IP Security

IP Security (IPSec) is 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; it uses IKE to handle negotiation of protocols and algorithms based on local policy, and to generate the encryption and authentication keys to be used by IPSec.

Cisco SDM lets you configure IPSec transform sets, rules, and policies. Use the IPSec tree to go to the IPSec configuration windows that you want to use.

IPSec Policies

This window displays the IPSec policies configured on the router, and the crypto maps associated with each policy. IPSec policies are used to define VPN connections. To learn about the relationship between IPSec policies, crypto maps, and VPN connections, see More about VPN Connections and IPSec Policies.

Icon

If this icon appears next to the IPSec policy, it is read-only, and it cannot be edited. An IPSec policy may be read-only if it contains commands that Cisco SDM does not support.
IPSec Policies

Name

The name of this IPSec policy.

Type

One of the following:

- **ISAKMP—IKE** will be used to establish the IPSec security associations for protecting the traffic specified by this crypto map entry. Cisco SDM supports Internet Security Association and Key Management Protocol (ISAKMP) crypto maps.

- **Manual**—IKE will not be used to establish the IPSec security associations for protecting the traffic specified by this crypto map entry. Cisco SDM does not support the creation of manual crypto maps. Cisco SDM treats as read-only any manual crypto maps that have been created using the command-line interface (CLI).

- **Dynamic**—Specifies that this crypto map entry is to reference a preexisting dynamic crypto map. Dynamic crypto maps are policy templates used in processing negotiation requests from a peer IPSec device. Cisco SDM does not support the creation of dynamic crypto maps. Cisco SDM treats as read-only any dynamic crypto maps created using the CLI.

Crypto Maps in this IPSec policy

Name

The name of the IPSec policy of which the crypto map is a part.

Seq. No.

When an IPSec policy is used in a VPN connection, the combination of the sequence number and IPSec policy name uniquely identifies the connection.

Peers

This column lists the IP addresses or host names of the peer devices specified in the crypto map. Multiple peers are separated by commas.

Transform Set

This column lists the transform sets used in the crypto map.
Dynamic Crypto Maps Sets in this IPSec Policy

**Dynamic Crypto Map Set Name**

The name of this dynamic crypto map set. Names enable administrators to understand how the crypto map set is used.

**Sequence Number**

The sequence number for this dynamic crypto map set.

**Type**

Type is always Dynamic.

What Do You Want to Do?

<table>
<thead>
<tr>
<th>If you want to:</th>
<th>Do this:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Add an IPSec policy to the configuration.</td>
<td>Click <strong>Add</strong>.</td>
</tr>
<tr>
<td>Edit an existing IPSec policy.</td>
<td>Select the policy, and click <strong>Edit</strong>.</td>
</tr>
<tr>
<td>Remove a crypto map entry from a policy.</td>
<td>Select the policy, and click <strong>Edit</strong>. In the window, select the crypto map you want to remove, and click <strong>Delete</strong>. Then, click <strong>OK</strong> to return to this window.</td>
</tr>
<tr>
<td>Remove an IPSec policy.</td>
<td>Select the policy, and click <strong>Delete</strong>.</td>
</tr>
</tbody>
</table>

Add or Edit IPSec Policy

Use this window to add or edit an IPSec policy.

Name

The name of this IPSec policy. This name can be any set of alphanumeric characters. It may be helpful to include the peer names in the policy name, or to include other information that will be meaningful to you.
Crypto Maps in this IPSec policy

This box lists the crypto maps in this IPSec policy. The list includes the name, the sequence number, and the transform set that makes up this crypto map. You can select a crypto map and edit it or delete it from the IPSec policy.

If you want to add a crypto map, click Add. If you want Cisco SDM to guide you through the process, check Use Add Wizard, and then click Add.

Icon

If a crypto map is read-only, the read-only icon appears in this column. A crypto map may be read-only if it contains commands that Cisco SDM does not support.

