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

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。Geneve の詳細については、RFC 8926 を参照してください。

カプセル化

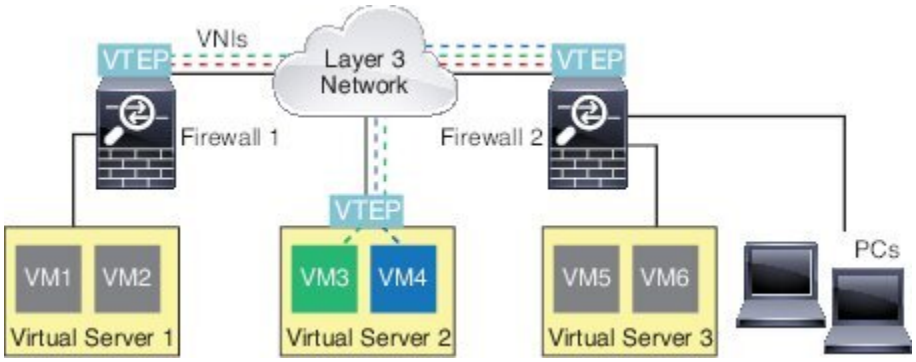
ASA は、次の 2 種類の VXLAN カプセル化をサポートしています。

- VXLAN（すべてのモデル）：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。
- Geneve（ASA 仮想 のみ）：Geneve には、MAC アドレスに限定されない柔軟な内部ヘッダーがあります。Geneve カプセル化は、Amazon Web Services（AWS）ゲートウェイロードバランサ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 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。VXLAN カプセル化の場合：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。Geneve では、ASA はスタティックピアのみをサポートします。デフォルトでは、 VXLAN の宛先ポートは UDP ポート 4789 です（ユーザ設定可能）。Geneve の宛先ポートは 6081 です。

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、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。設定できる VTEP

送信元インターフェイスは1つだけであるため、VXLANインターフェイスとGeneveインターフェイスの両方を同じデバイスに設定することはできません。AWS または Azure での ASA 仮想クラスタリングには例外があり、2 つの VTEP ソースインターフェイスを使用することができます。VXLANインターフェイスはクラスタ制御リンクに使用され、Geneve（AWS）またはVXLAN（Azure）インターフェイスはゲートウェイロードバランサに使用できます。

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、タギング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。AWS または Azure での ASA Virtual クラスタリングには例外があります。AWS クラスタリングの場合、2 つの VTEP ソースインターフェイスを使用することができます。VXLAN インターフェイスはクラスタ制御リンクに使用され、Geneve インターフェイスは AWS ゲートウェイロードバランサに使用できます。Azure クラスタリングの場合、2 つの VTEP ソースインターフェイスを使用することができます。VXLANインターフェイスはクラスタ制御リンクに使用され、2 つ目の VXLAN インターフェイスは Azure ゲートウェイロードバランサに使用できます。

VXLAN パケット処理

VXLAN

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。

Geneve

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、Geneve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、Geneve 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 には、設定したピア IP アドレスが設定されます。

カプセル化解除については、次の場合にASAによってGeneve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 6081 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。
- Geneve 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。

VXLAN ピア

ASA がこの情報を検出するには 2 つの方法あります。

- 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。

  IPv4 の場合：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。

  IPv6 の場合：ASA は IPv6 ネイバー要請メッセージを IPv6 要請ノード マルチキャスト アドレスに送信します。ピア VTEP は、そのリンクローカルアドレスを使用して IPv6 ネイバー アドバタイズメント メッセージで応答します。

- 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。

（注） このオプションは、Geneve ではサポートされていません。

  IPv4 の場合：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。

  IPv6 の場合：ASA は、VTEP 送信元インターフェイスを経由してマルチキャストリスナー検出（MLD）レポートメッセージを送信し、ASA が VTEP インターフェイスでマルチキャスト アドレス トラフィックをリッスンしていることを示します。

Geneve ピア

ASA 仮想 は、静的に定義されたピアのみをサポートします。AWS ゲートウェイロードバランサで ASA 仮想 ピアの IP アドレスを定義できます。ASA 仮想 はゲートウェイロードバランサへのトラフィックを開始しないため、ASA 仮想 でゲートウェイロードバランサの IP アドレスを指定する必要はありません。Geneve トラフィックを受信すると、ピア IP アドレスを学習します。マルチキャストグループは、Geneve ではサポートされていません。

