Interfaces VXLAN

Ce chapitre explique comment configurer des interfaces Virtual eXtensible LAN (VXLAN). Les VXLAN agissent comme des réseaux virtuels de couche 2 sur des réseaux physiques de couche 3 pour étendre les réseaux de couche 2.

À propos des interfaces VXLAN

Le réseau VXLAN fournit les mêmes services de réseau Ethernet de couche 2 que le réseau VLAN, mais avec une extensibilité et une flexibilité accrues. Par rapport au VLAN, le VXLAN offre les avantages suivants :

- Emplacement flexible des segments multidétenteurs dans le centre de données.
- Évolutivité accrue pour traiter un plus grand nombre de segments de couche 2 : jusqu'à 16 millions de segments VXLAN.

Cette section décrit le fonctionnement de VXLAN. Pour en savoir plus sur VXLAN, consultez RFC 7348. Pour des informations détaillées sur Geneve, consultez RFC 8926.

Encapsulation

L'ASA prend en charge deux types d'encapsulation VXLAN :

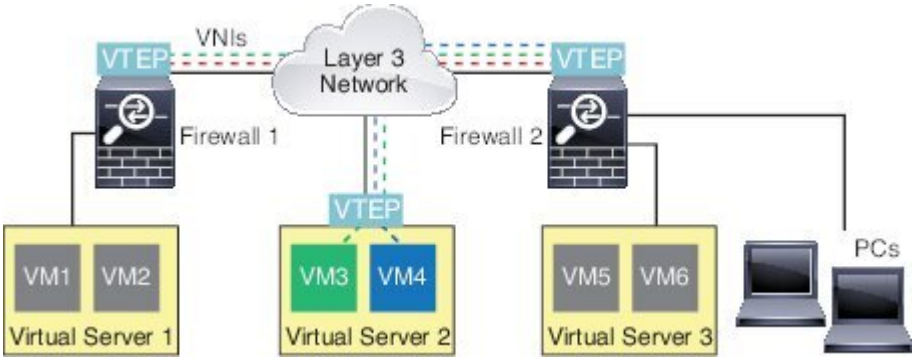
- VXLAN (tous les modèles) : VXLAN utilise l'encapsulation MAC Address-in-User Datagram Protocol (MAC-in-UDP). Un en-tête VXLAN est ajouté à la trame de couche 2 d'origine, qui est ensuite placée dans un paquet UDP-IP.

- Geneve (ASA virtuel uniquement) : Geneve a un en-tête interne flexible qui ne se limite pas à l'adresse MAC. L'encapsulation Geneve est requise pour un routage transparent des paquets entre un équilibreur de charge de passerelle Amazon Web Services (AWS) et les périphériques, et pour l'envoi d'informations supplémentaires.

Point terminal du tunnel VXLAN

Les périphériques de point terminal de tunnel VXLAN (VTEP) effectuent l'encapsulation et la désencapsulation VXLAN. Chaque VTEP a deux types d'interface : une ou plusieurs interfaces virtuelles appelées interfaces VNI (VXLAN Network Identifier) auxquelles vous appliquez votre politique de sécurité, et une interface normale appelée l'interface source VTEP qui canalise les interfaces VNI entre les VTEP. L'interface source du VTEP est connectée au réseau IP de transport pour la communication de VTEP à VTEP.

La figure suivante montre deux ASA et le serveur virtuel 2 agissant comme des VTEP dans un réseau de couche 3 et étendant les réseaux VNI 1, 2 et 3 entre les sites. Les ASA agissent comme des ponts ou des passerelles entre les réseaux VXLAN et les non-VXLAN.



Le réseau IP sous-jacent entre les VTEP est indépendant de la superposition VXLAN. Les paquets encapsulés sont acheminés en fonction de l'en-tête d'adresse IP externe, qui a le VTEP de départ comme adresse IP source et le VTEP de fin comme adresse IP de destination. Pour l'encapsulation VXLAN : l'adresse IP de destination peut être un groupe de multidiffusion lorsque le VTEP distant est inconnu. Avec Geneve, l'ASA ne prend en charge que les homologues statiques. Le port de destination de VXLAN est le port UDP 4789 par défaut (configurable par l'utilisateur). Le port de destination pour Geneve est le 6081.

Interface de la source VTEP

L'interface source de VTEP est une interface ASA normale (physique, EtherChannel ou même VLAN) à laquelle vous prévoyez d'associer toutes les interfaces VNI. Vous pouvez configurer une interface source de VTEP par ASA ou contexte de sécurité. Comme vous ne pouvez configurer qu'une seule interface source de VTEP, vous ne pouvez pas configurer les deux interfaces VXLAN et Geneve sur le même périphérique.Il y a une exception pour la mise en grappe d'ASA virtuel sur AWS, où vous pouvez avoir deux interfaces sources VTEP : une interface VXLAN est utilisée pour la liaison de commande de grappe, et une interface Geneve peut être utilisée pour l'équilibreur de charges de la passerelle.

L'interface source de VTEP peut être entièrement dédiée au trafic VXLAN, bien qu'elle ne se limite pas à cet usage. Si vous le souhaitez, vous pouvez utiliser l'interface pour le trafic normal et appliquer une politique de sécurité à l'interface pour ce trafic. Pour le trafic VXLAN, cependant, toute la politique de sécurité doit être appliquée aux interfaces VNI. L'interface VTEP sert uniquement de port physique.

En mode de pare-feu transparent, l'interface source de VTEP ne fait pas partie d'un BVI, et vous configurez une adresse IP pour elle, similaire à la façon dont l'interface de gestion est traitée.

Interface VNIs

Les interfaces VNI sont similaires aux interfaces VLAN : ce sont des interfaces virtuelles qui séparent le trafic réseau sur une interface physique donnée en utilisant le balisage. Vous appliquez votre politique de sécurité directement à chaque interface VNI.

Vous ne pouvez ajouter qu'une seule interface VTEP et toutes les interfaces VNI sont associées à la même interface VTEP.Il existe une exception pour la mise en grappe d'ASA virtuel sur AWS. Pour la mise en grappe d'AWS, vous pouvez avoir deux interfaces source VTEP : une interface VXLAN est utilisée pour la liaison de commande de grappe et une interface Geneve peut être utilisée pour AWS Gateway Load Balancer.

Traitement de paquet VXLAN

VXLAN

Le trafic entrant et sortant de l'interface source du VTEP est soumis au traitement VXLAN, en particulier à l'encapsulation ou à la désencapsulation.

Le traitement d'encapsulation comprend les tâches suivantes :

- L'interface source du VTEP encapsule la trame MAC interne avec l'en-tête VXLAN.
- Le champ de la somme de contrôle UDP est mis à zéro.
- L'adresse IP de la source de trame externe est définie sur l'adresse IP de l'interface VTEP.
- L'adresse IP de destination de la trame externe est déterminée par une recherche IP distante du VTEP.