Dynamic Crypto Maps Sets in this IPSec Policy

This box lists the dynamic crypto map sets in this IPSec policy. Use the Add button to add an existing dynamic crypto map set to the policy. Use the Delete button to remove a selected dynamic crypto map set from the policy.

What Do You Want to Do?

<table>
<thead>
<tr>
<th>If you want to:</th>
<th>Do this:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Add a crypto map to this policy.</td>
<td>Click Add, and create a crypto map in the Add crypto map panels. Or, check Use Add Wizard, and then click Add.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong> The wizard allows you to add only one transform set to the crypto map. If you need multiple transform sets in the crypto map, do not use the wizard.</td>
</tr>
<tr>
<td>Edit a crypto map in this policy.</td>
<td>Select the crypto map, click Edit, and edit the crypto map in the Edit crypto map panels.</td>
</tr>
<tr>
<td>Remove a crypto map from this policy.</td>
<td>Select the crypto map, and click Delete.</td>
</tr>
</tbody>
</table>
Add or Edit Crypto Map: General

Change general crypto map parameters in this window. This window contains the following fields.

Name of IPSec Policy

A read-only field that contains the name of the policy in which this crypto map is used. This field does not appear if you are using the Crypto Map Wizard.

Description

Enter or edit a description of the crypto map in this field. This description appears in the VPN Connections list, and it can be helpful in distinguishing this crypto map from others in the same IPSec policy.

Sequence Number

A number that, along with the IPSec policy name, is used to identify a connection. Cisco SDM generates a sequence number automatically. You can enter your own sequence number if you wish.

Security Association Lifetime

IPSec security associations use shared keys. These keys, and their security associations time out together. There are two lifetimes: a timed lifetime and a traffic-volume lifetime. The security association expires when the first of these lifetimes is reached.

You can use this field to specify a different security association lifetime for this crypto map than the lifetime that is specified globally. In the Kilobytes field, you can specify the lifetime in the number of kilobytes sent, up to a maximum of 4608000. In the HH:MM:SS fields, you can specify the lifetime in hours, minutes, and seconds. You can also specify both a timed and a traffic-volume lifetimes. If both are specified, the lifetime will expire when the first criterion has been satisfied.
Enable Perfect Forwarding Secrecy

When security keys are derived from previously generated keys, there is a security problem, because if one key is compromised, then the others can be compromised also. Perfect Forwarding Secrecy (PFS) guarantees that each key is derived independently. It thus ensures that if one key is compromised, no other keys will be. If you enable PFS, you can specify use of the Diffie-Hellman group1, group2, or group5 method.

Note

If your router does not support group5, it will not appear in the list.

Enable Reverse Route Injection

Reverse Route Injection (RRI) is used to populate the routing table of an internal router running Open Shortest Path First (OSPF) protocol or Routing Information Protocol (RIP) for remote VPN clients or LAN-to-LAN sessions.

Reverse Route Injection dynamically adds static routes to the clients connected to the Easy VPN server.

Add or Edit Crypto Map: Peer Information

A crypto map includes the hostnames or IP addresses of the peers involved in the security association. This screen allows you to add and remove peers associated with this crypto map. Multiple peers provide the router with multiple routes for encrypted data.

<table>
<thead>
<tr>
<th>If you want to:</th>
<th>Do this:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Add a peer to the Current List.</td>
<td>Enter the IP address or host name of the peer, and click <strong>Add</strong>.</td>
</tr>
<tr>
<td>Remove a peer from the Current List.</td>
<td>Select the peer, and click <strong>Remove</strong>.</td>
</tr>
</tbody>
</table>
Add or Edit Crypto Map: Transform Sets

Use this window to add and edit the transform set used in the crypto map. A crypto map includes the hostnames or IP addresses of the peers involved in the security association. Multiple peers provide the router with multiple routes for encrypted data. However, the devices at both ends of the VPN connection must use the same transform set.

Use the Crypto Map Wizard if it is sufficient for your router to offer a crypto map with one transform set.

