Site-to-Site VPN User Interface Reference

The pages that you access by selecting **Site-To-Site VPN Manager** from the **Tools** menu, or clicking the **Site-To-Site VPN Manager** button on the toolbar, help you configure site-to-site VPNs.

Note You can also configure site-to-site VPNs in Device view (**View** > **Device View)** and Policy view (**View** > **Policy View)**. For more information, see:

- Managing VPN Devices in Device View, page 9-53
- Managing Shared Site-to-Site VPN Policies in Policy View, page 9-56

These topics describe the pages that help you create VPN topologies, and the policies that will be assigned to them:

- Site-to-Site VPN Manager Window, page B-2
- Create VPN Wizard, page B-8
- Site to Site VPN Policies, page B-37
- VPN Topologies Device View Page, page B-85

Site-to-Site VPN Manager Window

Use the Site-to-Site VPN Manager window to:

- View all available VPN topologies.
- Create, edit, and delete VPN topologies.
- View detailed information about each VPN topology.
- View the endpoints defined for a VPN topology.
- View and edit the policies assigned to a VPN topology.

The VPNs selector, in the upper left pane of the window, lists all available VPN topologies, and enables you to select topologies for viewing or editing. The lower left pane of the page lists the policies that are assigned to the VPN topology selected in the upper pane.

Navigation Path

Click the **Site-To-Site VPN Manager** button on the toolbar or select **Tools** > **Site-To-Site VPN Manager**.

Related Topics

- Create VPN Wizard, page B-8
- Understanding VPN Topologies, page 9-2
- Working with VPN Topologies, page 9-10

Field Reference

Table B-1 Site-to-Site VPN Manager Window

Element	Description
VPNs selector	Lists each VPN topology, represented by its name and an icon indicating its VPN type (hub and spoke, point to point, or full mesh).
Create VPN Topology button	Click to create a VPN topology, then select the type of topology you want to create from the options that are displayed. The Create VPN wizard opens.

Table B-1 Site-to-Site VPN Manager Window (continued)

Element	Description
Edit VPN Topology button	Opens the Edit VPN dialog box for editing a selected VPN topology. **Note** You can also edit a VPN topology by right-clicking it in the VPNs selector, and selecting the **Edit** option.
Delete VPN Topology button	Deletes a selected VPN topology. **Note** You can also delete a selected VPN topology by right-clicking it and selecting the **Delete** option. A confirmation dialog box opens asking you to confirm the deletion.
Policies selector	Lists each individually named policy that is already assigned to, or can be configured on, devices in the selected VPN topology. **Note** **VPN Summary** and **Peers**, are not policies. For a description of these pages, see VPN Summary Page, page B-3 and Peers Page, page B-7. Select a policy to open a page on which you can view or edit the parameters for the selected policy. See Site to Site VPN Policies, page B-37.
Close button	Closes the window.
Help button	Opens help for this window.

VPN Summary Page

Use the VPN Summary page to view information about a selected VPN topology. This includes information about the type of VPN topology, its devices, the assigned technology, and specific policies that are configured in it.

Navigation Path

Open the Site-to-Site VPN Manager Window, page B-2, select a topology in the VPNs selector, then select **VPN Summary** in the Policies selector.

Note

- The VPN Summary page opens when you finish creating or editing a VPN topology.
- The VPN Summary page also opens from Device view, when editing the VPN policies defined for a VPN topology. For more information, see Managing VPN Devices in Device View, page 9-53.
- You can also open the VPN Summary page from Policy view. For more information, see Working with Site-to-Site VPN Policies in Policy View, page 9-56.

Related Topics

- Site-to-Site VPN Manager Window, page B-2
- Configuring High Availability in Your VPN Topology, page 9-51
- Configuring VRF-Aware IPSec Settings, page 9-45
- Configuring an IKE Proposal, page 9-62
- Configuring IPSec Proposals, page 9-67
- Configuring Preshared Key Policies, page 9-76
- Configuring Public Key Infrastructure Policies, page 9-84
- Configuring GRE or GRE Dynamic IP Policies, page 9-91
- Configuring DMVPN Policies, page 9-96

Field Reference

Table B-2 VPN Summary Page

Element	Description
Type	The VPN topology type—Hub-and-Spoke, Point-to-Point, or Full Mesh.
Description	A description of the VPN topology.

Table B-2 VPN Summary Page (continued)

Element	Description
Primary Hub	Available if the VPN topology type is hub-and-spoke. The name of the primary hub in the hub-and-spoke topology.
Failover Hubs	Available if the VPN topology type is hub-and-spoke. The name of any secondary backup hubs that are configured in the hub-and-spoke topology.
Number of Spokes	Available if the VPN topology type is hub-and-spoke. The number of spokes that are included in the hub-and-spoke topology.
Peer 1	Available if the VPN topology type is point-to-point. The name of the device that is defined as Peer One in the point-to-point VPN topology.
Peer 2	Available if the VPN topology type is point-to-point. The name of the device that is defined as Peer Two in the point-to-point VPN topology.
Number of Peers	Available if the VPN topology type is full mesh. The number of devices included in the full mesh VPN topology.
IPSec Technology	The IPSec technology assigned to the VPN topology. See Understanding IPSec Technologies and Policies, page 9-8.
IKE Proposal	The security parameters of the IKE proposal configured in the VPN topology. See IKE Proposal Page, page B-37.
Transform Sets	The transform sets that specify the authentication and encryption algorithms that will be used to secure the traffic in the VPN tunnel. See IPSec Proposal Page, page B-39.
Preshared Key	Unavailable if the selected technology is Easy VPN. Specifies whether the shared key to use in the preshared key policy is user defined or auto-generated. See Preshared Key Page, page B-53.
Public Key Infrastructure	If a Public Key Infrastructure policy is configured in the VPN topology, specifies the CA server. See Public Key Infrastructure Page, page B-57.

Table B-2 VPN Summary Page (continued)

Element	Description
Routing Protocol	Available only if the selected technology is GRE, GRE Dynamic IP, or DMVPN. The routing protocol and autonomous system (or process ID) number used in the secured IGP for configuring a GRE, GRE Dynamic IP, or DMVPN routing policy. **Note** Security Manager adds a routing protocol to all the devices in the secured IGP on deployment. If you want to maintain this secured IGP, you must create a router platform policy using this routing protocol and autonomous system (or process ID) number. See GRE Modes Page, page B-59.
Tunnel Subnet IP	Available only if the selected technology is GRE, GRE Dynamic IP, or DMVPN. If a tunnel subnet is defined, displays the inside tunnel interface IP address, including the unique subnet mask. See GRE Modes Page, page B-59.
High Availability	Available if the VPN topology type is hub-and-spoke. If a High Availability policy is configured on a device in your hub-and-spoke VPN topology, displays the details of the policy. See High Availability Page, page B-34.
VRF-Aware IPSec	Available if the VPN topology type is hub-and-spoke. If a VRF-Aware IPSec policy is configured on a hub in your hub-and-spoke VPN topology, displays the type of VRF solution (1-Box or 2-Box) and the name of the VRF policy. See VRF Aware IPSec Tab, page B-28.
Close button	Closes the page.
Help button	Opens help for this page.

Peers Page

Use the Peers page to view the endpoints defined for a VPN topology, including the internal and external VPN interfaces and protected networks assigned to the devices in the topology. The interface roles, or interfaces that match each interface role, may also be displayed for the VPN interfaces and protected networks.

The Peers page contains a scrollable table displaying the device roles, VPN interfaces and protected networks for all selected devices. By clicking the arrow displayed alongside any table heading, you can switch the order of the list to display from ascending to descending order, and vice versa. You can also filter the table contents using the filter controls above it to display only rows that match the criteria that you specify (see Filtering Tables, page 3-19).

Navigation Path

Open the Site-to-Site VPN Manager Window, page B-2, select a topology in the VPNs selector, then select **Peers** in the Policies selector.

Note You can also open the Peers page from Device view. For more information, see Managing VPN Devices in Device View, page 9-53.

Related Topics

- Site-to-Site VPN Manager Window, page B-2
- VPN Topologies Device View Page, page B-85

Field Reference

Table B-3 Peers Page

Element	Description
Role	The role of the device—hub (primary or failover), spoke, or peer.
Device	The name of the device.
VPN Interface	The VPN interface (external and internal) that is defined for the selected device.
Protected Networks	The protected networks that are defined for the selected device.

Table B-3 Peers Page (continued)

Element	Description
Show	Select to display either the interface roles or matching interfaces, for the VPN interfaces and protected networks in the table, as follows: • **Interface Roles Only** (default)—To display only the interface roles assigned to the VPN interfaces and protected networks. • **Matching Interfaces**—To display the interfaces that match the pattern of each interface role. If there are no matching interfaces "No Match" will be displayed.
Create button	Opens the Device Selection tab of the Edit VPN dialog box on which you can change the selection of devices in your VPN topology. See Device Selection Page, page B-10.
Edit button	Opens the Endpoints tab of the Edit VPN dialog box on which you can edit the VPN interfaces and protected networks for a selected device in the table. See Endpoints Page, page B-13.

Create VPN Wizard

Security Manager supports three basic types of topologies with which you can create a site-to-site VPN. Use the Create VPN wizard to create a hub-and-spoke, point-to-point, or full mesh VPN topology across multiple device types. For more information, see Understanding VPN Topologies, page 9-2.

Note You can deploy to your devices immediately after creating a VPN topology, using the default policy configurations provided by Security Manager. All you need to do is complete the steps of the Create VPN wizard.

Editing a VPN topology is done using the Edit VPN dialog box, which comprises tabs whose elements are identical (except for the buttons) to the pages of the Create VPN wizard. You can click a tab to go directly to the page that contains the fields you want to edit, without having to go through each step of the wizard. Clicking **OK** on any tab in the dialog box saves your definitions on all the tabs. For more information, see Editing a VPN Topology, page 9-24.

The following pages describe the steps in the Create VPN wizard:

- Name and Technology Page, page B-9
- Device Selection Page, page B-10
- Endpoints Page, page B-13
- High Availability Page, page B-34

Navigation Path

1. In the Site-to-Site VPN Manager Window, page B-2, click the **Create VPN Topology** button above the VPNs selector.
2. Select the type of VPN topology you want to create from the options that are displayed—Hub and Spoke, Point to Point, or Full Mesh.

Related Topics

- Understanding VPN Topologies, page 9-2
- Understanding IPSec Technologies and Policies, page 9-8
- Creating a VPN Topology, page 9-11

Name and Technology Page

Use the Name and Technology page of the Create VPN wizard to provide a name and description for the VPN topology, and select the IPSec technology that will be assigned to it.

Note When editing a VPN topology, the Name and Technology tab is used. The elements of the tab (except for the buttons) are identical to those that appear on the Name and Technology page. For more information, see Editing a VPN Topology, page 9-24.

Navigation Path

- When creating a VPN topology, open the Create VPN Wizard, page B-8.
- When editing a VPN topology, open the Site-to-Site VPN Manager Window, page B-2, then right-click a VPN topology in the VPNs selector, or click the Name and Technology tab in the Edit VPN dialog box.

Related Topics

- Create VPN Wizard, page B-8
- Editing a VPN Topology, page 9-24
- Understanding IPSec Technologies and Policies, page 9-8
- Defining a Name and IPSec Technology, page 9-12

Field Reference

Table B-4 Create VPN wizard > Name and Technology Page

Element	Description
Name	A unique name you want to specify for the VPN topology, for identification purposes.
Description	Any descriptive text or comments that you want to add about the VPN topology.
IPSec Technology	Select the IPSec technology that you want to assign to the VPN topology from the drop-down list. **Note** If you are editing an existing VPN, the assigned IPSec technology is displayed, but unavailable for editing. To edit the technology, you must delete the VPN topology and create a new one.
Next button	Advances to the next wizard page. See Device Selection Page, page B-10.
Cancel button	Closes the wizard without saving your changes.
Help button	Opens help for this page.

Device Selection Page

Use the Device Selection page of the Create VPN wizard to select the devices that will be included in the VPN topology.

Note When editing the device selection for a VPN topology, the Device Selection tab is used. The elements of the tab (except for the buttons) are identical to those that appear on the Device Selection page. For more information, see Editing a VPN Topology, page 9-24.

The contents of this page differ depending on the VPN topology type. For example, if you are creating or editing a hub-and-spoke topology, you also need to specify the devices as hubs or spokes.

Note The devices that are available for selection include only those that can be used for the selected VPN topology type, that support the IPSec technology type, and which you are authorized to view. For more information, see About Selecting Devices in a VPN Topology, page 9-14.

You can include devices in your VPN topology that are not managed by Security Manager. You cannot upload or download any configurations to these devices nor deploy to them. For more information, see Adding Unmanaged Devices to Your VPN Topology, page 9-14.

Navigation Path

- When creating a VPN topology, open the Create VPN Wizard, page B-8, then click **Next** on the Name and Technology page.
- When editing a VPN topology, click the **Device Selection** tab in the Edit VPN dialog box.
- In the VPN Topologies Device View Page, page B-85, click the **Edit VPN Topology** button.

Related Topics

- Create VPN Wizard, page B-8
- Editing a VPN Topology, page 9-24
- About Selecting Devices in a VPN Topology, page 9-14
- Selecting Devices for Your VPN Topology, page 9-15
- Removing Devices from a VPN Topology, page 9-23

Field Reference

Table B-5 Create VPN wizard > Device Selection Page

Element	Description
Available Devices	Lists all devices that can be included in your selected VPN topology, that support the IPSec technology type, and which you are authorized to view. **Note** Clicking a device group selects all its devices.
Hubs	The devices you selected to be hubs in your hub-and-spoke topology. In an Easy VPN topology, the selected devices are servers. **Note** If multiple devices are selected, you must make sure that the required primary hub device appears first in the list. You can use the **Up** and **Down** buttons to change the order of the Hubs in the list. To remove devices from the list, select them and click <<.
Spokes	The devices you selected to be spokes in your hub-and-spoke topology. In an Easy VPN topology, the selected devices are clients. To remove devices from the list, select them and click <<.
Peer One/Peer Two	The devices you selected to be peers in your point-to-point topology. To remove the selected device from the Peer One/Peer Two field, click <<.
Selected Devices	The devices you selected to be included in your full mesh topology. To remove selected devices from the Selected Devices list, click <<.
Back button	Returns to the previous wizard page. See Name and Technology Page, page B-9.
Next button	Advances to the next wizard page. See Endpoints Page, page B-13.
Cancel button	Closes the wizard without saving your changes.
Help	Opens help for this page.