Désencapsulation : l'ASA désencapsule un paquet VXLAN uniquement dans les cas suivants :

- Il s'agit d'un paquet UDP dont le port de destination est 4789 (cette valeur peut être configurée par l'utilisateur).
- L'interface d'entrée est l'interface source du VTEP.
- L'adresse IP de l'interface d'entrée est la même que l'adresse IP de destination.
- Le format des paquets VXLAN est conforme à la norme.

Geneve

Le trafic entrant et sortant de l'interface source du VTEP est soumis au traitement de Geneve, en particulier à l'encapsulation ou à la désencapsulation.

Le traitement d'encapsulation comprend les tâches suivantes :

- L'interface source du VTEP encapsule la trame MAC interne avec l'en-tête Geneve.
- Le champ de la somme de contrôle UDP est mis à zéro.
- L'adresse IP de la source de trame externe est définie sur l'adresse IP de l'interface VTEP.

- L’adresse IP de destination de la trame externe est définie sur l’adresse IP homologue que vous avez configurée.

Désencapsulation : l’ASA désencapsule un paquet Geneve uniquement dans les cas suivants :

- Il s’agit d’un paquet UDP dont le port de destination est 6081 (cette valeur peut être configurée par l’utilisateur).
- L’interface d’entrée est l’interface source du VTEP.
- L’adresse IP de l’interface d’entrée est la même que l’adresse IP de destination.
- Le format des paquets Geneve est conforme à la norme.

Pair VTEP

Lorsque l’ASA envoie un paquet à un périphérique derrière un VTEP homologue, l’ASA a besoin de deux renseignements importants :

- L’adresse MAC de destination du périphérique distant
- L’adresse IP de destination du VTEP homologue

L’ASA gère un mappage des adresses MAC de destination sur les adresses IP du VTEP distant pour les interfaces VNI.

Homologue VXLAN

L’ASA peut trouver ces renseignements de deux manières :

- Une adresse IP VTEP homologue unique peut être configurée de manière statique sur l’ASA.

  Vous ne pouvez pas définir manuellement plusieurs homologues.

  L’ASA envoie ensuite une diffusion ARP encapsulée dans VXLAN au VTEP pour connaître l’adresse MAC du nœud d’extrémité.

- Un groupe de multidiffusion peut être configuré sur chaque interface VNI (ou sur le VTEP dans son ensemble).

Remarque Cette option n’est pas prise en charge par Geneve.

: l’ASA envoie un paquet de diffusion ARP encapsulé dans VXLAN dans un paquet IP de multidiffusion par l’intermédiaire de l’interface source de VTEP. La réponse à cette requête ARP permet à l’ASA d’apprendre à la fois l’adresse IP du VTEP distant ainsi que l’adresse MAC de destination du nœud d’extrémité distant.

Homologue Geneve

L’ASA virtuel ne prend en charge que les homologues définis de manière statique. Vous pouvez définir l’adresse IP homologue ASA virtuel sur l'équilibreur de charge de passerelle AWS. Comme l’ASA virtuel n’initie jamais le trafic vers l’équilibreur de charges de passerelle, vous n’avez pas besoin de préciser l’adresse

IP de l'équilibreur de charges de passerelle sur l'ASA virtuel; il connaît l'adresse IP homologue lorsqu'il reçoit le trafic de Geneve. Les groupes de multidiffusion ne sont pas pris en charge avec Geneve.

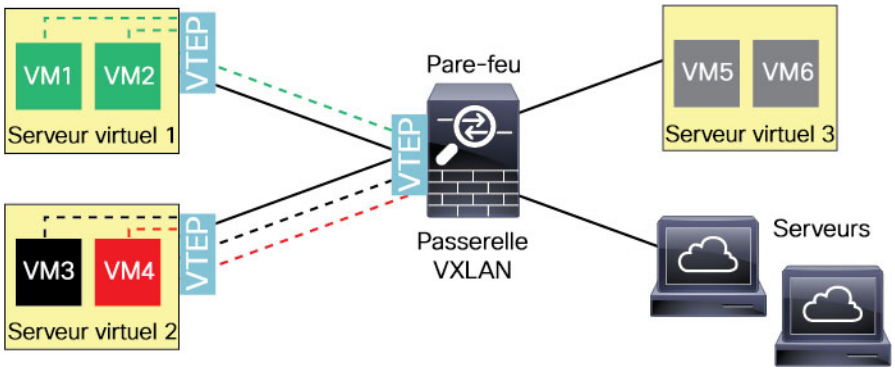
Scénarios VXLAN

Cette section décrit les scénarios d'utilisation de la mise en œuvre de VXLAN sur l'ASA.

Présentation du pont ou de la passerelle VXLAN

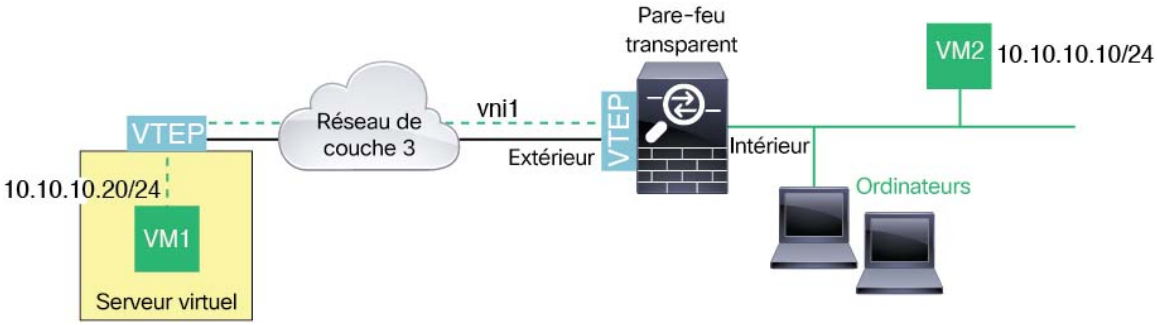
Chaque VTEP ASA agit comme un pont ou une passerelle entre les nœuds terminaux comme les machines virtuelles, les serveurs et les PC et le réseau de superposition VXLAN. Pour les trames entrantes reçues avec encapsulation VXLAN sur l'interface source de VTEP, ASA supprime l'en-tête VXLAN et le transfère vers une interface physique connectée à un réseau non VXLAN en fonction de l'adresse MAC de destination de la trame Ethernet interne.

L'ASA traite toujours les paquets VXLAN; il ne se contente pas de transférer des paquets VXLAN inchangés entre deux autres VTEP.



