Introduction to IP Security (IPSec)

This chapter briefly describes IPSec functionality and associated terminology.

Important IPSec is a suite of standard and licensed Cisco features. Contact your Cisco account representative for detailed information on specific licensing requirements. For information on installing and verifying licenses, refer to the *System Administration Guide*.

The following topics are discussed in this chapter:

Overview

IPSec is a suite of protocols that interact with one another to provide secure private communications across IP networks. These protocols allow the system to establish and maintain secure tunnels with peer security gateways. IPSec provides confidentiality, data integrity, access control, and data source authentication to IP datagrams.

IPSec AH and ESH

Authentication Header (AH) and Encapsulating Security Payload (ESP) are the two main wire-level protocols used by IPSec. They authenticate (AH) and encrypt-plus-authenticate (ESP) the data flowing over that connection.

- **AH** is used to authenticate – but not encrypt – IP traffic.Authentication is performed by computing a cryptographic hash-based message authentication code over nearly all the fields of the IP packet (excluding those which might be modified in transit, such as TTL or the header checksum), and stores this in a newly-added AH header that is sent to the other end. This AH header is injected between the original IP header and the payload.

- **ESP** provides encryption and optional authentication. It includes header and trailer fields to support the encryption and optional authentication. Encryption for the IP payload is supported in transport mode and for the entire packet in the tunnel mode. Authentication applies to the ESP header and the encrypted data.

IPSec Transport and Tunnel Mode

Transport Mode provides a secure connection between two endpoints as it encapsulates IP payload, while Tunnel Mode encapsulates the entire IP packet to provide a virtual "secure hop" between two gateways.

Tunnel Mode forms the more familiar VPN functionality, where entire IP packets are encapsulated inside another and delivered to the destination. It encapsulates the full IP header as well as the payload.

Security Associations (SAs) and Child SAs

An Internet Key Exchange-Security Association (IKE-SA) is used to secure IKE comicality. SA is identified by two, eight-byte Security Parameter Indices (SPIs) shared by each peer during the initial IKE exchange. Both SPIs are carried in all subsequent messages.

A Child-SA is created by IKE for use in AH or ESP security. Two Child-SAs are created as a result of one exchange – Inbound and Outbound. A Child-SA is identified by a single four-byte SPI, Protocol and Gateway IP Address and is carried in each AH/ESP packet.

Each SA (IKE or Child) has an associated lifetime. After the expiry of lifetime, SAs are deleted. To proactively establish an SA before the last one expires, SAs are rekeyed on soft lifetime expiry. Both IKE and Child SAs may be rekeyed.

Anti-Replay (IKEv2)

Anti-replay is a sub-protocol of IPSec (RFC 4303) that is supported for IKEv1 and IKEv2 tunnels. Its main goal is to prevent hackers injecting or making changes in packets that travel from a source to a destination. Anti-replay protocol employs a unidirectional security association to establish a secure connection between two nodes in the network.

Once a secure connection is established, the anti-replay protocol uses a sequence number or a counter. When the source sends a message, it adds a sequence number to its packet starting at 0 and increments every time it sends another message. At the destination end, the protocol receives the message and keeps a history of the number and shifts it as the new number. If the next message has a lower number, the destination drops the packet, and, if the number is larger than the previous one, it keeps and shifts it as the new number.

The anti-replay feature may be enabled or disabled via the StarOS CLI. Anti-Replay Window Sizes of 32, 64, 128, 256, 384 and 512 bits are supported (default = 64 bits).

Behavior for ACL-based calls differs from Subscriber-based calls.

- **ACL-based.** An anti-replay configuration change in the CLI will not be propagated until a call is cleared and re-established.
- **Subscriber-based.** An anti-replay configuration change in the CLI will not affect established calls but new calls will utilize the new anti-replay configuration.

