Sample L2 Intrachassis HA Configuration

This chapter provides a sample intrachassis wsg-service High Availability (HA) configuration for SecGW functionality between two ASR 9000 VSM CPUs running VPC-VSM instances (StarOS VMs) in the same ASR 9000 chassis. It includes StarOS monitoring of a public interface on an ASR 9000 line card (LC).

ASR 9000 RSP Configuration (IOS-XR)

Notes:

- Enable oneP communication. (TLS Protocol)
- Configure an IOS-XP access list.
- Configure a management interface
- Configure a public network LC interface for IKE and RSP traffic
- Configure actual and virtual interfaces for IKE, clear traffic and ICSR-SRP interfaces to VM-1 and VM-2.
- Configure Bridge-group Virtual Interfaces (BVIs) to bridge the IKE and clear traffic ports between VM-1 and VM-2.
- Configure Static Integrated Route Bridging (IRB) routes and L2 VLANs.
- Shutdown all unused ports.

```
<snip>

onep
 transport type tls localcert onep-tp disable-remotecert-validation

virtual-service enable
virtual-service SecGW1
 vnic interface TenGigE0/1/1/0
 vnic interface TenGigE0/1/1/1
 vnic interface TenGigE0/1/1/2
 activate

virtual-service SecGW3
 vnic interface TenGigE0/1/1/6
```

```
 vnic interface TenGigE0/1/1/7
 vnic interface TenGigE0/1/1/8
 activate

virtual-service SecGW4
 vnic interface TenGigE0/1/1/9
 vnic interface TenGigE0/1/1/10
 vnic interface TenGigE0/1/1/11
 activate

virtual-service SecGW2
 vnic interface TenGigE0/1/1/3
 vnic interface TenGigE0/1/1/4
 vnic interface TenGigE0/1/1/5
 activate

 crypto ca trustpoint onep-tp
 crl optional
 subject-name CN=ASR9K-8.cisco.com
 enrollment url terminal
ipv4 access-list public
 10 permit ipv4 host 55.55.33.30 any nexthop1 ipv4 34.34.34.101
 20 permit ipv4 any any

interface MgmtEth0/RSP0/CPU0/0
 ipv4 address 172.29.98.140 255.255.254.0

interface MgmtEth0/RSP0/CPU0/1
 shutdown

interface GigabitEthernet0/1/0/0
 shutdown

interface GigabitEthernet0/1/0/3
 description "LC Interface to Private Network: Clear traffic"
 ipv4 address 66.66.66.25 255.255.255.0

interface GigabitEthernet0/1/0/4
 shutdown

...

interface GigabitEthernet0/1/0/19
 shutdown

interface GigabitEthernet0/1/0/6
 shutdown

interface GigabitEthernet0/1/1/0
 shutdown

...

interface GigabitEthernet0/1/1/19
```

```
 shutdown

interface TenGigE0/2/1/0
 ipv4 address 192.168.122.1 255.255.255.0

interface TenGigE0/2/1/1
 description "IKE Interface on VSM1"
 l2transport


interface TenGigE0/2/1/2
 description "CLEAR Interface on VSM1"
 l2transport


interface TenGigE0/2/1/3
 description "SRP Interface on VSM1"
 ipv4 address 88.88.88.23 255.255.255.0

interface TenGigE0/2/1/4
 shutdown

...

interface TenGigE0/2/1/11
 shutdown

interface TenGigE0/4/1/0
 ipv4 address 192.168.120.1 255.255.255.0

interface TenGigE0/4/1/1
 shutdown

interface TenGigE0/4/1/1
 shutdown


interface TenGigE0/4/1/2
 shutdown


interface TenGigE0/4/1/3
 shutdown

interface TenGigE0/4/1/4
 description "IKE Interface on VSM2"
 l2transport


interface TenGigE0/4/1/6
 description "SRP Interface on VSM2"
 ipv4 address 86.86.86.23 255.255.255.0

interface TenGigE0/4/1/7
 shutdown
```

```
...

interface TenGigE0/4/1/11
 shutdown

interface BVI1
 description "Virtual Interface for IKE Bridge between VSM1 and VSM2 IKE
 ports"
 ipv4 address 34.34.34.100 255.255.255.0

interface BVI2
 description "Virtual Interface for CLEAR Bridge between VSM1 and VSM2
CLEAR Ports"
 ipv4 address 78.78.78.100 255.255.255.0

interface preconfigure TenGigE0/0/0/0
 shutdown

...
interface preconfigure TenGigE0/0/0/3
 shutdown

interface preconfigure TenGigE0/2/0/0
 shutdown

...

interface preconfigure TenGigE0/2/0/3
 shutdown

router static
 address-family ipv4 unicast
  55.55.33.0/24 22.22.22.24
  171.0.0.0/8 172.29.98.1
  172.0.0.0/8 172.29.98.1


l2vpn
 xconnect group wsg
 bridge group irb
  bridge-domain irb1
   interface TenGigE0/2/1/1

   interface TenGigE0/4/1/4

   routed interface BVI1

  bridge-domain irb2
   interface TenGigE0/2/1/2

   interface TenGigE0/4/1/5
```

```
   routed interface BVI2


router hsrp
 interface GigabitEthernet0/0/0/5
  address-family ipv4
   hsrp 3
    preempt
    priority 101
    address 87.87.87.20
    track object PrivateHsrp
    track object PublicHsrp


 interface GigabitEthernet0/0/0/18.1871
  address-family ipv4
   hsrp 3
    preempt
    priority 101
    address 187.0.1.20
    track object WsgIPsla
    track object PublicHsrp
    track object PrivateHsrp


ipsla
 operation 200
  type icmp echo
   destination address 31.31.31.100
   timeout 300
   frequency 1


 schedule operation 200
  start-time now
  life forever

track PublicHsrp
 type line-protocol state
  interface GigabitEthernet0/0/0/18

 delay up 1
 delay down

track PrivateHsrp
 type line-protocol state
  interface GigabitEthernet0/0/0/19
```

```
delay up 1
delay down
```

