VXLAN 接口

本章介绍如何配置虚拟可扩展局域网 (VXLAN) 接口。VXLAN 作为第 3 层物理网络之上的第 2 层虚拟网络，可对第 2 层网络进行扩展。

关于 VXLAN 接口

VXLAN 提供与 VLAN 相同的以太网第 2 层网络服务，但其可扩展性和灵活性更为出色。与 VLAN 相比，VXLAN 提供以下优势：

- 可在整个数据中心中灵活部署多租户网段。
- 更高的可扩展性可提供更多的第 2 层网段，最多可达 1600 万个 VXLAN 网段。

本节介绍 VXLAN 如何工作。有关 VXLAN 的详细信息，请参阅 RFC 7348。有关 Geneve 的详细信息，请参阅 RFC 8926。

封装

ASA 支持两种类型的 VXLAN 封装：

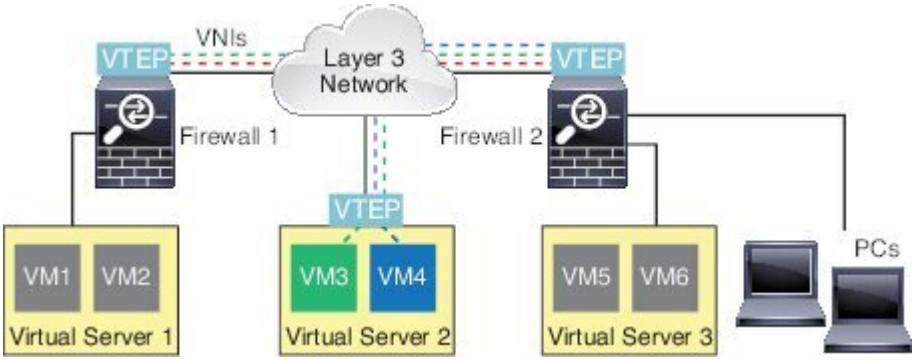
- VXLAN（所有型号）- VXLAN 使用 MAC Address-in-User 数据报协议 (MAC-in-UDP) 的封装方式。原始第 2 层帧已添加 VXLAN 报头，然后放入 UDP-IP 数据包中。

- Geneve（仅限 ASA virtual）- Geneve 具有不限于 MAC 地址的灵活内部报头。要在 Amazon Web 服务 (AWS) 网关负载均衡器和设备之间透明路由数据包，以及发送额外信息，则需要使用 Geneve 封装。

VXLAN 隧道端点

VXLAN 隧道终端 (VTEP) 设备执行 VXLAN 封装和解封。每个 VTEP 有两种接口类型：一个或多个虚拟接口称为 VXLAN 网络标识符 (VNI) 接口，您可以向其应用安全策略；以及称为 VTEP 源接口的常规接口，用于为 VTEP 之间的 VNI 接口建立隧道。VTEP 源接口连接到传输 IP 网络，进行 VTEP 至 VTEP 通信。

下图显示第 3 层网络范围内用作 VTEP 的两个 ASA 和虚拟服务器 2，扩展了站点之间的 VNI 1、2 和 3 网络。ASA 可用作 VXLAN 与非 VXLAN 网络之间的网桥或网关。



VTEP 之间的底层 IP 网络与 VXLAN 重叠无关。封装的数据包根据外部 IP 地址报头路由，该报头具有初始 VTEP（用作源 IP 地址）和终止 VTEP（作为目标 IP 地址）。对于 VXLAN 封装：当远程 VTEP 未知时，目标 IP 地址可以是组播组。在使用 Geneve 时，ASA 仅支持静态对等体。默认情况下， VXLAN 的目标端口是 UDP 端口 4789（用户可配置）。Geneve 的目的端口是 6081。

VTEP 源接口

VTEP 源接口是一个计划要与所有 VNI 接口相关联的常规 ASA 接口（物理EtherChannel 接口，甚至 VLAN 接口）。每个 ASA/安全情景可以配置一个 VTEP 源接口。 由于只能配置一个 VTEP 源接口，因此不能在同一设备上同时配置 VXLAN 和 Geneve 接口。AWS上的集群有一个例外，您可以在其中有两个 VTEP 源接口：一个 VXLAN 接口用于集群控制链路，一个 Geneve 接口可用于 AWS 网关负载均衡器。

尽管并未将 VTEP 源接口限制为全部用于传输 VXLAN 流量，但是可以实现该用途。如果需要，可以使用该接口传输常规流量，并将一个安全策略应用于传输此类流量的该接口。但是，对于 VXLAN 流量，必须对 VNI 接口应用所有安全策略。VTEP 接口仅作为物理端口。

在透明防火墙模式下，VTEP 源接口不是 BVI 的一部分，并且类似于对待管理接口的方式，不为该源接口配置 IP 地址。

VNI 接口

VNI 接口类似于 VLAN 接口：它们是虚拟接口，通过使用标记，实现网络流量在给定物理接口上的分离。将安全策略直接应用于每个 VNI 接口。

您智能添加一个 VTEP 接口，并且所有 VNI 接口都与同一 VTEP 接口相关联。 AWS上的 ASA Virtual 集群例外。对于 AWS 集群，您可以在其中有两个 VTEP 源接口：一个 VXLAN 接口用于集群控制链路，一个 Geneve 接口可用于 AWS 网关负载均衡器。

VXLAN 数据包处理

VXLAN

进出 VTEP 源接口的流量取决于 VXLAN 处理，特别是封装或解封。

封装处理包括以下任务：

- VTEP 源接口通过 VXLAN 报头封装内部 MAC 帧。
- UDP 校验和字段设置为零。
- 外部帧源 IP 设置为 VTEP 接口 IP。
- 外部帧目标 IP 通过远程 VTEP IP 查找确定。

解封；ASA 仅在以下条件下解封 VXLAN 数据包：

- VXLAN 数据包是目标端口设置为 4789（用户可配置该值）的 UDP 数据包。
- 入口接口是 VTEP 源接口。
- 入口接口 IP 地址与目标 IP 地址相同。
- VXLAN 数据包格式符合标准。

