Managing Remote Access VPNs on IOS and PIX 6.3 Devices

Note From version 4.17, though Cisco Security Manager continues to support IOS and PIX features/functionality, it does not support any enhancements.

You can configure and manage remote access IPsec on devices running Cisco IOS Software or PIX 6.3, and SSL VPNs on IOS 12.4(6)T or later devices (but not on PIX devices). For more information on the specific device models supported, see Understanding Devices Supported by Each Remote Access VPN Technology, page 30-8.

The configuration of these remote access VPNs are the same for these device types. ASA and PIX 7.0+ devices use different configurations for remote access VPNs (as explained in Chapter 31, "Managing Remote Access VPNs on ASA and PIX 7.0+ Devices").

The topics in this chapter explain how to configure policies that are specific to IOS and PIX 6.3 devices. Additionally, review the following topics for more information about remote access VPNs:

- Understanding Remote Access VPNs, page 30-1
- Understanding Devices Supported by Each Remote Access VPN Technology, page 30-8
- Discovering Remote Access VPN Policies, page 30-12
- Using the Remote Access VPN Configuration Wizard, page 30-13
  - Creating IPSec VPNs Using the Remote Access VPN Configuration Wizard (IOS and PIX 6.3 Devices), page 30-36
  - Creating SSL VPNs Using the Remote Access VPN Configuration Wizard (IOS Devices), page 30-32

This chapter contains the following topics:

Overview of Remote Access VPN Policies for IOS and PIX 6.3 Devices

Note From version 4.17, though Cisco Security Manager continues to support IOS and PIX features/functionality, it does not support any enhancements.

When you configure remote access VPNs on IOS or PIX 6.3 devices, you use the following policies based on the type of VPN you are configuring. Note that you cannot configure SSL VPNs on PIX 6.3 devices.

- **Policies used with both IPsec and SSL remote access VPNs:**
  - **Global Settings**—You can define global settings that apply to all devices in your remote access VPNs. These settings include Internet Key Exchange (IKE), IPsec, NAT, and fragmentation definitions. The global settings typically have defaults that work in most situations, so configuring the Global Settings policy is optional; configure it only if you need non-default behavior. For more information, see Configuring VPN Global Settings, page 26-30.
  - **Public Key Infrastructure**—You can create a Public Key Infrastructure (PKI) policy to generate enrollment requests for CA certificates and RSA keys, and to manage keys and certificates. Certification Authority (CA) servers are used to manage these certificate requests and issue certificates to users who connect to your IPsec or SSL remote access VPN. For more information, see Understanding Public Key Infrastructure Policies, page 26-51 and Configuring Public Key Infrastructure Policies for Remote Access VPNs, page 26-56.
- **Policies used in remote access IPsec VPNs only:**
  - **IKE Proposal**—Internet Key Exchange (IKE), also called ISAKMP, is the negotiation protocol that enables two hosts to agree on how to build an IPsec security association. IKE is used to authenticate IPsec peers, negotiate and distribute IPsec encryption keys, and to automatically establish IPsec security associations (SAs). Use the IKE Proposal policy to define the requirements for phase 1 of the IKE negotiation. For more information, see Configuring an IKE Proposal, page 26-9.
  - **IPsec Proposal (IOS/PIX 6.x)**—An IPsec proposal is a collection of one or more crypto maps. A crypto map combines all the components required to set up IPsec security associations (SAs), including IPsec rules, transform sets, remote peers, and other parameters that might be necessary to define an IPsec SA. The policy is used for IKE phase 2 negotiations. For more information, see Configuring an IPsec Proposal on a Remote Access VPN Server (IOS, PIX 6.3 Devices), page 33-3.
  - **High Availability**—High Availability (HA) is supported by the creation of an HA group made up of two or more hub devices that use Hot Standby Routing Protocol (HSRP) to provide transparent, automatic device failover. For more information, see Configuring High Availability in Remote Access VPNs (IOS), page 33-11.
  - **User Groups (IOS/PIX 6.x)**—A user group policy specifies the attributes that determine user access to and use of the VPN. For more information, see Configuring User Group Policies, page 33-13.
- **Policies used in remote access SSL VPNs only:**
  - **SSL VPN**—The SSL VPN policy table lists all of the contexts that define the virtual configurations of the SSL VPN. Each context has a gateway, domain or virtual hostname, and user group policies. For more information, see Configuring an SSL VPN Policy (IOS), page 33-14.

Configuring an IPsec Proposal on a Remote Access VPN Server (IOS, PIX 6.3 Devices)

Note From version 4.17, though Cisco Security Manager continues to support IOS and PIX features/functionality, it does not support any enhancements.

This procedure describes how to create or edit an IPsec proposal for your remote access VPN server when the server uses Cisco IOS Software or PIX release 6.3.

An IPsec proposal is a collection of one or more crypto maps. A crypto map combines all the components required to set up IPsec security associations (SAs), including IPsec rules, transform sets, remote peers, and other parameters that might be necessary to define an IPsec SA.