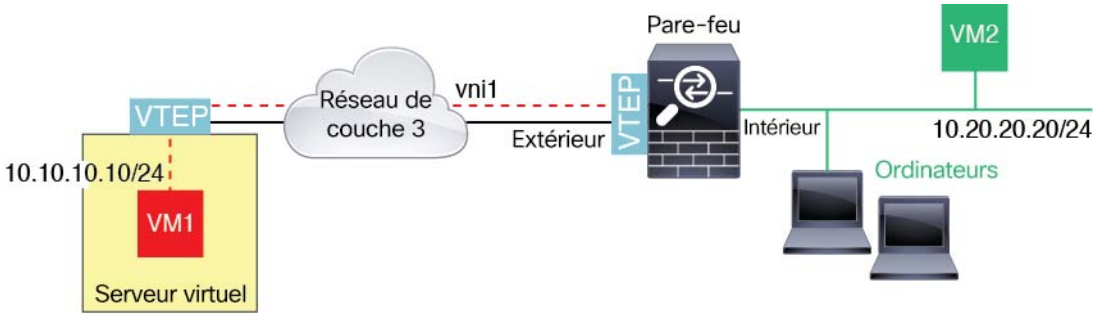
Pont VXLAN

Lorsque vous utilisez un groupe de ponts (mode de pare-feu transparent ou mode de routage facultatif), ASA peut servir de pont VXLAN entre un segment VXLAN (distant) et un segment local, où les deux se trouvent dans le même réseau. Dans ce cas, un membre du groupe de ponts est une interface standard tandis que l'autre membre est une interface VNI.



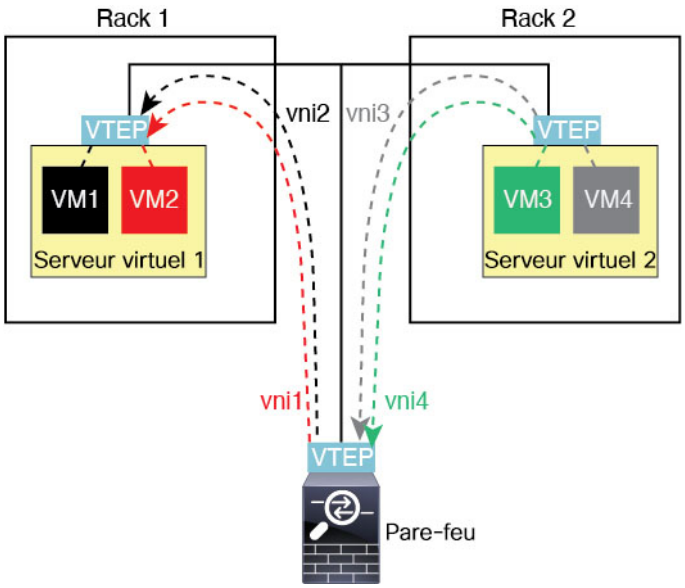
Passerelle VXLAN (mode routé)

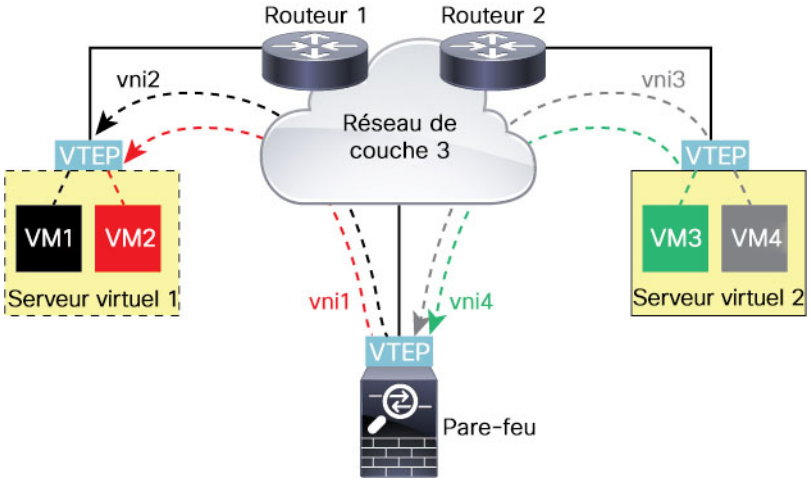
L'ASA peut servir de routeur entre les domaines VXLAN et non-VXLAN, connectant des périphériques sur différents réseaux.



Routeur entre domaines VXLAN

Avec un domaine de couche 2 étendu par VXLAN, une machine virtuelle peut pointer vers un ASA comme passerelle lorsque ASA ne se trouve pas sur le même rack, ou même lorsque l'ASA est éloigné sur le réseau de couche 3.





Consultez les remarques suivantes à propos de ce scénario :

1. Pour les paquets de la VM3 à la VM1, l'adresse MAC de destination est l'adresse MAC ASA, car l'ASA est la passerelle par défaut.
2. L'interface source de VTEP sur le serveur virtuel 2 reçoit les paquets de VM3, puis encapsule les paquets avec la balise VXLAN de VNI 3 et les envoie à l'ASA.
3. Lorsque l'ASA reçoit les paquets, il désencapsule les paquets pour obtenir les trames internes.
4. L'ASA utilise les cadres internes pour la recherche de routage, puis trouve que la destination est sur VNI 2. S'il n'a pas encore de mappage pour VM1, l'ASA envoie une diffusion ARP encapsulée sur l'adresse IP du groupe de multidiffusion sur VNI 2.

Remarque L'ASA doit utiliser la découverte d'homologues VTEP dynamique, car il a plusieurs homologues VTEP dans ce scénario.

5. L'ASA encapsule de nouveau les paquets avec la balise VXLAN pour VNI 2 et envoie les paquets au serveur virtuel 1. Avant l'encapsulation, l'ASA modifie l'adresse MAC de destination de la trame interne pour qu'elle corresponde à l'adresse MAC de VM1 (l'ARP encapsulé en multidiffusion peut être nécessaire pour que l'ASA apprenne l'adresse MAC de VM1).
6. Lorsque le serveur virtuel 1 reçoit les paquets VXLAN, il désencapsule les paquets et achemine les trames internes à la VM1.

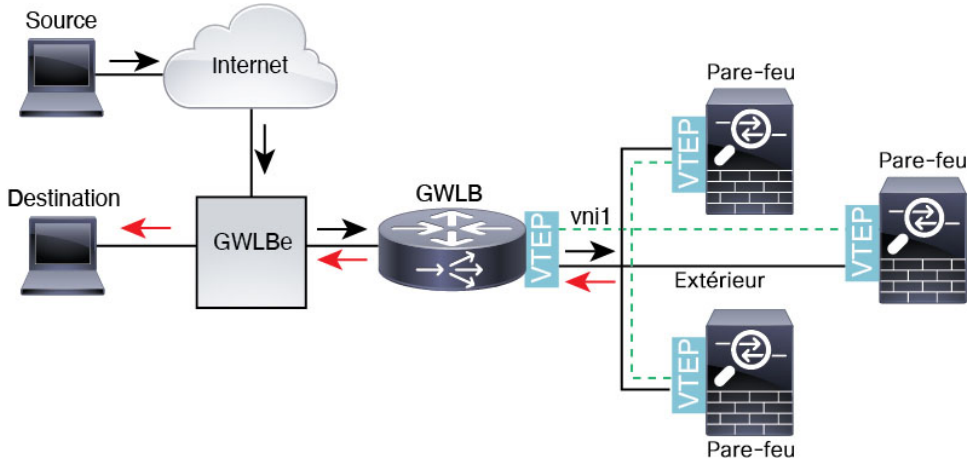
Équilibreur de charge de passerelle AWS et serveur mandataire à un seul volet de Geneve

Remarque Ce scénario est le seul actuellement pris en charge pour les interfaces de Geneve.

