Easy VPN

Easy VPN is a hub-and-spoke VPN topology that can be used with a variety of routers, PIX, and ASA devices. Policies are defined mostly on the hub and pushed to remote spoke VPN devices, ensuring that clients have up-to-date policies in place before establishing a secure connection.

This chapter contains the following topics:

- Understanding Easy VPN , on page 1
- Configuring Client Connection Characteristics for Easy VPN , on page 7
- Configuring an IPsec Proposal for Easy VPN , on page 10
- Configuring a Connection Profile Policy for Easy VPN , on page 14
- Configuring a User Group Policy for Easy VPN , on page 15

Understanding Easy VPN

Easy VPN simplifies VPN deployment for remote offices. With Easy VPN, security policies defined at the head end are pushed to remote VPN devices, ensuring that clients have up-to-date policies in place before establishing a secure connection.

Security Manager supports the configuration of Easy VPN policies on hub-and-spoke VPN topologies. In such a configuration, most VPN parameters are defined on the Easy VPN server, which acts as the hub device. The centrally managed IPsec policies are pushed to the Easy VPN client devices by the server, minimizing the remote (spoke) devices configuration.

The Easy VPN Server can be a Cisco IOS router, a PIX Firewall, or an ASA 5500 series device. The Easy VPN client is supported on PIX 501, 506, 506E Firewalls running PIX 6.3, Cisco 800-3900 Series routers, and ASA 5505 devices running ASA Software release 7.2 or later.

Beginning with version 4.17, Cisco Security Manager provides Easy VPN support with BVI. Typically, Easy VPN determines the highest and lowest security level interfaces during ASA startup. The lowest security level interface is used as the External interface on which vpn client initiates tunnel to the head-end, and highest security level interface is used as Internal Secured interface.

On ASA5506 platform, the default configuration includes BVI with highest security level interface 100 with security level of its member interfaces also set at level 100, along with an external interface with security level 0 (zero). VPN client rejects two or more interfaces having same highest security level. Easy VPN determines that there are more than two interfaces with same highest security level and hence vpn client is not enabled.

In order to overcome this issue, vpnclient secure interface CLI was introduced for all ASA 5506, 5508, and 5512 [x/h/w] devices from ASA 9.9(2) onwards. Thus, to support the CLI in Cisco Security Manager, starting from version 4.17, a new component “VPN Client Interface” is introduced in Hub & Spoke Topology of type (Easy VPN).

Note Some of the policies used in Easy VPN topologies are similar to those used in remote access VPNs. In remote access VPNs, policies are configured between servers and mobile remote PCs running VPN client software, whereas, in site-to-site Easy VPN topologies, the clients are hardware devices.

This section contains the following topics:

- Easy VPN with Dial Backup , on page 2
- Easy VPN with High Availability , on page 3
- Easy VPN with Dynamic Virtual Tunnel Interfaces , on page 3
- Easy VPN Configuration Modes , on page 4
- Easy VPN and IKE Extended Authentication (Xauth) , on page 4
- Overview of Configuring Easy VPN , on page 6
- Important Notes About Easy VPN Configuration , on page 7

Easy VPN with Dial Backup

Dial backup for Easy VPN allows you to configure a dial backup tunnel connection on your remote client device. The backup feature is activated only when real traffic is ready to be sent, eliminating the need for expensive dialup or ISDN links that must be created and maintained even when there is no traffic.

Note Easy VPN dial backup can be configured only on remote clients that are routers running IOS version 12.3(14)T or later.

In an Easy VPN configuration, when a remote device attempts to connect to the server and the tracked IP is no longer accessible, the primary connection is torn down and a new connection is established over the Easy VPN backup tunnel to the server. If the primary hub cannot be reached, the primary configuration switches to the failover hub with the same primary configuration and not to the backup configuration.

Only one backup configuration is supported for each primary Easy VPN configuration. Each inside interface must specify the primary and backup Easy VPN configuration. IP static route tracking must be configured for dial backup to work on an Easy VPN remote device. The object tracking configuration is independent of the Easy VPN remote dial backup configuration. The object tracking details are specified in the spoke’s Edit Endpoints dialog box.

For more information about dial backup, see Configuring Dial Backup.