Geneve

进出 VTEP 源接口的流量取决于 Geneve 处理，特别是封装或解封。

封装处理包括以下任务：

- VTEP 源接口通过 Geneve 报头封装内部 MAC 帧。
- UDP 校验和字段设置为零。
- 外部帧源 IP 设置为 VTEP 接口 IP。
- 外部帧目标 IP 会被设置为您配置的对等体 IP 地址。

解封；ASA 仅在以下条件下解封 Geneve 数据包：

- VXLAN 数据包是目标端口设置为 6081（用户可配置该值）的 UDP 数据包。

- 入口接口是 VTEP 源接口。
- 入口接口 IP 地址与目标 IP 地址相同。
- Geneve 数据包格式符合标准。

对等体 VTEP

ASA 向对等体 VTEP 后的设备发送数据包时，ASA 需要两条重要信息：

- 远程设备的目标 MAC 地址
- 对等体 VTEP 的目标 IP 地址

ASA 维护目标 MAC 地址到 VNI 接口的远程 VTEP IP 地址的映射。

VXLAN 对等体

ASA 可以通过两种方式找到这些信息：

- 单个对等体 VTEP IP 地址可以在 ASA 上静态配置。

  无法手动定义多个对等体。

  然后，ASA 设备将已封装 VXLAN 的 ARP 广播发送到 VTEP，以获取终端节点 MAC 地址。

- 可以在每个 VNI 接口（或者总的来说，在 VTEP 上）配置组播组。

注释 Geneve 不支持此选项。

ASA 将通过 VTEP 源接口在 IP 组播数据包内发送一个 VXLAN 封装的 ARP 广播数据包。对此 ARP 请求的响应使 ASA 可以获悉远程 VTEP IP 地址以及远程结束节点的目标 MAC 地址。

Geneve 对等体

ASA virtual 仅支持静态定义的对等设备。您可以在 AWS 网关负载均衡器上定义 ASA virtual 对等体 IP 地址。由于 ASA virtual 绝不会向网关负载均衡器发起流量，因此您也不必在 ASA virtual 上指定网关负载均衡器 IP 地址；它会在收到 Geneve 流量时获知对等体 IP 地址。Geneve 不支持组播组。

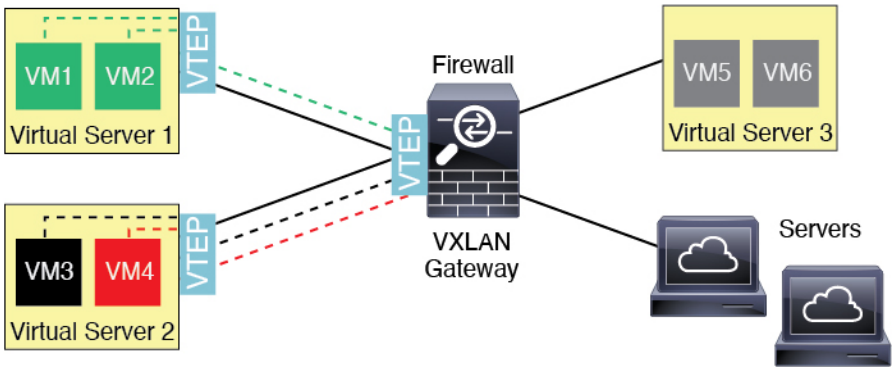
VXLAN 使用案例

本部分介绍在 ASA 上实施 VXLAN 的使用案例。

VXLAN 网桥或网关概述

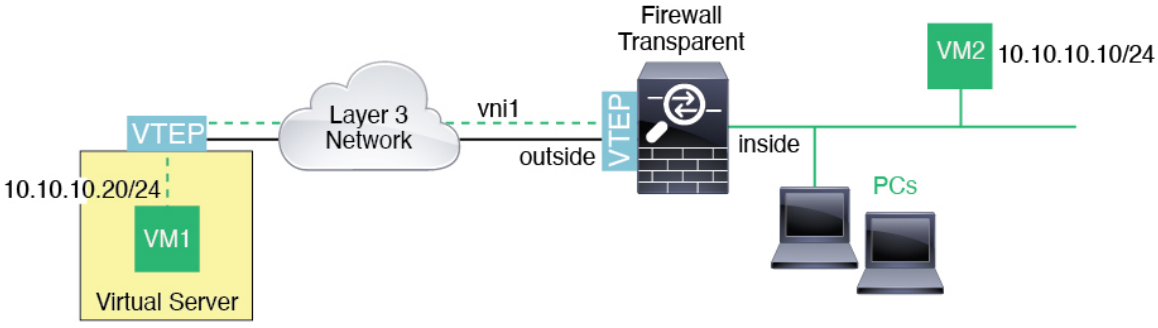
每个 ASA VTEP 都可作为终端节点（例如 VM、服务器和 PC）和 VXLAN 重叠网络之间的网桥或网关。对于通过 VTEP 源接口借助 VXLAN 封装接收的传入帧，ASA 去掉 VXLAN 报头，并基于内部以太网帧的目标 MAC 地址，将传入帧转发到连接非 VXLAN 网络的物理接口。

ASA 始终会处理 VXLAN 数据包；而不仅仅是在两个其他 VTEP 之间转发未处理的 VXLAN 数据包。



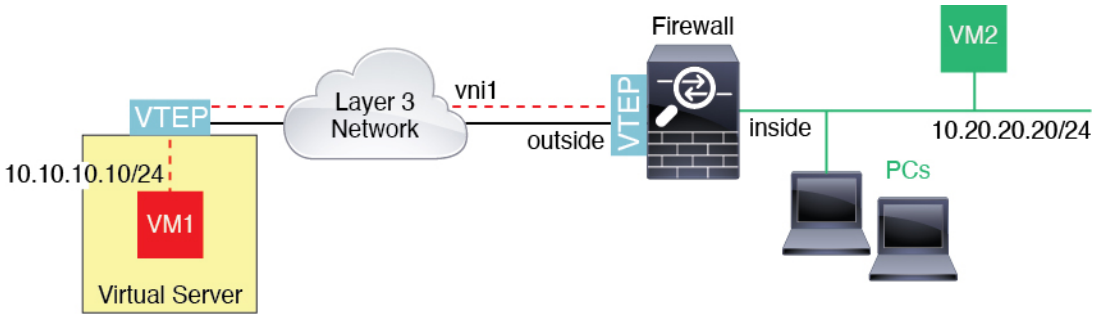
VXLAN 网桥

在使用网桥组（透明防火墙模式或可选的路由模式）时，ASA 可以用作 VXLAN 网段与本地网段之间的 VXLAN 网桥（远程），其中二者均位于同一网络中。在这种情况下，网桥组的一个成员是常规接口，而另一个成员是 VNI 接口。



