Multi-Chassis IPSec Redundancy

In This Chapter

This section provides information about multi-chassis IPSec redundancy configurations.

Topics in this section include:

Applicability

This feature is applicable to 7750 SR-7/12/12e with IOM3-XP or IMMs and chassis mode D and the 7450 ESS-6/7/12 with IOM3-XP or IMM in mixed mode.

The configuration was tested on release 12.0.R1.

Overview

Multi-Chassis IPSec redundancy (MC-IPSec) is a stateful inter-chassis IPSec failover mechanism. IPSec tunnel states are synchronized between the master and standby chassis. A tunnel-group failure on the master or a master chassis failure could trigger MC-IPSec failover to the standby chassis.

The following are some highlights of this feature:

- IKEv2 only
- Multi-active tunnel-group only
- The granularity of failover is tunnel-group, which means a specific tunnel-group could failover to the standby chassis independent of other tunnel-groups on the master chassis
- Supports both static and dynamic LAN-to-LAN tunnel

This feature has the following building blocks:

- Master election
  - → MIMP (MC-IPSec Mastership Protocol) runs between chassis to elect master, MIMP run for each tunnel-group independently
- Synchronization
  - → MCS (Multi-Chassis Synchronization) syncs IPSec states between chassis
- Routing
  - → MC-IPSec-aware routing attracts traffic to the master chassis
  - → Shunting support
  - → MC-IPSec aware VRRP

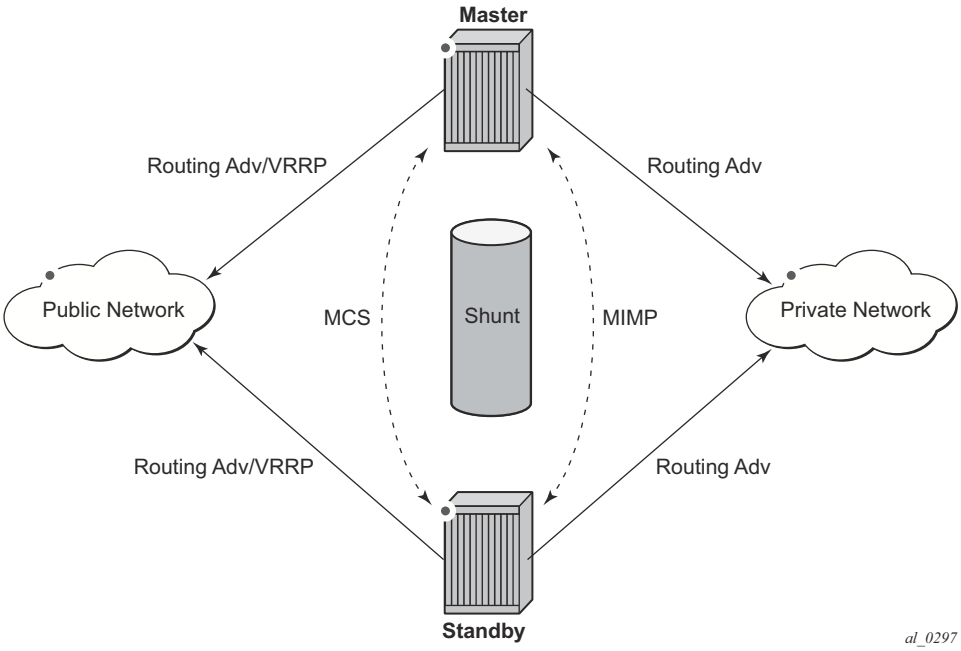

Figure 238: MC-IPSec Architecture

The fundamentals of MC-IPSec are:

- Only the master processes ESP and IKE traffic. If the standby receives traffic, it could shunt it to the master if possible. The traffic will be discarded if the standby fails to shunt the traffic.
- Same local gateway address should be provisioned on both chassis.
- MC-IPSec does not synchronize configurations.
- MC-IPSec aware routing attracts traffic to the master in both public and private service. This is achieved by exporting the corresponding IPSec routes to the routing protocol via a route policy and setting a different routing metric according to the MC-IPSec state.
- In case of a Layer 2 public network, MC-IPSec aware VRRP could be used to trigger VRRP switchover upon MC-IPSec switchover.
- MCS syncs IPSec states between chassis so that existing IPSec tunnels do not need to be re-established upon switchover.
- MIMP elects mastership between two chassis, and it could also detect chassis failure and tunnel-group failure; a central BFD session could be bound to the MIMP to achieve fast chassis failure detection.

Configuration

The test topology is shown in Figure 239.

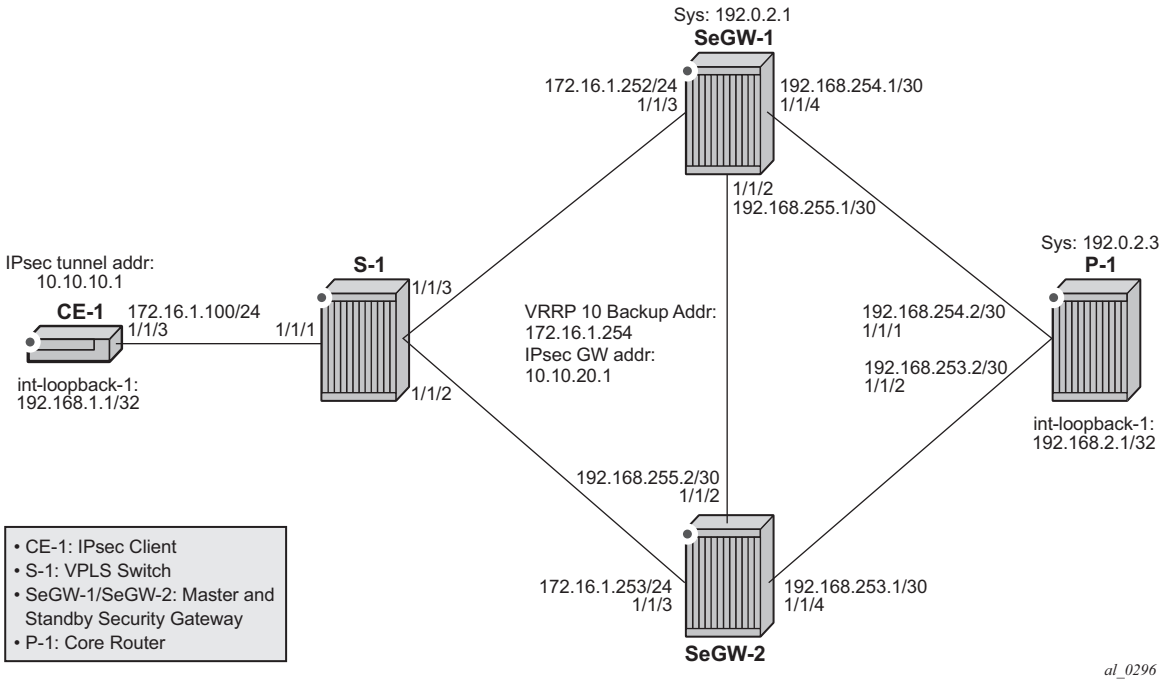

Figure 239: Test Topology

Test setup:

- An IPSec tunnel is initiated by CE-1 and terminated on the master of SeGW-1/SeGW-2.
- IES 1 and VPRN 2 are the public and private services, respectively, on SeGW-1/SeGW-2/CE-1.
- VPRN 2 is also configured on P-1.
- Static LAN-to-LAN tunnel with pre-shared key.
- Local VPLS service 100 on S-1 to simulate a layer2 switch.
- VRRP 10 between SeGW-1 and SeGW-2 to provide a backup address 192.168.1.254, which is also the default next-hop for CE-1.
- VRRP policy 1 is bound to VRRP 10 to change the in-use priority upon MC-IPSec switchover.
- OSPF is the IGP running in the base routing instance between SeGW-1, SeGW-2 and P-1.

