Configuring BGP EVPN VXLAN over IPsec

This chapter describes how to configure BGP EVPN VXLAN over IPsec. VXLAN support over IPsec provides an overlay which seamlessly extends secured services to enterprise branch locations.

Restrictions for BGP EVPN VXLAN over IPsec

- BGP EVPN VXLAN over IPsec is supported only on the Cisco Catalyst 9300X Series switch.
- Tenant Routed Multicast over BGP EVPN VXLAN over IPsec tunnel is currently not supported.
- A Catalyst 9300X switch supports a maximum of 128 IPsec tunnels. Hence the size of the BGP EVPN VXLAN fabric over IPsec tunnels is limited to 128 EVPN VXLAN VTEPs terminating the IPsec tunnels.

Information about BGP EVPN VXLAN over IPsec

Internet Protocol Security (IPsec) is a framework of open standards that are developed by the IETF. IPsec provides security for the transmission of sensitive information over unprotected networks such as the Internet. IPsec acts at the network layer, protecting and authenticating IP packets between participating IPsec devices such as hosts, and security gateways. For more information, see "Configuring IPsec" section in the *Security Configuration Guide*.

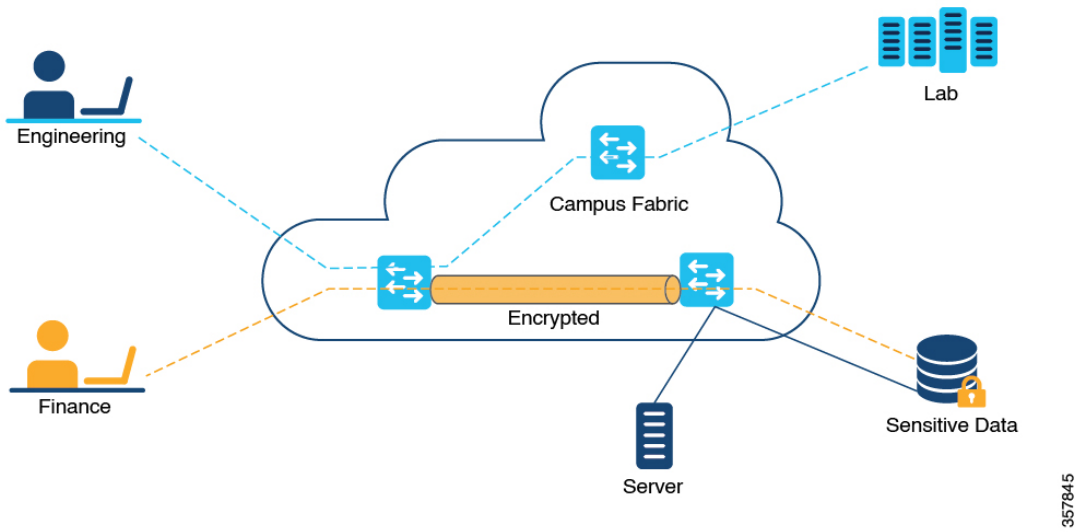
When a BGP EVPN VXLAN network is connected to an external network, the VXLAN traffic flows over the public network or internet, which is unencrypted and prone to data compromise. The traditional GRE Tunnel solution requires a unique tunnel and routing protocol session for each virtual routing and forwarding (VRF) or Layer 3 virtual network instance (L3VNI). The BGP EVPN VXLAN control plane simplifies the overlay network by having a single BGP session with the remote designated IPsec peer to enable large number of VRFs. BGP EVPN VXLAN, when deployed with IPsec, reduces operational complexity and enables secure remote branch access over WAN or internal zero-trust LAN network environments.

BGP EVPN VXLAN over IPsec enables secure encrypted network virtualization with Cisco Catalyst 9300X-based crypto hardware acceleration.

Zero-trust LAN network environments

A campus LAN network with Cisco Catalyst 9300X in the access layer can build secure, encrypted BGP EVPN VXLAN fabric to support a zero-trust network environment. A Cisco Catalyst 9300X at the access layer establishes IPsec tunnel with a Cisco Catalyst 9300X spine border that supports the BGP Route-Reflector functionality and external connectivity.

Figure 1: Campus LAN With Secure BGP EVPN VXLAN Network



Remote Access

Cisco Catalyst 9300X can be deployed as a border VTEP at a branch site to provide secure connectivity to the campus network over a WAN, with IPsec encryption.

Workflow to Configure BGP EVPN VXLAN over IPsec

Before you begin

Ensure that the devices have the correct license to run IPsec and EVPN VXLAN. For license information, refer Cisco 9300 Series Switch Data Sheet.