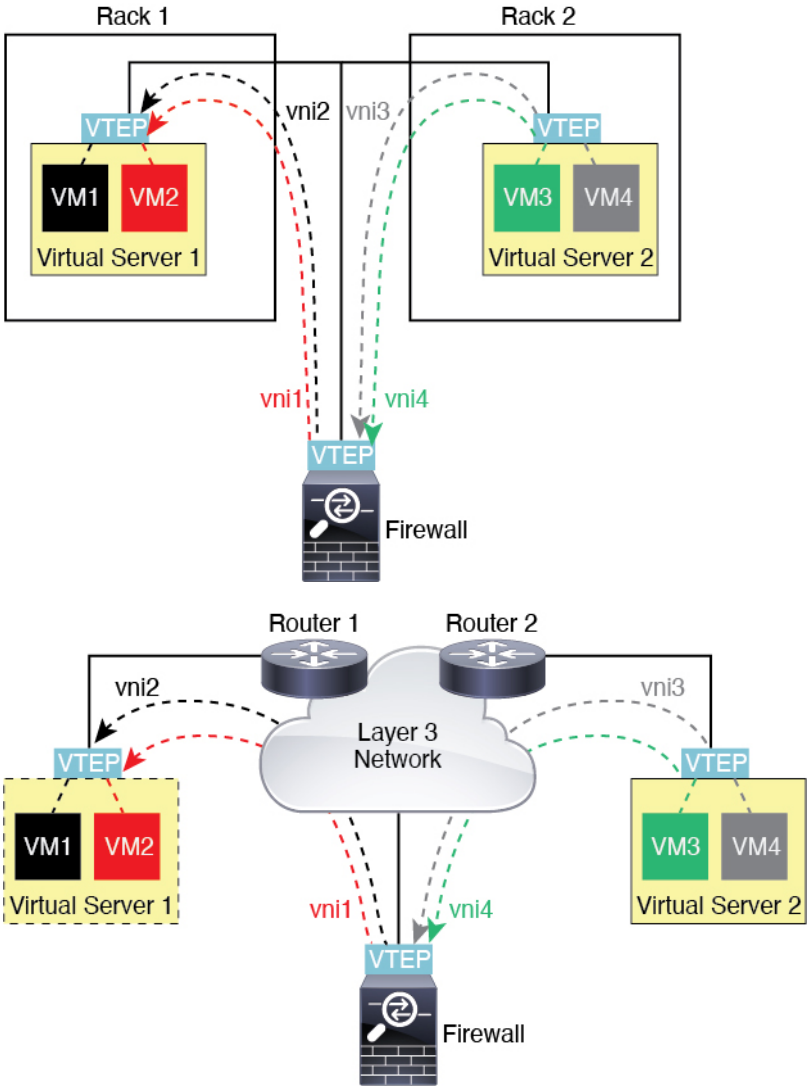
VXLAN 网关（路由模式）

ASA 可充当 VXLAN 和非 VXLAN 域之间的路由器，用于连接不同网络上的设备。



VXLAN 域之间的路由器

借助通过 VXLAN 扩展的第 2 层域，虚拟机可以指向一个 ASA 作为其网关，即使 ASA 位于不同机架中，甚至当 ASA 位于第 3 层网络上很远的位置也是如此。



请参阅有关此场景的以下注释：

1. 对于从 VM3 到 VM1 的数据包，目标 MAC 地址为 ASA MAC 地址，因为 ASA 是默认网关。
2. 虚拟服务器 2 上的 VTEP 源接口接收来自 VM3 的数据包，然后使用 VNI 3 的 VXLAN 标签封装数据包，并将数据包发送到 ASA。
3. 当 ASA 接收数据包时，会解封数据包以获得内部帧。
4. ASA 使用内部帧进行路由查找，然后发现目标位于 VNI 2 上。如果尚不具有 VM1 的映射，ASA 会在 VNI 2 上的组播组 IP 上发送封装的 ARP 广播。

注释 ASA 必须使用动态 VTEP 对等体发现，因为 ASA 在此场景下有多个 VTEP 对等体。

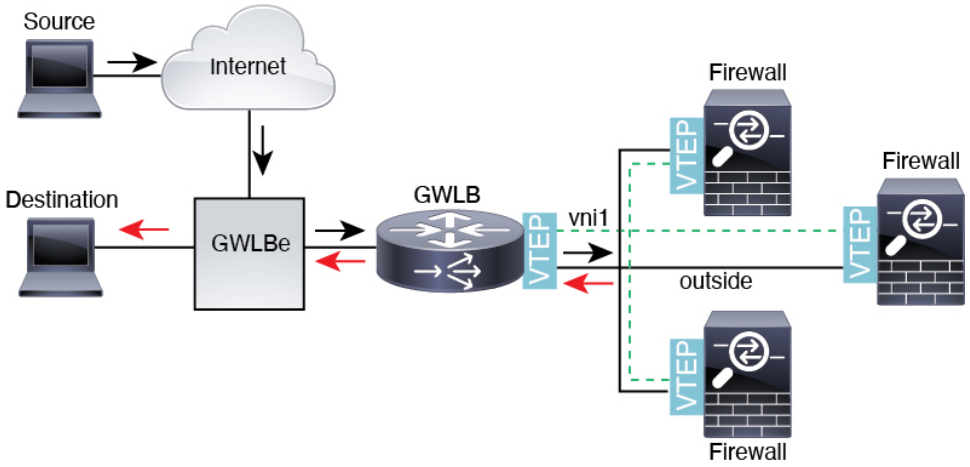
5. ASA 再次使用 VXLAN 标签为 VNI 2 封装数据包，并且将数据包发送到虚拟服务器 1。在封装之前，ASA 将内部帧目标 MAC 地址更改为 VM1 的 MAC 地址（ASA 可能需要组播封装的 ARP，以获取 VM1 MAC 地址）。
6. 当虚拟服务器 1 接收 VXLAN 数据包时，该虚拟服务器会解封数据包并向 VM1 提供内部帧。

