



# レイヤ4-レイヤ7ネットワークサービスの統合の設定

この章は、次の内容で構成されています。

- [VXLAN レイヤ4-レイヤ7サービスについて \(1 ページ\)](#)
- [VXLAN ファブリックでのレイヤ3 ファイアウォールの統合 \(2 ページ\)](#)
- [デフォルト ゲートウェイとしてのファイアウォール \(16 ページ\)](#)
- [トランスペアレント ファイアウォール挿入 \(17 ページ\)](#)
- [VXLAN BGP EVPN を使用したファイアウォールクラスタリング \(23 ページ\)](#)
- [VXLAN EVPN ファブリックのサービス リダイレクト \(27 ページ\)](#)

## VXLAN レイヤ4-レイヤ7サービスについて

この章では、VXLAN ファブリックへのレイヤ4〜レイヤ7ネットワーク サービス（ファイアウォール、ロード バランサなど）の挿入について説明します。

L4-L7 サービスがデフォルト ゲートウェイ（集約/配信）をホストするスイッチに接続されている従来の3層ネットワーク トポロジとは異なり、VXLAN ファブリック内の L4-L7 サービスは通常、しばしばサービス リーフと呼ばれる、リーフ スイッチまたは境界スイッチに接続されます。

L4-L7 サービス デバイスは、さまざまな方法で VXLAN ファブリックに接続できます。この章では、L4-L7 サービス デバイスの接続方法、およびデバイスとネットワークの要件に応じて考慮すべき事項について説明します。

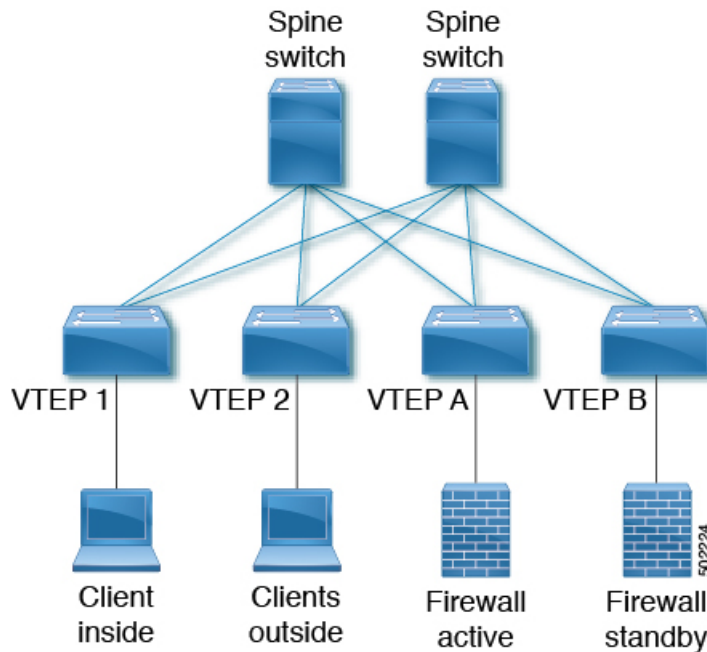
# VXLAN ファブリックでのレイヤ3 ファイアウォールの統合

ここでは、VXLAN EVPN ファブリック内にファイアウォールを統合する方法について詳しく説明します。レイヤ3ファイアウォールでは、異なるセキュリティゾーンを分離する必要があります。

VXLAN EVPN ファブリックにレイヤ3ファイアウォールを分散型エニーキャストゲートウェイと統合する場合、これらの各ゾーンはファブリック上のVRF/テナントに対応する必要があります。テナント内のトラフィックは、ファブリックによってルーティングされます。テナント間のトラフィックは、ファイアウォールによってルーティングされます。このシナリオは、多くの場合、テナント間またはテナントエッジファイアウォールに関連しています。

内部ゾーンと外部ゾーンの2つのゾーンを検討します。このシナリオでは、ファブリック上のVRF定義が必要です。VRFを内部VRFおよび外部VRFと呼ぶことができます。同じVRF内のサブネット間のトラフィックは、分散ゲートウェイを使用してVXLANファブリックでルーティングされます。VRF間のトラフィックは、ルールが適用されるファイアウォールによってルーティングされます。

図1: ファイアウォール接続を使用したトポロジの概要



## 静的ルーティングを使用するシングル接続ファイアウォール

ファイアウォールがルーティングプロトコルの実行をサポートしていない場合は、各VTEPにネクストホップとしてファイアウォールを指す静的ルートが必要です。ファイアウォールに

は、ネクスト ホップとしてエニーキャスト ゲートウェイ IP を指す静的ルートもあります。静的ルートの課題は、アクティブファイアウォールを備えたVTEPが、ファブリックへのルートをアドバタイズする必要があることです。これを実現する1つの方法は、HMM を介してアクティブなファイアウォールの到達可能性を追跡し、この追跡を使用してルートをファブリックにアドバタイズすることです。アクティブなファイアウォールがVTEP A に接続されている場合、VTEP A には、ファイアウォール IP がHMM ルートとして学習された場合にルートがアドバタイズされる場所を追跡する静的ルートがあります。ファイアウォールに障害が発生し、スタンバイファイアウォールが引き継ぐと、VTEP A はBGP を使用してファイアウォール IP を学習し、VTEP B はHMM を使用してファイアウォール IP を学習します。VTEP A はルートを取り消し、VTEP B はファブリックにルートをアドバタイズします。次の例を参照してください。

#### VTEP A および VTEP B:

```
Vlan 10
  Name inside
  Vn-segment 10010

Vlan 20
  Name outside
  Vn-segment 10020

Interface VLAN 10
  Description inside_vlan
  VRF member INSIDE
  IP address 10.1.1.254/24
  fabric forwarding mode anycast-gateway

Interface VLAN 20
  Description outside_vlan
  VRF member OUTSIDE
  IP address 20.1.1.254/24
  fabric forwarding mode anycast-gateway

interface nve1
  no shutdown
  host-reachability protocol bgp
  source-interface loopback1
  member vni 10010
    mcastgroup 239.1.1.1
  member vni 10020
    mcastgroup 239.1.1.1
  member vni 1001000 associate-vrf
  member vni 1002000 associate-vrf

track 10 ip route 10.1.1.1/32 reachability hmm
  vrf member INSIDE
!
VRF context INSIDE
  Vni 1001000
  IP route 20.1.1.0/24 10.1.1.1 track 10

track 20 ip route 20.1.1.1/32 reachability hmm
  vrf member OUTSIDE

!
VRF context OUTSIDE
```

## ファブリックの残りの部分に配布される再帰静的ルート

```

Vni 1001000
IP route 10.1.1.0/24 20.1.1.1 track 20

VTEPA# show track 10 Track 10
IP Route 20.1.1.1/32 Reachability Reachability is UP

VTEPA# show ip route 20.1.1.0/24 vrf INSIDE
IP Route Table for VRF "INSIDE"
'*' denotes best ucast next-hop
 '**' denotes best mcast next-hop
 '[x/y]' denotes [preference/metric]
 '%<string>' in via output denotes VRF <string>

20.1.1.0/24, ubest/mbest: 1/0
  *via 10.1.1.1 [1/0], 00:00:08, static

Firewall Failure on VTEP A caused the track to go down causing VTEP A to withdraw the
static route.

VTEPA# show track 20 Track 20
IP Route 20.1.1.1/32 Reachability Reachability is DOWN

VTEPA# show ip route 20.1.1.0/24 vrf INSIDE
IP Route Table for VRF "RED"
'*' denotes best ucast next-hop
 '**' denotes best mcast next-hop
 '[x/y]' denotes [preference/metric]
 '%<string>' in via output denotes VRF <string>

Route not found

```

## ファブリックの残りの部分に配布される再帰静的ルート

このアプローチでは、内部または外部 VRF が存在する場所に静的ルートが設定されます。ネクストホップはホストルート (EVPN Route-Type2) を介して到達可能であるため、アクティブファイアウォールのスタンバイへの変更、およびその逆の変更はローカルでのみ行われ、他の VXLAN ファブリックにチャーンは発生しません。このアプローチは、拡張性の向上とコンバージェンスの向上に役立ちます。

### 任意の VTEP :

```

VRF context OUTSIDE
  Vni 1002000
  IP route 10.1.1.0/24 20.1.1.1
  ! static route on VTEP pointing to Firewall next hop
  ! firewall VIP 20.1.1.1

VRF context INSIDE
  Vni 1001000
  IP route 20.1.1.0/24 10.1.1.1
  ! static route on VTEP pointing to Firewall next hop
  ! firewall VIP 10.1.1.1

```

## スタティックルートを BGP に再配布し、残りのファブリックにアドバタイズする

再配布によって、示されているアクティブなファイアウォールへのルートを、それが存在する VTEP に作成します。ルートはプレフィックスルート (EVPN Route-Type5) と見なされ、アク

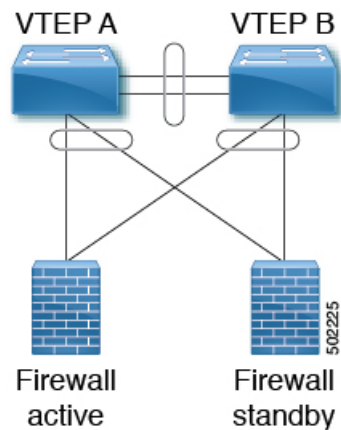
タイプなファイアウォールがあるVTEPへのルートのみが表示されます。ファイアウォールのアクティブ/スタンバイ変更の場合、トラッキングは変更を検出し、この変更をすべてのリモートVTEPに通知する必要があります。この動作は、ルートが「削除」され、その後に「追加」されることに相当します。このアプローチでは、VRFを使用してすべてのVTEPに通知する必要があります。このアプローチでは、より大きなチャーンが見られます。