Procedure

Step 1 Configure the BGP EVPN VXLAN overlay:

Based on the network reachability and segmentation requirements, configure the appropriate overlay topology. Refer to the respective sections for more details on each of the following overlay network segmentations:

a) Configure L2 overlay: Perform all the configuration tasks that are listed in *Configuring EVPN VXLAN Layer 2 Overlay Network*.

b) Configure L3 overlay: Perform all the configuration tasks that are listed in *Configuring EVPN VXLAN Layer 3 Overlay Network*.

c) Configure Distributed Anycast Gateway (DAG) or Centralized Gateway (CGW): Perform all the tasks that are listed in *Configuring EVPN VXLAN Integrated Routing and Bridging*.

Step 2 Configure IPsec in the underlay: Perform all the tasks that are listed in the "Configuring IPsec" section of the *Security Configuration Guide*.

Note Each secure packet that is transmitted has an IPsec header in addition to the BGP EVPN VXLAN header. Adjust the System MTU and TCP MSS size accordingly.

Step 3 Configure BGP neighborship over IPsec tunnel.

a) To establish BGP neighborship and for loopback interface reachability, configure interior gateway protocol (IGP) over IPsec tunnel.

Here is a sample configuration snippet:

NVE loopback and IPsec tunnel in one IGP instance: the following commands establish NVE or VXLAN neighborship over IPsec tunnel:

```
interface Loopback1
 description NVE Loopback
 ip address 172.16.254.1 255.255.255.255
 ip pim sparse-mode
 ip ospf 1 area 0
!
interface Tunnel10
 description “IPSEC tunnel”
 ip address 172.16.12.1 255.255.255.0
 ip pim sparse-mode
 ip ospf 1 area 0
 tunnel source Loopback10
 tunnel mode ipsec ipv4
 tunnel destination 172.16.10.2
 tunnel protection ipsec profile ipsec_prof10
```

Loopback that is used by IPsec Tunnel in another IGP instance: the following commands establish an IPsec tunnel between the endpoints:

```
interface Loopback10
description ipsec Loopback
 ip address 172.16.10.1 255.255.255.0
 ip ospf 2 area 0
!
```

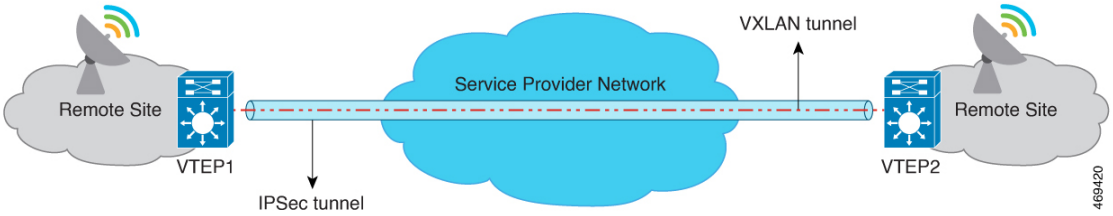
b) Alternatively, configure a static route for BGP neighborship, if you cannot run IGP over IPsec tunnel.

```
ip route 172.16.254.2 255.255.255.255 Tunnel10
```

Refer to the Configuration Example for BGP EVPN VXLAN over IPsec

Configuration Example for BGP EVPN VXLAN over IPsec

Figure 2: Secure VXLAN Traffic Between Two VTEPs



In this topology, VTEP1 and VTEP2 communicate through a secure VXLAN tunnel that runs through a service provider network.

The following table provides sample configurations for the devices in this topology.

VTEP1	VTEP2

VTEP1	VTEP2
hostname VTEP1 ! vrf definition red rd 1:100 ! address-family ipv4 route-target export 1:100 route-target import 1:100 route-target export 1:100 stitching route-target import 1:100 stitching exit-address-family ! address-family ipv6 route-target export 1:100 route-target import 1:100 route-target export 1:100 stitching route-target import 1:100 stitching exit-address-family ! ip routing ip multicast-routing ! ipv6 unicast-routing ipv6 multicast-routing ! l2vpn evpn replication-type ingress router-id Loopback1 ! l2vpn evpn instance 1500 vlan-based encapsulation vxlan replication-type ingress ! l2vpn evpn instance 1501 vlan-based encapsulation vxlan replication-type ingress ! license boot level network-advantage addon dna-advantage ! system mtu 9198 ! crypto engine compliance shield disable ! crypto ikev2 keyring ikev10_key peer mypeer address 0.0.0.0 0.0.0.0 pre-shared-key cisco123 ! crypto ikev2 profile ikev2_prof10 match identity remote address 172.16.10.2 255.255.255.255 authentication remote pre-share authentication local pre-share keyring local ikev10_key dpd 10 2 periodic ! vlan configuration 500 member vni 50000 vlan configuration 1500 member evpn-instance 1500 vni 11500 vlan configuration 1501	hostname VTEP2 ! vrf definition red rd 1:100 ! address-family ipv4 route-target export 1:100 route-target import 1:100 route-target export 1:100 stitching route-target import 1:100 stitching exit-address-family ! address-family ipv6 route-target export 1:100 route-target import 1:100 route-target export 1:100 stitching route-target import 1:100 stitching exit-address-family ! ip routing ip multicast-routing ! ipv6 unicast-routing ipv6 multicast-routing ! l2vpn evpn replication-type ingress router-id Loopback1 ! l2vpn evpn instance 1500 vlan-based encapsulation vxlan replication-type ingress ! l2vpn evpn instance 1501 vlan-based encapsulation vxlan replication-type ingress ! license boot level network-advantage addon dna-advantage ! system mtu 9198 ! crypto engine compliance shield disable ! crypto ikev2 keyring ikev10_key peer mypeer address 0.0.0.0 0.0.0.0 pre-shared-key cisco123 ! crypto ikev2 profile ikev2_prof10 match identity remote address 172.16.10.1 255.255.255.255 authentication remote pre-share authentication local pre-share keyring local ikev10_key dpd 10 2 periodic ! vlan configuration 500 member vni 50000 vlan configuration 1500 member evpn-instance 1500 vni 11500 vlan configuration 1501