Endpoints Page

Use the Endpoints page of the Create VPN wizard to view the devices in your VPN topology, and define or edit their external or internal interfaces and protected networks.

Note When editing a VPN topology, the Endpoints tab is used. The elements of the tab (except for the buttons) are identical to those that appear on the Endpoints page. For more information, see Editing a VPN Topology, page 9-24.

The Endpoints page displays a scrollable table listing the VPN interfaces and protected networks for all selected devices. By clicking on the arrow displayed alongside any table heading, you can switch the order of the list to display from ascending to descending order, and vice versa. You can also filter the table contents using the filter controls above it to display only rows that match the criteria that you specify (see Filtering Tables, page 3-19).

Navigation Path

- When creating a VPN topology, open the Create VPN Wizard, page B-8, then click **Next** on the Device Selection page.
- When editing a VPN topology, click the **Endpoints** tab in the Edit VPN dialog box.

Related Topics

- Create VPN Wizard, page B-8
- Editing a VPN Topology, page 9-24
- Edit Endpoints Dialog Box, page B-16
- About Defining and Editing the Endpoints and Protected Networks, page 9-16
- Defining the Endpoints and Protected Networks, page 9-18

Field Reference

Table B-6 Create VPN wizard > Endpoints Page

Element	Description
Role	The role of the device—hub, spoke, or peer.
Device	The name of the device.
VPN Interface	The primary or backup VPN interface that is currently defined for the selected device. Depending on the selection in the **Show** list, the interface roles, or the interfaces that match each interface role, for the VPN interface may also be displayed. Select a row and click **Edit** to change the device's VPN interfaces. The Edit Endpoints dialog box opens, from which you can select the required VPN interface. See VPN Interface Tab, page B-17. **Note** You can select more than one device at a time for editing. The changes you make in the VPN Interface tab will be applied to all the selected devices. **Note** When selecting multiple devices for editing the VPN interfaces, you cannot include Catalyst 6500/7600 devices in your selection. If you want to edit these devices, you must select them separately. **Note** To edit the VPN interface for a Catalyst 6500/7600 device, see VPN Interface Tab, page B-17.

Table B-6 Create VPN wizard > Endpoints Page (continued)

Element	Description
Protected Networks	The protected networks that are defined for the selected device. Depending on the selection in the **Show** list, the interface roles, or the interfaces that match each interface role, for the protected networks may also be displayed. Select a row and click **Edit** to change the device's protected networks. The Edit Endpoints dialog box opens, from which you can select the required protected networks. See Protected Networks Tab, page B-24. **Note** You can select more than one device at a time for editing. The changes you make in the Protected Networks tab will be applied to all the selected devices. **Note** When selecting multiple devices for editing the protected networks, you cannot include Catalyst VPN Service Module devices in your selection. If you want to edit these devices, you must select them separately.
Show	Select to display either the interface roles or matching interfaces, for the VPN interfaces and protected networks in the table, as follows: • **Interface Roles Only** (default)—To display only the interface roles assigned to the VPN interfaces and protected networks. • **Matching Interfaces**—To display the interfaces that match the pattern of each interface role. If there are no matching interfaces "No Match" will be displayed.
Edit button	Enables you to edit the VPN interface and/or protected networks for a selected device in the table. The Edit Endpoints dialog box opens. See Edit Endpoints Dialog Box, page B-16.
Back button	Returns to the previous wizard page. See Device Selection Page, page B-10.
Next button	Available only if you are creating or editing a hub-and-spoke VPN topology. Advances to the next wizard page. See High Availability Page, page B-34.

Table B-6 Create VPN wizard > Endpoints Page (continued)

Element	Description
Finish button	Saves your wizard definitions and closes the wizard. The new or edited VPN topology appears in the VPNs selector in the Site-to-Site VPN window, with the VPN Summary page displayed. See VPN Summary Page, page B-3.
Cancel button	Closes the wizard without saving your changes.
Help	Opens help for this page.

Edit Endpoints Dialog Box

Use the Edit Endpoints dialog box to:

- Edit the VPN interfaces and protected networks defined for devices.
- Configure a dial backup interface to use as a fallback link for a primary VPN interface.
- Define VPN Services Module (VPNSM) settings for a Catalyst 6500/7600 device.
- Define VPN SPA settings for a Catalyst 6500/7600 device.
- Configure FWSM on a Catalyst 6500/7600 device.
- Configure a VRF-Aware-IPSec policy on a hub device.

The following tabs may be available on the Edit Endpoints dialog box:

- VPN Interface Tab, page B-17
- Protected Networks Tab, page B-24
- FWSM Tab, page B-26
- VRF Aware IPSec Tab, page B-28

Note

- You can select more than one device at a time for editing. The changes you make on any tabs in the dialog box will be applied to all selected devices.
- When selecting multiple devices for editing the VPN interfaces, you cannot include Catalyst 6500/7600 devices in your selection. If you want to edit these devices, you must select them separately.

- Clicking **OK** on any tab in the dialog box saves your definitions on all the tabs.

Navigation Path

You can access the Edit Endpoints dialog box from the Endpoints Page, page B-13 (or tab). Then select a device in the Endpoints table, and click **Edit**.

Related Topics

- Endpoints Page, page B-13
- Defining the Endpoints and Protected Networks, page 9-18
- Configuring Dial Backup, page 9-28
- Configuring a Catalyst VPN Services Module (VPNSM) VPN Interface, page 9-30
- Configuring a Catalyst VPN Shared Port Adapter (VPN SPA) Blade, page 9-32
- Configuring a Firewall Services Module (FWSM) Interface with VPNSM or VPN SPA, page 9-38
- Configuring VRF-Aware IPSec Settings, page 9-45

VPN Interface Tab

Note If you selected a Catalyst 6500/7600 device in the Endpoints table for editing, the VPN Interface tab provides settings that enable you to configure a VPN Services Module (VPNSM) or a VPN SPA blade on the device. For more information, see Defining VPN Services Module (VPNSM) or VPN SPA Settings, page B-21. For a description of the elements that appear on the VPN Interface tab for a Catalyst 6500/7600 device, see Table B-8 on page B-22.

Use the VPN Interface tab in the Edit Endpoints dialog box to edit the VPN interfaces defined for devices in the Endpoints table. When defining a primary VPN interface for a router device, you can also configure a backup interface to use as a fallback link for the primary route VPN interface, if its connection link becomes unavailable. You can only configure a backup interface on a Cisco IOS security router, which is a spoke in the VPN topology. For more information, see Understanding Dial Backup, page 9-27.

Navigation Path

The VPN Interface tab is displayed when you open the Edit Endpoints Dialog Box, page B-16. You can also open it by clicking the VPN Interface tab from any other tab in the Edit Endpoints dialog box.

Related Topics

- Edit Endpoints Dialog Box, page B-16
- Defining the Endpoints and Protected Networks, page 9-18
- Configuring Dial Backup, page 9-28
- Procedure for Configuring a VPNSM or VPN SPA Blade, page 9-34

Field Reference

Table B-7 describes the elements on the VPN Interface tab when a device other than a Catalyst 6500/7600 is selected.

Table B-7 Edit Endpoints Dialog Box > VPN Interface Tab

Element	Description
Enable the VPN Interface Changes on All Selected Peers	Available if you selected more than one device for editing in the Endpoints page. When selected, applies any changes you make in the VPN interface tab to all the selected devices.
VPN Interface	The VPN interface defined for the selected device. VPN interfaces are predefined interface role objects. If required, click **Select** to open a dialog box that lists all available interfaces, and sets of interfaces defined by interface roles, in which you can make your selection, or create interface role objects. For more information, see Interface Roles Page, page C-126.

Table B-7 Edit Endpoints Dialog Box > VPN Interface Tab (continued)

Element	Description
Connection Type	**Note** This element is only available in a hub-and-spoke VPN topology, if the hub is an ASA or PIX 7.0 device and the selected technology is regular IPSec. To configure the ASA hub during an SA negotiation, select one of the following connection types: • **Answer Only**—To configure the hub to only respond to an SA negotiation, but not initiate it. • **Originate Only**—To configure the hub to only initiate an SA negotiation, but not respond to one. • **Bidirectional**—To configure the hub to both initiate and respond to an SA negotiation.
Peer IP Address	To define the IP address of the VPN interface of the peer device, click one of the following radio buttons: • **VPN Interface IP Address**—To use the configured IP address on the selected VPN interface. Only one VPN interface can match the interface role. • **IP Address for IPSec Termination**—To enter manually the IP address of the peer device. Enter the IP address in the field provided. Only one VPN interface can match the interface role. • **IP Address of Another Existing Interface to be Used as Local Address** (unavailable if IPSec technology is DMVPN)—To use the configured IP address on any interface as a local address, not necessarily a VPN interface. Enter the interface in the field provided. You can choose the required interface by clicking **Select**. A dialog box opens that lists all available predefined interface roles, and in which you can create an interface role object. For more information, see Interface Roles Page, page C-126.

Table B-7 Edit Endpoints Dialog Box > VPN Interface Tab (continued)

Element	Description
Tunnel Source	Available for a hub when the selected technology is GRE or DMVPN. To define the tunnel source address to be used by the GRE or DMVPN tunnel on the spoke side, click one of the following radio buttons: • **VPN Interface**—To use the selected VPN interface as the tunnel source address. • **Another Existing Interface**—To use any interface as the tunnel source address, not necessarily a VPN interface. Enter the interface in the field provided. You can choose the required interface by clicking **Select**. A dialog box opens that lists all available predefined interface roles, and in which you can create an interface role object. For more information, see Interface Roles Page, page C-126.
Dial Backup Settings	
Enable	Available only if the selected device is a Cisco IOS router which is a spoke in the VPN topology. When selected, enables you to configure a backup interface to use as a fallback link for the primary route VPN interface, if its connection link becomes unavailable. **Note** Before configuring a backup interface, you must first configure the dialer interface settings on the device. For more information, see Configuring Dialer Interfaces on Cisco IOS Routers, page 12-29.
Dialer Interface	Select the logical interface through which the secondary route traffic will be directed when the dialer interface is activated. This can be a Serial, Async, or BRI interface. The list displays all the interfaces of these types on the devices.

Table B-7 Edit Endpoints Dialog Box > VPN Interface Tab (continued)

Element	Description
Tracking IP Address	The IP address of the destination device to which connectivity must be maintained from the primary VPN interface connection. This is the device that is pinged by the Service Assurance agent through the primary route to track connectivity. The backup connection will be triggered if connectivity to this device is lost. **Note** If you do not specify an IP address, the primary hub VPN interface will be used in a hub-and-spoke VPN topology. In a point-to-point or full mesh VPN topology, the peer VPN interface will be used.
Primary Next Hop IP Address	Available only if the selected technology is IPSec, GRE, or GRE Dynamic IP. Enter the IP address to which the primary interface will connect when it is active. This is known as the next hop IP address. If you do not enter the next hop IP address, Security Manager will configure a static route using the interface name.
Advanced button	Available only if the selected technology is IPSec, GRE, or GRE Dynamic IP. Opens the Dial Backup Settings dialog box for configuring additional (optional) settings. See Dial Backup Settings Dialog Box, page B-32.
OK button	Saves your changes locally on the client and closes the dialog box. The changes appear in the Endpoints table for the selected device(s).
Cancel button	Closes the dialog box without saving your changes.
Help button	Opens help for this tab.

Defining VPN Services Module (VPNSM) or VPN SPA Settings

When you select a Catalyst 6500/7600 device in the Endpoints table for editing, the VPN Interface tab of the Edit Endpoints dialog box provides settings for configuring a VPN Services Module (VPNSM) or VPN SPA on the device. You can select more than one Catalyst 6500/7600 device at the same time. Your changes are applied to all the selected devices.

Note

- Before you define the VPNSM or VPN SPA settings, you must import your Catalyst 6500/7600 device to the Security Manager inventory and discover its interfaces. For more information, see Procedure for Configuring a VPNSM or VPN SPA Blade, page 9-34.
- If you are configuring a VPNSM or VPN SPA with VRF-Aware IPSec on a device, verify that the device does not belong to a different VPN topology in which VRF-Aware IPSec is *not* configured. Similarly, if you are configuring a VPNSM or VPN SPA without VRF-Aware IPSec, make sure that the device belongs to a different VPN topology in which VRF-Aware IPSec *is* configured.

Field Reference

Table B-8 describes the elements that appear on the VPN Interface tab of the Edit Endpoints dialog box, after you select a Catalyst 6500/7600 device.

Table B-8 Edit Endpoints Dialog Box > VPN Interface Tab > VPNSM/VPN SPA Settings

Element	Description
Enable the VPN Interface Changes on All Selected Peers	Available if you selected more than one Catalyst 6500/7600 device for editing in the Endpoints page. When selected, applies any changes you make in the VPN interface tab to all the selected devices.
VPNSM/VPN SPA Settings	
VPN Interface	The inside VLAN that serves as the inside interface to the VPN Services Module or VPN SPA. It is also the hub endpoint of the VPN tunnel (unless VRF-Aware IPSec is configured on the device). If required, click **Select** to open a dialog box that lists all available interfaces, and sets of interfaces defined by interface roles, in which you can make your selection, or create interface role objects. For more information, see Interface Roles Page, page C-126.