L'équilibreur de charge de passerelle AWS combine une passerelle de réseau transparente et un équilibreur de charge qui répartit le trafic et fait évoluer les périphériques virtuels à la demande. Le ASA virtuel prend en charge le plan de contrôle centralisé de l'équilibreur de charge de passerelle avec un plan de données distribué (point terminal de l'équilibreur de charge de passerelle). La figure suivante montre le trafic acheminé

vers l'équilibreur de charge de passerelle à partir du point terminal de l'équilibreur de charge de passerelle. L'équilibreur de charge de passerelle équilibre le trafic entre plusieurs ASA virtuel, qui inspectent le trafic avant de l'abandonner ou de le renvoyer à l'équilibreur de charge de passerelle (trafic à demi-tour). L'équilibreur de charge de passerelle renvoie ensuite le trafic au point terminal de l'équilibreur de charge de passerelle et à la destination.

Illustration 1 : Serveur mandataire à un seul volet Geneve

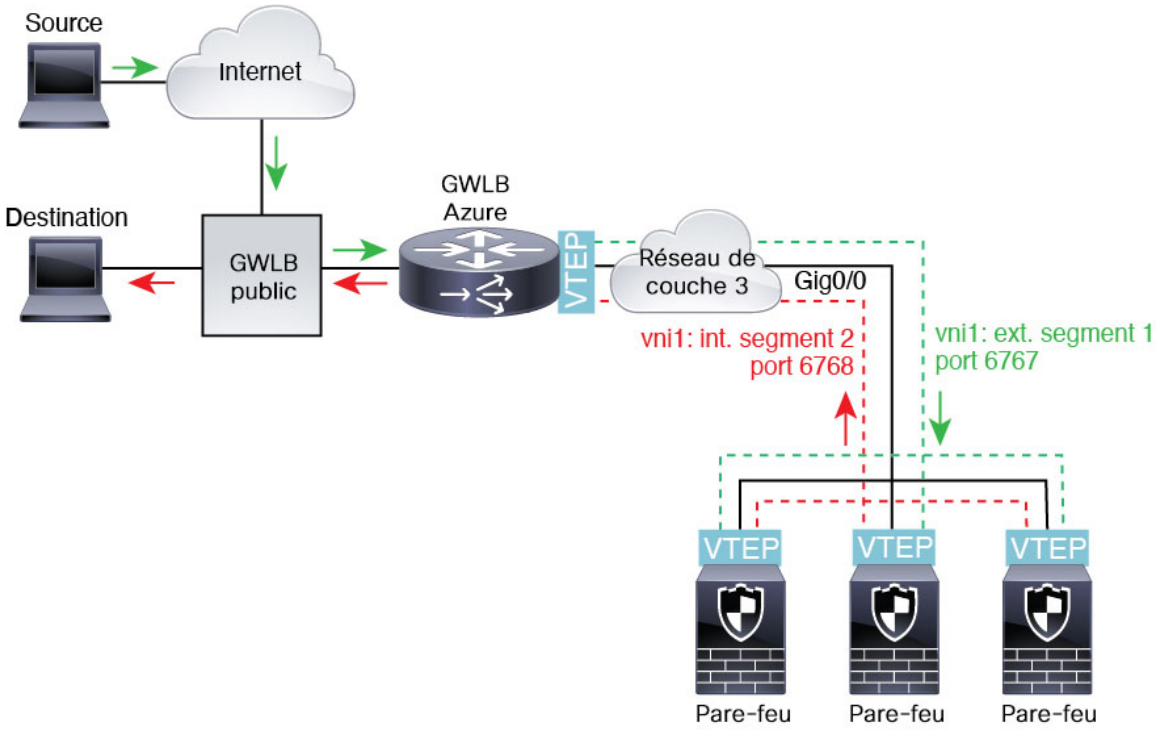


Équilibreur de charge de passerelle Azure et serveur mandataire jumelé

Dans une chaîne de service Azure, les ASA virtuelagissent comme une passerelle transparente qui peut intercepter les paquets entre Internet et le service client. Le ASA virtuel définit une interface externe et une interface interne sur une seule carte réseau en utilisant les segments VXLAN dans un serveur mandataire apparié.

La figure suivante montre le trafic transféré vers l'équilibreur de charge de passerelle Azure à partir de l'équilibreur de charge de passerelle publique sur le segment VXLAN externe. L'équilibreur de charge de passerelle équilibre le trafic entre plusieurs ASA virtuel, qui inspectent le trafic avant de l'abandonner ou de le renvoyer à l'équilibreur de charge de passerelle sur le segment VXLAN interne. L'équilibreur de charge de passerelle Azure renvoie ensuite le trafic vers l'équilibreur de charge de passerelle publique et vers la destination.

Illustration 2 : Équilibreur de charge de passerelle Azure avec mandataire jumelé



Exigences et conditions préalables pour les interfaces VXLAN

Exigences du modèle

- Les ports de commutation Firepower 1010 et les interfaces VLAN ne sont pas pris en charge en tant qu'interfaces VTEP.
- L'encapsulation Geneve est prise en charge pour les modèles suivants : ASAv30, ASAv50, ASAv100 sur Amazon Web Services (AWS)
- Le réseau VXLAN en mode proxy jumelé est pris en charge pour les modèles suivants :
  - ASA virtuel dans Azure

Lignes directrices pour les interfaces VXLAN

Mode pare-feu

- Les interfaces Geneve ne sont prises en charge qu'en mode de pare-feu routé.
- Les interfaces VXLAN mandataires jumelées ne sont prises en charge qu'en mode de pare-feu routé.

IPv6

- L'interface VNI prend en charge le trafic IPv4 et IPv6.
- L'adresse IP de l'interface source VTEP prend uniquement en charge IPv4.

Mise en grappe et mode de contexte multiple

- La mise en grappe d'ASA ne prend pas en charge VXLAN en mode d'interface individuelle, sauf pour la liaison de commande de grappe (ASA virtuel seulement). Seul le mode EtherChannel étendu prend en charge VXLAN.