#### VTEP A および VTEP B:

```
router bgp 65000
vrf OUTSIDE
address-family ipv4 unicast
redistribute static route-map Static-to-BGP
```

## 静的ルーティングを使用するデュアル接続ファイアウォール

図 2: 静的ルーティングを使用するデュアル接続ファイアウォール



#### VTEP A および VTEP B:

```
Vlan 10
Name inside
Vn-segment 10010

Vlan 20
Name outside
Vn-segment 10020

interface nve1
no shutdown
host-reachability protocol bgp
source-interface loopback1
member vni 10010
mcastgroup 239.1.1.1
member vni 10020
mcastgroup 239.1.1.1
member vni 1001000 associate-vrf
member vni 1002000 associate-vrf

Interface VLAN 10
Description inside_vlan
```

```

VRF member INSIDE
IP address 10.1.1.254/24
fabric forwarding mode anycast-gateway

Interface VLAN 20
Description outside_vlan
VRF member OUTSIDE
IP address 20.1.1.254/24
fabric forwarding mode anycast-gateway

VRF context INSIDE
Vni 1001000
IP route 20.1.1.0/24 10.1.1.1
! static route on VTEP pointing to Firewall next hop
! firewall VIP 10.1.1.1
VRF context OUTSIDE
Vni 1002000
IP route 10.1.1.0/24 20.1.1.1
! static route on VTEP pointing to Firewall next hop
! firewall VIP 20.1.1.1

router bgp 65000
vrf INSIDE
address-family ipv4 unicast
redistribute static route-map INSIDE-to-BGP
vrf OUTSIDE
address-family ipv4 unicast
redistribute static route-map OUTSIDE-to-BGP

```

## eBGP ルーティングを使用するシングル接続ドファイアウォール

ファイアウォールがBGPをサポートしている場合、1つのオプションは、ファイアウォールとサービス VTEP 間のプロトコルとして BGP を使用することです。エニーキャスト IP を使用したピアリングはサポートされていません。推奨される設計は、ループバックを使用して各 VTEP およびピアで専用ループバック IP を使用することです。ループバック インターフェイスが EVPN を介してアドバタイズされない限り、同じ IP アドレスをすべての属する VTEP で使用できます。VTEP 単位で個々の IP アドレスを使用することを推奨します。

ファイアウォールからループバックへの到達可能性は、VTEP 上のエニーキャストゲートウェイ IP を指すファイアウォール上のスタティック ルートを使用して設定できます。

次の例では、AS 65000 にある VTEP と AS 65002 にあるファイアウォールから eBGP ピアリングが確立されます。iBGP との BGP ピアリングはサポートされていません。



(注) 異なる VTEP に接続されたアクティブ/スタンバイファイアウォールへの **export-gateway-ip** を有効にする必要があります。

BGP ピアリングにエニーキャスト ゲートウェイを使用しないでください。

### VTEP A:

```

Vlan 10
Name inside

```

```
Vn-segment 10010

Vlan 20
Name outside
Vn-segment 10020

Interface VLAN 10
Description inside_vlan
VRF member INSIDE
IP address 10.1.1.254/24
fabric forwarding mode anycast-gateway

Interface loopback100
Vrf member INSIDE
Ip address 172.16.1.253/32

Interface VLAN 20
Description outside_vlan
VRF member OUTSIDE
IP address 20.1.1.254/24
fabric forwarding mode anycast-gateway

Interface loopback101
Vrf member OUTSIDE
Ip address 172.18.1.253/32

router bgp 65000
vrf INSIDE
! peer with Firewall Inside
neighbor 10.1.1.0/24 remote-as 65123
update-source loopback100
ebgp-multihop 5
address-family ipv4 unicast
local-as 65051 no-prepend replace-as

vrf OUTSIDE
! peer with Firewall Outside
neighbor 20.1.1.0/24 remote-as 65123
update-source loopback101
ebgp-multihop 5
address-family ipv4 unicast
local-as 65052 no-prepend replace-as
```

**VTEP B :**

```
Vlan 10
Name inside
Vn-segment 10010

Vlan 20
Name outside
Vn-segment 10020
Interface VLAN 10
Description inside_vlan
VRF member INSIDE
IP address 10.1.1.254/24
fabric forwarding mode anycast-gateway

Interface loopback100
Vrf member INSIDE
Ip address 172.16.1.254/32
```

```
Interface VLAN 20
Description outside_vlan
VRF member OUTSIDE
IP address 20.1.1.254/24
fabric forwarding mode anycast-gateway

Interface loopback101
Vrf member OUTSIDE
Ip address 172.18.1.254/32

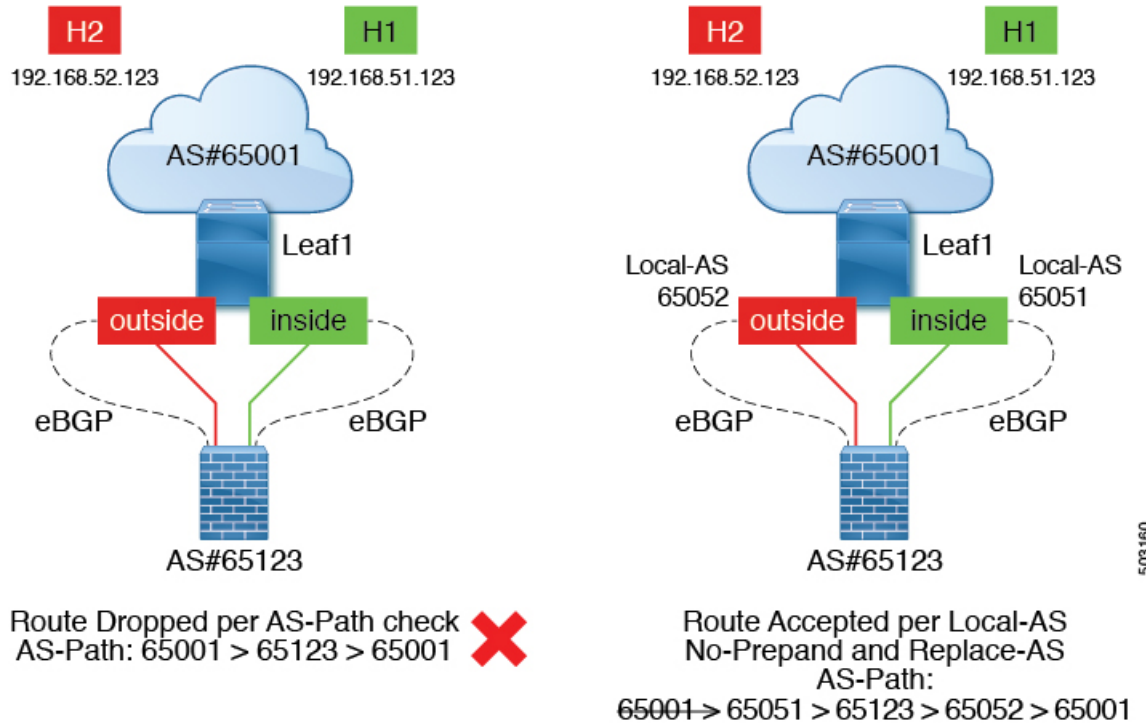
router bgp 65000
vrf INSIDE
! peer with Firewall Inside
neighbor 10.1.1.0/24 remote-as 65123
update-source loopback100
ebgp-multihop 5
address-family ipv4 unicast
local-as 65051 no-prepend replace-as

vrf OUTSIDE
! peer with Firewall Outside
neighbor 20.1.1.0/24 remote-as 65123
update-source loopback101
ebgp-multihop 5
address-family ipv4 unicast
local-as 65052 no-prepend replace-as
```

通常、VXLAN ファブリックは単一の BGP 自律システム (AS) 内にあるため、内部 VRF と外部 VRF の AS は同じです。BGP は、自身の AS から受信したルートをインストールしません。したがって、このルールをオーバーライドするには、AS パスを調整する必要があります。BGP が自身の AS からルートをドロップするというルールを無効にするなど、さまざまなアプローチが存在します。これは、ネットワークにさらに影響を与えます。すべての BGP 保護メカニズムを維持するために、「local-as」アプローチでは、異なる AS から発信されたルートを模倣できます。VRF ごとに異なる「local-as」を持つ各ファイアウォールピアリングに「local-as # ASN # no-prepend replace-as」を挿入することを推奨します。



図 3: eBGP AS-Path チェック



503160

## eBGP ルーティングを使用するデュアル接続ファイアウォール

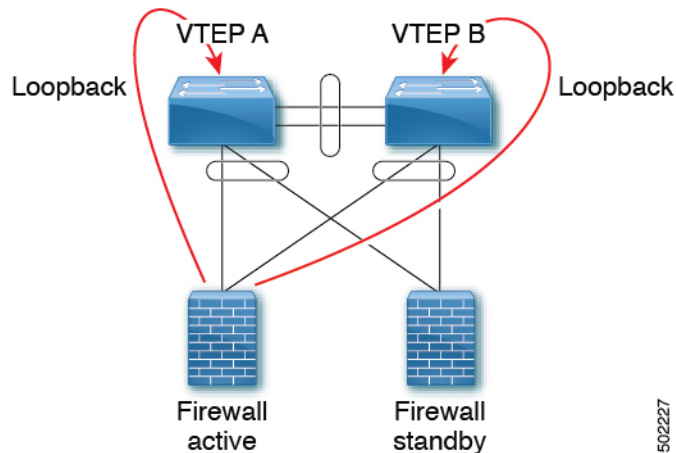
ファイアウォールがBGPをサポートしている場合、1つのオプションは、ファイアウォールとサービスVTEP間のプロトコルとしてBGPを使用することです。エニーキャストIPを使用したピアリングはサポートされていません。推奨される設計は、ループバックを使用して各VTEPおよびピアで専用ループバックIPを使用することです。ループバックインターフェイスがEVPNを介してアドバタイズされない限り、同じIPアドレスをすべての属するVTEPで使用できます。VTEP単位で個々のIPアドレスを使用することを推奨します。vPC環境の場合は必須です。

