EVPN 分散型 NAT

EVPN 分散型 NAT

Cisco NX-OSリリース10.2（1）F以降では、N9K-C9336C-FX2、N9K-C93240YC-FX2、N9K-C93360YC-FX2 TORスイッチでEVPN分散NAT機能がサポートされています。分散型Elastic NAT機能は、VXLANトポロジのリーフとスパインでNATを有効にします。

EVPN分散NATのガイドラインと制限事項

EVPN分散型NATは次をサポートします。

- 最大 8192 の NAT 変換
- スタティック NAT
- IPv4 NAT
- VRF対応NATでの一致
- スタティック内部設定のアドルート

EVPN分散型NATは、次をサポートしません。

- IPv6 NAT
- ダイナミック NAT
- NATモビリティ
- サブネットベースのフィルタリング
- ルールごとの統計情報
- NATはvPCを認識しません。NAT設定はｖＰＣピアの両方に同一でなければなりません。

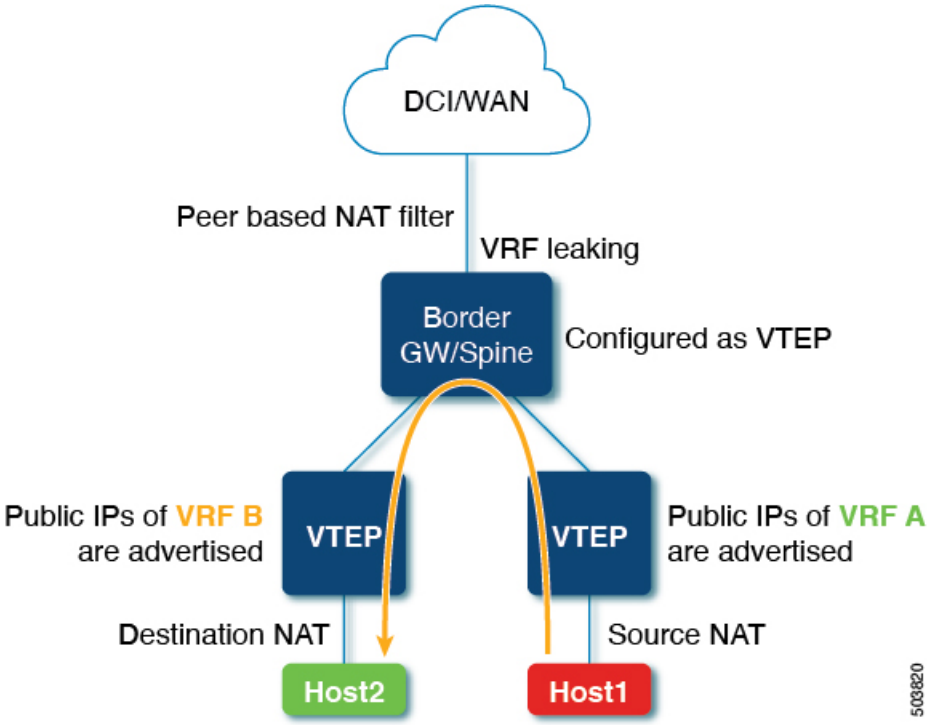
EVPN 分散型 NAT

- 送信元ホストと宛先ホストが同じVRFにある場合、ファブリック内では通常のNATを使用できます。EVPN分散NATは、同じVRF内ではサポートされません。異なるVRF間でサポートされます。

EVPN分散NATトポロジ

次のトポロジは、VTEPでのEVPN分散NAT設定を示しています。

図 *1 : EVPN*分散*NAT*設定トポロジ



上記のトポロジでは、次のようになります。

- EVPN分散NATは、VTEPでのみ設定されます。
- スパインには、EVPN分散NAT関連の設定は必要ありません。
- スパインはVTEPとして設定されます。
- VxLANアンダーレイルーティングプロトコルを使用した到達可能性のために、ルートだけがスパインにリークされます。
- 送信元と宛先NATは両方のリーフで設定されます。
- 送信元NATは、送信元に直接接続されたスイッチで実行されます。
- 宛先NATは、宛先に直接接続されたスイッチで実行されます。
- 送信元と宛先の両方が同じスイッチ上にある場合、最初に送信元NATが実行されます。パケットはスパインを介してループされ、宛先NATが実行されます。

- ホストは、要件に応じて、プライベートIPアドレスまたはパブリックIPアドレスを使用してトラフィックを送信できます。
- VXLANピアベースNATフィルタリングが設定されます。

ピアベースNATフィルタ

- ピアベースNATフィルタは、設定されたトンネルエンドポイント宛てのフローに対してのみNATを許可し、残りのフローは影響を受けません。
- ピアベースNATフィルタは、多数のプレフィックスをNAT変換する必要がある場合に役立ちます。
- NAT ACL領域は、ピアベースのNATフィルタが機能するように最初に切り分けられる必要があります。
- 境界ノードでピアベースのフィルタを設定できます。
- ピアベースNATフィルタは、集中型VRFリークが設定されているサービスリーフなどのVRF間ケースに役立ちます。
- を使用してピアベースNATフィルタを設定できます。<peer-ip>コマンド。**system nve nat peer-ip**

