



Advanced Encryption Standard (AES)

Feature History

Release	Modification
12.2(13)T	This feature was introduced.

This document describes the Advanced Encryption Standard (AES) feature in Cisco IOS Release 12.2(13)T. It includes the following sections:

- [Feature Overview, page 1](#)
- [Supported Platforms, page 2](#)
- [Supported Standards, MIBs, and RFCs, page 3](#)
- [Configuration Tasks, page 3](#)
- [Configuration Examples, page 6](#)
- [Command Reference, page 9](#)
- [Glossary, page 20](#)

Feature Overview

The Advanced Encryption Standard (AES) feature adds support for the new encryption standard AES, with Cipher Block Chaining (CBC) mode, to IP Security (IPSec).

The National Institute of Standards and Technology (NIST) has created AES, which is a new Federal Information Processing Standard (FIPS) publication that describes an encryption method. AES is a privacy transform for IPSec and Internet Key Exchange (IKE) and has been developed to replace the Data Encryption Standard (DES). AES is designed to be more secure than DES: AES offers a larger key size, while ensuring that the only known approach to decrypt a message is for an intruder to try every possible key. AES has a variable key length—the algorithm can specify a 128-bit key (the default), a 192-bit key, or a 256-bit key.



Note

Although AES is being developed to replace DES, the NIST anticipates that 3DES will remain an approved algorithm for the near future.

Benefits

This feature, which adds support for AES encryption to IPSec, introduces a new level of security strength and speed that was not present in the virtual private network (VPN) marketplace.

AES is a cryptographic algorithm that protects sensitive, unclassified information.

Restrictions

Router Requirements

To enable AES, your router must support IPSec and long keys (the “k9” subsystem).

Hardware IPSec Encryption Incompatibility

AES cannot encrypt IPSec and IKE traffic if an acceleration card is present. This restriction will be lifted in a future release.

Related Documents

- The chapters “Configuring IPSec Network Security” and “Configuring Internet Key Exchange Security Protocol” in the *Cisco IOS Security Configuration Guide*, Release 12.2
- The chapters “IPSec Network Security Commands” and “Internet Key Exchange Security Protocol Commands” in the *Cisco IOS Security Command Reference*, Release 12.2

Supported Platforms

For platforms supported in Cisco IOS Release 12.2(13)T, consult Cisco Feature Navigator.

Determining Platform Support Through Cisco Feature Navigator

Cisco IOS software is packaged in feature sets that are supported on specific platforms. To obtain updated information about platform support for this feature, access Cisco Feature Navigator. Cisco Feature Navigator dynamically updates the list of supported platforms as new platform support is added for the feature.

Cisco Feature Navigator is a web-based tool that enables you to determine which Cisco IOS software images support a specific set of features and which features are supported in a specific Cisco IOS image. You can search by feature or release. In the release section, you can compare releases side by side to display both the features unique to each software release and the features that releases in common.

To access Cisco Feature Navigator, 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 this URL: <http://www.cisco.com/register>

Cisco Feature Navigator is updated regularly when major Cisco IOS software releases and technology releases occur. For the most current information, go to the Cisco Feature Navigator home page at the following URL:

<http://www.cisco.com/go/fn>

Availability of Cisco IOS Software Images

Platform support for particular Cisco IOS software releases is dependent on the availability of the software images for those platforms. Software images for some platforms may be deferred, delayed, or changed without prior notice. For updated information about platform support and availability of software images for each Cisco IOS software release, refer to the online release notes or, if supported, Cisco Feature Navigator.

Supported Standards, MIBs, and RFCs

Standard

The AES Cipher Algorithm and Its Use with IPsec

MIBs

None

To obtain lists of supported MIBs by platform and Cisco IOS release, and to download MIB modules, go to the Cisco MIB website on Cisco.com at the following URL:

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

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/netmgt/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 this URL:

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

RFC

None

Configuration Tasks

See the following sections for configuration tasks for the Advanced Encryption Standard (AES) feature. Each task in the list is identified as either required or optional.

