



VPN Acceleration Module 2 (SA-VAM2)

Revised: March 27, 2006, OL-9848-01
First Published: May, 19, 2003
Last Updated: April 24, 2005

This feature module describes the Service Adapter VPN Acceleration Module 2 (SA-VAM2) feature. It includes the following sections:

- [Feature Overview, page 1](#)
- [Supported Platforms, page 7](#)
- [Supported Standards, MIBs, and RFCs, page 8](#)
- [Prerequisites, page 8](#)
- [Configuration Tasks, page 8](#)
- [Troubleshooting Tips, page 26](#)
- [Monitoring and Maintaining, page 28](#)
- [Configuration Examples, page 30](#)
- [Command Reference, page 31](#)
- [Glossary, page 32](#)

Feature Overview

The Service Adapter VPN Acceleration Module 2 (SA-VAM2) is a port adapter that installs in any single port-adapter slot on the Cisco 7200VXR series routers with the network processing engine NPE-225, NPE-400, or NPE-G1, or on the Cisco 7301 router.



Note

The NPE-300 processor and the Network Services Engine (NSE-1) services accelerator are no longer sold.

SA-VAM2 provides high-performance, hardware-assisted tunneling and encryption services suitable for Virtual Private Network (VPN) remote access, site-to-site intranet, and extranet applications. It also provides platform scalability and security, while working with all services necessary for successful VPN deployments — security, quality of service (QoS), firewall and intrusion detection, service-level validation, and management. The SA-VAM2 off-loads IPSec processing from the main processor, thus freeing resources on the processor engines for other tasks.

The SA-VAM2 can be installed directly in the port adapter slots of the Cisco 7000VXR series routers and the Cisco 7301 router. Alternatively, you can install the SA-VAM2 into a Port Adapter Jacket Card (product ID:C7200-JC-PA) that is inserted in the I/O controller slot of a Cisco 7200VXR router with an NPE-G1 processor, for additional bandwidth.

The SA-VAM2 support in the Port Adapter Jacket Card allows you to take advantage of the increase in NPE-G1 performance, while maintaining VPN performance. You allow more bandwidth to the regular port adapter slots when you install the SA-VAM2 in the Port Adapter Jacket Card. See the [Port Adapter Jacket Card Installation Guide](#) for more information.

The SA-VAM2 provides hardware-accelerated support for multiple encryption functions:

- 128-bit Advanced Encryption Standard (AES) in hardware and 192/256 bits in microcoded firmware
- 56-bit Data Encryption Standard (DES) standard mode: Cipher Block Chaining (CBC)
- Performance to OC3 full duplex with 300 byte packets
- 5000 tunnels for DES/3DES/AES
- Provides compression with IPSec at no extra overhead
- 3-Key Triple DES (168-bit)
- Secure Hash Algorithm (SHA)-1 and Message Digest 5 (MD5) hash algorithms
- Rivest, Shamir, Adelman (RSA) public-key algorithm
- Diffie-Hellman key exchange RC4-40
- IPSec tunnel mode

Benefits

The SA-VAM2 provides the following benefits:

- Up to 50 tunnels per second



Note Actual performance may vary depending on overall system usage and system configuration. We recommend that you use 512 MB of memory for maximum performance.

- RSA encryption
- Accelerated Crypto performance
- Accelerated Internet Key Exchange (IKE): RFCs 2401-2411 and 2451
- Certificate support for automatic authentication using digital certificates
- Encryption services to any port adapter installed in the router. The interface on the port adapter must be configured with a crypto map to support IPSec.
- Full-duplex data transmission of over 100 Mbps with various encryption and compression schemes for 300 byte packages
- Hardware-based Layer 3 IPPCP LZS compression
- IPPCP: RFCs 2393 and 2395
- LAN/WAN interface selection: Works with most Cisco 7200VXR compatible port adapters
- Network traffic compression that reduces bandwidth utilization
- Online Insertion and Removal (OIR)

- QoS, multiprotocol, and multicast feature interoperation
- Support for full Layer 3 routing, such as Enhanced Interior Gateway Routing Protocol (EIGRP), Open Shortest Path First (OSPF), and Border Gateway Protocol (BGP) across the IPsec VPN
- Up to 256 Mbps throughput using AES
- VPN initialization improvements

Hardware Requirements

Specific hardware prerequisites that ensure proper operation of the SA-VAM2 follow:

- The SA-VAM2 on the Cisco 7200VXR routers requires a network processing engine 225 (NPE-225), 400 (NPE-400), or G1 (NPE-G1).
- The Cisco 7200VXR routers support up to two SA-VAM2s.
- The Cisco 7301 router supports a single SA-VAM2 in the port adapter slot.
- (Optional) SA-VAM2 is only supported in a Port Adapter Jacket Card on Cisco 7200VXR routers with an NPE-G1 processor. See the [Port Adapter Jacket Card Installation Guide](#) for more information about the Port Adapter Jacket Card.

Software Requirements

[Table 0-1](#) lists the recommended minimum Cisco IOS software release required to use the SA-VAM2 in supported router or switch platforms. Use the **show version** command to display the system software version that is currently loaded and running.

Table 0-1 SA-VAM2 Software Requirements

Platform	Recommended Minimum Cisco IOS Release
Cisco 7200VXR router ¹	Cisco IOS Release 12.3(1)M or a later release of Cisco IOS Release 12.3M Cisco IOS Release 12.3(2)T1 or a later release of Cisco IOS Release 12.3T1
Cisco 7301 router	Cisco IOS Release 12.3(3)M or a later release of Cisco IOS Release 12.3M Cisco IOS Release 12.3(2)T1 or a later release of Cisco IOS Release 12.3T1
(Optional) Cisco 7200VXR Router with the Port Adapter Jacket Card	Cisco IOS Release 12.4(6)T or later release of Cisco IOS Release 12.4T Cisco IOS Release 12.4(7) or later release of Cisco IOS Release 12.4M Note Available only on the Cisco 7200VXR router with the NPE-G1 processor.

1. The Cisco IOS Release 12.2(14)SU is no longer available for sale.

To check the minimum software requirements of Cisco IOS software with the hardware installed on your router, Cisco maintains the Software Advisor tool on Cisco.com. Registered Cisco Direct users can access the Software Advisor at: <http://www.cisco.com/cgi-bin/Support/CompNav/Index.pl>. This tool does not verify whether modules within a system are compatible, but it does provide the minimum Cisco IOS software requirements for individual hardware modules or components.



Note

Access to this tool is limited to users with Cisco.com login accounts.

Restrictions

The SA-VAM2 has the following restrictions:

- SA-VAM2 does not interoperate with other crypto cards, such as ISA, VAM, or SA-VAM2, in a single Cisco 7204VXR or Cisco 7206VXR. See [“Interoperability Between SA-VAM2, ISA, and SA-VAM” section on page 4](#).
- The Cisco 7301 router only supports a single port adapter.
- Dual SA-VAM2 cards are only supported on the Cisco 7200VXR routers with the NPE-G1 processor.
- For routers using SA-VAM2, we recommend a minimum configuration of 256 MB of memory; for more efficient performance, we recommend 512 MB of memory.
- (Optional) SA-VAM2 is only supported in a Port Adapter Jacket Card on Cisco 7200VXR routers with an NPE-G1 processor. See the [Port Adapter Jacket Card Installation Guide](#) for more information about the Port Adapter Jacket Card.

Interoperability Between SA-VAM2, ISA, and SA-VAM

[Table 2](#) describes the interoperability restrictions between ISA, VAM, and SA-VAM2.