AWS 网关负载均衡器和 Geneve 单臂代理

注释 这是 Geneve 接口当前唯一支持的使用案例。

AWS 网关负载均衡器结合了透明网络网关和按需分配流量和扩展虚拟设备的负载均衡器。ASA virtual 支持具有分布式数据平面的网关负载均衡器集中控制平面（网关负载均衡器终端）。下图显示了从网关负载均衡器终端转发到网关负载均衡器的流量。网关负载均衡器会在多个流量之间进行均衡，这些流量在丢弃流量或将其发送回网关负载均衡器之前对其进行检查（掉头流量）。ASA virtual然后，网关负载均衡器会将流量发送回网关负载均衡器终端和目的地。

图 *1: Geneve* 单臂代理

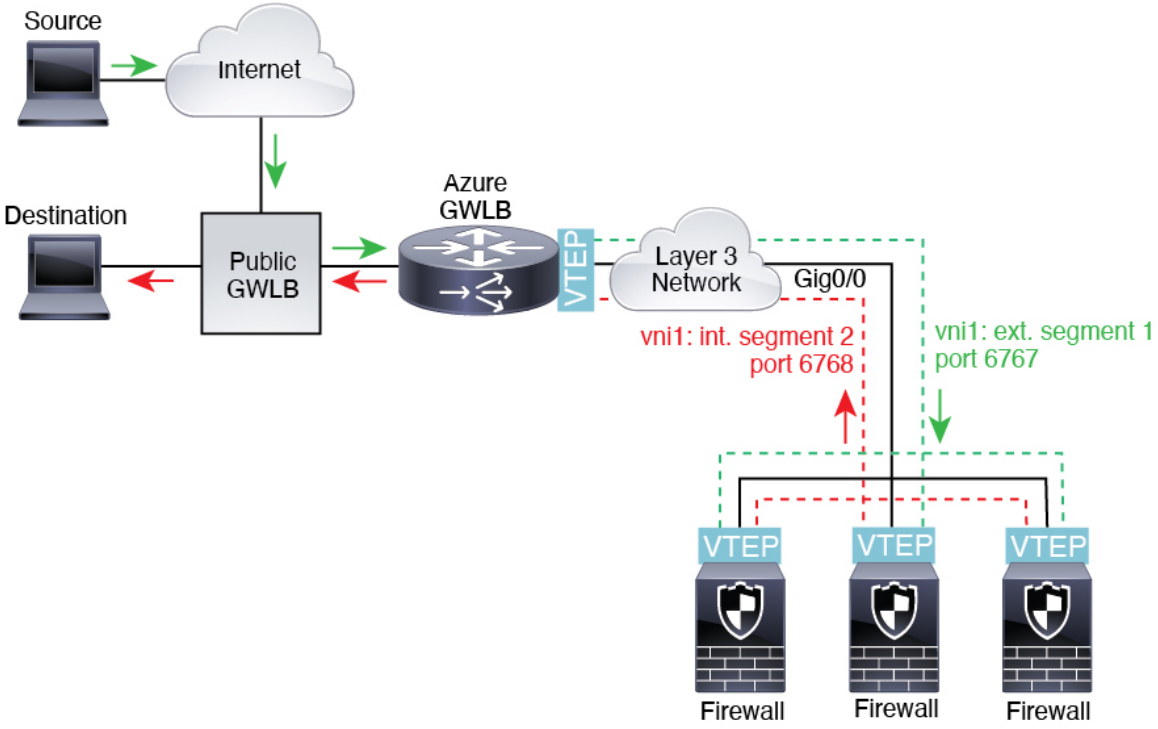


Azure 网关负载均衡器和配对代理

在 Azure 服务链中， ASA virtual充当可以拦截互联网和客户服务之间的数据包的透明网关。 ASA virtual 通过已配对代理中的 VXLAN 网段在单个 NIC 上定义外部接口和内部接口。

下图显示了从外部 VXLAN 网段上的公共网关负载均衡器转发到 Azure 门户负载均衡器的流量。网关负载均衡器会在多个 ASA virtual流量之间进行均衡，这些流量在丢弃流量或将其发送回在内部 VXLAN 部分的网关负载均衡器之前对其进行检查。然后，Azure 网关负载均衡器会将流量发送回公共网关负载均衡器和目的地。

图 *2: Azure* 网关负载均衡器和配对代理



VXLAN 接口的要求和前提条件

型号要求

- 不支持将 Firepower 1010 交换机端口和 VLAN 接口用作 VTEP 接口。
- 以下型号支持 Geneve 封装：Amazon Web Services (AWS) 上的 ASAv30、ASAv50、ASAv100
- 以下型号支持配对代理模式下的 VXLAN：
  - Azure 中的 ASA Virtual

VXLAN 接口准则

防火墙模式

- Geneve 接口仅在路由防火墙模式下支持。
- 配对代理 VXLAN 接口仅在路由防火墙模式下支持。

IPv6

- VNI 接口支持 IPv4 和 IPv6 流量。
- VTEP 源接口 IP 地址仅支持 IPv4。

集群和多情景模式

- 集群在单个接口模式 下不支持 VXLAN，但集群控制链路除外（仅限ASA virtual ）。仅跨区以太网通道模式支持 VXLAN。

  AWS 上的 ASA virtual例外，它可以使用额外的 Geneve 接口与 GWLB配合使用。
- Geneve 接口仅在独立的单情景模式下受支持。 多情景模式不支持它们。