Table B-8 Edit Endpoints Dialog Box > VPN Interface Tab > VPNSM/VPN SPA Settings

Element	Description
Slot	From the list of available slots, select the VPNSM blade slot number to which the inside VLAN interface is connected, or the number of the slot in which the VPN SPA blade is inserted. For more information, see Adding VPN SPA Slot Locations, page 5-44.
Subslot	The number of the subslot (0 or 1) on which the VPN SPA blade is actually installed. **Note** If you are configuring a VPNSM, select the blank option.
External Port	The external port or VLAN that connects to the inside VLAN. **Note** If VRF-Aware IPSec is configured on the device, the external port or VLAN must have an IP address. If VRF-Aware IPSec is not configured, the external port or VLAN must *not* have an IP address. Click **Select** to open a dialog box that lists all available interfaces, and sets of interfaces defined by interface roles, in which you can make your selection, or create interface role objects. For more information, see Interface Roles Page, page C-126. **Note** You must select an interface or interface role that differs from the one selected for the inside VLAN.
Enable Failover Blade	When selected, enables you to configure a failover VPNSM or VPN SPA blade for intra chassis high availability. **Note** A VPNSM blade and VPN SPA blade cannot be used on the same device as primary and failover blades.
Failover Slot	From the list of available slots, select the VPNSM blade slot number that will serve as the failover blade, or the number of the slot in which the failover VPN SPA blade is inserted.
Failover Subslot	Select the number of the subslot (0 or 1) on which the failover VPN SPA blade is actually installed. **Note** If you are configuring a VPNSM, select the blank option.

Table B-8 Edit Endpoints Dialog Box > VPN Interface Tab > VPNSM/VPN SPA Settings

Element	Description
Peer IP Address	To define the IP address of the VPN interface of the peer device, click one of the following radio buttons: • **VPN Interface IP Address**—To use the configured IP address on the selected VPN interface. • **IP Address for IPSec Termination**—To enter manually the IP address of the peer device. Enter the IP address in the field provided.
OK button	Saves your changes locally on the client and closes the dialog box. The changes appear in the Endpoints table for the selected device(s).
Cancel button	Closes the dialog box without saving your changes.
Help button	Opens help for this tab.

Protected Networks Tab

Use the Protected Networks tab on the Edit Endpoints dialog box to edit the protected networks that are defined on a selected device in the Endpoints table.

You can specify the protected networks as interface roles whose naming patterns match the internal VPN interface type of the device, as network objects containing one or more network or host IP addresses, interfaces, or other network objects, or as access control lists (if IPSec is the assigned technology).

For more information, see:

- Working with Interface Role Objects, page 8-120
- Working with Network/Host Objects, page 8-142
- Working with Access Control List Objects, page 8-32

Navigation Path

You can access the Protected Networks tab from the Edit Endpoints dialog box. Open the Edit Endpoints Dialog Box, page B-16, then click the **Protected Networks** tab.

Related Topics

- Edit Endpoints Dialog Box, page B-16
- Defining the Endpoints and Protected Networks, page 9-18

Field Reference

Table B-9 Edit Endpoints Dialog Box > Protected Networks Tab

Element	Description
Enable the Protected Networks Changes on All Selected Peers	Available if you selected more than one device for editing in the Endpoints page. When selected, applies any changes you make in the Protected Networks tab to all the selected devices.
Available Protected Networks	A hierarchy of all available protected networks, including the interface roles whose naming pattern may match the internal VPN interface type of the device. If IPSec is the assigned technology, access control lists (ACLs) are also included in the list of available protected networks. **Note** In a hub-and-spoke VPN topology in which IPSec is the assigned technology, when an ACL object is used to define the protected network on a spoke, Security Manager mirrors the spoke's ACL object on the hub to the matching crypto map entry. Select the interface role(s), protected networks, and/or access control lists that you want to define for the selected device, then click >>.
Selected Protected Networks	The protected networks and interface roles you selected for the device. **Note** You can reorder the selected protected networks/interface roles in the list by selecting them (one at a time), then clicking the Move Up or Move Down button, as required.
>> button	Moves protected networks from the available networks list to the selected networks list.
<< button	Removes protected networks from the selected list.

Table B-9 Edit Endpoints Dialog Box > Protected Networks Tab (continued)

Element	Description
Create button	If the required interface roles, protected networks, or access control lists do not appear in the Available Protected Networks list, click **Create** and select the required option to create an interface role, protected network, or access control list. **Note** The Access Control List option is only available if the assigned technology is IPSec. If you select the Interface Role option, the Interface Role Editor page opens in which you can create an interface role object. For more information, see Editing Interface Role Objects, page 8-124. If you select the Protected Network option, the Network Editor page opens in which you can create a network object. For more information, see Editing Network/Host Objects, page 8-146. If you select the Access Control List option, the Access Lists Editor page opens in which you can create an access control list object. For more information, see Editing Access Control List Objects, page 8-40.
OK button	Saves your changes locally on the client and closes the dialog box. The changes appear in the Endpoints table for the selected device(s).
Cancel button	Closes the dialog box without saving your changes.
Help button	Opens help for this tab.

FWSM Tab

Note The **FWSM** tab is only available in a hub-and-spoke VPN topology, when the selected hub is a Catalyst 6500/7600 device.

Use the FWSM tab on the Edit Endpoints dialog box to define the settings that enable you to connect between a Firewall Services Module (FWSM) and an IPSec VPN Services Module (VPNSM) or VPN SPA, that is already configured on a Catalyst 6500/7600 device.

Note Before defining the FWSM settings, you must import your Catalyst 6500/7600 device to the Security Manager inventory. Then open Cisco Catalyst Device Manager (Cisco CDM), and discover the FWSM configurations on the device, and assign a VLAN that will serve as the inside interface to the FWSM.

For more information, see:

- Configuring a Firewall Services Module (FWSM) Interface with VPNSM or VPN SPA, page 9-38
- Discovering Policies, page 6-5
- Creating a Single Layer 3 Ethernet VLAN, page 14-102

Navigation Path

You can access the FWSM tab from the Edit Endpoints dialog box. Open the Edit Endpoints Dialog Box, page B-16, then click the **FWSM** tab.

Note Make sure you selected a Catalyst 6500/7600 device in the table on the Endpoints Page, page B-13 (or tab), before opening the Edit Endpoints dialog box.

Related Topics

- Configuring a Firewall Services Module (FWSM) Interface with VPNSM or VPN SPA, page 9-38
- Defining VPN Services Module (VPNSM) or VPN SPA Settings, page B-21
- Edit Endpoints Dialog Box, page B-16

Field Reference

Table B-10 Edit Endpoints Dialog Box > FWSM Tab

Element	Description
Enable FWSM Settings	When selected, enables you to configure the connection between the Firewall Services Module (FWSM) and the VPN Services Module (VPNSM) or VPN SPA on the selected Catalyst 6500/7600 device.

Table B-10 Edit Endpoints Dialog Box > FWSM Tab (continued)

Element	Description
FWSM Inside VLAN	The VLAN which serves as the inside interface to the Firewall Services Module (FWSM). If required, click **Select** to open a dialog box that lists all available interfaces, and sets of interfaces defined by interface roles, and in which you can make your selection, or create interface role objects. For more information, see Interface Roles Page, page C-126.
FWSM Blade	From the list of available blades, select the blade number to which the selected FWSM inside VLAN interface is connected.
Security Context	If the selected FWSM inside VLAN is part of a security context, specify its name in this field. The name is case-sensitive. You can partition an FWSM into multiple virtual firewalls, known as security contexts. A security context is an independent virtual firewall that has its own security policy, interfaces, and administrators. You can define security contexts when you import a Catalyst 6500/7600 device into the Security Manager inventory. For more information, see Security Contexts Page, page C-475.
OK button	Saves your changes locally on the client and closes the dialog box.
Cancel button	Closes the dialog box without saving your changes.
Help button	Opens help for this tab.

VRF Aware IPSec Tab

Use the VRF-Aware IPSec tab on the Edit Endpoints dialog box to configure a VRF-Aware IPSec policy on a hub in your hub-and-spoke VPN topology. When you select the row in the Endpoints table that contains the required hub device (the IPSec Aggregator), and click **Edit**, the VRF Aware IPSec tab opens. You can configure VRF-Aware IPSec as a one-box or two-box solution.

Note

- In a VPN topology with two hubs, you must configure VRF-Aware IPSec on both devices.
- You cannot configure VRF-Aware IPSec on a device that belongs to another VPN topology in which VRF-Aware IPSec is *not* configured.

- Deployment may fail if the IPSec Aggregator is configured with the same keyring CLI command as the existing preshared key (keyring) command, and is not referenced by any other command. In this case, Security Manager does not use the VRF keyring CLI, but generates the keyring with a different name, causing deployment to fail. You must manually remove the preshared key keyring command through the CLI, before you can deploy the configuration.

For more information about creating or editing a VRF-Aware IPSec policy, see Understanding VRF-Aware IPSec, page 9-41.

Navigation Path

You can access the VRF-Aware IPSec tab from the Edit Endpoints dialog box. Open the Edit Endpoints Dialog Box, page B-16, then click the **VRF-Aware IPSec** tab.

Note Make sure you selected a hub device in the table on the Endpoints Page, page B-13 (or tab), before opening the Edit Endpoints dialog box.

Related Topics

- Edit Endpoints Dialog Box, page B-16
- Configuring VRF-Aware IPSec Settings, page 9-45
- Defining the Endpoints and Protected Networks, page 9-18

Field Reference

Table B-11 Edit Endpoints Dialog Box > VRF Aware IPSec Tab

Element	Description
Enable the VRF Settings Changes on All Selected Peers	Available if you selected more than one device for editing in the Endpoints page. When selected, applies any changes you make in the VRF Settings tab to all the selected devices.

Table B-11 Edit Endpoints Dialog Box > VRF Aware IPSec Tab (continued)

Element	Description
Enable VRF Settings	When selected, enables the configuration of VRF settings on the selected hub for the selected hub-and-spoke topology. **Note** To remove VRF settings that were defined for the VPN topology, deselect this check box.
1-Box (IPSec Aggregator + MPLS PE)	When selected, enables you to configure a one-box VRF solution. In the one-box solution, one device serves as the Provider Edge (PE) router that does the MPLS tagging of the packets in addition to IPSec encryption and decryption from the Customer Edge (CE) devices. For more information, see VRF-Aware IPSec One-Box Solution, page 9-42.
2-Box (IPSec Aggregator Only)	When selected, enables you to configure a two-box VRF solution. In the two-box solution, the PE device does just the MPLS tagging, while the IPSec Aggregator device does the IPSec encryption and decryption from the CEs. For more information, see VRF-Aware IPSec Two-Box Solution, page 9-43.
VRF Name	The name of the VRF routing table on the IPSec Aggregator. The VRF name is case-sensitive.
Route Distinguisher	The unique identifier of the VRF routing table on the IPSec Aggregator. This unique route distinguisher maintains the routing separation for each VPN across the MPLS core to the other PE routers. The identifier can be in either of the following formats: • *IP address*:*X* (where *X* is in the range 0-999999999). • *N*:*X* (where *N* is in the range 0-65535, and *X* is in the range 0-999999999). **Note** You cannot override the RD identifier after deploying the VRF configuration to your device. To modify the RD identifier after deployment, you must manually remove it using the device CLI, and then deploy again.

Table B-11 Edit Endpoints Dialog Box > VRF Aware IPSec Tab (continued)

Element	Description
Interface Towards Provider Edge	Available only when a 2-Box solution is selected. The VRF forwarding interface on the IPSec Aggregator towards the PE device. **Note** If the IPSec Aggregator (hub) is a Catalyst VPN service module, you must specify a VLAN. Interfaces and VLANs are predefined interface role objects. If required, you can click **Select** to open a dialog box that lists all available interfaces, and sets of interfaces defined by interface roles, in which you can make your selection, or create interface role objects. For more information, see Interface Roles Page, page C-126.
Routing Protocol	Available only when a 2-Box solution is selected. Select the routing protocol to be used between the IPSec Aggregator and the PE. If the routing protocol used for the secured IGP differs from the routing protocol between the IPSec Aggregator and the PE, select the routing protocol to use for redistributing the routing to the secured IGP. The options are BGP, EIGRP, OSPF, RIPv2, or Static route. For information about protocols, see Chapter 12, “Managing Routers”.
AS Number	Available only when a 2-Box solution is selected. Enter the number that will be used to identify the autonomous system (AS) area between the IPSec Aggregator and the PE. If the routing protocol used for the secured IGP differs from the routing protocol between the IPSec Aggregator and the PE, enter an AS number that will be used to identify the secured IGP into which the routing will be redistributed from the IPSec Aggregator and the PE. This is relevant only when GRE or DMVPN are applied. The AS number must be within the range 1-65535.

Table B-11 Edit Endpoints Dialog Box > VRF Aware IPSec Tab (continued)

Element	Description
Process Number	Available only if the 2-Box radio button is selected, and if the selected routing protocol is OSPF. The routing process ID number that will be used to identify the secured IGP. The range is 1-65535.
OSPF Area ID	Available only if the 2-Box radio button is selected, and if the selected routing protocol is OSPF. The ID number of the area in which the packet belongs. You can enter any number from 0-4294967295. **Note** All OSPF packets are associated with a single area, so all devices must have the same area ID number.
Next Hop IP Address	Available only when a 2-Box solution is selected with static routing. Specify the IP address of the interface that is connected to the IPSec Aggregator.
Redistribute Static Route	Available only when a 2-Box solution is selected with any routing protocol other than Static route. When selected, enables static routes to be advertised in the routing protocol configured on the IPSec Aggregator towards the PE device.
OK button	Saves your changes locally on the client and closes the dialog box. **Note** When you select the new or edited hub-and-spoke topology in the Site-to-Site VPN Manager window, an indication of VRF-Aware IPSec configuration appears in the VPN Summary page. See VPN Summary Page, page B-3.
Cancel button	Closes the dialog box without saving your changes.
Help button	Opens help for this tab.