Use **Add New Crypto Map...** with **Use Add Wizard** unchecked if you want to manually configure a crypto map with multiple transforms sets (up to six) to ensure that the router can offer one transform set that the peer it is negotiating with will accept. If you are already in the Crypto Map Wizard, exit the wizard, uncheck **Use Add Wizard**, and click **Add New Crypto Map...**

If you manually configure a crypto map with multiple transforms sets, you can also order the transform sets. This will be the order that the router will use to negotiate which transform set to use.

Available Transform Sets

Configured transform sets available for use in crypto maps. In the Crypto Map Wizard, the available transform sets are in the **Select Transform Set** drop-down list.

If no transform sets have been configured on the router, only the default transform sets provided with Cisco SDM are shown.

---

**Note**

- Not all routers support all transform sets (encryption types). Unsupported transform sets will not appear in the window.

- Not all IOS images support all the transform sets that Cisco SDM supports. Transform sets unsupported by the IOS image will not appear in the window.

- If hardware encryption is turned on, only those transform sets supported by both hardware encryption and the IOS image will appear in the window.
Details of Selected Transform Set (Crypto Map Wizard Only)

Shows the name, encryption, authentication characteristics, and other parameters of the chosen crypto map.

If this icon appears next to the transform set, it is read-only, and it cannot be edited.

Selected Transform Sets In Order of Preference (Manual Configuration of Crypto Map Only)

The transform sets that have been chosen for this crypto map, in the order in which they will be used. During negotiations with a peer, the router will offer transform sets in the order given in this list. You can use the up and down arrow buttons to reorder the list.

What Do You Want to Do? (Crypto Map Wizard Only)

<table>
<thead>
<tr>
<th>If you want to:</th>
<th>Do this:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Use the selected transform set for the crypto map.</td>
<td>Click <strong>Next</strong>.</td>
</tr>
<tr>
<td>Use another existing transform set.</td>
<td>Select it in the Select Transform Set list, and click <strong>Next</strong>.</td>
</tr>
<tr>
<td>Use a new transform set.</td>
<td>Click <strong>Add</strong>, and create the transform set in the Add Transform Set window. Then, return to this window, and click <strong>Next</strong>.</td>
</tr>
<tr>
<td>Edit the selected transform set.</td>
<td>Click <strong>Edit</strong>, and edit the transform set in the Edit Transform Set window.</td>
</tr>
<tr>
<td>Add more transform sets to this crypto map. You may wish to do this to ensure that the router can offer a transform set that the peer will agree to use.</td>
<td>Leave the crypto map wizard, uncheck <strong>Use Add Wizard</strong>, and click <strong>Add Crypto Map</strong>. The Transform Set tab allows you to add and order transform sets.</td>
</tr>
</tbody>
</table>
What Do You Want to Do? (Manual Configuration of Crypto Map Only)

<table>
<thead>
<tr>
<th>If you want to:</th>
<th>Do this:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Add a transform set to the Selected Transform Sets box.</td>
<td>Select a transform set in the Available Transform Sets box, and click the right-arrow button.</td>
</tr>
<tr>
<td>Remove a transform set from the Selected Transform Sets box.</td>
<td>Select the transform set you want to remove, and click the left-arrow button.</td>
</tr>
<tr>
<td>Change the preference order of the selected transform sets.</td>
<td>Select a transform set, and click the up button or the down button.</td>
</tr>
<tr>
<td>Add a transform set to the Available Transform Sets list.</td>
<td>Click Add, and configure the transform set in the Add Transform Set window.</td>
</tr>
<tr>
<td>Edit a transform set in the Available Transform Sets list.</td>
<td>Click Edit, and configure the transform set in the Edit Transform Set window.</td>
</tr>
</tbody>
</table>

Add or Edit Crypto Map: Protecting Traffic

You can configure the crypto map to protect all traffic (Crypto Map Wizard only) or choose an IPSec rule to protect specified traffic.

Protect all traffic between the following subnets (Crypto Map Wizard Only)

Use this option to specify a single source subnet (a subnet on the LAN) whose traffic you want to encrypt, and one destination subnet supported by the peer that you specified in the Peers window. All traffic flowing between other source and destination subnets will be sent unencrypted.

