



IPSec Configuration

IP Security Protocol (IPSec) is a network layer protocol that provides a process for encrypting and authenticating IP packets sent between VPN peers to VPN devices configured on a tunnel. Using IPSec, you can create an encrypted or authenticated communication path between two endpoints, allowing IP traffic to safely cross public or untrusted networks.

IPSec is a framework of open standards that provides data confidentiality, data integrity, and data origin authentication between peers that are connected over unprotected networks, such as the Internet. IPSec provides security services at the IP layer. It uses IKE to authenticate IPSec peers, negotiate IPSec keys, and automatically negotiate IPSec security associations.

With CVDM-VPNSM, you can do the following:

- Add and edit crypto maps.
- Configure IPSec rules, transform sets, and IKE policies to be applied to traffic on your network.
- Edit IPSec global settings and apply them to all peers on your network.

This chapter contains the following topics:

- [Configuring IPSec Settings, page 5-2](#)
- [Configuring Crypto Maps, page 5-3](#)
- [Configuring Access and IPSec Rules, page 5-33](#)
- [Configuring Transform Sets, page 5-47](#)
- [Configuring IKE Settings, page 5-53](#)
- [Configuring Global Settings, page 5-59](#)

Configuring IPsec Settings

You can view the IPsec information configured on the device. Click **Setup** at the top of the window and click IPsec from the left-most pane to display the main IPsec page (see [Figure 5-1](#)).

Figure 5-1 IPsec Page

The screenshot shows the CiscoView Device Manager for IPsec VPN configuration page. The interface is divided into several sections:

- Setup Pane (Left):** Contains navigation options: Wizards, Site to Site, Remote Access, IPsec (selected), AAA Configuration, and Statistics.
- IPsec Pane (Middle-Left):** Shows a tree view under 'Group by Connection' with sub-items: Crypto Maps, Site to Site, Remote Access, Access Rules, IPsec Rules, Transform Sets, IKE Settings, and GlobalSettings.
- Crypto Map Sets Table:**

Name	Type	Used By	Authen. List	Autho. List	Acc. List	Mode Conf	Status
RA_DYNAMIC_CM...	Dynamic	RA_STATIC_CMAP_1					
RA_STATIC_CMAP_1	Static	Vlan47	AUTHENLI...	AUTHORL...	ACCTLI...	Respond	
S2S_STATIC_CMA...	Static	Vlan45					
S2S_STATIC_CMA...	Static	Vlan49					
S2S_STATIC_CMA...	Static	Vlan51					
S2S_STATIC_CMA...	Static	Vlan52					
- Crypto Map: RA_DYNAMIC_CMAP_1 Table:**

Seq. No.	Peers	Transform Sets	Description	IPsec Rule	Dynamic Map	RRI	Status
1	43.43.43.4	fff					
- Crypto Map Entry: 1:**

Peer	Key	Transform Set	SA Lifetime (Kilobytes): 4608000
43.43.43.4		fff	SA Lifetime (Seconds): 3600
			SA Idle Time (Seconds): 0
			Perfect Forward Secrecy:

The status bar at the bottom indicates the user is logged in as 'dlevel15' and the date is 'Thu Jan 06 09:36:34 PST 2005'.

Configuring Crypto Maps

Crypto maps filter and classify traffic to be protected and define the policy applied to that traffic. IPsec crypto maps define:

- Traffic that should be protected using IPsec rules.
- IPsec peers to which the protected traffic can be forwarded; these are the peers with which a security association (SA) can be established.
- Transform sets that can be used with the protected traffic.

A crypto map comprises crypto map entries (for more information about crypto map entries, see [Adding Crypto Map Entries, page 5-17](#)). You apply crypto maps to interfaces against which IP traffic is evaluated. Only one crypto map can be applied to an interface.

You can filter Crypto Maps folder objects in the [selector](#) on this page by type of crypto map (static or dynamic) or by the type of VPN connection (site-to-site VPNs or remote access VPNs) on which the crypto maps are configured.

To view information about all the crypto maps configured on your device, click **Setup** at the top of the window, click **IPsec** from the left-most pane, and select **Crypto Maps** from the [selector](#). The main Crypto Maps page is displayed, providing information about all crypto maps configured on the device. You can also do the following:

- To display selector objects for crypto map type, select **Group by Type** from the list in the selector. The static and dynamic objects appear in the Crypto Maps folder.

The **Crypto Maps > Static** page displays information about static crypto maps. You can only add and edit static crypto maps and add dynamic crypto map references from this page. The **Crypto Maps > Dynamic** page displays information about dynamic crypto maps; you can only add and edit dynamic crypto maps from this page. Dynamic crypto maps are recommended for networks in which the peers are not always predetermined.

- To display selector objects for each connection type, select **Group by Connection** from the list in the selector. The site-to-site and remote access objects appear in the Crypto Maps folder.

The **Crypto Maps > Site to Site** page displays information about the crypto maps configured on site-to-site VPN connections; the **Crypto Maps > Remote Access** page displays information about the crypto maps configured on remote access VPN connections. You cannot add or edit dynamic crypto maps from these pages.

The crypto map pages provide the following information.

GUI Element	Description
Crypto Map Sets table	
Name column	Name of the crypto map on the device.
Type column	Type of crypto map (value can be Static or Dynamic).
Used By column	For a static crypto map, this field displays the interfaces on which the crypto map is applied. For a dynamic crypto map, this field displays the static crypto map for which the dynamic crypto map is used.
Authen. List column	Displays the name of the authentication list used by the crypto map if it is used for remote access VPN.
Autho. List column	Displays the name of the authorization list.
Acc. List column	Displays the name of the accounting list.
Mode Conf. column	Displays the mode of configuration (values can be Respond or Initiate).
Status column	Indicates if the crypto map is complete or incomplete.
Crypto Map Details: X table	
Seq. No. column	Sequence number of the crypto map entry.
Peers column	Peers associated with the crypto map entry.
Transform Sets column	Transform sets configured on the crypto map entry.
Description column	Description of the crypto map entry.

GUI Element	Description
IPsec Rule column	IPsec rule configured on the crypto map entry.
Dynamic Map column	Dynamic map associated with the crypto map entry.
RRI column	Indicates whether Reverse Route Injection (RRI) is enabled. RRI simplifies network design for VPNs that require redundancy and routing, by dynamically learning and advertising the IP address and subnets that belong to a remote site that connects through an IPsec VPN tunnel.
Status column	Indicates if the crypto map entry is complete or incomplete.
Crypto Map Entry: X pane	
Peer column	IP address of the remote peer.
Key column	Preshared key configured for the peer.
Transform Set column	Names of the transform sets configured on the selected crypto map entry.
SA Lifetime (kilobytes) field	Value, in kilobytes, to determine how long the SA between VPN devices will exist before it expires. When the data that flows through the IPsec tunnel reaches this value, the SA expires, and the IPsec tunnel between the devices disappears. The range of values is 2560 to 536870912. Note You can also apply this value globally. See Configuring Global Settings, page 5-59 for more information.
SA Lifetime (Seconds) field	Value, in seconds, to determine how long the SA between VPN devices will exist before it expires. The range of values is 120 to 864000.

GUI Element	Description
SA Idle Time (Seconds) field	Time, in seconds, that the idle timer will allow an inactive peer to maintain the SA. The range of values is 60 to 86400.
Perfect Forward Secrecy field	Indicates whether perfect forward secrecy is enabled. Perfect forward secrecy ensures that each preshared key is derived independently, so if one key is compromised, no other keys are compromised.


From the Crypto Maps page, you can access functions to do the following:

- Add a crypto map. See [Adding Crypto Maps, page 5-6](#).
- Edit a crypto map. See [Editing Crypto Maps, page 5-14](#).
- Delete a crypto map. See [Deleting Crypto Maps, page 5-17](#).
- Add a crypto map entry. See [Adding Crypto Map Entries, page 5-17](#).
- Edit a crypto map entry. See [Editing Crypto Map Entries, page 5-25](#).
- Delete a crypto map entry. See [Deleting Crypto Map Entries, page 5-32](#).

Adding Crypto Maps

- Step 1** Do the following:
- a. Click **Setup** at the top of the window, and click **IPsec** from the left-most pane.
 - b. Select one of the following from the [selector](#):
 - **Crypto Maps**
 - **Crypto Maps > Static**
 - **Crypto Maps > Dynamic**
 - **Crypto Maps > Site to Site**
 - **Crypto Maps > Remote Access**
- Step 2** From the [Crypto Map Sets table](#), click **Add...** The Add Crypto Map dialog box appears.

Step 3 Edit the appropriate values.