Table 2 Interoperability Between SA-VAM2, VAM, and ISA

SA-VAM2 with ISA	SA-VAM2 with VAM	SA-VAM2 with SA-VAM2
<ul style="list-style-type: none"> • Supports MPPE 	<ul style="list-style-type: none"> • Does not support MPPE 	<ul style="list-style-type: none"> • Does not support MPPE
<ul style="list-style-type: none"> • Supports ISAKMP/IPSec 	<ul style="list-style-type: none"> • Supports ISAKMP/IPSec 	<ul style="list-style-type: none"> • Supports ISAKMP/IPSec
<ul style="list-style-type: none"> • If ISA and SA-VAM2 are enabled in the chassis at power up, ISA is used for MPPE, and SA-VAM2 is used for ISAKMP/IPSec, provided the router running configuration includes the encryption mppe command 	<ul style="list-style-type: none"> • If SA-VAM2 and VAM are in the chassis at power up, the router supports SA-VAM2, and VAM remains inactive 	<ul style="list-style-type: none"> • If SA-VAM2 and SA-VAM2 are enabled in the chassis at power up, the router supports both
<ul style="list-style-type: none"> • If ISA is enabled in the chassis at bootup, and SA-VAM2 is added later, the SA-VAM2 remains inactive until the next reboot, or until the configuration is changed to enable the SA-VAM2 	<ul style="list-style-type: none"> • If VAM is enabled in the chassis at bootup, and SA-VAM2 is added later, the SA-VAM2 remains inactive until the next reboot, or until the configuration is changed to enable the SA-VAM2 	<ul style="list-style-type: none"> • If SA-VAM2 is enabled in the chassis at bootup, and another SA-VAM2 is added later, the second SA-VAM2 immediately becomes active and depending on the configuration, the system attempts to load-balance between the two SA-VAM2s

Online Insertion and Removal (OIR)

The Online Insertion and Removal (OIR) feature is described in this section.

SA-VAM2

Online insertion and removal (OIR) is supported on the SA-VAM2. Before removing the SA-VAM2, we recommend that you shut down the interface so that there is no traffic running through the SA-VAM2 when it is removed. Removing a SA-VAM2 while traffic is flowing through the ports can cause system disruption. See the IPsec Stateful Failover (VPN High Availability) Feature Module at http://www.cisco.com/en/US/products/ps6550/products_white_paper09186a0080116d4c.shtml to assess the impact of OIR on the VAM2.

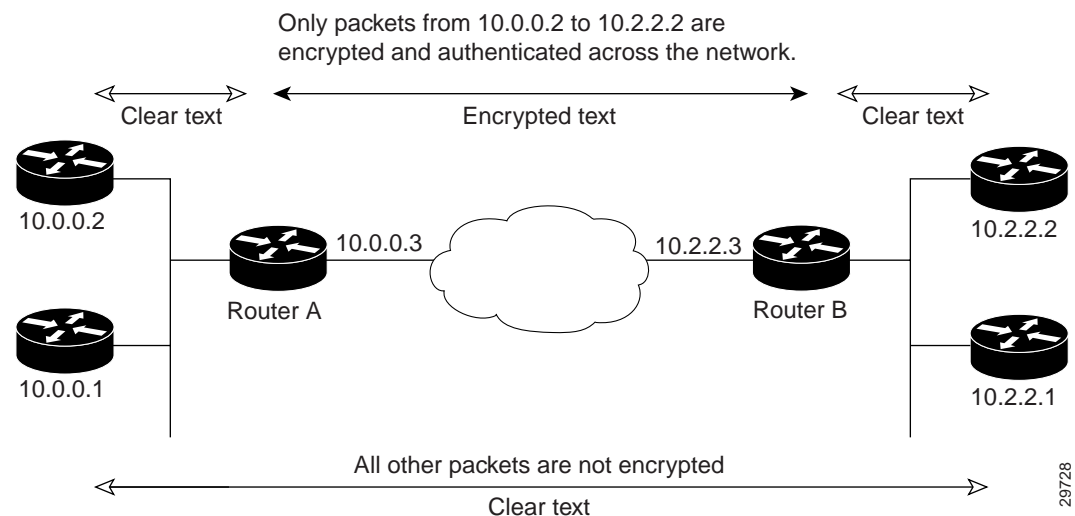
Port Adapter Jacket Card

OIR on the Port Adapter Jacket Card is not supported; however, the SA-VAM2 within the Port Adapter Jacket Card does support OIR. You must have the chassis powered off to install or remove the Port Adapter Jacket Card. See the [Port Adapter Jacket Card Installation Guide](#) for more information about the Port Adapter Jacket Card.

Basic IPsec Configuration Example

The following is an example of an IPsec configuration in which the security associations are established through IKE. In this example, an access list is used to restrict the packets that are encrypted and decrypted. In this example, all packets going from IP address 10.0.0.2 to IP address 10.2.2.2 are encrypted and decrypted and all packets going from IP address 10.2.2.2 to IP address 10.0.0.2 are encrypted and decrypted. Also, one IKE policy is created.

Figure 1 Basic IPsec Configuration



Router A Configuration

Specify the parameters to be used during an IKE negotiation:

```
crypto isakmp policy 15
  encryption des
  hash md5
  authentication pre-share
  group 2
  lifetime 5000

crypto isakmp key 1234567890 address 10.2.2.3
crypto isakmp identity address
```



Note

In the preceding example, the encryption DES of policy 15 would not appear in the written configuration because this is the default value for the encryption algorithm parameter.

A transform set defines how the traffic will be protected:

```
crypto ipsec transform-set auth1 ah-md5-hmac esp-des esp-md5-hmac
mode tunnel
```

A crypto map joins the transform set and specifies where the protected traffic is sent (the remote IPsec peer):

```
crypto map toRemoteSite 10 ipsec-isakmp
set peer 10.2.2.3
set transform-set auth1
```

The crypto map is applied to an interface:

```
interface Serial0
ip address 10.0.0.3
crypto map toRemoteSite
```

An IPsec access list defines which traffic to protect:

```
access-list 101 permit ip host 10.0.0.2 host 10.2.2.2
access-list 101 permit ip host 10.0.0.3 host 10.2.2.3
```

Router B Configuration

Specify the parameters to be used during an IKE negotiation:

```
crypto isakmp policy 15
  encryption des
  hash md5
  authentication pre-share
  group 2
  lifetime 5000

crypto isakmp key 1234567890 address 10.0.0.3
crypto isakmp identity address
```

A transform set defines how the traffic will be protected:

```
crypto ipsec transform-set auth1 ah-md5-hmac esp-des ah-md5-hmac
mode tunnel
```

A crypto map joins the transform set and specifies where the protected traffic is sent (the remote IPsec peer):

```
crypto map toRemoteSite 10 ipsec-isakmp
  set peer 10.0.0.3
  set transform-set auth1
```

The crypto map is applied to an interface:

```
interface Serial0
  ip address 10.2.2.3
  crypto map toRemoteSite
```

An IPSec access list defines which traffic to protect:

```
access-list 101 permit ip host 10.2.2.2 host 10.0.0.2
access-list 101 permit ip host 10.2.2.3 host 10.0.0.3
```

Related Features and Technologies

The following features and technologies are related to the SA-VAM2:

- Internet Key Exchange (IKE)
- IP Security (IPSec)

Related Documents

- The following document describes the Port Adapter Jacket Card:
[Port Adapter Jacket Card Installation Guide](#)
- The following document describes the SA-VAM2 hardware:
[VAM2 Installation and Configuration Guide](#)
- The following document describes the SA-VAM2 software:
[Release Notes for SA-VAM2](#)

Supported Platforms

The VPN Acceleration Module 2 (SA-VAM2) feature runs on the following platforms:

- Cisco 7200 series routers with single or dual SA-VAM2s on NPE-225, NPE-400, NSE-1, and NPE-G1
- Cisco 7301 routers

Finding Support Information for Platforms and Cisco IOS Software Images

Use Cisco Feature Navigator to find information about platform support and Cisco IOS software image support. Access Cisco Feature Navigator at <http://www.cisco.com/go/fn>. You must have an account on Cisco.com. If you do not have an account or have forgotten your username or password, click **Cancel** at the login dialog box and follow the instructions that appear.

Supported Standards, MIBs, and RFCs

Standards

- No new or modified standards are supported by this feature.