Dial Backup Settings Dialog Box

Use the Dial Backup Settings dialog box to define optional settings for configuring a dial backup policy for your site-to-site VPN. These settings are available for IPSec, GRE, GRE Dynamic IP, or DMVPN technologies.

Mandatory settings for dial backup are configured in the VPN Interface tab on the Edit Endpoints dialog box. See VPN Interface Tab, page B-17.

Note You must configure the dialer interface settings before dial backup can work properly. For more information, see Configuring Dialer Interfaces on Cisco IOS Routers, page 12-29.

Navigation Path

Open the VPN Interface Tab, page B-17 from the Edit Endpoints dialog box, select the **Enable** check box in the **Backup** area, and click **Advanced**.

Note Make sure you selected the required router device in the table on the Endpoints Page, page B-13 (or tab), before opening the Edit Endpoints dialog box.

Related Topics

- Defining the Endpoints and Protected Networks, page 9-18
- Configuring Dial Backup, page 9-28
- VPN Interface Tab, page B-17

Field Reference

Table B-12 Dial Backup Settings Dialog Box

Element	Description
Next Hop Forwarding	
Backup Next Hop IP Address	If required, enter the next hop IP address of the ISDN BRI or analog modem backup interface (that is, the IP address to which the backup interface will connect when it is active). If you do not enter the next hop IP address, Security Manager will configure a static route using the interface name.
Tracking Object Settings	
Timeout	The number of milliseconds the Service Assurance Agent operation waits to receive a response from the destination device. The default is 5000 ms.

Table B-12 Dial Backup Settings Dialog Box (continued)

Element	Description
Frequency	How often Response Time Reporter (RTR) should be used to detect loss of performance on the primary route. The default is every 60 seconds.
Threshold	The rising threshold in milliseconds that generates a reaction event and stores history information for the RTR operation. The default is 5000 ms.
OK button	Saves your changes locally on the client and closes the dialog box.
Cancel button	Closes the dialog box without saving your changes.
Help button	Opens help for this dialog box.

High Availability Page

Use the High Availability page to define a group of hubs as an HA group.

Note When editing a VPN topology, the High Availability tab is used. The elements of the tab (except for the buttons) are identical to those that appear on the High Availability page. For more information, see Editing a VPN Topology, page 9-24.

High Availability may be configured only in a hub-and-spoke VPN topology when IPSec is the assigned technology. For more information about the prerequisites for configuring high availability, see Understanding High Availability, page 9-48.

Navigation Path

- When creating a hub-and-spoke VPN topology, open the Create VPN Wizard, page B-8, then click **Next** on the Endpoints page.
- When editing a hub-and-spoke VPN topology, click the **High Availability** tab in the Edit VPN dialog box.

Related Topics

- Endpoints Page, page B-13
- Configuring High Availability in Your VPN Topology, page 9-51
- Create VPN Wizard, page B-8

Field Reference

Table B-13 Create VPN wizard > High Availability Page

Element	Description
Enable	When selected, enables you to configure high availability on a group of hubs. **Note** When deselected, enables you to remove an HA group that was defined for the VPN topology.
Inside Virtual IP	The IP address that will be shared by the hubs in the HA group and will represent the inside interface of the HA group. The virtual IP address must be on the same subnet as the inside interfaces of the hubs in the HA group, but must not be identical to the IP address of any of these interfaces. **Note** If there is an existing standby group on the device, make sure that the IP address you provide is different from the virtual IP address already configured on the device.
Inside Mask	The subnet mask for the inside virtual IP address.
VPN Virtual IP	The IP address that will be shared by the hubs in the HA group and will represent the VPN interface of the HA group. This IP address will serve as the hub endpoint of the VPN tunnel. **Note** If there is an existing standby group on the device, make sure that the IP address you provide is different from the virtual IP address already configured on the device.
VPN Mask	The subnet mask for the VPN virtual IP address.
Hello Interval	The duration in seconds (within the range of 1-254) between each hello message sent by a hub to the other hubs in the group to indicate status and priority.

Table B-13 Create VPN wizard > High Availability Page (continued)

Element	Description
Hold Time	The duration in seconds (within the range of 2-255) that a standby hub will wait to receive a hello message from the active hub before concluding that the hub is down.
Standby Group Number (Inside)	The standby number of the inside hub interface that matches the internal virtual IP subnet for the hubs in the HA group. The number must be within the range of 0-255.
Standby Group Number (Outside)	The standby number of the outside hub interface that matches the external virtual IP subnet for the hubs in the HA group. The number must be within the range of 0-255. **Note** The outside standby group number must be different to the inside standby group number.
Stateful Failover	When selected, enables SSO for stateful failover. You can only configure stateful failover on an HA group that contains two hubs which are Cisco IOS routers. This check box is disabled if the HA group contains more than two hubs. **Note** When deselected, stateless failover is configured on the HA group. Stateless failover will also be configured if the HA group contains more than two hubs. Stateless failover may be configured on Cisco IOS routers or Catalyst 6500/7600 devices. For more information, see Enabling Stateful Failover, page 9-50.
OK button	Saves your changes locally on the client and closes the dialog box. **Note** When you select the new or edited hub-and-spoke topology in the Site-to-Site VPN Manager window, the VPN Summary page displays the details of the High Availability policy configured. See VPN Summary Page, page B-3.
Cancel button	Closes the dialog box without saving your changes.
Help button	Opens help for this tab.

Site to Site VPN Policies

You can access site-to-site VPN policies by selecting **Tools** > **Site-To-Site VPN Manager**, or clicking the **Site-To-Site VPN Manager** button on the toolbar, and then selecting the required policy in the Policies selector of the Site-to-Site VPN window.

You can also access site-to-site VPN policies from Device view or Policy view.

In Device view, you can see the VPN topology (topologies) to which each device in the Security Manager inventory belongs, and if necessary, change its assignment to or from a VPN topology. For more information, see VPN Topologies Device View Page, page B-85.

For more information about accessing site-to-site VPN policies from Policy view, see Managing Shared Site-to-Site VPN Policies in Policy View, page 9-56.

These topics describe the pages of the policies that you can assign to your VPN topologies:

- IKE Proposal Page, page B-37
- IPSec Proposal Page, page B-39
- VPN Global Settings Page, page B-44
- Preshared Key Page, page B-53
- Public Key Infrastructure Page, page B-57
- GRE Modes Page, page B-59
- Easy VPN IPSec Proposal Page, page B-69
- User Group Policy Page, page B-73
- Tunnel Group Policy (PIX 7.0/ASA) Page, page B-74
- Client Connection Characteristics Page, page B-83

IKE Proposal Page

Use the IKE Proposal page to select the IKE proposal that will be used to secure the IKE negotiation between two peers. An IKE proposal is a mandatory policy that is already configured in your VPN topology with predefined default values.

On the IKE Proposal page, you can view the parameters of the selected IKE proposal, select a different one from a list of predefined IKE proposals, or create a new one.

Navigation Path

Open the Site-to-Site VPN Manager Window, page B-2, select a topology in the VPNs selector, then select **IKE Proposal** in the Policies selector.

Note You can also open the IKE Proposal page from Policy view. See Managing Shared Site-to-Site VPN Policies in Policy View, page 9-56.

Related Topics

- Configuring an IKE Proposal, page 9-62
- Understanding Preshared Key Policies, page 9-74
- Preshared Key Page, page B-53
- VPN Topologies Device View Page, page B-85
- Managing Shared Site-to-Site VPN Policies in Policy View, page 9-56

Field Reference

Table B-14 IKE Proposal Page

Element	Description
Available IKE Proposals	Lists the predefined IKE proposals available for selection. Select the required IKE proposal in the list. The IKE proposal replaces the one in the **Selected IKE Proposal** field. IKE proposals are predefined objects. If the required IKE proposal is not included in the list, click **Add** to open the IKE Editor dialog box that enables you to create or edit an IKE proposal object. For more information, see IKE Proposal Dialog Box, page C-123.

Table B-14 IKE Proposal Page (continued)

Element	Description
Selected IKE Proposal	The selected IKE proposal with its predefined default values. For more information about security parameters, see Understanding IKE, page 9-58. **Note** You cannot edit the selected IKE proposal because it is a predefined object. You can only edit the properties of an IKE proposal object you create. To remove the IKE proposal from this field, select a different one.
Create button	Opens the IKE Editor dialog box for creating an IKE proposal object. For more information, see IKE Proposal Dialog Box, page C-123.
Edit button	Opens the IKE Editor dialog box for editing the selected IKE proposal. For more information, see IKE Proposal Dialog Box, page C-123.
Save button	Saves your changes to the server but keeps them private. **Note** To publish your changes, click the **Submit** button on the toolbar.
Close button	Closes the Site-to-Site VPN window.
Help button	Opens help for this page.

IPSec Proposal Page

Use the IPSec Proposal page to edit the IPSec policy definitions for your VPN topology.

For more information about IPSec Proposals, see Understanding IPSec Tunnel Policies, page 9-63.

Note When configuring IPSec policy definitions on an Easy VPN server, the IPSec Proposal page contains different elements. See Easy VPN IPSec Proposal Page, page B-69.

Navigation Path

Open the Site-to-Site VPN Manager Window, page B-2, select a topology in the VPNs selector, then select **IPSec Proposal** in the Policies selector.

Note You can also open the IPSec Proposal page from Policy view. See Managing Shared Site-to-Site VPN Policies in Policy View, page 9-56.

Related Topics

- Configuring IPSec Proposals, page 9-67

Field Reference

Table B-15 IPSec Proposal Page

Element	Description
Crypto Map Type	Click one of the following radio buttons to select the required crypto map option: • Static—To generate only static crypto maps. **Note** In a point-to-point or full mesh VPN topology, you can only use a static crypto map. • Dynamic—To generate only dynamic crypto maps. For more information, see About Crypto Maps, page 9-66.

Table B-15 IPSec Proposal Page (continued)

Element	Description
Transform Sets	The transform set(s) to use for your tunnel policy. Transform sets specify which authentication and encryption algorithms will be used to secure the traffic in the tunnel. **Note** Transform sets may use tunnel mode or transport mode of IPSec operation. When IPSec or Easy VPN is the assigned technology, you cannot use transport mode. A default transform set is displayed. If you want to use a different transform set, or select additional transform sets, click **Select** to open a dialog box that lists all available transform sets, and in which you can create transform set objects. For more information, see IPSec Transform Sets Page, page C-130. If more than one of your selected transform sets is supported by both peers, the transform set that provides the highest security will be used. **Note** You can select up to six transform sets. For more information, see About Transform Sets, page 9-64.
Enable Perfect Forward Secrecy	When selected, enables the use of Perfect Forward Secrecy (PFS) to generate and use a unique session key for each encrypted exchange. The unique session key protects the exchange from subsequent decryption, even if the entire exchange was recorded and the attacker has obtained the preshared and/or private keys used by the endpoint devices. **Note** To enable PFS, you must also select a Diffie-Hellman group for generating the PFS session key.

Table B-15 IPSec Proposal Page (continued)

Element	Description
Modulus Group	Available if Enable Perfect Forward Secrecy is selected. Select the required Diffie-Hellman key derivation algorithm from the Modulus Group list box. Security Manager supports Diffie-Hellman group 1, group 2, group 5, and group 7 key derivation algorithms. Each group has a different size modulus: Group 1: 768-bit modulus. Group 2: 1024-bit modulus. Group 5: 1536-bit modulus. Group 7: Use when the elliptical curve field size is 163 characters. For more information, see Deciding Which Diffie-Hellman Group to Use, page 9-60.
Lifetime (sec)	The number of seconds an SA will exist before expiring. The default is 3600 seconds (one hour). Lifetime refers to the global lifetime settings for the crypto IPSec security association (SA). The IPSec lifetime can be specified in seconds, in kilobytes, or both.
Lifetime (kbytes)	The volume of traffic (in kilobytes) that can pass between IPSec peers using a given SA before it expires. The default is 4,608,000 kilobytes.
Advanced (IOS)	
QoS Preclassify	Supported on Cisco IOS routers, except 7600 devices. Select this check box if you want to enable the classification of packets before tunneling and encryption occur. The Quality of Service (QoS) for VPNs feature enables Cisco IOS QoS services to operate with tunneling and encryption on an interface. The QoS features on the output interface classify packets and apply the appropriate QoS service before the data is encrypted and tunneled, enabling traffic flows to be adjusted in congested environments, and resulting in more effective packet tunneling.

Table B-15 IPSec Proposal Page (continued)

Element	Description
Enable Reverse Route	Supported on ASA devices, PIX 7.0 devices, and Cisco IOS routers except 7600 devices, and when the selected technology is IPSec. Select this check box if you want to enable the RRI feature in the IPSec crypto map. Then click one of the following radio buttons: • **Reverse Route**—To create a route in the routing table from the host address. • **Reverse Route Remote Peer** (Cisco IOS routers only)—To create a route in the routing table for the remote tunnel endpoint. Then enter the IP address of the remote peer in the field provided. When enabled in an IPSec crypto map, Reverse Route Injection (RRI) learns all the subnets from any network that is defined in the crypto access control list (ACL) as the destination network. The learned routes are installed into the local routing table as static routes that point to the encrypted interface. When the IPSec tunnel is removed, the associated static routes will be removed. These static routes may then be redistributed into other dynamic routing protocols, so that they can be advertised to other parts of the network (usually done by redistributing RRI routes into dynamic routing protocols on the core side). **Note** Security Manager automatically configures RRI on devices with High Availability (HA), or on the IPSec Aggregator when VRF-Aware IPSec is configured.
Save button	Saves your changes to the server but keeps them private. **Note** To publish your changes, click the **Submit** button on the toolbar.
Close button	Closes the Site-to-Site VPN window.
Help button	Opens help for this page.