Easy VPN with High Availability

You can configure High Availability (HA) on devices in an Easy VPN topology. High Availability provides automatic device backup when configured on Cisco IOS routers or Catalyst 6500/7600 devices that run IP over LANs. You can create an HA group made up of two or more hub devices in your Easy VPN that use Hot Standby Routing Protocol (HSRP) to provide transparent, automatic device failover. For more information, see Configuring High Availability in Your VPN Topology.

Easy VPN with Dynamic Virtual Tunnel Interfaces

The IPsec virtual tunnel interface (VTI) feature simplifies the configuration of GRE tunnels that need to be protected by IPsec for remote access links. A VTI is an interface that supports IPsec tunneling, and allows you to apply interface commands directly to the IPsec tunnels. The configuration of a virtual tunnel interface reduces overhead as it does not require a static mapping of IPsec sessions to a particular physical interface where the crypto map is applied.

IPsec VTIs support both unicast and multicast encrypted traffic on any physical interface, such as in the case of multiple paths. Traffic is encrypted or decrypted when it is forwarded from or to the tunnel interface and is managed by the IP routing table. Dynamic or static IP routing can be used to route the traffic to the virtual interface. Using IP routing to forward traffic to the tunnel interface simplifies IPsec VPN configuration compared to the more complex process of using access control lists (ACLs) with a crypto map. Dynamic VTIs function like any other real interface so that you can apply quality of service (QoS), firewall, and other security services as soon as the tunnel is active.

Dynamic VTIs use a virtual template infrastructure for dynamic instantiation and management of IPsec interfaces. In an Easy VPN topology, Security Manager implicitly creates the virtual template interface for the device. If the device is a hub, the user must provide the IP address on the hub that will be used as the virtual template interface—this can be a subnet (pool of addresses) or an existing loopback or physical interface. On a spoke, the virtual template interface is created without an IP address.

In Security Manager, you configure Dynamic VTI in the Easy VPN IPsec Proposal page. See Configuring Dynamic VTI for Easy VPN , on page 13.

Notes

- Dynamic VTI can be configured only in a hub-and-spoke Easy VPN topology on routers running IOS version 12.4(2)T and later, except 7600 devices. It is not supported on PIX Firewalls, ASA devices, or Catalyst 6000 series switches.
- Not all the hubs/spokes require Dynamic VTI configuration during discovery or provision. You can extend the existing Easy VPN topology (including routers not supporting dVTI) to add routers that support dVTI.
- Dynamic VTI is supported on only servers, only clients (if server does not support dVTI), or both clients and servers.
- You cannot configure High Availability on hubs/servers that have been configured with dVTI.
- You can also configure Dynamic VTI in remote access VPNs. For more information, see Configuring Dynamic VTI/VRF Aware IPsec in Remote Access VPNs (IOS Devices).

Easy VPN Configuration Modes

Easy VPN can be configured in three modes—Client, Network Extension, and Network Extension Plus.

- Client mode—The default configuration that allows devices at the client site to access resources at the central site, but disallows access to the central site for resources at the client site. In client mode, a single IP address is pushed to the remote client from the server when the VPN connection is established. This address is typically a routable address in the private address space of the customer network. All traffic passing across the Easy VPN tunnel undergoes Port Address Translation (PAT) to that single pushed IP address.
- Network Extension mode—Allows users at the central site to access the network resources at the client site, and allows the client PCs and hosts direct access to the PCs and hosts at the central site. Network Extension mode specifies that the hosts at the client end of the VPN tunnel should be given IP addresses that are fully routable and reachable by the destination network. The devices at both ends of the connection will form one logical network. PAT is not used, so the hosts at the client end have direct access to the hosts at the destination network. In other words, the Easy VPN server (the hub) gives routable addresses to the Easy VPN client (the spoke), while the whole LAN behind the client will not undergo PAT.
- Network Extension Plus mode—An enhancement to Network Extension mode, which can be configured only on IOS routers. It enables an IP address that is received via mode configuration to be automatically assigned to an available loopback interface. This IP address can be used for connecting to your router for remote management and troubleshooting (ping, Telnet, and Secure Shell). If you select this option an some clienx`ts are not IOS routers, those clients are configured in Network Extension mode.