VRF 対応 NAT

- VRF対応NATにより、スイッチはVRF（仮想ルーティングおよび転送インスタンス）のアドレス空間を認識し、パケットを変換できます。これにより、NAT機能は2つのVRF間で使用される重複アドレス空間のトラフィックを変換できます。
- コマンドを使用してFPタイルベースのNATを有効にできます。**system routing vrf-aware-nat**
- VRF対応NATの詳細については、『Cisco Nexus 9000 NX-OS Interfaces Configuration Guide』を参照してください。https://www.cisco.com/c/en/us/td/docs/dcn/nx-os/nexus9000/102x/configuration/interfaces/cisco-nexus-9000-nx-os-interfaces-configuration-guide-102x/b-cisco-nexus-9000-nx-os-interfaces-configuration-guide-93x_chapter_01011.html#concept_6EB0DB9C8EDC40FB8C21EAA918A56627

EVPN分散NATの設定

次に、リーフ1のEVPN分散NAT設定を示します。

```
feature bgp
feature interface-vlan
feature vn-segment-vlan-based
feature nat
feature nv overlay

hardware access-list tcam region nat 512  (Carves NAT TCAM)


system routing vrf-aware-nat
system nve nat peer-ip 100.100.100.3      (peer-ip is the Spine address which is leaking
```

EVPN 分散型 NAT

```
 the route)

ip nat inside source static 21.1.1.10 172.21.1.10 vrf vrf1 match-in-vrf add-route

ip nat inside source static 31.1.1.10 172.31.1.10 vrf vrf2 match-in-vrf add-route

vlan 202
  vn-segment 20202

vlan 301
  vn-segment 20301

vlan 3200
  vn-segment 33200

vlan 3300
 vn-segment 33300


interface Vlan202
  no shutdown
  vrf member vrf1
  ip address 22.1.1.1/24
  fabric forwarding mode anycast-gateway
  ip nat inside

interface Vlan3200
  no shutdown
  vrf member vrf1
  ip forward
  ip nat outside

interface Vlan301
  no shutdown
  vrf member vrf2
  ip address 31.1.1.1/24
  fabric forwarding mode anycast-gateway
  ip nat inside

interface Ethernet1/11
  switchport mode trunk

interface Ethernet1/35
  switchport mode trunk

vrf context vrf1
  vni 33200
  rd auto
  address-family ipv4 unicast
    route-target both auto
    route-target both auto evpn

vrf context vrf2
  vni 33300
  rd auto
  address-family ipv4 unicast
    route-target both auto
    route-target both auto evpn

router bgp 100
  vrf vrf1
    address-family ipv4 unicast
      network 172.21.1.10/32
      advertise l2vpn evpn
```

EVPN 分散型 NAT

```
vrf vrf2
    address-family ipv4 unicast
      network 172.31.1.10/32
      advertise l2vpn evpn
```

次に、リーフ2のEVPN分散NAT設定を示します。

```
feature bgp
feature interface-vlan
feature vn-segment-vlan-based
feature nat
feature nv overlay

system routing vrf-aware-nat
system nve nat peer-ip 100.100.100.3   (peer-ip is the spine address which is leaking
the route)

ip nat inside source static 21.1.1.20 172.21.1.20 vrf vrf1 match-in-vrf add-route

ip nat inside source static 31.1.1.20 172.31.1.20 vrf vrf2 match-in-vrf add-route

vlan 202
  vn-segment 20202

vlan 301
  vn-segment 20301

vlan 3200
  vn-segment 33200

vlan 3300
 vn-segment 33300

interface Vlan202
  no shutdown
  vrf member vrf1
  ip address 22.1.1.1/24
  fabric forwarding mode anycast-gateway
  ip nat inside


interface Vlan3200
  no shutdown
  vrf member vrf1
  ip forward
  ip nat outside

interface Vlan301
  no shutdown
  vrf member vrf2
  ip address 31.1.1.1/24
  fabric forwarding mode anycast-gateway
  ip nat inside

interface Vlan3300
  no shutdown
  vrf member vrf2
  ip forward
  ip nat outside

interface Ethernet1/16
  switchport
  switchport mode trunk

interface Ethernet1/43
```

```
  switchport
  switchport mode trunk

vrf context vrf1
  vni 33200
  rd auto
  address-family ipv4 unicast
    route-target both auto
    route-target both auto evpn
vrf context vrf2
  vni 33300
  rd auto
  address-family ipv4 unicast
    route-target both auto
    route-target both auto evpn


router bgp 100
  vrf vrf1
    address-family ipv4 unicast
      network 172.21.1.20/32
      advertise l2vpn evpn
vrf vrf2
    address-family ipv4 unicast
      network 172.31.1.20/32
     advertise l2vpn evpn
```

次のshowコマンドは、EVPN分散型NATのスイッチで設定された絶縁ポリシーを表示します。

```
show ip nat translations
Pro Inside global Inside local Outside local Outside global
any 174.2.216.2 42.2.216.2 --- ---
any 174.3.217.2 42.3.217.2 --- ---
```

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。