When configuring an IPsec proposal, you must define the external interface through which the remote access clients connect to the server, and the encryption and authentication algorithms that protect the data in the VPN tunnel. You can also select a group authorization (Group Policy Lookup) method that defines the order in which group policies are searched (on the local server or on external AAA servers) and a user authentication (Xauth) method that defines the order in which user accounts are searched.

For more information on IPsec tunnel concepts, see Understanding IPsec Proposals, page 26-19.

When you create or edit an IPsec proposal, you can also configure:

- A VPN Services Module (VPNSM) interface IPsec VPN Shared Port Adapter (VPN SPA) on a Catalyst 6500/7600 device (see VPNSM/VPN SPA/VSPA Settings Dialog Box, page 33-6).
- A dynamic virtual interface on an IOS router running Cisco IOS Software version 12.4(2)T or later, except 7600 device. For more information, see Configuring Dynamic VTI/VRF Aware IPsec in Remote Access VPNs (IOS Devices), page 33-7.
- VRF-Aware IPsec on a router or Catalyst 6500/7600 device (see Configuring Dynamic VTI/VRF Aware IPsec in Remote Access VPNs (IOS Devices), page 33-7).

Related Topics

- Understanding VRF-Aware IPsec, page 25-14
- VPNSM/VPN SPA/VSPA Settings Dialog Box, page 33-6
- Table Columns and Column Heading Features, page 1-49

Step 1 Do one of the following:

- (Device view) Select **Remote Access VPN > IPSec VPN > IPsec Proposal (IOS/PIX 6.x)** from the Policy selector.
- (Policy view) Select **Remote Access VPN > IPSec VPN > IPsec Proposal (IOS/PIX 6.x)** from the Policy Type selector. Select an existing policy or create a new one.

The IPsec Proposal page opens and lists the configured proposals, including the VPN endpoint, IPsec transform set, and whether reverse route injection is configured for the proposal. You can add other columns to the default display to show the AAA, VRF, and dVTI configuration.

Step 2 Do any of the following:

- To add a new IPsec proposal, click the **Add Row (+)** button and fill in the IPsec Proposal Editor dialog box. For detailed information on the available options, see IPsec Proposal Editor (IOS, PIX 6.3 Devices), page 33-4.

- To edit an existing proposal, select it and click the **Edit Row (pencil)** button.
- To delete a proposal, select it and click the **Delete Row (trash can)** button.

IPsec Proposal Editor (IOS, PIX 6.3 Devices)

Note From version 4.17, though Cisco Security Manager continues to support IOS and PIX features/functionality, it does not support any enhancements.

Use the IPsec Proposal Editor to create or edit an IPsec proposal for an IOS or PIX 6.3 device, including Catalyst 6500/7600, in your remote access VPN. The editor has two tabs—General and Dynamic VTI/VRF Aware IPsec. This topic explains the basic settings on the General tab. For an explanation of Dynamic VTI/VRF Aware IPsec settings, see Configuring Dynamic VTI/VRF Aware IPsec in Remote Access VPNs (IOS Devices), page 33-7.

The elements in this dialog box differ according to the selected device. The table below describes the elements on the General tab in the IPsec Proposal Editor dialog box when a Cisco IOS router, Catalyst 6500/7600, or PIX 6.3 device is selected.

Note For a description of the elements in the dialog box when a PIX 7.0+ or ASA device is selected is selected, see IPsec Proposal Editor (ASA, PIX 7.0+ Devices), page 31-41.

Navigation Path

- (Device view) Select **Remote Access VPN > IPSec VPN > IPsec Proposal (IOS/PIX 6.x)** from the Policy selector. Click the Add Row (+) or Edit Row (pencil) buttons.
- (Policy view) Select **Remote Access VPN > IPSec VPN > IPsec Proposal (IOS/PIX 6.x)** from the Policy Type selector. Select an existing policy or create a new one. Click the Add Row (+) or Edit Row (pencil) buttons.

Related Topics

- Configuring an IPsec Proposal on a Remote Access VPN Server (IOS, PIX 6.3 Devices), page 33-3
- Understanding IPsec Proposals, page 26-19
- Creating Interface Role Objects, page 6-74
- Creating AAA Server Group Objects, page 6-48

Field Reference

Table 33-1 IPsec Proposal Editor, General Tab, IOS and PIX 6.3 Devices

Element	Description
External Interface	**Note** Available only if the selected device is an IOS router. The external interface through which remote access clients will connect to the server. Enter the name of the interface or interface role object, or click **Select** to select it or to create a new object.