Source

Enter the address of the subnet whose outgoing traffic you want to protect, and specify the subnet mask. You can either select a subnet mask from the list or type in a custom mask. The subnet number and mask must be entered in dotted decimal format. For more information, see IP Addresses and Subnet Masks.

All traffic from this source subnet that has a destination IP address on the destination subnet will be encrypted.
**Destination**
Enter the address of the destination subnet, and specify the mask for that subnet. You can either select a subnet mask from the list or type in a custom mask. The subnet number and mask must be entered in dotted decimal format.

All traffic going to the hosts in this subnet will be encrypted.

**IPSec Rule (Create/Select an access-list for IPSec traffic)**

You can add or change the IPSec rule used in this crypto map. Use this option if you need to specify multiple sources and destinations, and/or specific types of traffic to encrypt. An IPSec rule can consist of multiple entries, each specifying different traffic types and different sources and destinations. Any packets that do not match the criteria in the IPSec rule are sent unencrypted.

**Note**
If you are adding an IPSec rule for a VPN connection that uses a tunnel interface, the rule must specify the same source and destination data as the tunnel configuration.

To add or change the IPSec rule for the crypto map, click the … button to the right of the IPSec rule field and choose one of the following:

- **Select an existing rule (ACL)**—If the rule you want to use has already been created, choose the rule, then click **OK**.

- **Create a new rule and select**—If the rule you need has not been created, create the rule, then click **OK**.

- **None**—If you want to clear a rule association. The IPSec rule field shows the name of the IPSec rule in use, but if you choose **None**, the field becomes blank.

Another way to add or change the IPSec rule for this crypto map is to enter the number of the IPSec rule directly in the IPSec rule field.

**Note**
IPSec rules must be extended rules, not standard rules. If the number or name you enter identifies a standard rule, Cisco SDM will display a warning message when you click **OK**.
Dynamic Crypto Map Sets

This window lists the dynamic crypto map sets configured on the router.

Add/Edit/Delete Buttons

Use these buttons to manage the crypto maps in the window. If you try to delete a crypto map set associated with an IPSec policy, Cisco SDM prevents you from doing so. You must disassociate the crypto map from the policy before deleting it. You can do this in the IPSec Policies window.

Name

The name of the dynamic crypto map.

Type

Always Dynamic.

Add or Edit Dynamic Crypto Map Set

Add or edit a dynamic crypto map set in this window.

Name

If you are adding a dynamic crypto map, enter the name in this field. If you are editing a crypto map set, this field is disabled, and you cannot change the name.

Crypto maps in this IPSec Policy

This area lists the crypto maps used in this set. Use the Add, Edit, and Delete buttons to add, remove, or modify crypto maps in this list.
**Associate Crypto Map with this IPSec Policy**

**Sequence Number**

Enter a sequence number to identify this crypto map set. This sequence number cannot be in use by any other crypto map set.

**Select the Dynamic Crypto Map Set**

Select the dynamic crypto map set you want to add from this list.

**Crypto Maps in this Dynamic Crypto Map Set**

This area lists the names, sequence numbers, and peers in the dynamic crypto map set you selected.

**IPSec Profiles**

This window lists configured IPSec profiles on the router. IPSec profiles consist of one or more configured transform sets; the profiles are applied to mGRE tunnels to define how tunneled traffic is encrypted.

**Name**

The name of the IPSec profile.

**Transform Set**

The transform sets used in this profile.

**Description**

A description of the IPSec profile.

**Add**

Click to add a new IPSec profile.
Edit

Select an existing profile and click **Edit** to change the profile configuration.

Delete

Click to edit a selected IPSec profile. If the profile you are deleting is currently used in a DMVPN tunnel, you must configure the DMVPN tunnel to use a different IPSec profile.

Details of IPSec Profile

This area displays the configuration of the selected IPSec profile. For a description of the information displayed in this area see **Add or Edit IPSec Profile**.