ファイアウォールからループバックへの到達可能性は、VTEP上のエニーキャストゲートウェイIPを指すファイアウォール上のスタティックルートを使用して設定できます。

vPC導入では、vPCピアリングを介したVRFごとのピアリングが必要です。VRF単位のピアリングに加えて、**advertise-pip**コマンドを使用してプレフィックスルートのアドバタイズメント(EVPNルートタイプ5)を有効にできます。ファブリックピアリングを使用するvPCの場合、VRFごとのピアリングは必要なく、プレフィックスルートのアドバタイズメント(EVPN Route-Type5)が必要です。

次の例では、AS 65000にあるVTEPとAS 65002にあるファイアウォールからeBGPピアリングが確立されます。iBGPとのBGPピアリングはサポートされていません。

図 4: eBGP を使用したデュアル接続ファイアウォール



(注) 異なる VTEP に接続されたアクティブ/スタンバイファイアウォールへの **export-gateway-ip** を有効にする必要があります。

BGP ピアリングにエニーキャスト ゲートウェイを使用しないでください。

#### VTEP A:

```
Vlan 10
Name inside
Vn-segment 10010

Vlan 20
Name outside
Vn-segment 10020

Interface VLAN 10
Description inside_vlan
VRF member INSIDE
IP address 10.1.1.254/24
fabric forwarding mode anycast-gateway

Interface loopback100
Vrf member INSIDE
Ip address 172.16.1.253/32

Interface VLAN 20
Description outside_vlan
VRF member OUTSIDE
IP address 20.1.1.254/24
fabric forwarding mode anycast-gateway

Interface loopback101
Vrf member OUTSIDE
Ip address 172.18.1.253/32

router bgp 65000
vrf INSIDE
```

```
! peer with Firewall Inside
neighbor 10.1.1.0/24 remote-as 65123
update-source loopback100
ebgp-multihop 5
address-family ipv4 unicast
  local-as 65051 no-prepend replace-as

vrf OUTSIDE
! peer with Firewall Outside
neighbor 20.1.1.0/24 remote-as 65123
update-source loopback101
ebgp-multihop 5
address-family ipv4 unicast
  local-as 65052 no-prepend replace-as
```

**VTEP B :**

```
Vlan 10
Name inside
Vn-segment 10010

Vlan 20
Name outside
Vn-segment 10020

Interface VLAN 10
Description inside_vlan
VRF member INSIDE
IP address 10.1.1.254/24
fabric forwarding mode anycast-gateway

Interface loopback100
Vrf member INSIDE
Ip address 172.16.1.254/32

Interface VLAN 20
Description outside_vlan
VRF member OUTSIDE
IP address 20.1.1.254/24
fabric forwarding mode anycast-gateway

Interface loopback101
Vrf member OUTSIDE
Ip address 172.18.1.254/32

router bgp 65000
vrf INSIDE
! peer with Firewall Inside
neighbor 10.1.1.0/24 remote-as 65123
update-source loopback100
ebgp-multihop 5
address-family ipv4 unicast
  local-as 65051 no-prepend replace-as

vrf OUTSIDE
! peer with Firewall Outside
neighbor 20.1.1.0/24 remote-as 65123
update-source loopback101
ebgp-multihop 5
address-family ipv4 unicast
  local-as 65052 no-prepend replace-as
```

## vPC ピアリンクによる Per-VRF ピアリング

### VTEP A および VTEP B:

```

vlan 3966
! vlan use for peering between the vPC VTEPS

vlan 3967
! vlan use for peering between the vPC VTEPS

system nve infra-vlans 3966,3967

interface vlan 3966
vrf member INSIDE
ip address 100.1.1.1/31

interface vlan 3967
vrf member OUTSIDE
ip address 100.1.2.1/31

router bgp 65000
vrf INSIDE
neighbor 100.1.1.0 remote-as 65000
update-source vlan 3966
next-hop self
address-family ipv4 unicast

vrf OUTSIDE
neighbor 100.1.2.0 remote-as 65000
update-source vlan 3967
next-hop self
address-family ipv4 unicast

```

各 VRF で学習されたルートは、BGP EVPN 更新を介してファブリックの残りの部分にアドバタイズされます。

## OSPF を使用したシングル接続ファイアウォール

次の例は、ファイアウォールで OSPF ピアリングを実行している VTEP A からの設定スニペットを示しています。

SVI は、内部および外部の両方の VRF の VTEP で定義されます。これらの各 VRF 上のファイアウォールを持つ VTEP ピアは、1 つの VRF から別の VRF に移動するためのルーティング情報を動的に学習します。

### VTEP A および VTEP B:

```

vlan 10
name inside
vn-segment 10010

vlan 20
name outside
vn-segment 10020

interface VLAN 10
Description inside_vlan
VRF member INSIDE
IP address 10.1.1.254/24

```

```

IP router ospf 1 area 0
fabric forwarding mode anycast-gateway

Interface VLAN 20
Description outside_vlan
VRF member OUTSIDE
IP address 20.1.1.254/24
IP router ospf 1 area 0
fabric forwarding mode anycast-gateway

interface nve1
no shutdown
host-reachability protocol bgp
source-interface loopback1
member vni 10010
  mcastgroup 239.1.1.1
member vni 10020
  mcastgroup 239.1.1.1
member vni 1001000 associate-vrf
member vni 1002000 associate-vrf

router ospf 1
router-id 192.168.1.1
vrf INSIDE
VRF OUTSIDE

VTEPA# show ip route ospf-1 vrf OUTSIDE
IP Route Table for VRF "OUTSIDE"
'*' denotes best ucast next-hop
'***' denotes best mcast next-hop
'[x/y]' denotes [preference/metric]
'%<string>' in via output denotes VRF <string>

10.1.1.0/24, ubest/mbest: 1/0
  *via 20.1.1.1 Vlan20, [110/41], 1w5d, ospf-1, intra

VTEPA# show ip route ospf-1 vrf INSIDE
IP Route Table for VRF "INSIDE"
'*' denotes best ucast next-hop
'***' denotes best mcast next-hop
'[x/y]' denotes [preference/metric]
'%<string>' in via output denotes VRF <string>

20.1.1.0/24, ubest/mbest: 1/0
  *via 10.1.1.1 Vlan10, [110/41], 1w5d, ospf-1, intra

```

次に、このルートはBGPに再配布され、EVPNファブリックを介してアドバタイズされます。これにより、他のすべてのVTEPが、ネクストホップとしてVTEP Aをポイントする各VRF内のすべてのルートを持つようになります。

## OSPF ルートを BGP に再配布し、残りのファブリックにアドバタイズする

### VTEP A および VTEP B:

```

router bgp 65000
vrf OUTSIDE
  address-family ipv4 unicast
    redistribute ospf 1 route-map OUTSIDEOSPF-to-BGP
vrf INSIDE
  address-family ipv4 unicast
    redistribute ospf 1 route-map INSIDEOSPF-to-BGP

```

```
VTEPA# show ip route 10.1.1.0/24 vrf OUTSIDE
10.1.1.0/24 ubest/mbest: 1/0
  *via 10.1.1.18%default, [200/41], 1w1d, bgp-65000, internal, tag 65000 (evpn) segid:
200100 tunnelid: 0xa010112 encap: VXLAN
```

トラフィックは、VTEP からサービス VTEP にカプセル化された VXLAN であり、カプセル化解除されてファイアウォールに送信されます。ファイアウォールはルールを適用し、トラフィックを内部 VRF のサービス VTEP に送信します。このトラフィックは VXLAN でカプセル化され、宛先 VTEP に送信されます。宛先 VTEP では、トラフィックがカプセル化解除されてエンドクライアントに送信されます。

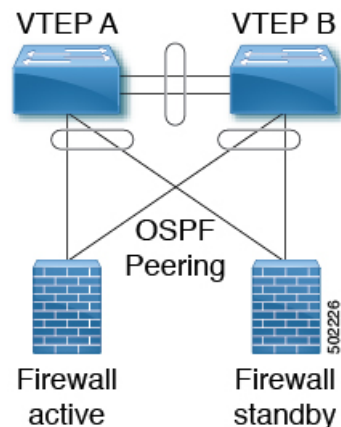
#### ファイアウォール フェールオーバー

アクティブ ファイアウォールに障害が発生し、スタンバイ ファイアウォールが引き継ぐと、ルートはサービス VTEP A から取り消され、サービス VTEP B によってファブリックにアドバタイズされます。

## OSPF を使用したデュアル接続ファイアウォール

Cisco NX-OS は、レイヤ3 を使用した vPC 経由のダイナミック OSPF ピアリングをサポートします。これにより、vPC を使用したファイアウォール接続が可能になり、このリンク上で OSPF ピアリングが確立されます。Cisco Nexus 9000 スイッチとファイアウォール間のピアリングを確立するために使用される VLAN は、非 VXLAN 対応 VLAN である必要があります。