Table 33-1 IPsec Proposal Editor, General Tab, IOS and PIX 6.3 Devices (continued)

Element	Description
Inside VLAN	**Note** Available only if the selected device is a Catalyst 6500/7600. The inside VLAN that serves as the inside interface to the VPN Services Module (VPNSM), VPN SPA, or VSPA. Click **Select** to configure the inside VLAN as explained in VPNSM/VPN SPA/VSPA Settings Dialog Box, page 33-6.
IKEv1 Transform Sets	The transform sets 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. You can select up to nine transform sets. For more information, see Understanding Transform Sets, page 26-20. 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. Click **Select** to select the IPsec transform set policy objects to use in the topology. If the required object is not yet defined, you can click the **Create (+)** button beneath the available objects list in the selection dialog box to create a new one. For more information, see Configuring IPSec IKEv1 or IKEv2 Transform Set Policy Objects, page 26-27.
Reverse Route Injection	Reverse Route Injection (RRI) enables static routes to be automatically inserted into the routing process for those networks and hosts protected by a remote tunnel endpoint. For more information, see Understanding Reverse Route Injection, page 26-21. Select one of the following options to configure RRI on the crypto map: • **None**—Disables the configuration of RRI on the crypto map. • **Standard**—Creates routes based on the destination information defined in the crypto map access control list (ACL). This is the default option. • **Remote Peer**—Creates two routes, one for the remote endpoint and one for route recursion to the remote endpoint via the interface to which the crypto map is applied. • **Remote Peer IP**—Specifies an address as the explicit next hop to the remote VPN device. Enter the IP address or a network/host object that specifies the address, or click **Select** to select the network/host object from a list or to create a new object. **Note** If you use network/host objects, you can select the **Allow Value Override per Device** option in the object to override the IP address, if required, for specific devices that use this object.

Table 33-1 IPsec Proposal Editor, General Tab, IOS and PIX 6.3 Devices (continued)

Element	Description
Group Policy Lookup/AAA Authorization Method	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. Remote users are grouped, so that when the remote client establishes a successful connection to the VPN server, the group policies for that particular user group are pushed to all clients belonging to the user group. Click **Select** to open a dialog box that lists all available AAA group servers, and in which you can create AAA group server objects. Select all that apply and use the up and down arrow buttons to put them in priority order.
User Authentication (Xauth)/AAA Authentication Method	The AAA or Xauth user authentication method that defines 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. Click **Select** to open a dialog box that lists all available AAA group servers, and in which you can create AAA group server objects. Select all that apply and use the up and down arrow buttons to put them in priority order.

VPNSM/VPN SPA/VSPA Settings Dialog Box

Note This dialog box is available only if the selected device is a Catalyst 6500/7600.

Use the VPNSM/VPN SPA/VSPA Settings dialog box to specify the settings for configuring a VPN Services Module (VPNSM), a VPN Shared Port Adapter (VPN SPA), or a Cisco VPN Service Port Adapters (VSPAs) on a Catalyst 6500/7600 device.

Notes

- Before you define the settings, you must import your Catalyst 6500/7600 device to the Security Manager inventory and discover its interfaces. For more information, see Configuring VPNSM or VPN SPA/VSPA Endpoint Settings, page 25-42.
- Before you configure VPNSM or VPN SPA with VRF-Aware IPsec on a device, verify that an IPsec proposal with VRF-Aware IPsec and an IPsec proposal without VRF-Aware IPsec were not configured on the device.

Navigation Path

In the General tab of the IPsec Proposal Editor Dialog Box (for Catalyst 6500/7600 Devices), click **Select** next to the Inside VLAN field. For more information about opening the IPsec Proposal Editor, see IPsec Proposal Editor (IOS, PIX 6.3 Devices), page 33-4.

Related Topics

- Creating Interface Role Objects, page 6-74

Field Reference

Table 33-2 VPNSM/VPN SPA/VSPA Settings Dialog Box

Element	Description
Inside VLAN	The inside VLAN that serves as the inside interface to the VPNSM, VPN SPA, or VSPA, and to which the required crypto maps will be applied. Enter the VLAN ID or click **Select** to select it or to create a new interface role object to identify the VLAN.
Slot Subslot	The number designating the slot location of the VPNSM or VPNSPA/VSPA. If you are configuring a VPNSPA/VSPA, the subslot number is also required. **Note** If you are configuring a VPNSM, select 0.
External Port	The external port or VLAN that connects to the inside VLAN. Enter the name of the VLAN or interface role object, or click **Select** to select it from a list. You must select an interface or interface role that differs from the one selected for 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.
Enable Failover Blade	Whether to configure a failover VPNSM or VPNSPA/VSPA blade for intra-chassis high availability. **Note** A VPNSM and VPNSPA/VSPA blade cannot be used on the same device as primary and failover blades. Specify the failover blade, as follows: • **Slot**—The slot number that identifies where the VPNSM blade or VPNSPA/VSPA blade is located. • **Subslot**—If you are configuring a VPNSPA/VSPA, select the number of the subslot on which the failover VPN SPA blade is installed. **Note** If you are configuring a VPNSM, select 0.

Configuring Dynamic VTI/VRF Aware IPsec in Remote Access VPNs (IOS Devices)

Note The Dynamic VTI/VRF Aware IPsec tab is available only when the selected device is a Cisco IOS router or Catalyst 6500/7600.

Use the Dynamic VTI/VRF Aware IPsec tab of the IPsec Proposal Editor to configure VRF Aware IPsec settings (on a Cisco IOS router or Catalyst 6500/7600 device), configure a dynamic virtual interface on a Cisco IOS router, or do both, in your remote access VPN.

