SecGW Administration Guide, StarOS Release 21.18

First Published: 2020-02-28

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

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.

All printed copies and duplicate soft copies of this document are considered uncontrolled. See the current online version for the latest version.

Cisco has more than 200 offices worldwide. Addresses and phone numbers are listed on the Cisco website at www.cisco.com/go/offices.

CONTENTS

PREFACE

CHAPTER 1

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 DI System Administration Guide
- IPSec Reference

Conventions Used

The following tables describe the conventions used throughout this documentation.

Notice Type	Description
Information Note	Provides information about important features or instructions.
Caution	Alerts you of potential damage to a program, device, or system.
Warning	Alerts you of potential personal injury or fatality. May also alert you of potential electrical hazards.

Typeface Conventions	Description
Text represented as a `screen display`	This typeface represents displays that appear on your terminal screen, for example: `Login:`
Text represented as **commands**	This typeface represents commands that you enter, for example: **show ip access-list** This document always gives the full form of a command in lowercase letters. Commands are not case sensitive.
Text represented as a **command** *variable*	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.
Text represented as menu or sub-menu names	This typeface represents menus and sub-menus that you access within a software application, for example: Click the **File** menu, then click **New**

Command Syntax Conventions	Description
{ keyword or *variable* **}**	Required keyword options and variables are those components that are required to be entered as part of the command syntax. Required keyword options and variables are surrounded by grouped braces { }. For example: **`sctp-max-data-chunks { limit`** *`max_chunks`* **`| mtu-limit }`** If a keyword or variable is not enclosed in braces or brackets, it is mandatory. For example: **`snmp trap link-status`**
[keyword or *variable* **]**	Optional keywords or variables, or those that a user may or may not choose to use, are surrounded by brackets.

Command Syntax Conventions	Description
|	Some commands support multiple options. These are documented within braces or brackets by separating each option with a vertical bar. These options can be used in conjunction with required or optional keywords or variables. For example: **action activate-flow-detection { intitiation | termination }** or **ip address [count** *number_of_packets* **| size** *number_of_bytes* **]**

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 (Cisco ASR 5500 Series) documentation:

http://www.cisco.com/en/US/products/ps11072/tsd_products_support_series_home.html

Use the following URL to access the ASR 9000 documentation:

http://www.cisco.com/en/US/products/ps9853/tsd_products_support_series_home.html

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 covered in this chapter:

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.

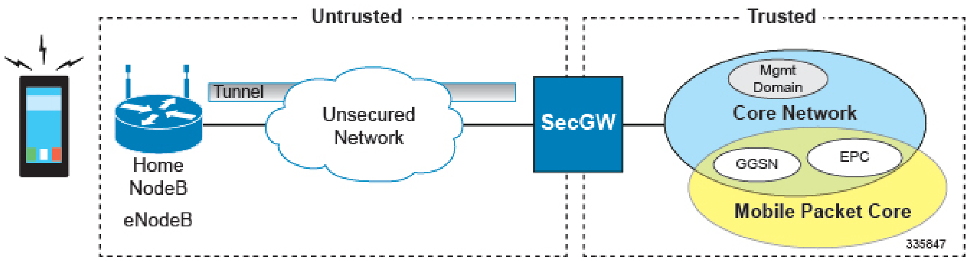
IPSec is an open standards set that provides confidentiality, integrity, and authentication for data between IP layer peers. The SecGW uses IPSec-protected tunnels to connect outside endpoints. SecGW implements the parts of IKE/IPSec required for its role in mobile networks.

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

Figure 1: SecGW Implementation



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.

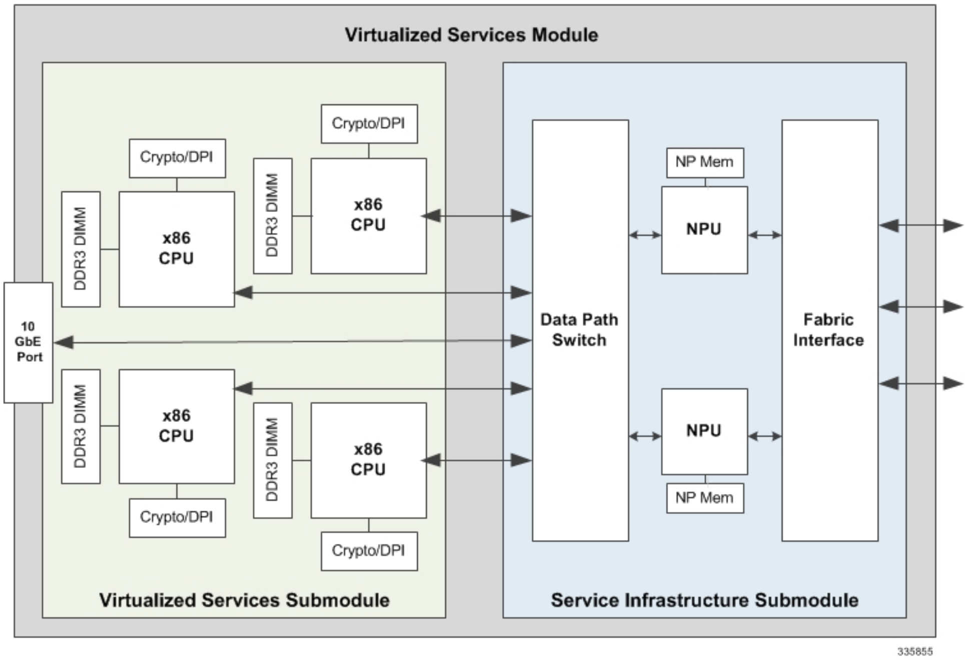
Also SecGW Suppors VPC-DI platform.

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

Figure 2: VSM High Level Block Diagram



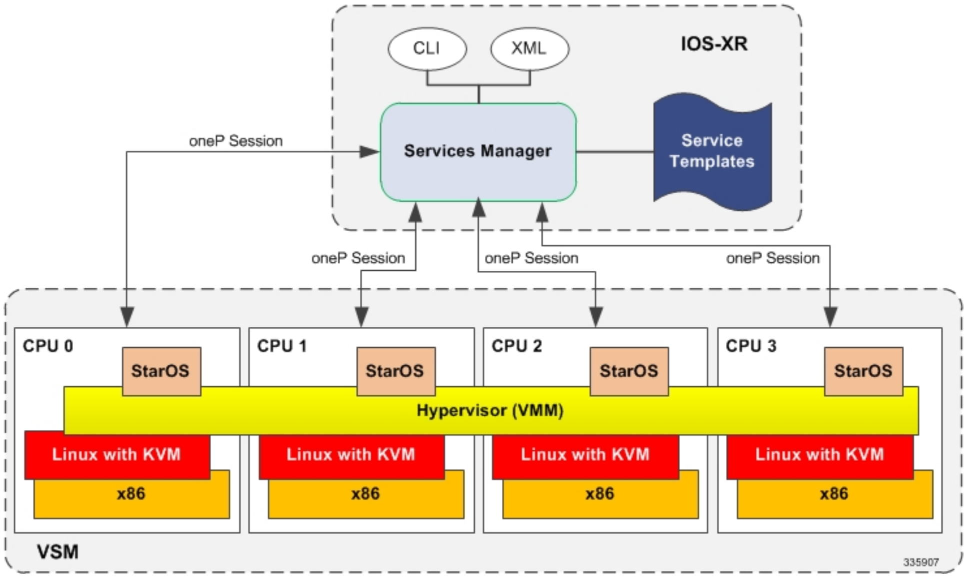
The ASR 9000 services architecture encompasses how the platform interfaces with the services independent of where the service is actually instantiated. It provides a common control plane, management plane and data plane infrastructure such that a consistent end user experience is provided whether the 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



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

CPU	Available Cores	Crypto Device	PCI Port ID	VM	vCPUs
0	16 (2–9, 42–49)	04:00.0	00.0.0	VM1	16
			00.0.1		
1	18 (11–19, 51–59)	45.00.0	42.0.0		
			42.0.1	VM2	16
			48.0.0		
			48.0.1		
2	20 (20-29, 60-69)	85:00.0	82:0.0	VM3	20
			82:0.1		
			88:0.0		
			88:0.1	—	—
3	20 (30-39, 70-79)	C5:00.0	C2:0.0	VM4	20
			C2:0.1		
			C8:0.0		
			C8:0.1	—	—

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

PCI Port ID	CPU	ASR 9000 TenG	VPC Slot/Port	VM	Application IF
00:0.0	0	TenGx/y/z/0	1/10	VM1	Uplink
00:0.1		TenGx/y/z/1	1/11		Downlink
42:0.0	1	TenGx/y/z/2	1/1		Management
42.0.1		TenGx/y/z/3	1/10	VM2	Uplink
48.0.0		TenGx/y/z/4	1/11		Downlink
48.0.1		TenGx/y/z/5	1/1		Management

PCI Port ID	CPU	ASR 9000 TenG	VPC Slot/Port	VM	Application IF
82:0.0	2	TenGx/y/z/6	1/10	VM3	Uplink
82:0.1		TenGx/y/z/7	1/11		Downlink
88:0.0		TenGx/y/z/8	1/1		Management
88:0.1		—	—	—	Unused
C2:0.0	3	TenGx/y/z/9	1/10	VM4	Uplink
C2:0.1		TenGx/y/z/10	1/11		Downlink
C8:0.0		TenGx/y/z/11	1/1		Management
C8:0.1		—	—	—	Unused

- 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 20.0.x is the last fully qualified build for ASR9k SecGW.

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, HMAC-SHA2 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 for a new WSG service in the existing SecGW instance.

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
- Support to provide DNS server address to the Peer

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, on page 8

HA functions are triggered for the following events:

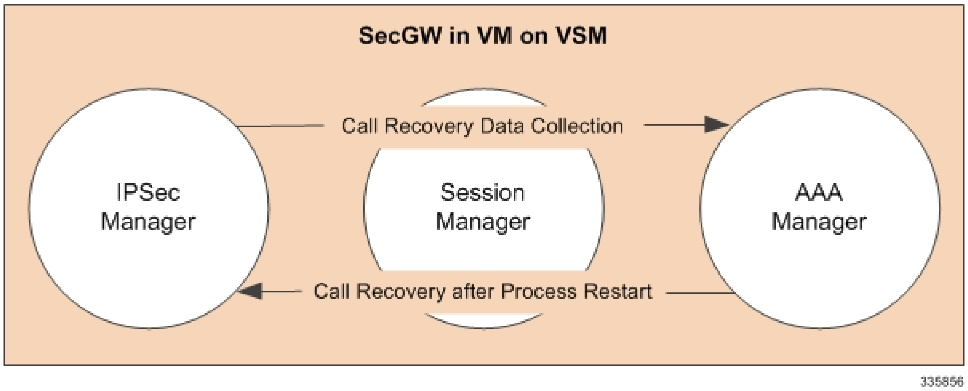
- Route Processor (RP) failure
- Virtual Machine (VM) failure
- VSM failure
- Link failure

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.

Figure 4: Process Recovery Diagram


SecGW in VM on VSM
IPSec Manager
Call Recovery Data Collection
Session Manager
AAA Manager
Call Recovery after Process Restart
335856

VSM-to-VSM ICSR 1:1 Redundancy

In this redundancy scenario, Interchassis Session Recovery ICSR utilizes the Service Redundancy Protocol (SRP) implemented between VMs in a VSM 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 VMs in a VSM 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 involves configuration of both SRP and ConnectedApps (CA) for RRI to work.

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

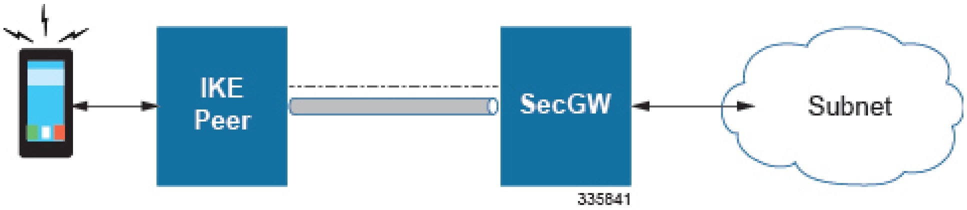
SecGW supports the following network deployment scenarios:

- Remote Access Tunnels, on page 9
- Site-to-Site Tunnels, on page 9

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.

Figure 5: RAS Tunnel



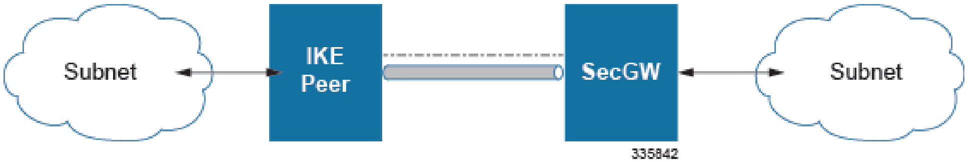
Site-to-Site Tunnels

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.

Figure 6: S2S Tunnel



Packet Flow

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

Figure 7: SecGW Packet Flow – RAS

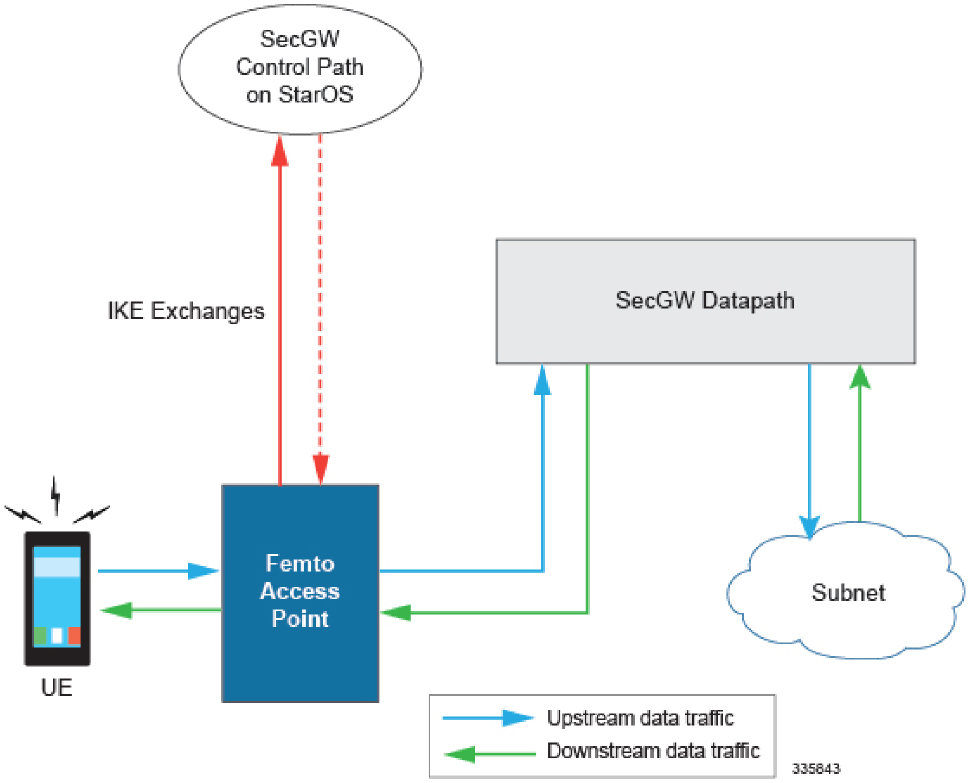
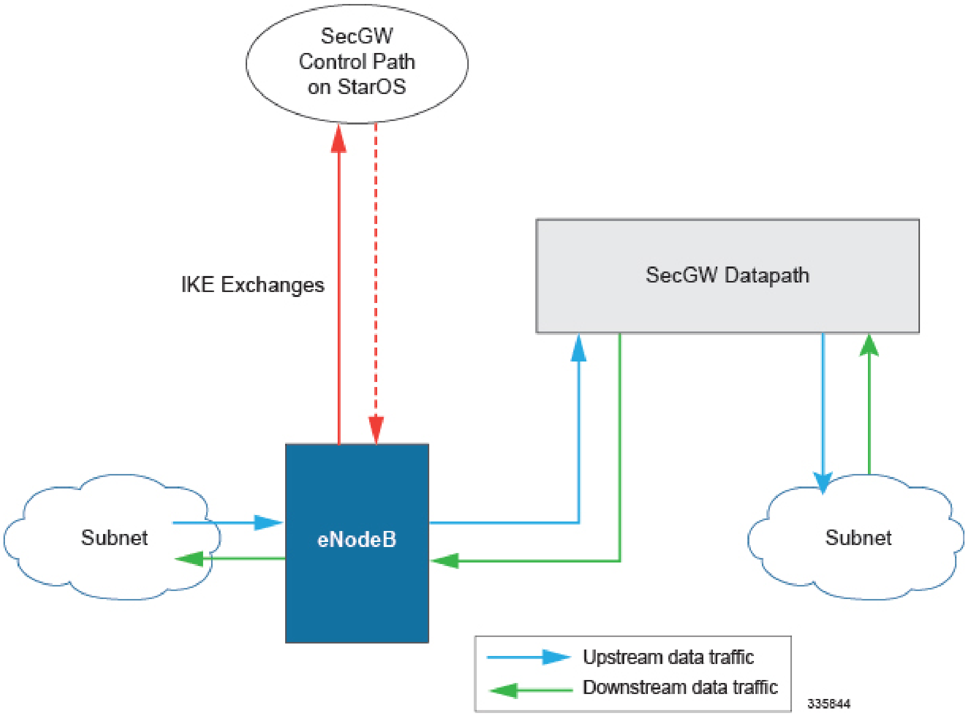


Figure 8: SecGW Packet Flow – S2S Scenario



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 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 4210 – Internet X.509 Public Key Infrastructure Certificate Management Protocol (CMP)
- 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 17
- DH Group 18
- 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.

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, on page 14
- Create Access Control Lists. See Access Control Lists, on page 16
- Enable and configure one or more WSG services. See WSG Service Configuration, on page 17
- Configure required IPSec features. See IPSec Configuration, on page 25

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: sha1
            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:
              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. Only 16 WSG services can be configured per context in StarOS instance, and there can be multiple contexts per StarOS instance.

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

```
config
    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.

```
bind 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.

For the site-to-site scenario, the WSG service should be associated with **access-group** for which source and destination can be a subnet. The ip address alloc-method/pool configurations are for RAS mode.

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
```

Important If the **access-group** is modified under the context then the same need to be reconfigured under WSG service for the changes to get affected. This procedure involves unbind and bind as well.

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, on page 19.

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*.

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 d1v4
            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 p1v4 35.35.34.0 255.255.255.0 public 0
```

Multi Child SA Support

A child SA is an Encapsulating Security Payload (ESP) or Authentication Header (AH) Security Association (SA) carrying the secure user traffic. An SA is a "simplex connection" to achieve bidirectional secure traffic. A pair of SAs are required (RFC 5996) to meet this common requirement. The IKE explicitly creates SA pairs, an SA pair is referred to as a "Child SA" and one child SA is a pair of IPsec SAs in each direction.

SecGW supports Multiple Child SAs with the following exceptions:

- MCSA is not supported with RAS tunnels.
- Deletion of single Child SA of the MCSA tunnel is not supported.
- SecGW allows same traffic selector IP range for MCSA's. However, it is not recommended as it could lead to unexpected results as explained below.

  Do NOT configure traffic selector range as shown below:

  Range from 150.0.0.0 to 150.0.255.255 (associated with Child SA1 of the MCSA tunnel)

  Range from 150.0.255.0 to 150.0.255.255 (associated with Child SA2 of the MCSA tunnel)

  In the above example the second traffic selector is the sub-set of the first traffic selector IP address range, SecGW does not validate such an overlap while creating Child SA for every new SPI index provided by peer initator (eNodeB). As a result of this even if a down link packet is meant for the second traffic selector, it might still pass though the first traffic selector. It is NOT recommended to configure overlapping IP addresses even though it is allowed by SecGW.

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 under the context but only one ACL list is allowed under WSG service.
- 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 attmpts: 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                  Admin disconnect:
            0
    Idle timeout:                              0                  Absolute timeout:
                 0
    Long duration timeout:            0                  Session setup timeout:
   0
    No resource:                                0                  Auth failure:
                      0
    Flow add failure:                      0                  Invalid dest-context:
         0
    Source address violation:      0                  Duplicate Request:
    0
    MAC validation failure:          0                  Addr assign failure:
    0
    Miscellaneous reasons:            0

Data Stats:
    Total Bytes Sent:                      0                  Total Packets Sent:
           0
    Total Bytes Rcvd:                      0                  Total Packets Rcvd:
           0
    Total Pkts Violations:            0

EAP Server Stats:
    Total Received:                          0
    Success Received:                      0                  Challenge Received:
           0
    Failures 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-duplicate-request
- wsg-total-disconnected-mac-validation-failure
- wsg-total-disconnected-addr-assign-failure
- 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-discarded
- wsg-total-eap-server-discarded
- 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.

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 **connectedaspps** 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 page 29 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:

```
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:

```
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 : db1jvk4
    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

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 and RAS; though the requirement is mainly for S2S. RRI route transaction is initiated is 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.

