Service Configurations

This chapter describes how to configure various StarOS services to support IPSec.

The following topics are discussed:

FA Services Configuration to Support IPSec

This section provides instructions for configuring FA (Foreign Agent) services to support IPSec. It assumes that the FA service was previously configured and system is ready to serve as an FA.

Important This section provides the minimum instruction set for configuring an FA service to support IPSec on the system. For more information on commands that configure additional parameters and options, see the *Command Line Interface Reference*.

To configure the FA service to support IPSec:

Step 1 Modify FA service configuration by following the steps in Modifying FA Service to Support IPSec, on page 2.

Step 2 Verify your FA service configuration by following the steps in Verifying the FA Service Configuration with IPSec, on page 2.

Step 3 Save your configuration to flash memory, an external memory device, and/or a network location using the Exec mode command **save configuration**. For additional information on how to verify and save configuration files, refer to the *System Administration Guide* and the *Command Line Interface Reference*.

Modifying FA Service to Support IPSec

Use the following example to modify FA service to support IPSec on your system:

```
configure
   context ctxt_name
      fa-service fa_svc_name
      isakmp peer-ha ha_address crypto-map map_name [ secret preshared_secret ]
      isakmp default crypto-map map_name [ secret preshared_secret ]
      end
```

Notes:

- *ctxt_name* is the system context in which the FA service is configured to support IPSec.
- *fa_svc_name* is name of the FA service for which you are configuring IPSec.
- *ha_address* is IP address of the HA service to which FA service will communicate on IPSec.
- *map_name* is name of the preconfigured ISAKMP or a manual crypto map.
- A default crypto map for the FA service to be used in the event that the AAA server returns an HA address that is not configured as an ISAKMP peer HA.
- For maximum security, the default crypto map should be configured in addition to peer-ha crypto maps instead of being used to provide IPSec SAs to all HAs. Note that once an IPSec tunnel is established between the FA and HA for a particular subscriber, all new Mobile IP sessions using the same FA and HA are passed over the tunnel regardless of whether or not IPSec is supported for the new subscriber sessions. Data for existing Mobile IP sessions is unaffected.

Verifying the FA Service Configuration with IPSec

Enter the following Exec mode command for the appropriate context to display and verify your FA service configuration:

```
show fa-service { name service_name | all }
```

The output of this command is a concise listing of FA service parameter settings.

HA Service Configuration to Support IPSec

This section provides instructions for configuring HA (Home Agent) services to support IPSec. It assumes that the HA service was previously configured and system is ready to serve as an HA.

Important This section provides the minimum instruction set for configuring an HA service to support IPSec on the system. For more information on commands that configure additional parameters and options, see the *Command Line Interface Reference*.

To configure the HA service to support IPSec:

Step 1 Modify HA service configuration by following the steps in Modifying HA Service to Support IPSec, on page 3.

Step 2 Verify your HA service configuration by following the steps in Verifying the HA Service Configuration with IPSec, on page 3.

Step 3 Save your configuration to flash memory, an external memory device, and/or a network location using the Exec mode command **save configuration**. For additional information on how to verify and save configuration files, refer to the *System Administration Guide* and the *Command Line Interface Reference*.

Modifying HA Service to Support IPSec

Use the following example to modify an existing HA service to support IPSec on your system:

```
configure
   context ctxt_name
      ha-service ha_svc_name
         isakmp aaa-context aaa_ctxt_name
         isakmp peer-fa fa_address crypto-map map_name [ secret preshared_secret ]
         end
```

Notes:

- *ctxt_name* is the system context in which the FA service is configured to support IPSec.
- *ha_svc_name* is name of the HA service for which you are configuring IPSec.
- *fa_address* is IP address of the FA service to which HA service will communicate on IPSec.
- *aaa_ctxt_name* name of the context through which the HA service accesses the HAAA server to fetch the IKE S Key and S Lifetime parameters.
- *map_name* is name of the preconfigured ISAKMP or a manual crypto map.

Verifying the HA Service Configuration with IPSec

Enter the following Exec mode command for the appropriate context to display and verify your HA service configuration:

```
show ha-service { name service_name | all }
```

The output of this command is a concise listing of HA service parameter settings.

PDSN Service Configuration for L2TP Support

PDSN service configuration is required for compulsory tunneling and optional for attribute-based tunneling.

For attribute-based tunneling, a configuration error could occur such that upon successful authentication, the system determines that the subscriber session requires L2TP but can not determine the name of the context in which the appropriate LAC (L2TP Access Concentrator) service is configured from the attributes supplied. As a precautionary, a parameter has been added to the PDSN service configuration options that will dictate the name of the context to use. It is strongly recommended that this parameter be configured.

