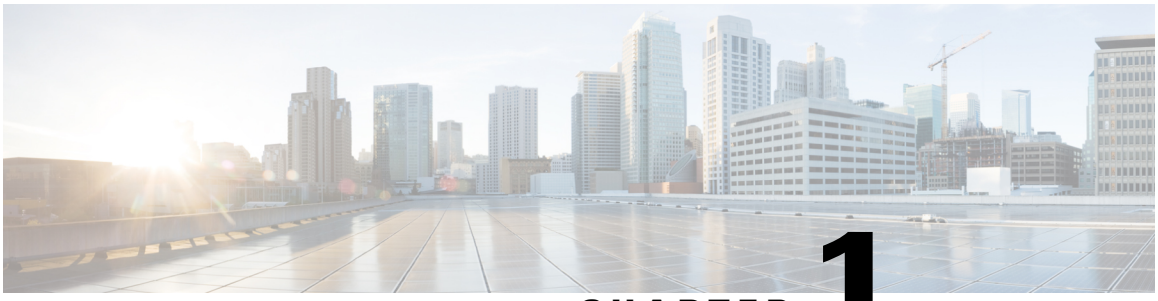
Easy VPN Configuration Guide, Cisco IOS Release 15S

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

CONTENTS



CHAPTER 1

Cisco Easy VPN Remote

This module provides information on configuring and monitoring the Cisco Easy VPN Remote feature to create IPsec VPN tunnels between a supported device and an Easy VPN server (Cisco IOS router, VPN 3000 concentrator, or Cisco PIX Firewall).

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table at the end of this module.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Prerequisites for Cisco Easy VPN Remote

Cisco Easy VPN Remote Feature

- A Cisco 800 series router running Cisco IOS Release 12.2(15)T, 12.3(2)T, 12.3(4)T, 12.3(7)T, or 12.3(7)XR2 configured as a Cisco Easy VPN remote.
- A Cisco 1700 series router running Cisco IOS Release 12.2(15)T, 12.3(2)T, 12.3(4)T, 12.3(7)T, or 12.3(7)XR configured as a Cisco Easy VPN remote.
- A Cisco 1800 series fixed configuration router running Cisco IOS Release 12.3(8)YI.
- A Cisco uBR905 or Cisco uBR925 cable access router running Cisco IOS Release 12.2(15)T and configured as a Cisco Easy VPN remote.
- A Cisco router or VPN concentrator that supports the Cisco Easy VPN Server feature and that is configured as a Cisco IOS Easy VPN server.
- A Dynamic Host Configuration Protocol (DHCP) server pool must be configured: for details see the *DHCP Features Roadmap*.
- An Easy VPN Server must be configured, for details see *Easy VPN Server*.
- Optionally, an Easy VPN Server on a Cisco PIX Firewall can be configured, for details see *Easy VPN Server*.

Reactivate Primary Peer Feature

- An existing Easy VPN remote configuration can be configured with the Reactivate Primary Peer feature using the **peer** command (with the **default** keyword) and the **idle-time** command. On configuring the Reactivate Primary Peer feature, the Easy VPN remote periodically checks the connectivity with the primary peer. The Reactivate Primary Peer feature takes effect after a tunnel between the Easy VPN remote and a nondefault peer is established. If the Easy VPN remote detects that the connectivity is not working, the Easy VPN remote discards the existing tunnel and establishes the tunnel with the primary peer.

Restrictions for Cisco Easy VPN Remote

Required Easy VPN Servers

The Cisco Easy VPN Remote feature requires that the destination peer be a Cisco IOS Easy VPN server or VPN concentrator that supports the Cisco Easy VPN Server feature. The Cisco Easy VON Remote feature is only supported on the following platforms, along with the indicated software releases:

- Cisco 806, Cisco 826, Cisco 827, Cisco 828, Cisco 831, Cisco 836, and Cisco 837 routers—Cisco IOS Release 12.2(8)T or later release. Cisco 800 series routers are not supported in Cisco IOS Release 12.3(7)XR, but they are supported in Cisco IOS Release 12.3(7)XR2.
- Cisco 870 series—Cisco IOS Release 12.3(8)YI1.
- Cisco 1700 series—Cisco IOS Release 12.2(8)T or later release.

- Cisco 1800 series fixed configuration router—Cisco IOS Release 12.3(8)YI.
- Cisco 1812 router—Cisco IOS Release 12.3(8)YH.
- Cisco 2600 series—Cisco IOS Release 12.2(8)T or later release.
- Cisco 3620—Cisco IOS Release 12.2(8)T or later release.
- Cisco 3640—Cisco IOS Release 12.2(8)T or later release.
- Cisco 3660—Cisco IOS Release 12.2(8)T or later release.
- Cisco 7100 series VPN routers—Cisco IOS Release 12.2(8)T or later release.
- Cisco 7200 series routers—Cisco IOS Release 12.2(8)T or later release.
- Cisco 7500 series routers—Cisco IOS Release 12.2(8)T or later release.
- Cisco PIX 500 series—Software Release 6.2 or later release.
- Cisco VPN 3000 series—Software Release 3.11 or later release.

Cascaded Access Control Lists

Cascaded access control lists (ACLs) are used to add new networks in the Easy VPN interest list. None of the entries in ACL should match the inside interface network. If a match occurs, Easy VPN fails to create NAT rules and, hence, packets will not be translated by Easy VPN.

cTCP Support on Easy VPN Clients

- cTCP listens on only up to 10 ports.
- If there are applications registered for a port on which cTCP is enabled, the applications will not work.

Dial Backup for Easy VPN Remote

Line-status-based backup is not supported.

Dual Tunnel Support

The following restrictions apply if you are using dual tunnels that share the common inside and outside interfaces:

- One tunnels should have a split tunnel configured on the server.
- Web Intercept can be configured for only on one tunnel. Web Intercept should not be used for the voice tunnel.
- Web Intercept cannot be used for IP phones until authorization proxy becomes aware of how to bypass the IP phone.
- Some features, such as Pushing a Configuration URL Through a Mode-Configuration Exchange, can be used only through a single tunnel.

Local-Traffic Triggered Activation

This feature sets up the Easy VPN connection with locally generated traffic under the following conditions:

- Easy VPN should be configured in Connect ACL mode.
- The local traffic feature will be enabled only when at least one inactive EasyVPN tunnel is in connect ACL mode.
- The local traffic feature will be automatically disabled if all Easy VPN tunnels in Connect ACL mode are active and when no Easy VPN client is configured in Connect ACL mode.

Multicast and Static NAT

Multicast and static Network Address Translation (NAT) are supported only for Easy VPN remote using dynamic virtual tunnel interfaces (DVTIs).

Multiple Subnet ACL

The maximum number of ACL entries that can be configured on the Easy VPN client is 20.

Network Address Translation Interoperability Support

Network Address Translation (NAT) interoperability is not supported in client mode with split tunneling.

Only ISAKMP Policy Group 2 Supported on Easy VPN Servers

The Unity Protocol only supports Internet Security Association Key Management Protocol (ISAKMP) policies that use group 2 (1024-bit Diffie-Hellman) Internet Key Exchange (IKE) negotiation. Therefore, the Easy VPN server that is associated with the Cisco Easy VPN Remote feature must be configured for a group 2 ISAKMP policy. The Easy VPN server cannot be configured for ISAKMP group 1 or group 5 when being used with a Cisco Easy VPN client.

Transform Sets Supported

To ensure a secure tunnel connection, the Cisco Easy VPN Remote feature does not support transform sets that provide encryption without authentication (ESP-DES and ESP-3DES) or transform sets that provide authentication without encryption (ESP-NULL ESP-SHA-HMAC and ESP-NULL ESP-MD5-HMAC).

Note The Cisco Unity Client Protocol does not support Authentication Header (AH) authentication, but supports Encapsulation Security Protocol (ESP).

Universal Client Mode Using DHCP

The Easy VPN Remote feature does not support universal client mode using DHCP.

Virtual IPsec Interface

- For the Virtual IPsec Interface Support feature to work, virtual templates support is required.
- If you are using a virtual tunnel interface on the Easy VPN remote, it is recommended that you configure a virtual tunnel interface on the server.

Information About Cisco Easy VPN Remote

Benefits of the Cisco Easy VPN Remote Feature

- Allows dynamic configuration of end-user policy, requiring less manual configuration by end users and field technicians, thereby reducing errors and further service calls.
- Allows the provider to change equipment and network configurations as needed, with little or no reconfiguration of the end-user equipment.
- Provides for centralized security policy management.
- Enables large-scale deployments with rapid user provisioning.
- Eliminates the need for end users to purchase and configure external VPN devices.
- Eliminates the need for end users to install and configure Easy VPN Client software on their PCs.
- Offloads the creation and maintenance of the VPN connections from the PC to the device.
- Reduces interoperability problems between the different PC-based software VPN clients, external hardware-based VPN solutions, and other VPN applications.
- Sets up a single IPsec tunnel regardless of the number of multiple subnets that are supported and the size of the split-include list.

Cisco Easy VPN Remote Overview

Cable modems and digital subscriber line (xDSL) routers are types of broadband access that provide high performance connections to the Internet. However, applications also require secure VPN connections to perform a high level of authentication and to encrypt data between two particular endpoints. However, establishing a VPN connection between two routers can be complicated because configuring VPN parameters on the routers requires coordination between network administrators.

The Cisco Easy VPN Remote feature eliminates the complication by implementing Cisco Unity Client Protocol, which allows most VPN parameters to be defined at a Cisco IOS Easy VPN server. This server can be a dedicated VPN device, such as a Cisco VPN 3000 concentrator or a Cisco PIX Firewall or a Cisco IOS router that supports the Cisco Unity Client Protocol.

After configuring the Cisco Easy VPN server, a VPN connection can be created with minimal configuration on an Easy VPN remote, such as a Cisco 800 series router or a Cisco 1700 series router. When the Easy VPN remote initiates the VPN tunnel connection, the Cisco Easy VPN server pushes the IPsec policies to the Easy VPN remote and creates the corresponding VPN tunnel connection.

The Cisco Easy VPN Remote feature automatically manages the following:

- Negotiate tunnel parameters, such as addresses, algorithms, and lifetime.
- Establish tunnels according to the parameters that were set.
- Automatically create the Network Address Translation (NAT) or Port Address Translation (PAT) and associated access lists that are needed, if any.
- Authenticate users by way of user names, group names, and passwords.

- Manage security keys for encryption and decryption.
- Authenticate, encrypt, and decrypt data through the tunnel.

Modes of Operation

The Cisco Easy VPN Remote feature supports three modes of operation: client, network extension, and network extension plus:

- Client—Specifies that NAT or PAT be performed so that PCs and other hosts at the remote end of the VPN tunnel form a private network that does not use any IP addresses in the IP address space of the destination server.
  An enhancement has been made so that the IP address that is received via mode configuration is automatically assigned to an available loopback interface. The IPsec security associations (SAs) for this IP address are automatically created by Easy VPN Remote. The IP address is typically used for troubleshooting (using ping, Telnet, and Secure Shell).
- Network extension—Specifies that the PCs and other hosts at the client end of the VPN tunnel should be given IP addresses that are fully routable and reachable by the destination network over the tunneled network so that they form one logical network. PAT is not used, which allows the client PCs and hosts to have direct access to the PCs and hosts at the destination network.
- Network extension plus (mode network-plus)—Identical to network extension mode except for the additional capability of requesting an IP address via mode configuration and automatically assign the IP address to an loopback interface. The IPsec SAs for this IP address are automatically created by Easy VPN Remote. The IP address is typically used for troubleshooting (using ping, Telnet, and secure shell).

Note This functionality is supported only when the Cisco Easy VPN server and the Cisco Easy VPN client have the same type of Easy VPN configuration. In other words, both must use a Legacy Easy VPN configuration, or both must use a dynamic virtual tunnel interface (dVTI) configuration.

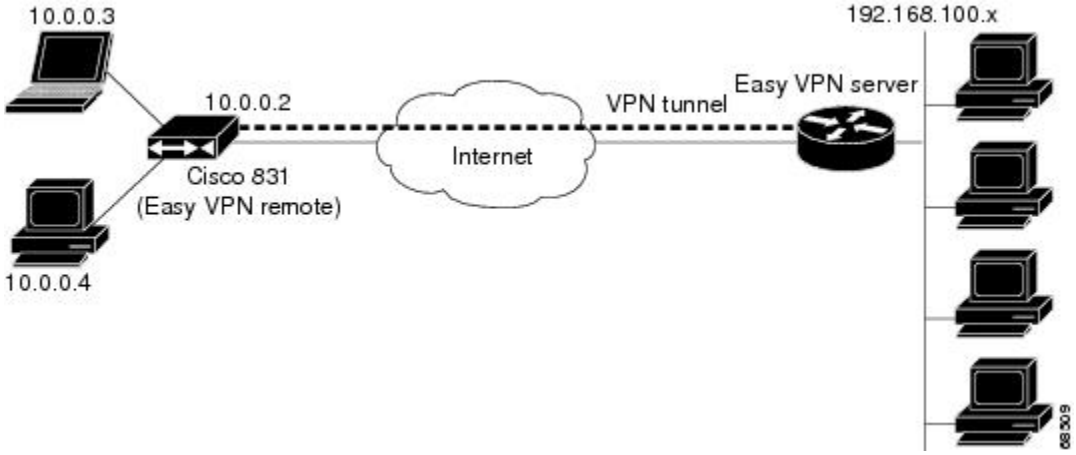
All modes of operation also optionally support split tunneling, which allows secure access to corporate resources through the VPN tunnel while also allowing Internet access through a connection to an Internet service provider (ISP) or other service--thereby eliminating the corporate network from the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

Client Mode and Network Extension Mode Scenarios

The figure below illustrates the client mode of operation. In this example, the Cisco 831 router provides access to two PCs, which have IP addresses in the 10.0.0.0 private network space. These PCs connect to the Ethernet interface on the Cisco 831 router, which also has an IP address in the 10.0.0.0 private network space. The

Cisco 831 router performs NAT or PAT translation over the VPN tunnel so that the PCs can access the destination network.

Figure 1: Cisco Easy VPN Remote Connection

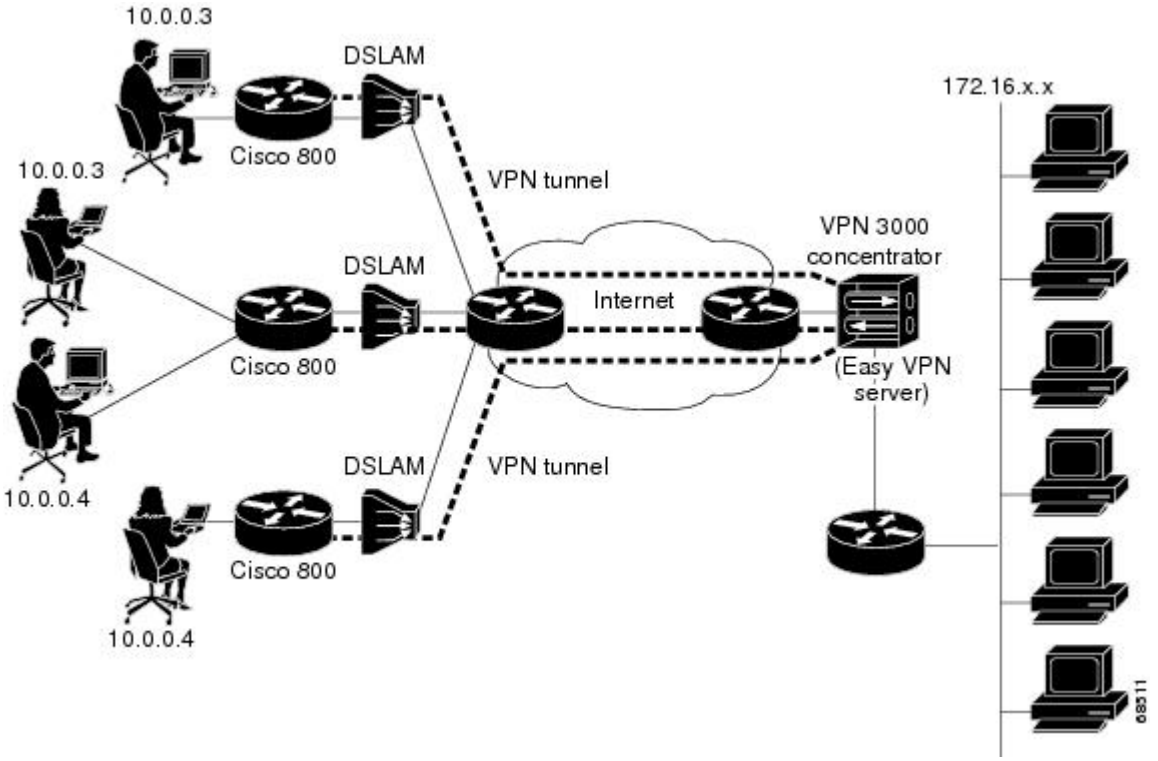


Note The figure above could also represent a split tunneling connection, in which the client PCs can access public resources in the global Internet without including the corporate network in the path for the public resources.

The figure below also illustrates the client mode of operation, in which a VPN concentrator provides destination endpoints to multiple xDSL clients. In this example, Cisco 800 series routers provide access to multiple small business clients, each of which uses IP addresses in the 10.0.0.0 private network space. The Cisco 800 series

routers perform NAT or PAT translation over the VPN tunnel so that the PCs can access the destination network.

Figure 2: Cisco Easy VPN Remote Connection (Using a VPN Concentrator)



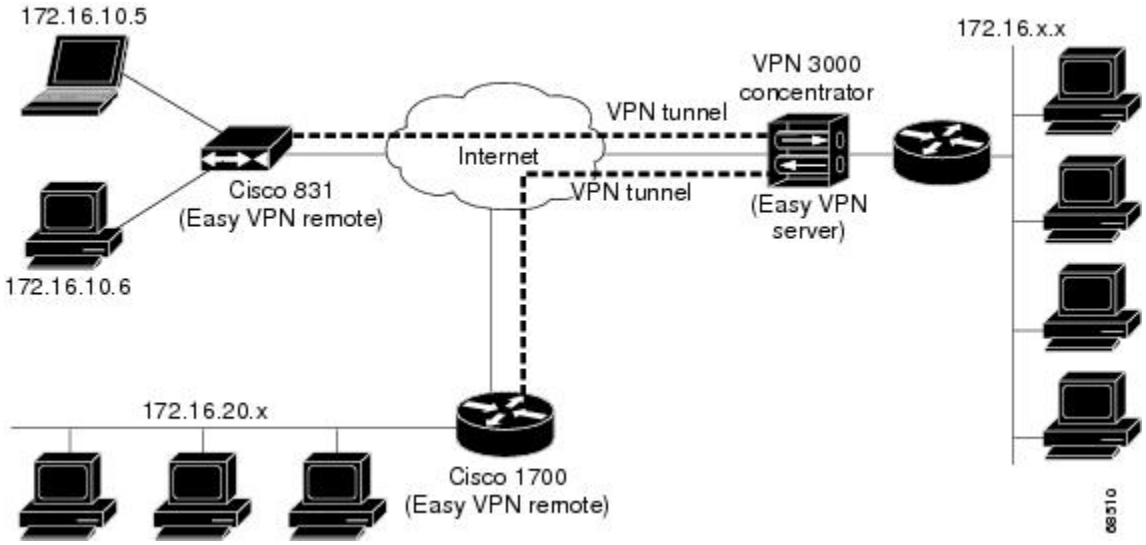
The figure below illustrates the network extension mode of operation. In this example, the Cisco 831 router and Cisco 1700 series router both act as Cisco Easy VPN remote devices, connecting to a Cisco VPN 3000 concentrator.