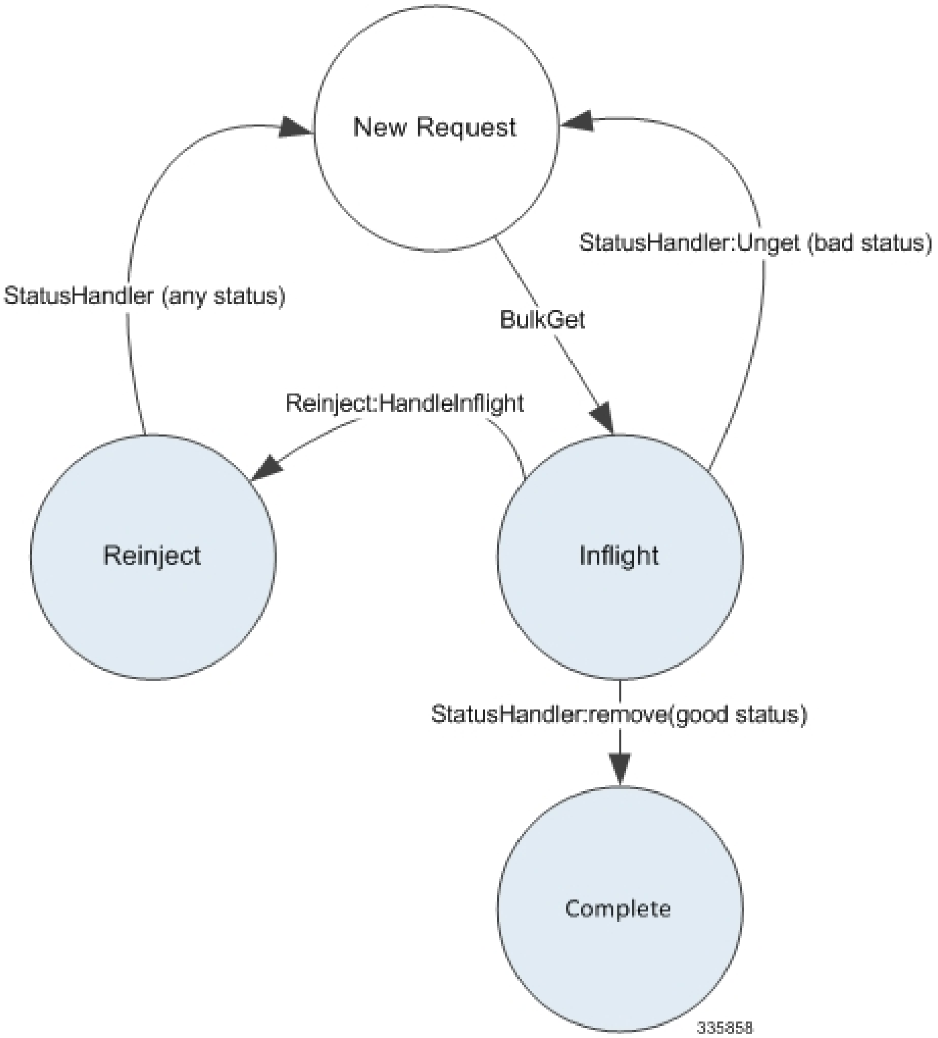
How It Works

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.

Figure 9: RRI Requests – State Diagram


New Request
StatusHandler (any status)
StatusHandler:Unget (bad status)
BulkGet
Reinject:HandleInflight
Reinject
Inflight
StatusHandler:remove(good status)
Complete
335858

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.
- 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 3: Recommended Mapping of Interchassis StarOS VMs

Active VSM	Standby VSM
VM1	VM1
VM2	VM2
VM3	VM3
VM4	VM4

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:

- Use this command for standalone and Interchassis L2-ICSR.
- *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 the SecGW clear interface physical address.
- *interface_name* specifies the egress interface.It should be unique and map the *vrf_name*, under the same context.
- The *vrf_name* is the VRF of clear interface in ASR 9000/RSP (external interface as well as the VSM interface) wherein the clear traffic is forwarded based on the RRI route.

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:

- Configuring Border Gateway Protocol (BGP) is required when this CLI is used, to support Interchassis L3-ICSR and Intrachassis ICSR. This CLI will add only 1st-leg route. The 2nd-leg routes are added using other routing protocols such as BGP, or OSPF, etc.
- This command is mandatory in the following scenarios:
  - L2 Intrachassis HA (where loopback IP is configured)
  - L3 Interchassis HA (where loopback 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 the SecGW clear interface physical address.
- *interface_name* specifies the egress interface. It should be unique and map the *vrf_name*, under the same context.
- The *vrf_name* is the VRF of clear interface in ASR 9000/RSP (external interface as well as the VSM interface) wherein the clear traffic is forwarded based on the RRI route.

ip/ipv6 sri-route Command

Important The **ip/ipv6 sri-route** CLI is deprecated, and not supported in 19.0 and later releases.

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.
- *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

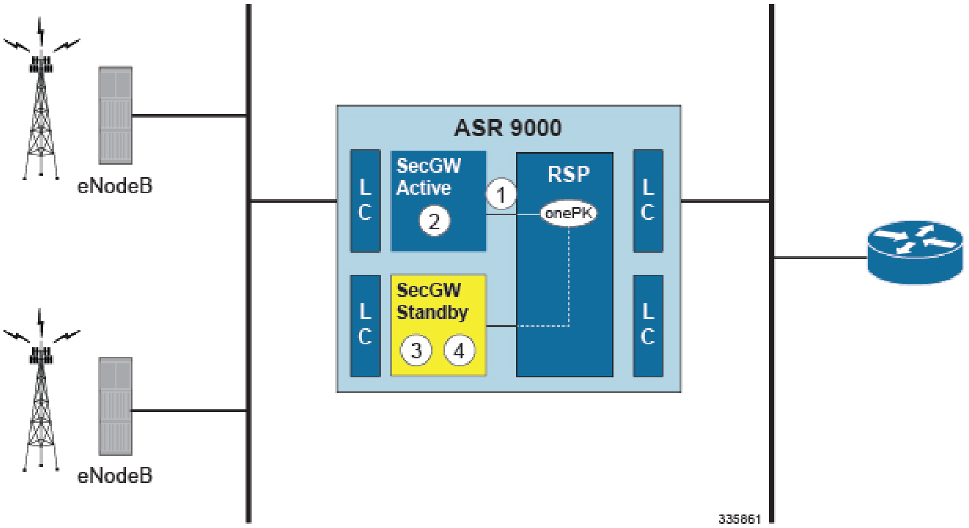
ConnectedApps (oneP) Configuration

```
config
     context local
          interface CA
               ip address 192.168.122.10 255.255.255.0
               exit
               subscriber default
               exit
               aaa group default
               exit
               no gtpp trigger 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

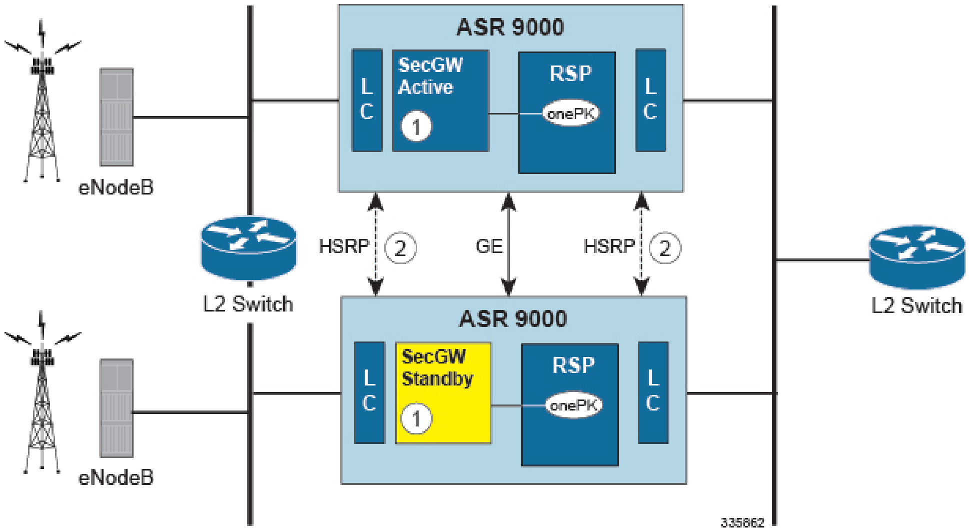


Item	Description
1	Common oneP session is used only by the active SecGW.
2	Only the active SecGW injects routes on tunnel setup.
3	Upon failover the currently active SecGW gives up its oneP session and the newly active SecGW takes over the session.
4	Upon failover the newly active SecGW injects routes for new tunnels.

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

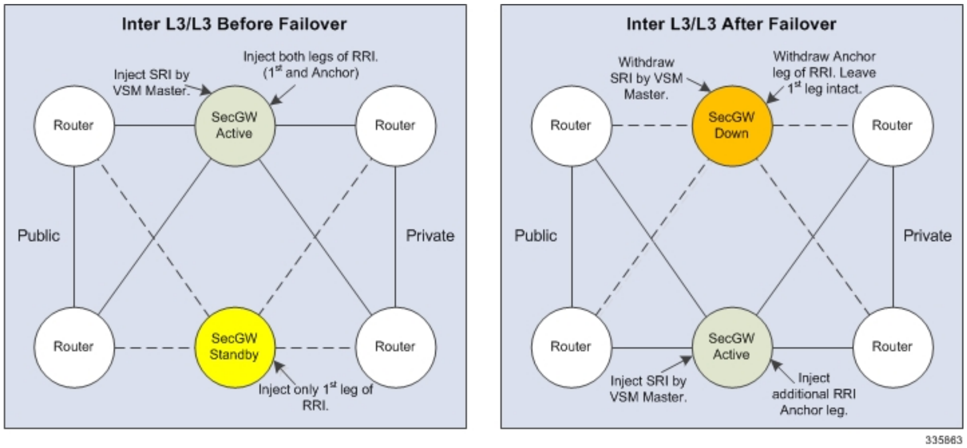


Item	Description
1	Both the active and standby SecGWs insert routes into local chassis only.
2	ICSR is configured to track RSP HSRP groups. HSRP also tracks SecGW using an SLA (Service Level Agreement).

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


Inter L3/L3 Before Failover
Inject SRI by VSM Master.
Inject both legs of RRI. (1st and Anchor)
Router
SecGW Active
Router
Public
Private
Router
SecGW Standby
Router
Inject only 1st leg of RRI.
Inter L3/L3 After Failover
Withdraw SRI by VSM Master.
Withdraw Anchor leg of RRI. Leave 1st leg intact.
Router
SecGW Down
Router
Public
Private
Router
SecGW Active
Router
Inject SRI by VSM Master.
Inject additional RRI Anchor leg.
335863

HSRP

Overview

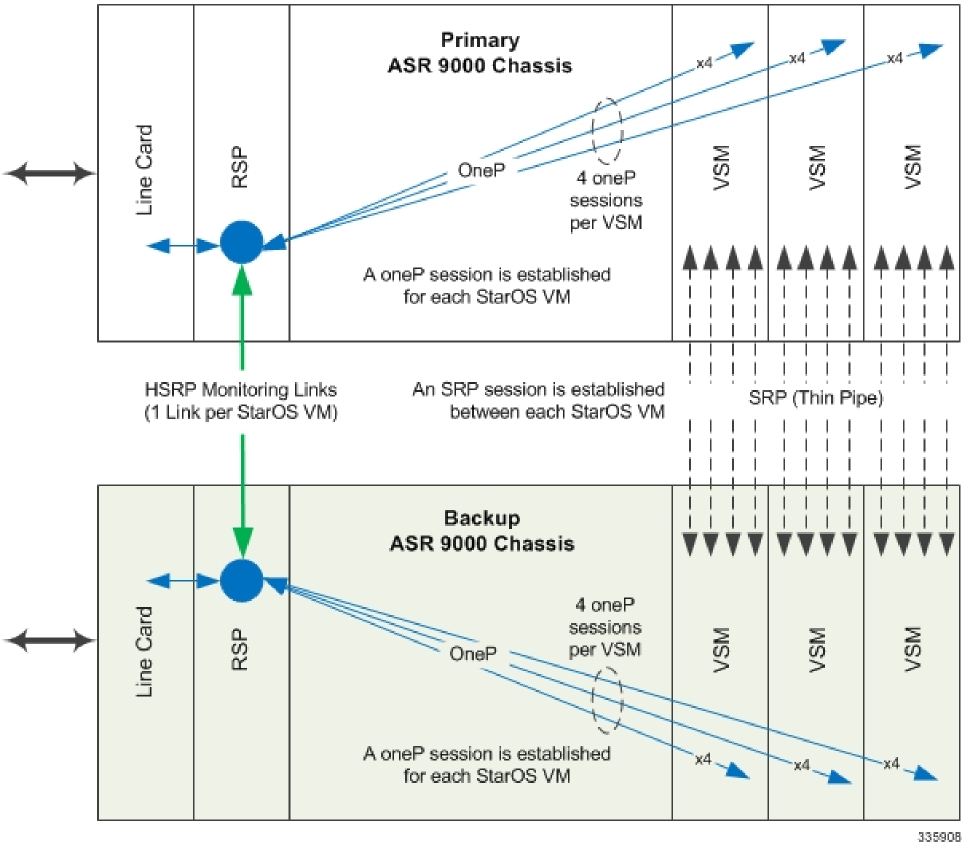
Hot Standby Router Protocol (HSRP) is a Cisco proprietary redundancy protocol for establishing a fault-tolerant default gateway (RFC 2281). The protocol establishes a framework between network routers in order to achieve default gateway failover if the primary gateway becomes inaccessible.

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


Primary
ASR 9000 Chassis
Line Card
RSP
OneP
4 oneP sessions per VSM
x4
x4
x4
VSM
VSM
VSM
A oneP session is established for each StarOS VM
HSRP Monitoring Links (1 Link per StarOS VM)
An SRP session is established between each StarOS VM
SRP (Thin Pipe)
Backup
ASR 9000 Chassis
Line Card
RSP
OneP
4 oneP sessions per VSM
VSM
VSM
VSM
A oneP session is established for each StarOS VM
x4
x4
x4
335908

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:

```
config
 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.

```
configure
     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
               bind address 88.88.88.37
               exit
```

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

```
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.

WSG Context (StarOS)

```
config
  context wsg
    ip access-list one
      permit ip 66.66.0.0 0.0.255.255 45.45.0.0 0.0.255.255 protocol 255
      exit
    ipsec transform-set tselsa-foo
    exit
    ikev2-ikesa transform-set ikesa-foo
    exit
    crypto template foo ikev2-dynamic
      authentication local pre-shared-key key foo
      authentication remote pre-shared-key key foo
      ikev2-ikesa transform-set list ikesa-foo
      identity local id-type ip-addr id 33.33.33.3
      peer network 55.55.33.30 mask 255.255.255.255
      natt

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

    interface ike
      ip address 33.33.33.33 255.255.255.0
    exit

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

Clear Traffic Interface – Primary

```
interface clear
ip address 77.77.77.33 255.255.255.0

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

Clear Traffic Interface – Backup

```
interface clear
ip address 77.77.77.34 255.255.255.0

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

SRP Context (StarOS)

SRP – Primary Chassis

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

SRP – Backup Chassis

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

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

HSRP Configuration (IOS-XR)

Primary Chassis

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

Backup Chassis

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

Port Configuration (StarOS)

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

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

oneP (Connected Apps) Communication

oneP Configuration (IOS-XR)

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

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

Session Establishment ASR 9000 SecGW

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

1. Configure crypto ca trustpoint onep-tp configurations in ASR9000, refer ASR 9000 RSP Configuration (IOS-XR), on page 49

2. Configure ' onep' configurations in ASR9000, refer ASR 9000 RSP Configuration (IOS-XR), on page 49

3. Copy and Paste the contents of the generated CA certificate after executing the CLI ' crypto ca authenticate onep-tp' in ASR 9000

4. Configure the XR Server's 'Certificate request' with the CLI ' crypto ca enroll onep-tp'. Below is the snippet collected during certificate request generation,

```
Password: (cisco)

Re-enter Password:  (cisco)

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

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

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

% The serial number in the certificate will be: f15db8e1

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

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

    Fingerprint:  44383334 43413532 30324435 35393534

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

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

5. Now collect the generated 'certificate request' and get it signed by the Certificate Authority (CA)

6. Import the signed certificate in ASR90000 with the CLI ' crypto ca import onep-tp certificate' (copy paste the signed certificate here)

7. Can check the certificate status in ASR90000 with the show CLI ' show crypto ca certificates'

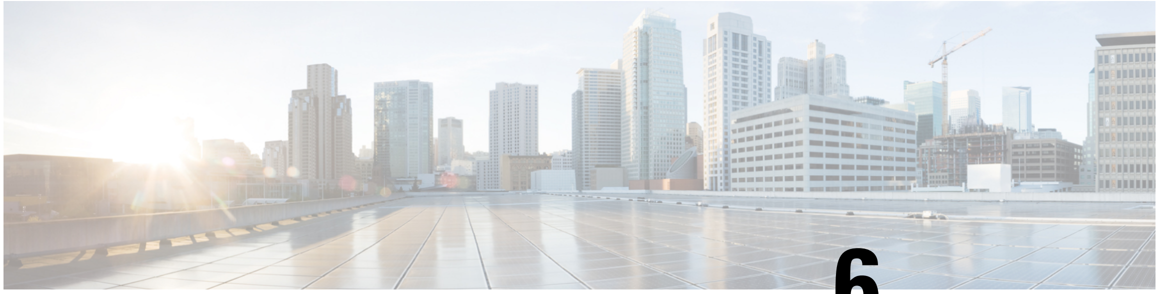
8. Now load the ca-cert in secgw as well and map the 'ca-cert' name under 'connectedapps' configuration, refer Configuring a Client CA Session, on page 28

9. Configure 'Activate' under secgw 'connectedapps' to initiate the connectedapps session establishment request.

10. Enable debug for ' connectedapps' in secgw to monitor the process (optional)

CA Client Session (StarOS)

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



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).

ASR 9000 RSP Configuration (IOS-XR)

Notes:

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

```
<snip>

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

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

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

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

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

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

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

interface MgmtEth0/RSP0/CPU0/1
 shutdown

interface GigabitEthernet0/1/0/0
 shutdown

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

interface GigabitEthernet0/1/0/4
 shutdown

...

interface GigabitEthernet0/1/0/19
 shutdown

interface GigabitEthernet0/1/0/6
 shutdown

interface GigabitEthernet0/1/1/0
 shutdown

...

interface GigabitEthernet0/1/1/19
```

```
 shutdown

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

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


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


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

interface TenGigE0/2/1/4
 shutdown

...

interface TenGigE0/2/1/11
 shutdown

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

interface TenGigE0/4/1/1
 shutdown

interface TenGigE0/4/1/1
 shutdown


interface TenGigE0/4/1/2
 shutdown


interface TenGigE0/4/1/3
 shutdown

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


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

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

```
...

interface TenGigE0/4/1/11
 shutdown

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

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

interface preconfigure TenGigE0/0/0/0
 shutdown

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

interface preconfigure TenGigE0/2/0/0
 shutdown

...

interface preconfigure TenGigE0/2/0/3
 shutdown

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


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

   interface TenGigE0/4/1/4

   routed interface BVI1

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

   interface TenGigE0/4/1/5
   routed interface BVI2


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



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



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


 schedule operation 200
  start-time now
  life forever

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

 delay up 1
 delay down

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

```
delay up 1
delay down
```

WSG Configuration VM-1 (StarOS)

Notes:

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

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

```
config
   context local
      interface CA
         ip address 192.168.122.15 255.255.255.0
      exit
      subscriber default
      exit
      administrator cisco encrypted password <encrypted_password>
      aaa group default
      exit
   exit
   port ethernet 1/1
      no shutdown
      bind interface CA local
   exit
   context wsg
      ip access-list one
         permit ip 66.66.0.0 0.0.255.255 45.45.0.0 0.0.255.255 protocol
255
      exit
      ipsec transform-set tselsa-foo
      exit
      ikev2-ikesa transform-set ikesa-foo
      exit
      crypto template foo ikev2-dynamic
         authentication local pre-shared-key encrypted key <encrypted_key>
         authentication remote pre-shared-key encrypted key <encrypted_key>
         ikev2-ikesa transform-set list ikesa-foo
         payload foo-sa0 match childsa match ipv4
            ip-address-alloc dynamic
            ipsec transform-set list tselsa-foo
         exit
         identity local id-type ip-addr id 32.32.32.30
      exit

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

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

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

WSG Configuration VM-2 (StarOS)

Notes:

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

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

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

```
config
   context local
      interface CA
         ip address 192.168.122.15 255.255.255.0
      exit
      subscriber default
      exit
      administrator cisco encrypted password <encrypted_password>
      aaa group default
      exit
   exit
   port ethernet 1/1
      no shutdown
      bind interface CA local
   exit
   context wsg
      ip access-list one
         permit ip 66.66.0.0 0.0.255.255 45.45.0.0 0.0.255.255 protocol
255
      exit
      ipsec transform-set tselsa-foo
      exit
      ikev2-ikesa transform-set ikesa-foo
      exit
      crypto template foo ikev2-dynamic
         authentication local pre-shared-key encrypted key <encrypted_key>
         authentication remote pre-shared-key encrypted key <encrypted_key>
         ikev2-ikesa transform-set list ikesa-foo
         payload foo-sa0 match childsa match ipv4
            ip-address-alloc dynamic
            ipsec transform-set list tselsa-foo
         exit
         identity local id-type ip-addr id 32.32.32.30
      exit

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

      ip rri-route network-mode L2 78.78.78.50 next-hop 78.78.78.34
interface clear
      ip rri-route network-mode L2 78.78.78.50 next-hop 78.78.78.34
interface clear
   exit
   context srp
      service-redundancy-protocol
         chassis-mode primary
         hello-interval 3
         configuration interval 60
         dead interval 15
         checkpoint session duration non-ims-session 30
         route-modifier threshold 10
         priority 10
         monitor hsrp interface GigabitEthernet0/0/0/5 afi-type IPv4
hsrp-group 3
         peer-ip-address 88.88.88.33
         bind address 86.86.86.33
      exit
      interface icsr
         ip address 86.86.86.33 255.255.255.0
      exit
      subscriber default
      exit
      aaa group default
      exit
      ip route 88.88.88.0 255.255.255.0 86.86.86.23 icsr
   exit
   connectedapps
      sess-userid cisco
      sess-passwd encrypted password <encrypted_password>
      sess-name intraCh
      sess-ip-address 192.168.120.1
      rri-mode S2S
      ha-chassis-mode intra
      ha-network-mode L2
      ca-certificate-name cert_name
      activate
   exit
   wsg-lookup
      priority 1 source-netmask 28 destination-netmask 28
      priority 2 source-netmask 32 destination-netmask 32
      priority 3 source-netmask 16 destination-netmask 16
      priority 4 source-netmask 24 destination-netmask 24
   exit
   port ethernet 1/10
      no shutdown
      bind interface ike wsg
   exit
   port ethernet 1/11
      no shutdown
      bind interface clear wsg
      vlan 12
    vlan 12
      description "ICSR"
      no shutdown
      bind interface icsr srp
    #exit
  #exit
end
```

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.

