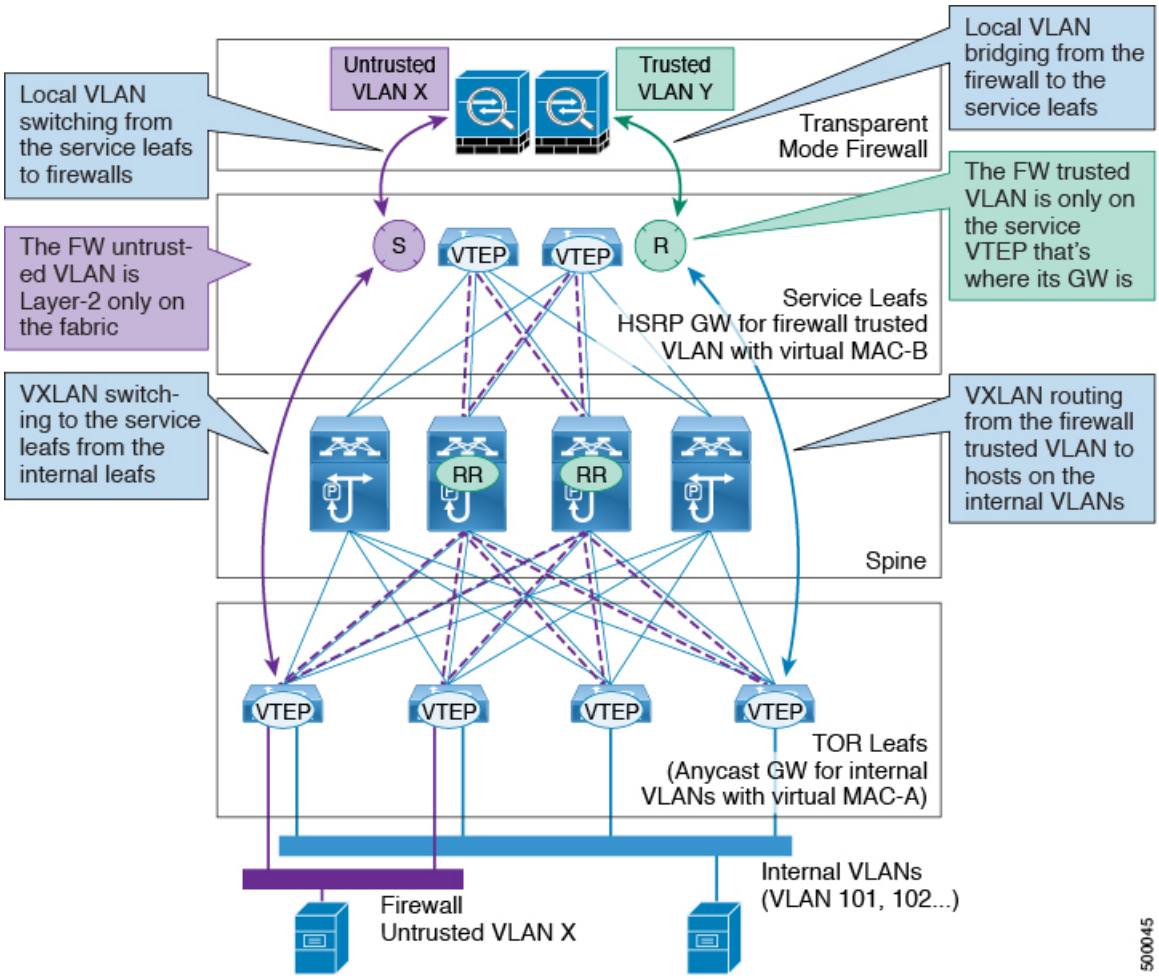
EVPN でのトランスペアレント ファイアウォール挿入

- 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，1 ページ
- EVPN でのトランスペアレント ファイアウォール挿入の例，3 ページ
- show コマンドの例，6 ページ

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

一部のシナリオでは、すべてのルーティング トラフィックを、レイヤ 2 のトランスペアレント ファイアウォールを経由させて送信する必要があります。ただし、デフォルトで VXLAN EVPN は、分散エニーキャスト ゲートウェイをすべてのリーフで必要とします。

VXLAN EVPN でのレイヤ 2 トランスペアレント ファイアウォールの要件については、特別なトポロジを使用した対応が可能です。



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 VLANS 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。