  Une exception est faite pour l'ASA virtuel sur AWS, qui peut utiliser une interface Geneve supplémentaire à utiliser avec GWLB.
- Les interfaces Geneve ne sont prises en charge qu'en mode en mode de contexte unique. Elles ne sont pas prises en charge avec le mode de contexte multiple.

Routage

- Seul le routage statique ou le routage basé sur des politiques est pris en charge sur l'interface VNI; les protocoles de routage dynamique ne sont pas pris en charge.

VPN

Vous ne pouvez pas configurer l'interface source VTEP pour le VPN ou l'utiliser comme VTI.

MTU

- Encapsulation VXLAN : si la MTU de l'interface source est inférieure à 1 554 octets pour IPv4 ou à 1 574 octets pour IPv6 ou 1 574 octets. Dans ce cas, le datagramme Ethernet entier est encapsulé, de sorte que le nouveau paquet est plus volumineux et nécessite une MTU plus grande. Si la MTU utilisée par d'autres périphériques est supérieure, vous devez définir la MTU de l'interface source comme étant la MTU du réseau + 54 octets. Cette MTU nécessite l'activation de la réservation de bâti grand format sur certains modèles; voir Activez la prise en charge des bâtis grand format (ASA virtuel et ISA 3000).
- Encapsulation Geneve : si la MTU de l'interface source est inférieure à 1 806 octets, l'ASA fait automatiquement passer la MTU à 1 806 octets. Dans ce cas, le datagramme Ethernet entier est encapsulé, de sorte que le nouveau paquet est plus volumineux et nécessite une MTU plus grande. Si la MTU utilisée par d'autres périphériques est supérieure, vous devez définir la MTU de l'interface source comme étant la MTU du réseau + 306 octets. Cette MTU nécessite l'activation de la réservation de bâti grand format sur certains modèles; voir Activez la prise en charge des bâtis grand format (ASA virtuel et ISA 3000).

Paramètres par défaut des interfaces VXLAN

Les interfaces VNI sont activées par défaut.

Configurer les interfaces VXLAN

Pour configurer les interfaces VXLAN, procédez comme suit.

Remarque Vous pouvez configurer VXLAN ou Geneve (ASA virtuel uniquement). Pour les interfaces Geneve, consultez Configurer les interfaces Geneve, à la page 16.

Procédure

Étape 1 Configurer l'interface source VTEP, à la page 11.

Étape 2 Configurer l'interface VNI, à la page 13

Étape 3 (Facultatif) Modifier le port UDP VXLAN, à la page 16.

Étape 4 (Azure GWLB) Autoriser les vérifications de l'intégrité de l'équilibreur de charges de la passerelle, à la page 19.

Configurer l'interface source VTEP

Vous pouvez configurer une interface source de VTEP par ASA ou par contexte de sécurité. Le VTEP est défini comme un terminal de virtualisation de réseau (NVE).

Avant de commencer

Pour le mode de contexte multiple, effectuez cette procédure dans l'espace d'exécution du système. Saisissez la commande **changeto context** *name* pour remplacer le contexte que vous souhaitez configurer.

Procédure

Étape 1 (Mode transparent) Spécifiez que l'interface source est NVE uniquement :

interface *id*

nve-only

Exemple :

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

Ce paramètre vous permet de configurer une adresse IP pour l'interface. Cette commande est facultative pour le mode routé où ce paramètre limite le trafic à VXLAN et au trafic de gestion commun uniquement sur cette interface.

Étape 2 Configurez le nom de l'interface source et l'adresse IPv4 .

Exemple :

(Mode routé)

```
ciscoasa(config)# interface gigabitethernet 1/1
```

```
ciscoasa(config-if)# nameif outside
ciscoasa(config-if)# ip address 10.1.1.1 255.255.255.0
```

Exemple :

(Mode transparent)

```
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
```

Étape 3 Spécifiez l'instance NVE :

nve 1

Vous ne pouvez spécifier qu'une seule instance NVE, avec l'ID 1.

Exemple :

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

Étape 4 Spécifiez l'encapsulation VXLAN.

encapsulation vxlan

Exemple :

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

Étape 5 Spécifiez le nom de l'interface source que vous avez configuré à l'étape 2 :

source-interface *interface-name*

Exemple :

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

Remarque
Si la MTU de l'interface VTEP est inférieure à 1 554 octets, l'ASA augmente automatiquement la MTU à 1 554 octets.

Étape 6 (Mode de contexte multiple; facultatif pour le mode unique) Spécifiez manuellement l'adresse IP VTEP de l'homologue :

peer ip *ip_address*

Exemple :

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

Si vous spécifiez l'adresse IP de l'homologue, vous ne pouvez pas utiliser la découverte de groupe de multidiffusion. La multidiffusion n'est pas prise en charge en mode de contexte multiple, la configuration manuelle est donc la seule option. Vous ne pouvez définir qu'un seul homologue pour le VTEP.

Étape 7 (Facultatif; mode unique seulement) Spécifiez un groupe de multidiffusion par défaut pour toutes les interfaces VNI associées :

default-mcast-group *mcast_ip*

Exemple :

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

Si vous ne configurez pas le groupe de multidiffusion par interface VNI, ce groupe est utilisé. Si vous configurez un groupe au niveau de l'interface VNI, ce groupe remplace ce paramètre.

Configurer l'interface VNI

Ajoutez une interface VNI, associez-la à l'interface source VTEP et configurez les paramètres de l'interface de base.

Pour l'ASA virtuel dans Azure, vous pouvez configurer une interface VXLAN standard ou une interface VXLAN en mode de mandataire jumelé à utiliser avec la GWLB Azure.

Procédure

Étape 1 Créez l'interface VNI :

interface vni *vni_num*

Exemple :

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

Définissez l'ID entre 1 et 10 000. Cet ID est uniquement un identifiant d'interface interne.

Étape 2 (VXLAN standard) Spécifiez l'ID de segment VXLAN :

segment-id *ID*

Exemple :

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

Définissez l'ID entre 1 et 16777215. L'ID de segment est utilisé pour le balisage VXLAN.

Étape 3 (Serveur mandataire VXLAN jumelé pour Azure GWLB) Activez le mode de mandataire jumelé et définissez les paramètres requis.

a) Activez le mode de mandataire jumelé.

proxy paired

Exemple :

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

b) Définissez le port interne.

internal-port *port_number*

Lorsque le paramètre *port_number* est compris entre 1024 et 65535.

Exemple :

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

c) Définissez l'ID de segment interne.

internal-segment-id *id_number*

Lorsque le paramètre *id_number* est compris entre 1 et 16777215.

Exemple :

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

d) Définissez le port externe.

external-port *port_number*

Lorsque le paramètre *port_number* est compris entre 1024 et 65535.

Exemple :

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

e) Définissez l'ID de segment externe.

external-segment-id *id_number*

Lorsque le paramètre *id_number* est compris entre 1 et 16777215.