VTEP1	VTEP2
member evpn-instance 1501 vni 11501 ! crypto ipsec transform-set tfs esp-gcm esn mode tunnel ! crypto ipsec profile ipsec_prof10 set transform-set tfs set ikev2-profile ikev2_prof10 ! ! interface Loopback0 ip address 172.16.255.1 255.255.255.255 ip pim sparse-mode ip ospf 1 area 0 ! interface Loopback1 ip address 172.16.254.1 255.255.255.255 ip pim sparse-mode ip ospf 1 area 0 ! interface Loopback10 ip address 172.16.10.1 255.255.255.0 ip ospf 2 area 0 ! interface Tunnel10 description “IPSEC tunnel” ip address 172.16.12.1 255.255.255.0 ip pim sparse-mode ip ospf 1 area 0 tunnel source Loopback10 tunnel mode ipsec ipv4 tunnel destination 172.16.10.2 tunnel protection ipsec profile ipsec_prof10 ! ! interface TwentyFiveGigE1/0/1 ! interface TwentyFiveGigE1/0/2 ! ! ! interface TwentyFiveGigE1/0/3 description “Connected to VTEP2” no switchport ip address 10.3.1.1 255.255.255.0 ip pim sparse-mode ip ospf network point-to-point ip ospf 2 area 0 ! interface TwentyFiveGigE1/0/16 description “Host” switchport trunk allowed vlan 1500-1503 switchport mode trunk ! ! interface Vlan500 description “Core SVI” vrf forwarding red ip unnumbered Loopback1 ip pim sparse-mode ipv6 enable	member evpn-instance 1501 vni 11501 ! crypto ipsec transform-set tfs esp-gcm esn mode tunnel ! crypto ipsec profile ipsec_prof10 set transform-set tfs set ikev2-profile ikev2_prof10 responder-only ! interface Loopback0 ip address 172.16.255.2 255.255.255.255 ip pim sparse-mode ip ospf 1 area 0 ! interface Loopback1 ip address 172.16.254.2 255.255.255.255 ip pim sparse-mode ip ospf 1 area 0 ! interface Loopback10 ip address 172.16.10.2 255.255.255.255 ip ospf 2 area 0 ! interface Tunnel10 description “IPSEC tunnel” ip address 172.16.12.2 255.255.255.0 ip pim sparse-mode ip ospf 1 area 0 tunnel source Loopback10 tunnel mode ipsec ipv4 tunnel destination 172.16.10.1 tunnel protection ipsec profile ipsec_prof10 ! ! interface TwentyFiveGigE1/0/1 description “Host” switchport access vlan 1500 switchport trunk allowed vlan 1500-1503 switchport mode trunk ! interface TwentyFiveGigE1/0/3 description “connected to VTEP1” no switchport ip address 10.3.1.2 255.255.255.0 ip pim sparse-mode ip ospf network point-to-point ip ospf 2 area 0 ! ! ! ! ! ! interface Vlan500 description “Core SVI” vrf forwarding red ip unnumbered Loopback1 ip pim sparse-mode ipv6 enable

