The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB’s public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED “AS IS” WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Cisco and the Cisco Logo are trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and other countries. A listing of Cisco's trademarks can be found at www.cisco.com/go/trademarks. Third party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company.

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

SecGW Administration Guide, StarOS Release 18

© 2015 Cisco Systems, Inc. All rights reserved.
## CONTENTS

### About this Guide
- Conventions Used ....................................................... viii
- Documents and Resources .............................................. ix
- Related Common Documentation .................................... ix
- ASR 9000 Documentation ............................................... ix
- Obtaining Cisco Documentation ...................................... ix
- Contacting Customer Support ....................................... x

### Security Gateway Overview
- Product Overview ....................................................... 11
- ASR 9000 VSM ............................................................ 12
- VSM Resource Mapping to VPC-VSM VMs ....................... 14
- VPC-VSM ................................................................. 16
- SecGW Application ....................................................... 16
  - Key Features .......................................................... 16
  - IPSec Capabilities .................................................. 17
  - Reverse Route Injection ........................................... 18
  - SecGW Management ................................................ 18
- oneP Communication .................................................. 18
- ASR 9000 VSM IPSec High Availability ........................... 19
  - Process Recovery .................................................... 19
  - VSM-to-VSM ICSR 1:1 Redundancy ............................... 19
  - Chassis-to-Chassis ICSR Redundancy ............................ 20
  - HA Configuration .................................................... 20
- Network Deployment ................................................... 21
  - Remote Access Tunnels ............................................. 21
  - Site-to-Site Tunnels ................................................. 21
- Packet Flow .............................................................. 22
- Standards .................................................................. 24
  - Compliant .............................................................. 24
  - Non-compliant ......................................................... 24
  - Standards ............................................................... 24
  - Hashed Message Authentication Codes ......................... 24
  - Encryption Algorithms ............................................. 25
  - Certificates ........................................................... 25

### SecGW Service Creation
- Prerequisites .............................................................. 27
- VPC-VSM Installation ................................................... 28
- Network Interfaces ...................................................... 28
- SecGW Configuration Sequence ..................................... 29
- Crypto Templates ........................................................ 30
- Access Control Lists ................................................... 34
- WSG Service Configuration ........................................... 35
- WSG Service .............................................................. 35
  - Bind Address and Crypto Template .............................. 35
About this Guide

This preface defines the Security Gateway, the organization of this guide and its document conventions.

The Security Gateway (SecGW) is a StarOS product that runs in a VPC-VSM instance as a StarOS virtual machine (VM) on a Virtualized Services Module (VSM) in a Cisco ASR 9000 router.

This guide assumes that Virtualized Packet Core for VSM (VPC-VSM) instances are already installed and running on one or more VSMs. There are four CPUs on the VSM, each capable of running a single VPC-VSM instance. This guide describes how to create a StarOS Wireless Security Gateway (WSG) service that enables SecGW IPSec functions on each VPC-VSM instance.

To complete the SecGW configuration process you must also have at hand the following user documentation:

- *VPC-VSM System Administration Guide*
- *IPSec Reference*
# Conventions Used

The following tables describe the conventions used throughout this documentation.

## Icon

<table>
<thead>
<tr>
<th>Notice Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Information Note</td>
<td>Provides information about important features or instructions.</td>
</tr>
<tr>
<td>Caution</td>
<td>Alerts you of potential damage to a program, device, or system.</td>
</tr>
<tr>
<td>Warning</td>
<td>Alerts you of potential personal injury or fatality. May also alert you of potential electrical hazards.</td>
</tr>
</tbody>
</table>

## Typeface Conventions

<table>
<thead>
<tr>
<th>Description</th>
<th>Typeface</th>
</tr>
</thead>
<tbody>
<tr>
<td>Text represented as a screen display</td>
<td>This typeface represents displays that appear on your terminal screen, for example: Login:</td>
</tr>
<tr>
<td>Text represented as commands</td>
<td>This typeface represents commands that you enter, for example: show ip access-list</td>
</tr>
<tr>
<td>Text represented as a command variable</td>
<td>This typeface represents a variable that is part of a command, for example: show card slot_number slot_number is a variable representing the desired chassis slot number.</td>
</tr>
<tr>
<td>Text represented as menu or sub-menu names</td>
<td>This typeface represents menus and sub-menus that you access within a software application, for example: Click the File menu, then click New</td>
</tr>
</tbody>
</table>
Documents and Resources

Related Common Documentation

The most up-to-date information for this product is available in the Release Notes provided with each product release. The following user documents are available:

- **AAA Interface Administration Reference**
- **Command Line Interface Reference**
- **GTPP Interface Administration Reference**
- **IPSec Reference**
- **VPC-VSM System Administration Guide**
- **Release Change Reference**
- **Statistics and Counters Reference**
- **Thresholding Configuration Guide**

ASR 9000 Documentation

The following user documents describe how to install and configure the ASR 9000 Virtualized Service Module (VSM) via IOS-XR.

- **Cisco ASR 9000 Series Aggregated Services Router VSM (Virtualized Service Module) Line Card Installation Guide (OL-30446-01) [available March, 2014]**
- **Cisco ASR 9000 Series Aggregation Services Router Interface and Hardware Component Configuration Guide – Configuring Virtual Services on the Cisco ASR 9000 Series Router**
- **Cisco ASR 9000 Series Aggregation Services Router Carrier Grade IPv6 (CGv6) Configuration Guide – Carrier Grade IPv6 over Virtualized Services Module (VSM)**
- **Cisco ASR 9000 Series Aggregation Services Router IP Addresses and Services Configuration Guide**

Obtaining Cisco Documentation

The most current Cisco documentation is available on the following website:

http://www.cisco.com/cisco/web/psa/default.html

Use the following URL to access the StarOS (ASR 5000 Series) documentation:


Use the following URL to access the ASR 9000 documentation:

Contacting Customer Support

Use the information in this section to contact customer support.

Refer to the support area of http://www.cisco.com for up-to-date product documentation or to submit a service request. A valid username and password are required to access this site. Please contact your Cisco sales or service representative for additional information.
Chapter 1
Security Gateway Overview

This chapter contains general overview information about the Security Gateway (SecGW) running on an ASR 9000 Virtualized Service Module (VSM) as a VPC-VSM instance.

The following topics are discussed in this chapter:

- Product Overview
- ASR 9000 VSM IPSec High Availability
- Network Deployment
- Packet Flow
- Supported Standards
Product Overview

The SecGW is a high-density IP Security (IPSec) gateway for mobile wireless carrier networks. It is typically used to secure backhaul traffic between the Radio Access Network (RAN) and the operator core network.

IPSec is an open standards set that provides confidentiality, integrity, and authentication for data between IP layer peers. The SecGW uses IPSec-protected tunnels to connect outside endpoints. SecGW implements the parts of IKE/IPSec required for its role in mobile networks.

The SecGW is enabled as a Wireless Security Gateway (WSG) service in a StarOS instance running in a virtual machine on a Virtualized Services Module (VSM) in an ASR 9000.

The following types of LTE traffic may be carried over encrypted IPSec tunnels in the Un-trusted access domain:

- S1-C and S1-U: Control and User Traffic between eNodeB and EPC
- X2-C and X2-U: Control and User Traffic between eNodeBs during Handoff
- SPs typically carry only Control Traffic, however there exists a case for carrying non-Internet User traffic over secured tunnels

![SecGW Implementation](image)

ASR 9000 VSM

SecGW is enabled via a StarOS image running in a virtualized environment supported on the ASR 9000 VSM. StarOS runs in four hypervisor-initiated virtual machines (one per CPU) on the VSM.

The VSM is a service blade for the ASR 9000 router that supports multiple services and applications running simultaneously on top of a virtualized hardware environment.

The VSM supports the following major hardware components:

- (4) CPUs [20 cores per socket]
- (4) hardware crypto devices
- (1) Data Path Switch supporting (12) 10 Gigabit Ethernet (GbE) devices
- (2) NPUs
The ASR 9000 services architecture encompasses how the platform interfaces with the services independent of where the service is actually instantiated. It provides a common control plane, management plane and data plane infrastructure such that a consistent end user experience is provided whether the service is running on a service blade, on the RSP, on an attached appliance or server, or even running inline in the router.

The ASR 9000 platform supports the following functions:

- Enables services via IOS-XR
- Provides platform management via CLI and XML for:
  - Service parameter specification
  - Validation of service package including licenses
  - Service instantiation with associated parameters
  - Service health monitoring
  - Service termination, re-start and upgrades
- Decouples configuration of the WSG service from the service creation infrastructure
- Provides a set of templates for service parameters
- Interfaces with the hypervisor (Virtual Machine Manager client) to setup the StarOS WSG service on multiple virtual machines (VMs)
The figure below shows the relationship between IOS-XR running on the ASR 9000 and StarOS running on the VSM.

**Figure 3.** IOS-XR and VSM

![Diagram showing the relationship between IOS-XR and VSM](image)

The 10GE interfaces on the SecGW virtual machines are visible as 10GbE interfaces on the ASR 9000. The ASR 9000 line card forwards IP traffic to VSM 10GbE ports.

### VSM Resource Mapping to VPC-VSM VMs

There are four CPU sockets on the VSM. Each CPU supports multiple cores. A VPC-VSM instance uses multiple virtual CPUs (vCPUs) consisting of available cores for its virtual machine.

Each CPU socket is associated with a Crypto engine. PCI Ports are also assigned to accept traffic from the ASR 9000 line cards.

The table below shows how resources are assigned among the four CPUs on the VSM.

**Table 1. Resource Assignments for VSM CPUs**

<table>
<thead>
<tr>
<th>CPU</th>
<th>Available Cores</th>
<th>Crypto Device</th>
<th>PCI Port ID</th>
<th>VM</th>
<th>vCPUs</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>16 (2–9, 42–49)</td>
<td>04:00.0</td>
<td>00.0.0</td>
<td>VM1</td>
<td>16</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>00.1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>1</td>
<td>18 (11–19, 51–59)</td>
<td>45:00.0</td>
<td>42:0.0</td>
<td>VM2</td>
<td>16</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>42.0.1</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Only twelve PCI ports can be mapped to ASR 9000 line card traffic. The table below shows how the interfaces are distributed.

Table 2. PCI Port Mapping

<table>
<thead>
<tr>
<th>PCI Port ID</th>
<th>CPU</th>
<th>ASR 9000 TenG</th>
<th>VPC Slot/Port</th>
<th>VM</th>
<th>Application IF</th>
</tr>
</thead>
<tbody>
<tr>
<td>00:0.0</td>
<td>0</td>
<td>TenGx/y/z/0</td>
<td>1/10</td>
<td>VM1</td>
<td>Uplink</td>
</tr>
<tr>
<td>00:0.1</td>
<td></td>
<td>TenGx/y/z/1</td>
<td>1/11</td>
<td></td>
<td>Downlink</td>
</tr>
<tr>
<td>42:0.0</td>
<td>1</td>
<td>TenGx/y/z/2</td>
<td>1/1</td>
<td></td>
<td>Management</td>
</tr>
<tr>
<td>42.0.0</td>
<td></td>
<td>TenGx/y/z/3</td>
<td>1/10</td>
<td>VM2</td>
<td>Uplink</td>
</tr>
<tr>
<td>48.0.0</td>
<td></td>
<td>TenGx/y/z/4</td>
<td>1/11</td>
<td></td>
<td>Downlink</td>
</tr>
<tr>
<td>48.0.1</td>
<td></td>
<td>TenGx/y/z/5</td>
<td>1/1</td>
<td></td>
<td>Management</td>
</tr>
<tr>
<td>82:0.0</td>
<td>2</td>
<td>TenGx/y/z/6</td>
<td>1/10</td>
<td>VM3</td>
<td>Uplink</td>
</tr>
<tr>
<td>82:0.1</td>
<td></td>
<td>TenGx/y/z/7</td>
<td>1/11</td>
<td></td>
<td>Downlink</td>
</tr>
<tr>
<td>88:0.0</td>
<td></td>
<td>TenGx/y/z/8</td>
<td>1/1</td>
<td></td>
<td>Management</td>
</tr>
<tr>
<td>88:0.1</td>
<td></td>
<td>—</td>
<td>—</td>
<td></td>
<td>Unused</td>
</tr>
<tr>
<td>C2:0.0</td>
<td>3</td>
<td>TenGx/y/z/9</td>
<td>1/10</td>
<td>VM4</td>
<td>Uplink</td>
</tr>
<tr>
<td>C2:0.1</td>
<td></td>
<td>TenGx/y/z/10</td>
<td>1/11</td>
<td></td>
<td>Downlink</td>
</tr>
<tr>
<td>C8:0.0</td>
<td></td>
<td>TenGx/y/z/11</td>
<td>1/1</td>
<td></td>
<td>Management</td>
</tr>
<tr>
<td>C8:0.1</td>
<td></td>
<td>—</td>
<td>—</td>
<td></td>
<td>Unused</td>
</tr>
</tbody>
</table>

- For all VMs except VM1, the NICs are allocated from the corresponding socket. But in VM1, the third NIC (42:0.0) is picked from a different socket. To achieve maximum throughput, that NIC is used as the management port and the other two are used for the service.
To make the interface-to-port mapping symmetric across all the VMs, the third NIC is always used as the management port.

**VPC-VSM**

Virtualized Packet Core for VSM (VPC-VSM) consists of the set virtualized mobility functions that implement mobility specific services and applications within the core of the network. VPC-VSM is essentially StarOS running within a Virtual Machine (VM).

VPC-VSM only interacts with supported hypervisors. It has little or no knowledge of physical devices.

Each VPC-VSM VM takes on the roles of an entire StarOS system. The only interfaces exposed outside the VM are those for external management and service traffic. Each VM is managed independently.

Each VPC-VSM VM performs the following StarOS functions:

- Controller tasks
- Out-of-band management for CLI and Logging
- Local context (management)
- NPU simulation via fastpath and slowpath
- Non-local context (subscriber traffic)
- Crypto processing (IPSec)

For a complete description of VPC-VSM functionality, refer to the *VPC-VSM System Administration Guide*.

**Important:** Up to four instances of VPC-VSM can run on an ASR 9000 VSM. Each VSM CPU supports only one VPC-VSM instance. VSM resources are allocated to each SecGW VM; no other application VM is supported on any VSM CPU. vNICs must be passed to the SecGW VMs from RSP.

**SecGW Application**

The StarOS-based Security Gateway (SecGW) application is a solution for Remote-Access (RAS) and Site-to-Site (S2S) mobile network environments. It is implemented via StarOS as a WSG (Wireless Security Gateway) service that leverages the IPSec features supported by StarOS.

SecGW delivers the S2S IP Encryption capabilities required in UMTS/HSPA and LTE 3GPP LTE/SAE network architectures.

For complete descriptions of supported IPSec features, see the *IPSec Reference*.

**Important:** The SecGW is a licensed StarOS feature. A separate license is required for each VPC-VSM instance and SecGW. Contact your Cisco account representative for detailed information on specific licensing requirements.

**Key Features**

The following are key features of the SecGW product:

- Functions in a virtualized environment on one or more VSM blades in an ASR9000
• Supports IKEv2.
• Supports DES, 3DES, AES and NULL Encryption algorithms, and MD5, SHA1/2 and AES-XCBC Hash algorithms.
• Provides mechanisms for High Availability both within and outside of the ASR 9000 chassis.
• IPv6 support encompasses Inner-Outer pairs – v6-v6, v6-v4, v4-v6, v4-v4
• Allows dynamic provisioning of IPSec configuration when a new SecGW is instantiated on the router.

Each of the four SecGWs on a VSM must be configured separately.

Load balancing has not been implemented for the SecGWs; incoming calls will not be automatically distributed across the four SecGWs on a VSM. A workaround is to use VLANs for load balancing. The public side interface of each SecGW can be configured for a separate VLAN. Calls from multiple peers are routed to the same IP address via a different VLAN to distribute the traffic load.

**IPSec Capabilities**

The following IPSec features are supported by StarOS for implementation in an SecGW application:

• Anti Replay
• Multiple Child SA (MCSA)
• Certificate Management Protocol (CMPv2)
• Session Recovery/Interchassis Session Recovery for both RAS and S2S
• Support for IKE ID Type
• PSK support with up to 255 octets
• Online Certificate Status Protocol (OCSP)
• Reverse DNS Lookup for Peer IP in show Commands
• Blacklist/Whitelist by IDi
• Rekey Traffic Overlap
• CRL fetching with LDAPv3
• Sequence Number based Rekey
• IKE Call Admission Control (CAC)
• PSK Support for up to 1000 Remote Secrets
• Certificate Chaining
• RFC 5996 Compliance
• Duplicate Session Detection
• Extended Sequence Number
• Security Gateway as IKE Initiator
Reverse Route Injection

SecGW also supports Reverse Route Injection (RRI). RRI injects routes in the reverse direction onto the ASR 9000 VSM so that clear traffic can be routed to the correct interface on the target VPC-VSM. For additional information, see the Reverse Route Injection chapter.

SecGW Management

Each SecGW instance is configured individually via its Management port. However, the Cisco Prime network management tool can be used to configure and manage individual SecGW instances.

A common or default configurations can be captured as “templates” in Cisco Prime which are then applied to each SecGW instance or all SecGW instances in the network.

For additional information on the Cisco Prime Mobility suite, contact your Cisco account representative.

Alternatively an operator can create a StarOS configuration file on the first gateway. The resulting configuration file can then be copied and edited offline with different parameters. The edited configuration file is then copied to the flash drive of the second SecGW. The process is repeated until all four SecGWs have been initially configured.

Subsequent changes made to the configuration of each SecGW must be saved to the local configuration file. For security and recovery the individual configuration files should then be saved off the VMS to a target network destination.

For additional information, see the VPC-VSM System Administration Guide.

oneP Communication

Each SecGW creates a oneP session with the ASR 9000 for route insertions, policy creation and flow creation. For additional information, refer to the oneP Communication chapter.
ASR 9000 VSM IPSec High Availability

This section briefly describes the IPSec High Availability (HA) capabilities for VSM service cards within an ASR 9000. For this release, the ASR 9000 supports the following levels of High Availability:

- Process Recovery
- VSM-to-VSM ICSR 1:1 Redundancy
- Chassis-to-Chassis ICSR Redundancy

HA functions are triggered for the following events:

- Route Processor (RP) failure
- Virtual Machine (VM) failure
- VSM failure
- Link failure

**Important:** The IPSec HA architecture is based on StarOS Interchassis Session Recovery (ICSR). For a complete description of ICSR and its configuration requirements, see the VPC-VSM System Administration Guide.

Process Recovery

The process recovery feature stores backup Security Association (SA) data in an AAA manager task. This manager runs on the SecGW where the recoverable tasks are located.

![Process Recovery Diagram](image)

VSM-to-VSM ICSR 1:1 Redundancy

In this redundancy scenario, Interchassis Session Recovery ICSR utilizes the Service Redundancy Protocol (SRP) implemented between two VSMs running separate instances of VPC-VSM/SecGW in the same ASR 9000 chassis.
VSM card status data is exchanged between VPN managers on active and standby VSMs via SRP. SA data is also exchanged via SRP.

The *VPC-VSM System Administration Guide* fully describes ICSR configuration procedures.

**Chassis-to-Chassis ICSR Redundancy**

SecGW HA supports hot standby redundancy between two VSMs in different ASR 9000 chassis. The Standby VSM is ready to become active once a switchover is triggered. SA re-negotiation is not required and traffic loss is minimal.

For additional information, see the *Reverse Route Injection (RRI)* chapter.

**HA Configuration**

HA employs ConnectedApps (CA) communication between the client running on the wsg-service VM and IOS-XR running on the ASR 9000.

StarOS *connectedapps* commands configure the CA client parameters, including those associated with HA mode. For additional information, refer to the *oneP Communication* chapter.
Network Deployment

SecGW supports the following network deployment scenarios:

- Remote Access (RAS) Tunnels
- Site-to-Site (S2S) Tunnels

Remote Access Tunnels

In a RAS scenario, a remote host negotiates a child SA with the SecGW and sends traffic inside the child SA that belongs to a single IP address inside the remote host. This is the inner IP address of the child SA. The outer IP address is the public IP address of the remote host. The addresses on the trusted network behind the SecGW to which the host talks could be a single IP or a network.

The remote host could set up multiple child SAs to the SecGW. This is still a remote access scenario, as long as a unique single IP address is used for the inner IP of each child SA. The uniqueness of the inner IP must be maintained across all child SAs of all remote hosts talking to the SecGW.

The traffic that is carried inside the child SA is defined during the creation of the child SA, using the traffic selector (TS) field of the IKE message.

![RAS Tunnel](image)

Site-to-Site Tunnels

In an S2S scenario, the remote peer sets up a child SA to the SecGW. The source of the traffic inside the child SA can be from multiple IP addresses on the remote peer's side. As in the remote access scenario, the addresses on the trusted network behind the SecGW can be a single IP or a network.

In this scenario also, the remote peer can setup multiple child SAs to the SecGW.

For S2S tunnels established using the WSG service, the TSi and TSr contain protocol as well as source and destination IP ranges.

![S2S Tunnel](image)
Packet Flow

The figures below indicate traffic packet flows to and from the SecGW.

Figure 7. SecGW Packet Flow – RAS
Figure 8. SecGW Packet Flow – S2S Scenario
Standards

Compliant

- RFC 1853 – IP in IP Tunneling
- RFC 2401 – Security Architecture for the Internet Protocol
- RFC 2402 – IP Authentication Header
- RFC 2406 – IP Encapsulating Security Payload (ESP)
- RFC 2407 – The Internet IP Security Domain of Interpretation for ISAKMP
- RFC 2408 – Internet Security Association and Key Management Protocol (ISAKMP)
- RFC 2409 – The Internet Key Exchange (IKE)
- RFC 2410 – Internet X.509 Public Key Infrastructure Certificate Management Protocol (CMP)
- RFC 3280 – Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile
- RFC 3554 – On the Use of Stream Control Transmission Protocol (SCTP) with IPsec [Partially compliant, ID_LIST is not supported.]
- RFC 4306 – Internet Key Exchange (IKEv2) Protocol
- RFC 4718 – IKEv2 Clarifications and Implementation Guidelines
- RFC 5996 – Internet Key Exchange Protocol Version 2 (IKEv2)
- Hashed Message Authentication Codes:
  - AES 96
  - MD5
  - SHA1/SHA2
- X.509 Certificate Support – maximum key size = 2048

Non-compliant

Standards

- RFC 3173 – IP Payload Compression Protocol (IPComp)
- RFC 5723 – Internet Key Exchange Protocol Version 2 (IKEv2) Session Resumption
- RFC 5840 – Wrapped Encapsulating Security Payload (ESP) for Traffic Visibility
- RFC 5856 – Integration of Robust Header Compression over IPsec Security Associations

Hashed Message Authentication Codes

- HMAC AES 128 GMAC
• HMAC AES 192 GMAC
• HMAC AES 256 GMAC

**Encryption Algorithms**

• Diffie Hellman (DH) Group 19
• DH Group 20
• DH Group 21
• DH Group 24

**Certificates**

• Digital Signature Algorithm (DSA)
• xAuth
Chapter 2
SecGW Service Creation

This chapter describes the requirements and procedures for enabling the WSG (Wireless Security Gateway) service within StarOS. Enabling this service creates the SecGW.

This chapter discusses the following topics:

- Prerequisites
- SecGW Configuration Sequence
- Crypto Templates
- Access Control Lists
- WSG Service Configuration
- IPSec Configuration
- Multiple SecGW Configurations per VSM
Prerequisites

This section describes the requirements that must be met prior to configuring the SecGW.

VPC-VSM Installation

VPC-VSM must be running in a virtual machine on a VSM CPU within the ASR 9000 chassis. This guide does not describe the installation process. Refer to other ASR 9000 documentation for detailed installation instructions.

The StarOS command line interface (CLI) for each VPC-VSM instance should be accessible via a remote access management port that is defined during the installation process. Refer to the VPC-VSM System Administration Guide for additional information on setting primary and secondary IP addresses for StarOS management ports. Alternatively, the StarOS CLI can be accessed via a hypervisor vConsole port.

For intrachassis and interchassis IPSec High Availability (HA) deployments, VPC-VSM must be installed on VSMs in the ASR 9000 chassis. StarOS Interchassis Session Recovery (ICSR) must also be enabled. Refer to the VPC-VSM System Administration Guide for ICSR installation and configuration information. For additional configuration requirements, see the High Availability for RRI section in the Reverse Route Injection chapter of this guide.

Refer to ASR 9000 documentation for additional information on HA active-standby configuration.

Network Interfaces

You will need to know the addressing information for all external interfaces to StarOS. The list of addresses is included but not limited to:

- WSG service (endpoints, access groups)
- VLANs
- SNMP
- DHCP
SecGW Configuration Sequence

The configuration sequence for enabling an SecGW is as follows:

- Create a crypto template with the desired IPSec functions. See Crypto Templates.
- Create Access Control Lists. See Access Control Lists.
- Enable and configure one or more WSG services. See WSG Service Configuration.
- Configure required IPSec features. See IPSec Configuration.

For additional information, see the sample configurations provided in this guide.

**Important:** SecGW (WSG service) must be separately enabled and configured on each VPC-VSM instance. There are four CPUs on the VSM; each CPU runs a separate instance of VPC-VSM.
Crypto Templates

The StarOS CLI Crypto Template Configuration Mode is used to configure an IKEv2 IPSec policy. It includes most of the IPSec parameters and IKEv2 dynamic parameters for cryptographic and authentication algorithms. A security gateway service will not function without a configured crypto template. Only one crypto template can be configured per service.

A crypto template requires the configuration of the following parameters:

- **allow-cert-enc cert-hash-url** – Enables support for certificate enclosure type other than default.
- **allow-custom-fqdn-idr** – Allows non-standard FQDN (Fully Qualified Domain Name) strings in the IDr (Identification - Responder) payload of IKE_AUTH messages received from the UE with the payload type as FQDN.
- **authentication** – Configures the gateway and subscriber authentication methods to be used by this crypto template.
- **blacklist** – Enables use of a blacklist file
- **ca-certificate list** – Binds an X.509 Certificate Authority (CA) root certificate to a crypto template.
- **ca-crl list** – Binds one or more Certificate Authority-Certificate Revocation Lists (CA-CRLs) to this crypto template.
- **certificate** – Binds a single X.509 trusted certificate to a crypto template.
- **control-dont-fragment** – Controls the Don't Fragment (DF) bit in the outer IP header of the IPSec tunnel data packet.
- **dns-handling** – Adds a custom option to define the ways a DNS address is returned based on proscribed circumstances described below.
- **dos cookie-challenge notify-payload** – Configures the cookie challenge parameters for IKEv2 INFO Exchange notify payloads for the given crypto template.
- **identity local** – Configures the identity of the local IPSec Client (IKE ID).
- **ikev2-ikesa** – Configures parameters for the IKEv2 IKE Security Associations within this crypto template.
- **keepalive** – Configures keepalive or dead peer detection for security associations used within this crypto template.
- **max-childsa** – Defines a soft limit for the number of child Security Associations (SAs) per IKEv2 policy.
- **nai** – Configures the Network Access Identifier (NAI) parameters to be used for the crypto template IDr (recipient's identity).
- **natt** – Configures Network Address Translation - Traversal (NAT-T) for all security associations associated with this crypto template. This feature is disabled by default.
- **ocsp** – Enables Online Certificate Store Protocol (OCSP) requests from the crypto map/template.
- **payload** – Creates a new, or specifies an existing, crypto template payload and enters the Crypto Template Payload Configuration Mode.
- **peer network** – Configures a list of allowed peer addresses on this crypto template.
- **remote-secret-list** – Configures Remote Secret List.
- **whitelist** – Enables use of a whitelist file.

You must create a crypto template before creating the WSG service that enables the SecGW.
**Important:** Refer to the *IPSec Reference* for comprehensive information regarding the creation of crypto templates.

A sample crypto template is shown below. It represents the output of the `show crypto template tag template_name` command.

```
Map Name: cryptotmplt01

-----------------------------------------
Map Status: Complete

Crypto Map Type: IPSEC IKEv2 Template

IKE SA Transform 1/1

Transform Set: ikesa-cryptotmplt01
  Encryption Cipher: aes-chc-128
  Pseudo Random Function: sha
  Hashed Message Authentication Code: sha1-96
  Diffie-Hellman Group: 2
IKE SA Rekey: Disabled
Blacklist/Whitelist : None

OCSP Status: : Disabled
OCSP Nounce Status : Enabled

NAI: 99.99.99.30

Remote-secret-list: <not configured>

Authentication Local:
```

---

SecGW Administration Guide, StarOS Release 18
Phase 1 - Pre-Shared Key (Size = 3)

Self-certificate Validation: Disabled

IPSec SA Payload 1/1 (Generic)
Name : cryptotmplt01-sa0
Payload Local
Protocol 255 Port 0-0 Address Range 67.67.0.1-67.67.0.1
Payload Remote
Protocol 255 Port 0-0 Address Range 45.45.0.1-45.45.0.1
IPSec SA Transform 1/1
Transform Set: tselsa-cryptotmplt01
Protocol: esp
Encryption Cipher: aes-cbc-128
Hashed Message Authentication Code: sha1-96
Diffie-Hellman Group: none
IPSec SA Rekey: Enabled

Dead Peer Detection: Disabled

Maximum CHILD_SA: 2 Overload Action: Ignore

DOS Cookie Challenge: Disabled
Dont Fragment: Copy bit from inner header

Local Gateway: Not Set
Remote Gateway: Not Set
Access Control Lists

IP access lists, commonly known as access control lists (ACLs), control the flow of packets into and out of the service. They are configured on a per-context basis and consist of “rules” (ACL rules) or filters that control the action taken on packets that match the filter criteria.

Separate ACLs may be created for IPv4 and IPv6 access routes.

WSG Service uses ACLs to specify traffic selectors for site-to-site tunnels. The wsg-service supports multiple access-lists.

You separately define ACLs outside of the wsg-service, at the context level. For information on creating and configuring ACLs, see the following:

- *Access Control Lists* chapter in the *VPC-VSM System Administration Guide*
- *ACL Configuration Mode Commands* chapter of the *Command Line Interface Reference*.
WSG Service Configuration

Configuring WSG Service enables SecGW functionality. The general configuration sequence includes:

- WSG Service
- Lookup Priority
- show Commands
- WSG Bulk Statistics

Important: You must be logged into the StarOS CLI of a VPC-VSM instance to execute the commands described below.

Important: For complete information on CLI commands described below, see the Command Line Interface Reference.

WSG Service

This procedure enables WSG service and moves to WSG Configuration mode. The Wireless Security Gateway Configuration Mode is used to define the operating parameters for IPSec-based access control and handling of Encapsulating Security Payload (ESP) packets. Up to 25 WSG services can be configured per StarOS instance.

Execute the following command sequence to move to the Wireless Security Gateway Configuration Mode:

```
cfg
  context context_name
  wsg-service service_name
```

For additional information, see the WSG-Service Configuration Mode Commands chapter of the Command Line Interface Reference.

Bind Address and Crypto Template

In the WSG Configuration mode, the following command sequence binds the WSG service to the specified IPv4 or IPv6 address and crypto template.

```
binding address ip_address crypto-template template_name
```

The `ip_address` may be in IPv4 dotted-decimal or IPv6 colon-separated hexadecimal notation.

The `template_name` specifies an existing crypto template as an alphanumeric string of 0 through 127 characters.
Deployment Mode

A given instance of the WSG service can either support Remote Access tunnels or Site-to-Site tunnels. In the WSG Configuration mode, the following command sequence specifies the desired deployment mode.

```
deployment-mode { remote-access | site-to-site }
```

**Important:** There is no default deployment mode. You must configure the deployment mode as either remote-access or site-to-site before binding the service. Failure to specify a deployment mode will generate an error message when attempting to bind the address.

