Triple DES Encryption for IPSec

**Feature Summary**

IPSec supports the Triple DES encryption algorithm (168-bit) in addition to 56-bit encryption. Triple DES (3DES) is a strong form of encryption that allows sensitive information to be transmitted over untrusted networks. It enables customers, particularly in the finance industry, to utilize network layer encryption.

**Platforms**

This feature is supported only on the following platforms:

- 1720
- 2600 Series
- 3600 Series
- 4000 Series
- 4500 Series
- AS5300 Series
- 7200 Series
- 7500 Series

**Prerequisites**

This feature is available only in software images with the Triple DES encryption feature set for IPSec.

**Supported MIBs and RFCs**

None.
## Configuration Tasks

Configuring the router for Triple DES encryption has two parts:

- Internet key exchange policy configuration
- Crypto map policy configuration

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

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>crypto isakmp policy priority</td>
<td>Identify the policy to create. (Each policy is uniquely identified by the priority number you assign.)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>(This command puts you into the config-isakmp command mode.)</td>
</tr>
<tr>
<td>2</td>
<td>encryption 3des</td>
<td>Specify the encryption algorithm.</td>
</tr>
<tr>
<td>3</td>
<td>hash {sha</td>
<td>md5}</td>
</tr>
<tr>
<td>4</td>
<td>authentication {rsa-sig</td>
<td>rsa-encr</td>
</tr>
<tr>
<td>5</td>
<td>group {1</td>
<td>2}</td>
</tr>
<tr>
<td>6</td>
<td>lifetime seconds</td>
<td>Specify the security association’s lifetime.</td>
</tr>
<tr>
<td>7</td>
<td>exit</td>
<td>Exit the config-isakmp command mode.</td>
</tr>
<tr>
<td>8</td>
<td>exit</td>
<td>Exit the global configuration mode.</td>
</tr>
<tr>
<td>9</td>
<td>show crypto isakmp policy</td>
<td>(Optional) View all existing IKE policies. (Use this command in EXEC mode.)</td>
</tr>
</tbody>
</table>

To configure an IPSec crypto map policy, use the following commands starting in global configuration mode:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>access-list access-list-number permit ip source source-wildcard destination destination-wildcard</td>
<td>Configure Access Control Lists (ACLs) to permit through the router interface the IP network traffic that you want to protect.</td>
</tr>
<tr>
<td>2</td>
<td>crypto ipsec transform-set transform-set-name esp-3Des</td>
<td>Configure a transform-set that identifies the IPSec triple DES transform to use for encapsulating network traffic.</td>
</tr>
<tr>
<td>3</td>
<td>crypto map map-name seq-num ipsec-isakmp</td>
<td>Create a crypto map that binds together elements of the IPSec configuration. (This command puts you into the crypto map command mode.)</td>
</tr>
<tr>
<td>4</td>
<td>match address [access-list-id</td>
<td>name]</td>
</tr>
<tr>
<td>5</td>
<td>set transform-set transform-set-name</td>
<td>Specify which transform set can be used with the crypto map entry.</td>
</tr>
<tr>
<td>6</td>
<td>set peer [hostname</td>
<td>ip-address]</td>
</tr>
<tr>
<td>7</td>
<td>exit</td>
<td>Exit the crypto map command mode.</td>
</tr>
<tr>
<td>8</td>
<td>interface type number</td>
<td>Specify an interface on which to apply the crypto map. (This command puts you into the interface command mode.)</td>
</tr>
</tbody>
</table>
Configuration Example

This IPSec configuration example has two parts:

- Configuring IKE policy
- Configuring IPSec policy, including the access list, transform set, crypto map, and interface definition

This example creates an IKE policy, with **3des** as the encryption algorithm.

```
crypto isakmp policy 15
  encryption 3des
  hash md5
  authentication rsa-sig
  group 2
  lifetime 5000
```

The following is an example of a minimal IPSec configuration where the security associations will be established via IKE. In this example, IKE must be enabled.

