Configure DVTI with Dynamic Routing Protocols on Secure Firewall

Contents

Introduction

This document describes how to configure a Dynamic Virtual Tunnel Interface (DVTI) on Secure Firewall 9.20.

Prerequisites

- Have one Cisco Secure Firewall with ASA 9.20 or later with a basic routing configuration and IKEV2 support that works as the hub with one Loopback interface to simulate local network on premises of 192.168.9.0/24.
- Have one Cisco Secure Firewall with ASA 9.20 or later with basic routing configuration and IKEv2 support to work as a spoke-1 with one Loopback interface preconfigured to simulate remote network of 192.168.7.0/24.

Requirements

- General knowledge of all dynamic routing protocols described on this document (OSPF, EIGRP and BGP).
- Be familiar with CLI configuration on Cisco Secure Firewall devices.

Components Used

The information in this document is based on these software versions:

- Cisco Secure Firewall with ASA 9.20 or later.

> **Note**: The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command.

Background Information

Dynamic Virtual Tunnel Interfaces

Dynamic Virtual Tunnel Interfaces (DVTI) can provide highly secure and scalable connectivity for remote-access Virtual Private Networks (VPN).

DVTIs can be used for both Hub and Spoke configuration. The tunnels provide an on-demand separate virtual access interface for each VPN session.

1. The spoke initiates an IKE exchange request with the hub for a VPN connection.

2. The hub authenticates the spoke.

3. The Cisco Secure Firewall Management Centerassigns a dynamic virtual template on the hub.

4. The virtual template dynamically generates a virtual access interface on the hub. This interface is unique for the VPN session per spoke.

5. The hub establishes a dynamic VTI tunnel with the spoke that uses the virtual access interface.

6. The hub and spoke exchange traffic over the tunnel that uses dynamic routing protocols (BGP/OSPF/EIGRP) or with protected networks feature (Multiple-Security Association VTI).

7. Dynamic VTIs function like any other interface so that you can apply QoS, firewall rules, routing protocols and other features as soon as the tunnel is active.

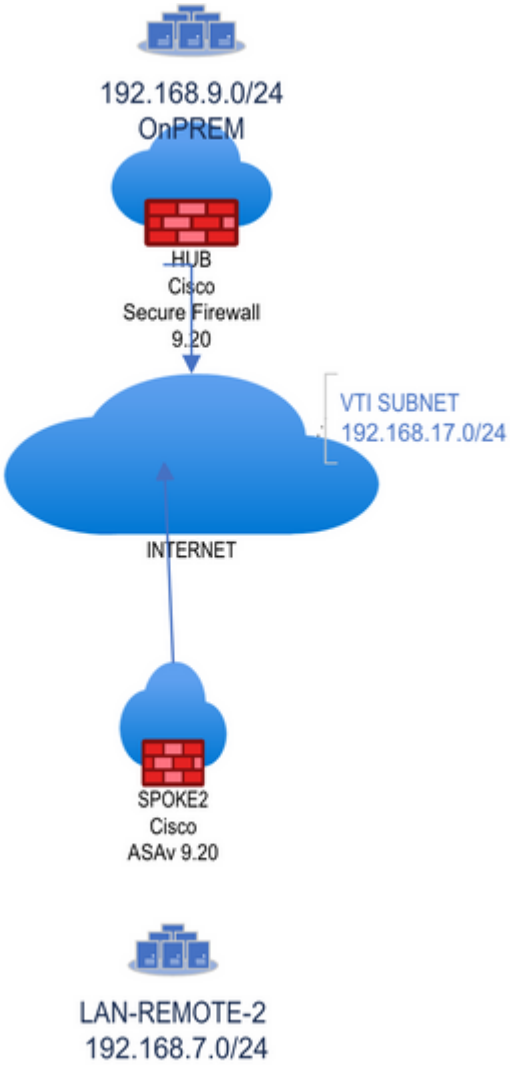
8. A single DVTI is created at the HUB device and multiple Static Tunnel Interfaces for multiple remote/spoke sites.

In this article BGP, OSPF and EIGRP can be tested over DVTI.

> **Note**: Cisco Secure Firewall added support fot DVTI on version 7.3 and currently it only supports one single DVTI as per Cisco bug ID CSCwe13781.