GUI Element	Action/Description
Name field	Enter the name of the crypto map.
Type list or field	<p>Select, from the list, the type of crypto map (static or dynamic).</p> <p>The list is displayed only when you are adding crypto maps from the main Crypto maps page; it allows you to create a dynamic or static crypto map.</p> <p>When adding crypto maps from the Static, Crypto, Site to Site, or Remote Access pages, you can only add static crypto maps; in these pages, the value of this field is <i>static</i> and cannot be changed.</p> <p>When adding crypto maps from the Dynamic page, you can only add dynamic crypto maps; in this page, the value of this field is <i>dynamic</i> and cannot be changed.</p>
Local Address	<p>Click  and select Select Interface. The Select Interface for Local Address dialog box appears. See Select Interface for Local Address Dialog Box, page 5-10. You cannot select a local interface for dynamic crypto maps.</p> <p>You can also clear your entry by selecting Clear Entry.</p>

GUI Element	Action/Description
Remote Access check box	<p>Select this check box if you want to use this crypto map for the remote access VPNs. You cannot edit any of these values for dynamic crypto maps.</p> <p>Then, do the following:</p> <ul style="list-style-type: none"> In the Authentication List field, specify the list for authentication to use for this crypto map. Click <input type="button" value="▽..."/> and select Authentication List. The Select an Authentication list dialog box appears. See Select an Authentication List Dialog Box, page 5-11. You can also clear your entry by selecting Clear Entry. In the Authorization List field, specify the list for authorization to use for this crypto map. Click <input type="button" value="▽..."/> and select Authorization List. The Select an Authorization list dialog box appears. See Select an Authorization List Dialog Box, page 5-12. You can also clear your entry by selecting Clear Entry. In the Accounting List field, specify the list for accounting to use for this crypto map. Click <input type="button" value="▽..."/> and select Accounting List. The Select an Accounting list dialog box appears. See Select an Accounting List dialog box, page 5-13. You can also clear your entry by selecting Clear Entry. From the Mode Config pane, select the Respond and/or Initiate check box to configure the crypto map mode.

Crypto Map Entries table

Seq. Number	Sequence number of the crypto map entry.
Peers	IP address of the remote peer.
Transform Sets	Names of the transform sets configured on the crypto map entry.
IPSec Rule	Names of the IPSec rules configured on the crypto map entry.
Dynamic Map	Name of the dynamic crypto map configured on the crypto map entry.

GUI Element	Action/Description
Add button	<p>Click to add a crypto map entry for the corresponding crypto map.</p> <p>If you are adding a static crypto map, you can add a static crypto map entry; click Add > Add Crypto Map Entry to open the Add Static Crypto Map Entry dialog box. If you are adding a dynamic crypto map entry, click Add to open the Add Dynamic Crypto Map Entry dialog box. See Adding Crypto Map Entries, page 5-17.</p> <p>If you are adding a static crypto map, you can add a reference to a dynamic crypto map by selecting Add > Add Reference to Dynamic Crypto Map. See Adding Dynamic Crypto Map References, page 5-24 for more information.</p>
Edit button	<p>You can edit your crypto map entries; select an entry from the table and click Edit.</p> <p>If you are adding a static crypto map, you can add a static crypto map entry; click Edit to open the Edit Static Crypto Map Entry dialog box. If you are adding a dynamic crypto map entry, click Edit to open the Edit Dynamic Crypto Map Entry dialog box. See Editing Crypto Map Entries, page 5-25.</p>
Delete button	<p>To delete a crypto map entry, select an entry from the table and click Delete.</p>

- Step 4** Click **Deliver** at the top of the window. For more information on delivering accumulated CLI commands, see [Delivering CLI Commands to the Device, page 1-22](#).

Select Interface for Local Address Dialog Box

GUI Element	Action/Description
Interfaces column	<p>The table in the Interfaces column, displays all interfaces and VLANs on the device. I</p> <p>From the table, select the interface you want to configure. When you select an interface to track, the table displays the following columns:</p> <ul style="list-style-type: none"> • Name—Indicates the name assigned to an interface. • Type—Indicates the hardware type of an interface. • Mode—Indicates the mode of an interface. <p>When you select a VLAN to track, the table displays the following column:</p> <ul style="list-style-type: none"> • Name—Indicates the name of the VLAN.
Add>> button	With interfaces selected in the Interfaces column, click to add selected interfaces to the Selected Interfaces table .
<<Remove button	With interfaces selected, click to remove selected interfaces from the table.
Clear All button	Click to remove all interfaces listed in the Selected Interfaces table and put them back in the Available Ports table.
Selected Interfaces table	<p>Displays all selected interfaces.</p> <p>The Name field indicates the name of a selected interface.</p>

Select an Authentication List Dialog Box

Column	Description
Name	Name of the authentication list.
Type	Type of authentication list.
Method 1	<p>The name of the method that the device will attempt to use first for authentication. Authentication services identify users before they are permitted access to the network or network services. Authentication provides the method for identifying users, including username and password, challenge and response, messaging support, and, depending on the security protocol selected, encryption.</p> <p>A method is a configured server group used for authenticating users. You can configure up to four methods and specify the order in which you want the device to query them. The device attempts to communicate with the first method. If one of the servers in this method authenticates the user, then authentication is successful. If authentication fails, then the router uses the next method in the list.</p>
Method 2	The name of the method that the device will attempt to use for authentication if the servers referenced in method 1 do not respond.
Method 3	The name of the method that the device will attempt to use for authentication if the servers referenced in method 1 and method 2 do not respond.
Method 4	The name of the method that the device will attempt to use for authentication if the servers referenced in method 1, method 2, and method 3 do not respond.

Select an Authorization List Dialog Box

Column	Description
Name	Name of the authorization list.
Type	Type of authorization list.
Method 1	<p>The name of the method that the device will attempt to use first for authorization. Authorization services compose a set of attribute-value pairs that describe privileges for the identified user. These attribute-value pairs are compared to the information contained in a TACACS+ or RADIUS server database.</p> <p>A method is a configured server group used for authorizing users. You can configure up to four methods and specify the order in which you want the device to query them. The device attempts to communicate with the first method. If one of the servers in this method authenticates the user, then authentication is successful. If authentication fails, then the router uses the next method in the list.</p>
Method 2	The name of the method that the device will attempt to use for authentication if the servers referenced in method 1 do not respond.
Method 3	The name of the method that the device will attempt to use for authentication if the servers referenced in method 1 and method 2 do not respond.
Method 4	The name of the method that the device will attempt to use for authentication if the servers referenced in method 1, method 2, and method 3 do not respond.

Select an Accounting List dialog box

Column	Description
Name	Name of the accounting list.
Type	Type of accounting list.
Method 1	<p>The name of the method that the device will attempt to use first for accounting. Accounting services log the services accessed and the network resources used by users. It provides the method for collecting and distributing information such as user identities, start and stop times, executed commands, number of packets, and number of bytes.</p> <p>A method is a configured server group used for accounting users. You can configure up to four methods and specify the order in which you want the device to query them. The device attempts to communicate with the first method. If one of the servers in this method authenticates the user, then authentication is successful. If authentication fails, then the router uses the next method in the list.</p>
Method 2	The name of the method that the device will attempt to use for authentication if the servers referenced in method 1 do not respond.
Method 3	The name of the method that the device will attempt to use for authentication if the servers referenced in method 1 and method 2 do not respond.
Method 4	The name of the method that the device will attempt to use for authentication if the servers referenced in method 1, method 1, and method 3 do not respond.

Column	Description
Notice column	Indicates whether accounting notices are sent. Values can be: <ul style="list-style-type: none"> • <i>None</i>—No accounting notices are sent. • <i>Start-stop</i>—A start accounting notice is sent at the beginning of a process and a stop accounting notice is sent at the end of a process. • <i>Stop-only</i>—A stop accounting notice is sent at the end of a process.
Broadcast column	Indicates whether AAA Broadcast Accounting is enabled. AAA Broadcast Accounting allows accounting information to be broadcast to one or more AAA servers simultaneously.

Editing Crypto Maps

- Step 1** Do the following:
- a. Click **Setup** at the top of the window, and click **IPsec** from the left-most pane.
 - b. Select one of the following from the [selector](#):
 - **Crypto Maps**
 - **Crypto Maps > Static**
 - **Crypto Maps > Dynamic**
 - **Crypto Maps > Site to Site**
 - **Crypto Maps > Remote Access**
- Step 2** From the [Crypto Map Sets table](#), select the crypto map you want to edit and click **Edit...** The Edit Crypto Map dialog box appears.
- Step 3** Edit the appropriate values.