MIBs

The following MIBs were introduced or modified in this feature:

- CISCO-IPSEC-FLOW-MONITOR-MIB
- CISCO-IPSEC-MIB
- CISCO-IPSEC-POLICY-MAP-MIB

To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL:

<http://tools.cisco.com/ITDIT/MIBS/servlet/index>

If Cisco MIB Locator does not support the MIB information that you need, you can also obtain a list of supported MIBs and download MIBs from the Cisco MIBs page at the following URL:

<http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml>

To access Cisco MIB Locator, you must have an account on Cisco.com. If you have forgotten or lost your account information, send a blank e-mail to cco-locksmith@cisco.com. An automatic check will verify that your e-mail address is registered with Cisco.com. If the check is successful, account details with a new random password will be e-mailed to you. Qualified users can establish an account on Cisco.com by following the directions found at the following URL:

<http://www.cisco.com/register>

RFCs

- IPPCP: RFC 2393, 2395
- IPSec/IKE: RFCs 2401-2411, 2451

Prerequisites

You must configure IPSec and IKE on the router and a crypto map to all interfaces that require encryption service from the SA-VAM2. See the [“Configuration Examples” section on page 30](#) for configuration procedures.

Configuration Tasks

On power up if the enabled LED is on, the SA-VAM2 is fully functional and does not require any configuration commands. However, for the SA-VAM2 to provide encryption services, you must complete the steps in the following sections:

- [Using the EXEC Command Interpreter, page 9](#) (required)
- [Disabling OIR, page 9](#) (required)

- [Configuring an IKE Policy, page 10](#) (required)
- [Configuring a Transform Set, page 12](#) (required)
- [Configuring IPSec, page 15](#) (required)
- [Configuring Compression, page 24](#) (optional)

Optionally, you can configure certification authority (CA) interoperability (refer to the “Configuring Certification Authority Interoperability” chapter in the *Security Configuration Guide*).

Using the EXEC Command Interpreter

You modify the configuration of your router through the software command interpreter called the *EXEC* (also called enable mode). You must enter the privileged level of the EXEC command interpreter with the **enable** command before you can use the **configure** command to configure a new interface or change the existing configuration of an interface. The system prompts you for a password if one has been set.

The system prompt for the privileged level ends with a pound sign (#) instead of an angle bracket (>). At the console terminal, use the following procedure to enter the privileged level:

-
- Step 1** At the user-level EXEC prompt, enter the **enable** command. The EXEC prompts you for a privileged-level password as follows:
- ```
Router> enable

Password:
```
- Step 2** Enter the password (the password is case sensitive). For security purposes, the password is not displayed. When you enter the correct password, the system displays the privileged-level system prompt (#):
- ```
Router#
```
-

This completes the procedure for entering the privileged level of the EXEC command interpreter.

Disabling OIR

Online insertion and removal (OIR) on the SA-VAM2 is enabled by default.

To disable OIR of the SA-VAM2, use the following commands, starting in global configuration mode:

	Command	Purpose
Step 1	<code>no crypto engine accelerator <slot number></code>	Disables OIR on the SA-VAM2.
Step 2	<code>crypto engine accelerator <slot number></code>	Enables OIR on the SA-VAM2.

This completes the procedure for disabling and enabling OIR.

Configuring an IKE Policy

If you do not specify a value for a parameter, the default value is assigned. For information on default values, refer to the “IP Security and Encryption” chapter of the *Security Command Reference* publication.

To configure an IKE policy, use the following commands beginning in global configuration mode:

	Command	Purpose
Step 1	<code>Router(config)# crypto isakmp policy priority</code>	Defines an IKE policy and enters Internet Security Association Key Management Protocol (ISAKMP) policy configuration (config-isakmp) mode.
Step 2	<code>Router(config-isakmp)# encryption {des 3des aes aes 192 aes 256}</code>	Specifies the encryption algorithm within an IKE policy. <ul style="list-style-type: none"> • des—Specifies 56-bit DES as the encryption algorithm. • 3des—Specifies 168-bit DES as the encryption algorithm. • aes—Specifies 128-bit AES as the encryption algorithm. • aes 192—Specifies 192-bit AES as the encryption algorithm. • aes 256—Specifies 256-bit AES as the encryption algorithm.
Step 3	<code>Router(config-isakmp)# authentication {rsa-sig rsa-encr pre-share}</code>	(Optional) Specifies the authentication method within an IKE policy. <ul style="list-style-type: none"> • rsa-sig—Specifies Rivest, Shamir, and Adelman (RSA) signatures as the authentication method. • rsa-encr—SA-VAM2 does not support this authentication method. <p>Note Use RSA signature-based authentication without certification authority. To do this, apply the same configuration used for rsa-encr, but change the isakmp authentication method to rsa-sig.</p> <ul style="list-style-type: none"> • pre-share—Specifies preshared keys as the authentication method. <p>Note If this command is not enabled, the default value (rsa-sig) will be used.</p>
Step 4	<code>Router(config-isakmp)# lifetime seconds</code>	(Optional) Specifies the lifetime of an IKE security association (SA). <p><i>seconds</i>—Number of seconds that each SA should exist before expiring. Use an integer from 60 to 86,400 seconds.</p> <p>Note If this command is not enabled, the default value (86,400 seconds [one day]) will be used.</p>

	Command	Purpose
Step 5	Router(config-isakmp)# hash { sha md5 }	<p>(Optional) Specifies the hash algorithm within an IKE policy.</p> <ul style="list-style-type: none"> • sha—Specifies SHA-1 (HMAC variant) as the hash algorithm. • md5—Specifies MD5 (HMAC variant) as the hash algorithm. <p>Note If this command is not enabled, the default value (sha) will be used.</p>
Step 6	Router(config-isakmp)# group { 1 2 5 }	<p>(Optional) Specifies the Diffie-Hellman (DH) group identifier within an IKE policy.</p> <p>1—Specifies the 768-bit DH group. 2—Specifies the 1024-bit DH group. 5—Specifies the 1536-bit DH group.</p> <p>Note If this command is not enabled, the default value (768-bit) will be used.</p>

For detailed information on creating IKE policies, refer to the “Configuring Internet Key Exchange Security Protocol” chapter in the *Security Configuration Guide* publication.

Verifying IKE Configurations

To view information about your IKE configurations, use **show crypto isakmp policy EXEC** command.



Note

If a user enters an IKE encryption method that the hardware does not support, a warning message will be displayed in the **show crypto isakmp policy** output.

The following sample output from the **show crypto isakmp policy** command displays a warning message after a user tries to configure an IKE encryption method that the hardware does not support:

```
Router# show crypto isakmp policy

Protection suite of priority 1
  encryption algorithm: AES - Advanced Encryption Standard (256 bit keys).
WARNING:encryption hardware does not support the configured
encryption method for ISAKMP policy 1
  hash algorithm:      Secure Hash Standard
  authentication method: Pre-Shared Key
  Diffie-Hellman group: #1 (768 bit)
  lifetime:           3600 seconds, no volume limit
```

Configuring a Transform Set

See the [Advanced Encryption Standard \(AES\)](#) feature module for more information on configuring a transform set.

This section includes the following topics:

- [Defining a Transform Set, page 12](#) (required)
- [IPSec Protocols: AH and ESP, page 14](#) (optional)
- [Selecting Appropriate Transforms, page 14](#) (optional)
- [The Crypto Transform Configuration Mode, page 14](#) (optional)
- [Changing Existing Transforms, page 15](#) (optional)
- [Transform Example, page 15](#) (optional)

A transform set is an acceptable combination of security protocols, algorithms, and other settings to apply to IPSec protected traffic. During the IPSec security association (SA) negotiation, the peers agree to use a particular transform set when protecting a particular data flow.

Defining a Transform Set

A transform set is a combination of security protocols and algorithms. During the IPSec security association negotiation, peers agree to use a specific transform set to protect a particular data flow.