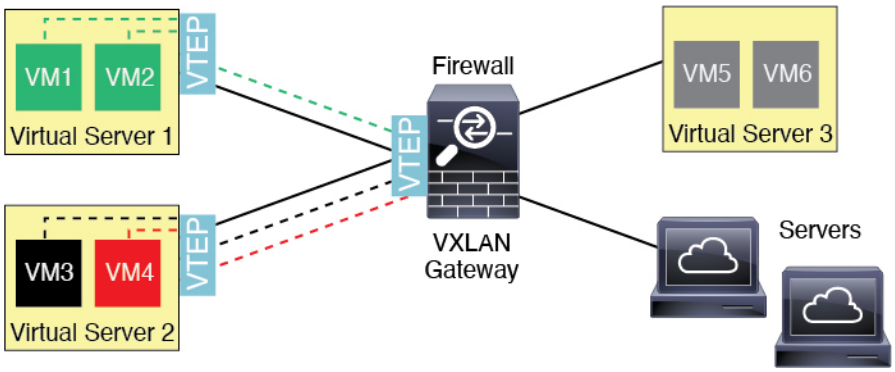
VXLAN 使用例

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

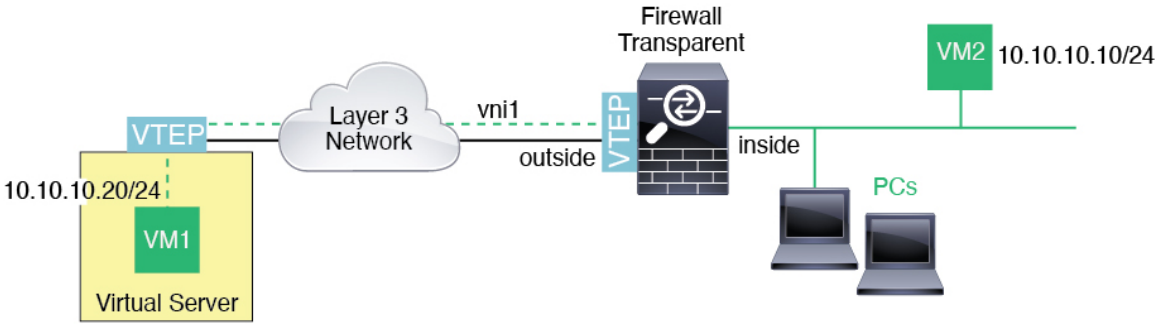
各 ASA の VTEP は、VM、サーバ、PC、VXLANのオーバーレイ ネットワークなどのエンドノード間のブリッジまたはゲートウェイとして機能します。VTEP 送信元インターフェイスを介して VXLAN カプセル化で受信した受信フレームの場合、ASA は VXLAN ヘッダーを除去して、内部イーサネット フレームの宛先 MAC アドレスに基づいて非 VXLAN ネットワークに接続されている物理インターフェイスに転送します。

