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 2
- Create Access Control Lists. See Access Control Lists, on page 4
- Enable and configure one or more WSG services. See WSG Service Configuration, on page 5
- Configure required IPSec features. See IPSec Configuration, on page 13

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 7.

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).