Security Gateway Overview

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

The following topics are covered in this chapter:

Product Overview

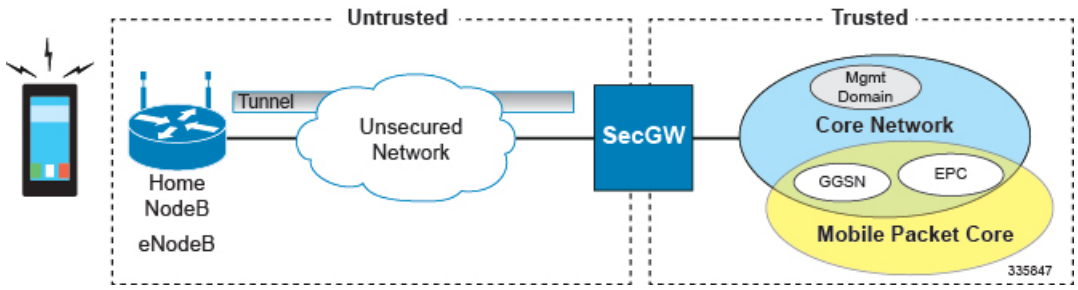
The SecGW is a high-density IP Security (IPSec) gateway for mobile wireless carrier networks. It is typically used to secure backhaul traffic between the Radio Access Network (RAN) and the operator core network.

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 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



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.

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

IPSec Capabilities

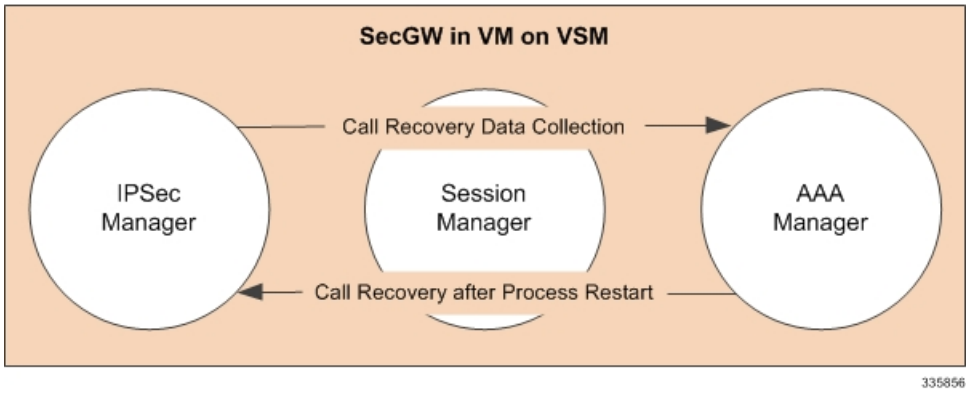
The following IPSec features are supported by StarOS for implementation in an SecGW application:

- Anti Replay
- Certificate Management Protocol (CMPv2)
- Session Recovery
- Support for IKE ID Type
- PSK support with up to 255 octets
- Online Certificate Status Protocol (OCSP)
- Blacklist/Whitelist by IDi
- Rekey Traffic Overlap
- CRL fetching with LDAPv3
- Sequence Number based Rekey
- PSK Support for up to 1000 Remote Secrets
- Certificate Chaining
- RFC 5996 Compliance
- Duplicate Session Detection
- Extended Sequence Number
- Support to provide DNS server address to the Peer

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 2: Process Recovery Diagram



Network Deployment

SecGW supports the following network deployment scenarios:

- Remote Access Tunnels, on page 3

Remote Access Tunnels

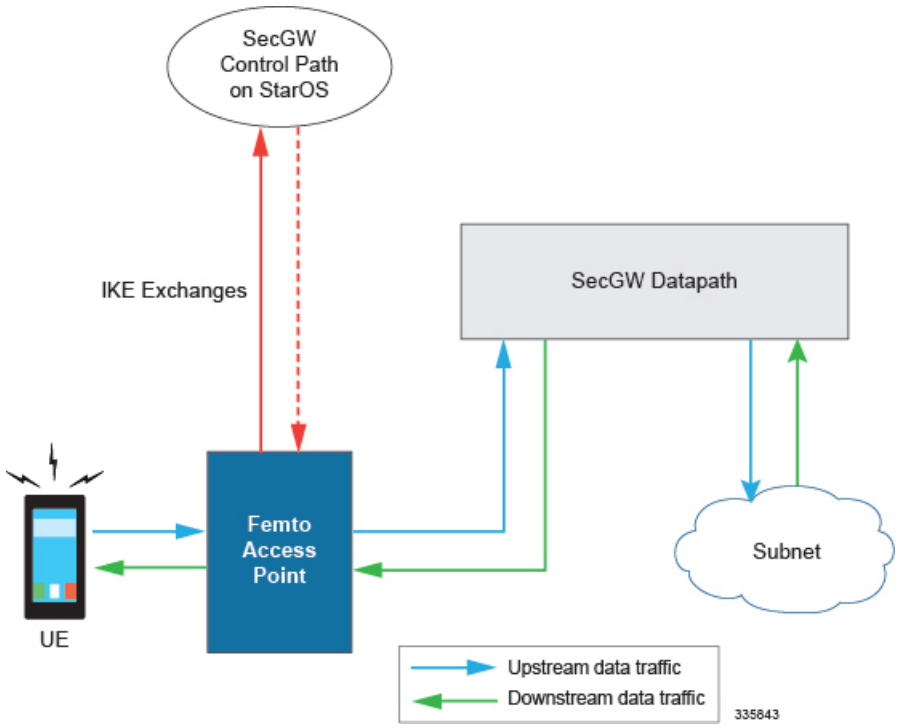
In a RAS scenario, a remote host negotiates a child SA with the SecGW and sends traffic inside the child SA that belongs to a single IP address inside the remote host. This is the inner IP address of the child SA. The outer IP address is the public IP address of the remote host. The addresses on the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

Figure 3: RAS Tunnel

Packet Flow

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

Figure 4: SecGW Packet Flow – RAS



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

Supported Algorithms

SecGW supports the protocols in the table below, which are specified in RFC 5996.

Table 1: Supported Algorithms

Protocol	Type	Supported Options
Internet Key Exchange version 2	IKEv2 Encryption	DES-CBC, 3DES-CBC, AES-CBC-128, AES-CBC-256
	IKEv2 Pseudo Random Function	PRF-HMAC-SHA1, PRF-HMAC-MD5, AES-XCBC-PRF-128
	IKEv2 Integrity	HMAC-SHA1-96, HMAC-SHA2-256-128, HMAC-SHA2-384-192. HMAC-SHA2-512-256, HMAC-MD5-96, AES-XCBC-96
	IKEv2 Diffie-Hellman Group	Group 1 (768-bit), Group 2 (1024-bit), Group 5 (1536-bit), Group 14 (2048-bit)

Protocol	Type	Supported Options
IP Security	IPSec Encapsulating Security Payload Encryption	NULL, DES-CBC, 3DES-CBC, AES-CBC-128, AES-CBC-256, AES-128-GCM-128, AES-128-GCM-64, AES-128-GCM-96, AES-256-GCM-128, AES-256-GCM-64, AES-256-GCM-96 **Note** AES-GCM algorithms are supported only on vPC-DI and vPC-SI Platform.
	Extended Sequence Number	Value of 0 or off is supported (ESN itself is not supported)
	IPSec Integrity	NULL, HMAC-SHA1-96, HMAC-MD5-96, AES-XCBC-96, HMAC-SHA2-256-128, HMAC-SHA2-384-192, HMAC-SHA2-512-256 **Important** HMAC-SHA2-384-192 and HMAC-SHA2-512-256 are not supported on vPC-DI and vPC-SI platforms if the hardware doesn't have crypto hardware.