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。



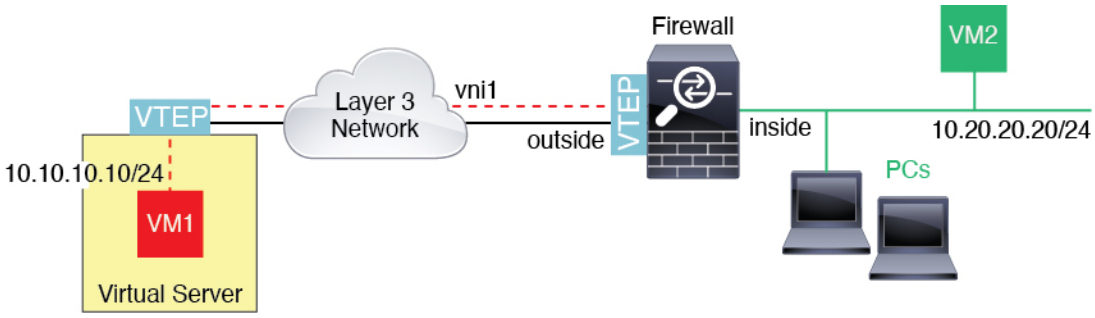
VXLAN ブリッジ

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。



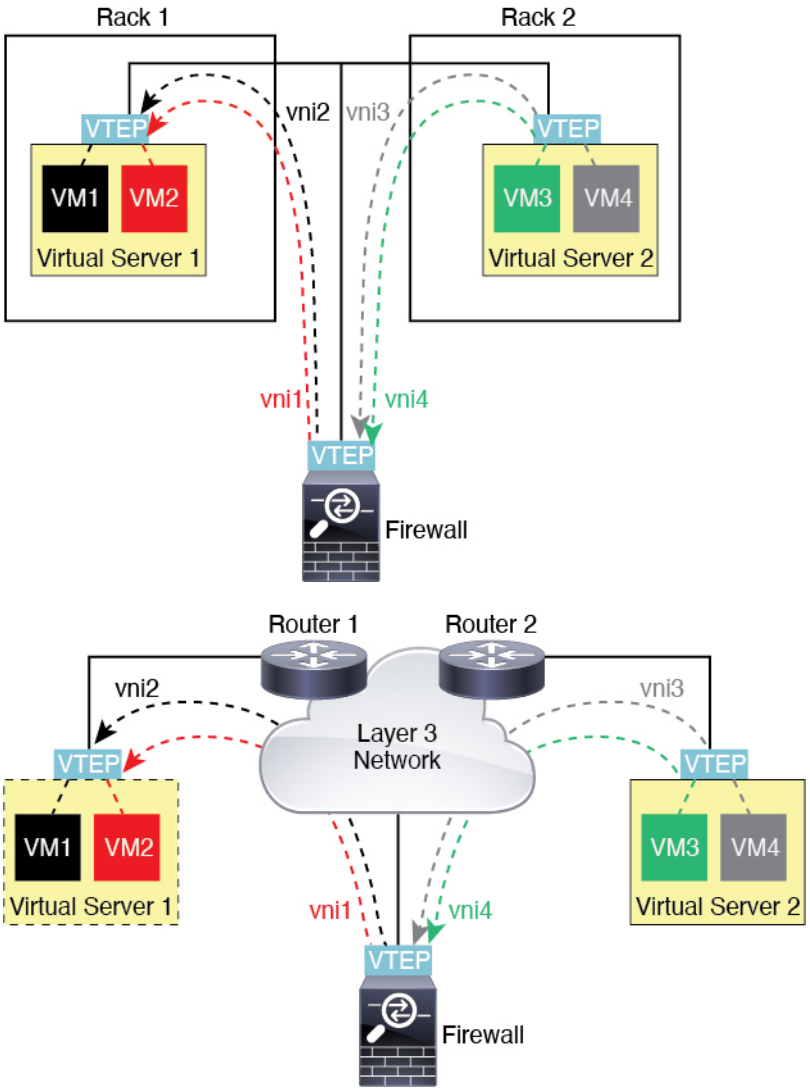
VXLAN ゲートウェイ（ルーテッド モード）

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sの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、VNI 3 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 VNI 2 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、VNI 2 カプセル化された ARP ブロードキャストを VNI 2 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。

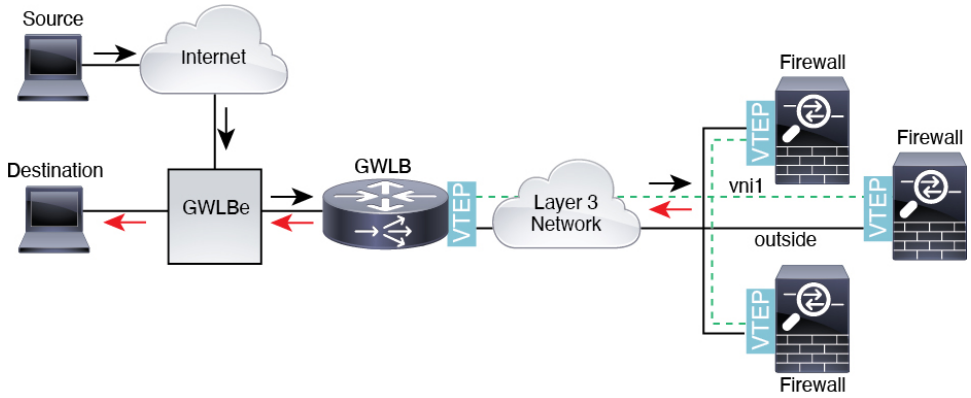
5. ASA は、VNI 2 の VXLAN タグでパケットを再度カプセル化し、仮想サーバ 1 に送信します。カプセル化の前に、ASA は、内部フレームの宛先 MAC アドレスを変更して VM1 の MAC にします（ASA で VM1 の MAC アドレスを取得するためにマルチキャスト カプセル化 ARP が必要な場合があります）。
6. 仮想サーバー 1 は、VXLAN パケットを受信すると、パケットをカプセル化解除して内部フレームを VM1 に配信します。

AWS ゲートウェイロードバランサおよび Geneve シングルアームプロキシ

（注） この使用例は、現在サポートされている Geneve インターフェイスの唯一の使用例です。

AWS ゲートウェイロードバランサは、透過的なネットワークゲートウェイと、トラフィックを分散し、仮想アプライアンスをオンデマンドで拡張するロードバランサを組み合わせます。Cisco ASA Virtual は、分散データプレーン（ゲートウェイ ロード バランサ エンドポイント）を備えたゲートウェイロードバランサ集中型コントロールプレーンをサポートします。次の図は、ゲートウェイロードバランサのエンドポイントからゲートウェイロードバランサに転送されるトラフィックを示しています。ゲートウェイロードバランサは、複数の Cisco ASA Virtual の間でトラフィックのバランスをとり、トラフィックをドロップするか、ゲートウェイロードバランサに送り返す（U ターントラフィック）前に検査します。ゲートウェイロードバランサは、トラフィックをゲートウェイロードバランサのエンドポイントと宛先に送り返します。

図 *1: Geneve* シングルアームプロキシ



AWS ゲートウェイロードバランサおよび Geneve デュアルアームプロキシ

（注） この使用例は、現在サポートされている Geneve インターフェイスの唯一の使用例です。

Cisco ASA Virtual は、シングルアームまたはデュアルアームモードの分散データプレーン（ゲートウェイ ロード バランサ エンドポイント）を備えたゲートウェイロードバランサ集中型コントロールプレーンをサポートします。次の図は、GWLB および GWLB エンドポイントへのトラフィックホップを必要とせずに宛先（インターネット）に直接転送されるアウトバウンドトラフィック（Cisco ASA Virtual によって検査されるトラフィック）を示しています。 Cisco ASA Virtual はアウトバウンドを検査し、トラフィックの NAT を実行してから、トラフィックをドロップするか、NAT ゲートウェイを介してインターネットに送り返します。デュアルアームプロキシは、マルチ VPC 展開に共通の出力パスを提供します。ファイアウォールは、複数の VPC からのアウトバウンドトラフィックを検査し、トラフィックは単一のポイントからインターネットに出るため、費用対効果の高いインフラストラクチャ ソリューションです。