Note All modes of operation can also support split tunneling, which allows secure access to corporate resources through the VPN tunnel while also allowing Internet access through a connection to an ISP or other service (thereby eliminating the corporate network from the path for web access).

You configure the mode in the Client Connection Characteristics policy as described in Configuring Client Connection Characteristics for Easy VPN , on page 7.

Related Topics

- Important Notes About Easy VPN Configuration , on page 7
- Understanding Easy VPN , on page 1

Easy VPN and IKE Extended Authentication (Xauth)

When negotiating tunnel parameters for establishing IPsec tunnels in an Easy VPN configuration, IKE Extended Authentication (Xauth) adds another level of authentication that identifies the user who requests the IPsec connection. If the VPN server is configured for Xauth, the client waits for a username/password challenge after the IKE security association (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.

The information that is entered is checked against authentication entities using authentication, authorization, and accounting (AAA) protocols such as RADIUS and TACACS+. Token cards may also be used via AAA proxy. During Xauth, a user-specific attribute can be retrieved if the credentials of that user are validated via RADIUS.

Note VPN servers that are configured to handle remote clients should always be configured to enforce user authentication.

Security Manager allows you to save the Xauth username and password on the device itself so you do not need to enter these credentials manually each time the Easy VPN tunnel is established. The information is saved in the device's configuration file and used each time the tunnel is established. Saving the credentials in the device's configuration file is typically used if the device is shared between several PCs and you want to keep the VPN tunnel up all the time, or if you want the device to automatically bring up the tunnel whenever there is traffic to be sent.

Saving the credentials in the device's configuration file, however, could create a security risk, because anyone who has access to the device configuration can obtain this information. An alternative method for Xauth authentication is to manually enter the username and password each time Xauth is requested. You can select whether to use a web browser window or the router console to enter the credentials. Using web-based interaction, a login page is returned, in which you can enter the credentials to authenticate the VPN tunnel. After the VPN tunnel comes up, all users behind this remote site can access the corporate LAN without being prompted again for the username and password. Alternatively, you can choose to bypass the VPN tunnel and connect only to the Internet, in which case a password is not required.

Easy VPN Tunnel Activation

If the device credentials (Xauth username and password) are stored on the device itself, you must select a tunnel activation method for IOS router clients. Two options are available:

- Auto—The Easy VPN tunnel is established automatically when the Easy VPN configuration is delivered to the device configuration file. If the tunnel times out or fails, the tunnel automatically reconnects and retries indefinitely. This is the default option.
- Traffic Triggered Activation—The Easy VPN tunnel is established whenever outbound local (LAN side) traffic is detected. Traffic Triggered Activation is recommended for use with the Easy VPN dial backup configuration so that backup is activated only when there is traffic to send across the tunnel. When using this option, you must specify the Access Control List (ACL) that defines the "interesting" traffic.

Note Manual tunnel activation is configured implicitly if you select to configure the Xauth password interactively. In this case, the device waits for a command before attempting to establish the Easy VPN remote connection. When the tunnel times out or fails, subsequent connections will also have to wait for the command.

You configure the xauth and tunnel activation mode in the Client Connection Characteristics policy as described in Configuring Client Connection Characteristics for Easy VPN , on page 7.

Related Topics

- Important Notes About Easy VPN Configuration , on page 7
- Understanding Easy VPN , on page 1
- Configuring Credentials Policy Objects , on page 9

Overview of Configuring Easy VPN

When a remote client initiates a connection to a VPN server, device authentication between the peers occurs using IKE, followed by user authentication using IKE Extended Authentication (Xauth), VPN policy push (in Client, Network Extension, or Network Extension Plus mode), and IPsec security association (SA) creation.

The following provides an overview of this process:

1. The client initiates IKE Phase 1 via aggressive mode if a preshared key is to be used for authentication, or main mode if digital certificates are used. If the client identifies itself with a preshared key, the accompanying user group name (defined during configuration) is used to identify the group profile associated with this client. If digital certificates are used, the organizational unit (OU) field of a distinguished name (DN) is used to identify the user group name. See PKI Enrollment Dialog Box—Certificate Subject Name Tab.

Note Because the client may be configured for preshared key authentication, which initiates IKE aggressive mode, the administrator should change the identity of the VPN device via the crypto isakmp identity hostname command. This will not affect certificate authentication via IKE main mode.