Configure

Network Diagram



Configurations

Cisco Secure Firewall Hub configuration

Configure physical tunnel source interface.

```
interface GigabitEthernet0/0
 nameif vlan2820
 security-level 100
 ip address 10.28.20.98 255.255.255.0
```

Configure IkEv2 policy.

```
crypto ikev2 policy 1
 encryption aes-256 aes-192 aes
 integrity sha512 sha384 sha256 sha
 group 21 20 14
 prf sha256
 lifetime seconds 86400
```

Configure IPSEC policy and attach it to a new IPSEC profile.

```
crypto ipsec ikev2 ipsec-proposal VPN-LAB
 protocol esp encryption aes-256 aes-192 aes
 protocol esp integrity sha-512 sha-256 sha-1

crypto ipsec profile VPN-LAB-PROFILE
 set ikev2 ipsec-proposal VPN-LAB
 set security-association lifetime seconds 1000
```

Configure Virtual-template with with the IPSEC Profile previously created and assign it to a Loopback interface that provides the IP Address for the DVTI.

Note: Virtual-template is used to configure DVTI for on-demand tunnels.

```
interface Loopback200
 nameif DVTI-LOOPBACK
 ip address 172.16.17.1 255.255.255.255

interface Virtual-Template1 type tunnel
 nameif DVTI-HUB
 ip unnumbered DVTI-LOOPBACK
 tunnel source interface vlan2820
 tunnel mode ipsec ipv4
 tunnel protection ipsec profile FMC_IPSEC_PROFILE_2
```

Create a secondary Loopback interface to simulate traffic from OnPREM network behind hub.

Note: Skip this step if you have local traffic behind the hub.

```
interface Loopback100
 nameif ON-PREM
 ip address 192.168.9.1 255.255.255.255
```

Configure tunnel-group.

Note: The command route set interface sends the DVTI IP address as a static IP address to the peer.

```
tunnel-group 10.28.20.100 type ipsec-l2l
tunnel-group 10.28.20.100 ipsec-attributes
 virtual-template 1
 ikev2 remote-authentication pre-shared-key *****
 ikev2 local-authentication pre-shared-key *****
```

```
 ikev2 route set interface
```

Enable IKEv2 on the interface that builds the tunnel.

```
crypto ikev2 enable vlan2820
```

Cisco Secure Firewall spoke configuration

Configure physical tunnel source interface.

```
interface GigabitEthernet0/0
 nameif vlan2820
 security-level 100
 ip address 10.28.20.100 255.255.255.0
```

Configure IKEv2 policy.

```
crypto ikev2 policy 1
 encryption aes-256 aes-192 aes
 integrity sha512 sha384 sha256 sha
 group 21 20 14
 prf sha256
 lifetime seconds 86400
```

Configure IPSEC policy and attach it to a new IPSEC profile.

```
crypto ipsec ikev2 ipsec-proposal VPN-LAB
 protocol esp encryption aes-256 aes-192 aes
 protocol esp integrity sha-512 sha-256 sha-1
crypto ipsec profile VPN-LAB-PROFILE
 set ikev2 ipsec-proposal VPN-LAB
 set security-association lifetime seconds 1000
```

Configure Static Virtual Tunnel Interface with the IPSEC Profile, previously created and assign it to a Loopback interface that provides the unnumbered IP Address.

```
interface Loopback200
 nameif VTI-LOOPBACK
 ip address 172.16.17.2 255.255.255.255

interface Tunnel2
 nameif SVTI-SPOKE-3
```

```
 ip unnumbered VTI-LOOPBACK
 tunnel source interface vlan2820
 tunnel destination 10.28.20.98
 tunnel mode ipsec ipv4
 tunnel protection ipsec profile VPN-LAB-PROFILE
```

Create a secondary Loopback interface to simulate traffic from LAN-REMOTE-1 network behind spoke.

```
interface Loopback100
 nameif LAN-REMOTE-1
 ip address 192.168.7.1 255.255.255.255
```

Configure tunnel-group.