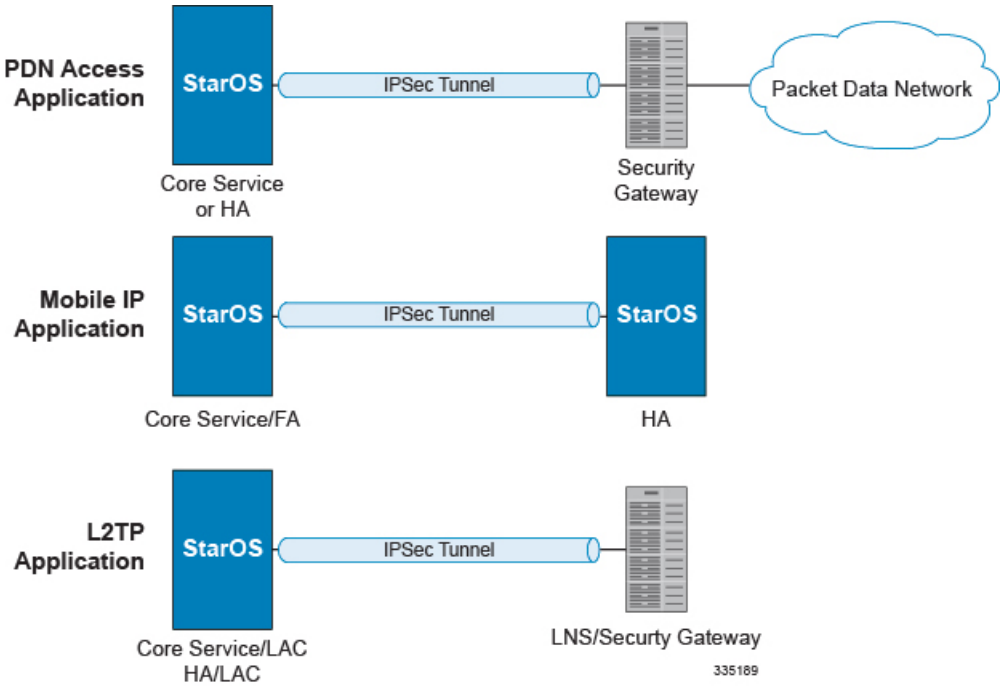
IPSec Applications

Important Support for IPSec features varies per platform, service type and StarOS release. Refer to the gateway administration guide and StarOS *Release Notes* for additional information.

IPSec can be implemented via StarOS for the following applications:

- **PDN Access:** Subscriber IP traffic is routed over an IPSec tunnel from the system to a secure gateway on the packet data network (PDN) as determined by access control list (ACL) criteria. This application can be implemented for both core network service and HA-based systems. The following figure shows several IPSec configurations.

Figure 1: IPSec Applications



- **Mobile IP:** Mobile IP (MIP) control signals and subscriber data is encapsulated in IPSec tunnels that are established between foreign agents (FAs) and home agents (HAs) over the Pi interfaces.

Important Once an IPSec tunnel is established between an 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.

- **L2TP:** L2TP-encapsulated packets are routed from the system to an LNS/secure gateway over an IPSec tunnel.

Note that: IPSec can be implemented for both attribute-based and compulsory tunneling applications for 3GPP2 services.

IPSec Terminology

There are several items related to IPSec support under StarOS that must be understood prior to beginning configuration. They include:

Crypto Access Control List (ACL)

Access Control Lists define rules, usually permissions, for handling subscriber data packets that meet certain criteria. Crypto ACLs, however, define the criteria that must be met in order for a subscriber data packet to be routed over an IPSec tunnel.

Unlike other ACLs that are applied to interfaces, contexts, or one or more subscribers, crypto ACLs are matched with crypto maps. In addition, crypto ACLs contain only a single rule while other ACL types can consist of multiple rules.

Prior to routing, the system examines the properties of each subscriber data packet. If the packet properties match the criteria specified in the crypto ACL, the system will initiate the IPSec policy dictated by the crypto map.

For additional information refer to the *Access Control* chapter of this guide. There you will find a discussion of blacking and whitelisting, as well as IKE Call Admission Control (CAC).