Access List

A WSG service that supports site-to-site tunnels should bind to an access list that specifies a single IP address for the destination IP; the subnet should be “32” for IPv4 and “128” for IPv6.

For the site-to-site scenario, the destination can be a subnet.

In the WSG Configuration mode, the following command sequence specifies the desired IPv4 access groups or address pools:

```
ip { access-group acl_list_name | address { alloc-method { dhcp-proxy | local } | pool name pool_name
```

In the WSG Configuration mode, the following command sequence specifies the desired IPv6 access groups or prefix pools:

```
ipv6 { access-group acl_list_name | address prefix-pool pool_name
```

**Important:** Remote Access (RA) tunnels require address pools that can be specified under the service.

The dhcp command in the WSG service specifies the DHCPv4 context and service name to be used when the IP address allocation method is set to dhcp-proxy. The specified DHCPv4 service is designated via the ip address alloc-method dhcp-proxy command. See IP Address Allocation Method.

Duplicate Session Detection

The duplicate-session-detection command enables or disables allowing only one IKE-SA per remote IKE-ID. A new request will overwrite the existing tunnel. For a complete description of this feature, refer to the IPSec Reference.

Peer List

The peer-list command configures an SecGW to initiate an IKEv2 session setup request when the peer does not initiate a setup request within a specified time interval. For a complete description of this feature, refer to the IPSec Reference.

Pre-fragment MTU

You can specify the Maximum Transmission Unit (MTU) size (576–2048 bytes, default = 1400) which when exceeded initiates pre-tunnel (before encryption) fragmentation of clear packets within this WSG service.
In the WSG Configuration mode, the following command specifies the pre-fragment MTU:

```
pre_fragment mtu size
```

Pre-Tunnel-Fragmentation improves packet processing performance as compared to post-tunnel-fragmentation.

If a clear IPv4 packet is longer than the predefined MTU size, it will be fragmented before the packet is encrypted and transmitted to the Internet.

If a clear IPv6 packet is longer than the predefined MTU size, it is dropped and an ICMP packet with the maximum length is sent back to the source. The source will then fragment the IPv6 packet and retransmit.

**Responder Mode Duration**

Use this command to specify the interval during which the WSG service (SecGW) will wait or a response from an IKE peer before switching to initiator mode (default is 10 seconds). This command is only available when a peer-list has been configured for the WSG service. See the *IPSec Reference* for additional information on configuring an SecGW as an IKE initiator.

**IP Address Allocation Method**

The default method for IPv4 address allocation is from a local pool. You also have the option of specifying a DHCPv4 proxy server.

The wsg-service configuration command sequence for changing to a DHCPv4 server is:

```
configure
  context ctx_name
  wsg-service service_name
  ip address alloc-method dhcp-proxy
```

To specify the DHCP service to use when the alloc-method is **dhcp proxy**, the wsg-service configuration command sequence is:

```
dhcp context-name context_name

dhcp service-name service_name
```

You must specify the context in which the DHCP service is configured, as well as the name of the DHCP service. Only one DHCPv4 service can be configured.

You must restart the WSG service for this setting to be effective. You restart the service by unbinding and binding the IP address to the service context.

A sample configuration sequence follows below.

```
configure
  context wsg
  wsg-service abc
  deployment-mode remote-access
```
ip address alloc-method dhcp-proxy

dhcp service-name dlv4

dhcp context-name dhcp

bind address 32.32.32.30 crypto-template foo

exit

StarOS defaults to client-id none. Currently the wsg-service only supports **client-identifier ike-id** which must be set in the dhcp-service used by the wsg-service. See the sample configuration below.

```
configure
context dhcp

dhcp-service dlv4

dhcp client-identifier ike-id

dhcp server 22.22.22.1

lease-time 1200

lease-duration min 900 max 10800

dhcp server selection-algorithm use-all

bind address 35.35.35.30

exit
```

**Important:** StarOS limits the length of the IKE-ID to 128 bytes. If the IKE-ID is DER encoded, the encoded IKE-ID must be within this limit.

**Important:** If a DER encoded IKE-ID contains a common name, the common name is sent as the client-id. The common name is limited to 64 characters to comply with the X.509 ASN.1 specification.

StarOS also needs an IP pool to setup flows for the range of addresses which may be assigned by the DHCP server. Without the IP pool definition, the tunnel is setup but does not pass traffic. The IP pool must be defined in either the WSG or DHCP context. See the sample configuration below.

```
configure
context dhcp

ip pool plv4 35.35.34.0 255.255.255.0 public 0
```
Characteristics and Limitations

The following factors characterize WSG service configuration:

- A WSG service configuration has precedence over the equivalent configuration in subscriber mode or the template payload.
- Any changes made to a WSG service require that the service be restarted to apply any changed parameters. You restart the service by unbinding and binding the IP address to the service context.
- Up to 16 named IPv4 pools can be configured. The list is sorted, and the addresses are allocated from the first pool in the list with available addresses.
- Multiple IPv6 pools can be configured.
- Multiple IPv4 and IPv6 ACLs can be configured.
- IPv4 pools are only used for IPv4 calls; IPv6 pools are only used for IPv6 calls.

Lookup Priority

The Wireless Security Gateway Lookup Priority List Configuration Mode is used to set the priority (1–6) of subnet combinations for site-to-site tunnels.

The following command sequence sets the lookup priority:

```
config
wsg-lookup
  priority priority_level source-netmask subnet_size destination netmask subnet_size
```

For the packet lookup to work optimally, the top bits in the negotiated TSi for all the tunnels should be unique. The top number of bits that must be unique is equal to the lowest “destination-netmask” configured under all lookup priorities.

For example, if the lowest destination-netmask configured under any priority is 16:

```
priority 1 source-netmask 20 destination-netmask 18
priority 2 source-netmask 22 destination-netmask 16
```

A valid set of traffic selectors for the configured set of lookup priorities would be:
- IPSec Tunnel 1: 10.11.1.0(tsi) - 20.20.1.0(tsr)
- IPSec Tunnel 2: 10.10.2.0(tsi) - 20.20.2.0(tsr)

An invalid set of traffic selectors would be:
- IPSec Tunnel 1: 10.10.1.0(tsi) - 20.20.1.0(tsr)
- IPSec Tunnel 2: 10.10.2.0(tsi) - 20.20.2.0(tsr)

The above set is invalid because the top 16 bits for these two tunnels are not unique, both are 10.10.

The network should be designed to accommodate this requirement.

For additional information, see the WSG Lookup Priority List Configuration Mode chapter of the Command Line Interface Reference.
show Commands

The following Exec mode show commands display information associated with WSG service parameters and operating statistics. For detailed descriptions of these commands, see the Exec Mode show Commands chapter of the Command Line Interface Reference.

show wsg-lookup

This command displays the priority levels, as well as source and destination netmasks for all configured lookup priorities. The command syntax is:

```
show wsg-lookup
```

The following is a sample output for show wsg-lookup:

```
wsg-lookup
priority 1 source-netmask 32 destination-netmask 32
priority 2 source-netmask 24 destination-netmask 32
priority 3 source-netmask 32 destination-netmask 24
priority 4 source-netmask 24 destination-netmask 24
```

show wsg-service

This command displays information about all WSG services or a specified service. It also displays statistics for a specified WSG service or peer address.

The command syntax is:

```
show wsg-service { all | name | srvc_name | statistics [ name srvc_name | peer-address ip_address ] [ | { grep grep_options | more } ] }
```

The following is a sample output for show wsg-service name wsg01:

```
Servicename: wsg01
Context: wsg
Bind: Done
Max Sessions : 8000
IP address: 10.10.10.30 UDP Port: 500
MTU: 1400
Service State: Started
Crypto-template: cryptotmplt01
deployment-mode : 1
```
peer-list : N/A
initiator-mode-duration : 10
responder-mode-duration : 10
Duplicate session detection: Disabled

The following is a sample output for **show wsg-service statistics name wsg01**:

WSG statistics for Service: wsg01

Session Stats:

Current sessions total: 0
Simple-IP IPv4 current: 0  Simple-IP IPv6 current 0
Data-Clients: 0
Active current: 0  Dormant current: 0

Total Simple-IP: 0
Simple-IP-Fallback attempts: 0
  Successes: 0  Failures: 0
Simple-IP-Fallback failure reasons:
  No Mobile-IP RRQ Rx: 0  Not allowed 0
  Tagged Pool Address: 0  Misc.: 0

Simple-IP-attempts: 0
Simple-IP successes: 0

Total setup attempts: 0
Total setup successes: 0  Total Attempts Failed: 0
Disconnected locally: 0

Disconnect remotely
  Before connect: 0
Session Disconnect reason:

- Remote disc. ipsec: 0
- Idle timeout: 0
- Long duration timeout: 0
- No resource: 0
- Flow add failure: 0
- Source address violation: 0
- MAC validation failure: 0
- Miscellaneous reasons: 0

Admin disconnect: 0

Absolute timeout: 0

Session setup timeout: 0

Auth failure: 0

Invalid dest-context: 0

Duplicate Request: 0

Addr assign failure: 0

Data Stats:

- Total Bytes Sent: 0
- Total Bytes Rcvd: 0
- Total Packets Sent: 0
- Total Packets Rcvd: 0
- Total Pkts Violations: 0

EAP Server Stats:

- Total Received: 0
- Success Received: 0
- Failures Received: 0
- Challenge Received: 0
- Discarded: 0

- Total Sent: 0
- Initial Requests: 0
- Requests Forwarded: 0

EAP Mobile Stats:

- Total Received: 0
- Discarded: 0
WSG Bulk Statistics

The wsg-service schema supports a number of bulk statistics that provide much more data than the show wsg command. This data is displayed by executing the Exec mode show bulkstats variables wsg command.

The following wsg-service bulk statistics support the Security Gateway (SecGW):

- wsg-current-sessions-total
- wsg-current-active-sessions
- wsg-current-dormant-sessions
- wsg-current-active-ipv4-sessions
- wsg-current-dormant-ipv4-sessions
- wsg-current-active-ipv6-sessions
- wsg-current-dormant-ipv6-sessions
- wsg-current-simple-ipv4-total
- wsg-current-simple-ipv6-total
- wsg-current-data-clients-total
- wsg-total-simple-ip-attempts
- wsg-total-simple-ip-successes
- wsg-total-simple-ip-failures
- wsg-total-simple-ip-fallback-successes
- wsg-total-simple-ip-fallback-failures
- wsg-total-simple-ip-fallback-no-mobile-ip-rrq-rx
- wsg-total-simple-ip-fallback-not-allowed
- wsg-total-simple-ip-fallback-tagged-pool-address
- wsg-total-simple-ip-fallback-fail-misc-reasons
- wsg-total-setup-successes
- wsg-total-setup-attempts
- wsg-total-attempts-failed
- wsg-total-disconnected
- wsg-total-disconnected-locally
- wsg-total-disconnected-remotely
- wsg-total-simple-ip-ipv4-sessions
- wsg-total-disconnected-remotely-before-connect
- wsg-total-disconnected-remote-disc-ipsec
- wsg-total-disconnected-admin-disconnect
- wsg-total-disconnected-idle-timeout
- wsg-total-disconnected-absolute-timeout
- wsg-total-disconnected-long-duration-timeout
- wsg-total-disconnected-session-setup-timeout
- wsg-total-disconnected-no-resource
- wsg-total-disconnected-auth-failure
- wsg-total-disconnected-flow-add-failure
- wsg-total-disconnected-invalid-dest-context
- wsg-total-disconnected-source-addr-violation
- wsg-total-disconnected-addr-violation
- wsg-total-disconnected-misc-reasons
- wsg-total-eap-server-total-received
- wsg-total-eap-server-challenge-received
- wsg-total-eap-server-success-received
- wsg-total-eap-server-failure-received
- wsg-total-eap-mobile-total-received
- wsg-total-sent-to-eap-server
- wsg-total-initial-requests-sent-to-eap-server
- wsg-total-eap-server-requests-forwarded
- wsg-total-eap-mobile-dropped
- wsg-total-eap-server-dropped
- wsg-total-packets-sent
- wsg-total-bytes-sent
- wsg-total-packets-rcvd
- wsg-total-bytes-rcvd
- wsg-total-packets-violations

For additional information on these bulk statistics, see the Statistics and Counters Reference.
IPSec Configuration

SecGW functionality also requires configuration of StarOS IPSec features. See the Product Feature Mapping chapter in the IPSec Reference for a list of features supported on the SecGW.

The IPSec Reference provides detailed configuration information for individual features, including sample configurations.
Multiple SecGW Configurations per VSM

You must complete the configuration process described in this chapter on each VPC-VSM instance. There will be a total of four distinct SecGW configurations on each VSM (one per CPU).
Chapter 3
oneP Communication

Communication between IOS-XR and a WSG service is based on the oneP (StarOS Connected Apps) infrastructure. This bidirectional communication allows the service to send and receive information to/from IOS-XR.

This chapter describes the configuration of oneP client communication and includes the following topics:

- Overview
- CA Sessions
- HA Mode
- show connectedapps Command
Overview

The oneP infrastructure supported by IOS-XR on the ASR 9000 is used to communicate with StarOS service virtual machines (VMs). OneP libraries consists a set of “C” libraries running as Linux user space processes so that a WSG service can interface with IOS-XR. An instance of the oneP (StarOS Connected Apps [CA]) library running within a wsg-service VM is completely independent from another instance running as part of a different wsg-service VM. A StarOS connectedasapps command allows an operator to configure and initiate a oneP (Connected Apps) session with the IOS-XR server.

For additional information on the ASR 9000 and the oneP infrastructure refer to:

- Cisco ASR 9000 Series Aggregation Services Router Interface and Hardware Component Configuration Guide – Configuring Virtual Services on the Cisco ASR 9000 Series Router
- Implementing CGv6 over VSM
Connected Apps Sessions

The StarOS client Connected Apps (oneP) application running on the wsg-service VM can set up a TLS (Transport Layer Security) session with the oneP server running on the ASR 9000 route processor (RP).

Enabling oneP on ASR 9000 RSP

To enable oneP communication with the VSM, the corresponding oneP server configuration should be done on the ASR 9000 Route Switch Processor (RSP). For IOS-XR 5.2.0 version onwards, only TLS transport type is supported for oneP connection. The basic configuration sequence is:

```
onep

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

! 

crypto ca trustpoint onep-tp

  crl optional

  subject-name CN=ASR9K-8.cisco.com

  enrollment url terminal

! 
```

By default, OneP flows are blocked at the LPTS layer on the VSM. That is why you must configure a policer rate for OneP flow for VSM.

For additional information, refer to the Cisco ASR 9000 Series Aggregation Services Router Interface and Hardware Component Configuration Guide – Configuring Virtual Services on the Cisco ASR 9000 Series Router

Configuring a Client CA Session

Before a CA session can be activated via StarOS, the operator must configure the session parameters – IP address, session name, username and password.

⚠️ Important: A client CA session must be configured via StarOS on each VPC-VSM instance running on the VSM (one per CPU).

The following sample StarOS CA mode CLI command sequence configures the CA session parameters:

```
configure

  connectedapps
```
ca-certificate-name cert_name

ha-chassis-mode inter

ha-network-mode L2

rri-mode BOTH

sess-ip-address ip_address

sess-name session_name

sess-passwd { encrypted | password } password

sess-userid username

activate

ip_address may be specified in IPv4 dotted-decimal or IPv6 colon-separated-hexadecimal format.

For a complete description of these command keywords, see the Global Configuration Mode Commands and Connected Apps Configuration Mode Commands chapters of the Command Line Interface Reference.

Activating a Client Connected Apps Session

Important: You must configure HA Mode on each VPC-VSM instance before activating a client CA session via StarOS.

To activate a CA session with the IOS-XR oneP server execute the following StarOS command sequence:

configure

    connectedapps

    activate

For a complete description this command, see the Global Configuration Mode Commands and Connected Apps Configuration Mode Commands chapters of the Command Line Interface Reference.

For additional information on IOS-XR commands, refer to ASR 9000 user documentation.
HA Mode

High Availability (HA) mode for a wsg-service VM is configured via StarOS Connected Apps mode commands as described below.

Configuring HA Chassis Mode

High Availability can be configured between ASR 9000 chassis (inter), within a single chassis (intra) [VSM-to-VSM] or standalone VSM.

The following StarOS CA mode command sequence enables the preferred HA chassis mode:

```plaintext
configure
connectedapps

ha-chassis-mode { inter | intra | standalone }
```

For a complete description this command, see the Global Configuration Mode Commands and Connected Apps Configuration Mode Commands chapters of the Command Line Interface Reference.

Configuring HA Network Mode

HA network mode can be specified as:

- **L2** – Layer 2
- **L3** – Layer 3
- **NA** – Not Applicable (standalone VSM)

The following StarOS CA mode command sequence enables the preferred HA network mode:

```plaintext
configure
connectedapps

ha-network mode { L2 | L3 | NA }
```

For a complete description this command, see the Global Configuration Mode Commands and Connected Apps Configuration Mode Commands chapters of the Command Line Interface Reference.
show connectedapps Command

The StarOS `show connectedapps` command displays information about the current CA configuration. The following is a sample output of this command:

```
Current connectedapps controller configuration
  CA session userid : iosxr01
  CA session password : dbljvk4
  CA session name : vm0-1
  CA session IP address : 192.168.120.1
  CA session ca certificate name : test
  RRI mode : S2S & RAS
  HA chassis mode : inter
  HA network mode : L2
  CA session Activation : YES
  CA session ID : 28677
  CA SRP Status : ACTIVE
  CA SRP State : SOCK_ACTIVE
```

SRP refers to the Session Redundancy Protocol supported by the StarOS Interchassis Session Recovery (ICSR) function. For additional information on SRP and ICSR, refer to the *VPC-VSM System Administration Guide*.

For additional information about this command, see the *Exec Mode show Commands* chapter in the *Command Line Interface Reference*.
Chapter 4
Reverse Route Injection

This chapter describes the Reverse Route Injection (RRI) feature supported by the SecGW.

The following topics are covered:

- Overview
- How It Works
- High Availability for RRI
- HSRP
Overview

RRI injects routes in the reverse direction onto the ASR 9000 VSM (IOS-XR blade) so that clear traffic can be routed to the correct interface on the target VSM. The OneP (ConnectedApps [CA]) library provides the necessary API calls to CA clients to communicate to the oneP server (running on IOS-XR).

The RRI feature is used in conjunction with the StarOS SecGW to deal with Site-to-Site (S2S) IPSec SAs. RRI route transaction is initiated when a tunnel SA is being created.

Interchassis Session Recovery (ICSR) works with RRI to ensure that traffic is correctly routed following an HA switchover.

For additional information, see the sample configurations that appear at the end of this guide.
How It Works

The Connected Apps Linux Process (CALP) receives single or batched route insertion/deletion request, validates the message received is complete, and initiates the update of the route request. A route update API then injects the routes contained in the Routing Information Base (RIB) table of the ASR 9000 Route Processor (RP).

A re-inject (replay) is an asynchronous event message from the ASR 9000 RP asking the StarOS CA client to replay all the route entries in its database from scratch. This message is usually generated in a drastic failure case where the RP has lost all the previously injected RRI routes in its Forwarding Information Base (FIB) table.

Status Handler processes all incoming responses from CALP to batch requests. Each response has a batch_id which will be correlated to the corresponding batch request. Route entries that are not acknowledged are regrouped and retransmitted. Those that are successful are moved to the route database hash table and removed from this batch. State diagram provided below shows the various states that a RRI route entry can be based on the responses for its batch request.

A StarOS proclet (cactrl) manages the creation and maintenance of the session with CALP. This session is the only communication channel between each StarOS VM and the ASR 9000 RSP. This oneP communication session must be established before any form of communication can occur between the two entities. See the oneP Communication chapter for detailed information.
High Availability for RRI

Interchassis Session Recovery (ICSR) is implemented for RRI to ensure that the routes are injected correctly on the appropriate VSM to route the traffic to the correct interface after an ICSR switchover.

ICSR can be implemented for:

- Intrachassis or cluster card-level redundancy
- Interchassis L2 card-level redundancy
- Interchassis L3 card-level redundancy

**Important:** RRI is mandatory for S2S StarOS WSG service and optional for RAS.

Intrachassis/Cluster Redundancy

This mode only supports Layer 2, 1:1 redundancy between VPC-VSM instances (StarOS VMs) across two VSMs in the same ASR 9000 chassis. Both instances are located in the same chassis and, therefore, the routes injected by the active VPC-VSM instance to the IOS-XR will still be valid after the failure when the standby card takes over. In this case, the NPU Manager on the standby VSM does not inject the routes to the IOS-XR. The routes only need to be added to the Route DB.

The main requirements for ICSR in this mode are:

- The route DB on the standby VSM must contain only routes that have been successfully injected by the active VPC-VSM instance.
- To prevent IOS-XR from removing the routes, CALP on the standby StarOS VM reconnects to the CA server via the same session ID used prior to the timeout. The session ID is stored in the shared configuration task (SCT) of the CA Controller and a new micro-checkpoint is sent to the standby VPC-VSM instance.

The session manager which programs the IPSec manager and other sessions managers synchronizes the tunnels with the standby VPC-VSM instance via SRP.

Interchassis Redundancy

**Overview**

This mode supports hot standby redundancy between two VPC-VSM instances in different ASR 9000 chassis. The standby instance is ready to become active once a switchover is triggered. SA re-negotiation is not required and traffic loss is minimal.

The Interchassis Session Recovery (ICSR) model supports both Layer 2 and Layer 3 levels of redundancy. Basic ICSR requirements are:

- The route database on the standby VSM must contain only the routes that were successfully injected by the active VSM.
Reverse Route Injection

High Availability for RRI

- L3-based HA SecGW deployment uses the onePK Routing Service Set (RSS) infrastructure to support geo-redundancy. It does this by inserting the necessary routes on the ASR 9000 RSP. The RSP then distributes the relevant routes outwardly such that external traffic would reach the active VSM instead of the standby VSM.

- For Layer 3 redundancy, the routes are injected via IOS-XR as two legs. Only the first leg of the routes is injected to IOS-XR running on the chassis with the standby VSM. The small set of secondary leg routes are reconfigured to point to the newly active VSM after the switchover.

For additional information on StarOS ICSR, see the VPC-VSM System Administration Guide.

Mapping of VPC-VSM Instances between VSMs

Because of the asymmetric assignment of VSM resources among StarOS VMs, an operator should configure one-to-one mapping between StarOS VMs across active/standby VSMs in different ASR 9000 chassis. See the table below.

<table>
<thead>
<tr>
<th>Active VSM</th>
<th>Standby VSM</th>
</tr>
</thead>
<tbody>
<tr>
<td>VM1</td>
<td>VM1</td>
</tr>
<tr>
<td>VM2</td>
<td>VM2</td>
</tr>
<tr>
<td>VM3</td>
<td>VM3</td>
</tr>
<tr>
<td>VM4</td>
<td>VM4</td>
</tr>
</tbody>
</table>

Each VM will be monitored via separate HSRP configurations and connected to separate oneP (CA) sessions so that switchover of one VM will not affect the other VMs.

RRI Configuration Commands

There are several StarOS CLI commands associated with RRI configurations. They are briefly described below. For additional information, see the Command Line Interface Reference.

**Important:** You must separately configure RRI on each StarOS VM (VPC-VSM instance).

**ip/ipv6 rri Command**

This Context Configuration mode CLI command configures Reverse Route Injection egress clear port IP parameters. This command is supported for both Remote Access Service and S2S configurations.

```
configure

    context context_name

    { ip | ipv6 } rri { ip_address | next-hop nexthop_address } interface
    interface_name [ vrf vrf_name ]
```

Notes:
Reverse Route Injection

High Availability for RRI

- `ip_address` and `nexthop_address` can be specified in IPv4 dotted-decimal (ip rri) or IPv6 colon-separated-hexadecimal (ipv6 rri) format.
- The next hop IP address is not required for point-to-point and tunnel interfaces.
- `interface_name` specifies the egress interface.

**ip/ipv6 rri-route Command**

This Context Configuration mode CLI command configures High Availability Routing Parameters for Reverse Route Injection.

```
configure

context context_name

   { ip | ipv6 } rri-route network-mode { L2 | L3 } { clear_loopback_ip | rri-ip virtual_ip_address } { ip_address | next-hop nexthop_address } interface
interface_name [ vrf vrf_name ]

end
```

Notes:
- This command is mandatory in the following scenarios:
  - L2 Intrachassis HA (where loopback IP is configured)
  - L3 Interchassis HA (where IP is configured)
- `ip_address`, `virtual_ip_address` and `nexthop_address` can be specified in IPv4 dotted-decimal (ip rri-route) or IPv6 colon-separated-hexadecimal (ipv6 rri-route) format.
- The next hop IP address is not required for point-to-point and tunnel interfaces.
- `interface_name` specifies the egress interface.

**ip/ipv6 sri-route Command**

This Context Configuration mode command configures L3 High Availability Service Route Injection parameters:

```
configure

context context_name

   { ip | ipv6 } sri-route sri-ip network_address next hop nexthop_address
interface interface_name [ vrf vrf_name ]

end
```

Notes:
- `network_address` and `nexthop_address` are specified in IPv4 dotted-decimal (ip sri-route) or IPv6 colon-separated hexadecimal (ipv6 sri-route) notation.
- The next hop IP address is not required for point-to-point and tunnel interfaces.
- `interface_name` specifies the egress interface.
**rri-mode Command**

This ConnectedApps Configuration mode CLI command configures the supported RRI mode.

```
configure
  connectedapps
    rri-mode { both | none | ras | s2s }
  end
```

**Notes:**
- This command configures the anchor-route for an L3-L3 interchassis HA scenario.
- **both** = enabled for RAS and S2S
- **none** = disabled for all flow types
- **ras** = Remote Access Service only
- **s2s** = site-to-site only

**Sample StarOS RRI HA Configurations**

**ConnectedApps (oneP) Configuration**

```
config
  context local
  interface CA
    ip address 192.168.122.10 255.255.255.0
  exit
  subscriber default
  exit
  aaa group default
  exit
  no gtp policy direct-tunnel
  ip route 0.0.0.0 0.0.0.0 192.168.122.110 CA
  exit
  port ethernet 1/1
  no shutdown
```
bind interface CA local
exit

Intrachassis/Cluster Redundancy

config
  connectedapps
    sess-userid cisco
    sess-passwd cisco
    sess-name secgw
    sess-ip-address 172.29.98.14
    rri-mode ras
    ha-chassis-mode intra
    ha-network-mode L2
    activate
  exit
Figure 10. Intra-chassis/Cluster Redundancy

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Common oneP session is used only by the active SecGW.</td>
</tr>
<tr>
<td>Item</td>
<td>Description</td>
</tr>
<tr>
<td>------</td>
<td>-------------</td>
</tr>
<tr>
<td>2</td>
<td>Only the active SecGW injects routes on tunnel setup.</td>
</tr>
<tr>
<td>3</td>
<td>Upon failover the currently active SecGW gives up its oneP session and the newly active SecGW takes over the session.</td>
</tr>
<tr>
<td>4</td>
<td>Upon failover the newly active SecGW injects routes for new tunnels.</td>
</tr>
</tbody>
</table>

**L2 Interchassis Redundancy**

```
config

  connectedapps

    sess-userid cisco
    sess-passwd cisco
    sess-name secgw
    sess-ip-address 172.29.98.14
    rri-mode ras
    ha-chassis-mode inter
    ha-network-mode L2

  activate

  exit
```

Figure 11. L2 Interchassis Redundancy
<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Both the active and standby SecGWs insert routes into local chassis only.</td>
</tr>
<tr>
<td>2</td>
<td>ICSR is configured to track RSP HSRP groups. HSRP also tracks SecGW using an SLA (Service Level Agreement).</td>
</tr>
</tbody>
</table>

**L3 Interchassis Redundancy**

```
config
  connectedapps
    sess-userid cisco
    sess-passwd cisco
    sess-name secgw
    sess-ip-address 172.29.98.14
    rri-mode ras
    ha-chassis-mode inter
    ha-network-mode L3
    activate
  exit
```

**Figure 12. L3 Interchassis (Geo Redundancy) Mode**
HSRP

Overview

Hot Standby Router Protocol (HSRP) is a Cisco proprietary redundancy protocol for establishing a fault-tolerant default gateway (RFC 2281). The protocol establishes a framework between network routers in order to achieve default gateway failover if the primary gateway becomes inaccessible.

Chassis-to-chassis redundancy employs HSRP to detect failure in the system and notify other elements of the need to change their HA State. Each VSM receives these notifications via oneP (Connected Apps) communication.

An external HSRP-aware entity switches traffic from the primary to the backup chassis. All application instances must failover to the backup chassis.

For additional information on HSRP, see the *ASR 9000 Series Aggregation Services Router IP Addresses and Services Configuration Guide*.

Figure 13. HSRP Notification

Each StarOS VM requires a separate oneP connection to the RSP (four oneP connections per VSM). Each StarOS VM is monitored by a separate HSRP link that is established using sub-interfaces.
HSRP Configuration

Parameters

HSRP configuration parameters include:

- Interface name
- Address Family Identifier (AFI) type (IPv4 or IPv6)
- HSRP group number

*Important:* The above parameters must match those of the HSRP configuration in the ASR 9000 RSP.

The following limits also apply to the HSRP configuration

- A maximum of one HSRP monitor is supported per VPC-VSM instance.
- The `monitor hsrp` command is associated with the SRP context.

**monitor hsrp Command**

The syntax for the `monitor hsrp` command is as follows:

```plaintext
cfg
  context srp_context
    monitor hsrp interface ifname afi-type type group hsrp_group
```

**StarOS Configuration**

HSRP monitoring must be enabled in the SRP configuration. A sample configuration is provided below.

*Important:* You must configure HSRP for each VPC-VSM instance (StarOS VM) on the active and standby VSMs.

```plaintext
cfg
  context srp
    service-redundancy-protocol
    checkpoint session duration 30
    route-modifier threshold 10
    priority 10
    monitor hsrp interface GigabitEthernet0/0/1/1 afi-type ipv4 hsrp-group 4
    peer-ip-address 88.88.88.36
```
Important: HSRP monitoring is done via the ConnectedApps (oneP) interface in StarOS. A oneP session is established to all VPC-VSM instances on each VSM.

ASR 9000 RSP Configuration

HSRP must be configured on both the primary and backup ASR 9000 chassis. Sample IOS-XR configurations are provided below.

Primary ASR 9000 Chassis

```plaintext
router hsrp

interface GigabitEthernet0/1/0/3

address-family ipv4

hsrp 2

priority 110

address 10.10.10.100

|  

|  

|  

|  

Backup ASR 9000 Chassis

router hsrp

interface GigabitEthernet0/2/0/2

address-family ipv4

hsrp 2

priority 100

address 10.10.10.100

|  

|  

|  

|  

```
Chapter 5
Sample Basic wsg-service Configuration

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

This same configuration includes the following sections:

- WSG Context (StarOS)
- SRP Context (StarOS)
- HSRP Configuration (IOS-XR)
- Port Configuration (StarOS)
- oneP (Connected Apps) Communication
WSG Context (StarOS)

```plaintext
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 33.33.33.3 255.255.255.0
    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

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

Backup Chassis

```conf
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)

```plaintext
onep
    transport type tls localcert onep-tp disable-remotecert-validation
!
config
lpts pifib hardware police flow ONEPK rate 2000
commit
!
```

CA Client Session (StarOS)

```plaintext
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
```
Chapter 6
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).