路由

- VNI 接口上仅支持静态路由或基于策略的路由；动态路由协议不受支持。

MTU

- VXLAN 封装-如果源接口 MTU 少于 1554 个字节或 1574 字节。在这种情况下，整个以太网数据报将被封装，因此，新数据包更大，需要更大的 MTU。如果其他设备使用的 MTU 更大，则您应。此 MTU 需要您在一些型号上启用巨帧保留；请参阅 启用巨帧支持（ASA Virtual、ISA 3000）。
- Geneve 封装- 如果源接口 MTU 少于 1806 个字节，ASA 会自动将 MTU 提高到 1806 个字节。在这种情况下，整个以太网数据报将被封装，因此，新数据包更大，需要更大的MTU。如果其他设备使用的 MTU 更大，您应将源接口 MTU 设置为网络 MTU + 306 个字节。此 MTU 需要您在一些型号上启用巨帧保留；请参阅 启用巨帧支持（ASA Virtual、ISA 3000）。

VXLAN 接口默认设置

默认启用 VNI 接口。

配置 VXLAN 接口

要配置 VXLAN，请执行下列步骤：

注释 您可以配置 VXLAN 或 Geneve（仅限 ASA virtual）。有关 Geneve 接口，请参阅配置 Geneve 接口，第 15 页。

过程

步骤 1 配置 VTEP 源接口，第 10 页。

步骤 2 配置 VNI 接口，第 12 页

步骤 3 （可选）更改 VXLAN UDP 端口，第 14 页。

步骤 4 (Azure GWLB) 允许网关负载均衡器运行状况检查，第 18 页。

配置 VTEP 源接口

每个 ASA 或安全情景可以配置一个 VTEP 源接口。VTEP 定义为网络虚拟化终端 (NVE)。

开始之前

对于多情景模式，请在情景执行空间完成本节所述的任务。输入 **changeto context** *name* 命令以更改为要配置的情景。

过程

步骤 1 （透明模式）将源接口指定为仅 NVE：

interface *id*

nve-only

示例：

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

可以通过此设置配置接口的 IP 地址。在路由模式下，此设置限制此接口上仅允许流向 VXLAN 的流量和常见的管理流量，这种情下此命令是可选的。

步骤 2 配置源接口名称和 IPv4 地址。

示例：

（路由模式）

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

示例：

（透明模式）

```
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
```

步骤 3 指定 NVE 实例：

nve 1

只能指定一个 NVE 实例，其中 ID 为 1。

示例：

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

步骤 4 指定 VXLAN 封装。

encapsulation vxlan

示例：

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

步骤 5 指定您在第 2 步配置的源接口名称：

source-interface *interface-name*

示例：

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

注释 如果 VTEP 接口 MTU 少于 1554 个字节，则 ASA 会自动将 MTU 提高到 1554 个字节。

步骤 6 （多情景模式；对于单情景模式为可选）手动指定对等体 VTEP IP 地址：

peer ip *ip_address*

示例：

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

如果指定对等体 IP 地址，则无法使用组播组发现。在多情景模式中不支持组播，因此只能选择手动配置。只能为 VTEP 指定一个对等体。

步骤 7 （可选；仅限单情景模式）为所有关联的 VNI 接口指定默认组播组：

default-mcast-group *mcast_ip*

示例：

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

如果每个 VNI 接口未配置组播组，则使用该组。如果配置一个 VNI 接口级别的组，则该组将覆盖此设置。

配置 VNI 接口

添加 VNI 接口，将其与 VTEP 源接口相关联，并配置基本的接口参数。

对于 Azure 中的 ASA Virtual，您可以配置常规 VXLAN 接口，也可以配置配对代理模式 VXLAN 接口，以便与 Azure GWLB 配合使用。

过程

步骤 1 创建 VNI 接口：

interface vni *vni_num*

示例：

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

将 ID 设置为 1 和 10000 之间的整数。此 ID 仅为内部接口标识符。

步骤 2 (Regular VXLAN) 指定 VXLAN 网段 ID：

segment-id *id*

示例：

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

将 ID 设置为 1 和 16777215 之间的整数。网段 ID 用于 VXLAN 标记。

步骤 3 （Azure GWLB 的已配对代理 VXLAN）启用代理配对模式并设置所需的参数。

a) 启用代理配对模式。

proxy paired

示例：

```
ciscoasa(config-if)# proxy paired
```

b) 设置内部端口。

internal-port *port_number*

其中 *port_number* 介于 1024 和 65535 之间。

示例：

```
ciscoasa(config-if)# internal-port 2000
```

c) 设置内部网段 ID。

internal-segment-id *id_number*

其中 *id_number* 介于 1 和 16777215 之间。

示例：

```
ciscoasa(config-if)# internal-segment-id 101
```

d) 设置外部端口。

external-port *port_number*

其中 *port_number* 介于 1024 和 65535 之间。

示例：

```
ciscoasa(config-if)# external-port 2001
```

e) 设置外部网段 ID。

external-segment-id *id_number*

其中 *id_number* 介于 1 和 16777215 之间。

示例：

```
ciscoasa(config-if)# external-segment-id 102
```

f) 允许流量进出同一接口。

same-security-traffic permit intra-interface

示例：

```
ciscoasa(config)# same-security-traffic permit intra-interface
```

步骤 4 （透明模式下需要）指定要将此接口关联至的网桥组：

bridge-group 编号

示例：

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

请参阅 配置网桥组接口 配置 BVI 接口并将普通接口关联至此 网桥组。

步骤 5 将此接口与 VTEP 源接口相关联：

vtep-nve 1

步骤 6 为接口命名：

nameif *vni_interface_name*

示例：

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

name 是长度最多为 48 个字符的文本字符串，并且不区分大小写。使用一个新值重新输入此命令可更改名称。请勿输入 **no** 形式，因为该命令会导致删除所有引用该名称的命令。

步骤 7 （路由模式）分配 IPv4 和/或 IPv6 地址：

ip address {*ip_address* [*mask*] [**standby** *ip_address*] | **dhcp** [**setroute**] | **pppoe** [**setroute**]}

{| ipv6-address / prefix-length [ipv6-address]} **ipv6 addressautoconfigstandby**