IOS devices allow dynamic virtual template interfaces (VTIs), which provide highly secure and scalable connectivity for remote-access VPNs, replacing dynamic crypto maps and the dynamic hub-and-spoke method for establishing tunnels. You can use dynamic VTIs for both the server and remote configuration. The tunnels provide an on-demand separate virtual access interface for each VPN session. The configuration of the virtual access interfaces is duplicated from a virtual template configuration, which includes the IPsec configuration and any features configured on the virtual template interface. Dynamic VTIs provide efficiency in the use of IP addresses and provide secure connectivity. They enable dynamically downloadable per-group and per-user policies to be configured on a RADIUS server. Dynamic VTI simplifies VRF-Aware IPsec deployment, as the VRF is configured on the interface.

When this feature is enabled, Security Manager implicitly creates the virtual template interface for the selected device in a remote access VPN. All you must do is provide the IP address on the server that will be used as the virtual template interface, or use an existing loopback interface. The virtual template interface is created on the remote client without an IP address.

Notes

- You can configure dynamic VTI only on routers running Cisco IOS Release 12.4(2)T and later, except 7600 devices.
- You can configure dynamic VTI with or without VRF-Aware IPsec. For more information about VRF-Aware IPsec, see Understanding VRF-Aware IPsec, page 25-14.
- You can also configure dynamic VTI in a site-to-site Easy VPN topology. For more information, see Easy VPN with Dynamic Virtual Tunnel Interfaces, page 28-3.

Navigation Path

In the IPsec Proposal Editor Dialog Box (for IOS routers and Catalyst 6500/7600 devices), click the **Dynamic VTI/VRF Aware IPsec** tab. For more information, see IPsec Proposal Editor (IOS, PIX 6.3 Devices), page 33-4.

Related Topics

- Configuring an IPsec Proposal on a Remote Access VPN Server (IOS, PIX 6.3 Devices), page 33-3
- Creating Interface Role Objects, page 6-74

Field Reference

Table 33-3 IPsec Proposal Editor, Dynamic VTI/VRF Aware IPsec Tab

Element	Description
Enable Dynamic VTI	When selected, enables Security Manager to implicitly create a dynamic virtual template interface on an IOS router. **Note** Dynamic VTI can be configured only on IOS routers running Cisco IOS Release 12.4(2)T and later, except 7600 devices. If the device does not support Dynamic VTI, the option is greyed out.
Enable VRF Settings	When selected, enables you to configure VRF settings on the device for the selected hub-and-spoke topology. **Note** To remove VRF settings that were defined for the VPN topology, deselect this check box.

Table 33-3 IPsec Proposal Editor, Dynamic VTI/VRF Aware IPsec Tab (continued)

Element	Description
User Group	When you configure a remote access VPN server, remote clients must have the same group name as the user group object configured on the VPN server so that they can connect to the device. Enter the name of the user group policy object associated with the device, or click **Select** to select it from a list. You can also create new objects or edit existing ones from the selection list.
CA Server	Select the Certification Authority (CA) server to use for managing certificate requests for the device. Click **Select** to select the PKI enrollment policy object that defines the CA server, or to create a new object. For more information, see PKI Enrollment Dialog Box, page 26-58. For more information about IPsec configuration with CA servers, see Understanding Public Key Infrastructure Policies, page 26-51.
Virtual Template IP Type	Available if you selected **Enable Dynamic VTI**. Specify the virtual template interface to use: • **IP**—To use an IP address as the virtual template interface. Specify the private IP address. • **Use Loopback Interface**—To use the IP address taken from an existing loopback interface as the virtual template interface. Click **Select** to select the interface or interface role object, or to create a new object that identifies the loopback interface.
VRF Solution	Available if you selected **Enable VRF Settings**. Select the VRF solution: • **1-Box (IPsec Aggregator + MPLS PE)**—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 25-14. • **2-Box (IPsec Aggregator Only)**—The PE device does only 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 25-15.
VRF Name	The name of the VRF routing table on the IPsec Aggregator. The VRF name is case-sensitive.

Table 33-3 IPsec Proposal Editor, Dynamic VTI/VRF Aware IPsec Tab (continued)