The client hosts are given IP addresses that are fully routable by the destination network over the tunnel. These IP addresses could be either in the same subnet space as the destination network or in separate subnets, assuming that the destination routers are configured to properly route those IP addresses over the tunnel.

In this example, the PCs and hosts attached to the two routers have IP addresses that are in the same address space as the destination enterprise network. The PCs connect to the Ethernet interface of the Cisco 831 router,

which also has an IP address in the enterprise address space. This scenario provides a seamless extension of the remote network.

Figure 3: Cisco Easy VPN Network Extension Connection



Authentication with Cisco Easy VPN Remote

The Cisco Easy VPN Remote feature supports a two-stage process for authenticating the remote router to the central concentrator. The first step is Group Level Authentication and is part of the control channel creation. In this first stage, two types of authentication credentials can be used: preshared keys or digital certificates. The following paragraphs provide details about these options.

The second authentication step is called Extended Authentication or Xauth. In this step, the remote side (in this case the Easy VPN router) submits a username and password to the central site router. This step is the same process as that which occurs when a user of the Cisco VPN software client on a PC enters his or her username and password to activate his or her VPN tunnel. When using the router, the difference is that the router itself is being authenticated to the network, not a PC with Cisco VPN Client software. Xauth is an optional step (it can be disabled) but is normally enabled to improve security. After Xauth is successful and the tunnel comes up, all PCs behind the Easy VPN remote router have access to the tunnel.

If Xauth is enabled, it is key to decide how to input the username and password. There are two options. The first option is to store the Xauth username and password in the configuration file of the router. This option is typically used if the router is shared between several PCs and the goal is to keep the VPN tunnel up all the time (see the section "Automatic Activation, on page 18") or to have the router automatically bring up the tunnel whenever there is data to be sent (see the section "Traffic-Triggered Activation, on page 18"). An example of this application is a branch office situation, in which the users in the branch office want the VPN tunnel to be available whenever they have data to send and do not want to have to do anything special to activate the VPN tunnel. If the PCs in the branch office must be individually authenticated on the basis of the ID of each user, the correct configuration is to put the Easy VPN router in Automatic Activation mode to keep the tunnel "up" all the time and to use Cisco IOS Authentication Proxy or 802.1x to authenticate the individual PCs. Because the tunnel is always up, Authentication Proxy or 802.1x can access a central site user database such as AAA/RADIUS to authenticate the individual user requests as they are submitted by PC users. (See the "Authentication with Cisco Easy VPN Remote, on page 9" sections "General information on IPsec and

VPN" for a reference to configuring Authentication Proxy and "802.1x authentication" for a reference to configuring 802.1x authentication.)

The second option for entry of the Xauth username and password is not to store it on the router. Instead, a PC user who is connected to the router is presented with a special web page that allows the user to manually enter the username and password (see the section "Manual Activation, on page 18"). The router sends the username and password to the central site concentrator, and if the username and password are correct, the tunnel comes up. The typical application for this configuration is a teleworker network. The teleworker wants to control when the tunnel is up and has to enter his or her personal user credentials (which could include one-time passwords) to activate the tunnel. Also, the network administrator may want teleworker tunnels up only when someone is using them to conserve resources on the central concentrators. (See the section "Web-Based Activation, on page 11" for details about this configuration.)

The Xauth username and password can also be manually entered from the command-line interface (CLI) of the router. This method is not recommended for most situations because the user must first log in to the router (and needs a user ID on the router to do so). However, it can be useful for network administrators during troubleshooting.

Use of Preshared Keys

Using preshared keys, each peer is aware of the key of the other peer. Preshared keys are displayed in running configurations, so they can be seen by anyone (referred to as clear format). When a more secure type of authentication is required, Cisco software also supports another type of preshared key: the encrypted preshared key.

Using an encrypted preshared key for authentication allows you to securely store plain-text passwords in type 6 (encrypted) format in NVRAM. A group preshared key can be preconfigured on both VPN-tunnel peers. The encrypted form of the keyword can be seen in the running configuration, but the actual keyword is not visible. (For more information about encrypted preshared keys, see Encrypted Preshared Key.)

Use of Digital Certificates

Digital certificates provide for the support of Rivest, Shamir, and Adelman (RSA) signatures on Easy VPN remote devices. The support is provided through a RSA certificate that can be stored on or off the remote device.

Note The recommended timeout for Easy VPN using digital certificates is 40 seconds.

For more information about digital certificates, see the Easy VPN Remote RSA Signature Support feature guide, Release 12.3(7)T1.

Use of Xauth

Xauth is an additional level of authentication that can be used. Xauth is applicable when either group preshared keys or digital certificates are used. Xauth credentials can be entered using a web interface manager, such as Security Device Manager (SDM), or using the CLI. (See the section "Cisco Easy VPN Remote Web Managers, on page 24.")

The Save Password feature allows the Xauth username and password to be saved in the Easy VPN Remote configuration so that you are not required to enter the username and password manually. One-Time Passwords

(OTPs) are not supported by the Save Password feature and must be entered manually when Xauth is requested. The Easy VPN server must be configured to "Allow Saved Passwords." (For more information about how to configure the Save Password feature, see the section "Dead Peer Detection Periodic Message Option, on page 24.")

Xauth is controlled by the Easy VPN server. When the Cisco IOS Easy VPN server requests Xauth authentication, the following messages are displayed on the console of the router:

```
EZVPN: Pending XAuth Request, Please enter the following command:
crypto ipsec client ezvpn xauth
```

When you see this message, you can provide the necessary user ID, password, and other information by entering the **crypto ipsec client ezvpn connect** command and responding to the prompts that follow.

The recommended Xauth timeout is 50 seconds or fewer.

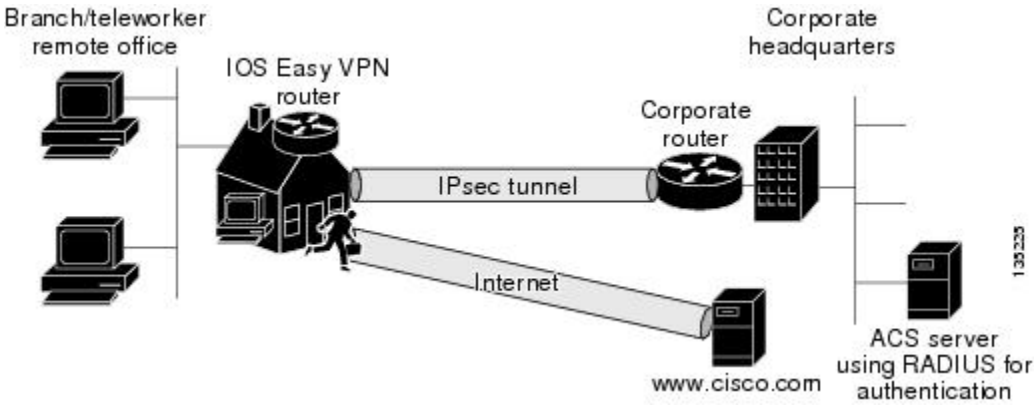
Note The timeout for entering the username and password is determined by the configuration of the Cisco IOS Easy VPN server. For servers running Cisco IOS software, this timeout value is specified by the **crypto isakmp xauth timeout** command.

Web-Based Activation

Web-Based Activation provides a user-friendly method for a remote teleworker to authenticate the VPN tunnel between his or her remote Easy VPN router and the central site router. This feature allows administrators to set up their remote LANs so that the initial HTTP request that is coming from any of the remote PCs is intercepted by the remote Easy VPN router. A login page is returned to the user, whereby the user may enter 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 reprompted for the username and password. Alternatively, the user may choose to bypass the VPN tunnel and connect only to the Internet, in which case a password is not required.

A typical application for web-based activation is a home teleworker who brings up the Easy VPN tunnel only when he or she needs to connect to the corporate LAN. If the remote teleworker is not present, other members of the household (such as a spouse or children) can use the Internet Only option to browse the Internet without activating the VPN tunnel. The figure below shows a typical scenario for web-based activation.

Figure 4: Typical Web-Based Activation Scenario



Note Entering the Xauth credentials brings up the tunnel for all users who are behind this remote site. After the tunnel is up, any additional PCs that are behind the remote site do not get prompted for Xauth credentials. Web-Based Activation is an authentication to bring up the VPN tunnel for all remote PCs and cannot be considered individual user authentication. Individual user authentication for VPN tunnel access is available using the Cisco IOS Authentication Proxy or 802.1x features, which can be configured on the remote Easy VPN router. (See the "Web-Based Activation, on page 11" sections "General information on IPsec and VPN" for a reference to configuring Authentication Proxy and "802.1x authentication" for a reference to configuring 802.1x authentication.)

To configure web-based activation, see the section "Configuring Web-Based Activation, on page 62."

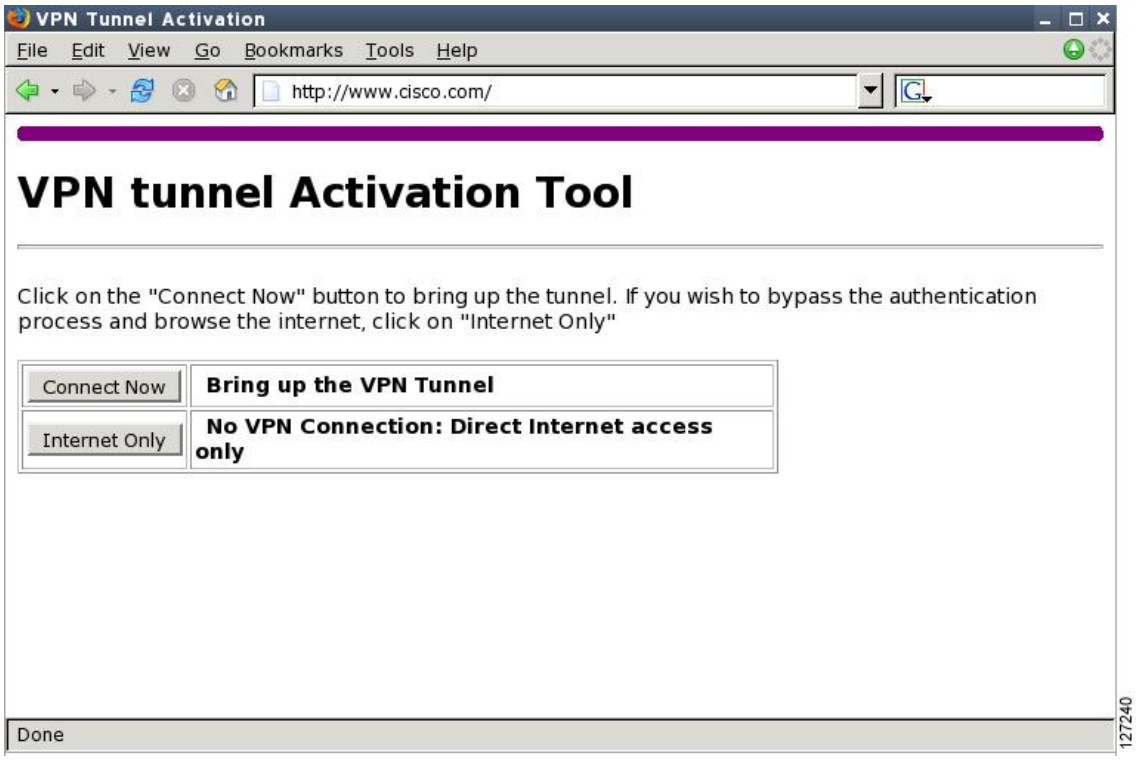
The following sections show the various screen shots that a remote teleworker sees when the Web-Based Activation feature is turned on:

Web-Based Activation Portal Page

The figure below is an example of a web-based activation portal page. The user may choose to connect to the corporate LAN by clicking Connect Now or he or she may choose to connect only to the Internet by clicking Internet Only.

Note If the user chooses to connect only to the Internet, a password is not required.

Figure 5: Portal Page

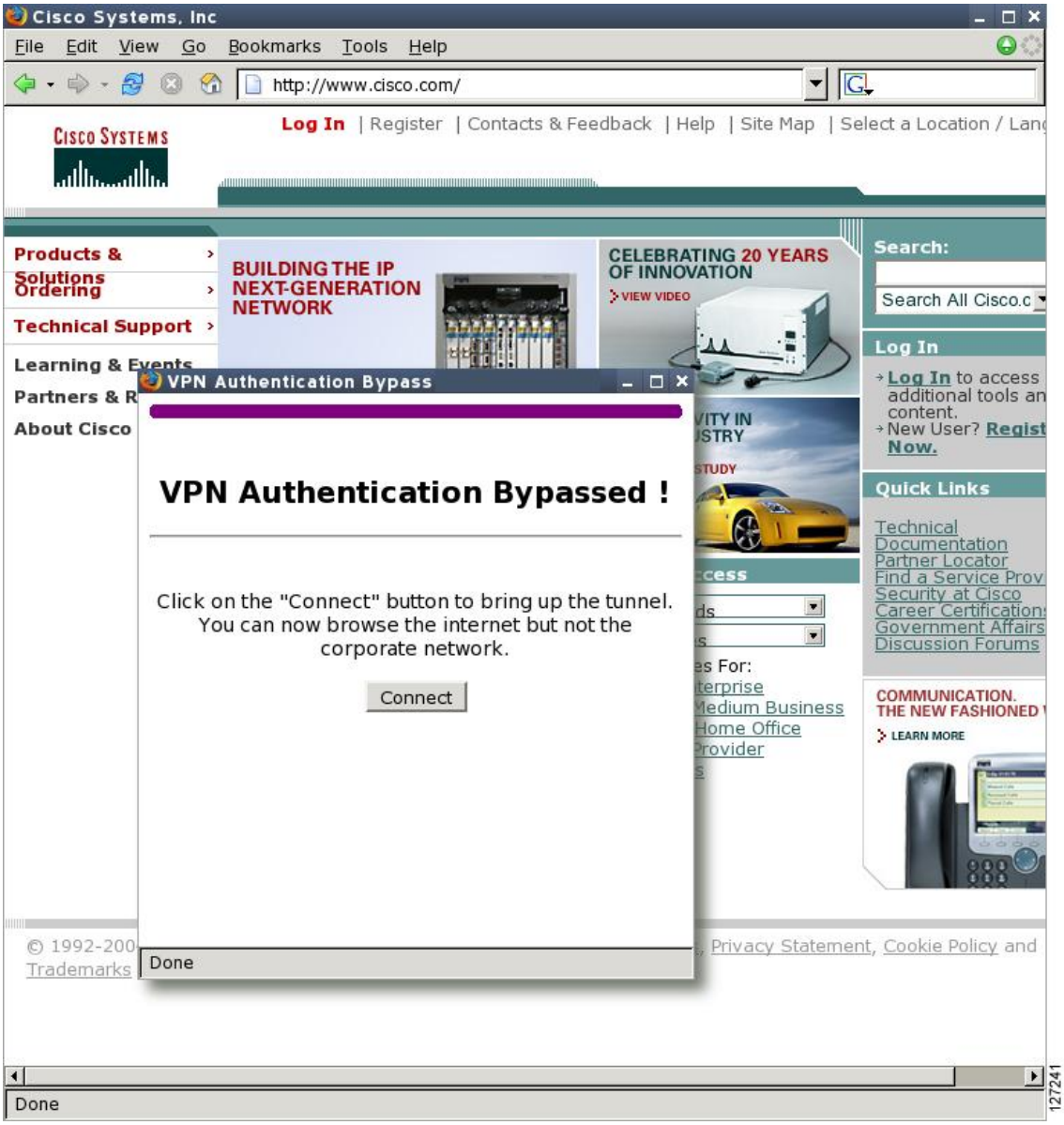


VPN Authentication Bypass

The figure below is an example of a web-based activation in which the user chose to connect only to the Internet by clicking the Internet Only option. This option is most useful for household members who need to

browse the Internet while the remote teleworker is not available to authenticate the VPN tunnel for corporate use.

Figure 6: VPN Authentication Bypass Page



If the Web-Based Activation window is mistakenly closed, to connect again, a user should follow this two-step process:

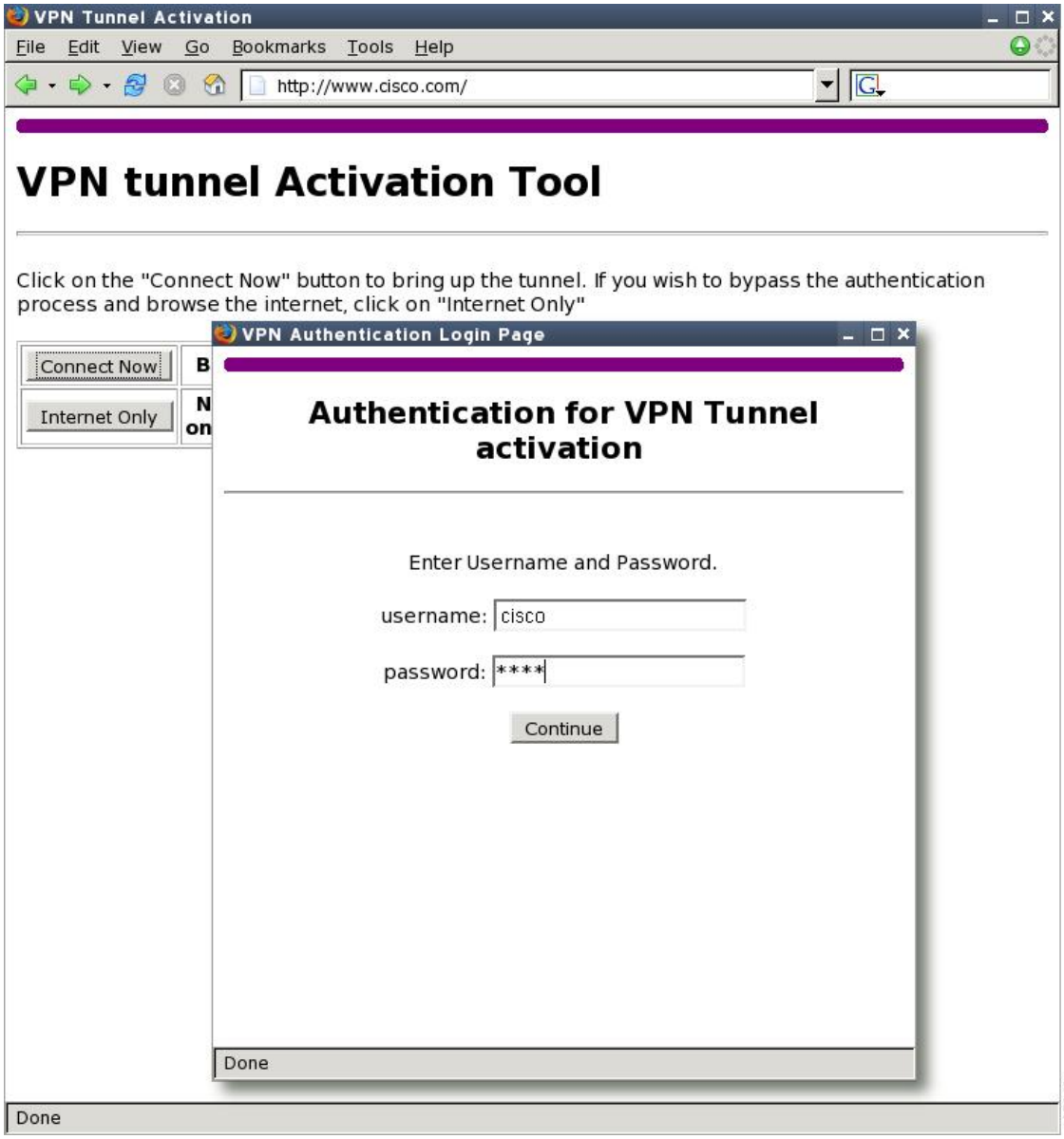
1. In a browser, type “http://routeripaddress/ezvpn/bypass” and try to connect to the URL. Entering this URL clears the bypass state that was created for your IP address (when the “Internet only” button was pressed). If you get a message saying that no such page is found, it does not matter because the only purpose of accessing the URL is to clear the bypass state.