VTEP1	VTEP2
no autostate ! interface Vlan1500 mac-address 0000.00aa.00aa vrf forwarding red ip address 192.168.1.1 255.255.255.0 ip pim sparse-mode ip igmp version 3 ! interface Vlan1501 mac-address 0000.00bb.00bb vrf forwarding red ip address 192.168.2.1 255.255.255.0 ip pim sparse-mode ip igmp version 3 ! interface nve1 no ip address source-interface Loopback1 host-reachability protocol bgp member vni 50000 vrf red member vni 11500 ingress-replication member vni 11501 ingress-replication ! router ospf 1 ! router ospf 2 ! router bgp 1 bgp router-id interface Loopback0 bgp log-neighbor-changes bgp update-delay 1 bgp graceful-restart no bgp default ipv4-unicast neighbor 172.16.255.2 remote-as 1 neighbor 172.16.255.2 update-source Loopback0 ! address-family ipv4 redistribute static redistribute connected neighbor 172.16.255.2 activate exit-address-family ! address-family ipv6 redistribute connected redistribute static exit-address-family ! address-family l2vpn evpn neighbor 172.16.255.2 activate neighbor 172.16.255.2 send-community both exit-address-family ! address-family ipv4 vrf red advertise l2vpn evpn redistribute static redistribute connected exit-address-family ! address-family ipv6 vrf red redistribute connected	no autostate ! interface Vlan1500 mac-address 0000.00aa.00aa vrf forwarding red ip address 192.168.1.1 255.255.255.0 ip pim sparse-mode ip igmp version 3 ! interface Vlan1501 mac-address 0000.00bb.00bb vrf forwarding red ip address 192.168.2.1 255.255.255.0 ip pim sparse-mode ip igmp version 3 ! interface nve1 no ip address source-interface Loopback1 host-reachability protocol bgp member vni 50000 vrf red member vni 11500 ingress-replication member vni 11501 ingress-replication ! router ospf 1 ! router ospf 2 ! router bgp 1 bgp router-id interface Loopback0 bgp log-neighbor-changes bgp update-delay 1 bgp graceful-restart no bgp default ipv4-unicast neighbor 172.16.255.1 remote-as 1 neighbor 172.16.255.1 update-source Loopback0 ! address-family ipv4 redistribute static redistribute connected neighbor 172.16.255.1 activate exit-address-family ! address-family ipv6 redistribute connected redistribute static exit-address-family ! address-family l2vpn evpn neighbor 172.16.255.1 activate neighbor 172.16.255.1 send-community both exit-address-family ! address-family ipv4 vrf red advertise l2vpn evpn redistribute static redistribute connected exit-address-family ! address-family ipv6 vrf red redistribute connected redistribute static

VTEP1	VTEP2
redistribute static advertise l2vpn evpn exit-address-family ! ip pim rp-address 172.16.255.2 !	advertise l2vpn evpn exit-address-family ! ip pim rp-address 172.16.255.2 !

Verifying BGP EVPN VXLAN over IPsec

The following sections provide sample output of **show** commands to verify the BGP EVPN VXLAN over IPsec configuration on the devices in the Configuration Example for BGP EVPN VXLAN over IPsec.