- MP-BGP is running between SeGW-1, SeGW-2 and P-1 for exchanging VPRN 2's routes.

- A ping between loopback interface address: 192.168.1.1 on CE-1 and 192.168.2.1 on P-1 in VPRN 2 is used to verify the connectivity over the IPSec tunnel.

The MC-IPSec configuration commands are shown below.

```
config>redundancy>multi-chassis>
     peer <ip-address> [create]
          sync
               ipsec
               tunnel-group <tunnel-group-id> sync-tag <tag-name> [create]
          mc-ipsec
               bfd-enable
               discovery-interval <interval-1> [boot <interval-2>]
               hold-on-neighbor-failure <multiplier>
               keep-alive-interval <interval>
               tunnel-group <tunnel-group-id> [create]
                    peer-group <tunnel-group-id>
                    priority <priority>
                    shutdown

config>router>policy-options>policy-statement>entry>from>
     state ipsec-master-with-peer|ipsec-non-master|ipsec-master-without-peer
     protocol ipsec

config>service>ies>if>
config>service>vprn>if>
     static-tunnel-redundant-next-hop <ip-address>
     dynamic-tunnel-redundant-next-hop <ip-address>

config>isa>tunnel-grp>
     ipsec-responder-only

config>vrrp>policy>priority-event>
     mc-ipsec-non-forwarding <tunnel-grp-id>
          hold-clear <seconds>
          hold-set <seconds>
          priority <priority-level> explicit
```

Parameters:

- **peer** <*ip-address*> [**create**] — This command creates or enters a multi-chassis peer. The peer's address by default is the peer's system address. This can be changed on the peer using the **config>redundancy>multi-chassis>peer>source-address** command.
- **sync**>**ipsec** — This command enables MCS to synchronize IPSec states.
- **tunnel-group** <*tunnel-group-id*> **sync-tag** <*tag-name*> [**create**] — This command enables MCS to synchronize the IPSec states of the specified tunnel-group.The **sync-tag** parameter is used to match peer's tunnel-group. The tunnel-group states with same sync-tag on both chassis will be synced.
- **mc-ipsec** — This command enters the multi-chassis IPSec configuration context.

- **bfd-enable** — This command enables tracking a central BFD session, if the BFD session goes down, then the system considers the peer is down and changes the mc-ipsec status of the configured tunnel-group accordingly.

  The BFD session uses the source address of MCS as its source address and the MCS peer address as the destination address. Other BFD parameters are configured with the **bfd** command on the interface that the MCS source address resides on.

  Configuration of this command is optional.

- **discovery-interval** <*interval-1*> [**boot** <*interval-2*>] — This command specifies the time interval that the tunnel-group stays in "Discovery" state. Interval-1 is used as discovery-interval when a new tunnel-group is added to multi-chassis redundancy (mp-ipsec); interval-2 is used as discovery-interval after system boot-up, it is optional, and when it is not specified, interval-1's value will be used. Both intervals have a default value of 300 seconds.
- **hold-on-neighbor-failure** <*multiplier*> — This command specifies the number of keep-alive failures before considering the peer to be down. Default is 3.
- **keep-alive-interval** <*interval*> — This command specifies the time interval of the mastership election protocol keep-alive packets. Default value is 1 seconds, range: 0.5 ~ 50 seconds.
- **tunnel-group** <*tunnel-group-id*> [**create**] — This command enables multi-chassis redundancy for the specified tunnel-group, or enters an already configured tunnel-group context. The configured tunnel-groups could failover independently.
- **peer-group** <*tunnel-group-id*> — This command specifies the corresponding tunnel-group id on the peer node. The peer tunnel-group id is not necessary equal to local tunnel-group id.
- **priority** <*priority*> — This command specifies the local priority of the tunnel-group, this is used to elect a master, where the higher number wins. If the priorities are the same, then the peer which has more active ISAs wins; if priority and the number of active ISAs are same, then the peer with higher IP address wins. Default value is 100, range: 0..255
- **shutdown** — This command disables the multi-chassis redundancy for the specified tunnel-group
- **state ipsec-master-with-peer**|**ipsec-non-master**|**ipsec-master-without-peer** — These commands specify the mc-ipsec state in a "from" statement of a route policy entry.
  ipsec-master-with-peer: The corresponding tunnel-group is Master with peer reachable.
  ipsec-master-without-peer: The corresponding tunnel-group is Master with peer unreachable.
  ipsec-non-master: The corresponding tunnel-group is **not** Master.
- **protocol ipsec** — This command specifies the IPSec as protocol in a "from" statement of a route policy entry. **protocol ipsec** means the /32 local gateway routes (of both static and dynamic tunnels) and reverse route of dynamic tunnel.
- **static-tunnel-redundant-next-hop** <*ip-address*>
  dynamic-tunnel-redundant-next-hop <*ip-address*> — This command specifies the

redundant next-hop address on a public or private IPSec interface (with public or private tunnel-sap) for a static/dynamic IPSec tunnel. The specified next-hop address will be used by the standby node to shunt traffic to the master in case it receives any traffic.

The next-hop address will be resolved in the routing table of the corresponding service.

Notes:

→ Shunting is supported over:
  – Directly connected SAP
  – Spoke SDP terminated IP interface

→ Shunting over auto-bind tunnel is not supported.

→ Shunting will not work if the tunnel-group is down.

- **ipsec-responder-only** — With this command configured, the system will only act as IKE responder except for the automatic CHILD_SA rekey upon MC-IPSec switchover.

  This command is required for MC-IPSec support of static LAN-to-LAN tunnel

- **mc-ipsec-non-forwarding** <*tunnel-grp-id*> — This command creates a new VRRP policy priority event: **mc-ipsec-non-forwarding**. It will be triggered whenever the specified tunnel-group enters non-forwarding state.
- **hold-clear** <*seconds*> — This command configures hold time before clearing the event. Default value is 0 seconds. Range: 0..86400 seconds
- **hold-set** <*seconds*> — This command configures hold time before setting the event. Default value is 0 seconds. Range: 0..86400 seconds
- **priority** <*priority-level*> **explicit** — This command sets the VRRP in-use priority to the configured value upon the event. Default value is 0, range: 0..254

Before starting

- The system time of SeGW-1 and SeGW-2 must be the same. Otherwise, this feature will not work. Using a time sync protocol like NTP/SNTP is the recommended method.
- SeGW-1 and SeGW-2 must be IP reachable in the base routing instance because both MCS and MIMP run in the base routing instance.

Step 0: Configure CE-1.