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 4: Recommended Mapping of Interchassis StarOS VMs

Active VSM	Standby VSM
VM1 – SecGW1	VM1 – SecGW1
VM2 – SecGW2	VM2 – SecGW2
VM3 – SecGW3	VM3 – SecGW3
VM4 – SecGW4	VM4 – SecGW4

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
 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
 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_SRP_IPv6-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_backupy_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
  2038::38/128 2044::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 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 GigabitEthernet0/0/0/19.1881
  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 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

Variable	Primary ASR 9000	Backup ASR 9000
<interfsace_LOCAL1_IPv4-address>	100.100.100.1 255.255.255.0	192.168.122.15 255.255.255.0
<iproute_:LOCAL1_IPv4-address_mask>	0.0.0.0 0.0.0.0 100.100.100.10	0.0.0.0 0.0.0.0 192.168.122.2
<wsg_acl1_permit_IPv4-address_mask>	65.65.0.0 0.0.255.255 45.45.0.0 0.0.255.255	65.65.0.0 0.0.255.255 45.45.0.0 0.0.255.255
<wsg_acl1_permit_IPv6-address/mask>	2065:: ::ffff:ffff:ffff:ffff 2045:: ::ffff:ffff:ffff:ffff	2065:: ::ffff:ffff:ffff:ffff 2045:: ::ffff:ffff:ffff:ffff
<wsg_pool1_IPv4-address>	45.45.0.1 45.45.58.254	45.45.0.1 45.45.58.254
<wsg_pool1_IPv6-address/mask>	2045::/56	2045::/56
<crypto_foo_local_IPv4-addrress>	35.35.35.35	35.35.35.35
<crypto_foo-1_local_IPv6-addrress>	2035::35	2035::35
<wsg_interface_clear_IPv4-address_mask>	51.51.51.11 255.255.255.0	61.61.61.11 255.255.255.0
<wsg_interface_clear_IPv6-address/mask>	2051::11/64	2061::11/64

Variable	Primary ASR 9000	Backup ASR 9000
<wsg_interface_ike_IPv4-address_mask>	31.31.31.11 255.255.255.0	41.41.41.11 255.255.255.0
<wsg_interface_ike_IPv6-address/mask>	2031::11/64	2041::11/64
<wsg_interface_ike-loop_IPv4-address_mask>	35.35.35.35 255.255.255.255	35.35.35.35 255.255.255.255
<wsg_interface_ike-loop_IPv6-address/mask>	2035::35/128	2035::35/128
<wsg_interface_ike-loop1_IPv4-address_mask>	31.31.31.100 255.255.255.255	41.41.41.100 255.255.255.255
<wsg-service_bind_IPv4-address>	35.35.35.35	35.35.35.35
<wsg-service_bind_IPv6-address>	2035::35	2035::35
<wsg_iproute_clear_IPv4-address_mask>	65.65.0.0 255.255.0.0	65.65.0.0 255.255.0.0
<wsg_iproute_clear_IPv4-address>	51.51.51.10	61.61.61.10
<wsg_iproute_ike1_IPv4-address_mask>	187.0.1.0 255.255.255.0	187.0.1.0 255.255.255.0
<wsg_iproute_ike1_IPv4-address>	31.31.31.10	41.41.41.10
<wsg_iproute_ike2_IPv4-address_mask>	92.0.0.0 255.0.0.0	92.0.0.0 255.0.0.0
<wsg_iproute_ike2_IPv4-address>	31.31.31.10	41.41.41.10
<wsg_iproute_ike3_IPv4-address_mask>	188.0.1.0 255.255.255.0	188.0.1.0 255.255.255.0
<wsg_iproute_ike3_IPv4-address>	31.31.31.10	41.41.41.10
<wsg_iproute_clear_IPv6-address/mask>	2065::/64	2065::/64
<wsg_iproute_clear_nexthop_IPv6-address>	2051::10	2061::10
<wsg_iproute_ike1_IPv6-address/mask>	2092::/64	2092::/64
<wsg_iproute_ike1_nexthop_IPv6-address>	2031::10	2041::10
<wsg_iproute_ike2_IPv6-address/mask>	1871::/64	1871::/64
<wsg_iproute_ike2_nexthop_IPv6-address>	2031::10	2041::10
<wsg_iproute_ike2_IPv6-address/mask>	1881::/64	1881::/64
<wsg_iproute_ike2_nexthop_IPv6-address>	2031::10	2041::10
<wsg_rri_nexthop_IPv4-address>	51.51.51.11	61.61.61.11
<wsg_rri_nexthop_IPv6-address>	—	—
<srp_monitor_hsrp_vlan_id>	1871	1871
<srp_hsrp-group_number>	4	4
<srp_peer_IPv4-address>	81.81.81.11	71.71.71.11
<srp_bind_IPv4-address>	71.71.71.11	81.81.81.11
<srp_interface_icsr_IPv4-address_mask>	71.71.71.11 255.255.255.0	81.81.81.11 255.255.255.0
<srp_iproute_icsr_IPv4-address_mask>	81.81.81.0 255.255.255.0	71.71.71.0 255.255.255.0
<srp_iproute_icsr_IPv4-address>	71.71.71.10	81.81.81.10

Variable	Primary ASR 9000	Backup ASR 9000
<connectedapps_session_IPv4-address>	100.100.100.10	192.168.122.2
<port_1/10_vlan_id>	—	—
<port_1/11_vlan_id_srp>	1259	1871
<port_1/11_vlan_id_wsg>	1881	1881

Table 6: StarOS IP Address Mapping - SecGW2

Variable	Primary ASR 9000	Backup ASR 9000
<interfsace_LOCAL1_IPv4-address>	100.100.100.2 255.255.255.0	192.168.122.16 255.255.255.0
<iproute_LOCAL1_IPv4-address_mask>	0.0.0.0 0.0.0.0 100.100.100.10	0.0.0.0 0.0.0.0 192.168.122.2
<wsg_acl1_permit_IPv4-address_mask>	66.66.0.0 0.0.255.255 46.46.0.0 0.0.255.255	66.66.0.0 0.0.255.255 46.46.0.0 0.0.255.255
<wsg_acl1_permit_IPv6-address/mask>	2066:: ::ffff:ffff:ffff:ffff 2046:: ::ffff:ffff:ffff:ffff	2066:: ::ffff:ffff:ffff:ffff 2046:: ::ffff:ffff:ffff:ffff
<wsg_pool1_IPv4-address>	46.46.0.1 46.46.58.254	46.46.0.1 46.46.58.254
<wsg_pool1_IPv6-address/mask>	2046::/56	2046::/56
<crypto_foo_local_IPv4-addrress>	36.36.36.36	36.36.36.36
<crypto_foo-1_local_IPv6-addrress>	2036::36	2036::36
<wsg_interface_clear_IPv4-address_mask>	52.52.52.11 255.255.255.0	62.62.62.11 255.255.255.0
<wsg_interface_clear_IPv6-address/mask>	2052::11/64	2062::11/64
<wsg_interface_ike_IPv4-address_mask>	52.52.52.11 255.255.255.0	42.42.42.12 255.255.255.0
<wsg_interface_ike_IPv6-address/mask>	2032::11/64	2042::11/64
<wsg_interface_ike-loop_IPv4-address_mask>	36.36.36.36 255.255.255.255	36.36.36.36 255.255.255.255
<wsg_interface_ike-loop_IPv6-address/mask>	2036::36/128	2036::36/128
<wsg_interface_ike-loop1_IPv4-address_mask>	32.32.32.100 255.255.255.255	42.42.42.100 255.255.255.255
<wsg-service_bind_IPv4-address>	36.36.36.36	36.36.36.36
<wsg-service_bind_IPv6-address>	2036::36	2036::36
<wsg_iproute_clear_IPv4-address_mask>	66.66.0.0 255.255.0.0	66.66.0.0 255.255.0.0
<wsg_iproute_clear_IPv4-address>	52.52.52.10	62.62.62.10
<wsg_iproute_ike1_IPv4-address_mask>	187.0.2.0 255.255.255.0	187.0.2.0 255.255.255.0
<wsg_iproute_ike1_IPv4-address>	32.32.32.10	42.42.42.10
<wsg_iproute_ike2_IPv4-address_mask>	93.0.0.0 255.0.0.0	93.0.0.0 255.0.0.0

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

Table 7: StarOS IP Address Mapping - SecGW3

Variable	Primary ASR 9000	Backup ASR 9000
<interfsace_LOCAL1_IPv4-address>	100.100.100.3 255.255.255.0	192.168.122.17 255.255.255.0
<iproute_LOCAL1_IPv4-address_mask>	0.0.0.0 0.0.0.0 100.100.100.10	0.0.0.0 0.0.0.0 192.168.122.2
<wsg_acl1_permit_IPv4-address_mask>	67.67.0.0 0.0.255.255 47.47.0.0 0.0.255.255	67.67.0.0 0.0.255.255 47.47.0.0 0.0.255.255

Variable	Primary ASR 9000	Backup ASR 9000
<wsg_acl1_permit_IPv6-address/mask>	2067:: ::ffff:ffff:ffff:ffff 2047:: ::ffff:ffff:ffff:ffff	2067:: ::ffff:ffff:ffff:ffff 2047:: ::ffff:ffff:ffff:ffff
<wsg_pool1_IPv4-address>	47.47.0.1 47.47.58.254	47.47.0.1 47.47.58.254
<wsg_pool1_IPv6-address/mask>	2047::/56	2047::/56
<crypto_foo_local_IPv4-addrress>	37.37.37.37	37.37.37.37
<crypto_foo-1_local_IPv6-addrress>	2037::37	2037::37
<wsg_interface_clear_IPv4-address_mask>	53.53.53.11 255.255.255.0	63.63.63.11 255.255.255.0
<wsg_interface_clear_IPv6-address/mask>	2053::11/64	2063::11/64
<wsg_interface_ike_IPv4-address_mask>	33.33.33.11 255.255.255.0	43.43.43.12 255.255.255.0
<wsg_interface_ike_IPv6-address/mask>	2033::11/64	2043::11/64
<wsg_interface_ike-loop_IPv4-address_mask>	37.37.37.37 255.255.255.255	37.37.37.37 255.255.255.255
<wsg_interface_ike-loop_IPv6-address/mask>	2037::37/128	2037::37/128
<wsg_interface_ike-loop1_IPv4-address_mask>	33.33.33.100 255.255.255.255	43.43.43.100 255.255.255.255
<wsg-service_bind_IPv4-address>	37.37.37.37	37.37.37.37
<wsg-service_bind_IPv6-address>	2037::37	2037::37
<wsg_iproute_clear_IPv4-address_mask>	67.67.0.0 255.255.0.0	67.67.0.0 255.255.0.0
<wsg_iproute_clear_IPv4-address>	53.53.53.10	63.63.63.10
<wsg_iproute_ike1_IPv4-address_mask>	187.0.3.0 255.255.255.0	187.0.3.0 255.255.255.0
<wsg_iproute_ike1_IPv4-address>	33.33.33.10	43.43.43.10
<wsg_iproute_ike2_IPv4-address_mask>	94.0.0.0 255.0.0.0	94.0.0.0 255.0.0.0
<wsg_iproute_ike2_IPv4-address>	33.33.33.10	43.43.43.10
<wsg_iproute_ike3_IPv4-address_mask>	188.0.3.0 255.255.255.0	188.0.3.0 255.255.255.0
<wsg_iproute_ike3_IPv4-address>	33.33.33.10	43.43.43.10
<wsg_iproute_clear_IPv6-address/mask>	2067::/64	2067::/64
<wsg_iproute_clear_nexthop_IPv6-address>	2053::10	2063::10
<wsg_iproute_ike1_IPv6-address/mask>	2094::/64	2094::/64
<wsg_iproute_ike1_nexthop_IPv6-address>	2033::10	2043::10
<wsg_iproute_ike2_IPv6-address/mask>	1873::/64	1873::/64
<wsg_iproute_ike2_nexthop_IPv6-address>	2033::10	2043::10
<wsg_iproute_ike2_IPv6-address/mask>	1883::/64	1883::/64
<wsg_iproute_ike2_nexthop_IPv6-address>	2033::10	2043::10

Variable	Primary ASR 9000	Backup ASR 9000
<wsg_rri_nexthop_IPv4-address>	53.53.53.11	63.63.63.11
<wsg_rri_nexthop_IPv6-address>	2053::11	2063::11
<srp_monitor_hsrp_vlan_id>	1873	1873
<srp_hsrp-group_number>	6	5
<srp_peer_IPv4-address>	83.83.83.11	73.73.73.11
<srp_bind_IPv4-address>	73.73.73.11	83.83.83.11
<srp_interface_icsr_IPv4-address_mask>	73.73.73.11 255.255.255.0	83.83.83.11 255.255.255.0
<srp_iproute_icsr_IPv4-address_mask>	83.83.83.0 255.255.255.0	73.73.73.0 255.255.255.0
<srp_iproute_icsr_IPv4-address>	73.73.73.11	83.83.83.11
<connectedapps_session_IPv4-address>	100.100.100.10	192.168.122.2
<port_1/10_vlan_id>	1873	1873
<port_1/11_vlan_id_srp>	1260	1361
<port_1/11_vlan_id_wsg>	1882	1883

Table 8: StarOS IP Address Mapping - SecGW4

Variable	Primary ASR 9000	Backup ASR 9000
<interfsace_LOCAL1_IPv4-address>	100.100.100.4 255.255.255.0	192.168.122.18 255.255.255.0
<iproute_LOCAL1_IPv4-address_mask>	0.0.0.0 0.0.0.0 100.100.100.10	0.0.0.0 0.0.0.0 192.168.122.2
<wsg_acl1_permit_IPv4-address_mask>	68.68.0.0 0.0.255.255 48.48.0.0 0.0.255.255	68.68.0.0 0.0.255.255 48.48.0.0 0.0.255.255
<wsg_acl1_permit_IPv6-address/mask>	2068:: ::ffff:ffff:ffff:ffff 2048:: ::ffff:ffff:ffff:ffff	2068:: ::ffff:ffff:ffff:ffff 2048:: ::ffff:ffff:ffff:ffff
<wsg_pool1_IPv4-address>	48.48.0.1 48.48.58.254	48.48.0.1 48.48.58.254
<wsg_pool1_IPv6-address/mask>	2048::/56	2048::/56
<crypto_foo_local_IPv4-addrress>	38.38.38.38	38.38.38.38
<crypto_foo-1_local_IPv6-addrress>	2038::38	2038::38
<wsg_interface_clear_IPv4-address_mask>	54.54.54.11 255.255.255.0	64.64.64.11 255.255.255.0
<wsg_interface_clear_IPv6-address/mask>	2054::11/64	2064::11/64
<wsg_interface_ike_IPv4-address_mask>	34.34.34.11 255.255.255.0	44.44.44.12 255.255.255.0
<wsg_interface_ike_IPv6-address/mask>	2034::11/64	2044::11/64
<wsg_interface_ike-loop_IPv4-address_mask>	38.38.38.38 255.255.255.255	38.38.38.38 255.255.255.255

Variable	Primary ASR 9000	Backup ASR 9000
<wsg_interface_ike-loop_IPv6-address/mask>	2038::38/128	2038::38/128
<wsg_interface_ike-loop1_IPv4-address_mask>	34.34.34.100 255.255.255.255	44.44.44.100 255.255.255.255
<wsg-service_bind_IPv4-address>	38.38.38.38	38.38.38.38
<wsg-service_bind_IPv6-address>	2038::38	2038::38
<wsg_iproute_clear_IPv4-address_mask>	68.68.0.0 255.255.0.0	68.68.0.0 255.255.0.0
<wsg_iproute_clear_IPv4-address>	54.54.54.10	64.64.64.10
<wsg_iproute_ike1_IPv4-address_mask>	187.0.4.0 255.255.255.0	187.0.4.0 255.255.255.0
<wsg_iproute_ike1_IPv4-address>	34.34.34.10	44.44.44.10
<wsg_iproute_ike2_IPv4-address_mask>	95.0.0.0 255.0.0.0	95.0.0.0 255.0.0.0
<wsg_iproute_ike2_IPv4-address>	34.34.34.10	44.44.44.10
<wsg_iproute_ike3_IPv4-address_mask>	188.0.4.0 255.255.255.0	188.0.4.0 255.255.255.0
<wsg_iproute_ike3_IPv4-address>	34.34.34.10	44.44.44.10
<wsg_iproute_clear_IPv6-address/mask>	2068::/64	2068::/64
<wsg_iproute_clear_nexthop_IPv6-address>	2054::10	2064::10
<wsg_iproute_ike1_IPv6-address/mask>	2095::/64	2095::/64
<wsg_iproute_ike1_nexthop_IPv6-address>	2034::10	2044::10
<wsg_iproute_ike2_IPv6-address/mask>	1874::/64	1874::/64
<wsg_iproute_ike2_nexthop_IPv6-address>	2034::10	2044::10
<wsg_iproute_ike2_IPv6-address/mask>	1884::/64	1884::/64
<wsg_iproute_ike2_nexthop_IPv6-address>	2034::10	2044::10
<wsg_rri_nexthop_IPv4-address>	54.54.54.11	64.64.64.11
<wsg_rri_nexthop_IPv6-address>	2054::11	2064::11
<srp_monitor_hsrp_vlan_id>	1874	1874
<srp_hsrp-group_number>	7	7
<srp_peer_IPv4-address>	84.84.84.11	74.74.74.11
<srp_bind_IPv4-address>	74.74.74.11	84.84.84.11
<srp_interface_icsr_IPv4-address_mask>	74.74.74.11 255.255.255.0	84.84.84.11 255.255.255.0
<srp_iproute_icsr_IPv4-address_mask>	84.84.84.0 255.255.255.0	74.74.74.0 255.255.255.0
<srp_iproute_icsr_IPv4-address>	74.74.74.11	84.84.84.11
<connectedapps_session_IPv4-address>	100.100.100.10	192.168.122.2
<port_1/10_vlan_id>	1874	1874
<port_1/11_vlan_id_srp>	1262	1362

Variable	Primary ASR 9000	Backup ASR 9000
<port_1/11_vlan_id_wsg>	1884	1884

SecGW VM Configuration - Primary ASR 9000 Chassis

```
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
  #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
  ca-certificate 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/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_iroute_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

```
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
 ca-certificate 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/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_iroute_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
```

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.

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

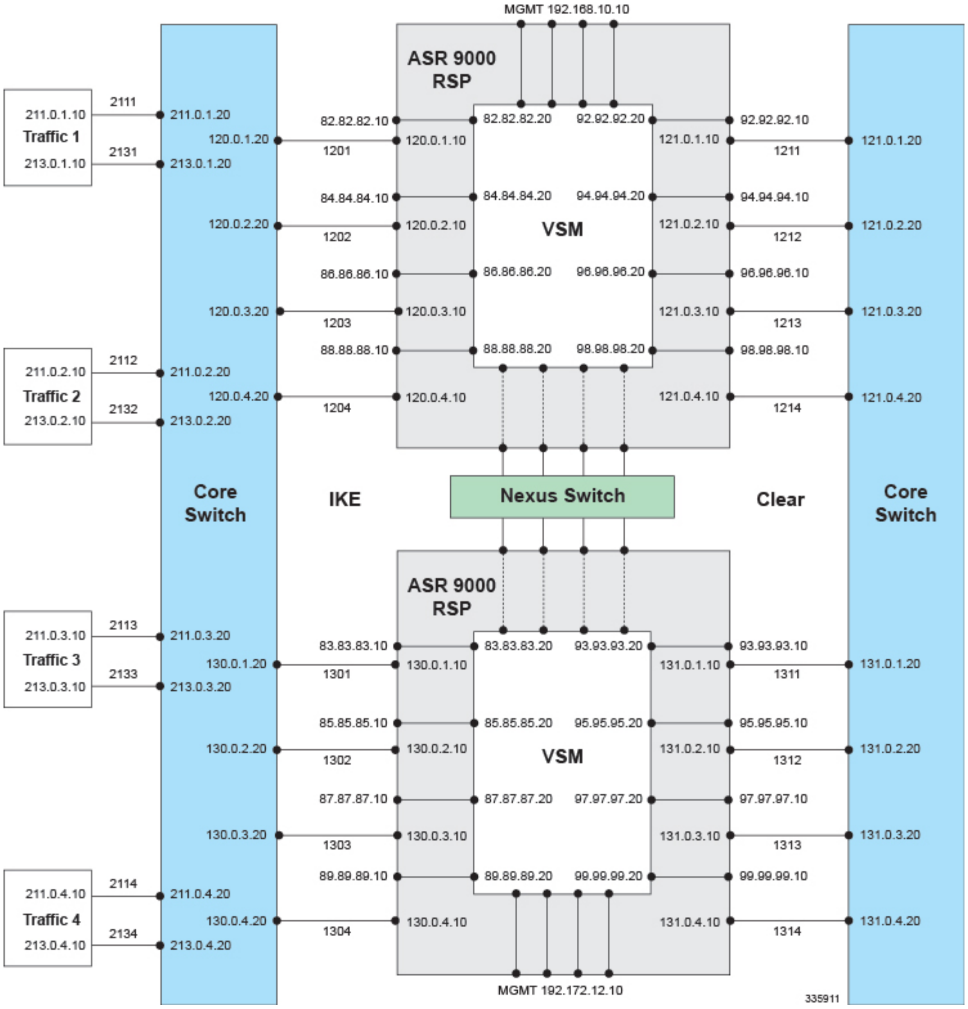
Active VSM	Standby VSM
VM1 – SecGW1	VM1 – SecGW1
VM2 – SecGW2	VM2 – SecGW2
VM3 – SecGW3	VM3 – SecGW3
VM4 – SecGW4	VM4 – SecGW4

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