2 After clearing the bypass state, you can browse to any external site. The Connect and Bypass page appears again. You can connect to VPN by pressing the Connect button.

VPN Tunnel Authentication

The figure below is an example of a web-based activation in which the user chose to connect to the corporate LAN by entering a username and password. After the user is successfully authenticated, the Easy VPN tunnel is brought up for this remote site. If there are multiple PCs behind this remote site, none of the additional users who are connecting to the corporate LAN will be requested for the Xauth credentials because the tunnel is already up.

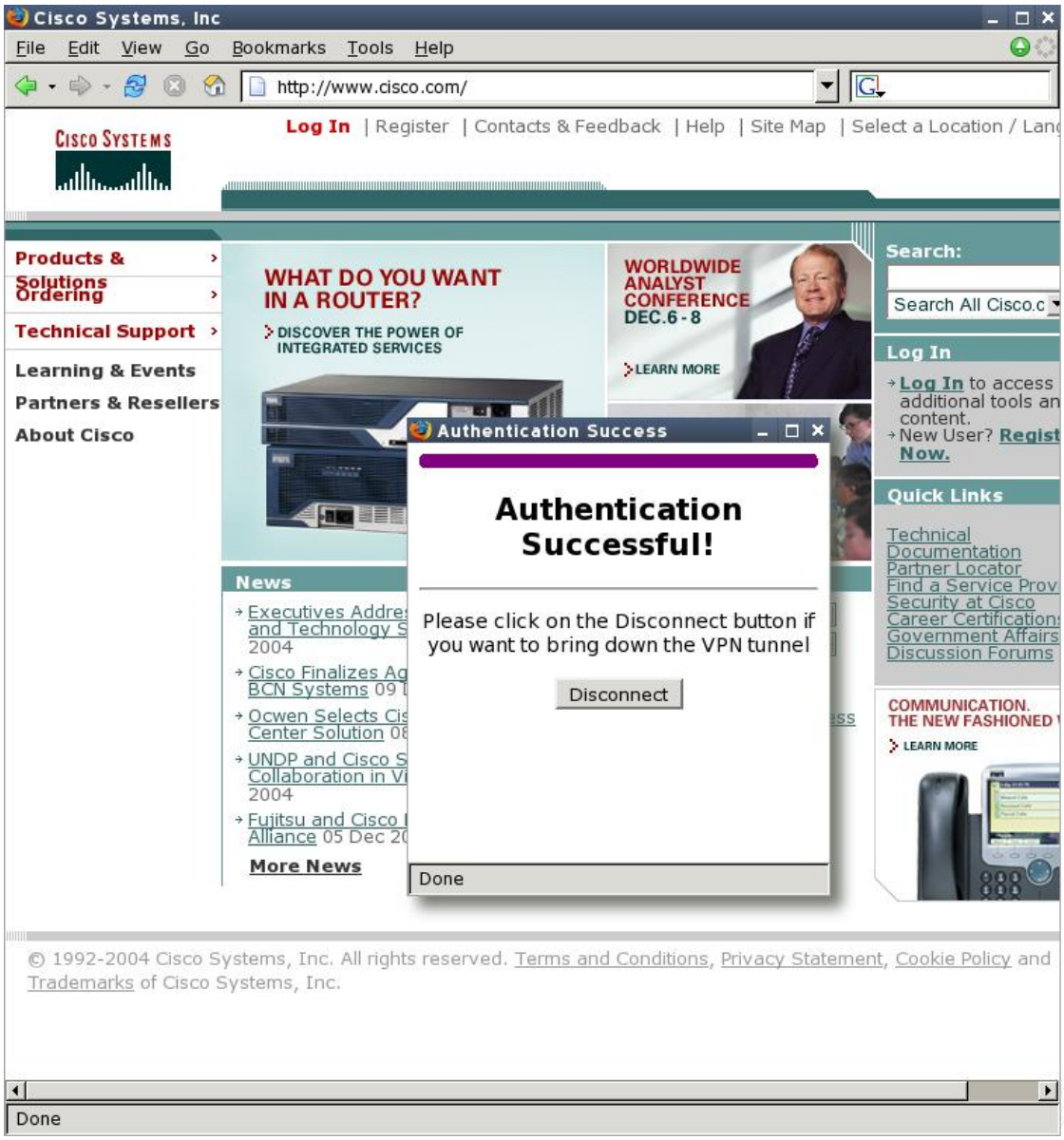
Figure 7: VPN Tunnel Authentication



Successful Authentication

The figure below is an example of a successful activation. If the user chooses to deactivate the VPN tunnel, he or she should click the Disconnect button. After the IKE security association (SA) times out (the default value is 24 hours), the remote teleworker has to enter the Xauth credentials to bring up the tunnel.

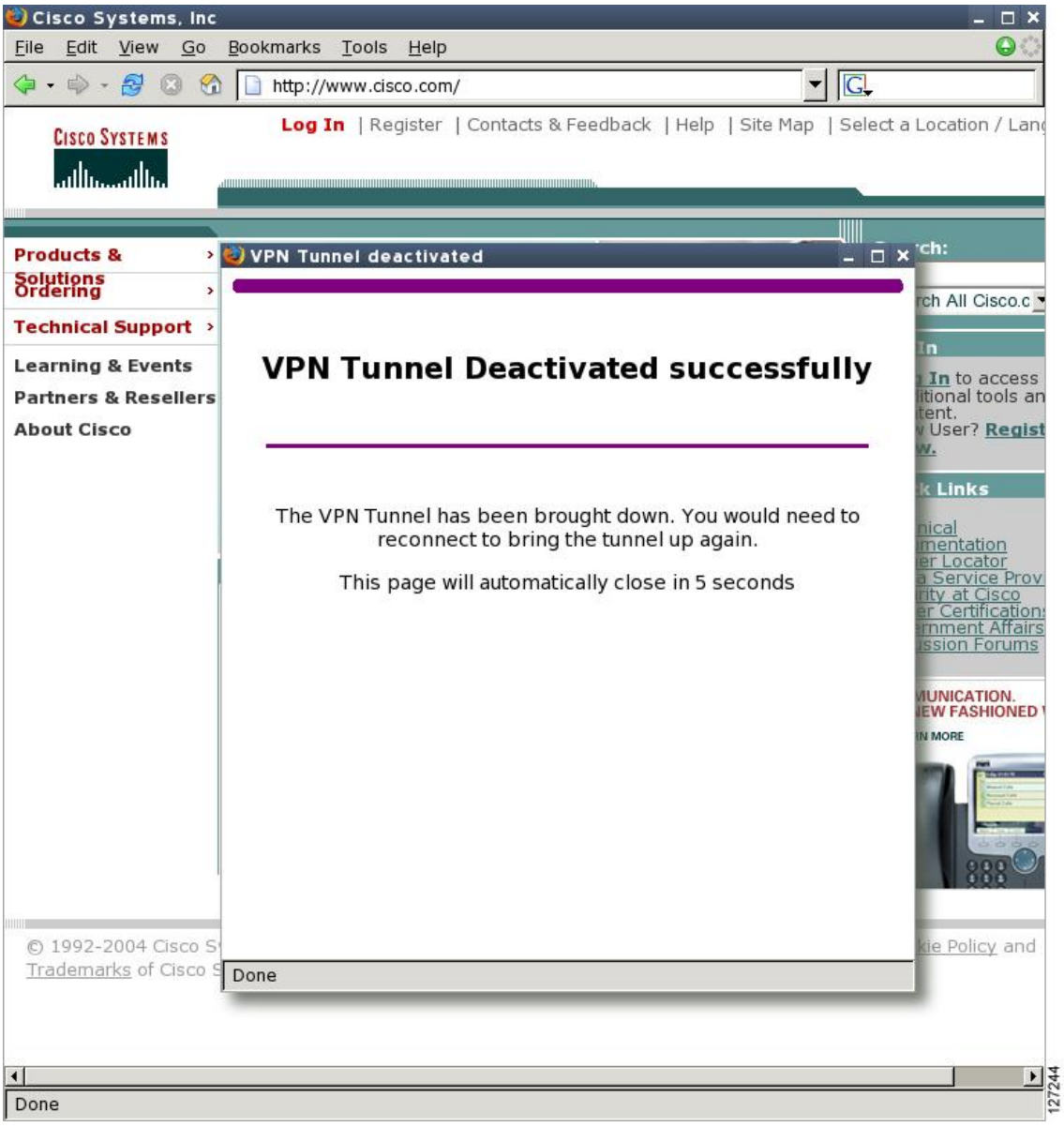
Figure 8: Successful Activation



Deactivation

The figure below is an example of a VPN tunnel that has been deactivated successfully. The page automatically closes in 5 seconds.

Figure 9: VPN Tunnel Deactivated Successfully



802.1x Authentication

The 802.1x Authentication feature allows you to combine Easy VPN client mode operation with 802.1x authentication on Cisco IOS routers. For more information about this feature, see “802.1 Authentication” in the section “Additional References, on page 100.”

Tunnel Activation Options

There are three tunnel activation options:

- Automatic activation
- Manual activation
- Traffic-triggered activation (not available in Cisco IOS Release 12.3(11)T)

Tunnel connect and disconnect options are available with SDM.

Automatic Activation

The Cisco Easy VPN tunnel is automatically connected when the Cisco Easy VPN Remote feature is configured on an interface. If the tunnel times out or fails, the tunnel automatically reconnects and retries indefinitely.

To specify automatic tunnel control on a Cisco Easy VPN remote device, you need to configure the **crypto ipsec client ezvpn** command and then the **connect auto** command. However, you do not need to use these two commands when you are creating a new Easy VPN remote configuration because the default is "automatic."

To disconnect or reset a particular tunnel, you should use the **clear crypto ipsec client ezvpn** command, or you can use SDM.

Manual Activation

The Cisco Easy VPN Remote software implements manual control of the Cisco Easy VPN tunnels so that you can establish and terminate the tunnel on demand.

To specify manual tunnel control on a Cisco Easy VPN remote device, you need to input the **crypto ipsec client ezvpn** command and then the **connect manual** command.

The manual setting means that the Cisco Easy VPN remote will wait for a command before attempting to establish the Cisco Easy VPN Remote connection. When the tunnel times out or fails, subsequent connections will also have to wait for the command.

If the configuration is manual, the tunnel is connected only after you issue the command **crypto ipsec client ezvpn connect** .

To disconnect or reset a particular tunnel, you should use the **clear crypto ipsec client ezvpn** command, or you can use SDM.

See the "Configuring Manual Tunnel Control, on page 42" section for specific information on how to configure manual control of a tunnel.

Traffic-Triggered Activation

Note This feature is not available in Cisco IOS Release 12.3(11)T.

The Traffic-Triggered Activation feature is recommended for transactional-based VPN applications. It is also recommended for use with the Easy VPN dial backup feature for the backup Easy VPN configuration so that backup is activated only when there is traffic to send across the tunnel.

To use Access Control List (ACL) tunnel control, you must first describe the traffic that is considered "interesting." For more information about ACLs, refer to the "IP Access List Overview" chapter of the *Security Configuration Guide: Access Control Lists*. To actually configure an ACL-triggered tunnel, use the **crypto ipsec client ezvpn** command with the **connect acl** command.

Dead Peer Detection Stateless Failover Support

Two options are available for configuring Dead Peer Detection Stateless Failover Support:

Backup Server List Local Configuration

Backup Server List Local Configuration allows users to enter multiple peer statements. With this feature configured, if the client is connecting to a peer and the negotiation fails, Easy VPN fails over to the next peer. This failover continues through the list of peers. When the last peer is reached, Easy VPN rolls over to the first peer. The IKE and IPsec SAs to the previous peer are deleted. Multiple peer statements work for both IP addresses as well as for hostnames. Setting or unsetting the peer statements will not affect the order of the peer statements.

To use this feature, use the **peer** command after the **crypto ipsec client ezvpn** command.

Backup Server List AutoConfiguration

Easy VPN remote that is based on Cisco IOS software can have up to 10 backup servers configured for redundancy. The Backup Server feature allows the Easy VPN server to "push" the backup server list to the Easy VPN remote.

The backup list allows the administrator to control the backup servers to which a specific Easy VPN remote will connect in case of failure, retransmissions, or dead peer detection (DPD) messages.

Note Before the backup server feature can work, the backup server list has to be configured on the server.

How a Backup Server Works

If remote A goes to server A and the connection fails, remote A goes to server B. If server B has a backup list configured, that list will override the backup server list of server A. If the connection to server B fails, remote A will continue through the backup servers that have been configured.

Note If you are in auto mode and you have a failure, you will transition automatically from server A to server B. However, if you are in manual mode, you have to configure the transition manually. To configure the transition manually, use the **crypto ipsec client ezvpn** command with the **connect** keyword.

No new configuration is required at the Easy VPN remote to enable this feature. If you want to display the current server, you can use the **show crypto ipsec client ezvpn** command. If you want to find out which peers were pushed by the Easy VPN server, you can use the same command.

To troubleshoot this feature, use the **debug crypto ipsec client ezvpn** command. If more information is needed for troubleshooting purposes, use the **debug crypto isakmp** command. The **show crypto ipsec client ezvpn** command may also be used for troubleshooting.

Cisco Easy VPN Remote Features

The Cisco Easy VPN Remote feature is a collection of features that improves the capabilities of the Cisco Easy VPN Remote feature introduced in Cisco IOS Release 12.2(4)YA. The Cisco Easy VPN Remote feature includes the following:

Default Inside Interface

Easy VPN Remote supports the autoconfiguration of the default Easy VPN inside interface for Cisco 800 series routers. The interface Ethernet 0 is the default inside interface.

If you want to disable the default inside interface and configure another inside interface on the Cisco 800 series router, you must configure the other inside interface first and then disable the default inside interface. You can use the following command to disable the default inside interface:

no crypto ipsec client ezvpn
name **inside**

If you did not configure the other inside interface first before disabling the default inside interface, you will receive a message such as the following (see lines three and four):

```
Router(config)# interface ethernet0
Router(config-if)# no crypto ipsec client ezvpn hw-client inside
Cannot remove the single inside interface unless
one other inside interface is configured
```

Multiple Inside Interfaces

Inside interface support is enhanced in the Cisco Easy VPN Remote feature to support multiple inside interfaces for all platforms. Inside interfaces can be configured manually with the enhanced command.:

interface
interface-name **crypto ipsec client ezvpn**
name [**outside** | **inside**]

Note Multiple inside interfaces are supported only when the Cisco Easy VPN server and the Cisco Easy VPN client have the same type of Easy VPN configuration. In other words, both must use a Legacy Easy VPN configuration, or both must use a DVTI configuration.

See the "Configuring Multiple Inside Interfaces, on page 44" section for information on how to configure more than one inside interface.

Multiple inside interfaces offer the following capabilities:

- Up to eight inside interfaces are supported on the Cisco 800 and Cisco 1700 series routers.
- At least one inside interface must be configured for each outside interface; otherwise, the Cisco Easy VPN Remote feature does not establish a connection.

- Adding a new inside interface or removing an existing inside interface automatically resets the Cisco Easy VPN Remote connection (the currently established tunnel). You must reconnect a manually configured tunnel, and if Xauth is required by the Cisco Easy VPN server, the user is reprompted. If you have set the Cisco Easy VPN Remote configuration to connect automatically and no Xauth is required, no user input is required.
- Inside interfaces that are configured or the default setting can be shown by using the **show crypto ipsec client ezvpn** command.

Multiple Outside Interfaces

The Easy VPN Remote feature supports one Easy VPN tunnel per outside interface. You can configure up to four Easy VPN tunnels per Cisco router. Each Easy VPN tunnel can have multiple inside interfaces configured, but they cannot overlap with another Easy VPN tunnel unless dial backup is configured. For more information about dial backup, see the section "Dial Backup, on page 25." To configure multiple outside interfaces, use the **crypto ipsec client ezvpn** command and **outside** keyword.

To disconnect or clear a specific tunnel, the **clear crypto ipsec client ezvpn** command specifies the IPsec VPN tunnel name. If there is no tunnel name specified, all existing tunnels are cleared.

See the "Configuring Multiple Outside Interfaces, on page 46" section for more information on configuring more than one outside interface.

VLAN Support

VLAN support allows VLANs to be configured as valid Easy VPN inside interfaces, which was not possible before Cisco IOS Release 12.3(7)XR. With this feature, SAs can be established at connection using the VLAN subnet address or mask as a source proxy.

For the inside interface support on VLANs to work, you must define each VLAN as an Easy VPN inside interface. In addition, IPsec SAs should be established for each inside interface in the same manner as for other inside interfaces. For more information about inside and outside interfaces, see the sections "Multiple Inside Interfaces, on page 20" and "Multiple Outside Interfaces, on page 21."

Inside interface support on VLANs is supported only on Cisco routers that support VLANs.

Multiple Subnet Support

For situations in which you have multiple subnets connected to an Easy VPN inside interface, you can optionally include these subnets in the Easy VPN tunnel. First, you must specify the subnets that should be included by defining them in an ACL. To configure an ACL, see "Access control lists, configuring" in the "Additional References, on page 100" section. Next, you have to use the **acl** command after the **crypto ipsec client ezvpn** (global) command to link your ACL to the Easy VPN configuration. Easy VPN Remote will automatically create the IPsec SAs for each subnet that is defined in the ACL as well as for the subnets that are defined on the Easy VPN inside interface.

Note Multiple subnets are not supported in client mode.

Note This functionality is supported only when the Cisco Easy VPN server and the Cisco Easy VPN client have the same type of Easy VPN configuration. In other words, both must use a Legacy Easy VPN configuration, or both must use a DVTI configuration.

NAT Interoperability Support

Cisco Easy VPN Remote supports interoperability with NAT. You can have a NAT configuration and a Cisco Easy VPN Remote configuration that coexist. When an IPsec VPN tunnel is down, the NAT configuration works.

In the Cisco Easy VPN Remote feature, the router automatically restores the previous NAT configuration when the IPsec VPN tunnel is torn down. The user-defined access lists are not disturbed. Users can continue to access nontunnel areas of the Internet when the tunnel times out or disconnects.

Note NAT interoperability is not supported in client mode with split tunneling.

Local Address Support

The Cisco Easy VPN Remote feature is enhanced to support an additional local-address attribute. This attribute specifies which interface is used to determine the IP address that is used to source the Easy VPN Remote tunnel traffic. After specifying the interface with the **local-address** command, you can manually assign a static IP address to the interface or use the **cable-modem dhcp-proxy interface** command to automatically configure the specified interface with a public IP address. See the "Configuring Proxy DNS Server Support, on page 49" section for configuration information.

Local Address Support is available for all platforms, but it is more applicable to the Cisco uBR905 and Cisco uBR925 cable access routers in conjunction with the **cable-modem dhcp-proxy interface** command. Typically, the loopback interface is the interface used to source tunnel traffic for the Cisco uBR905 and Cisco uBR925 cable access routers.