Element	Description
Route Distinguisher	The unique identifier of the VRF routing table on the IPsec Aggregator. This unique route distinguisher maintains 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 of 0-999999999. • *N:X*, where *N* is in the range of 0-65535, and X is in the range of 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 through the device CLI and then deploy again.
Interface Towards Provider Edge	Available only for 2-Box VRF. The VRF forwarding interface on the IPsec Aggregator towards the PE device. Click **Select** to select the interface or interface role object, or to create a new object that identifies the interface. **Note** If the IPsec Aggregator (hub) is a Catalyst VPN service module, you must specify a VLAN.
Routing Protocol	Available only for 2-Box VRF. Select the routing protocol to use between the IPsec Aggregator and the PE. The options are BGP, EIGRP, OSPF, RIPv2, or Static route. If the routing protocol for the secured IGP differs from the routing protocol between the IPsec Aggregator and the PE, select the routing protocol for redistributing the routing to the secured IGP.
AS Number	Available only for 2-Box VRF with BGP or EIGRP routing. The number to use to identify the autonomous system (AS) area between the IPsec Aggregator and the PE. The AS number must be between 1 and 65535. If the routing protocol for the secured IGP differs from the routing protocol between the IPsec Aggregator and the PE, enter an AS number that identifies the secured IGP into which the routing will be redistributed from the IPsec Aggregator and the PE. This is relevant only if GRE or DMVPN are applied.
Process Number	Available only for 2-Box VRF with OSPF routing. The routing process ID number to use to configure the routing between the IPsec Aggregator and the PE. The process number must be between 1 and 65535.
OSPF Area ID	Available only for 2-Box VRF with OSPF routing. The ID number of the area in which the packet belongs. You can enter any number from 0 to 4294967295. **Note** All OSPF packets are associated with a single area, so all devices must have the same area ID number.

Table 33-3 IPsec Proposal Editor, Dynamic VTI/VRF Aware IPsec Tab (continued)

Element	Description
Redistribute Static Route	Available only for 2-Box VRF 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. **Note** If this check box is deselected and Enable Reverse Route Injection is enabled (default) for the IPsec proposal, static routes are still advertised in the routing protocol on the IPsec Aggregator.
Next Hop IP Address	Available only for 2-Box VRF with Static routing. The IP address of the provider edge device (or the interface that is connected to the IPSec aggregator).

Configuring High Availability in Remote Access VPNs (IOS)

Use the High Availability page to configure a High Availability (HA) policy on a Cisco IOS router or Cisco Catalyst switch in a remote access VPN.

In Security Manager, High Availability (HA) is supported by the creation of an HA group made up of two or more devices that use Hot Standby Routing Protocol (HSRP) to provide transparent, automatic device failover. By sharing a virtual IP address, the devices in the HA group present the appearance of a single virtual device or default gateway to the remote access users. One device in the HA group is always active and assumes the virtual IP address, while the others are standby devices. The devices in the group watch for hello packets from active and standby devices. If the active device becomes unavailable for any reason, a standby device takes ownership of the virtual IP address and takes over the remote access VPN. This transfer is seamless and transparent to remote access users.

Stateful SwitchOver (SSO) is used to ensure that state information is shared between the HSRP devices in the HA group. If a device fails, the shared state information enables the standby device to maintain IPsec sessions without having to re-establish the tunnel or renegotiate the security associations.

Tips

- When configuring an HA group, you must provide an inside virtual IP that matches the subnet of one of the interfaces on the device, in addition to a VPN virtual IP that matches the subnet of one of the device's interfaces and is configured with an IPsec proposal. See Configuring an IPsec Proposal on a Remote Access VPN Server (IOS, PIX 6.3 Devices), page 33-3.
- A remote access VPN server device on which HA is configured cannot be configured as a hub in a site-to-site VPN topology on which HA is configured, using the same outside interface that was used for the remote access VPN server.

Step 1 Do one of the following:

- (Device view) With an IOS device selected, select **Remote Access VPN > IPSec VPN > High Availability** from the Policy selector.
- (Policy view) Select **Remote Access VPN > IPSec VPN > High Availability** from the Policy Type selector. Select an existing policy or create a new one.

The High Availability page opens.

Step 2 Configure the options explained in the following table.

Table 33-4 High Availability Page, Remote Access VPNs

Element	Description
Inside Virtual IP	The IP address that is shared by the devices in the HA group and that represents the inside interface of the HA group. The virtual IP address must be on the same subnet as the inside interfaces of the devices in the HA group, but must not be identical to the IP address of any of these interfaces. You must provide an inside virtual IP that matches the subnet of one of the interfaces on the device, in addition to a VPN virtual IP that matches the subnet of one of the device's interfaces and is configured with an IPsec proposal. **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 is shared by the devices in the HA group and represents the VPN interface of the HA group. This IP address serves as the 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 device to the other devices in the group to indicate status and priority. The default is 5 seconds.
Hold Time	The duration in seconds (within the range of 2-255) that a standby device will wait to receive a hello message from the active device before concluding that the device is down. The default is 15 seconds.
Standby Group Number (Inside)	The standby number of the inside device interface that matches the internal virtual IP subnet for the devices in the HA group. The number must be within the range of 0-255. The default is 1.
Standby Group Number (Outside)	The standby number of the outside device interface that matches the external virtual IP subnet for the devices in the HA group. The number must be within the range of 0-255. The default is 2. **Note** The outside standby group number must be different to the inside standby group number.
Failover Server	The IP address or network/host policy object that identifies the inside interface of the remote peer failover servers. Enter the IP address or network/host object name, or click **Select** to select an object or to create a new object.
Enable Stateful Failover	Enables SSO for stateful failover. This option is always selected and you cannot deselect it for remote access VPNs.

Configuring User Group Policies

Use the User Groups (IOS/PIX 6.x) policy to specify user groups for your remote access IPSec VPN server. You can configure user groups on a Cisco IOS router, PIX 6.3 Firewall, or Catalyst 6500 /7600 device.

