ERICSSON

IPsec VPN Overview

TECHNICAL PRODUCT DESCRIPTION

2/221 02-CRA 119 1170/1-V1 Uen D

Contents

1 IPsec VPN Overview

The IP Security (IPsec) Virtual Private Network (VPN) application provided by the security service on the ASE card enables support of IPsec on site-to-site tunnels between two security gateways, referred to as peers in this document.

For instructions on how to configure site-to-site IPsec VPNs, see Reference [1]. For details on all the CLI commands used to configure site-to-site IPsec VPNs, see Reference [2].

1.1 Site-to-Site Connections Examples

You can create IPsec tunnels between two SmartEdge® routers or between one managed SmartEdge router and an unmanaged device (referred to as an extranet device), such as Customer Premises Equipment (CPE) or remote special-purpose server. Figure 1 shows the physical links for an IPsec VPN that must exist between two managed SmartEdge routers and between the two SmartEdge routers and the protected networks at each end of the IPsec tunnel. Figure 2 shows the physical links for an IPsec tunnel that must exist between the NetOp™ Element Management System (EMS) host, a managed SmartEdge router, and an extranet device as well as the SmartEdge router and the protected network at its end of the IPsec tunnel.

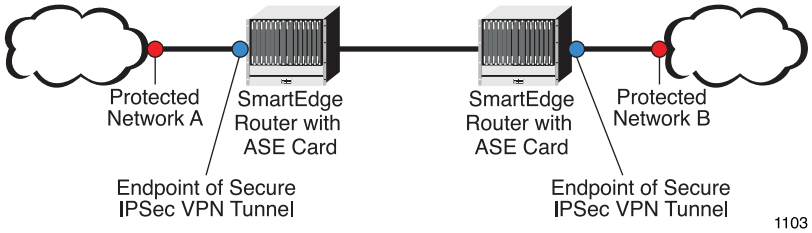

Figure 1 An IPsec VPN Between Two Managed SmartEdge Routers

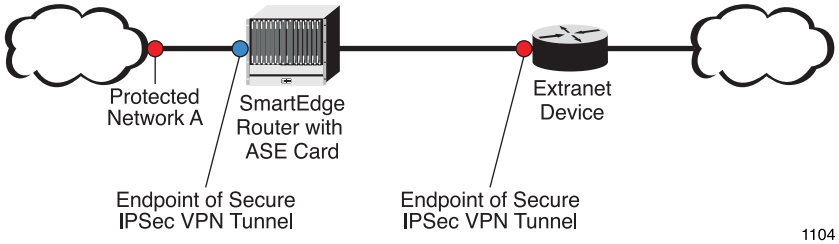

Figure 2 An IPsec Tunnel Between a Managed SmartEdge Router and an Extranet Device

You can use these two basic configurations to implement a variety of individual secure site-to-site IPsec tunnels.

1.1.1 Connecting Remote Protected Networks

An IPsec tunnel between two managed SmartEdge routers protects traffic across the untrusted network between the routers. This type of IPsec tunnel allows a service provider to offer protected traffic support between the endpoints that it manages.

For example, Figure 3 shows an IPsec VPN that connects two protected networks at each end of the tunnel for a multisite business customer (a total of four protected networks). The customer trusts the traffic between its premises and the SmartEdge routers, but does not trust the traffic between the SmartEdge routers managed by the service provider (also known as Provider Equipment [PE]).

To secure the traffic of the business customer between its SmartEdge routers, the service provider uses an IPsec tunnel. This ensures that all the traffic for the business customer between the two endpoints the service provider manages is protected.