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:

```
crypto ipsec transform-set myset 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 myset
  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
```
Command Reference

This section documents changes to the `crypto ipsec transform-set` and `crypto isakmp policy` commands. All other commands used with this feature are documented in the Cisco IOS Release 12.0 Security Configuration Guide in the “Internet Key Exchange Security Protocol Commands” chapter and the “IPSec Network Security Commands” chapter.

- crypto ipsec transform-set
- encryption (IKE policy)
crypto 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. This command is documented in the Cisco IOS Release 12.0 Security Command Reference.

```plaintext
crypto ipsec transform-set transform-set-name transform1 [transform2 [transform3]]
no crypto ipsec transform-set transform-set-name
```

Syntax Description

- **transform-set-name**: Specify the name of the transform set to create (or modify).
- **transform1**: Specify up to three “transforms.” These transforms define the IPSec security protocol(s) and algorithm(s). Accepted transform values are described in the “Usage Guidelines” section.
- **transform2**, **transform3**: Specify up to three “transforms.” These transforms define the IPSec security protocol(s) and algorithm(s). Accepted transform values are described in the “Usage Guidelines” section.

Command Mode

- **Global configuration**. This command invokes the crypto transform configuration mode.

Usage Guidelines

This command first appeared in Cisco IOS Release 11.3 T. The **esp-3des** option first appeared in Cisco IOS Release 12.0(1) XA.

Acceptable combinations of transforms are shown in Table 1.

**Table 1 Selecting Transforms for a Transform Set: Allowed Transform Combinations**

<table>
<thead>
<tr>
<th>AH Transform</th>
<th>ESP Encryption Transform</th>
<th>ESP Authentication Transform, only if you also selected the esp-des transform (not esp-rfc1829)</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>ah-md5-hmac</strong></td>
<td>esp-des</td>
<td>esp-md5-hmac ( esp des encryption algorithm )</td>
</tr>
<tr>
<td><strong>ah-sha-hmac</strong></td>
<td>esp-3des</td>
<td>esp-sha-hmac ( esp des encryption algorithm, 3DES or Triple DES )</td>
</tr>
<tr>
<td><strong>ah-rfc1829</strong></td>
<td>esp-rfc1829</td>
<td>esp-sha-hmac ( esp with the SHA (HMAC variant) authentication algorithm )</td>
</tr>
</tbody>
</table>
Examples of acceptable transform combinations are:

- ah-md5-hmac
- esp-des
- esp-3des and esp-md5-hmac
- ah-sha-hmac and esp-des and esp-sha-hmac
- ah-rfc1828 and esp-rfc1829

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.

Example

This 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
```
encryption (IKE policy)

To specify the encryption algorithm within an IKE policy, use the `encryption (IKE policy)` ISAKMP policy configuration command. IKE policies define a set of parameters to be used during IKE negotiation. Use the `no` form of this command to reset the encryption algorithm to the default value.

```
encryption {des | 3des}
no encryption
```

**Syntax Description**

- **des** Specifies 56-bit DES-CBC as the encryption algorithm.
- **3des** Specifies 168-bit DES (3DES) as the encryption algorithm.

**Default**

The 56-bit DES-CBC encryption algorithm.

**Command Mode**

ISAKMP policy configuration (config-isakmp)

**Usage Guidelines**

This command first appeared in Cisco IOS Release 11.3 T. The **3des** option first appeared in Cisco IOS Release 12.0(1) XA.

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

**Example**

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

```
router(config)#crypto isakmp policy
router(config-isakmp)#encryption 3des
router(config-isakmp)#
```

**Related Commands**

- `authentication (IKE policy)`
- `crypto isakmp policy`
- `group (IKE policy)`
- `hash (IKE policy)`
- `lifetime (IKE policy)`
- `show crypto isakmp policy`