GUI Element	Action/Description
Name field	Name of the crypto map. This value cannot be changed.
Type field	The type of crypto map (static or dynamic). This value cannot be changed.
Local Address	<p>Click <input type="text" value="▽..."/> and select Select Interface. The Select Interface for Local Address dialog box appears. See Select Interface for Local Address Dialog Box, page 5-10. You cannot select an interface for dynamic crypto maps.</p> <p>You can also clear your entry by selecting Clear Entry.</p>
Remote Access check box	<p>Select this check box if you want to use this crypto map for the remote access VPNs. You cannot edit any of these values for dynamic crypto maps.</p> <p>Then, do the following:</p> <ul style="list-style-type: none"> <p>In the Authentication List field, specify the list for authentication to use for this crypto map.</p> <p>Click <input type="text" value="▽..."/> and select Authentication List. The Select an Authentication list dialog box appears. See Select an Authentication List Dialog Box, page 5-11.</p> <p>You can also clear your entry by selecting Clear Entry.</p> <p>In the Authorization List field, specify the list for authorization to use for this crypto map.</p> <p>Click <input type="text" value="▽..."/> and select Authorization List. The Select an Authorization list dialog box appears. See Select an Authorization List Dialog Box, page 5-12.</p> <p>You can also clear your entry by selecting Clear Entry.</p> <p>In the Accounting List field, specify the list for accounting to use for this crypto map.</p> <p>Click <input type="text" value="▽..."/> and select Accounting List. The Select an Accounting list dialog box appears. See Select an Accounting List dialog box, page 5-13.</p> <p>You can also clear your entry by selecting Clear Entry.</p> <p>From the Mode Configuration pane, select the Response and/or Initiate check box to configure the crypto map mode.</p>

GUI Element	Action/Description
Crypto Map Entries table	
Seq. Number	Sequence number of the crypto map entry.
Peers	IP address of the remote peer.
Transform Sets	Names of the transform sets configured on the crypto map entry.
IPsec Rule	Names of the IPsec rules configured on the crypto map entry.
Dynamic Map column	Dynamic map configured on the crypto map entry.
Add button	<p>Click to add a crypto map entry for the corresponding crypto map.</p> <p>If you are adding a static crypto map, you can add a static crypto map entry; click Add > Add Crypto Map Entry to open the Add Static Crypto Map Entry dialog box. If you are adding a dynamic crypto map entry, click Add to open the Add Dynamic Crypto Map Entry dialog box. See Adding Crypto Map Entries, page 5-17.</p> <p>If you are adding a static crypto map, you can add a reference to a dynamic crypto map by clicking Add > Add Reference to Dynamic Crypto Map. See Adding Dynamic Crypto Map References, page 5-24 for more information.</p>
Edit button	<p>You can edit your crypto map entries; select an entry from the table and click Edit.</p> <p>If you are adding a static crypto map, you can add a static crypto map entry; click Edit to open the Edit Static Crypto Map Entry dialog box. If you are adding a dynamic crypto map entry, click Edit to open the Edit Dynamic Crypto Map Entry dialog box. See Editing Crypto Map Entries, page 5-25.</p>
Delete button	To delete an entry from the table, select the entry and click Delete .

- Step 4** Click **Deliver** at the top of the window. For more information on delivering accumulated CLI commands, see [Delivering CLI Commands to the Device, page 1-22](#).

Deleting Crypto Maps

- Step 1** Do the following:
- a. Click **Setup** at the top of the window, and click **IPsec** from the left-most pane.
 - b. Select one of the following from the [selector](#):
 - **Crypto Maps**
 - **Crypto Maps > Static**
 - **Crypto Maps > Dynamic**
 - **Crypto Maps > Site to Site**
 - **Crypto Maps > Remote Access**
- Step 2** From the [Crypto Map Sets](#) table, select the map you want to delete.
- Step 3** Click **Delete**.
-

Adding Crypto Map Entries

Crypto map entries reference specific transform sets and apply them to the traffic flow. Crypto map entries created for IPsec pull together the various parts used to set up IPsec SAs. Crypto map entries with the same crypto map name but different sequence numbers are grouped together and are applied to an interface against which all traffic passing through the interface is evaluated. The crypto map entries on the peers must be configured with compatible information for that information to be exchanged between peers.

You can add and edit both static and dynamic crypto map entries. For a static crypto map entry, you configure all parameters. A dynamic crypto map entry is a crypto map entry that does not have all its parameters configured. Its missing parameters are dynamically configured to match a peer's requirements, allowing peers to exchange traffic with the VPN device even if the VPN device does not have a crypto map entry configured to meet the requirements of the peer.

See the following topics:


- [Adding Static Crypto Map Entries, page 5-18](#)
- [Adding Dynamic Crypto Map Entries, page 5-21](#)
- [Adding Dynamic Crypto Map References, page 5-24](#)

Adding Static Crypto Map Entries

-
- Step 1** Do the following:
- a. Click **Setup** at the top of the window, and click **IPSec** from the left-most pane.
 - b. Select one of the following from the **selector**:
 - **Crypto Maps**
 - **Crypto Maps > Static**
 - **Crypto Maps > Site to Site**
 - **Crypto Maps > Remote Access**
- Step 2** From the [Crypto Map Sets table](#), select the static crypto map to which you want to add a crypto map entry
- Step 3** From the [Crypto Maps Details table](#), click **Add...**, then select **Add Crypto Map Entry**. The Add Static Crypto Map dialog box appears.
- Step 4** Edit the appropriate values.

GUI Element	Action/Description
General tab	
Sequence Number	Sequence number of the static crypto map entry.
Description	Description of the static crypto map entry.

GUI Element	Action/Description
Security Association pane	
Lifetime (kilobytes)	<p>Value, in kilobytes, to determine how long the SA between VPN devices will exist before it expires. When the data that flows through the IPsec tunnel reaches this value, the SA expires, and the IPsec tunnel between the devices disappears.</p> <p>The default value is 4608000. The range of values you can use is 2560 to 536870912.</p> <p>Note You can also apply this value globally. See Configuring Global Settings, page 5-59 for more information.</p>
Lifetime (seconds)	<p>Value, in seconds, to determine how long the SA between VPN devices will exist before it expires.</p> <p>The default value is 3600. The range of values you can use is 120 to 864000.</p>
Idle time (seconds) check box and field	<p>Time, in seconds, that the idle timer will allow an inactive peer to maintain the SA. The range of values you can use is 60 to 86400.</p>
Enable perfect forward secrecy (PFS) check box	<p>Click this check box to enable perfect forward secrecy. Perfect forward secrecy guarantees that each preshared key is derived independently, so if one key is compromised, no other keys are compromised.</p> <p>Then, from the D-H group list, select the D-H algorithm (group1, group2, or group5) to use.</p>
Enable Reverse Route Injection check box	<p>Click to enable Reverse Route Injection (RRI).</p> <p>RRI simplifies network design for VPNs which require redundancy and routing by dynamically learning and advertising the IP address and subnets that belong to a remote site that connects through an IPsec VPN tunnel.</p>

GUI Element	Action/Description
Select Traffic to Protect pane	
IPsec Rule field	You can add an IPsec rule to this crypto map entry. Click  and select Select IPsec rule to specify an existing IPsec rule. The Select a Rule dialog box appears. Select a rule from the table and click OK . You can clear this field by selecting Clear Selection .
Peer tab	
IP Address	Enter the IP address of the peer.
Add>> button	After entering a peer IP address, click to add to the Peers table .
Remove button	To remove an entry from the Peers table , select the entry and click Remove .
Clear All button	To clear all entries from the Peers table, click Clear All .
Peers table	Displays all peers.
Transform Set tab	
Select Transform Sets table	Displays available transform sets.
Add>> button	To add a transform set, select the transform set from the Select Transform Sets table and click Add>> .
<<Remove button	To remove a transform set, select the transform set from the Selected Transform Sets table and click <<Remove .
Clear All button	To clear all entries from the Selected Transform Sets table , click Clear All .
Selected Transform Sets table	Displays the transform sets selected.

Step 5 Click **Deliver** at the top of the window. For more information on delivering accumulated CLI commands, see [Delivering CLI Commands to the Device, page 1-22](#).

Adding Dynamic Crypto Map Entries




Note You can use dynamic crypto map entries only when Internet Key Exchange (IKE) is enabled.

- Step 1** Do the following:
- a. Click **Setup** at the top of the window, and click **IPsec** from the left-most pane.
 - b. Select one of the following from the **selector**:
 - **Crypto Maps**
 - **Crypto Maps > Dynamic**
- Step 2** From the **Crypto Map Sets** table, select the dynamic crypto map to which you want to add a crypto map entry.
- Step 3** From the **Crypto Maps Details** table, click **Add...**, then select **Add Crypto Map Entry**. The Add Dynamic Crypto Map dialog box appears.
- Step 4** Edit the appropriate values.

GUI Element	Action/Description
General tab	
Sequence Number	Sequence number of the dynamic crypto map entry.
Description	Description of the dynamic crypto map entry.