このトポロジでは、信頼できない VLAN X と信頼できる VLAN Y というアプローチを使用します。

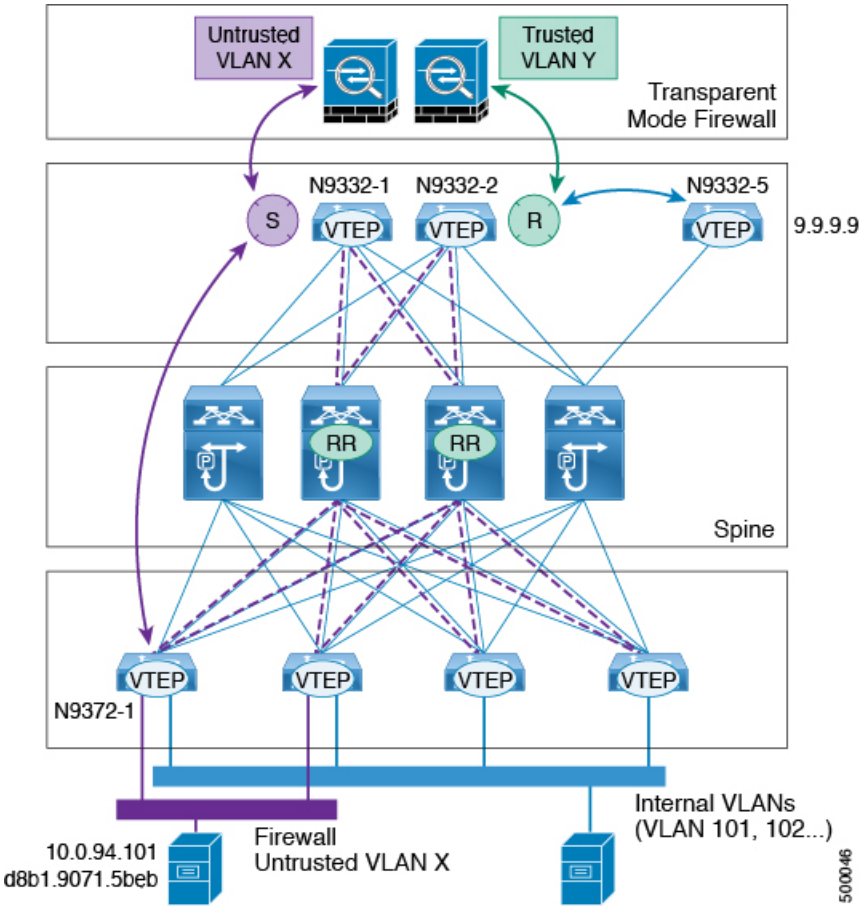
すべての TOR リーフには、レイヤ 2 VNI VLAN X があります。VLAN X の SVI はありません。

ファイアウォールと接続したサービス リーフにあるのは、レイヤ 2 VNI VLAN X、非 VXLAN VLAN Y、および SVI Y に HSRP ゲートウェイを配置したものです。

（注） VXLAN フラッディングおよび学習でサポートされているのは、集中型ゲートウェイだけです。これは、1 つの VPC ペア VTEP でのみ VXLAN ごとの SVI を持てることを意味します。他の VTEP は、VXLAN VLAN に SVI を持つことはできません。

VXLANがサポートするのは、エニーキャスト ゲートウェイだけであり、集中型ゲートウェイはサポートされません。

EVPN でのトランスペアレント ファイアウォール挿入の例



（注）
- VLAN X 中のホスト：10.0.94.101
- TOR リーフ：N9372-1
- vPC 中のサービス リーフ：N9332-1 および N9332-2
- 境界リーフ：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 l2vpn 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
```

- 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
 descrition 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 l2
  rd auto
  route-target import auto
  route-target export auto
```

- 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_vla
 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 l2
  rd auto
  route-target import auto
  route-target export auto
```

show コマンドの例

- 入力 LEAF 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。

```
N93721# 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。

```
N93321# sh mac add vl 94 | i VLAN|eb
VLAN MAC Address Type age Secure NTFY Ports
* 94 d8b1.9071.5beb dynamic 0 F F nve1(1.1.2.1)

N93322# sh mac add vl 94 | i VLAN|eb
VLAN MAC Address Type age Secure NTFY Ports
* 94 d8b1.9071.5beb dynamic 0 F F nve1(1.1.2.1)

N93321# 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

N93322# 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。

```
N93322# sh ip arp vrf ten-1
Address     Age       MAC Address    Interface
10.0.94.101 00:00:26 d8b1.9071.5beb Vlan95

Service Leaf learns 9.9.9.9 from EVPN.

N93322# 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: VXLA
```

- 境界リーフが学習した BGP によるホスト ルートの情報を表示します。

```
N93965# 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
```