図 5: OSPF を使用したデュアル接続ファイアウォール



(注) OSPF 隣接にはエニーキャスト ゲートウェイを使用しないでください。

#### VTEP A:

```
Vlan 10
Name inside
```

```
Vlan 20
  Name outside

Interface VLAN 10
  Description inside_vlan
  VRF member INSIDE
  IP address 10.1.1.253/24
  Ip router ospf 1 area 0

Interface VLAN 20
  Description outside_vlan
  VRF member OUTSIDE
  IP address 20.1.1.253/24
  Ip router ospf 1 area 0

vpc domain 100
  layer3 peer-router
  peer-gateway
  peer-switch
  peer-keepalive destination x.x.x.x source x.x.x.x peer-gateway
  ipv6 nd synchronize
  ip arp synchronize

router ospf 1
  vrf INSIDE VRF OUTSIDE
```

**VTEP B :**

```
Vlan 10
  Name inside

Vlan 20
  Name outside

Interface VLAN 10
  Description inside_vlan
  VRF member INSIDE
  IP address 10.1.1.254/24
  Ip router ospf 1 area 0

Interface VLAN 20
  Description outside_vlan
  VRF member OUTSIDE
  IP address 20.1.1.254/24
  Ip router ospf 1 area 0

vpc domain 100
  layer3 peer-router
  peer-gateway
  peer-switch
  peer-keepalive destination x.x.x.x source x.x.x.x peer-gateway
  ipv6 nd synchronize
  ip arp synchronize

router ospf 1
  vrf INSIDE VRF OUTSIDE

VTEPA# show ip route ospf-1 vrf OUTSIDE
IP Route Table for VRF "OUTSIDE"
'*' denotes best ucast next-hop
'***' denotes best mcast next-hop
'[x/y]' denotes [preference/metric]
'%<string>' in via output denotes VRF <string>
```

## OSPF ルートを BGP に再配布し、残りのファブリックにアドバタイズする

```

10.1.1.0/24, ubest/mbest: 1/0
  *via 20.1.1.1 Vlan20, [110/41], 1w5d, ospf-1, intra

VTEPA# show ip route ospf-1 vrf INSIDE
IP Route Table for VRF "INSIDE"
'*' denotes best ucast next-hop
 '**' denotes best mcast next-hop
 '[x/y]' denotes [preference/metric]
 '%<string>' in via output denotes VRF <string>

20.1.1.0/24, ubest/mbest: 1/0
  *via 10.1.1.1 Vlan10, [110/41], 1w5d, ospf-1, intra

```

## OSPF ルートを BGP に再配布し、残りのファブリックにアドバタイズする

## VTEP A および VTEP B:

```

router bgp 65000
 vrf OUTSIDE
  address-family ipv4 unicast
    redistribute ospf 1 route-map OUTSIDEOSPF-to-BGP
 vrf INSIDE
  address-family ipv4 unicast
    redistribute ospf 1 route-map INSIDEOSPF-to-BGP

```

## デフォルト ゲートウェイとしてのファイアウォール

この導入モデルでは、VXLAN ファブリックはレイヤ2 ファブリックであり、デフォルトゲートウェイはファイアウォール上にあります。

次に例を示します。

```

vlan 10
  name WEB
  vn-segment 10010
vlan 20
  name APPLICATION
  vn-segment 10020
vlan 30
  name DATABASE
  vn-segment 10030

interface nve1
  no shutdown
  host-reachability protocol bgp
  source-interface loopback1
  member vni 10010
    mcastgroup 239.1.1.1
  member vni 10020
    mcastgroup 239.1.1.1
  member vni 10030
    mcastgroup 239.1.1.1

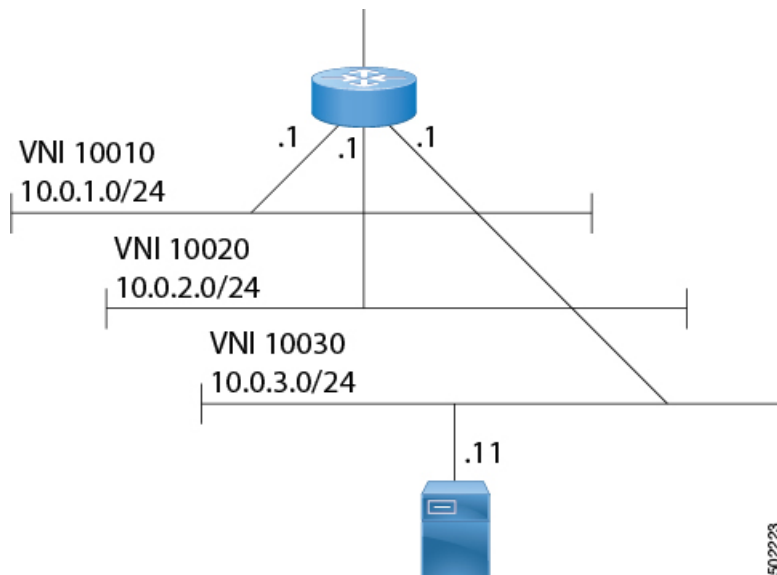
```

ファイアウォールは、各 VNI に論理インターフェイスを持ち、すべてのエンドポイントのデフォルトゲートウェイです。すべての VNI 間通信はファイアウォールを通過します。ファイ



ファイアウォールがボトルネックにならないように、ファイアウォールのサイジングには特に注意してください。したがって、この設計は、低帯域幅要件の環境で使用してください。

図 6: レイヤ 2 VXLAN ファブリックを使用したデフォルトゲートウェイとしてのファイアウォール



## トランスペアレントファイアウォール挿入

トランスペアレントファイアウォールまたはレイヤ2ファイアウォール（IPS/IDSを含む）は、通常、内部VLANと外部VLANをブリッジし、トラフィックが通過するときに検査します。VLANスウィッチングは、サービスのデフォルトゲートウェイを内部VLANに配置することによって行われます。このゲートウェイへのレイヤ2の到達可能性は、外部VLANで行われます。

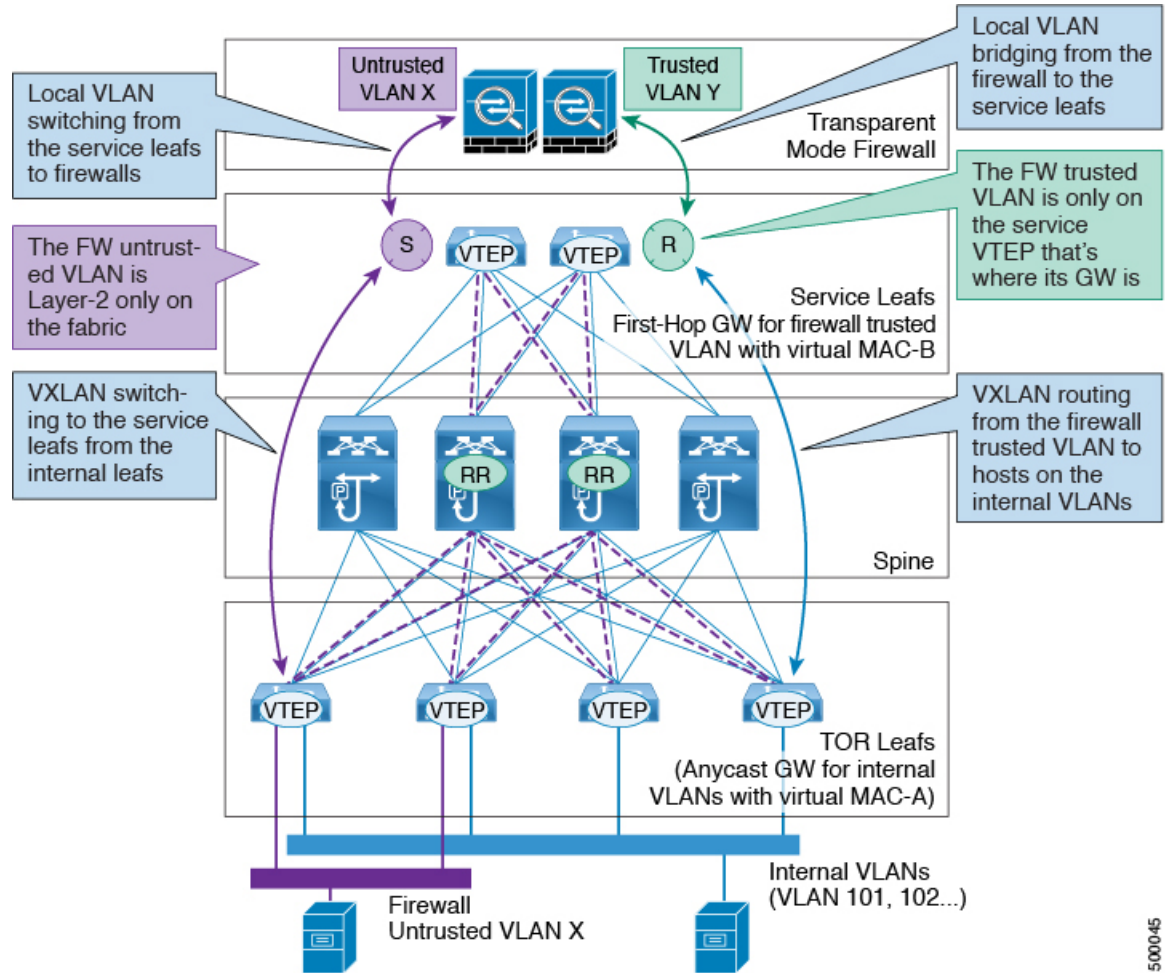
## EVPNでのトランスペアレントファイアウォール挿入の概要

トポロジには、次のタイプのVLANが含まれます。

- 内部VLAN（通常のVXLANをToRリーフにエニーキャストゲートウェイ付きで配置）
- ファイアウォール非信頼VLAN X
- ファイアウォール信頼VLAN Y