This section contains instructions for modifying the PDSN service configuration for either compulsory or attribute-based tunneling.

These instructions assume that the PDSN service was previously configured and system is ready to serve as a PDSN.

This section provides the minimum instruction set for configuring an L2TP service on the PDSN system. For more information on commands that configure additional parameters and options, refer to the Command Line Interface Reference.

To configure the PDSN service to support L2TP:

Step 1 Modify PDSN service to configure compulsory tunneling or attribute-based tunneling by applying the example configuration in any of the following sections:

- Modifying PDSN Service to Support Attribute-based L2TP Tunneling, on page 4
- Modifying PDSN Service to Support Compulsory L2TP Tunneling, on page 5

Step 2 Verify your LAC service configuration by following the steps in Verifying the PDSN Service Configuration for L2T, on page 5.

Step 3 Save your configuration to flash memory, an external memory device, and/or a network location using the Exec mode command **save configuration**. For additional information on how to verify and save configuration files, refer to the *System Administration Guide* and the *Command Line Interface Reference*.

Modifying PDSN Service to Support Attribute-based L2TP Tunneling

Use the following example to modify an existing PDSN service to support attribute-based L2TP tunneling on your system:

```
configure
   context ctxt_name
      pdsn-service pdsn_svc_name
         ppp tunnel-context lac_ctxt_name
         end
```

Notes:

- *ctxt_name* is the destination context where the PDSN service is configured.
- *pdsn_svc_name* is name of the PDSN service for which you are configuring attribute-based L2TP tunneling.
- *lac_ctxt_name* is the name of the destination context where the LAC service is located.
- Refer to for additional information on RADIUS/Subscriber attributes.

RADIUS and Subscriber Attributes for L2TP Application IPSec Support

The table below lists the RADIUS and Subscriber attributes required to support IPSec for use with attribute-based L2TP tunneling.

These attributes are contained in the following dictionaries:

- Starent
- Starent-835

Table 1: Subscriber Attributes for IPSec encrypted L2TP Support

RADIUS Attribute	Local Subscriber Attribute	Description	Variable
SN1-Tunnel-ISAKMP-Crypto-Map	tunnel l2tp crypto-map	The name of a crypto map configured on the system.	A salt-encrypted ASCII string specifying the crypto-map to use for this subscriber. It can be tagged, in which case it is treated as part of a tunnel group.
SN1 -Tunnel-ISAKMP-Secret	tunnel l2tp crypto-map isakmp-secret	The pre-shared secret that will be used as part of the D-H exchange to negotiate an IKE SA.	A salt-encrypted string specifying the IKE secret. It can be tagged, in which case it is treated as part of a tunnel group.

Modifying PDSN Service to Support Compulsory L2TP Tunneling

Use the following example to modify an existing PDSN service to support compulsory L2TP tunneling on your system:

```
configure
   context ctxt_name
      pdsn-service pdsn_svc_name
         ppp tunnel-context lac_ctxt_name
         ppp tunnel-type l2tp
         end
```

Notes:

- *ctxt_name* is the destination context where the PDSN service is configured.
- *pdsn_svc_name* is name of the PDSN service for which you are configuring attribute-based L2TP tunneling.
- *lac_ctxt_name* is the name of the destination context where the LAC service is located.

Verifying the PDSN Service Configuration for L2T

Enter the following Exec mode command for the appropriate context to display and verify your PDSN service with L2TP configuration:

```
show pdsn-service name service_name
```

The output of this command is a concise listing of PDSN service parameter settings configured on the system.

LAC Service Configuration to Support IPSec

This section provides instructions for configuring LAC (L2TP Access Concentrator) services to support IPSec.

Important These instructions are required for compulsory tunneling. They should only be performed for attribute-based tunneling if the Tunnel-Service-Endpoint, the SN1-Tunnel-ISAKMP-Crypto-Map, or the SN1 -Tunnel-ISAKMP-Secret are not configured in the subscriber profile.

These instructions assume that the LAC service was previously configured and system is ready to serve as an LAC server.

Important This section provides the minimum instruction set for configuring an LAC service to support IPSec on the system. For more information on commands that configure additional parameters and options, refer to the *Command Line Interface Reference*.

To configure the LAC service to support IPSec:

Step 1 Modify LAC service configuration by following the steps in Modifying LAC service to Support IPSec, on page 6.

Step 2 Verify your LAC service configuration by following the steps in Verifying the LAC Service Configuration with IPSec, on page 7.