GUI Element	Action/Description
Security Association pane	
Lifetime (kilobytes)	<p>Value, in kilobytes, to determine how long the SA between VPN devices will exist before it expires. When the data that flows through the IPsec tunnel reaches this value, the SA expires, and the IPsec tunnel between the devices disappears.</p> <p>The default value is 4608000. The range of values you can use is 2560 to 536870912.</p> <p>Note You can also apply this value globally. See Configuring Global Settings, page 5-59 for more information.</p>
Lifetime (seconds)	<p>Value, in seconds, to determine how long the SA between VPN devices will exist before it expires.</p> <p>The default value is 3600. The range of values you can use is 120 to 864000.</p>
Idle time (seconds) check box and field	<p>Time, in seconds, that the idle timer will allow an inactive peer to maintain the SA. The range of values you can use is 60 to 86400.</p>
Enable perfect forward secrecy (PFS) check box	<p>Click this check box to enable perfect forward secrecy. Perfect forward secrecy guarantees that each preshared key is derived independently, so if one key is compromised, no other keys are compromised.</p> <p>Then, from the D-H group list, select the D-H algorithm (group1, grup2, or group5) to use.</p>
Enable Reverse Route Injection check box	<p>Click to enable Reverse Route Injection (RRI).</p> <p>RRI simplifies network design for VPNs which require redundancy and routing by dynamically learning and advertising the IP address and subnets that belong to a remote site that connects through an IPsec VPN tunnel.</p>

GUI Element	Action/Description
Select Traffic to Protect pane	
IPsec Rule	You can add an IPsec rule to this crypto map entry. Click  and select Select IPsec rule to specify an existing IPsec rule. The Select a Rule dialog box appears. Select a rule from the table and click OK . You can clear this field by selecting Clear Selection .
Peer tab	
IP Address	Enter the IP address of the peer.
Add>> button	After entering a peer IP address, click to add to the Peers table .
<<Remove button	To remove an entry from the Peers table , select an entry and click << Remove .
Clear All button	To clear all entries from the Peers table , click Clear All .
Peers table	Displays all peers.
Transform Set tab	
Select Transform Sets table	Displays available transform sets.
Add>> button	To add a transform set, select the transform set from the Select Transform Sets table and click Add>> .
<<Remove button	To remove a transform set, select the transform set from the Selected Transform Sets table and click << Remove .
Clear button	To clear all entries from the Selected Transform Sets table , click Clear All .
Selected Transform Sets table	Displays the transform sets selected.

- Step 5** Click **Deliver** at the top of the window. For more information on delivering accumulated CLI commands, see [Delivering CLI Commands to the Device, page 1-22](#).

Adding Dynamic Crypto Map References

You can add a dynamic crypto map reference to a crypto map entry for a static crypto map.

-
- Step 1** Do the following:
- a. Click **Setup** at the top of the window, and click **IPsec** from the left-most pane.
 - b. Select one of the following from the [selector](#):
 - **Crypto Maps**
 - **Crypto Maps > Static**
 - **Crypto Maps > Site to Site**
 - **Crypto Maps > Remote Access**
- Step 2** From the [Crypto Map Sets table](#), select the static crypto map to which you want to add a dynamic crypto map entry.
- Step 3** From the [Crypto Maps Details table](#), click **Add...**, then select **Add Dynamic Crypto Map Reference**.

GUI Element	Action/Description
Sequence Number field	Enter the crypto map entry sequence number.
Dynamic Crypto Map field	Select a dynamic crypto map. Click <input type="button" value="▽..."/> and select Select Dynamic Crypto Map to open the Select Crypto Map dialog box. See Select Crypto Map Dialog Box, page 3-11 for more information.

- Step 4** Click **Deliver** at the top of the window. For more information on delivering accumulated CLI commands, see [Delivering CLI Commands to the Device, page 1-22](#).
-

Editing Crypto Map Entries

You can edit static and dynamic crypto map entries. See the following topics:


- [Editing Static Crypto Map Entries, page 5-25](#)
- [Editing Dynamic Crypto Map Entries, page 5-28](#)
- [Editing Dynamic Crypto Map References, page 5-31](#)

Editing Static Crypto Map Entries

-
- Step 1** Do the following:
- a. Click **Setup** at the top of the window, and click **IPsec** from the left-most pane.
 - b. Select one of the following from the [selector](#):
 - **Crypto Maps**
 - **Crypto Maps > Static**
 - **Crypto Maps > Site to Site**
 - **Crypto Maps > Remote Access**
- Step 2** From the [Crypto Map Sets table](#), select the static crypto map whose entry you want to edit.
- Step 3** From the [Crypto Maps Details table](#), select the crypto map entry that you want to edit and click **Edit...** The Edit Static Crypto Map dialog box appears.
- Step 4** Edit the appropriate values.

GUI Element	Action/Description
General tab	
Sequence Number	Sequence number of the static crypto map entry.
Description	Description of the static crypto map entry.

GUI Element	Action/Description
Security Association pane	
Lifetime (kilobytes)	<p>Value, in kilobytes, to determine how long the SA between VPN devices will exist before it expires. When the data that flows through the IPsec tunnel reaches this value, the SA expires, and the IPsec tunnel between the devices disappears.</p> <p>The default value is 4608000. The range of values you can use is 2560 to 536870912.</p> <p>Note You can also apply this value globally. See Configuring Global Settings, page 5-59 for more information.</p>
Lifetime (seconds)	<p>Value, in seconds, to determine how long the SA between VPN devices will exist before it expires.</p> <p>The default value is 3600. The range of values you can use is 120 to 864000.</p>
Idle time (seconds) check box and field	<p>Time, in seconds, that the idle timer will allow an inactive peer to maintain the SA. The range of values you can use is 60 to 86400.</p>
Enable perfect forward secrecy (PFS) check box	<p>Click this check box to enable perfect forward secrecy. Perfect forward secrecy guarantees that each preshared key is derived independently, so if one key is compromised, no other keys are compromised.</p> <p>Then, from the D-H group list, select the D-H algorithm (group1, grup2, or group5) to use.</p>
Enable Reverse Route Injection check box	<p>Click to enable Reverse Route Injection (RRI).</p> <p>RRI simplifies network design for VPNs which require redundancy and routing by dynamically learning and advertising the IP address and subnets that belong to a remote site that connects through an IPsec VPN tunnel.</p>

GUI Element	Action/Description
IPsec Rules pane	
IPsec Rule	You can add an IPsec rule to this crypto map entry. Click  and select Select IPsec rule to specify an existing IPsec rule. The Select a Rule dialog box appears. Select a rule from the table and click OK . You can clear this field by selecting Clear Selection .
Peer tab	
IP Address field	Enter the IP address of the peer.
Add>> button	After entering a peer IP address, click to add to the Peers table .
Remove button	To remove an entry from the Peers table , select an entry and click Remove .
Clear All button	To clear all entries from the Peers table, click Clear All .
Peers table	Displays all peers.
Transform Set tab	
Select Transform Sets table	Displays available transform sets.
Add>> button	To add a transform set, select the transform set from the Select Transform Sets table and click Add>> .
<<Remove button	To remove a transform set, select the transform set from the Selected Transform Sets table and click <<Remove .
Clear button	To clear all entries from the Selected Transform Sets table , click Clear All .
Selected Transform Sets table	Displays the transform sets selected.


- Step 5** Click **Deliver** at the top of the window. For more information on delivering accumulated CLI commands, see [Delivering CLI Commands to the Device, page 1-22](#).

Editing Dynamic Crypto Map Entries

- Step 1** Do the following:
- a. Click **Setup** at the top of the window, and click **IPsec** from the left-most pane.
 - b. Select one of the following from the [selector](#):
 - **Crypto Maps**
 - **Crypto Maps > Dynamic**
- Step 2** From the [Crypto Map Sets table](#), select the dynamic crypto map whose entry you want to edit.
- Step 3** From the [Crypto Maps Details table](#), select the crypto map entry that you want to edit and click **Edit...** The Edit Dynamic Crypto Map dialog box appears.
- Step 4** Edit the appropriate values.

GUI Element	Action/Description
General tab	
Sequence Number	Sequence number of the dynamic crypto map entry.
Description	Description of the dynamic crypto map entry.

GUI Element	Action/Description
Security Association pane	
Lifetime (kilobytes)	<p>Value, in kilobytes, to determine how long the SA between VPN devices will exist before it expires. When the data that flows through the IPsec tunnel reaches this value, the SA expires, and the IPsec tunnel between the devices disappears.</p> <p>The default value is 4608000. The range of values you can use is 2560 to 536870912.</p> <p>Note You can also apply this value globally. See Configuring Global Settings, page 5-59 for more information.</p>
Lifetime (seconds)	<p>Value, in seconds, to determine how long the SA between VPN devices will exist before it expires.</p> <p>The default value is 3600. The range of values you can use is 120 to 864000.</p>
Idle time (seconds) check box and field	<p>Time, in seconds, that the idle timer will allow an inactive peer to maintain the SA. The range of values you can use is 60 to 86400.</p>
Enable perfect forward secrecy (PFS) check box	<p>Click this check box to enable perfect forward secrecy. Perfect forward secrecy guarantees that each preshared key is derived independently, so if one key is compromised, no other keys are compromised.</p> <p>Then, from the D-H group list, select the D-H algorithm (group1, grup2, or group5) to use.</p>
Enable Reverse Route Injection check box	<p>Click to enable Reverse Route Injection (RRI).</p> <p>RRI simplifies network design for VPNs which require redundancy and routing by dynamically learning and advertising the IP address and subnets that belong to a remote site that connects through an IPsec VPN tunnel.</p>

GUI Element	Action/Description
Select Traffic to Protect pane	
IPSec Rule field	<p>You can add an IPsec rule to this crypto map entry. Click  and do one of the following:</p> <ul style="list-style-type: none"> • Select Select IPsec rule to specify an existing IPsec rule. The Select a Rule dialog box appears. Select a rule from the table and click OK. • Select Create IPsec Rule to create a new IPsec rule. The Add IPsec Rule dialog box appears. For more information, see Adding IPsec Rules, page 5-35. <p>You can clear this field by selecting Clear Selection.</p>
Peer tab	
IP Address field	Enter the IP address of the peer.
Add>> button	After entering a peer IP address, click to add to the Peers table .
<<Remove button	To remove an entry from the Peers table , select the entry and click <<Remove .
Clear All button	To clear all entries from the Peers table, click Clear All .
Peers table	Displays all peers.
Transform Set tab	
Select Transform Sets table	Displays available transform sets.
Add>> button	To add a transform set, select the transform set from the Select Transform Sets table and click Add>> .
<<Remove button	To remove a transform set, select the transform set from the Selected Transform Sets table and click <<Remove .
Clear button	To clear all entries from the Selected Transform Sets table , click Clear All .
Selected Transform Sets table	Displays the transform sets selected.