```
  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>
line console
   exec-timeout 0 0
   length 50
   absolute-timeout 10000
   session-timeout 35791

line default
   exec-timeout 0 0
   length 50

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 secgw2
   vnic interface TenGigE0/3/1/3
   vnic interface TenGigE0/3/1/4
   vnic interface TenGigE0/3/1/5
   activate

virtual-service secgw3
   vnic interface TenGigE0/3/1/6
   vnic interface TenGigE0/3/1/7
   vnic interface TenGigE0/3/1/8
   activate

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
   dot1q tunneling ethertype 0x9200

interface GigabitEthernet0/2/0/0.1201
   description "Public Interface: IKE and ESP Traffic - VM1"
   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 GigabitEthernet0/2/0/2
   shutdown

interface GigabitEthernet0/2/0/3
   description "Private Interface, Clear Traffic"
   transceiver permit pid all
   dot1q tunneling ethertype 0x9200

interface GigabitEthernet0/2/0/3.1211
   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 GigabitEthernet0/2/0/3.1212
   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 GigabitEthernet0/2/0/3.1213
   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 GigabitEthernet0/2/0/3.1214
```

```
   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 ethertype 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 TenGigE0/1/1/11
   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
   l2transport


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 ethertype 0x9200

interface TenGigE0/3/1/6.1203
   description "IKE traffic for VM3"
   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 and srp 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

interface preconfigure TenGigE0/0/1/0
   shutdown

interface preconfigure TenGigE0/0/1/1
   shutdown

interface preconfigure TenGigE0/0/1/2
   shutdown

interface preconfigure TenGigE0/0/1/3
   shutdown

interface preconfigure TenGigE0/0/1/4
   shutdown
```

```
interface preconfigure TenGigE0/0/1/5
   shutdown

interface preconfigure TenGigE0/0/1/6
   shutdown

interface preconfigure TenGigE0/0/1/7
   shutdown

interface preconfigure TenGigE0/0/1/8
   shutdown

interface preconfigure TenGigE0/0/1/9
   shutdown

interface preconfigure TenGigE0/0/1/10
   shutdown

interface preconfigure TenGigE0/0/1/11
   shutdown

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 (43.43.43.43/32 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
      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
      65.65.0.0/16 121.0.1.20
      66.66.0.0/16 121.0.2.20
      67.67.0.0/16 121.0.3.20
      68.68.0.0/16 121.0.4.20
      73.73.73.0/24 206.0.1.30
      75.75.75.0/24 206.0.1.30
      77.77.77.0/24 206.0.1.30
      79.79.79.0/24 206.0.1.30
      202.153.144.25/32 8.40.0.1
      211.0.1.0/24 120.0.1.20
      211.0.2.0/24 120.0.2.20
      211.0.3.0/24 120.0.3.20
      211.0.4.0/24 120.0.4.20
      213.0.1.0/24 121.0.1.20
      213.0.2.0/24 121.0.2.20
      213.0.3.0/24 121.0.3.20
      213.0.4.0/24 121.0.4.20

router bgp 2000
   bgp router-id 2.2.2.2
   address-family ipv4 unicast
      redistribute application hsrp
      redistribute application hsrp-2-1
      redistribute application hsrp-2-2
      redistribute application hsrp-2-3
      redistribute application hsrp-2-4
      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

         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


   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_primary_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 PrivateHsrp
   type line-protocol state
      interface GigabitEthernet0/2/0/3

   delay up 1
   delay down 1

end
```

ASR 9000 Backup Chassis

```
  IOS XR Configuration 5.2.2
Last configuration change at<timestamp> by root

hostname <ASR9K_backup_hostname>
logging events level informational
tftp vrf default ipv4 server homedir disk0: max-servers 10
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 secgw2
   vnic interface TenGigE0/1/1/3
   vnic interface TenGigE0/1/1/4
   vnic interface TenGigE0/1/1/5
   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

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 8.40.4.100 255.255.0.0

interface GigabitEthernet0/2/0/0
   description "Private Interface: IKE and ESP Traffic"
   transceiver permit pid all
   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 GigabitEthernet0/2/0/1.1311
   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 GigabitEthernet0/2/0/1.1312
   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 GigabitEthernet0/2/0/1.1313
   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 GigabitEthernet0/2/0/1.1314
   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 GigabitEthernet0/2/0/13
   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 ethertype 0x9200

interface GigabitEthernet0/2/0/18.2061
```

```
   ipv4 address 206.0.1.30 255.255.255.0
   ipv6 address 2026::30/64
   encapsulation dot1q 2061

interface GigabitEthernet0/2/0/18.2062
   ipv4 address 206.0.2.30 255.255.255.0
   ipv6 address 2022::30/64
   ipv6 enable
   encapsulation dot1q 2062

interface GigabitEthernet0/2/0/18.2063
   ipv4 address 206.0.3.30 255.255.255.0
   ipv6 address 2023::30/64
   ipv6 enable
   encapsulation dot1q 2063

interface GigabitEthernet0/2/0/18.2064
   ipv4 address 206.0.4.30 255.255.255.0
   ipv6 address 2024::30/64
   ipv6 enable
   encapsulation dot1q 2064

interface GigabitEthernet0/2/0/18.2065
   ipv4 address 206.0.5.30 255.255.255.0
   ipv6 address 2025::30/64
   ipv6 enable
   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 TenGigE0/1/1/1.1321
   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 TenGigE0/1/1/6.1303
   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 and 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
```

```
interface BVI1
   ipv4 address 192.172.12.10 255.255.255.0

interface preconfigure TenGigE0/3/1/0

interface preconfigure TenGigE0/3/1/1
   shutdown

interface preconfigure TenGigE0/3/1/2
   shutdown

interface preconfigure TenGigE0/3/1/3
   shutdown

interface preconfigure TenGigE0/3/1/4

interface preconfigure TenGigE0/3/1/5

interface preconfigure TenGigE0/3/1/6

interface preconfigure TenGigE0/3/1/7
   shutdown

interface preconfigure TenGigE0/3/1/8
   shutdown

interface preconfigure TenGigE0/3/1/9
   shutdown

interface preconfigure TenGigE0/3/1/10
   shutdown

interface preconfigure TenGigE0/3/1/11
   shutdown

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 (23.23.23.23/32 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
      65.65.0.0/16 131.0.1.20
      66.66.0.0/16 131.0.2.20
      67.67.0.0/16 131.0.3.20
      68.68.0.0/16 131.0.4.20
      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
      redistribute application hsrp-3-1
      redistribute application hsrp-3-2
      redistribute application hsrp-3-3
      redistribute application hsrp-3-4
      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
      address-family ipv4 unicast
         route-policy block-ike-01 out


   neighbor 131.0.2.20
      remote-as 6000
      address-family ipv4 unicast
         route-policy block-ike-02 out


   neighbor 131.0.3.20
```

```
      remote-as 6000
      address-family ipv4 unicast
         route-policy block-ike-03 out


   neighbor 131.0.4.20
      remote-as 6000
      address-family ipv4 unicast
         route-policy block-ike-04 out



l2vpn
   xconnect group wsg

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

         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


   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 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 PublicHsrp
   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

track PrivateHsrp
   type line-protocol state
```

```
    interface GigabitEthernet0/2/0/1

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

Variable	Primary ASR 9000	Backup ASR 9000
<interface_LOCAL1_IPv4-address_mask>	10.78.1.115 255.255.255.0	10.78.1.111 255.255.255.0
<interface_LOCAL1_IPv4-address_mask_secondary>	192.172.12.11 255.255.255.0	192.168.10.11 255.255.255.0
<iproute_:LOCAL1_IPv4-address_mask>	0.0.0.0 0.0.0.0 10.78.1.1	0.0.0.0 0.0.0.0 10.78.1.1
<wsg_acl1_permit1_IPv4-address_mask>	65.65.0.0 0.0.255.255 45.45.0.0 0.0.255.255	65.65.0.0 0.0.255.255 45.45.0.0 0.0.255.255
<wsg_acl1_permit2_IPv4-address_mask>	66.66.0.0 0.0.255.25 46.46.0.0 0.0.255.255	66.66.0.0 0.0.255.25 46.46.0.0 0.0.255.255
<wsg_acl1_permit3_IPv4-address_mask>	67.67.0.0 0.0.255.255 47.47.0.0 0.0.255.255	67.67.0.0 0.0.255.255 47.47.0.0 0.0.255.255

Variable	Primary ASR 9000	Backup ASR 9000
<wsg_acl1_permit4_IPv4-address_mask>	68.68.0.0 0.0.255.255 48.48.0.0 0.0.255.255	68.68.0.0 0.0.255.255 48.48.0.0 0.0.255.255
<wsg_acl1_permit5_IPv4-address_mask>	69.69.0.0 0.0.255.255 49.49.0.0 0.0.255.255	69.69.0.0 0.0.255.255 49.49.0.0 0.0.255.255
<wsg_acl1_permit1_IPv6-address_mask>	2065:: 0:ffff:ffff:ffff:ffff:ffff:ffff:ffff 2045:: 0:ffff:ffff:ffff:ffff:ffff:ffff:ffff	2065:: 0:ffff:ffff:ffff:ffff:ffff:ffff:ffff 2045:: 0:ffff:ffff:ffff:ffff:ffff:ffff:ffff
<wsg_acl1_permit2_IPv6-address_mask>	2066: 0:ffff:ffff:ffff:ffff:ffff:ffff:ffff 2046:: 0:ffff:ffff:ffff:ffff:ffff:ffff:ffff	2066: 0:ffff:ffff:ffff:ffff:ffff:ffff:ffff 2046:: 0:ffff:ffff:ffff:ffff:ffff:ffff:ffff
<wsg_acl1_permit3_IPv6-address_mask>	2067:: 0:ffff:ffff:ffff:ffff:ffff:ffff:ffff 2047:: 0:ffff:ffff:ffff:ffff:ffff:ffff:ffff	2067:: 0:ffff:ffff:ffff:ffff:ffff:ffff:ffff 2047:: 0:ffff:ffff:ffff:ffff:ffff:ffff:ffff
<wsg_acl1_permit4_IPv6-address_mask>	2068:: 0:ffff:ffff:ffff:ffff:ffff:ffff:ffff 2048:: 0:ffff:ffff:ffff:ffff:ffff:ffff:ffff	2068:: 0:ffff:ffff:ffff:ffff:ffff:ffff:ffff 2048:: 0:ffff:ffff:ffff:ffff:ffff:ffff:ffff
<wsg_acl1_permit5_IPv6-address_mask>	2069:: 0:ffff:ffff:ffff:ffff:ffff:ffff:ffff 2049:: 0:ffff:ffff:ffff:ffff:ffff:ffff:ffff	2069:: 0:ffff:ffff:ffff:ffff:ffff:ffff:ffff 2049:: 0:ffff:ffff:ffff:ffff:ffff:ffff:ffff
<wsg_pool1_IPv4-address_mask>	—	20.13.0.1 20.13.255.255
<wsg_pool2_IPv4-address_mask>	45.45.0.1 45.45.255.254	20.14.0.1 20.14.255.255
<wsg_pool2_IPv6-address/mask>	2013::/56	2013::/56
<crypto_ike-ts-1_local_IPv6-addrress>	2023::23	2023::33
<wsg_interface_clear_IPv4-address_mask>	93.93.93.20 255.255.255.0	92.92.92.20 255.255.255.0
<wsg_interface_clear_IPv6-address/mask>	2093::23/64	2092::23/64
<wsg_interface_clear-loopback_IPv4-address_mask>	93.93.93.100 255.255.255.255	92.92.92.100 255.255.255.255
<wsg_interface_ike_IPv4-address_mask>	83.83.83.20 255.255.255.0	82.82.82.20 255.255.255.0
<wsg_interface_ike_IPv6-address/mask>	2083::23/64	2082::23/64
<wsg_interface_ike-loop_IPv4-address_mask>	83.83.83.100 255.255.255.255	82.82.82.100 255.255.255.255
<wsg_interface_wsg-service_loop_IPv4-address_mask>	23.23.23.23 255.255.255.255	23.23.23.23 255.255.255.255
<wsg_interface_wsg-service_loop_IPv6-address_mask>	2023::23/128	2023::33/128
<wsg-service_bind_ras_IPv4-address>	23.23.23.23	—
<wsg-service_bind_s2s_IPv4-address>	—	23.23.23.23
<wsg-service_bind_s2s_IPv6-address>	2023::23	2023::23
<wsg_iproute_ike1_IPv4-address_mask>	181.8.0.0 255.255.255.0	181.8.0.0 255.255.255.0
<wsg_iproute_ike1_IPv4-address>	83.83.83.10	82.82.82.10

Variable	Primary ASR 9000	Backup ASR 9000
<wsg_iproute_ike2_IPv4-address_mask>	186.0.0.0 255.0.0.0	186.0.0.0 255.0.0.0
<wsg_iproute_ike2_IPv4-address>	83.83.83.10	82.82.82.10
<wsg_iproute_ike3_IPv4-address_mask>	120.0.1.0 255.255.255.0	120.0.1.0 255.255.255.0
<wsg_iproute_ike3_IPv4-address>	83.83.83.10	82.82.82.10
<wsg_iproute_ike4_IPv4-address_mask>	—	211.0.1.0 255.255.255.0
<wsg_iproute_ike4_IPv4-address>	—	82.82.82.10
<wsg_iproute_ike5_IPv4-address_mask>	11.0.0.0 255.0.0.0	11.0.0.0 255.0.0.0
<wsg_iproute_ike5_IPv4-address>	83.83.83.10	82.82.82.10
<wsg_iproute_clear1_IPv4-address_mask>	65.65.0.0 255.255.0.0	65.65.0.0 255.255.0.0
<wsg_iproute_clear1_IPv4-address>	93.93.93.10	92.92.92.10
<wsg_iproute_clear2_IPv4-address_mask>	66.66.0.0 255.255.0.0	66.66.0.0 255.255.0.0
<wsg_iproute_clear2_IPv4-address>	93.93.93.10	92.92.92.10
<wsg_iproute_clear3_IPv4-address_mask>	67.67.0.0 255.255.0.0	67.67.0.0 255.255.0.0
<wsg_iproute_clear3_IPv4-address>	93.93.93.10	92.92.92.10
<wsg_iproute_clear4_IPv4-address_mask>	68.68.0.0 255.255.0.0	68.68.0.0 255.255.0.0
<wsg_iproute_clear4_IPv4-address>	93.93.93.10	92.92.92.10
<wsg_iproute_clear5_IPv4-address_mask>	69.69.0.0 255.255.0.0	69.69.0.0 255.255.0.0
<wsg_iproute_clear5_IPv4-address>	93.93.93.10	92.92.92.10
<wsg_iproute_ike1_IPv6-address/mask>	2061::/16	2061::/16
<wsg_iproute_ike1_nexthop_IPv6-address>	2083::10	2082::10
<wsg_iproute_ike2_IPv6-address/mask>	2186::/16	2186::/16
<wsg_iproute_ike2_nexthop_IPv6-address>	2083::10	2082::10
<wsg_iproute_clear1_IPv6-address/mask>	2065::/16	2065::/16
<wsg_iproute_clear1_nexthop_IPv6-address>	2093::10	2092::10
<wsg_iproute_clear2_IPv6-address/mask>	2066::/16	2066::/16
<wsg_iproute_clear2_nexthop_IPv6-address>	2093::10	2092::10
<wsg_iproute_clear3_IPv6-address/mask>	2068::/16	2068::/16
<wsg_iproute_clear3_nexthop_IPv6-address>	2093::10	2092::10
<wsg_iproute_clear4_IPv6-address/mask>	2067::/16	2067::/16
<wsg_iproute_clear4_nexthop_IPv6-address>	2093::10	2092::10
<wsg_iproute_clear5_IPv6-address/mask>	2069::/16	2069::/16
<wsg_iproute_clear5_nexthop_IPv6-address>	2093::10	2092::10

Variable	Primary ASR 9000	Backup ASR 9000
<wsg_sri-route_IPv4-address>	23.23.23.23	23.23.23.23
<wsg_sri-route_nexthop_IPv4-address>	83.83.83.20	82.82.82.2
<wsg_rri_nexthop_IPv4-address>	93.93.93.20	—
<wsg_rri_network-mode_IPv4-address>	185.186.187.188	135.135.135.85
<wsg_rri_network-mode_nexthop_IPv4-address>	93.93.93.20	92.92.92.20
<srp_monitor_hsrp_vlan_id>	2062	2062
<srp_hsrp-group_number>	401	401
<srp_peer_IPv4-address>	72.72.72.20	73.73.73.20
<srp_bind_IPv4-address>	73.73.73.20	72.72.72.20
<srp_interface_icsr_IPv4-address_mask>	73.73.73.20 255.255.255.0	72.72.72.20 255.255.255.0
<srp_iproute_icsr_IPv4-address_mask>	0.0.0.0 0.0.0.0 73.73.73.10	0.0.0.0 0.0.0.0 72.72.72.10
<connectedapps_session_IPv4-address>	192.172.12.10	192.168.10.10
<port_1/10_vlan_id>	1301	1201
<port_1/11_vlan_id_wsg>	1311	1211
<port_1/11_vlan_id_srp>	1321	1221

Table 11: StarOS IP Address Mapping - SecGW2

Variable	Primary ASR 9000	Backup ASR 9000
<interface_LOCAL1_IPv4-address_mask>	10.78.1.116 255.255.255.0	10.78.1.112 255.255.255.0
<interface_LOCAL1_IPv4-address_mask_secondary>	192.172.12.13 255.255.255.0	192.168.10.2 255.255.255.0
<iproute_:LOCAL1_IPv4-address_mask>	0.0.0.0 0.0.0.0 10.78.1.1	0.0.0.0 0.0.0.0 10.78.1.1
<wsg_acl1_permit1_IPv4-address_mask>	65.65.0.0 0.0.255.255 45.45.0.0 0.0.255.255	65.65.0.0 0.0.255.255 45.45.0.0 0.0.255.255
<wsg_acl1_permit2_IPv4-address_mask>	66.66.0.0 0.0.255.25 46.46.0.0 0.0.255.255	66.66.0.0 0.0.255.25 46.46.0.0 0.0.255.255
<wsg_acl1_permit3_IPv4-address_mask>	67.67.0.0 0.0.255.255 47.47.0.0 0.0.255.255	67.67.0.0 0.0.255.255 47.47.0.0 0.0.255.255
<wsg_acl1_permit4_IPv4-address_mask>	68.68.0.0 0.0.255.255 48.48.0.0 0.0.255.255	68.68.0.0 0.0.255.255 48.48.0.0 0.0.255.255
<wsg_acl1_permit5_IPv4-address_mask>	69.69.0.0 0.0.255.255 49.49.0.0 0.0.255.255	69.69.0.0 0.0.255.255 49.49.0.0 0.0.255.255