- IES 1 and VPRN 2 are the public and private service.
- A static default route points to the VRRP backup address 172.16.1.254.
- Static IPSec tunnel “tunnel-1” with local address 10.10.10.1 and remote address 10.10.20.1.
- A loopback interface in VPRN 2 with address 192.168.1.1/32, which is used as source address for the ping traffic in later step.
  → The ping traffic is used to test the connectivity between CE-1 and P-1 over IPSec tunnel “tunnel-1”.

```
#--------------------------------------------------
echo "Router (Network Side) Configuration"
#--------------------------------------------------
    router
        interface "int-CE1-S1"
            address 172.16.1.100/24
            port 1/1/3
            no shutdown
        exit
        interface "system"
            no shutdown
        exit
        autonomous-system 64496
#--------------------------------------------------
echo "Static Route Configuration"
#--------------------------------------------------
        static-route 0.0.0.0/0 next-hop 172.16.1.254
#--------------------------------------------------
echo "IPsec Configuration"
#--------------------------------------------------
    ipsec
        ike-policy 1 create
            ike-version 2
            dpd
        exit
        ipsec-transform 1 create
        exit
    exit
#--------------------------------------------------
echo "Service Configuration"
#--------------------------------------------------
```

```
    service
        ies 1 customer 1 create
            interface "int-IPsec-Public-1" create
                address 10.10.10.254/24
                tos-marking-state untrusted
                sap tunnel-1.public:1 create
                exit
            exit
            no shutdown
        exit
        vprn 2 customer 1 create
            ipsec
                security-policy 1 create
                    entry 10 create
                        local-ip 192.168.1.1/32
                        remote-ip 192.168.2.1/32
                    exit
                exit
            exit
            route-distinguisher 64496:2
            interface "int-loopback-1" create
                address 192.168.1.1/32
                loopback
            exit
            interface "int-IPsec-private-1" tunnel create
                sap tunnel-1.private:1 create
                    ipsec-tunnel "tunnel-1" create
                        security-policy 1
                        local-gateway-address 10.10.10.1 peer 10.10.20.1
                                                          delivery-service 1
                        dynamic-keying
                            ike-policy 1
                            pre-shared-key "ALU"
                            transform 1
                        exit
                        no shutdown
                    exit
                exit
            exit
            static-route 192.168.2.1/32 ipsec-tunnel "tunnel-1"
            no shutdown
        exit
exit
```

Step 1. Configure S-1.

- A local VPLS service 3 to simulate a layer2 switch between CE-1, SeGW-1 and SeGW-2.

```
    vpls 3 customer 1 create
        stp
            shutdown
        exit
        sap 1/1/1 create
        exit
        sap 1/1/2 create
        exit
        sap 1/1/3 create
```

```
            exit
            no shutdown
        exit
```

Step 2. Configure P-1

- P-1 simulates the core network router, which connects to both SeGW-1 and SeGW-2.
- A loopback interface with address 192.168.2.1/32 in VPRN 2 is the destination address of the ping traffic from CE-1.
- MP-BGP session between P-1 and SeGW-1/SeGW-2 to receive 192.168.1.1/32 route in VPRN 2.
- GRE spoke SDPs to connect to SeGW-1 and SeGW-2.

```
#--------------------------------------------------
echo "Router (Network Side) Configuration"
#--------------------------------------------------
    router
        interface "int-P1-SeGW1"
            address 192.168.254.2/30
            port 1/1/1
            no shutdown
        exit
        interface "int-P1-SeGW2"
            address 192.168.253.2/30
            port 1/1/2
            no shutdown
        exit
        interface "system"
            address 192.0.2.3/32
            no shutdown
        exit
        autonomous-system 64496
#--------------------------------------------------
echo "OSPFv2 Configuration"
#--------------------------------------------------
        ospf
            area 0.0.0.0
                interface "system"
                    no shutdown
                exit
                interface "int-P1-SeGW1"
                    no shutdown
                exit
                interface "int-P1-SeGW2"
                    no shutdown
                exit
            exit
        exit

#--------------------------------------------------
echo "Service Configuration"
#--------------------------------------------------
    service
        sdp 200 create
```

```
            far-end 192.0.2.1
            signaling off
            keep-alive
                shutdown
            exit
            no shutdown
        exits
        sdp 300 create
            far-end 192.0.2.2
            signaling off
            keep-alive
                shutdown
            exit
            no shutdown
        exit
        vprn 2 customer 1 create
            route-distinguisher 64496:2
            vrf-target target:64496:2
            interface "int-loopback-1" create
                address 192.168.2.1/32
                loopback
            exit
            spoke-sdp 200 create
                description "SDP to SeGW-1"
            exit
            spoke-sdp 300 create
                description "SDP to SeGW-2"
            exit
            no shutdown
        exit
    exit
#--------------------------------------------------
echo "BGP Configuration"
#--------------------------------------------------
        bgp
            group "MPBGP"
                family vpn-ipv4
                peer-as 64496
                neighbor 192.0.2.1
                exit
                neighbor 192.0.2.2
                exit
            exit
            no shutdown
        exit
    exit
```

Step 3. Configure IPSec tunnel on SeGW-1.

- The tunnel-group must be in multi-active mode before MC-IPSec can be enabled for it.
- Interface "int-Redundant-1" is a spoke-sdp terminated interface, which is used for shunting.
- SDP 100 and 200 are the GRE SDP towards SeGW-2 and P-1.
- IPSec tunnel “tunnel-1” is the tunnel to CE-1; both SeGW-1 and SeGW-2 use same local gateway address: 10.10.20.1.

```
#--------------------------------------------------
echo "ISA Configuration"
#--------------------------------------------------
    isa
        tunnel-group 1 create
            ipsec-responder-only
            multi-active
            mda 1/2
            no shutdown
        exit
exit
#--------------------------------------------------
echo "Router (Network Side) Configuration"
#--------------------------------------------------
    router
        interface "int-SeGW1-P1"
            address 192.168.254.1/30
            port 1/1/4
            no shutdown
        exit
        interface "int-SeGW1-SeGW2"
            address 192.168.255.1/30
            port 1/1/2
            no shutdown
        exit
        interface "system"
            address 192.0.2.1/32
            bfd 100 receive 100 multiplier 3
            no shutdown
        exit
        autonomous-system 64496
#--------------------------------------------------
echo "Static Route Configuration"
#--------------------------------------------------
        static-route 10.10.10.0/24 next-hop 172.16.1.100
#--------------------------------------------------
echo "OSPFv2 Configuration"
#--------------------------------------------------
        ospf
            area 0.0.0.0
                interface "system"
                    no shutdown
                exit
                interface "int-SeGW1-SeGW2"
                    no shutdown
                exit
```

```
                interface "int-SeGW1-P1"
                    no shutdown
                exit
            exit
        exit
#--------------------------------------------------
echo "IPsec Configuration"
#--------------------------------------------------
    ipsec
        ike-policy 1 create
            ike-version 2
            ipsec-lifetime 7200
            isakmp-lifetime 172800
        exit
        ipsec-transform 1 create
        exit
    exit
#--------------------------------------------------
echo "Service Configuration"
#--------------------------------------------------
    service
        sdp 100 create
            signaling off
            far-end 192.0.2.2
            keep-alive
                shutdown
            exit
            no shutdown
        exit
        sdp 200 create
            signaling off
            far-end 192.0.2.3
            keep-alive
                shutdown
            exit
            no shutdown
        exit
        ies 1 customer 1 create
            interface "int-SeGW1-S1" create
                address 172.16.1.252/24
                vrrp 10
                    backup 172.16.1.254
                    priority 200
                    policy 1
                    ping-reply
                exit
                sap 1/1/3 create
                exit
            exit
            interface "int-IPsec-Public-1" create
                address 10.10.20.254/24
                tos-marking-state untrusted
                sap tunnel-1.public:1 create
                exit
                static-tunnel-redundant-next-hop 192.168.255.2
            exit
            no shutdown
        exit
        vprn 2 customer 1 create
```

```
            ipsec
                security-policy 1 create
                    entry 10 create
                        local-ip 192.168.2.1/32
                        remote-ip 192.168.1.1/32
                    exit
                exit
            exit
            vrf-export "IPsec-to-MPBGP"
            route-distinguisher 64496:2
            vrf-target target:64496:2
            interface "int-IPsec-Private-1" tunnel create
                sap tunnel-1.private:1 create
                    ipsec-tunnel "tunnel-1" create
                        security-policy 1
                        local-gateway-address 10.10.20.1 peer 10.10.10.1
                                                          delivery-service 1
                        dynamic-keying
                            ike-policy 1
                            pre-shared-key "ALU"
                            transform 1
                        exit
                        no shutdown
                    exit
                exit
                static-tunnel-redundant-next-hop 192.168.20.2
            exit
            interface "int-Redundant-1" create
                address 192.168.20.1/30
                spoke-sdp 100:20 create
                    ingress
                        vc-label 2049
                    exit
                    egress
                        vc-label 2048
                    exit
                    no shutdown
                exit
            exit
            static-route 192.168.1.1/32 ipsec-tunnel "tunnel-1"
            spoke-sdp 100 create
                description "SDP to SeGW-2"
            exit
            spoke-sdp 200 create
                description "SDP to P-1"
            exit
            no shutdown
        exit
    exit
```

