- VM1 のデフォルト ゲートウェイは ASA であり、仮想サーバー 1 と同じのポッドにありませんが、VM1 はそれを認識しません。VM1 は、そのデフォルト ゲートウェイの IP アドレスが 10.10.10.1 であることだけを認識します。同様に、VM2 はデフォルト ゲートウェイの IP アドレスが 10.20.20.1 であることだけを認識します。
- 仮想サーバー 1 および 2 の VTEP サポート型ハイパーバイザは、同じサブネットまたはレイヤ 3 ネットワーク (表示なし。この場合、ASA と仮想サーバーのアップリンクに異なるネットワーク アドレスがある) 経由で ASA と通信できます。
- VM1 のパケットは、そのハイパーバイザの VTEP によってカプセル化され、VXLAN トンネリングを使用してそのデフォルト ゲートウェイに送信されます。
- VM1 がパケットを VM2 に送信すると、パケットはその観点からデフォルト ゲートウェイ 10.10.10.1 を介して送信されます。仮想サーバー 1 は 10.10.10.1 がローカルにないことを認識しているので、VTEP は VXLAN 経由でパケットをカプセル化し、ASA の VTEP に送信します。
- ASA で、パケットはカプセル化解除されます。VXLAN セグメント ID は、カプセル化解除時に取得されます。次に、ASA は、VXLAN セグメント ID に基づいて、VNI インターフェイス (vni1) に対応する内部フレームを再投入します。その後、ASA はルートルックアップを実行し、別の VNI インターフェイス (vni2) 経由で内部パケットを送信します。vni2 を経由するすべての出力パケットは、VXLAN セグメント 8000 でカプセル化され、VTEP 経由で外部に送信されます。
- 最後に、カプセル化されたパケットが仮想サーバー 2 の VTEP によって受信され、カプセル化解除され、VM2 に転送されます。

ASA の設定

```
interface gigabitethernet0/0
  nameif outside
  ip address 192.168.1.30 255.255.255.0
  no shutdown
!
nve 1
  encapsulation vxlan
  source-interface outside
  default-mcast-group 235.0.0.100
!
interface vni1
  segment-id 6000
  nameif vxlan6000
  security-level 0
  vtep-nve 1
  ip address 10.20.20.1 255.255.255.0
!
interface vni2
  segment-id 8000
  nameif vxlan8000
  security-level 0
  vtep-nve 1
```

```
ip address 10.10.10.1 255.255.255.0  
!
```

VXLAN インターフェイスの履歴

表 1: VXLAN インターフェイスの履歴

機能名	リリース	機能情報
VXLAN のサポート	9.4(1)	<p>VXLAN のサポートが追加されました (VXLAN トンネルエンドポイント (VTEP) のサポートを含む)。ASA またはセキュリティ コンテキストごとに 1 つの VTEP 送信元インターフェイスを定義できます。</p> <p>次のコマンドが導入されました。 debug vxlan、default-mcast-group、encapsulation vxlan、inspect vxlan、interface vni、mcast-group、nve、nve-only、peer ip、segment-id、show arp vtep-mapping、show interface vni、show mac-address-table vtep-mapping、show nve、show vni vlan-mapping、source-interface、vtep-nve、vxlan port</p>

翻訳について

このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。