Exemple :

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

f) Autorisez le trafic à entrer et à sortir de la même interface.

same-security-traffic permit intra-interface

Exemple :

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

Étape 4 (Obligatoire pour le mode transparent) Spécifiez le groupe de ponts auquel vous souhaitez associer cette interface :

bridge-group *number*

Exemple :

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

Consultez Configurer les interfaces de groupe de ponts pour configurer l'interface BVI et associer des interfaces standard à ce groupe de ponts.

Étape 5 Associez cette interface à l'interface source VTEP :

vtep-nve 1

Étape 6 Nommez l'interface :

nameif *vni_interface_name*

Exemple :

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

Le *nom* est une chaîne de texte de 48 caractères maximum et n'est pas sensible à la casse. Vous pouvez modifier le nom en saisissant à nouveau cette commande avec une nouvelle valeur. Ne saisissez pas la forme **no** (non), car cette commande entraîne la suppression de toutes les commandes qui font référence à ce nom.

Étape 7 (Mode routé) Attribuez une adresse IPv4 et/ou IPv6 :

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

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

Exemple :

```
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
```

Étape 8 Définissez le niveau de sécurité :

security-level *level*

Exemple :

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

Où *number* est un entier compris entre 0 (le plus bas) et 100 (le plus élevé).

Étape 9 (Mode unique) Définissez l'adresse du groupe de multidiffusion :

mcast-group *multicast_ip*

Exemple :

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

Si vous ne définissez pas le groupe de multidiffusion pour l'interface VNI, le groupe par défaut de la configuration de l'interface source VTEP est utilisé, s'il est disponible. Si vous définissez manuellement une

adresse IP homologue VTEP pour l'interface source de VTEP, vous ne pouvez pas spécifier de groupe de multidiffusion pour l'interface VNI. La multidiffusion n'est pas prise en charge en mode de contexte multiple.

(Facultatif) Modifier le port UDP VXLAN

Par défaut, l'interface source VTEP accepte le trafic VXLAN vers le port UDP 4789. Si votre réseau utilise un port non standard, vous pouvez le modifier.

Avant de commencer

Pour le mode de contexte multiple, effectuez cette tâche dans l'espace d'exécution du système. Pour passer du contexte à l'espace d'exécution du système, saisissez la commande **changeto system**.

Procédure

Définissez le port UDP VXLAN :

vxlan *port number*

Exemple :

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

Configurer les interfaces Geneve

Pour configurer les interfaces de Geneve pour ASA virtuel, procédez comme suit.

Remarque Vous pouvez configurer VXLAN ou Geneve. Pour les interfaces VXLAN, consultez Configurer les interfaces VXLAN, à la page 10.

Procédure

Étape 1 Configurer l'interface source VTEP pour Geneve, à la page 17.

Étape 2 Configurer l'interface VNI pour Geneve, à la page 18

Étape 3 Autoriser les vérifications de l'intégrité de l'équilibreur de charges de la passerelle, à la page 19.

Configurer l'interface source VTEP pour Geneve

Vous pouvez configurer une interface source de VTEP par ASA virtuel. Le VTEP est défini comme un point terminal de virtualisation du réseau (NVE).

Procédure

Étape 1 (Facultatif) Indiquez que l'interface source est NVE uniquement.

interface *id*

nve-only

Exemple :

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

Ce paramètre limite le trafic à VXLAN et au trafic de gestion commun uniquement sur cette interface.

Étape 2 Configurez le nom de l'interface source et l'adresse IPv4.

Exemple :

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

Étape 3 Spécifiez l'instance NVE :

nve 1

Vous ne pouvez spécifier qu'une seule instance NVE, avec l'ID 1.

Exemple :

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

Étape 4 Spécifiez l'encapsulation Geneve.

encapsulation geneve

Ne modifiez pas le port Geneve; AWS nécessite un port 6081.

Exemple :

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

Étape 5 Spécifiez le nom de l'interface source que vous avez configuré à l'étape 2 :

source-interface *interface-name*

Exemple :

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

Remarque
Si la MTU de l'interface source est inférieure à 1 806 octets, l'ASA augmente automatiquement la MTU à 1 806 octets.

Configurer l'interface VNI pour Geneve

Ajoutez une interface VNI, associez-la à l'interface source VTEP et configurez les paramètres de l'interface de base.

Procédure

Étape 1 Créez l'interface VNI :

interface vni *vni_num*

Exemple :

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

Définissez l'ID entre 1 et 10 000. Cet ID est uniquement un identifiant d'interface interne.

Étape 2 Associez cette interface à l'interface source VTEP :

vtep-nve 1

Étape 3 Nommez l'interface :

nameif *vni_interface_name*

Exemple :

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

Le *nom* est une chaîne de texte de 48 caractères maximum et n'est pas sensible à la casse. Vous pouvez modifier le nom en saisissant à nouveau cette commande avec une nouvelle valeur. Ne saisissez pas la forme **no** (non), car cette commande entraîne la suppression de toutes les commandes qui font référence à ce nom.

Étape 4 Attribuez une adresse IPv4 et/ou IPv6 :

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

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

Geneve ne prend en charge qu'une adresse IP statique.

Exemple :

```
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
```

Étape 5 Définissez le niveau de sécurité :

security-level *level*

Où *level* est un entier compris entre 0 (le plus bas) et 100 (le plus élevé).

Exemple :

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

Étape 6 Activez le serveur mandataire à un seul volet .

proxy single-arm

Exemple :

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

Étape 7 Autorisez le trafic à entrer et à sortir de la même interface.

same-security-traffic permit intra-interface

Exemple :

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

Autoriser les vérifications de l'intégrité de l'équilibreur de charges de la passerelle

L'équilibreur de charges de la passerelle AWS ou Azure nécessite des périphériques pour répondre correctement à une vérification de l'intégrité. L'équilibreur de charges de la passerelle AWS enverra uniquement le trafic vers des périphériques considérés comme intègres.

Vous devez configurer l'ASA virtuel pour répondre à une vérification de l'intégrité SSH, HTTP ou HTTPS.

Connexion SSH

Pour SSH, autorisez SSH à partir de l'équilibreur de charges de la passerelle. L'équilibreur de charges de la passerelle tentera d'établir une connexion à ASA virtuel, et l'invite de connexion de ASA virtuel est considérée comme une preuve de l'intégrité.

Remarque Une tentative de connexion SSH expirera après 1 minute. Vous devrez configurer un intervalle de vérification de l'intégrité plus long sur l'équilibreur de charges de la passerelle pour tenir compte de ce délai.

Exemple

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

```
ssh 10.0.1.0 255.255.255.0 outside
```

Connexion Telnet

Pour Telnet, autorisez Telnet à partir de l'équilibreur de charges de la passerelle. L'équilibreur de charges de la passerelle tentera d'établir une connexion à ASA virtuel, et l'invite de connexion de ASA virtuel est considérée comme une preuve de l'intégrité.