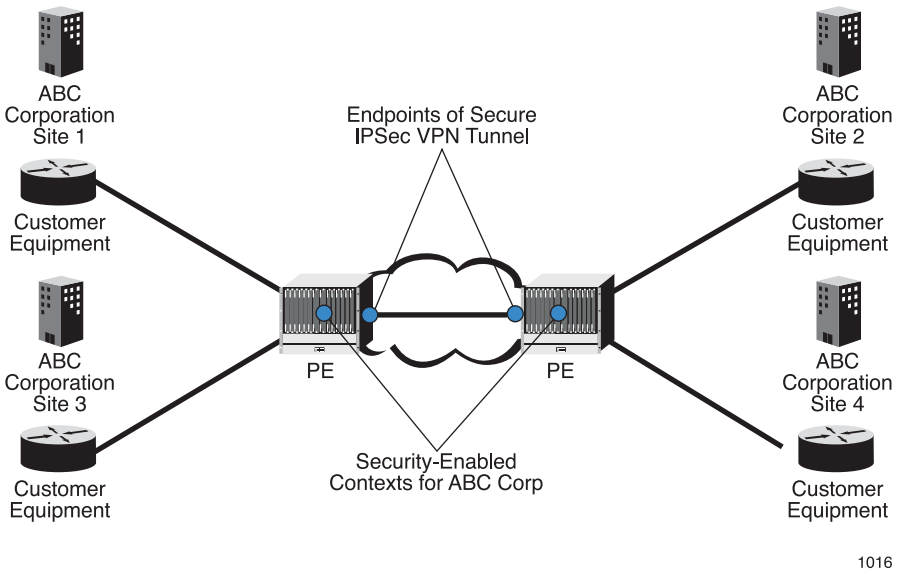

Figure 3 An IPsec Tunnel That Protects Traffic Between Two SmartEdge Routers

In this scenario, the connections between the equipment on the premises of the customer and the SmartEdge routers of the service provider, as well as the connection between the SmartEdge routers, must already be configured. To protect the customer traffic between the two managed SmartEdge routers, the service provider must configure both endpoints of the secured IPsec tunnel.

1.1.2 Securing the Last Mile

An IPsec tunnel between a managed SmartEdge router and a CPE device protects traffic on the last mile. This type of IPsec tunnel allows a service

provider to offer protected services between an endpoint it manages and one that it does not.

For example, Figure 4 shows four IPsec tunnels that connect the four protected networks to two SmartEdge routers for a multisite business customer. The customer expects the service provider to protect the traffic between its premises and the SmartEdge routers.

To secure this traffic, the service provider uses four IPsec tunnels to ensure all the traffic between each CPE device at the customer site and the SmartEdge router it manages is protected.

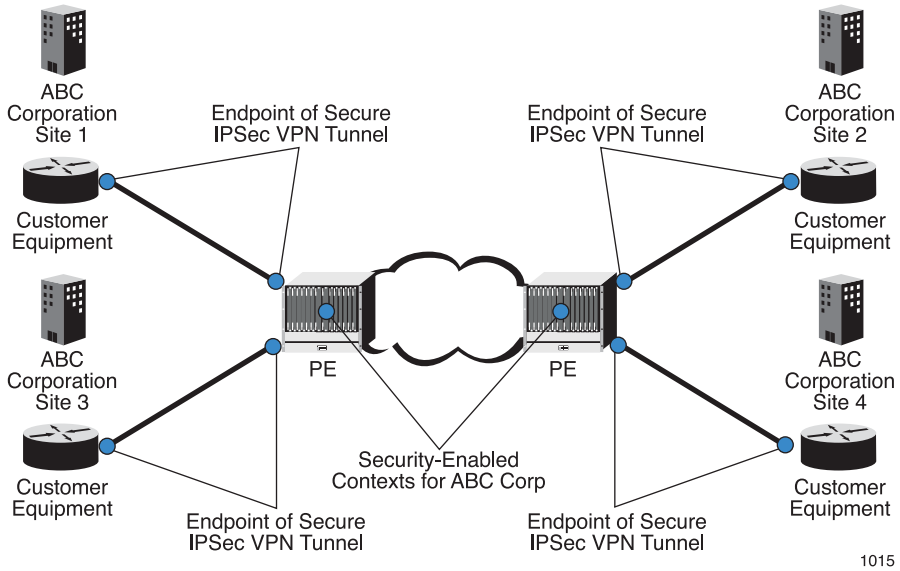

Figure 4 An IPsec Tunnel That Protects Traffic Between Customer Equipment and a SmartEdge Router

In this scenario, the connections between the equipment on the customer premises and the service provider SmartEdge routers, as well as the connection between the SmartEdge routers, must already be configured. To protect the customer traffic between its premises and the service provider SmartEdge router, on each IPsec tunnel the service provider must configure the endpoint on the SmartEdge router and identify the peer endpoint on the extranet device on the customer premises.