Variable	Primary ASR 9000	Backup ASR 9000
<wsg_acl1_permit1_IPv6-address_mask>	2065:: 0:ffff:ffff:ffff:ffff:ffff:ffff:ffff 2045:: 0:ffff:ffff:ffff:ffff:ffff:ffff:ffff	2065:: 0:ffff:ffff:ffff:ffff:ffff:ffff:ffff 2045:: 0:ffff:ffff:ffff:ffff:ffff:ffff:ffff
<wsg_acl1_permit2_IPv6-address_mask>	2066: 0:ffff:ffff:ffff:ffff:ffff:ffff:ffff 2046:: 0:ffff:ffff:ffff:ffff:ffff:ffff:ffff	2066: 0:ffff:ffff:ffff:ffff:ffff:ffff:ffff 2046:: 0:ffff:ffff:ffff:ffff:ffff:ffff:ffff
<wsg_acl1_permit3_IPv6-address_mask>	2067:: 0:ffff:ffff:ffff:ffff:ffff:ffff:ffff 2047:: 0:ffff:ffff:ffff:ffff:ffff:ffff:ffff	2067:: 0:ffff:ffff:ffff:ffff:ffff:ffff:ffff 2047:: 0:ffff:ffff:ffff:ffff:ffff:ffff:ffff
<wsg_acl1_permit4_IPv6-address_mask>	2068:: 0:ffff:ffff:ffff:ffff:ffff:ffff:ffff 2048:: 0:ffff:ffff:ffff:ffff:ffff:ffff:ffff	2068:: 0:ffff:ffff:ffff:ffff:ffff:ffff:ffff 2048:: 0:ffff:ffff:ffff:ffff:ffff:ffff:ffff
<wsg_acl1_permit5_IPv6-address_mask>	2069:: 0:ffff:ffff:ffff:ffff:ffff:ffff:ffff 2049:: 0:ffff:ffff:ffff:ffff:ffff:ffff:ffff	2069:: 0:ffff:ffff:ffff:ffff:ffff:ffff:ffff 2049:: 0:ffff:ffff:ffff:ffff:ffff:ffff:ffff
<wsg_pool1_IPv4-address_mask>	20.13.0.1 20.13.255.255	20.13.0.1 20.13.255.255
<wsg_pool2_IPv4-address_mask>	20.14.0.1 20.14.255.255	20.14.0.1 20.14.255.255
<wsg_pool2_IPv6-address/mask>	2013::/56	2013::/56
<crypto_ike-ts-1_local_IPv6-addrress>	2033::33	2033::23
<wsg_interface_clear_IPv4-address_mask>	95.95.95.20 255.255.255.0	94.94.94.20 255.255.255.0
<wsg_interface_clear_IPv6-address/mask>	2095::23/64	2094::23/64
<wsg_interface_clear-loopback_IPv4-address_mask>	95.95.95.100 255.255.255.255	94.94.94.100 255.255.255.255
<wsg_interface_ike_IPv4-address_mask>	85.85.85.20 255.255.255.0	84.84.84.20 255.255.255.0
<wsg_interface_ike_IPv6-address/mask>	2085::23/64	2084::23/64
<wsg_interface_ike-loop_IPv4-address_mask>	85.85.85.100 255.255.255.255	84.84.84.100 255.255.255.255
<wsg_interface_wsg-service_loop_IPv4-address_mask>	33.33.33.33 255.255.255.255	33.33.33.33 255.255.255.255
<wsg_interface_wsg-service_loop_IPv6-address_mask>	2033::33/128	2033::23/128
<wsg-service_bind_ras_IPv4-address>	33.33.33.33	—
<wsg-service_bind_s2s_IPv4-address>	—	33.33.33.33
<wsg-service_bind_s2s_IPv6-address>	2033::33	2033::23
<wsg_iproute_ike1_IPv4-address_mask>	181.8.0.0 255.255.255.0	181.8.0.0 255.255.255.0
<wsg_iproute_ike1_IPv4-address>	85.85.85.10	84.84.84.10
<wsg_iproute_ike2_IPv4-address_mask>	186.0.0.0 255.0.0.0	186.0.0.0 255.0.0.0
<wsg_iproute_ike2_IPv4-address>	85.85.85.10	84.84.84.10
<wsg_iproute_ike3_IPv4-address_mask>	120.0.1.0 255.255.255.0	120.0.1.0 255.255.255.0
<wsg_iproute_ike3_IPv4-address>	85.85.85.10	84.84.84.10
<wsg_iproute_ike4_IPv4-address_mask>	211.0.1.0 255.255.255.0	211.0.1.0 255.255.255.0

Variable	Primary ASR 9000	Backup ASR 9000
<wsg_iproute_ike4_IPv4-address>	85.85.85.10	84.84.84.10
<wsg_iproute_ike5_IPv4-address_mask>	15.0.0.0 255.0.0.0	15.0.0.0 255.0.0.0
<wsg_iproute_ike5_IPv4-address>	85.85.85.10	84.84.84.10
<wsg_iproute_clear1_IPv4-address_mask>	65.65.0.0 255.255.0.0	65.65.0.0 255.255.0.0
<wsg_iproute_clear1_IPv4-address>	95.95.95.10	94.94.94.10
<wsg_iproute_clear2_IPv4-address_mask>	66.66.0.0 255.255.0.0	66.66.0.0 255.255.0.0
<wsg_iproute_clear2_IPv4-address>	95.95.95.10	94.94.94.10
<wsg_iproute_clear3_IPv4-address_mask>	67.67.0.0 255.255.0.0	67.67.0.0 255.255.0.0
<wsg_iproute_clear3_IPv4-address>	95.95.95.10	94.94.94.10
<wsg_iproute_clear4_IPv4-address_mask>	68.68.0.0 255.255.0.0	68.68.0.0 255.255.0.0
<wsg_iproute_clear4_IPv4-address>	95.95.95.10	94.94.94.10
<wsg_iproute_clear5_IPv4-address_mask>	69.69.0.0 255.255.0.0	69.69.0.0 255.255.0.0
<wsg_iproute_clear5_IPv4-address>	95.95.95.10	94.94.94.10
<wsg_iproute_ike1_IPv6-address/mask>	2061::/16	2061::/16
<wsg_iproute_ike1_nexthop_IPv6-address>	2085::10	2084::10
<wsg_iproute_ike2_IPv6-address/mask>	2186::/16	2186::/16
<wsg_iproute_ike2_nexthop_IPv6-address>	2085::10	2084::10
<wsg_iproute_clear1_IPv6-address/mask>	2065::/16	2065::/16
<wsg_iproute_clear1_nexthop_IPv6-address>	2095::10	2094::10
<wsg_iproute_clear2_IPv6-address/mask>	2066::/16	2066::/16
<wsg_iproute_clear2_nexthop_IPv6-address>	2095::10	2094::10
<wsg_iproute_clear3_IPv6-address/mask>	2068::/16	2068::/16
<wsg_iproute_clear3_nexthop_IPv6-address>	2095::10	2094::10
<wsg_iproute_clear4_IPv6-address/mask>	2067::/16	2067::/16
<wsg_iproute_clear4_nexthop_IPv6-address>	2095::10	2094::10
<wsg_iproute_clear5_IPv6-address/mask>	2069::/16	2069::/16
<wsg_iproute_clear5_nexthop_IPv6-address>	2095::10	2094::10
<wsg_sri-route_IPv4-address>	33.33.33.33	33.33.33.33
<wsg_sri-route_nexthop_IPv4-address>	85.85.85.20	84.84.84.20
<wsg_rri_nexthop_IPv4-address>	—	—
<wsg_rri_network-mode_IPv4-address>	86.86.86.86	86.86.86.86
<wsg_rri_network-mode_nexthop_IPv4-address>	95.95.95.20	94.94.94.20

Variable	Primary ASR 9000	Backup ASR 9000
<srp_monitor_hsrp_vlan_id>	2063	2063
<srp_hsrp-group_number>	402	402
<srp_peer_IPv4-address>	74.74.74.20	75.75.75.20
<srp_bind_IPv4-address>	75.75.75.20	74.74.74.20
<srp_interface_icsr_IPv4-address_mask>	75.75.75.20 255.255.255.0	74.74.74.20 255.255.255.0
<srp_iproute_icsr_IPv4-address_mask>	0.0.0.0 0.0.0.0 75.75.75.10	0.0.0.0 0.0.0.0 74.74.74.10
<connectedapps_session_IPv4-address>	192.172.12.10	192.168.10.10
<port_1/10_vlan_id>	1302	1202
<port_1/11_vlan_id_wsg>	1312	1212
<port_1/11_vlan_id_srp>	1322	1222

Table 12: StarOS IP Address Mapping - SecGW3

Variable	Primary ASR 9000	Backup ASR 9000
<interface_LOCAL1_IPv4-address_mask>	10.78.1.117 255.255.255.0	10.78.1.113 255.255.255.0
<interface_LOCAL1_IPv4-address_mask_secondary>	192.172.12.13 255.255.255.0	192.168.10.13 255.255.255.0
<iproute_:LOCAL1_IPv4-address_mask>	0.0.0.0 0.0.0.0 10.78.1.1	0.0.0.0 0.0.0.0 10.78.1.1
<wsg_acl1_permit1_IPv4-address_mask>	65.65.0.0 0.0.255.255 45.45.0.0 0.0.255.255	65.65.0.0 0.0.255.255 45.45.0.0 0.0.255.255
<wsg_acl1_permit2_IPv4-address_mask>	66.66.0.0 0.0.255.25 46.46.0.0 0.0.255.255	66.66.0.0 0.0.255.25 46.46.0.0 0.0.255.255
<wsg_acl1_permit3_IPv4-address_mask>	67.67.0.0 0.0.255.255 47.47.0.0 0.0.255.255	67.67.0.0 0.0.255.255 47.47.0.0 0.0.255.255
<wsg_acl1_permit4_IPv4-address_mask>	68.68.0.0 0.0.255.255 48.48.0.0 0.0.255.255	68.68.0.0 0.0.255.255 48.48.0.0 0.0.255.255
<wsg_acl1_permit5_IPv4-address_mask>	69.69.0.0 0.0.255.255 49.49.0.0 0.0.255.255	69.69.0.0 0.0.255.255 49.49.0.0 0.0.255.255
<wsg_acl1_permit1_IPv6-address_mask>	2065:: 0:ffff:ffff:ffff:ffff:ffff:ffff:ffff 2045:: 0:ffff:ffff:ffff:ffff:ffff:ffff:ffff	2065:: 0:ffff:ffff:ffff:ffff:ffff:ffff:ffff 2045:: 0:ffff:ffff:ffff:ffff:ffff:ffff:ffff
<wsg_acl1_permit2_IPv6-address_mask>	2066: 0:ffff:ffff:ffff:ffff:ffff:ffff:ffff 2046:: 0:ffff:ffff:ffff:ffff:ffff:ffff:ffff	2066: 0:ffff:ffff:ffff:ffff:ffff:ffff:ffff 2046:: 0:ffff:ffff:ffff:ffff:ffff:ffff:ffff

Variable	Primary ASR 9000	Backup ASR 9000
<wsg_acl1_permit3_IPv6-address_mask>	2067:: 0:ffff:ffff:ffff:ffff:ffff:ffff:ffff 2047:: 0:ffff:ffff:ffff:ffff:ffff:ffff:ffff	2067:: 0:ffff:ffff:ffff:ffff:ffff:ffff:ffff 2047:: 0:ffff:ffff:ffff:ffff:ffff:ffff:ffff
<wsg_acl1_permit4_IPv6-address_mask>	2068:: 0:ffff:ffff:ffff:ffff:ffff:ffff:ffff 2048:: 0:ffff:ffff:ffff:ffff:ffff:ffff:ffff	2068:: 0:ffff:ffff:ffff:ffff:ffff:ffff:ffff 2048:: 0:ffff:ffff:ffff:ffff:ffff:ffff:ffff
<wsg_acl1_permit5_IPv6-address_mask>	2069:: 0:ffff:ffff:ffff:ffff:ffff:ffff:ffff 2049:: 0:ffff:ffff:ffff:ffff:ffff:ffff:ffff	2069:: 0:ffff:ffff:ffff:ffff:ffff:ffff:ffff 2049:: 0:ffff:ffff:ffff:ffff:ffff:ffff:ffff
<wsg_pool1_IPv4-address_mask>	20.13.0.1 20.13.255.255	20.13.0.1 20.13.255.255
<wsg_pool2_IPv4-address_mask>	20.14.0.1 20.14.255.255	20.14.0.1 20.14.255.255
<wsg_pool2_IPv6-address/mask>	2013::/56	2013::/56
<crypto_ike-ts-1_local_IPv6-addrress>	2043::33	2043::23
<wsg_interface_clear_IPv4-address_mask>	97.97.97.20 255.255.255.0	96.96.96.100 255.255.255.255
<wsg_interface_clear_IPv6-address/mask>	2096::23/64	2096::23/64
<wsg_interface_clear-loopback_IPv4-address_mask>	97.97.97.100 255.255.255.255	96.96.96.100 255.255.255.25
<wsg_interface_ike_IPv4-address_mask>	87.87.87.20 255.255.255.0	86.86.86.20 255.255.255.0
<wsg_interface_ike_IPv6-address/mask>	2086::23/64	2086::23/64
<wsg_interface_ike-loop_IPv4-address_mask>	87.87.87.100 255.255.255.255	86.86.86.100 255.255.255.255
<wsg_interface_wsg-service_loop_IPv4-address_mask>	43.43.43.43 255.255.255.255	43.43.43.43 255.255.255.255
<wsg_interface_wsg-service_loop_IPv6-address_mask>	2043::43/128	2043::43/128
<wsg-service_bind_ras_IPv4-address>	—	—
<wsg-service_bind_s2s_IPv4-address>	43.43.43.43	43.43.43.43
<wsg-service_bind_s2s_IPv6-address>	2043::43	2043::43
<wsg_iproute_ike1_IPv4-address_mask>	181.8.0.0 255.255.255.0	181.8.0.0 255.255.255.0
<wsg_iproute_ike1_IPv4-address>	87.87.87.10	84.84.84.10
<wsg_iproute_ike2_IPv4-address_mask>	186.0.0.0 255.0.0.0	186.0.0.0 255.0.0.0
<wsg_iproute_ike2_IPv4-address>	87.87.87.10	86.86.86.10
<wsg_iproute_ike3_IPv4-address_mask>	120.0.1.0 255.255.255.0	120.0.1.0 255.255.255.0
<wsg_iproute_ike3_IPv4-address>	87.87.87.10	86.86.86.10
<wsg_iproute_ike4_IPv4-address_mask>	—	211.0.1.0 255.255.255.0
<wsg_iproute_ike4_IPv4-address>	—	86.86.86.10
<wsg_iproute_ike5_IPv4-address_mask>	17.0.0.0 255.0.0.0	17.0.0.0 255.0.0.0
<wsg_iproute_ike5_IPv4-address>	87.87.87.10	86.86.86.10
<wsg_iproute_clear1_IPv4-address_mask>	65.65.0.0 255.255.0.0	65.65.0.0 255.255.0.0

Variable	Primary ASR 9000	Backup ASR 9000
<wsg_iproute_clear1_IPv4-address>	97.97.97.10	96.96.96.10
<wsg_iproute_clear2_IPv4-address_mask>	66.66.0.0 255.255.0.0	66.66.0.0 255.255.0.0
<wsg_iproute_clear2_IPv4-address>	97.97.97.10	96.96.96.10
<wsg_iproute_clear3_IPv4-address_mask>	67.67.0.0 255.255.0.0	67.67.0.0 255.255.0.0
<wsg_iproute_clear3_IPv4-address>	97.97.97.10	96.96.96.10
<wsg_iproute_clear4_IPv4-address_mask>	68.68.0.0 255.255.0.0	68.68.0.0 255.255.0.0
<wsg_iproute_clear4_IPv4-address>	97.97.97.10	96.96.96.10
<wsg_iproute_clear5_IPv4-address_mask>	69.69.0.0 255.255.0.0	69.69.0.0 255.255.0.0
<wsg_iproute_clear5_IPv4-address>	97.97.97.10	96.96.96.10
<wsg_iproute_ike1_IPv6-address/mask>	—	2061::/16
<wsg_iproute_ike1_nexthop_IPv6-address>	—	2086::10
<wsg_iproute_ike2_IPv6-address/mask>	—	2186::/16
<wsg_iproute_ike2_nexthop_IPv6-address>	—	2086::10
<wsg_iproute_clear1_IPv6-address/mask>	—	2065::/16
<wsg_iproute_clear1_nexthop_IPv6-address>	—	2096::10
<wsg_iproute_clear2_IPv6-address/mask>	—	2066::/16
<wsg_iproute_clear2_nexthop_IPv6-address>	—	2096::10
<wsg_iproute_clear3_IPv6-address/mask>	—	2068::/16
<wsg_iproute_clear3_nexthop_IPv6-address>	—	2096::10
<wsg_iproute_clear4_IPv6-address/mask>	—	2067::/16
<wsg_iproute_clear4_nexthop_IPv6-address>	—	2096::10
<wsg_iproute_clear5_IPv6-address/mask>	—	2069::/16
<wsg_iproute_clear5_nexthop_IPv6-address>	—	2096::10
<wsg_sri-route_IPv4-address>	43.43.43.43	43.43.43.43
<wsg_sri-route_nexthop_IPv4-address>	87.87.87.20	86.86.86.20
<wsg_rri_nexthop_IPv4-address>	—	—
<wsg_rri_network-mode_IPv4-address>	87.87.87.8	87.87.87.87
<wsg_rri_network-mode_nexthop_IPv4-address>	97.97.97.20	96.96.96.20
<srp_monitor_hsrp_vlan_id>	2064	2064
<srp_hsrp-group_number>	403	403
<srp_peer_IPv4-address>	76.76.76.20	77.77.77.20
<srp_bind_IPv4-address>	77.77.77.20	76.76.76.20

Variable	Primary ASR 9000	Backup ASR 9000
<srp_interface_icsr_IPv4-address_mask>	77.77.77.20 255.255.255.0	76.76.76.20 255.255.255.0
<srp_iproute_icsr_IPv4-address_mask>	0.0.0.0 0.0.0.0 77.77.77.10	0.0.0.0 0.0.0.0 76.76.76.10
<connectedapps_session_IPv4-address>	192.172.12.10	192.168.10.10
<port_1/10_vlan_id>	1303	1203
<port_1/11_vlan_id_wsg>	1313	1213
<port_1/11_vlan_id_srp>	1323	1223

Table 13: StarOS IP Address Mapping - SecGW4

Variable	Primary ASR 9000	Backup ASR 9000
<interface_LOCAL1_IPv4-address_mask>	10.78.1.118 255.255.255.0	10.78.1.114 255.255.255.0
<interface_LOCAL1_IPv4-address_mask_secondary>	192.172.12.14 255.255.255.0	92.168.10.14 255.255.255.0
<iproute_:LOCAL1_IPv4-address_mask>	0.0.0.0 0.0.0.0 10.78.1.1	0.0.0.0 0.0.0.0 10.78.1.1
<wsg_acl1_permit1_IPv4-address_mask>	65.65.0.0 0.0.255.255 45.45.0.0 0.0.255.255	65.65.0.0 0.0.255.255 45.45.0.0 0.0.255.255
<wsg_acl1_permit2_IPv4-address_mask>	66.66.0.0 0.0.255.25 46.46.0.0 0.0.255.255	66.66.0.0 0.0.255.25 46.46.0.0 0.0.255.255
<wsg_acl1_permit3_IPv4-address_mask>	67.67.0.0 0.0.255.255 47.47.0.0 0.0.255.255	67.67.0.0 0.0.255.255 47.47.0.0 0.0.255.255
<wsg_acl1_permit4_IPv4-address_mask>	68.68.0.0 0.0.255.255 48.48.0.0 0.0.255.255	68.68.0.0 0.0.255.255 48.48.0.0 0.0.255.255
<wsg_acl1_permit5_IPv4-address_mask>	69.69.0.0 0.0.255.255 49.49.0.0 0.0.255.255	69.69.0.0 0.0.255.255 49.49.0.0 0.0.255.255
<wsg_acl1_permit1_IPv6-address_mask>	2065:: 0:ffff:ffff:ffff:ffff:ffff:ffff:ffff 2045:: 0:ffff:ffff:ffff:ffff:ffff:ffff:ffff	2065:: 0:ffff:ffff:ffff:ffff:ffff:ffff:ffff 2045:: 0:ffff:ffff:ffff:ffff:ffff:ffff:ffff
<wsg_acl1_permit2_IPv6-address_mask>	2066: 0:ffff:ffff:ffff:ffff:ffff:ffff:ffff 2046:: 0:ffff:ffff:ffff:ffff:ffff:ffff:ffff	2066: 0:ffff:ffff:ffff:ffff:ffff:ffff:ffff 2046:: 0:ffff:ffff:ffff:ffff:ffff:ffff:ffff
<wsg_acl1_permit3_IPv6-address_mask>	2067:: 0:ffff:ffff:ffff:ffff:ffff:ffff:ffff 2047:: 0:ffff:ffff:ffff:ffff:ffff:ffff:ffff	2067:: 0:ffff:ffff:ffff:ffff:ffff:ffff:ffff 2047:: 0:ffff:ffff:ffff:ffff:ffff:ffff:ffff
<wsg_acl1_permit4_IPv6-address/_>	2068:: 0:ffff:ffff:ffff:ffff:ffff:ffff:ffff 2048:: 0:ffff:ffff:ffff:ffff:ffff:ffff:ffff	2068:: 0:ffff:ffff:ffff:ffff:ffff:ffff:ffff 2048:: 0:ffff:ffff:ffff:ffff:ffff:ffff:ffff

Variable	Primary ASR 9000	Backup ASR 9000
<wsg_acl1_permit5_IPv6-address_mask>	2069:: 0:ffff:ffff:ffff:ffff:ffff:ffff:ffff 2049:: 0:ffff:ffff:ffff:ffff:ffff:ffff:ffff	2069:: 0:ffff:ffff:ffff:ffff:ffff:ffff:ffff 2049:: 0:ffff:ffff:ffff:ffff:ffff:ffff:ffff
<wsg_pool1_IPv4-address_mask>	20.13.0.1 20.13.255.255	20.13.0.1 20.13.255.255
<wsg_pool2_IPv4-address_mask>	20.14.0.1 20.14.255.255	20.14.0.1 20.14.255.255
<wsg_pool2_IPv6-address/mask>	2013::/56	2013::/56
<crypto_ike-ts-1_local_IPv6-addrress>	2053::53	2023::23
<wsg_interface_clear_IPv4-address_mask>	99.99.99.20 255.255.255.0	98.98.98.20 255.255.255.0
<wsg_interface_clear_IPv6-address/mask>	2099::23/64	2098::23/64
<wsg_interface_clear-loopback_IPv4-address_mask>	99.99.99.100 255.255.255.255	98.98.98.100 255.255.255.255
<wsg_interface_ike_IPv4-address_mask>	89.89.89.20 255.255.255.0	88.88.88.20 255.255.255.0
<wsg_interface_ike_IPv6-address/mask>	2089::23/64	2088::23/64
<wsg_interface_ike-loop_IPv4-address_mask>	89.89.89.100 255.255.255.255	88.88.88.100 255.255.255.255
<wsg_interface_wsg-service_loop_IPv4-address_mask>	53.53.53.53 255.255.255.255	53.53.53.53 255.255.255.255
<wsg_interface_wsg-service_loop_IPv6-address_mask>	2053::53/128	2053::53/128
<wsg-service_bind_ras_IPv4-address>	—	—
<wsg-service_bind_s2s_IPv4-address>	53.53.53.53	53.53.53.53
<wsg-service_bind_s2s_IPv6-address>	2053::53	2053::53
<wsg_iproute_ike1_IPv4-address_mask>	181.8.0.0 255.255.255.0	181.8.0.0 255.255.255.0
<wsg_iproute_ike1_IPv4-address>	89.89.89.10	88.88.88.10
<wsg_iproute_ike2_IPv4-address_mask>	186.0.0.0 255.0.0.0	186.0.0.0 255.0.0.0
<wsg_iproute_ike2_IPv4-address>	89.89.89.10	88.88.88.10
<wsg_iproute_ike3_IPv4-address_mask>	120.0.1.0 255.255.255.0	120.0.1.0 255.255.255.0
<wsg_iproute_ike3_IPv4-address>	89.89.89.10	88.88.88.10
<wsg_iproute_ike4_IPv4-address_mask>	—	211.0.1.0 255.255.255.0
<wsg_iproute_ike4_IPv4-address>	—	88.88.88.10
<wsg_iproute_ike5_IPv4-address_mask>	19.0.0.0 255.0.0.0	19.0.0.0 255.0.0.0
<wsg_iproute_ike5_IPv4-address>	89.89.89.10	88.88.88.10
<wsg_iproute_clear1_IPv4-address_mask>	65.65.0.0 255.255.0.0	65.65.0.0 255.255.0.0
<wsg_iproute_clear1_IPv4-address>	99.99.99.10	98.98.98.10
<wsg_iproute_clear2_IPv4-address_mask>	66.66.0.0 255.255.0.0	66.66.0.0 255.255.0.0
<wsg_iproute_clear2_IPv4-address>	99.99.99.10	98.98.98.10
<wsg_iproute_clear3_IPv4-address_mask>	67.67.0.0 255.255.0.0	67.67.0.0 255.255.0.0