To define a transform set, use the following commands, starting in global configuration mode:

	Command	Purpose
Step 1	<pre>Router(config)# crypto ipsec transform-set transform-set-name transform1 [transform2 [transform3]]</pre>	Defines a transform set and enters crypto transform configuration mode. <ul style="list-style-type: none"> • <i>transform-set-name</i>—Specifies the name of the transform set to create (or modify). • <i>transform1 [transform2 [transform3] [transform4]]</i>—Defines the IPSec security protocols and algorithms. Accepted transform values are described in Table 3.
Step 2	<pre>Router(cfg-crypto-tran)# mode [tunnel transport]</pre>	(Optional) Changes the mode associated with the transform set. The mode setting is only applicable to traffic whose source and destination addresses are the IPSec peer addresses; it is ignored for all other traffic. (All other traffic is in tunnel mode only.)
Step 3	<pre>end</pre>	Exits the crypto transform configuration mode to enabled mode.
Step 4	<pre>clear crypto sa or clear crypto sa peer {ip-address peer-name} or clear crypto sa map map-name or clear crypto sa spi destination-address protocol spi</pre>	Clears existing IPSec security associations so that any changes to a transform set take effect on subsequently established security associations (SAs). (Manually established SAs are reestablished immediately.) Using the clear crypto sa command without parameters clears out the full SA database, which clears out active security sessions. You may also specify the peer , map , or entry keywords to clear out only a subset of the SA database.

Table 3 shows allowed transform combinations for the AH and ESP protocols.

Table 3 Allowed Transform Combinations

Transform type	Transform	Description
AH Transform (Pick up to one.)	ah-md5-hmac	AH with the MD5 (Message Digest 5) (HMAC variant) authentication algorithm
	ah-sha-hmac	AH with the SHA (Secure Hash Algorithm) (HMAC variant) authentication algorithm
ESP Encryption Transform (Note: If an ESP Authentication Transform is used, you must pick one.)	esp-aes	ESP with the 128-bit Advanced Encryption Standard (AES) encryption algorithm
	esp-aes 192	ESP with the 192-bit AES encryption algorithm
	esp-aes 256	ESP with the 256-bit AES encryption algorithm
	esp-des	ESP with the 56-bit Data Encryption Standard (DES) encryption algorithm
	esp-3des	ESP with the 168-bit DES encryption algorithm (3DES or Triple DES)
	esp-null	Null encryption algorithm
ESP Authentication Transform (Pick up to one.)	esp-md5-hmac	ESP with the MD5 (HMAC variant) authentication algorithm
	esp-sha-hmac	ESP with the SHA (HMAC variant) authentication algorithm
IP Compression Transform (Pick up to one.)	comp-lzs	IP compression with the Lempel-Ziv-Stac (LZS) algorithm

Examples of acceptable transform combinations are as follows:

- **ah-md5-hmac**
- **esp-des**
- **esp-3des** and **esp-md5-hmac**
- **ah-sha-hmac** and **esp-des** and **esp-sha-hmac**
- **comp-lzs**

The parser will prevent you from entering invalid combinations; for example, once you specify an AH transform it will not allow you to specify another AH transform for the current transform set.

IPSec Protocols: AH and ESP

Both the AH and ESP protocols implement security services for IPSec.

AH provides data authentication and antireplay services.

ESP provides packet encryption and optional data authentication and antireplay services.

ESP encapsulates the protected data—either a full IP datagram (or only the payload)—with an ESP header and an ESP trailer. AH is embedded in the protected data; it inserts an AH header immediately after the outer IP header and before the inner IP datagram or payload. Traffic that originates and terminates at the IPSec peers can be sent in either tunnel or transport mode; all other traffic is sent in tunnel mode. Tunnel mode encapsulates and protects a full IP datagram, while transport mode encapsulates/protects the payload of an IP datagram. For more information about modes, refer to the **mode** (IPSec) command description.

Selecting Appropriate Transforms

The following tips may help you select transforms that are appropriate for your situation:

- If you want to provide data confidentiality, include an ESP encryption transform.
- If you want to ensure data authentication for the outer IP header as well as the data, include an AH transform. (Some consider the benefits of outer IP header data integrity to be debatable.)
- If you use an ESP encryption transform, also consider including an ESP authentication transform or an AH transform to provide authentication services for the transform set.
- If you want data authentication (either using ESP or AH) you can choose from the MD5 or SHA (HMAC keyed hash variants) authentication algorithms. The SHA algorithm is generally considered stronger than MD5 but is slightly slower.
- Note that some transforms might not be supported by the IPSec peer.



Note If a user enters an IPSec transform that the hardware (the IPSec peer) does not support, a warning message will be displayed immediately after the **crypto ipsec transform-set** command is entered.

- In cases where you need to specify an encryption transform but do not actually encrypt packets, you can use the **esp-null** transform.

Suggested transform combinations follow:

- **esp-eas** and **esp-sha-hmac**
- **ah-sha-hmac** and **esp-eas** and **esp-sha-hmac**

The Crypto Transform Configuration Mode

After you issue the **crypto ipsec transform-set** command, you are put into the crypto transform configuration mode. While in this mode, you can change the mode to tunnel or transport. (These are optional changes.) After you have made these changes, type **exit** to return to global configuration mode. For more information about these optional changes, refer to the **match address** (IPSec) and **mode** (IPSec) command descriptions.

Changing Existing Transforms

If one or more transforms are specified in the **crypto ipsec transform-set** command for an existing transform set, the specified transforms will replace the existing transforms for that transform set.

If you change a transform set definition, the change is only applied to crypto map entries that reference the transform set. The change will not be applied to existing SAs, but will be used in subsequent negotiations to establish new SAs. If you want the new settings to take effect sooner, you can clear all or part of the SA database by using the **clear crypto sa** command.

Transform Example

The following example defines two transform sets. The first transform set will be used with an IPSec peer that supports the newer ESP and AH protocols. The second transform set will be used with an IPSec peer that only supports the older transforms.

```
crypto ipsec transform-set newer esp-3des esp-sha-hmac
crypto ipsec transform-set older ah-rfc-1828 esp-rfc1829
```

The following example is a sample warning message that is displayed when a user enters an IPSec transform that the hardware does not support:

```
crypto ipsec transform transform-1 esp-aes 256 esp-md5
WARNING:encryption hardware does not support transform
esp-aes 256 within IPSec transform transform-1
```

Configuring IPSec

This section includes the following topics:

- [Ensuring That Access Lists Are Compatible with IPSec, page 15](#) (required)
- [Setting Global Lifetimes for IPSec Security Associations, page 16](#) (required)
- [Creating Crypto Access Lists, page 16](#) (required)
- [Creating Crypto Map Entries, page 17](#) (required)
- [Creating Dynamic Crypto Maps, page 19](#) (required)
- [Applying Crypto Map Sets to Interfaces, page 21](#) (required)
- [Verifying IPSec Configurations, page 21](#) (optional)

For IPSec configuration examples, refer to the [“Configuring IPSec Example” section on page 30](#).

See the “Configuring IPSec Network Security” of the *Cisco IOS Security Configuration Guide* publication for more information on configuring IPSec.

Ensuring That Access Lists Are Compatible with IPSec

IKE uses UDP port 500. The IPSec Encapsulating Security Payload (ESP) and Authentication Header (AH) protocols use protocol numbers 50 and 51. Ensure that your interface access lists are configured so that protocol numbers 50, 51, and UDP port 500 traffic are not blocked at interfaces used by IPSec. In some cases you might need to add a statement to your access lists to explicitly permit this traffic.

Setting Global Lifetimes for IPSec Security Associations

You can change the global lifetime values which are used when negotiating new IPSec security associations. (These global lifetime values can be overridden for a particular crypto map entry).

These lifetimes only apply to security associations established via IKE. Manually established security associations do not expire.