When you configure a remote access VPN server, you must create user groups to which remote clients will belong. A user group policy specifies the attributes that determine user access to and use of the VPN. User groups simplify system management, enabling you to quickly configure VPN access for large numbers of users.

For example, in a typical remote access VPN, you might allow a finance group to access one part of a private network, a customer support group to access another part, and an MIS group to access other parts. In addition, you might allow specific users within MIS to access systems that other MIS users cannot access. User group policies provide the flexibility to do so securely.

Remote clients must have the same group name as the user group configured on the VPN server so that they can connect to the device; otherwise, a connection cannot be established. When a remote client establishes a connection to the VPN server, the group policies for that user group are pushed to all clients belonging to the same user group. You can configure user groups on the local remote access VPN server and external AAA servers.

Notes

- You can also specify user groups using the Remote Access VPN Configuration Wizard. For more information, see Using the Remote Access VPN Configuration Wizard, page 30-13.
- To specify group policies for an SSL VPN on an IOS device, use the SSL VPN policy as explained in Configuring an SSL VPN Policy (IOS), page 33-14.

Related Topics

- Understanding Remote Access IPSec VPNs, page 30-2

Step 1 Do one of the following:

- (Device view) With an IOS router, Catalyst 6500/7600, or PIX 6.3 device selected, select **Remote Access VPN > IPSec VPN > User Groups (IOS/PIX 6.x)** from the Policy selector.
- (Policy view) Select **Remote Access VPN > IPSec VPN > User Groups (IOS/PIX6.x)** from the Policy Type selector. Select an existing policy or create a new one.

The User Groups page opens.

The page contains two lists: Available User Groups lists all existing User Group policy objects that are configured for remote access IPsec VPNS; Selected User Groups lists all of the User Group policy objects that will be configured on the device.

Step 2 Ensure that the list of selected user groups contains the desired User Group policy objects:

- To create a new User Group policy object, click the Create (+) button beneath the available user groups list to open the Add User Group dialog box. For instructions on creating the object, see Add or Edit User Group Dialog Box, page 34-73.

  After you create the group, it is added to the available list, and you must add it to the selected list if you want to use it.
- To add a User Group to the selected list, select it in the available list and click >>.
- To remove a User Group, select it in the selected list and click <<. If the group is already configured on the device, it will be removed during the next deployment.

- You can edit the properties of a User Group object by selecting it in either list and clicking the **Edit** button.

Configuring an SSL VPN Policy (IOS)

Use the SSL VPN policy to configure the SSL VPN connection policies for an IOS router. From this page, you can create, edit, or delete SSL VPN policies.

Related Topics

- Understanding Remote Access SSL VPNs, page 30-2
- Creating SSL VPNs Using the Remote Access VPN Configuration Wizard (IOS Devices), page 30-32
- Filtering Tables, page 1-48

Step 1 Do one of the following:

- (Device view) With an IOS device selected, select **Remote Access VPN > SSL VPN** from the Policy selector.
- (Policy view) Select **Remote Access VPN > SSL VPN > SSL VPN Policy (IOS)** from the Policy Type selector. Select an existing policy or create a new one.

The SSL VPN page appears.

The table lists all of the contexts that define the virtual configurations of the SSL VPN. Each context has a gateway, domain or virtual hostname, and user group policies. The status of the context is also shown, either In Service or Out of Service.

Step 2 Do either of the following:

- To add a context, click the **Add Row** button to open the SSL VPN Context Editor Dialog Box (IOS), page 33-15.
- To edit a context, select it and click the **Edit Row** button.

Note To delete a context, select it and click the **Delete Row** button.

Step 3 Configure at least the following general settings for the policy. For information on other fields, see General Tab, page 33-16.

- **Name, Domain**—For new policies, the name of the context that defines the virtual configuration of the SSL VPN. To simplify the management of multiple context configurations, make the context name the same as the domain or virtual hostname.
- **Gateway**—The SSL VPN gateway policy object that identifies the gateway device to which users will connect, including interface and port configuration. Click **Select** to select the object from a list or to create a new object.

  When you select the object, the Portal Page URL field shows the URL to which users connect.
- **Authentication Server Group**—A prioritized list of AAA server group objects that identify the AAA servers to use for authenticating users.

- **User Groups**— The user groups that will be used in your SSL VPN policy. User groups define the resources available to users when connecting to an SSL VPN gateway.

  To add a user group, click **Add Row** to open a list of existing user group policy objects from which you can select the group. If the desired group does not already exist, click the **Create** button below the available groups list and create it. For more information about user group objects, see Add or Edit User Group Dialog Box, page 34-73.

Step 4 Click the **Portal Page** tab and customize the design of the login page. You can customize the title, the logo graphic, the message that appears above the login prompt, and the background and text colors.

If you want to select a different graphic, you must first copy the graphic onto the Security Manager server. You cannot select it from your workstation's hard drive.

