

Security Gateway as Initiator

This chapter describes how to configure a Security Gateway (SecGW) running on an ASR 9000 Virtualized Services Module (VSM) as an initiator of an IKEv2 session.

This chapter includes the following sections:

- Overview, on page 1
- Configuring SecGW as Initiator, on page 2
- Verifying the SecGW as Initiator Configuration, on page 3

Overview

By default SecGW (WSG service) only responds to a setup request for an IKEv2 session. However, an SecGW can also be configured to initiate an IKEv2 session setup request when the peer does not initiate a setup request within a specified time interval.

Important This functionality is only applicable for site-to-site (S2S) based tunnels within a WSG service. For remote access tunnels the peer is always the initiator.

Responder-Initiator Sequence

The following is the general event sequence for an SecGW acting as an initiator.

1. The SecGW waits for the peer to initiate a tunnel within a configurable time interval during which it is in responder mode. The default responder mode interval is 10 seconds.
2. Upon expiry of the responder mode timer, the SecGW switches to initiator mode for a configurable time interval. The default initiator mode interval is 10 seconds.
3. The SecGW retries the call if there is no response from the peer during the initiator mode interval.
4. When the SecGW is in initiator mode and the peer does not respond to the IKE messages or fails to establish the call, SecGW reverts to responder mode and waits for the peer to initiate the IKEv2 session.
5. If call creation is successful, the SecGW stops initiating any further calls to that peer.
6. If the SecGW and peer initiate a session call simultaneously (possible collision), the SecGW defers to the peer initiated call and drops any incoming packets.

When the SecGW as initiator feature is enabled, the SecGW only supports up to 1,000 peer addresses. This restriction is applied when configuring a crypto peer list. See Create a crypto peer-list, on page 2.

Limitations

The following limitations apply when the SecGW as initiator feature is enabled:

- The SecGW will only support up to 1,000 peers. This restriction is applied when configuring a crypto peer list.
- SecGW will not support the modification of an IPv4/IPv6 peer list on the fly (call sessions in progress). The modification will be allowed only after all the calls are removed.

The SecGW does support wild card peer address provisioning along with subnets.

Configuring SecGW as Initiator

The following is the general sequence for configuring this feature:

- Create a crypto peer-list, on page 2.
- Configure the Peer List in the WSG Service, on page 2.
- Configure Initiator Mode and Responder Mode Durations, on page 3.

See the *Command Line Interface Reference* for complete information about the commands described below.

Create a crypto peer-list

The CLI command sequence for creating a crypto peer list is shown below.

```
configure
  context context_name
    crypto peer-list { ipv4 | ipv6 } peer_list_name
      address peer_address
      exit
```

Notes:

- *peer_list_name* is specified as an alphanumeric string of 1 through 32 characters.
- Running the **crypto peer-list** command moves you to the Peer List Configuration mode where you have access to the **address** command.
- Repeat the **address** *peer_address* command to add up to 1,000 peer IP addresses. The IP addresses in the list can only be entered in either IPv4 or IPv6 notation, depending on the address type specified when the list was created.
- Use the **no address** *peer_address* command to remove a peer address from the peer list.

Configure the Peer List in the WSG Service

The following CLI command sequence configures the previously created peer list for use in the WSG service.

```
configure
  context wsg_ctxt_name
    wsg-service wsg_service_name
      peer-list peer_list_name
      exit
```

Notes:

- *peer_list_name* must have been previously configured as described in Create a crypto peer-list, on page 2.
- Use the **no peer-list** command to remove the peer-list and disable the SecGW as initiator feature.
- Any changes made to a WSG service require that the service must be restarted to apply any changed parameters. You restart the service by unbinding and binding the IP address to the service context.

Configure Initiator Mode and Responder Mode Durations

When a peer list has been configured in the WSG service, the initiator and responder mode timer intervals each default to 10 seconds. The SecGW will wait for 10 seconds in the responder mode for a peer session initiation request before switching to the initiator mode and waiting 10 seconds for a peer response.

You can change the default settings for the initiator and/or responder mode intervals using the following CLI command sequence.

```
configure
   context wsg_ctxt_name
      wsg-service wsg_service_name
         initiator-mode-duration seconds
         responder-mode-duration seconds
         exit
```

Notes:

- *seconds* is an integer from 5 through 250.

Restrictions

The following restrictions apply when configuring an SecGW as an Initiator:

- The **peer-list** *peer_list_name* command is only executed if the deployment mode for WSG service is **site-to-site**, and the bind address matches with the peer list address type (IPv4 or IPv6).
- You cannot change the WSG service deployment-mode if **peer-list** *peer_list_name* is enabled under the service. You will be prompted to remove the peer list before changing the mode.
- A maximum of 1,000 peer IP addresses can be added to the peer list via the Peer List Configuration mode **address** command.
- WSG service address binding is not allowed if a peer list is configured and both address types do not match. An error message is generated if they do not match.
- An IPv4 or IPv6 peer list cannot be modified if **peer-list** *peer_list_name* is enabled under the WSG service.

Verifying the SecGW as Initiator Configuration

Run the **show wsg-service** CLI command to display the current crypto peer list configuration. A sample output of this command appears below.

```
show wsg-service all
Service name: wsg1
  Context: wsg
  ...
  peer list : peer01
```

```
Initiator mode duration : 10 seconds
Responder mode duration : 10 seconds
```