Chapter 10

Using IPSec to Protect Communications Between the SAE and CMTS Device

This chapter describes the SRC application's support for the *PacketCable Multimedia Specification* (PCMM) as defined by Cable Television Laboratories, Inc. (CableLabs). It contains the following sections:

If you use the SRC software to manage a PCMM environment, IP security (IPSec) protects communications between the SAE and RADIUS and between the SAE and the CMTS device. The *PacketCable Multimedia Specification* outlines the security requirements for communication between components in a PCMM environment.

Overview of IPSec

IPSec provides IP-level security for packets sent between specified hosts by using both authentication and encryption:

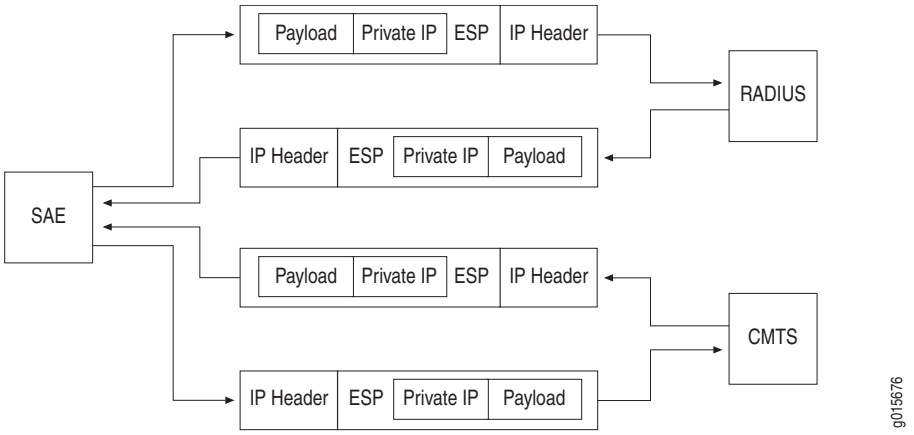
- Authentication ensures data integrity and verifies the identity of the sender and receiver.
- Encryption ensures data confidentiality; only the sender and intended recipient can read the information.

IPSec uses cryptographic keys during authentication and encryption. For authentication, the key and the data form a checksum value; for encryption, a key encrypts data before it is sent and decrypts data when it is received.

Before IPSec-protected communication can be established, both sender and receiver share configuration information with each other. As a result, IPSec defines a security association (SA), the set of security parameters that dictate how IPSec processes a packet, for a sender and for a receiver. These parameters include addressing and key information, both of which must be common to both hosts. Typically, a security association includes parameters for packets transmitted in one direction. Another security association is needed for packets transmitted in the opposite direction.

Figure 17 shows Encapsulating Security Payload (ESP) encapsulated packets sent between SAE and a RADIUS server, and between SAE and a CMTS device.

Figure 17: IPSec-Protected Communications



The SAE uses the IPSec implementation available on the Solaris platform on which the SAE runs. The SAE provides a configuration interface to simplify IPSec configuration for the SAE. For information about the IPSec implementation on the Solaris operating system, see the Sun product documentation at

http://docs.sun.com/app/docs/prod/solaris#hic

Security Keys

For a sender and receiver to participate in IPSec-protected communication, both must use the same type of key that is based on the algorithms used.

Key Types

IPSec uses different key algorithms for authentication and encryption. The SAE supports use of the following algorithms for authentication:

- Hashed Message Authentication Code using a Message Digest 5 key (HMAC-MD5)
- Hashed Message Authentication Code using a Secure Hash Standard 1 key (HMAC-SHA-1)

The SAE supports use of the following algorithms for encryption:

- Data Encryption Standard (DES)
- Triple Data Encryption Standard (3DES)
- Advanced Encryption Standard (AES)
- Blowfish

Which encryption algorithms are available depends on whether the system has the Solaris Encryption Kit installed. See the Solaris documentation for more information.

Key Management

The implementation of IPSec for the SAE uses automatic key management through Internet Key Management (IKE). IKE is a protocol that provides key generation and secure distribution. It also secures negotiations to create security associations.