> **Note**: The command route set interface sends the SVTI IP address as a static IP address to the peer.

```
tunnel-group 10.28.20.98 type ipsec-l2l
tunnel-group 10.28.20.98 ipsec-attributes
 ikev2 remote-authentication pre-shared-key *****
 ikev2 local-authentication pre-shared-key *****
 ikev2 route set interface
```

Enable IKEv2 on the interface that can build the tunnel.

```
crypto ikev2 enable vlan2820
```

Configure OSPF

Hub configuration

> **Note**: Redistribute connected subnets command is used to advertise OnPREM network to the spokes via OSPF. Redistribution can be different as per design.

```
router ospf 1
 router-id 172.16.17.1
 network 172.16.17.0 255.255.255.0 area 0
 log-adj-changes
 redistribute connected subnets
```

Spoke configuration

```
router ospf 1
 router-id 172.16.17.2
 network 172.16.17.0 255.255.255.0 area 0
 log-adj-changes
 redistribute connected subnets
```

Verify OSPF

Hub verification

```
ASAV2-hub# show ospf

 Routing Process "ospf 1" with ID 172.16.17.1
 Start time: 4d23h, Time elapsed: 3d04h
 Supports only single TOS(TOS0) routes
 Supports opaque LSA
 Supports Link-local Signaling (LLS)
 Supports area transit capability
 Event-log enabled, Maximum number of events: 1000, Mode: cyclic
 It is an autonomous system boundary router
 Redistributing External Routes from,
    connected, includes subnets in redistribution
 Router is not originating router-LSAs with maximum metric
 Initial SPF schedule delay 5000 msecs
 Minimum hold time between two consecutive SPFs 10000 msecs
 Maximum wait time between two consecutive SPFs 10000 msecs
 Incremental-SPF disabled
 Minimum LSA interval 5 secs
 Minimum LSA arrival 1000 msecs
 LSA group pacing timer 240 secs
 Interface flood pacing timer 33 msecs
 Retransmission pacing timer 66 msecs
 Number of external LSA 5. Checksum Sum 0x39716
 Number of opaque AS LSA 0. Checksum Sum 0x0
 Number of DCbitless external and opaque AS LSA 0
 Number of DoNotAge external and opaque AS LSA 0
 Number of areas in this router is 1. 1 normal 0 stub 0 nssa
 Number of areas transit capable is 0
 External flood list length 0
 IETF NSF helper support enabled
 Cisco NSF helper support enabled
 Reference bandwidth unit is 100 mbps
    Area BACKBONE(0)
        Number of interfaces in this area is 3 (1 loopback)
        Area has no authentication
        SPF algorithm last executed 2d04h ago
        SPF algorithm executed 10 times
        Area ranges are
        Number of LSA 2. Checksum Sum 0x1c99f
        Number of opaque link LSA 0. Checksum Sum 0x0
        Number of DCbitless LSA 0
        Number of indication LSA 0
        Number of DoNotAge LSA 0
        Flood list length 0

ASAV2-hub# show ospf neighbor
```

```
Neighbor ID     Pri   State           Dead Time   Address         Interface
172.16.17.2       0   FULL/  -        0:00:39     172.16.17.2     DVTI-HUB_va11
```

Routing table on hub now shows LAN-REMOTE-1 network via OSPF.

```
ASAV2-hub# show route ospf

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, V - VPN
       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
       o - ODR, P - periodic downloaded static route, + - replicated route
       SI - Static InterVRF, BI - BGP InterVRF
Gateway of last resort is 10.28.20.101 to network 0.0.0.0

O E2     192.168.7.0 255.255.255.255
           [110/20] via 172.16.17.2, 2d04h, DVTI-HUB_va11
```