VPN Global Settings Page

Use the VPN Global Settings page to define global settings for IKE, IPSec, NAT, and fragmentation, that apply to devices in your VPN topology.

The following tabs are available on the VPN Global Settings page:

- ISAKMP/IPSec Settings Tab, page B-44
- NAT Settings Tab, page B-48
- General Settings Tab, page B-50

Navigation Path

Open the Site-to-Site VPN Manager Window, page B-2, select a topology in the VPNs selector, then select **VPN Global Settings** in the Policies selector.

Note You can also open the VPN Global Settings page from Policy view. See Managing Shared Site-to-Site VPN Policies in Policy View, page 9-56.

ISAKMP/IPSec Settings Tab

Use the ISAKMP/IPSec Settings tab of the VPN Global Settings page to specify global settings for Internet Key Exchange (IKE) and IPSec.

Internet Key Exchange (IKE), also called Internet Security Association and Key Management Protocol (ISAKMP), is the negotiation protocol that lets two hosts agree on how to build an IPSec security association.

Navigation Path

The ISAKMP/IPSec Settings tab appears when you open the VPN Global Settings Page, page B-44. You can also open it by clicking the **ISAKMP/IPSec Settings** tab from any other tab in the VPN Global Settings page.

Related Topics

- VPN Global Settings Page, page B-44
- Understanding IKE, page 9-58
- Understanding IPSec Tunnel Policies, page 9-63
- Understanding ISAKMP/IPSec Settings, page 9-69

- Configuring VPN Global Settings, page 9-73

Field Reference

Table B-16 VPN Global Settings Page > ISAKMP/IPSec Settings Tab

Element	Description
ISAKMP Settings	
Enable Keepalive	**Enable**—When selected, enables you to configure IKE keepalive as the default failover and routing mechanism. **Note** IKE keepalive is defined on the spokes in a hub-and-spoke VPN topology, or on both devices in a point-to-point VPN topology.
Interval	The number of seconds that a device waits between sending IKE keepalive packets. The default is 10 seconds.
Retry	The number of seconds a device waits between attempts to establish an IKE connection with the remote peer. The default is 2 seconds.
Periodic	Available only if Enable Keepalive is selected, and supported on routers running IOS version 12.3(7)T and later, except 7600 devices. When selected, enables you to send dead-peer detection (DPD) keepalive messages even if there is no outbound traffic to be sent. Usually, DPD keepalive messages are sent between peer devices only when no incoming traffic is received but outbound traffic needs to be sent. For more information, see About IKE Keepalive, page 9-69.
Identity	During Phase I IKE negotiations, peers must identify themselves to each other. Select to use the IP address or the hostname of the device that it will use to identify itself in IKE negotiations. You can also select to use a Distinguished Name (DN) to identify a user group name.

Table B-16 VPN Global Settings Page > ISAKMP/IPSec Settings Tab (continued)

Element	Description
SA Requests System Limit	Supported on routers running IOS version 12.3(8)T and later, except 7600 routers. The maximum number of SA requests allowed before IKE starts rejecting them. You can enter a value in the range of 0-99999. **Note** Make sure the specified value equals or exceeds the number of peers, or the VPN tunnels may be disconnected.
SA Requests System Threshold	Supported on Cisco IOS routers and Catalyst 6500/7600 devices. The percentage of system resources that can be used before IKE starts rejecting new SA requests.
Enable Aggressive Mode	Supported on ASA devices and PIX 7.0 devices. When selected, enables you to use aggressive mode in ISAKMP negotiations, for an ASA device. Aggressive mode is enabled by default. Deselect this check box to disable the use of aggressive mode in ISAKMP negotiations, for an ASA device. See Understanding IKE, page 9-58.
IPSec Settings	
Enable Lifetime	When selected, enables you to configure the global lifetime settings for the crypto IPSec security associations (SAs) on the devices in your VPN topology.
Lifetime (secs)	The number of seconds a security association will exist before expiring. The default is 3,600 seconds (one hour).
Lifetime (kbytes)	The volume of traffic (in kilobytes) that can pass between IPSec peers using a given security association before it expires. The default is 4,608,000 kilobytes.

Table B-16 VPN Global Settings Page > ISAKMP/IPSec Settings Tab (continued)

Element	Description
Xauth Timeout	Available when Easy VPN is the selected technology, and the selected device is a Cisco IOS router or Catalyst 6500/7600 device. The number of seconds the device waits for a response from the end user after an IKE SA has been established. When negotiating tunnel parameters for establishing IPSec tunnels in an Easy VPN configuration, Xauth adds another level of authentication that identifies the user who requests the IPSec connection. Using the Xauth feature, the client waits for a "username/password" challenge after the IKE SA has been established. When the end user responds to the challenge, the response is forwarded to the IPSec peers for an additional level of authentication.
Max Sessions Number	Supported on ASA devices and PIX 7.0 devices. The maximum number of SAs that can be enabled simultaneously on the device.
Enable IPSec via Sysopt	Supported on ASA devices and PIX Firewalls versions 6.3 or 7.0. When selected, enables you to specify that any packet that comes from an IPSec tunnel be implicitly trusted (permitted).
Enable SPI Recovery	Supported on routers running IOS version 12.3(2)T and later, in addition to Catalyst 6500/7600 devices running version 12.2(18)SXE and later. When selected, enables the SPI recovery feature to configure your device so that if an invalid SPI (Security Parameter Index) occurs, an IKE SA will be initiated. SPI (Security Parameter Index) is a number which, together with a destination IP address and security protocol, uniquely identifies a particular security association. When using IKE to establish security associations, the SPI for each security association is a pseudo-randomly derived number. Without IKE, the SPI is manually specified for each security association. When an invalid SPI occurs during IPSec packet processing, the SPI recovery feature enables an IKE SA to be established.

Table B-16 VPN Global Settings Page > ISAKMP/IPSec Settings Tab (continued)

Element	Description
Save button	Saves your changes to the server but keeps them private. **Note** To publish your changes, click the **Submit** button on the toolbar.
Close button	Closes the Site-to-Site VPN window.
Help button	Opens help for this tab.

NAT Settings Tab

Use the NAT Settings tab of the VPN Global Settings page to define the NAT settings that will be configured on the devices in your VPN topology.

Note If you want to bypass NAT configuration on IOS routers, make sure the **Do Not Translate VPN Traffic** check box is selected in the NAT Dynamic Rule platform policy (see NAT Dynamic Rule Dialog Box, page C-503). To exclude NAT on PIX Firewalls or ASA devices, make sure this check box is selected in the NAT Translation Options platform policy (see Translation Options Page, page C-231).

For more information about NAT, see Understanding NAT, page 9-70.

Navigation Path

Open the VPN Global Settings Page, page B-44, then click the **NAT Settings** tab.

Related Topics

- VPN Global Settings Page, page B-44
- Understanding NAT, page 9-70

Field Reference

Table B-17 VPN Global Settings Page > NAT Settings Tab

Element	Description
Enable NAT Traversal	When selected, enables you to configure NAT traversal on a device. You use NAT traversal when there is a device (referred to as the middle device) located between a VPN-connected hub and spoke, that performs Network Address Translation (NAT) on the IPSec traffic. For more information, see About NAT Traversal, page 9-71.
Keepalive Interval	Available when NAT Traversal is enabled. The interval, in seconds, between the keepalive signals sent between the spoke and the middle device to indicate that the session is active. The keepalive value can be from 5 to 3600 seconds.
Enable PAT (Port Address Translation) on Split Tunneling for Spokes	Supported on Cisco IOS routers and Catalyst 6500/7600 devices. When selected, enables Port Address Translation (PAT) to be used for split-tunneled traffic on spokes in your VPN topology. PAT can associate thousands of private NAT addresses with a small group of public IP address, through the use of port addressing. PAT is used if the addressing requirements of your network exceed the available addresses in your dynamic NAT pool. See Understanding NAT, page 9-70. **Note** When this check box is enabled, Security Manager implicitly creates an additional NAT rule for split-tunneled traffic, on deployment. This NAT rule, which denies VPN-tunneled traffic and permits all other traffic (using the external interface as the IP address pool), will not be reflected as a router platform policy. For information on creating or editing a dynamic NAT rule as a router platform policy, see Defining Dynamic NAT Rules, page 12-20.
Save button	Saves your changes to the server but keeps them private. **Note** To publish your changes, click the **Submit** button on the toolbar.

Table B-17 VPN Global Settings Page > NAT Settings Tab (continued)

Element	Description
Close button	Closes the Site-to-Site VPN window.
Help button	Opens help for this tab.

General Settings Tab

Use the General Settings tab of the VPN Global Settings page to define fragmentation settings including maximum transmission unit (MTU) handling parameters.

Navigation Path

Open the VPN Global Settings Page, page B-44, then click the **General Settings** tab.

Related Topics

- VPN Global Settings Page, page B-44
- Understanding Fragmentation, page 9-72

Field Reference

Table B-18 VPN Global Settings Page > General Settings Tab

Element	Description
Fragmentation Settings	
Fragmentation Mode	Supported on Cisco IOS routers and Catalyst 6500/7600 devices. Fragmentation minimizes packet loss in a VPN tunnel when transmitted over a physical interface that cannot support the original size of the packet. Select the required fragmentation mode option from the list: • **No Fragmentation** - Select if you do not want to fragment prior to IPSec encapsulation. After encapsulation, the device fragments packets that exceed the MTU setting before transmitting them through the public interface. • **End to End MTU Discovery** - Select to use ICMP messages for the discovery of MTU. Use this option when the selected technology is IPSec. End-to-end MTU discovery uses Internet Control Message Protocol (ICMP) messages to determine the maximum MTU that a host can use to send a packet through the VPN tunnel without causing fragmentation. • **Local MTU Handling** - Select to set the MTU locally on the devices. This option is typically used when ICMP is blocked, and when the selected technology is GRE. For more information, see Understanding Fragmentation, page 9-72.
Local MTU Size	Supported on Cisco IOS routers and Catalyst 6500/7600 devices, when Local MTU Handling is the selected fragmentation mode option. The MTU size can be between 540 and 1500 bytes.

Table B-18 VPN Global Settings Page > General Settings Tab (continued)

Element	Description
DF Bit	Supported on Cisco IOS routers, Catalyst 6500/7600 devices, PIX 7.0 and ASA devices. A Don't Fragment (DF) bit within an IP header determines whether a device is allowed to fragment a packet. For more information, see Understanding Fragmentation, page 9-72. Select the required setting for the DF bit: • **Copy**—To copy the DF bit from the encapsulated header in the current packet to all the device's packets. If the packet's DF bit is set to fragment, all future packets will be fragmented. This is the default option. • **Set**—To set the DF bit in the packet you are sending. A large packet that exceeds the MTU will be dropped and an ICMP message sent to the packet's initiator. • **Clear**—If you want the device to fragment packets regardless of the original DF bit setting. If ICMP is blocked, MTU discovery will fail and packets will only be fragmented after encryption.
Enable Fragmentation Before Encryption	Supported on Cisco IOS routers, Catalyst 6500/7600 devices, PIX 7.0 and ASA devices. When selected, enables fragmentation to occur before encryption, if the expected packet size exceeds the MTU. Lookahead Fragmentation (LAF) is used before encryption takes place to calculate the packet size that would result after encryption, depending on the transform sets configured on the IPSec SA. If the packet size exceeds the specified MTU, the packet will be fragmented before encryption.
Enable Notification on Disconnection	Supported on PIX 7.0 and ASA devices. When selected, enables the device to notify qualified peers of sessions that are about to be disconnected. The peer receiving the alert decodes the reason and displays it in the event log or in a pop-up panel. This feature is disabled by default.

Table B-18 VPN Global Settings Page > General Settings Tab (continued)

Element	Description
Enable Split Tunneling	When selected (the default), enables you to configure split tunneling in your VPN topology. Split tunneling enables you to transmit both secured and unsecured traffic on the same interface. Split tunneling requires that you specify exactly which traffic will be secured and what the destination of that traffic is, so that only the specified traffic enters the IPSec tunnel, while the rest is transmitted unencrypted across the public network.
Enable Spoke-to-Spoke Connectivity through the Hub	Supported on PIX 7.0 and ASA devices. When selected, enables direct communication between spokes in a hub-and-spoke VPN topology, in which the hub is an ASA/PIX 7.0 device.
Enable Default Route	Supported on Cisco IOS routers and Catalyst 6500/7600 devices. When selected, the device uses the configured external interface as the default outbound route for all incoming traffic.
Save button	Saves your changes to the server but keeps them private. **Note** To publish your changes, click the **Submit** button on the toolbar.
Close button	Closes the Site-to-Site VPN window.
Help button	Opens help for this tab.

Preshared Key Page

Use the Preshared Key page to view or edit the parameters for a preshared key policy.

For information about Preshared Key policies, see Understanding Preshared Key Policies, page 9-74.

Note A preshared key policy is not available when configuring Easy VPN.

Navigation Path

Open the Site-to-Site VPN Manager Window, page B-2, select a topology in the VPNs selector, then select **Preshared Key** in the Policies selector.

Note You can also open the Preshared Key page from Policy view. For more information, see Managing Shared Site-to-Site VPN Policies in Policy View, page 9-56.