To change a global lifetime for IPSec security associations, use one or more of the following commands in global configuration mode:

Step	Command	Purpose
Step 1	Router(config)# crypto ipsec security-association lifetime seconds seconds	Changes the global “timed” lifetime for IPSec SAs. This command causes the security association to time out after the specified number of seconds have passed.
Step 2	Router(config)# crypto ipsec security-association lifetime kilobytes kilobytes	Changes the global “traffic-volume” lifetime for IPSec SAs. This command causes the security association to time out after the specified amount of traffic (in kilobytes) have passed through the IPSec “tunnel” using the security association.
Step 3	Router(config)# clear crypto sa or Router(config)# clear crypto sa peer {ip-address peer-name} or Router(config)# clear crypto sa map map-name or Router (config)# clear crypto sa entry destination-address protocol spi	(Optional) Clears existing security associations. This causes any existing security associations to expire immediately; future security associations will use the new lifetimes. Otherwise, any existing security associations will expire according to the previously configured lifetimes. Note Using the clear crypto sa command without parameters will clear out the full SA database, which will clear out active security sessions. You may also specify the peer , map , or entry keywords to clear out only a subset of the SA database. For more information, see the clear crypto sa command.

Creating Crypto Access Lists

Crypto access lists define which IP traffic will be protected by encryption. (These access lists are *not* the same as regular access lists, which determine what traffic to forward or block at an interface.) For example, access lists can be created to protect all IP traffic between Subnet A and Subnet Y or Telnet traffic between Host A and Host B.

To create crypto access lists, use the following command in global configuration mode:

Step	Command	Purpose
Step 1	Router(config)# access-list <i>access-list-number</i> { deny permit } <i>protocol source source-wildcard destination destination-wildcard [log]</i> or Router(config)# ip access-list extended <i>name</i>	Specifies conditions to determine which IP packets will be protected. ¹ (Enable or disable crypto for traffic that matches these conditions.) We recommend that you configure “mirror image” crypto access lists for use by IPsec and that you avoid using the any keyword.
Step 2	Add permit and deny statements as appropriate.	Adds permit or deny statements to access lists.
Step 3	End	Exits the configuration command mode.

1. You specify conditions using an IP access list designated by either a number or a name. The **access-list** command designates a numbered extended access list; the **ip access-list extended** command designates a named access list.

For detailed information on configuring access lists, refer to the “Configuring IPsec Network Security” chapter in the *Cisco IOS Security Configuration Guide* publication.

Creating Crypto Map Entries

You can apply only one crypto map set to a single interface. The crypto map set can include a combination of IPsec/IKE and IPsec/manual entries. Multiple interfaces can share the same crypto map set if you want to apply the same policy to multiple interfaces.

To create crypto map entries that use IKE to establish the security associations, use the following commands, starting in global configuration mode:

	Command	Purpose
Step 1	Router(config)# crypto map <i>map-name seq-num ipsec-manual</i>	Specifies the crypto map entry to create (or modify). This command puts you into the crypto map configuration mode.
Step 2	Router(config-crypto-m)# match address <i>access-list-id</i>	Names an IPsec access list. This access list determines which traffic should be protected by IPsec and which traffic should not be protected by IPsec security in the context of this crypto map entry. (The access list can specify only one permit entry when IKE is not used.)
Step 3	Router(config-crypto-m)# set peer { <i>hostname</i> <i>ip-address</i> }	Specifies the remote IPsec peer. This is the peer to which IPsec protected traffic should be forwarded. (Only one peer can be specified when IKE is not used.)
Step 4	Router(config-crypto-m)# set transform-set <i>transform-set-name</i>	Specifies which transform set should be used. This must be the same transform set that is specified in the corresponding crypto map entry of the remote peer. (Only one transform set can be specified when IKE is not used.)

	Command	Purpose
Step 5	<pre>Router(config-crypto-m)# set session-key inbound ah spi hex-key-string and Router(config-crypto-m)# set session-key outbound ah spi hex-key-string</pre>	<p>Sets the AH Security Parameter Indexes (SPIs) and keys to apply to inbound and outbound protected traffic if the specified transform set includes the AH protocol.</p> <p>(This manually specifies the AH security association to be used with protected traffic.)</p>
Step 6	<pre>Router(config-crypto-m)# set session-key inbound esp spi cipher hex-key-string [authenticator hex-key-string] and Router(config-crypto-m)# set session-key outbound esp spi cipher hex-key-string [authenticator hex-key-string]</pre>	<p>Sets the ESP Security Parameter Indexes (SPIs) and keys to apply to inbound and outbound protected traffic if the specified transform set includes the ESP protocol. Specifies the cipher keys if the transform set includes an ESP cipher algorithm. Specifies the authenticator keys if the transform set includes an ESP authenticator algorithm.</p> <p>(This manually specifies the ESP security association to be used with protected traffic.)</p>
Step 7	<pre>Router(config-crypto-m)# exit</pre>	Exits crypto-map configuration mode and return to global configuration mode.

To create crypto map entries that will use IKE to establish the security associations, use the following commands starting in global configuration mode:

	Command	Purpose
Step 1	<pre>Router(config)# crypto map map-name seq-num ipsec-isakmp</pre>	<p>Names the crypto map entry to create (or modify). This command puts you into the crypto map configuration mode.</p>
Step 2	<pre>Router(config-crypto-m)# match address access-list-id</pre>	Names an extended access list. This access list determines which traffic should be protected by IPSec and which traffic should not be protected by IPSec security in the context of this crypto map entry.
Step 3	<pre>Router(config-crypto-m)# set peer {hostname ip-address}</pre>	<p>Specifies a remote IPSec peer. This is the peer to which IPSec protected traffic can be forwarded.</p> <p>Repeat for multiple remote peers.</p>
Step 4	<pre>Router(config-crypto-m)# set transform-set transform-set-name1 [transform-set-name2...transform-set-name6]</pre>	Specifies which transform sets are allowed for this crypto map entry. List multiple transform sets in order of priority (highest priority first).
Step 5	<pre>Router(config-crypto-m)# set security-association lifetime seconds seconds and Router (config-crypto-m)# set security-association lifetime kilobytes kilobytes</pre>	<p>(Optional) Specifies a security association lifetime for the crypto map entry.</p> <p>Use this command if you want the security associations for this crypto map entry to be negotiated using different IPSec security association lifetimes than the global lifetimes.</p>

	Command	Purpose
Step 6	Router(config-crypto-m)# set security-association level per-host	<p>(Optional) Specifies that separate security associations should be established for each source/destination host pair.</p> <p>Without this command, a single IPsec “tunnel” could carry traffic for multiple source hosts and multiple destination hosts.</p> <p>With this command, when the router requests new security associations it will establish one set for traffic between Host A and Host B, and a separate set for traffic between Host A and Host C.</p> <p>Use this command with care, as multiple streams between given subnets can rapidly consume resources.</p>
Step 7	Router(config-crypto-m)# set pfs [group1 group2]	(Optional) Specifies that IPsec should ask for perfect forward secrecy (PFS) when requesting new security associations for this crypto map entry, or should demand PFS in requests received from the IPsec peer.
Step 8	Router(config-crypto-m)# exit	Exits crypto-map configuration mode and return to global configuration mode.

Creating Dynamic Crypto Maps

A dynamic crypto map entry is a crypto map entry with some parameters not configured. The missing parameters are later dynamically configured (as the result of an IPsec negotiation). Dynamic crypto maps are only available for use by IKE.

Dynamic crypto map entries are grouped into sets. A set is a group of dynamic crypto map entries all with the same *dynamic-map-name*, each with a different *dynamic-seq-num*.

