IPSec to Product Feature Mapping

The IPSec feature is supported for various products. This chapter indicates the products on which IPSec is supported, as well as the relevant sections within this guide that pertain to that product.

Important This guide documents IPSec features that appear in the StarOS command line interface (CLI). IPSec features are not universally supported across all StarOS products and platforms. Refer to the Administration Guide for individual products for IPSec limitations.

IPSec support is outlined for the following products:

PDSN, FA and HA

The following chapters (in bold) and sections apply to PDSN (Packet Data Serving Node), FA (Foreign Agent) and HA (Home Agent) gateway products:

- **Introduction to IP Security (IPSec)**
- **IPSec Network Applications**
  - IPSec for PDN Access Applications
  - IP Sec for Mobile IP Applications
  - RADIUS Attributes for IPSec-based Mobile IP Applications
- **Transform Set Configuration**
- **ISAKMP Policy Configuration**
- **Crypto Maps**
  - Dynamic Crypto Map Configuration (IKEv1 only)
  - Manual Crypto MAp Configuration (IKEv1 only)
  - Crypto Map and Interface Association

- **Service Configurations**
  - FA Services Configuration to Support IPSec
  - HA Services Configuration to Support IPSec
  - PDSN Services Configuration to L2TP Support
  - LAC Service Configuration to Support IPSec
  - RADIUS and Subscriber Attributes for L2TP Application IPSec Support
- **Redundant IPSec Tunnel Fail-Over**
  - Redundant IPSec Tunnel Fail-Over (IKEv1 only)
  - Dead Peer Detection (DPD) Configuration
- **IKEv2 RFC 5996 Compliance**

GGSN, FA and HA

The following chapters (in bold) and sections apply to GGSN (Gateway GPRS Support Node), FA (Foreign Agent) and HA (Home Agent) gateway products:

- **Introduction to IP Security (IPSec)**
- **IPSec Network Applications**
  - IPSec for PDN Access Applications
  - IPSec for Mobile IP Applications
  - IPSec for L2TP Applications
  - RADIUS Attributes for IPSec-based Mobile IP Applications
- **Transform Set Configuration**
- **ISAKMP Policy Configuration**
- **Crypto Maps**
  - Dynamic Crypto Map Configuration (IKEv1 only)
  - Manual Crypto Map Configuration (IKEv1 only)
  - Crypto Map and Interface Association
- **Service Configurations**
  - FA Services Configuration to Support IPSec
  - HA Services Configuration to Support IPSec
  - LAC Service Configuration to Support IPSec
  - RADIUS and Subscriber Attributes for L2TP Application IPSec Support
- **Redundant IPSec Tunnel Fail-Over**
  - Redundant IPSec Tunnel Fail-Over (IKEv1 only)
  - Dead Peer Detection (DPD) Configuration
- **IKEv2 RFC 5996 Compliance**

HeNBGW, HNBGW and HSGW

The following chapters (in bold) and sections apply to HeNBGW (Home evolved Node B Gateway), HNBGW (Home node B Gateway), and HRPD Serving Gateway (HSGW):

Important HNBGW is not supported from Release 20 and later, and HeNBGW is not supported in Releases 20, 21.0 and 21.1. For more information, contact your Cisco account representative.

- **Introduction to IP Security (IPSec)**
- **IPSec Network Applications**
  - IPSec for PDN Access Applications
  - IPSec for Mobile IP Applications
  - IPSec for L2TP Applications
  - RADIUS Attributes for IPSec-based Mobile IP Applications
- **Transform Set Configuration**
- **ISAKMP Policy Configuration**
- **Crypto Maps**
  - Dynamic Crypto Map Configuration (IKEv1 only)
  - Manual Crypto Map Configuration (IKEv1 only)
  - Crypto Map and Interface Association
- **Service Configurations**
  - FA Services Configuration to Support IPSec
  - HA Services Configuration to Support IPSec
  - LAC Service Configuration to Support IPSec
  - RADIUS and Subscriber Attributes for L2TP Application IPSec Support
- **Redundant IPSec Tunnel Fail-Over**
  - Redundant IPSec Tunnel Fail-Over (IKEv1 only)
  - Dead Peer Detection (DPD) Configuration
- **IKEv2 RFC 5996 Compliance**

ePDG

The following chapters (in bold) and sections apply to an evolved Packet Data Gateway (ePDG):

- **Introduction to IP Security (IPSec)**
- **IPSec Network Applications**
  - IPSec for Mobile IP Applications
  - IPSec for L2TP Applications
  - RADIUS Attributes for IPSec-based Mobile IP Applications
- **Transform Set Configuration**
- **ISAKMP Policy Configuration**
- **Crypto Templates**
- **Redundant IPSec Tunnel Fail-Over**
  - Redundant IPSec Tunnel Fail-Over (IKEv1 only)
  - Dead Peer Detection (DPD) Configuration
- **IKEv2 RFC 5996 Compliance**

MME, S-GW, P-GW and SAE-GW

The following chapters (in bold) and sections apply to LTE components, including Mobile Management Entity (MME), Serving Gateway (S-GW), PDN Gateway (P-GW) and System Architecture Evolution Gateway (SAE-GW):

- **Introduction to IP Security (IPSec)**
- **IPSec Network Applications**
  - IPSec for PDN Access Applications
  - IPSec for Mobile IP Applications
  - IPSec for L2TP Applications
  - IPSec for LTE/SAE Networks
  - RADIUS Attributes for IPSec-based Mobile IP Applications
- **Transform Set Configuration**
- **ISAKMP Policy Configuration**
- **Crypto Maps**
  - Dynamic Crypto Map Configuration (IKEv1 only)
  - Manual Crypto Map Configuration (IKEv1 only)
  - Crypto Map and Interface Association
- **Crypto Templates** (MME, S-GW)
- **Service Configurations**
  - LAC Service Configuration to Support IPSec
  - RADIUS and Subscriber Attributes for L2TP Application IPSec Support
- **Redundant IPSec Tunnel Fail-Over**

  - Redundant IPSec Tunnel Fail-Over (IKEv1 only)
  - Dead Peer Detection (DPD) Configuration
- **IKEv2 RFC 5996 Compliance**

SecGW

The following chapters (in bold) and sections apply to a Security Gateway (SecGW, WSG service) running within a Virtualized Packet Core-Standalone Instance (VPC-SI) in a virtual machine on an ASR 9000 Virtualized Service Module (VSM).

- **Introduction to IP Security (IPSec)**
- **IPSec Network Applications**
  - IPSec for PDN Access Applications
  - IPSec for Mobile IP Applications
  - IPSec for L2TP Applications
  - RADIUS Attributes for IPSec-based Mobile IP Applications
  - IPSec for consumer and enterprise small cell
  - IPSec for Macro Cell
  - IPSec for Unlicensed Mobile Access (UMA)
- **Transform Set Configuration**
- **ISAKMP Policy Configuration**
- **Service Configurations**
  - WSG Service
- **Redundant IPSec Tunnel Fail-Over**
  - Redundant IPSec Tunnel Fail-Over
  - Dead Peer Detection (DPD) Configuration
- **IPSec X.509 Certificates**
- **Rekeying SAs**
- **Access Control**
- **Remote Secrets**
- **IKEv2 RFC 5996 Compliance**
- **Duplicate Session Detection**
- **Extended Sequence Number**
- **Security Gateway as Intiator**