This sample configuration includes the following sections:

- ASR 9000 RSP Configuration (IOS-XR)
- WSG Configuration VM-1 (StarOS)
- WSG Configuration VM-2 (StarOS)
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.

```plaintext
<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
ccontext 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-allo 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

clear 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
Chapter 7
Sample L2 Interchassis HA Configuration

This chapter provides a sample interchassis wsg-service High Availability (HA) configuration for SecGW functionality between four VPC-VSM instances (StarOS VMs) running on VSMs in separate ASR 9000 chassis.

This sample configuration includes the following sections:

- Configuration Overview
- ASR 9000 Chassis RSP Configuration (IOS-XR)
- SecGW VM Configuration (StarOS)
Configuration Overview

Interchassis Layer 2 redundancy supports hot standby redundancy between two VPC-VSM instances in different ASR 9000 chassis. The standby instance is ready to become active once a switchover is triggered. SA re-negotiation is not required and traffic loss is minimal.

The route database on the standby VSM must contain only the routes that were successfully injected by the active VSM. Because of the asymmetric assignment of VSM resources among StarOS VMs, an operator should configure one-to-one mapping between StarOS VMs across active/standby VSMs in different ASR 9000 chassis. See the table below.

<table>
<thead>
<tr>
<th>Active VSM</th>
<th>Standby VSM</th>
</tr>
</thead>
<tbody>
<tr>
<td>VM1 – SecGW1</td>
<td>VM1 – SecGW1</td>
</tr>
<tr>
<td>VM2 – SecGW2</td>
<td>VM2 – SecGW2</td>
</tr>
<tr>
<td>VM3 – SecGW3</td>
<td>VM3 – SecGW3</td>
</tr>
<tr>
<td>VM4 – SecGW4</td>
<td>VM4 – SecGW4</td>
</tr>
</tbody>
</table>

Each VM will be monitored via separate HSRP configurations and connected to separate oneP (CA) sessions so that switchover of one VM will not affect the other VMs.

Sample ASR 9000 chassis RSP configurations are provided for primary and standby chassis.

The sample configurations provided for an SecGW VM (Virtual Machine) configuration must be replicated on each CPU-VM complex on both the active and standby VSMs. Each VSM supports four CPU-VM complexes (SecGWs).
ASR 9000 Chassis RSP Configuration (IOS-XR)

**Important:** Primary and standby ASR 9000 chassis must be configured to handle the SecGWs (CPU-VM complexes) running on ASR 9000 VSMs. There are four CPU-VM complexes per VSM.

The sample configurations must be applied to the primary and backup ASR 9000 chassis. Each chassis will have unique and shared IP addresses to assure high availability across chassis.

Notes:

- Set basic chassis parameters
- Enable oneP communication. (TLS protocol)
- Enable virtual services and assign virtual interfaces for each CPU-VM complex.
- Configure physical Gigabit Ethernet (GigE) ASR 9000 interfaces. Shutdown unused ports.
- Configure a GigE public interface (with VLANs) for IKE and ESP traffic on each CPU-VM complex.
- Configure a GigE private interface (with VLANs) for clear traffic on each CPU-VM complex.
- Configure a 10 Gigabit Ethernet (10GigE) interface for IKE and ESP traffic on each CPU-VM complex. Shut down unused ports.
  - Configure a VLAN on this interface for clear and SRP traffic.
  - Configure a VLAN on this interface for SRP traffic.
  - Configure a VLAN on this interface for clear traffic
- Configure a 10GigE Management interface on each CPU-VM complex.
- Configure a Bridged Virtual Interface (BVI) for the chassis. A BVI interface configured on the RSP is used as the sess-ip-address in all four SecGW(s) for bringing up the oneP session between the RSP and SecGW.
- Configure static IPv4 and IPV6 addresses.
- Configure an L2 VPN.
- Configure HSRP tracking for each CPU-VM complex (shared parameters across ASR 9000 chassis).
- Configure IP Service Level Agreement (SLA) operations.

### ASR 9000 Primary Chassis

```
hostname <ASR9K_primary_hostname>
clock timezone <timezone>
clock <clock_settings>
logging console critical
logging buffered 99999999
```

tftp vrf default ipv4 server homedir /

```
telnet vrf default ipv4 server max-servers 50
domain name <domain_name>
cdp
configuration commit auto-save filename <unique_ASR9K_config_filename>
vrf ike1
!
vrf ike2
!
vrf ike3
!
vrf ike4
!
line console
   exec-timeout 0 0
   length 50
!
line default
   exec-timeout 0 0
!
onep
   transport type tls localcert onep-tp disable-remotecert-validation
!
virtual-service enable
virtual-service SecGW1
   vnic interface TenGigE0/4/1/0
   vnic interface TenGigE0/4/1/1
   vnic interface TenGigE0/4/1/2
   activate
!
virtual-service enable
virtual-service SecGW2
  vnic interface TenGigE0/4/1/3
  vnic interface TenGigE0/4/1/4
  vnic interface TenGigE0/4/1/5
  activate
!
virtual-service enable
virtual-service SecGW3
  vnic interface TenGigE0/4/1/6
  vnic interface TenGigE0/4/1/7
  vnic interface TenGigE0/4/1/8
  activate
!
virtual-service enable
virtual-service SecGW4
  vnic interface TenGigE0/4/1/9
  vnic interface TenGigE0/4/1/10
  vnic interface TenGigE0/4/1/11
  activate
!
interface Loopback1
  ipv4 address 65.65.0.1 255.255.255.255
!
interface MgmtEth0/RSP0/CPU0/0
  ipv4 address 10.78.1.40 255.255.255.0
!
interface MgmtEth0/RSP0/CPU0/1
  ipv4 address 8.40.2.101 255.255.0.0
interface GigabitEthernet0/0/0/0
shutdown
!
interface GigabitEthernet0/0/0/1
shutdown
!
interface GigabitEthernet0/0/0/2
shutdown
!
interface GigabitEthernet0/0/0/3
shutdown
!
interface GigabitEthernet0/0/0/4
shutdown
!
interface GigabitEthernet0/0/0/5
  description "SRP Link - direct Connect to <ASR9K_primary_hostname>
gigabitEthernet 0/0/0/5"
  ipv4 address 87.87.87.10 255.255.255.0
  speed 1000
  transceiver permit pid all
!
interface GigabitEthernet0/0/0/6
shutdown
!
interface GigabitEthernet0/0/0/7
shutdown
!
interface GigabitEthernet0/0/0/8
  shutdown
!
interface GigabitEthernet0/0/0/9
  shutdown
!
interface GigabitEthernet0/0/0/10
  shutdown
!
interface GigabitEthernet0/0/0/11
  shutdown
!
interface GigabitEthernet0/0/0/12
  shutdown
!
interface GigabitEthernet0/0/0/13
  shutdown
!
interface GigabitEthernet0/0/0/14
  shutdown
!
interface GigabitEthernet0/0/0/15
  shutdown
!
interface GigabitEthernet0/0/0/16
  shutdown
!
interface GigabitEthernet0/0/0/17
  shutdown
interface GigabitEthernet0/0/0/18
    description "Public Interface: IKE and ESP Traffic"
cdp
transceiver permit pid all
dot1q tunneling ethertype 0x9200
!
interface GigabitEthernet0/0/0/18.1871
description "Public Interface: IKE and ESP Traffic - VM1"
ipv4 address 187.0.1.10 255.255.255.0
ipv6 address 1871::10/64
ipv6 enable
encapsulation dot1q 1871
!
interface GigabitEthernet0/0/0/18.1872
description "Public Interface: IKE and ESP Traffic - VM2"
ipv4 address 187.0.2.10 255.255.255.0
ipv6 address 1872::10/64
ipv6 enable
encapsulation dot1q 1872
!
interface GigabitEthernet0/0/0/18.1873
description "Public Interface: IKE and ESP Traffic - VM3"
ipv4 address 187.0.3.10 255.255.255.0
ipv6 address 1873::10/64
ipv6 enable
encapsulation dot1q 1873
!
interface GigabitEthernet0/0/0/18.1874
description "Public Interface: IKE and ESP Traffic - VM4"
ipv4 address 187.0.4.10 255.255.255.0
ipv6 address 1874::10/64
ipv6 enable
encapsulation dot1q 1874
!
interface GigabitEthernet0/0/0/19
description Private Interface, Clear Traffic
cdp
transceiver permit pid all
dot1q tunneling ethertype 0x9200
!
interface GigabitEthernet0/0/0/19.1881
description "Private Interface, Clear Traffic - VM1"
ipv4 address 188.0.1.10 255.255.255.0
ipv6 address 1881::10/64
ipv6 enable
encapsulation dot1q 1881
!
interface GigabitEthernet0/0/0/19.1882
description "Private Interface, Clear Traffic - VM2"
ipv4 address 188.0.2.10 255.255.255.0
ipv6 address 1882::10/64
ipv6 enable
encapsulation dot1q 1882
!
interface GigabitEthernet0/0/0/19.1883
description "Private Interface, Clear Traffic - VM3"
ipv4 address 188.0.3.10 255.255.255.0
ipv6 address 1883::10/64
ipv6 enable
en encapsulation dot1q 1883
!
interface GigabitEthernet0/0/0/19.1884<clear-traffic_VLANid_VM4>
description "Private Interface, Clear Traffic - VM4"
ipv4 address 188.0.4.10 255.255.255.0
ipv6 address 1884::10/64
ipv6 enable
en encapsulation dot1q 1884
!
interface GigabitEthernet0/0/0/20
shutdown
!
interface GigabitEthernet0/0/0/21
shutdown
!
interface GigabitEthernet0/0/0/22
shutdown
!
interface GigabitEthernet0/0/0/23
shutdown
!
interface GigabitEthernet0/0/0/24
shutdown
!
interface GigabitEthernet0/0/0/25
shutdown
!
interface GigabitEthernet0/0/0/26
    shutdown
!
interface GigabitEthernet0/0/0/27
    shutdown
!
interface GigabitEthernet0/0/0/28
    shutdown
!
interface GigabitEthernet0/0/0/29
    shutdown
!
interface GigabitEthernet0/0/0/30
    shutdown
!
interface GigabitEthernet0/0/0/31
    shutdown
!
interface GigabitEthernet0/0/0/32
    shutdown
!
interface GigabitEthernet0/0/0/33
    shutdown
!
interface GigabitEthernet0/0/0/34
    shutdown
!
interface GigabitEthernet0/0/0/35
    shutdown
!
interface GigabitEthernet0/0/0/36
  shutdown
!
interface GigabitEthernet0/0/0/37
  shutdown
!
interface GigabitEthernet0/0/0/38
  shutdown
!
interface GigabitEthernet0/0/0/39
  shutdown
!
interface TenGigE0/4/1/0
  description "IKE and ESP traffic VM1"
  transceiver permit pid all
  dot1q tunneling ethertype 0x9200
!
interface TenGigE0/4/1/0.1871
  description "IKE and ESP traffic for VM1"
  ipv4 address 31.31.31.10 255.255.255.0
  ipv6 address 2031::10/64
  encapsulation dot1q 1871
!
interface TenGigE0/4/1/1
  description "Clear and srp traffic VM1"
  transceiver permit pid all
  dot1q tunneling ethertype 0x9200
!
interface TenGigE0/4/1/1.1259
  description "srp traffic VM1"
  ipv4 address 71.71.71.10 255.255.255.0
  ipv6 address <10Gig_SRIPv6-address/mask>
  encapsulation dot1q 2071::10/64
!
interface TenGigE0/4/1/2
  description "Management interface for VM1"
  transceiver permit pid all
  l2transport

!
interface TenGigE0/4/1/3
  description "IKE and ESP traffic VM2"
  transceiver permit pid all
  dot1q tunneling ethertype 0x9200
!
interface TenGigE0/4/1/3.1872
  description "IKE and ESP traffic for VM2"
  ipv4 address 32.32.32.10 255.255.255.0
  ipv6 address 2032::10/64
  encapsulation dot1q 1872
!
interface TenGigE0/4/1/4
  description "Clear and srp traffic VM2"
  transceiver permit pid all
  dot1q tunneling ethertype 0x9200
!
interface TenGigE0/4/1/4.1260
description "srp traffic VM2"
ipv4 address 72.72.72.10 255.255.255.0
ipv6 address 2072::10/64
encapsulation dot1q 1260
!
interface TenGigE0/4/1/4.1882
description "clear traffic VM2"
ipv4 address 52.52.52.10 255.255.255.0
ipv6 address 2052::10/64
encapsulation dot1q 1882
!
interface TenGigE0/4/1/5
description "Management interface for VM2"
transceiver permit pid all
l2transport
!
!
interface TenGigE0/4/1/6
description "IKE and ESP traffic VM3"
transceiver permit pid all
dot1q tunneling ethertype 0x9200
!
interface TenGigE0/4/1/6.1873
description "IKE and ESP traffic for VM3"
ipv4 address 33.33.33.10 255.255.255.0
ipv6 address 2033::10/64
encapsulation dot1q 1873
!
interface TenGigE0/4/1/7
description "Clear and srp traffic VM3"
transceiver permit pid all
dot1q tunneling ethertype 0x9200
!
interface TenGigE0/4/1/7.1261
description "srp traffic VM3"
ipv4 address 73.73.73.10 255.255.255.0
ipv6 address 2073::10/64
encapsulation dot1q 1261
!
interface TenGigE0/4/1/7.1883
description "clear traffic VM3"
ipv4 address 53.53.53.10 255.255.255.0
ipv6 address 2053::10/64
encapsulation dot1q 1883
!
interface TenGigE0/4/1/8
description "Management interface for VM3"
transceiver permit pid all
l2transport
!
!
interface TenGigE0/4/1/9
description "IKE and ESP traffic VM4"
transceiver permit pid all
dot1q tunneling ethertype 0x9200
!
interface TenGigE0/4/1/9.1874
description "IKE and ESP traffic for VM3"
ipv4 address 34.34.34.10 255.255.255.0
ipv6 address 2034::10/64
encapsulation dot1q 1874
!
interface TenGigE0/4/1/10
description "Clear and srp traffic VM4"
transceiver permit pid all
dot1q tunneling ethertype 0x9200
!
interface TenGigE0/4/1/10.1262
description "srp traffic VM4"
ipv4 address 74.74.74.10 255.255.255.0
ipv6 address 2074::10/64
encapsulation dot1q 1262
!
interface TenGigE0/4/1/10.1884
description "clear traffic VM4"
ipv4 address 54.54.54.10 255.255.255.0
ipv6 address 2054::10/64
encapsulation dot1q 1884
!
interface TenGigE0/4/1/11
description "Management interface for VM4"
transceiver permit pid all
l2transport
!
!
interface BVI1
ipv4 address 100.100.100.10 255.255.255.0
router static

address-family ipv4 unicast
5.5.0.0/16 34.34.34.33
10.78.0.0/16 MgmtEth0/RSP0/CPU0/0
35.35.35.35/32 31.31.31.11
36.36.36.36/32 32.32.32.11
37.37.37.37/32 33.33.33.11
38.38.38.38/32 34.34.34.11
64.103.217.0/24 10.78.1.1
65.65.0.0/16 188.0.1.100
66.66.0.0/16 188.0.2.100
67.67.0.0/16 188.0.3.100
68.68.0.0/16 188.0.4.100
81.81.81.0/24 GigabitEthernet0/0/0/5 87.87.87.9
82.82.82.0/24 GigabitEthernet0/0/0/5 87.87.87.9
83.83.83.0/24 GigabitEthernet0/0/0/5 87.87.87.9
84.84.84.0/24 GigabitEthernet0/0/0/5 87.87.87.9
92.0.0.0/8 187.0.1.11
93.0.0.0/8 187.0.2.11
94.0.0.0/8 187.0.3.11
95.0.0.0/8 187.0.4.11
202.153.144.0/24 8.40.0.1

address-family ipv6 unicast
2035::35/128 2031::11
2036::36/128 2032::11
2037::37/128 2034::11
2038::38/128 2034::11
2065::/64 1881::100
2066::/64 1882::100
2067::/64 1883::100
2068::/64 1884::100
2092::/64 1871::11
2093::/64 1872::11
2094::/64 1873::11
2095::/64 1874::11

!
!
l2vpn
xconnect group wsg
!
bridge group irb
bridge-domain irb1
  interface TenGigE0/4/1/2
  !
  interface TenGigE0/4/1/5
  !
  interface TenGigE0/4/1/8
  !
  interface TenGigE0/4/1/11
  !
routed interface BVI1
  !
  !
router hsrp
  interface GigabitEthernet0/0/0/18.1871
address-family ipv4
hsrp 4
preempt
priority 101
address 187.0.1.20
track object WsgIPsla
track object PublicHsrp
!
!
address-family ipv6
hsrp 12
preempt
priority 101
track object WsgIPsla
track object PublicHsrp
address global 1871::20
address linklocal autoconfig
!
!
interface GigabitEthernet0/0/0/18.1872
address-family ipv4
hsrp 5
preempt
priority 101
address 187.0.2.20
track object WsgIPsla1
track object PublicHsrp
!
! address-family ipv6
hsrp 13
preempt
priority 101
track object WsgIPsla1
track object PublicHsrp
address global 1872::20
address linklocal autoconfig
!
!
!
interface GigabitEthernet0/0/0/18.1873
address-family ipv4
hsrp 6
preempt
priority 101
address 187.0.3.20
track object WsgIPsla2
track object PublicHsrp
!
!
!
interface GigabitEthernet0/0/0/18.1874
address-family ipv6
hsrp 14
preempt
priority 101
track object WsgIPsla2
track object PublicHsrp
address global 1873::20
address linklocal autoconfig
!
!
!
address-family ipv4
hsrp 7
preempt
priority 101
address 187.0.4.20
track object WsgIPsla3
track object PublicHsrp
!
!
!
address-family ipv6
hsrp 15
preempt
priority 101
track object WsgIPsla3
track object PublicHsrp
address global 1874::20
address linklocal autoconfig
!
!
!
interface GigabitEthernet0/0/0/19.1881
address-family ipv4
hsrp 8
preempt
priority 101
address 188.0.1.20
track object WsgIPsla
track object PublicHsrp

address-family ipv6
hsrp 16
preempt
priority 101
track object WsgIPsla
track object PublicHsrp
address global 1881::20
address linklocal autoconfig

interface GigabitEthernet0/0/0/19.1882
address-family ipv4
hsrp 9
preempt
priority 101
address 188.0.2.20
track object WsgIPsla1
track object PublicHsrp

address-family ipv6
hsrp 17
preempt
priority 101
track object WsgIPsla1
track object PublicHsrp
address global 1882::20
address linklocal autoconfig
!
!
!
interface GigabitEthernet0/0/0/19.1883
address-family ipv4
hsrp 10
preempt
priority 101
address 188.0.3.20
track object WsgIPsla2
track object PublicHsrp
!
!
address-family ipv6
hsrp 18
preempt
priority 101
track object WsgIPsla2
track object PublicHsrp
address global 1883::20
address linklocal autoconfig
!
interface GigabitEthernet0/0/0/19.1884
address-family ipv4
hsrp 11
preempt
priority 101
address 188.0.4.20
track object WsgIPsla3
track object PublicHsrp
!
address-family ipv6
hsrp 19
preempt
priority 101
track object WsgIPsla3
track object PublicHsrp
address global 1884::20
address linklocal autoconfig
!
!
ipsla
operation 200
type icmp echo
destination address 31.31.31.100
timeout 300
frequency 1
!
!
operation 201
type icmp echo
destination address 32.32.32.100
timeout 300
frequency 1
!
!
operation 202
type icmp echo
destination address 33.33.33.100
timeout 300
frequency 1
!
!
operation 203
type icmp echo
destination address 34.34.34.100
timeout 300
frequency 1
!
!
schedule operation 200
start-time now
life forever
!
schedule operation 201
start-time now

life forever

!
schedule operation 202
start-time now
life forever

!
schedule operation 203
start-time now
life forever

!

! track WsgIPsla
  type rtr 200 reachability
delay up 1
delay down 1

!

! track WsgIPsla1
  type rtr 201 reachability
delay up 1
delay down 1

!

! track WsgIPsla2
  type rtr 202 reachability
delay up 1
delay down 1

!

! track WsgIPsla3
  type rtr 203 reachability
delay up 1
delay down 1
!
track PublicHsrp
type line-protocol state
    interface GigabitEthernet0/0/0/18
!
delay up 1
delay down
!
crypto ca trustpoint onep-tp
crl optional
    subject-name CN=<ASR9K_PRIMARY_HOSTNAME>.<domain_name>
enrollment url terminal
!
end

ASR 9000 Backup Chassis

hostname <ASR9K_BACKUP_HOSTNAME>
clock timezone <timezone>
clock <clock_settings>
logging console critical
logging buffered 99999999
tftp vrf default ipv4 server homedir disk:0
telnet vrf default ipv4 server max-servers 10
domain name <domain_name>
cdp advertise v1
configuration commit auto-save filename <unique_ASR9K_CONFIG_FILENAME>
vrf ike1
vrf ike2
vrf ike3
vrf ike4
line console
  exec-timeout 0 0
  length 50
line default
  exec-timeout 0 0
onep
  transport type tls localcert onep-tp disable-remotecert-validation
virtual-service enable
virtual-service SecGW1
  vnic interface TenGigE0/4/1/0
  vnic interface TenGigE0/4/1/1
  vnic interface TenGigE0/4/1/2
  activate
virtual-service enable
virtual-service SecGW2
  vnic interface TenGigE0/4/1/3
  vnic interface TenGigE0/4/1/4
  vnic interface TenGigE0/4/1/5
activate
!
virtual-service enable
virtual-service SecGW3
  vnic interface TenGigE0/4/1/6
  vnic interface TenGigE0/4/1/7
  vnic interface TenGigE0/4/1/8
  activate
!
virtual-service enable
virtual-service SecGW4
  vnic interface TenGigE0/4/1/9
  vnic interface TenGigE0/4/1/10
  vnic interface TenGigE0/4/1/11
  activate
!
interface Loopback1
  ipv4 address 65.65.0.1 255.255.255.255
!
interface MgmtEth0/RSP0/CPU0/0
  ipv4 address 10.78.1.50 255.255.255.0
!
interface MgmtEth0/RSP0/CPU0/1
  ipv4 address 8.40.4.200 255.255.0.0
!
interface GigabitEthernet0/0/0/0
  shutdown
!
interface GigabitEthernet0/0/0/1
shutdown
!
interface GigabitEthernet0/0/0/2
  shutdown
!
interface GigabitEthernet0/0/0/3
  shutdown
!
interface GigabitEthernet0/0/0/4
  shutdown
!
interface GigabitEthernet0/0/0/5
  description "SRP Link - direct Connect to <ASR9K_backup_hostname> 
  gigabitEthernet 0/0/0/5"
  ipv4 address 87.87.87.9 255.255.255.0
  speed 1000
  transceiver permit pid all
!
interface GigabitEthernet0/0/0/6
  shutdown
!
interface GigabitEthernet0/0/0/7
  shutdown
!
interface GigabitEthernet0/0/0/8
  shutdown
!
interface GigabitEthernet0/0/0/9
  shutdown
interface GigabitEthernet0/0/0/10
shutdown
!
interface GigabitEthernet0/0/0/11
shutdown
!
interface GigabitEthernet0/0/0/12
shutdown
!
interface GigabitEthernet0/0/0/13
shutdown
!
interface GigabitEthernet0/0/0/14
shutdown
!
interface GigabitEthernet0/0/0/15
shutdown
!
interface GigabitEthernet0/0/0/16
shutdown
!
interface GigabitEthernet0/0/0/17
shutdown
!
interface GigabitEthernet0/0/0/18
description "Public Interface: IKE and ESP Traffic"
cdp
transceiver permit pid all
dot1q tunneling ethertype 0x9200
!

interface GigabitEthernet0/0/0/18.1871
description "Public Interface: IKE and ESP Traffic - VM1"
ipv4 address 187.0.1.9 255.255.255.0
ipv6 address 1871::9/64
ipv6 enable
encapsulation dot1q 1871
!

interface GigabitEthernet0/0/0/18.1872
description "Public Interface: IKE and ESP Traffic - VM2"
ipv4 address 187.0.2.9 255.255.255.0
ipv6 address 1872::9/64
ipv6 enable
encapsulation dot1q 1872
!

interface GigabitEthernet0/0/0/18.1873
description "Public Interface: IKE and ESP Traffic - VM3"
ipv4 address 187.0.3.9 255.255.255.0
ipv6 address 1873::9/64
ipv6 enable
encapsulation dot1q 1873
!

interface GigabitEthernet0/0/0/18.1874
description "Public Interface: IKE and ESP Traffic - VM4"
ipv4 address 187.0.4.9 255.255.255.0
ipv6 address 1874::9/64
ipv6 enable
encapsulation dot1q 1874
interface GigabitEthernet0/0/0/19
  description Private Interface, Clear Traffic
cdp
transceiver permit pid all
dot1q tunneling ethertype 0x9200
!
interface GigabitEthernet0/0/0/19.1881
description "Private Interface, Clear Traffic - VM1"
  ipv4 address 188.0.1.9 255.255.255.0
  ipv6 address 1881::9/64
  ipv6 enable
  encapsulation dot1q 1881
!
interface GigabitEthernet0/0/0/19.1882
description "Private Interface, Clear Traffic - VM2"
  ipv4 address 188.0.2.9 255.255.255.0
  ipv6 address 1882::9/64
  ipv6 enable
  encapsulation dot1q 1882
!
interface GigabitEthernet0/0/0/19.1883
description "Private Interface, Clear Traffic - VM3"
  ipv4 address 188.0.3.9 255.255.255.0
  ipv6 address 1883::9/64
  ipv6 enable
  encapsulation dot1q 1883
!
interface GigabitEthernet0/0/0/19.1884<clear-traffic_VLANid_VM4>
description "Private Interface, Clear Traffic - VM4"

ipv4 address 188.0.4.9 255.255.255.0
ipv6 address 1884::9/64
ipv6 enable
encapsulation dot1q 1884
!
interface GigabitEthernet0/0/0/20
  shutdown
!
interface GigabitEthernet0/0/0/21
  shutdown
!
interface GigabitEthernet0/0/0/22
  shutdown
!
interface GigabitEthernet0/0/0/23
  shutdown
!
interface GigabitEthernet0/0/0/24
  shutdown
!
interface GigabitEthernet0/0/0/25
  shutdown
!
interface GigabitEthernet0/0/0/26
  shutdown
!
interface GigabitEthernet0/0/0/27
  shutdown


! interface GigabitEthernet0/0/0/28
  shutdown
!

interface GigabitEthernet0/0/0/29
  shutdown
!

interface GigabitEthernet0/0/0/30
  shutdown
!

interface GigabitEthernet0/0/0/31
  shutdown
!

interface GigabitEthernet0/0/0/32
  shutdown
!

interface GigabitEthernet0/0/0/33
  shutdown
!

interface GigabitEthernet0/0/0/34
  shutdown
!

interface GigabitEthernet0/0/0/35
  shutdown
!

interface GigabitEthernet0/0/0/36
  shutdown
!

interface GigabitEthernet0/0/0/37
shutdown

!

interface GigabitEthernet0/0/0/38
shutdown
!

interface GigabitEthernet0/0/0/39
shutdown
!

interface TenGigE0/4/1/0
description "IKE and ESP traffic VM1"
transceiver permit pid all
dot1q tunneling ethertype 0x9200
!

interface TenGigE0/4/1/0.1871
description "IKE and ESP traffic for VM1"
ipv4 address 41.41.41.10 255.255.255.0
ipv6 address 2041::10/64
encapsulation dot1q 1871
!

interface TenGigE0/4/1/1
description "Clear and srp traffic VM1"
transceiver permit pid all
dot1q tunneling ethertype 0x9200
!

interface TenGigE0/4/1/1.1359
description "srp traffic VM1"
ipv4 address 81.81.81.10 255.255.255.0
ipv6 address 2081::10/64
encapsulation dot1q 1359
interface TenGigE0/4/1/1.1881
  description "clear traffic VM1"
  ipv4 address 61.61.61.10 255.255.255.0
  ipv6 address 2061::10/64
  encapsulation dot1q 1881

interface TenGigE0/4/1/2
  description "Management interface for VM1"
  transceiver permit pid all
  l2transport

interface TenGigE0/4/1/3
  description "IKE and ESP traffic VM2"
  transceiver permit pid all
  dot1q tunneling ethertype 0x9200

interface TenGigE0/4/1/3.1872
  description "IKE and ESP traffic for VM2"
  ipv4 address 42.42.42.10 255.255.255.0
  ipv6 address 2042::10/64
  encapsulation dot1q 1872

interface TenGigE0/4/1/4
  description "Clear and srp traffic VM2"
  transceiver permit pid all
  dot1q tunneling ethertype 0x9200
interface TenGigE0/4/1/4.1360
  description "srp traffic VM2"
  ipv4 address 82.82.82.10 255.255.255.0
  ipv6 address 2082::10/64
  encapsulation dot1q 1360
!
interface TenGigE0/4/1/4.1882
  description "clear traffic VM2"
  ipv4 address 62.62.62.10 255.255.255.0
  ipv6 address 2062::10/64
  encapsulation dot1q 1882
!
interface TenGigE0/4/1/5
  description "Management interface for VM2"
  transceiver permit pid all
  l2transport
!
interface TenGigE0/4/1/6
  description "IKE and ESP traffic VM3"
  transceiver permit pid all
  dot1q tunneling ethertype 0x9200
!
interface TenGigE0/4/1/6.1873
  description "IKE and ESP traffic for VM3"
  ipv4 address 43.43.43.10 255.255.255.0
  ipv6 address 2043::10/64
  encapsulation dot1q 1873
interface TenGigE0/4/1/7
   description "Clear and srp traffic VM3"
   transceiver permit pid all
   dot1q tunneling ethertype 0x9200

interface TenGigE0/4/1/7.1361
   description "srp traffic VM3"
   ipv4 address 83.83.83.10 255.255.255.0
   ipv6 address 2083::10/64
   encapsulation dot1q 1361

interface TenGigE0/4/1/7.1883
   description "clear traffic VM3"
   ipv4 address 63.63.63.10 255.255.255.0
   ipv6 address 2063::10/64
   encapsulation dot1q 1883

interface TenGigE0/4/1/8
   description "Management interface for VM3"
   transceiver permit pid all
   l2transport

interface TenGigE0/4/1/9
   description "IKE and ESP traffic VM4"
   transceiver permit pid all
   dot1q tunneling ethertype 0x9200
interface TenGigE0/4/1/9.1874
  description "IKE and ESP traffic for VM3"
  ipv4 address 44.44.44.10 255.255.255.0
  ipv6 address 2044::10/64
  encapsulation dot1q 1874
!
interface TenGigE0/4/1/10
  description "Clear and srp traffic VM4"
  transceiver permit pid all
  dot1q tunneling ethertype 0x9200
!
interface TenGigE0/4/1/10.1362
  description "srp traffic VM4"
  ipv4 address 84.84.84.10 255.255.255.0
  ipv6 address 2084::10/64
  encapsulation dot1q 1362
!
interface TenGigE0/4/1/10.1884
  description "clear traffic VM4"
  ipv4 address 64.64.64.10 255.255.255.0
  ipv6 address 2064::10/64
  encapsulation dot1q 1884
!
interface TenGigE0/4/1/11
  description "Management interface for VM4"
  transceiver permit pid all
  l2transport
!
!
interface BVI3
  ipv4 address 192.168.122.2 255.255.255.0
!
router static
  address-family ipv4 unicast
    10.78.0.0/16 MgmtEth0/RSP0/CPU0/0
    35.35.35.35/32 41.41.41.11
    36.36.36.36/32 42.42.42.11
    37.37.37.37/32 43.43.43.11
    38.38.38.38/32 44.44.44.11
    64.103.217.0/24 10.78.1.1
    65.65.0.0/16 188.0.1.100
    66.66.0.0/16 188.0.2.100
    67.67.0.0/16 188.0.3.100
    68.68.0.0/16 188.0.4.100
    81.81.81.0/24 GigabitEthernet0/0/0/5 87.87.87.10
    82.82.82.0/24 GigabitEthernet0/0/0/5 87.87.87.10
    83.83.83.0/24 GigabitEthernet0/0/0/5 87.87.87.10
    84.84.84.0/24 GigabitEthernet0/0/0/5 87.87.87.10
    92.0.0.0/8 187.0.1.11
    93.0.0.0/8 187.0.2.11
    94.0.0.0/8 187.0.3.11
    95.0.0.0/8 187.0.4.11
    202.153.144.25/32 8.40.0.1
!
  address-family ipv6 unicast
    2035::35/128 2041::11
    2036::36/128 2042::11
    2037::37/128 2044::11
l2vpn

xconnect group wsg

bridge group irb

bridge-domain irb1

interface TenGigE0/4/1/2

interface TenGigE0/4/1/5

interface TenGigE0/4/1/8

interface TenGigE0/4/1/11

routed interface BVI3

router hsrp
interface GigabitEthernet0/0/0/18.1871
address-family ipv4
hsrp 4
preempt
priority 101
address 187.0.1.20
track object WsgIPsla
track object PublicHsrp
!
!
address-family ipv6
hsrp 12
preempt
priority 101
track object WsgIPsla
track object PublicHsrp
address global 1871::20
address linklocal autoconfig
!
!
!
interface GigabitEthernet0/0/0/18.1872
address-family ipv4
hsrp 5
preempt
priority 101
address 187.0.2.20
track object WsgIPsla1
track object PublicHsrp
'address-family ipv6
hsrp 13
preempt
priority 101
track object WsgIPsla1
track object PublicHsrp
address global 1872::20
address linklocal autoconfig

interface GigabitEthernet0/0/0/18.1873
address-family ipv4
hsrp 6
preempt
priority 101
address 187.0.3.20
track object WsgIPsla2
track object PublicHsrp

interface GigabitEthernet0/0/0/18.1874
address-family ipv6
hsrp 14
preempt
priority 101
track object WsgIPsla2
track object PublicHsrp
address global 1873::20
address linklocal autoconfig
!

address-family ipv4
hsrp 7
preempt
priority 101
address 187.0.4.20
track object WsgIPsla3
track object PublicHsrp
!

address-family ipv6
hsrp 15
preempt
priority 101
track object WsgIPsla3
track object PublicHsrp
address global 1874::20
address linklocal autoconfig
!