このトポロジにおいて、VLAN Xから他のVLANへのトラフィックは、サービスリーフに接続されているトランスペアレントレイヤ2ファイアウォールを経由する必要があります。このトポロジは、信頼できないVLAN Xと信頼できるVLAN Yのアプローチを使用します。すべてのToRリーフにはレイヤ2VNI VLAN Xがあります。VLAN XのSVIはありません。ファイアウォールに接続されているサービスリーフにはレイヤ2VNI VLAN X、非VXLANVLAN Y、およびHSRPゲートウェイを使用するSVI Yがあります。

## EVPNでのトランスペアレントファイアウォール挿入の概要



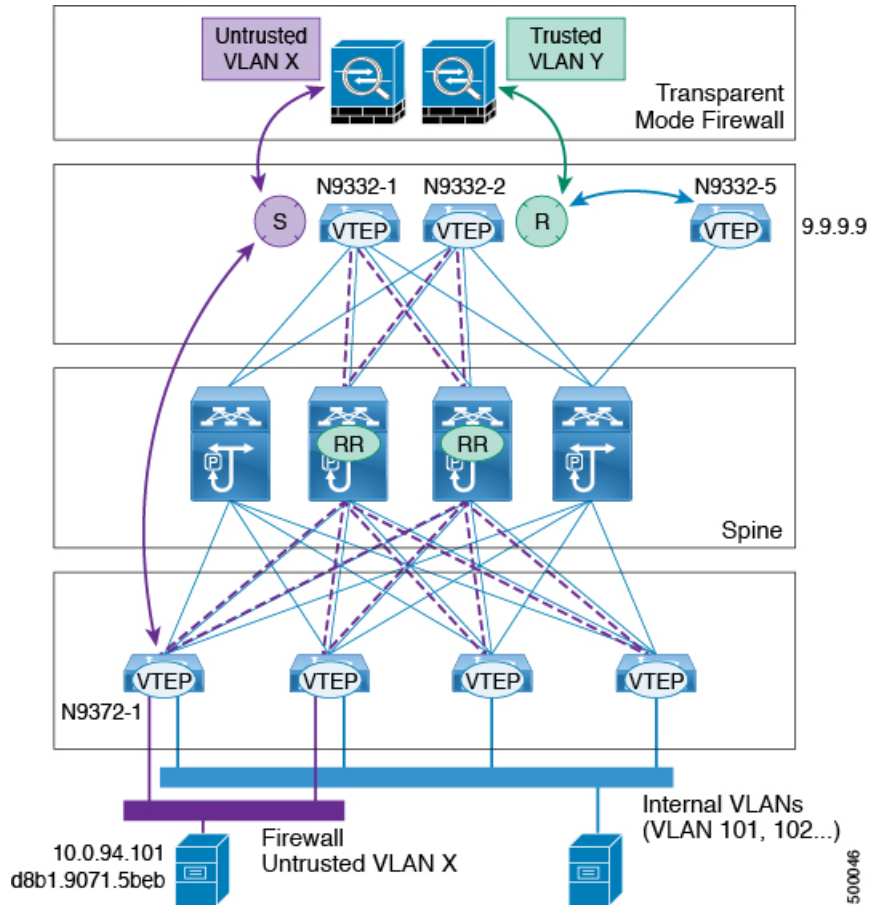
500045



- (注) VXLAN EVPNの場合、トランスペアレントファイアウォールを挿入した分散型エニーキャストゲートウェイを使用することを推奨します。これにより、すべてのVLANをVXLAN対応にできます。HSRP/VRRPベースのファーストホップゲートウェイを使用する場合、SVIのVLANはVXLAN対応にできず、冗長性のためにvPCペア上に存在する必要があります。

## EVPN でのトランスパレントファイアウォール挿入の例

EVPN でのトランスパレントファイアウォール挿入の例



- VLAN X のホスト: 10.1.94.101
- ToR リーフ: N9372-1
- vPC 中のサービス リーフ: N9332-1 および N9332-2
- ボーダー リーフ : N9332-5

### ToR リーフ設定

```
vlan 94
vn-segment 100094

interface nve1
member vni 100094
mcastgroup 239.1.1.1

router bgp 64500
routerid 1.1.2.1
neighbor 1.1.1.1 remote-as 64500
address-family 12vpn evpn
```

```

        send-community extended
neighbor 1.1.1.2 remote-as 64500
address-family l2vpn evpn
    send-community extended
vrf Ten1
    address-family ipv4 unicast
        advertise l2vpn evpn

evpn
vni 100094 l2
    rd auto
    route-target import auto
    route-target export auto

```

### HSRPを使用したサービス リーフ 1 設定

```

vlan 94
description untrusted_vlan
    vn-segment 100094

vlan 95
    description trusted_vlan

vpc domain 10
    peer-switch
    peer-keepalive destination 10.1.59.160
    peer-gateway
    auto-recovery
    ip arp synchronize

interface Vlan2
description vpc_backup_svi_for_overlay
    no shutdown
    no ip redirects
    ip address 10.10.60.17/30
    no ipv6 redirects
    ip router ospf 100 area 0.0.0.0
    ip ospf bfd
    ip pim sparsemode

interface Vlan95
description SVI_for_trusted_vlan
    no shutdown
    mtu 9216
    vrf member Ten-1
    no ip redirects
    ip address 10.0.94.2/24
    hsrp 0
        preempt priority 255
    ip 10.0.94.1

interface nve1
    member vni 100094
    mcast-group 239.1.1.1

router bgp 64500
    routerid 1.1.2.1
    neighbor 1.1.1.1 remote-as 64500
    address-family l2vpn evpn
        send-community extended
    neighbor 1.1.1.2 remote-as 64500
    address-family l2vpn evpn
        send-community extended
    vrf Ten-1

```

```
address-family ipv4 unicast
  network 10.0.94.0/24 /*advertise /24 for SVI 95 subnet; it is not VXLAN anymore*/
  advertise l2vpn evpn

evpn
vni 100094 12
  rd auto
  route-target import auto
  route-target export auto
```

## HSRP を使用したサービス リーフ 2 設定

```
vlan 94
  description untrusted_vlan
  vnsegment 100094

vlan 95
  description trusted_vlan

vpc domain 10
  peer-switch
  peer-keepalive destination 10.1.59.159
  peer-gateway
  auto-recovery
  ip arp synchronize

interface Vlan2
description vpc_backup_svi_for_overlay
  no shutdown
  no ip redirects
  ip address 10.10.60.18/30
  no ipv6 redirects
  ip router ospf 100 area 0.0.0.0
  ip pim sparsemode

interface Vlan95
description SVI_for_trusted_vlan
  no shutdown
  mtu 9216
  vrf member Ten-1
  no ip redirects
  ip address 10.0.94.3/24
  hsrp 0
  preempt priority 255
  ip 10.0.94.1

interface nve1
  member vni 100094
  mcastgroup 239.1.1.1

router bgp 64500
  router-id 1.1.2.1
  neighbor 1.1.1.1 remote-as 64500
  address-family l2vpn evpn
    send-community extended
  neighbor 1.1.1.2 remote-as 64500
  address-family l2vpn evpn
    send-community extended
  vrf Ten-1
    address-family ipv4 unicast
      network 10.0.94.0/24 /*advertise /24 for SVI 95 subnet; it is not VXLAN anymore*/
      advertise l2vpn evpn

evpn
```

```
vni 100094 12
  rd auto
  route-target import auto
  route-target export auto
```

## show コマンドの例

入力リーフが学習したホストからのローカル MAC の情報を表示します。

```
switch# sh mac add vl 94 | i 5b|MAC
* primary entry, G - Gateway MAC, (R) Routed - MAC, O - Overlay MAC
VLAN MAC Address Type age Secure NTFY Ports
* 94 d8b1.9071.5beb dynamic 0 F F Eth1/1
```

サービスリーフが検出したホストの MAC の情報を表示します。



(注) VLAN 94 において、サービスリーフが学習するホスト MAC は、BGP によってリモートピアから得られます。

```
switch# sh mac add vl 94 | i VLAN|eb

VLAN MAC Address Type age Secure NTFY Ports
* 94 d8b1.9071.5beb dynamic 0 F F nvel(1.1.2.1)

switch# sh mac add vl 94 | i VLAN|eb

VLAN MAC Address Type age Secure NTFY Ports
* 94 d8b1.9071.5beb dynamic 0 F F nvel(1.1.2.1)

switch# sh mac add vl 95 | i VLAN|eb

VLAN MAC Address Type age Secure NTFY Ports
+ 95 d8b1.9071.5beb dynamic 0 F F Po300

switch# sh mac add vl 95 | i VLAN|eb

VLAN MAC Address Type age Secure NTFY Ports
+ 95 d8b1.9071.5beb dynamic 0 F F Po300
```

サービスリーフが学習した VLAN 95 にあるホストの ARP の情報を表示します。

```
switch# sh ip arp vrf ten-1
Address      Age      MAC Address      Interface
10.0.94.101  00:00:26 d8b1.9071.5beb  Vlan95
```

サービスリーフはEVPNから9.9.9.9を学習します。

```
switch# sh ip route vrf ten-1 9.9.9.9
IP Route Table for VRF "Ten-1"
'*' denotes best ucast nexthop
'**' denotes best mcast nexthop
'[x/y]' denotes [preference/metric]
'%<string>' in via output denotes VRF <string>

9.9.9.9/32, ubest/mbest: 1/0
```

```
*via 1.1.2.7%default, [200/0], 02:57:27, bgp64500,internal, tag 65000 (evpn) segid:
10011
tunnelid: 0x1
010207 encap: VXLAN
```