Step 4. Enable MC-IPSec for tunnel-group 1 on SeGW-1

- Create a multi-chassis peer for SeGW-2 by using SeGW-2's system address.
- Enable MCS for IPSec and tunnel-group 1.
- Enable MC-IPSec for tunnel-group with a configured priority 200.
- Bind a central BFD session to MC-IPSec from system interface.

```
*A:SeGW-1>config>redundancy# info
----------------------------------------------
        multi-chassis
            peer 192.0.2.2 create
                sync
                    ipsec
                    tunnel-group 1 sync-tag "tag-1" create
                    no shutdown
                exit
                mc-ipsec
                    bfd-enable
                    tunnel-group 1 create
                        peer-group 1
                        priority 200
                        no shutdown
                    exit
                exit
                no shutdown
            exit
        exit
----------------------------------------------
*A:SeGW-1>config>router# info
----------------------------------------------
        interface "system"
            address 192.0.2.1/32
            bfd 100 receive 100 multiplier 3
            no shutdown
        exit
```

Step 5. Configure MC-IPSec aware routing on SeGW-1.

- Export static route 192.168.1.1/32 in VPRN 2 to P-1 by using route-policy "IPsec-to-MPBGP".
- Set the local preference of the 192.168.1.1/32 according to the MC-IPSec state:

  → ipsec-master-with-peer: 200

  → ipsec-non-master:100

  → ipsec-master-without-peer: 200

  State “ipsec-master-without-peer” could be used to attract traffic to the designated master in case of “Dual Master” (meaning two chassis lose the MIMP connection in base routing instance). In this example, SeGW-1 has local preference 200 and SeGW-2 has local preference 100 for ipsec-master-without-peer.
- Apply the policy “IPsec-to-MPBGP” in VPRN 2.

```
#--------------------------------------------------
echo "Policy Configuration"
#--------------------------------------------------
        policy-options
            begin
            prefix-list "CE1-Internal"
                prefix 192.168.1.1/32 exact
            exit
            community "vprn2" members "target:64496:2"
            policy-statement "IPsec-to-MPBGP"
                entry 10
                    from
                        prefix-list "CE1-Internal"
                        state ipsec-master-with-peer
                    exit
                    action accept
                        community add "vprn2"
                        local-preference 200
                    exit
                exit
                entry 20
                    from
                        prefix-list "CE1-Internal"
                        state ipsec-non-master
                    exit
                    action accept
                        community add "vprn2"
                        local-preference 100
                    exit
                exit
                entry 30
                    from
                        prefix-list "CE1-Internal"
                        state ipsec-master-without-peer
                    exit
                    action accept
                        community add "vprn2"
                        local-preference 200
```

```
                    exit
                exit
                default-action accept
                    community add "vprn2"
                exit
            exit
            commit
        exit
#--------------------------------------------------
echo "BGP Configuration"
#--------------------------------------------------
        bgp
            group "MPBGP"
                family vpn-ipv4
                peer-as 64496
                neighbor 192.0.2.2
                exit
                neighbor 192.0.2.3
                exit
            exit
            no shutdown
        exit
exit
-------------------------------------------
A:SeGW-1>config>service>
        vprn 2 customer 1 create
            vrf-export "IPsec-to-MPBGP"
            …
```

Step 6. Configure MC-IPSec-aware VRRP on SeGW-1.

- VRRP instance needs to be in preempt mode.
- Use “mc-ipsec-non-forwarding” priority event to lower the in-use VRRP priority upon MC-IPSec switchover, which makes sure VRRP and MC-IPSec have the same master.
- Apply the vrrp-policy on interface "int-SeGW1-S1" of IES 1.
  → This only needs to be configured on the designated VRRP master, in this case, SeGW-1.

```
*A:SeGW-1>config>vrrp# info
----------------------------------------------
        policy 1
            priority-event
                mc-ipsec-non-forwarding 1
                    priority 50 explicit
                exit
            exit
        exit
----------------------------------------------
*A:SeGW-1>config>service>ies# info
----------------------------------------------
            interface "int-SeGW1-S1" create
                address 172.16.1.252/24
                vrrp 10
                    backup 172.16.1.254
                    priority 200
                    policy 1
                    ping-reply
                exit
                sap 1/1/3 create
                exit
            exit
```

