EVPN Distributed NAT

EVPN Distributed NAT

Beginning with Cisco NX-OS Release 10.2(1)F, EVPN Distributed NAT feature is supported on N9K-C9336C-FX2, N9K-C93240YC-FX2, N9K-C93360YC-FX2 TOR switches. The Distributed Elastic NAT feature enables NAT on the leaf and spine in the VXLAN topology.

Guidelines and Limitations of EVPN Distributed NAT

EVPN Distributed NAT supports the following:

- Up to 8192 NAT translations
- Static NAT
- IPv4 NAT
- Match in VRF-aware NAT
- Add-route for static inside configuration

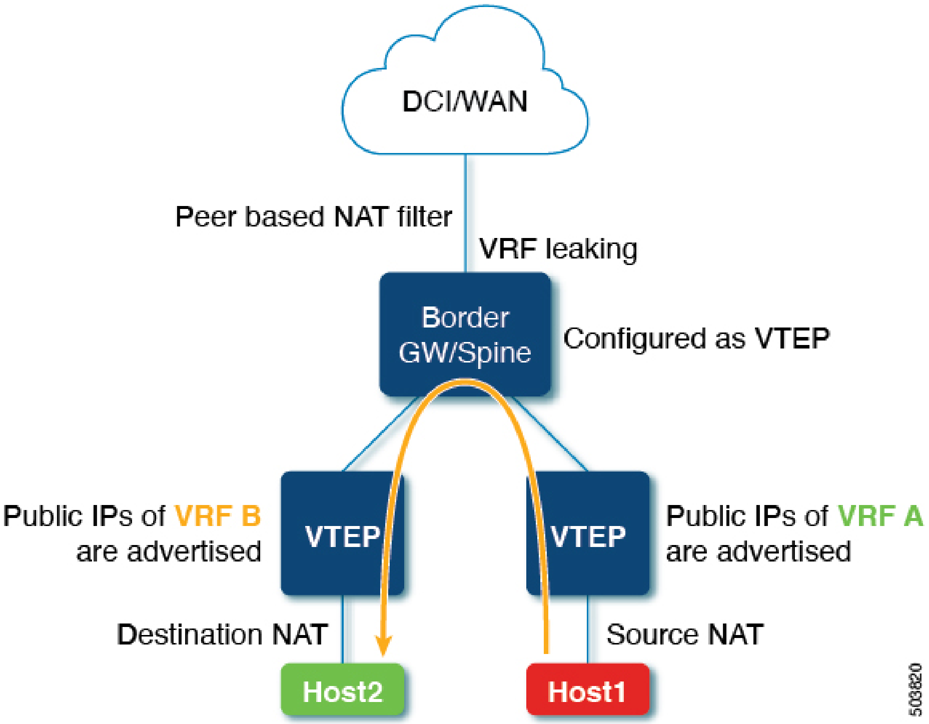
EVPN Distributed NAT does not support the following:

- IPv6 NAT
- Dynamic NAT
- NAT mobility
- Subnet-based filtering
- Per rule statistics
- NAT is unaware of vPC. NAT configuration should be identical on both vPC peers.
- Within a fabric if source and destination hosts are in same VRF, regular NAT can be used. EVPN Distributed NAT is not supported within same VRF. It is supported between different VRF's.

EVPN Distributed NAT Topology

The following topology illustrates the EVPN Distributed NAT configuration on VTEPs.

Figure 1: EVPN Distributed NAT Configuration Topology



In the above topology:

- EVPN Distributed NAT is configured only on the VTEPs.
- The spine does not require any EVPN Distributed NAT related configuration.
- Spine is configured as a VTEP.
- Only the routes are leaked in the spine for reachability using VxLAN underlay routing protocols.
- The Source and Destination NAT are configured on both the leaf.
- Source NAT is performed on the switch directly connected to the Source.
- Destination NAT is performed on the switch directly connected to the Destination.
- If both Source and Destination are on the same switch, Source NAT is performed first. The packet is then looped through Spine, and the Destination NAT is performed.
- Hosts can send traffic using private IP address or public IP address, depending on the requirement.
- VXLAN Peer-based NAT filtering is configured.

Peer-based NAT Filter

- The peer-based NAT filter allows NAT only for the flows that are destined to the configured tunnel endpoints and the rest of the flows remain unaffected.

- Peer-based NAT filter is useful in cases where large number of prefixes needs to be NATed.
- NAT ACL region must be carved first so that the peer-based NAT filter can work.
- You can configure peer-based filters on the border nodes.
- Peer-based NAT filter is useful for inter-VRF cases such as a service leaf where centralized VRF leak is configured.
- You can configure peer-based NAT filter using the **system nve nat peer-ip** <*peer-ip*> command.

VRF-Aware NAT

- The VRF aware NAT enables a switch to understand an address space in a VRF (virtual routing and forwarding instances) and to translate the packet. This allows the NAT feature to translate traffic in an overlapping address space that is used between two VRFs.
- You can enable FP Tile-based NAT using **system routing vrf-aware-nat** command.
- For more details on VRF aware NAT, see Cisco Nexus 9000 NX-OS Interfaces Configuration Guide.

Configuring EVPN Distributed NAT

The following is the EVPN Distributed NAT configuration in Leaf-1.

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

The following is the EVPN Distributed NAT configuration in Leaf-2.

```
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
```

The following show command provides the display of insulation policies configured in the switch for EVPN Distributed NAT.

```
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 --- ---
```