Add or Edit IPSec Profile

Enter the information to create an IPSec profile in this dialog. An IPSec profile specifies the transform sets to be used, how the Security Association (SA) lifetime is to be determined, and other information.

Transform Set Columns

Use the two columns at the top of the dialog to specify the transform sets that you want to include in the profile. The left-hand column contains the transform sets configured on the router. To add a configured transform set to the profile, select it and click the **>>** button. If there are no transform sets in the left-hand column, or if you need a transform set that has not been created, click **Add** and create the transform set in the displayed dialog.

IKE Profile Association

If you want to associate an IKE profile with this IPSec profile, choose an existing profile from the list. If an IKE profile has already been associated, this field is read only.
**Time Based IPSec SA Lifetime**

Click **Time Based IPSec SA Lifetime** if you want a new SA to be established after a set period of time has elapsed. Enter the time period in the HH:MM:SS fields to the right.

**Traffic Volume Based IPSec SA Lifetime**

Click **Traffic Volume Based IPSec SA Lifetime** if you want a new SA to be established after a specified amount of traffic has passed through the IPSec tunnel. Enter the number of kilobytes that should pass through the tunnel before an existing SA is taken down and a new one is established.

**IPSec SA Idle Time**

Click IPSec SA Idle Time if you want a new SA to be established after the peer has been idle for a specified amount of time. Enter the idle time period in the HH:MM:SS fields to the right.

**Perfect Forwarding Secrecy**

Click **Perfect Forwarding Secrecy** if IPSec should ask for perfect forward secrecy (PFS) when requesting new security associations for this virtual template interface, or should require PFS in requests received from the peer. You can specify the following values:

- **group1**—The 768-bit Diffie-Hellman prime modulus group is used to encrypt the PFS request.
- **group2**—The 1024-bit Diffie-Hellman prime modulus group is used to encrypt the PFS request.
- **group5**—The 1536-bit Diffie-Hellman prime modulus group is used to encrypt the PFS request.

**Add or Edit IPSec Profile and Add Dynamic Crypto Map**

Use this window to add or to edit an IPSec profile, or to add a dynamic crypto map.
Name

Enter a name for this profile.

Available Transform Sets

This column lists the transform sets configured on this router. To add a transform set from this list to the Selected Transform Sets column, select a transform set and click the right arrow (>>) button.

If you need to configure a new transform set, click the Transform Sets node in the IPSec tree to go to the Transform Sets window. In that window, click Add to create a new transform set.

Selected Transform Sets

This column lists the transform sets that you are using in this profile. You can select multiple transform sets so that the router you are configuring and the router at the other end of the tunnel can negotiate which transform set to use.

Transform Set

This screen allows you to view transform sets, add new ones, and edit or remove existing transform sets. A transform set is a particular combination of security protocols and algorithms. During the IPSec security association negotiation, the peers agree to use a particular transform set for protecting a particular data flow.

You can create multiple transform sets and then specify one or more of them in a crypto map entry. The transform set defined in the crypto map entry will be used in the IPSec security association negotiation to protect the data flows specified by that crypto map entry’s access list.

During IPSec security association negotiations with IKE, the peers search for a transform set that is the same at both peers. When that transform set is found, it is selected and applied to the protected traffic as part of both peers’ IPSec security associations.

Name

Name given to the transform set.
ESP Encryption

Cisco SDM recognizes the following ESP encryption types:

- **ESP_3DES**—ESP, Triple DES. This is a stronger form of encryption than DES, supporting 168-bit encryption.
- **ESP_AES_128**—ESP, Advanced Encryption Standard (AES). Encryption with a 128-bit key. AES provides greater security than DES and is computationally more efficient than 3DES.
- **ESP_AES_192**—ESP, AES encryption with a 192-bit key.
- **ESP_AES_256**—ESP, AES encryption with a 256-bit key.
- **ESP_NULL**—Null encryption algorithm, but encryption transform used.
- **ESP_SEAL**—ESP with the 160-bit encryption key Software Encryption Algorithm (SEAL) encryption algorithm. SEAL (Software Encryption Algorithm) is an alternative algorithm to software-based Data Encryption Standard (DES), Triple DES (3DES), and Advanced Encryption Standard (AES). SEAL encryption uses a 160-bit encryption key and has a lower impact to the CPU when compared to other software-based algorithms.