- Step 5** Click **Deliver** at the top of the window. For more information on delivering accumulated CLI commands, see [Delivering CLI Commands to the Device, page 1-22](#).

Editing Dynamic Crypto Map References

You can edit a dynamic crypto map reference to a crypto map entry for a static crypto map.

- Step 1** Do the following:
- a. Click **Setup** at the top of the window, and click **IPsec** from the left-most pane.
 - b. Select one of the following from the [selector](#):
 - **Crypto Maps**
 - **Crypto Maps > Static**
 - **Crypto Maps > Site to Site**
 - **Crypto Maps > Remote Access**
- Step 2** From the [Crypto Map Sets table](#), select the static crypto map whose dynamic crypto map entry you want to edit.
- Step 3** From the [Crypto Maps Details table](#), select the dynamic crypto map reference you want to edit and click **Edit**. The Edit Crypto Map Entry dialog box appears.
- Step 4** Edit the appropriate values.

GUI Element	Action/Description
Sequence Number field	Enter the crypto map entry sequence number.
Dynamic Crypto Map field	Select a dynamic crypto map. Click <input type="text" value="▽..."/> and select Select Dynamic Crypto Map to open the Select Crypto Map dialog box. See Select Crypto Map Dialog Box, page 3-11 for more information.

- Step 5** Click **Deliver** at the top of the window. For more information on delivering accumulated CLI commands, see [Delivering CLI Commands to the Device](#), page 1-22.
-

Deleting Crypto Map Entries

You can delete your crypto map entries. To delete a static crypto map entry, see [Deleting Static Crypto Map Entries](#), page 5-32; to delete a dynamic crypto map entry, see [Deleting Dynamic Crypto Map Entries](#), page 5-33.



Note You cannot delete the last remaining crypto map; at least one must be configured.

Deleting Static Crypto Map Entries

- Step 1** Do the following:
- Click **Setup** at the top of the window, and click **IPsec** from the left-most pane.
 - Select one of the following from the [selector](#):
 - **Crypto Maps**
 - **Crypto Maps > Static**
 - **Crypto Maps > Site to Site**
 - **Crypto Maps > Remote Access**
- Step 2** From the [Crypto Map Sets table](#), select the static crypto map from which you want to delete a crypto map entry.
- Step 3** From the [Crypto Maps Details table](#), select the crypto map entry you want to delete.
- Step 4** Click **Delete**.
-

Deleting Dynamic Crypto Map Entries

- Step 1** Do the following:
- a. Click **Setup** at the top of the window, and click **IPSec** from the left-most pane.
 - b. Select one of the following from the [selector](#):
 - **Crypto Maps**
 - **Crypto Maps > Dynamic**
- Step 2** From the [Crypto Map Sets table](#), select the dynamic crypto map from which you want to delete a crypto map entry.
- Step 3** From the [Crypto Maps Details table](#), select the crypto map entry you want to delete.
- Step 4** Click **Delete**.
-

Configuring Access and IPSec Rules

Access rules define how a traffic flow of packets is encrypted. Information described by access rules includes source and destination devices, protocols and services used, and interfaces associated with the rule. IPSec rules, which contain one or more IPSec rule entries (see [Adding IPSec Rule Entries, page 5-41](#) for more information), are those that are used in IPSec configuration.

You can view information about the access and IPSec rules configured on your device. Click **Setup** at the top of the window, click **IPSec** from the left-most pane, and then do one of the following:

- Select **Access Rules** from the [selector](#) to display the main Access Rules page. This page displays all access control lists (ACLs) configured on the device.
- Select **Access Rules > IPSec Rules** from the [selector](#) to display the main IPSec Rules page. This Rules page displays all ACLs used in IPSec configuration. All access lists generated by CVDVM-VPNSM are IPSec rules.

The following information is displayed.

GUI Element	Description
IPsec Rules table	
Name/Number column	Name or number of the rule.
Type column	Type (extended) of rule.
Used by column	Crypto maps on which this rule is applied.
Description column	Description of the rule.
IPsec Rules Details: X table	
Action column	<p>Indicates whether this rule protects the traffic on the network.</p> <p>Values can be either Permit or Deny. Permit means that packets matching the criteria in this rule are protected by encryption. Deny means that matching packets are sent unencrypted.</p> <p>Note This table shows the details for the rule you select from the IPsec Rules table.</p>
Source column	<p>Contains the following subcolumns:</p> <ul style="list-style-type: none"> • IPAddress/Mask—IP address and subnet mask address of the source of the traffic to which the IPsec rule is applied. • Port—Service specified on the source port, if TCP or UDP protocol is applied to the IPsec rule.
Destination column	<p>Contains the following subcolumns:</p> <ul style="list-style-type: none"> • IPAddress/Mask—IP address and subnet mask address of the destination of the traffic to which the IPsec rule is applied. • Port—Service specified on the destination port, if TCP or UDP protocol is applied to the IPsec rule.
Protocol/Type column	Protocol and corresponding service applied to the IPsec rule.
Description column	Description of the IPsec rule.

From this page, you can access functions to do the following:

- Add an IPsec rule. See [Adding IPsec Rules](#), page 5-35.
- Edit an IPsec rule. See [Editing IPsec Rules](#), page 5-39.
- Delete an IPsec rule. See [Deleting Access and IPsec Rules](#), page 5-40.
- Add an IPsec rule entry. See [Adding IPsec Rule Entries](#), page 5-41.
- Edit an IPsec rule entry. See [Editing IPsec Rule Entries](#), page 5-44.
- Delete an IPsec rule entry. See “[Deleting IPsec Rule Entries](#)” section on page 5-47.

Adding IPsec Rules



Note

CVDM-VPNSM supports only the adding and editing of extended IPsec rules.

Step 1

Do one of the following:

- Click **Setup** at the top of the window, click **IPsec** from the left-most pane, and select **Access Rules > IPsec Rules** from the [selector](#).
- Click **Setup** at the top of the window, click **IPsec** from the left-most pane, and select **Access Rules** from the [selector](#).

Step 2

From the [IPsec Rules table](#), click **Add...** The Add IPsec Rule dialog box appears.

Step 3

Edit the appropriate values.

GUI Element	Action/Description
Name field	Enter a name for the IPsec rule.
Type list	Select the type (extended) of IPsec rule.

GUI Element	Action/Description
Description field	Enter a brief description of the IPsec rule.
Rule entry table	<p>Displays the IPsec rule entries applied to the IPsec rule. You can do the following:</p> <ul style="list-style-type: none"> To add an entry, click Add... The Add an Extended Rule Entry dialog box appears. See Adding IPsec Rule Entries, page 5-41 for more information. To edit an entry, select an IPsec rule entry and click Edit... The Edit an Extended Rule Entry dialog box appears. See Editing IPsec Rule Entries, page 5-44 for more information. To clone an entry, select the entry from the table and click Clone... The Clone an Extended Rule Entry dialog box appears. See Clone an Extended Rule Entry Dialog Box, page 5-37 for more information. To delete an IPsec rule entry, select the entry from the table and click Delete...

Step 4 Click **Deliver** at the top of the window. For more information on delivering accumulated CLI commands, see [Delivering CLI Commands to the Device, page 1-22](#).

Clone an Extended Rule Entry Dialog Box

Use this dialog box to create a copy of an existing IPsec rule.

GUI Element	Description
Select an Action pane	
Select an action list	Specify whether or not you want the IPsec rule to protect traffic on the network.
Description pane	
Description field	Enter a description of the IPsec rule.
Source Host/Network pane	
Type list	Select, from the list, the type of network source; you can select one of the following: <ul style="list-style-type: none"> Any IP Address—Select to specify the source using any IP address. Host IP Address—Select to specify the source using its IP address; then, in the Host IP Address field, enter the IP address of the network source. Network—Select to specify the source using its network information; then, in the IP address field, enter the IP address of the network source. From the Wildcard Mask list, select the wildcard subnet mask address of the network source.
Destination Host/Network pane	
Type list	Select, from the list, the type of network destination; you can select one of the following: <ul style="list-style-type: none"> Any IP Address—Select to specify the destination using any IP address. Host IP Address —Select to specify the destination using its IP address; then, in the Host IP Address field, enter the IP address of the network destination. Network—Select to specify the destination using its network information; then, in the IP address field, enter the IP address of the network destination. From the Wildcard Mask list, select the wildcard subnet mask address of the network destination.