Related Topics

- Configuring Preshared Key Policies, page 9-76

Field Reference

Table B-19 Preshared Key Page

Element	Description
Key Specification	
User Defined	Click to use a manually defined preshared key, then enter the required preshared key in the **Key** field.
Auto Generated	Click to allocate a random key to the participating peers. This ensures security because a different key is generated for every hub-spoke connection. Auto Generate is the default selection. **Note** The key is allocated during the first deployment to the devices and is used in all subsequent deployments to the same devices, until you select the Regenerate Key (Only in Next Deployment) check box.
Key Length	The required length of the preshared key to be automatically generated (maximum 127 characters).
Same Key for All Tunnels	Unavailable in a point-to-point VPN topology. Select this check box to use the same auto-generated key for all tunnels. If you do not select this check box, different keys are used for the tunnels, except in cases, such as DMVPN configuration, when different multipoint GRE interfaces in the same network must use the same preshared key.

Table B-19 Preshared Key Page (continued)

Element	Description
Regenerate Key (Only in Next Deployment)	Only available if Auto Generate is selected. Select this check box if you want Security Manager to generate a new key for the next deployment to the device(s). This is useful if it is possible that the secrecy of the keys might be compromised. **Note** When you submit the job for deployment, this check box is cleared. It does not remain selected because the new key will only be generated for the upcoming deployment, and not for subsequent deployments (unless you select it again).

Table B-19 Preshared Key Page (continued)

Element	Description
Negotiation Method	
Main Mode Address	Select this negotiation method for exchanging key information, if the IP address of the devices is known. Negotiation is based on IP address. Main mode provides the highest security because it has three two-way exchanges between the initiator and receiver. Main mode address is the default negotiation method. Then click one of the following radio buttons to define the negotiation address type: • **Peer Address**—Negotiation is based on the unique IP address of each peer. A key is created for each peer, providing high security. • **Subnet**—Creates a group preshared key on a hub in a hub-and-spoke topology to use for communication with any device in a specified subnet, even if the IP address of the device is unknown. Each peer is identified by its subnet. After selecting this option, enter the subnet in the field provided. In a point-to-point or full mesh VPN topology, a group preshared key is created on the peers. • **Wildcard**—Creates a wildcard key on a hub or on a group of hubs in a hub-and-spoke topology to use when a spoke does not have a fixed IP address or belong to a specific subnet. In this case, all spokes connecting to the hub will have the same preshared key, which could compromise security. Use this option if a spoke in your hub-and-spoke VPN topology has a dynamic IP address. In a point-to-point or full mesh VPN topology, a wildcard key is created on the peers. **Note** When configuring DMVPN with direct spoke-to-spoke connectivity, you create a wildcard key on the spokes.
Main Mode FQDN	Select this negotiation method for exchanging key information, if the IP address is not known and DNS resolution is available for the device(s). Negotiation is based on DNS resolution, with no reliance on IP address.

Table B-19 Preshared Key Page (continued)

Element	Description
Aggressive Mode	Available only in a hub-and-spoke VPN topology. Select this negotiation method for exchanging key information, if the IP address is not known and DNS resolution might not be available on the devices. Negotiation is based on hostname and domain name. **Note** If direct spoke to spoke tunneling is enabled, you cannot use aggressive mode.
Save button	Saves your changes to the server but keeps them private. **Note** To publish your changes, click the **Submit** button on the toolbar.
Close button	Closes the Site-to-Site VPN window.
Help button	Opens help for this page.

Public Key Infrastructure Page

Use the Public Key Infrastructure page to select the CA server that will be used to create a Public Key Infrastructure (PKI) policy, for generating enrollment requests for CA certificates.

Note For information about Public Key Infrastructure policies, see Understanding Public Key Infrastructure Policies, page 9-78.

Navigation Path

Open the Site-to-Site VPN Manager Window, page B-2, select a topology in the VPNs selector, then select **Public Key Infrastructure** in the Policies selector.

Note You can also open the Public Key Infrastructure page from Policy view. For more information, see Working with Site-to-Site VPN Policies, page 9-55.

Related Topics

- Configuring Public Key Infrastructure Policies, page 9-84
- Working with PKI Enrollment Objects, page 8-153

Field Reference

Table B-20 Public Key Infrastructure (PKI) Page

Element	Description
Available CA Servers	Lists the predefined CA servers available for selection. CA servers are predefined PKI enrollment objects that contain server information and enrollment parameters that are required for creating enrollment requests for CA certificates. Select the required CA server if you want to replace the default one in the **Selected** field. If the required CA server is not included in the list, click **Create** to open a dialog box that enables you to create or edit a PKI enrollment object. For more information, see PKI Enrollment Dialog Box, page C-140. **Note** If you are making a PKI enrollment request on an Easy VPN remote access system, you must configure each remote component (spoke) with the name of the user group to which it connects. You specify this information in the Organization Unit (OU) field in the Certificate Subject Name tab of the PKI Enrollment Editor dialog box. You do not need to configure the name of the user group on the hub (Easy VPN Server). For more information, see Defining Additional PKI Attributes, page 8-162.
Selected	The selected CA server. **Note** You cannot edit the selected CA server because it is a predefined object. You can only edit the properties of an object you define. To remove the selected CA server, select a different one.

Table B-20 Public Key Infrastructure (PKI) Page (continued)

Element	Description
Save button	Saves your changes to the server but keeps them private. To publish your changes, click the **Submit** button on the toolbar. **Note** To save the RSA key pairs and the CA certificates between reloads permanently to Flash memory on a PIX firewall version 6.3, you must configure the "ca save all" command. You can do this manually on the device or using a FlexConfig (see Working with FlexConfigs, page 16-40).
Close button	Closes the Site-to-Site VPN window.
Help button	Opens help for this page.

GRE Modes Page

Use the GRE Modes page to define the routing and tunnel parameters, that enable you to configure IPSec tunneling with GRE, GRE Dynamic IP, and DMVPN policies.

The elements that are displayed on the GRE Modes page depend on the selected IPSec technology—GRE, GRE Dynamic IP, or DMVPN. For more information, see Understanding IPSec Technologies and Policies, page 9-8.

Table B-21 on page B-60 describes the elements on the GRE Modes page for configuring IPSec tunneling with GRE or GRE Dynamic IP.

Table B-22 on page B-65 describes the elements on the GRE Modes page for configuring DMVPN.

Note When configuring a GRE, GRE Dynamic IP, or DMVPN routing policy, Security Manager adds a routing protocol to all the devices in the secured IGP, on deployment. If you want to maintain this secured IGP, you must create a router platform policy using the same routing protocol and autonomous system (or process ID) number as defined in the GRE Modes policy.

For more information about GRE and GRE Dynamic IP policies, see Understanding GRE, page 9-86 and Understanding GRE Configuration for Dynamically Addressed Spokes, page 9-90.

Navigation Path

Open the Site-to-Site VPN Manager Window, page B-2, select a topology in the VPNs selector, then select **GRE Modes** in the Policies selector.

Note You can also open the GRE Modes page from Policy view. For more information, see Managing Shared Site-to-Site VPN Policies in Policy View, page 9-56.

Related Topics

- Understanding GRE, page 9-86
- Configuring GRE or GRE Dynamic IP Policies, page 9-91
- Understanding DMVPN, page 9-94
- Configuring DMVPN Policies, page 9-96

Field Reference

Table B-21 describes the elements on the GRE Modes page for configuring IPSec tunneling with GRE or GRE Dynamic IP.

Table B-21 GRE Modes Page > GRE or GRE Dynamic IP Policy

Element	Description
Routing Parameters Tab	
Routing Protocol	Select the required dynamic routing protocol (EIGRP, OSPF, or RIPv2,) or static route to be used for GRE or GRE Dynamic IP. For more information, see Prerequisites for Successful Configuration of GRE, page 9-87.

Table B-21 GRE Modes Page > GRE or GRE Dynamic IP Policy (continued)

Element	Description
AS Number	Available only if you selected the EIGRP routing protocol. The number that will be used to identify the autonomous system (AS) area to which the EIGRP packet belongs. The range is 1-65535. The default is 110. An autonomous system (AS) is a collection of networks that share a common routing strategy. An AS can be divided into a number of areas, which are groups of contiguous networks and attached hosts. Routers with multiple interfaces can participate in multiple areas. An AS ID identifies the area to which the packet belongs. All EIGRP packets are associated with a single area, so all devices must have the same AS number.
Process Number	Available only if you selected the OSPF routing protocol. The routing process ID number that will be used to identify the secured IGP that Security Manager adds when configuring GRE. The range is 1-65535. The default is 110. Security Manager adds an additional Interior Gateway Protocol (IGP) that is dedicated for IPSec and GRE secured communication. An IGP refers to a group of devices that receive routing updates from one another by means of a routing protocol. Each “routing group” is identified by the process number. For more information, see How Does Security Manager Implement GRE?, page 9-87.
Hello Interval	Available only if you selected the EIGRP routing protocol. The interval between hello packets sent on the interface, from 1 to 65535 seconds. The default is 5 seconds.
Hold Time	Available only if you selected the EIGRP routing protocol. The number of seconds the router will wait to receive a hello message before invalidating the connection. The range is 1-65535. The default hold time is 15 seconds (three times the hello interval).

Table B-21 GRE Modes Page > GRE or GRE Dynamic IP Policy (continued)

Element	Description
Delay	Available only if you selected the EIGRP routing protocol. The throughput delay for the primary route interface, in microseconds. The range of the tunnel delay time is 1-16777215. The default is 1000.
Failover Delay	Available only if you selected the EIGRP routing protocol. The throughput delay for the failover route interface, in microseconds. The range of the tunnel delay time is 1-16777215. The default is 1500.
Hub Network Area ID	Available only if you selected the OSPF routing protocol. The ID number of the area in which the hub's protected networks will be advertised, including the tunnel subnet. You can specify any number. The default is 1.
Spoke Protected Network Area ID	Available only if you selected the OSPF routing protocol. The ID number of the area in which the remote protected networks will be advertised, including the tunnel subnet. You can specify any number. The default is 2.
Authentication	Available if you selected the OSPF or RIPv2 routing protocol. A string that specifies the OSPF or RIPv2 authentication key. The string can be up to eight characters long.
Cost	Available if you selected the OSPF or RIPv2 routing protocol. The cost of sending a packet on the primary route interface. You can enter a value in the range 1-65535. The default is 100.
Failover Cost	Available if you selected the OSPF or RIPv2 routing protocol. The cost of sending a packet on the secondary (failover) route interface. You can enter a value in the range 1-65535. The default is 125.
Filter Dynamic Updates on Spokes	Select to enable the creation of a redistribution list that filters all dynamic routing updates on the spokes. This forces the spoke devices to advertise (populate on the hub device) only their own protected subnets and not other IP addresses.

Table B-21 GRE Modes Page > GRE or GRE Dynamic IP Policy (continued)

Element	Description
Tunnel Parameters Tab	
Tunnel IP	Click one of the following radio buttons to specify the GRE or GRE Dynamic IP tunnel interface IP address: • **Use Physical Interface**—To use the private IP address of the tunnel taken from the protected network. • **Use Subnet**—To use the tunnel IP address taken from an IP range. Then, in the **Subnet** field, enter the private IP address including the unique subnet mask, for example 10.1.1.0/24. If you are also configuring a dial backup interface, enter its subnet in the **Dial Backup Subnet** field provided. • **Use Loopback Interface**—To use the tunnel IP address taken from an existing loopback interface. Then, in the **Role** field, enter the interface, or select it from the list of interface roles provided. For more information, see Interface Roles Page, page C-126. **Note** To view the newly created GRE tunnel and/or loopback interfaces in the Router Interfaces page, you must rediscover the device inventory details after successfully deploying the VPN to the device. For more information, see Configuring Cisco IOS Router Interfaces, page 12-2.
Tunnel Source IP Range	Available only if the assigned IPSec technology is GRE Dynamic IP. The private IP address including the unique subnet mask that supports the loopback for GRE. The GRE tunnel interface has an IP address (inside tunnel IP address) which is taken from a loopback interface that Security Manager creates specifically for this purpose. When a spoke has a dynamic IP address, there is no fixed GRE tunnel source address (to be used by the GRE tunnel on the spoke side) or destination address (to be used by the GRE tunnel on the hub side). Therefore, Security Manager creates additional loopback interfaces on the hub and the spoke to use as the GRE tunnel endpoints. You must specify a subnet from which Security Manager can allocate an IP address for the loopback interfaces.

Table B-21 GRE Modes Page > GRE or GRE Dynamic IP Policy (continued)

Element	Description
Enable IP Multicast	Select to enable multicast transmissions across your GRE tunnels. IP multicast delivers application source traffic to multiple receivers without burdening the source or the receivers, while using a minimum of network bandwidth.
Rendezvous Point	Only available if you selected the Enable IP Multicast check box. If required, you can enter the IP address of the interface that will serve as the rendezvous point (RP) for multicast transmission. Sources send their traffic to the RP. This traffic is then forwarded to receivers down a shared distribution tree.
Save button	Saves your changes to the server but keeps them private. **Note** To publish your changes, click the **Submit** button on the toolbar.
Close button	Closes the Site-to-Site VPN window.
Help button	Opens help for this page.

Table B-22 describes the elements on the GRE Modes page for configuring a DMVPN policy.

Table B-22 GRE Modes Page > DMVPN Policy

Element	Description
Routing Parameters Tab	
Routing Protocol	Select the required dynamic routing protocol, or static route, to be used in the DMVPN tunnel. Options include the EIGRP, OSPF, and RIPv2 dynamic routing protocols, and GRE static routes. On-Demand Routing (ODR) is also supported. On-Demand Routing is not a routing protocol. It can be used in a hub-and-spoke VPN topology when the spoke routers connect to no other router other than the hub. If you are running dynamic protocols, On-Demand Routing is not suitable for your network environment. For more information, see Prerequisites for Successful Configuration of GRE, page 9-87.
AS Number	Available only if you selected the EIGRP routing protocol. The number that is used to identify the autonomous system (AS) area to which the EIGRP packet belongs. The range is 1-65535. The default is 110. An autonomous system (AS) is a collection of networks that share a common routing strategy. An AS can be divided into a number of areas, which are groups of contiguous networks and attached hosts. Routers with multiple interfaces can participate in multiple areas. An AS ID identifies the area to which the packet belongs. All EIGRP packets are associated with a single area, so all devices must have the same AS number.
Process Number	Available only if you selected the OSPF routing protocol. The routing process ID number that will be used to identify the secured IGP that Security Manager adds when configuring DMVPN. The valid range for either protocol is 1-65535. The default is 110.