Step 7. Repeat Step 3 to Step 5 on SeGW-2.

```
#--------------------------------------------------
echo "ISA Configuration"
#--------------------------------------------------
    isa
        tunnel-group 1 create
            ipsec-responder-only
            multi-active
            mda 1/2
            no shutdown
        exit
    exit
#--------------------------------------------------
echo "Redundancy Configuration"
#--------------------------------------------------
    redundancy
        multi-chassis
            peer 192.0.2.1 create
                sync
                    ipsec
                    tunnel-group 1 sync-tag "tag-1" create
                    no shutdown
                exit
                mc-ipsec
                    bfd-enable
                    tunnel-group 1 create
                        peer-group 1
                        priority 150
                        no shutdown
                    exit
                exit
                no shutdown
            exit
        exit
    exit

#--------------------------------------------------
echo "Router (Network Side) Configuration"
#--------------------------------------------------
    router
        interface "int-SeGW2-P1"
            address 192.168.253.1/30
            port 1/1/4
            no shutdown
        exit
        interface "int-SeGW2-SeGW1"
            address 192.168.255.2/30
            port 1/1/2
            no shutdown
        exit
        interface "system"
            address 192.0.2.2/32
            bfd 100 receive 100 multiplier 3
            no shutdown
        exit
        autonomous-system 64496
#--------------------------------------------------
```

```
echo "Static Route Configuration"
#------------------------------------------------
        static-route 10.10.10.0/24 next-hop 172.16.1.100
#------------------------------------------------
echo "OSPFv2 Configuration"
#------------------------------------------------
        ospf
            area 0.0.0.0
                interface "system"
                    no shutdown
                exit
                interface "int-SeGW2-SeGW1"
                    no shutdown
                exit
                interface "int-SeGW2-P1"
                    no shutdown
                exit
            exit
        exit

#------------------------------------------------
echo "IPsec Configuration"
#------------------------------------------------
    ipsec
        ike-policy 1 create
            ike-version 2
            ipsec-lifetime 7200
            isakmp-lifetime 172800
        exit
        ipsec-transform 1 create
        exit
    exit
#------------------------------------------------
echo "Service Configuration"
#------------------------------------------------
    service
        sdp 100 create
            far-end 192.0.2.1
            signaling off
            keep-alive
                shutdown
            exit
            no shutdown
        exit
        sdp 300 create
            far-end 192.0.2.3
            signaling off
            keep-alive
                shutdown
            exit
            no shutdown
        exit
        ies 1 customer 1 create
            interface "int-SeGW2-S1" create
                address 172.16.1.253/24
                vrrp 10
                    backup 172.16.1.254
                    ping-reply
                exit
```

```
            sap 1/1/3 create
            exit
        exit
        interface "int-IPsec-Public-1" create
            address 10.10.20.254/24
            tos-marking-state untrusted
            sap tunnel-1.public:1 create
            exit
            static-tunnel-redundant-next-hop 192.168.255.1
        exit
        no shutdown
    exit
    vprn 2 customer 1 create
        ipsec
            security-policy 1 create
                entry 10 create
                    local-ip 192.168.2.1/32
                    remote-ip 192.168.1.1/32
                exit
            exit
        exit
        vrf-export "IPsec-to-MPBGP"
        route-distinguisher 64496:2
        vrf-target target:64496:2
        interface "int-IPsec-Private-1" tunnel create
            sap tunnel-1.private:1 create
                ipsec-tunnel "tunnel-1" create
                    security-policy 1
                    local-gateway-address 10.10.20.1 peer 10.10.10.1
                                                       delivery-service 1
                    dynamic-keying
                        ike-policy 1
                        pre-shared-key "ALU"
                        transform 1
                    exit
                    no shutdown
                exit
            exit
            static-tunnel-redundant-next-hop 192.168.20.1
        exit
        interface "int-Redundant-1" create
            address 192.168.20.2/30
            spoke-sdp 100:20 create
                ingress
                    vc-label 2048
                exit
                egress
                    vc-label 2049
                exit
                no shutdown
            exit
        exit
        static-route 192.168.1.1/32 ipsec-tunnel "tunnel-1"
        spoke-sdp 100 create
            description "SDP to SeGW-1"
        exit
        spoke-sdp 300 create
            description "SDP to P-1"
        exit
```

```
            no shutdown
        exit
    exit
#--------------------------------------------------
echo "Router (Service Side) Configuration"
#--------------------------------------------------
    router
#--------------------------------------------------
echo "Policy Configuration"
#--------------------------------------------------
        policy-options
            begin
            prefix-list "CE1-Internal"
                prefix 192.168.1.1/32 exact
            exit
            community "vprn2" members "target:64496:2"
            policy-statement "IPsec-to-MPBGP"
                entry 10
                    from
                        prefix-list "CE1-Internal"
                        state ipsec-master-with-peer
                    exit
                    action accept
                        community add "vprn2"
                        local-preference 200
                    exit
                exit
                entry 20
                    from
                        prefix-list "CE1-Internal"
                        state ipsec-non-master
                    exit
                    action accept
                        community add "vprn2"
                        local-preference 100
                    exit
                exit
                entry 30
                    from
                        prefix-list "CE1-Internal"
                        state ipsec-master-without-peer
                    exit
                    action accept
                        community add "vprn2"
                        local-preference 100
                    exit
                exit
                default-action accept
                    community add "vprn2"
                exit
            exit
            commit
        exit
#--------------------------------------------------
echo "BGP Configuration"
#--------------------------------------------------
        bgp
            group "MPBGP"
                family vpn-ipv4
```

```
            peer-as 64496
            neighbor 192.0.2.1
            exit
            neighbor 192.0.2.3
            exit
        exit
        no shutdown
    exit
exit
```

Step 8. Verify the MC-IPSec status on SeGW-1 and SeGW-2.

- Verify that SeGW-1 is the master and SeGW-2 is the standby for tunnel-group 1 because SeGW-1 has higher priority 200.
- Verify that SeGW-1 is the VRRP 10 master and SeGW-2 is the backup.

```
A:SeGW-1# show redundancy multi-chassis mc-ipsec peer 192.0.2.2
===============================================================================
Multi-Chassis MC-IPsec
===============================================================================
Peer Name       : (Not Specified)
Peer Addr       : 192.0.2.2
Keep Alive Intvl: 1.0 secs            Hold on Nbr Fail     : 3
Discovery Intvl : 300 secs            Discovery Boot Intvl : 300 secs
BFD             : Enable
Last update     : 04/04/2014 10:23:35

===============================================================================
Multi-Chassis IPsec Multi Active Tunnel-Group Table
===============================================================================
ID             Peer Group     Priority  Admin State    Mastership
-------------------------------------------------------------------------------
1              1              200       Up             master
-------------------------------------------------------------------------------
Multi Active Tunnel Group Entries found: 1
===============================================================================
===============================================================================
A:SeGW-1#


A:SeGW-2# show redundancy multi-chassis mc-ipsec peer 192.0.2.1
===============================================================================
Multi-Chassis MC-IPsec
===============================================================================
Peer Name       : (Not Specified)
Peer Addr       : 192.0.2.1
Keep Alive Intvl: 1.0 secs            Hold on Nbr Fail     : 3
Discovery Intvl : 300 secs            Discovery Boot Intvl : 300 secs
BFD             : Enable
Last update     : 04/04/2014 10:23:50

===============================================================================
Multi-Chassis IPsec Multi Active Tunnel-Group Table
===============================================================================
ID             Peer Group     Priority  Admin State    Mastership
-------------------------------------------------------------------------------
1              1              150       Up             standby
-------------------------------------------------------------------------------
Multi Active Tunnel Group Entries found: 1
===============================================================================
===============================================================================
A:SeGW-2#


A:SeGW-1# show router vrrp instance
===============================================================================
VRRP Instances
```

```
===============================================================================
Interface Name                   VR Id Own Adm  State       Base Pri   Msg Int
                                 IP        Opr  Pol Id      InUse Pri  Inh Int
-------------------------------------------------------------------------------
int-SeGW1-S1                     10    No  Up   Master       200       1
                                 IPv4      Up   1           200       No
  Backup Addr: 172.16.1.254
-------------------------------------------------------------------------------
Instances : 1
===============================================================================
A:SeGW-1#


A:SeGW-2# show router vrrp instance
===============================================================================
VRRP Instances
===============================================================================
Interface Name                   VR Id Own Adm  State       Base Pri   Msg Int
                                 IP        Opr  Pol Id      InUse Pri  Inh Int
-------------------------------------------------------------------------------
int-SeGW2-S1                     10    No  Up   Backup       100       1
                                 IPv4      Up   n/a         100       No
  Backup Addr: 172.16.1.254
-------------------------------------------------------------------------------
Instances : 1
===============================================================================
A:SeGW-2#
```

.