In a typical DOCSIS network, the Cisco uBR905 and Cisco uBR925 cable access routers are normally configured with a private IP address on the cable modem interface. In the initial Cisco Easy VPN Remote feature, a public IP address was required on the cable modem interface to support the Easy VPN remote.

In the Cisco Easy VPN Remote feature, cable providers can use the Cable DHCP Proxy feature to obtain a public IP address and assign it to the cable modem interface, which is usually the loopback interface.

For more information on the **cable-modem dhcp-proxy interface** command, see the Master Command List at Cisco IOS Master Command List, All Releases.

Note The **cable-modem dhcp-proxy interface** command is supported only for the Cisco uBR905 and Cisco uBR925 cable access routers.

Peer Hostname

The peer in a Cisco Easy VPN Remote configuration can be defined as an IP address or a hostname. Typically, when a peer is defined as a hostname, a DNS lookup is done immediately to get an IP address. In the Cisco Easy VPN Remote feature, the peer hostname operation is enhanced to support DNS entry changes. The text string of the hostname is stored so that the DNS lookup is done at the time of the tunnel connection, not when the peer is defined as a hostname.

See the "Configuring and Assigning the Easy VPN Remote Configuration, on page 37" section for information on enabling the peer hostname functionality.

Proxy DNS Server Support

When the Easy VPN tunnel is down, the DNS addresses of the ISP or cable provider should be used to resolve DNS requests. When the WAN connection is up, the DNS addresses of the enterprise should be used.

As a way of implementing use of the DNS addresses of the cable provider when the WAN connection is down, the router in a Cisco Easy VPN Remote configuration can be configured to act as a proxy DNS server. The router, acting as a proxy DNS server for LAN-connected users, receives DNS queries from local users on behalf of the real DNS server. The DHCP server then can send out the LAN address of the router as the IP address of the DNS server. After the WAN connection comes up, the router forwards the DNS queries to the real DNS server and caches the DNS query records.

See the "Configuring Proxy DNS Server Support, on page 49" section for information on enabling the proxy DNS server functionality.

Cisco IOS Firewall Support

The Cisco Easy VPN Remote feature works in conjunction with Cisco IOS Firewall configurations on all platforms.

Easy VPN Remote and Server on the Same Interface

This feature allows the Easy VPN remote and Easy VPN server to be supported on the same interface, making it possible to both establish a tunnel to another Easy VPN server and terminate the Easy VPN software client on the same interface simultaneously. A typical application would be a geographically remote location for which Easy VPN Remote is being used to connect to a corporate Easy VPN server and also to terminate local software client users.

For more information about the Easy VPN Remote and Server on the Same Interface feature, see "Easy VPN Remote and Server on the Same Interface" in the section "Additional References, on page 100."

Easy VPN Remote and Site to Site on the Same Interface

This feature allows the Easy VPN remote and site to site (crypto map) to be supported on the same interface, making it possible to both establish a tunnel to another Easy VPN server and have another site to site on the same interface simultaneously. A typical application would be a third-party VPN service provider that is managing a remote router via the site-to-site tunnel and using Easy VPN Remote to connect the remote site to a corporate Easy VPN server.

For more information about the Easy VPN Remote and Site to Site on the Same Interface feature, see "Easy VPN Remote and Site to Site on the Same Interface" in the section "Additional References, on page 100."

Cisco Easy VPN Remote Web Managers

Web interface managers may be used to manage the Cisco Easy VPN Remote feature. One such web interface manager is SDM, which is supported on the Cisco 830 series, Cisco 1700 series, Cisco 2600 series, Cisco 3600 series, and Cisco 3700 series routers. SDM enables you to connect or disconnect the tunnel and provides a web interface for Xauth. For more information about SDM, see Cisco Router and Security Device Manager.

A second web interface manager is the Cisco Router Web Setup (CRWS) tool, which is supported on the Cisco 806 router. The CRWS provides a similar web interface as SDM.

A third web interface manager, Cisco Easy VPN Remote Web Manager, is used to manage the Cisco Easy VPN Remote feature for Cisco uBR905 and Cisco uBR925 cable access routers. You do not need access to the CLI to manage the Cisco Easy VPN remote connection.

The web interface managers allow you to do the following:

- See the current status of the Cisco Easy VPN remote tunnel.
- Connect a tunnel that is configured for manual control.
- Disconnect a tunnel that is configured for manual control or reset a tunnel configured for automatic connection.
- Be prompted for Xauth information, if needed.

See "Troubleshooting the VPN Connection, on page 67" for more information about Cisco Easy VPN Remote Web Manager.

Dead Peer Detection Periodic Message Option

The dead peer detection periodic message option allows you to configure your router to query the liveliness of its IKE peer at regular intervals. The benefit of this approach over the default approach (on-demand dead peer detection) is earlier detection of dead peers. For more information about the dead peer detection periodic message option, see "*Dead peer detection*" *in the section* "Additional References, on page 100."

Load Balancing

When the Cisco VPN 3000 concentrator is configured for load balancing, the VPN 3000 will accept an incoming IKE request from the VPN remote on its virtual IP address. If the device is loaded and unable to accept more traffic, the VPN 3000 will send a notify message that contains an IP address that represents the new IKE server to which the remote should connect. The old connection will be torn down and a new connection established to the redirected VPN gateway.

There is no configuration required for load balancing to occur. If the VPN gateway is configured for load balancing, and it notifies the VPN remote that it is performing load balancing, the VPN remote has access to the load balancing feature.

To verify whether load balancing is occurring, use the **debug crypto isakmp**, **debug crypto ipsec client ezvpn**, and **show crypto ipsec** commands. To troubleshoot the load balancing process, use the **show crypto ipsec** command.

Management Enhancements

Management enhancements for Easy VPN remotes allow for the remote management of the VPN remote. The feature provides for the IPv4 address to be pushed by configuration mode to the VPN remote. The IPv4 address is assigned to the first available loopback interface on the VPN remote, and any existing statically defined loopbacks are not overridden. On disconnect, the address and loopback interface are removed from the list of active interfaces.

After the VPN remote is connected, the loopback interface should be accessible from the remote end of the tunnel. All PAT activities will be translated through this interface IP address.

If a loopback exists, and an IP address is associated with it and its state is unassigned, the interface is a good candidate for mode configuration address management.

Note After you assign an address to the loopback interface, if you save the configuration to NVRAM and reboot the VPN remote, the configuration address is permanently contained in the configuration. If you saved the configuration to NVRAM and rebooted the VPN remote, you must enter configuration mode and remove the IP address from the loopback interface manually.

You can use the **show ip interface** command with the **brief** keyword to verify that a loopback has been removed. The output of this **show** command also displays the interface.

PFS Support

The PFS configuration mode attribute is sent by the server if requested by the VPN remote device. If any subsequent connection by the remote device shows that PFS is not received by the remote, PFS will not be sent in IPsec proposal suites.

Note The PFS group that will be proposed in the IPsec proposal suites is the same as the group used for IKE.

You can use the **show crypto ipsec client ezvpn** command to display the PFS group and to verify that you are using PFS.

Dial Backup

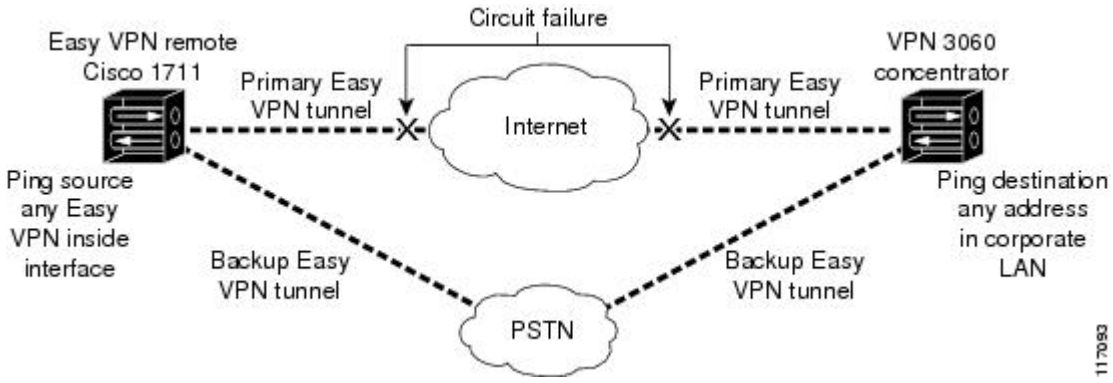
Note The Dial Backup feature is not available in Cisco IOS Release 12.3(11)T.

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

The figure below illustrates a typical Easy VPN remote-with-dial-backup scenario. In this scenario, Cisco 1751 remote device is attempting to connect to another Cisco 1751 (acting as a server). There is a failure in

the primary Easy VPN tunnel, and the connection is rerouted through the Easy VPN backup tunnel to the Cisco 1751 server.

Figure 10: Dial Backup for Easy VPN Scenario



Dial Backup Using a Dial-on-Demand Solution

IP static route tracking enable Cisco IOS software to identify when a Point-to-Point Protocol over Ethernet (PPPoE) or IPsec VPN tunnel "goes down" and initiates a Dial-on-Demand (DDR) connection to a preconfigured destination from any alternative WAN or LAN port (for example, a T1, ISDN, analog, or auxiliary port). The failure may be caused by several catastrophic events (for example, by Internet circuit failures or peer device failure). The remote route has only a static route to the corporate network. The IP static-route-tracking feature allows an object to be tracked (using an IP address or hostname) using Internet Control Message Protocol (ICMP), TCP, or other protocols, and it installs or removes the static route on the basis of the state of the tracked object. If the tracking feature determines that Internet connectivity is lost, the default route for the primary interface is removed, and the floating static route for the backup interface is enabled.

Dial Backup Using Object Tracking

IP static route tracking must be configured for dial backup on an Easy VPN remote device to work. The object tracking configuration is independent of the Easy VPN remote dial backup configuration. (For more information about object tracking, see the feature guide *Reliable Static Routing Backup Using Object Tracking*.)

Easy VPN Remote Dial Backup Support Configuration

You can configure dial backup for your Easy VPN remote using two Easy VPN remote options that allow a connection to the backup Easy VPN configuration and a connection to the tracking system.

- To specify the Easy VPN configuration that will be activated when backup is triggered, use the **backup** command after the **crypto ipsec client ezvpn** (global) command.
- The Easy VPN remote device registers to the tracking system to get the notifications for change in the state of the object. Use the **track** command to inform the tracking process that the Easy VPN remote device is interested in tracking an object, which is identified by the object number. The tracking process, in turn, informs the Easy VPN remote device when the state of this object changes. This notification prompts the Easy VPN remote device when the state of this object changes. This notification prompts the Easy VPN remote device to bring up the backup connection when the tracked object state is DOWN.

When the tracked object is UP again, the backup connection is torn down and the Easy VPN remote device will switch back to using the primary connection.

Note Only one backup configuration is supported for each primary Easy VPN configuration. Each inside interface must specify the primary and backup Easy VPN configuration.

Dynamically Addressed Environments

To allow dial backup to be deployed in dynamically addressed environments, use the IP SLA Pre-Routed ICMP Echo Probe feature. (For more information about this feature, see the Release Notes for Cisco 1700 Series Routers for Cisco IOS Release 12.3(7)XR. To use the IP SLA Pre-Routed ICMP Echo Probe feature, use the **icmp-echo** command with the **source-interface** keyword.

Dial Backup Examples

For examples of dial backup configurations, see the section "Dial Backup Examples, on page 80."

Virtual IPsec Interface Support

The Virtual IPsec Interface Support feature provides a routable interface to selectively send traffic to different Easy VPN concentrators as well as to the Internet.

Before Cisco IOS Release 12.4(4)T, at the tunnel-up/tunnel-down transition, attributes that were pushed during the mode configuration had to be parsed and applied. When such attributes resulted in the configurations being applied on the interface, the existing configuration had to be overridden. With the Virtual IPsec Interface Support feature, the tunnel-up configuration can be applied to separate interfaces, making it easier to support separate features at tunnel-up time. Features that are applied to the traffic going into the tunnel can be separate from the features that are applied to traffic that is not going through the tunnel (for example, split-tunnel traffic and traffic leaving the device when the tunnel is not up). When the Easy VPN negotiation is successful, the line protocol state of the virtual-access interface gets changed to up. When the Easy VPN tunnel goes down because the security association (SA) expires or is deleted, the line protocol state of the virtual-access interfaces changes to down.

Routes act as traffic selectors in an Easy VPN virtual interface, that is, the routes replace the access list on the crypto map. In a virtual-interface configuration, Easy VPN negotiates a single IPsec SA if the Easy VPN server has been configured with a dynamic virtual IPsec interface. This single SA is created irrespective of the Easy VPN mode that is configured.

After the SA is established, routes that point to the virtual-access interface are added to direct traffic to the corporate network. Easy VPN also adds a route to the VPN concentrator so that IPsec-encapsulated packets get routed to the corporate network. A default route that points to the virtual-access interface is added in the case of a nonsplit mode. When the Easy VPN server "pushes" the split tunnel, the split tunnel subnet becomes the destination to which the routes that point to the virtual access are added. In either case, if the peer (VPN concentrator) is not directly connected, Easy VPN adds a route to the peer.

Note Most routers that run the Cisco Easy VPN Client software have a default route configured. The default route that is configured should have a metric value greater than 1. The metric value must be greater than 1 because Easy VPN adds a default route that has a metric value of 1. The route points to the virtual-access interface so that all traffic is directed to the corporate network when the concentrator does not "push" the split tunnel attribute.

For more information about the IPsec Virtual Tunnel Interface feature, see the document *IPSec Virtual Tunnel Interface*.

The table below presents the different methods of configuring a remote device and the corresponding headend IPsec aggregator configurations. Each row represents a way to configure a remote device. The third column shows the different headend configurations that can be used with IPsec interfaces. See the second table below for a description of terms that are used in the first table below and Virtual IPsec Interface Support, on page 27.

Table 1: How Different Remote Device Configurations Interact with Various Headendsand Configurations

Remote Device Configurations	Cisco IOS Headend--Using Crypto Maps	Cisco IOS Headend --Using IPsec Interfaces	VPN3000/ASA
Crypto maps	• Supported.	—	—
Easy VPN virtual interface	• Supported. • Will create multiple SAs for a split tunnel. • Because there is no interface on the headend, interface features cannot be supported. • Limited quality of service (QoS) is supported.	• Supported. • Creates only a single SA in split and no-split tunnels. • Route injection is accomplished on the server. • Routes are injected on the remote devices to direct traffic to the interface.	• Supported. • Will create multiple SAs for a split tunnel.
Legacy Easy VPN	• Creates a single IPsec SA on the headend when a default policy is pushed. • Creates multiple SAs when a split-tunnel policy is pushed to the remote device.	• Not supported. • Cannot be used with split tunnels because the headend interface does not support multiple SAs on a single interface.	• Supported. • Creates multiple SAs for split tunnels.

Remote Device Configurations	Cisco IOS Headend--Using Crypto Maps	Cisco IOS Headend --Using IPsec Interfaces	VPN3000/ASA
Static virtual interface	• Not supported.	• Supported. • Can be used with a static interface or dynamic interface on the headend. • Routing support is mandatory to reach the network.	• Not supported.

The table below provides a description of the terms used in the table above and Virtual IPsec Interface Support, on page 27.

Table 2: Terms Used in the Table Above and the Table Below

Terms	Description
ASA	Cisco Adaptive Security Appliance, a threat-management security appliance.
Crypto maps	Commonly used for configuring IPsec tunnels. The crypto map is attached to an interface. For more information on crypto maps, see the "Creating Crypto Map Sets" section in the *Security for VPNs with IPsec Configuration Guide*.
Easy VPN dual tunnel remote device	Two Easy VPN remote device configurations in which both are using a dynamic IPsec virtual tunnel interface.
Easy VPN virtual interface remote device (Easy VPN virtual interface)	Easy VPN remote configuration that configures the usage of a dynamic IPsec virtual tunnel interface.
IPsec interface	Consists of static and dynamic IPsec virtual interfaces.
IPsec Virtual Tunnel Interface	Tunnel interface that is created from a virtual template tunnel interface using mode IPsec. For more information on virtual tunnel interface configurations, see the document *IPSec Virtual Tunnel Interface*.
Legacy Easy VPN	Easy VPN remote device configuration that uses crypto maps and does not use IPsec interfaces.

Terms	Description
Static IPsec virtual tunnel interface (static virtual tunnel interface)	Tunnel interface used with mode IPsec that proposes and accepts only an ipv4 any any selector. For more information on static virtual tunnel interface configurations, see the document *IPSec Virtual Tunnel Interface*.
VPN 3000	Cisco VPN 3000 series routers.

Dual Tunnel Support

Easy VPN now supports the ability to configure two easy VPN tunnels that have the same inside and outside interfaces. The feature is called the Easy VPN Dual Tunnel. Configuring multiple tunnels on a single remote device can be accomplished in a number of ways, which are listed in the table below along with their configuration and usage considerations. Further discussion in this section refers to only one such method of configuring dual tunnels using Easy VPN tunnels that have virtual interfaces. This method will be referred to as Dual Tunnel Support.

In a dual-tunnel Easy VPN setup, each Easy VPN tunnel is configured using virtual IPsec interface support, as shown in the section "Virtual IPsec Interface Support, on page 27." Each Easy VPN tunnel has its unique virtual interface, which is created when the Easy VPN configuration is complete.

There are two possible combinations in which the dual tunnels can be used.

- Dual Easy VPN tunnels that have one tunnel using a nonsplit tunnel policy and the other tunnel using a split tunnel policy that has been pushed from the respective headend.
- Dual Easy VPN tunnel in which both tunnels are using an independent split tunnel policy that has been pushed from the respective headend.

Note It is not permitted to have dual Easy VPN tunnels in which both tunnels are using a nonsplit tunnel policy.

The Easy VPN dual tunnel makes use of route injections to direct the appropriate traffic through the correct Easy VPN virtual tunnel interface. When the Easy VPN tunnel on the remote device "comes up," it "learns" the split or nonsplit policy from the headend. The Easy VPN remote device injects routes in its routing table that correspond to the nonsplit networks that have been learned. If the headend pushes a nonsplit tunnel policy to the Easy VPN remote device, the Easy VPN remote device installs a default route in its routing table that directs all traffic out of the Easy VPN virtual interface that corresponds to this Easy VPN tunnel. If the headend pushes split-tunnel networks to the remote device, the remote device installs specific routes to the split networks in its routing table, directing the traffic to these networks out of the virtual tunnel interface.

Note Dual Tunnel Easy VPN uses destination-based routing to send traffic to the respective tunnels.

Output features can be applied to this virtual interface. Examples of such output features are Cisco IOS quality of service and Cisco IOS Firewall. These features must be configured on the virtual template that is configured in the Easy VPN client configuration.

The table below explains how this feature should be used. See Dual Tunnel Support, on page 30 for a description of terms that are used in Dual Tunnel Support, on page 30 and the table below.