Spoke verification

```
ASAv-spoke-2# show ospf

 Routing Process "ospf 1" with ID 172.16.17.2
 Start time: 3w3d, Time elapsed: 3d04h
 Supports only single TOS(TOS0) routes
 Supports opaque LSA
 Supports Link-local Signaling (LLS)
 Supports area transit capability
 Event-log enabled, Maximum number of events: 1000, Mode: cyclic
 It is an autonomous system boundary router
 Redistributing External Routes from,
    connected, includes subnets in redistribution
 Router is not originating router-LSAs with maximum metric
 Initial SPF schedule delay 5000 msecs
 Minimum hold time between two consecutive SPFs 10000 msecs
 Maximum wait time between two consecutive SPFs 10000 msecs
 Incremental-SPF disabled
 Minimum LSA interval 5 secs
 Minimum LSA arrival 1000 msecs
 LSA group pacing timer 240 secs
 Interface flood pacing timer 33 msecs
 Retransmission pacing timer 66 msecs
 Number of external LSA 4. Checksum Sum 0x37bc8
 Number of opaque AS LSA 0. Checksum Sum 0x0
 Number of DCbitless external and opaque AS LSA 0
 Number of DoNotAge external and opaque AS LSA 0
 Number of areas in this router is 1. 1 normal 0 stub 0 nssa
 Number of areas transit capable is 0
 External flood list length 0
 IETF NSF helper support enabled
 Cisco NSF helper support enabled
 Reference bandwidth unit is 100 mbps
```

```
    Area BACKBONE(0)
        Number of interfaces in this area is 2 (1 loopback)
        Area has no authentication
        SPF algorithm last executed 2d04h ago
        SPF algorithm executed 1 times
        Area ranges are
        Number of LSA 2. Checksum Sum 0x1fe9a
        Number of opaque link LSA 0. Checksum Sum 0x0
        Number of DCbitless LSA 0
        Number of indication LSA 0
        Number of DoNotAge LSA 0
        Flood list length 0

ASAv-spoke-2#  show ospf neighbor
Neighbor ID     Pri   State           Dead Time   Address         Interface
172.16.17.1       0   FULL/  -        0:00:34     172.16.17.1     SVTI-SPOKE-3
```

Routing table on spoke now shows OnPREM network via OSPF.

```
ASAv-spoke-2# show route ospf

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, V - VPN
       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
       o - ODR, P - periodic downloaded static route, + - replicated route
       SI - Static InterVRF, BI - BGP InterVRF
Gateway of last resort is 10.28.20.101 to network 0.0.0.0

O E2     192.168.9.1 255.255.255.255
           [110/20] via 172.16.17.1, 2d04h, SVTI-SPOKE-3
```

Now spoke LAN-REMOTE-1 is able to reach OnPREM.

```
ASAv-spoke-2# ping LAN-REMOTE-1 192.168.9.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.9.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/10 ms

ASAv-spoke-2# show crypto ipsec sa peer  10.28.20.98 | i cap|iden|spi
      local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
      remote ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
      #pkts encaps: 9, #pkts encrypt: 9, #pkts digest: 9
      #pkts decaps: 9, #pkts decrypt: 9, #pkts verify: 9
      #PMTUs sent: 0, #PMTUs rcvd: 0, #decapsulated frgs needing reassembly: 0
      current outbound spi: 4BC1FF2C
      current inbound spi : FB455CB8
      spi: 0xFB455CB8 (4215626936)
      spi: 0x4BC1FF2C (1271004972)
```

Now hub OnPREM is able to reach LAN-REMOTE-1.

```
ASAV2-hub# ping ON-PREM  192.168.7.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.7.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/10 ms

ASAV2-hub# show crypto ipsec sa peer 10.28.20.100
peer address: 10.28.20.100
interface: DVTI-HUB_va12
    Crypto map tag: DVTI-HUB_vtemplate_dyn_map, seq num: 1, local addr: 10.28.20.98

      Protected vrf (ivrf): Global
      local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
      remote ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
      current_peer: 10.28.20.100


      #pkts encaps: 15, #pkts encrypt: 15, #pkts digest: 15
      #pkts decaps: 15, #pkts decrypt: 15, #pkts verify: 15
      #pkts compressed: 0, #pkts decompressed: 0
      #pkts not compressed: 15, #pkts comp failed: 0, #pkts decomp failed: 0
      #pre-frag successes: 0, #pre-frag failures: 0, #fragments created: 0
      #PMTUs sent: 0, #PMTUs rcvd: 0, #decapsulated frgs needing reassembly: 0
      #TFC rcvd: 0, #TFC sent: 0
      #Valid ICMP Errors rcvd: 0, #Invalid ICMP Errors rcvd: 0
      #send errors: 0, #recv errors: 0

      local crypto endpt.: 10.28.20.98/500, remote crypto endpt.: 10.28.20.100/500
      path mtu 1500, ipsec overhead 94(44), media mtu 1500
      PMTU time remaining (sec): 0, DF policy: copy-df
      ICMP error validation: disabled, TFC packets: disabled
```