Step 5 Click the **Secure Desktop** tab to configure Cisco Secure Desktop (CSD) software. CSD policies define entry requirements for client systems and provide a single, secure location for session activity and removal on the client system, ensuring that sensitive data is shared only for the duration of an SSL VPN session.

If you want to use CSD, select **Enable Cisco Secure Desktop** and click **Select** to select a Secure Desktop Configuration policy object, which defines the rules you want to use to control VPN access and host scanning. You can create a new object from the selection list. For information about configuring these objects, see Creating Cisco Secure Desktop Configuration Objects, page 33-18.

Note You must install and activate the Secure Desktop Client software on a device for your configuration to work.

Step 6 Click the **Advanced** tab to configure a maximum number of simultaneous users for the context or if you are using VRF, the name of the VRF instance that is associated with the SSL VPN context.

Step 7 Click **OK** to save your changes.

SSL VPN Context Editor Dialog Box (IOS)

Use this dialog box to create or modify a context that defines the virtual configuration of an SSL VPN. For more information, see Configuring an SSL VPN Policy (IOS), page 33-14.

Navigation Path

Open the SSL VPN (IOS) policy, then click **Add Row (+)**, or select a context in the table and click **Edit Row**. For information on opening the SSL VPN policy, see Configuring an SSL VPN Policy (IOS), page 33-14.

Field Reference

Table 33-5 SSL VPN Context Editor Dialog Box

Element	Description
General tab	Defines the general settings required for an SSL VPN policy. General settings include specifying the gateway, domain, AAA servers for accounting and authentication, and user groups. For a description of the fields on this tab, see General Tab, page 33-16.

Table 33-5 SSL VPN Context Editor Dialog Box (continued)

Element	Description
Portal Page tab	Defines the design of the login page for the SSL VPN policy. The display box at the bottom of the tab changes to show you how your selections will look. You can configure: • Title—The text displayed at the top of the page. Control the color using the Primary settings in the Title Color and Text Color fields. • Logo—The graphic displayed next to the title. Select None, Default, or Custom. To configure a custom graphic, you must copy the desired graphic to the Security Manager server, then click **Browse** to select the file. Supported graphic types are GIF, JPG, and PNG, with a maximum size of 100 KB. • Login Message—The text displayed immediately above the login prompt. Control the color using the Secondary settings in the Title Color and Text Color fields.
Secure Desktop tab	Configures the Cisco Secure Desktop (CSD) software on the router. CSD policies define entry requirements for client systems and provide a single, secure location for session activity and removal on the client system, ensuring that sensitive data is shared only for the duration of an SSL VPN session. **Note** You must install and activate the Secure Desktop Client software on a device for your configuration to work. If you want to use CSD, select **Enable Cisco Secure Desktop** and click **Select** to select a Secure Desktop Configuration policy object, which defines the rules you want to use to control VPN access and host scanning. You can create a new object from the selection list. For information about configuring these objects, see Creating Cisco Secure Desktop Configuration Objects, page 33-18.
Advanced tab	Configures these additional settings: • Maximum Number of Users—The maximum number of SSL VPN user sessions allowed at one time, from 1-1000. • VRF Name—If Virtual Routing Forwarding (VRF) is configured on the device, the name of the VRF instance that is associated with the SSL VPN context. For information about VRF, see Understanding VRF-Aware IPsec, page 25-14.

General Tab

Use the General tab of the SSL VPN Context Editor dialog box to define or edit the general settings required for an SSL VPN policy. General settings include specifying the gateway, domain, AAA servers for accounting and authentication, and user groups.

Navigation Path

Open the SSL VPN Context Editor Dialog Box (IOS), page 33-15, then click the **General** tab.

Related Topics

- Configuring an SSL VPN Policy (IOS), page 33-14
- Add or Edit SSL VPN Gateway Dialog Box, page 34-64
- Understanding AAA Server and Server Group Objects, page 6-27

Field Reference

Table 33-6 SSL VPN Context Editor General Tab (IOS)

Element	Description
Enable SSL VPN	Whether to activate the SSL VPN connection, putting it "In Service".
Name	The name of the context that defines the virtual configuration of the SSL VPN. **Note** To simplify the management of multiple context configurations, make the context name the same as the domain or virtual hostname.
Gateway	The name of the SSL VPN gateway policy object that defines the characteristics of the gateway to which users connect when entering the VPN. A gateway object provides the interface and port configuration for an SSL VPN connection. Enter the name of the object or click **Select** to select it from a list or to create a new object.
Domain	The domain or virtual hostname of the SSL VPN connection.
Portal Page URL	The URL for the SSL VPN, which is filled in when you select a gateway object. Users connect to this URL to enter the VPN.
Authentication Server Group	The authentication server groups. The list is in prioritized order. Authentication is attempted using the first group and proceeds through the list until the user is successfully authenticated or denied. Use the LOCAL group if the users are defined on the gateway itself. Enter the names of the AAA server groups; separate multiple entries with commas. You can click **Select** to select the groups or to create new ones.
Authentication Domain	A list or method for SSL VPN remote user authentication. If you do not specify a list or method, the gateway uses global AAA parameters for remote-user authentication.
Accounting Server Group	The accounting server group. Enter the name of the AAA server group policy object, or click **Select** to select it from a list or to create a new object.