1.1.3 Encrypting Local Stack Packets

Service providers need to encrypt their own data to send to customers because the data has encryption requirements associated with it. Common requirements include organizational best practices, risk associated with the data, regulatory demands, and privacy concerns.

For example, Figure 5 shows three IPsec tunnels that protect the traffic of a service provider on connections between its own equipment in the network.

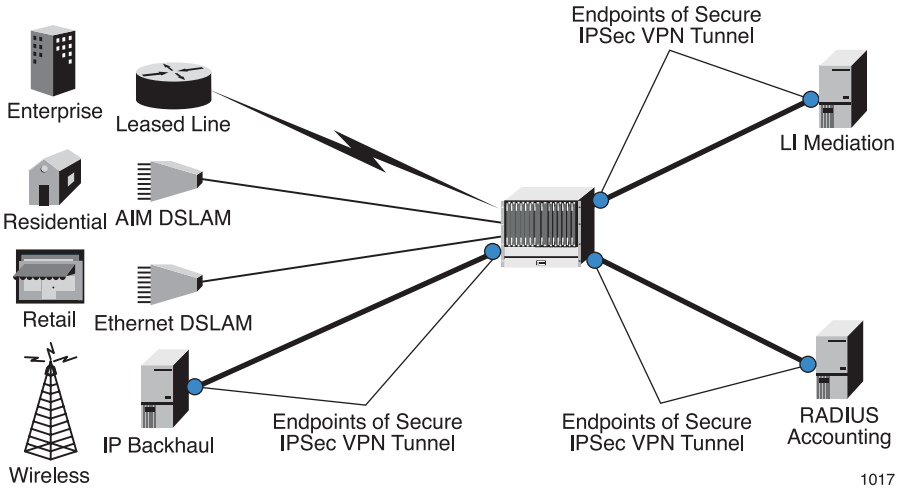

Figure 5 Service Provider Data Requiring Encryption

In this scenario, the service provider is protecting its own data, and the connections between all equipment involved in communicating the encrypted data must already be configured. To protect its own traffic, the service provider must also configure individual IPsec tunnels and identify the appropriate endpoints.

1.2 IPsec Services

An IPsec VPN session requires a secure connection for the tunnel and secure traffic for the duration of the session. You can set up a secure connection dynamically by using an Internet Key Exchange (IKE) protocol and preshared keys, or manually by using predefined keys. You secure traffic by using a combination of authentication algorithms to validate the identity of each peer, and encryption algorithms to make the traffic unreadable to anyone without the required decryption key.

IPsec secures a VPN by providing several security services:

- Data and traffic-flow confidentiality—Protects data from unauthorized disclosure, especially of application-level data. Traffic-flow confidentiality addresses the unauthorized disclosure of the external characteristics of communication by concealing the source and destination addresses or message length. Confidentiality is provided by encrypting the data traffic. Encryption transforms data from an intelligible form (plaintext) into an unintelligible form (ciphertext); decryption restores the plaintext from the ciphertext.

- Data origin authentication—Verifies the identity of the claimed source of data. IPsec provides this type of authentication together with support of data integrity.

- Data integrity—Ensures that modifications to data are detectable. IPsec data integrity mechanisms support detection of the following:

- Data modification/tampering—Detects the modification of an individual IP datagram in a stream of traffic.
- Replay of valid data—Detects the arrival of duplicate IP datagrams, within a constrained antireplay window.

1.3 IPsec Protocols

IPsec consists of three main protocols:

- IKE—Supports the dynamic negotiation of Security Associations (SAs) to secure an IPsec tunnel.
- Authentication Header (AH)—Supports authentication algorithms that verify the identity of the sender.
- Encapsulating Security Payload (ESP) —Supports both encryption and authentication algorithms.

  Encryption makes a message unreadable without a special key that decrypts the message.