!

interface GigabitEthernet0/0/19.1881
address-family ipv4
hsrp 8
preempt
priority 101
address 188.0.1.20
track object WsgIPsla
track object PublicHsrp
!
!
address-family ipv6
hsrp 16
preempt
priority 101
track object WsgIPsla
track object PublicHsrp
address global 1881::20
address linklocal autoconfig
!
!
!
interface GigabitEthernet0/0/0/19.1882
address-family ipv4
hsrp 9
preempt
priority 101
address 188.0.2.20
track object WsgIPslal
track object PublicHsrp
!
!
address-family ipv6

hsrp 17
preempt
priority 101
track object WsgIPsla1
track object PublicHsrp
address global 1882::20
address linklocal autoconfig
!
!
!
interface GigabitEthernet0/0/0/19.1883

address-family ipv4

hsrp 10
preempt
priority 101
address 188.0.3.20
track object WsgIPsla2
track object PublicHsrp
!
!
!

address-family ipv6

hsrp 18
preempt
priority 101
track object WsgIPsla2
track object PublicHsrp
address global 1883::20
address linklocal autoconfig
interface GigabitEthernet0/0/0/19.1884
address-family ipv4
hsrp 11
preempt
priority 101
address 188.0.4.20
track object WsgIPsla3
track object PublicHsrp
!
!
address-family ipv6
hsrp 19
preempt
priority 101
track object WsgIPsla3
track object PublicHsrp
address global 1884::20
address linklocal autoconfig
!
!
!
ipsla
operation 200
type icmp echo
destination address 41.41.41.100
timeout 300
frequency 1
!
!
operation 201
type icmp echo
destination address 42.42.42.100
timeout 300
frequency 1
!
!
operation 202
type icmp echo
destination address 43.43.43.100
timeout 300
frequency 1
!
!
operation 203
type icmp echo
destination address 44.44.44.100
timeout 300
frequency 1
!
!
schedule operation 200
start-time now
life forever
!
schedule operation 201
  start-time now
  life forever
!
schedule operation 202
  start-time now
  life forever
!
schedule operation 203
  start-time now
  life forever
!
!
track WsgIPsla
  type rtr 200 reachability
delay up 1
delay down 1
!
track WsgIPsla1
  type rtr 201 reachability
delay up 1
delay down 1
!
track WsgIPsla2
  type rtr 202 reachability
delay up 1
delay down 1
!
track WsgIPsla3
type rtr 203 reachability

delay up 1

delay down 1
!

track PublicHsrp

type line-protocol state

    interface GigabitEthernet0/0/0/18
!

delay up 1

delay down
!

crypto ca trustpoint onep-tp

crl optional

    subject-name CN=<ASR9K_backup_hostname>.<domain_name>

    enrollment url terminal
!

end
SecGW VM Configuration (StarOS)

**Important:** Each SecGW (CPU-VM complex) must be separately configured as described below for corresponding VSMs in both the primary and backup ASR 9000 chassis. There are four CPU-VM complexes per ASR 9000 VSM.

The unique parameters for each CPU-VM complex must correspond with interface settings configured for the primary and backup ASR 9000 chassis.

Notes:
- Enable hidden CLI test-commands.
- Install SecGW License.
- Assign unique host name per CPU-VM complex.
- Set crash log size to 2048 with compression.
- Require Session Recovery.
- Create local context with unique parameters per CPU-VM complex.
- Enable wsg-service with unique parameters per CPU-VM complex.
- Create SRP context with unique parameters per CPU-VM complex.
- Enable Connected Apps session with unique password and session name per CPU-VM complex.
- Set wsg-lookup priorities.
- Appropriately configure ethernet ports with unique parameters per CPU-VM complex. Refer to the tables below for mapping of sample IP addresses for each SecGW.

### Table 5. StarOS IP Address Mapping - SecGW1

<table>
<thead>
<tr>
<th>Variable</th>
<th>Primary ASR 9000</th>
<th>Backup ASR 9000</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>&lt;interfaces LOCAL1_IPv4-address&gt;</code></td>
<td>100.100.100.1 255.255.255.0</td>
<td>192.168.122.15 255.255.255.0</td>
</tr>
<tr>
<td><code>&lt;iproute LOCAL1_IPv4-address_mask&gt;</code></td>
<td>0.0.0.0 0.0.0.0 100.100.100.10</td>
<td>0.0.0.0 0.0.0.0 192.168.122.2</td>
</tr>
<tr>
<td><code>&lt;wsg_acl1_permit_IPv4-address_mask&gt;</code></td>
<td>65.65.0.0 0.0.255.255 45.45.0.0 0.0.255.255</td>
<td>65.65.0.0 0.0.255.255 45.45.0.0 0.0.255.255</td>
</tr>
<tr>
<td><code>&lt;wsg_acl1_permit_IPv6-address_mask&gt;</code></td>
<td>2065::::ffff::ffff:ffff:ffff</td>
<td>2065::::ffff::ffff:ffff</td>
</tr>
<tr>
<td></td>
<td>2045::::ffff::ffff:ffff:ffff</td>
<td>2045::::ffff::ffff:ffff:ffff</td>
</tr>
<tr>
<td><code>&lt;wsg_pool1_IPv4-address&gt;</code></td>
<td>45.45.0.1 45.45.58.254</td>
<td>45.45.0.1 45.45.58.254</td>
</tr>
<tr>
<td><code>&lt;wsg_pool1_IPv6-address_mask&gt;</code></td>
<td>2045::56</td>
<td>2045::56</td>
</tr>
<tr>
<td><code>&lt;crypto_foo_local_IPv4-address&gt;</code></td>
<td>35.35.35.35</td>
<td>35.35.35.35</td>
</tr>
<tr>
<td><code>&lt;crypto_foo-1_local_IPv6-address&gt;</code></td>
<td>2035::35</td>
<td>2035::35</td>
</tr>
<tr>
<td><code>&lt;wsg_interface_clear_IPv4-address_mask&gt;</code></td>
<td>51.51.11 255.255.255.0</td>
<td>61.61.11 255.255.255.0</td>
</tr>
<tr>
<td>Variable</td>
<td>Primary ASR 9000</td>
<td>Backup ASR 9000</td>
</tr>
<tr>
<td>-------------------------------------------------------------------------</td>
<td>---------------------------------------</td>
<td>---------------------------------------</td>
</tr>
<tr>
<td>&lt;wsg_interface_clear_IPv6-address/mask&gt;</td>
<td>2051::11/64</td>
<td>2061::11/64</td>
</tr>
<tr>
<td>&lt;wsg_interface_ike_IPv4-address_mask&gt;</td>
<td>31.31.31.11 255.255.255.0</td>
<td>41.41.41.11 255.255.255.0</td>
</tr>
<tr>
<td>&lt;wsg_interface_ike_IPv6-address/mask&gt;</td>
<td>2031::11/64</td>
<td>2041::11/64</td>
</tr>
<tr>
<td>&lt;wsg_interface_ike-loop_IPv4-address_mask&gt;</td>
<td>35.35.35.35 255.255.255.255</td>
<td>35.35.35.35 255.255.255.255</td>
</tr>
<tr>
<td>&lt;wsg_interface_ike-loop_IPv6-address/mask&gt;</td>
<td>2035::35/128</td>
<td>2035::35/128</td>
</tr>
<tr>
<td>&lt;wsg_interface_ike-loop1_IPv4-address_mask&gt;</td>
<td>31.31.31.100 255.255.255.255</td>
<td>41.41.41.100 255.255.255.255</td>
</tr>
<tr>
<td>&lt;wsg-service_bind_IPv4-address&gt;</td>
<td>35.35.35.35</td>
<td>35.35.35.35</td>
</tr>
<tr>
<td>&lt;wsg-service_bind_IPv6-address&gt;</td>
<td>2035::35</td>
<td>2035::35</td>
</tr>
<tr>
<td>&lt;wsg_iproute_clear_IPv4-address_mask&gt;</td>
<td>65.65.0.0 255.255.255.0</td>
<td>65.65.0.0 255.255.255.0</td>
</tr>
<tr>
<td>&lt;wsg_iproute_clear_IPv4-address&gt;</td>
<td>51.51.51.10</td>
<td>61.61.61.10</td>
</tr>
<tr>
<td>&lt;wsg_iproute_ike1_IPv4-address_mask&gt;</td>
<td>187.0.1.0 255.255.255.0</td>
<td>187.0.1.0 255.255.255.0</td>
</tr>
<tr>
<td>&lt;wsg_iproute_ike1_IPv4-address&gt;</td>
<td>31.31.31.10</td>
<td>41.41.41.10</td>
</tr>
<tr>
<td>&lt;wsg_iproute_ike2_IPv4-address_mask&gt;</td>
<td>92.0.0.0 255.0.0 255.0.0.0</td>
<td>92.0.0.0 255.0.0 255.0.0.0</td>
</tr>
<tr>
<td>&lt;wsg_iproute_ike2_IPv4-address&gt;</td>
<td>31.31.31.10</td>
<td>41.41.41.10</td>
</tr>
<tr>
<td>&lt;wsg_iproute_ike3_IPv4-address_mask&gt;</td>
<td>188.0.1.0 255.255.255.0</td>
<td>188.0.1.0 255.255.255.0</td>
</tr>
<tr>
<td>&lt;wsg_iproute_ike3_IPv4-address&gt;</td>
<td>31.31.31.10</td>
<td>41.41.41.10</td>
</tr>
<tr>
<td>&lt;wsg_iproute_clear_IPv6-address/mask&gt;</td>
<td>2065::/64</td>
<td>2065::/64</td>
</tr>
<tr>
<td>&lt;wsg_iproute_clear_nexthop_IPv6-address&gt;</td>
<td>2051::10</td>
<td>2061::10</td>
</tr>
<tr>
<td>&lt;wsg_iproute_ike1_IPv6-address/mask&gt;</td>
<td>2092::/64</td>
<td>2092::/64</td>
</tr>
<tr>
<td>&lt;wsg_iproute_ike1_nexthop_IPv6-address&gt;</td>
<td>2031::10</td>
<td>2041::10</td>
</tr>
<tr>
<td>&lt;wsg_iproute_ike2_IPv6-address/mask&gt;</td>
<td>1871::/64</td>
<td>1871::/64</td>
</tr>
<tr>
<td>&lt;wsg_iproute_ike2_nexthop_IPv6-address&gt;</td>
<td>2031::10</td>
<td>2041::10</td>
</tr>
<tr>
<td>&lt;wsg_iproute_ike2_IPv6-address/mask&gt;</td>
<td>1881::/64</td>
<td>1881::/64</td>
</tr>
<tr>
<td>&lt;wsg_iproute_ike2_nexthop_IPv6-address&gt;</td>
<td>2031::10</td>
<td>2041::10</td>
</tr>
<tr>
<td>&lt;wsg_rri_nexthop_IPv4-address&gt;</td>
<td>51.51.51.11</td>
<td>61.61.61.11</td>
</tr>
<tr>
<td>&lt;wsg_rri_nexthop_IPv6-address&gt;</td>
<td>—</td>
<td>—</td>
</tr>
<tr>
<td>&lt;srp_monitor_hsrp_vlan_id&gt;</td>
<td>1871</td>
<td>1871</td>
</tr>
<tr>
<td>&lt;srp_hsrp-group_number&gt;</td>
<td>4</td>
<td>4</td>
</tr>
<tr>
<td>&lt;srp_peer_IPv4-address&gt;</td>
<td>81.81.81.11</td>
<td>71.71.71.11</td>
</tr>
<tr>
<td>&lt;srp_bind_IPv4-address&gt;</td>
<td>71.71.71.11</td>
<td>81.81.81.11</td>
</tr>
<tr>
<td>&lt;srp_interface_icsr_IPv4-address_mask&gt;</td>
<td>71.71.71.11 255.255.255.255</td>
<td>81.81.81.11 255.255.255.255</td>
</tr>
<tr>
<td>&lt;srp_iproute_icsr_IPv4-address_mask&gt;</td>
<td>81.81.81.0 255.255.255.255</td>
<td>71.71.71.0 255.255.255.255</td>
</tr>
<tr>
<td>Variable</td>
<td>Primary ASR 9000</td>
<td>Backup ASR 9000</td>
</tr>
<tr>
<td>----------------------------------------------</td>
<td>----------------------</td>
<td>---------------------</td>
</tr>
<tr>
<td>&lt;srp_iproute_icsr_IPv4-address&gt;</td>
<td>71.71.71.10</td>
<td>81.81.81.10</td>
</tr>
<tr>
<td>&lt;connectedapps_session_IPv4-address&gt;</td>
<td>100.100.100.10</td>
<td>192.168.122.2</td>
</tr>
<tr>
<td>&lt;port_1/10_vlan_id&gt;</td>
<td>—</td>
<td>—</td>
</tr>
<tr>
<td>&lt;port_1/11_vlan_id_srp&gt;</td>
<td>1259</td>
<td>1871</td>
</tr>
<tr>
<td>&lt;port_1/11_vlan_id_wsg&gt;</td>
<td>1881</td>
<td>1881</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Table 6. StarOS IP Address Mapping - SecGW2</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Variable</th>
<th>Primary ASR 9000</th>
<th>Backup ASR 9000</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;interface_LOCAL1_IPv4-address&gt;</td>
<td>100.100.100.2 255.255.255.0</td>
<td>192.168.122.16 255.255.255.0</td>
</tr>
<tr>
<td>&lt;iproute_LOCAL1_IPv4-address_mask&gt;</td>
<td>0.0.0.0 0.0.0.0 100.100.100.10</td>
<td>0.0.0.0 0.0.0.0 192.168.122.2</td>
</tr>
<tr>
<td>&lt;wsg_acl1_permit_IPv4-address_mask&gt;</td>
<td>66.66.0.0 0.0.255.255 46.46.0.0 0.0.255.255</td>
<td>66.66.0.0 0.0.255.255 46.46.0.0 0.0.255.255</td>
</tr>
<tr>
<td>&lt;wsg_pool1_IPv4-address&gt;</td>
<td>46.46.0.1 46.46.58.254</td>
<td>46.46.0.1 46.46.58.254</td>
</tr>
<tr>
<td>&lt;wsg_pool1_IPv6-address/mask&gt;</td>
<td>2046::/56</td>
<td>2046::/56</td>
</tr>
<tr>
<td>&lt;crypto_foo_local_IPv4-address&gt;</td>
<td>36.36.36.36</td>
<td>36.36.36.36</td>
</tr>
<tr>
<td>&lt;crypto_foo-1_local_IPv6-address&gt;</td>
<td>2036::36</td>
<td>2036::36</td>
</tr>
<tr>
<td>&lt;wsg_interface_clear_IPv4-address_mask&gt;</td>
<td>52.52.52.11 255.255.255.0</td>
<td>62.62.62.11 255.255.255.0</td>
</tr>
<tr>
<td>&lt;wsg_interface_clear_IPv6-address/mask&gt;</td>
<td>2052::11/64</td>
<td>2062::11/64</td>
</tr>
<tr>
<td>&lt;wsg_interface_ike_IPv4-address_mask&gt;</td>
<td>52.52.52.11 255.255.255.0</td>
<td>42.42.42.12 255.255.255.0</td>
</tr>
<tr>
<td>&lt;wsg_interface_ike_IPv6-address_mask&gt;</td>
<td>2032::11/64</td>
<td>2042::11/64</td>
</tr>
<tr>
<td>&lt;wsg_interface_ike-loop_IPv4-address_mask&gt;</td>
<td>36.36.36.36 255.255.255.255</td>
<td>36.36.36.36 255.255.255.255</td>
</tr>
<tr>
<td>&lt;wsg_interface_ike-loop_IPv6-address_mask&gt;</td>
<td>2036::36/128</td>
<td>2036::36/128</td>
</tr>
<tr>
<td>&lt;wsg_interface_ike-loop1_IPv4-address_mask&gt;</td>
<td>32.32.32.100 255.255.255.255</td>
<td>42.42.42.100 255.255.255.255</td>
</tr>
<tr>
<td>&lt;wsg-service_bind_IPv4-address&gt;</td>
<td>36.36.36.36</td>
<td>36.36.36.36</td>
</tr>
<tr>
<td>&lt;wsg-service_bind_IPv6-address&gt;</td>
<td>2036::36</td>
<td>2036::36</td>
</tr>
<tr>
<td>&lt;wiproute_clear_IPv4-address_mask&gt;</td>
<td>66.66.0.0 255.255.0.0</td>
<td>66.66.0.0 255.255.0.0</td>
</tr>
<tr>
<td>&lt;wiproute_clear_IPv4-address&gt;</td>
<td>52.52.52.10</td>
<td>62.62.62.10</td>
</tr>
<tr>
<td>&lt;wiproute_ike1_IPv4-address_mask&gt;</td>
<td>187.0.2.0 255.255.255.0</td>
<td>187.0.2.0 255.255.255.0</td>
</tr>
<tr>
<td>&lt;wiproute_ike1_IPv4-address&gt;</td>
<td>32.32.32.10</td>
<td>42.42.42.10</td>
</tr>
</tbody>
</table>
### Sample L2 Interchassis HA Configuration

#### SecGW VM Configuration (StarOS)

<table>
<thead>
<tr>
<th>Variable</th>
<th>Primary ASR 9000</th>
<th>Backup ASR 9000</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;wsg_iproute_ike2_IPv4-address_mask&gt;</td>
<td>93.0.0.0 255.0.0.0</td>
<td>93.0.0.0 255.0.0.0</td>
</tr>
<tr>
<td>&lt;wsg_iproute_ike2_IPv4-address&gt;</td>
<td>32.32.32.10</td>
<td>42.42.42.10</td>
</tr>
<tr>
<td>&lt;wsg_iproute_ike3_IPv4-address_mask&gt;</td>
<td>188.0.2.0 255.255.255.0</td>
<td>188.0.2.0 255.255.255.0</td>
</tr>
<tr>
<td>&lt;wsg_iproute_ike3_IPv4-address&gt;</td>
<td>32.32.32.10</td>
<td>42.42.42.10</td>
</tr>
<tr>
<td>&lt;wsg_iproute_clear_IPv6-address_mask&gt;</td>
<td>2066::/64</td>
<td>2066::/64</td>
</tr>
<tr>
<td>&lt;wsg_iproute_clear_nexthop_IPv6-address&gt;</td>
<td>2052::10</td>
<td>2062::10</td>
</tr>
<tr>
<td>&lt;wsg_iproute_ike1_IPv6-address_mask&gt;</td>
<td>2093::/64</td>
<td>2093::/64</td>
</tr>
<tr>
<td>&lt;wsg_iproute_ike1_nexthop_IPv6-address&gt;</td>
<td>2032::10</td>
<td>2042::10</td>
</tr>
<tr>
<td>&lt;wsg_iproute_ike2_IPv6-address_mask&gt;</td>
<td>1872::/64</td>
<td>1872::/64</td>
</tr>
<tr>
<td>&lt;wsg_iproute_ike2_nexthop_IPv6-address&gt;</td>
<td>2032::10</td>
<td>2042::10</td>
</tr>
<tr>
<td>&lt;wsg_iproute_ike2_IPv6-address&gt;</td>
<td>1882::/64</td>
<td>1882::/64</td>
</tr>
<tr>
<td>&lt;wsg_iproute_ike2_nexthop_IPv6-address&gt;</td>
<td>2032::10</td>
<td>2042::10</td>
</tr>
<tr>
<td>&lt;wsg_rri_nexthop_IPv4-address&gt;</td>
<td>52.52.52.11</td>
<td>62.62.62.11</td>
</tr>
<tr>
<td>&lt;wsg_rri_nexthop_IPv6-address&gt;</td>
<td>2052::11</td>
<td>2062::1</td>
</tr>
<tr>
<td>&lt;srp_monitor_hsrp_vlan_id&gt;</td>
<td>1872</td>
<td>1872</td>
</tr>
<tr>
<td>&lt;srp_hsrp-group_number&gt;</td>
<td>5</td>
<td>5</td>
</tr>
<tr>
<td>&lt;srp_peer_IPv4-address&gt;</td>
<td>82.82.82.11</td>
<td>72.72.72.11</td>
</tr>
<tr>
<td>&lt;srp_bind_IPv4-address&gt;</td>
<td>72.72.72.11</td>
<td>82.82.82.11</td>
</tr>
<tr>
<td>&lt;srp_interface_icsr_IPv4-address_mask&gt;</td>
<td>72.72.72.11 255.255.255.0</td>
<td>82.82.82.11 255.255.255.0</td>
</tr>
<tr>
<td>&lt;srp_iproute_icsr_IPv4-address_mask&gt;</td>
<td>82.82.82.0 255.255.255.0</td>
<td>71.71.71.0 255.255.255.0</td>
</tr>
<tr>
<td>&lt;srp_iproute_icsr_IPv6-address&gt;</td>
<td>72.72.72.11</td>
<td>82.82.82.11</td>
</tr>
<tr>
<td>&lt;connectedapps_session_IPv4-address&gt;</td>
<td>100.100.100.10</td>
<td>192.168.122.2</td>
</tr>
<tr>
<td>&lt;port_1/10_vlan_id&gt;</td>
<td>—</td>
<td>—</td>
</tr>
<tr>
<td>&lt;port_1/11_vlan_id_srp&gt;</td>
<td>1260</td>
<td>1360</td>
</tr>
<tr>
<td>&lt;port_1/11_vlan_id_wsg&gt;</td>
<td>1882</td>
<td>1882</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Variable</th>
<th>Primary ASR 9000</th>
<th>Backup ASR 9000</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;interface LOCAL1_IPv4-address&gt;</td>
<td>100.100.100.3 255.255.255.0</td>
<td>192.168.122.17 255.255.255.0</td>
</tr>
<tr>
<td>&lt;iproute LOCAL1_IPv4-address_mask&gt;</td>
<td>0.0.0.0 0.0.0.0 100.100.100.10</td>
<td>0.0.0.0 0.0.0.0 192.168.122.2</td>
</tr>
</tbody>
</table>

Table 7. StarOS IP Address Mapping - SecGW3
<table>
<thead>
<tr>
<th>Variable</th>
<th>Primary ASR 9000</th>
<th>Backup ASR 9000</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;wsg_ac11_permit_IPv4-address_mask&gt;</td>
<td>67.67.0.0 0.0.255.255 47.47.0.0 0.0.255.255</td>
<td>67.67.0.0 0.0.255.255 47.47.0.0 0.0.255.255</td>
</tr>
<tr>
<td>&lt;wsg_pool1_IPv4-address&gt;</td>
<td>47.47.0.1 47.47.58.254</td>
<td>47.47.0.1 47.47.58.254</td>
</tr>
<tr>
<td>&lt;wsg_pool1_IPv6-address/mask&gt;</td>
<td>2047::/56</td>
<td>2047::/56</td>
</tr>
<tr>
<td>&lt;crypto_foo_local_IPv4-address&gt;</td>
<td>37.37.37.37</td>
<td>37.37.37.37</td>
</tr>
<tr>
<td>&lt;crypto_foo-1_local_IPv6-address&gt;</td>
<td>2037:37</td>
<td>2037:37</td>
</tr>
<tr>
<td>&lt;wsg_interface_clear_IPv4-address_mask&gt;</td>
<td>53.53.53.11 255.255.255.0</td>
<td>63.63.63.11 255.255.255.0</td>
</tr>
<tr>
<td>&lt;wsg_interface_clear_IPv6-address/mask&gt;</td>
<td>2053::11/64</td>
<td>2063::11/64</td>
</tr>
<tr>
<td>&lt;wsg_interface_ike_IPv4-address_mask&gt;</td>
<td>33.33.33.11 255.255.255.0</td>
<td>43.43.43.12 255.255.255.0</td>
</tr>
<tr>
<td>&lt;wsg_interface_ike_IPv6-address/mask&gt;</td>
<td>2033::11/64</td>
<td>2043::11/64</td>
</tr>
<tr>
<td>&lt;wsg_interface_ike-loop_IPv4-address_mask&gt;</td>
<td>37.37.37.37 255.255.255.255</td>
<td>37.37.37.37 255.255.255.255</td>
</tr>
<tr>
<td>&lt;wsg_interface_ike-loop_IPv6-address/mask&gt;</td>
<td>2037::37/128</td>
<td>2037::37/128</td>
</tr>
<tr>
<td>&lt;wsg_interface_ike-loop1_IPv4-address_mask&gt;</td>
<td>33.33.33.100 255.255.255.255</td>
<td>43.43.43.100 255.255.255.255</td>
</tr>
<tr>
<td>&lt;wsg-service_bind_IPv4-address&gt;</td>
<td>37.37.37.37</td>
<td>37.37.37.37</td>
</tr>
<tr>
<td>&lt;wsg-service_bind_IPv6-address&gt;</td>
<td>2037:37</td>
<td>2037:37</td>
</tr>
<tr>
<td>&lt;wsg_iproute_clear_IPv4-address_mask&gt;</td>
<td>67.67.0.0 255.255.0.0</td>
<td>67.67.0.0 255.255.0.0</td>
</tr>
<tr>
<td>&lt;wsg_iproute_clear_IPv4-address&gt;</td>
<td>53.53.53.10</td>
<td>63.63.63.10</td>
</tr>
<tr>
<td>&lt;wsg_iproute_ike1_IPv4-address_mask&gt;</td>
<td>187.0.3.0 255.255.255.0</td>
<td>187.0.3.0 255.255.255.0</td>
</tr>
<tr>
<td>&lt;wsg_iproute_ike1_IPv4-address&gt;</td>
<td>33.33.33.10</td>
<td>43.43.43.10</td>
</tr>
<tr>
<td>&lt;wsg_iproute_ike2_IPv4-address_mask&gt;</td>
<td>94.0.0.0 255.0.0.0</td>
<td>94.0.0.0 255.0.0.0</td>
</tr>
<tr>
<td>&lt;wsg_iproute_ike2_IPv4-address&gt;</td>
<td>33.33.33.10</td>
<td>43.43.43.10</td>
</tr>
<tr>
<td>&lt;wsg_iproute_ike3_IPv4-address_mask&gt;</td>
<td>188.0.3.0 255.255.255.0</td>
<td>188.0.3.0 255.255.255.0</td>
</tr>
<tr>
<td>&lt;wsg_iproute_ike3_IPv4-address&gt;</td>
<td>33.33.33.10</td>
<td>43.43.43.10</td>
</tr>
<tr>
<td>&lt;wsg_iproute_clear_IPv6-address_mask&gt;</td>
<td>2067::/64</td>
<td>2067::/64</td>
</tr>
<tr>
<td>&lt;wsg_iproute_clear_nexthop_IPv6-address&gt;</td>
<td>2053::10</td>
<td>2063::10</td>
</tr>
<tr>
<td>&lt;wsg_iproute_ike1_IPv6-address_mask&gt;</td>
<td>2094::/64</td>
<td>2094::/64</td>
</tr>
<tr>
<td>&lt;wsg_iproute_ike1_nexthop_IPv6-address&gt;</td>
<td>2033::10</td>
<td>2043::10</td>
</tr>
<tr>
<td>&lt;wsg_iproute_ike2_IPv6-address_mask&gt;</td>
<td>1873::/64</td>
<td>1873::/64</td>
</tr>
<tr>
<td>&lt;wsg_iproute_ike2_nexthop_IPv6-address&gt;</td>
<td>2033:10</td>
<td>2043:10</td>
</tr>
<tr>
<td>&lt;wsg_iproute_ike2_IPv6-address_mask&gt;</td>
<td>1883::/64</td>
<td>1883::/64</td>
</tr>
</tbody>
</table>
### Table 8. StarOS IP Address Mapping - SecGW4