ESP Integrity

Indicates the integrity algorithm being used. This column will contain a value when the transform set is configured to provide both data integrity and encryption. The column will contain one of the following values:

- **ESP-SHA-HMAC**—Security Hash Algorithm, HMAC.

AH Integrity

Indicates the integrity algorithm being used. This column will contain a value when the transform set is configured to provide data integrity but not encryption. The column will contain one of the following values:

- **AH-MD5-HMAC**—Message Digest 5.
- **AH-SHA-HMAC**—Security Hash Algorithm.
Chapter 17      IP Security

Transform Set

IP Compression

Indicates whether IP data compression is used.

Note
If your router does not support IP compression, this box will be disabled.

Mode

This column contains one of the following values:

- Tunnel—Both the headers and data are encrypted. The mode used in VPN configurations.
- Transport—Only the data is encrypted. This mode is used when the encryption endpoints and the communication endpoints are the same.

Type

Either User Defined or Cisco SDM Default.

What Do You Want to Do?

<table>
<thead>
<tr>
<th>If you want to:</th>
<th>Do this:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Add a new transform set to the router’s configuration.</td>
<td>Click Add, and create the transform set in the Add Transform Set window.</td>
</tr>
<tr>
<td>Edit an existing transform set.</td>
<td>Select the transform set, and click <strong>Edit</strong>. Then edit the transform set in the Edit Transform Set window.</td>
</tr>
</tbody>
</table>
|                                          | **Note**  
Cisco SDM Default transform sets are read-only and cannot be edited. |
| Delete an existing transform set.       | Select the transform set, and click **Delete**.                        |
|                                          | **Note**  
Cisco SDM Default transform sets are read-only and cannot be deleted. |
Add or Edit Transform Set

Use this window to add or edit a transform set.

To obtain a description of the allowable transform combinations, and descriptions of the transforms, click **Allowable Transform Combinations**.

**Note**
- Not all routers support all transform sets (encryption types). Unsupported transform sets will not appear in the screen.
- Not all IOS images support all the transform sets that Cisco SDM supports. Transform sets unsupported by the IOS image will not appear in the screen.
- If hardware encryption is turned on, only those transform sets supported by both hardware encryption and the IOS image will appear in the screen.
- Easy VPN servers only support tunnel mode. Transport mode is not supported by Easy VPN servers.
- Easy VPN Servers only support transform sets with ESP encryption. Easy VPN servers do not support the AH algorithm.
- Easy VPN Servers do not support ESP-SEAL encryption.

**Name of this transform set**

This can be any name that you want. The name does not have to match the name in the transform set that the peer uses, but it may be helpful to give corresponding transform sets the same name.

**Data integrity and encryption (ESP)**

Check this box if you want to provide Encapsulating Security Payload (ESP) data integrity and encryption.

**Integrity Algorithm**

Select one of the following:
- ESP_MD5_HMAC. Message Digest 5.
- ESP_SHA_HMAC. Security Hash Algorithm.
Encryption

Cisco SDM recognizes the following ESP encryption types:

- ESP_3DES. ESP, Triple DES. This is a stronger form of encryption than DES, supporting 168-bit encryption.
- ESP_AES_128. ESP, Advanced Encryption Standard (AES). Encryption with a 128-bit key. AES provides greater security than DES and is computationally more efficient than 3DES.
- ESP_AES_192. ESP, AES encryption with a 192-bit key.
- ESP_AES_256. ESP, AES encryption with a 256-bit key.
- ESP_SEAL—ESP with the 160-bit encryption key Software Encryption Algorithm (SEAL) encryption algorithm. SEAL (Software Encryption Algorithm) is an alternative algorithm to software-based Data Encryption Standard (DES), Triple DES (3DES), and Advanced Encryption Standard (AES). SEAL encryption uses a 160-bit encryption key and has a lower impact to the CPU when compared to other software-based algorithms.
- ESP_NULL. Null encryption algorithm, but encryption transform used.