The AH and ESP protocols support two modes of use: transport mode and tunnel mode. In transport mode, AH and ESP provide protection primarily for next layer protocols; in tunnel mode, AH and ESP are applied to tunneled IP packets. Tunnel mode is the only mode supported in this release.

IPsec protects data exchanged between the two parties on the tunnel by using the security parameters, including the authentication and encryption algorithms, that the parties negotiated when the tunnel was established.

1.3.1 IKE

The IKE protocol uses either preshared keys or Rivest, Shamir and Adleman (RSA) certificates to authenticate the peers at each end of the connection and enable the dynamic negotiation of SAs to secure an IPsec tunnel. An IPsec tunnel set up using IKE is called an auto key IPsec tunnel.

When you set up an autokey IPsec tunnel, either IKE version 1 (IKEv1) or IKE version 2 (IKEv2) is used to secure the connection and the traffic that passes through the tunnel.

Table 1 Differences Between IKEv1 and IKEv2

Characteristic	IKEv1	IKEv2	Comment
Number of messages to secure connection	4	2	

Characteristic	IKEv1	IKEv2	Comment
Number of messages to secure traffic	3	2	Multiple SAs can be established; each one requ ires message exchange.
Negotiation modes	Two modes: • Main—Slower, but more secure. Six messages are exchanged. Endpoint IDs are exchanged after a secure channel is established. • Aggressive—F aster, but less secure. Only three messages are exchanged; however, because endpoint IDs are exchanged in clear text, it is less secure.	None	
Negotiable fixed SA lifetime	Yes	No	With IKEv2, the lifetime of an SA is controlled by each endpoint.
Rekeying of SAs	No	Yes	Rekeying allows extension of the lifetime of an SA.

Characteristic	IKEv1	IKEv2	Comment
Asymmetric authentication between endpoints	No IKEv1 requires symmetric peer authentication, and the authentication method is negotiated.	Yes IKEv2 supports asymmetric peer authentication, reducing negotiation.	Two authentication methods are supported: • Preshared keys • RSA certificates To use RSA certificates, Public Key Infrastructure (PKI) must be configured.
Pseudo-Random Function (PRF) in IKE proposal	No	Yes	The PRF provides more robust encryption of keying material in SAs.
Multiple traffic selectors in a single tunnel configuration	No	Yes	Supports IPsec QoS priority queuing.
Narrowing of traffic selectors	No	Yes	

1.3.2 AH

The AH protocol enables you to provide source and content authentication of a packet. AH uses a hashing algorithm that breaks up messages into fixed size blocks and then applies security procedures to them to authenticate them. To authenticate a packet using the Hash-Based Message Authentication Code (HMAC) technique, a secret key is applied along with either a Message Digest 5 (MD5) or Secure Hash Algorithm-1 (SHA-1) function. Both MD5 and SHA-1 are cryptographic hash functions; MD5 produces a 16-byte hash value, SHA-1 produces a 20-byte hash value.

1.3.3 ESP

The ESP protocol enables you to provide data confidentiality as well as source and content authentication. ESP in tunnel mode encapsulates the entire IP packet (header and payload) and then adds a new IP header to the front of the encrypted packet. This new IP header contains the destination address needed to route the protected data through the network.

With ESP, you can both encrypt and authenticate. You can also choose to encrypt only or to simply authenticate. For encryption, you can choose one of the following cryptographic algorithms

- Data Encryption Standard (DES)—An encryption method applied with a 56-bit key.
- Triple DES (3DES)—A cryptographically stronger version of DES in which the original DES algorithm is applied three times with a 168-bit key.
- Advanced Encryption Standard (AES)—A newer encryption method that offers strong cryptographic protection. Three key lengths are supported: 128, 192, and 256 bits.

1.4 Public Key Infrastructure

The SmartEdge OS supports a manual Public Key Infrastructure (PKI) to import trusted and self certificates provided by a Certificate Authority (CA), create key pairs, and request signed certificates using the generated key pairs from the CA. With PKI configured, you can use RSA certificates to authenticate peers during IKE negotiations as an alternative to using preshared keys.

1.5 Key Management and Distribution

Key management and distribution is an important part of using VPNs. IPsec supports two key management and distribution methods for SAs: manual key and auto key.