<table>
<thead>
<tr>
<th>Variable</th>
<th>Primary ASR 9000</th>
<th>Backup ASR 9000</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;interface_LOCAL1_IPv4-address&gt;</td>
<td>100.100.100.4 255.255.255.255.0</td>
<td>192.168.122.18 255.255.255.255.0</td>
</tr>
<tr>
<td>&lt;iproute_LOCAL1_IPv4-address_mask&gt;</td>
<td>0.0.0.0 0.0.0.0 100.100.100.10</td>
<td>0.0.0.0 0.0.0.0 192.168.122.2</td>
</tr>
<tr>
<td>&lt;wsg_ac11_permit_IPv4-address_mask&gt;</td>
<td>68.68.0.0 0.0.255.255</td>
<td>68.68.0.0 0.0.255.255</td>
</tr>
<tr>
<td></td>
<td>48.48.0.0 0.0.255.255</td>
<td>48.48.0.0 0.0.255.255</td>
</tr>
<tr>
<td>&lt;wsg_pool1_IPv4-address&gt;</td>
<td>48.48.0.1</td>
<td>48.48.0.1</td>
</tr>
<tr>
<td></td>
<td>48.48.58.254</td>
<td>48.48.58.254</td>
</tr>
<tr>
<td>&lt;wsg_pool1_IPv6-address/mask&gt;</td>
<td>2048::/56</td>
<td>2048::/56</td>
</tr>
<tr>
<td>&lt;crypto_foo_local_IPv4-address&gt;</td>
<td>38.38.38.38</td>
<td>38.38.38.38</td>
</tr>
<tr>
<td>&lt;crypto_foo-1_local_IPv6-address&gt;</td>
<td>2038::38</td>
<td>2038::38</td>
</tr>
<tr>
<td>&lt;wsg_interface_clear_IPv4-address_mask&gt;</td>
<td>54.54.54.11 255.255.255.255.0</td>
<td>64.64.64.11 255.255.255.255.0</td>
</tr>
<tr>
<td>&lt;wsg_interface_clear_IPv6-address_mask&gt;</td>
<td>2054::11/64</td>
<td>2064::11/64</td>
</tr>
<tr>
<td>&lt;wsg_interface_ike_IPv4-address_mask&gt;</td>
<td>34.34.34.11 255.255.255.255.0</td>
<td>44.44.44.12 255.255.255.255.0</td>
</tr>
<tr>
<td>&lt;wsg_interface_ike_IPv6-address_mask&gt;</td>
<td>2034::11/64</td>
<td>2044::11/64</td>
</tr>
<tr>
<td>Variable</td>
<td>Primary ASR 9000</td>
<td>Backup ASR 9000</td>
</tr>
<tr>
<td>----------------------------------------------</td>
<td>----------------------------------------</td>
<td>---------------------------------------</td>
</tr>
<tr>
<td><code>&lt;wsg_interface_ike-loop_IPv4-address_mask&gt;</code></td>
<td>38.38.38.38 255.255.255 255.255.255</td>
<td>38.38.38.38 255.255.255 255.255.255</td>
</tr>
<tr>
<td><code>&lt;wsg_interface_ike-loop_IPv6-address&gt;</code></td>
<td>2038::38/128</td>
<td>2038::38/128</td>
</tr>
<tr>
<td><code>&lt;wsg_interface_ike-loop1_IPv4-address_mask&gt;</code></td>
<td>34.34.34.100 255.255.255 255.255.255</td>
<td>44.44.44.100 255.255.255 255.255.255</td>
</tr>
<tr>
<td><code>&lt;wsg-service_bind_IPv4-address&gt;</code></td>
<td>38.38.38.38</td>
<td>38.38.38.38</td>
</tr>
<tr>
<td><code>&lt;wsg-service_bind_IPv6-address&gt;</code></td>
<td>2038::38</td>
<td>2038::38</td>
</tr>
<tr>
<td><code>&lt;wsg_iproute_clear_IPv4-address_mask&gt;</code></td>
<td>68.68.0.0 255.255.0 255.255.0.0</td>
<td>68.68.0.0 255.255.0 255.255.0.0</td>
</tr>
<tr>
<td><code>&lt;wsg_iproute_clear_IPv4-address&gt;</code></td>
<td>54.54.54.10</td>
<td>64.64.64.10</td>
</tr>
<tr>
<td><code>&lt;wsg_iproute_ike1_IPv4-address&gt;</code></td>
<td>187.0.4.0 255.255.255.0</td>
<td>187.0.4.0 255.255.255.0</td>
</tr>
<tr>
<td><code>&lt;wsg_iproute_ike1_IPv4-address&gt;</code></td>
<td>34.34.34.10</td>
<td>44.44.44.10</td>
</tr>
<tr>
<td><code>&lt;wsg_iproute_ike2_IPv4-address_mask&gt;</code></td>
<td>95.0.0.0 255.0.0.0 255.0.0.0</td>
<td>95.0.0.0 255.0.0.0 255.0.0.0</td>
</tr>
<tr>
<td><code>&lt;wsg_iproute_ike2_IPv4-address&gt;</code></td>
<td>34.34.34.10</td>
<td>44.44.44.10</td>
</tr>
<tr>
<td><code>&lt;wsg_iproute_ike3_IPv4-address_mask&gt;</code></td>
<td>188.0.4.0 255.255.255.0</td>
<td>188.0.4.0 255.255.255.0</td>
</tr>
<tr>
<td><code>&lt;wsg_iproute_ike3_IPv4-address&gt;</code></td>
<td>34.34.34.10</td>
<td>44.44.44.10</td>
</tr>
<tr>
<td><code>&lt;wsg_iproute_clear_IPv6-address_mask&gt;</code></td>
<td>2068::64</td>
<td>2068::64</td>
</tr>
<tr>
<td><code>&lt;wsg_iproute_clear_nexthop_IPv6-address&gt;</code></td>
<td>2054::10</td>
<td>2064::10</td>
</tr>
<tr>
<td><code>&lt;wsg_iproute_ike1_IPv6-address&gt;</code></td>
<td>2095::64</td>
<td>2095::64</td>
</tr>
<tr>
<td><code>&lt;wsg_iproute_ike1_nexthop_IPv6-address&gt;</code></td>
<td>2034::10</td>
<td>2044::10</td>
</tr>
<tr>
<td><code>&lt;wsg_iproute_ike2_nexthop_IPv6-address&gt;</code></td>
<td>1874::64</td>
<td>1874::64</td>
</tr>
<tr>
<td><code>&lt;wsg_iproute_ike2_IPv6-address&gt;</code></td>
<td>2034::10</td>
<td>2044::10</td>
</tr>
<tr>
<td><code>&lt;wsg_iproute_ike2_nexthop_IPv6-address&gt;</code></td>
<td>1884::64</td>
<td>1884::64</td>
</tr>
<tr>
<td><code>&lt;wsg_rri_nexthop_IPv4-address&gt;</code></td>
<td>54.54.54.11</td>
<td>64.64.64.11</td>
</tr>
<tr>
<td><code>&lt;srp_monitor_hsrp_vlan_id&gt;</code></td>
<td>1874</td>
<td>1874</td>
</tr>
<tr>
<td><code>&lt;srp_hsrp-group_number&gt;</code></td>
<td>7</td>
<td>7</td>
</tr>
<tr>
<td><code>&lt;srp_peer_IPv4-address&gt;</code></td>
<td>84.84.84.11</td>
<td>74.74.74.11</td>
</tr>
<tr>
<td><code>&lt;srp_bind_IPv4-address&gt;</code></td>
<td>74.74.74.11</td>
<td>84.84.84.11</td>
</tr>
<tr>
<td><code>&lt;srp_interface_icsr_IPv4-address_mask&gt;</code></td>
<td>74.74.74.11 255.255.255.0 255.255.255.0</td>
<td>84.84.84.11 255.255.255.0 255.255.255.0</td>
</tr>
<tr>
<td><code>&lt;srp_iproute_icsr_IPv4-address_mask&gt;</code></td>
<td>84.84.84.0 255.255.255.0 255.255.255.0</td>
<td>74.74.74.0 255.255.255.0 255.255.255.0</td>
</tr>
<tr>
<td><code>&lt;srp_iproute_icsr_IPv4-address&gt;</code></td>
<td>74.74.74.11</td>
<td>84.84.84.11</td>
</tr>
<tr>
<td><code>&lt;connectedapps_session_IPv4-address&gt;</code></td>
<td>100.100.100.10</td>
<td>192.168.122.2</td>
</tr>
<tr>
<td><code>&lt;port_1/10_vlan_id&gt;</code></td>
<td>1874</td>
<td>1874</td>
</tr>
</tbody>
</table>
### SecGW VM Configuration - Primary ASR 9000 Chassis

```plaintext
config
  cli hidden
  tech-support test-commands encrypted password <unique_encrypted_password>
  cli test-commands encrypted password <unique_encrypted_password>
  license key "\n  <SecGW_license_key>
  system hostname <ASR9K_hostname>-<SecGW#>
  orbem
    no siop-port
    no iiop-port
#exit
  crash max-size 2048 compression gzip
  require session recovery
  context local
    no ip guarantee framed-route local-switching
  interface LOCAL1
    ip address <LOCAL1_IPv4-address>
#exit
  server ftpd
#exit
  ssh key
  <unique_encrypted_ssh_key1>
  ssh key
```

<table>
<thead>
<tr>
<th>Variable</th>
<th>Primary ASR 9000</th>
<th>Backup ASR 9000</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;port_1/11_vlan_id_srp&gt;</td>
<td>1262</td>
<td>1362</td>
</tr>
<tr>
<td>&lt;port_1/11_vlan_id_wsg&gt;</td>
<td>1884</td>
<td>1884</td>
</tr>
</tbody>
</table>
<unique_encrypted_ssh_key2>
  ssh key
<unique_encrypted_ssh_key3>
  server sshd
    subsystem sftp
    #exit
  server telnetd
    #exit
  subscriber default
  exit
  administrator admin encrypted password <unique_encrypted_password>
  aaa group default
    #exit
  ip route <iproute LOCAL1 IPv4 address_mask> LOCAL1
    #exit
  port ethernet 1/1
    no shutdown
    bind interface LOCAL1 local
    #exit
  ca-certificate name test \\n  pem data \\n  "-----BEGIN CERTIFICATE-----\n  <certificate_data>\n  -----END CERTIFICATE-----"
    #exit
  context wsg
  ip access-list acl1
    permit ip <wsg_acl1_permit_IPv4-address_mask> <wsg_acl1_permit_IPv4-address_mask>
#exit

ipv6 access-list acl1

   permit ip <wsg_acl1_permit_IPV6-address_mask> <wsg_acl1_permit_IPV6-address_mask>

#exit

no ip guarantee framed-route local-switching

ip pool pool1 range <wsg_pool1_IPV4-address/mask> <wsg_pool1_IPV4-address> public 0

ipv6 pool ipv6-pool1 prefix <wsg_pool1_IPV6-address/mask> public 0

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
   <unique_encrypted_key_per_CPU-VM>

   authentication remote pre-shared-key encrypted key
   <unique_encrypted_key_per_CPU-VM>

   ikev2-ikesa transform-set list ikesa-foo

ikev2-ikesa rekey

payload foo-sa0 match childsa match ipv4

   ipsec transform-set list tselsa-foo

   rekey keepalive

#exit

identity local id-type ip-addr id <crypto_foo_IPV4-address>

#exit

crypto template foo-1 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
ikev2-ikesa rekey
payload foo-sa0 match childsa match ipv6
 ipsec transform-set list tselsa-foo
 rekey keepalive
 #exit
identity local id-type ip-addr id <crypto_foo1_local_IPv6-address_mask>
 #exit
interface clear
 ip address <wsg_interface_clear_IPv4-address>
 ipv6 address <wsg_interface_clear_IPv6-address> secondary
 #exit
interface ike loopback
 ip address <wsg_interface_ike_IPv4-address_mask> srp-activate
 ipv6 address <wsg_interface_ike_IPv6-address/mask> srp-activate
 #exit
interface ike-loop loopback
 ip address <wsg_interface_ike-loop_IPv4-address_mask> srp-activate
 #exit
interface ike-loop-v6 loopback
 ipv6 address <wsg_interface_ike-loop(IPv6-address/mask> srp-activate
 #exit
interface ike-loop1 loopback
 ip address <wsg_interface_ike-loop1_IPv4-address_mask> srp-activate
 #exit
subscriber default
exit
aaa group default
 #exit
wsg-service ipv4
deployment-mode site-to-site
ip access-group acl1
bind address <wsg-service_bind_IPv4-address> crypto-template foo
#exit
wsg-service ipv6
deployment-mode site-to-site
ipv6 access-group acl1
bind address <wsg-service_bind_IPv6-address_per_CPU-VM> crypto-template foo-1
#exit
ip route <wsg_iproute_clear_IPv4-address_mask> <wsg_iproute_clear__IPv4-address> clear
ip route <wsg_iproute_ike1_IPv4-address_mask> <wsg_iproute_ike1_IPv4-address> ike
ip route <wsg_iproute_ike2_IPv4-address_mask> <wsg_iproute_ike2_IPv4-address> ike
ip route <wsg_iproute_ike3_IPv4-address_mask> <wsg_iproute_ike3_IPv4-address> ike
ipv6 route <wsg_iproute_clear_IPv6-address/mask> <wsg_iproute_clear_nexthop_IPv6-address> interface clear
ipv6 route <wsg_iproute_ike1_IPv6-address/mask> <wsg_iproute_ike1_nexthop_IPv6-address> interface ike
ipv6 route <wsg_iproute_ike2_IPv6-address/mask> <wsg_iproute_ike2_nexthop_IPv6-address> interface ike
ipv6 route <wsg_iproute_ike3_IPv6-address/mask> <wsg_iproute_ike3_nexthop_IPv6-address> interface ike
ip rri next-hop <wsg_rri_nexthop_IPv4-address> interface clear
ipv6 rri next-hop <wsg_rri_nexthop_IPv6-address> interface clear
#exit
context srp
no ip guarantee framed-route local-switching
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 GigabitEthernet0/0/0/18<srp_monitor_hsrp_vlan_ID>
afi-type IPv4 hsrp-group <srp_hsrp-group_number>
    peer-ip-address <srp_peer_IPv4-address>
    bind address <srp_bind_IPv4-address>
#exit
interface icsr
    ip address <srp_interface_icsr_IPv4-address_mask_per_CPU-VM>
#exit
subscriber default
exit
aaa group default
#exit
    ip route <srp_iproute_IPv4-address_mask> <srp_iproute_IPv4-address> icsr
#exit
connectedapps
    sess-userid cisco
    sess-passwd encrypted password <encrypted_password>
    sess-name hsrp
    sess-ip-address <connectapps_session_IPv4-address>
rri-mode BOTH
ha-chassis-mode inter
ha-network-mode L2
ca-certificate-name test
activate
#exit
wsg-lookup
priority 1 source-netmask 32 destination-netmask 32
priority 2 source-netmask 128 destination-netmask 128
priority 3 source-netmask 64 destination-netmask 64
#exit
port ethernet 1/10
  no shutdown
  vlan <port_1/10_vlan_id>
    no shutdown
    bind interface ike wsg
#exit
#exit
port ethernet 1/11
  no shutdown
  vlan <port_1/11_vlan_id_srp>
    no shutdown
    bind interface icsr srp
#exit
vlan <port_1/11_vlan_id_wsg>
  no shutdown
  bind interface clear wsg
#exit
#exit
end
SecGW VM Configuration - Backup ASR 9000 Chassis

```plaintext
config
  cli hidden

  tech-support test-commands encrypted password <unique_encrypted_password>
  cli test-commands encrypted password <unique_encrypted_password>

---

Important: The logging disable eventid entries should only be applied to SecGW2, SecGW3 and SecGW4.

  logging disable eventid 10171
  logging disable eventid 10638
  logging disable eventid 12690
  logging disable eventid 1298
  logging disable eventid 55629
  logging disable eventid 77601 to 77602

  license key "\
  <SecGW_license_key>

  system hostname <ASR9K_hostname>+<SecGW#>

  orbem
    no siop-port
    no iiop-port

  #exit
  crash max-size 2048 compression gzip
  require session recovery

  context local
    no ip guarantee framed-route local-switching

  interface LOCAL1
    ip address <LOCAL1_ipv4-address>

  #exit
  server ftpd
```
#exit

ssh key
<unique_encrypted_ssh_key1>
ssh key
<unique_encrypted_ssh_key2>
ssh key
<unique_encrypted_ssh_key3>

server sshd
  subsystem sftp
#exit

server telnetd
#exit

subscriber default
exit

administrator admin encrypted password <unique_encrypted_password>

aaa group default
#exit

ip route <iproute_:LOCAL1_IPv4-address_mask> LOCAL1
#exit

port ethernet 1/1
  no shutdown
  bind interface LOCAL1 local
#exit

cacertificate name test \ 
pem data \ 
"-----BEGIN CERTIFICATE-----\n<certificate_data> 
-----END CERTIFICATE-----"
#exit
context wsg

ip access-list acl1

   permit ip <wsg_acl1_permit_IPv4-address_mask> <wsg_acl1_permit_IPv4-address_mask>

   #exit

ipv6 access-list acl1

   permit ip <wsg_acl1_permit_IPv6-address_mask> <wsg_acl1_permit_IPv6-address_mask>

   #exit

no ip guarantee framed-route local-switching

ip pool pool1 range <wsg_pool1_IPv4-address/mask> <wsg_pool1_IPv4-address>

   public 0

ipv6 pool ipv6-pool1 prefix <wsg_pool1_IPv6-address/mask> public 0

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 <unique_encrypted_key_per_CPU-VM>

   authentication remote pre-shared-key encrypted key <unique_encrypted_key_per_CPU-VM>

   ikev2-ikesa transform-set list ikesa-foo

   ikev2-ikesa rekey

   payload foo-sa0 match childsa match ipv4

   ipsec transform-set list tselsa-foo

   rekey keepalive

   #exit

   identity local id-type ip-addr id <crypto_foo_IPv4-address>

   #exit

crypto template foo-1 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
ikev2-ikesa rekey
payload foo-sa0 match childsa match ipv6
   ipsec transform-set list tselsa-foo
   rekey keepalive
#exit
identity local id-type ip-addr id <crypto_foo1_local_IPv6-address_mask>
#exit
interface clear
   ip address <wsg_interface_clear_IPv4-address>
   ipv6 address <wsg_interface_clear_IPv6-address> secondary
#exit
interface ike loopback
   ip address <wsg_interface_ike_IPv4-address_mask> srp-activate
   ipv6 address <wsg_interface_ike_IPv6-address> srp-activate
#exit
interface ike-loop loopback
   ip address <wsg_interface_ike-loop_IPv4-address_mask> srp-activate
#exit
interface ike-loop-v6 loopback
   ipv6 address <wsg_interface_ike-loop_IPv6-address> srp-activate
#exit
interface ike-loop1 loopback
   ip address <wsg_interface_ike-loop1_IPv4-address_mask> srp-activate
#exit
subscriber default
exit
aaa group default
#exit
wsg-service ipv4
  deployment-mode site-to-site
  ip access-group acl1
  bind address <wsg-service_bind_IPV4-address> crypto-template foo
#exit
wsg-service ipv6
  deployment-mode site-to-site
  ipv6 access-group acl1
  bind address <wsg-service_bind_IPV6-address_per_CPU-VM> crypto-template foo-1
#exit
  ip route <wsg_iproute_clear_IPV4-address_mask> <wsg_iproute_clear_IPV4-address> clear
  ip route <wsg_iproute_ike1_IPV4-address_mask> <wsg_iproute_ike1_IPV4-address> ike
  ip route <wsg_iproute_ike2_IPV4-address_mask> <wsg_iproute_ike2_IPV4-address> ike
  ip route <wsg_iproute_ike3_IPV4-address_mask> <wsg_iproute_ike3_IPV4-address> ike
  ipv6 route <wsg_iproute_clear_IPV6-address/mask> <wsg_iproute_clear_nexthop_IPV6-address> interface clear
  ipv6 route <wsg_iproute_ike1_IPV6-address/mask> <wsg_iproute_ike1_nexthop_IPV6-address> interface ike
  ipv6 route <wsg_iproute_ike2_IPV6-address/mask> <wsg_iproute_ike2_nexthop_IPV6-address> interface ike
  ipv6 route <wsg_iproute_ike3_IPV6-address/mask> <wsg_iproute_ike3_nexthop_IPV6-address> interface ike
  ip rri next-hop <wsg_rri_nexthop_IPV4-address> interface clear
  ipv6 rri next-hop <wsg_rri_nexthop_IPV6-address> interface clear
#exit
  context srp
no ip guarantee framed-route local-switching

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 GigabitEthernet0/0/0/18.<srp_monitor_hsrp_vlan_ID>
afi-type IPv4 hsrp-group <srp_hsrp_group_number>

peer-ip-address <srp_peer_IPv4-address>

bind address <srp_bind_IPv4-address>

#exit

interface icsr

ip address <srp_interface_icsr_IPv4-address_mask_per_CPU-VM>

#exit

subscriber default

exit

aaa group default

#exit

ip route <srp_iproute_IPv4-address_mask> <srp_iproute_IPv4-address> icsr

#exit

cconnectadapps

sess-userid cisco

nenpassed encrypted password <encrypted_password>

sess-name hsrp

sess-ip-address <connectadapps_session_IPv4-address>
rrri-mode BOTH
ha-chassis-mode inter
ha-network-mode L2
certificate-name test
activate
#exit
wsg-lookup
  priority 1 source-netmask 32 destination-netmask 32
  priority 2 source-netmask 128 destination-netmask 128
  priority 3 source-netmask 64 destination-netmask 64
#exit
port ethernet 1/10
  no shutdown
  vlan <port_1/10_vlan_id>
    no shutdown
    bind interface ike wsg
  #exit
  #exit
port ethernet 1/11
  no shutdown
  vlan <port_1/11_vlan_id_srp>
    no shutdown
    bind interface icsr srp
  #exit
  vlan <port_1/11_vlan_id_wsg>
    no shutdown
    bind interface clear wsg
  #exit
  #exit
Chapter 8
Sample L3 Interchassis HA Configuration

This chapter provides a sample interchassis wsg-service High Availability (HA) configuration for SecGW functionality between four VPC-VSM instances (StarOS VMs) running on VSMs in separate ASR 9000 chassis.

This sample configuration includes the following sections:

- Configuration Overview
- ASR 9000 Chassis RSP Configuration (IOS-XR)
- SecGW VM Configuration (StarOS)
Configuration Overview

Interchassis Layer 3 redundancy supports hot standby redundancy between two VPC-VSM instances in different ASR 9000 chassis. The standby instance is ready to become active once a switchover is triggered. SA re-negotiation is not required and traffic loss is minimal.

- The route database on the standby VSM must contain only the routes that were successfully injected by the active VSM.
- L3-based HA SecGW deployment uses the onePK Routing Service Set (RSS) infrastructure to support geo-redundancy. It does this by inserting the necessary routes on the ASR 9000 RSP. The RSP then distributes the relevant routes outwardly such that external traffic would reach the active VSM instead of the standby VSM.
- For Layer 3 redundancy, the routes are injected via IOS-XR as two legs. Only the first leg of the routes is injected to IOS-XR running on the chassis with the standby VSM. The small set of secondary leg routes are reconfigured to point to the newly active VSM after the switchover.

Because of the asymmetric assignment of VSM resources among StarOS VMs, an operator should configure one-to-one mapping between StarOS VMs across active/standby VSMs in different ASR 9000 chassis. See the table below.

Table 9. Recommended Mapping of Interchassis StarOS VMs

<table>
<thead>
<tr>
<th>Active VSM</th>
<th>Standby VSM</th>
</tr>
</thead>
<tbody>
<tr>
<td>VM1 – SecGW1</td>
<td>VM1 – SecGW1</td>
</tr>
<tr>
<td>VM2 – SecGW2</td>
<td>VM2 – SecGW2</td>
</tr>
<tr>
<td>VM3 – SecGW3</td>
<td>VM3 – SecGW3</td>
</tr>
<tr>
<td>VM4 – SecGW4</td>
<td>VM4 – SecGW4</td>
</tr>
</tbody>
</table>

Each VM will be monitored via separate HSRP configurations and connected to separate oneP (CA) sessions so that switchover of one VM will not affect the other VMs.

Sample ASR 9000 chassis RSP configurations are provided for primary and standby chassis.

The sample configurations provided for an SecGW VM (Virtual Machine) configuration must be replicated on each CPU-VM complex on both the active and standby VSMs. Each VSM supports four CPU-VM complexes (SecGWs).
Figure 14. Network Diagram for Sample L3 HA Configuration
ASR 9000 Chassis RSP Configuration (IOS-XR)

**Important:** Primary and standby ASR 9000 chassis must be configured to handle the SecGWs (CPU-VM complexes) running on ASR 9000 VSMs. There are four CPU-VM complexes per VSM.

The sample configurations must be applied to the primary and backup ASR 9000 chassis. Each chassis will have unique and shared IP addresses to assure high availability across chassis.

Notes:
- Set basic chassis parameters
- Enable virtual services and assign virtual interfaces for each CPU-VM complex.
- Configure physical Gigabit Ethernet (GigE) ASR 9000 interfaces. Shutdown unused ports.
- Configure a GigE public interface (with VLANs) for IKE and ESP traffic on each CPU-VM complex.
- Configure a GigE private interface (with VLANs) for clear traffic on each CPU-VM complex.
- Configure a 10 Gigabit Ethernet (10GigE) interface for IKE and ESP traffic on each CPU-VM complex. Shut down unused ports.
  - Configure a VLAN on this interface for clear and SRP traffic.
  - Configure a VLAN on this interface for SRP traffic.
  - Configure a VLAN on this interface for clear traffic
- Configure a Bridged Virtual Interface (BVI) for the chassis. A BVI interface configured on the RSP is used as the sess-ip-address in all four SecGW(s) for bringing up the oneP session between the RSP and SecGW.
- Configure routing policies for pass and block traffic.
- Configure static IPv4 and IPV6 addresses.
- Configure BGP routing.
- Configure an L2 VPN.
- Configure HSRP tracking for each CPU-VM complex (shared parameters across ASR 9000 chassis).
- Configure IP Service Level Agreement (SLA) operations.

ASR 9000 Primary Chassis

```plaintext
!! IOS XR Configuration 5.2.2
!! Last configuration change at <timestamp> by root
!
hostname <ASR9K Primary Hostname>
tftp vrf default ipv4 server homedir disk0:
telnet vrf default ipv4 server max-servers 100
```
domain name <domain_name>
cdp advertise v1
vrf clear
!
line console
exec-timeout 0 0
length 50
session-timeout 35791
!
line default
exec-timeout 0 0
length 50
absolute-timeout 10000
session-timeout 35791
!
vty-pool default 0 50 line-template default
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 enable
virtual-service SecGW2
vnic interface TenGigE0/1/1/3
vnic interface TenGigE0/1/1/4
vnic interface TenGigE0/1/1/5
activate
!

virtual-service enable
virtual-service SecGW3
vnic interface TenGigE0/1/1/6
vnic interface TenGigE0/1/1/7
vnic interface TenGigE0/1/1/8
activate
!

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

interface Loopback1
ipv4 address 65.65.65.1 255.255.255.255
!

interface MgmtEth0/RSP0/CPU0/0
ipv4 address 10.78.1.30 255.255.255.0
!

interface MgmtEth0/RSP0/CPU0/1
ipv4 address 8.40.4.10 255.255.0.0
!

interface GigabitEthernet0/2/0/0
description "Private Interface: IKE and ESP Traffic"
transceiver permit pid all
interface GigabitEthernet0/0/0/3
dot1q tunneling ethertype 0x9200
!
interface GigabitEthernet0/2/0/0.1301
description "Private Interface: IKE and ESP Traffic - VM1"
ipv4 address 130.0.1.10 255.255.255.0
ipv6 address 1301::10/64
ipv6 enable
encapsulation dot1q 1301
!
interface GigabitEthernet0/2/0/0.1302
description "Private Interface: IKE and ESP Traffic - VM2"
ipv4 address 130.0.2.10 255.255.255.0
ipv6 address 1302::10/64
ipv6 enable
encapsulation dot1q 1302
!
interface GigabitEthernet0/2/0/0.1303
description "Private Interface: IKE and ESP Traffic - VM3"
ipv4 address 130.0.3.10 255.255.255.0
ipv6 address 1303::10/64
ipv6 enable
encapsulation dot1q 1303
!
interface GigabitEthernet0/2/0/0.1304
description "Private Interface: IKE and ESP Traffic - VM4"
ipv4 address 130.0.4.10 255.255.255.0
ipv6 address 1304::10/64
ipv6 enable
encapsulation dot1q 1304
!
interface GigabitEthernet0/2/0/1
description "Public Interface, Clear Traffic"
transceiver permit pid all
dot1q tunneling ethertype 0x9200
!
interface GigabitEthernet0/2/0/0.1311
description "Public Interface, Clear Traffic - VM1"
ipv4 address 131.0.1.10 255.255.255.0
ipv6 address 1311::10/64
ipv6 enable
encapsulation dot1q 1311
!
interface GigabitEthernet0/2/0/0.1312
description "Public Interface, Clear Traffic - VM2"
ipv4 address 131.0.2.10 255.255.255.0
ipv6 address 1312::10/64
ipv6 enable
encapsulation dot1q 1312
!
interface GigabitEthernet0/2/0/0.1313
description "Public Interface, Clear Traffic - VM3"
ipv4 address 131.0.3.10 255.255.255.0
ipv6 address 1313::10/64
ipv6 enable
encapsulation dot1q 1313
!
interface GigabitEthernet0/2/0/0.1314
  description "Public Interface, Clear Traffic - VM4"
  ipv4 address 131.0.4.10 255.255.255.0
  ipv6 address 1314::10/64
  ipv6 enable
  encapsulation dot1q 1314
!
interface GigabitEthernet0/2/0/2
  speed 1000
  transceiver permit pid all
  l2transport
!
!
interface GigabitEthernet0/2/0/3
  shutdown
!
interface GigabitEthernet0/2/0/4
  shutdown
!
interface GigabitEthernet0/2/0/5
  shutdown
!
interface GigabitEthernet0/2/0/6
  shutdown
!
interface GigabitEthernet0/2/0/7
  shutdown
!
interface GigabitEthernet0/2/0/8
shutdown
!
interface GigabitEthernet0/2/0/9
  shutdown
!
interface GigabitEthernet0/2/0/10
  shutdown
!
interface GigabitEthernet0/2/0/11
  shutdown
!
interface GigabitEthernet0/2/0/12
  shutdown
!
interface GigabitEthernet0/2/0/14
  shutdown
!
interface GigabitEthernet0/2/0/15
  shutdown
!
interface GigabitEthernet0/2/0/16
  shutdown
!
interface GigabitEthernet0/2/0/17
  shutdown
!
interface GigabitEthernet0/2/0/18
  speed 1000
  transceiver permit pid all
dot1q tunneling ethertype 0x9200
!
interface GigabitEthernet0/0/2/0/18.2061
ipv4 address 206.0.1.30 255.255.255.0
ipv6 address 2026::30/64
encapsulation dot1q 2061
!
interface GigabitEthernet0/0/2/0/18.2062
ipv4 address 206.0.2.30 255.255.255.0
ipv6 address 2022::30/64
encapsulation dot1q 2062
!
interface GigabitEthernet0/0/2/0/18.2063
ipv4 address 206.0.3.30 255.255.255.0
ipv6 address 2023::30/64
encapsulation dot1q 2063
!
interface GigabitEthernet0/0/2/0/18.2064
ipv4 address 206.0.4.30 255.255.255.0
ipv6 address 2024::30/64
encapsulation dot1q 2064
!
interface GigabitEthernet0/0/2/0/18.2065
ipv4 address 206.0.5.30 255.255.255.0
ipv6 address 2025::30/64
encapsulation dot1q 2065
!
interface GigabitEthernet0/2/0/19
shutdown
! interface TenGigE0/1/1/0
description "IKE traffic VM1"
transceiver permit pid all
dot1q tunneling ethertype 0x9200
!
interface TenGigE0/1/1/0.1301
description "IKE traffic for VM1"
ipv4 address 83.83.83.10 255.255.255.0
ipv6 address 2083::10/64
encapsulation dot1q 1301
!
interface TenGigE0/1/1/1
description "Clear and srp traffic VM1"
transceiver permit pid all
dot1q tunneling ethertype 0x9200
!
interface TenGigE0/1/1/1.1311
description "Clear traffic VM1"
ipv4 address 93.93.93.10 255.255.255.0
ipv6 address 2093::10/64
encapsulation dot1q 1311
!
interface TenGigE0/3/1/1.1321
description "srp traffic VM1"
ipv4 address 73.73.73.10 255.255.255.0
ipv6 address 2071::10/64
encapsulation dot1q 1321
!
! interface TenGigE0/1/1/2
transceiver permit pid all
l2transport
!