Outputs to Verify the Configuration on VTEP1

```
VTEP1# show nve peers
'M' - MAC entry download flag  'A' - Adjacency download flag
'4' - IPv4 flag  '6' - IPv6 flag

Interface  VNI      Type Peer-IP          RMAC/Num_RTs   eVNI     state flags UP time
nve1       50000    L3CP 172.16.254.2     34ed.1b7e.44d0 50000      UP  A/M/4 00:18:51
nve1       11500    L2CP 172.16.254.2     3              11500      UP   N/A  00:18:51
nve1       11501    L2CP 172.16.254.2     3              11501      UP   N/A  00:18:51


VTEP1# show l2vpn evpn evi detail
EVPN instance:       1500 (VLAN Based)
  RD:                172.16.254.1:1500 (auto)
  Import-RTs:        1:1500
  Export-RTs:        1:1500
  Per-EVI Label:     none
  State:             Established
  Replication Type:  Ingress
  Encapsulation:     vxlan
  IP Local Learn:    Enabled (global)
  Adv. Def. Gateway: Disabled (global)
  Re-originate RT5:  Disabled
  Adv. Multicast:    Disabled (global)
  Vlan:              1500
    Protected:       False
    Ethernet-Tag:    0
    State:           Established
    Flood Suppress:  Attached
    Core If:         Vlan500
    Access If:       Vlan1500
    NVE If:          nve1
    RMAC:            34ed.1b7e.4350
    Core Vlan:       500
    L2 VNI:          11500
    L3 VNI:          50000
    VTEP IP:         172.16.254.1
    VRF:             red
    IPv4 IRB:        Enabled
    IPv6 IRB:        Disabled
    Pseudoports:
      TwentyFiveGigE1/0/16 service instance 1500
        Routes: 1 MAC, 1 MAC/IP
    Peers:
      172.16.254.2
```

```
        Routes: 1 MAC, 1 MAC/IP, 1 IMET, 0 EAD

EVPN instance:       1501 (VLAN Based)
  RD:                172.16.254.1:1501 (auto)
  Import-RTs:        1:1501
  Export-RTs:        1:1501
  Per-EVI Label:     none
  State:             Established
  Replication Type:  Ingress
  Encapsulation:     vxlan
  IP Local Learn:    Enabled (global)
  Adv. Def. Gateway: Disabled (global)
  Re-originate RT5:  Disabled
  Adv. Multicast:    Disabled (global)
  Vlan:              1501
    Protected:       False
    Ethernet-Tag:    0
    State:           Established
    Flood Suppress:  Attached
    Core If:         Vlan500
    Access If:       Vlan1501
    NVE If:          nve1
    RMAC:            34ed.1b7e.4350
    Core Vlan:       500
    L2 VNI:          11501
    L3 VNI:          50000
    VTEP IP:         172.16.254.1
    VRF:             red
    IPv4 IRB:        Enabled
    IPv6 IRB:        Disabled
    Pseudoports:
      TwentyFiveGigE1/0/16 service instance 1501
        Routes: 1 MAC, 1 MAC/IP
    Peers:
      172.16.254.2
        Routes: 1 MAC, 1 MAC/IP, 1 IMET, 0 EAD


VTEP1# show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, m - OMP
       n - NAT, Ni - NAT inside, No - NAT outside, Nd - NAT DIA
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       H - NHRP, G - NHRP registered, g - NHRP registration summary
       o - ODR, P - periodic downloaded static route, l - LISP
       a - application route
       + - replicated route, % - next hop override, p - overrides from PfR
       & - replicated local route overrides by connected

Gateway of last resort is not set

      10.0.0.0/8 is variably subnetted, 2 subnets, 3 masks
C        10.3.1.0/24 is directly connected, TwentyFiveGigE1/0/3
L        10.3.1.1/32 is directly connected, TwentyFiveGigE1/0/3
      172.16.0.0/16 is variably subnetted, 9 subnets, 2 masks
C        172.16.10.0/24 is directly connected, Loopback10
L        172.16.10.1/32 is directly connected, Loopback10
O        172.16.10.2/32 [110/2] via 10.3.1.2, 00:35:52, TwentyFiveGigE1/0/3
C        172.16.12.0/24 is directly connected, Tunnel10
L        172.16.12.1/32 is directly connected, Tunnel10
C        172.16.254.1/32 is directly connected, Loopback1
```

```
O        172.16.254.2/32 [110/1001] via 172.16.12.2, 00:29:07, Tunnel10
C        172.16.255.1/32 is directly connected, Loopback0
O        172.16.255.2/32 [110/1001] via 172.16.12.2, 00:29:07, Tunnel10


VTEP1# show ip route  vrf red

Routing Table: red
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, m - OMP
       n - NAT, Ni - NAT inside, No - NAT outside, Nd - NAT DIA
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       H - NHRP, G - NHRP registered, g - NHRP registration summary
       o - ODR, P - periodic downloaded static route, l - LISP
       a - application route
       + - replicated route, % - next hop override, p - overrides from PfR
       & - replicated local route overrides by connected

Gateway of last resort is not set

      192.168.1.0/24 is variably subnetted, 4 subnets, 2 masks
C        192.168.1.0/24 is directly connected, Vlan1500
L        192.168.1.1/32 is directly connected, Vlan1500
S        192.168.1.100/32 is directly connected, Vlan1500
B        192.168.1.200/32 [200/0] via 172.16.254.2, 00:33:05, Vlan500
      192.168.2.0/24 is variably subnetted, 4 subnets, 2 masks
C        192.168.2.0/24 is directly connected, Vlan1501
L        192.168.2.1/32 is directly connected, Vlan1501