The keys for SAs can be configured in two ways

- Manual Key—network administrators on both sides of the connection configure the SAs manually, and specify the SAs to be used when configuring an IPsec tunnel.

  With manual keys, parties at both ends of a tunnel configure the security parameters. This technique is straightforward for small, static networks where management and distribution of keys is relatively simple. However, manual key-based configurations create potential for security breaches.

- Auto Key—SAs are established automatically using the IKE protocol between the two parties on both sides of the tunnel using information configured in IKE policies and IKE proposals.

  This technique is more secure and removes the potential for error compared to the manual technique. You can deploy IKE using preshared keys to authenticate both parties.

1.5.1 Diffie-Hellman Exchange

A Diffie-Hellman exchange allows parties in a communication session to produce a shared secret key over an unsecured channel. A Diffie-Hellman exchange is configured using a DH group. A number of DH groups are defined; DH groups 1, 2, 5, and 14 are supported in the current release.

Each IKE proposal specifies a DH group setting. An additional DH group is specified when Perfect Forward Secrecy (PFS) is enabled in an IPsec policy.

1.5.2 Perfect Forward Secrecy

PFS is a service provided by the IKE protocol to preserve the integrity of keys. PFS ensures that compromise of a single key permits access to only data protected by that key. For PFS to exist, the key used to protect transmission of data is never used to derive any additional keys, or the material used to derive a key is not used to derive additional keys. When PFS is enabled, additional processing to ensure that the material used to derive individual keys is used only once and then deleted.

1.6 Security Associations

An SA defines security parameters for protecting packets exchanged between each side of the connection. Each SA is uniquely identified by a Security Parameter Index (SPI), destination IP address, and security protocol. The security protocol used by the connection can be either AH or ESP. An SA may involve either AH only, ESP only, or both. The SPI is a 32-bit value that is assigned by the receiver. An SA also specifies the authentication and encryption algorithms used to secure traffic.

For a manual key IPsec tunnel, there is no need to secure the connection to negotiate the securing of the data traffic. To secure the IPsec VPN data traffic for a manual key IPsec tunnel, you configure IPsec SAs on each peer to provide confidentiality to data traffic. Each peer provides the other peer one or more manually configured IPsec SAs that it supports, and the agreed upon IPsec SAs enable the securing of the data traffic in each direction across the IPsec tunnel using a set of matching authentication and encryption settings.

For an auto key tunnel you need to negotiate the two types of SAs to secure the connection and to secure the data traffic:

- IKE SA—The shared protocols and keys or certificates used by the negotiating peers to establish a secure, authenticated, bidirectional control channel with which to negotiate other security associations used for IPsec.

- IPsec SA—The shared protocols and keys used between a sender and a receiver to provide security services using either the AH or ESP protocol (or both) to the traffic carried by the SA.

1.7 Security Association Negotiation

The starting point for dynamic negotiations for an auto key IPsec tunnel is a proposal. Each peer provides the other peer one or more proposals that it supports in a policy. An IKE policy contains IKE proposals and an IPsec policy contains IPsec proposals. A proposal defines authentication and encryption parameters used for negotiations. The negotiations proceed as follows:

- An IKE policy provides fixed and negotiable settings used to negotiate an IKE SA. The negotiable settings are provided in IKE proposals. An IKE proposal is agreed on by the peers and the resulting IKE SAs create a secure connection. If IKEv1 is used, this negotiation is completed in four messages and is called Phase 1. If IKEv2 is used, negotiation is completed in two messages. After the parties have created a secure connection, negotiation to secure the data traffic is initiated.

- An IPsec policy provides fixed and negotiable settings used to negotiate an IPsec SA. An IPsec proposal is agreed on by the peers and the resulting IPsec SAs secure the data traffic in each direction across the IPsec tunnel by using a set of matching authentication and encryption settings. If IKEv1 is used, this negotiation is completed in three messages and is called Phase 2. If IKEv2 is used, negotiation is completed in two messages.