! interface TenGigE0/1/1/3
description "IKE traffic VM2"
transceiver permit pid all
dot1q tunneling ethertype 0x9200
!
interface TenGigE0/1/1/3.1302
description "IKE traffic for VM2"
ipv4 address 85.85.85.10 255.255.255.0
ipv6 address 2085::10/64
encapsulation dot1q 1302
!
interface TenGigE0/1/1/4
description "Clear and srp traffic VM2"
transceiver permit pid all
dot1q tunneling ethertype 0x9200
!
interface TenGigE0/1/1/4.1312
description "clear traffic VM2"
ipv4 address 95.95.95.10 255.255.255.0
ipv6 address 2095::10/64
encapsulation dot1q 1312
!
interface TenGigE0/1/1/4.1322
description "srp traffic VM2"
ipv4 address 75.75.75.10 255.255.255.0
ipv6 address 2075::10/64
encapsulation dot1q 1322
!
interface TenGigE0/1/1/5
  transceiver permit pid all
  l2transport
  !

interface TenGigE0/1/1/6
  description "IKE traffic VM3"
  transceiver permit pid all
  dot1q tunneling ethertype 0x9200
  !
interface TenGigE0/3/1/6.1303
  description "IKE traffic for VM3"
  ipv4 address 87.87.87.10 255.255.255.0
  ipv6 address 2087::10/64
  encapsulation dot1q 1303
  !
interface TenGigE0/1/1/7
  description "Clear qnd srp traffic VM3"
  transceiver permit pid all
  dot1q tunneling ethertype 0x9200
  !
interface TenGigE0/1/1/7.1313
  description "clear traffic VM3"
  ipv4 address 97.97.97.10 255.255.255.0
ipv6 address 2097::10/64
encapsulation dot1q 1313
!
interface TenGigE0/1/1/7.1323
description "srp traffic VM3"
ipv4 address 77.77.77.10 255.255.255.0
ipv6 address 2077::10/64
encapsulation dot1q 1323
!
interface TenGigE0/1/1/8
transceiver permit pid all
l2transport
!
!
interface TenGigE0/1/1/9
description "IKE traffic VM4"
transceiver permit pid all
dot1q tunneling ethertype 0x9200
!
interface TenGigE0/1/1/9.1304
description "IKE traffic for VM4"
ipv4 address 89.89.89.10 255.255.255.0
ipv6 address 2089::10/64
encapsulation dot1q 1304
!
interface TenGigE0/1/1/10
description "Clear and srp traffic VM4"
transceiver permit pid all
dot1q tunneling ethertype 0x9200
interface TenGigE0/1/1/10.1314
  description "clear traffic VM4"
  ipv4 address 99.99.99.10 255.255.255.0
  ipv6 address 2099::10/64
  encapsulation dot1q 1314

interface TenGigE0/1/1/10.1324
  description "srp traffic VM4"
  ipv4 address 79.79.79.10 255.255.255.0
  ipv6 address 2079::10/64
  encapsulation dot1q 1324

interface TenGigE0/1/1/11
  transceiver permit pid all
  l2transport

prefix-set test
  1.1.1.1/32
end-set

route-policy test
  if rib-has-route in (1.1.1.1/32 ge 32 le 32) then
    pass
  endif
end-policy

!
route-policy pass-all
pass
end-policy

!
route-policy test-rib
if rib-has-route in (1.1.1.1/32) then
    pass
endif
end-policy

!
route-policy block-clear
if destination in (80.80.80.80/32 le 32) then
    drop
endif
pass
end-policy

!
route-policy block-ike-01
if destination in (23.23.23/32 le 32) then
    drop
endif
if destination in (2023::23/128 le 128) then
    drop
endif
pass
end-policy

!
route-policy block-ike-02
  if destination in (33.33.33.33/32 le 32) then
      drop
  endif
  if destination in (2033::33/128 le 128) then
      drop
  endif
  pass
end-policy
!
route-policy block-ike-03
  if destination in (43.43.43.43/32 le 32) then
      drop
  endif
  if destination in (2043::43/128 le 128) then
      drop
  endif
  pass
end-policy
!
route-policy block-ike-04
  if destination in (53.53.53.53/32 le 32) then
      drop
  endif
  if destination in (2053::53/128 le 128) then
      drop
  endif
  pass
end-policy
! route-policy pass-only-ike-01
  if destination in (23.23.23.23/32 le 32) then
    pass
  endif
  if destination in (2023::23/128 le 128) then
    pass
  endif
end-policy
!
route-policy pass-only-ike-02
  if destination in (33.33.33.33/32 le 32) then
    pass
  endif
  if destination in (2033::33/128 le 128) then
    pass
  endif
end-policy
!
route-policy pass-only-ike-03
  if destination in (43.43.43.43/32 le 32) then
    pass
  endif
  if destination in (2043::43/128 le 128) then
    pass
  endif
end-policy
!
route-policy pass-only-ike-04
if destination in (53.53.53.53/32 le 32) then
  pass
endif
if destination in (2053::53/128 le 128) then
  pass
endif
end-policy
!
router static
  address-family ipv4 unicast
    10.0.0.0/8 10.78.1.1
    11.0.0.0/8 130.0.1.20
    15.0.0.0/8 130.0.2.20
    17.0.0.0/8 130.0.3.20
    19.0.0.0/8 130.0.4.20
    64.0.0.0/8 10.78.1.1
    72.72.72.0/24 206.0.1.20
    74.74.74.0/24 206.0.1.20
    76.76.76.0/24 206.0.1.20
    78.78.78.0/24 206.0.1.20
    202.153.144.25/32 8.40.0.1
    211.0.1.0/24 130.0.1.20
    211.0.2.0/24 130.0.2.20
    211.0.3.0/24 130.0.3.20
    211.0.4.0/24 130.0.4.20
    213.0.1.0/24 131.0.1.20
    213.0.2.0/24 131.0.2.20
    213.0.3.0/24 131.0.3.20
    213.0.4.0/24 131.0.4.20
router bgp 3000
  bgp router-id 3.3.3.3
  address-family ipv4 unicast
  redistribute application hsrp
  allocate-label all
  
  neighbor 130.0.1.20
  remote-as 6000
  address-family ipv4 unicast
  route-policy pass-only-ike-01 out
  
  neighbor 130.0.2.20
  remote-as 6000
  address-family ipv4 unicast
  route-policy pass-only-ike-02 out
  
  neighbor 130.0.3.20
  remote-as 6000
  address-family ipv4 unicast
  route-policy pass-only-ike-03 out
  
  neighbor 130.0.4.20
  remote-as 6000
  address-family ipv4 unicast
route-policy pass-only-ike-04 out
!
!
neighbor 131.0.1.20
  remote-as 6000
diffserv
  address-family ipv4 unicast
    route-policy block-ike-01 out
!
!
neighbor 131.0.2.20
  remote-as 6000
diffserv
  address-family ipv4 unicast
    route-policy block-ike-02 out
!
!
neighbor 131.0.3.20
  remote-as 6000
diffserv
  address-family ipv4 unicast
    route-policy block-ike-03 out
!
!
neighbor 131.0.4.20
  remote-as 6000
diffserv
  address-family ipv4 unicast
    route-policy block-ike-04 out
!
!
12vpn
xconnect group wsg
!
bridge group wsg
bridge-domain mgmt
   interface TenGigE0/1/1/2
!
   interface TenGigE0/1/1/5
!
   interface TenGigE0/1/1/8
!
   interface TenGigE0/1/1/11
!
   interface GigabitEthernet0/2/0/2
!
   routed interface BVI1
!
!
router hsrp

   interface GigabitEthernet0/2/0/18.2062
   address-family ipv4
   hsrp 401
       timers msec 300 msec 900
       preempt
       priority 101
       address 206.0.2.110
       track object PublicHsrp
       track object WsgIPsla-1
       track object PrivateHsrp
interface GigabitEthernet0/2/0/18.2063
  address-family ipv4
  hsrp 402
  timers msec 300 msec 900
  preempt
  priority 101
  address 206.0.3.120
  track object PublicHsrp
  track object WsgIPsla-2
  track object PrivateHsrp

interface GigabitEthernet0/2/0/18.2064
  address-family ipv4
  hsrp 403
  timers msec 300 msec 900
  preempt
  priority 101
  address 206.0.4.130
  track object PublicHsrp
  track object WsgIPsla-3
  track object PrivateHsrp

address-family ipv4
hsrp 404
    timers msec 300 msec 900
    preempt
    priority 101
    address 206.0.5.140
    track object PublicHsrp
    track object WsgIPsla-4
    track object PrivateHsrp
    
    
    
    !
    !
    !
    !
crypto ca trustpoint onep-tp
    crl optional
    subject-name CN=<ASR9K_primary_hostname>.<domain_name>
    enrollment url terminal
    
    ipsla
    operation 100
    type icmp echo
    destination address 83.83.83.100
    timeout 300
    frequency 1
    
    
    operation 200
    type icmp echo
    destination address 85.85.85.100
    timeout 300
frequency 1
!
!
operation 300
type icmp echo
destination address 87.87.87.100
timeout 300
frequency 1
!
!
operation 400
type icmp echo
destination address 89.89.89.100
timeout 300
frequency 1
!
!
schedule operation 100
start-time now
life forever
!
schedule operation 200
start-time now
life forever
!
schedule operation 300
start-time now
life forever
!
schedule operation 400
  start-time now
  life forever

track PublicHsre
  type line-protocol state
    interface GigabitEthernet0/2/0/0

track WsgIPsla-1
  type rtr 100 reachability
  delay up 1
  delay down 1

track WsgIPsla-2
  type rtr 200 reachability
  delay up 1
  delay down 1

track WsgIPsla-3
  type rtr 300 reachability
  delay up 1
  delay down 1

track WsgIPsla-4
  type rtr 400 reachability
  delay up 1
  delay down 1
ASR 9000 Backup Chassis

!! IOS XR Configuration 5.2.2
!! Last configuration change at <timestamp> by root
!
hostname <ASR9K_backup_hostname>
clock timezone <timezone>
tftp vrf default ipv4 server homedir disk0:
telnet vrf default ipv4 server max-servers 100
domain name <domain_name>
line console
  exec-timeout 0 0
  exec-timeout 0 0
  absolute-timeout 10000
  session-timeout 35791
!
line default
  exec-timeout 0 0
  length 50
!

ASR 9000 Backup Chassis

track PrivateHsrpsrp
type line-protocol state
interface GigabitEthernet0/2/0/3
!
delay up 1
delay down
!
end
vty-pool default 0 50 line-template default
onep
  transport type tls localcert onep-tp disable-remotecert-validation
!
virtual-service enable
virtual-service SecGW1
  vnic interface TenGigE0/3/1/0
  vnic interface TenGigE0/3/1/1
  vnic interface TenGigE0/3/1/2
  activate
!
virtual-service enable
virtual-service SecGW2
  vnic interface TenGigE0/3/1/3
  vnic interface TenGigE0/3/1/4
  vnic interface TenGigE0/3/1/5
  activate
!
virtual-service enable
virtual-service SecGW3
  vnic interface TenGigE0/3/1/6
  vnic interface TenGigE0/3/1/7
  vnic interface TenGigE0/3/1/8
  activate
!
virtual-service enable
virtual-service SecGW4
  vnic interface TenGigE0/3/1/9
  vnic interface TenGigE0/3/1/10
vnic interface TenGigE0/3/1/11
activate
!
ntp
server 10.78.1.30
server 64.104.193.12
!
interface Loopback1
ipv4 address 65.65.65.1 255.255.255.255
!
interface MgmtEth0/RSP0/CPU0/0
ipv4 address 10.78.1.20 255.255.255.0
!
interface MgmtEth0/RSP0/CPU0/1
ipv4 address 8.40.2.10 255.255.0.0
!
interface GigabitEthernet0/2/0/0
description "Public Interface: IKE and ESP Traffic"
transceiver permit pid all
interface GigabitEthernet0/0/0/3
dot1q tunneling ethertype 0x9200
!
interface GigabitEthernet0/2/0/0.1201
description "Public Interface: IKE and ESP Traffic - VMI"
ipv4 address 120.0.1.10 255.255.255.0
ipv6 address 1201::10/64
ipv6 enable
encapsulation dot1q 1201
!
interface GigabitEthernet0/2/0/0.1202
  description "Public Interface: IKE and ESP Traffic - VM2"
  ipv4 address 120.0.2.10 255.255.255.0
  ipv6 address 1202::10/64
  ipv6 enable
  encapsulation dot1q 1202
!
interface GigabitEthernet0/2/0/0.1203
  description "Public Interface: IKE and ESP Traffic - VM3"
  ipv4 address 120.0.3.10 255.255.255.0
  ipv6 address 1203::10/64
  ipv6 enable
  encapsulation dot1q 1203
!
interface GigabitEthernet0/2/0/0.1204
  description "Public Interface: IKE and ESP Traffic - VM4"
  ipv4 address 120.0.4.10 255.255.255.0
  ipv6 address 1204::10/64
  ipv6 enable
  encapsulation dot1q 1204
!
interface GigabitEthernet0/2/0/1
  speed 1000
  transceiver permit pid all
  l2transport
!
!
!  
interface GigabitEthernet0/0/2/0/3  
description "Private Interface, Clear Traffic"  
transceiver permit pid all  
dot1q tunneling ethertype 0x9200  
!  
interface GigabitEthernet0/0/2/0/3.1211  
description "Private Interface, Clear Traffic - VM1"  
ipv4 address 121.0.1.10 255.255.255.0  
ipv6 address 1211::10/64  
ipv6 enable  
encapsulation dot1q 1211  
!  
interface GigabitEthernet0/0/2/0/3.1212  
description "Private Interface, Clear Traffic - VM2"  
ipv4 address 121.0.2.10 255.255.255.0  
ipv6 address 1212::10/64  
ipv6 enable  
encapsulation dot1q 1212  
!  
interface GigabitEthernet0/0/2/0/3.1213  
description "Private Interface, Clear Traffic - VM3"  
ipv4 address 121.0.3.10 255.255.255.0  
ipv6 address 1213::10/64  
ipv6 enable  
encapsulation dot1q 1213  
!  
interface GigabitEthernet0/0/2/0/3.1214  
description "Private Interface, Clear Traffic - VM4"  

ipv4 address 121.0.4.10 255.255.255.0
ipv6 address 1214::10/64
ipv6 enable
encapsulation dot1q 1214

interface GigabitEthernet0/2/0/4
  shutdown

interface GigabitEthernet0/2/0/5
  shutdown

interface GigabitEthernet0/2/0/6
  shutdown

interface GigabitEthernet0/2/0/7
  shutdown

interface GigabitEthernet0/2/0/8
  shutdown

interface GigabitEthernet0/2/0/9
  shutdown

interface GigabitEthernet0/2/0/10
  shutdown

interface GigabitEthernet0/2/0/11
  shutdown
interface GigabitEthernet0/2/0/12
  shutdown
!
interface GigabitEthernet0/2/0/13
  shutdown
!
interface GigabitEthernet0/2/0/14
  shutdown
!
interface GigabitEthernet0/2/0/15
  shutdown
!
interface GigabitEthernet0/2/0/16
  shutdown
!
interface GigabitEthernet0/2/0/17
  shutdown
!
interface GigabitEthernet0/2/0/18
  speed 1000
  transceiver permit pid all
dot1q tunneling ethtype 0x9200
!
interface GigabitEthernet0/2/0/18.2061
  ipv4 address 206.0.1.20 255.255.255.0
  ipv6 address 2026::20/64
  ipv6 enable
  encapsulation dot1q 2061
!
interface GigabitEthernet0/2/0/18.2062
ipv4 address 206.0.2.20 255.255.255.0
ipv6 address 2022::20/64
ipv6 enable
encapsulation dot1q 2062
!
interface GigabitEthernet0/2/0/18.2063
ipv4 address 206.0.3.20 255.255.255.0
ipv6 address 2023::20/64
ipv6 enable
encapsulation dot1q 2063
!
interface GigabitEthernet0/2/0/18.2064
ipv4 address 206.0.4.20 255.255.255.0
ipv6 address 2024::20/64
ipv6 enable
encapsulation dot1q 2064
!
interface GigabitEthernet0/2/0/18.2065
ipv4 address 206.0.5.20 255.255.255.0
ipv6 address 2025::20/64
ipv6 enable
encapsulation dot1q 2065
!
interface GigabitEthernet0/2/0/19
shutdown
!
interface TenGigE0/1/1/0
shutdown
! interface TenGigE0/1/1/1 shutdown
! interface TenGigE0/1/1/2 shutdown
! interface TenGigE0/1/1/3 shutdown
! interface TenGigE0/1/1/4 shutdown
! interface TenGigE0/1/1/5 shutdown
! interface TenGigE0/1/1/6 shutdown
! interface TenGigE0/1/1/7 shutdown
! interface TenGigE0/1/1/8 shutdown
! interface TenGigE0/1/1/9 shutdown
! interface TenGigE0/1/1/10
shutdown
!
interface TenGigE0/1/1/1
shutdown
!
interface TenGigE0/3/1/0
description "IKE traffic VM1"
transceiver permit pid all
dot1q tunneling ethertype 0x9200
!
interface TenGigE0/3/1/0.1201
description "IKE traffic for VM1"
ipv4 address 82.82.82.10 255.255.255.0
ipv6 address 2082::10/64
encapsulation dot1q 1201
!
interface TenGigE0/3/1/1
description "Clear and srp traffic VM1"
transceiver permit pid all
dot1q tunneling ethertype 0x9200
!
interface TenGigE0/3/1/1.1211
description "clear traffic VM1"
ipv4 address 92.92.92.10 255.255.255.0
ipv6 address 2092::10/64
encapsulation dot1q 1211
!
interface TenGigE0/3/1/1.1221
description "srp traffic VM1"
ipv4 address 72.72.72.10 255.255.255.0
ipv6 address 2071::10/64
encapsulation dot1q 1221
!
!
interface TenGigE0/3/1/2
  transceiver permit pid all
dot1q tunneling ethertype 0x9200
!
interface TenGigE0/3/1/3
description "IKE traffic VM2"
  transceiver permit pid all
dot1q tunneling ethertype 0x9200
!
interface TenGigE0/3/1/3.1202
description "IKE traffic for VM2"
ipv4 address 84.84.84.10 255.255.255.0
ipv6 address 2084::10/64
encapsulation dot1q 1202
!
interface TenGigE0/3/1/4
description "Clear and srp traffic VM2"
  transceiver permit pid all
dot1q tunneling ethertype 0x9200
!
interface TenGigE0/3/1/4.1212
description "clear traffic VM2"
ipv4 address 94.94.94.10 255.255.255.0
ipv6 address 2094::10/64
encapsulation dot1q 1212
!
interface TenGigE0/3/1/4.1222
description "srp traffic VM2"
ipv4 address 74.74.74.10 255.255.255.0
ipv6 address 2074::10/64
encapsulation dot1q 1222
!
interface TenGigE0/3/1/5
transceiver permit pid all
l2transport
!
!
interface TenGigE0/3/1/6
description "IKE traffic VM3"
transceiver permit pid all
dot1q tunneling ethtype 0x9200
!
interface TenGigE0/3/1/6.1203
description "IKE traffic for VM3"
transceiver permit pid all
ipv4 address 86.86.86.10 255.255.255.0
ipv6 address 2086::10/64
encapsulation dot1q 1203
!
interface TenGigE0/3/1/7
description "clear traffic VM3"
transceiver permit pid all
dot1q tunneling ethertype 0x9200
!
interface TenGigE0/3/1/7.1213
description "clear traffic VM3"
ipv4 address 96.96.96.10 255.255.255.0
ipv6 address 2096::10/64
encapsulation dot1q 1213
!
interface TenGigE0/3/1/7.1223
description "srp traffic VM3"
ipv4 address 76.76.76.10 255.255.255.0
ipv6 address 2076::10/64
encapsulation dot1q 1223
!
interface TenGigE0/3/1/8
transceiver permit pid all
l2transport
!
!
interface TenGigE0/3/1/9
description "IKE traffic VM4"
transceiver permit pid all
dot1q tunneling ethertype 0x9200
!
interface TenGigE0/3/1/9.1204
description "IKE traffic for VM4"
ipv4 address 88.88.88.10 255.255.255.0
ipv6 address 2088::10/64
encapsulation dot1q 1204
interface TenGigE0/3/1/10
  description "Clear and srp traffic VM4"
  transceiver permit pid all
  dot1q tunneling ethertype 0x9200
!
interface TenGigE0/3/1/10.1214
  description "clear traffic VM4"
  ipv4 address 98.98.98.10 255.255.255.0
  ipv6 address 2098::10/64
  encapsulation dot1q 1214
!
interface TenGigE0/3/1/10.1224
  description "srp traffic VM4"
  ipv4 address 78.78.78.10 255.255.255.0
  ipv6 address 2078::10/64
  encapsulation dot1q 1224
!
interface TenGigE0/3/1/11
  transceiver permit pid all
  l2transport
!
!
interface BVI1
  ipv4 address 192.168.10.10 255.255.255.0
!
route-policy pass-all
  pass
end-policy
! route-policy block-ike-01
  if destination in (23.23.23.23/32 le 32) then
drop
endif
if destination in (2023::23/128 le 128) then
drop
endif
pass
end-policy
!
route-policy block-ike-02
  if destination in (33.33.33.33/32 le 32) then
drop
endif
if destination in (2033::33/128 le 128) then
drop
endif
pass
end-policy
!
route-policy block-ike-03
  if destination in (43.43.43.43/32 le 32) then
drop
endif
if destination in (2043::43/128 le 128) then
drop
endif
pass
end-policy

!

route-policy block-ike-04
  if destination in (53.53.53.53/32 le 32) then
    drop
  endif
  if destination in (2053::53/128 le 128) then
    drop
  endif
  pass
end-policy

!

route-policy pass-only-ike-01
  if destination in (23.23.23.23/32 le 32) then
    pass
  endif
  if destination in (2023::23/128 le 128) then
    pass
  endif
end-policy

!

route-policy pass-only-ike-02
  if destination in (33.33.33.33/32 le 32) then
    pass
  endif
  if destination in (2033::33/128 le 128) then
    pass
  endif
end-policy
route-policy pass-only-ike-03
  if destination in (43.43.43/32 le 32) then
    pass
  endif
  if destination in (2043:43/128 le 128) then
    pass
  endif
end-policy
!
route-policy pass-only-ike-04
  if destination in (53.53.53/32 le 32) then
    pass
  endif
  if destination in (2053:53/128 le 128) then
    pass
  endif
end-policy
!
router static
  address-family ipv4 unicast
  10.0.0.0/8 10.78.1.1
  10.78.27.0/24 10.78.1.1
  11.0.0.0/8 120.0.1.20
  15.0.0.0/8 120.0.2.20
  17.0.0.0/8 120.0.3.20
  19.0.0.0/8 120.0.4.20
  64.0.0.0/8 10.78.1.1
  73.73.73.0/24 206.0.1.30
router bgp 2000
   bgp router-id 2.2.2.2
   address-family ipv4 unicast
      redistribute application hsrp
      allocate-label all
   !
   address-family ipv6 unicast
      redistribute application hsrp
      allocate-label all
   !
neighbor 120.0.1.20
   remote-as 6000
   address-family ipv4 unicast
      route-policy pass-only-ike-01 out
   !
neighbor 120.0.2.20
remote-as 6000
address-family ipv4 unicast
  route-policy pass-only-ike-02 out
!
!
neighbor 120.0.3.20
remote-as 6000
address-family ipv4 unicast
  route-policy pass-only-ike-03 out
!
!
neighbor 120.0.4.20
remote-as 6000
address-family ipv4 unicast
  route-policy pass-only-ike-04 out
!
!
neighbor 121.0.1.20
remote-as 6000
address-family ipv4 unicast
  route-policy block-ike-01 out
!
!
neighbor 121.0.2.20
remote-as 6000
address-family ipv4 unicast
  route-policy block-ike-02 out
neighbor 121.0.3.20
remote-as 6000
address-family ipv4 unicast
  route-policy block-ike-03 out

neighbor 121.0.4.20
remote-as 6000
address-family ipv4 unicast
  route-policy block-ike-04 out

l2vpn
  xconnect group wsg

bridge group wsg
  bridge-domain mgmt
    interface TenGigE0/3/1/2

    interface TenGigE0/3/1/5

    interface TenGigE0/3/1/8

    interface TenGigE0/3/1/11

    interface GigabitEthernet0/2/0/1
router hsrp

interface GigabitEthernet0/2/0/18.2062
  address-family ipv4
  hsrp 401
    timers msec 300 msec 900
    preempt
    priority 101
    address 206.0.2.110
    track object PublicHsrp
    track object WsgIPsla-1
    track object PrivateHsrp

interface GigabitEthernet0/2/0/18.2063
  address-family ipv4
  hsrp 402
    timers msec 300 msec 900
    preempt
    priority 101
    address 206.0.3.110
    track object PublicHsrp
    track object WsgIPsla-2
    track object PrivateHsrp
interface GigabitEthernet0/2/0/18.2064
  address-family ipv4
  hsrp 403
  timers msec 300 msec 900
  preempt
  priority 101
  address 206.0.4.130
  track object PublicHsrp
  track object WsgIPsla-3
  track object PrivateHsrp

interface GigabitEthernet0/2/0/18.2065
  address-family ipv4
  hsrp 404
  timers msec 300 msec 900
  preempt
  priority 101
  address 206.0.5.140
  track object PublicHsrp
  track object WsgIPsla-4
  track object PrivateHsrp

crypto ca trustpoint onep-tp
crl optional
subject-name CN=<ASR9K_backup_hostname>.<domain_name>
enrollment url terminal
!
ipsla
operation 100
type icmp echo
destination address 82.82.82.100
timeout 300
frequency 1
!
!
operation 200
type icmp echo
destination address 84.84.84.100
timeout 300
frequency 1
!
!
operation 300
type icmp echo
destination address 86.86.86.100
timeout 300
frequency 1
!
!
operation 400
type icmp echo
destination address 88.88.88.100
timeout 300
frequency 1
!
!
schedule operation 100
start-time now
life forever
!
schedule operation 200
start-time now
life forever
!
schedule operation 300
start-time now
life forever
!
schedule operation 400
start-time now
life forever
!
!
track PublicHsrp
type line-protocol state
interface GigabitEthernet0/2/0/0
!
delay up 1
delay down 1
!
track WsgIPsla-1
type rtr 100 reachability
delay up 1
delay down 1
!
track WsgIPsla-2
type rtr 200 reachability
delay up 1
delay down 1
!
track WsgIPsla-3
type rtr 300 reachability
delay up 1
delay down 1
!
track WsgIPsla-4
type rtr 400 reachability
delay up 1
delay down 1
!
track PrivateHsrpsrp
type line-protocol state
   interface GigabitEthernet0/2/0/3
!
delay up 1
delay down
!
end
SecGW VM Configuration (StarOS)

**Important:** Each SecGW (CPU-VM complex) must be separately configured as described below for corresponding VSMs in both the primary and backup ASR 9000 chassis. There are four CPU-VM complexes per ASR 9000 VSM.

The unique parameters for each CPU-VM complex must correspond with interface settings configured for the primary and backup ASR 9000 chassis.

Notes:

- Enable hidden CLI test-commands.
- Install SecGW License.
- Assign unique host name per CPU-VM complex.
- Set crash log size to 2048 with compression.
- Require Session Recovery.
- Create local context with unique parameters per CPU-VM complex.
- Enable wsg-service with unique parameters per CPU-VM complex. Add SRI and RRI parameters.
- Create SRP context with unique parameters per CPU-VM complex.
- Enable Connected Apps session with unique password and session name per CPU-VM complex.
- Set wsg-lookup priorities.
- Appropriately configure ethernet ports with unique parameters per CPU-VM complex. Refer to the tables below for mapping of sample IP addresses for each SecGW.