S        192.168.2.100/32 is directly connected, Vlan1501
B        192.168.2.200/32 [200/0] via 172.16.254.2, 00:01:39, Vlan500


VTEP1# show bgp l2vpn evpn all
BGP table version is 249, local router ID is 172.16.255.1
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              r RIB-failure, S Stale, m multipath, b backup-path, f RT-Filter,
              x best-external, a additional-path, c RIB-compressed,
              t secondary path, L long-lived-stale,
Origin codes: i - IGP, e - EGP, ? - incomplete
RPKI validation codes: V valid, I invalid, N Not found

     Network          Next Hop            Metric LocPrf Weight Path
Route Distinguisher: 172.16.254.1:1500
 *>i  [2][172.16.254.1:1500][0][48][001201000001][0][*]/20
                      172.16.254.2             0    100      0 ?
 *>i  [2][172.16.254.1:1500][0][48][001201000001][32][192.168.1.200]/24
                      172.16.254.2             0    100      0 ?
 *>   [2][172.16.254.1:1500][0][48][001501000001][0][*]/20
                      0.0.0.0                            32768 ?
 *>   [2][172.16.254.1:1500][0][48][001501000001][32][192.168.1.100]/24
                      0.0.0.0                            32768 ?
Route Distinguisher: 172.16.254.1:1501
 *>i  [2][172.16.254.1:1501][0][48][001201000002][0][*]/20
                      172.16.254.2             0    100      0 ?
 *>i  [2][172.16.254.1:1501][0][48][001201000002][32][192.168.2.200]/24
     Network          Next Hop            Metric LocPrf Weight Path
                      172.16.254.2             0    100      0 ?
 *>   [2][172.16.254.1:1501][0][48][001501000002][0][*]/20
                      0.0.0.0                            32768 ?
 *>   [2][172.16.254.1:1501][0][48][001501000002][32][192.168.2.100]/24
                      0.0.0.0                            32768 ?
Route Distinguisher: 172.16.254.2:1500
```

```
 *>i  [2][172.16.254.2:1500][0][48][001201000001][0][*]/20
                      172.16.254.2             0    100      0 ?
 *>i  [2][172.16.254.2:1500][0][48][001201000001][32][192.168.1.200]/24
                      172.16.254.2             0    100      0 ?
Route Distinguisher: 172.16.254.2:1501
 *>i  [2][172.16.254.2:1501][0][48][001201000002][0][*]/20
                      172.16.254.2             0    100      0 ?
 *>i  [2][172.16.254.2:1501][0][48][001201000002][32][192.168.2.200]/24
                      172.16.254.2             0    100      0 ?
Route Distinguisher: 172.16.254.1:1500
 *>   [3][172.16.254.1:1500][0][32][172.16.254.1]/17
                      0.0.0.0                            32768 ?
 *>i  [3][172.16.254.1:1500][0][32][172.16.254.2]/17
                      172.16.254.2             0    100      0 ?
Route Distinguisher: 172.16.254.1:1501
 *>   [3][172.16.254.1:1501][0][32][172.16.254.1]/17
     Network          Next Hop            Metric LocPrf Weight Path
                      0.0.0.0                            32768 ?
 *>i  [3][172.16.254.1:1501][0][32][172.16.254.2]/17
                      172.16.254.2             0    100      0 ?
Route Distinguisher: 172.16.254.2:1500
 *>i  [3][172.16.254.2:1500][0][32][172.16.254.2]/17
                      172.16.254.2             0    100      0 ?
Route Distinguisher: 172.16.254.2:1501
 *>i  [3][172.16.254.2:1501][0][32][172.16.254.2]/17
                      172.16.254.2             0    100      0 ?
Route Distinguisher: 1:100 (default for vrf red)
 * i  [5][1:100][0][24][192.168.1.0]/17
                      172.16.254.2             0    100      0 ?
 *>                    0.0.0.0                  0         32768 ?
 * i  [5][1:100][0][24][192.168.2.0]/17
                      172.16.254.2             0    100      0 ?
 *>                    0.0.0.0                  0         32768 ?
```

```
VTEP1# show crypto session detail
Crypto session current status

Code: C - IKE Configuration mode, D - Dead Peer Detection
K - Keepalives, N - NAT-traversal, T - cTCP encapsulation
X - IKE Extended Authentication, F - IKE Fragmentation
R - IKE Auto Reconnect, U - IKE Dynamic Route Update
S - SIP VPN

Interface: Tunnel10
Profile: ikev2_prof10
Uptime: 00:16:58
Session status: UP-ACTIVE
Peer: 172.16.10.2 port 500 fvrf: (none) ivrf: (none)
      Phase1_id: 172.16.10.2
      Desc: (none)
  Session ID: 3
  IKEv2 SA: local 172.16.10.1/500 remote 172.16.10.2/500 Active
          Capabilities:DU connid:1 lifetime:23:43:02
  IPSEC FLOW: permit ip   0.0.0.0/0.0.0.0 0.0.0.0/0.0.0.0
        Active SAs: 2, origin: crypto map
        Inbound:  #pkts dec'ed 1016508 drop 0 life (KB/Sec) 1058011/2581
        Outbound: #pkts enc'ed 239 drop 0 life (KB/Sec) 36/2581
```

```
VTEP1# show int tunnel10 stats
Tunnel10
          Switching path    Pkts In   Chars In   Pkts Out  Chars Out
               Processor          0          0          2         64
             Route cache          0          0          0          0
       Distributed cache    1056533 1092057464        484      56333
```

```
                    Total    1056533 1092057464        486      56397
```