GUI Element	Description
Protocol and Service pane	
Protocol and Service radio buttons	<p>Specify the protocol and corresponding services applied to the IPsec rule. The service specifies the type of traffic that packets matching the IPsec rule must contain. A rule permitting or denying multiple services between the same end points must contain an entry for each service. You can select TCP, UDP, ICMP, or IP for the protocol.</p> <ul style="list-style-type: none"> • If you select the TCP or UDP radio button, you must specify source port and destination port information. From the Service list, in both the Service Port and Destination Port panes, select one of the following parameters: <ul style="list-style-type: none"> – = The rule entry applies to the value that you specify; click <input type="text" value="..."/> to specify the service corresponding to the parameter you selected from the Service list. The Service dialog box appears. See Service Dialog Box, page 5-39 for more information. – not= The rule entry applies to any value except the one that you specify; click <input type="text" value="..."/> to specify the service corresponding to the parameter you selected from the Service list. The Service dialog box appears. See Service Dialog Box, page 5-39 for more information. – > The rule entry applies to all port numbers higher than the number you enter. Enter the port number in the corresponding field. – < The rule entry applies to all port numbers lower than the number you enter. Enter the port number in the corresponding field. – range The entry applies to the range of port numbers that you specify in the fields to the right. Enter the range of port numbers in the corresponding fields. • If you select the ICMP or IP radio button, in the ICMP Message pane, click <input type="text" value="..."/>. The Service dialog box appears. See Service Dialog Box, page 5-39. • If you select the IP radio button, in the IP Protocol Type pane, click <input type="text" value="..."/>. The Service dialog box appears. See Service Dialog Box, page 5-39.
Log matches against this entry check box	Select this check box to record matches in the log file sent to the syslog server.

Service Dialog Box

This dialog box displays the services that can be used for a specified protocol for an IPsec rule entry. The services that are available may vary depending upon the protocol used.

Select a service from the dialog box, then click **OK**.

Editing IPsec Rules

-
- Step 1** Do one of the following:
- Click **Setup** at the top of the window, click **IPsec** from the left-most pane, and select **Access Rules > IPsec Rules** from the [selector](#).
 - Click **Setup** at the top of the window, click **IPsec** from the left-most pane, and select **Access Rules** from the [selector](#).
- Step 2** From the [IPsec Rules table](#), select the IPsec rule you want to edit and click **Edit....** The Edit IPsec Rule dialog box appears.
- Step 3** Edit the appropriate values.

GUI Element	Action/Description
Name field	Enter a name for the IPsec rule.
Type list	Select the type of IPsec rule.

GUI Element	Action/Description
Description field	Enter a brief description of the IPsec rule.
Rule entry table	<p>Displays the IPsec rule entries applied to the IPsec rule. You can do the following:</p> <ul style="list-style-type: none"> To add an entry, click Add... The Add an Extended Rule Entry dialog box appears. See Adding IPsec Rule Entries, page 5-41 for more information. To delete an entry, select an IPsec rule entry from the table and click Edit... The Edit an Extended Rule Entry dialog box appears. See Editing IPsec Rule Entries, page 5-44 for more information. To clone an entry, select the entry from the table and click Clone... The Clone an Extended Rule Entry dialog box appears. See Clone an Extended Rule Entry Dialog Box, page 5-37 for more information. To delete an entry, select the entry from the table and click Delete...

- Step 4** Click **Deliver** at the top of the window. For more information on delivering accumulated CLI commands, see [Delivering CLI Commands to the Device, page 1-22](#).

Deleting Access and IPsec Rules

- Step 1** Do one of the following:
- Click **Setup** at the top of the window, click **IPsec** from the left-most pane, and select **Access Rules > IPsec Rules** from the [selector](#).
 - Click **Setup** at the top of the window, click **IPsec** from the left-most pane, and select **Access Rules** from the [selector](#).

The Access Rules page displays all ACLs configured, including IPsec rules; the IPsec rules page only displays ACLs applied to IPsec traffic.

- Step 2** From the [IPsec Rules table](#), select the IPsec rule you want to delete.
- Step 3** Click **Delete**.

Adding IPsec Rule Entries

IPsec rule entries are assigned to an IPsec rule. An IPsec rule entry defines information, such as whether IPsec traffic should be protected, through which subnets the traffic should be protected, and which protocol to apply to traffic exchanged between two peers.

- Step 1** Do one of the following:
- Click **Setup** at the top of the window, click **IPsec** from the left-most pane, and select **Access Rules > IPsec Rules** from the [selector](#).
 - Click **Setup** at the top of the window, click **IPsec** from the left-most pane, and select **Access Rules** from the [selector](#).
- Step 2** From the [IPsec Rules table](#), select the IPsec rule to which you want to add a rule.
- Step 3** From the [IPsec Rule Details: X table](#), click **Add...**. The Add an Extended Rule Entry dialog box appears.
- Step 4** Edit the appropriate values.

GUI Element	Description
Select an Action pane	
Select an action list	Specify whether or not you want the IPsec rule to protect the traffic on the network.
Description pane	
Description field	Enter a description of the IPsec rule.

Source Host/Network pane

Type list	<p>Select, from the list, the type of network source; you can select one of the following:</p> <ul style="list-style-type: none"> • Any IP Address—Select to specify the source using any IP address. • Host IP Address—Select to specify the source using its IP address; then, in the Host IP field, enter the IP address of the network source. • Network—Select to specify the source using its network information; then, in the IP address field, enter the IP address of the network source. From the Wildcard Mask list, select the wildcard subnet mask address of the network source.
-----------	--

Destination Host/Network pane

Type list	<p>Select, from the list, the type of network destination; you can select one of the following:</p> <ul style="list-style-type: none"> • Any IP Address—Select to specify the destination using any IP address. • Host IP Address—Select to specify the destination using its IP address; then, in the Host IP field, enter the IP address of the network destination. • Network—Select to specify the destination using its network information; then, in the IP address field, enter the IP address of the network destination. From the Wildcard Mask list, select the wildcard subnet mask address of the network destination.
-----------	---

Protocol and Service pane

Protocol and Service radio buttons

Specify the protocol and corresponding services applied to the IPsec rule. The service specifies the type of traffic that packets matching the IPsec rule must contain. A rule permitting or denying multiple services between the same end points must contain an entry for each service. You can select TCP, UDP, ICMP, or IP for the protocol.

- If you select the TCP or UDP radio button, you must specify source port and destination port information. From the Service list, in both the Service Port and Destination Port panes, select one of the following parameters:
 - = The rule entry applies to the value that you specify; click to specify the service corresponding to the parameter you selected from the Service list. The Service dialog box appears. See [Service Dialog Box, page 5-39](#) for more information.
 - **not=** The rule entry applies to any value except the one that you specify; click to specify the service corresponding to the parameter you selected from the Service list. The Service dialog box appears. See [Service Dialog Box, page 5-39](#) for more information.
 - > The rule entry applies to all port numbers higher than the number you enter. Enter the port number in the corresponding field.
 - < The rule entry applies to all port numbers lower than the number you enter. Enter the port number in the corresponding field.
 - **range** The entry applies to the range of port numbers that you specify in the fields to the right. Enter the range of port numbers in the corresponding fields.
- If you select the ICMP or IP radio button, in the ICMP Message pane, click . The Service dialog box appears. See [Service Dialog Box, page 5-39](#).
- If you select the IP radio button, in the IP Protocol Type pane, click . The Service dialog box appears. See [Service Dialog Box, page 5-39](#).

Log matches against this entry check box

Select this check box to record matches in the log file sent to the syslog server.

- Step 5** Click **Deliver** at the top of the window. For more information on delivering accumulated CLI commands, see the [“Delivering CLI Commands to the Device” section on page 1-22.](#)
-

Editing IPsec Rule Entries

- Step 1** Do one of the following:
- Click **Setup** at the top of the window, click **IPsec** from the left-most pane, and select **Access Rules > IPsec Rules** from the [selector](#).
 - Click **Setup** at the top of the window, click **IPsec** from the left-most pane, and select **Access Rules** from the [selector](#).
- Step 2** From the [IPsec Rules table](#), select the IPsec rule you whose entry you want to edit.
- Step 3** From the [IPsec Rule Details: X table](#), select the entry you want to edit and click **Edit....** The Edit an Extended Rule Entry dialog box appears.
- Step 4** Edit the appropriate values:

GUI Element	Description
Select an Action pane	
Select an action list	Specify whether or not you want the IPsec rule to protect the traffic on the network.
Description pane	
Description field	Enter a description of the IPsec rule.
Source Host/Network pane	
Type list	Select, from the list, the type of network source; you can select one of the following: <ul style="list-style-type: none"> Any IP Address—Select to specify the source using any IP address. Host IP Address—Select to specify the source using its IP address; then, in the Host IP field, enter the IP address of the network source. Network—Select to specify the source using its network information; then, in the IP address field, enter the IP address of the network source. From the Wildcard Mask list, select the wildcard subnet mask address of the network source.
Destination Host/Network pane	
Type list	Select, from the list, the type of network destination; you can select one of the following: <ul style="list-style-type: none"> Any IP Address—Select to specify the destination using any IP address. Host IP Address—Select to specify the destination using its IP address; then, in the Host IP field, enter the IP address of the network destination. Network—Select to specify the destination using its network information; then, in the IP address field, enter the IP address of the network destination. From the Wildcard Mask list, select the wildcard subnet mask address of the network destination.