Table 10. StarOS IP Address Mapping - SecGW1

<table>
<thead>
<tr>
<th>Variable</th>
<th>Primary ASR 9000</th>
<th>Backup ASR 9000</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;interface_LOCAL1_IPv4-address_mask&gt;</td>
<td>10.78.1.115 255.255.255.0</td>
<td>10.78.1.111 255.255.255.0</td>
</tr>
<tr>
<td>&lt;interface_LOCAL1_IPv4-address_mask_secondary&gt;</td>
<td>192.172.12.11 255.255.255.0</td>
<td>192.168.10.11 255.255.255.0</td>
</tr>
<tr>
<td>&lt;iproute_LOCAL1_IPv4-address_mask&gt;</td>
<td>0.0.0.0 0.0.0.0 10.78.1.1</td>
<td>0.0.0.0 0.0.0.0 10.78.1.1</td>
</tr>
<tr>
<td>&lt;wsg_acl1_permit1_IPv4-address_mask&gt;</td>
<td>65.65.0.0 0.0.255.255</td>
<td>65.65.0.0 0.0.255.255</td>
</tr>
<tr>
<td></td>
<td>45.45.0.0 0.0.255.255</td>
<td>45.45.0.0 0.0.255.255</td>
</tr>
<tr>
<td>&lt;wsg_acl1_permit2_IPv4-address_mask&gt;</td>
<td>66.66.0.0 0.0.255.255</td>
<td>66.66.0.0 0.0.255.255</td>
</tr>
<tr>
<td></td>
<td>46.46.0.0 0.0.255.255</td>
<td>46.46.0.0 0.0.255.255</td>
</tr>
<tr>
<td>&lt;wsg_acl1_permit3_IPv4-address_mask&gt;</td>
<td>67.67.0.0 0.0.255.255</td>
<td>67.67.0.0 0.0.255.255</td>
</tr>
<tr>
<td></td>
<td>47.47.0.0 0.0.255.255</td>
<td>47.47.0.0 0.0.255.255</td>
</tr>
<tr>
<td>&lt;wsg_acl1_permit4_IPv4-address_mask&gt;</td>
<td>68.68.0.0 0.0.255.255</td>
<td>68.68.0.0 0.0.255.255</td>
</tr>
<tr>
<td></td>
<td>48.48.0.0 0.0.255.255</td>
<td>48.48.0.0 0.0.255.255</td>
</tr>
<tr>
<td>Variable</td>
<td>Primary ASR 9000</td>
<td>Backup ASR 9000</td>
</tr>
<tr>
<td>----------</td>
<td>------------------</td>
<td>------------------</td>
</tr>
<tr>
<td>&lt;wsg_acl1_permit5_IPv4-address_mask&gt;</td>
<td>69.69.0.0 0.0.255.255 49.49.0.0 0.0.255.255</td>
<td>69.69.0.0 0.0.255.255 49.49.0.0 0.0.255.255</td>
</tr>
<tr>
<td>&lt;wsg_pool1_IPv4-address_mask&gt;</td>
<td>—</td>
<td>20.13.0.1 20.13.255.255</td>
</tr>
<tr>
<td>&lt;wsg_pool2_IPv4-address_mask&gt;</td>
<td>45.45.0.1 45.45.255.254 20.14.0.1 20.14.255.255</td>
<td></td>
</tr>
<tr>
<td>&lt;wsg_pool2_IPv6-address/mask&gt;</td>
<td>2013::/56</td>
<td>2013::/56</td>
</tr>
<tr>
<td>&lt;crypto_ike-ts-1_local_IPv6-address&gt;</td>
<td>2023::23</td>
<td>2023::33</td>
</tr>
<tr>
<td>&lt;wsg_interface_clear_IPv4-address_mask&gt;</td>
<td>93.93.93.20 255.255.255.0 92.92.92.20 255.255.255.0</td>
<td>93.93.93.100 255.255.255.255 92.92.92.100 255.255.255.255</td>
</tr>
<tr>
<td>&lt;wsg_interface_clear_IPv6-address/mask&gt;</td>
<td>2093::23/64</td>
<td>2092::23/64</td>
</tr>
<tr>
<td>&lt;wsg_interface_clear-loopback_IPv4-address_mask&gt;</td>
<td>93.93.93.100 255.255.255.255</td>
<td>93.93.93.100 255.255.255.255</td>
</tr>
<tr>
<td>&lt;wsg_interface_ike_IPv4-address_mask&gt;</td>
<td>83.83.83.20 255.255.255.0 82.82.82.20 255.255.255.0</td>
<td>83.83.83.100 255.255.255.255 82.82.82.100 255.255.255.255</td>
</tr>
<tr>
<td>&lt;wsg_interface_ike_IPv6-address/mask&gt;</td>
<td>2083::23/64</td>
<td>2082::23/64</td>
</tr>
<tr>
<td>&lt;wsg_interface_ike-loop_IPv4-address_mask&gt;</td>
<td>83.83.83.100 255.255.255.255</td>
<td>83.83.83.100 255.255.255.255</td>
</tr>
<tr>
<td>&lt;wsg_interface_wsg-service_loop_IPv4-address_mask&gt;</td>
<td>23.23.23.23 255.255.255.255</td>
<td>23.23.23.23 255.255.255.255</td>
</tr>
<tr>
<td>&lt;wsg_interface_wsg-service_loop_IPv6-address_mask&gt;</td>
<td>2023::23/128</td>
<td>2023::33/128</td>
</tr>
<tr>
<td>&lt;wsg_service_bind_ras_IPv4-address&gt;</td>
<td>23.23.23.23</td>
<td>—</td>
</tr>
<tr>
<td>&lt;wsg_service_bind_s2s_IPv4-address&gt;</td>
<td>—</td>
<td>23.23.23.23</td>
</tr>
<tr>
<td>&lt;wsg_service_bind_s2s_IPv6-address&gt;</td>
<td>2023::23</td>
<td>2023::23</td>
</tr>
<tr>
<td>Variable</td>
<td>Primary ASR 9000</td>
<td>Backup ASR 9000</td>
</tr>
<tr>
<td>--------------------------------</td>
<td>------------------</td>
<td>-----------------</td>
</tr>
<tr>
<td>&lt;wsg_iproute_ike1_IPv4-address_mask&gt;</td>
<td>181.8.0.0 255.255.255.0</td>
<td>181.8.0.0 255.255.255.0</td>
</tr>
<tr>
<td>&lt;wsg_iproute_ike1_IPv4-address&gt;</td>
<td>83.83.83.10</td>
<td>82.82.82.10</td>
</tr>
<tr>
<td>&lt;wsg_iproute_ike2_IPv4-address_mask&gt;</td>
<td>186.0.0.0 255.0.0.0</td>
<td>186.0.0.0 255.0.0.0</td>
</tr>
<tr>
<td>&lt;wsg_iproute_ike2_IPv4-address&gt;</td>
<td>83.83.83.10</td>
<td>82.82.82.10</td>
</tr>
<tr>
<td>&lt;wsg_iproute_ike3_IPv4-address_mask&gt;</td>
<td>120.0.1.0 255.255.255.0</td>
<td>120.0.1.0 255.255.255.0</td>
</tr>
<tr>
<td>&lt;wsg_iproute_ike3_IPv4-address&gt;</td>
<td>83.83.83.10</td>
<td>82.82.82.10</td>
</tr>
<tr>
<td>&lt;wsg_iproute_ike4_IPv4-address_mask&gt;</td>
<td>—</td>
<td>211.0.1.0 255.255.255.0</td>
</tr>
<tr>
<td>&lt;wsg_iproute_ike4_IPv4-address&gt;</td>
<td>—</td>
<td>82.82.82.10</td>
</tr>
<tr>
<td>&lt;wsg_iproute_ike5_IPv4-address_mask&gt;</td>
<td>11.0.0.0 255.0.0.0</td>
<td>11.0.0.0 255.0.0.0</td>
</tr>
<tr>
<td>&lt;wsg_iproute_ike5_IPv4-address&gt;</td>
<td>83.83.83.10</td>
<td>82.82.82.10</td>
</tr>
<tr>
<td>&lt;wsg_iproute_clear1_IPv4-address_mask&gt;</td>
<td>65.65.0.0 255.255.0.0</td>
<td>65.65.0.0 255.255.0.0</td>
</tr>
<tr>
<td>&lt;wsg_iproute_clear1_IPv4-address&gt;</td>
<td>93.93.93.10</td>
<td>92.92.92.10</td>
</tr>
<tr>
<td>&lt;wsg_iproute_clear2_IPv4-address_mask&gt;</td>
<td>66.66.0.0 255.255.0.0</td>
<td>66.66.0.0 255.255.0.0</td>
</tr>
<tr>
<td>&lt;wsg_iproute_clear2_IPv4-address&gt;</td>
<td>93.93.93.10</td>
<td>92.92.92.10</td>
</tr>
<tr>
<td>&lt;wsg_iproute_clear3_IPv4-address_mask&gt;</td>
<td>67.67.0.0 255.255.0.0</td>
<td>67.67.0.0 255.255.0.0</td>
</tr>
<tr>
<td>&lt;wsg_iproute_clear3_IPv4-address&gt;</td>
<td>93.93.93.10</td>
<td>92.92.92.10</td>
</tr>
<tr>
<td>&lt;wsg_iproute_clear4_IPv4-address_mask&gt;</td>
<td>68.68.0.0 255.255.0.0</td>
<td>68.68.0.0 255.255.0.0</td>
</tr>
<tr>
<td>&lt;wsg_iproute_clear4_IPv4-address&gt;</td>
<td>93.93.93.10</td>
<td>92.92.92.10</td>
</tr>
<tr>
<td>&lt;wsg_iproute_clear5_IPv4-address_mask&gt;</td>
<td>69.69.0.0 255.255.0.0</td>
<td>69.69.0.0 255.255.0.0</td>
</tr>
<tr>
<td>&lt;wsg_iproute_clear5_IPv4-address&gt;</td>
<td>93.93.93.10</td>
<td>92.92.92.10</td>
</tr>
<tr>
<td>&lt;wsg_iproute_ike1_IPv6-address/mask&gt;</td>
<td>2061::/16</td>
<td>2061::/16</td>
</tr>
<tr>
<td>&lt;wsg_iproute_ike1_nexthop_IPv6-address&gt;</td>
<td>2083::10</td>
<td>2082::10</td>
</tr>
<tr>
<td>&lt;wsg_iproute_ike2_IPv6-address/mask&gt;</td>
<td>2186::/16</td>
<td>2186::/16</td>
</tr>
<tr>
<td>&lt;wsg_iproute_ike2_nexthop_IPv6-address&gt;</td>
<td>2083::10</td>
<td>2082::10</td>
</tr>
<tr>
<td>&lt;wsg_iproute_clear1_IPv6-address/mask&gt;</td>
<td>2065::/16</td>
<td>2065::/16</td>
</tr>
<tr>
<td>&lt;wsg_iproute_clear1_nexthop_IPv6-address&gt;</td>
<td>2093::10</td>
<td>2092::10</td>
</tr>
<tr>
<td>&lt;wsg_iproute_clear2_IPv6-address/mask&gt;</td>
<td>2066::/16</td>
<td>2066::/16</td>
</tr>
<tr>
<td>&lt;wsg_iproute_clear2_nexthop_IPv6-address&gt;</td>
<td>2093::10</td>
<td>2092::10</td>
</tr>
<tr>
<td>&lt;wsg_iproute_clear3_IPv6-address/mask&gt;</td>
<td>2068::/16</td>
<td>2068::/16</td>
</tr>
<tr>
<td>&lt;wsg_iproute_clear3_nexthop_IPv6-address&gt;</td>
<td>2093::10</td>
<td>2092::10</td>
</tr>
<tr>
<td>&lt;wsg_iproute_clear4_IPv6-address/mask&gt;</td>
<td>2067::/16</td>
<td>2067::/16</td>
</tr>
<tr>
<td>&lt;wsg_iproute_clear4_nexthop_IPv6-address&gt;</td>
<td>2093::10</td>
<td>2092::10</td>
</tr>
</tbody>
</table>
## Sample L3 Interchassis HA Configuration

### SecGW VM Configuration (StarOS)

#### Table 11. StarOS IP Address Mapping - SecGW2

<table>
<thead>
<tr>
<th>Variable</th>
<th>Primary ASR 9000</th>
<th>Backup ASR 9000</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;wsg_iproute_clear5_IPV6-address/mask&gt;</td>
<td>2069::/16</td>
<td>2069::/16</td>
</tr>
<tr>
<td>&lt;wsg_iproute_clear5_nexthop_IPV6-address&gt;</td>
<td>2093::10</td>
<td>2092::10</td>
</tr>
<tr>
<td>&lt;wsg_sri-route_IPv4-address&gt;</td>
<td>23.23.23.23</td>
<td>23.23.23.23</td>
</tr>
<tr>
<td>&lt;wsg_sri-route_nexthop_IPv4-address&gt;</td>
<td>83.83.83.20</td>
<td>82.82.82.2</td>
</tr>
<tr>
<td>&lt;wsg_rri_nexthop_IPv4-address&gt;</td>
<td>93.93.93.20</td>
<td>—</td>
</tr>
<tr>
<td>&lt;wsg_rri_network-mode_IPv4-address&gt;</td>
<td>185.186.187.188</td>
<td>135.135.135.85</td>
</tr>
<tr>
<td>&lt;wsg_rri_network-mode_nexthop_IPv4-address&gt;</td>
<td>93.93.93.20</td>
<td>92.92.92.20</td>
</tr>
<tr>
<td>&lt;srp_monitor_hsrp_vlan_id&gt;</td>
<td>2062</td>
<td>2062</td>
</tr>
<tr>
<td>&lt;srp_hsrp-group_number&gt;</td>
<td>401</td>
<td>401</td>
</tr>
<tr>
<td>&lt;srp_peer_IPv4-address&gt;</td>
<td>72.72.72.20</td>
<td>73.73.73.20</td>
</tr>
<tr>
<td>&lt;srp_bind_IPv4-address&gt;</td>
<td>73.73.73.20</td>
<td>72.72.72.20</td>
</tr>
<tr>
<td>&lt;srp_interface_icsr_IPv4-address_mask&gt;</td>
<td>73.73.72.20 255.255.255.255</td>
<td>72.72.72.20 255.255.255.255</td>
</tr>
<tr>
<td>&lt;srp_iproute_icsr_IPv4-address_mask&gt;</td>
<td>0.0.0.0 0.0.0.0 73.73.73.10</td>
<td>0.0.0.0 0.0.0.0 72.72.72.10</td>
</tr>
<tr>
<td>&lt;connectedapps_session_IPv4-address&gt;</td>
<td>192.172.12.10</td>
<td>192.168.10.10</td>
</tr>
<tr>
<td>&lt;port_1/10_vlan_id&gt;</td>
<td>1301</td>
<td>1201</td>
</tr>
<tr>
<td>&lt;port_1/11_vlan_id_wsg&gt;</td>
<td>1311</td>
<td>1211</td>
</tr>
<tr>
<td>&lt;port_1/11_vlan_id_srp&gt;</td>
<td>1321</td>
<td>1221</td>
</tr>
<tr>
<td>&lt;interface_LOCAL1_IPv4-address_mask&gt;</td>
<td>10.78.1.116 255.255.255.0</td>
<td>10.78.1.112 255.255.255.0</td>
</tr>
<tr>
<td>&lt;interface_LOCAL1_IPv4-address_mask&gt;</td>
<td>192.172.12.13 255.255.255.0</td>
<td>192.168.10.2 255.255.255.0</td>
</tr>
<tr>
<td>&lt;iproute_LOCAL1_IPv4-address_mask&gt;</td>
<td>0.0.0.0 0.0.0.0 10.78.1.1</td>
<td>0.0.0.0 0.0.0.0 10.78.1.1</td>
</tr>
<tr>
<td>&lt;wsg_acl1_permit1_IPv4-address_mask&gt;</td>
<td>65.65.0.0 0.0.0.255.255</td>
<td>65.65.0.0 0.0.0.255.255</td>
</tr>
<tr>
<td>&lt;wsg_acl1_permit2_IPv4-address_mask&gt;</td>
<td>45.45.0.0 0.0.0.255.255</td>
<td>45.45.0.0 0.0.0.255.255</td>
</tr>
<tr>
<td>&lt;wsg_acl1_permit3_IPv4-address_mask&gt;</td>
<td>66.66.0.0 0.0.0.255.255</td>
<td>66.66.0.0 0.0.0.255.255</td>
</tr>
<tr>
<td>&lt;wsg_acl1_permit4_IPv4-address_mask&gt;</td>
<td>46.46.0.0 0.0.0.255.255</td>
<td>46.46.0.0 0.0.0.255.255</td>
</tr>
<tr>
<td>&lt;wsg_acl1_permit3_IPv4-address_mask&gt;</td>
<td>67.67.0.0 0.0.0.255.255</td>
<td>67.67.0.0 0.0.0.255.255</td>
</tr>
<tr>
<td>&lt;wsg_acl1_permit4_IPv4-address_mask&gt;</td>
<td>47.47.0.0 0.0.0.255.255</td>
<td>47.47.0.0 0.0.0.255.255</td>
</tr>
<tr>
<td>&lt;wsg_acl1_permit4_IPv4-address_mask&gt;</td>
<td>68.68.0.0 0.0.0.255.255</td>
<td>68.68.0.0 0.0.0.255.255</td>
</tr>
<tr>
<td></td>
<td>48.48.0.0 0.0.0.255.255</td>
<td>48.48.0.0 0.0.0.255.255</td>
</tr>
<tr>
<td>Variable</td>
<td>Primary ASR 9000</td>
<td>Backup ASR 9000</td>
</tr>
<tr>
<td>----------------------------------</td>
<td>---------------------------------------------------------------------------------</td>
<td>---------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>&lt;wsg_acl1_permit5_IPv4-address_mask&gt;</td>
<td>69.69.0.0 0.0.255.255 49.49.0.0 0.0.255.255</td>
<td>69.69.0.0 0.0.255.255 49.49.0.0 0.0.255.255</td>
</tr>
<tr>
<td>&lt;wsg_acl1_permit1_IPv6-address_mask&gt;</td>
<td>2065:: 0::ff:ff:ff:ff:ff:ff 2045:: 0::ff:ff:ff:ff:ff:ff:ff 2065:: 0::ff:ff:ff:ff:ff:ff:ff</td>
<td>2065:: 0::ff:ff:ff:ff:ff:ff 2045:: 0::ff:ff:ff:ff:ff:ff:ff 2065:: 0::ff:ff:ff:ff:ff:ff:ff</td>
</tr>
<tr>
<td>&lt;wsg_acl1_permit2_IPv6-address_mask&gt;</td>
<td>2066:: 0::ff:ff:ff:ff:ff:ff 2046:: 0::ff:ff:ff:ff:ff:ff:ff 2066:: 0::ff:ff:ff:ff:ff:ff:ff</td>
<td>2066:: 0::ff:ff:ff:ff:ff:ff 2046:: 0::ff:ff:ff:ff:ff:ff:ff 2066:: 0::ff:ff:ff:ff:ff:ff:ff</td>
</tr>
<tr>
<td>&lt;wsg_acl1_permit3_IPv6-address_mask&gt;</td>
<td>2067:: 0::ff:ff:ff:ff:ff:ff 2047:: 0::ff:ff:ff:ff:ff:ff:ff 2067:: 0::ff:ff:ff:ff:ff:ff:ff</td>
<td>2067:: 0::ff:ff:ff:ff:ff:ff 2047:: 0::ff:ff:ff:ff:ff:ff:ff 2067:: 0::ff:ff:ff:ff:ff:ff:ff</td>
</tr>
<tr>
<td>&lt;wsg_acl1_permit4_IPv6-address_mask&gt;</td>
<td>2068:: 0::ff:ff:ff:ff:ff:ff 2048:: 0::ff:ff:ff:ff:ff:ff:ff 2068:: 0::ff:ff:ff:ff:ff:ff:ff</td>
<td>2068:: 0::ff:ff:ff:ff:ff:ff 2048:: 0::ff:ff:ff:ff:ff:ff:ff 2068:: 0::ff:ff:ff:ff:ff:ff:ff</td>
</tr>
<tr>
<td>&lt;wsg_acl1_permit5_IPv6-address_mask&gt;</td>
<td>2069:: 0::ff:ff:ff:ff:ff:ff 2049:: 0::ff:ff:ff:ff:ff:ff:ff 2069:: 0::ff:ff:ff:ff:ff:ff:ff</td>
<td>2069:: 0::ff:ff:ff:ff:ff:ff 2049:: 0::ff:ff:ff:ff:ff:ff:ff 2069:: 0::ff:ff:ff:ff:ff:ff:ff</td>
</tr>
<tr>
<td>&lt;wsg_pool1_IPv4-address_mask&gt;</td>
<td>20.13.0.1 20.13.255.255</td>
<td>20.13.0.1 20.13.255.255</td>
</tr>
<tr>
<td>&lt;wsg_pool2_IPv6-address/mask&gt;</td>
<td>2013::/56</td>
<td>2013::/56</td>
</tr>
<tr>
<td>&lt;crypto_ike-ts-1_local_IPv6-address&gt;</td>
<td>2033::33</td>
<td>2033::23</td>
</tr>
<tr>
<td>&lt;wsg_interface_clear_IPv4-address_mask&gt;</td>
<td>95.95.95.20 255.255.255.0 94.94.94.20 255.255.255.0</td>
<td>94.94.94.20 255.255.255.0 94.94.94.20 255.255.255.0</td>
</tr>
<tr>
<td>&lt;wsg_interface_clear_IPv6-address/mask&gt;</td>
<td>2095::23/64</td>
<td>2094::23/64</td>
</tr>
<tr>
<td>&lt;wsg_interface_clear-loopback_IPv4-address_mask&gt;</td>
<td>95.95.95.100 255.255.255.255 94.94.94.100 255.255.255.255</td>
<td>94.94.94.100 255.255.255.255 94.94.94.100 255.255.255.255</td>
</tr>
<tr>
<td>&lt;wsg_interface_ike_IPv4-address_mask&gt;</td>
<td>85.85.85.20 255.255.255.255 84.84.84.20 255.255.255.255</td>
<td>84.84.84.20 255.255.255.255 84.84.84.20 255.255.255.255</td>
</tr>
<tr>
<td>&lt;wsg_interface_ike_IPv6-address/mask&gt;</td>
<td>2085::23/64</td>
<td>2084::23/64</td>
</tr>
<tr>
<td>&lt;wsg_interface_ike-loop_IPv4-address_mask&gt;</td>
<td>85.85.85.100 255.255.255.255 84.84.84.100 255.255.255.255</td>
<td>84.84.84.100 255.255.255.255 84.84.84.100 255.255.255.255</td>
</tr>
<tr>
<td>&lt;wsg_interface_wsg-service_loop_IPv4-address_mask&gt;</td>
<td>33.33.33.33 255.255.255.255 33.33.33.33 255.255.255.255</td>
<td>33.33.33.33 255.255.255.255 33.33.33.33 255.255.255.255</td>
</tr>
<tr>
<td>&lt;wsg_interface_wsg-service_loop_IPv6-address_mask&gt;</td>
<td>2033::33/128</td>
<td>2033::23/128</td>
</tr>
<tr>
<td>&lt;wsg-service_bind_ras_IPv4-address&gt;</td>
<td>33.33.33.33</td>
<td>—</td>
</tr>
<tr>
<td>&lt;wsg-service_bind_s2s_IPv4-address&gt;</td>
<td>—</td>
<td>33.33.33.33</td>
</tr>
<tr>
<td>&lt;wsg-service_bind_s2s_IPv6-address&gt;</td>
<td>2033::33</td>
<td>2033::23</td>
</tr>
<tr>
<td>Variable</td>
<td>Primary ASR 9000</td>
<td>Backup ASR 9000</td>
</tr>
<tr>
<td>-------------------------------</td>
<td>----------------------------------</td>
<td>----------------------------------</td>
</tr>
<tr>
<td>&lt;wsg_iproute_ike1_IPv4-address_mask&gt;</td>
<td>181.8.0.0 255.255.255.0</td>
<td>181.8.0.0 255.255.255.0</td>
</tr>
<tr>
<td>&lt;wsg_iproute_ike1_IPv4-address&gt;</td>
<td>85.85.85.10</td>
<td>84.84.84.10</td>
</tr>
<tr>
<td>&lt;wsg_iproute_ike2_IPv4-address_mask&gt;</td>
<td>186.0.0.0 255.0.0.0</td>
<td>186.0.0.0 255.0.0.0</td>
</tr>
<tr>
<td>&lt;wsg_iproute_ike2_IPv4-address&gt;</td>
<td>85.85.85.10</td>
<td>84.84.84.10</td>
</tr>
<tr>
<td>&lt;wsg_iproute_ike3_IPv4-address_mask&gt;</td>
<td>120.0.1.0 255.255.255.0</td>
<td>120.0.1.0 255.255.255.0</td>
</tr>
<tr>
<td>&lt;wsg_iproute_ike3_IPv4-address&gt;</td>
<td>85.85.85.10</td>
<td>84.84.84.10</td>
</tr>
<tr>
<td>&lt;wsg_iproute_ike4_IPv4-address_mask&gt;</td>
<td>211.0.1.0 255.255.255.0</td>
<td>211.0.1.0 255.255.255.0</td>
</tr>
<tr>
<td>&lt;wsg_iproute_ike4_IPv4-address&gt;</td>
<td>85.85.85.10</td>
<td>84.84.84.10</td>
</tr>
<tr>
<td>&lt;wsg_iproute_ike5_IPv4-address_mask&gt;</td>
<td>15.0.0.0 255.0.0.0</td>
<td>15.0.0.0 255.0.0.0</td>
</tr>
<tr>
<td>&lt;wsg_iproute_ike5_IPv4-address&gt;</td>
<td>85.85.85.10</td>
<td>84.84.84.10</td>
</tr>
<tr>
<td>&lt;wsg_iproute_clear1_IPv4-address_mask&gt;</td>
<td>65.65.0.0 255.255.0.0</td>
<td>65.65.0.0 255.255.0.0</td>
</tr>
<tr>
<td>&lt;wsg_iproute_clear1_IPv4-address&gt;</td>
<td>95.95.95.10</td>
<td>94.94.94.10</td>
</tr>
<tr>
<td>&lt;wsg_iproute_clear2_IPv4-address_mask&gt;</td>
<td>66.66.0.0 255.255.0.0</td>
<td>66.66.0.0 255.255.0.0</td>
</tr>
<tr>
<td>&lt;wsg_iproute_clear2_IPv4-address&gt;</td>
<td>95.95.95.10</td>
<td>94.94.94.10</td>
</tr>
<tr>
<td>&lt;wsg_iproute_clear3_IPv4-address_mask&gt;</td>
<td>67.67.0.0 255.255.0.0</td>
<td>67.67.0.0 255.255.0.0</td>
</tr>
<tr>
<td>&lt;wsg_iproute_clear3_IPv4-address&gt;</td>
<td>95.95.95.10</td>
<td>94.94.94.10</td>
</tr>
<tr>
<td>&lt;wsg_iproute_clear4_IPv4-address_mask&gt;</td>
<td>68.68.0.0 255.255.0.0</td>
<td>68.68.0.0 255.255.0.0</td>
</tr>
<tr>
<td>&lt;wsg_iproute_clear4_IPv4-address&gt;</td>
<td>95.95.95.10</td>
<td>94.94.94.10</td>
</tr>
<tr>
<td>&lt;wsg_iproute_clear5_IPv4-address_mask&gt;</td>
<td>69.69.0.0 255.255.0.0</td>
<td>69.69.0.0 255.255.0.0</td>
</tr>
<tr>
<td>&lt;wsg_iproute_clear5_IPv4-address&gt;</td>
<td>95.95.95.10</td>
<td>94.94.94.10</td>
</tr>
<tr>
<td>&lt;wsg_iproute_ike1_IPv6-address/mask&gt;</td>
<td>2061::/16</td>
<td>2061::/16</td>
</tr>
<tr>
<td>&lt;wsg_iproute_ike1_nexthop_IPv6-address&gt;</td>
<td>2085::10</td>
<td>2084::10</td>
</tr>
<tr>
<td>&lt;wsg_iproute_ike2_IPv6-address/mask&gt;</td>
<td>2186::/16</td>
<td>2186::/16</td>
</tr>
<tr>
<td>&lt;wsg_iproute_ike2_nexthop_IPv6-address&gt;</td>
<td>2085::10</td>
<td>2084::10</td>
</tr>
<tr>
<td>&lt;wsg_iproute_clear1_IPv6-address/mask&gt;</td>
<td>2065::/16</td>
<td>2065::/16</td>
</tr>
<tr>
<td>&lt;wsg_iproute_clear1_nexthop_IPv6-address&gt;</td>
<td>2095::10</td>
<td>2094::10</td>
</tr>
<tr>
<td>&lt;wsg_iproute_clear2_IPv6-address/mask&gt;</td>
<td>2066::/16</td>
<td>2066::/16</td>
</tr>
<tr>
<td>&lt;wsg_iproute_clear2_nexthop_IPv6-address&gt;</td>
<td>2095::10</td>
<td>2094::10</td>
</tr>
<tr>
<td>&lt;wsg_iproute_clear3_IPv6-address/mask&gt;</td>
<td>2068::/16</td>
<td>2068::/16</td>
</tr>
<tr>
<td>&lt;wsg_iproute_clear3_nexthop_IPv6-address&gt;</td>
<td>2095::10</td>
<td>2094::10</td>
</tr>
<tr>
<td>&lt;wsg_iproute_clear4_IPv6-address/mask&gt;</td>
<td>2067::/16</td>
<td>2067::/16</td>
</tr>
<tr>
<td>&lt;wsg_iproute_clear4_nexthop_IPv6-address&gt;</td>
<td>2095::10</td>
<td>2094::10</td>
</tr>
</tbody>
</table>
### Table 12. StarOS IP Address Mapping - SecGW3

<table>
<thead>
<tr>
<th>Variable</th>
<th>Primary ASR 9000</th>
<th>Backup ASR 9000</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;interface_LOCAL1_IPv4-address_mask&gt;</td>
<td>10.78.1.117 255.255.255.0</td>
<td>10.78.1.113 255.255.255.0</td>
</tr>
<tr>
<td>&lt;interface_LOCAL1_IPv4-address_mask_secondary&gt;</td>
<td>192.172.12.13 255.255.255.0</td>
<td>192.168.10.13 255.255.255.0</td>
</tr>
<tr>
<td>iproute_LOCAL1_IPv4-address_mask&gt;</td>
<td>0.0.0.0 0.0.0.0 10.78.1.1</td>
<td>0.0.0.0 0.0.0.0 10.78.1.1</td>
</tr>
<tr>
<td>wsg_acl1_permit1_IPv4-address_mask&gt;</td>
<td>65.65.0.0 0.0.255.255</td>
<td>65.65.0.0 0.0.255.255</td>
</tr>
<tr>
<td>wsg_acl1_permit2_IPv4-address_mask&gt;</td>
<td>66.66.0.0 0.0.255.255</td>
<td>66.66.0.0 0.0.255.255</td>
</tr>
<tr>
<td>wsg_acl1_permit3_IPv4-address_mask&gt;</td>
<td>67.67.0.0 0.0.255.255</td>
<td>67.67.0.0 0.0.255.255</td>
</tr>
<tr>
<td>wsg_acl1_permit4_IPv4-address_mask&gt;</td>
<td>68.68.0.0 0.0.255.255</td>
<td>68.68.0.0 0.0.255.255</td>
</tr>
</tbody>
</table>
### Sample L3 Interchassis HA Configuration