Outputs to Verify the Configuration on VTEP2

```
VTEP2# show nve peers
'M' - MAC entry download flag  'A' - Adjacency download flag
'4' - IPv4 flag  '6' - IPv6 flag

Interface  VNI      Type Peer-IP          RMAC/Num_RTs   eVNI     state flags UP time
nve1       50000    L3CP 172.16.254.1     34ed.1b7e.4350 50000      UP  A/M/4 00:20:04
nve1       11500    L2CP 172.16.254.1     3              11500      UP   N/A  00:20:04
nve1       11501    L2CP 172.16.254.1     3              11501      UP   N/A  00:20:04


VTEP2# show l2vpn evpn evi detail
EVPN instance:       1500 (VLAN Based)
  RD:                172.16.254.2:1500 (auto)
  Import-RTs:        1:1500
  Export-RTs:        1:1500
  Per-EVI Label:     none
  State:             Established
  Replication Type:  Ingress
  Encapsulation:     vxlan
  IP Local Learn:    Enabled (global)
  Adv. Def. Gateway: Disabled (global)
  Re-originate RT5:  Disabled
  Adv. Multicast:    Disabled (global)
  Vlan:              1500
    Protected:       False
    Ethernet-Tag:    0
    State:           Established
    Flood Suppress:  Attached
    Core If:         Vlan500
    Access If:       Vlan1500
    NVE If:          nve1
    RMAC:            34ed.1b7e.44d0
    Core Vlan:       500
    L2 VNI:          11500
    L3 VNI:          50000
    VTEP IP:         172.16.254.2
    VRF:             red
    IPv4 IRB:        Enabled
    IPv6 IRB:        Disabled
    Pseudoports:
      TwentyFiveGigE1/0/1 service instance 1500
        Routes: 1 MAC, 1 MAC/IP
    Peers:
      172.16.254.1
        Routes: 1 MAC, 1 MAC/IP, 1 IMET, 0 EAD

EVPN instance:       1501 (VLAN Based)
  RD:                172.16.254.2:1501 (auto)
  Import-RTs:        1:1501
  Export-RTs:        1:1501
  Per-EVI Label:     none
  State:             Established
  Replication Type:  Ingress
  Encapsulation:     vxlan
  IP Local Learn:    Enabled (global)
  Adv. Def. Gateway: Disabled (global)
  Re-originate RT5:  Disabled
  Adv. Multicast:    Disabled (global)
```

```
  Vlan:              1501
    Protected:       False
    Ethernet-Tag:    0
    State:           Established
    Flood Suppress:  Attached
    Core If:         Vlan500
    Access If:       Vlan1501
    NVE If:          nve1
    RMAC:            34ed.1b7e.44d0
    Core Vlan:       500
    L2 VNI:          11501
    L3 VNI:          50000
    VTEP IP:         172.16.254.2
    VRF:             red
    IPv4 IRB:        Enabled
    IPv6 IRB:        Disabled
    Pseudoports:
      TwentyFiveGigE1/0/1 service instance 1501
        Routes: 1 MAC, 1 MAC/IP
    Peers:
      172.16.254.1
        Routes: 1 MAC, 1 MAC/IP, 1 IMET, 0 EAD
```

```
VTEP2# show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, m - OMP
       n - NAT, Ni - NAT inside, No - NAT outside, Nd - NAT DIA
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       H - NHRP, G - NHRP registered, g - NHRP registration summary
       o - ODR, P - periodic downloaded static route, l - LISP
       a - application route
       + - replicated route, % - next hop override, p - overrides from PfR
       & - replicated local route overrides by connected

Gateway of last resort is not set

      10.0.0.0/8 is variably subnetted, 2 subnets, 3 masks
C        10.3.1.0/24 is directly connected, TwentyFiveGigE1/0/3
L        10.3.1.2/32 is directly connected, TwentyFiveGigE1/0/3
      172.16.0.0/16 is variably subnetted, 9 subnets, 2 masks
B        172.16.10.0/24 [200/0] via 172.16.255.1, 00:30:42
O        172.16.10.1/32 [110/2] via 10.3.1.1, 00:33:32, TwentyFiveGigE1/0/3
C        172.16.10.2/32 is directly connected, Loopback10
C        172.16.12.0/24 is directly connected, Tunnel10
L        172.16.12.2/32 is directly connected, Tunnel10
O        172.16.254.1/32 [110/1001] via 172.16.12.1, 00:26:48, Tunnel10
C        172.16.254.2/32 is directly connected, Loopback1
O        172.16.255.1/32 [110/1001] via 172.16.12.1, 00:26:48, Tunnel10
C        172.16.255.2/32 is directly connected, Loopback0
```

```
VTEP2# show ip route  vrf red

Routing Table: red
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, m - OMP
       n - NAT, Ni - NAT inside, No - NAT outside, Nd - NAT DIA
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
```

```
       H - NHRP, G - NHRP registered, g - NHRP registration summary
       o - ODR, P - periodic downloaded static route, l - LISP
       a - application route
       + - replicated route, % - next hop override, p - overrides from PfR
       & - replicated local route overrides by connected

Gateway of last resort is not set

      192.168.1.0/24 is variably subnetted, 4 subnets, 2 masks
C        192.168.1.0/24 is directly connected, Vlan1500
L        192.168.1.1/32 is directly connected, Vlan1500
B        192.168.1.100/32 [200/0] via 172.16.254.1, 00:00:41, Vlan500
S        192.168.1.200/32 is directly connected, Vlan1500
      192.168.2.0/24 is variably subnetted, 4 subnets, 2 masks
C        192.168.2.0/24 is directly connected, Vlan1501
L        192.168.2.1/32 is directly connected, Vlan1501