1. The client attempts to establish an IKE SA between its public IP address and the public IP address of the VPN server. To reduce the amount of manual configuration on the client, every combination of encryption and hash algorithms, in addition to authentication methods and D-H group sizes, is proposed.
2. Depending on its IKE policy configuration, the VPN server determines which proposal is acceptable to continue negotiating Phase 1.

Note Device authentication ends and user authentication begins at this point.

1. After the IKE SA is successfully established, and if the VPN server is configured for Xauth, the client waits for a “username/password” challenge and then responds to the challenge of the peer. The information that is entered is checked against authentication entities using authentication, authorization, and accounting (AAA) protocols such as RADIUS and TACACS+. Token cards may also be used via AAA proxy. During Xauth, a user-specific attribute can be retrieved if the credentials of that user are validated via RADIUS.

Note VPN servers that are configured to handle remote clients should always be configured to enforce user authentication.

1. If the server indicates that authentication was successful, the client requests further configuration parameters from the peer. The remaining system parameters (for example, IP address, DNS, and split tunnel attributes) are pushed to the client using client or network extension mode configuration.

Note The IP address pool and group preshared key (if Rivest, Shamir, and Adelman [RSA] signatures are not being used) are the only required parameter in a group profile. All other parameters are optional.

1. After each client is assigned an internal IP address via mode configuration, Reverse Route Injection (RRI), if configured, ensures that a static route is created on the device for each client internal IP address.
2. IKE quick mode is initiated to negotiate and create IPsec SAs.

The connection is complete.

Important Notes About Easy VPN Configuration

Before you configure an Easy VPN policy in your topology, you should know the following:

- In an Easy VPN topology configuration, deployment fails if a 72xx series router is used as a remote client device. The Easy VPN client is supported on PIX 501, 506, 506E Firewalls running PIX 6.3, Cisco 800-3900 Series routers, and ASA 5505 devices running ASA Software release 7.2 or later.
- If you try to configure a Public Key Infrastructure (PKI) policy on a PIX 6.3 remote client in an Easy VPN topology configuration, deployment fails. For successful deployment on this device, you must first issue the PKI certificate on the CA server, and then try again to deploy the device. For more information about PKI policies, see Understanding Public Key Infrastructure Policies.
- In some cases, deployment fails on a device that serves as an Easy VPN client if the crypto map is configured on the NAT (or PAT) internal interface instead of the external interface. On some platforms, the inside and outside interfaces are fixed. For example, on a Cisco 1700 series router the VPN interface must be the device's FastEthernet0 interface. On a Cisco 800 series router the VPN interface could be either the device's Ethernet0 or Dialer1 interface, depending on the configuration. On a Cisco uBR905/uBR925 cable access router, the VPN interface must be the Ethernet0 interface.

Configuring Client Connection Characteristics for Easy VPN

Use the Client Connection Characteristics page to specify how traffic will be routed in the Easy VPN topology and how the VPN tunnel will be established. The characteristics defined in this policy are configured on the remote clients. Before configuring this policy, read the following topics:

- Easy VPN Configuration Modes , on page 4
- Easy VPN and IKE Extended Authentication (Xauth) , on page 4

Navigation Path

- (Site-to-Site VPN Manager Window) Select an Easy VPN topology in the VPNs selector, then select **Client Connection Characteristics** in the Policies selector.
- (Policy view) Select **Site-to-Site VPN > Client Connection Characteristics** and create a new policy or edit an existing policy.

Related Topics

- Understanding Easy VPN , on page 1
- Creating Access Control List Objects
- Important Notes About Easy VPN Configuration , on page 7