To create a dynamic crypto map entry, use the following commands starting in global configuration mode:

	Command	Purpose
Step 1	Router(config)# crypto dynamic-map <i>dynamic-map-name</i> <i>dynamic-seq-num</i>	Creates a dynamic crypto map entry.
Step 2	Router(config-crypto-m)# set transform-set <i>transform-set-name1</i> [<i>transform-set-name2</i> ... <i>transform-set-name6</i>]	<p>Specifies which transform sets are allowed for the crypto map entry. List multiple transform sets in order of priority (highest priority first).</p> <p>This is the only configuration statement required in dynamic crypto map entries.</p>

	Command	Purpose
Step 3	Router(config-crypto-m)# match address <i>access-list-id</i>	<p>(Optional) Accesses list number or name of an extended access list. This access list determines which traffic should be protected by IPsec and which traffic should not be protected by IPsec security in the context of this crypto map entry.</p> <p>Note Although access lists are optional for dynamic crypto maps, they are highly recommended.</p> <p>If this is configured, the data flow identity proposed by the IPsec peer must fall within a permit statement for this crypto access list.</p> <p>If this is not configured, the router will accept any data flow identity proposed by the IPsec peer. However, if this is configured but the specified access list does not exist or is empty, the router will drop all packets. This is similar to static crypto maps because they also require that an access list be specified.</p> <p>Care must be taken if the any keyword is used in the access list, because the access list is used for packet filtering as well as for negotiation.</p>
Step 4	Router(config-crypto-m)# set peer { <i>hostname</i> <i>ip-address</i> }	<p>(Optional) Specifies a remote IPsec peer. Repeat for multiple remote peers.</p> <p>This is rarely configured in dynamic crypto map entries. Dynamic crypto map entries are often used for unknown remote peers.</p>
Step 5	Router(config-crypto-m)# set security-association lifetime seconds <i>seconds</i> and Router (config-crypto-m)# set security-association lifetime kilobytes <i>kilobytes</i>	<p>(Optional) If you want the security associations for this crypto map to be negotiated using shorter IPsec security association lifetimes than the globally specified lifetimes, specify a key lifetime for the crypto map entry.</p>
Step 6	Router(config-crypto-m)# set pfs [<i>group1</i> <i>group2</i>]	<p>(Optional) Specifies that IPsec should ask for perfect forward secrecy when requesting new security associations for this crypto map entry or should demand perfect forward secrecy in requests received from the IPsec peer.</p>
Step 7	Router(config-crypto-m)# exit	Exits crypto-map configuration mode and return to global configuration mode.
Step 8	Repeat these steps to create additional crypto map entries as required.	

To add a dynamic crypto map set into a crypto map set, use the following command in global configuration mode:

Command	Purpose
Router(config)# crypto map <i>map-name seq-num</i> ipsec-isakmp dynamic <i>dynamic-map-name</i>	Adds a dynamic crypto map set to a static crypto map set.

Applying Crypto Map Sets to Interfaces

Apply a crypto map set to each interface through which IPsec traffic will flow. Crypto maps instruct the router to evaluate the interface traffic against the crypto map set and use the specified policy during connection or security association negotiation on behalf of traffic to be protected by crypto.

To apply a crypto map set to an interface, use the following command in interface configuration mode:

Command	Purpose
Router(config-if)# crypto map <i>map-name</i>	Applies a crypto map set to an interface.

To specify redundant interfaces and name an identifying interface, use the following command in global configuration mode:

Command	Purpose
Router(config)# crypto map <i>map-name</i> local-address <i>interface-id</i>	Permits redundant interfaces to share the same crypto map, using the same local identity.

Verifying IPsec Configurations

Some configuration changes take effect only after subsequent security associations are negotiated. For the new settings to take effect immediately, clear the existing security associations.

To clear (and reinitialize) IPsec security associations, use one of the commands in [Table 4](#) in global configuration mode:

Table 4 Commands to Clear IPsec Security Associations

Command	Purpose
clear crypto sa or clear crypto sa peer { <i>ip-address</i> <i>peer-name</i> } or clear crypto sa map <i>map-name</i> or clear crypto sa spi <i>destination-address</i> <i>protocol spi</i>	Clear IPsec security associations (SAs). Using the clear crypto sa command without parameters clears out the full SA database, which clears out active security sessions. You may also specify the peer , map , or spi keywords to clear out only a subset of the SA database.

The following steps provide information on verifying your configurations:

Step 1 Enter the **show crypto ipsec transform-set** command to view your transform set configuration:

```
Router# show crypto ipsec transform-set
Transform set combined-des-md5: {esp-des esp-md5-hmac}
    will negotiate = {Tunnel,},
Transform set t1: {esp-des esp-md5-hmac}
    will negotiate = {Tunnel,},
Transform set t100: {ah-sha-hmac}
    will negotiate = {Transport,},
Transform set t2: {ah-sha-hmac}
    will negotiate = {Tunnel,},
    {esp-des}
    will negotiate = {Tunnel,},
```



Note

If a user enters an IPSec transform that the hardware (the IPSec peer) does not support, a warning message will be displayed in the **show crypto ipsec transform-set** output.

The following sample output from the **show crypto ipsec transform-set** command displays a warning message after a user tries to configure an IPSec transform that the hardware does not support:

```
Router# show crypto ipsec transform-set
Transform set transform-1:{esp-256-aes esp-md5-hmac}
    will negotiate = {Tunnel, },

WARNING:encryption hardware does not support transform
esp-aes 256 within IPSec transform transform-1
```

Step 2 Enter the **show crypto map [interface interface | tag map-name]** command to view your crypto map configuration:

```
Router# show crypto map
Crypto Map: "router-alice" idb: Ethernet0 local address: 172.21.114.123
Crypto Map "router-alice" 10 ipsec-isakmp
    Peer = 172.21.114.67
    Extended IP access list 141
        access-list 141 permit ip
            source: addr = 172.21.114.123/0.0.0.0
            dest:   addr = 172.21.114.67/0.0.0.0
    Current peer: 172.21.114.67
    Security-association lifetime: 4608000 kilobytes/120 seconds
    PFS (Y/N): N
    Transform sets={t1,}
```

Step 3 Enter the **show crypto ipsec sa [map map-name | address | identity | detail | interface]** command to view information about IPSec security associations:

```
Router# show crypto ipsec sa
interface: Ethernet0
    Crypto map tag: router-alice, local addr. 172.21.114.123
    local ident (addr/mask/prot/port): (172.21.114.123/255.255.255.255/0/0)
    remote ident (addr/mask/prot/port): (172.21.114.67/255.255.255.255/0/0)
    current_peer: 172.21.114.67
        PERMIT, flags={origin_is_acl,}
    #pkts encaps: 10, #pkts encrypt: 10, #pkts digest 10
    #pkts decaps: 10, #pkts decrypt: 10, #pkts verify 10
    #send errors 10, #recv errors 0
        local crypto endpt.: 172.21.114.123, remote crypto endpt.: 172.21.114.67
    path mtu 1500, media mtu 1500
```

```

current outbound spi: 20890A6F
inbound esp sas:
  spi: 0x257A1039(628756537)
    transform: esp-des esp-md5-hmac,
    in use settings ={Tunnel,}
    slot: 0, conn id: 26, crypto map: router-alice
    sa timing: remaining key lifetime (k/sec): (4607999/90)
    IV size: 8 bytes
    replay detection support: Y
inbound ah sas:
outbound esp sas:
  spi: 0x20890A6F(545852015)
    transform: esp-des esp-md5-hmac,
    in use settings ={Tunnel,}
    slot: 0, conn id: 27, crypto map: router-alice
    sa timing: remaining key lifetime (k/sec): (4607999/90)
    IV size: 8 bytes
    replay detection support: Y
outbound ah sas:
interface: Tunnel0
Crypto map tag: router-alice, local addr. 172.21.114.123
local ident (addr/mask/prot/port): (172.21.114.123/255.255.255.255/0/0)
remote ident (addr/mask/prot/port): (172.21.114.67/255.255.255.255/0/0)
current peer: 172.21.114.67
  PERMIT, flags={origin_is_acl,}
#pkts encaps: 10, #pkts encrypt: 10, #pkts digest 10
#pkts decaps: 10, #pkts decrypt: 10, #pkts verify 10
#send errors 10, #recv errors 0
local crypto endpt.: 172.21.114.123, remote crypto endpt.: 172.21.114.67
path mtu 1500, media mtu 1500
current outbound spi: 20890A6F
inbound esp sas:
  spi: 0x257A1039(628756537)
    transform: esp-des esp-md5-hmac,
    in use settings ={Tunnel,}
    slot: 0, conn id: 26, crypto map: router-alice
    sa timing: remaining key lifetime (k/sec): (4607999/90)
    IV size: 8 bytes
    replay detection support: Y
inbound ah sas:
outbound esp sas:
  spi: 0x20890A6F(545852015)
    transform: esp-des esp-md5-hmac,
    in use settings ={Tunnel,}
    slot: 0, conn id: 27, crypto map: router-alice
    sa timing: remaining key lifetime (k/sec): (4607999/90)
    IV size: 8 bytes
    replay detection support: Y
outbound ah sas:

```

For a detailed description of the information displayed by the **show** commands, refer to the “IP Security and Encryption” chapter of the *Security Command Reference* publication.