ボーダー リーフが学習した BGP によるホスト ルートの情報を表示します。

```
switch# sh ip route 10.0.94.101

IP Route Table for VRF "default"
'*' denotes best ucast nexthop
'***' denotes best mcast nexthop
'[x/y]' denotes [preference/metric]
'%<string>' in via output denotes VRF <string>

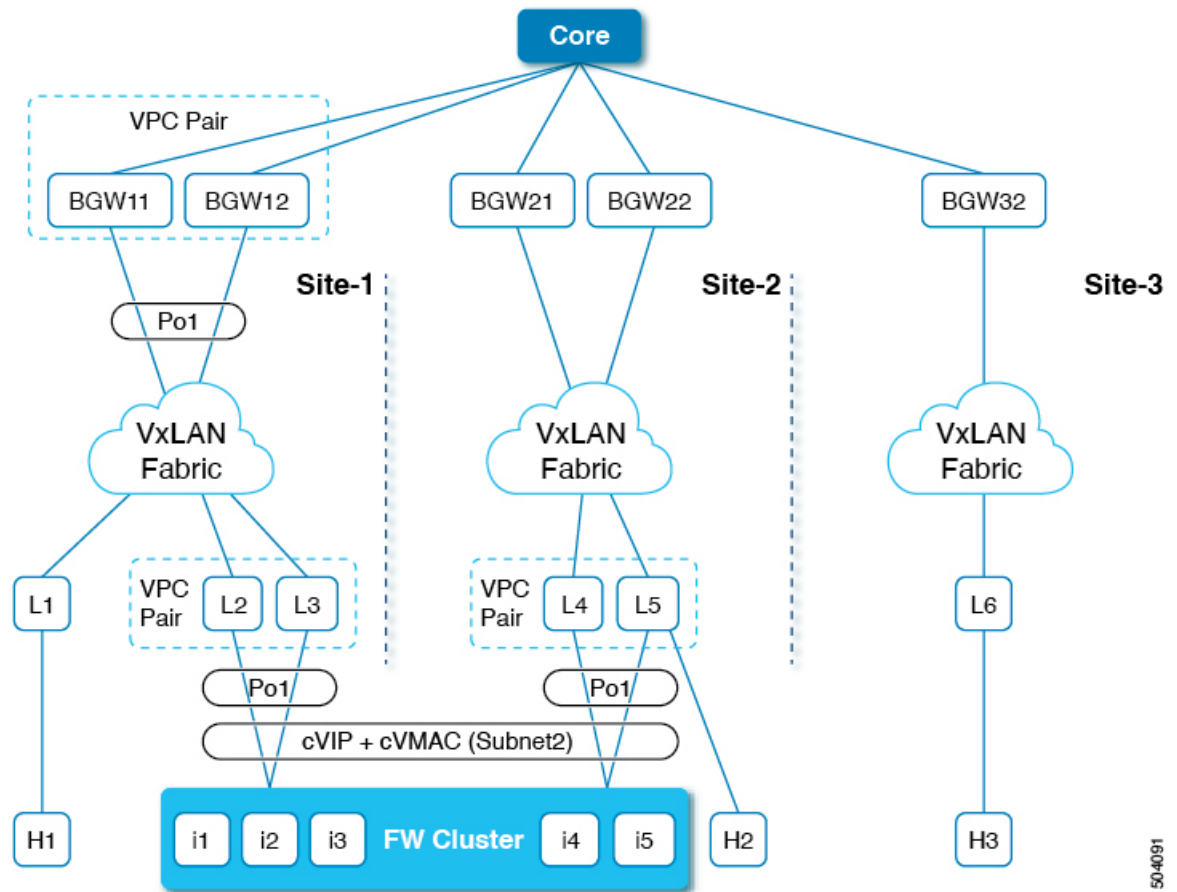
10.0.94.0/24, ubest/mbest: 1/0
  *via 10.100.5.0, [20/0], 03:14:27, bgp65000,external, tag 6450
```

## VXLAN BGP EVPN を使用したファイアウォール クラスタリング

このセクションでは、BGP EVPN コントロールプレーンを使用して VXLAN ファブリックを実行している複数のサイトにまたがるファイアウォール クラスタを構成する方法について詳しく説明します。

次のトポロジは、VXLAN EVPN を使用したファイアウォール クラスタリングを示しています。

図 7: VXLAN EVPNによるファイアウォールクラスタリング



このトポロジは、次のものをカバーします。

- ファイアウォールクラスタは、単一デバイスとして動作する複数のインスタンスで構成されています。
- ファイアウォールへのルーテッドアクセスは、異なるサブネットまたは同じサブネットを介して行うことができます。
- ファイアウォールは、すべてのインスタンスにまたがる L2 ポート チャンネルを採用しています。
- 共通の ESI では、ファイアウォール クラスタに接続するすべての vPC ポートチャンネルが示されます。
- すべてのインスタンスに単一の VIP/VMAC が存在します。
- サイトごとの BGP-EVPN VXLAN オーバーレイは、ボーダー ゲートウェイでステッチされます。



- 同じサイト内のアクティブからアクティブへのインスタンスのエニーキャスト転送と、トラフィックフローのためのサイト全体のファイアウォールへのアクティブからバックアップへのアクセスがサポートされています。
- 各サイトには、ポートチャンネルインターフェイスが割り当てられたクラスタに接続された単一の vPC ペアがあります。
- クラスタ VIP およびクラスタ VMAC は、BGP EVPN ルート ターゲット -2s として VXLAN EVPN ファブリックにアドバタイズされます (ESI は各 vPC のポートチャンネルインターフェイスで構成された値に設定されます)。ルートターゲット 2 のネクストホップは、vPC ペアの VTEP VIP アドレスです。
- 各サイトには複数のクラスタが含まれる場合があります。クラスタは、固有の ESI を持つ個々のポートチャンネルを使用して vPC ペアに接続されます。
- 各クラスタには、BGP EVPN ルート ターゲット -2s として VXLAN EVPN ファブリックにアドバタイズされる独自の cVIP と cVMAC があります (ESI はその vPC のポートチャンネルインターフェイスで構成された値に設定されています)。
- クラスタには、vPC ペアに接続されたポートチャンネル上に複数の VLAN がある場合があります。VLAN で学習された各 cVIP/cVMAC は、対応する L2VNI を使用してルート T-2 EVPN ルートとしてアドバタイズされます。
- VIP および VMAC (ファイアウォールホスト) は、単一の spanned Ether-channel に接続されます。
- Spanned Ether-channel はサイト全体に拡張されます。
- VIP へのエニーキャスト転送は、既存の BGP パス属性と最適パスの選択を利用して決定されます。

ファイアウォールクラスタに接続されている VTEP リーフでは、BGP はルートマップを使用してコミュニティをファイアウォールクラスタ関連の EVPNEAD/ES (タイプ1) および MAC/IP (タイプ2) ルートに接続します。

```
router bgp 12000
 address-family l2vpn evpn
 originate-map set_esi
 template peer SITE-BGW
   remote-as 12000
   update-source loopback1
   address-family l2vpn evpn
     send-community
     send-community extended
 template peer VTEP-PEERS
   remote-as 12000
   update-source loopback1
   address-family l2vpn evpn
     send-community
     send-community extended
```

ボーダー ゲートウェイでは、BGP はルートマップを使用して、EVPN EAD/ES (タイプ1) および MAC/IP (タイプ2) ルートに接続されたファイアウォールクラスタリングコミュニティを照合します。

```
router bgp 11000
  bestpath as-path multipath-relax
  neighbor 111.111.10.1 remote-as 12000
  peer-type fabric-external
  address-family l2vpn evpn
    send-community
    send-community extended
  route-map preserve_esi out
  rewrite-evpn-rt-asn
```

ファイアウォールクラスタに接続されている VTEP リーフで、コミュニティをファイアウォールクラスタ関連の EVPN EAD/ES (タイプ1) および MAC/IP (タイプ2) ルートに接続するようにルートマップを構成する必要があります。

```
route-map set_esi permit 10
  match tag 100000
  match evpn route-type 1 2
  set community 23456:12345
route-map set_esi permit 15
```



**注意** ネイバー アドレス ファミリ モードの下の `route-map <name>` 外 BGP コマンドに関連付けられているルートマップの **match tag** コマンドは、`address-family l2vpn evpn` の下で構成されている場合のみサポートされます。

ボーダー ゲートウェイでは、EVPN EAD/ES (タイプ1) および MAC/IP (タイプ2) ルートに接続されたファイアウォールクラスタリング コミュニティと一致するように、ファブリック内部ピアとファブリック外部ピアに個別のルートマップを構成する必要があります。

アウトバウンド L2VPN/EVPN ルート マップをファブリック内部ピアに一致させる：

```
route-map preserve_esi permit 10
  match community preserve_esi
  match evpn route-type 2
  set esi unchanged
route-map preserve_esi permit 15
route-map preserve_esi permit 30
```

アウトバウンド L2VPN/EVPN ルート マップをファブリック外部ピアに一致させる：

```
route-map preserve_esi_external permit 10
  match community preserve_esi
  match evpn route-type 2
  set esi unchanged
route-map preserve_esi_external permit 15
  match community preserve_esi
  match evpn route-type 1
route-map preserve_esi_external permit 20
  match evpn route-type 1
  match route-type local
route-map preserve_esi_external deny 25
  match evpn route-type 1
route-map preserve_esi_external permit 30
```