- [Configuring an IKE Policy](#) (required)
- [Configuring an AES Transform Set](#) (required)
- [Verifying IKE and IPsec Configurations](#) (optional)

Configuring an IKE Policy

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

	Command	Purpose
Step 1	<code>Router(config)# crypto isakmp policy <i>priority</i></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 {aes aes 192 aes 256}</code>	Specifies the encryption algorithm within an IKE policy. <ul style="list-style-type: none"> • 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—Specifies RSA encrypted nonces as the authentication method. • 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 <i>seconds</i></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>
Step 5	<code>Router(config-isakmp)# hash {sha md5}</code>	(Optional) Specifies the hash algorithm within an IKE policy. <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	<code>Router(config-isakmp)# group {1 2 5}</code>	(Optional) Specifies the Diffie-Hellman (DH) group identifier within an IKE policy. <p>1—Specifies the 768-bit DH group.</p> <p>2—Specifies the 1024-bit DH group.</p> <p>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>

Configuring an AES Transform Set

To define an AES transform set, use the following commands beginning in global configuration mode:

	Command	Purpose
Step 1	<pre>Router(config)# crypto ipsec transform-set transform-set-name transform1 [transform2 [transform3]]</pre>	<p>Defines a transform set and enters crypto transform configuration mode.</p> <ul style="list-style-type: none"> <i>transform-set-name</i>—Specifies the name of the transform set to create (or modify). <i>transform1</i> [<i>transform2</i> [<i>transform3</i>] [<i>transform4</i>]]—Defines the IPsec security protocols and algorithms. Accepted transform values are described in Table 1.
Step 2	<pre>Router(cfg-crypto-tran)# mode [tunnel transport]</pre>	<p>(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.)</p>

Verifying IKE and IPsec Configurations

To view information about your IPsec configurations, use **show crypto ipsec transform-set EXEC** command.



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
```

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

```

Troubleshooting Tips

- Clear (and reinitialize) IPsec security associations by using the **clear crypto sa** EXEC command. 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, refer to the **clear crypto sa** command in the chapter “IPsec Network Security Commands” of the *Cisco IOS Security Command Reference*, Release 12.2.

- Any IPsec transforms or IKE encryption methods that the current hardware does not support should be disabled; they are ignored whenever an attempt to negotiate with the peer is made.

If a user enters an IPsec transform or an IKE encryption method that the hardware does not support, a warning message will be generated. These warning messages are also generated at boot time. When an encrypted card is inserted, the current configuration is scanned. If any IPsec transforms or IKE encryption methods are found that are not supported by the hardware, a warning message will be generated. For examples of these warning messages, see the section “[Configuration Examples](#)” immediately following this section.

Configuration Examples

This section provides the following configuration examples:

- [AES Configuration Example](#)
- [IPsec Transform Warning Message Example](#)
- [IKE Encryption Warning Message Example](#)
- [Running Configuration Warning Message Example](#)

AES Configuration Example

The following example is sample output from the **show running-config** command. In this example, the AES 256-bit key is enabled.

```

Current configuration : 1665 bytes
!
version 12.2
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname "Router1"
!
!
ip subnet-zero
!
!
no ip domain lookup

```

```
!  
ip audit notify log  
ip audit po max-events 100  
!  
crypto isakmp policy 10  
  encryption aes 256  
  authentication pre-share  
  lifetime 180  
crypto isakmp key cisco123 address 10.0.110.1  
!  
!  
crypto ipsec transform-set aasset esp-aes 256 esp-sha-hmac  
mode transport  
!  
crypto map aesmap 10 ipsec-isakmp  
  set peer 10.0.110.1  
  set transform-set aasset  
  match address 120  
!  
!  
!  
voice call carrier capacity active  
!  
!  
!  
!  
!  
!  
!  
mta receive maximum-recipients 0  
!  
!  
!  
!  
interface FastEthernet0/0  
  ip address 10.0.110.2 255.255.255.0  
  ip nat outside  
  no ip route-cache  
  no ip mroute-cache  
  duplex auto  
  speed auto  
  crypto map aesmap  
!  
interface Serial0/0  
  no ip address  
  shutdown  
!  
interface FastEthernet0/1  
  ip address 11.0.110.1 255.255.255.0  
  ip nat inside  
  no ip route-cache  
  no ip mroute-cache  
  duplex auto  
  speed auto  
!  
ip nat inside source list 110 interface FastEthernet0/0 overload  
ip classless  
ip route 0.0.0.0 0.0.0.0 10.5.1.1  
ip route 12.0.110.0 255.255.255.0 FastEthernet0/0  
ip route 172.18.124.0 255.255.255.0 10.5.1.1  
ip route 172.18.125.3 255.255.255.255 10.5.1.1  
ip http server
```

```

!
!
access-list 110 deny ip 11.0.110.0 0.0.0.255 12.0.110.0 0.0.0.255
access-list 110 permit ip 11.0.110.0 0.0.0.255 any
access-list 120 permit ip 11.0.110.0 0.0.0.255 12.0.110.0 0.0.0.255
!
route-map nonat permit 10
 match ip address 110
!
call rsvp-sync
!
!
mgcp profile default
!
dial-peer cor custom
!
!
!
!
!
line con 0
 exec-timeout 0 0
line aux 0
line vty 0 4
 login
!
!
end