Table B-22 GRE Modes Page > DMVPN Policy (continued)

Element	Description
Hello Interval	Available only if you selected the EIGRP routing protocol. The interval between hello packets sent on the interface, from 1 to 65535 seconds. The default is 5 seconds.
Hold Time	Available only if you selected the EIGRP routing protocol. The number of seconds the router will wait to receive a hello message before invalidating the connection. The range is 1-65535. The default hold time is 15 seconds (three times the hello interval)
Delay	Available only if you selected the EIGRP routing protocol. The throughput delay for the primary route interface, in microseconds. The range of the tunnel delay time is 1-16777215. The default is 1000.
Failover Delay	Available only if you selected the EIGRP routing protocol. The throughput delay for the failover route interface, in microseconds. The range of the tunnel delay time is 1-16777215. The default is 1500.
Hub Network Area ID	Available only if you selected the OSPF routing protocol. The ID number of the area in which the hub’s protected networks will be advertised, including the tunnel subnet. You can enter any number. The default is 1.
Spoke Protected Network Area ID	Available only if you selected the OSPF routing protocol. The ID number of the area in which the remote protected networks will be advertised, including the tunnel subnet. You can enter any number. The default is 2.
Authentication	A string that indicates the OSPF authentication key. The string can be up to eight characters long.
Cost	Available if you selected the OSPF or RIPv2 routing protocol. The cost of sending a packet on the primary route interface. You can enter a value in the range 1-65535. The default is 100.

Table B-22 GRE Modes Page > DMVPN Policy (continued)

Element	Description
Failover Cost	Available if you selected the OSPF or RIPv2 routing protocol. The cost of sending a packet on the secondary (failover) route interface. You can enter a value in the range 1-65535. The default is 125.
Allow Direct Spoke to Spoke Connectivity	When selected, enables direct communication between spokes, without going through the hub. **Note** With direct spoke-to-spoke communication, you must use the Main Mode Address option for preshared key negotiation. For more information, see Understanding Preshared Key Policies, page 9-74.
Filter Dynamic Updates On Spokes	Unavailable if you are using On-Demand Routing or a static route for your DMVPN tunnel. When selected, enables the creation of a redistribution list that filters all dynamic routing updates (EIGRP, OSPF, and RIPv2) on spokes. This forces the spoke devices to advertise (populate on the hub device) only their own protected subnets and not other IP addresses.
Tunnel Parameters Tab	
Tunnel IP Range	The IP range of the inside tunnel interface IP address, including the unique subnet mask. **Note** If Security Manager detects that a tunnel interface IP address already exists on the device, and its IP address matches the tunnel's IP subnet field, it will use that interface as the GRE tunnel.
Dial Backup Tunnel IP Range	If you are configuring a dial backup interface, enter its inside tunnel interface IP address, including the unique subnet mask.

Table B-22 GRE Modes Page > DMVPN Policy (continued)

Element	Description
Server Load Balance	When selected, enables the configuration of load balancing on a Cisco IOS router that serves as a hub in a multiple hubs configuration. Server load balancing optimizes performance in a multiple hubs configuration, by sharing the workload. In this configuration, the DMVPN server hubs share the same tunnel IP and source IP addresses, presenting the appearance of a single device to the spokes in a VPN topology.
Enable IP Multicast	When selected, enables multicast transmissions across your GRE tunnels. IP multicast delivers application source traffic to multiple receivers without burdening the source or the receivers, while using a minimum of network bandwidth.
Rendezvous Point	Only available if you selected the Enable IP Multicast check box. If required, you can enter the IP address of the interface that will serve as the rendezvous point (RP) for multicast transmission. Sources send their traffic to the RP. This traffic is then forwarded to receivers down a shared distribution tree.
Tunnel Key	A number that identifies the tunnel key. The default is 1. The tunnel key differentiates between different multipoint GRE (mGRE) tunnel Non Broadcast Multiple Access (NBMA) networks. All mGRE interfaces in the same NBMA network must use the same tunnel key value. If there are two mGRE interfaces on the same router, they must have different tunnel key values. **Note** To view the newly created tunnel interfaces in the Router Interfaces page, you must rediscover the device inventory details after successfully deploying the VPN to the device. For more information, see Configuring Cisco IOS Router Interfaces, page 12-2.

Table B-22 GRE Modes Page > DMVPN Policy (continued)

Element	Description
NHRP Parameters	
Network ID	All Next Hop Resolution Protocol (NHRP) stations within one logical Non-Broadcast Multi-Access (NBMA) network must be configured with the same network identifier. Enter a globally unique, 32-bit network identifier within the range of 1 to 4294967295.
Hold time	The time, in seconds, that routers will keep information provided in authoritative NHRP responses. The cached IP-to-NBMA address mapping entries are discarded after the hold time expires. The default is 300 seconds.
Authentication	An authentication string that controls whether the source and destination NHRP stations allow intercommunication. All routers within the same network using NHRP must share the same authentication string. The string can be up to eight characters long.
Save button	Saves your changes to the server but keeps them private. **Note** To publish your changes, click the **Submit** button on the toolbar.
Close button	Closes the Site-to-Site VPN window.
Help button	Opens help for this page.

Easy VPN IPSec Proposal Page

Use the Easy VPN IPSec Proposal page to create or edit the IPSec policy definitions for your Easy VPN server.

For more information, see Configuring an IPSec Proposal for Easy VPN, page 9-103.

Note This topic describes the IPSec Proposal page when the assigned technology is Easy VPN. For a description of the IPSec Proposal page when the assigned technology is IPSec, GRE, GRE Dynamic IP, or DMVPN, see IPSec Proposal Page, page B-39.

Navigation Path

Open the Site-to-Site VPN Manager Window, page B-2, select a topology in the VPNs selector, then select **Easy VPN IPSec Proposal** in the Policies selector.

Note You can also open the Easy VPN IPSec Proposal page from Policy view. For more information, see Managing Shared Site-to-Site VPN Policies in Policy View, page 9-56.

Related Topics

- Understanding Easy VPN, page 9-100

Field Reference

Table B-23 Easy VPN IPSec Proposal Page

Element	Description
Transform Sets	The transform set(s) to be used for your tunnel policy. Transform sets specify which authentication and encryption algorithms will be used to secure the traffic in the tunnel. **Note** Transform sets may use only tunnel mode IPSec operation. A default transform set is displayed. If you want to use a different transform set, or select additional transform sets, click **Select** to open a dialog box that lists all available transform sets, and in which you can create transform set objects. For more information, see IPSec Transform Sets Page, page C-130. If more than one of your selected transform sets is supported by both peers, the transform set that provides the highest security will be used. **Note** You can select up to six transform sets. For more information, see About Transform Sets, page 9-64.

Table B-23 Easy VPN IPSec Proposal Page (continued)

Element	Description
Enable RRI	Supported on Cisco IOS routers, PIX 7.0 and ASA devices. When selected (the default), enables Reverse Route Injection (RRI) on the crypto map (static or dynamic) for the support of VPN clients. Reverse Route injection (RRI) ensures that a static route is created on a device for each client internal IP address. Deselect this check box if the crypto map is being applied to a Generic Routing Encapsulation (GRE) tunnel that is already being used to distribute routing information. Reverse Route Injection (RRI) learns all the subnets from any network that is defined in a crypto access control list (ACL) as the destination network. The learned routes are installed into the local routing table as static routes that point to the encrypted interface. When the IPSec tunnel is removed, the associated static routes will be removed. These static routes may then be redistributed into other dynamic routing protocols, so that they can be advertised to other parts of the network (usually done by redistributing RRI routes into dynamic routing protocols on the core side). **Note** Security Manager automatically configures RRI on devices with High Availability (HA), or on the IPSec Aggregator when VRF-Aware IPSec is configured.
Enable Network Address Translation	Supported on PIX 7.0 and ASA devices. When selected, enables you to configure Network Address Translation (NAT) on a device. NAT enables devices that use internal IP addresses to send and receive data through the Internet. Private NAT addresses are converted to globally routable IP addresses when they try to access data on the Internet. For more information, see Understanding NAT, page 9-70.

Table B-23 Easy VPN IPSec Proposal Page (continued)

Element	Description
Group Policy Lookup/AAA Authorization Method	Supported on Cisco IOS routers only. The AAA authorization method list that will be used to define the order in which the group policies are searched. Group policies can be configured on both the local server or on an external AAA server. You can click **Select** to open a dialog box that lists all available AAA group servers, and in which you can create AAA group server objects. For more information, see Working with AAA Server Group Objects, page 8-6.
User Authentication (Xauth)/AAA Authentication Method	Supported on Cisco IOS routers only. The AAA or Xauth user authentication method used to define the order in which user accounts are searched. Xauth allows all Cisco IOS software AAA authentication methods to perform user authentication in a separate phase after the IKE authentication phase 1 exchange. The AAA configuration list-name must match the Xauth configuration list-name for user authentication to occur. For more information about defining user accounts, see Defining Device Access Policies, page 12-26. You can click **Select** to open a dialog box that lists all available AAA group servers from which you can make your selection, and in which you can create additional AAA group server objects. For more information, see Working with AAA Server Group Objects, page 8-6.
Save button	Saves your changes to the server but keeps them private. **Note** To publish your changes, click the **Submit** button on the toolbar.
Close button	Closes the Site-to-Site VPN window.
Help button	Opens help for this page.

User Group Policy Page

Use the User Group Policy page to create or edit a user group policy on your Easy VPN server. For more information about user group policies in Easy VPN, see Configuring a User Group Policy for Easy VPN, page 9-106.

Note You can also configure user group policies in remote access VPNs. For more information, see Understanding User Group Policies in Remote Access VPNs, page 10-4.

Navigation Path

Open the Site-to-Site VPN Manager Window, page B-2, select a topology in the VPNs selector, then select **User Group Policy** in the Policies selector.

Note You can also open the User Group Policy page from Policy view. For more information, see Managing Shared Site-to-Site VPN Policies in Policy View, page 9-56.

Related Topics

- Understanding Easy VPN, page 9-100
- Working with User Group Objects, page 8-237

Field Reference

Table B-24 Easy VPN Server > User Group Policy Page

Element	Description
Available User Groups	Lists the predefined user groups available for selection. Select the required user group if you want to replace the default one in the **Selected** field. User groups are predefined objects. If the required user group is not included in the list, click **Create** to open the User Groups Editor dialog box that enables you to create or edit a user group object. For more information, see Editing User Group Objects, page 8-245.

Table B-24 Easy VPN Server > User Group Policy Page (continued)

Element	Description
Selected	The selected user group. **Note** You cannot edit the selected user group because it is a predefined object. You can only edit the properties of an object you create. To remove the selected user group, select a different one.
Save button	Saves your changes to the server but keeps them private. **Note** To publish your changes, click the **Submit** button on the toolbar.
Close button	Closes the Site-to-Site VPN window.
Help button	Opens help for this page.

Tunnel Group Policy (PIX 7.0/ASA) Page

Use the Tunnel Group Policy (PIX 7.0/ASA) page to create or edit tunnel group policies on your Easy VPN server. An Easy VPN tunnel group policy can be configured only on PIX Firewalls running version 7.0, and ASA devices.

For more information about configuring tunnel group policies in Easy VPN, see Configuring a Tunnel Group Policy for Easy VPN, page 9-107.

Note You can also configure tunnel group policies in remote access VPNs. For more information, see Understanding Tunnel Group Policies in Remote Access VPNs, page 10-7.

The following tabs are available on the Tunnel Group Policy (PIX 7.0/ASA) page:

- Tunnel Group Policy > General Tab, page B-75
- Tunnel Group Policy > IPSec Tab, page B-78
- Tunnel Group Policy > Advanced Tab, page B-80
- Tunnel Group Policy > Client VPN Software Update Tab, page B-82

Navigation Path

Open the Site-to-Site VPN Manager Window, page B-2, select a topology in the VPNs selector, then select **Tunnel Group Policy (PIX 7.0/ASA)** in the Policies selector.

Note You can also open the Tunnel Group Policy (PIX 7.0/ASA) page from Policy view. For more information, see Working with Site-to-Site VPN Policies in Policy View, page 9-56.

Related Topics

- Understanding Easy VPN, page 9-100

Tunnel Group Policy > General Tab

Use the General tab of the Tunnel Group Policy (PIX 7.0/ASA) page to specify the global AAA settings for your tunnel group. On this tab you can also select the method (or methods) of address assignment to use.

Navigation Path

The General tab appears when you open the Tunnel Group Policy (PIX 7.0/ASA) Page, page B-74. You can also open it by clicking the **General** tab from any other tab on the Tunnel Group Policy (PIX 7.0/ASA) page.

Related Topics

- Tunnel Group Policy (PIX 7.0/ASA) Page, page B-74
- Configuring a Tunnel Group Policy for Easy VPN, page 9-107

Field Reference

Table B-25 Easy VPN Server > Tunnel Group Policy (PIX 7.0/ASA) Page > General Tab

Element	Description
Tunnel Group Name	The name of the tunnel group that contains the policies for this IPSec connection.