図 *2 : Geneve* デュアルアームプロキシ：単一 *VPC* からの出力トラフィック

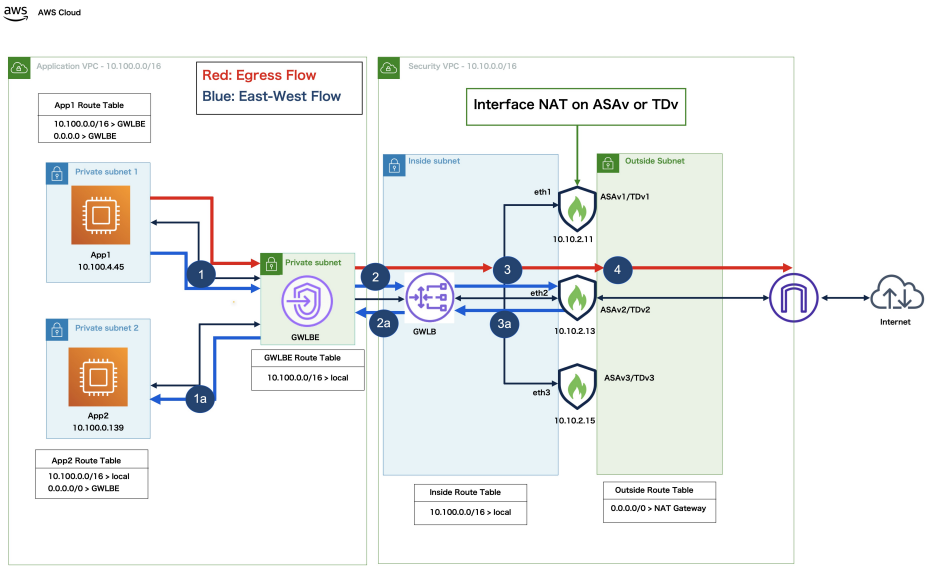
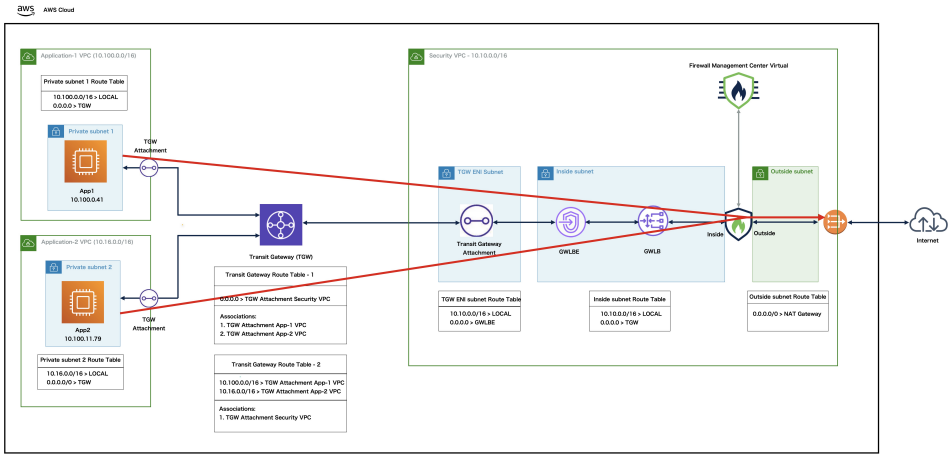