#### SecGW VM Configuration (StarOS)

<table>
<thead>
<tr>
<th>Variable</th>
<th>Primary ASR 9000</th>
<th>Backup ASR 9000</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>&lt;wsg_acl1_permit5_IPv4-address_mask&gt;</code></td>
<td>69.69.0.0 0.0.255.255</td>
<td>69.69.0.0 0.0.255.255</td>
</tr>
<tr>
<td></td>
<td>49.49.0.0 0.0.255.255</td>
<td>49.49.0.0 0.0.255.255</td>
</tr>
<tr>
<td><code>&lt;wsg_acl1_permit1_IPv6-address_mask&gt;</code></td>
<td>2065:::</td>
<td>2065:::</td>
</tr>
<tr>
<td></td>
<td>2045:::</td>
<td>2045:::</td>
</tr>
<tr>
<td><code>&lt;wsg_acl1_permit2_IPv6-address_mask&gt;</code></td>
<td>2066:::</td>
<td>2066:::</td>
</tr>
<tr>
<td></td>
<td>2046:::</td>
<td>2046:::</td>
</tr>
<tr>
<td><code>&lt;wsg_acl1_permit3_IPv6-address_mask&gt;</code></td>
<td>2067:::</td>
<td>2067:::</td>
</tr>
<tr>
<td></td>
<td>2047:::</td>
<td>2047:::</td>
</tr>
<tr>
<td><code>&lt;wsg_acl1_permit4_IPv6-address_mask&gt;</code></td>
<td>2068:::</td>
<td>2068:::</td>
</tr>
<tr>
<td></td>
<td>2048:::</td>
<td>2048:::</td>
</tr>
<tr>
<td><code>&lt;wsg_acl1_permit5_IPv6-address_mask&gt;</code></td>
<td>2069:::</td>
<td>2069:::</td>
</tr>
<tr>
<td></td>
<td>2049:::</td>
<td>2049:::</td>
</tr>
<tr>
<td><code>&lt;wsg_pool1_IPv4-address_mask&gt;</code></td>
<td>20.13.0.1 20.13.255.255</td>
<td>20.13.0.1 20.13.255.255</td>
</tr>
<tr>
<td><code>&lt;wsg_pool2_IPv6-address/mask&gt;</code></td>
<td>2013::/56</td>
<td>2013::/56</td>
</tr>
<tr>
<td><code>&lt;crypto_ike-ts-1_local_IPv6-address&gt;</code></td>
<td>2043::33</td>
<td>2043::33</td>
</tr>
<tr>
<td><code>&lt;wsg_interface_clear_IPv4-address_mask&gt;</code></td>
<td>97.97.97.20 255.255.255.0</td>
<td>96.96.96.100 255.255.255.255</td>
</tr>
<tr>
<td><code>&lt;wsg_interface_clear_IPv6-address/mask&gt;</code></td>
<td>2096::23/64</td>
<td>2096::23/64</td>
</tr>
<tr>
<td><code>&lt;wsg_interface_clear-loopback_IPv4-address_mask&gt;</code></td>
<td>97.97.97.100 255.255.255.255</td>
<td>96.96.96.100 255.255.255.255</td>
</tr>
<tr>
<td><code>&lt;wsg_interface_ike_IPv4-address_mask&gt;</code></td>
<td>87.87.87.20 255.255.255.0</td>
<td>86.86.86.20 255.255.255.0</td>
</tr>
<tr>
<td><code>&lt;wsg_interface_ike_IPv6-address/mask&gt;</code></td>
<td>2086::23/64</td>
<td>2086::23/64</td>
</tr>
<tr>
<td><code>&lt;wsg_interface_ike-loop_IPv4-address_mask&gt;</code></td>
<td>87.87.87.100 255.255.255.255</td>
<td>86.86.86.100 255.255.255.255</td>
</tr>
<tr>
<td><code>&lt;wsg_interface_wsg-service_loop_IPv4-address_mask&gt;</code></td>
<td>43.43.43.43 255.255.255.255</td>
<td>43.43.43.43 255.255.255.255</td>
</tr>
<tr>
<td><code>&lt;wsg_interface_wsg-service_loop_IPv6-address_mask&gt;</code></td>
<td>2043::43/128</td>
<td>2043::43/128</td>
</tr>
<tr>
<td><code>&lt;wsg-service_bind_ras_IPv4-address&gt;</code></td>
<td>—</td>
<td>—</td>
</tr>
<tr>
<td><code>&lt;wsg-service_bind_s2s_IPv4-address&gt;</code></td>
<td>43.43.43.43</td>
<td>43.43.43.43</td>
</tr>
<tr>
<td><code>&lt;wsg-service_bind_s2s_IPv6-address&gt;</code></td>
<td>2043::43</td>
<td>2043::43</td>
</tr>
<tr>
<td>Variable</td>
<td>Primary ASR 9000</td>
<td>Backup ASR 9000</td>
</tr>
<tr>
<td>----------------------------------------------</td>
<td>------------------------------</td>
<td>----------------------------</td>
</tr>
<tr>
<td>&lt;wsg_iproute_ike1_IPv4-address_mask&gt;</td>
<td>181.8.0.0 255.255.255.0</td>
<td>181.8.0.0 255.255.255.0</td>
</tr>
<tr>
<td>&lt;wsg_iproute_ike1_IPv4-address&gt;</td>
<td>87.87.87.10</td>
<td>84.84.84.10</td>
</tr>
<tr>
<td>&lt;wsg_iproute_ike2_IPv4-address_mask&gt;</td>
<td>186.0.0.0 255.0.0.0</td>
<td>186.0.0.0 255.0.0.0</td>
</tr>
<tr>
<td>&lt;wsg_iproute_ike2_IPv4-address&gt;</td>
<td>87.87.87.10</td>
<td>86.86.86.10</td>
</tr>
<tr>
<td>&lt;wsg_iproute_ike3_IPv4-address_mask&gt;</td>
<td>120.0.1.0 255.255.255.0</td>
<td>120.0.1.0 255.255.255.0</td>
</tr>
<tr>
<td>&lt;wsg_iproute_ike3_IPv4-address&gt;</td>
<td>87.87.87.10</td>
<td>86.86.86.10</td>
</tr>
<tr>
<td>&lt;wsg_iproute_ike4_IPv4-address_mask&gt;</td>
<td>—</td>
<td>211.0.1.0 255.255.255.0</td>
</tr>
<tr>
<td>&lt;wsg_iproute_ike4_IPv4-address&gt;</td>
<td>—</td>
<td>86.86.86.10</td>
</tr>
<tr>
<td>&lt;wsg_iproute_ike5_IPv4-address_mask&gt;</td>
<td>17.0.0.0 255.0.0.0</td>
<td>17.0.0.0 255.0.0.0</td>
</tr>
<tr>
<td>&lt;wsg_iproute_ike5_IPv4-address&gt;</td>
<td>87.87.87.10</td>
<td>86.86.86.10</td>
</tr>
<tr>
<td>&lt;wsg_iproute_clear1_IPv4-address_mask&gt;</td>
<td>65.65.0.0 255.255.0.0</td>
<td>65.65.0.0 255.255.0.0</td>
</tr>
<tr>
<td>&lt;wsg_iproute_clear1_IPv4-address&gt;</td>
<td>97.97.97.10</td>
<td>96.96.96.10</td>
</tr>
<tr>
<td>&lt;wsg_iproute_clear2_IPv4-address_mask&gt;</td>
<td>66.66.0.0 255.255.0.0</td>
<td>66.66.0.0 255.255.0.0</td>
</tr>
<tr>
<td>&lt;wsg_iproute_clear2_IPv4-address&gt;</td>
<td>97.97.97.10</td>
<td>96.96.96.10</td>
</tr>
<tr>
<td>&lt;wsg_iproute_clear3_IPv4-address_mask&gt;</td>
<td>67.67.0.0 255.255.0.0</td>
<td>67.67.0.0 255.255.0.0</td>
</tr>
<tr>
<td>&lt;wsg_iproute_clear3_IPv4-address&gt;</td>
<td>97.97.97.10</td>
<td>96.96.96.10</td>
</tr>
<tr>
<td>&lt;wsg_iproute_clear4_IPv4-address_mask&gt;</td>
<td>68.68.0.0 255.255.0.0</td>
<td>68.68.0.0 255.255.0.0</td>
</tr>
<tr>
<td>&lt;wsg_iproute_clear4_IPv4-address&gt;</td>
<td>97.97.97.10</td>
<td>96.96.96.10</td>
</tr>
<tr>
<td>&lt;wsg_iproute_clear5_IPv4-address_mask&gt;</td>
<td>69.69.0.0 255.255.0.0</td>
<td>69.69.0.0 255.255.0.0</td>
</tr>
<tr>
<td>&lt;wsg_iproute_clear5_IPv4-address&gt;</td>
<td>97.97.97.10</td>
<td>96.96.96.10</td>
</tr>
<tr>
<td>&lt;wsg_iproute_ike1_IPv6-address/mask&gt;</td>
<td>—</td>
<td>2061::/16</td>
</tr>
<tr>
<td>&lt;wsg_iproute_ike1_nexthop_IPv6-address&gt;</td>
<td>—</td>
<td>2086::/10</td>
</tr>
<tr>
<td>&lt;wsg_iproute_ike2_IPv6-address/mask&gt;</td>
<td>—</td>
<td>2186::/16</td>
</tr>
<tr>
<td>&lt;wsg_iproute_ike2_nexthop_IPv6-address&gt;</td>
<td>—</td>
<td>2086::/10</td>
</tr>
<tr>
<td>&lt;wsg_iproute_clear1_IPv6-address/mask&gt;</td>
<td>—</td>
<td>2065::/16</td>
</tr>
<tr>
<td>&lt;wsg_iproute_clear1_nexthop.IPv6-address&gt;</td>
<td>—</td>
<td>2096::/10</td>
</tr>
<tr>
<td>&lt;wsg_iproute_clear2_IPv6-address/mask&gt;</td>
<td>—</td>
<td>2066::/16</td>
</tr>
<tr>
<td>&lt;wsg_iproute_clear2_nexthop_IPv6-address&gt;</td>
<td>—</td>
<td>2096::/10</td>
</tr>
<tr>
<td>&lt;wsg_iproute_clear3_IPv6-address/mask&gt;</td>
<td>—</td>
<td>2068::/16</td>
</tr>
<tr>
<td>&lt;wsg_iproute_clear3_nexthop_IPv6-address&gt;</td>
<td>—</td>
<td>2096::/10</td>
</tr>
<tr>
<td>&lt;wsg_iproute_clear4_IPv6-address/mask&gt;</td>
<td>—</td>
<td>2067::/16</td>
</tr>
<tr>
<td>&lt;wsg_iproute_clear4_nexthop_IPv6-address&gt;</td>
<td>—</td>
<td>2096::/10</td>
</tr>
</tbody>
</table>
### Table 13. StarOS IP Address Mapping - SecGW4

<table>
<thead>
<tr>
<th>Variable</th>
<th>Primary ASR 9000</th>
<th>Backup ASR 9000</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;interface_LOCAL1_IPv4-address_mask&gt;</td>
<td>10.78.1.118 255.255.255.0</td>
<td>10.78.1.114 255.255.255.0</td>
</tr>
<tr>
<td>&lt;interface_LOCAL1_IPv4-address_mask_secondary&gt;</td>
<td>192.172.12.14 255.255.255.0</td>
<td>92.168.10.14 255.255.255.0</td>
</tr>
<tr>
<td>&lt;iproute_LOCAL1_IPv4-address_mask&gt;</td>
<td>0.0.0.0 0.0.0.0 10.78.1.1</td>
<td>0.0.0.0 0.0.0.0 10.78.1.1</td>
</tr>
<tr>
<td>&lt;wsg_acl1_permit1_IPv4-address_mask&gt;</td>
<td>65.65.0.0 0.0.255.255</td>
<td>65.65.0.0 0.0.255.255</td>
</tr>
<tr>
<td></td>
<td>45.45.0.0 0.0.255.255</td>
<td>45.45.0.0 0.0.255.255</td>
</tr>
<tr>
<td>&lt;wsg_acl1_permit2_IPv4-address_mask&gt;</td>
<td>66.66.0.0 0.0.255.25</td>
<td>66.66.0.0 0.0.255.25</td>
</tr>
<tr>
<td></td>
<td>46.46.0.0 0.0.255.25</td>
<td>46.46.0.0 0.0.255.25</td>
</tr>
<tr>
<td>&lt;wsg_acl1_permit3_IPv4-address_mask&gt;</td>
<td>67.67.0.0 0.0.255.25</td>
<td>67.67.0.0 0.0.255.25</td>
</tr>
<tr>
<td></td>
<td>47.47.0.0 0.0.255.25</td>
<td>47.47.0.0 0.0.255.25</td>
</tr>
<tr>
<td>&lt;wsg_acl1_permit4_IPv4-address_mask&gt;</td>
<td>68.68.0.0 0.0.255.25</td>
<td>68.68.0.0 0.0.255.25</td>
</tr>
<tr>
<td></td>
<td>48.48.0.0 0.0.255.25</td>
<td>48.48.0.0 0.0.255.25</td>
</tr>
</tbody>
</table>
### Sample L3 Interchassis HA Configuration

#### SecGW VM Configuration (StarOS)

<table>
<thead>
<tr>
<th>Variable</th>
<th>Primary ASR 9000</th>
<th>Backup ASR 9000</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;wsg_acl1_permit5_IPv4-address_mask&gt;</td>
<td>69.69.0.0 0.0.255.255 49.49.0.0 0.0.255.255</td>
<td>69.69.0.0 0.0.255.255 49.49.0.0 0.0.255.255</td>
</tr>
<tr>
<td>&lt;wsg_pool1_IPv4-address_mask&gt;</td>
<td>20.13.0.1 20.13.255.255</td>
<td>20.13.0.1 20.13.255.255</td>
</tr>
<tr>
<td>&lt;wsg_pool2_IPv6-address_mask&gt;</td>
<td>2013::/56</td>
<td>2013::/56</td>
</tr>
<tr>
<td>&lt;crypto_ike-ts-1_local_IPv6-address&gt;</td>
<td>2053::53</td>
<td>2023::23</td>
</tr>
<tr>
<td>&lt;wsg_interface_clear_IPv4-address_mask&gt;</td>
<td>99.99.99.20 255.255.255.0</td>
<td>98.98.98.20 255.255.255.0</td>
</tr>
<tr>
<td>&lt;wsg_interface_clear_IPv6-address_mask&gt;</td>
<td>2099::23/64</td>
<td>2098::23/64</td>
</tr>
<tr>
<td>&lt;wsg_interface_clear-loopback_IPv4-address_mask&gt;</td>
<td>99.99.99.100 255.255.255.255</td>
<td>98.98.98.100 255.255.255.255</td>
</tr>
<tr>
<td>&lt;wsg_interface_ike_IPv4-address_mask&gt;</td>
<td>89.89.89.20 255.255.255.0</td>
<td>88.88.88.20 255.255.255.0</td>
</tr>
<tr>
<td>&lt;wsg_interface_ike_IPv6-address_mask&gt;</td>
<td>2089::23/64</td>
<td>2088::23/64</td>
</tr>
<tr>
<td>&lt;wsg_interface_ike-loop_IPv4-address_mask&gt;</td>
<td>89.89.89.100 255.255.255.255</td>
<td>88.88.88.100 255.255.255.255</td>
</tr>
<tr>
<td>&lt;wsg_interface_wsg-service_loop_IPv4-address_mask&gt;</td>
<td>53.53.53.53 255.255.255.255</td>
<td>53.53.53.53 255.255.255.255</td>
</tr>
<tr>
<td>&lt;wsg_interface_wsg-service_loop_IPv6-address_mask&gt;</td>
<td>2053::53/128</td>
<td>2053::53/128</td>
</tr>
<tr>
<td>&lt;wsg-service_bind_ras_IPv4-address&gt;</td>
<td>—</td>
<td>—</td>
</tr>
<tr>
<td>&lt;wsg-service_bind_s2s_IPv4-address&gt;</td>
<td>53.53.53.53</td>
<td>53.53.53.53</td>
</tr>
<tr>
<td>&lt;wsg-service_bind_s2s_IPv6-address&gt;</td>
<td>2053::53</td>
<td>2053::53</td>
</tr>
<tr>
<td>Variable</td>
<td>Primary ASR 9000</td>
<td>Backup ASR 9000</td>
</tr>
<tr>
<td>----------------------------------------------</td>
<td>----------------------------------</td>
<td>-----------------------------------</td>
</tr>
<tr>
<td>&lt;wsg_iproute_ike1_IPv4-address_mask&gt;</td>
<td>181.8.0.0 255.255.255.0</td>
<td>181.8.0.0 255.255.255.0</td>
</tr>
<tr>
<td>&lt;wsg_iproute_ike1_IPv4-address&gt;</td>
<td>89.89.89.10</td>
<td>88.88.88.10</td>
</tr>
<tr>
<td>&lt;wsg_iproute_ike2_IPv4-address_mask&gt;</td>
<td>186.0.0.0 255.0.0.0</td>
<td>186.0.0.0 255.0.0.0</td>
</tr>
<tr>
<td>&lt;wsg_iproute_ike2_IPv4-address&gt;</td>
<td>89.89.89.10</td>
<td>88.88.88.10</td>
</tr>
<tr>
<td>&lt;wsg_iproute_ike3_IPv4-address_mask&gt;</td>
<td>120.0.1.0 255.255.255.0</td>
<td>120.0.1.0 255.255.255.0</td>
</tr>
<tr>
<td>&lt;wsg_iproute_ike3_IPv4-address&gt;</td>
<td>89.89.89.10</td>
<td>88.88.88.10</td>
</tr>
<tr>
<td>&lt;wsg_iproute_ike4_IPv4-address_mask&gt;</td>
<td>—</td>
<td>211.0.1.0 255.255.255.0</td>
</tr>
<tr>
<td>&lt;wsg_iproute_ike4_IPv4-address&gt;</td>
<td>—</td>
<td>88.88.88.10</td>
</tr>
<tr>
<td>&lt;wsg_iproute_ike5_IPv4-address_mask&gt;</td>
<td>19.0.0.0 255.0.0.0</td>
<td>19.0.0.0 255.0.0.0</td>
</tr>
<tr>
<td>&lt;wsg_iproute_ike5_IPv4-address&gt;</td>
<td>89.89.89.10</td>
<td>88.88.88.10</td>
</tr>
<tr>
<td>&lt;wsg_iproute_clear1_IPv4-address_mask&gt;</td>
<td>65.65.0.0 255.255.255.0</td>
<td>65.65.0.0 255.255.255.0</td>
</tr>
<tr>
<td>&lt;wsg_iproute_clear1_IPv4-address&gt;</td>
<td>99.99.99.10</td>
<td>98.98.98.10</td>
</tr>
<tr>
<td>&lt;wsg_iproute_clear2_IPv4-address_mask&gt;</td>
<td>66.66.0.0 255.255.255.0</td>
<td>66.66.0.0 255.255.255.0</td>
</tr>
<tr>
<td>&lt;wsg_iproute_clear2_IPv4-address&gt;</td>
<td>99.99.99.10</td>
<td>98.98.98.10</td>
</tr>
<tr>
<td>&lt;wsg_iproute_clear3_IPv4-address_mask&gt;</td>
<td>67.67.0.0 255.255.255.0</td>
<td>67.67.0.0 255.255.255.0</td>
</tr>
<tr>
<td>&lt;wsg_iproute_clear3_IPv4-address&gt;</td>
<td>99.99.99.10</td>
<td>98.98.98.10</td>
</tr>
<tr>
<td>&lt;wsg_iproute_clear4_IPv4-address_mask&gt;</td>
<td>68.68.0.0 255.255.255.0</td>
<td>68.68.0.0 255.255.255.0</td>
</tr>
<tr>
<td>&lt;wsg_iproute_clear4_IPv4-address&gt;</td>
<td>99.99.99.10</td>
<td>98.98.98.10</td>
</tr>
<tr>
<td>&lt;wsg_iproute_clear5_IPv4-address_mask&gt;</td>
<td>69.69.0.0 255.255.255.0</td>
<td>69.69.0.0 255.255.255.0</td>
</tr>
<tr>
<td>&lt;wsg_iproute_clear5_IPv4-address&gt;</td>
<td>99.99.99.10</td>
<td>98.98.98.10</td>
</tr>
<tr>
<td>&lt;wsg_iproute_ike1_IPv6-address&gt;</td>
<td>2061::/16</td>
<td>2061::/16</td>
</tr>
<tr>
<td>&lt;wsg_iproute_ike1_nexthop_IPv6-address&gt;</td>
<td>2089::10</td>
<td>2088::10</td>
</tr>
<tr>
<td>&lt;wsg_iproute_ike2_IPv6-address&gt;</td>
<td>2186::/16</td>
<td>2186::/16</td>
</tr>
<tr>
<td>&lt;wsg_iproute_ike2_nexthop_IPv6-address&gt;</td>
<td>2089::10</td>
<td>2088::10</td>
</tr>
<tr>
<td>&lt;wsg_iproute_clear1_IPv6-address&gt;</td>
<td>2065::/16</td>
<td>2065::/16</td>
</tr>
<tr>
<td>&lt;wsg_iproute_clear1_nexthop_IPv6-address&gt;</td>
<td>2099::10</td>
<td>2098::10</td>
</tr>
<tr>
<td>&lt;wsg_iproute_clear2_IPv6-address&gt;</td>
<td>2066::/16</td>
<td>2066::/16</td>
</tr>
<tr>
<td>&lt;wsg_iproute_clear2_nexthop_IPv6-address&gt;</td>
<td>2099::10</td>
<td>2098::10</td>
</tr>
<tr>
<td>&lt;wsg_iproute_clear3_IPv6-address&gt;</td>
<td>2068::/16</td>
<td>2068::/16</td>
</tr>
<tr>
<td>&lt;wsg_iproute_clear3_nexthop_IPv6-address&gt;</td>
<td>2099::10</td>
<td>2098::10</td>
</tr>
<tr>
<td>&lt;wsg_iproute_clear4_IPv6-address&gt;</td>
<td>2067::/16</td>
<td>2067::/16</td>
</tr>
<tr>
<td>&lt;wsg_iproute_clear4_nexthop_IPv6-address&gt;</td>
<td>2099::10</td>
<td>2098::10</td>
</tr>
</tbody>
</table>
## SecGW VM Configuration - Primary and Backup ASR 9000 Chassis

```plaintext
config
  cli hidden
  tech-support test-commands encrypted password <unique_encrypted_password>
  cli test-commands encrypted password <unique_encrypted_password>
  license key "\
  <SecGW_license_key>
  system hostname <ASR9K_hostname>-<SecGW#>
  orbem
    no siop-port
    no iiop-port
```

### Variable

<table>
<thead>
<tr>
<th>Variable</th>
<th>Primary ASR 9000</th>
<th>Backup ASR 9000</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;wsg_iproute_clear5_IPv6-address/mask&gt;</td>
<td>2069::/16</td>
<td>2069::/16</td>
</tr>
<tr>
<td>&lt;wsg_iproute_clear5_nexthop_IPv6-address&gt;</td>
<td>2099::10</td>
<td>2098::10</td>
</tr>
<tr>
<td>&lt;wsg_sri-route_IPv4-address&gt;</td>
<td>53.53.53.53</td>
<td>53.53.53.53</td>
</tr>
<tr>
<td>&lt;wsg_sri-route_nexthop_IPv4-address&gt;</td>
<td>89.89.89.20</td>
<td>88.88.88.20</td>
</tr>
<tr>
<td>&lt;wsg_rri_nexthop_IPv4-address&gt;</td>
<td>—</td>
<td>—</td>
</tr>
<tr>
<td>&lt;wsg_rri_network-mode_IPv4-address&gt;</td>
<td>88.88.88.88</td>
<td>88.88.88.88</td>
</tr>
<tr>
<td>&lt;wsg_rri_network-mode_nexthop_IPv4-address&gt;</td>
<td>99.99.99.2</td>
<td>98.98.98.20</td>
</tr>
<tr>
<td>&lt;srp_monitor_hsrp_vlan_id&gt;</td>
<td>2065</td>
<td>2065</td>
</tr>
<tr>
<td>&lt;srp_hsrp-group_number&gt;</td>
<td>404</td>
<td>404</td>
</tr>
<tr>
<td>&lt;srp_peer_IPv4-address&gt;</td>
<td>78.78.78.20</td>
<td>79.79.79.20</td>
</tr>
<tr>
<td>&lt;srp_bind_IPv4-address&gt;</td>
<td>79.79.79.20</td>
<td>78.78.78.20</td>
</tr>
<tr>
<td>&lt;srp_interface_icsr_IPv4-address_mask&gt;</td>
<td>79.79.79.20 255.255.255.0</td>
<td>78.78.78.20 255.255.255.0</td>
</tr>
<tr>
<td>&lt;sr_iproute_icsr_IPv4-address_mask&gt;</td>
<td>0.0.0.0 0.0.0.0 79.79.79.10</td>
<td>0.0.0.0 0.0.0.0 78.78.78.10</td>
</tr>
<tr>
<td>&lt;connectedapps_session_IPv4-address&gt;</td>
<td>192.172.12.10</td>
<td>192.168.10.10</td>
</tr>
<tr>
<td>&lt;port_1/10_vlan_id&gt;</td>
<td>1304</td>
<td>1204</td>
</tr>
<tr>
<td>&lt;port_1/11_vlan_id_wsg&gt;</td>
<td>1314</td>
<td>1214</td>
</tr>
<tr>
<td>&lt;port_1/11_vlan_id_srp&gt;</td>
<td>1324</td>
<td>1224</td>
</tr>
</tbody>
</table>
#exit

crash enable encrypted url <encrypted_url>
require session recovery
context local
  no ip guarantee framed-route local-switching
interface LOCAL1
  ip address <LOCAL1_IPv4-address_mask>
  ip address <LOCAL1_IPv4-address_mask_secondary>
#exit
  server ftpd
#exit
  ssh key
    <unique_encrypted_ssh_key1>
    ssh key
    <unique_encrypted_ssh_key2>
    ssh key
    <unique_encrypted_ssh_key3>
  server sshd
    subsystem sftp
  #exit
  server telnetd
  #exit
  subscriber default
  exit
  administrator admin encrypted password <unique_encrypted_password>
  aaa group default
  #exit
  ip route <iproute_:LOCAL1_IPv4-address_mask> LOCAL1
#exit
port ethernet 1/1
description ICSR
no shutdown
bind interface LOCAL1 local

#exit
cacertificate name test \
pem data \
"-----BEGIN CERTIFICATE-----\n<certificate_data>
-----END CERTIFICATE-----"
task facility sessmgr max 384

#exit
ccontext wsg
ip access-list acl1
permit ip <wsg_acl1_permit1_IPv4-address_mask> <wsg_acl1_permit1_IPv4-address_mask>
permit ip <wsg_acl1_permit2_IPv4-address_mask> <wsg_acl1_permit2_IPv4-address_mask>
permit ip <wsg_acl1_permit3_IPv4-address_mask> <wsg_acl1_permit3_IPv4-address_mask>
permit ip <wsg_acl1_permit4_IPv4-address_mask> <wsg_acl1_permit4_IPv4-address_mask>
permit ip <wsg_acl1_permit5_IPv4-address_mask> <wsg_acl1_permit5_IPv4-address_mask>

#exit
ipv6 access-list acl1
permit ip <wsg_acl1_permit1_IPv6-address_mask> <wsg_acl1_permit1_IPv6-address_mask>
permit ip <wsg_acl1_permit2_IPv6-address_mask> <wsg_acl1_permit2_IPv6-address_mask>
permit ip <wsg_acl1_permit3_IPv6-address_mask> <wsg_acl1_permit3_IPv6-address_mask>
permit ip <wsg_ac1l_permit4_IPv6-address_mask> <wsg_ac1l_permit5_IPv6-address_mask>
permit ip <wsg_ac1l_permit6_IPv6-address_mask> <wsg_ac1l_permit5_IPv6-address_mask>

#exit

no ip guarantee framed-route local-switching

ip pool pool1 range <wsg_pool1_IPv4-address/mask> <wsg_pool2_IPv4-address/mask> public 0
    ip pool pool2 range <wsg_pool2_IPv4-address/mask> <wsg_pool2_IPv4-address/mask> public 0
    ipv6 pool ipv6-pool1 prefix <wsg_pool1_IPv6-address/mask> public 0
    ipsec transform-set ike-ts-1
    #exit

ikev2-ikesa transform-set ikesa-f00
#exit

crypto template ipv4 ikev2-dynamic
    authentication local pre-shared-key encrypted key <unique_encrypted_key>
    authentication remote pre-shared-key encrypted key <unique_encrypted_key>
    max-childsa 5 overload-action ignore
    ikev2-ikesa transform-set list ike-ts-1
    ikev2-ikesa rekey
    payload ipv4 match childsa match ipv4
        ip-address-alloc dynamic
        ipsec transform-set list ipsec-ts-1
        rekey keepalive
        #exit

crypto template ipv4 ikev2-dynamic
    authentication local pre-shared-key encrypted key <unique_encrypted_key>
    authentication remote pre-shared-key encrypted key <unique_encrypted_key>
max-childsa 5 overload-action ignore
ikev2-ikesa transform-list ike-ts-1
ikev2-ikesa rekey
payload ipv6 match childsa match ipv6
    ipv-address-alloc dynamic
ipsec transform-list ipsec-ts-1
    rekey keepalive
    #exit
identity local id-type ip-addr id <crypto_ike-ts-1_IPv6-address>
    #exit
interface clear
    ip address <wsg_interface_clear_IPV4-address>
    ipv6 address <wsg_interface_clear_IPV6-address> secondary
    #exit
interface clear-loop loopback
    ip address <wsg_interface_clear-loopback_IPV4-address_mask> srp-activate
    #exit
interface ike
    ip address <wsg_interface_ike_IPV4-address_mask> srp-activate
    ipv6 address <wsg_interface_ike_IPV6-address_mask> srp-activate
    #exit
interface ike-loop loopback
    ip address <wsg_interface_ike-loop_IPV4-address_mask> srp-activate
    #exit
interface ike-loop-v6 loopback
    ipv6 address <wsg_interface_ike-loop_IPV6-address_mask> srp-activate
    #exit
interface wsg-service-ipv4 loopback
    ip address <wsg_interface_wsg-service_loop_IPV4-address_mask> srp-activate
#exit
interface wsg-service-ipv6 loopback
   ipv6 address <wsg_interface_wsg-service_loop_IPv6-address/mask> srp-activate
#exit
subscriber default
exit
aaa group default
#exit
wsg-service ipv4-ras
   deployment-mode remote-acces
   ip access-group acl1
   bind address <wsg-service_bind_rar_IPv4-address> crypto-template ipv4
#exit
wsg-service ipv6-s2s
   deployment-mode site-to-site
   ipv6 access-group acl1
   bind address <wsg-service_bind_s2s_IPv6-address> crypto-template ipv6
#exit
ip route <wsg_iproute_ike1_IPv4-address mask> <wsg_iproute_ike1_IPv4-address> ike
ip route <wsg_iproute_ike2_IPv4-address mask> <wsg_iproute_ike2_IPv4-address> ike
ip route <wsg_iproute_ike3_IPv4-address mask> <wsg_iproute_ike3_IPv4-address> ike
ip route <wsg_iproute_ike4_IPv4-address mask> <wsg_iproute_ike4_IPv4-address> ike
ip route <wsg_iproute_ike5_IPv4-address mask> <wsg_iproute_ike5_IPv4-address> ike
ip route <wsg_iproute_clear1_IPv4-address_mask> <wsg_iproute_clear1__IPv4-address> clear
ip route <wsg_iproute_clear2_IPv4-address mask> <wsg_iproute_clear2_IPv4-address> ike
ip route <wsg_iproute_clear3_IPv4-address mask> <wsg_iproute_clear3_IPv4-address> ike
ip route <wsg_iproute_clear4_IPv4-address mask> <wsg_iproute_clear4_IPv4-address> ike
ip route <wsg_iproute_clear5_IPv4-address mask> <wsg_iproute_clear5_IPv4-address> ike
ip route <wsg_iproute_clear6_IPv4-address mask> <wsg_iproute_clear6_IPv4-address> ike
ipv6 route <wsg_iproute_ike1_IPv6-address/mask> <wsg_iproute_ike1_nexthop_IPv6-address> interface ike
ipv6 route <wsg_iproute_ike2_IPv6-address/mask> <wsg_iproute_ike2_nexthop_IPv6-address> interface ike
ipv6 route <wsg_iproute_clear1_IPv6-address/mask> <wsg_iproute_clear1_nexthop_IPv6-address> interface clear
ipv6 route <wsg_iproute_clear2_IPv6-address/mask> <wsg_iproute_clear2_nexthop_IPv6-address> interface ike
ipv6 route <wsg_iproute_clear3_IPv6-address/mask> <wsg_iproute_clear3_nexthop_IPv6-address> interface ike
ipv6 route <wsg_iproute_clear4_IPv6-address/mask> <wsg_iproute_clear4_nexthop_IPv6-address> interface ike
ipv6 route <wsg_iproute_clear5_IPv6-address/mask> <wsg_iproute_clear5_nexthop_IPv6-address> interface ike
ip sri <wsg_sri_IPv4-address> next-hop <wsg_sri_nexthop_IPv4-address>interface ike
ip rri next-hop <wsg_rri_nexthop_IPv4-address> interface clear
ip rri next-hop network-mode L3 <wsg_rri_network-mode_IPv4-address> nexthop <wsg_rri_network-mode_nexthop_IPv4-address> interface clear
#exit
context srp
no ip guarantee framed-route local-switching
service-redundancy-protocol
hello-interval 4
configuration-interval 60
dead-interval 12
checkpoint session duration non-ims-session 30
route-modifier threshold 10
priority 101
monitor hsrp interface GigabitEthernet0/2/0/18.<srp_monitor_hsrp_vlan_ID>
afi-type IPv4 hsrp-group <srp_hsrp-group_number>
peer-ip-address <srp_peer_IPv4-address>
bind address <srp_bind_IPv4-address>
#exit
interface icsr
ip address <srp_interface_icsr_IPv4-address_mask_per_CPU-VM>
#exit
subscriber default
exit
aaa group default
#exit
ip route <srp_iproute_IPv4-address_mask> <srp_iproute_IPv4-address> icsr
#exit
connectedapps
sess-userid cisco
sess-passwd encrypted password <encrypted_password>
sess-name <srp_hsrp-group_number>
sess-ip-address <connectapps_session_IPv4-address>
rri-mode BOTH
ha-chassis-mode inter
ha-network-mode L3
ca-certificate-name ca-cert-tls
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
    priority 5 source-netmask 16 destination-netmask 24
#exit
port ethernet 1/10
    no shutdown
    vlan <port_1/10_vlan_id>
        no shutdown
        bind interface ike wsg
    #exit
    #exit

#exit

port ethernet 1/11
    no shutdown
    vlan <port_1/11_vlan_id_wsg>
        no shutdown
        bind interface clear wsg
    #exit
    #exit
    vlan <port_1/11_vlan_id_srp>
        no shutdown
        bind interface icsr srp
    #exit
    #exit
end