The SAE configuration uses a preshared key for IKE negotiations. A preshared key is one whose value is shared by the administrators of the systems that participate in IPSec-protected communication. You define a value for the key and communicate the value of the key out-of-band to the system administrator who is configuring the CMTS device or RADIUS server. When you communicate the key value, make sure that only trusted parties have access to the key information.

NOTE: When you configure the value of this key for the SAE, you use SDX Configuration Editor. Anyone who can open SDX Configuration Editor can read the value for this key. The key value, however, is not stored in the LDAP directory.

Although SDX Configuration Editor supports only configuration of preshared keys, the Solaris operating system also supports certificate authentication. We recommend that you use preshared keys; however, you can configure certificate authentication directly from Solaris if required by your environment.

IPSec Configuration for the SAE

The SAE uses the IPSec implementation available on a system running the Solaris operating system version 5.9 or higher. These versions of the operating system support IKE.

SRC software configures basic IPSec parameters and provides a management interface in SDX Configuration Editor to simplify configuration tasks for properties specific to your environment. For example, the SAE configuration lets you configure the IP address to be used on the local host and the IP address to be used on the remote host for IPSec-protected traffic.

The basic IPSec configuration created by the SAE includes the following:

- IPv4 addressing—Supports IP addressing in the IPv4 format for local and remote identity types.
- Preshared keys—Lets you share key values between systems.
- Automatic key management through IKE—Manages security keys during negotiation of SAs.
- ESP—Provides confidentiality and authentication for each packet.
- IPSec transport mode—Specifies that ESP follow the IP header for a packet; ESP encapsulates the remainder of the packet.

Before You Configure IPSec

Before you start to configure IPSec for the SAE:

- Verify that the system on which the SAE is uses the Solaris operating system version 5.9 or higher.
- Verify which authentication algorithms and encryption algorithms are available on your Solaris platform.

  Which encryption algorithms are available depends on whether the system has the Solaris Encryption Kit installed. See the Solaris documentation for more information.
- Make sure that you are familiar with any configuration for IPSec present on the system running the SAE. If IPSec is already configured on the Solaris platform, make sure that system-wide policies are compatible with the IPSec configuration for SAE.

Before you start to configure IPSec from SDX Configuration Editor, collect the following information:

- Value of the preshared key

  Use a random key generator to obtain this value. To generate a random number, you can use the **od** command on a Solaris platform. See the Solaris documentation.
- Authentication algorithm to use
- Encryption algorithm to use
- IP address of the remote host
- (Optional) Port number to be used on the remote system

Protecting IPSec Configuration Properties

Make sure that a malicious user cannot obtain the IPSec configuration information. You can protect the configuration information by:

- Making configuration changes from the console of the terminal on which the SAE is running.
- Configuring SSH between the host from which you access the SAE and the host on which the SAE runs.

  See the documentation for these systems for information about setting up SSH between the hosts.

Configuring IPSec for the SAE

The procedure for configuring IPSec between the SAE and another application comprises the following steps:

1. Make sure that the authentication and encryption algorithms you plan to use are available on the local and remote hosts.
2. Configure IPSec on the system running the SAE.

   See *Configuring IPSec with SDX Configuration Editor* on page 95.
3. Configure IPSec on the remote system, such as a CMTS device or a RADIUS server.

   See the documentation for the remote system.
4. Test the IPSec connection. See the Solaris documentation.

NOTE: Before you activate the IPSec configuration, make sure that the IPSec configuration is working; otherwise, troubleshooting the IPSec configuration becomes very difficult.

Configuring IPSec with SDX Configuration Editor

You can use SDX Configuration Editor to configure IPSec properties required to protect traffic between the SAE and another system. For information about using SDX Configuration Editor, see *SRC-PE Getting Started Guide, Chapter 39, Using SDX Configuration Editor*.

