Sample Basic WSG-Service Configuration

This chapter provides a sample basic wsg-service configuration that enables SecGW functionality on an ASR 9000 VSM CPU.

WSG Context (StarOS)

```
config
  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 key foo
      authentication remote pre-shared-key key foo
      ikev2-ikesa transform-set list ikesa-foo
      identity local id-type ip-addr id 33.33.33.3
      peer network 55.55.33.30 mask 255.255.255.255
      natt

    wsg-service abc
      deployment-mode site-to-site
      ip access-group one
      bind address 33.33.33.30 crypto-template foo
    exit

    interface ike
      ip address 33.33.33.33 255.255.255.0
    exit

    interface loopback-ike loopback
      ip address 33.33.33.30 255.255.255.255 srp-activate
    exit
```

Clear Traffic Interface – Primary

```
interface clear
ip address 77.77.77.33 255.255.255.0

interface loopback-clear loopback
ip address 77.77.77.254 255.255.255.255 srp-activate
exit
```

Clear Traffic Interface – Backup

```
interface clear
ip address 77.77.77.34 255.255.255.0

interface loopback-clear loopback
ip address 77.77.77.254 255.255.255.255 srp-activate
exit
```

SRP Context (StarOS)

SRP – Primary Chassis

```
context srp
service-redundancy-protocol
chassis-mode backup
checkpoint session duration 30
route-modifier threshold 10
priority 10
peer-ip-address 35.35.35.37
bind address 35.35.35.36
monitor hsrp interface GigabitEthernet0/1/0/3 afi-type ipv4 group 2
exit
interface icsr
ip address 35.35.35.36 255.255.255.0
```

SRP – Backup Chassis

```
context srp
service-redundancy-protocol
chassis-mode backup
checkpoint session duration 30
```

```
route-modifier threshold 10
priority 10
peer-ip-address 35.35.35.36
bind address 35.35.35.37
monitor hsrp interface GigabitEthernet0/2/0/2 afi-type ipv4 group 2
exit
interface icsr
ip address 35.35.35.37 255.255.255.0
```

HSRP Configuration (IOS-XR)

Primary Chassis

```
router hsrp
  interface GigabitEthernet0/1/0/3
    address-family ipv4
      hsrp 2
        priority 110
        address 10.10.10.100
       |
      |
     |
    |
```

Backup Chassis

```
router hsrp
  interface GigabitEthernet0/2/0/2
    address-family ipv4
      hsrp 2
        priority 100
        address 10.10.10.100
       |
      |
     |
    |
```

Port Configuration (StarOS)

```
config
  port ethernet 1/10
    no shutdown
    bind interface ike wsg

  port ethernet 1/11
    no shutdown
    bind interface clear wsg
  vlan 12
   description "ICSR"
   no shutdown
   bind interface icsr srp
  #exit
#exit
```

oneP (Connected Apps) Communication

oneP Configuration (IOS-XR)

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

config
 lpts pifib hardware police flow ONEPK rate 2000
 commit
```

Session Establishment ASR 9000 SecGW

Below are the steps for connectedapps session establishment between ASR 9000 XR and secgw VM.

1. Configure crypto ca trustpoint onep-tp configurations in ASR9000, refer ASR 9000 RSP Configuration (IOS-XR)
2. Configure ' onep' configurations in ASR9000, refer ASR 9000 RSP Configuration (IOS-XR)
3. Copy and Paste the contents of the generated CA certificate after executing the CLI ' crypto ca authenticate onep-tp' in ASR 9000
4. Configure the XR Server's 'Certificate request' with the CLI ' crypto ca enroll onep-tp'. Below is the snippet collected during certificate request generation,

   ```
   Password: (cisco)

   Re-enter Password:  (cisco)

   % The subject name in the certificate will include: CN=ASR9K-8.cisco.com

   % The subject name in the certificate will include: ASR9K-8.cisco.com

   % Include the router serial number in the subject name? [yes/no]: yes

   % The serial number in the certificate will be: f15db8e1

   % Include an IP address in the subject name? [yes/no]: yes

   Enter IP Address[] 192.168.122.1     (This should be RSP address used for establishing
    the connected apps)

       Fingerprint:  44383334 43413532 30324435 35393534

   Display Certificate Request to terminal? [yes/no]: yes Certificate Request follows:

   # --License--
   ```

```
---End - This line not part of the certificate request--- Redisplay enrollment request?
 [yes/no]: no
```

5. Now collect the generated 'certificate request' and get it signed by the Certificate Authority (CA)
6. Import the signed certificate in ASR90000 with the CLI ' crypto ca import onep-tp certificate' (copy paste the signed certificate here)
7. Can check the certificate status in ASR90000 with the show CLI ' show crypto ca certificates'
8. Now load the ca-cert in secgw as well and map the 'ca-cert' name under 'connectedapps' configuration, refer Configuring a Client CA Session
9. Configure 'Activate' under secgw 'connectedapps' to initiate the connectedapps session establishment request.
10. Enable debug for ' connectedapps' in secgw to monitor the process (optional)

CA Client Session (StarOS)

```
configure
   connectedapps
      ha-chassis-mode inter
      ha-network-mode L2
      rri-mode both
      sess-ip-address 30.30.30.13
      sess-name wsg
      sess-passwd password cisco123
      sess-userid vsm01
```