Table 33-6 SSL VPN Context Editor General Tab (IOS) (continued)

Element	Description
User Groups	The user groups that will be used in your SSL VPN policy. User groups define the resources available to users when connecting to an SSL VPN gateway. The table shows whether full client, CIFS file access, and thin client is enabled for the group. • To add a user group, click **Add Row** to open a list of existing user group policy objects from which you can select the group. If the desired group does not already exist, click the **Create** button below the available groups list and create it. For more information about user group objects, see Add or Edit User Group Dialog Box, page 34-73. • To edit a user group, select it and click the **Edit Row** button. • To delete a user group, select it and click the **Delete Row** button. This deletes the group only from the policy, it does not delete the user group policy object.

Creating Cisco Secure Desktop Configuration Objects

Cisco Secure Desktop (CSD) Configuration objects define the settings you want to use if you enable Secure Desktop in an SSL VPN policy for an IOS device (see Configuring an SSL VPN Policy (IOS), page 33-14). For ASA devices, the feature is set up as part of the Dynamic Access Policy (see Understanding Dynamic Access Policies, page 32-1 and Configuring Cisco Secure Desktop Policies on ASA Devices, page 32-9).

Cisco Secure Desktop (CSD) provides a reliable means of eliminating all traces of sensitive data by providing a single, secure location for session activity and removal on the client system. CSD provides a session-based interface where sensitive data is shared only for the duration of an SSL VPN session. All session information is encrypted, and all traces of the session data are removed from the remote client when the session is terminated, even if the connection terminates abruptly.

About Windows Locations

Windows locations let you determine how clients connect to your virtual private network, and protect it accordingly. For example, clients connecting from within a workplace LAN on a 10.x.x.x network behind a NAT device are an unlikely risk for exposing confidential information. For these clients, you might set up a CSD Windows Location named Work that is specified by IP addresses on the 10.x.x.x network, and disable both the Cache Cleaner and the Secure Desktop function for this location.

In contrast, users' home PCs might be considered more at risk to viruses due to their mixed use. For these clients, you might set up a location named Home that is specified by a corporate-supplied certificate that employees install on their home PCs. This location would require the presence of antivirus software and specific, supported operating systems to grant full access to the network.

Alternatively, for untrusted locations such as Internet cafes, you might set up a location named "Insecure" that has no matching criteria (thus making it the default for clients that do not match other locations). This location would require full Secure Desktop functions, and include a short timeout period to prevent access by unauthorized users. If you create a location and do not specify criteria, make sure it is the last entry in the Locations list.

Related Topics

- Cisco Secure Desktop on IOS Configuration Example Using SDM, http://www.cisco.com/en/US/products/ps6496/products_configuration_example09186a008072aa7b.shtml
- Setting Up CSD for Microsoft Windows Clients, http://www.cisco.com/en/US/docs/security/csd/csd311/csd_for_vpn3k_cat6k/configuration/guide/CSDwin.html
- Creating Policy Objects, page 6-9

Step 1 Select **Manage > Policy Objects** to open the Policy Object Manager (see Policy Object Manager, page 6-4).

Step 2 Select **Cisco Secure Desktop Configuration** from the Object Type selector.

Step 3 Right-click in the work area and select **New Object** to open the Add or Edit Secure Desktop Configuration Dialog Box, page 34-35.

Step 4 Enter a name for the object and optionally a description of the object.

Step 5 Select **Windows Location Settings** to create locations (such as Work, Home, or Insecure), and define the location-based settings (also called adaptive policies) for CSD.

a. For each location you want to configure, enter its name in the **Location to Add** field and click **Add** to move it to the Locations field. You can reorder the locations using the Move Up and Move Down buttons. When users connect, these locations are evaluated in order and the first one that matches is used to define the policies for the user.

   When you add a location, a folder for the location is added to the table of contents. The folder and its subfolders define the policies for the location.

b. If you want all the open browser windows to close after the Secure Desktop installation, make sure to select the corresponding check box.

c. Select the required check boxes to configure a VPN Feature policy that enables web browsing, file access, port forwarding, and full tunneling, if installation or location matching fails.

Step 6 Select the folders and subfolders for the Windows locations you added and configure their settings. For detailed information about these settings, see *Setting Up CSD for Microsoft Windows Clients* at http://www.cisco.com/en/US/docs/security/csd/csd311/csd_for_vpn3k_cat6k/configuration/guide/CSDwin.html.

Step 7 Select **Windows CE** to configure a VPN feature policy to enable or restrict web browsing and remote server file access for remote clients running Microsoft Windows CE.

Step 8 Select **Mac and Linux Cache Cleaner** to configure the Cache Cleaner and a VPN Feature Policy for these clients, such as enabling or restricting web browsing, remote server file access, and port forwarding.

Step 9 (Optional) Under Category, select a category to help you identify this object in the Objects table. See Using Category Objects, page 6-13.

Step 10 Click **OK** to save the object.