示例：

```
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
```

步骤 8 设置安全级别：

security-level 级别

示例：

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

其中 *number* 为 0（最低）到 100（最高）之间的整数。

步骤 9 （单情景模式）设置组播组地址：

mcast-group *multicast_ip*

示例：

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

如果没有为 VNI 接口设置组播组，请使用源自 VTEP 源接口配置的默认组（如果有）。如果手动设置 VTEP 源接口的 VTEP 对等体 IP，则无法为 VNI 接口指定组播组。多情景模式下不支持组播。

（可选）更改 VXLAN UDP 端口

默认情况下，VTEP 源接口接收发往 UDP 端口 4789 的 VXLAN 流量。如果网络使用非标准端口，可以对其进行更改。

开始之前

对于多情景模式，请在系统执行空间中完成此任务。要从该情景切换到系统执行空间，请输入**changeto system** 命令。

过程

设置 VXLAN UDP 端口：

vxlan 端口号

示例：

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

配置 Geneve 接口

要为 ASA virtual 配置 Geneve 接口，请执行以下步骤：

注释 您可以配置 VXLAN 或 Geneve。有关 VXLAN 接口的信息，请参阅配置 VXLAN 接口，第 9 页。

过程

步骤 1 为 Geneve 配置 VTEP 源接口，第 15 页。

步骤 2 为 Geneve 配置 VNI 接口，第 16 页

步骤 3 允许网关负载均衡器运行状况检查，第 18 页。

为 Geneve 配置 VTEP 源接口

每个 ASA virtual 设备可以配置一个 VTEP 源接口。VTEP 定义为网络虚拟化终端 (NVE)。

过程

步骤 1 （可选） 将源接口指定为仅限 NVE。

interface *id*

nve-only

示例：

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

此设置限制此接口上仅允许流向 VXLAN 的流量和常见的管理流量，这种情下此设置是可选的。

步骤 2 配置源接口名称和 IPv4 地址。

示例：

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

步骤 3 指定 NVE 实例：

nve 1

只能指定一个 NVE 实例，其中 ID 为 1。

示例：

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

步骤 4 指定 Geneve 封装。

encapsulation geneve

请勿更改 Geneve 端口；AWS 需要使用端口 6081。

示例：

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

步骤 5 指定您在第 2 步配置的源接口名称：

source-interface *interface-name*

示例：

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

注释 如果源接口 MTU 少于 1806 个字节，ASA 会自动将 MTU 提高到 1806 个字节。

为 Geneve 配置 VNI 接口

添加 VNI 接口，将其与 VTEP 源接口相关联，并配置基本的接口参数。

过程

步骤 1 创建 VNI 接口：

interface vni *vni_num*

示例：

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

将 ID 设置为 1 和 10000 之间的整数。此 ID 仅为内部接口标识符。

步骤 2 将此接口与 VTEP 源接口相关联：

vtep-nve 1

步骤 3 为接口命名：

nameif *vni_interface_name*

示例：

```
ciscoasa(config-if)# nameif geneve1000
```

name 是长度最多为 48 个字符的文本字符串，并且不区分大小写。使用一个新值重新输入此命令可更改名称。请勿输入 **no** 形式，因为该命令会导致删除所有引用该名称的命令。

步骤 4 分配 IPv4 和/或 IPv6 地址：

ip address {*ip_address* [*mask*] [**standby** *ip_address*]}

{| ipv6-address / prefix-length [ipv6-address]} **ipv6 addressautoconfigstandby**

Geneve 仅支持静态 IP 地址。

示例：

```
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
```

步骤 5 设置安全级别：

security-level 级别

级别 为 0（最低）到 100（最高）之间的整数。

示例：

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

步骤 6 启用单臂代理。

proxy single-arm

示例：

```
ciscoasa(config-if)# proxy single-arm
```

步骤 7 允许流量进出同一接口。

same-security-traffic permit intra-interface

示例：

```
ciscoasa(config)# same-security-traffic permit intra-interface
```

允许网关负载均衡器运行状况检查

AWS 或 Azure 网关负载均衡器要求设备对运行状况检查进行正确应答。AWS 网关负载均衡器只会将流量发送到被视为正常的设备。

您必须将 ASA virtual 配置为响应 SSH、Telent、HTTP 或 HTTPS 运行状况检查。

SSH 连接

对于 SSH，允许来自网关负载均衡器的 SSH。网关负载均衡器将尝试与 ASA virtual 建立连接，而 ASA virtual 的登录提示将被视为运行状况的证明。

注释 SSH 登录尝试会在 1 分钟后超时。为了适应此超时，您需要在网关负载均衡器上配置更长的运行状况检查间隔。

示例

```
! Allow SSH connections from GWLB network: 10.0.1.0/24
ssh 10.0.1.0 255.255.255.0 outside
```

Telnet 连接

对于 Telnet，允许来自网关负载均衡器的 Telnet。网关负载均衡器将尝试与 ASA virtual 建立连接，而 ASA virtual 的登录提示将被视为运行状况的证明。

注释 您无法通过 Telnet 连接到最低安全级别的接口，因此此方法可能不实用。

示例

```
! Allow Telnet connections from GWLB network: 10.0.1.0/24
telnet 10.0.1.0 255.255.255.0 outside
```

HTTP(S) 直通代理

您可以将 ASA 配置为提示网关负载均衡器进行 HTTP(S) 登录。

示例

```
! Identify health probe HTTP traffic from GWLB nw 10.0.1.0/24 to ASAv interface 10.2.2.2
access-list gwlb extended permit tcp 10.0.1.0 255.255.255.0 host 10.2.2.2 eq www
! Enable HTTP authentication
aaa authentication http console LOCAL
! Require authentication for the health probe traffic
aaa authentication match gwlb outside LOCAL
! Use an HTTP login page on the ASA
aaa authentication listener http outside port www
```

使用支持端口转换的静态接口 NAT 的 HTTP(S) 重定向。

您可以将 ASA virtual 配置为将运行状况检查重定向到元数据 HTTP(S) 服务器。对于 HTTP(S) 运行状况检查，HTTP(S) 服务器必须使用 200 到 399 范围内的状态代码来回复网关负载均衡器。由于 ASA virtual 对同时管理连接的数量存在限制，因此您可以选择将运行状况检查分流到外部服务器。