Variable	Primary ASR 9000	Backup ASR 9000
<wsg_iproute_clear3_IPv4-address>	99.99.99.10	98.98.98.10
<wsg_iproute_clear4_IPv4-address_mask>	68.68.0.0 255.255.0.0	68.68.0.0 255.255.0.0
<wsg_iproute_clear4_IPv4-address>	99.99.99.10	98.98.98.10
<wsg_iproute_clear5_IPv4-address_mask>	69.69.0.0 255.255.0.0	69.69.0.0 255.255.0.0
<wsg_iproute_clear5_IPv4-address>	99.99.99.10	98.98.98.10
<wsg_iproute_ike1_IPv6-address/mask>	2061::/16	2061::/16
<wsg_iproute_ike1_nexthop_IPv6-address>	2089::10	2088::10
<wsg_iproute_ike2_IPv6-address/mask>	2186::/16	2186::/16
<wsg_iproute_ike2_nexthop_IPv6-address>	2089::10	2088::10
<wsg_iproute_clear1_IPv6-address/mask>	2065::/16	2065::/16
<wsg_iproute_clear1_nexthop_IPv6-address>	2099::10	2098::10
<wsg_iproute_clear2_IPv6-address/mask>	2066::/16	2066::/16
<wsg_iproute_clear2_nexthop_IPv6-address>	2099::10	2098::10
<wsg_iproute_clear3_IPv6-address/mask>	2068::/16	2068::/16
<wsg_iproute_clear3_nexthop_IPv6-address>	2099::10	2098::10
<wsg_iproute_clear4_IPv6-address/mask>	2067::/16	2067::/16
<wsg_iproute_clear4_nexthop_IPv6-address>	2099::10	2098::10
<wsg_iproute_clear5_IPv6-address/mask>	2069::/16	2069::/16
<wsg_iproute_clear5_nexthop_IPv6-address>	2099::10	2098::10
<wsg_sri-route_IPv4-address>	53.53.53.53	53.53.53.53
<wsg_sri-route_nexthop_IPv4-address>	89.89.89.20	88.88.88.20
<wsg_rri_nexthop_IPv4-address>	—	—
<wsg_rri_network-mode_IPv4-address>	88.88.88.88	88.88.88.88
<wsg_rri_network-mode_nexthop_IPv4-address>	99.99.99.2	98.98.98.20
<srp_monitor_hsrp_vlan_id>	2065	2065
<srp_hsrp-group_number>	404	404
<srp_peer_IPv4-address>	78.78.78.20	79.79.79.20
<srp_bind_IPv4-address>	79.79.79.20	78.78.78.20
<srp_interface_icsr_IPv4-address_mask>	79.79.79.20 255.255.255.0	78.78.78.20 255.255.255.0
<srp_iproute_icsr_IPv4-address_mask>	0.0.0.0 0.0.0.0 79.79.79.10	0.0.0.0 0.0.0.0 78.78.78.10
<connectedapps_session_IPv4-address>	192.172.12.10	192.168.10.10
<port_1/10_vlan_id>	1304	1204

Variable	Primary ASR 9000	Backup ASR 9000
<port_1/11_vlan_id_wsg>	1314	1214
<port_1/11_vlan_id_srp>	1324	1224

SecGW VM Configuration - Primary ASR 9000 Chassis

```
config
  cli hidden
  tech-support test-commands encrypted password <unique_encrypted_password>
  logging disable eventid 10171
  logging disable eventid 10638
  logging disable eventid 12822
  logging disable eventid 12987
  license key "\
<SecGW_license_key>"
 system hostname <ASR9k_hostname>-<SecGW#>
  autoconfirm
  orbem
     no siop-port
     no iiop-port
  #exit
  require session recovery
  context local
     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> len <length>
     ssh key <unique_encrypted_ssh_key2> len <length> type v2-rsa
     ssh key <unique_encrypted_ssh_key3> len <length> type v2-dsa
     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
   ca-certificate name ca-cert-tls \
  pem data \
"-----BEGIN CERTIFICATE-----\n\
<certificate-data>
-----END CERTIFICATE-----"
   task facility mmedemux mmemgr-startup-percentage 90
mmemgr-startup-wait-time 600
   #exit
   #exit
   context srp
      service-redundancy-protocol
         hello-interval 3
         configuration-interval 60
         dead-interval 15
         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
   context wsg
     ip access-list acl1
        permit ip <wsg_acl1_permit1_IPv4-address_mask>
<wsg_acl1_permit1_IPv4-address_mask> protocol <IPv4-address_mask>
        permit ip <wsg_acl1_permit2_IPv4-address_mask>
<wsg_acl1_permit2_IPv4-address_mask> protocol <IPv4-address_mask>
        permit ip <wsg_acl1_permit3_IPv4-address_mask>
<wsg_acl1_permit3_IPv4-address_mask> protocol <IPv4-address_mask>
        permit ip <wsg_acl1_permit4_IPv4-address_mask>
<wsg_acl1_permit4_IPv4-address_mask> protocol <IPv4-address_mask>
        permit ip <wsg_acl1_permit5_IPv4-address_mask>
<wsg_acl1_permit5_IPv4-address_mask> protocol <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_acl1_permit4_IPv6-address_mask>
<wsg_acl1_permit4_IPv6-address_mask>
        permit ip <wsg_acl1_permit5_IPv6-address_mask>
<wsg_acl1_permit5_IPv6-address_mask>
     #exit
     ip pool <IPv4_pool_name> range <wsg_pool1_IPv4-address/mask>
<wsg_pool2_IPv4-address_mask> public <pool_priority>
     ip pool <IPv4_pool_name> range <wsg_pool2_IPv4-address/mask>
<wsg_pool2_IPv4-address_mask> public <pool_priority>
     ipv6 pool <IPv6_pool_name> prefix <wsg_pool1_IPv6-address/mask>
public<pool_priority>
     ipsec transform-set ipsec-ts-1
     #exit
     ikev2-ikesa transform-set ike-ts-1
     #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
     #exit
     crypto template ipv6 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 ipv6 match childsa match ipv6
         ip-address-alloc dynamic
         ipsec transform-set 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 ike
       ip address <wsg_interface_ike_IPv4-address>
       ipv6 address <wsg_interface_ike_IPv6-address> secondary
     #exit
```

```
        interface ike-loop loopback
          ip address <wsg_interface_ike-loop_IPv4-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-access
        #exit
        wsg-service ipv4-s2s
          deployment-mode site-to-site
          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_clear1_IPv4-address_mask> <wsg_iproute_clear1_IPv4-address>
    clear
        ip route <wsg_iproute_ike1_IPv4-address mask> <wsg_iproute_ike1_IPv4-address> ike

        ip route <wsg_iproute_clear2_IPv4-address_mask> <wsg_iproute_clear2_IPv4-address>
    clear
        ip route <wsg_iproute_clear3_IPv4-address_mask> <wsg_iproute_clear3_IPv4-address>
    clear
        ip route <wsg_iproute_clear4_IPv4-address_mask> <wsg_iproute_clear4_IPv4-address>
    clear
        ip route <wsg_iproute_clear5_IPv4-address_mask> <wsg_iproute_clear5_IPv4-address>
    clear
        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 clear
        ipv6 route <wsg_iproute_clear3_IPv6-address/mask>
   <wsg_iproute_clear3_nexthop_IPv6-address> interface clear
        ipv6 route <wsg_iproute_ike2_IPv6-address/mask>
   <wsg_iproute_ike2_nexthop_IPv6-address> interface 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_clear4_IPv6-address/mask>
```

```
<wsg_iproute_clear4_nexthop_IPv6-address> interface clear
     ipv6 route <wsg_iproute_clear5_IPv6-address/mask>
<wsg_iproute_clear5_nexthop_IPv6-address> interface clear
     ipv6 route <wsg_iproute_ike3_IPv6-address/mask>
<wsg_iproute_ike3_nexthop_IPv6-address> interface 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 sri-route <wsg_sri-route_IPv4-address>
next-hop<wsg_sri-route_nexthop_IPv4-address> interface ike
     ip rri-route network-mode L3 <wsg_rri-route_network-mode_IPv4-address>
next-hop<wsg_rri-route_network-mode_nexthop_IPv4-address> interface clear
   #exit
   connectedapps
     sess-userid root
     sess-passwd encrypted password <unique_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
   port ethernet 1/11
     no shutdown
     vlan <port_1/11_vlan_id_wsg>
       no shutdown
       bind interface clear wsg
     #exit
     vlan <port_1/11_vlan_id_srp>
       no shutdown
       bind interface icsr srp
     #exit
   #exit
end
```

SecGW VM Configuration - Backup ASR 9000 Chassis

```
  config
   cli hidden
   tech-support test-commands encrypted password <unique_encrypted_password>
   license key "\
<SecGW_license_key>"
   system hostname <ASR9k_hostname>-<SecGW#>
   autoconfirm
   orbem
      no siop-port
      no iiop-port
   #exit
   crash enable encrypted url <encrypted_url>
   require session recovery
   context local
     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> len <length>
      ssh key <unique_encrypted_ssh_key2> len <length> type v2-rsa
      ssh key <unique_encrypted_ssh_key3> len <length> type v2-dsa
     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
   ca-certificate name ca-cert-tls \
  pem data \
"-----BEGIN CERTIFICATE-----\n\
<certificate-data>
-----END CERTIFICATE-----"
   task facility mmedemux mmemgr-startup-percentage 90
mmemgr-startup-wait-time 600
   #exit
   #exit
   context srp
     service-redundancy-protocol
       hello-interval 3
       configuration-interval 60
       dead-interval 15
       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
   context wsg
     ip access-list acl1
      permit ip <wsg_acl1_permit1_IPv4-address_mask> <wsg_acl1_permit1_IPv4-address_mask>
 protocol <IPv4-address_mask>
      permit ip <wsg_acl1_permit2_IPv4-address_mask> <wsg_acl1_permit2_IPv4-address_mask>
 protocol <IPv4-address_mask>
      permit ip <wsg_acl1_permit3_IPv4-address_mask> <wsg_acl1_permit3_IPv4-address_mask>
 protocol <IPv4-address_mask>
      permit ip <wsg_acl1_permit4_IPv4-address_mask> <wsg_acl1_permit4_IPv4-address_mask>
 protocol <IPv4-address_mask>
      permit ip <wsg_acl1_permit5_IPv4-address_mask> <wsg_acl1_permit5_IPv4-address_mask>
 protocol <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_acl1_permit4_IPv6-address_mask>
<wsg_acl1_permit4_IPv6-address_mask>
        permit ip <wsg_acl1_permit5_IPv6-address_mask>
<wsg_acl1_permit5_IPv6-address_mask>
     #exit
     ip pool <IPv4_pool_name> range <wsg_pool1_IPv4-address/mask>
<wsg_pool2_IPv4-address_mask> public <pool_priority>
     ipv6 pool <IPv6_pool_name> prefix <wsg_pool1_IPv6-address/mask>
public<pool_priority>
     ipsec transform-set ipsec-ts-1
```

```
  #exit
  ikev2-ikesa transform-set ike-ts-1
  #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
  #exit
  crypto template ipv6 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 ipv6 match childsa match ipv6
      ip-address-alloc dynamic
      ipsec transform-set 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 ike
    ip address <wsg_interface_ike_IPv4-address>
    ipv6 address <wsg_interface_ike_IPv6-address> secondary
  #exit
  interface ike-loop loopback
    ip address <wsg_interface_ike-loop_IPv4-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-s2s
       deployment-mode site-to-site
       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_clear1_IPv4-address_mask> <wsg_iproute_clear1_IPv4-address>
 clear
     ip route <wsg_iproute_ike1_IPv4-address mask> <wsg_iproute_ike1_IPv4-address> ike

     ip route <wsg_iproute_clear2_IPv4-address_mask> <wsg_iproute_clear2_IPv4-address>
 clear
     ip route <wsg_iproute_clear3_IPv4-address_mask> <wsg_iproute_clear3_IPv4-address>
 clear
     ip route <wsg_iproute_clear4_IPv4-address_mask> <wsg_iproute_clear4_IPv4-address>
 clear
     ip route <wsg_iproute_clear5_IPv4-address_mask> <wsg_iproute_clear5_IPv4-address>
 clear
     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 clear
     ipv6 route <wsg_iproute_clear3_IPv6-address/mask>
<wsg_iproute_clear3_nexthop_IPv6-address> interface clear
     ipv6 route <wsg_iproute_ike2_IPv6-address/mask>
<wsg_iproute_ike2_nexthop_IPv6-address> interface 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_clear4_IPv6-address/mask>
<wsg_iproute_clear4_nexthop_IPv6-address> interface clear
     ipv6 route <wsg_iproute_clear5_IPv6-address/mask>
<wsg_iproute_clear5_nexthop_IPv6-address> interface clear
     ipv6 route <wsg_iproute_ike3_IPv6-address/mask>
<wsg_iproute_ike3_nexthop_IPv6-address> interface 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 sri-route <wsg_sri-route_IPv4-address>
next-hop<wsg_sri-route_nexthop_IPv4-address> interface ike
     ip rri-route network-mode L3 <wsg_rri-route_network-mode_IPv4-address>
next-hop<wsg_rri-route_network-mode_nexthop_IPv4-address> interface clear
   #exit
   connectedapps
```

```
     sess-userid root
     sess-passwd encrypted password <unique_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
   port ethernet 1/11
     no shutdown
     vlan <port_1/11_vlan_id_wsg>
       no shutdown
       bind interface clear wsg
     #exit
     vlan <port_1/11_vlan_id_srp>
       no shutdown
       bind interface icsr srp
     #exit
   #exit
end
```

CHAPTER 9

ASR 9000 SecGW without Connectedapps-OnePk

This chapter provides configuration support for ASR 9000 SecGW handling of Inter chassis WSG-Service High Availability and Reverse Route Injection without using Connectedapps-onePK communication. Connectedapps is SecGW function and OnePK is a supervisor function.

For more information on OnePK, refer *IOS-XR Guide*.

L2 Interchassis HA Configuration without Connectedapps - OnePK

Configuration Overview

This section 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 without connectedapps – OnePK usage.

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 when 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, operator should configure one-to-one mapping between StarOS VMs across active/standby VSMs in different ASR 9000 chassis.

Table 14: Recommended Mapping of Interchassis StarOS VMs

Active VSM	Standby VSM
VM1-SecGW1	VM1-SecGW1
VM2-SecGW2	VM2-SecGW2
VM3-SecGW3	VM3-SecGW3

Active VSM	Standby VSM
VM4-SecGW4	VM4-SecGW4

Each VM is monitored through SRP and each Chassis is monitored through HSRP configurations and BGP is used for Chassis to VM communication.

How Chassis Failover Happens

When an ASR 9000 interface in RSP goes down, a BGP notification is sent from that RSP to its SecGW stating the same. Immediately, SecGW will sends SRP HELLO packet to its SecGW peer with its state changed to "ActivePendingStandby" from "Active". When standby SecGW receives the hello packet it becomes New Active and sends HELLO response with its state changed from "standby" to "Active".

ASR 9000 Chassis RSP Configuration (IOS-XR)

This section provides sample RSP configuration for chassis failover (active) without OnePK.

```
.
.
.
router bgp 20
 bfd minimum-interval 150
 bfd multiplier 3
 bgp router-id 2.2.2.1
 address-family ipv4 unicast
  maximum-paths ebgp 2
 !
 neighbor 172.27.54.12
  remote-as 220
  bfd fast-detect
  description SecGW1-clear
  address-family ipv4 unicast
   route-policy pass-all in
   route-policy pass-all out
   soft-reconfiguration inbound always
.
.
.
 neighbor 172.27.54.44
  remote-as 220
  bfd fast-detect
  description SecGW2-ike
  address-family ipv4 unicast
   route-policy pass-all in
   route-policy pass-all out
   soft-reconfiguration inbound always
.
.
.
router hsrp
 interface BVI1871
  hsrp delay minimum 1 reload 240
  address-family ipv4
   hsrp 3 version 2
    timers msec 300 1
    preempt
    priority 100
    address 172.27.54.35
    track object WsgIPsla
```

```
.
.
.
 interface BVI1881
  hsrp delay minimum 1 reload 240
  address-family ipv4
   hsrp 1 version 2
    timers msec 300 1
    preempt
    priority 100
    address 172.27.54.3
    track object WsgIPsla
.
.
.
```

ASR 9000 Backup Chassis Configuration

This section provides sample RSP configuration for chassis failover (standby) without OnePK.

```
.
.
.
router bgp 20
 bfd minimum-interval 150
 bfd multiplier 3
 bgp router-id 2.2.2.2
 address-family ipv4 unicast
  maximum-paths ebgp 2
.
.
.
 neighbor 172.27.54.13
  remote-as 220
  bfd fast-detect
  description SecGW2-clear
  address-family ipv4 unicast
   route-policy pass-all in
   route-policy pass-all out
   soft-reconfiguration inbound always
.
.
.
 neighbor 172.27.54.45
  remote-as 220
  bfd fast-detect
  description SecGW1-ike
  address-family ipv4 unicast
   route-policy pass-all in
   route-policy pass-all out
   soft-reconfiguration inbound always
.
.
.
router hsrp
 interface BVI1871
  hsrp delay minimum 1 reload 240
  address-family ipv4
   hsrp 3 version 2
    timers msec 300 1
    preempt
    priority 100
    address 172.27.54.35
    track object WsgIPsla
```

```
.
.
.
 interface BVI1881
  hsrp delay minimum 1 reload 240
  address-family ipv4
   hsrp 1 version 2
    timers msec 300 1
    preempt
    priority 100
    address 172.27.54.3
    track object WsgIPsla
.
.
.
```

SecGW1 Configuration on Active Chassis

This section provides sample SecGW configuration for VM failover (active) without OnePk.

```
.
.
.
    router bgp 220
      neighbor 172.27.54.33 remote-as 20
      neighbor 172.27.54.33 timers keepalive-interval 1 holdtime-interval 3
      neighbor 172.27.54.33 fall-over bfd
      no neighbor 172.27.54.33 capability graceful-restart
      neighbor 172.27.54.1 remote-as 20
      neighbor 172.27.54.1 timers keepalive-interval 1 holdtime-interval 3
      neighbor 172.27.54.1 fall-over bfd
      no neighbor 172.27.54.1 capability graceful-restart
      address-family ipv4
        neighbor 172.27.54.33 distribute-list PermitLoopbackEncr out
        neighbor 172.27.54.1 distribute-list DenyInRoutes in
        neighbor 172.27.54.1 distribute-list PermitLoopbackClr out
      #exit
.
.
.
    service-redundancy-protocol
.
.
.
      monitor bgp context wsg 172.27.54.33 group 3
      monitor bgp context wsg 172.27.54.1 group 1
.
.
.
```

SecGW1 Configuration on Standby Chassis

This section provides sample SecGW configuration for VM failover (standby) without OnePK.

```
.
.
.
    router bgp 220
      neighbor 172.27.54.34 remote-as 20
      neighbor 172.27.54.34 timers keepalive-interval 1 holdtime-interval 3
      neighbor 172.27.54.34 fall-over bfd
      no neighbor 172.27.54.34 capability graceful-restart
      neighbor 172.27.54.2 remote-as 20
      neighbor 172.27.54.2 timers keepalive-interval 1 holdtime-interval 3
      neighbor 172.27.54.2 fall-over bfd
      no neighbor 172.27.54.2 capability graceful-restart
      address-family ipv4
        neighbor 172.27.54.34 distribute-list PermitLoopbackEncr out
        neighbor 172.27.54.2 distribute-list DenyInRoutes in
        neighbor 172.27.54.2 distribute-list PermitLoopbackClr out
      #exit
.
.
.
      bfd multihop-peer 172.27.54.106 interval 250 min_rx 250 multiplier 3
    #exit
    service-redundancy-protocol
.
.
.
      monitor bgp context wsg 172.27.54.34 group 3
      monitor bgp context wsg 172.27.54.2 group 1
.
.
.
```

RRI workaround without ConnectedApps – OnePK

Reverse route injection can be replaced with static route configuration in RSP. This way, downlink packets will be appropriately routed from RSP to the corresponding SecGW VM.