WSG Configuration VM-1 (StarOS)

Notes:

- Configure a ConnectedApps (oneP) interface in the local context for StarOS VM-1.
- Configure a "wsg" context with an ACL, IPSec transform set and crypto template.
- Configure clear traffic, srpa and srvip loopback interfaces with **srp-activate**.
- Set aaa group and subscriber to **default**.
- Configure wsg-service "abc". Bind to crypto template with site-to-site deployment mode and IP access group "one".
- Configure IP routes for IKE and clear traffic.
- Configure RRI route to network mode.
- Configure "srp" context with service-redundancy-protocol enabled.
- Configure interface "icsr" with an IP route.
- Configure oneP/ConnectedApps session. (TLS Protocol)
- Set wsg-lookup priorities.
- Configure ethernet ports 1/10 (IKE), 1/11 (clear traffic) and 1/12 (ICSR-SRP).

Important The session name specified in the configuration on both the active and standby SecGW must be the same.

```
config
   context local
      interface CA
         ip address 192.168.122.15 255.255.255.0
      exit
      subscriber default
      exit
      administrator cisco encrypted password <encrypted_password>
      aaa group default
      exit
   exit
   port ethernet 1/1
      no shutdown
      bind interface CA local
   exit
   context wsg
      ip access-list one
         permit ip 66.66.0.0 0.0.255.255 45.45.0.0 0.0.255.255 protocol
255
      exit
      ipsec transform-set tselsa-foo
      exit
      ikev2-ikesa transform-set ikesa-foo
      exit
```

```
      crypto template foo ikev2-dynamic
         authentication local pre-shared-key encrypted key <encrypted_key>
         authentication remote pre-shared-key encrypted key <encrypted_key>
         ikev2-ikesa transform-set list ikesa-foo
         payload foo-sa0 match childsa match ipv4
            ip-address-alloc dynamic
            ipsec transform-set list tselsa-foo
         exit
         identity local id-type ip-addr id 32.32.32.30
      exit

      interface clear
         ip address 78.78.78.33 255.255.255.0
      exit
      interface ike
         ip address 34.34.34.33 255.255.255.0
      exit
      interface loopback-clear loopback
         ip address 78.78.78.50 255.255.255.255 srp-activate
      exit
      interface loopback-srpa loopback
         ip address 34.34.34.101 255.255.255.255 srp-activate
      exit
       interface loopback-srvip loopback
         ip address 32.32.32.30 255.255.255.255 srp-activate
      exit
      subscriber default
      exit
      aaa group default
      exit
      wsg-service abc
         deployment-mode site-to-site
         ip access-group one
         bind address 32.32.32.30 crypto-template foo
      exit
      ip route 55.55.33.0 255.255.255.0 34.34.34.100 ike
      ip route 66.66.66.0 255.255.255.0 78.78.78.100 clear

      ip rri-route network-mode L2 78.78.78.50 next-hop 78.78.78.33
interface clear
      ip rri-remote-access next-hop 78.78.78.33 interface clear
   exit
   context srp
      service-redundancy-protocol
         chassis-mode primary
         hello-interval 3
         configuration interval 60
         dead interval 15
         checkpoint session duration non-ims-session 30
         route-modifier threshold 10
         priority 10
         monitor hsrp interface GigabitEthernet0/0/0/5 afi-type IPv4
```

```
hsrp-group 3
         peer-ip-address 81.81.81.11
         bind address 71.71.71.11
      exit
      interface icsr
         ip address 88.88.88.33 255.255.255.0
      exit
      subscriber default
      exit
      aaa group default
      exit
      ip route 86.86.86.0 255.255.255.0 88.88.88.23 icsr
   exit
   connectedapps
      sess-userid cisco
      sess-passwd encrypted password <encrypted_password>
      sess-name intraCh
      sess-ip-address 192.168.122.1
      rri-mode S2S
      ha-chassis-mode intra
      ha-network-mode L2
      ca-certificate-name cert_name
      activate
   exit
   wsg-lookup
      priority 1 source-netmask 28 destination-netmask 28
      priority 2 source-netmask 32 destination-netmask 32
      priority 3 source-netmask 16 destination-netmask 16
      priority 4 source-netmask 24 destination-netmask 24
   exit
   port ethernet 1/10
      no shutdown
      bind interface ike wsg
   exit
   port ethernet 1/11
      no shutdown
      bind interface clear wsg
      vlan 12
        description "ICSR"
        no shutdown
        bind interface icsr srp
      #exit
   #exit
end
```

WSG Configuration VM-2 (StarOS)

Notes:

- Configure a ConnectedApps (oneP) interface in the local context for StarOS VM-2.