```

IPSec Transform Warning Message Example

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

```

IKE Encryption Warning Message Example

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

```

encryption aes 256
WARNING:encryption hardware does not support the configured
encryption method for ISAKMP policy 1

```

Running Configuration Warning Message Example

The following example is a sample warning message that is displayed in the running configuration whenever a user tries to configure an IPSec transform or IKE encryption method that the hardware does not support:

```
crypto isakmp policy 1
  encryption aes 256
! Policy disabled because algorithm not supported by encryption hardware
!
crypto ipsec transform-set transform-1 esp-aes 256 esp-md5-hmac
! Disabled because transform not supported by encryption hardware
```

Command Reference

This section documents modified commands. All other commands used with this feature are documented in the Cisco IOS Release 12.2 command reference publications.

- [crypto ipsec transform-set](#)
- [encryption \(IKE policy\)](#)
- [show crypto isakmp policy](#)
- [show crypto ipsec transform-set](#)

crypto ipsec transform-set

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

```
crypto ipsec transform-set transform-set-name transform1 [transform2 [transform3]
[transform4]]
```

```
no crypto ipsec transform-set transform-set-name
```

Syntax Description

<i>transform-set-name</i>	Specifies the name of the transform set to create (or modify).
<i>transform1</i>	Specifies up to four “transforms”: one Authentication Header (AH), one Encapsulating Security Payload (ESP) encryption, one ESP authentication, and one compression. These transforms define the IP Security (IPSec) security protocols and algorithms. Accepted transform values are described in Table 1 .
<i>transform2</i>	
<i>transform3</i>	
<i>transform4</i>	

Defaults

No default behavior or values.

Command Modes

Global configuration.

This command invokes the crypto transform configuration mode.

Command History

Release	Modification
11.3 T	This command was introduced.
12.2(13)T	The following transform options were added: esp-aes , esp-aes 192 , and esp-aes 256 .

Usage Guidelines

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.

You can configure multiple transform sets, and then specify one or more of these transform sets in a crypto map entry. The transform set defined in the crypto map entry is used in the IPSec SA negotiation to protect the data flows specified by that crypto map entry’s access list. During the negotiation, the peers search for a transform set that is the same at both peers. When such a transform set is found, it is selected and will be applied to the protected traffic as part of both peer’s IPSec SAs.

When IKE is not used to establish SAs, a single transform set must be used. The transform set is not negotiated.

Before a transform set can be included in a crypto map entry it must be defined using this command.

A transform set specifies one or two IPSec security protocols (either AH, ESP, or both) and specifies which algorithms to use with the selected security protocol. The AH and ESP IPSec security protocols are described in the section “[IPSec Protocols: AH and ESP](#).”

To define a transform set, you specify one to four “transforms”—each transform represents an IPSec security protocol (AH or ESP) plus the algorithm you want to use. When the particular transform set is used during negotiations for IPSec SAs, the entire transform set (the combination of protocols, algorithms, and other settings) must match a transform set at the remote peer.

In a transform set you could specify the AH protocol, the ESP protocol, or both. If you specify an ESP protocol in a transform set, you can specify just an ESP encryption transform or both an ESP encryption transform and an ESP authentication transform.

Table 1 lists the acceptable transform combination selections for the AH and ESP protocols.

Table 1 Allowed Transform Combinations

Transform type	Transform	Description
AH Transform (Pick up to one.)	ah-md5-hmac	AH with the MD5 (Message Digest 5) (an HMAC variant) authentication algorithm
	ah-sha-hmac	AH with the SHA (Secure Hash Algorithm) (an HMAC variant) authentication algorithm
ESP Encryption Transform (Pick up to 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	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 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-des** and **esp-sha-hmac**
- **ah-sha-hmac** and **esp-des** 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.

Examples

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
```