Sample `show route output`

Show Output displays RRI installed routes.

```
#show route ipv4 application
a    160.0.0.3/32 [254/641547737] via 172.27.54.17, 05:49:20
a    160.0.0.4/32 [254/641547737] via 172.27.54.17, 05:49:20


Sample Static Route configuration replacing RRI:
router static
 address-family ipv4 unicast
  160.0.0.0/29 172.27.54.17
```

CHAPTER 10

Pre-Tunnel Fragmentation

SecGW supports post-tunnel fragmentation for IPsec ESP data packets. If an encrypted packet exceeds an interface MTU size the packet is fragmented. Post-tunnel fragmentation can cause performance degradation and pre-tunnel fragmentation has better packet processing rate.

The following sections provide more detailed information:

Pre-Tunnel fragmentation at ASR 9000 XR

XR already supports fragmentation at interface level. SecGW in ASR 9000 has the advantage of using the XR functionality because the packets are always forwarded via XR.

The MTU size can be configured at the VSM interface used for clear traffic. The MTU size should be the PMTU of the encrypted network subtracted by the outer IP header size and crypto overhead (which is up to 100 bytes). If PMTU of the encrypted network is 1400 then the VSM clear interface MTU size must be 1300 for pre-tunnel fragmentation to work.

Configuration

The below configuration at XR enables Pre-Tunnel Fragmentation feature.

To enable the feature configure the MTU size in VSM interface used for clear traffic in XR. The MTU size is calculated by subtracting 100 bytes (overhead for encryption) from the PMTU size of the encrypted network.

```
interface TenGigE0/1/1/1
 description "CLEAR Interface"
 mtu 500    ----------------------- if PMTU is 600
 ipv4 address 79.79.79.14 255.255.255.0
 ipv6 address 2001:79:79:79::14/64
 !
```

CHAPTER 11

ACL Based Load Balancing Support

With this release ACL Based Load Balancing Support is introduced in SecGW. SecGW runs as a vPC-SI instance on Virtualized Services Module (VSM) card in ASR9K chassis. Each chassis can have multiple VSM cards running separate SecGW instances (separate IPs). So it becomes important to have a single virtual IP for SecGW and a load balancing solution to distribute the load across VSMs. Also, with 4VM approach (introduced in 17.1 for performance improvement), each VSM runs 4 different SecGW instances (vPC-SI instances). This makes the load balancing solution even more valuable for the SecGW.

The solution allows us to configure a single virtual IP for all SecGW instances in a chassis. ACL Based Load Balancing feature distributes the load and packets for each tunnel are directly forwarded to the particular SecGW instance to achieve better throughput.

The following sections provide more detailed information:

ABF based Load Balancing at ASR 9000

XR already supports ABF (ACL based forwarding) at interface level. ACL needs to be applied at the interface level in INGRESS direction and it is applicable for both control and data traffic (Upstream). It allows configuration of multiple ACL rules with different priorities. These rules can be applied at the interface level to forward the packet via a specific physical interface. Please refer ASR 9000 user guide for more detail on ABF.

This rule can be used to have a source based forwarding for SecGW. Traffic from a set of peers can be forwarded to a particular SecGW instance supporting a static load balancing.

ABF based load balancing is static load balancing. Load from one peer always goes to a particular SecGW. There are chances of one SecGW getting loaded compared to others. Also there might be some impact on the overall throughput in a fully loaded chassis in future releases where single VM approach is planned with 30Gbps traffic.

Memory and Performance Impact

On Typhoon Line Card(LC) we expect 40% impact with small packets (64B) on fully loaded ports (assuming the ports running 10G traffic). But minimum impact on Tomahawk LC.

This impact is again based on number of ACLs configured. We can configure around 50K ACLs per interface. The impact will be seen if the numbers are in 1000s. If the rules are in 10s and 100s, the impact is not much. It is assumed that with 10s, there will not be any impact, and with 100s, it will be very minimal.

ACL Based Load Balancing Configuration

Use the below configuration to enable ACL Based Load Balancing.

To enable the feature configure the ACL rules under an access-list. The rules can be designed based on the deployment (peers and how the distribution should be). For e.g. below, packets from peers 1.0.0.0 are handled by VSM1-VM1 and 1.0.0.1 are handled by VSM1-VM2, etc.

```
      ipv4 access-list acl1
     10 permit ipv4 1.0.0.0 255.255.255.252 any nexthop1 ipv4 192.168.5.2
 --> VSM1-VM1
     20 permit ipv4 1.0.0.1 255.255.255.252 any nexthop1 ipv4 192.168.6.2
 --> VSM1-VM2
     40 permit ipv4 1.0.0.2 255.255.255.252 any nexthop1 ipv4 192.168.7.2
 --> VSM2-VM1
     40 permit ipv4 1.0.0.3 255.255.255.252 any nexthop1 ipv4 192.168.8.2
 --> VSM2-VM2
      ..........
      !
      interface TenGigE0/0/0/0 --> external physical ike int
      ipv4 address 192.173.0.7 255.255.0.0
      ipv4 access-group acl1 ingress!
      ..........
      !
      interface TenGigE0/2/1/0 --> forge ike int for VSM1-VM1
      ipv4 address 192.168.5.1 255.255.255.0
      ..........
      !
      interface TenGigE0/2/4/0 --> forge ike int for VSM1-VM2
      ipv4 address 192.168.6.1 255.255.255.0
      ..........
      !
      interface TenGigE0/3/1/0 --> forge ike int for VSM2-VM1
      ipv4 address 192.168.7.1 255.255.255.0
      ..........
      !
      interface TenGigE0/3/4/0 --> forge ike int for VSM2-VM2
      ipv4 address 192.168.8.1 255.255.255.0
```

CHAPTER 12

Sub Second Inter Chassis Failover

SecGW support 3 modes of ICSR (intra chassis L2, inter chassis L2 ICSR and inter chassis L3 ICSR). based on the type of failure and ICSR mode.

BFD permits much more aggressive detection time compared to existing SRP protocols. This BFD monitoring is already implemented and integrated with SRP, which can be used in SecGW to reduce the SecGW switchover time to 1-3 seconds. This section will explain the configuration details for different modes.

The BFD configuration can be done for single-hop and multi-hop SRP links. In an L2 setup, the SRP link can be part of same network so a single hop configuration is valid. And for rest of the cases, a multi-hop BFD configuration needs to be used.

Single-hop config example:

```
context srp
    bfd-protocol
    #exit
    service-redundancy-protocol
      hello-interval 3
      configuration-interval 60
      dead-interval 15
      checkpoint session duration non-ims-session 30
      route-modifier threshold 10
      priority 10
      monitor bfd context srp 71.71.71.5 chassis-to-chassis
      monitor hsrp interface BVI1871 afi-type IPv4 hsrp-group 4
      peer-ip-address 71.71.71.5
      bind address 71.71.71.4
    #exit
    interface icsr
      ip address 71.71.71.4 255.255.255.0
      bfd interval 50 min_rx 50 multiplier 3
    #exit
    subscriber default
    exit
    aaa group default
    #exit
```

```
        ip route static bfd  icsr 71.71.71.5
      #exit
```

Multi Hop Config Example

```
context srp
    bfd-protocol
      bfd multihop-peer 81.81.81.4 interval 50 min_rx 50 multiplier 3
    #exit
    service-redundancy-protocol
      hello-interval 3
      configuration-interval 60
      dead-interval 15
      checkpoint session duration non-ims-session 30
      route-modifier threshold 10
      priority 10
      monitor bfd context srp 81.81.81.4 chassis-to-chassis
     monitor hsrp interface GigabitEthernet0/0/0/5 afi-type IPv4 hsrp-group 4
      peer-ip-address 81.81.81.4
      bind address 71.71.71.4
    #exit
    interface ifSRP
      ip address 71.71.71.4 255.255.255.0
    #exit
    ip route static multihop bfd  mbfd 71.71.71.4 81.81.81.4
    ip route 81.81.81.0 255.255.255.0 71.71.71.5 ifSRP
    #exit
  #exit
```

HSRP Switchover Improvement

Below are the changes to improve the HSRP Switchover:

- Bridge together the external and VSM interfaces for all the paths (ike and clear).
- Configure SRP activated loopback interfaces in both SecGWs and assign address from the same network (The loopback address will be up only in active SecGW.).
- Add RRI routes with nexthop as the loopback address.
- For encrypted traffic, forward the packets towards the loopback address from L2-Switch. This makes sure the packets are always forwarded to the chassis where SRP is active even if HSRP is not.
- For clear traffic, forward the packets towards the hsrp address from L2-Switch as the RRI routes are added in chassis (not forwarded to L2 switch). If SecGW is not active in that chassis (SRP-HSRP not in sync), packets will be forwarded towards the other chassis (towards the loopback address).

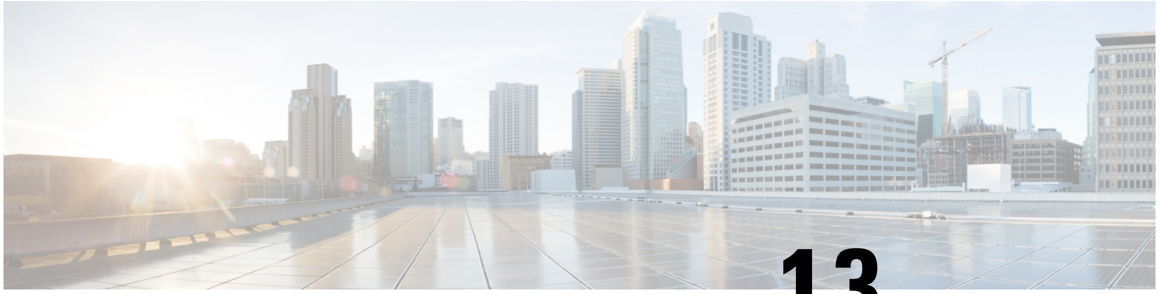
ASR9K RSP configuration example

```
interface GigabitEthernet0/0/0/5
        transceiver permit pid all
        dot1q tunneling ethertype 0x9200
      !
interface GigabitEthernet0/0/0/5.1259 l2transport
 description “External port for SRP Traffic”
 encapsulation dot1q 1259
 rewrite ingress tag pop 1 symmetric
!
interface GigabitEthernet0/0/0/18
 transceiver permit pid all
 dot1q tunneling ethertype 0x9200
!
interface GigabitEthernet0/0/0/18.1871 l2transport
 description "External port for IKE and ESP Traffic"
 encapsulation dot1q 1871
 rewrite ingress tag pop 1 symmetric
!
interface GigabitEthernet0/0/0/19
 transceiver permit pid all
 dot1q tunneling ethertype 0x9200
!
interface GigabitEthernet0/0/0/19.1881 l2transport
 description “External port for Clear Traffic”
 encapsulation dot1q 1881
 rewrite ingress tag pop 1 symmetric
!
interface TenGigE0/5/1/0
!
interface TenGigE0/5/1/0.1871 l2transport
 description “VSM port for IKE and ESP Traffic”
 encapsulation dot1q 1871
 rewrite ingress tag pop 1 symmetric
!
interface TenGigE0/5/1/1
!
interface TenGigE0/5/1/1.1259 l2transport
 description “VSM port for SRP Traffic”
 encapsulation dot1q 1259
 rewrite ingress tag pop 1 symmetric
!
interface TenGigE0/5/1/1.1881 l2transport
 description “VSM port for Clear Traffic”
 encapsulation dot1q 1881
 rewrite ingress tag pop 1 symmetric
!
interface BVI1259
 description “BVI for SRP Traffic”
 ipv4 address 71.71.71.9 255.255.255.0
!
interface BVI1871
 description “BVI for IKE and ESP Traffic”
 ipv4 address 187.0.1.12 255.255.255.0
 ipv6 address 1871::12/64
!
interface BVI1881
 description “BVI for Clear Traffic”
 ipv4 address 188.0.1.12 255.255.255.0
 ipv6 address 1881::12/64
!
       router static
        address-family ipv4 unicast
        35.35.35.35/32 187.0.1.20
       #exit
l2vpn
 bridge group secgw
  bridge-domain ike
   interface TenGigE0/5/1/0.1871
   !
   interface GigabitEthernet0/0/0/18.1871
   !
   routed interface BVI1871
  !
  bridge-domain srp
   interface TenGigE0/5/1/1.1259
   !
   interface GigabitEthernet0/0/0/5.1259
   !
   routed interface BVI1259
  !
  bridge-domain clear
   interface TenGigE0/5/1/1.1881
   !
   interface GigabitEthernet0/0/0/19.1881
   !
   routed interface BVI1881
  !
 !
!
```

SecGW Configuration Example

```
context wsg
  …….. 
  interface clear    —————————————> VSM Clear interface
    ip address 188.0.1.10 255.255.255.0
  #exit
  interface clear-active loopback    —————————————> Clear interface active SecGW only
    ip address 188.0.1.20 255.255.255.255 srp-activate
  #exit
  interface ike    —————————————> VSM IKE and ESP interface
    ip address 187.0.1.10 255.255.255.0
  #exit
  interface ike-active loopback    —————————————> IKE and ESP interface active SecGW only

    ip address 187.0.1.20 255.255.255.255 srp-activate
  #exit
  interface ike-loop loopback    —————————————> ipv4 SecGW ip
    ip address 35.35.35.35 255.255.255.255 srp-activate
  #exit
  interface ike-loop-v6 loopback    —————————————> ipv6 SecGW ip
    ipv6 address 2035::35/128 srp-activate
  #exit
  wsg-service ipv4
    deployment-mode site-to-site
    ip access-group acl1
    bind address 35.35.35.35 crypto-template foo
  #exit
  wsg-service ipv6
    deployment-mode site-to-site
    ipv6 access-group acl1
    bind address 2035::35 crypto-template foo-1
  #exit
  ip route 65.65.0.0 255.255.0.0 188.0.1.100 clear
  ip route 92.0.0.0 255.0.0.0 187.0.1.11 ike
  ip rri next-hop 188.0.1.20 interface clear-active
#exit
context srp
  bfd-protocol
  #exit
  service-redundancy-protocol
           hello-interval 3
           configuration-interval 60
           dead-interval 15
           checkpoint session duration non-ims-session 30
           route-modifier threshold 10
           priority 10
    monitor bfd context srp 71.71.71.5 chassis-to-chassis
    monitor hsrp interface BVI1871 afi-type IPv4 hsrp-group 4
    peer-ip-address 71.71.71.5
    bind address 71.71.71.4
  #exit
  interface icsr
    ip address 71.71.71.4 255.255.255.0
    bfd interval 50 min_rx 50 multiplier 3
  #exit
  ip route static bfd  icsr 71.71.71.5
#exit
port ethernet 1/10
  no shutdown
  vlan 1871
    no shutdown
    bind interface ike wsg
  #exit
#exit
port ethernet 1/11
  no shutdown
  vlan 1259
    no shutdown
    bind interface icsr srp
  #exit
  vlan 1881
    no shutdown
    bind interface clear wsg
  #exit
#exit
```



CHAPTER 13

S-GW Paging Enhancements

Feature Description

S-GW Paging includes the following scenarios:

Scenario 1: S-GW sends a DDN message to the MME/S4-SGSN nodes. MME/S4-SGSN responds to the S-GW with a DDN Ack message. While waiting for the DDN Ack message from the MME/S4-SGSN, if the S-GW receives a high priority downlink data, it does not resend a DDN to the MME/S4-SGSN.

Scenario 2: If a DDN is sent to an MME/S4-SGSN and TAU/RAU MBR is received from another MME/S4-SGSN, S-GW does not send DDN.

Scenario 3: DDN is sent to an MME/S4-SGSN and DDN Ack with Cause #110 is received. DDN Ack with cause 110 is treated as DDN failure and standard DDN failure action procedure is initiated.

To handle these scenarios, the following two enhancements have been added to the DDN functionality:

- High Priority DDN at S-GW
- MBR-DDN Collision Handling

These enhancements support the following:

- Higher priority DDN on S-GW and SAEGW, which helps MME/S4-SGSN to prioritize paging.
- Enhanced paging KPI and VoLTE services.
- DDN message and mobility procedure so that DDN is not lost.
- MBR guard timer, which is started when DDN Ack with temporary HO is received. A new CLI command **ddn temp-ho-rejection mbr-guard-timer** has been introduced to enable the guard timer to wait for MBR once the DDN Ack with cause #110 (Temporary Handover In Progress) is received.
- TAU/RAU with control node change triggered DDNs.

In addition to the above functionality, to be compliant with 3GPP standards, support has been enhanced for Downlink Data Notification message and Mobility procedures. As a result, DDN message and downlink data which triggers DDN is not lost. This helps improve paging KPI and VoLTE success rates in scenarios where DDN is initiated because of SIP invite data.

Licensing

This is a license-controlled feature. Contact your Cisco account or support representative for detailed licensing information.

How It Works

This section describes working of these features related to S-GW Paging.

High Priority DDN at S-GW

High Priority DDN at S-GW

1. S-GW sends a Downlink Data Notification message to the MME/S4-SGSN node for which it has control plane connectivity for the given UE.
2. The MME/S4-SGSN responds to the S-GW with a Downlink Data Notification Ack message.
3. The S-GW, while waiting for the user plane to be established, might send a second Download Data Notification based on the priority of received data. The following table lists the cases when it will happen.
4. The following table lists different scenarios with different DDN priorities and the action taken by the S-GW.

Table 15: DDN Priority Scenarios

Scenario	Action Taken by S-GW Action Taken by S-GW Prior This Feature	Action Taken by S-GW Action Taken by S-GW Post This Feature
ARP Priority of second bearer is higher than the first bearer on which first DDN was sent.	No DDN was sent.	Sends DDN message with higher priority to the MME/S4-SGSN.
ARP Priority of second bearer is higher than the first bearer on which first DDN was sent.	Buffers these downlink data packets and the does not send a new DDN. However, separate Paging DDN is always sent out and this restriction does not apply to it.	Buffers these downlink data packets and the does not send a new DDN. However, separate Paging DDN is always sent out and this restriction does not apply to it.
S-GW has sent the second DDN message indicating higher priority and receives extra downlink data packets for this UE.	Buffers these downlink data packets and the does not send a new DDN.	Buffers these downlink data packets and the does not send a new DDN.

Important Separate paging is always sent.

MBR-DDN Collision Handling

The following table lists different MBR-DDN collision scenarios and action taken by S-GW to handle these scenarios:

Table 16: MBR-DDN Collision Handling Scenarios

Scenario	Action Taken by S-GW Action Taken by S-GW Prior This Feature	Action Taken by S-GW Action Taken by S-GW Post This Feature
DDN is sent to an MME/S4-SGSN and TAU/RAU MBR is received from another MME/S4-SGSN without any data TEIDs.	No DDN was sent.	DDN is triggered to this new control node as part of mobility handover process.
DDN is sent to an MME/S4-SGSN and DDN Ack with Cause #110 is received.	DDN Ack with cause 110 is treated as DDN failure and standard DDN failure action procedure is initiated.	S-GW starts a guard timer and wait for TAU/RAU MBR from the new MME/S4-SGSN. The timer is stopped if any MBR or DDN failure indication is received. But, if none of them is received, and the timer expires all buffered downlink data packets are flushed. If this is followed by mobility handover without any data TEIDs, DDN is resent to this new control node as well.
MBR received with bearer context to be removed.	There is a possibility that DDN could be sent with EBIs corresponding to bearers marked for deletion.	Bearers marked for deletion are not included in any of the DDN messages.

Limitations

High Priority DDN at S-GW

This section lists the limitations for High Priority DDN at S-GW feature.

1. High Priority DDN is always enabled whenever the license is available.
2. High priority DDN is sent only once. Any further higher priority data does not trigger another DDN.
3. DDN delay timer and DDN throttling is not applicable to High Priority DDN.
4. Separate Paging DDN is always sent out and above restriction does not apply to it.
5. No-user-connect behavior restarts the moment high priority DDN is sent out.

MBR-DDN Collision Handling

This section lists the limitations for MBR-DDN Collision Handling feature.

1. EBI of a bearer marked for removal is not sent in any of the DDN messages.
2. TAU/RAU triggered DDN is sent only once and is never reattempted even if aborted due to the collision of MBR with DDN at the S-GW Ingress.
3. DDN delay and throttling are not applicable to the TAU/RAU triggered DDN.
4. No-user-connect behavior restarts the moment high priority DDN is sent out.
5. High Priority DDN is not sent if high priority downlink data is received:
    - After DDN Ack with Cause #110 is received
    - Before any MBR is received
6. Separate paging IE is not supported for TAU/RAU triggered DDN.
7. If DDN Ack with cause #110 is received and then later a downlink packet matches the configured 3-tuple of "Separate Paging", then also "Separate Paging DDN" is not sent as the UE is undergoing handoff.
8. The MBR guard timer is not restarted when the DDN Ack with cause #110 is received while the MBR guard timer is running.

Configuring High Priority DDN Interaction Feature

Operators can use this CLI command to enable guard timer to wait for MBR once the DDN Ack with cause #110 (Temporary Handover In Progress) is received.

Configuring mbr-guard-timer

This CLI sets the guard timer to wait for a MBR when DDN Ack with Cause #110 temp-ho-rejection) is received.

If the guard timer expires and if no MBR of any type or DDN Failure Indication is received, all the buffered downlink data is flushed out and paging flags are reset.

If the guard timer is running and any MBR is received, the timer is stopped and no further action is taken.

If the guard timer is running and DDN Failure Indication is received, the timer is stopped and standard DDN failure action is taken.

By default, this CLI command is always enabled.

```
configure
   context context_name
     sgw-service service_name
       ddn temp-ho-rejection mbr-guard-timer time_in_seconds
       { no | default } ddn temp-ho-rejection mbr-guard-timer
       end
```

Notes:

- **no:** Disables the guard timer.
- **default:** Enables the guard timer and sets it to the default value, 60 seconds.