Table 3: Dual Tunnel Usage Guidelines

Dual Tunnel Combinations	Headends Supported	Configuration and Usage Considerations on the Easy VPN Remote Device and Headend
Two legacy Easy VPN tunnels	Cisco IOS software, ASA, and VPN 3000	• Two tunnels cannot share a common outside interface. • Two tunnels cannot share a common inside interface. • The two tunnels should use separate inside and outside interfaces. • Traffic from an inside interface that belongs to one Easy VPN tunnel cannot be pushed into another tunnel.
One legacy Easy VPN tunnel and one crypto map	Cisco IOS software, ASA, and VPN 3000	The crypto map can share the same outside interface as the legacy Easy VPN client configuration. However, the behavior of the two remote devices depends on the mode of Easy VPN as well as the IPsec selectors of the crypto map and the Easy VPN remote device. This is not a recommended combination.
One legacy Easy VPN tunnel and one static virtual interface	Cisco IOS software	Both tunnels cannot terminate on the same headend. The static virtual interface remote device tunnel has to be terminated on a static virtual interface on the headend router. The legacy Easy VPN remote device tunnel can terminate on the virtual tunnel interface or crypto map that is configured on the headend.

Dual Tunnel Combinations	Headends Supported	Configuration and Usage Considerations on the Easy VPN Remote Device and Headend
One legacy Easy VPN tunnel and one Easy VPN virtual interface	Cisco IOS software, ASA, and VPN 3000	• Both tunnels cannot terminate on the same headend. • The legacy Easy VPN tunnel and the Easy VPN virtual interface can share a common inside and outside interface. • An Easy VPN virtual interface should be used only with split tunneling. • Legacy Easy VPN can use a split tunnel or no split tunnel. • The Web-Based Activation feature cannot be applied on both Easy VPN tunnels. • Using two Easy VPN virtual interfaces is preferable to using this combination.
One Easy VPN virtual interface and one static virtual interface	Cisco IOS software	• Both tunnels cannot terminate on the same peer. The static virtual interface and the Easy VPN virtual interface can use the same outside interface. • The Easy VPN virtual interface should use split tunneling.
Two Easy VPN virtual interfaces	Cisco IOS software, ASA, and VPN 3000	• Both tunnels cannot terminate on the same peer. • At least one of the tunnels should use split tunneling. • Web-Based Activation cannot be applied to both Easy VPN tunnels.

Banner

The Easy VPN server pushes a banner to the Easy VPN remote device. The Easy VPN remote device can use the banner during Xauth and web-based activation. The Easy VPN remote device displays the banner the first time that the Easy VPN tunnel is brought up.

The banner is configured under group configuration on the Easy VPN server.

Configuration Management Enhancements (Pushing a Configuration URL Through a Mode-Configuration Exchange)

After this feature has been configured on the server using the commands **configuration url** and **configuration version** (after use of the **crypto isakmp client configuration group** command), the server can "push" the configuration URL and configuration version number to the Easy VPN remote device. With this information, the Easy VPN remote device can download the configuration content and apply it to its running configuration. For more information about this feature, see the section "Configuration Management Enhancements" in the Easy VPN Server feature module.

Reactivate Primary Peer

The Reactivate Primary Peer feature allows a default primary peer to be defined. The default primary peer (a server) is one that is considered better than other peers for reasons such as lower cost, shorter distance, or more bandwidth. With this feature configured, if Easy VPN fails over during Phase 1 SA negotiations from the primary peer to the next peer in its backup list, and if the primary peer is again available, the connections with the backup peer are torn down and the connection is again made with the primary peer.

Dead Peer Detection is one of the mechanisms that acts as a trigger for primary peer reactivation. Idle timers that are configured under Easy VPN is another triggering mechanism. When configured, the idle timer detects inactivity on the tunnel and tears it down. A subsequent connect (which is immediate in auto mode) is attempted with the primary preferred peer rather than with the peer last used.

Note Only one primary peer can be defined.

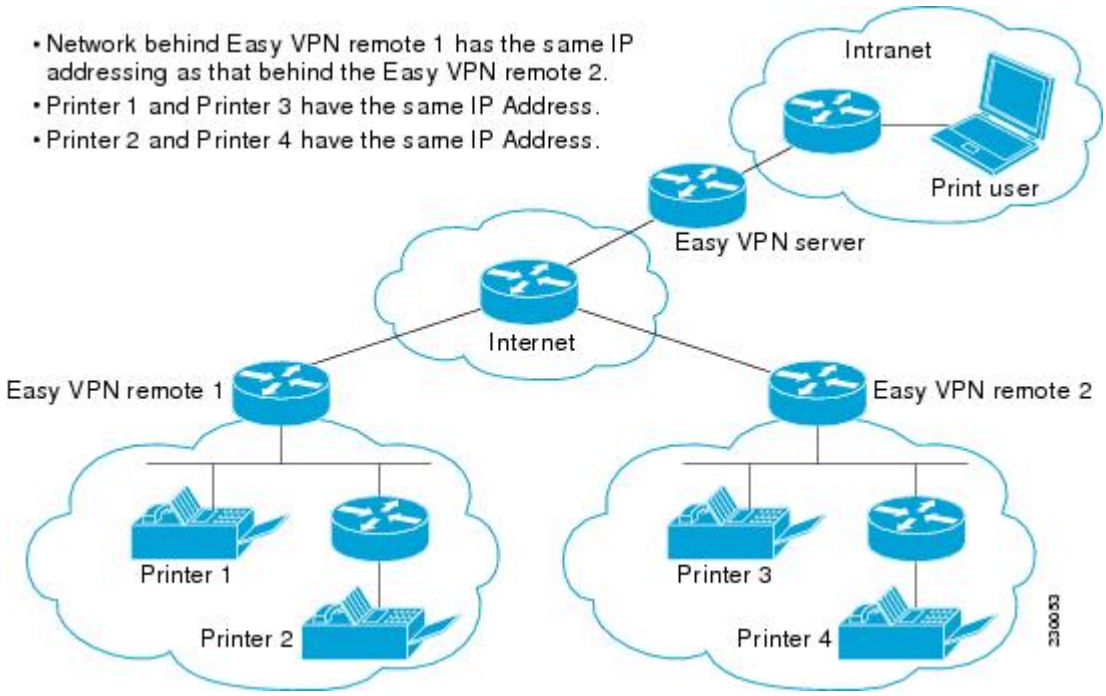
Identical Addressing Support

The Identical Addressing Support feature supports identically addressed LANs on Easy VPN remotes. Network resources, such as printers and web servers on the LAN side of the EasyVPN remotes, that have overlapping addressing with other Easy VPN remotes are now reachable. The Easy VPN Remote feature was enhanced to work with NAT to provide this functionality.

- The Easy VPN server requires no changes to support the Identical Addressing Support feature.
- The Identical Addressing Support feature is supported only in network extension modes (network-extension and network-plus).
- Virtual tunnel interfaces must be configured on the Easy VPN remote before using the Identical Addressing Support feature.

The diagram below shows an example of the Identical Addressing Support feature configuration.

Figure 11: Identical Addressing Support



The Identical Addressing Support feature can be configured with the following command and enhanced commands:

```
crypto  ipsec client ezvpn name
```

Enhanced Commands

- **nat acl** {*acl-name* | *acl-number*}—Enables split tunneling for the traffic specified by the ACL name or the ACL number.
  - The *acl-name* argument is the name of the ACL.
  - The *acl-number* argument is the number of the ACL.
- **nat allow**—Allows NAT to be integrated with Cisco Easy VPN.

For detailed steps on how to configure Identical Addressing Support, see Configuring Identical Addressing Support, on page 56.

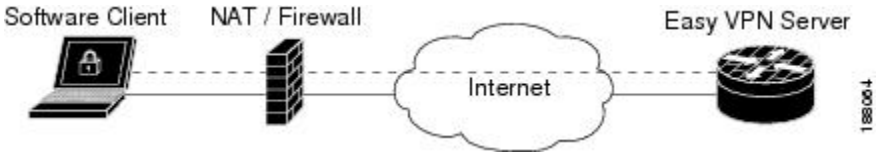
cTCP Support on Easy VPN Clients

The Cisco Tunneling Control Protocol (cTCP) feature can be used for situations in which an Easy VPN client (remote device) is operating in an environment in which standard IPsec does not function or in which it does not function transparently without modification to existing firewall rules. These situations include the following:

- Small office or home office router performing Network Address Translation (NAT) or Port Address Translation (PAT)
- PAT-provided IP address behind a larger router (for example, in a corporation)
- Non-NAT firewall (packet filtering or stateful)
- Proxy server

The diagram below illustrates how IPsec traffic that is tunneled inside the cTCP traverses Network Address Translation (NAT) and the firewall (see the dashed line).

Figure 12: cTCP on an Easy VPN Remote Device



For detailed steps on how to configure cTCP on Easy VPN remote devices, see the section "Configuring cTCP on an Easy VPN Client, on page 60."

For more information about cTCP support on Easy VPN remote devices, including configuration and troubleshooting examples, see "cTCP on Cisco Easy VPN remote devices" in the section "cTCP Support on Easy VPN Clients, on page 34."

Easy VPN Server on a VPN 3000 Series Concentrator

This section describes the guidelines required to configure the Cisco VPN 3000 series concentrator for use with the Cisco Easy VPN Remote feature. As a general rule, you can use the default configuration except for IP addresses, server addresses, routing configurations, and for the following parameters and options:

Note You must be using Cisco VPN 3000 series concentrator software Release 3.11 or later to support Cisco Easy VPN software clients and remotes.

Peer Configuration on a Cisco Easy VPN Remote Using the Hostname

After you have configured the Cisco Easy VPN server on the VPN 3000 concentrator to use hostname as its identity, you must configure the peer on the Cisco Easy VPN remote using the hostname. You can either configure DNS on the client to resolve the peer hostname or configure the peer hostname locally on the client using the **ip host** command. As an example, you can configure the peer hostname locally on an Easy VPN remote as follows:

```
ip host crypto-gw.cisco.com 10.0.0.1
```

Or you can configure the Easy VPN remote to use the hostname with the **peer** command and *hostname* argument, as follows:

```
peer crypto-gw.cisco.com
```

Interactive Hardware Client Authentication Version 3.5

The Cisco Easy VPN Remote feature does not support the Interactive Hardware Client Authentication Version 3.5 feature. This feature must be disabled. You can disable the feature on the VPN 3000 series concentrator by clicking the **HW Client** tab on the **Configuration | User Management | Base Group** screen.

IPsec Tunnel Protocol

IPsec Tunnel Protocol enables the IPsec tunnel protocol so that it is available for users. The IPsec Tunnel Protocol is configured on the Cisco VPN 3000 series concentrator by clicking the **General** tab on the **Configuration | User Management | Base Group** screen.

IPsec Group

IPsec group configures the Cisco VPN 3000 series concentrator with a group name and password that match the values configured for the Cisco Easy VPN remote configuration on the router. These values are configured on the router with the **group** *group-name* **key** *group-key* command and arguments. The values are configured on the Cisco VPN 3000 series concentrator using the **Configuration | User Management | Groups** screen.

Group Lock

If you are defining multiple users in multiple groups on the VPN 3000 series concentrator, you must check the **Group Lock** box in the **IPsec** tab to prevent users in one group from logging in with the parameters of another group. For example, if you have configured one group for split tunneling access and another group without split tunneling access, clicking the **Group Lock** box prevents users in the second group from gaining access to the split tunneling features. The **Group Lock** checkbox appears in the **IPsec** tab in the **Configuration | User Management | Base Group** screen and in the **IPsec** tab in the **Configuration | User Management | Groups | Add/Modify** screens.

Xauth

To use Xauth, set the **Authentication** parameter to **None**. The Authentication parameter appears in the **IPsec** tab in the **Configuration | User Management | Base Group** screen and in the **IPsec** tab in the **Configuration | User Management | Groups | Add/Modify** screens.

Split Tunneling

The **Configuration | User Management | Base Group, Mode Configuration Parameters Tab** screen includes a **Split Tunnel** option with a checkbox that says “Allow the networks in the list to bypass the tunnel.”

IKE Proposals

The Cisco VPN 3000 series concentrator is preconfigured with a default IKE proposal, CiscoVPNClient-3DES-MD5, that can be used with Cisco Easy VPN remotes. This IKE proposal supports preshared keys with Xauth using the MD5/HMAC-128 algorithm and Diffie-Hellman Group 2.

This IKE proposal is active by default, but you should verify that it is still an active proposal using the **Configuration | System | Tunneling Protocols | IPsec | IKE Proposals** screen.

In addition, as part of configuring the Cisco VPN 3000 series concentrator--for the Cisco Easy VPN Remote image, you do not need to create a new IPsec SA. Use the default IKE and Easy VPN remote lifetime configured on the Cisco VPN 3000 series concentrator.

Note You can also use the default IKE proposals IKE-DES-MD5 and IKE-3DES-MD5, but they do not enable Xauth support by default.

New IPsec SA

You can create a new IPsec SA. Cisco Easy VPN clients use a SA having the following parameters:

- Authentication Algorithm=ESP/MD5/HMAC-128
- Encryption Algorithm=DES-56 or 3DES-168 (recommended)
- Encapsulation Mode=Tunnel
- IKE Proposal=CiscoVPNClient-3DES-MD5 (preferred)

The Cisco VPN 3000 series concentrator is preconfigured with several default security associations (SAs), but they do not meet the IKE proposal requirements. To use an IKE proposal of CiscoVPNClient-3DES-MD5 , copy the ESP/IKE-3DES-MD5 SA and modify it to use CiscoVPNClient-3DES-MD5 as its IKE proposal. An IKE proposal is configured on the VPN 3000 series concentrator using the **Configuration | Policy Management | Traffic Management | Security Associations** screen.

How to Configure Cisco Easy VPN Remote

Remote Tasks

Configuring and Assigning the Easy VPN Remote Configuration

The device acting as the Easy VPN remote must create a Cisco Easy VPN Remote configuration and assign it to the outgoing interface. To configure and assign the remote configuration, perform the following steps.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **crypto ipsec client ezvpn** *name*
4. **group** *group-name* **key** *group-key*
5. **peer** [*ip-address* | *hostname*]
6. **mode** {**client** | **network-extension**}
7. **exit**
8. **interface** *type number*
9. **crypto ipsec client ezvpn** *name* [**outside**]
10. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**crypto ipsec client ezvpn** *name* **Example:** `Device(config)# crypto ipsec client ezvpn easy client remote`	Creates a remote configuration and enters Cisco Easy VPN Remote configuration mode.
Step 4	**group** *group-name* **key** *group-key* **Example:** `Device(config-crypto-ezvpn)# group easy-vpn-remote-groupname key easy-vpn-remote-password`	Specifies the IPsec group and IPsec key value to be associated with this configuration. **Note** The value of the *group-name* argument must match the group defined on the Easy VPN server. On Cisco IOS devices, use the **crypto isakmp client configuration group** and **crypto map dynmap isakmp authorization list** commands. **Note** The value of the *group-key* argument must match the key defined on the Easy VPN server. On Cisco IOS devices, use the **crypto isakmp client configuration group** command.

	Command or Action	Purpose
Step 5	**peer** [*ip-address* | *hostname*] **Example:** `Device(config-crypto-ezvpn)# peer 192.185.0.5`	Specifies the IP address or hostname for the destination peer (typically the IP address on the outside interface of the destination route). • Multiple peers may be configured. **Note** You must have a DNS server configured and available to use the *hostname* argument.
Step 6	**mode** {**client** | **network-extension**} **Example:** `Device(config-crypto-ezvpn)# mode client`	Specifies the type of VPN connection that should be made. • **client—**Specifies that the device is configured for VPN client operation, using NAT or PAT address translation. Client operation is the default if the type of VPN connection is not specified • **network-extension—**Specifies that the device is to become a remote extension of the enterprise network at the destination of the VPN connection.
Step 7	**exit** **Example:** `Device (config-crypto-ezvpn)# exit`	Exits Cisco Easy VPN Remote configuration mode.
Step 8	**interface** *type number* **Example:** `Device (config)# interface Ethernet1`	Enters interface configuration mode for the interface. • This interface will become the outside interface for the NAT or PAT translation.
Step 9	**crypto ipsec client ezvpn** *name* [**outside**] **Example:** `Device (config-if)# crypto ipsec client ezvpn easy_vpn_remote1 outside`	Assigns the Cisco Easy VPN Remote configuration to the interface. • This configuration automatically creates the necessary NAT or PAT translation parameters and initiates the VPN connection (if you are in client mode). **Note** The inside interface must be specified on Cisco 1700 and higher platforms.
Step 10	**end** **Example:** `Device (config-if)# end`	Exits interface configuration mode and returns to privileged EXEC mode.

Verifying the Cisco Easy VPN Configuration

To verify that the Cisco Easy VPN Remote configuration has been correctly configured, that the configuration has been assigned to an interface, and that the IPsec VPN tunnel has been established, perform the following steps.

SUMMARY STEPS

1. **show crypto ipsec client ezvpn**
2. **show ip nat statistics**

DETAILED STEPS

Step 1 show crypto ipsec client ezvpn

Example:

```
Device# show crypto ipsec client ezvpn

Tunnel name : hw1
Inside interface list: FastEthernet0/0, Serial0/0,
Outside interface: Serial1/0
Current State: IPSEC_ACTIVE
Last Event: SOCKET_UP
Address: 10.0.0.5
Mask: 255.255.255.255
Default Domain: cisco.com
Tunnel name : hw2
Inside interface list: Serial0/1,
Outside interface: Serial1/1
Current State: IPSEC_ACTIVE
Last Event: SOCKET_UP
Default Domain: cisco.com
```

If the IPSEC_ACTIVE is displayed in your output, everything is operating as expected.

Step 2 show ip nat statistics

Example:

```
Device# show ip nat statistics

Total active translations: 0 (0 static, 0 dynamic; 0 extended)
Outside interfaces:
  cable-modem0
Inside interfaces:
  Ethernet0
Hits: 1489  Misses: 1
Expired translations: 1
Dynamic mappings:
-- Inside Source
access-list 198 pool enterprise refcount 0
 pool enterprise: netmask 255.255.255.0
        start 192.168.1.90 end 192.168.1.90
        type generic, total addresses 1, allocated 0 (0%), misses 0\
```

Displays the NAT or PAT configuration that was automatically created for the VPN connection using the command. The “Dynamic mappings” field of this display provides details for the NAT or PAT translation that occurs on the VPN tunnel.

Configuring the Save Password

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **password encryption aes**
4. **crypto ipsec client ezvpn** *name*
5. **username** *name* **password** {**0** | **6**} *password*
6. **end**
7. **show running-config**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**password encryption aes** **Example:** `Device (config)# password encryption aes`	Enables a type 6 encrypted preshared key.
Step 4	**crypto ipsec client ezvpn** *name* **Example:** `Device (config)# crypto ipsec client ezvpn ezvpn1`	Creates a Cisco Easy VPN remote configuration and enters the Cisco Easy VPN remote configuration mode.
Step 5	**username** *name* **password** {**0**	**6**} *password* **Example:** `Device (config-crypto-ezvpn)# username server_1 password 0 blue`	Allows you to save your Xauth password locally on the PC. • The **0** keyword specifies that an unencrypted password will follow. • The **6** keyword specifies that an encrypted password will follow. • The *password* argument is the unencrypted (cleartext) user password.

	Command or Action	Purpose
Step 6	**end** **Example:** `Device (config-crypto-ezvpn)# end`	Exits the Cisco Easy VPN remote configuration mode and returns to privileged EXEC mode.
Step 7	**show running-config** **Example:** `Device# show running-config`	Displays the contents of the configuration file that is currently running.

Configuring Manual Tunnel Control

To configure control of IPsec VPN tunnels manually so that you can establish and terminate the IPsec VPN tunnels on demand, perform the following steps.

Note CLI is one option for connecting the tunnel. The preferred method is via the web interface (using SDM).

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **crypto ipsec client ezvpn** *name*
4. **connect** [**auto** | **manual**]
5. **end**
6. **crypto ipsec client ezvpn connect** *name*

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.