Related Commands

Command	Description
mode (IPSec)	Changes the mode for a transform set.
set transform-set	Specifies which transform sets can be used with the crypto map entry.
show crypto ipsec transform-set	Displays the configured transform sets.

encryption (IKE policy)

To specify the encryption algorithm within an Internet Key Exchange (IKE) policy, use the **encryption** command in Internet Security Association Key Management Protocol (ISAKMP) policy configuration mode. IKE policies define a set of parameters to be used during IKE negotiation. To reset the encryption algorithm to the default value, use the **no** form of this command.

```
encryption { des | 3des | aes | aes 192 | aes 256 }
```

```
no encryption
```

Syntax Description

des	Specifies 56-bit Data Encryption Standard (DES)-CBC as the encryption algorithm.
3des	Specifies 168-bit DES (3DES) as the encryption algorithm.
aes	Specifies 128-bit Advanced Encryption Standard (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.

Defaults

The 56-bit DES-CBC encryption algorithm.

Command Modes

ISAKMP policy configuration

Command History

Release	Modification
11.3 T	This command was introduced.
12.0(2)T	The 3des option was added.
12.2(13)T	The following keywords were added: aes , aes 192 , and aes 256 .

Usage Guidelines

Use this command to specify the encryption algorithm to be used in an IKE policy.

If a user enters an IKE encryption method that the hardware does not support, a warning message will be displayed immediately after the **encryption** command is entered.

Examples

The following example configures an IKE policy with the 3DES encryption algorithm (all other parameters are set to the defaults):

```
crypto isakmp policy
  encryption 3des
exit
```

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

```
encryption aes 256
WARNING:encryption hardware does not support the configured
encryption method for ISAKMP policy 1
```

Related Commands	Command	Description
	authentication (IKE policy)	Specifies the authentication method within an IKE policy.
	crypto isakmp policy	Defines an IKE policy.
	group (IKE policy)	Specifies the DH group identifier within an IKE policy.
	hash (IKE policy)	Specifies the hash algorithm within an IKE policy.
	lifetime (IKE policy)	Specifies the lifetime of an IKE SA.
	show crypto isakmp policy	Displays the parameters for each IKE policy.

show crypto isakmp policy

To view the parameters for each Internet Key Exchange (IKE) policy, use the **show crypto isakmp policy** command in EXEC mode.

```
show crypto isakmp policy
```

Syntax Description This command has no arguments or keywords.

Command Modes EXEC

Command History	Release	Modification
	11.3 T	This command was introduced.
	12.2(13)T	The command output was expanded to include a warning message for users who try to configure an IKE encryption method that the hardware does not support.

Examples

The following is sample output from the **show crypto isakmp policy** command, after two IKE policies have been configured (with priorities 15 and 20 respectively):

```
Router# show crypto isakmp policy

Protection suite priority 15
  encryption algorithm:  DES - Data Encryption Standard (56 bit keys)
  hash algorithm:       Message Digest 5
  authentication method: Rivest-Shamir-Adleman Signature
  Diffie-Hellman Group: #2 (1024 bit)
  lifetime:             5000 seconds, no volume limit
Protection suite priority 20
  encryption algorithm:  DES - Data Encryption Standard (56 bit keys)
  hash algorithm:       Secure Hash Standard
  authentication method: preshared Key
  Diffie-Hellman Group: #1 (768 bit)
  lifetime:             10000 seconds, no volume limit
Default protection suite
  encryption algorithm:  DES - Data Encryption Standard (56 bit keys)
  hash algorithm:       Secure Hash Standard
  authentication method: Rivest-Shamir-Adleman Signature
  Diffie-Hellman Group: #1 (768 bit)
  lifetime:             86400 seconds, no volume limit
```



Note

Although the output shows “no volume limit” for the lifetimes, you can currently configure only a time lifetime (such as 86,400 seconds); volume limit lifetimes are not used.