Configure EIGRP

Hub configuration:

```
ASAV2-hub# sh run router
router eigrp 10
 network 172.16.17.0 255.255.255.0
 redistribute connected
```

Spoke configuration:

```
ASAv-spoke-2# sh run router
router eigrp 10
 network 172.16.17.0 255.255.255.0
 redistribute connected
```

Now spoke LAN-REMOTE-1 is able to reach OnPREM.

```
ASAv-spoke-2# ping LAN-REMOTE-1 192.168.9.1 rep 100
Type escape sequence to abort.
Sending 100, 100-byte ICMP Echos to 192.168.9.1, timeout is 2 seconds:
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!
Success rate is 100 percent (100/100), round-trip min/avg/max = 1/2/10 ms

ASAv-spoke-2# show crypto ipsec sa peer 10.28.20.98  | i cap|iden|spi
      local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
      remote ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
      #pkts encaps: 102, #pkts encrypt: 102, #pkts digest: 102
      #pkts decaps: 102, #pkts decrypt: 102, #pkts verify: 102
      #PMTUs sent: 0, #PMTUs rcvd: 0, #decapsulated frgs needing reassembly: 0
      current outbound spi: 3EED404C
      current inbound spi : 646D2C0C
      spi: 0x646D2C0C (1684876300)
      spi: 0x3EED404C (1055735884)
```

Now hub OnPREM is able to reach LAN-REMOTE-1.

```
ASAV2-hub# ping ON-PREM 192.168.7.1 rep 100
Type escape sequence to abort.
Sending 100, 100-byte ICMP Echos to 192.168.7.1, timeout is 2 seconds:
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!
Success rate is 100 percent (100/100), round-trip min/avg/max = 1/1/10 ms

ASAV2-hub# show crypto ipsec sa peer 10.28.20.100 | i cap|iden|spi
      local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
      remote ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
      #pkts encaps: 208, #pkts encrypt: 208, #pkts digest: 208
      #pkts decaps: 208, #pkts decrypt: 208, #pkts verify: 208
      #PMTUs sent: 0, #PMTUs rcvd: 0, #decapsulated frgs needing reassembly: 0
      current outbound spi: 646D2C0C
      current inbound spi : 3EED404C
      spi: 0x3EED404C (1055735884)
      spi: 0x646D2C0C (1684876300)
```

Verify EIGRP

Hub verification:

```
ASAV2-hub# show eigrp neighbors
EIGRP-IPv4 Neighbors for AS(10)
H   Address                 Interface       Hold Uptime   SRTT   RTO   Q  Seq
                                            (sec)         (ms)        Cnt Num
0   172.16.17.2             DVTI-HUB_va12    12  00:02:01 8      200  0     4
```

Routing table on hub now shows LAN-REMOTE-1 network via EIGRP.

```
ASAV2-hub# show route eigrp

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, V - VPN
       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
       o - ODR, P - periodic downloaded static route, + - replicated route
       SI - Static InterVRF, BI - BGP InterVRF
Gateway of last resort is 10.28.20.101 to network 0.0.0.0

D EX     192.168.7.1 255.255.255.255
           [170/53760] via 172.16.17.2, 00:05:28, DVTI-HUB_va12
```

Spoke verification:

```
ASAv-spoke-2# show eigrp neighbors
EIGRP-IPv4 Neighbors for AS(10)
H   Address                 Interface       Hold Uptime   SRTT   RTO   Q  Seq
                                            (sec)         (ms)        Cnt Num
0   172.16.17.1             SVTI-SPOKE-3     12  00:07:05 34     204  0     3
```

Routing table on spoke now shows OnPREM network via EIGRP.

```
ASAv-spoke-2# show route eigrp

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, V - VPN
       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
       o - ODR, P - periodic downloaded static route, + - replicated route
       SI - Static InterVRF, BI - BGP InterVRF
Gateway of last resort is 10.28.20.101 to network 0.0.0.0

D EX     192.168.9.1 255.255.255.255
           [170/53760] via 172.16.17.1, 00:07:43, SVTI-SPOKE-3
```

Configure BGP

> **Note**: When static or dynamic VTI interfaces are combined with eBGP, ensure that the value of the TTL hop is more than one if you use BGP.