図 *3 : Geneve* デュアルアームプロキシ：複数の *VPC* からの出力トラフィック



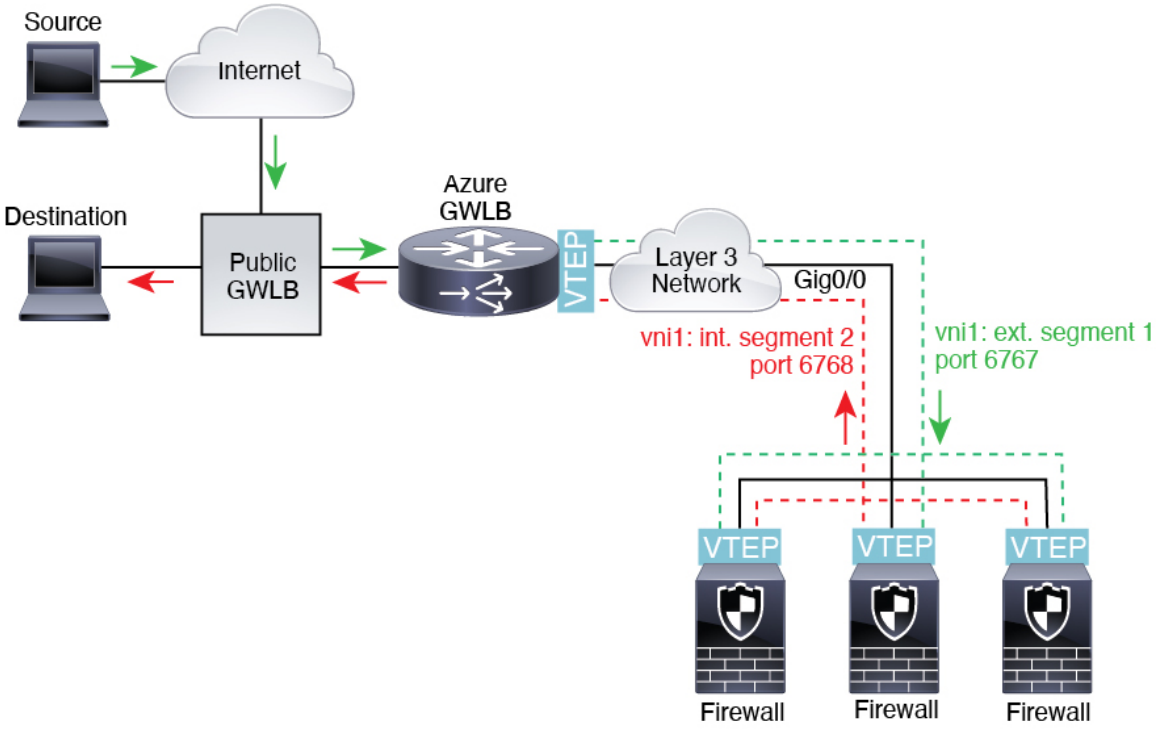
Azure ゲートウェイロードバランサおよびペアプロキシ

Azure サービスチェーンでは、Cisco ASA Virtual がインターネットと顧客サービス間のパケットをインターセプトできる透過的なゲートウェイとして機能します。Cisco ASA Virtual は、ペアリングされたプロキシの VXLAN セグメントを利用して、単一の NIC に外部インターフェイスと内部インターフェイスを定義します。

次の図は、外部 VXLAN セグメント上のパブリックゲートウェイロードバランサから Azure ゲートウェイロードバランサに転送されるトラフィックを示しています。ゲートウェイロードバランサは、複数の Cisco ASA Virtual の間でトラフィックのバランスをとり、トラフィックをドロップするか、外部 VXLAN セグメント上のゲートウェイロードバランサに送り返す前に検

査します。Azure ゲートウェイロードバランサは、トラフィックをパブリックゲートウェイロードバランサと宛先に送り返します。

図 *4 :* ペアリングされたプロキシを使用した *Azure Gateway* ロードバランサ



VXLAN インターフェイスの要件と前提条件

モデルの要件

- Firepower 1010 および Cisco Secure Firewall 1210/1220：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。
- Geneve カプセル化は、Amazon Web Services（AWS）の ASAv30、ASAv50、ASAv100 のモデルでサポートされています。
- ペアプロキシモードの VXLAN は、次のモデルでサポートされています。
  - Azure での ASA Virtual

VXLAN インターフェイスのガイドライン

ファイアウォール モード

- Geneve インターフェイスは、ルーテッド ファイアウォール モードでのみサポートされています。
- ペアプロキシの VXLAN インターフェイスは、ルーテッド ファイアウォール モードでのみサポートされています。

IPv6

- VNI インターフェイスは、IPv4 と IPv6 の両方のトラフィックをサポートします。
- VXLAN カプセル化の場合、VTEP 送信元インターフェイスは IPv4 と IPv6 の両方をサポートします。ASA 仮想 クラスタ制御リンクの VTEP 送信元インターフェイスは、IPv4 のみをサポートします。

  Geneve の場合、VTEP 送信元インターフェイスは IPv4 のみをサポートします。

クラスタリングとマルチコンテキストモード

- ASA クラスタリングは、クラスタ制御リンク（ASA 仮想 のみ）を除いて、個別インターフェイスモードの VXLAN をサポートしません。スパンド EtherChannel モードでのみ VXLAN をサポートしています。

  GWLB で使用する追加の Geneve インターフェイスを使用できる AWS の ASA 仮想 と、GWLB で使用する追加のペアプロキシの VXLAN インターフェイスを使用できる Azure の場合は例外です。

- Geneve インターフェイスは、のシングルコンテキストモードでのみサポートされます。マルチコンテキストモードではサポートされません。

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。

VPN

VPN に VTEP 送信元インターフェイスを構成したり、VTI として使用したりすることはできません。

MTU

- VXLAN カプセル化：送信元インターフェイスの MTU が 1554 バイト未満（IPv4 の場合）または 1574 バイト未満（IPv6 の場合）の場合、ASA は自動的に MTU を増やします。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（IPv4 の場合）または＋64 バイト（IPv6 の場合）に設定する必要があります。この MTU は、一部のフレームでジャンボ 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 仮想、ISA 3000） を参照してください。
- Geneve カプセル化：送信元インターフェイスの MTU が 1806 バイト未満の場合、ASA は自動的に MTU を 1806 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+306バイトに設定する必要があります。このMTUは、一部のフレームでジャンボ 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 仮想、ISA 3000） を参照してください。

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。

（注） VXLAN または Geneve を設定できます（ASA 仮想 のみ）。Geneve インターフェイスについては、Geneve インターフェイスの設定 （16 ページ）を参照してください。