B        192.168.2.100/32 [200/0] via 172.16.254.1, 00:00:35, Vlan500
S        192.168.2.200/32 is directly connected, Vlan1501


VTEP2# show bgp l2vpn evpn all
BGP table version is 309, local router ID is 172.16.255.2
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              r RIB-failure, S Stale, m multipath, b backup-path, f RT-Filter,
              x best-external, a additional-path, c RIB-compressed,
              t secondary path, L long-lived-stale,
Origin codes: i - IGP, e - EGP, ? - incomplete
RPKI validation codes: V valid, I invalid, N Not found

     Network          Next Hop            Metric LocPrf Weight Path
Route Distinguisher: 172.16.254.1:1500
 *>i  [2][172.16.254.1:1500][0][48][001501000001][0][*]/20
                      172.16.254.1             0    100      0 ?
 *>i  [2][172.16.254.1:1500][0][48][001501000001][32][192.168.1.100]/24
                      172.16.254.1             0    100      0 ?
Route Distinguisher: 172.16.254.1:1501
 *>i  [2][172.16.254.1:1501][0][48][001501000002][0][*]/20
                      172.16.254.1             0    100      0 ?
 *>i  [2][172.16.254.1:1501][0][48][001501000002][32][192.168.2.100]/24
                      172.16.254.1             0    100      0 ?
Route Distinguisher: 172.16.254.2:1500
 *>   [2][172.16.254.2:1500][0][48][001201000001][0][*]/20
                      0.0.0.0                            32768 ?
     Network          Next Hop            Metric LocPrf Weight Path
 *>   [2][172.16.254.2:1500][0][48][001201000001][32][192.168.1.200]/24
                      0.0.0.0                            32768 ?
 *>i  [2][172.16.254.2:1500][0][48][001501000001][0][*]/20
                      172.16.254.1             0    100      0 ?
 *>i  [2][172.16.254.2:1500][0][48][001501000001][32][192.168.1.100]/24
                      172.16.254.1             0    100      0 ?
Route Distinguisher: 172.16.254.2:1501
 *>   [2][172.16.254.2:1501][0][48][001201000002][0][*]/20
                      0.0.0.0                            32768 ?
 *>   [2][172.16.254.2:1501][0][48][001201000002][32][192.168.2.200]/24
                      0.0.0.0                            32768 ?
 *>i  [2][172.16.254.2:1501][0][48][001501000002][0][*]/20
                      172.16.254.1             0    100      0 ?
 *>i  [2][172.16.254.2:1501][0][48][001501000002][32][192.168.2.100]/24
                      172.16.254.1             0    100      0 ?
Route Distinguisher: 172.16.254.1:1500
 *>i  [3][172.16.254.1:1500][0][32][172.16.254.1]/17
                      172.16.254.1             0    100      0 ?
Route Distinguisher: 172.16.254.1:1501
 *>i  [3][172.16.254.1:1501][0][32][172.16.254.1]/17
                      172.16.254.1             0    100      0 ?
```

```
Route Distinguisher: 172.16.254.2:1500
     Network          Next Hop            Metric LocPrf Weight Path
 *>i  [3][172.16.254.2:1500][0][32][172.16.254.1]/17
                      172.16.254.1             0    100      0 ?
 *>   [3][172.16.254.2:1500][0][32][172.16.254.2]/17
                      0.0.0.0                            32768 ?
Route Distinguisher: 172.16.254.2:1501
 *>i  [3][172.16.254.2:1501][0][32][172.16.254.1]/17
                      172.16.254.1             0    100      0 ?
 *>   [3][172.16.254.2:1501][0][32][172.16.254.2]/17
                      0.0.0.0                            32768 ?
Route Distinguisher: 1:100 (default for vrf red)
 * i  [5][1:100][0][24][192.168.1.0]/17
                      172.16.254.1             0    100      0 ?
 *>                    0.0.0.0                  0         32768 ?
 * i  [5][1:100][0][24][192.168.2.0]/17
                      172.16.254.1             0    100      0 ?
 *>                    0.0.0.0                  0         32768 ?


VTEP2# show crypto session detail
Crypto session current status

Code: C - IKE Configuration mode, D - Dead Peer Detection
K - Keepalives, N - NAT-traversal, T - cTCP encapsulation
X - IKE Extended Authentication, F - IKE Fragmentation
R - IKE Auto Reconnect, U - IKE Dynamic Route Update
S - SIP VPN

Interface: Tunnel10
Profile: ikev2_prof10
Uptime: 00:17:28
Session status: UP-ACTIVE
Peer: 172.16.10.1 port 500 fvrf: (none) ivrf: (none)
      Phase1_id: 172.16.10.1
      Desc: (none)
  Session ID: 4
  IKEv2 SA: local 172.16.10.2/500 remote 172.16.10.1/500 Active
          Capabilities:DU connid:1 lifetime:23:42:32
  IPSEC FLOW: permit ip   0.0.0.0/0.0.0.0 0.0.0.0/0.0.0.0
        Active SAs: 2, origin: crypto map
        Inbound:  #pkts dec'ed 245 drop 0 life (KB/Sec) 30/2552
        Outbound: #pkts enc'ed 1043067 drop 0 life (KB/Sec) 1118249/2552


VTEP2# show int tunnel10 stats
Tunnel10
          Switching path    Pkts In   Chars In   Pkts Out  Chars Out
               Processor          0          0          0          0
            Route cache           0          0          0          0
       Distributed cache        228      21855    1027163 1082443955
                   Total        228      21855    1027163 1082443955
```