Hub configuration:

```
router bgp 100
 bgp log-neighbor-changes
 bgp bestpath compare-routerid
 address-family ipv4 unicast
  neighbor 172.16.17.2 remote-as 200
  neighbor 172.16.17.2 ebgp-multihop 10
  neighbor 172.16.17.2 activate
  redistribute connected
  no auto-summary
  no synchronization
 exit-address-family
```

Spoke configuration

```
router bgp 200
 bgp log-neighbor-changes
 bgp bestpath compare-routerid
 address-family ipv4 unicast
  neighbor 172.16.17.1 remote-as 100
  neighbor 172.16.17.1 ebgp-multihop 10
  neighbor 172.16.17.1 activate
  redistribute connected
  no auto-summary
  no synchronization
 exit-address-family
```

Verify BGP

Hub verification:

```
ASAV2-hub# show bgp neighbors

BGP neighbor is 172.16.17.2,  context single_vf,  remote AS 200, external link
  BGP version 4, remote router ID 192.168.7.1
  BGP state = Established, up for 00:05:28
  Last read 00:00:01, last write 00:01:00, hold time is 180, keepalive interval is 60 seconds
  Neighbor sessions:
    1 active, is not multisession capable (disabled)
  Neighbor capabilities:
    Route refresh: advertised and received(new)
    Four-octets ASN Capability: advertised and received
    Address family IPv4 Unicast: advertised and received
    Multisession Capability:
  Message statistics:
    InQ depth is 0
    OutQ depth is 0

                   Sent       Rcvd
    Opens:         1          1
```

```
    Notifications: 0          0
    Updates:       2          2
    Keepalives:    6          6
    Route Refresh: 0          0
    Total:         9          9
  Default minimum time between advertisement runs is 30 seconds

 For address family: IPv4 Unicast
  Session: 172.16.17.2
  BGP table version 7, neighbor version 7/0
  Output queue size : 0
  Index 1
  1 update-group member
                            Sent       Rcvd
  Prefix activity:          ----       ----
    Prefixes Current:       3          3          (Consumes 240 bytes)
    Prefixes Total:         3          3
    Implicit Withdraw:      0          0
    Explicit Withdraw:      0          0
    Used as bestpath:       n/a        2
    Used as multipath:      n/a        0

                                  Outbound    Inbound
  Local Policy Denied Prefixes: --------    -------
    Bestpath from this peer:     2          n/a
    Total:                       2          0
  Number of NLRIs in the update sent: max 3, min 0

  Address tracking is enabled, the RIB does have a route to 172.16.17.2
  Connections established 1; dropped 0
  Last reset never
  External BGP neighbor may be up to 10 hops away.
  Transport(tcp) path-mtu-discovery is enabled
  Graceful-Restart is disabled

ASAV2-hub#
ASAV2-hub#  sh run router
router bgp 100
 bgp log-neighbor-changes
 bgp bestpath compare-routerid
 address-family ipv4 unicast
  neighbor 172.16.17.2 remote-as 200
  neighbor 172.16.17.2 ebgp-multihop 10
  neighbor 172.16.17.2 activate
  redistribute connected
  no auto-summary
  no synchronization
 exit-address-family
!
ASAV2-hub# sh run all router
router bgp 100
 bgp log-neighbor-changes
 no bgp always-compare-med
 no bgp asnotation dot
 no bgp bestpath med
 bgp bestpath compare-routerid
 bgp default local-preference 100
 no bgp deterministic-med
 bgp enforce-first-as
 bgp maxas-limit 0
 bgp transport path-mtu-discovery
 timers bgp 60 180 0
```

```
 address-family ipv4 unicast
  bgp scan-time 60
  bgp nexthop trigger enable
  bgp nexthop trigger delay 5
  bgp aggregate-timer 30
  neighbor 172.16.17.2 remote-as 200
  neighbor 172.16.17.2 ebgp-multihop 10
  neighbor 172.16.17.2 activate
  no bgp redistribute-internal
  no bgp soft-reconfig-backup
  no bgp suppress-inactive
  redistribute connected
  distance bgp 20 200 200
  no auto-summary
  no synchronization
 exit-address-family
!
```