手順

ステップ 1 VTEP 送信元インターフェイスの設定 （14 ページ）を使用して無効にすることができます。
ステップ 2 VNI インターフェイスの設定 （15 ページ）
ステップ 3 （Azure GWLB）ゲートウェイロードバランサのヘルスチェックの許可 （18 ページ）。

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。Azure のASA 仮想 でのクラスタリングには例外があり、1 つの VTEP ソースインターフェイスをクラスタ制御リンクに使用し、2 つ目のソースインターフェイスを Azure GWLB に接続されたデータインターフェイスに使用できます。

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。[Configuration] > [Device List] ペインで、アクティブなデバイスの IP アドレスの下にあるコンテキスト名をダブルクリックします。

手順

ステップ 1 **[構成（Configuration）] > [デバイスの設定（Device Setup）] > [インターフェイス設定（Interface Settings）] > [インターフェイス（Interfaces）]** の順に選択し、VTEP 送信元インターフェイスに使用するインターフェイスを編集します。

ステップ 2 （トランスペアレント モード）[VTEP Source Interface] チェック ボックスをオンにします。

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 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 3 送信元インターフェイス名と IPv4 および/または IPv6 アドレスを設定し、[OK] をクリックします。

ASA 仮想 クラスタ制御リンクは IPv6 をサポートしません。

ステップ 4 **[構成（Configuration）] > [デバイスの設定（Device Setup）] > [インターフェイス設定（Interface Settings）] > [VXLAN]** の順に選択します。

ステップ 5 （オプション）デフォルト 4789 から変更する場合は、[VXLAN Destination Port] の値を入力します。

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この設定を行います。

ステップ 6 [使用してネットワーク仮想化エンドポイントのカプセル化を有効にする（Enable Network Virtualization Endpoint encapsulation using）] ドロップダウンメニューで、[VXLAN] を選択します。

ステップ 7 ドロップダウン リストから [VTEP Tunnel Interface] を選択します。

（注）
VTEP インターフェイスの MTU が 1554 バイト（IPv4 の場合）または 1574 バイト（IPv6 の場合）未満の場合、ASA は自動的に MTU を 1554 バイトまたは 1574 バイトに増やします。

ステップ 8 （オプション）[Configure Packet Recipient] チェック ボックスをオンにします。

- （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）[Specify Peer VTEP IP Address] を入力して、手動でピア VTEP の IP アドレスを指定します。

  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。

- （シングル モードのみ）[Multicast traffic to default multicast address] を入力して、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。

  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。

ステップ 9 [Apply] をクリックします。

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。

Azure の ASA virtual の場合、通常の VXLAN インターフェイスを設定するか、Azure GWLB で使用するペアプロキシモードの VXLAN インターフェイスを設定できます。ペアプロキシモードは、クラスタリングでサポートされる唯一のモードです。

手順

ステップ 1 **[構成（Configuration）]** > **[デバイス設定（Device Setup）]** > **[インターフェイス設定（Interface Settings）]** > **[インターフェイス（Interfaces）]**の順に選択し、**[追加（Add）]** > **[VNIインターフェイス（VNI Interface）]**をクリックします。

ステップ 2 [VNI ID] は 1 ～ 10000 の間で入力します。

この ID は内部インターフェイス識別子です。

ステップ 3 [VNI Segment ID] は 1 ～ 16777215 の間で入力します。

セグメント ID は VXLAN タギングに使用されます。

ステップ 4 （トランスペアレント モード）このインターフェイスを割り当てる [Bridge Group] を指定します。

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、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 5 [Interface Name] を入力します。

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。

ステップ 6 [Security Level] に 0（最低）～100（最高）を入力します。セキュリティ レベルを参照してください。

ステップ 7 （シングル モード）[Multicast Group IP Address] を入力します。

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。

ステップ 8 [VTEP トンネルインターフェイスへマッピング（Map to VTEP Tunnel Interface）] チェックボックスをオンにします。

この設定により、VNI インターフェイスが VTEP 送信元インターフェイスに関連付けられます。

ステップ 9 [Enable Interface] チェック ボックスをオンにします。この設定はデフォルトでイネーブルになっています。

ステップ 10 （ルーテッド モード）[IP Address] 領域で、IPv4 アドレスを設定します。IPv6 を設定するには、[IPv6] タブをクリックします。

ステップ 11 [OK]、続いて [Apply] をクリックします。

Geneve インターフェイスの設定

ASA 仮想 の Geneve インターフェイスを設定するには、次の手順を実行します。

（注） VXLAN または Geneve を設定できます。VXLAN インターフェイスについては、VXLAN インターフェイスの設定 （13 ページ）を参照してください。

手順

ステップ 1 Geneve の VTEP 送信元インターフェイスの設定 （17 ページ）。

ステップ 2 Geneve の VNI インターフェイスの設定 （17 ページ）

ステップ 3 ゲートウェイロードバランサのヘルスチェックの許可 （18 ページ）。

Geneve の VTEP 送信元インターフェイスの設定

ASA 仮想 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。

手順

ステップ 1 **[構成（Configuration）]** > **[デバイスの設定（Device Setup）]** > **[インターフェイス設定（Interface Settings）]** > **[インターフェイス（Interfaces）]** の順に選択し、VTEP 送信元インターフェイスに使用するインターフェイスを編集します。