Remarque Vous ne pouvez pas vous connecter via Telnet à l'interface du niveau de sécurité le plus bas, donc cette méthode peut ne pas être pratique.

Exemple

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

Mandataire direct HTTP(S)

Vous pouvez configurer l'ASA pour demander à l'équilibreur de charges de la passerelle de vous connecter par HTTP(S).

Exemple

```
! 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
```

Redirection HTTP(S) à l'aide de la NAT d'interface statique avec traduction de port

Vous pouvez configurer ASA virtuel pour rediriger les vérifications de l'intégrité vers un serveur HTTP(S) de métadonnées. Pour les vérifications de l'intégrité HTTP(S), le serveur HTTP(S) doit répondre à l'équilibreur de charges de la passerelle avec un code d'état compris entre 200 et 399. Étant donné que l'ASA virtuel a des limites sur le nombre de connexions de gestion simultanées, vous pouvez choisir de décharger le contrôle de l'intégrité sur un serveur externe.

La NAT d'interface statique avec traduction de port vous permet de rediriger une connexion vers un port (comme le port 80) vers une adresse IP différente. Par exemple, traduisez un paquet HTTP de l'équilbreur de charges de la passerele avec la destination de l'interface externe ASA virtuel de sorte qu'il semble provenir de l'interface externe ASA virtuel avec la destination du serveur HTTP. Le ASA virtuel transfère ensuite le paquet vers l'adresse de destination mappée. Le serveur HTTP répond à l'interface externe ASA virtuel, puis ASA virtuel renvoie la réponse à l'équilibreur de charges de la passerelle. Vous avez besoin d'un critère d'accès qui autorise le trafic de l'équilibreur de charges de la passerelle vers le serveur HTTP.

Exemple

```
! 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
```

Supervision des interfaces VXLAN

Consultez les commandes suivantes pour superviser les interfaces VTEP et VNI.

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

  Cette commande affiche les paramètres, l'état et les statistiques d'une interface NVE, l'état de son interface de transport (interface source), l'adresse IP de l'interface de transport, les VNI qui utilisent ce NVE comme le VXLAN VTEP et les adresses IP VTEP des pairs associées à cette interface NVE. Avec l'option **summary**, cette commande affiche uniquement l'état de l'interface NVE, le nombre de VNI derrière l'interface NVE et le nombre de VTEP découverts.

  Consultez la sortie suivante pour la commande **show nve 1** :

```
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
```

  Consultez la sortie suivante pour la commande **show nve 1 summary** :

```
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**]

  Cette commande affiche les paramètres, l'état et les statistiques d'une interface VNI, l'état de son interface pontée (si configurée) et l'interface NVE à laquelle elle est associée. L'option **summary** affiche uniquement les paramètres d'interface VNI.

  Consultez la sortie suivante pour la commande **show interface vni 1** :

```
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
```

  Consultez la sortie suivante pour la commande **show interface vni 1 summary** :

```
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**

  Cette commande affiche le mappage entre les ID de segment VNI et les interfaces VLAN ou les interfaces physiques. Cette commande n'est valide qu'en mode de pare-feu transparent, car en mode routé, le mappage entre les VXLAN et les VLAN peut inclure trop de valeurs à afficher.

  Consultez la sortie suivante pour la commande **show vni vlan-mapping** :

```
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**

Cette commande affiche les adresses MAC mises en mémoire cache sur l'interface VNI pour les adresses IP situées dans le domaine de segment distant et les adresses IP VTEP distantes.

Consultez la sortie suivante pour la commande **show arp vtep-mapping** :

```
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**

  Cette commande affiche le tableau de transfert de couche 2 (table d'adresses MAC) sur l'interface VNI avec les adresses IP VTEP distantes.

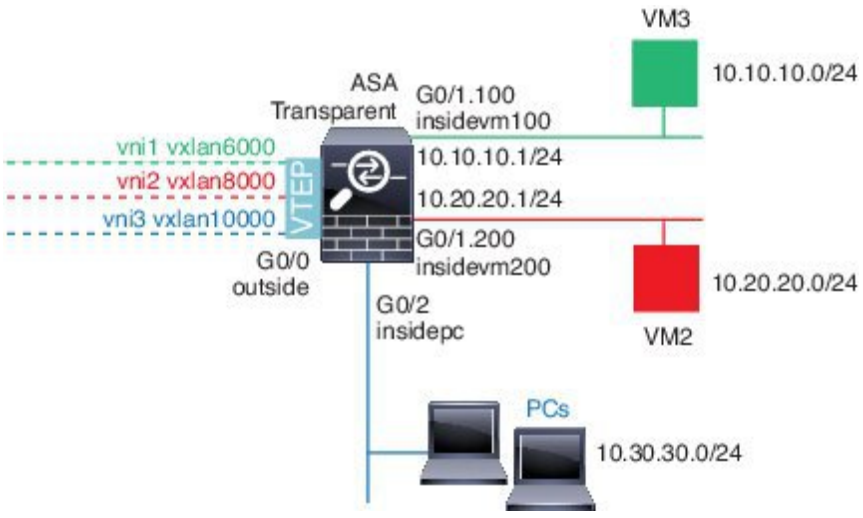
  Consultez la sortie suivante pour la commande **show mac-address-table vtep-mapping** :

```
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
```

Exemples d'interfaces VXLAN

Consultez les exemples de configuration suivants pour VXLAN.

Exemple de passerelle VXLAN transparente



Consultez la description suivante de cet exemple :

- L'interface externe sur GigabitEthernet 0/0 est utilisée comme interface source VTEP et est connectée au réseau de couche 3.

- La sous-interface VLAN insidevm100 sur GigabitEthernet 0/1.100 est connectée au réseau 10.10.10.0/24, sur lequel réside VM3. Lorsque VM3 communique avec VM1 (non affiché; les deux ont des adresses IP 10.10.10.0/24), l'ASA utilise la balise VXLAN 6000.
- La sous-interface VLAN insidevm200 sur GigabitEthernet 0/1.200 est connectée au réseau 10.20.20.0/24, sur lequel réside VM2. Lorsque VM2 communique avec VM4 (non affiché; les deux ont des adresses IP 10.20.20.0/24), l'ASA utilise la balise VXLAN 8000.
- L'interface insidepc de GigabitEthernet 0/2 est connectée au réseau 10.30.30.0/24 sur lequel se trouvent quelques ordinateurs. Lorsque ces ordinateurs communiquent avec des VM/PC (non affichés) derrière un VTEP distant qui appartient au même réseau (tous ont des adresses IP 10.30.30.0/24), l'ASA utilise la balise VXLAN 10000.