Transform Set

Transform Sets are used to define IPSec security associations (SAs). IPSec SAs specify the IPSec protocols to use to protect packets.

Transform sets are used during Phase 2 of IPSec establishment. In this phase, the system and a peer security gateway negotiate one or more transform sets (IPSec SAs) containing the rules for protecting packets. This negotiation ensures that both peers can properly protect and process the packets.

For additional information refer to the *Transform Set Configuration* chapter of this guide,

ISAKMP Policy

Internet Security Association Key Management Protocol (ISAKMP) policies are used to define Internet Key Exchange (IKE) SAs. The IKE SAs dictate the shared security parameters (such as which encryption parameters to use, how to authenticate the remote peer, etc.) between the system and a peer security gateway.

During Phase 1 of IPSec establishment, the system and a peer security gateway negotiate IKE SAs. These SAs are used to protect subsequent communications between the peers including the IPSec SA negotiation process.

For additional information refer to the *ISAKMP Policy Configuration* chapter of this guide.

Crypto Map

Crypto Maps define the tunnel policies that determine how IPSec is implemented for subscriber data packets.

There are several types of crypto maps supported by StarOS. They are:

- Manual crypto maps
- IKEv2 crypto maps
- Dynamic crypto maps

Important The **map ip pool** command is not supported within crypto maps on the ASR 5500.

Manual Crypto Maps (IKEv1)

These are static tunnels that use pre-configured information (including security keys) for establishment. Because they rely on statically configured information, once created, the tunnels never expire; they exist until their configuration is deleted.

Manual crypto maps define the peer security gateway to establish a tunnel with, the security keys to use to establish the tunnel, and the IPSec SA to be used to protect data sent/received over the tunnel. Additionally, manual crypto maps are applied to specific system interfaces.

Important Because manual crypto map configurations require the use of static security keys (associations), they are not as secure as crypto maps that rely on dynamically configured keys. Therefore, it is recommended that they only be configured and used for testing purposes.

IKEv2 Crypto Maps

These tunnels are similar to manual crypto maps in that they require some statically configured information such as the IP address (IPv4 or IPv6) of a peer security gateway and that they are applied to specific system interfaces.

However, IKEv2 crypto maps offer greater security because they rely on dynamically generated security associations through the use of the Internet Key Exchange (IKE) protocol.

When IKEv2 crypto maps are used, the system uses the pre-shared key configured for the map as part of the Diffie-Hellman (D-H) exchange with the peer security gateway to initiate Phase 1 of the establishment process. Once the exchange is complete, the system and the security gateway dynamically negotiate IKE SAs to complete Phase 1. In Phase 2, the two peers dynamically negotiate the IPSec SAs used to determine how data traversing the tunnel will be protected.

Dynamic Crypto Maps (IKEv1)

These tunnels are used for protecting L2TP-encapsulated data between the system and an LNS/security gateway or Mobile IP data between an FA service configured on one system and an HA service configured on another.

The system determines when to implement IPSec for L2TP-encapsulated data either through attributes returned upon successful authentication for attribute based tunneling, or through the configuration of the L2TP Access Concentrator (LAC) service used for compulsory tunneling.

The system determines when to implement IPSec for Mobile IP based on RADIUS attribute values as well as the configurations of the FA and HA service(s).

For additional information, refer to the *Crypto Maps* chapter of this guide

Crypto Template

A Crypto Template configures 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. However, a single StarOS instance can run multiple instances of the same service with each associated with that crypto template.

For additional information, refer to the *Crypto Templates* chapter of this guide.

IKEv1 versus IKEv2

StarOS supports features associated with:

- IKEv1 as defined in RFC 2407, RFC 2408 and RFC 2409
- IKEv2 as defined in RFC 4306, RFC 4718 and RFC 5996

The table below compares features supported by IKEv1 and IKEv2.