Field Reference

Table 1: Easy VPN Client Connection Characteristics Page

Element	Description
Mode	The configuration mode for the remote devices: • **Client**—Specifies that all traffic from the remote client's inside network will undergo Port Address Translation (PAT) to a single IP address which was assigned for the device by the head end server at connect time. • **Network Extension**—Specifies that PCs and other hosts at the client end of the VPN tunnel should be given IP addresses that are fully routable and reachable by destination network. PAT is not used, allowing the client PCs and hosts to have direct access to the PCs and hosts at the destination network. • **Network Extension Plus**—An enhancement to Network Extension mode, that enables an IP address that is received via mode configuration to be automatically assigned to an available loopback interface. The IPsec SAs for this IP address are automatically created by the Easy VPN client. The IP address is typically used for troubleshooting (using ping, Telnet, and Secure Shell). If you select Network Extension Plus, this mode is configured on IOS routers only. Clients that are PIX or ASA devices are configured in Network Extension mode. For more information, see Easy VPN Configuration Modes , on page 4.
Xauth Credentials Source	Select how you want to enter the Xauth credentials for user authentication when you establish a VPN connection with the server: • Device Stored Credentials (default)—The username and password are saved on the device itself in the device's configuration file to be used each time the tunnel is established. • Interactive Entered Credentials—Enables you to manually enter the username and password each time Xauth is requested, in a web browser window or from the router console. For more information, see Easy VPN and IKE Extended Authentication (Xauth) , on page 4.
Xauth Credentials	Available only if you selected **Device Stored Credentials** as the Xauth Credentials Source. The credentials policy object that defines the default Xauth credentials. Enter the name of the object or click **Select** to select it from a list or to create a new object. For more information, see Configuring Credentials Policy Objects , on page 9. **Note** If you want to configure different Xauth credentials on your remote client, you must configure the credentials policy object to allow overrides (select **Allow Value Override per Device** in the object definition).

Element	Description
Tunnel Activation (IOS)	Available only if you selected the **Device Stored Credentials** option for the Xauth password source. For IOS router clients, select a tunnel activation method: • **Auto** (default)—The Easy VPN tunnel is established automatically when the Easy VPN configuration is delivered to the device configuration file. If the tunnel times out or fails, the tunnel automatically reconnects and retries indefinitely. • **Traffic Triggered Activation**—The Easy VPN tunnel is established whenever outbound local (LAN side) traffic is detected. If you select traffic triggered activation, also enter the name of the Access Control List (ACL) policy object that defines the traffic that should activate the tunnel. Click **Select** to select the object or to create a new object. Traffic Triggered Activation is recommended for use when Easy VPN dial backup is configured so that backup is activated only when there is traffic to send across the tunnel. **Note** Manual tunnel activation is configured implicitly when you select to configure the Xauth password interactively.
User Authentication Method (IOS)	Available only if you selected the **Interactive Entered Credentials** option for the Xauth credentials source. The option applies to remote IOS routers only. Select one of these ways to enter the Xauth username and password interactively each time Xauth authentication is requested: • Web Browser (default)—Manually in a web browser window. • Router Console—Manually from the router's command line.

Configuring Credentials Policy Objects

Use the Credentials dialog box to create, copy and edit Credential objects.

Credential objects are used in Easy VPN configuration during IKE Extended Authentication (Xauth) when authenticating user access to the network and network services. When negotiating tunnel parameters for establishing IPsec tunnels in an Easy VPN configuration, Xauth identifies the user who requests the IPsec connection. If the VPN server is configured for Xauth, 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. You can save the Xauth credentials (username and password) on the device itself so you do not need to enter them manually each time the Easy VPN tunnel is established.

Navigation Path

Select **Manage > Policy Objects**, then select **Credentials** from the Object Type Selector. Right-click inside the work area and select **New Object** or right-click a row and select **Edit Object**.

Related Topics

- Easy VPN and IKE Extended Authentication (Xauth) , on page 4
- Configuring Client Connection Characteristics for Easy VPN , on page 7
- Policy Object Manager

Field Reference

Table 2: Credentials Dialog Box

Element	Description
Name	The object name, which can be up to 128 characters. Object names are not case-sensitive. For more information, see Creating Policy Objects.
Description	An optional description of the object (up to 1024 characters).
Username	The name that will be used to identify the user during Xauth authentication.
Password Confirm	The password for the user, entered in both fields. The password must be alphanumeric and a maximum of 128 characters. Spaces are not allowed.
Category	The category assigned to the object. Categories help you organize and identify rules and objects. See Using Category Objects.
Allow Value Override per Device Overrides Edit button	Whether to allow the object definition to be changed at the device level. For more information, see Allowing a Policy Object to Be Overridden and Understanding Policy Object Overrides for Individual Devices. If you allow device overrides, you can click the **Edit** button to create, edit, and view the overrides. The **Overrides** field indicates the number of devices that have overrides for this object.