イーサネットセグメントは、vPC ポート チャネルの下でのみ構成できます。

```
interface port-channel 100
  ethernet-segment vpc
  esi <esi> [ tag <uint >]
interface port-channel 200
  ethernet-segment vpc
  esi system-mac <system-mac> <local-identifier> [tag <uint>]
```

共通の ESI では、ファイアウォール クラスタに接続するすべての vPC ポートチャンネルが示されます。vPC ポート チャンネルで ESI を構成できます。

```
evpn esi multihoming
port-channel 100
  ethernet-segment 1
    system-mac aa.bb.cc <anycast-host>
```

同じファイアウォール クラスタをホストするすべての vPC ポート チャンネルに対して、同じシステム MAC を維持します。

ファイアウォールの詳細については、「[VXLAN ファブリックでのレイヤ3 ファイアウォールの統合](#)」を参照してください。

## VXLAN EVPN ファブリックのサービス リダイレクト

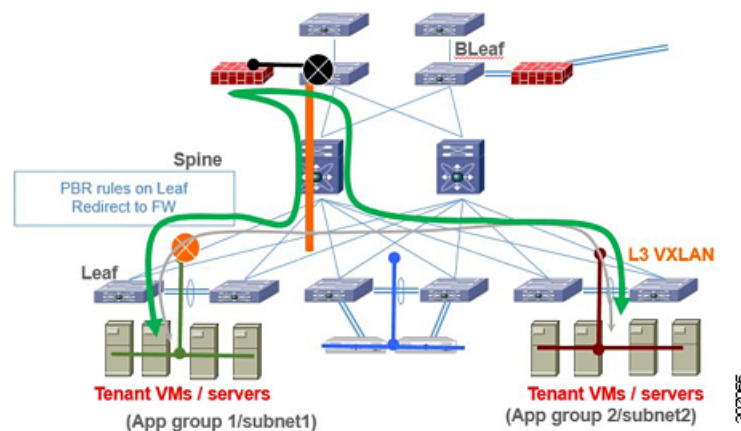
今日では、データセンター内のアプリケーションを保護および最適化するために、ファイアウォール、ロードバランサなどのサービス アプライアンス（サービス ノードまたはサービス エンドポイントとも呼ばれる）の挿入が必要です。このセクションでは、VXLAN EVPN ファブリックで提供されるレイヤ4～レイヤ7サービスの挿入およびリダイレクト機能について説明します。これらのサービスにトラフィックをオンボードして選択的にリダイレクトする高度なメカニズムを提供します。

### サービス挿入のポリシーベース リダイレクトの使用

ポリシーベースのリダイレクト（PBR）は、ルーティング テーブル ルックアップをバイパスし、VXLAN 経由で到達可能なネクスト ホップ IP にトラフィックをリダイレクトするメカニズムを提供します。この機能により、ファイアウォールやロードバランサなどのレイヤ4-レイヤ7デバイスへのサービス リダイレクションが可能になります。

PBRでは、トラフィックの転送先を指定するルールを使用してルート マップを設定します。ルートマップは、テナント側のSVIに適用され、ホスト側のインターフェイスからファブリック経由で到達可能なネクスト ホップへのトラフィックに影響を与えます。

トラフィックがオーバーレイからVTEPに着信し、別のネクストホップにリダイレクトする必要があるシナリオでは、レイヤ3VNIインターフェイスに面するファブリックにPBRポリシーを適用する必要があります。



前の図では、アプリケーショングループ1とアプリケーショングループ2間の通信は、デフォルトでテナント VRF のVLAN 間/VNI ルーティングを介して行われます。アプリケーショングループ1からアプリケーショングループ2へのトラフィックがファイアウォールを通過する必要があるという要件がある場合、PBR ポリシーを使用してトラフィックをリダイレクトできます。「ポリシーベースリダイレクトの構成例」のセクションの例では、トラフィックフローをリダイレクトするために必要な構成が示されています。

この VXLAN PBR 機能は非常に基本的なものであり、VXLAN ファブリックにサービスを適切に挿入するために必要な機能が多くが不足しています。したがって、「[Enhanced-Policy Based Redirect \(ePBR\)](#) (33 ページ)」セクションで説明されているすべての理由から、代わりに ePBR を確認することをお勧めします。

## ポリシーベースのリダイレクトの注意事項と制約事項

PBR over VXLAN には、次の注意事項と制限事項が適用されます。

- 次のプラットフォームは、PBR over VXLAN をサポートしています。
  - Cisco Nexus 9332C および 9364C プラットフォーム スイッチ
  - Cisco Nexus 9300-EX プラットフォーム スイッチ
  - Cisco Nexus 9300-FX/FX2/FX3 プラットフォーム スイッチ
  - Cisco Nexus 9300-GX プラットフォーム スイッチ
  - -EX/FX ラインカードを備えた Cisco Nexus 9504 および 9508 プラットフォーム スイッチ
- Cisco NX-OS リリース 10.2(3)F 以降、VXLAN 経由の SRv6 は Cisco Nexus 9300-GX2 プラットフォーム スイッチでサポートされます。
- Cisco NX-OS リリース 10.2(3) 以降、VXLAN PBR 機能は、すべての TOR スイッチの VXLANv6 でサポートされます。
- PBR over VXLAN は、`set {ip | ipv6} next-hopip-address` コマンドの VTEP ECMP、および `load-share` キーワードをサポートしていません。

## ポリシーベース リダイレクト機能のイネーブル化

高度な（および推奨される）ePBR 機能が展開されていない場合に基本的な PBR を構成するには、次のセクションを参照してください。

- [ポリシーベース リダイレクト機能のイネーブル化 \(29 ページ\)](#)
- [ルート ポリシーの設定 \(30 ページ\)](#)
- [ポリシーベース リダイレクトの設定の確認 \(31 ページ\)](#)
- [ポリシーベース リダイレクトの設定例 \(32 ページ\)](#)

### 始める前に

ルート ポリシーを設定するには、あらかじめポリシーベース リダイレクト機能をイネーブル化しておく必要があります。

### 手順の概要

1. **configure terminal**
2. **[no] feature pbr**
3. (任意) **show feature**
4. (任意) **copy running-config startup-config**

### 手順の詳細

	コマンドまたはアクション	目的
ステップ 1	<b>configure terminal</b> 例： switch# <b>configure terminal</b>	グローバル コンフィギュレーション モードを開始します。
ステップ 2	<b>[no] feature pbr</b> 例： switch(config)# <b>feature pbr</b>	ポリシーベースルーティング機能をイネーブルにします。
ステップ 3	(任意) <b>show feature</b> 例： switch(config)# <b>show feature</b>	有効および無効にされた機能を表示します。
ステップ 4	(任意) <b>copy running-config startup-config</b> 例： switch(config)# <b>copy running-config startup-config</b>	この設定変更を保存します。

## ルータポリシーの設定

ポリシーベースルーティングでルートマップを使用すると、着信インターフェイスにルーティングポリシーを割り当てることができます。Cisco NX-OSはネクストホップおよびインターフェイスを検出するときに、パケットをルーティングします。



(注) スイッチには、IPv4トラフィック用のRACL TCAMリージョンがデフォルトで用意されています。

### 始める前に

ポリシーベースルーティングポリシーを適用するには、あらかじめRACL TCAMリージョンを(TCAMカービングを使用して)設定する必要があります。詳細については『[Cisco Nexus 9000 Series NX-OS Security Configuration Guide, Release 9.2\(x\)](#)』の「Configuring ACL TCAM Region Sizes」の項を参照してください。

### 手順の概要

1. **configure terminal**
2. **interface** *type slot/port*
3. **{ip | ipv6} policy route-map** *map-name*
4. **route-map** *map-name* [**permit** | **deny**] [*seq*]
5. **match** **{ip | ipv6} address** *access-list-name name* [*name...*]
6. **set ip next-hop** *address1*
7. **set ipv6 next-hop** *address1*
8. (任意) **set interface null0**
9. (任意) **copy running-config startup-config**

### 手順の詳細

	コマンドまたはアクション	目的
ステップ 1	<b>configure terminal</b> 例： switch# <b>configure terminal</b>	グローバル コンフィギュレーション モードを開始します。
ステップ 2	<b>interface</b> <i>type slot/port</i> 例： switch(config)# <b>interface ethernet 1/2</b>	インターフェイス設定モードを開始します。
ステップ 3	<b>{ip   ipv6} policy route-map</b> <i>map-name</i> 例： switch(config-inf)# <b>ip policy route-map Testmap</b>	IPv4 または IPv6 ポリシーベース ルーティング用のルートマップをインターフェイスに割り当てます。

	コマンドまたはアクション	目的
ステップ 4	<b>route-map</b> <i>map-name</i> [ <b>permit</b>   <b>deny</b> ] [ <i>seq</i> ] 例： switch(config-inf)# <b>route-map</b> Testmap	ルート マップを作成するか、または既存のルート マップに対応するルートマップ設定モードを開始します。ルートマップのエントリを順序付けるには、 <i>seq</i> を使用します。
ステップ 5	<b>match</b> { <b>ip</b>   <b>ipv6</b> } <b>address</b> <b>access-list-name</b> <i>name</i> [ <i>name...</i> ] 例： switch(config-route-map)# <b>match ip address</b> <b>access-list-name</b> ACL1	1 つまたは複数の IPv4 または IPv6 アクセス コントロールリスト (ACL) に対して IPv4 または IPv6 アドレスを照合します。このコマンドはポリシーベースルーティング用であり、ルート フィルタリングまたは再配布では無視されます。
ステップ 6	<b>set ip next-hop</b> <i>address1</i> 例： switch(config-route-map)# <b>set ip next-hop</b> 192.0.2.1	ポリシーベースルーティング用の IPv4 ネクストホップアドレスを設定します。
ステップ 7	<b>set ipv6 next-hop</b> <i>address1</i> 例： switch(config-route-map)# <b>set ipv6 next-hop</b> 2001:0DB8::1	ポリシーベースルーティング用の IPv6 ネクストホップアドレスを設定します。
ステップ 8	(任意) <b>set interface null0</b> 例： switch(config-route-map)# <b>set interface null0</b>	ルーティングに使用するインターフェイスを設定します。パケットをドロップするには <b>null0</b> インターフェイスを使用します。
ステップ 9	(任意) <b>copy running-config startup-config</b> 例： switch(config-route-map)# <b>copy running-config</b> <b>startup-config</b>	この設定変更を保存します。