Configuration ASA

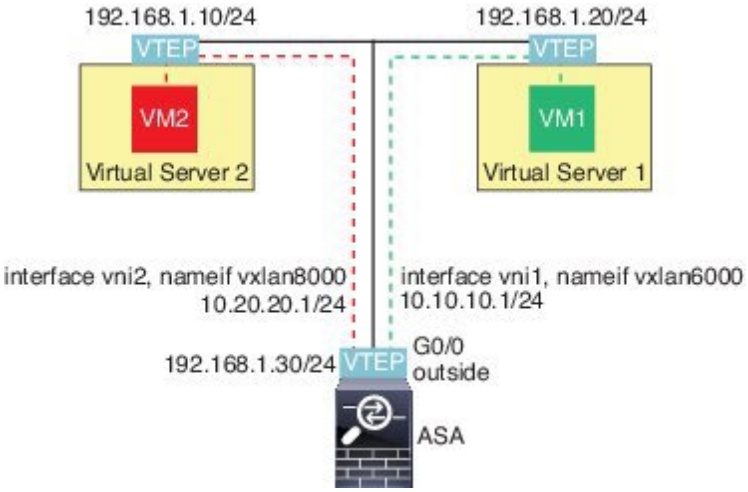
```
firewall transparent
vxlan port 8427
!
interface gigabitethernet0/0
  nve-only
  nameif outside
  ip address 192.168.1.30 255.255.255.0
  no shutdown
!
nve 1
  encapsulation vxlan
  source-interface outside
!
interface vni1
  segment-id 6000
  nameif vxlan6000
  security-level 0
  bridge-group 1
  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
```

Notes

- Pour les interfaces VNI vni1 et vni2, la balise VLAN interne est supprimée pendant l'encapsulation.
- Les interfaces VNI vni2 et vni3 partagent la même adresse IP de multidiffusion pour l'ARP encapsulé sur la multidiffusion. Ce partage est autorisé.
- L'ASA relie le trafic VXLAN vers des interfaces non prises en charge par VXLAN en fonction des BVI et des configurations de groupes de ponts ci-dessus. Pour chacun des segments de réseau étendus de couche 2 (10.10.10.0/24, 10.20.20.0/24 et 10.30.30.0/24), l'ASA sert de pont.
- Il est autorisé d'avoir plusieurs VNI ou plusieurs interfaces standard (VLAN ou simplement interface physique) dans un groupe de ponts. Le transfert ou l'association entre l'ID de segment VXLAN et l'ID de VLAN (ou une interface physique) est décidé par l'adresse MAC de destination et l'interface qui se connecte à la destination.
- L'interface source VTEP est une interface de couche 3 en mode de pare-feu transparent, indiquée par **nve-only** dans la configuration de l'interface. L'interface source VTEP n'est pas une interface BVI ni une interface de gestion, mais elle a une adresse IP et utilise la table de routage.

Exemple de routage VXLAN



Consultez la description suivante de cet exemple :

- VM1 (10.10.10.10) est hébergé sur le serveur virtuel 1 et VM2 (10.20.20.20) est hébergé sur le serveur virtuel 2.
- La passerelle par défaut pour VM1 est l'ASA, qui ne se trouve pas dans le même module que le serveur virtuel 1, mais VM1 ne le sait pas. VM1 sait uniquement que l'adresse IP de sa passerelle par défaut est 10.10.10.1. De même, VM2 sait uniquement que l'adresse IP de sa passerelle par défaut est 10.20.20.1.
- Les hyperviseurs pris en charge par le VTEP sur les serveurs virtuels 1 et 2 peuvent communiquer avec l'ASA sur le même sous-réseau ou par l'intermédiaire d'un réseau de couche 3 (non illustré; dans ce cas, l'ASA et les liaisons ascendantes des serveurs virtuels ont des adresses réseau différentes).
- Le paquet de VM1 sera encapsulé par le VTEP de son hyperviseur et envoyé à sa passerelle par défaut sur la tunnellisation VXLAN.
- Lorsque VM1 envoie un paquet à VM2, le paquet sera envoyé par la passerelle par défaut 10.10.10.1 de son point de vue. Le serveur virtuel 1 sait que la passerelle 10.10.10.1 n'est pas locale; par conséquent, le VTEP encapsule le paquet sur VXLAN et l'envoie au VTEP de l'ASA.
- Sur l'ASA, le paquet est désencapsulé. L'ID de segment VXLAN est appris lors de la désencapsulation. L'ASA réinjecte ensuite le cadre interne dans l'interface VNI (vni1) correspondante en fonction de l'ID de segment VXLAN. L'ASA effectue ensuite une recherche de route et envoie le paquet interne par une autre interface VNI, vni2. Tous les paquets sortants par vni2 sont encapsulés avec le segment VXLAN 8000 et envoyés par le VTEP à l'extérieur.
- Finalement, le paquet encapsulé est reçu par le VTEP du serveur virtuel 2, qui le désencapsule et le transfère à VM2.

Configuration ASA

```
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
!
```

Historique des interfaces VXLAN

Tableau 1 : Historique des interfaces VXLAN

Nom de la caractéristique	Versions	Renseignements sur les fonctionnalités
Proxy jumelé VXLAN pour l'ASA virtuel pour l'équilibreur de charges de la passerelle Azure.	9.19(1)	Vous pouvez configurer une interface VXLAN en mode proxy apparié pour l'ASA virtuel dans Azure afin de l'utiliser avec l'équilibreur de charges de la passerelle Azure (GWLB). L'ASA virtuel définit une interface externe et une interface interne sur un seul NIC en utilisant des segments VXLAN dans un serveur mandataire jumelé. Commandes nouvelles/modifiées : **port externe, segment-id externe, port interne, segment-id interne, proxy paired**
Prise en charge de Geneve pour le ASA virtuel sur AWS pour l'équilibreur de charges de la passerelle AWS	9.17(1)	La prise en charge de l'encapsulation Geneve a été ajoutée pour l'ASAv30, ASAv50 et ASAv100 afin de prendre en charge le serveur mandataire à un seul volet pour l'équilibreur de charges de passerelle AWS. Commandes nouvelles ou modifiées : **debug geneve**, **debug nve**, **debug vxlan**, **encapsulation**, **packet-tracer geneve**, **proxy single-arm**, **show asp drop**, **show capture**, **show interface**, **show nve**
Prise en charge de VXLAN	9.4(1)	La prise en charge de VXLAN a été ajoutée, y compris la prise en charge du terminal de tunnel VXLAN (VTEP). Vous pouvez définir une interface source VTEP par ASA ou contexte de sécurité. Nous avons introduit les commandes suivantes : **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**

À propos de la traduction

Cisco peut fournir des traductions du présent contenu dans la langue locale pour certains endroits. Veuillez noter que des traductions sont fournies à titre informatif seulement et, en cas d’incohérence, la version anglaise du présent contenu prévaudra.