Configuring an IPsec Proposal for Easy VPN

Use the Easy VPN IPsec Proposal page to configure the IPsec proposal used during IKE Phase 2 negotiations for Easy VPN topologies. The IPsec proposal is configured on the IPSec Proposal tab; the options are described below.

In Easy VPN topologies, you can also configure a dynamic virtual interface on the Dynamic VTI tab. For an explanation of dVTI configuration, see Configuring Dynamic VTI for Easy VPN , on page 13 .

Note This topic describes the IPsec Proposal page when the site-to-site VPN technology is Easy VPN. For a description of the IPsec Proposal page when the site-to-site VPN technology is something else, see Configuring IPsec Proposals in Site-to-Site VPNs .

Navigation Path

- (Site-to-Site VPN Manager Window) Select an Easy VPN topology in the VPNs selector, then select **Easy VPN IPsec Proposal** in the Policies selector. Click the **IPSec Proposal** tab.
- (Policy view) Select **Site-to-Site VPN > Easy VPN IPsec Proposal** from the Policy Types selector. Select an existing shared policy or create a new one. Click the **IPSec Proposal** tab.

Related Topics

- Understanding Easy VPN , on page 1
- Configuring an IPsec Proposal for Easy VPN , on page 10
- Understanding AAA Server and Server Group Objects
- Understanding IPsec Proposals

Field Reference

Table 3: Easy VPN IPsec Proposal Tab

Element	Description
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 11 transform sets. For more information, see Understanding Transform Sets. Transform sets may use only tunnel mode IPsec operation. 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.

Element	Description
Reverse Route	Supported on ASA 5500 series devices, PIX 7.0+ devices, and Cisco IOS routers except 7600 devices. 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. Select one of the following options to configure RRI on the crypto map: • **None**—Disables the configuration of RRI on the crypto map. • **Standard**—(ASA, PIX 7.0+, IOS devices) Creates routes based on the destination information defined in the crypto map access control list (ACL). This is the default option. • **Remote Peer**—(IOS devices only) 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**—(IOS devices only) 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.
Enable Network Address Translation Traversal	Supported on PIX 7.0+ and ASA 5500 series devices. Whether to allow Network Address Translation (NAT) traversal. Use NAT traversal when there is a device between a VPN-connected hub and spoke, and that performs Network Address Translation (NAT) on the IPsec traffic. For information about NAT traversal, see Understanding NAT in VPNs.
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. 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.

Element	Description
User Authentication (Xauth)/AAA Authentication Method	Supported on Cisco IOS routers and PIX 6.3 firewalls only. The AAA or Xauth user authentication method used to define the order in which user accounts are searched. Xauth allows all 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. After the IKE SA is successfully established, and if the device is configured for Xauth, the client waits for a username/password challenge and then responds to the challenge of the peer. The information that is entered is checked against authentication entities using authentication, authorization, and accounting (AAA) protocols such as RADIUS and TACACS+. 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.

Configuring Dynamic VTI for Easy VPN

Use the Dynamic VTI tab of the Easy VPN IPSec Proposal policy to configure a dynamic virtual tunnel interface on a device in a hub-and-spoke Easy VPN topology. For more information, see Easy VPN with Dynamic Virtual Tunnel Interfaces , on page 3.

Note Dynamic VTI can be configured only on IOS routers running IOS version 12.4(2)T and later, except 7600 devices.

Navigation Path

- (Site-to-Site VPN Manager Window) Select an Easy VPN topology in the VPNs selector, then select **Easy VPN IPsec Proposal** in the Policies selector. Click the **Dynamic VTI** tab.
- (Policy view) Select **Site-to-Site VPN > Easy VPN IPsec Proposal** from the Policy Types selector. Select an existing shared policy or create a new one. Click the **Dynamic VTI** tab.