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
```

Related Commands

Command	Description
authentication (IKE policy)	Specifies the authentication method within an IKE policy.
crypto isakmp policy	Defines an IKE policy.
encryption (IKE policy)	Specifies the encryption algorithm within an IKE policy.
group (IKE policy)	Specifies the DH group identifier within an IKE policy.
hash (IKE policy)	Specifies the hash algorithm within an IKE policy.
lifetime (IKE policy)	Specifies the lifetime of an IKE SA.

show crypto ipsec transform-set

To view the configured transform sets, use the **show crypto ipsec transform-set** command in EXEC mode.

```
show crypto ipsec transform-set [tag transform-set-name]
```

Syntax Description	tag <i>transform-set-name</i> (Optional) Displays only the transform sets with the specified <i>transform-set-name</i> .						
Command Modes	EXEC						
Command History	<table border="1"> <thead> <tr> <th>Release</th> <th>Modification</th> </tr> </thead> <tbody> <tr> <td>11.3 T</td> <td>This command was introduced.</td> </tr> <tr> <td>12.2(13)T</td> <td>The command output was expanded to include a warning message for users who try to configure an IPSec transform that the hardware does not support.</td> </tr> </tbody> </table>	Release	Modification	11.3 T	This command was introduced.	12.2(13)T	The command output was expanded to include a warning message for users who try to configure an IPSec transform that the hardware does not support.
Release	Modification						
11.3 T	This command was introduced.						
12.2(13)T	The command output was expanded to include a warning message for users who try to configure an IPSec transform that the hardware does not support.						

Examples

The following is sample output for the **show crypto ipsec transform-set** command:

```
Router# show crypto ipsec transform-set

Transform set combined-des-sha: { esp-des esp-sha-hmac }
    will negotiate = { Tunnel, },

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, },
```

The following configuration was in effect when the previous **show crypto ipsec transform-set** command was issued:

```
crypto ipsec transform-set combined-des-sha esp-des esp-sha-hmac
crypto ipsec transform-set combined-des-md5 esp-des esp-md5-hmac
crypto ipsec transform-set t1 esp-des esp-md5-hmac
crypto ipsec transform-set t100 ah-sha-hmac
    mode transport
crypto ipsec transform-set t2 ah-sha-hmac esp-des
```

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
```

Glossary

DES—Data Encryption Standard. DES is used to encrypt packet data. Cisco IOS implements the mandatory 56-bit DES-CBC with Explicit IV. Cipher Block Chaining (CBC) requires an initialization vector (IV) to start encryption. The IV is explicitly given in the IPSec packet.

Cisco IOS also implements Triple DES (168-bit) encryption, depending on the software versions available for a specific platform. Triple DES (3DES) is a strong form of encryption that allows sensitive information to be transmitted over untrusted networks. It enables customers to utilize network layer encryption.

IKE—Internet Key Exchange. A hybrid protocol that implements Oakley key exchange and Skeme key exchange inside the ISAKMP framework. Although IKE can be used with other protocols, its initial implementation is with IPSec. IKE provides authentication of the IPSec peers, negotiates IPSec keys, and negotiates IPSec security associations.

IPSec—IP Security. A framework of open standards developed by the Internet Engineering Task Force (IETF). IPSec provides security for transmission of sensitive information over unprotected networks such as the Internet. IPSec acts at the network layer, protecting and authenticating IP packets between participating IPSec devices (“peers”), such as Cisco routers.

SA—security association. Security association is a description of how two or more entities will use security services in the context of a particular security protocol (AH or ESP) to communicate securely on behalf of a particular data flow. It includes such things as the transform and the shared secret keys to be used for protecting the traffic.

The IPSec security association is established either by IKE or by manual user configuration. Security associations are unidirectional and are unique per security protocol. So when security associations are established for IPSec, the security associations (for each protocol) for both directions are established at the same time.

When using IKE to establish the security associations for the data flow, the security associations are established when needed and expire after a period of time (or volume of traffic). If the security associations are manually established, they are established as soon as the necessary configuration is completed and do not expire.

transform—Transform is the list of operations done on a dataflow to provide data authentication, data confidentiality, and data compression. For example, one transform is the ESP protocol with the HMAC-MD5 authentication algorithm; another transform is the AH protocol with the 56-bit DES encryption algorithm and the ESP protocol with the HMAC-SHA authentication algorithm.