To configure IPSec attributes from SDX Configuration Editor:

1. In the navigation pane of SDX Configuration Editor, right-click an object, select **SDX System Configuration**, and then select **New Configuration File**.
2. In the Create a New Configuration File dialog box, enter a filename in the File Name field, select ipSec_conf in the Template field, and click **OK**.

3. In the navigation pane, double-click the name of the new file.

   The IPSec Transport Connections pane appears.

4. Click **Solaris Hosts** to expand it, select **Host** in the drop-down list box, click **Create a New Instance of**, and enter the Instance Name in the Create a New Instance dialog box.

   The new instance appears.

5. Configure host properties. Use the field descriptions in *Configuring Host Properties* on page 96 to configure the properties.

6. Expand IPSec Connections; then for each connection, select **Connection** in the drop-down list box, click **Create a New Instance of**, and enter the Instance Name in the Create a New Instance dialog box.

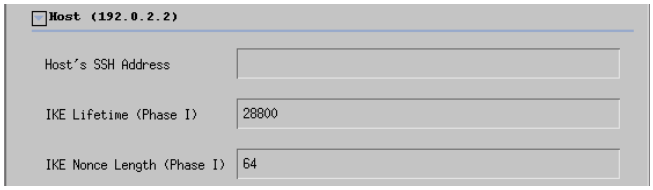
   The new connection instance appears.

7. Expand the Connection section for a specified connection, and enter field values. Use the field descriptions in *Configuring Connection Properties* on page 97 to configure the properties.

8. Expand the IPSec Details section for a specified connection, and enter field values. Use the field descriptions in *Configuring IPSec Properties to Establish Key Exchange and SAs* on page 99 to configure the properties.

Configuring Host Properties

Use the host properties area to define IPSec configuration properties for the Solaris platform.



Host's SSH Address

- IP address or hostname to be used for IPSec configuration on the Solaris platform.
- Value—IP address or fully qualified hostname used for IPSec configuration on the on the Solaris platform; can include the port for an SSH server.
- Default—No value
- Example

  IP address with port 22 for SSH—192.0.2.2:22

  Hostname—sae.company.com
- Property name—sshAddress

IKE Lifetime (Phase 1)

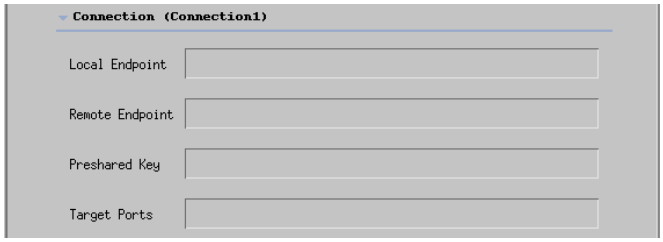
- Length of time phase 1 SA can be active for all IPSec connections on the Solaris platform.
- Value—Length of time in seconds
- Guidelines—We recommend a minimum lifetime of 28800 seconds (8 minutes).
- Default—28800
- Property name—ikeNonceLength

IKE Nonce Length (Phase 1)

- Size of the nonce token used during phase 1 of IKE negotiation.
- Value—Number of bytes in the range 1–64
- Guidelines—This property sets this value for all IPSec connections on the Solaris platform.
- Default—64
- Property name—ikeLifeTime

Configuring Connection Properties

Use the Connection properties area to define the source and destination for IPSec-protected communications, and the type of key to use in IKE negotiation.



Local Endpoint

- IP address for IPSec to use on the local Solaris platform on which the SAE is running.
- Value— < IP address >
- Guidelines—This is a required entry.
- Property name—localEndPt

Remote Endpoint

- IP address to use on the remote system.
- Value— < IP address >
- Guidelines—This is a required entry.
- Property name—RemoteEndPt

Preshared Key

- Value of the key to be shared between the SAE and the remote system. IKE negotiation uses this key.
- Value—A number in hexadecimal notation
- Guidelines—This is a required entry.

  The different IKE algorithms support keys of various lengths. In general, longer keys provide more security than shorter keys provide. The length of the key should comply with the security policies at your site.