Related Topics

- Understanding Easy VPN , on page 1
- Configuring an IPsec Proposal for Easy VPN , on page 10

Field Reference

Table 4: Easy VPN IPSec Proposal, Dynamic VTI Tab

Element	Description
Enable Dynamic VTI	When selected, enables Security Manager to implicitly create a dynamic virtual template interface on the device. If the device is a hub server that does not support Dynamic VTI, a warning message is displayed, and a crypto map is deployed without dynamic VTI. In the case of a client device, an error message is displayed.
Virtual Template IP	If you are configuring Dynamic VTI on a hub in the topology, specify either the subnet address or interface role: • **Subnet**—To use the IP address taken from a pool of addresses. Enter the private IP address including the subnet mask, for example 10.1.1.0/24. • **Interface Role**—To use a physical or loopback interface on the device. If required, click **Select** to open the Interface selector where you can select the interface role object that identifies the desired interface. If an appropriate object does not already exist, you can create one in the selection dialog box. If you are configuring Dynamic VTI on a spoke in the topology, select **None**.

Configuring a Connection Profile Policy for Easy VPN

A connection profile consists of a set of records that contain IPsec tunnel connection policies. Connection profiles, or tunnel groups, identify the group policy for a specific connection, and include user-oriented attributes. If you do not assign a particular group policy to a user, the default group policy for the connection applies. For a successful connection, the username of the remote client must exist in the database, otherwise the connection is denied.

In site-to site VPNs, you configure connection profile policies on an Easy VPN server, which can be a PIX Firewall version 7.0+ or an ASA 5500 series device. The Easy VPN connection profile policy is similar to the one used for remote access VPNs.You can unassign the connection profile policy if none of the Easy VPN servers are ASA or PIX 7.0+ devices.

Creating a connection profile policy involves specifying:

- The group policy—A collection of user-oriented attributes stored either internally on the device or externally on RADIUS/LDAP server.
- Global AAA settings—Authentication, Authorization, and Accounting servers.
- The DHCP servers to be used for client address assignment, and the address pools from which the IP addresses will be assigned.
- Settings for Internet Key Exchange (IKE) and IPsec (such as preshared key).

On the PIX7.0+/ASA Connection Profiles page, you can connection profiles on your Easy VPN server.

Related Topics

- Creating or Editing VPN Topologies
- Understanding IPsec Technologies and Policies
- Understanding Easy VPN , on page 1

Procedure

Step 1 Do one of the following:

- (Site-to-Site VPN Manager Window) Select an Easy VPN topology in the VPNs selector, then select **Connection Profiles (PIX 7.0/ASA)** in the Policies selector.
- (Policy view) Select **Site-to-Site VPN > Connection Profiles (PIX 7.0/ASA)** from the Policy Types selector. Select an existing shared policy or create a new one.

For information on the policy, see Connection Profiles Page.

Step 2 On the **General** tab, specify the connection profile name and group policies and select which method (or methods) of address assignment to use. For a description of the available properties, see General Tab (Connection Profiles).

Step 3 Click the **AAA** tab and specify the AAA authentication parameters for an the connection profile. For a description of the elements on the tab, see AAA Tab (Connection Profiles).

Step 4 Click the **IPsec** tab and specify IPsec and IKE parameters for the connection profile. For a description of the elements on the tab, see IPSec Tab (Connection Profiles).

Configuring a User Group Policy for Easy VPN

Use the User Group Policy page to create or edit a user group policy on your Easy VPN server. When you configure an Easy VPN server, you create a user group to which remote clients belong. An Easy VPN user group policy can be configured on a Cisco IOS security router, PIX 6.3 Firewall, or Catalyst 6500 /7600 device. You can unassign the user group policy if none of the Easy VPN servers are IOS routers, Catalyst 6500/7600 devices, or PIX 6.3 firewalls.

Remote clients must have the same group name as the user group configured on the server in order to connect to the device, otherwise no connection is established. 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.

Select the user group policy object that you want to use in the policy from the Available User Groups list. You can create a new user group object by clicking the **Create (+)** button, or edit an existing group by selecting it and clicking the **Edit (pencil icon)** button. For information about configuring the user group object, see Add or Edit User Group Dialog Box.

Navigation Path

- (Site-to-Site VPN Manager Window) Select an Easy VPN topology in the VPNs selector, then select **User Group Policy** in the Policies selector.
- (Policy view) Select **Site-to-Site VPN > User Group Policy** from the Policy Types selector. Select an existing shared policy or create a new one.

Related Topics

- Understanding Easy VPN , on page 1