GUI Element	Description
Protocol and Service pane	
Protocol and Service radio buttons	<p>Specify the protocol and corresponding services applied to the IPsec rule. The service specifies the type of traffic that packets matching the IPsec rule must contain. A rule permitting or denying multiple services between the same end points must contain an entry for each service. You can select to use TCP, UDP, ICMP, or IP for the protocol.</p> <ul style="list-style-type: none"> • If you select the TCP or UDP radio button, you must specify source port and destination port information. From the Service list, in both the Service Port and Destination Port panes, select one of the following parameters: <ul style="list-style-type: none"> – = The rule entry applies to the value that you specify; click <input type="text" value="..."/> to specify the service corresponding to the parameter you selected from the Service list. The Service dialog box appears. See Service Dialog Box, page 5-39 for more information. – not= The rule entry applies to any value except the one that you specify; click <input type="text" value="..."/> in to specify the service corresponding to the parameter you selected from the Service list. The Service dialog box appears. See Service Dialog Box, page 5-39 for more information. – > The rule entry applies to all port numbers higher than the number you enter. Enter the port number in the corresponding field. – < The rule entry applies to all port numbers lower than the number you enter. Enter the port number in the corresponding field. – range The entry applies to the range of port numbers that you specify in the fields to the right. Enter the range of port numbers in the corresponding fields. • If you select the ICMP or IP radio button, in the ICMP Message pane, click <input type="text" value="..."/>. The Service dialog box appears. See Service Dialog Box, page 5-39. • If you select the IP radio button, in the IP Protocol Type pane, click <input type="text" value="..."/>. The Service dialog box appears. See Service Dialog Box, page 5-39.
Log matches against this entry check box	Select this check box to record matches in the log file sent to the syslog server.

- Step 5** Click **Deliver** at the top of the window. For more information on delivering accumulated CLI commands, see [Delivering CLI Commands to the Device](#), page 1-22.
-

Deleting IPsec Rule Entries

- Step 1** Do one of the following:
- Click **Setup** at the top of the window, click **IPsec** from the left-most pane, and select **Access Rules > IPsec Rules** from the [selector](#).
 - Click **Setup** at the top of the window, click **IPsec** from the left-most pane, and select **Access Rules** from the [selector](#).
- Step 2** From the [IPsec Rules table](#), select the IPsec rule you whose entry you want to delete.
- Step 3** From the [IPsec Rule Details: X table](#), select the entry you want to delete.
- Step 4** Click **Delete**.
-

Configuring Transform Sets

A transform set is a combination of security protocols, algorithms, and other settings to apply to IPsec protected traffic; a transform set specifies how data will be encrypted and authenticated. You configure transform sets and apply them to crypto map entries (for more information, see [Adding Crypto Map Entries](#), page 5-17).

You can view information about the transform sets configured. Click **Setup** at the top of the window, click **IPsec** from the left-most pane, and select **Transform Sets** from the [selector](#) to display the main Transform Sets page. The following information is displayed:

GUI Element	Description
Transform Sets table	
Name column	Name of the transform set. Note When you select an entry from this table, the details of the transform set are displayed in the Details pane.
ESP Encryption column	Type of Encapsulating Security Payload (ESP) encryption protocol (DES, 3DES, Null, AES, AES-192, or AES-256) used for traffic flow.
ESP Authentication column	Type of ESP authentication algorithm (MD5 or SHA) used for traffic flow.
AH Authentication column	Type of Authentication Header (AH) used for traffic flow (SHA or MD5). AH allows for data integrity, but it does not offer data encryption.
Mode column	Method of data transport (tunnel or transport). Use tunnel mode when VPN devices are communicating over a public network, such as the Internet. Use transport mode when a VPN client is communicating over a private network to encrypt the device's inside IP address and any data sent on the private network.
Details: X pane	
ESP Encryption field	Type of ESP encryption protocol that is used for traffic flow for the selected transform set.
ESP Authentication field	Type of ESP authentication algorithm that is used for traffic flow for the selected transform set.
AH Authentication field	Type of Authentication Header (AH) used for traffic flow (SHA or MD5) for the selected transform set. AH allows for data integrity, but it does not offer data encryption.
Mode field	Method of data transport (tunnel or transport) for the selected transform set.

GUI Element	Description
Map Name column	Name of the crypto map on which the selected transform set is configured.
Applied On column	Name of the VLAN to which the transform set is applied.

From this page, you can access functions to do the following:

- Add a transform set. See [Adding Transform Sets, page 5-49](#).
- Edit a transform set. See [Editing Transform Sets, page 5-51](#).
- Delete a transform set. See [Deleting Transform Sets, page 5-52](#).

Adding Transform Sets

- Step 1** Click **Setup** at the top of the window, click **IPsec** from the left-most pane, and select **Transform Sets** from the [selector](#).
- Step 2** Click **Add...** The Add Transform Set dialog box appears.
- Step 3** Edit the appropriate values.

GUI Element	Action/Description
Name	Enter the name of the transform set.
Data and Integrity Encryption (ESP) check box	<p>Click this check box to use Encapsulating Security Payload (ESP) for data encryption and authentication. Then, do the following:</p> <ul style="list-style-type: none"> • From the Encryption list, select the ESP protocol (DES, 3DES, Null, AES, AES-192, or AES-256) for data encryption. • From the Authentication list, select the ESP algorithm (SHA or MD5) for data authentication. Use ESP encryption when ESP authentication is selected. <p>Note If the ESP encryption value is <i>Null</i>, you should use ESP authentication for data authentication; you should not use AH authentication</p>
Data and Address Integrity without Encryption (AH)	Click this check box to use Authentication Header (AH) to send data without encrypting it. Then, select the authentication method (SHA or MD5) from the Authentication list.
Mode pane	<p>Select the mode of the transform set; do one of the following:</p> <ul style="list-style-type: none"> • Select the Tunnel Mode (Encrypt Data and IP Header) radio button if you want to encrypt both the data sent by VPN clients and the inside IP address of the client. Use this method when you are sending data over a private network. • Select the Transport Mode (Encrypt Only Data) radio button if you want to encrypt only the data sent by VPN clients. Use this method when you are sending data over a public network, such as the Internet.

- Step 4** Click **Deliver** at the top of the window. For more information on delivering accumulated CLI commands, see [Delivering CLI Commands to the Device](#), page 1-22.

Editing Transform Sets

- Step 1** Click **Setup** at the top of the window, click **IPsec** from the left-most pane, and select **Transform Sets** from the [selector](#).
- Step 2** Select the transform set you want to edit and click **Edit...** The Edit Transform Set dialog box appears.
- Step 3** Edit the appropriate values.

GUI Element	Action/Description
Name	Enter the name of the transform set. You cannot change this value.
Data and Integrity Encryption (ESP) check box	<p>Click this check box to use Encapsulating Security Payload (ESP) for data encryption and authentication. Then do the following:</p> <ul style="list-style-type: none"> From the Encryption list, select the ESP protocol (DES, 3DES, Null, AES, AES-192, or AES-256) for data encryption. From the Authentication list, select the ESP algorithm (SHA or MD5) for data authentication. Use ESP encryption when ESP authentication is selected. <p>Note If the ESP encryption value is <i>Null</i>, you should use ESP authentication for data authentication; you should not use AH authentication</p>

GUI Element	Action/Description
Data and Address Integrity without Encryption (AH)	Click this check box to use Authentication Header (AH) to send data without encrypting it. Then, select the authentication method (SHA or MD5) from the Authentication list.
Mode pane	Select the mode of the transform set; do one of the following: <ul style="list-style-type: none"> Select the Tunnel Mode (Encrypt Data and IP Header) radio button if you want to encrypt both the data sent by VPN clients and the inside IP address of the client. Use this method when you are sending data over a private network. Select the Transport Mode (Encrypt Only Data) radio button if you want to encrypt only the data sent by VPN clients. Use this method when you are sending data over a public network, such as the Internet.

- Step 4** Click **Deliver** at the top of the window. For more information on delivering accumulated CLI commands, see [Delivering CLI Commands to the Device, page 1-22](#).

Deleting Transform Sets

- Step 1** Click **Setup** at the top of the window, click **IPsec** from the left-most pane, and select **Transform Sets** from the [selector](#).
- Step 2** From the table, select the transform set you want to delete.
- Step 3** Click **Delete**.

Configuring IKE Settings

Internet Key Exchange (IKE) is a protocol used to authenticate IPsec peers, negotiate and distribute encryption keys, and establish IPsec security associations. An IKE policy defines a combination of security parameters used during IKE negotiation. When the IKE negotiation begins, the peer that initiates the negotiation sends all its IKE policies to the remote peer. The remote peer looks for a policy match by comparing its own policies against the policies received from the initiating peers.

IKE preshared keys allow for one or more peers to use individual shared secrets to authenticate encrypted tunnels to a gateway. The same preshared key must be set on the remote peer and any other participating peers.