Step 9. Trigger the tunnel-1 setup on CE-1 by sending pings.

```
A:CE-1# ping router 2 192.168.2.1
PING 192.168.2.1 56 data bytes
64 bytes from 192.168.2.1: icmp_seq=2 ttl=63 time=2.35ms.
64 bytes from 192.168.2.1: icmp_seq=3 ttl=63 time=2.31ms.
64 bytes from 192.168.2.1: icmp_seq=4 ttl=63 time=2.28ms.
64 bytes from 192.168.2.1: icmp_seq=5 ttl=63 time=2.27ms.
Request timed out. icmp_seq=1.

---- 192.168.2.1 PING Statistics ----
5 packets transmitted, 4 packets received, 20.00% packet loss
round-trip min = 2.27ms, avg = 2.30ms, max = 2.35ms, stddev = 0.031ms
A:CE-1#


A:CE-1# show ipsec tunnel
===============================================================================
IPsec Tunnels
===============================================================================
TunnelName                      LocalAddress      SvcId        Admn   Keying
  SapId                           RemoteAddress     DlvrySvcId   Oper   Sec
                                                                        Plcy
-------------------------------------------------------------------------------
tunnel-1                        10.10.10.1        2            Up     Dynamic
  tunnel-1.private:1              10.10.20.1        1            Up     1
-------------------------------------------------------------------------------
IPsec Tunnels: 1
===============================================================================
A:CE-1#
```

Step 10. Verify that the tunnel status on SeGW-1/SeGW-2 is “up”.

- Verify that MCS database is in-sync, so the tunnel status is “up” on both chassis.
- Verify P-1 receives two 192.168.1.1/32 VPN IPv4 routes, the route from SeGW-1 has local preference 200, and the one from SeGW-2 has 100.

```
A:SeGW-1# show ipsec tunnel
===============================================================================
IPsec Tunnels
===============================================================================
TunnelName                      LocalAddress      SvcId        Admn   Keying
  SapId                           RemoteAddress     DlvrySvcId   Oper   Sec
                                                                        Plcy
-------------------------------------------------------------------------------
tunnel-1                        10.10.20.1        2            Up     Dynamic
  tunnel-1.private:1              10.10.10.1        1            Up     1
-------------------------------------------------------------------------------
IPsec Tunnels: 1
===============================================================================
A:SeGW-1#


A:SeGW-2# show ipsec tunnel
===============================================================================
IPsec Tunnels
===============================================================================
TunnelName                      LocalAddress      SvcId        Admn   Keying
  SapId                           RemoteAddress     DlvrySvcId   Oper   Sec
                                                                        Plcy
-------------------------------------------------------------------------------
tunnel-1                        10.10.20.1        2            Up     Dynamic
  tunnel-1.private:1              10.10.10.1        1            Up     1
-------------------------------------------------------------------------------
IPsec Tunnels: 1
===============================================================================
A:SeGW-2#


A:SeGW-2# show redundancy multi-chassis sync
===============================================================================
Multi-chassis Peer Table
===============================================================================
Peer
-------------------------------------------------------------------------------
Peer IP Address         : 192.0.2.1
Description             : (Not Specified)
Authentication          : Disabled
Source IP Address       : 192.0.2.2
Admin State             : Enabled
Warm standby            : No
Remote warm standby     : No
-------------------------------------------------------------------------------
Sync-status
-------------------------------------------------------------------------------
Client Applications     : IPsec
Sync Admin State        : Up
Sync Oper State         : Up
```

```
Sync Oper Flags         :
DB Sync State           : inSync
Num Entries             : 2
Lcl Deleted Entries     : 0
Alarm Entries           : 0
OMCR Standby Entries    : 0
OMCR Alarm Entries      : 0
Rem Num Entries         : 2
Rem Lcl Deleted Entries : 0
Rem Alarm Entries       : 0
Rem OMCR Standby Entries: 0
Rem OMCR Alarm Entries  : 0
===============================================================================
===============================================================================
A:SeGW-2#


A:P-1# show router bgp routes vpn-ipv4
===============================================================================
 BGP Router ID:192.0.2.3        AS:64496       Local AS:64496
===============================================================================
 Legend -
 Status codes  : u - used, s - suppressed, h - history, d - decayed, * - valid
 Origin codes  : i - IGP, e - EGP, ? - incomplete, > - best, b - backup

===============================================================================
BGP VPN-IPv4 Routes
===============================================================================
Flag  Network                                           LocalPref   MED
      Nexthop                                           Path-Id     Label
      As-Path
-------------------------------------------------------------------------------
u*>i  64496:2:192.168.1.1/32                            200         None
      192.0.2.1                                         None        262143
      No As-Path
*i    64496:2:192.168.1.1/32                            100         None
      192.0.2.2                                         None        262143
      No As-Path
u*>i  64496:2:192.168.20.0/30                           100         None
      192.0.2.1                                         None        262143
      No As-Path
*>i   64496:2:192.168.20.0/30                           100         None
      192.0.2.2                                         None        262143
      No As-Path
-------------------------------------------------------------------------------
Routes : 4
===============================================================================
A:P-1#
```

Step 11. Trigger MC-IPSec switchover by shutting down the MS-ISA.

- Verify the VRRP/MC-IPSec state on SeGW-1 is “master”, SeGW-2 is “backup”/ ”standby”.
- Shutdown the MS-ISA on SeGW-1, which is currently Master.
- Verify that the MC-IPSec state of tunnel-group 1 on SeGW-1 becomes “notEligible”, SeGW-2 becomes “master”.