	Command or Action	Purpose
Step 3	**crypto ipsec client ezvpn** *name* **Example:** `Device (config)# crypto ipsec client ezvpn easy vpn remote1`	Assigns a Cisco Easy VPN remote configuration to an interface and enters Cisco Easy VPN Remote configuration mode. • The *name* argument specifies the configuration name to be assigned to the interface.
Step 4	**connect** [**auto** | **manual**] **Example:** `Device (config-crypto-ezvpn)# connect manual`	Connects the VPN tunnel. Specify **manual** to configure manual tunnel control. • Automatic is the default; you do not need to use the **manual** keyword if your configuration is automatic.
Step 5	**end** **Example:** `Device (config-crypto-ezvpn)# end`	Exits Cisco Easy VPN Remote configuration mode and returns to privileged EXEC mode.
Step 6	**crypto ipsec client ezvpn connect** *name* **Example:** `Device# crypto ipsec client ezvpn connect easy vpn remote1`	Connects a given Cisco Easy VPN remote configuration. • The *name* argument specifies the IPsec VPN tunnel name. **Note** If the tunnel name is not specified, the active tunnel is connected. If there is more than one active tunnel, the command fails with an error requesting that you specify the tunnel name.

Configuring Automatic Tunnel Control

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **crypto ipsec client ezvpn** *name*
4. **connect** [**auto** | **manual**]
5. **end**
6. **crypto ipsec client ezvpn connect** *name*

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable**	Enables privileged EXEC mode.

	Command or Action	Purpose
	Example: `Device> enable`	• Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**crypto ipsec client ezvpn** *name* **Example:** `Device (config)# crypto ipsec client ezvpn easy vpn remote1`	Assigns a Cisco Easy VPN remote configuration to an interface and enters Cisco Easy VPN Remote configuration mode. • Specify the configuration name to be assigned to the interface.
Step 4	**connect** [**auto** | **manual**] **Example:** `Device (config-crypto-ezvpn)# connect auto`	Connects the VPN tunnel. • Specify **auto** to configure automatic tunnel control. Automatic is the default; you do not need to use this command if your configuration is automatic.
Step 5	**end** **Example:** `Device (config-crypto-ezvpn)# end`	Exits Cisco Easy VPN Remote configuration mode and returns to privileged EXEC mode.
Step 6	**crypto ipsec client ezvpn connect** *name* **Example:** `Device# crypto ipsec client ezvpn connect easy vpn remote1`	Connects a given Cisco Easy VPN remote configuration. • The *name* argument specifies the IPsec VPN tunnel name. **Note** If the tunnel name is not specified, the active tunnel is connected. If there is more than one active tunnel, the command fails with an error requesting that you specify the tunnel name.

Configuring Multiple Inside Interfaces

You can configure up to three inside interfaces for all platforms.

Note Multiple inside interfaces are supported only when the Cisco Easy VPN server and the Cisco Easy VPN client have the same type of Easy VPN configuration. In other words, both must use a Legacy Easy VPN configuration, or both must use a DVTI configuration.

You need to manually configure each inside interface using the following procedure.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *interface-name*
4. **exit**
5. **crypto ipsec client ezvpn** *name* [**outside** | **inside**]
6. **interface** *interface-name*
7. **exit**
8. **crypto ipsec client ezvpn** *name* [**outside** | **inside**]

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**interface** *interface-name* **Example:** `Device (config)# interface Ethernet0`	Selects the interface you want to configure by specifying the interface name and enters interface configuration mode.
Step 4	**exit** **Example:** `Device (config-if)# exit`	Exits interface configuration mode.
Step 5	**crypto ipsec client ezvpn** *name* [**outside**	**inside**] **Example:** `Device (config)# crypto ipsec client ezvpn easy vpn remote 1 inside`	Specifies the Cisco Easy VPN remote configuration name to be assigned to the first inside interface. • You must specify **inside** for each inside interface.

	Command or Action	Purpose
Step 6	**interface** *interface-name* **Example:** `Device (config)# interface Ethernet1`	Selects the next interface you want to configure by specifying the next interface name and enters interface configuration mode.
Step 7	**exit** **Example:** `Device (config-if)# exit`	Exits interface configuration mode.
Step 8	**crypto ipsec client ezvpn** *name* [**outside** | **inside**] **Example:** `Device (config)# crypto ipsec client ezvpn easy vpn remote2 inside`	Specifies the Cisco Easy VPN remote configuration name to be assigned to the next inside interface. • You must specify **inside** for each inside interface. Repeat Step 3 through Step 4 to configure an additional tunnel if desired.

Configuring Multiple Outside Interfaces

You can configure multiple tunnels for outside interfaces, setting up a tunnel for each outside interface. You can configure a maximum of four tunnels using the following procedure for each outside interface.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *interface-name*
4. **exit**
5. **crypto ipsec client ezvpn** *name* [**outside** | **inside**]
6. **interface** *interface-name*
7. **exit**
8. **crypto ipsec client ezvpn** *name* [**outside** | **inside**]

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable**	Enables privileged EXEC mode.

	Command or Action	Purpose
	Example: `Device> enable`	• Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**interface** *interface-name* **Example:** `Device (config)# interface Ethernet0`	Selects the first outside interface you want to configure by specifying the interface name and enters interface configuration mode.
Step 4	**exit** **Example:** `Device (config-if)# exit`	Exits interface configuration mode.
Step 5	**crypto ipsec client ezvpn** *name* [**outside** | **inside**] **Example:** `Device (config)# crypto ipsec client ezvpn easy vpn remote1 outside`	Specifies the Cisco Easy VPN remote configuration name to be assigned to the first outside interface. • Specify **outside** (optional) for each outside interface. If neither **outside** nor **inside** is specified for the interface, the default is **outside**.
Step 6	**interface** *interface-name* **Example:** `Device (config)# interface Ethernet1`	Selects the next outside interface you want to configure by specifying the next interface name.
Step 7	**exit** **Example:** `Device (config-if)# exit`	Exits interface configuration mode.
Step 8	**crypto ipsec client ezvpn** *name* [**outside** | **inside**] **Example:** `Device (config)# crypto ipsec client ezvpn easy vpn remote2 outside`	Specifies the Cisco Easy VPN remote configuration name to be assigned to the next outside interface. • Specify **outside** (optional) for each outside interface. If neither **outside** nor **inside** is specified for the interface, the default is **outside**. • Repeat Step 3 through Step 4 to configure additional tunnels if desired.

	Command or Action	Purpose

Configuring Multiple Subnet Support

When configuring multiple subnet support, you must first configure an access list to define the actual subnets to be protected. Each source subnet or mask pair indicates that all traffic that is sourced from this network to any destination is protected by IPsec.

Note Multiple subnets are not supported in client mode. This functionality is supported only when the Cisco Easy VPN server and the Cisco Easy VPN client have the same type of Easy VPN configuration. In other words, both must use a Legacy Easy VPN configuration, or both must use a dVTI configuration.

After you have defined the subnets, you must configure the crypto IPsec client EZVPN profile to use the ACLs.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *interface-name*
4. **exit**
5. **crypto ipsec client ezvpn** *name*
6. **acl** {*acl-name* | *acl-number*}

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**interface** *interface-name* **Example:** `Device (config)# interface Ethernet1`	Selects the interface you want to configure by specifying the interface name and enters interface configuration mode.

	Command or Action	Purpose
Step 4	**exit** **Example:** `Device (config-if)# exit`	Exits interface configuration mode.
Step 5	**crypto ipsec client ezvpn** *name* **Example:** `Device (config)# crypto ipsec client ezvpn ez1`	Creates a Cisco Easy VPN remote configuration and enters crypto Easy VPN configuration mode.
Step 6	**acl** {*acl-name* | *acl-number*} **Example:** `Device (config-crypto-ezvpn)# acl acl-list1`	Specifies multiple subnets in a VPN tunnel.

Configuring Proxy DNS Server Support

As a way of implementing the use of the DNS addresses of the ISP when the WAN connection is down, the router in a Cisco Easy VPN remote configuration can be configured to act as a proxy DNS server. To enable the proxy DNS server functionality with the **ip dns server** command, perform the following steps.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip dns server**
4. **exit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.

	Command or Action	Purpose
Step 3	**ip dns server** **Example:** `Device (config)# ip dns server`	Enables the device to act as a proxy DNS server. **Note** This definition is Cisco specific.
Step 4	**exit** **Example:** `Device (config)# exit`	Exits global configuration mode and returns to privileged EXEC mode.

What to Do Next

After configuring the router, you configure the Cisco IOS Easy VPN server as follows:

- Under the **crypto isakmp client configuration group** command, configure the **dns** command as in the following example:

dns A.B.C.D A1.B1.C1.D1

These DNS server addresses should be pushed from the server to the Cisco Easy VPN remote and dynamically added to or deleted from the running configuration of the router.

For information about general DNS server functionality in Cisco IOS software applications, see the "Configuring DNS" chapter of the *Catalyst 6500 Series Software Configuration Guide* and the Configuring DNS on Cisco Routers design technical note.

Configuring Dial Backup

Note The Dial Backup feature is not available in Cisco IOS Release 12.3(11)T.

SUMMARY STEPS

1. Create the Easy VPN dial backup configuration.
2. Add the backup command details to the primary configuration.
3. Apply the backup Easy VPN configuration to the dial backup outside interface (for example, serial, async, or dialer).
4. Apply the Easy VPN profile to the inside interfaces (there can be more than one).

DETAILED STEPS

	Command or Action	Purpose
Step 1	Create the Easy VPN dial backup configuration.	For details about the backup configuration, see the section "Dial Backup, on page 25."
Step 2	Add the backup command details to the primary configuration.	Use the **backup** command and **track** keyword of the **crypto ipsec client ezvpn** command.
Step 3	Apply the backup Easy VPN configuration to the dial backup outside interface (for example, serial, async, or dialer).	For details about applying the backup configuration to the dial backup outside interface, see the section "Configuring Multiple Outside Interfaces, on page 46."
Step 4	Apply the Easy VPN profile to the inside interfaces (there can be more than one).	For details about applying the Easy VPN profile to the inside interfaces, see the section "Configuring Multiple Inside Interfaces, on page 44."

Resetting a VPN Connection

To reset the VPN connection, perform the following steps. The **clear** commands can be configured in any order or independent of one another.

SUMMARY STEPS

1. **enable**
2. **clear crypto ipsec client ezvpn**
3. **clear crypto sa**
4. **clear crypto isakmp**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**clear crypto ipsec client ezvpn** **Example:** `Device# clear crypto ipsec client ezvpn`	Resets the Cisco Easy VPN remote state machine and brings down the Cisco Easy VPN remote connection on all interfaces or on a given interface (tunnel).

	Command or Action	Purpose
Step 3	**clear crypto sa** **Example:** `Device# clear crypto sa`	Deletes IPsec SAs.
Step 4	**clear crypto isakmp** **Example:** `Device# clear crypto isakmp`	Clears active IKE connections.

Monitoring and Maintaining VPN and IKE Events

SUMMARY STEPS

1. **enable**
2. **debug crypto ipsec client ezvpn**
3. **debug crypto ipsec**
4. **debug crypto isakmp**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**debug crypto ipsec client ezvpn** **Example:** `Device# debug crypto ipsec client ezvpn`	Displays information showing the configuration and implementation of the Cisco Easy VPN Remote feature.
Step 3	**debug crypto ipsec** **Example:** `Device# debug crypto ipsec`	Displays IPsec events.

	Command or Action	Purpose
Step 4	**debug crypto isakmp** **Example:** `Device# debug crypto isakmp`	Displays messages about IKE events.

Configuring a Virtual Interface

Before the virtual interface is configured, ensure that the Easy VPN profile is not applied on any outside interface. Remove the Easy VPN profile from the outside interface and then configure the virtual interface.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface virtual-template** *number* **type** *type-of-virtual-template*
4. **tunnel mode ipsec ipv4**
5. **exit**
6. **crypto ipsec client ezvpn** *name*
7. **virtual-interface** *virtual-template-number*

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**interface virtual-template** *number* **type** *type-of-virtual-template* **Example:** `Device (config)# interface virtual-template1 type tunnel`	(Optional) Creates a virtual template of the type tunnel and enters interface configuration mode. • Steps 3, 4, and 5 are optional, but if one is configured, they must all be configured.

	Command or Action	Purpose
Step 4	**tunnel mode ipsec ipv4** **Example:** `Device (if-config)# tunnel mode ipsec ipv4`	(Optional) Configures the tunnel that does the IPsec tunneling.
Step 5	**exit** **Example:** `Device (if-config)# exit`	(Optional) Exits interface (virtual-tunnel) configuration mode.
Step 6	**crypto ipsec client ezvpn** *name* **Example:** `Device (config)# crypto ipsec client ezvpn EasyVPN1`	Creates a Cisco Easy VPN remote configuration and enters the Cisco Easy VPN remote configuration mode.
Step 7	**virtual-interface** *virtual-template-number* **Example:** `Device (config-crypto-ezvpn)# virtual-interface 3`	Instructs the Easy VPN remote to create a virtual interface to be used as an outside interface. If the virtual template number is specified, the virtual-access interface is derived from the virtual interface that was specified. If a virtual template number is not specified, a generic virtual-access interface is created.

Troubleshooting Dual Tunnel Support

The following **debug** and **show** commands may be used to troubleshoot your dual-tunnel configuration.

SUMMARY STEPS

1. **enable**
2. **debug crypto ipsec client ezvpn**
3. **debug ip policy**
4. **show crypto ipsec client ezvpn**
5. **show ip interface**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable**	Enables privileged EXEC mode.

	Command or Action	Purpose
	Example: `Device> enable`	• Enter your password if prompted.
Step 2	**debug crypto ipsec client ezvpn** **Example:** `Device# debug crypto ipsec client ezvpn`	Displays information about Cisco Easy VPN remote connections.
Step 3	**debug ip policy** **Example:** `Device# debug ip policy`	Displays IP policy routing packet activity.
Step 4	**show crypto ipsec client ezvpn** **Example:** `Device# show crypto ipsec client ezvpn`	Displays the Cisco Easy VPN Remote configuration.
Step 5	**show ip interface** **Example:** `Device# show ip interface`	Displays the usability status of interfaces that are configured for IP.

Configuring Reactivate (a Default) Primary Peer

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **crypto ipsec client ezvpn** *name*
4. **peer** {*ip-address* | *hostname*} [**default**]
5. **idle-time** *idle-time*
6. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable**	Enables privileged EXEC mode.

	Command or Action	Purpose
	Example: `Device> enable`	• Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**crypto ipsec client ezvpn** *name* **Example:** `Device (config)# crypto ipsec client ezvpn ez1`	Creates a Cisco Easy VPN remote configuration and enters crypto Easy VPN configuration mode.
Step 4	**peer** {*ip-address* | *hostname*} [**default**] **Example:** `Device (config-crypto-ezvpn)# peer 10.2.2.2 default`	Sets the peer IP address or hostname for the VPN connection. • A hostname can be specified only when the device has a DNS server available for hostname resolution. • The **peer** command may be input multiple times. However, only one default or primary peer entry can exist at a time (for example, 10.2.2.2 default). • The **default** keyword defines the peer as the primary peer.
Step 5	**idle-time** *idle-time* **Example:** `Device (config-crypto-ezvpn)# idle-time 60`	(Optional) Idle time in seconds after which an Easy VPN tunnel is brought down. • Idle time=60 through 86400 seconds. **Note** If idle time is configured, the tunnel for the primary server is not brought down.
Step 6	**end** **Example:** `Device (config-crypto-ezvpn)# end`	Exits crypto Easy VPN configuration mode and returns to privileged EXEC mode.

Configuring Identical Addressing Support

Configuring Identical Addressing Support comprises the following tasks:

- Defining the Easy VPN remote in network-extension mode and enabling **nat allow**.
- Assigning the Cisco Easy VPN Remote configuration to the Outside interface.

- Creating a loopback interface and assigning the Cisco Easy VPN Remote configuration to the Inside interface of the loopback interface.
- Configuring a one-to-one static NAT translation for each host that needs to be accessible from the EasyVPN server-side network or from other client locations.
- Configuring dynamic overloaded NAT or PAT using an access list for all the desired VPN traffic. The NAT or PAT traffic is mapped to the Easy VPN inside interface IP address.
- And, if split-tunneling is required, using the **nat acl** command to enable split-tunneling for the traffic specified by the *acl-name* or the *acl-number* argument. The ACL is the same as the ACL used by the NAT or PAT mapping in the preceding bullet item.

Before You Begin

Easy VPN Remote must be configured in network extension mode before you can configure the Identical Addressing Support feature.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **crypto ipsec client ezvpn** *name*
4. **mode network-extension**
5. **nat allow**
6. **exit**
7. **interface** *interface*
8. **crypto ipsec client ezvpn** *name* **outside**
9. **exit**
10. **interface** *interface*
11. **ip address** *ip mask*
12. **crypto ipsec client ezvpn** *name* **inside**
13. **exit**
14. **ip nat inside source static** *local-ip global-ip*
15. **ip nat inside source list** {*acl-name* | *acl-number*} **interface** *interface* **overload**
16. **crypto ipsec client ezvpn** *name*
17. **nat acl** {*acl-name* | *acl-number*}
18. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.

	Command or Action	Purpose
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**crypto ipsec client ezvpn** *name* **Example:** `Device (config)# crypto ipsec client ezvpn easyclient`	Creates a remote configuration and enters Cisco Easy VPN Remote configuration mode.
Step 4	**mode network-extension** **Example:** `Device (config-crypto-ezvpn)# mode network-extension`	Configures Easy VPN client in network-extension mode.
Step 5	**nat allow** **Example:** `Device (config-crypto-ezvpn)# nat allow`	Allows NAT to be integrated with Easy VPN and enables the Identical Addressing feature.
Step 6	**exit** **Example:** `Device (config-crypto-ezvpn)# exit`	Exits Cisco Easy VPN Remote configuration mode.
Step 7	**interface** *interface* **Example:** `Device (config)# interface Ethernet1`	Enters interface configuration mode for the interface. • This interface will become the outside interface for the NAT or PAT translation.
Step 8	**crypto ipsec client ezvpn** *name* **outside** **Example:** `Device (config-if)# crypto ipsec client ezvpn easyclient outside`	Assigns the Cisco Easy VPN Remote configuration to the outside interface. • This configuration automatically creates the necessary NAT or PAT translation parameters and initiates the VPN connection (if you are in client mode).
Step 9	**exit** **Example:** `Device (config-if)# exit`	Exits interface configuration mode.
Step 10	**interface** *interface*	Enters interface configuration mode for the loopback interface.