- Configure a "wsg" context with an ACL, IPSec transform set and crypto template.
- Configure clear traffic, srpa and srvip loopback interfaces with **srp-activate**.
- Set aaa group and subscriber to **default**.
- Configure wsg-service "abc". Bind to crypto template with site-to-site deployment mode and IP access group "one".
- Configure IP routes for IKE and clear traffic (IP addresses unique to VM-2).
- Configure RRI route to network mode (IP address unique to VM-2).
- Configure "srp" context with service-redundancy-protocol enabled (peer-ip-address and bind address reversed from VSM-1).
- Configure interface "icsr" with an IP route (IP address unique to VM-2).
- Configure oneP/ConnectedApps session (sess-ip-address unique to VM-2). [TLS protocol]
- Set wsg-lookup priorities.
- Configure ethernet ports 1/10 (IKE), 1/11 (clear traffic) and 1/12 (ICSR-SRP).

Important The session name specified in the configuration on both the active and standby SecGW must be the same.

```
config
   context local
      interface CA
         ip address 192.168.122.15 255.255.255.0
      exit
      subscriber default
      exit
      administrator cisco encrypted password <encrypted_password>
      aaa group default
      exit
   exit
   port ethernet 1/1
      no shutdown
      bind interface CA local
   exit
   context wsg
      ip access-list one
         permit ip 66.66.0.0 0.0.255.255 45.45.0.0 0.0.255.255 protocol
255
      exit
      ipsec transform-set tselsa-foo
      exit
      ikev2-ikesa transform-set ikesa-foo
      exit
      crypto template foo ikev2-dynamic
         authentication local pre-shared-key encrypted key <encrypted_key>
         authentication remote pre-shared-key encrypted key <encrypted_key>
         ikev2-ikesa transform-set list ikesa-foo
         payload foo-sa0 match childsa match ipv4
            ip-address-alloc dynamic
            ipsec transform-set list tselsa-foo
         exit
```

```
         identity local id-type ip-addr id 32.32.32.30
      exit

      interface clear
         ip address 78.78.78.34 255.255.255.0
      exit
      interface ike
         ip address 34.34.34.34 255.255.255.0
      exit
      interface loopback-clear loopback
         ip address 78.78.78.50 255.255.255.255 srp-activate
      exit
      interface loopback-srpa loopback
         ip address 34.34.34.101 255.255.255.255 srp-activate
      exit
       interface loopback-srvip loopback
         ip address 32.32.32.30 255.255.255.255 srp-activate
      exit
      subscriber default
      exit
      aaa group default
      exit
      wsg-service abc
         deployment-mode site-to-site
         ip access-group one
         bind address 32.32.32.30 crypto-template foo
      exit
      ip route 55.55.33.0 255.255.255.0 34.34.34.100 ike
      ip route 66.66.66.0 255.255.255.0 78.78.78.100 clear

      ip rri-route network-mode L2 78.78.78.50 next-hop 78.78.78.34
interface clear
      ip rri-route network-mode L2 78.78.78.50 next-hop 78.78.78.34
interface clear
   exit
   context srp
      service-redundancy-protocol
         chassis-mode primary
         hello-interval 3
         configuration interval 60
         dead interval 15
         checkpoint session duration non-ims-session 30
         route-modifier threshold 10
         priority 10
         monitor hsrp interface GigabitEthernet0/0/0/5 afi-type IPv4
hsrp-group 3
         peer-ip-address 88.88.88.33
         bind address 86.86.86.33
      exit
      interface icsr
         ip address 86.86.86.33 255.255.255.0
      exit
```

```
      subscriber default
      exit
      aaa group default
      exit
      ip route 88.88.88.0 255.255.255.0 86.86.86.23 icsr
   exit
   connectedapps
      sess-userid cisco
      sess-passwd encrypted password <encrypted_password>
      sess-name intraCh
      sess-ip-address 192.168.120.1
      rri-mode S2S
      ha-chassis-mode intra
      ha-network-mode L2
      ca-certificate-name cert_name
      activate
   exit
   wsg-lookup
      priority 1 source-netmask 28 destination-netmask 28
      priority 2 source-netmask 32 destination-netmask 32
      priority 3 source-netmask 16 destination-netmask 16
      priority 4 source-netmask 24 destination-netmask 24
   exit
   port ethernet 1/10
      no shutdown
      bind interface ike wsg
   exit
   port ethernet 1/11
      no shutdown
      bind interface clear wsg
      vlan 12
    vlan 12
      description "ICSR"
      no shutdown
      bind interface icsr srp
     #exit
  #exit
end
```