Step 3 Save your configuration to flash memory, an external memory device, and/or a network location using the Exec mode command **save configuration**. For additional information on how to verify and save configuration files, refer to the *System Administration Guide* and the *Command Line Interface Reference*.

Modifying LAC service to Support IPSec

Use the following example to modify an existing LAC service to support IPSec on your system:

```
configure
   context ctxt_name
      lac-service lac_svc_name
        peer-lns ip_address [encrypted] secret secret [crypto-map map_name {
[encrypted] isakmp-secret secret } ] [ description text ] [ preference integer
 ]
        isakmp aaa-context aaa_ctxt_name
        isakmp peer-fa fa_address crypto-map map_name [ secret preshared_secret ]
        end
```

Notes:

- *ctxt_name* is the destination context where the LAC service is configured to support IPSec.
- *lac_svc_name* is name of the LAC service for which you are configuring IPSec.
- *lns_address* is IP address of the LNS node to which LAC service will communicate on IPSec.

- *aaa_ctxt_name* name of the context through which the HA service accesses the HAAA server to fetch the IKE S Key and S Lifetime parameters.
- *map_name* is name of the preconfigured ISAKMP or a manual crypto map.

Verifying the LAC Service Configuration with IPSec

Enter the following Exec mode command for the appropriate context to display and verify your LAC service with IPSec configuration:

show lac-service name *service_name*

The output of this command is a concise listing of LAC service parameter settings configured on the system.

APN Template Configuration to Support L2TP

This section provides instructions for adding L2TP support for APN templates configured on the system.

These instructions assume that the APN template was previously configured on this system.

Important This section provides the minimum instruction set for configuring an APN template to support L2TP for APN. For more information on commands that configure additional parameters and options, refer to the *Command Line Interface Reference*.

To configure the APN to support L2TP:

Step 1 Modify preconfigured APN template by following the steps in Modifying an APN Template to Support L2TP, on page 7.

Step 2 Verify your APN configuration by following the steps in Verifying the APN Configuration for L2TP, on page 8.

Step 3 Save your configuration to flash memory, an external memory device, and/or a network location using the Exec mode command **save configuration**. For additional information on how to verify and save configuration files, refer to the *System Administration Guide* and the *Command Line Interface Reference*.

Modifying an APN Template to Support L2TP

Use the following example to modify APN template to support L2TP:

```
configure
  context ctxt_name
    apn apn_name
      tunnel l2tp [ peer-address lns_address [ [ encrypted ] secret l2tp_secret
 ] [ preference num ] [ tunnel-context tunnel_ctxt_name ] [ local-address
agw_ip_address ] [ crypto-map map_name { [ encrypted ] isakmp-secret crypto_secret
 } ]
       end
```

Notes:

- *ctxt_name* is the system context in which the APN template is configured.
- *apn_name* is name of the preconfigured APN template in which you want to configure L2TP support.
- *lns_address* is the IP address of the LNS node with which this APN will communicate.
- *tunnel_ctxt_name* is the L2TP context in which the L2TP tunnel is configured.
- *agw_ip_address* is the local IP address of the GGSN in which this APN template is configured.
- *map_name* is the preconfigured crypto map (ISAKMP or manual) which is to use for L2TP.

Verifying the APN Configuration for L2TP

Enter the following Exec mode command for the appropriate context to display and verify your APN L2TP configuration:

show apn name *apn_name*

The output of this command contains a concise listing of LT2P settings configured for the specified APN.

WSG Service Configuration to Support IPSec

This section provides an overview of the process for enabling a WSG service with a crypto template supporting IPSec features. WSG service must be enabled to support a Security Gateway (SecGW) running on an ASR 9000 router equipped with a Virtualized Services Module (VSM).

For additional information refer to the *Security Gateway Administration Guide*.

Creating a Crypto Template to Support a SecGW

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 for a SecGW may require 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.

Creating a WSG Service

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

```
config
   context context_name
   wsg-service service_name
      bind address ip_address crypto-template template_name
      deployment-mode { remote-access | site-to-site }
      ip { access-group acl_list_name | address pool name pool_name
      ipv6 { access-group acl_list_name | address prefix-pool pool_name
      pre_fragment mtu size
```

The following command sequence sets the lookup priority:

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

For additional information, see the *WSG-Service Configuration Mode Commands* and the *WSG Lookup Priority List Configuration Mode* chapters of the *Command Line Interface Reference*.

Verifying WSG Service Creation

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** – Displays the priority levels, as well source an destination netmasks for all configured lookup priorities.
- **show wsg-service** – Displays information about all WSG services or a specified service. It also displays statistics for a specified WSG service or peer address.