Routing table on hub now shows LAN-REMOTE-1 network via BGP.

```
ASAV2-hub# show route bgp

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, V - VPN
       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
       o - ODR, P - periodic downloaded static route, + - replicated route
       SI - Static InterVRF, BI - BGP InterVRF
Gateway of last resort is 10.28.20.101 to network 0.0.0.0

B        192.168.7.1 255.255.255.255 [20/0] via 172.16.17.2, 00:06:16
```

Spoke verification:

```
ASAv-spoke-2# show bgp neighbors

BGP neighbor is 172.16.17.1,  context single_vf,  remote AS 100, external link
  BGP version 4, remote router ID 192.168.9.1
  BGP state = Established, up for 00:06:59
  Last read 00:00:27, last write 00:00:20, hold time is 180, keepalive interval is 60 seconds
  Neighbor sessions:
    1 active, is not multisession capable (disabled)
  Neighbor capabilities:
    Route refresh: advertised and received(new)
    Four-octets ASN Capability: advertised and received
    Address family IPv4 Unicast: advertised and received
    Multisession Capability:
  Message statistics:
    InQ depth is 0
    OutQ depth is 0

                    Sent       Rcvd
```

```
    Opens:         1          1
    Notifications: 0          0
    Updates:       2          2
    Keepalives:    7          8
    Route Refresh: 0          0
    Total:         10         11
  Default minimum time between advertisement runs is 30 seconds

 For address family: IPv4 Unicast
  Session: 172.16.17.1
  BGP table version 9, neighbor version 9/0
  Output queue size : 0
  Index 1
  1 update-group member
                            Sent       Rcvd
  Prefix activity:          ----       ----
    Prefixes Current:       3          3          (Consumes 240 bytes)
    Prefixes Total:         3          3
    Implicit Withdraw:      0          0
    Explicit Withdraw:      0          0
    Used as bestpath:       n/a        2
    Used as multipath:      n/a        0

                                  Outbound    Inbound
  Local Policy Denied Prefixes: --------    -------
    Bestpath from this peer:     3          n/a
    Total:                       3          0
  Number of NLRIs in the update sent: max 3, min 0

  Address tracking is enabled, the RIB does have a route to 172.16.17.1
  Connections established 1; dropped 0
  Last reset never
  External BGP neighbor may be up to 10 hops away.
  Transport(tcp) path-mtu-discovery is enabled
  Graceful-Restart is disabled
```

Routing table on spoke now shows OnPREM network via BGP.

```
ASAv-spoke-2#   show route bgp

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, V - VPN
       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
       o - ODR, P - periodic downloaded static route, + - replicated route
       SI - Static InterVRF, BI - BGP InterVRF
Gateway of last resort is 10.28.20.101 to network 0.0.0.0

B        192.168.9.1 255.255.255.255 [20/0] via 172.16.17.1, 00:09:22
```

Troubleshoot

To troubleshoot OSPF, use these debugs and show commands:

```
debug ip ospf
debug ip ospf packet
debug ip ospf events
debug ip ospf hello
debug ip ospf adj

show ospf
show ospf neighbor
show ospf interface
```

To troubleshoot EIGRP, use these debugs and show commands:

```
debug ip eigrp
debug ip eigrp neighbor
debug ip eigrp notifications

show eigrp
show eigrp <AS>
show eigrp interfaces
show eigrp neighbors
show eigrp topology
```

To troubleshoot BGP, use these debugs and show commands:.

```
debug ip bgp all
debug ip bgp updates
debug ip bgp events

show bgp
show bgp summary
show bgp neighbors
```

To troubleshoot IKEv2, use these debugs and show commands:

```
debug crypto ikev2 protocol 255
debug crypto ikev2 platform 255
debug crypto ipsec 255
```

Related Information

- **Cisco Technical Support & Downloads**