Configuring Compression

This section includes the following topics:

- [Configuring IKE Policy, page 24](#) (required)
- [Configuring IKE Preshared Key, page 24](#) (required)
- [Configuring an IPSec Transform Set, page 25](#) (required)
- [Configuring Access Lists, page 25](#) (required)
- [Configuring Crypto Maps, page 25](#) (required)
- [Applying crypto map to the Interface, page 26](#) (required)

For IPSec configuration examples, refer to the “[Configuring IPSec Example](#)” section on page 30.

See the “Configuring IPSec Network Security” of the *Cisco IOS Security Configuration Guide* publication for more information on configuring IPSec.

Configuring IKE Policy

To configure IKE policy, follow the steps in “[Configuring an IKE Policy](#)” section on page 10, using the commands in global configuration mode.

Configuring IKE Preshared Key

To specify preshared keys at a peer, use the following commands in global configuration mode:

	Command	Purpose
Step 1	<pre>Router (config)# crypto isakmp key <i>keystring</i> address peer-address or Router (config)# crypto isakmp key <i>keystring</i> hostname peer-hostname</pre>	<p>At the local peer: Specify the shared key to be used with a particular remote peer.</p> <p>If the remote peer specified their ISAKMP identity with an address, use the address keyword in this step; otherwise use the hostname keyword in this step.</p>
Step 2	<pre>Router (config)# crypto isakmp key_<i>keystring</i> address peer-address or Router (config)# crypto isakmp key_<i>keystring</i> hostname peer-hostname</pre>	<p>At the remote peer: Specify the shared key to be used with the local peer. This is the same key you just specified at the local peer.</p> <p>If the local peer specified their ISAKMP identity with an address, use the address keyword in this step; otherwise use the hostname keyword in this step.</p>
Step 3	Repeat the previous two steps for each remote peer.	

Remember to repeat these tasks at each peer that uses preshared in an IKE policy.

Configuring an IPSec Transform Set

To define a transform set—an acceptable combination of security protocols and algorithms—use the **crypto ipsec transform-set global** configuration command. To delete a transform set, use the **no** form of the command.

Command	Purpose
Router (config)# crypto ipsec transform-set <i>transform-set-name transform1 [transform2 [transform3]]</i>	<i>transform-set-name</i> Specify the name of the transform set to create (or modify). <i>transform1</i> <i>transform2</i> <i>transform3</i> Specify up to three transforms (one is required) that define the IPSec security protocol(s) and algorithm(s).

Configuring Access Lists

To establish MAC address access lists, use the **access-list** global configuration command. To remove a single access list entry, use the **no** form of this command.

Command	Purpose
Router (config)# access-list <i>access-list-number {permit deny} address mask</i>	<i>access-list-number</i> Specify an integer from 700 to 799 that you select for the list. permit Permits the frame. deny Denies the frame. <i>address mask</i> Specify 48-bit MAC addresses written in dotted triplet form. The ones bits in the mask argument are the bits to be ignored in the address value.

Configuring Crypto Maps

To create crypto map entries that use IKE to establish the security associations, use the following commands, starting in global configuration mode:

	Command	Purpose
Step 1	Router (config)# crypto map <i>map-name seq-num ipsec-isakmp</i>	Create the crypto map and enter crypto map configuration mode.
Step 2	Router (config)# set peer { <i>hostname ip-address</i> }	Specify a remote IPSec peer. This is the peer to which IPSec-protected traffic can be forwarded. Repeat for multiple remote peers.

	Command	Purpose
Step 3	Router (config)# set transform-set <i>transform-set-name1</i> <i>[transform-set-name2...transform-set-name6]</i>	Specify which transform sets are allowed for this crypto map entry. List multiple transform sets in order of priority (highest priority first).
Step 4	Router (config)# match address <i>access-list-id</i>	Specify an extended access list. This access list determines which traffic is protected by IPSec and which is not.

Applying crypto map to the Interface

To apply a crypto map set to an interface, use the following commands, starting in global configuration mode:

	Command	Purpose
Step 1	Router (config)# interface <i>type number</i>	Specify an interface on which to apply the crypto map and enter interface configuration mode.
Step 2	Router (config)# crypto map <i>map-name</i>	Apply a crypto map set to an interface.
Step 3	Router (config)# end	Exit interface configuration mode.

This completes the process for configuring compression on the VAM2.

Troubleshooting Tips

To verify that Cisco IOS software has recognized SA-VAM2, enter the **show diag** command and check the output. For example, when the router has the SA-VAM2 in slot 1, the following output appears:

```
Router# show diag
Slot 6:
VAM2 Encryption/Compression engine, Port adapter
Port adapter is analyzed
Port adapter insertion time 00:01:32 ago
EEPROM contents at hardware discovery:
Hardware Revision      :1.0
PCB Serial Number     :
Part Number           :73-8491-00
Board Revision        :
RMA Test History      :00
RMA Number            :0-0-0-0
RMA History           :00
Deviation Number      :0-0
Product Number        :SA-VAM2
Top Assy. Part Number :800-22836-00
CLEI Code             :
EEPROM format version 4
EEPROM contents (hex):
0x00:04 FF 40 03 E4 41 01 00 C1 8B 00 00 00 00 00 00
0x10:00 00 00 00 00 82 49 21 2B 00 42 00 00 03 00 81
0x20:00 00 00 00 04 00 80 00 00 00 00 CB 94 53 41 2D
0x30:56 41 4D 32 20 20 20 20 20 20 20 20 20 20 20 20
0x40:20 C0 46 03 20 00 59 34 00 C6 8A 00 00 00 00 00
```

```

0x50:00 00 00 00 00 FF FF FF FF FF FF FF FF FF FF FF
0x60:FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF
0x70:FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF

```

To see if the SA-VAM2 is currently processing crypto packets, enter the **show pas vam2 interface** command. The following is sample output:

```

Router# show pas vam2 interface
VPN Acceleration Module Version II in slot : 3
Statistics for Hardware VPN Module since the last clear
of counters 314 seconds ago
      5290894 packets in                5290895 packets out
1882478960 bytes in                   1327439698 bytes out
      16850 paks/sec in                 16850 paks/sec out
      47940 Kbits/sec in                33805 Kbits/sec out
      4222173 pkts compressed           0 pkts not compressed
1190662374 bytes before compress      405331872 bytes after compress
      2.9:1 compression ratio           2.9:1 overall
      58 commands out                   58 commands acknowledged

Last 5 minutes:
      4855704 packets in                4855705 packets out
      16185 paks/sec in                 16185 paks/sec out
      46723079 bits/sec in              32921855 bits/sec out

Errors:
  ppq full errors      :      0  ppq rx errors      :      0
  cmdq full errors    :      0  cmdq rx errors    :      0
  no buffer            :      0  replay errors     :      0
  dest overflow       :      0  authentication errors :      0
  Other error         :      0  RNG self test fail  :      0
  DF Bit set          :      0  Hash Miscompare    :      0
Unwrappable object   :      0  Missing attribute   :      0
  Invalid attribute value:      0  Bad Attribute       :      0
  Verification Fail     :      0  Decrypt Failure     :      0
  Invalid Packet        :      0  Invalid Key         :      0
  Input Overrun         :      0  Input Underrun     :      0
  Output buffer overrun :      0  Bad handle value    :      0
  Invalid parameter     :      0  Bad function code   :      0
  Out of handles        :      0  Access denied       :      0

Warnings:
  sessions_expired     :      0  packets_fragmented  :      0
  general               :      0  compress_bypassed   :      4

HSP details:
  hsp_operations       :      75  hsp_sessions        :      6

```

When the SA-VAM2 processes packets, the “packets in” and “packets out” counter changes. Counter “packets out” represents the number of packets directed to the SA-VAM2. Counter “packets in” represents the number of packets received from the SA-VAM2.