支持端口转换的静态接口 NAT 允许您将某个端口（例如端口 80）的连接重定向到其他 IP 地址。例如，将来自网关负载均衡器的 HTTP 数据包转换为 ASA virtual 外部接口的目标，使其看起来像是来自目标为 HTTP 服务器的 ASA virtual 外部接口。ASA virtual 随后会将数据包转发到映射的目标地址。HTTP 服务器会响应 ASA virtual 外部接口，然后 ASA virtual 会将响应转发回网关负载均衡器。您需要允许从网关负载均衡器到 HTTP 服务器的流量的访问规则。

示例

```
! Permit HTTP traffic from GWLB nw 10.0.1.0/24 to HTTP server 10.2.2.3
access-list gwlb-health extended permit tcp 10.0.1.0 255.255.255.0 host 10.2.2.3 eq www
access-group gwlb-health in interface outside

! Create network objects
object network gwlb-subnet
 subnet 10.0.1.0 255.255.255.0
object-group network gwlb
    network-object object gwlb-subnet
object-group network http-server
    network-object host 10.2.2.3
object service http80
    service tcp destination eq www

! For HTTP, translate src GWLB IP to outside IP; translate dest of outside IP to HTTP Server
 IP
nat (outside,outside) source static gwlb interface destination static interface http-server
 service http80 http80
```

监控 VXLAN 接口

参阅以下命令，以监控 VTEP 和 VNI 接口。

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

此命令显示 NVE 接口的参数、状态和统计信息，其载频接口（源接口）的状态，承载接口的 IP 地址，已将此 NVE 用作 VXLAN VTEP 的 VNI，以及与此 NVE 接口相关联的对等体 VTEP IP 地址。使用 **summary** 选项，此命令仅显示 NVE 接口的状态、NVE 接口后 VNI 的数量，以及所发现的 VTEP 数量。

请参阅以下所示的 **show nve 1** 命令输出：

```
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
```

请参阅以下所示的 **show nve 1 summary** 命令输出：

```
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**]

  此命令显示 VNI 接口的参数、状态和统计信息，其桥接接口（如果已配置）的状态，以及与其关联的 NVE 接口。**summary** 选项仅显示 VNI 接口参数。

  请参阅以下所示的 **show interface vni 1** 命令输出：

```
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
```

请参阅以下所示的 **show interface vni 1 summary** 命令输出：

```
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**

  此命令显示 VNI 网段 ID 和 VLAN 接口或物理接口之间的映射。此命令仅在透明防火墙模式下有效，因为在路由模式下，VXLAN 和 VLAN 之间的映射可能会显示过多的值。

  请参阅以下所示的 **show vni vlan-mapping** 命令输出：

```
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**

  此命令可显示 VNI 接口上缓存的与远程网段域中的 IP 地址和远程 VTEP IP 地址对应的 MAC 地址。

  请参阅以下所示的 **show arp vtep-mapping** 命令输出：

```
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**

  此命令将使用远程 VTEP IP 地址在 VNI 接口上显示第 2 层转发表（MAC 地址表）。

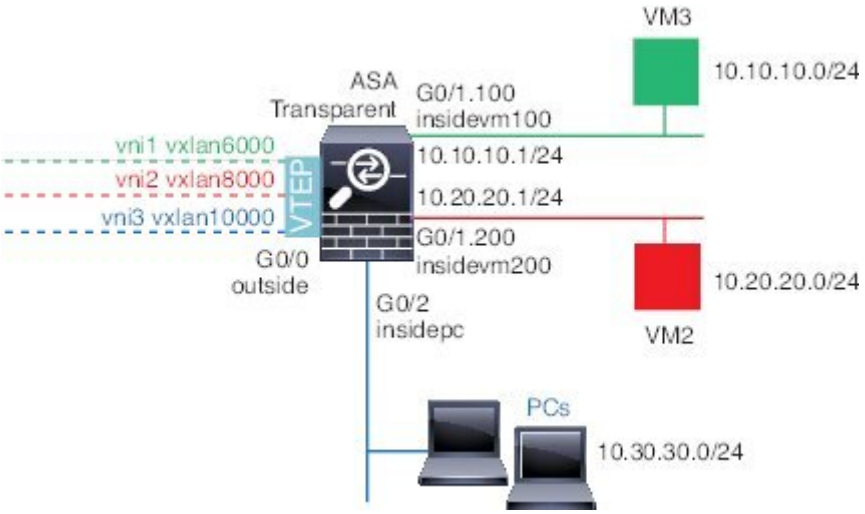
  请参阅以下所示的 **show mac-address-table vtep-mapping** 命令输出：

```
ciscoasa# show mac-address-table vtep-mapping
interface                  mac  address       type     Age(min)   bridge-group    VTEP
-------------------------------------------------------------------------------------------
vni-outside               00ff.9200.0000      dynamic      5         1        10.9.1.3
vni-inside                 0041.9f00.0000      dynamic      5         1      10.9.1.3
```

VXLAN 接口示例

请参阅以下所示的 VXLAN 配置示例。

透明 VXLAN 网关示例



请参见以下有关此示例的说明：

- GigabitEthernet 0/0 上的外部接口用作 VTEP 源接口，并且连接到第 3 层网络。
- GigabitEthernet 0/1.100 上的 insidevm100 VLAN 子接口连接到 VM3 所在的 10.10.10.0/24 网络。当 VM3 与 VM1（未显示；两者均有 10.10.10.0/24 IP 地址）通信时，ASA 使用 VXLAN 标签 6000。
- GigabitEthernet 0/1.200 上的 insidevm200 VLAN 子接口连接到 VM2 所在的 10.20.20.0/24 网络。当 VM2 与 VM4（未显示；两者均有 10.20.20.0/24 IP 地址）通信时，ASA 使用 VXLAN 标签 8000。
- GigabitEthernet 0/2 上的 insidepc 接口连接到若干 PC 所在的 10.30.30.0/24 网络。当这些 PC 与属于同一网络（全部具有 10.30.30.0/24 IP 地址）的远程 VTEP 后面的 VM/PC（未显示）进行通信时，ASA 使用 VXLAN 标签 10000。