ステップ 2 （任意）[VTEP送信元インターフェイス（VTEP Source Interface）] チェック ボックスをオンにします。

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 のみに制限されます。

ステップ 3 送信元インターフェイス名と IPv4 アドレスを設定し、[OK] をクリックします。

ステップ 4 **[構成（Configuration）]** > **[デバイスの設定（Device Setup）]** > **[インターフェイス設定（Interface Settings）]** > **[VXLAN]** の順に選択します。

ステップ 5 [使用してネットワーク仮想化エンドポイントのカプセル化を有効にする（Enable Network Virtualization Endpoint encapsulation using）] ドロップダウンメニューで、[Geneve] を選択します。

ステップ 6 [Geneveポート（Geneve Port）] は変更しないでください。AWS にはポート 6081 が必要です。

ステップ 7 ドロップダウン リストから [VTEP Tunnel Interface] を選択します。

（注）
VTEP インターフェイスの MTU が 1806 バイト未満の場合、ASA は自動的に MTU を 1806 バイトに増やします。

ステップ 8 [Apply] をクリックします。

Geneve の 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 **[構成（Configuration）]** > **[デバイス設定（Device Setup）]** > **[インターフェイス設定（Interface Settings）]** > **[インターフェイス（Interfaces）]**の順に選択し、**[追加（Add）]** > **[VNIインターフェイス（VNI Interface）]**をクリックします。

ステップ 2 [VNI ID] は 1 ～ 10000 の間で入力します。

この ID は内部インターフェイス識別子です。

ステップ 3 [Interface Name] を入力します。

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。

ステップ 4 [Security Level] に 0（最低）～100（最高）を入力します。セキュリティ レベルを参照してください。

ステップ 5 [VTEP トンネルインターフェイスへマッピング（Map to VTEP Tunnel Interface）] チェックボックスをオンにします。

この設定により、VNI インターフェイスが VTEP 送信元インターフェイスに関連付けられます。

ステップ 6 [Enable Interface] チェック ボックスをオンにします。この設定はデフォルトでイネーブルになっています。

ステップ 7 [シングルアームプロキシを有効にする（Enable Single-Arm Proxy）] をオンにします。

ステップ 8 [IPアドレス（IP Address）] 領域で、IPv4 アドレスを設定します。IPv6 を設定するには、[IPv6] タブをクリックします。

ステップ 9 [OK] をクリックします。

ステップ 10 トラフィックが同一インターフェイスに出入りできるようにするには、[同じインターフェイスに接続されている2つ以上のホスト間のトラフィックを有効にする（Enable traffic between two or more hosts connected to the same interface）] をオンにします。

ステップ 11 [Apply] をクリックします。

ゲートウェイロードバランサのヘルスチェックの許可

AWS または Azure ゲートウェイロードバランサでは、アプライアンスがヘルスチェックに正しく応答する必要があります。AWS ゲートウェイロードバランサは、正常と見なされるアプライアンスにのみトラフィックを送信します。

SSH、Telnet、HTTP、または HTTPS のヘルスチェックに応答するように ASA 仮想 を設定する必要があります。

SSH 接続

SSH の場合、ゲートウェイロードバランサからの SSH を許可します。ゲートウェイロードバランサは、ASA 仮想 への接続の確立を試行し、ログインするための ASA 仮想 プロンプトが正常性の証拠として取得されます。

（注） SSH ログインの試行は 1 分後にタイムアウトします。このタイムアウトに対応するには、ゲートウェイロードバランサでより長いヘルスチェック間隔を設定する必要があります。

Telnet 接続

Telnet の場合、ゲートウェイロードバランサからの Telnet を許可します。ゲートウェイロードバランサは、ASA 仮想 への接続の確立を試行し、ログインするための ASA 仮想 プロンプトが正常性の証拠として取得されます。