Click **Setup** at the top of the window, click **IPsec** from the left-most pane, and select **IKE Settings** from the **selector** to display the main IKE Policies page. This page displays a table that contains the following information:

GUI Element	Description
IKE Policies table	
Priority column	IKE policy priority value; this value uniquely identifies the policy.
Encryption column	Encryption algorithm for the policy.
Hash column	Hash algorithm for the policy.
D-H Group column	Diffie-Hellman (D-H) group for the policy. Value can be group1, group2, or group5. A D-H key is an algorithm that allows two VPN peers who have agreed to policies to exchange information over untrusted and unencrypted networks and develop a shared key.
Authentication column	Authentication list used for the policy.
Lifetime column	Value, in seconds, that the IKE security association (SA) will exist before it expires.

GUI Element	Description
IKE Preshared Keys table	
Peer IP Address column	IP address of the peer for which the preshared key is configured.
Subnet Mask column	Subnet mask address of the peer for which the preshared key is configured.
Preshared Key column	Preshared key configured for the peer. The text of the key is not displayed; an asterisk (*) denotes a character in the key.
XAuth column	Indicates whether extended authentication (XAuth) is enabled for the peer.

From this page, you can access functions to do the following:

- Add an IKE policy. For more information, see [Adding IKE Policies, page 5-54](#).
- Edit an IKE policy. For more information, see [Editing IKE Policies, page 5-56](#).
- Delete an IKE policy. See [Deleting IKE Policies, page 5-57](#).
- Add a preshared key. For more information, see [Adding Preshared Keys](#).
- Edit a preshared key. For more information, see [Editing Preshared Keys](#).
- Delete a preshared key. See [Deleting Preshared Keys, page 5-59](#).

Adding IKE Policies

-
- Step 1** Click **Setup** at the top of the window, click **IPsec** from the left-most pane, and select **IKE Settings** from the [selector](#).
- Step 2** From the IKE Policies table, click **Add...** The Add IKE Policy dialog box appears.
- Step 3** Edit the appropriate values.

GUI Element	Action/Description
Priority field	Enter the IKE policy priority value. Each policy is uniquely identified by the priority number you assign. The range of values is 1 to 10000.
Encryption list	Select the encryption algorithm (DES, 3DES, AES_128, AES_192, or AES_256) for the policy.
Hash list	Select the hash algorithm (MD5 or SHA_1) for the policy.
Authentication list	Select the authentication method (PRE_SHARE) for the policy. Only preshared keys can be used.
D-H Group list	Select the D-H group for the policy. Value can be group1, group2, or group5. A D-H key is an algorithm that allows 2 VPN peers who have agreed to policies to exchange information over untrusted and unencrypted networks and develop a shared key.
Lifetime field	Specify the time, in seconds, that the IKE SA will exist before it expires. The default value is 86400. The range of values you can use is 60 to 86400.

- Step 4** Click **Deliver** at the top of the window. For more information on delivering accumulated CLI commands, see [Delivering CLI Commands to the Device, page 1-22](#).

Editing IKE Policies

- Step 1** Click **Setup** at the top of the window, click **IPsec** from the left-most pane, and select **IKE Settings** from the [selector](#).
- Step 2** From the IKE Policies table, select the IKE policy you want to edit and click **Edit....** The Edit IKE Policy dialog box appears.
- Step 3** Edit the appropriate values.

GUI Element	Action/Description
Priority field	IKE policy priority value; this value uniquely identifies the policy. This field cannot be edited.
Encryption list	Select the encryption algorithm (DES, 3DES, AES_128, AES_192, or AES_256) for the policy.
Hash list	Select the hash algorithm (MD5 or SHA_1) for the policy.
Authentication list	Select the authentication method (PRE_SHARE) for the policy. Only preshared keys can be used.
D-H Group list	Select the D-H group for the policy. Value can be group1, group2, or group5. A D-H key is an algorithm that allows 2 VPN peers who have agreed to policies to exchange information over untrusted and unencrypted networks and develop a shared key.
Lifetime field	Specify the time, in seconds, that the IKE SA will exist before it expires. The default value is 86400. The range of values you can use is 60 to 86400.

- Step 4** Click **Deliver** at the top of the window. For more information on delivering accumulated CLI commands, see [Delivering CLI Commands to the Device, page 1-22](#).

Deleting IKE Policies

-
- Step 1** Click **Setup** at the top of the window, click **IPsec** from the left-most pane, and select **IKE Settings** from the [selector](#).
- Step 2** From the IKE Policies table, select the IKE policy you want to delete.
- Step 3** Click **Delete**.
-

Adding Preshared Keys

-
- Step 1** Click **Setup** at the top of the window, click **IPsec** from the left-most pane, and select **IKE Settings** from the [selector](#).
- Step 2** From the IKE Preshared Keys table, click **Add...** The Add Preshared Key dialog box appears.
- Step 3** Edit the appropriate values.

GUI Element	Description
Peer Info pane	
IP Address field	Enter the IP address of the peer.
Mask list	Select, from the list, the subnet mask address of the peer.
Key field	Enter the key to be used for the peer.
Confirm Key field	Reenter the key (specified previously in the Key field) to be used for the peer.
Extended Authentication (XAuth) check box	Select this check box to enable extended authentication.

- Step 4** Click **Deliver** at the top of the window. For more information on delivering accumulated CLI commands, see [Delivering CLI Commands to the Device, page 1-22](#).

Editing Preshared Keys

- Step 1** Click **Setup** at the top of the window, click **IPsec** from the left-most pane, and select **IKE Settings** from the [selector](#).
- Step 2** From the IKE PreShared Keys table, select the preshared key you want to edit and click **Edit....** The Edit Preshared Key dialog box appears.
- Step 3** Edit the appropriate values.

GUI Element	Description
Peer Info pane	
IP Address field	Enter the IP address of the peer.
Mask list	Select, from the list, the subnet mask address of the peer.
Key field	Enter the key to be used for the peer.
Confirm Key field	Reenter the key (specified previously in the Key field) to be used for the peer.
Extended Authentication (XAuth) check box	Select this check box to enable extended authentication (XAuth).

- Step 4** Click **Deliver** at the top of the window. For more information on delivering accumulated CLI commands, see [Delivering CLI Commands to the Device, page 1-22](#).

Deleting Preshared Keys

-
- Step 1** Click **Setup** at the top of the window, click **IPsec** from the left-most pane, and select **IKE Settings** from the [selector](#).
- Step 2** From the IKE Preshared Keys table, select the preshared key you want to delete.
- Step 3** Click **Delete**.
-

Configuring Global Settings

You can view information about the global settings configured on your device. Click **Setup** at the top of the window, click **IPsec** from the left-most pane, and select **Global Settings** from the [selector](#) to display the main Global Settings page. The following information is displayed:

Field	Description
IKE Enabled	Indicates whether IKE is enabled on the device.
IKE Keepalive	Number of seconds that the device waits between sending IKE keepalive packets.
IKE Retry	Number of seconds that the device waits between attempts to establish an IKE connection with the remote peer.
IKE Identity	Hostname of the device or the IP address that the device will use to identify itself in IKE negotiations.
IPsec Security Association Lifetime (kilobytes)	Value, in kilobytes, to determine how long the SA between all devices will exist before it expires. When the data that flows through the IPsec tunnel reaches this value, the SA expires, and the IPsec tunnel between the devices disappears.

Field	Description
IPsec Security Association Lifetime (time)	Value, in hours, minutes, and seconds, to determine how long the SA between devices will exist before it expires.
IPsec Security Idle Time	Time, in seconds, that the idle timer will allow an inactive peer to maintain the SA.

You can edit your global settings from this page. See the [Editing Global Settings, page 5-60](#).

Editing Global Settings

- Step 1** Click **Setup** at the top of the window, click **IPsec** from the left-most pane, and select **IPsec > Global Settings** from the [selector](#).
- Step 2** Click **Edit...** The VPN Global Settings dialog box appears.
- Step 3** Edit the appropriate values.

Field	Description
Internet Key Exchange (IKE) Settings pane	
Enable IKE check box	Select to enable IKE.
Identity (of this router) list	Select, from the list, how the device is identified (hostname or address).
Keepalive (Sec) field	Enter the number of seconds that the device waits between sending IKE keepalive packets
Retry (Sec) field	Enter the number of seconds that the device waits between attempts to establish an IKE connection with the remote peer.

Field	Description
IPsec settings pane	
Authenticate and generate new key after every (HH:MM:SS) field	Enter the value, in hours, minutes, and seconds, to determine how long the SA between devices will exist before it expires. Note You can also apply this value per crypto map. See Configuring Crypto Maps, page 5-3 for more information.
Generate new key after the current key encrypts a volume of field	Enter the value, in kilobytes, to determine how long the SA between all devices will exist before it expires. When the data that flows through the IPsec tunnel reaches this value, the SA expires, and the IPsec tunnel between the devices disappears. The range of values you can use is 2560 to 536870912. Note You can also apply this value per crypto map. See Configuring Crypto Maps, page 5-3 for more information.
Set idle time of field	Enter the time, in seconds, that the idle timer will allow an inactive peer to maintain the SA. The range of values you can use is 2560 to 536870912.

- Step 4** Click **Deliver** at the top of the window. For more information on delivering accumulated CLI commands, see [Delivering CLI Commands to the Device, page 1-22](#).