1.8 IPsec VPN Implementation Concepts

IPsec VPNs are of two types: a site-to-site VPN, which is a permanent connection between two peers in a network, and a remote access VPN, which is a connection between a remote-access client and a VPN gateway to a private network. In the current release of Security Services, only site-to-site VPNs are supported.

Two methods exist for specifying how the traffic on an IPsec VPN is selected for encryption: route-based or policy-based. In a route-based VPN, routing determines which traffic is forwarded over an IPsec tunnel. In a policy-based VPN, Access Control List (ACL) rules are typically used to select the subset of traffic that is forwarded over an IPsec tunnel. In the current release, only route-based traffic selection is supported.

The SmartEdge OS supports two IPsec VPN modes:

- Circuit-based (default)
- Economical

In circuit-based mode, the SmartEdge OS:

- Forwards incoming clear tunnel traffic from the Ingress Packet Processing ASIC (iPPA) to the Egress Packet Processing ASIC (ePPA) on the ingress line card to complete tunnel egress processing.
- Loops the traffic back to the iPPA.
- Forwards the traffic to the ASE card for encryption.
- Forwards it to the egress line card for physical egress processing and to the egress port.

In circuit-based mode, traffic accesses the circuit-based resources available on line cards. Circuit-based mode is required when using OSPF and RIP, which automatically install IP routes to the IPsec tunnel as soon as the tunnel is operational.

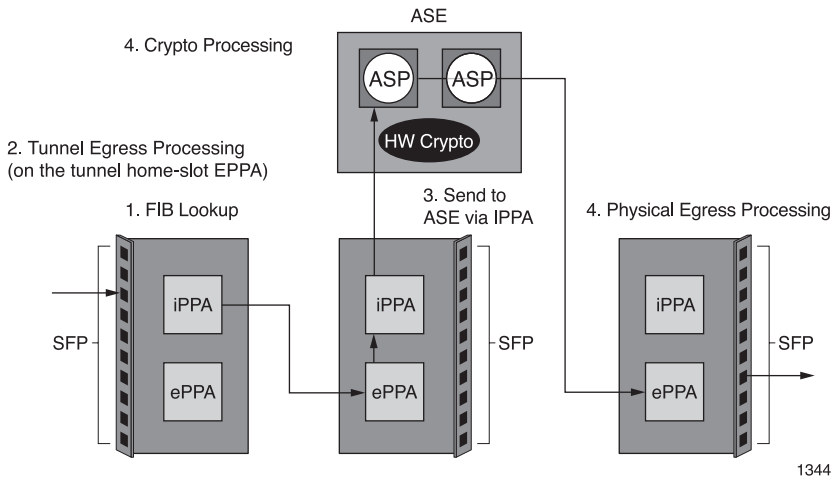

Figure 6 Traffic Path for Circuit-Based Mode

Economical mode forwards incoming clear tunnel traffic directly from the iPPA on the ingress line card to the ASE card for encryption, and then forwards it to the egress line card for egress processing. Economical mode uses less resources by eliminating the loopback from the iPPA to the ePPA and back to the iPPA, not using tunnel circuits on the ePPA, and reducing the amount of backplane traversal. In the current release, economical mode does not support any dynamic routing protocols except Border Gateway Protocol (BGP). To use economical mode, specify it explicitly when you configure an IPsec tunnel.