ASA 配置

```
firewall transparent
vxlan port 8427
!
interface gigabitethernet0/0
  nve-only
  nameif outside
  ip address 192.168.1.30 255.255.255.0
  no shutdown
!
```

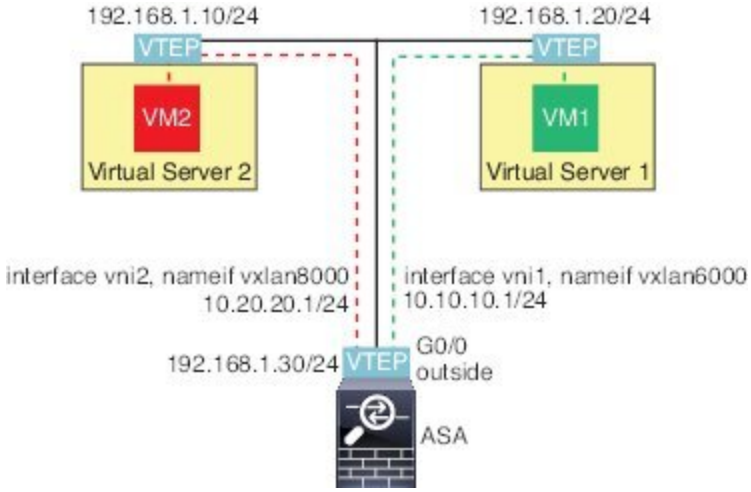
```
nve 1
  encapsulation vxlan
  source-interface outside
!
interface vni1
  segment-id 6000
  nameif vxlan6000
  security-level 0
  bridge-group 1
  vtep-nve 1
  mcast-group 235.0.0.100
!
interface vni2
  segment-id 8000
  nameif vxlan8000
  security-level 0
  bridge-group 2
  vtep-nve 1
  mcast-group 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
```

备注

- 对于 VNI 接口 vni1 和 vni2，在封装过程中将删除内部 VLAN 标签。
- VNI 接口 vni2 和 vni3 通过组播共享封装的 ARP 的同一组播 IP 地址。系统允许此共享。
- ASA 基于以上 BVI 和网桥组配置，将 VXLAN 流量桥接到非 VXLAN 支持的接口。对于每个扩展的第 2 层网段（10.10.10.0/24、10.20.20.0/24 和 10.30.30.0/24），ASA 充当网桥。

- 在网桥组中允许有多个 VNI 或多个常规接口（VLAN 或仅物理接口）。VXLAN 网段 ID 与 VLAN ID（或物理接口）之间的转发或关联，由目标 MAC 地址和连接到目标的接口决定。
- VTEP 源接口是透明防火墙模式下，由接口配置中的 **nve-only** 所指示的第 3 层接口。VTEP 源接口不是 BVI 接口或管理接口，但是具有 IP 地址，并且使用路由表。

VXLAN 路由示例



请参见以下有关此示例的说明：

- VM1 (10.10.10.10) 通过虚拟服务器 1 进行托管，VM2 (10.20.20.20) 通过虚拟服务器 2 进行托管。
- VM1 的默认网关是 ASA，它不与虚拟服务器 1 位于同一个 pod 上，但 VM1 对此并不知晓。VM1 只知道其默认网关 IP 地址为 10.10.10.1。同样，VM2 只知道其默认网关 IP 地址为 10.20.20.1。
- 虚拟服务器 1 和 2 上的支持 VTEP 的虚拟机监控程序可以通过相同的子网或第 3 层网络（未显示；不管是哪种情况，ASA 和虚拟服务器的上行链路都具有不同的网络地址）与 ASA 进行通信。
- VM1 的数据包将通过其虚拟机监控程序的 VTEP 进行封装，并通过 VXLAN 隧道发送到其默认网关。
- 当 VM1 将数据包发送到 VM2 时，对数据包而言，它将通过默认网关 10.10.10.1 进行发送。虚拟服务器 1 知道 10.10.10.1 不是本地地址，因此 VTEP 会通过 VXLAN 封装数据包，并将其发送至 ASA 的 VTEP。
- 在 ASA 上，对数据包进行解封。在解封过程中可获取 VXLAN 网段 ID。然后，ASA 会基于 VXLAN 网段 ID 将内部帧重新注入到对应的 VNI 接口 (vni1)。ASA 然后会执行路由查找，并通过 VNI 接口 vni2 发送内部数据包所有通过 vni2 的传出数据包都使用 VXLAN 网段 8000 进行封装，并通过 VTEP 发送到外部。
- 最终，虚拟服务器 2 的 VTEP 接收封装的数据包、解封数据包，并将数据包转发到 VM2。

ASA 配置

```
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 接口历史记录

表 *1: VXLAN* 接口历史记录

功能名称	版本	功能信息
ASA Virtual用于 Azure网关负载均衡器的已配对代理 VXLAN	9.19(1)	您可以在 Azure 中为 ASA Virtual 配置配对代理模式 VXLAN 接口，以便与 Azure 网关负载均衡器 (GWLB) 配合使用。ASA Virtual 通过利用成对代理中的 VXLAN 网段在单个 NIC 上定义外部接口和内部接口。 新增/修改的命令： **external-port**、**external-segment-id**、**internal-port**、**internal-segment-id**、**proxy paired**
AWS 网关负载均衡器对 AWS 上 ASA virtual 的 Geneve 支持	9.17(1)	添加了 Geneve 封装支持，以支持 ASAv30、ASAv50 和 ASAv100 网关负载均衡器的单臂代理。 新增/修改的命令： **调试 geneve**、 **调试 nve**、 **调试 vxlan**、 **封装**、 **数据包跟踪器 geneve**、 **代理单臂**、 **显示 asp drop**、 **显示捕获**、 **显示接口**、 **显示 nve**、

功能名称	版本	功能信息
VXLAN 支持	9.4(1)	增加了 VXLAN 支持，包括 VXLAN 隧道终端 (VTEP) 支持。每个 ASA 或安全情景可以定义一个 VTEP 源接口。 引入了以下命令：**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**

当地语言翻译版本说明

思科可能会在某些地方提供本内容的当地语言翻译版本。请注意，翻译版本仅供参考，如有任何不一致之处，以本内容的英文版本为准。