	Command or Action	Purpose
	Example: `Device (config)# interface Loopback0`	• This interface will become the inside interface for the NAT or PAT translation.
Step 11	**ip address** *ip mask* **Example:** `Device (config-if)# ip address 10.1.1.1 255.255.255.252`	Assigns the IP address and mask to the loopback interface.
Step 12	**crypto ipsec client ezvpn** *name* **inside** **Example:** `Device (config-if)# crypto ipsec client ezvpn easyclient inside`	Assigns the Cisco Easy VPN Remote configuration to the inside interface.
Step 13	**exit** **Example:** `Device (config-if)# exit`	Exits interface configuration mode.
Step 14	**ip nat inside source static** *local-ip global-ip* **Example:** `Device (config)# ip nat inside source static 10.10.10.10 5.5.5.5`	Configure a one-to-one static NAT translation for each host that needs to be accessible from the Easy VPN server side network, or from other client locations.
Step 15	**ip nat inside source list** {*acl-name* | *acl-number*} **interface** *interface* **overload** **Example:** `Device (config)# ip nat inside source list 100 interface Loopback0 overload`	Configure dynamic overloaded NAT or PAT, which uses an ACL for all the desired VPN traffic. The NAT and PAT traffic is mapped to the Easy VPN inside interface IP address. • The *acl-name* argument is the name of the ACL. • The *acl-number* argument is the number of the ACL.
Step 16	**crypto ipsec client ezvpn** *name* **Example:** `Device (config)# crypto ipsec client ezvpn easyclient`	(Optional, if using split tunneling) Enters Cisco Easy VPN Remote configuration mode.
Step 17	**nat acl** {*acl-name* | *acl-number*} **Example:** `Device (config-crypto-ezvpn)# nat acl 100`	(Optional, if using split tunneling) Enables split-tunneling for the traffic specified by the *acl-name* or the *acl-number* argument. The ACL is the same as the ACL used by the NAT or PAT mapping in the Step 15. • The *acl-name* argument is the name of the ACL.

	Command or Action	Purpose
		• The *acl-number* argument is the number of the ACL.
Step 18	**end** **Example:** `Device (config-crypto-ezvpn)# end`	Exits Cisco Easy VPN Remote configuration mode and returns to privileged EXEC mode.

Configuring cTCP on an Easy VPN Client

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **crypto ctcp** [**keepalive** *number-of-seconds* | **port** *port-number*]
4. **crypto ipsec client ezvpn** *name*
5. **ctcp port** *port-number*
6. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**crypto ctcp** [**keepalive** *number-of-seconds*	**port** *port-number*] **Example:** `Device (config)# crypto ctcp keepalive 15`	Sets cTCP keepalive interval for the remote device. • *number-of-seconds*—Number of seconds between keepalives. The range is from 5 through 3600. • **port** *port-number*—Port number that cTCP listens to. Up to 10 numbers can be configured. **Note** The cTCP client has to send periodic keepalives to the server to keep NAT or firewall sessions alive.

	Command or Action	Purpose
Step 4	**crypto ipsec client ezvpn** *name* **Example:** `Device (config)# crypto ipsec client ezvpn ezvpn1`	Creates a Cisco Easy VPN remote configuration and enters Cisco Easy VPN remote configuration mode.
Step 5	**ctcp port** *port-number* **Example:** `Device (config-crypto-ezvpn)# ctcp port 200`	Sets the port number for cTCP encapsulation for Easy VPN. • *port-number*—Port number on the hub. The range is from 1 through 65535.
Step 6	**end** **Example:** `Device (config-crypto-ezvpn)# end`	Exits Cisco Easy VPN remote configuration mode and returns to privileged EXEC mode.

Configuring cTCP on an Easy VPN Client

Perform this task to restrict the client from sending traffic in clear text when a tunnel is down.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **crypto ipsec client ezvpn** *name*
4. **flow allow acl** [**name** | **number**]
5. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.

	Command or Action	Purpose
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**crypto ipsec client ezvpn** *name* **Example:** `Device (config)# crypto ipsec client ezvpn ezvpn1`	Creates a Cisco Easy VPN remote configuration and enters Cisco Easy VPN remote configuration mode.
Step 4	**flow allow acl** [**name** | **number**] **Example:** `Device (config-crypto-ezvpn)# flow allow acl 102`	Restricts the client from sending traffic in clear text when the tunnel is down. • *name*—Access list name. • *number*—Access list number. The range is from 100 through 199.
Step 5	**end** **Example:** `Device (config-crypto-ezvpn)# end`	Exits Cisco Easy VPN remote configuration mode and returns to privileged EXEC mode.

Web Interface Tasks

Configuring Web-Based Activation

To configure a LAN so that any HTTP requests coming from any of the PCs on the private LAN are intercepted, providing corporate users with access to the corporate Web page, perform the following steps.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **crypto ipsec client ezvpn** *name*
4. **xauth userid mode** {**http-intercept** | **interactive** | **local**}
5. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**crypto ipsec client ezvpn** *name* **Example:** `Device (config)# crypto ipsec client ezvpn easy vpn remote1`	Assigns a Cisco Easy VPN remote configuration to an interface and enters Cisco Easy VPN Remote configuration mode. • The *name* argument specifies the configuration name to be assigned to the interface.
Step 4	**xauth userid mode** {**http-intercept** | **interactive** | **local**} **Example:** `Device (config-crypto-ezvpn)# xauth userid mode http-intercept`	Specifies how the VPN device handles Xauth requests or prompts from the server.
Step 5	**end** **Example:** `Device (config-crypto-ezvpn)# end`	Exits Cisco Easy VPN Remote configuration mode and returns to privileged EXEC mode.

Monitoring and Maintaining Web-Based Activation

To monitor and maintain web-based activation, perform the following steps. (The **debug** and **show** commands may be used independently, or they may all be configured.)

SUMMARY STEPS

1. **enable**
2. **debug crypto ipsec client ezvpn**
3. **debug ip auth-proxy ezvpn**
4. **show crypto ipsec client ezvpn**
5. **show ip auth-proxy config**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**debug crypto ipsec client ezvpn** **Example:** `Device# debug crypto ipsec client ezvpn`	Displays information about the Cisco Easy VPN connection.
Step 3	**debug ip auth-proxy ezvpn** **Example:** `Device# debug ip auth-proxy ezvpn`	Displays information related to proxy authentication behavior for web-based activation.
Step 4	**show crypto ipsec client ezvpn** **Example:** `Device# show crypto ipsec client ezvpn`	Shows that the username and password used for user credentials during Xauth negotiations will be obtained by intercepting HTTP connections from the user.
Step 5	**show ip auth-proxy config** **Example:** `Device# show ip auth-proxy config`	Displays the auth-proxy rule that has been created and applied by Easy VPN.

Examples

The following is sample **debug** output for a typical situation in which a user has opened a browser and connected to the corporate website:

```
Device# debug ip auth-proxy ezvpn

Dec 10 12:41:13.335: AUTH-PROXY: New request received by EzVPN WebIntercept
! The following line shows the ip address of the user.
from 10.4.205.205
Dec 10 12:41:13.335: AUTH-PROXY:GET request received
Dec 10 12:41:13.335: AUTH-PROXY:Normal auth scheme in operation
Dec 10 12:41:13.335: AUTH-PROXY:Ezvpn is NOT active. Sending connect-bypass page to user
```

At this point, the user chooses “connect” on his or her browser:

```
Dec 10 12:42:43.427: AUTH-PROXY: New request received by EzVPN WebIntercept
from 10.4.205.205
Dec 10 12:42:43.427: AUTH-PROXY:POST request received
Dec 10 12:42:43.639: AUTH-PROXY:Found attribute <connect> in form
Dec 10 12:42:43.639: AUTH-PROXY:Sending POST data to EzVPN
Dec 10 12:42:43.639: EZVPN(tunnel22): Communication from Interceptor
```

```
  application.
Request/Response from 10.4.205.205, via Ethernet0
Dec 10 12:42:43.639:         connect: Connect Now
Dec 10 12:42:43.639: EZVPN(tunnel22): Received CONNECT from 10.4.205.205!
Dec 10 12:42:43.643: EZVPN(tunnel22): Current State: CONNECT_REQUIRED
Dec 10 12:42:43.643: EZVPN(tunnel22): Event: CONNECT
Dec 10 12:42:43.643: EZVPN(tunnel22): ezvpn_connect_request
```

Easy VPN contacts the server:

```
Dec 10 12:42:43.643: EZVPN(tunnel22): Found valid peer 192.168.0.1
Dec 10 12:42:43.643: EZVPN(tunnel22): Added PSK for address 192.168.0.1
Dec 10 12:42:43.643: EZVPN(tunnel22): New State: READY
Dec 10 12:42:44.815: EZVPN(tunnel22): Current State: READY
Dec 10 12:42:44.815: EZVPN(tunnel22): Event: IKE_PFS
Dec 10 12:42:44.815: EZVPN(tunnel22): No state change
Dec 10 12:42:44.819: EZVPN(tunnel22): Current State: READY
Dec 10 12:42:44.819: EZVPN(tunnel22): Event: CONN_UP
Dec 10 12:42:44.819: EZVPN(tunnel22): ezvpn_conn_up B8E86EC7 E88A8A18 D0D51422
  8AFF32B7
```

The server requests Xauth information:

```
Dec 10 12:42:44.823: EZVPN(tunnel22): No state change
Dec 10 12:42:44.827: EZVPN(tunnel22): Current State: READY
Dec 10 12:42:44.831: EZVPN(tunnel22): Event: XAUTH_REQUEST
Dec 10 12:42:44.831: EZVPN(tunnel22): ezvpn_xauth_request
Dec 10 12:42:44.831: EZVPN(tunnel22): ezvpn_parse_xauth_msg
Dec 10 12:42:44.831: EZVPN: Attributes sent in xauth request message:
Dec 10 12:42:44.831:         XAUTH_TYPE_V2(tunnel22): 0
Dec 10 12:42:44.831:         XAUTH_USER_NAME_V2(tunnel22):
Dec 10 12:42:44.831:         XAUTH_USER_PASSWORD_V2(tunnel22):
Dec 10 12:42:44.831:         XAUTH_MESSAGE_V2(tunnel22) <Enter Username and
Password.>
Dec 10 12:42:44.831: EZVPN(tunnel22): Requesting following info for xauth
Dec 10 12:42:44.831:         username:(Null)
Dec 10 12:42:44.835:         password:(Null)
Dec 10 12:42:44.835:         message:Enter Username and Password.
Dec 10 12:42:44.835: EZVPN(tunnel22): New State: XAUTH_REQ
```

The username and password prompt are displayed in the browser of the user:

```
Dec 10 12:42:44.835: AUTH-PROXY: Response to POST  is CONTINUE
Dec 10 12:42:44.839: AUTH-PROXY: Displayed POST response successfully
Dec 10 12:42:44.843: AUTH-PROXY:Served POST response to the user
```

When the user enters his or her username and password, the following is sent to the server:

```
Dec 10 12:42:55.343: AUTH-PROXY: New request received by EzVPN WebIntercept
  from 10.4.205.205
Dec 10 12:42:55.347: AUTH-PROXY:POST request received
Dec 10 12:42:55.559: AUTH-PROXY:No of POST parameters is 3
Dec 10 12:42:55.559: AUTH-PROXY:Found attribute <username> in form
Dec 10 12:42:55.559: AUTH-PROXY:Found attribute <password> in form
Dec 10 12:42:55.559: AUTH-PROXY:Found attribute <ok> in form
Dec 10 12:42:55.563: AUTH-PROXY:Sending POST data to EzVPN
Dec 10 12:42:55.563: EZVPN(tunnel22): Communication from Interceptor application.
Request/Response from 10.4.205.205, via Ethernet0
Dec 10 12:42:55.563:         username:http
Dec 10 12:42:55.563:         password:<omitted>
Dec 10 12:42:55.563:         ok:Continue
Dec 10 12:42:55.563: EZVPN(tunnel22): Received usename|password from 10.4.205.205!
Dec 10 12:42:55.567: EZVPN(tunnel22): Current State: XAUTH_PROMPT
Dec 10 12:42:55.567: EZVPN(tunnel22): Event: XAUTH_REQ_INFO_READY
Dec 10 12:42:55.567: EZVPN(tunnel22): ezvpn_xauth_reply
Dec 10 12:42:55.567:         XAUTH_TYPE_V2(tunnel22): 0
Dec 10 12:42:55.567:         XAUTH_USER_NAME_V2(tunnel22): http
Dec 10 12:42:55.567:         XAUTH_USER_PASSWORD_V2(tunnel22): <omitted>
Dec 10 12:42:55.567: EZVPN(tunnel22): New State: XAUTH_REPLIED
Dec 10 12:42:55.891: EZVPN(tunnel22): Current State: XAUTH_REPLIED
Dec 10 12:42:55.891: EZVPN(tunnel22): Event: XAUTH_STATUS
Dec 10 12:42:55.891: EZVPN(tunnel22): xauth status received: Success
```

After using the tunnel, the user chooses “Disconnect”:

```
Dec 10 12:48:17.267: EZVPN(tunnel22): Received authentic disconnect credential
Dec 10 12:48:17.275: EZVPN(): Received an HTTP request: disconnect
Dec 10 12:48:17.275: %CRYPTO-6-EZVPN_CONNECTION_DOWN: (Client)  User=
  Group=tunnel22  Client_public_addr=192.168.0.13  Server_public_addr=192.168.0.1
  Assigned_client_addr=10.3.4.5
```

Show Output Before the User Is Connected to the Tunnel

The following output from the two **show** commands (**show crypto ipsec client ezvpn** and **show ip auth-proxy config**) displays what you might see before a user is connected to a VPN tunnel:

```
Device# show crypto ipsec client ezvpn tunnel22

Tunnel name : tunnel22
Inside interface list: Ethernet0
Outside interface: Ethernet1
Current State: CONNECT_REQUIRED
Last Event: RESET
Save Password: Disallowed
! Note the next line.
        XAuth credentials: HTTP intercepted
        HTTP return code : 200
        IP addr being prompted: 0.0.0.0
Current EzVPN Peer: 192.168.0.1
Router# show ip auth-proxy config
Authentication global cache time is 60 minutes
Authentication global absolute time is 0 minutes
Authentication Proxy Watch-list is disabled
Authentication Proxy Rule Configuration
! Note that the next line is the Easy VPN-defined internal rule.
    Auth-proxy name ezvpn401***
      Applied on Ethernet0
      http list not specified inactivity-timer 60 minutes
```

Show Output After the User Is Connected to the Tunnel

The following output from the two **show** commands (**show crypto ipsec client ezvpn** and **show ip auth-proxy config**) displays what you might see after the user has been connected to the tunnel:

```
Device# show crypto ipsec client ezvpn tunnel22

Tunnel name : tunnel22
Inside interface list: Ethernet0
Outside interface: Ethernet1
Current State: IPSEC_ACTIVE
Last Event: SOCKET_UP
Address: 10.3.4.5
Mask: 255.255.255.255
Save Password: Disallowed
        XAuth credentials: HTTP intercepted
        HTTP return code : 200
        IP addr being prompted: 192.168.0.0
Current EzVPN Peer: 192.168.0.1
Router# show ip auth-proxy config
Authentication global cache time is 60 minutes
Authentication global absolute time is 0 minutes
Authentication Proxy Watch-list is disabled
Auth-proxy name ezvpnWeb*** (EzVPN-defined internal rule)
http list not specified inactivity-timer 60 minutes
```

Troubleshooting the VPN Connection

Troubleshooting a VPN Connection Using the Cisco Easy VPN Remote Feature

To troubleshoot a VPN connection created using the Cisco Easy VPN Remote feature, use the following suggested techniques.

- Be aware that any changes to an active Cisco Easy VPN remote configuration or IP address changes to the involved interfaces, such as adding or removing an inside interface, result in a reset of the Cisco Easy VPN Remote connection.
- Enable debugging of the Cisco Easy VPN Remote feature using the **debug crypto ipsec client ezvpn** command.
- Enable debugging of IKE events using the **debug crypto ipsec** and **debug crypto isakmp** commands.
- Display the active IPsec VPN connections using the **show crypto engine connections active** command.
- To reset the VPN connection, use the **clear crypto ipsec client ezvpn** command. If you have debugging enabled, you might prefer to use the **clear crypto sa** and **clear crypto isakmp** commands.

Troubleshooting the Client Mode of Operation

The following information may be used to troubleshoot the Easy VPN Remote configuration for the client mode of operation.

In client mode, the Cisco Easy VPN Remote feature automatically configures the NAT or PAT translation and access lists that are needed to implement the VPN tunnel. These configurations are automatically created when the IPsec VPN connection is initiated. When the tunnel is torn down, the NAT or PAT and access list configurations are automatically deleted.

The NAT or PAT configuration is created with the following assumptions:

- The **ip nat inside** command is applied to all inside interfaces, including default inside interfaces. The default inside interface is the Ethernet 0 interface (for the Cisco 806, Cisco 826, Cisco 827, Cisco 828, Cisco 831, Cisco 836, and Cisco 837 routers).
- The **ip nat outside** command is applied to the interface that is configured with the Cisco Easy VPN Remote configuration. On the Cisco 800 series and Cisco 1700 series routers, the outside interface is configured with the Cisco Easy VPN Remote configuration. On the Cisco 1700 series routers, Cisco 2600 series routers, Cisco 3600 series routers, and Cisco 3700 series routers, multiple outside interfaces can be configured.

Note Configuring the **ip nat inside** and **ip nat outside** commands on the EasyVPN outside and inside interfaces respectively leads to undefined behavior. This configuration is considered invalid.

Tip The NAT or PAT translation and access list configurations that are created by the Cisco Easy VPN Remote feature are not written to either the startup configuration or running configuration files. These configurations, however, can be displayed using the **show ip nat statistics** and **show access-list** commands.

Troubleshooting Remote Management

To troubleshoot remote management of the VPN remote, use the **show ip interface** command. Using the **brief** keyword, you can verify that the loopback has been removed and that the interface is shown correctly.

Examples

Following is a typical example of output from the **show ip interface** command.

```
Device# show ip interface brief

Interface                  IP-Address      OK? Method Status                Protocol
Ethernet0                  unassigned      YES NVRAM  administratively down down

Ethernet1                  10.0.0.11       YES NVRAM  up                    up

Loopback0                  192.168.6.1     YES manual up                    up

Loopback1                  10.12.12.12     YES NVRAM  up                    up
Router# show ip interface brief
Interface                  IP-Address      OK? Method Status                Protocol
Ethernet0                  unassigned      YES NVRAM  administratively down down
Ethernet1                  10.0.0.11       YES NVRAM  up                    up
Loopback1                  10.12.12.12     YES NVRAM  up                    up
```

Troubleshooting Dead Peer Detection

To troubleshoot dead peer detection, use the **show crypto ipsec client ezvpn** command.

Examples

The following typical output displays the current server and the peers that have been pushed by the Easy VPN server:

```
Device# show crypto ipsec client ezvpn

Easy VPN Remote Phase: 4
Tunnel name : ez1
Inside interface list: Loopback1,
Outside interface: Ethernet1
Current State: IPSEC_ACTIVE
Last Event: CONNECT
Address: 192.168.6.5
Mask: 255.255.255.255
DNS Primary: 10.2.2.2
DNS Secondary: 10.2.2.3
NBMS/WINS Primary: 10.6.6.6
Default Domain: cisco.com
Save Password: Allowed
Current EzVPN Peer:10.0.0.110
Backup Gateways
```

```
(0): green.cisco.com
(1): blue
```

Configuration Examples for Cisco Easy VPN Remote

Easy VPN Remote Configuration Examples

Client Mode Configuration Examples

The examples in this section show configurations for the Cisco Easy VPN Remote feature in client mode. Also shown are the Cisco IOS Easy VPN server configurations that correspond to these client configurations.

Note Typically, users configure the Cisco 800 series routers with the SDM or CRWS web interface, not by entering CLI commands. However, the configurations shown here for the Cisco 800 series routers display typical configurations that can be used if manual configuration is desired.