  Note: notEligible means the tunnel-group is down, refer to the SR OS MS-ISA Guide for details description of MIMP states.
- Verify that the VRRP state on SeGW-1 becomes “backup” and SeGW-2 becomes “master”. This is triggered by MC-IPSec switchover, configured via mc-ipsec-non-forwarding event in vrrp-policy 1.

```
A:SeGW-1# show redundancy multi-chassis mc-ipsec peer 192.0.2.2
===============================================================================
Multi-Chassis MC-IPsec
===============================================================================
Peer Name       : (Not Specified)
Peer Addr       : 192.0.2.2
Keep Alive Intvl: 1.0 secs            Hold on Nbr Fail     : 3
Discovery Intvl : 300 secs            Discovery Boot Intvl : 300 secs
BFD             : Enable
Last update     : 04/04/2014 10:23:35
===============================================================================
Multi-Chassis IPsec Multi Active Tunnel-Group Table
===============================================================================
ID             Peer Group     Priority  Admin State    Mastership
-------------------------------------------------------------------------------
1              1              200       Up             master
-------------------------------------------------------------------------------
Multi Active Tunnel Group Entries found: 1
===============================================================================
===============================================================================
A:SeGW-1#


A:SeGW-1# show router vrrp instance
===============================================================================
VRRP Instances
===============================================================================
Interface Name                   VR Id Own Adm  State       Base Pri   Msg Int
                                 IP        Opr  Pol Id      InUse Pri  Inh Int
-------------------------------------------------------------------------------
int-SeGW1-S1                     10    No  Up   Master       200       1
                                 IPv4      Up   1           200        No
  Backup Addr: 172.16.1.254
-------------------------------------------------------------------------------
Instances : 1
===============================================================================
A:SeGW-1#


A:SeGW-2# show redundancy multi-chassis mc-ipsec peer 192.0.2.1
```

```
===============================================================================
Multi-Chassis MC-IPsec
===============================================================================
Peer Name       : (Not Specified)
Peer Addr       : 192.0.2.1
Keep Alive Intvl: 1.0 secs            Hold on Nbr Fail     : 3
Discovery Intvl : 300 secs            Discovery Boot Intvl : 300 secs
BFD             : Enable
Last update     : 04/04/2014 10:23:50

===============================================================================
Multi-Chassis IPsec Multi Active Tunnel-Group Table
===============================================================================
ID             Peer Group     Priority  Admin State    Mastership
-------------------------------------------------------------------------------
1              1              150       Up             standby
-------------------------------------------------------------------------------
Multi Active Tunnel Group Entries found: 1
===============================================================================
===============================================================================
A:SeGW-2#


A:SeGW-2# show router vrrp instance

===============================================================================
VRRP Instances
===============================================================================
Interface Name                    VR Id Own Adm  State       Base Pri   Msg Int
                                  IP        Opr  Pol Id      InUse Pri  Inh Int
-------------------------------------------------------------------------------
int-SeGW2-S1                      10    No  Up   Backup       100       1
                                  IPv4      Up   n/a         100        No
  Backup Addr: 172.16.1.254
-------------------------------------------------------------------------------
Instances : 1
===============================================================================
A:SeGW-2#


*A:SeGW-1# configure card 1 mda 2 shutdown


*A:SeGW-1# show redundancy multi-chassis mc-ipsec peer 192.0.2.2

===============================================================================
Multi-Chassis MC-IPsec
===============================================================================
Peer Name       : (Not Specified)
Peer Addr       : 192.0.2.2
Keep Alive Intvl: 1.0 secs            Hold on Nbr Fail     : 3
Discovery Intvl : 300 secs            Discovery Boot Intvl : 300 secs
BFD             : Enable
Last update     : 04/04/2014 10:23:35

===============================================================================
Multi-Chassis IPsec Multi Active Tunnel-Group Table
===============================================================================
ID             Peer Group     Priority  Admin State    Mastership
```

```
-------------------------------------------------------------------------
1              1              200       Up             notEligible
-------------------------------------------------------------------------
Multi Active Tunnel Group Entries found: 1
=========================================================================
===============================================================================
*A:SeGW-1#



*A:SeGW-1# show router vrrp instance
===============================================================================
VRRP Instances
===============================================================================
Interface Name                   VR Id Own Adm  State       Base Pri   Msg Int
                                 IP        Opr  Pol Id      InUse Pri  Inh Int
-------------------------------------------------------------------------------
int-SeGW1-S1                     10    No  Up   Backup       200       1
                                 IPv4      Up   1           50         No
  Backup Addr: 172.16.1.254
-------------------------------------------------------------------------------
Instances : 1
===============================================================================
*A:SeGW-1#


A:SeGW-2# show redundancy multi-chassis mc-ipsec peer 192.0.2.1
===============================================================================
Multi-Chassis MC-IPsec
===============================================================================
Peer Name       : (Not Specified)
Peer Addr       : 192.0.2.1
Keep Alive Intvl: 1.0 secs            Hold on Nbr Fail     : 3
Discovery Intvl : 300 secs            Discovery Boot Intvl : 300 secs
BFD             : Enable
Last update     : 04/04/2014 10:23:50
=========================================================================
Multi-Chassis IPsec Multi Active Tunnel-Group Table
=========================================================================
ID             Peer Group     Priority  Admin State    Mastership
-------------------------------------------------------------------------
1              1              150       Up             master
-------------------------------------------------------------------------
Multi Active Tunnel Group Entries found: 1
=========================================================================
===============================================================================
A:SeGW-2#


A:SeGW-2# show router vrrp instance
===============================================================================
VRRP Instances
===============================================================================
Interface Name                   VR Id Own Adm  State       Base Pri   Msg Int
                                 IP        Opr  Pol Id      InUse Pri  Inh Int
-------------------------------------------------------------------------------
int-SeGW2-S1                     10    No  Up   Master       100       1
                                 IPv4      Up   n/a         100        No
```

```
  Backup Addr: 172.16.1.254
-------------------------------------------------------------------------------
Instances : 1
===============================================================================
A:SeGW-2#
```

Step 12. Trigger the MC-IPSec switchover by rebooting SeGW-1.

- Restore state as in Step 10 (before the MC-IPSec switchover).
  → Note: The MC-IPSec switchover could be triggered manually with the **tools perform redundancy multi-chassis mc-ipsec force-switchover tunnel-group 1** command.
- Verify the VRRP/MC-IPSec state on SeGW-1 is “master”, SeGW-2 is “backup”/ ”standby”.
- Reboot SeGW-1 which is the current Master.
- Verify the MC-IPSec state of tunnel-group 1 on SeGW-2 becomes “eligible” during SeGW-1 rebooting.
- Verify the VRRP state on SeGW-2 becomes “master” during SeGW-1 reboot.
- After SeGW-1 comes up, verify MC-IPSec state of tunnel-group 1 is “discovery” initially, and then becomes “standby”;
  → Note: The “discovery” state means system has not established the MIMP session with peer yet.
- Verify the MC-IPSec state of tunnel-group 1 on SeGW-2 becomes “master” when SeGW-1 becomes “standby”.
- After SeGW-1 comes up, verify the VRRP state is “backup”.

```
*A:SeGW-1# show redundancy multi-chassis mc-ipsec peer 192.0.2.2
===============================================================================
Multi-Chassis MC-IPsec
===============================================================================
Peer Name       : (Not Specified)
Peer Addr       : 192.0.2.2
Keep Alive Intvl: 1.0 secs            Hold on Nbr Fail     : 3
Discovery Intvl : 300 secs            Discovery Boot Intvl : 300 secs
BFD             : Enable
Last update     : 04/04/2014 10:23:35
===============================================================================
Multi-Chassis IPsec Multi Active Tunnel-Group Table
===============================================================================
ID             Peer Group     Priority  Admin State    Mastership
-------------------------------------------------------------------------------
1              1              200       Up             master
-------------------------------------------------------------------------------
Multi Active Tunnel Group Entries found: 1
===============================================================================
===============================================================================
*A:SeGW-1#


*A:SeGW-1# show router vrrp instance
===============================================================================
VRRP Instances
===============================================================================
Interface Name                   VR Id Own Adm  State       Base Pri   Msg Int
                                 IP        Opr  Pol Id      InUse Pri  Inh Int
-------------------------------------------------------------------------------
```

```
int-SeGW1-S1                      10    No  Up   Master       200       1
                                  IPv4      Up   1            200       No
  Backup Addr: 172.16.1.254
-------------------------------------------------------------------------------
Instances : 1
===============================================================================
*A:SeGW-1#



A:SeGW-2# show redundancy multi-chassis mc-ipsec peer 192.0.2.1
===============================================================================
Multi-Chassis MC-IPsec
===============================================================================
Peer Name       : (Not Specified)
Peer Addr       : 192.0.2.1
Keep Alive Intvl: 1.0 secs            Hold on Nbr Fail     : 3
Discovery Intvl : 300 secs            Discovery Boot Intvl : 300 secs
BFD             : Enable
Last update     : 04/04/2014 10:23:50

===============================================================================
Multi-Chassis IPsec Multi Active Tunnel-Group Table
===============================================================================
ID              Peer Group     Priority  Admin State    Mastership
-------------------------------------------------------------------------------
1               1              150       Up             standby
-------------------------------------------------------------------------------
Multi Active Tunnel Group Entries found: 1
===============================================================================
===============================================================================
A:SeGW-2#


A:SeGW-2# show router vrrp instance
===============================================================================
VRRP Instances
===============================================================================
Interface Name                    VR Id Own Adm  State       Base Pri   Msg Int
                                  IP        Opr  Pol Id      InUse Pri  Inh Int
-------------------------------------------------------------------------------
int-SeGW2-S1                      10    No  Up   Backup       100       1
                                  IPv4      Up   n/a         100       No
  Backup Addr: 172.16.1.254
-------------------------------------------------------------------------------
Instances : 1
===============================================================================
A:SeGW-2#


A:SeGW-1# admin reboot
Are you sure you want to reboot (y/n)? y

A:SeGW-2# show redundancy multi-chassis mc-ipsec peer 192.0.2.1
===============================================================================
Multi-Chassis MC-IPsec
===============================================================================
Peer Name       : (Not Specified)
Peer Addr       : 192.0.2.1
```

```
Keep Alive Intvl: 1.0 secs            Hold on Nbr Fail     : 3
Discovery Intvl : 300 secs            Discovery Boot Intvl : 300 secs
BFD             : Enable
Last update     : 04/04/2014 10:23:50
===============================================================================
Multi-Chassis IPsec Multi Active Tunnel-Group Table
===============================================================================
ID             Peer Group     Priority  Admin State    Mastership
-------------------------------------------------------------------------------
1              1              150       Up             eligible
-------------------------------------------------------------------------------
Multi Active Tunnel Group Entries found: 1
===============================================================================
===============================================================================
A:SeGW-2#


A:SeGW-2# show router vrrp instance
===============================================================================
VRRP Instances
===============================================================================
Interface Name                   VR Id Own Adm  State       Base Pri   Msg Int
                                 IP        Opr  Pol Id      InUse Pri  Inh Int
-------------------------------------------------------------------------------
int-SeGW2-S1                     10    No  Up   Master       100       1
                                 IPv4      Up   n/a         100       No
  Backup Addr: 172.16.1.254
-------------------------------------------------------------------------------
Instances : 1
===============================================================================
A:SeGW-2#
```