  Protect the value of this key. Unauthorized access to the key value can compromise data that is protected by this key.

- Property name—presharedKey

Target Ports

- Well-known port numbers associated with applications that participate in IPSec-protected communications.
- Value—Port number associated with an application

  Blank—All port numbers

- Guidelines—This is a required entry.

  We recommend that the field remain blank to have IPSec protect all traffic between the local and remote systems.

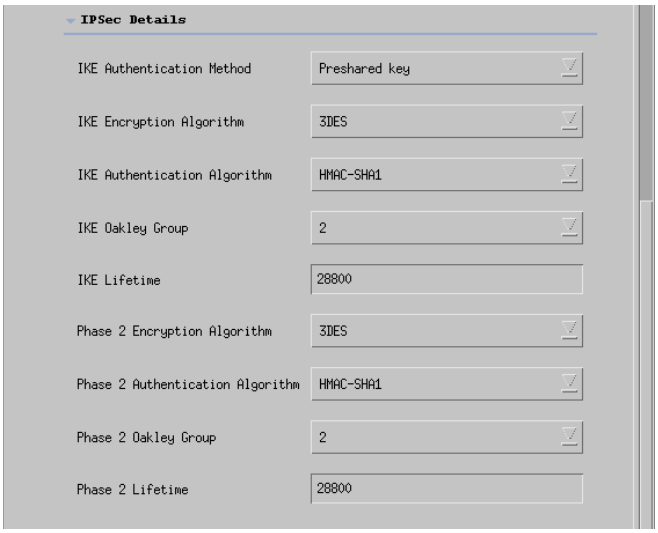
  If you specify port numbers, you can enter more than one port number, with commas separating the port numbers. The following list shows well-known port numbers for components in a PCMM environment:

  - RADIUS server—1812
  - RADIUS accounting—1813
  - COPS-PR (used for communication between the SAE and CMTS device)—3918

- Property name—targetPorts

Configuring IPSec Properties to Establish Key Exchange and SAs

Use the IPSec Details pane to configure properties to establish IKE, also referred to a phase 1 IKE exchange, and to set up an SA between peers, also referred to as phase 2 exchange. SDX Configuration Editor supplies default values for all fields. You can change values as needed.



IKE Authentication Method

- Authentication method used for IKE.
- Value—preshared key

NOTE: This value cannot be changed.

- Guidelines—This is a required entry.
- Property name—ikeAuthMethod

IKE Encryption Algorithm

- Encryption algorithm for use by during IKE negotiation.
- Values
  - DES
  - 3DES
  - AES
  - Blowfish
- Guidelines—This is a required entry.
- Default—DES
- Property name—ikeEncAlg

IKE Authentication Algorithm

- Authentication algorithm for use during IKE negotiation.
- Values
  - HMAC-MD5
  - HMAC-SHA-1
- Guidelines—This is a required entry.
- Default—HMAC-SHA-1
- Property name—ikeAuthAlg

IKE Oakley Group

- An Oakley group, the type of Diffie-Hellman key exchange algorithm that the Oakley key exchange protocol uses to distribute keying information during IKE negotiation. The Diffie-Hellman key exchange algorithm provides a way for two parties to exchange keying information and to agree on a shared key.
- Value
  - 1—768-bit Diffie-Hellman group
  - 2—1,024-bit Diffie-Hellman group
  - 5—1,536-bit Diffie-Hellman group
- Guidelines—This is a required entry.

  Group 1 provides the weakest security and group 5 the strongest security.
- Default—5
- Property name—ikeOakleyGroup

IKE Lifetime

- Length of time phase 1 SA can be active.
- Value—Length of time in seconds
- Default—28800
- Property name—ikeLifetime

Phase 2 Encryption Algorithm

- Encryption algorithm for use by IKE and is used during negotiation of the security association between hosts.
- Values
  - DES
  - 3DES
  - AES
  - Blowfish
- Guidelines—This is a required entry.