Note

The types of ESP encryption available depend on the router. Depending on the type of router you are configuring, one or more of these encryption types may not be available.

Data and address integrity without encryption (AH)

This check box and the fields below it appear if you click Show Advanced.

Check this box if you want the router to provide Authentication Header (AH) data and address integrity. The authentication header will not be encrypted.

Integrity Algorithm

Select one of the following:

- AH_MD5_HMAC—Message Digest 5.
Mode

Select which parts of the traffic you want to encrypt:

- **Transport.** Encrypt data only—Transport mode is used when both endpoints support IPsec; this mode places the AH or ESP after the original IP header; thus, only the IP payload is encrypted. This method allows users to apply network services such as quality-of-service (QoS) controls to encrypted packets. Transport mode should be used only when the destination of the data is always the remote VPN peer.

- **Tunnel.** Encrypt data and IP header—Tunnel mode provides stronger protection than transport mode. Because the entire IP packet is encapsulated within AH or ESP, a new IP header is attached, and the entire datagram can be encrypted. Tunnel mode allows network devices such as a router to act as an IPsec proxy for multiple VPN users; tunnel mode should be used in those configurations.

**IP Compression (COMP-LZS)**

Check this box if you want to use data compression.

**Note**

Not all routers support IP compression. If your router does not support IP compression, this box is disabled.

**IPSec Rules**

This window shows the IPSec rules configured for this router. IPSec rules define which traffic IPSec will encrypt. The top part of the window lists the access rules defined. The bottom part shows the access rule entries for the access rule selected in the rule list.

IPSec rules contain IP address and type-of-service information. Packets that match the criteria specified in the rule are encrypted. Packets that do not match the criteria are sent unencrypted.

**Name/Num**

The name or number of this rule.
IPSec Rules

Used By

Which crypto maps this rule is used in.

Type

IPSec rules must specify both source and destination and must be able to specify the type of traffic the packet contains. Therefore, IPSec rules are extended rules.

Description

A textual description of the rule, if available.

Action

Either Permit or Deny. Permit means that packets matching the criteria in this rules are protected by encryption. Deny means that matching packets are sent unencrypted. For more information see Meanings of the Permit and Deny Keywords.

Source

An IP address or keyword that specifies the source of the traffic. Any specifies that the source can be any IP address. An IP address in this column may appear alone, or it may be followed by a wildcard mask. If present, the wildcard mask specifies the portions of the IP address that the source IP address must match. For more information, see IP Addresses and Subnet Masks.

Destination

An IP address or keyword that specifies the destination of the traffic. Any specifies that the destination can be any IP address. An IP address in this column may appear alone, or it may be followed by a wildcard mask. If present, the wildcard mask specifies the portions of the IP address that the destination IP address must match.

Service

The type of traffic that the packet must contain.
## What Do You Want to Do?

<table>
<thead>
<tr>
<th>If you want to:</th>
<th>Do this:</th>
</tr>
</thead>
<tbody>
<tr>
<td>See the access rule entries for a particular rule.</td>
<td>Select the rule in the rule list. The entries for that rule appear in the lower box.</td>
</tr>
<tr>
<td>Add an IPSec rule.</td>
<td>Click <strong>Add</strong>, and create the rule in the rule window displayed.</td>
</tr>
<tr>
<td>Delete an IPSec rule.</td>
<td>Select the rule in the rule list, and click <strong>Delete</strong>.</td>
</tr>
<tr>
<td>Delete a particular rule entry.</td>
<td>Select the rule in the rule list, and click <strong>Edit</strong>. Then, delete the entry in the rule window displayed.</td>
</tr>
<tr>
<td>Apply an IPSec rule to an interface.</td>
<td>Apply the rule in the interface configuration window.</td>
</tr>
</tbody>
</table>