SeGW-1 comes up.

```
A:SeGW-1# show redundancy multi-chassis mc-ipsec peer 192.0.2.2
===============================================================================
Multi-Chassis MC-IPsec
===============================================================================
Peer Name       : (Not Specified)
Peer Addr       : 192.0.2.2
Keep Alive Intvl: 1.0 secs            Hold on Nbr Fail     : 3
Discovery Intvl : 300 secs            Discovery Boot Intvl : 300 secs
BFD             : Enable
Last update     : 04/04/2014 10:58:07

===============================================================================
Multi-Chassis IPsec Multi Active Tunnel-Group Table
===============================================================================
ID             Peer Group     Priority  Admin State    Mastership
-------------------------------------------------------------------------------
1              1              200       Up             discovery
-------------------------------------------------------------------------------
Multi Active Tunnel Group Entries found: 1
===============================================================================
===============================================================================
A:SeGW-1#
```

```
A:SeGW-1# show redundancy multi-chassis mc-ipsec peer 192.0.2.2
===============================================================================
Multi-Chassis MC-IPsec
===============================================================================
Peer Name       : (Not Specified)
Peer Addr       : 192.0.2.2
Keep Alive Intvl: 1.0 secs            Hold on Nbr Fail     : 3
Discovery Intvl : 300 secs            Discovery Boot Intvl : 300 secs
BFD             : Enable
Last update     : 04/04/2014 10:58:07

=============================================================================
Multi-Chassis IPsec Multi Active Tunnel-Group Table
=============================================================================
ID             Peer Group     Priority  Admin State    Mastership
-----------------------------------------------------------------------------
1              1              200       Up             standby
-----------------------------------------------------------------------------
Multi Active Tunnel Group Entries found: 1
=============================================================================
===============================================================================
A:SeGW-1#


A:SeGW-1# show router vrrp instance
===============================================================================
VRRP Instances
===============================================================================
Interface Name                    VR Id Own Adm  State       Base Pri   Msg Int
                                  IP        Opr  Pol Id      InUse Pri  Inh Int
-------------------------------------------------------------------------------
int-SeGW1-S1                      10    No  Up   Backup       200       1
                                  IPv4      Up   1           50         No
  Backup Addr: 172.16.1.254
-------------------------------------------------------------------------------
Instances : 1
===============================================================================
A:SeGW-1#


A:SeGW-2# show redundancy multi-chassis mc-ipsec peer 192.0.2.1
===============================================================================
Multi-Chassis MC-IPsec
===============================================================================
Peer Name       : (Not Specified)
Peer Addr       : 192.0.2.1
Keep Alive Intvl: 1.0 secs            Hold on Nbr Fail     : 3
Discovery Intvl : 300 secs            Discovery Boot Intvl : 300 secs
BFD             : Enable
Last update     : 04/04/2014 10:23:50

=============================================================================
Multi-Chassis IPsec Multi Active Tunnel-Group Table
=============================================================================
ID             Peer Group     Priority  Admin State    Mastership
-----------------------------------------------------------------------------
1              1              150       Up             master
-----------------------------------------------------------------------------
Multi Active Tunnel Group Entries found: 1
```

```
===============================================================================
===============================================================================
A:SeGW-2#
```

Configuration Guidelines

The following is a list of configuration and operational guidelines that the user should follow for MC-IPSec:

- To avoid high CPU load and issues in some complex cases, the following are suggestions for configuring IKEv2 lifetime:

1. Both IKE_SA and CHILD_SA lifetime on MC-IPSec chassis (SeGW-1 and SeGW-2) should be around 3 times larger than on the IPSec peer (CE-1).
2. With the first rule, the lifetime of the side with smaller lifetime should NOT be too small (these being the default values):
   - → IKE_SA: >= 86400 seconds
   - → CHILD_SA: >= 3600 seconds
3. With the first rule, on the side with smaller lifetime, the IKE_SA lifetime should be at least 3 times larger than CHILD_SA lifetime.

- IKE protocol is the control plane of IPSec, so IKE packet should be treated as high QoS priority in end-to-end path of public service.
  - → On public interface, a sap-ingress qos policy should be configured to ensure IKE packet gets high QoS priority.
- Configure responder-only under tunnel-group for static LAN-to-LAN tunnel.
- Enable DPD (Dead Peer Detection) on peer side, configure “no dpd” on MC-IPSec chassis side.
- Direct and redundant physical link between MC-IPSec chassis should be configured with enough bandwidth for MCS and shunting traffic, and proper QoS configuration to make sure the MIMP/MCS packet treated as high priority traffic.
- System time must be same on both MC-IPSec chassis.
- Check and make sure the protection status is "nominal" on both chassis before you do a controlled switchover. Protection status could be displayed via command “show redundancy multi-chassis mc-ipsec peer <addr>”.
- Wait at least 5 minutes between two consecutive switchovers if possible to prevent a second switchover happening before the standby is ready to take over mastership.

Conclusion

MC-IPSec provides a stateful multi-chassis IPSec redundancy solution. This is very important in a carrier grade network, especially in applications like mobile backhaul where high value 3G/4G mobile service run over IPSec tunnels.