- Default—DES
- Property name—phase2EncAlg

Phase 2 Authentication Algorithm

- Authentication algorithm for use by IKE during negotiation of the security association between hosts.
- Value
  - HMAC-MD5
  - HMAC-SHA-1
- Guidelines—This is a required entry.
- Default—HMAC-SHA1
- Property name—phase2AuthAlg

Phase 2 Oakley Group

- An Oakley group, the type of Diffie-Hellman key exchange algorithm that the Oakley key exchange protocol uses to distribute keying information during SA negotiation. The Diffie-Hellman key exchange algorithm provides a way for two parties to exchange keying information and to agree on a shared key.
- Value
  - 1—768-bit Diffie-Hellman group
  - 2—1,024-bit Diffie-Hellman group
  - 5—1536-bit Diffie-Hellman group
- Guidelines—This is a required entry.

  Group 1 provides the weakest security and group 5 the strongest security.
- Default—5
- Property name—phase2OakleyGroup

Phase 2 Lifetime

- How long the SA between hosts can be active. At the end of the interval specified, the system refreshes the encryption key.
- Value— Length of time
- Default—28800 seconds
- Property name—phase2Lifetime

Applying the IPSec Configuration

After you configure IPSec properties, you can export the configuration properties to the Solaris operating system. The properties are applied to IPSec configuration for the Solaris platform on which the SAE is running.

To apply IPSec configuration properties.

1. In the navigation pane of SDX Configuration Editor, right-click the IPSec object, select **SDX System Configuration**, and then select **Export IPSec to Host**.

2. Select the host to which to export the configuration, and provide a password if you are using SSH between hosts.

   The Solaris platform activates the IPSec configuration.

Changing IPSec Configuration

To configure IPSec attributes from SDX Configuration Editor:

1. In the navigation pane of SDX Configuration Editor, double-click an IPSec object.

2. In the IPSec Transport Connections pane, change field values.

3. In the navigation pane, right-click the IPSec object, select **SDX System Configuration**, and then select **Export IPSec to Host**.

   The Solaris platform activates the updated IPSec configuration.

4. Make corresponding configuration changes on the system with which the SAE has IPSec-protected communication.

5. Test the updated configuration.

Configuring IPSec on a Remote System

For another system, such as a RADIUS server or a CMTS device, and the SAE to participate in IPSec-protected communications, make sure that the IPSec configuration for the remote system includes the values in Table 8. The table describes configuration properties as phase 1 or phase 2. Phase 1 indicates IKE phase 1 exchange and phase 2 indicates IKE phase 2 exchange.

Table 8: Configuration Properties for Remote Hosts

Configuration Property	Description of Value
IKE Configuration	
Phase 1 local identity type	IPv4
Phase 1 remote identity type	IPv4
IKE local identity	IP address for the application (CMTS device or RADIUS)
IKE remote identity	IP address of the SAE

Table 8: Configuration Properties for Remote Hosts (continued)

Configuration Property	Description of Value
Phase 1 authentication method	Preshared key
Phase 1 encryption algorithm	IKE encryption algorithm configured on the SAE
Phase 1 authentication algorithm	IKE authentication algorithm configured on the SAE
Phase 1 IKE mode	Main mode
Phase 1 Perfect Forward Security (PFS) group	IKE Oakley group configured on the SAE
Phase 1 lifetime	IKE lifetime configured on the SAE
Preshared key	Preshared key configured for the SAE
IPSec policy to secure traffic flow	Policy that ensures that traffic between applications is protected; for example, between SAE and RADIUS, or between SAE and CMTS device over COPS-PR
IPSec Policy Configuration	
Phase 2 encryption algorithm	Value configured on the SAE
Phase 2 authentication algorithm	Value configured on the SAE
Phase 2 PFS group	Phase 2 Oakley group configured on the SAE
Phase 2 lifetime	Value configured on the SAE

Testing the IPSec Connection

After you configure IPSec on the system running the SAE and on a remote host, make sure that the hosts are communicating over the connection. For information about testing and troubleshooting IPSec connections, see the IPSec documentation for the system running the SAE and the documentation for the remote system.