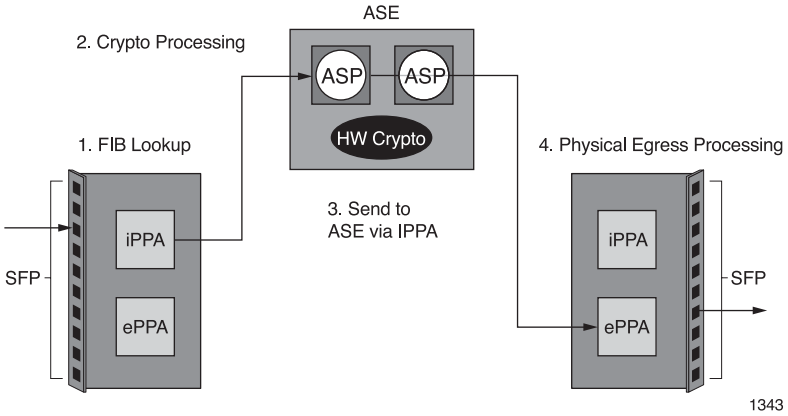

Figure 7 Traffic Path for Economical Mode

1.8.1 Site-to-Site VPNs

A site-to-site VPN secures traffic on the Internet. It is also used to connect networks, such as those of a remote office and a corporate center. VPN gateways are typically used at each site to secure the traffic. The VPN gateway encapsulates and encrypts outbound traffic and sends it through an IPsec tunnel over the Internet. When the peer VPN gateway receives the data, it removes headers and decrypts the data, sending the packet towards the target host inside its local private network.

A site-to-site VPN consists of one or more IPsec tunnels. An IPsec tunnel is configured over a connection between two gateways, with a tunnel endpoint on each gateway. Three tunnel variations are supported in the current release:

- Static auto key tunnel endpoint —A static auto key tunnel can only be configured between a known local endpoint and a known remote endpoint and uses an IKE protocol to automatically negotiate IPsec SAs. A static auto key tunnel supports tunnel interface, static, and traffic-selector-based routes in both circuit-based and economical modes. If you use circuit-based mode, BGP, OSPF, and RIP dynamic routes are supported. If you use economical mode, only BGP dynamic routes are supported. You need to configure individual tunnels to connect the same local endpoint to multiple remote endpoints.

- On-demand auto key IPsec tunnel endpoint—An on-demand auto key tunnel can be configured between a known local endpoint and an unknown remote endpoint and uses an IKE protocol to automatically negotiate IPsec SAs. If the IKEv1 protocol is used to negotiate IPsec SAs, only the aggressive mode for key exchange is supported. An on-demand auto key tunnel supports traffic-selector-based routes and BGP dynamic routes, and, if circuit-based mode is used, OSPF and RIP dynamic routes are also supported. Tunnel interface and static routes are not supported. A single on-demand tunnel configuration using the same local IP address and local ID can establish connections to multiple remote endpoints dynamically.

- Manual key IPsec tunnel endpoint—A manual key IPsec tunnel can only be configured between a known local endpoint and a known remote endpoint and requires that compatible IPsec SAs are manually configured at both endpoints. A manual key tunnel supports tunnel interface and static routes in both circuit-based and economical modes. Traffic-selector-based routes are not supported. If you use circuit-based mode, OSPF and RIP dynamic routes are supported. If you use economical mode, only BGP dynamic routes are supported. Manual key tunnel configuration is not easily scalable and is unsuitable if more than a small number of tunnels is required.

1.8.2 Remote Access VPNs

Remote access VPNs connect individual nodes or users to private or corporate networks. An example is a telecommuter who needs to securely access the company's network over the Internet. In a remote access VPN, all hosts have VPN client software. The host attempts to transmit information and the VPN client software encapsulates and encrypts that traffic before sending it over the Internet to the VPN gateway at the destination network.

Currently, the SmartEdge OS does not support remote access VPNs.

Glossary

3DES
Triple DES

ACL
Access Control List

AES
Advanced Encryption Standard

AH
Authentication Header

BGP
Border Gateway Protocol

CA
Certificate Authority

CPE
Customer Premises Equipment

DES
Data Encryption Standard

EMS
Element Management System

ePPA
Processing ASIC

ESP
Encapsulating Security Payload

HMAC
Hash-Based Message Authentication Code

IKE
Internet Key Exchange

IKEv1
IKE version 1

IKEv2
IKE version 2

iPPA
Processing ASIC

IPsec
IP Security

MD5
Message Digest 5

PFS
Perfect Forward Secrecy

PKI
Public Key Infrastructure

PRF
Pseudo-Random Function

RSA
Rivest, Shamir and Adleman

SAs
Security Associations

SHA-1
Secure Hash Algorithm-1

SPI
Security Parameter Index

VPN
Virtual Private Network

Reference List

[1] *IPsec VPN Configuration and Operation Using the SmartEdge OS CLI*, 2/1543-CRA 119 1170/1-V1

[2] *IPsec VPN Command Reference*, 2/190 80-CRA 119 1170/1-V1