## ポリシーベース リダイレクトの設定の確認

ポリシーベース リダイレクト設定情報を表示するには、次の作業のいずれかを行います。

コマンド	目的
<b>show</b> [ <b>ip</b>   <b>ipv6</b> ] <b>policy</b> [ <i>name</i> ]	IPv4 または IPv6 ポリシーに関する情報を表示します。
<b>show route-map</b> [ <i>name</i> ] <b>pbr-statistics</b>	ポリシー統計情報を表示します。

**route-map** *map-name* **pbr-statistics** コマンドを使用してポリシーを有効にします。**clear route-map** *map-name* **pbr-statistics** コマンドを使用してこれらのポリシーをクリアします。

## ポリシーベースリダイレクトの設定例

サービス VTEP を除くすべてのテナント VTEP で次の設定を実行します。

```

feature pbr

ipv6 access-list IPV6_App_group_1
10 permit ipv6 any 2001:10:1:1::0/64

ip access-list IPV4_App_group_1
10 permit ip any 10.1.1.0/24

ipv6 access-list IPV6_App_group_2
10 permit ipv6 any 2001:20:1:1::0/64

ip access-list IPV4_App_group_2
10 permit ip any 20.1.1.0/24

route-map IPV6_PBR_Appgroup1 permit 10
  match ipv6 address IPV6_App_group_2
  set ipv6 next-hop 2001:100:1:1::20 (next hop is that of the firewall)

route-map IPV4_PBR_Appgroup1 permit 10
  match ip address IPV4_App_group_2
  set ip next-hop 10.100.1.20 (next hop is that of the firewall)

route-map IPV6_PBR_Appgroup2 permit 10
  match ipv6 address IPV6_App_group_1
  set ipv6 next-hop 2001:100:1:1::20 (next hop is that of the firewall)

route-map IPV4_PBR_Appgroup2 permit 10
  match ip address IPV4_App_group_1
  set ip next-hop 10.100.1.20 (next hop is that of the firewall)

interface Vlan10
! tenant SVI appgroup 1
vrf member appgroup
  ip address 10.1.1.1/24
  no ip redirect
  ipv6 address 2001:10:1:1::1/64
  no ipv6 redirects
  fabric forwarding mode anycast-gateway
ip policy route-map IPV4_PBR_Appgroup1
ipv6 policy route-map IPV6_PBR_Appgroup1
interface Vlan20
! tenant SVI appgroup 2
vrf member appgroup
  ip address 20.1.1.1/24
  no ip redirect
  ipv6 address 2001:20:1:1::1/64
  no ipv6 redirects
  fabric forwarding mode anycast-gateway
ip policy route-map IPV4_PBR_Appgroup2
ipv6 policy route-map IPV6_PBR_Appgroup2

On the service VTEP, the PBR policy is applied on the tenant VRF SVI. This ensures the
traffic post decapsulation will be redirected to firewall.
feature pbr

ipv6 access-list IPV6_App_group_1
10 permit ipv6 any 2001:10:1:1::0/64

ip access-list IPV4_App_group_1

```



```
10 permit ip any 10.1.1.0/24

ipv6 access-list IPV6_App_group_2
10 permit ipv6 any 2001:20:1:1::0/64

ip access-list IPV4_App_group_2
10 permit ip any 20.1.1.0/24

route-map IPV6_PBR_Appgroup1 permit 10
  match ipv6 address IPV6_App_group_2
  set ipv6 next-hop 2001:100:1:1::20 (next hop is that of the firewall)

route-map IPV6_PBR_Appgroup permit 20
  match ipv6 address IPV6_App_group1
  set ipv6 next-hop 2001:100:1:1::20 (next hop is that of the firewall)

route-map IPV4_PBR_Appgroup permit 10
  match ip address IPV4_App_group_2
  set ip next-hop 10.100.1.20 (next hop is that of the firewall)

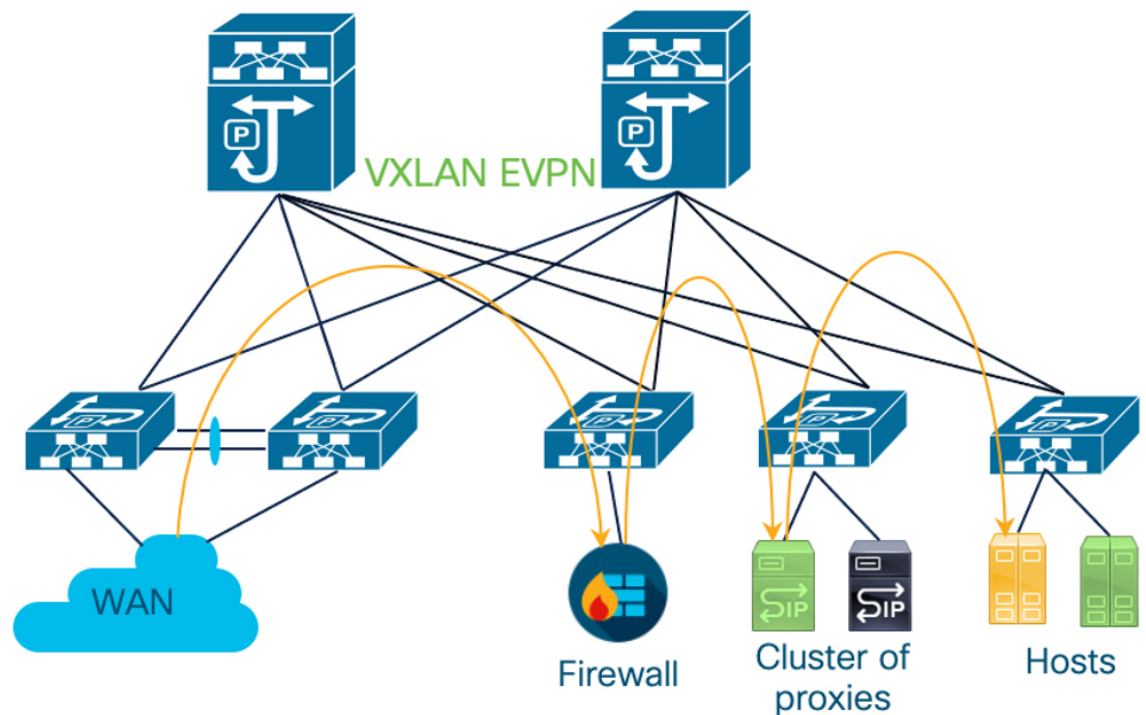
route-map IPV4_PBR_Appgroup permit 20
  match ip address IPV4_App_group_1
  set ip next-hop 10.100.1.20 (next hop is that of the firewall)

interface vlan1000
!L3VNI SVI for Tenant VRF
vrf member appgroup
ip forward
ipv6 forward
ipv6 ipv6 address use-link-local-only
ip policy route-map IPV4_PBR_Appgroup
ipv6 policy route-map IPV6_PBR_Appgroup
```

## Enhanced-Policy Based Redirect (ePBR)

トラフィックを選択的にリダイレクトするソリューションとしてのVXLAN PBRは、単純なトラフィックのリダイレクト要件にのみ対応できます。サービスチェーン、対称ロードバランシング、サービスアプライアンスの正常性の追跡など、より複雑なユースケースでは、PBRの使用が困難になります。PBRを使用したサービスチェーンの課題は、ユーザーがノードごとに一意のポリシーを作成し、チェーン内のすべてのノードでリダイレクションルールを手動で管理する必要があることです。また、サービスノードのステータフルな性質を考えると、PBRルールはリバーストラフィックの対称性を保証する必要があり、これによりPBRポリシーの構成と管理がさらに複雑になります。

Enhanced Policy-Based Redirect (ePBR) は、サービスノードを挿入し、トラフィックを選択的にリダイレクトしてロードバランシングするための包括的なソリューションを提供します。ePBRは、トラフィックチェーンとロードバランシングルールを作成するための簡素化されたワークフローを提供するとともに、サービスアプライアンスのヘルスをプローブ/モニタし、障害が発生した場合に修正措置を講じるためのオプションを提供します。ePBRは、単一サイトとマルチサイトの両方のVXLAN EVPN展開でサポートされます。



この図では、WANから発信される選択的なトラフィックがファイアウォールにチェーンされ、宛先ホストに転送される前に、トラフィックはプロキシのクラスタ全体で負荷分散されます。ePBRは、順方向と逆方向の両方のトラフィックがTCPプロキシのクラスタ内の同じサービスエンドポイントにリダイレクトされるようにすることで、特定のフローの対称性を維持します。

ePBRの詳細、注意事項、および構成例については、『Cisco Nexus 9000 Series NX-OS ePBR 構成ガイド』、『』、『』、『』および『拡張ポリシーベースリダイレクトホワイトペーパーを持つレイヤ4からレイヤLayer7サービスリダイレクト』を参照してください。

## 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。