- **temp-ho-rejection:** Action to be taken when peer node indicates temporary rejection of paging due to handover-in-progress.
- **mbr-guard-timer:** Sets the guard timer for a MBR when DDN Ack with Cause #110 (temp-ho-rejection) is received. When the timer expires, S-GW flushes all the buffered downlink data packets. The range of this timer is from 60 seconds to 300 seconds. Default timer value is 60 seconds.

Verifying the Configuration

The configuration of this feature can be verified using the following commands from the `exec` mode:

- **show sgw-service statistics all**
- **show sgw-service [name <service-name> | all]**
- **show saegw-service statistics all function sgw**

See the section Monitoring and Troubleshooting High Priority DDN Interaction Feature, on page 177 for the command output.

Monitoring and Troubleshooting High Priority DDN Interaction Feature

The following section describes commands available to monitor and troubleshoot "High Priority DDN" & "DDN-MBR Collision Handling" Features .

Show Commands for High Priority DDN Interaction Feature

show sgw-service [name <service-name> | all]

This CLI is enhanced to show the MBR-guard-timer configuration which can be a value between "60-300 Seconds" when enabled OR "Disabled". The MBR-guard-timer is started when a DDN Ack with Temporary-HO-Rejection (Cause #110) is received.

Important If the MBR-guard-timer is disabled, DDN Ack with Temporary-HO-Rejection is treated as DDN Failure Indication.

This command displays the following output:

```
show sgw-service name sgw-srv
Service name                      : sgw-srv
  Service-Id                      : 18
  Context                         : ingress
  Accounting context              : ingress
  Accounting gtpp group           : default
  Accounting mode                 : Gtpp
  Accounting stop-trigger         : Default
  Status                          : STARTED
  Egress protocol                 : gtp-pmip
```

```
Ingress EGTP service          : egtp-sgw-ingress
Egress context                : ingress
Egress EGTP service           : egtp-sgw-egress
Egress MAG service            : n/a
IMS auth. service             : n/a
Peer Map                      : n/a
Access Peer Map               : n/a
Accounting policy             : n/a
Newcall policy                : n/a
Internal QOS Application      : Backward-compatible
QCI-QOS mapping table         : n/a
Event Reporting               : Disabled
DDN Throttling                : Disabled
Page UE for PGW initiated proc: Disabled
Temp-Failure Handling for DBR proc: Disabled
PGW Ctrl FTEID in Relocation Create Session Response: Enabled
...
....
ddn success-action no-user-connect ddn-retry-timer: 60
ddn failure-action pkt-drop-time: 300
ddn isr-sequential-paging delay-time: 10
MBR Guard Timer for DDN Ack with Temporary-HO-Rejection: 60-300 seconds/Disabled

Idle timeout                  : n/a
PLMN ID List                  : Not defined
Subscriber Map Name: smap
SAEGW service                 : saegw
EGTP NTSR: Disabled
 Session Hold Timer: n/a
   Timeout: n/a

GTP-C Load Control Profile        : Not Defined
GTP-C Overload Control Profile    : Not Defined
```

show sgw-service statistics all

This CLI command has been enhanced to show the following:

- Number of times 'High Priority Paging' is triggered and number of times it could not be triggered as it was already sent. This shows data corresponding to only S-GW service(s) which is part of SAEGW service(s).
- Number of times DDN Ack with a cause #110 is received and number of times TAU/RAU MBR with control node change triggers a DDN automatically.
- Number of packets and bytes discarded when MBR-guard-timer expires; this timer is started when a DDN Ack with Temporary-HO-Rejection (Cause #110) is received.
- This CLI shows data only corresponding to standalone sgw-service(s).

This command displays the following output:

```
show sgw-service statistics all
…
…
Paging Statistics:
  Requests:                             3   Success :                           2
  Rejects:                              1   Failures:                           0
  UE State Transitions:
    Idle-to-Active:                     0   Active-to-Idle:                     1
  Data Statistics Related To Paging:
    Packets Buffered:                 3    Bytes Buffered:                  15
    Packets Discarded:                9    Bytes Discarded:                 45
    Idle Mode ACL Statistics:
      Packets Discarded:              0    Bytes Discarded:                  0

  Data Discarded By Reason-Type:
    Shared Buffer Full:
      Packets Discarded:              0    Bytes Discarded:                  0
    Dedicated Buffer Full:
      Packets Discarded:              0    Bytes Discarded:                  0
    S1U State Inactive:
      Packets Discarded:              0    Bytes Discarded:                  0
    Paging Throttled:
      Packets Discarded:              0    Bytes Discarded:                  0
    Paging Failure:
      Packets Discarded:              9    Bytes Discarded:                 45
    No User Connect Data Flushed:
      Packets Discarded:              0    Bytes Discarded:                  0
    MBR Guard Timer Expiry Flushed Data:
      Packets Discarded:          0    Bytes Discarded:                  0
    Buffered Data Flushed:
      Packets Discarded:              0    Bytes Discarded:                  0

   High Priority Paging Statistics:
     Initiated:                   1    Suppressed:                       1

   Handover Paging Statistics:
     DDN Ack with Temporary-HO-Rejection (Cause #110):                   0
     TAU/RAU MBR Triggered DDN:                                          1
 …
…
```

show saegw-service statistics all function sgw

This CLI is enhanced to show the following:

- Number of times 'High Priority Paging' was triggered and number of times it could not be as it was already sent.
- Number of times DDN Ack with a cause #110 is received and number of times TAU/RAU MBR with control node change triggers a DDN automatically.
- Data only corresponding to the S-GW service(s) which is associated with a SAEGW service(s).
- Number of packets and bytes discarded when MBR-guard-timer expires; this timer is started when a DDN Ack with Temporary-HO-Rejection (Cause #110) is received
- Number of packets and bytes discarded when MBR-guard-timer expires; this timer is started when a DDN Ack with Temporary-HO-Rejection (Cause #110) is received
- Packets/Bytes dropped due to MBR-guard-timer expiry are not shown for collapsed calls.

Important Paging packets dropped statistics are not incremented for collapsed calls and hence the newly added counter of "MBR Guard timer Expiry Flushed Data" is also not updated in that case.

This command displays the following output:

```
 show saegw-service statistics all function sgw
Paging Statistics:
  Requests:                            3    Success :                          2
  Rejects:                             1    Failures:                          0
  UE State Transitions:
    Idle-to-Active:                    0    Active-to-Idle:                    1

  Data Statistics Related To Paging:
    Packets Buffered:                  3    Bytes Buffered:                   15
    Packets Discarded:                 9    Bytes Discarded:                  45
    Idle Mode ACL Statistics:
      Packets Discarded:               0    Bytes Discarded:                   0

  Data Discarded By Reason-Type:
    Shared Buffer Full:
      Packets Discarded:               0    Bytes Discarded:                   0
    Dedicated Buffer Full:
      Packets Discarded:               0    Bytes Discarded:                   0
    S1U State Inactive:
      Packets Discarded:               0    Bytes Discarded:                   0
    Paging Throttled:
      Packets Discarded:               0    Bytes Discarded:                   0
    Paging Failure:
      Packets Discarded:               9    Bytes Discarded:                  45
    No User Connect Data Flushed:
      Packets Discarded:               0    Bytes Discarded:                   0
    MBR Guard Timer Expiry Flushed Data:
      Packets Discarded:               0    Bytes Discarded:                   0
    Buffered Data Flushed:
    Packets Discarded:               0    Bytes Discarded:                   0

    High Priority Paging Statistics:
      Initiated:                         1    Suppressed:                        1

    Handover Paging Statistics:
      DDN Ack with Temporary-HO-Rejection (Cause #110):                          0
      TAU/RAU MBR Triggered DDN:                                                 1
```

CHAPTER 14

Config Payload extension for DHCP Address

This feature when implemented supports INTERNAL_IP4_DHCP, INTERNAL_IP6_DHCP as part of Configuration Attributes in Auth payloads. This instructs the host to send any internal DHCP requests to the address contained within the attribute. Multiple DHCP servers may be requested. SecGW may respond with zero or more DHCP server addresses.

Config Payload Extension for DHCP Address Configuration

Assumptions and Limitations

- In current release only 3 dhcp addresses per INTERNAL_IP4_DHCP or INTERNAL_IP6_DHCP requests will be supported.
- The DHCP addresses will be configured as part of wsg-service. 3 ipv4 and 3 ipv6 dhcp server addresses will be allowed per service.

Server dhcp

Specifies the dhcp server addresses to be sent to the peer in authentication response.

Product

SecGW (WSG)

Privilege

Security Administrator

Command Modes

Exec > Global Configuration > Context Configuration > WSG-Service Configuration

configure > **context** *context_name* > **wsg-service** *service_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-wsg-service)#
```

Syntax Description

```
server dhcp { ipv4 ipv4_address [ IP-ADDRESS | IP-ADDRESS ] | ipv6  ipv6_address
 [ IPv6-ADDRESS | IPv6-ADDRESS ] }
no server dhcp { ipv4 [ ipv6 ] | ipv6 [ ipv4 ] }
```

no

Deletes the specified parameter.

ipv4_address

Specifies the ipv4 address of the dhcp-server to be sent to the peer. The IPV4 address should be in the format ##.##.##.## which is the first ipv4 dhcp-server's address.

IP-ADDRESS

Specifies ipv4 address of the dhcp-server to be sent to the peer.

ipv6_address

Specifies the ipv6 address of the dhcp-server to be sent to the peer. The IPV6 address should be in the format ####:####:####:####:####:####:####:#### (IPv6 also supports :: notation).

IPv6-ADDRESS

Specifies ipv6 address of the dhcp-server to be sent to the peer.

Usage Guidelines

This command specifies the dhcp server addresses to be sent to the peer in authentication response

Example

The following command specifies the dhcp server ipv4 addresses to be sent to the peer in authentication response:

```
server dhcp ipv4 123.234.345.567
```

Config Payload extension for DHCP Address Support Show Command Outputs

As part of " Config Payload extension for DHCP Address " feature below show commands output are introduced:

Show wsg-Service all Server:

- DHCP: ipv4 : <##.##.##.## > or NA(if not configured)

  <##.##.##.## >

  <##.##.##.## >

- ipv6 : < #:#:#:#:#:#:#:#> or NA(if not configured)

  <##.##.##.## >

  <##.##.##.## >

Show Configuration:

- server dhcp ipv4 <v4 address> <v4 address> <v4 address> <cr>
- server dhcp ipv6 <v6 address> <v6 address> <v6 address> <cr>

CHAPTER 15

SecGW TLS Support

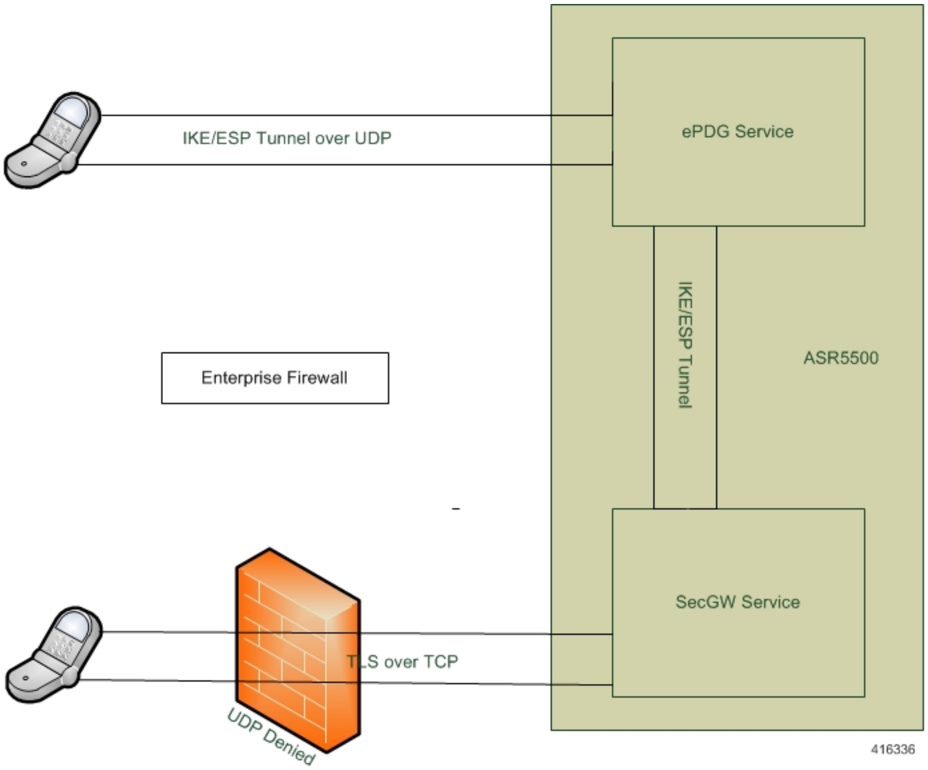
This feature enables Secure Socket Layer (SSL) based connection endpoints in SecGW. Earlier only IKE/IPSEC based connection endpoints were supported in SecGW.

This support is added to facilitate UE in the enterprise networks to connect with security where the IKEv2 UDP ports are blocked and only TCP based connections are permitted.

SecGW TLS Support

SecGW TLS support enables peer devices to connect securely to SecGw using TLS/TCP based connections. The application data which is received on the TLS/TCP is IKE/ESP data which will be IP/UDP encapsulated and forwarded to local ePDG service. This will help UE penetrate enterprise firewalls while connecting to ePDG.

Figure 15: `SecGW accessesing ePDG using TLS over TCP`



Assumptions and Limitations

- Only TLS/TCP data can be IP/UDP encapsulated and forwarded to local ePDG service
- It is possible that UE can send the IKE/ESP over SSL as application data
- IKE protocol is UDP encapsulated. But for this feature the IKE/ESP should be part for SSL data which is TCP based connection
- Ports supported for TLS/TCP connection is configurable in wsg-service
- TLS/TPC should be used as a fallback only when UDP is blocked in the firewall
- From SecGW point of view, network side is ePDG
- The SecGW supports both IKEv2/IPSec based as well SSL based connections simultaneously
- SecGW can be authenticated by UE based on a X.509 certificate. This is optional in TLS
- SSL should be used to provide data security between UE and SecGW
- SSL and TCP protocol stacks has been implemented at SecGW to support the authentication and connection security requirements

SecGW TLS Support Configuration

Product

Binds the WSG service to the specified IPv4 or IPv6 address and crypto template (VPC only).

Product

SecGW (WSG)

Privilege

Security Administrator

Command Modes

Exec > Global Configuration > Context Configuration > WSG-Service Configuration

configure > **context** *context_name* > **wsg-service** *service_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-wsg-service)#
```

Syntax Description

```
bind address IPv4 / IPv6  crypto-template template_name | Secure-tunnel [
Max-sessions  sessions ]
no bind address
```

no

Unbinds the WSG service from the IP address.

IPv4 / IPv6

IPV4 ##.##.##.## or IPV6 ####:####:####:####:####:####:####:#### (IPV6 also supports :: notation).

template_name

Specifies the name of an existing crypto template as an alphanumeric string of 0 through 127 characters.

Usage Guidelines

Bind the WSG service to an IPv4 or IPv6 address.

Example

The following command binds the WSG service to 10.1.1.1.

```
bind address 10.1.1.1 crypto template tplt01
```

Show Command Changes

As part of " TLS Support " feature below show commands output are introduced:

show wsg-service all

Secure tunnel parameters:

- Param 1
  - Protocol
  - Port

    - SSL template
    - WSG Application

- Param 1
    - Protocol
    - Port
    - SSL template
    - WSG Application

show configuration

- secure-tunnel protocol <type> port <port-num> ssl-template <template-name> wsg-application app1
- secure-tunnel protocol <type> port <port-num> ssl-template <template-name> wsg-application <application-name>
- bind address 176.0.10.167 secure-tunnel

show ssl statistics

WSG SSL Data Stats:

- Total Packets Rcvd from Nw:
- Total Bytes Rcvd from Nw:
- Total Packets Sent to User:
- Total Bytes Sent to User:
- Total Packets Rcvd from User:
- Total Bytes Rcvd from User:
- Total Packets Sent to Nw:
- Total Bytes Sent to Nw:

show ssl statistics

WSG TCP Data Stats:

- Total Buffer Rcvd from Nw:
- Total Bytes Rcvd from Nw:
- Total Buffer Sent to User:
- Total Bytes Sent to User:
- Total Buffer Rcvd from User :
- Total Bytes Rcvd from User:
- Total Buffer Sent to Nw:

- Total Bytes Sent to Nw:

show subscriber all

- USERNAME

show wsg-application

Displays wsg-application information.

Product

SecGW (WSG)

Privilege

Security Administrator, Administrator, Operator

Command Modes

Exec

The following prompt is displayed in the Exec mode:

`[local]host_name#`

Syntax Description

```
show wsg-application ( all | name | application_name [ counter ] [ | {
grep grep_options | more } ] | statistics [ all ] [ name ] [ | { grep grep
 options | more } ] }
```

all

Displays information for all configured application

name *application_name*

Displays specific application. Must be followed by application name which is a string of size 1 through 63.

counter

Displays information for all configured application.

statistics

Displays information for all configured application.

[| { grep *grep options* | more }] }

Pipes (sends) the output of the command to the command specified. You must specify a command to which the output will be sent. For details on the usage of the grep and more commands, refer to the Regulating a Command's Output section of the Command Line Interface Overview chapter.

Usage Guidelines

Use this command to display wsg-application information.

Example

The following example displays information for all configured application:

```
show wsg-application statistics
```

CHAPTER 16

Authorization based on Certificate fields

This feature enables to authorize peer while IKEv2 tunnel establishment in case of SecGW product while using Certificate based authentication method.

Feature Description

Authorization of peer will be based on match of CN field in peer's certificate with list of configured allowed entries.

Assumptions and Limitations

- CN part will be such a way that it matches fully with one of the configured value.
- All peers are provided with the same Certificate or some set of known certificates. Hence CN will be same (or set of CN's) and will be limited in exclusive numbers. One such configuration can match all peers using said certificate.
- This feature is not applicable for non-certificate authentication method.
- Only 64 entries can be configured under one cert-policy and one cert-policy can be attached to one crypto template used for SecGW service.

Configuring Authorization based on Certificate fields

Use the following configuration to configure Authorization based on Certificate fields.

certificate policy

```
config
   context context_name
       [ no ]  certificate policy   ert-policy_name
          end
```

id

```
config
   context context_name
       [ no ]  id  id
        id  id_value  match-criteria { common-name value comm-name_val  |
domain-name value dom_name_value }
         end
```

Performance Indicator Changes

Below are the show commands outputs added as part of this feature to support Authorization based on Certificate fields:

show crypto ikev2-ikesa certificate policy

Crypto Cert Policy Name cert_test

- ID 1 Match-Type common-name Match-Value wsg0@cisco.com
- ID 2 Match-Type common-name Match-Value wsg1@cisco.com
- ID 3 Match-Type common-name Match-Value wsg2@cisco.com

Crypto Cert Policy Name cert_test1

- ID 2 Match-Type common-name Match-Value wsg1@cisco.com

Crypto Cert Policy Name test

- ID 1 Match-Type common-name Match-Value wsg_test@cisco.com

show config

ikev2-ikesa certificate policy cert_test1

- id 2 match-criteria common-name value wsg1@cisco.com

ikev2-ikesa certificate policy cert_test

- id 1 match-criteria common-name value wsg0@cisco.com
- id 2 match-criteria common-name value wsg1@cisco.com
- id 2 match-criteria common-name value wsg1@cisco.com

crypto template template-name ikev2-dynamic

- ikev2-ikesa cert-policy cert_test

Bulkstats

Below fields are added for Certificate Authentication Statistics:

- Authorisation policy failure

CHAPTER 17

SecGW Support for EAP-MD5

Feature Description

SecGW uses RADIUS interface between AAA and SecGW for EAP-MD5 authentication of IPSec peer. Radius protocol is used between AAA Server and SecGW. SecGW will act as EAP-pass-through only.

Assumptions and Limitation

- The implementation will be valid only for SecGW RAS mode.
- EAP payload will not be validated only header will be validated.
- The prefix in Idi payload, which decides the EAP-Type to be performed for authentication is out of scope for this feature. As there is no prefix digit assigned to it, it will be decided by mutual agreement between SecGW peer (like FAP) and AAA server.

Configuring SecGW Support for EAP-MD5

Use the following configuration to configure SecGW Support for EAP-MD5.

associate subscriber-map *subscriber-map_name*

```
config
   context context_name
       wsg-service  service_name
           associate subscriber-map   subscriber_map_name
         end
```

Performance Indicator Changes

Below are the show commands outputs added as part of this feature SecGW Support for EAP-MD5:

show crypto stats ikev2:

EAP-MD5:

- Current: Failure:
- Attempt: Success:

Existing Show command outputs significant to EAP-MD5 feature:

show wsg-service stats

- Auth failure:

show radius counters all

- Access-Request Sent:
- Access-Challenge Received:
- Access-Accept Received:
- Access-Reject Received:

CHAPTER 18

IP Address stickiness for FAP

This feature allows to preserve allocated internal IP address for configured timer after tunnel tear down. Also helps to allocate same IP if new tunnel from same peer attaches within configured time.

Feature Description

If IPsec tunnel tear down happens and when a new tunnel is created with same peer, usually new IP gets allocated each time. With this in some case, there in-occurs a need to reconfigure peer's environment. In order to avoid such scenario**,** preservation of allocated internal IP is suggested for some configured timer.

IP preservation is with respect to WSG RAS mode only. IP Address Stickiness is not required for S2s mode.

IPv6 allocated IP will not be preserved and is out of scope of this feature.