Note

The **show pas vam2 interface** command output includes ‘compression ratio’ (or the efficiency of the tunnel bandwidth) which represents the ratio of the original packet to the compressed packet plus the IPSec headers. It does not represent the ratio of the IPSec payload before compression to the IPSec payload after compression.

This ratio may fall below 1 when small packets are not compressible, resulting in the ratio representing unencrypted packets to the encrypted packets plus the IPSec header.

To see if the IKE/IPSec packets are being redirected to the SA-VAM2 for IKE negotiation and IPSec encryption and decryption, enter the **show crypto eli** command. The following is sample output when Cisco IOS software redirects packets to SA-VAM2:

```
Router# show crypto eli
Hardware Encryption Layer : ACTIVE
Number of crypto engines = 1 .

CryptoEngine-0 (slot-5) details.
Capability-IPSec :IPPCP, 3DES, AES, RSA

IKE-Session   :    0 active,  5120 max,  0 failed
DH-Key        :    0 active,  5120 max,  0 failed
IPSec-Session :    0 active, 10230 max,  0 failed
```

When the software crypto engine is active, the **show crypto eli** command yields no output.

During bootup or OIR, when the Cisco IOS software agrees to redirect crypto traffic to the SA-VAM2, it prints a message similar to the following:

```
%ISA-6-INFO:Recognised crypto engine (0) at slot-1
...switching to hardware crypto engine
```

To disable the SA-VAM2, use the configuration mode **no crypto engine accelerator <slot>** command, as follows:

```
Router(config)# no crypto engine accelerator <slot>
Router#
3w4d:%ISA-6-SHUTDOWN:SA-VAM2 shutting down
3w4d:%ISA-6-INFO:Crypto Engine 0 in slot 1 going DOWN
3w4d:...switching to software crypto engine
```

Monitoring and Maintaining

Use the commands that follow to monitor and maintain the SA-VAM2:

Command	Purpose
Router# show pas isa interface	Displays the ISA interface configuration.
Router# show pas isa controller	Displays the ISA controller configuration.
Router# show pas vam2 interface	Verifies the SA-VAM2 is currently processing crypto packets.
Router# show pas vam2 controller	Displays the SA-VAM2 controller configuration.
Router# Show version	Displays integrated service adapter as part of the interfaces.

To clear (and reinitialize) IPsec security associations, use one of the following commands in global configuration mode:

Command	Purpose
<pre>Router(config)# clear crypto sa</pre> <p>or</p> <pre>Router(config)# clear crypto sa peer {ip-address peer-name}</pre> <p>or</p> <pre>Router(config)# clear crypto sa map map-name</pre> <p>or</p> <pre>Router(config)# clear crypto sa entry destination-address protocol spi</pre>	<p>Clears IPsec security associations.</p> <p>Note Using the clear crypto sa command without parameters will clear out the full SA database, which will clear out active security sessions. You may also specify the peer, map, or entry keywords to clear out only a subset of the SA database. For more information, see the clear crypto sa command.</p>

To view information about your IPsec configuration, use one or more of the following commands in EXEC mode:

Command	Purpose
<pre>Router# show crypto ipsec transform-set</pre>	Displays your transform set configuration.
<pre>Router# show crypto map [interface interface tag map-name]</pre>	Displays your crypto map configuration.
<pre>Router# show crypto ipsec sa [map map-name address identity] [detail]</pre>	Displays information about IPsec security associations.
<pre>Router# show crypto dynamic-map [tag map-name]</pre>	Displays information about dynamic crypto maps.
<pre>Router# show crypto ipsec security-association lifetime</pre>	Displays global security association lifetime values.

Configuration Examples

This section provides the following configuration examples:

- [Configuring IKE Policies Example, page 30](#)
- [Configuring IPsec Example, page 30](#)
- [Configuring Compression Example, page 31](#)

Configuring IKE Policies Example

In the following example, two IKE policies are created, with policy 15 as the highest priority, policy 20 as the next priority, and the existing default priority as the lowest priority. It also creates a preshared key to be used with policy 20 with the remote peer whose IP address is 192.168.224.33.

```
crypto isakmp policy 15
  encryption 3des
  hash md5
  authentication rsa-sig
  group 2
  lifetime 5000
crypto isakmp policy 20
  authentication pre-share
  lifetime 10000
crypto isakmp key 1234567890 address 192.168.224.33
```

Configuring IPsec Example

The following example shows a minimal IPsec configuration where the security associations will be established via IKE:

An IPsec access list defines which traffic to protect:

```
access-list 101 permit ip 10.0.0.0 0.0.0.255 10.2.2.0 0.0.0.255
```

A transform set defines how the traffic will be protected. In this example, transform set “myset1” uses DES encryption and SHA for data packet authentication:

```
crypto ipsec transform-set myset1 esp-des esp-sha
```

Another transform set example is “myset2,” which uses Triple DES encryptions and MD5 (HMAC variant) for data packet authentication:

```
crypto ipsec transform-set myset2 esp-3des esp-md5-hmac
```

A crypto map joins together the IPsec access list and transform set and specifies where the protected traffic is sent (the remote IPsec peer):

```
crypto map toRemoteSite 10 ipsec-isakmp
  match address 101
  set transform-set myset2
  set peer 10.2.2.5
```

The crypto map is applied to an interface:

```
interface Serial0
  ip address 10.0.0.2
```

```
crypto map toRemoteSite
```

**Note**

In this example, IKE must be enabled.

Configuring Compression Example

The following example shows a simple configuration example for configuring compression.

To configure an IKE policy:

```
crypto isakmp policy 1
hash md5
authentication pre-share
group 2
```

To configure an IKE preshared key:

```
crypto isakmp key 12abcjhrweit345 address 16.0.0.2
```

To configure an IPsec transform set:

```
crypto ipsec transform-set proposal_01 esp-3des esp-md5-hmac comp-lzs
```

To configure an access list:

```
access-list 101 permit ip host 16.0.0.1 host 16.0.0.2
```

To configure a crypto map:

```
crypto map MAXCASE 10 ipsec-isakmp
set peer 16.0.0.2
set transform-set proposal_01
match address 101
```

To apply crypto map to the interface:

```
interface FastEthernet1/0
crypto map MAXCASE
```

Command Reference

There are no new or modified commands for this feature. All other commands used with this feature are documented in the Cisco IOS Release 12.3 command reference publications.

Glossary

ACL—access control list

AH—Authentication Header

DPD—Dead Peer Detection

ESP—Encapsulating Security Payload

GRE—Generic Routing Encapsulation

HSRP—Hot Standby Routing Protocol

IKE—Internet Key Exchange. IKE establishes a shared security policy and authenticates keys for services (such as IPSec) that require keys. Before any IPSec traffic can be passed, each router/firewall/host must verify the identity of its peer. This can be done by manually entering preshared keys into both hosts or by a CA service.

IPSec—IP Security. A framework of open standards that provides data confidentiality, data integrity, and data authentication between participating peers. IPSec provides these security services at the IP layer. IPSec uses IKE to handle the negotiation of protocols and algorithms based on local policy and to generate the encryption and authentication keys to be used by IPSec. IPSec can protect one or more data flows between a pair of hosts, between a pair of security gateways, or between a security gateway and a host.

ISA—Integrated Services Adapter

ISAKMP—Internet Security Association Key Management Protocol

HA—High Availability

MM—IKE Main Mode

MODECFG—Mode Configuration

QM—IKE Quick Mode

SA—security association

SA-VAM2—Service Adapter VPN Acceleration Module 2

VAM—VPN Acceleration Module

VAM2 - VPN Acceleration Module 2

VPN—Virtual Private Network

XAUTH—Extended Authentication