Table 1: IKEv1 versus IKEv2 Features

IKEv1	IKEv2
IPSec Security Associations (SAs)	Child Security Associations (Child SAs)
Exchange modes: • Main mode • Aggressive mode	Only one exchange mode is defined. Exchange modes were obsoleted.
Number of exchanged messages required to establish a VPN: • Main mode = 9 messages • Aggressive mode = 6 messages	Only 4 messages are required to establish a VPN.

IKEv1	IKEv2
Authentication methods: • Pre-Shared Key (PSK) • Digital Signature (RSA-Sig) • Public Key Encryption • Revised mode of public Key Encryption	Authentication methods: • Pre-Shared Key (PSK) • Digital Signature (RSA-Sig)
Traffic Selector: • Only a combination of a source IP range, a destination IP range, a source port and a destination port is allowed per IPSec SA. • Exact agreement of the traffic selection between peers is required.	Traffic Selector: • Multiple combinations of of a source IP range, a destination IP range, a source port and a destination port are allowed per Child SA. IPv4 and IPv6 addresses can be configured for the same Child SA. • Narrowing traffic selectors between peers is allowed.
Lifetime for SAs requires negotiation between peers.	Lifetime for SAs is not negotiated. Each peer can delete SAs by exchanging DELETE payloads.
Multihosting is not supported	Multihosting is supported by using multiple IDs on a single IP address and port pair.
Rekeying is not defined.	Rekeying is defined and supported.
Dead peer Detection (DPD) for SAs is defined as an extension.	DPD is supported by default.
NAT Transversal (NATT) is not supported.	NAT Transversal (NATT) is supported only for subscriber mode.
Remote Access VPN is not defined, but is supported by vendor-specific implementations for Mode config and XAUTH.	Remote Access VPN is supported by default: • Extensible Authentication Protocol (EAP) • User authentication via EAP is associated with IKE authentication • Configuration payload (CP)
Multihoming is not supported.	Multihoming is supported by MOBIKE (IKEv2 Mobility and Multihoming Protocol, RFC 4555)
Mobile Clients are not supported.	Mobile Clients are supported by MOBIKE.
Denial of Service (DoS) protections are not supported.	DoS protections include an anti-replay function.

Supported Algorithms

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

Table 2: 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.

Boost Crypto Performance

An **require ipsec-large** command boosts IPSec crypto performance by enabling the resource manager (RM) task to assign additional IPSec managers to packet processing cards that have sufficient processing capacity.

```
configure
    require ipsec-large
    end
```

This command works with ePDG, PDIF and other StarOS applications.

Important When IPSec large and demux on MIO are configured together, enable the IPsec large feature (using the **require ipsec-large** command) before enabling the demux on MIO (using the **require demux management-card** command).

Refer to the *Release Notes* accompanying each StarOS build for the latest information on supported products and packet processing cards.

Multiple Authentication Configuration

List of authentication methods are defined and associated in Crypto Template. The basic sample configuration required for OCSP and Certificate based authentication is as follows. For backward compatibility, the configuration for auth method inside Crypto Template will be working.

The following are the configuration considerations:

- A maximum of three sets of authentication methods in the list can be associated.
- Each set can have only one local and one remote authentication method configuration.
- The existing configuration inside the Crypto Template takes precedence over the new auth-method-set defined, in case same authentication method is configured at both places.

configure

CA Certificate for device certificate authentication:

```
ca-certificate name <ca-name> pem url file: <ca certificate path>
```

Gateway Certificate:

```
ca-certificate name <gateway-name> pem url file: <gateway certificate path>
private-key pem url file:<gateway private key path>
            eap-profile <profile name>
                 mode authenticator-pass-through
                 exit
            ikev2-ikesa auth-method-set <list-name-1>
                 authentication remote certificate
                 authentication local certificate
                 exit
            ikev2-ikesa auth-method-set <list-name-2>
                 authentication eap-profile eap1
                 exit
            crypto template boston ikev2-subscriber
                 ikev2-ikesa auth-method-set list <list-name-2> <list-name-2>
                 ca-certificate list ca-cert-name <ca-name>
                 exit
```