Table B-25 Easy VPN Server > Tunnel Group Policy (PIX 7.0/ASA) Page > General Tab

Element	Description
Group Policy	The group policy to be applied to the tunnel group. A group policy is a collection of user-oriented attribute/value pairs stored either internally on the device or externally on a RADIUS/LDAP server. Click **Select** to open a dialog box that lists all available ASA group policies, and in which you can create an ASA group policy object. For more information, see Working with ASA User Groups, page 8-45.
AAA	
Authentication Server Group	The name of the authentication server group (LOCAL if the tunnel group is configured on the local device). You can click **Select** to open a dialog box that lists all available AAA server groups, and in which you can create AAA server group objects. For more information, see Working with AAA Server Group Objects, page 8-6. **Note** If you want to set the authentication server group per interface, click the **Advanced** tab.
User LOCAL if Server Group fails	Available if you selected LOCAL for the authentication server group. When selected, enables fallback to the local database for authentication if the selected authentication server group fails.
Authorization Server Group	The name of the authorization server group (LOCAL if the tunnel group is configured on the local device). You can click **Select** to open a dialog box that lists all available AAA server groups, and in which you can create AAA server group objects. For more information, see Working with AAA Server Group Objects, page 8-6.
User must exist in the authorization database to connect	When selected, specifies that the username of the remote client must exist in the database so a successful connection can be established. If the username does not exist in the authorization database, then the connection is denied.

Table B-25 Easy VPN Server > Tunnel Group Policy (PIX 7.0/ASA) Page > General Tab

Element	Description
Accounting Server Group	The name of the accounting server group (LOCAL if the tunnel group is configured on the local device). You can click **Select** to open a dialog box that lists all available AAA server groups, and in which you can create AAA server group objects. For more information, see Working with AAA Server Group Objects, page 8-6.
Strip Realm from Username	When selected, removes the realm from the username before passing the username on to the AAA server. A realm is an administrative domain. Enabling this option allows the authentication to be based on the username alone. You must select this check box if your server cannot parse delimiters.
Strip Group from Username	When selected, removes the group name from the username before passing the username on to the AAA server. Enabling this option allows the authentication to be based on the username alone. You must select this check box if your server cannot parse delimiters.
Client Address Assignment	
DHCP Server	The DHCP servers to be used for client address assignments. The server uses the DHCP servers in the order listed. You can add up to 10 servers. A default DHCP server is displayed. DHCP servers are predefined network objects. If you want to use a different DHCP server, or select additional DHCP servers, click **Select** to open the Network/Hosts selector that lists all available network hosts, and in which you can create network host objects. For more information about network objects, see Working with Network/Host Objects, page 8-142.

Table B-25 Easy VPN Server > Tunnel Group Policy (PIX 7.0/ASA) Page > General Tab

Element	Description
Address Pools	The address pools from which IP addresses will be assigned. The server uses these pools in the order listed. If all addresses in the first pool have been assigned, it uses the next pool, and so on. You can specify up to 6 pools. A default address pool is displayed. Address pools are predefined network objects. If you want to use a different address pool, or select additional address pools, click **Select** to open the Network/Hosts selector that lists all available network hosts, and in which you can create network host objects. For more information about network objects, see Working with Network/Host Objects, page 8-142.
Save button	Saves your changes to the server but keeps them private. **Note** To publish your changes, click the **Submit** button on the toolbar.
Close button	Closes the Site-to-Site VPN window.
Help button	Opens help for this tab.

Tunnel Group Policy > IPSec Tab

Use the IPSec tab of the Tunnel Group Policy (PIX 7.0/ASA) page to specify IPSec and IKE parameters for the tunnel group policy.

Navigation Path

Open the Tunnel Group Policy (PIX 7.0/ASA) Page, page B-74, then click the **IPSec** tab. You can also open the IPSec tab by clicking it from any other tab on the Tunnel Group Policy (PIX 7.0/ASA) page.

Related Topics

- Tunnel Group Policy (PIX 7.0/ASA) Page, page B-74
- Configuring a Tunnel Group Policy for Easy VPN, page 9-107

Field Reference

Table B-26 Easy VPN Server > Tunnel Group Policy (PIX 7.0/ASA) Page > IPSec Tab

Element	Description
Preshared Key	The value of the preshared key for the tunnel group. The maximum length of a preshared key is 127 characters.
Trustpoint Name	The trustpoint name if any trustpoints are configured. A trustpoint represents a CA/identity pair and contains the identity of the CA, CA-specific configuration parameters, and an association with one enrolled identity certificate.
IKE Peer ID Validation	Select whether IKE peer ID validation is ignored, required, or checked only if supported by a certificate. During IKE negotiations, peers must identify themselves to one another.
Enable Sending Certificate Chain	When selected, enables the sending of the certificate chain for authorization. A certificate chain includes the root CA certificate, identity certificate, and key pair.
Enable Password Update with RADIUS Authentication	When selected, enables passwords to be updated with the RADIUS authentication protocol. For more information, see Supported AAA Server Types, page 8-21.
ISAKMP Keepalive	
Monitor Keepalive	When selected, enables you to configure IKE keepalive as the default failover and routing mechanism. For more information, see About IKE Keepalive, page 9-69.
Confidence Interval	The number of seconds that a device waits between sending IKE keepalive packets.
Retry Interval	The number of seconds a device waits between attempts to establish an IKE connection with the remote peer. The default is 2 seconds.

Table B-26 Easy VPN Server > Tunnel Group Policy (PIX 7.0/ASA) Page > IPSec Tab (continued)

Element	Description
Authorization Settings	
Use Entire DN as the Username	Select to use the entire Distinguished Name (DN) as the identifier for the username. A distinguished name (DN) is a unique identification, made up of individual fields, that can be used as the identifier when matching users to a tunnel group. DN rules are used for enhanced certificate authentication on PIX Firewalls and ASA devices.
Specify Individual DN fields as the Username	Select to use individual DN fields as the username when matching users to the tunnel group. A DN certificate is made up of different field identifiers to match users to tunnel groups.
Primary DN field	Available if you selected to use individual DN fields as the username. Select the primary DN field identifier to be used for identification from the list.
Secondary DN field	Available if you selected to use individual DN fields as the username. Select the secondary DN field indentifier to be used for identification. Select **None** if no secondary field identifier is required.
Save button	Saves your changes to the server but keeps them private. **Note** To publish your changes, click the **Submit** button on the toolbar.
Close button	Closes the Site-to-Site VPN window.
Help button	Opens help for this tab.

Tunnel Group Policy > Advanced Tab

Use the Advanced tab of the PIX7.0/ASA Tunnel Group Policy page to specify interface-specific information for your tunnel group.

Navigation Path

Open the Tunnel Group Policy (PIX 7.0/ASA) Page, page B-74, then click the **Advanced** tab. You can also open the Advanced tab by clicking it from any other tab on the Tunnel Group Policy (PIX 7.0/ASA) page.

Related Topics

- Tunnel Group Policy (PIX 7.0/ASA) Page, page B-74
- Configuring a Tunnel Group Policy for Easy VPN, page 9-107

Field Reference

Table B-27 Easy VPN Server > Tunnel Group Policy (PIX 7.0/ASA) Page > Advanced Tab

Element	Description
Interface-Specific Authentication Server Groups	
Interface Role	The interface role to be associated with the authentication server group. You can click **Select** to open a dialog box that lists all available interfaces, and sets of interfaces defined by interface roles, in which you can make your selection, or create interface role objects. For more information, see Working with Interface Role Objects, page 8-120.
Server Group	The server group to be associated with the selected interface role. You can click **Select** to open a dialog box that lists all available AAA server groups, and in which you can create AAA server group objects. For more information, see Working with AAA Server Group Objects, page 8-6**.**
Use LOCAL if server group fails.	When selected, enables fallback to the LOCAL database if the selected server group fails.
Add >> button	Click to add the specified interface role and server group to the list.
Remove button	Click to remove an associated interface role and server group from the list.

Table B-27 Easy VPN Server > Tunnel Group Policy (PIX 7.0/ASA) Page > Advanced Tab

Element	Description
Interface-Specific Client Address Pools	
Interface Role	The interface role to assign a client address to. You can click **Select** to open a dialog box that lists all available interfaces, and sets of interfaces defined by interface roles, in which you can make your selection, or create interface role objects. For more information, see Working with Interface Role Objects, page 8-120.
Address Pool	The address pool to be used to assign to a client address to the selected interface. Address pools are predefined network objects. You can click **Select** to open a dialog box that lists all available network hosts, and in which you can create or edit network host objects. For more information about network objects, see Working with Network/Host Objects, page 8-142.
Add >> button	Click to add the specified interface role and address pool to the list.
Remove button	Click to remove an associated interface role and address pool from the list.
Close button	Closes the Site-to-Site VPN window.
Help button	Opens help for this tab.

Tunnel Group Policy > Client VPN Software Update Tab

Use the Client VPN Software Update tab of the PIX7.0/ASA Tunnel Group Policy page to view or edit the client type, VPN Client revisions, and image URL for each client VPN software package installed.

Navigation Path

Open the Tunnel Group Policy (PIX 7.0/ASA) Page, page B-74, then click the **Client VPN Software Update** tab. You can also open the Client VPN Software Update tab by clicking it from any other tab on the Tunnel Group Policy (PIX 7.0/ASA) page.

Related Topics

- Tunnel Group Policy (PIX 7.0/ASA) Page, page B-74
- Configuring a Tunnel Group Policy for Easy VPN, page 9-107

Field Reference

Table B-28 Easy VPN Server > Tunnel Group Policy (PIX 7.0/ASA) Page > Client VPN Software Update Tab

Element	Description
Windows Configuration	
All Windows Platforms	When selected, enables you to configure the specific revision level and URL of the VPN client on all Windows platforms. Then enter the appropriate information in the fields provided.
Various Windows Platforms	When selected, enables you to configure the specific revision level and URL of the VPN client on Windows 95/98/ME or NT4.1/2000/XP platforms. Then enter the appropriate information in the fields provided.
VPN3002 Hardware Client	
VPN Client Revisions	The specific revision level of the VPN3002 client.
Image URL	The specific URL of the VPN3002 client software image.
Save button	Saves your changes to the server but keeps them private. **Note** To publish your changes, click the **Submit** button on the toolbar.
Close button	Closes the Site-to-Site VPN window.
Help button	Opens help for this tab.

Client Connection Characteristics Page

Use the Client Connection Characteristics page to specify how traffic will be routed in the VPN and how the VPN tunnel will be established. Easy VPN can be configured in client mode or network extension mode on a remote device.

Navigation Path

Open the Site-to-Site VPN Manager Window, page B-2, select a topology in the VPNs selector, then select **Client Connection Characteristics** in the Policies selector.

Note You can also open the Client Connection Characteristics page from Policy view. For more information, see Working with Site-to-Site VPN Policies, page 9-55.

Related Topics

- Understanding Easy VPN, page 9-100
- Configuring Client Connection Characteristics for Easy VPN, page 9-109

Field Reference

Table B-29 Easy VPN Remote > Client Connection Characteristics Page

Element	Description
Mode	
Client	Select if you want the devices on the router's inside networks to form a private network with private IP addresses. NAT and PAT will be used. Devices outside the LAN will not be able to ping devices on the LAN, or reach them directly.
Network Extension	Select if you want the devices connected to the inside interfaces to have IP addresses that are routable and reachable by the destination network. The devices at both ends of the connection will form one logical network. PAT will be disabled, allowing the hosts at both ends of the connection to have direct access to each other.
Save button	Saves your changes to the server but keeps them private. **Note** To publish your changes, click the **Submit** button on the toolbar.
Close button	Closes the Site-to-Site VPN window.
Help button	Opens help for this page.

VPN Topologies Device View Page

Device view provides an easy way to view and edit the structure of your VPN topologies at the device level. Use this page to view the VPN topology (topologies) to which each device in the Security Manager inventory belongs, and if necessary, change its assignment to or from a VPN topology. From this page, you can also create and delete VPN topologies, edit the properties of a VPN topology, including its device selection, and edit its policies.

Navigation Path

1. Select **View** > **Device View** or click the **Device View** button on the toolbar.
2. Select the device from the Device selector.
3. Select **Site-to-Site VPN** from the Device Policies selector.

Related Topics

- Working with VPN Topologies, page 9-10
- Creating a VPN Topology, page 9-11
- Editing a VPN Topology, page 9-24
- About Locking in Site-to-Site VPN Topologies, page 9-23
- Managing VPN Devices in Device View, page 9-53
- Working with Site-to-Site VPN Policies, page 9-55

Field Reference

Table B-30 VPN Topologies Device View Page

Element	Description
Type	An icon that depicts the topology type.
Name	The unique name that identifies the VPN topology.
IPSec Technology	The IPSec technology assigned to the VPN topology.
Description	Any description defined for the VPN topology.

Table B-30 VPN Topologies Device View Page (continued)

Element	Description
Edit VPN Policies button	Click to edit the VPN policies defined for a selected VPN topology. The VPN Summary page opens, displaying information about the VPN topology, including its defined policies. **Note** You can also open the VPN Summary page by right-clicking the VPN topology in the table, and selecting the **Edit VPN Policies** option. To edit a policy, select it in the Policies selector. A page opens on which you can view or edit the parameters for the selected policy. See Site to Site VPN Policies, page B-37.
Create VPN Topology button	Click to open the Create VPN wizard to create a VPN topology. See Create VPN Wizard, page B-8. **Note** You can also create a VPN topology by right-clicking in the table and selecting the **Create VPN Topology** option.
Edit VPN Topology button	Click to edit the properties of a selected VPN topology. The Edit VPN dialog box opens, displaying the Device Selection tab. See Device Selection Page, page B-10. **Note** You can also edit the properties of a VPN topology by double-clicking its row in the table, or right-clicking it and selecting the **Edit VPN Topology** option. For more information, see About Editing a VPN Topology, page 9-22.
Delete VPN Topology button	Select a VPN topology, then click to delete it from the table. A dialog box opens asking you to confirm the deletion. **Note** You can also delete a VPN topology by right-clicking it in the table and selecting the **Delete VPN Topology** option. For more information, see Deleting a VPN Topology, page 9-26.