（注） 最も低いセキュリティレベルのインターフェイスに Telnet で接続できないため、この方法は実用的ではありません。

HTTP（S）カットスループロキシ

ゲートウェイロードバランサに HTTP（S）ログインを要求するように ASA を設定できます。

ポート変換を設定したスタティック インターフェイス NAT を使用した HTTP（S）リダイレクト

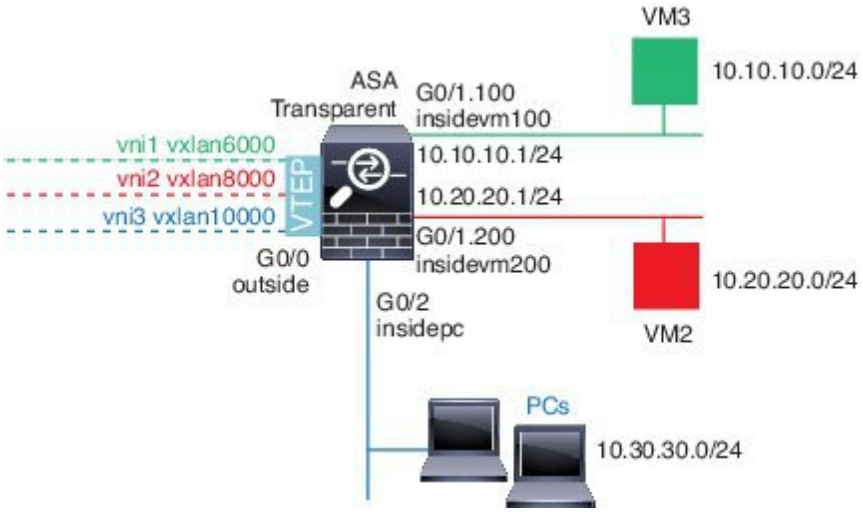
ヘルスチェックをメタデータ HTTP(S) サーバーにリダイレクトするように ASA 仮想 を設定できます。HTTP（S）ヘルスチェックの場合、HTTP（S）サーバは 200 ー 399 の範囲のステータスコードでゲートウェイロードバランサに応答する必要があります。ASA 仮想 では同時管理接続の数に制限があるため、ヘルスチェックを外部サーバーにオフロードすることもできます。

ポート変換を設定したスタティック インターフェイス NAT を使用すると、ポート（ポート 80 など）への接続を別の IP アドレスにリダイレクトできます。たとえば、ASA 仮想 外部インターフェイスの宛先を持つゲートウェイロードバランサからの HTTP パケットを、HTTP サーバーの宛先を持つ ASA 仮想 外部インターフェイスからのように変換します。次に ASA 仮想 はパケットをマッピングされた宛先アドレスに転送します。HTTP サーバーは ASA 仮想 外部インターフェイスに応答し、ASA 仮想 はゲートウェイロードバランサに応答を転送します。ゲートウェイロードバランサから HTTP サーバへのトラフィックを許可するアクセスルールが必要です。

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
```

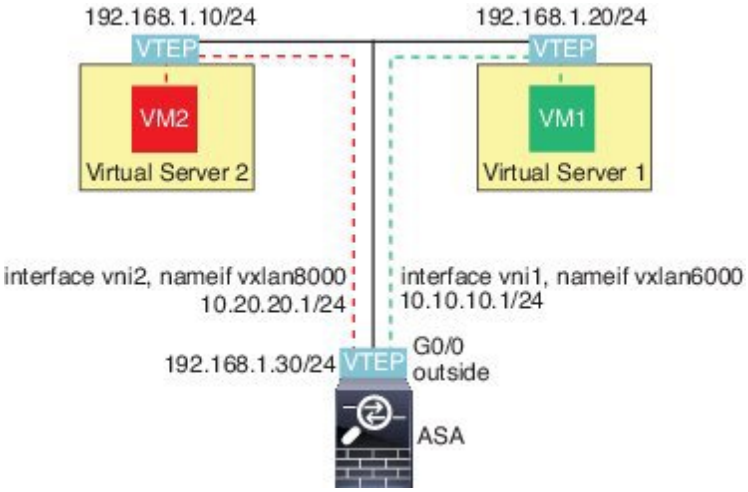
注意

- 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 インターフェイス 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。その後に、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 VTEP IPv6 のサポート	9.20(1)	VXLAN VTEP インターフェイスに IPv6 アドレスを指定できるようになりました。IPv6 では、ASA 仮想 クラスタ制御リンクまたは Geneve カプセル化がサポートされていません。 新しい/変更された画面： • **[構成（Configuration）] > [デバイスの設定（Device Setup）] > [インターフェイスの設定（Interface Settings）] > [VXLAN]** • **[構成（Configuration）] > [デバイスの設定（Device Setup）] > [インターフェイスの設定（Interface Settings）] > [インターフェイス（Interfaces）] > [追加（Add）] > [VNIインターフェイス（VNI Interface）]**
Azure ゲートウェイロードバランサーの ASA Virtual のペアプロキシ VXLAN	9.19(1)	Azure ゲートウェイ ロードバランサ（GWLB）で使用するために、Azure の ASA Virtual のペアプロキシモード VXLAN インターフェイスを構成できます。ASA Virtual は、ペアプロキシの VXLAN セグメントを利用して、単一の NIC に外部インターフェイスと内部インターフェイスを定義します。 新規/変更されたコマンド：**external-port、external-segment-id、internal-port、internal-segment-id、proxy paired** ASDM サポートはありません。
AWS ゲートウェイロードバランサの AWS での ASA 仮想 の Geneve サポート	9.17(1)	AWS ゲートウェイロードバランサのシングルアームプロキシをサポートするために、ASAv30、ASAv50、および ASAv100 の Geneve カプセル化サポートが追加されました。 新しい/変更された画面： **[Configuration] > [Device Setup] > [Interface Settings] > [Interfaces] > [Add] > [VNI Interface]** **[Configuration] > [Device Setup] > [Interface Settings] > [VXLAN]**

機能名	リリース	機能情報
VXLAN のサポート	9.4(1)	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。 次の画面が導入されました。 **[Configuration] > [Device Setup] > [Interface Settings] > [Interfaces] > [Add] > [VNI Interface]** **[Configuration] > [Device Setup] > [Interface Settings] > [VXLAN]**

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。

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。