Cisco Easy VPN Client in Client Mode (Cisco 831) Example

In the following example, a Cisco 831 router is configured as an Easy VPN remote using the Cisco Easy VPN Remote feature in client mode. This example shows the following components of the Cisco Easy VPN Remote configuration:

- DHCP server pool--The **ip dhcp pool** command creates a pool of IP addresses to be assigned to the PCs connected to the Ethernet 0 interface of the router. The pool assigns addresses in the class C private address space (192.168.100.0) and configures each PC so that its default route is 192.168.100.1, which is the IP address assigned to the Ethernet interface of the router. The DHCP lease period is one day.
- Cisco Easy VPN remote configuration--The first **crypto ipsec client ezvpn easy vpn remote** command (global configuration mode) creates a Cisco Easy VPN remote configuration named “easy vpn remote.” This configuration specifies the group name “easy vpn remote-groupname” and the shared key value “easy vpn remote-password,” and it sets the peer destination to the IP address **192.185.0.5** (which is the address assigned to the interface connected to the Internet on the destination peer router). The Cisco Easy VPN Remote configuration is configured for the default **client** mode.

Note If DNS is also configured on the router, the **peer** keyword option also supports a hostname instead of an IP address.

- The second **crypto ipsec client ezvpn easy vpn remote** command (interface configuration mode) assigns the Cisco Easy VPN Remote configuration to the Ethernet 1 interface so that all traffic that is received and transmitted on that interface is sent through the VPN tunnel.

```
! Cisco Router Web Setup Template
!
```

```
no service pad
no service tcp-small-servers
no service udp-small-servers
service timestamps debug uptime
service timestamps log uptime
service password-encryption
!
hostname 806Router
!
!
ip subnet-zero
ip domain-lookup
ip dhcp excluded-address 10.10.10.1
!
ip dhcp pool CLIENT
   import all
   network 10.10.10.0 255.255.255.255
   default-router 10.10.10.1
   lease 1 0 0
!
!
crypto ipsec client ezvpn easy_vpn_remote
 peer 192.168.0.5
 group easy_vpn_remote_groupname key easy_vpn_remote_password
 mode client
!
!
interface Ethernet0
 ip address 10.10.10.1 255.255.255.255
 no cdp enable
 hold-queue 32 in
!
interface Ethernet1
 ip address dhcp
 no cdp enable
 crypto ipsec client ezvpn easy_vpn_remote
!
ip classless
ip http server
!
!
ip route 10.0.0.0 10.0.0.0 Ethernet1
!
line con 0
 exec-timeout 120 0
 stopbits 1
line vty 0 4
 exec-timeout 0 0
 login local
```

Cisco Easy VPN Client in Client Mode (Cisco 837) Example

In the following example, a Cisco 837 router is configured as an Easy VPN remote using the Cisco Easy VPN Remote feature in the client mode of operation. This example shows the following components of the Cisco Easy VPN remote configuration:

- PPPoE configuration--The ATM 0 interface is configured to support PPPoE connections over the Dialer 1 virtual interface. Because the interfaces use PPPoE, a DHCP IP address pool is not required to provide IP addresses to the connected PCs.
- Cisco Easy VPN Remote configuration--The first **crypto ipsec client ezvpn** command (global configuration mode) creates a Cisco Easy VPN remote configuration named “easy vpn remote.” This configuration specifies the group name “easy vpn remote-groupname” and the shared key value of “easy vpn remote-password,” and it sets the peer destination to the IP address 10.0.0.5 (which is the address assigned to the interface connected to the Internet on the destination peer router). The Cisco Easy VPN remote configuration is configured for the default client mode.

Note If DNS is also configured on the router, the **peer** keyword option also supports a hostname instead of an IP address.

- The second **crypto ipsec client ezvpn** command (interface configuration mode) assigns the Cisco Easy VPN remote configuration to the Dialer 1 interface so that all traffic received and transmitted on that interface is sent through the VPN tunnel.

```
version 12.2
no service pad
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname c827
!
!
mmi polling-interval 60
no mmi auto-configure
no mmi pvc
mmi snmp-timeout 180
ip subnet-zero
!
ip ssh time-out 120
ip ssh authentication-retries 3
vpdn enable
!
vpdn-group pppoe
 request-dialin
  protocol pppoe
 ip mtu adjust
!!
!
crypto ipsec client ezvpn easy_vpn_remote
 group easy_vpn_remote_groupname key easy_vpn_remote_password
 mode client
 peer 10.0.0.5
!!
!
interface Ethernet0
 ip address 10.0.0.117 255.0.0.0
 hold-queue 100 out
!
interface ATM0
 no ip address
 no atm ilmi-keepalive
 pvc 1/40
  pppoe-client dial-pool-number 1
 !
 dsl operating-mode auto
!
interface Dialer1
 ip address 10.0.0.3 255.0.0.0
 ip mtu 1492
 encapsulation ppp
 dialer pool 1
 crypto ipsec client ezvpn easy_vpn_remote
!
ip classless
ip route 0.0.0.0 0.0.0.0 ATM0
ip route 0.0.0.0 0.0.0.0 Dialer1 permanent
ip route 10.0.0.0 255.0.0.0 10.0.0.13
ip http server
ip pim bidir-enable
!
line con 0
```

```
 stopbits 1
line vty 0 4
 login
!
scheduler max-task-time 5000
end
```

Cisco Easy VPN Client in Client Mode (Cisco 1700 Series) Example

In the following example, a Cisco 1753 router is configured as an Easy VPN remote using the Cisco Easy VPN Remote feature in the client mode of operation. This example shows a running configuration of a Cisco 1753 that has two inside interfaces and one outside interface on one tunnel. The **connect auto** command manually establishes the IPsec VPN tunnel.

```
Device# show running-config

Building configuration...
Current configuration : 881 bytes
!
version 12.2
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname mma-1753
!
!
memory-size iomem 15
ip subnet-zero
!!
!
ip ssh time-out 120
ip ssh authentication-retries 3
! !
!
crypto ipsec client ezvpn easy_vpn_remote
connect auto
group ezvpn key ezvpn
mode client
peer 10.6.6.1
! !
!
interface FastEthernet0/0
ip address 10.4.4.2 255.255.255.0
speed auto
crypto ipsec client ezvpn easy_vpn_remote inside
!
interface Serial0/0
ip address 10.6.6.2 255.255.255.0
no fair-queue
crypto ipsec client ezvpn easy_vpn_remote
!
interface Serial1/0
ip address 10.5.5.2 255.255.255.0
clock rate 4000000
crypto ipsec client ezvpn easy_vpn_remote inside
!
ip classless
no ip http server
ip pim bidir-enable
! !
!
line con 0
line aux 0
line vty 0 4
login
!
end
```

The following example shows a running configuration of a Cisco 1760 router that has two active, automatically connected tunnels, easy vpn remote1 and easy vpn remote2. Tunnel easy vpn remote1 has two configured inside interfaces and one configured outside interface. Tunnel easy vpn remote2 has one configured inside interface and one configured outside interface. The example also shows the output for the **show crypto ipsec client ezvpn** command that lists the tunnel names and the outside and inside interfaces.

```
Device# show running-config

Building configuration...
Current configuration : 1246 bytes
!
version 12.2
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname 1760
!
aaa new-model
!
!
aaa session-id common
!
ip subnet-zero
!!
!
crypto ipsec client ezvpn easy_vpn_remote2
connect auto
group ez key ez
mode network-extension
peer 10.7.7.1
crypto ipsec client ezvpn easy_vpn_remote1
connect auto
group ezvpn key ezvpn
mode client
peer 10.6.6.1
! !
!
interface FastEthernet0/0
ip address 10.5.5.2 255.255.255.0
speed auto
no cdp enable
crypto ipsec client ezvpn easy_vpn_remote1 inside
!
interface Serial0/0
ip address 10.4.4.2 255.255.255.0
no ip route-cache
no ip mroute-cache
no fair-queue
no cdp enable
crypto ipsec client ezvpn easy_vpn_remote1 inside
!
interface Serial0/1
ip address 10.3.3.2 255.255.255.0
no cdp enable
crypto ipsec client ezvpn easy_vpn_remote2 inside
!
interface Serial1/0
ip address 10.6.6.2 255.255.255.0
clockrate 4000000
no cdp enable
crypto ipsec client ezvpn easy_vpn_remote1
!
interface Serial1/1
ip address 10.7.7.2 255.255.255.0
no keepalive
no cdp enable
crypto ipsec client ezvpn easy_vpn_remote2
!
ip classless
```

```
no ip http server
ip pim bidir-enable
!
!
radius-server retransmit 3
radius-server authorization permit missing Service-Type
!
line con 0
line aux 0
line vty 0 4
!
no scheduler allocate
end
Device# show crypto ipsec client ezvpn

Tunnel name : easy_vpn_remote1
Inside interface list: FastEthernet0/0, Serial0/0,
Outside interface: Serial1/0
Current State: IPSEC_ACTIVE
Last Event: SOCKET_UP
Address: 10.0.0.5
Mask: 255.255.255.255
Default Domain: cisco.com
Tunnel name : easy_vpn_remote2
Inside interface list: Serial0/1,
Outside interface: Serial1/1
Current State: IPSEC_ACTIVE
Last Event: SOCKET_UP
Default Domain: cisco.com
```

Local Address Support for Easy VPN Remote Example

The following example shows that the **local-address** command is used to specify the loopback 0 interface for sourcing tunnel traffic:

```
Device> enable
Device# configure terminal
Device(config)# crypto ipsec client ezvpn telecommuter-client
Device(config-crypto-ezvpn)# local-address loopback0
```

Network Extension Mode Configuration Examples

In this section, the following examples demonstrate how to configure the Cisco Easy VPN Remote feature in the network extension mode of operation. Also shown are the Cisco IOS Easy VPN server configurations that correspond to these client configurations.

Cisco Easy VPN Client in Network Extension Mode (Cisco 831) Example

In the following example, a Cisco 831 router is configured as an Easy VPN remote using the Cisco Easy VPN Remote feature. This example shows the following components of the Cisco Easy VPN remote configuration:

- The Ethernet 0 interface is assigned an address in the network address space of the Cisco IOS Easy VPN server. The **ip route** command directs all traffic for this network space from the Ethernet 1 interface to the destination server.
- Cisco Easy VPN Remote configuration--The first **crypto ipsec client ezvpn** command (global configuration mode) creates a Cisco Easy VPN remote configuration named “easy vpn remote.” This configuration specifies the group name “easy vpn remote-groupname” and the shared key value “easy vpn remote-password,” and it sets the peer destination to the IP address 192.185.0.5 (which is the address

assigned to the interface connected to the Internet on the destination peer router). The Cisco Easy VPN remote configuration is configured for network extension mode.

Note If DNS is also configured on the router, the **peer** keyword option also supports a hostname instead of an IP address.

- The second **crypto ipsec client ezvpn** command (interface configuration mode) assigns the Cisco Easy VPN Remote configuration to the Ethernet 1 interface so that all traffic that is received and transmitted on that interface is sent through the VPN tunnel.

```
! Cisco Router Web Setup Template
!
no service pad
no service tcp-small-servers
no service udp-small-servers
service timestamps debug uptime
service timestamps log uptime
service password-encryption
!
hostname Router
!
!
ip subnet-zero
ip domain-lookup
!
!
ip dhcp excluded-address 172.31.1.1
!
ip dhcp pool localpool
   import all
   network 172.31.1.0 255.255.255.255
   default-router 172.31.1.1
   lease 1 0 0
!
!
crypto ipsec client ezvpn easy_vpn_remote
 peer 192.168.0.5
 group easy_vpn_remote_groupname key easy_vpn_remote_password
 mode network-extension
!
!
interface Ethernet0
 ip address 172.31.1.1 255.255.255.255
 no cdp enable
 hold-queue 32 in
!
interface Ethernet1
 ip address dhcp
 no cdp enable
 crypto ipsec client ezvpn easy_vpn_remote
!
ip classless
ip route 172.31.0.0 255.255.255.255 Ethernet1
ip http server
!
!
line con 0
 exec-timeout 120 0
 stopbits 1
line vty 0 4
 exec-timeout 0 0
 login local
```

Cisco Easy VPN Client in Network Extension Mode (Cisco 837) Example

In the following example, a Cisco 837 router is configured as an Easy VPN remote using the Cisco Easy VPN Remote feature in client mode. This example shows the following components of the Cisco Easy VPN remote configuration:

- PPPoE configuration--The ATM 0 interface is configured to support PPPoE connections over the Dialer 1 virtual interface. Because the interfaces use PPPoE, a DHCP IP address pool is not required to provide IP addresses to the connected PCs.
- The Ethernet 0 interface is assigned an address in the network address space of the Cisco IOS Easy VPN server. The **ip route** command directs all traffic for this network space from the Dialer 1 interface to the destination server.
- Cisco Easy VPN Remote configuration--The first **crypto ipsec client ezvpn** command (global configuration mode) creates a Cisco Easy VPN remote configuration named “easy vpn remote.” This configuration specifies the group name “easy vpn remote-groupname” and the shared key value “easy vpn remote-password,” and it sets the peer destination to the IP address 10.0.0.5 (which is the address assigned to the interface connected to the Internet on the destination peer router). The Cisco Easy VPN remote configuration is configured for the default network extension mode.

Note If DNS is also configured on the router, the **peer** keyword option also supports a hostname instead of an IP address.

- The second **crypto ipsec client ezvpn** command (interface configuration mode) assigns the Cisco Easy VPN remote configuration to the Dialer1 interface so that all traffic that is received and transmitted on that interface is sent through the VPN tunnel.

```
version 12.2
no service pad
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname c827
!
!
mmi polling-interval 60
no mmi auto-configure
no mmi pvc
mmi snmp-timeout 180
ip subnet-zero
!
ip ssh time-out 120
ip ssh authentication-retries 3
vpdn enable
!
vpdn-group pppoe
 request-dialin
  protocol pppoe
 ip mtu adjust
!
!
crypto ipsec client ezvpn easy_vpn_remote
 group easy_vpn_remote_groupname key easy_vpn_remote_password
 mode network-extension
 peer 10.0.0.5
!
```

```
!
interface Ethernet0
 ip address 172.16.0.30 255.255.255.192
 hold-queue 100 out
!
interface ATM0
 no ip address
 no atm ilmi-keepalive
 pvc 1/40
  pppoe-client dial-pool-number 1
 !
 dsl operating-mode auto
!
interface Dialer1
 ip address 10.0.0.3 255.0.0.0
 ip mtu 1492
 encapsulation ppp
 dialer pool 1
 crypto ipsec client ezvpn easy_vpn_remote
!
ip classless
ip route 172.16.0.0 255.255.255.128 Dialer1
ip route 0.0.0.0 0.0.0.0 ATM0
ip route 0.0.0.0 0.0.0.0 Dialer1 permanent
ip route 10.0.0.0 255.0.0.0 10.0.0.13
ip http server
ip pim bidir-enable
!
line con 0
 stopbits 1
line vty 0 4
 login
!
scheduler max-task-time 5000
```

Cisco Easy VPN Client in Network Extension Mode (Cisco 1700 Series) Example

In the following example, a Cisco 1700 series router is configured as an Easy VPN remote using the Cisco Easy VPN Remote feature in the network extension mode of operation. This example shows the following components of the Cisco Easy VPN remote configuration:

- Cisco Easy VPN Remote configuration—The first **crypto ipsec client ezvpn** command (global configuration mode) creates a Cisco Easy VPN remote configuration that is named “easy vpn remote.” This configuration specifies the group name “easy vpn remote-groupname” and the shared key value “easy vpn remote-password,” and it sets the peer destination to the IP address 10.0.0.2 (which is the address assigned to the interface connected to the Internet on the destination peer router). The Cisco Easy VPN remote configuration is configured for network extension mode.

Note If DNS is also configured on the router, the **peer** keyword option also supports a hostname instead of an IP address.

- The second **crypto ipsec client ezvpn easy vpn remote** command (interface configuration mode) assigns the Cisco Easy VPN remote configuration to Ethernet 0 interface so that all traffic that is received and transmitted on that interface is sent through the VPN tunnel.

```
!
version 12.2
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
```

```
!
hostname 1710
!
!
mmi polling-interval 60
no mmi auto-configure
no mmi pvc
mmi snmp-timeout 180
ip subnet-zero
!
!
ip ssh time-out 120
ip ssh authentication-retries 3
!
!
ip dhcp excluded-address 10.0.0.10
!
ip dhcp pool localpool
   import all
   network 10.70.0.0 255.255.255.248
   default-router 10.70.0.10
   lease 1 0 0
!
!
crypto ipsec client ezvpn easy_vpn_remote
 group easy_vpn_remote_groupname key easy_vpn_remote_password
 mode network-extension
 peer 10.0.0.2
!
!
interface Ethernet0
 ip address 10.50.0.10 255.0.0.0
 half-duplex
 crypto ipsec client ezvpn easy_vpn_remote
!
interface FastEthernet0
 ip address 10.10.0.10 255.0.0.0
 speed auto
!
ip classless
ip route 10.20.0.0 255.0.0.0 Ethernet0
ip route 10.20.0.0 255.0.0.0 Ethernet0
no ip http server
ip pim bidir-enable
!!
!
line con 0
 exec-timeout 0 0
line aux 0
line vty 0 4
 login
```

Save Password Configuration Example

The following sample **show running-config** output shows that the Save Password feature has been configured (note the **password encryption aes** command and **username** keywords in the output):

```
Device# show running-config
133.CABLEMODEM.CISCO: Oct 28 18:42:07.115: %SYS-5-CONFIG_I: Configured from console by
consolen
Building configuration...

Current configuration : 1269 bytes
!
! Last configuration change at 14:42:07 UTC Tue Oct 28 2003
!
version 12.3
no service pad
service timestamps debug datetime msec
```

```
service timestamps log datetime msec
no service password-encryption
!
hostname Router
!
boot-start-marker
boot-end-marker
!
!
clock timezone UTC -4
no aaa new-model
ip subnet-zero
no ip routing
!
!
ip audit notify log
ip audit po max-events 100
ip ssh break-string
no ftp-server write-enable
password encryption aes
!
!
no crypto isakmp enable
!
!
crypto ipsec client ezvpn remote_vpn_client
 connect auto
 mode client
 username user1 password  6 ARiFgh`SOJfMHLK[MHMQJZagR\M
!
!
interface Ethernet0
 ip address 10.3.66.4 255.255.255.0
 no ip route-cache
 bridge-group 59
```

PFS Support Examples

The following**show crypto ipsec client ezvpn** command output shows the group name (“2”) and that PFS is being used:

```
Device# show crypto ipsec client ezvpn
Easy VPN Remote Phase: 4
Tunnel name : ez1
Inside interface list: Loopback1,
Outside interface: Ethernet1
Current State: IPSEC_ACTIVE
Last Event: SOCKET_UP
Address: 192.168.6.6
Mask: 255.255.255.255
Using PFS Group: 2
Save Password: Allowed
Current EzVPN Peer:10.0.0.110
```

Note that on a Cisco IOS EasyVPN server, PFS must be included in IPsec proposals by adding to the crypto map, as in the following example:

```
crypto dynamic-map mode 1
 set security-association lifetime seconds 180
 set transform-set client
 set pfs group2
 set isakmp-profile fred
 reverse-route
```

Dial Backup Examples

Static IP Addressing

The following example shows that static IP addressing has been configured for a Cisco 1711 router:

```
Router# show running-config
Building configuration...
Current configuration : 3427 bytes
!
version 12.3
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname ph4_R5
!
boot-start-marker
boot-end-marker
!
no logging buffered
!
username ph4_R8 password 0 cisco
username ph4_R7 password 0 lab
mmi polling-interval 60
no mmi auto-configure
no mmi pvc
mmi snmp-timeout 180
aaa new-model
!
!
aaa session-id common
ip subnet-zero
!
!
no ip domain lookup
ip cef
ip ids po max-events 100
ip dhcp-client default-router distance 1
no ftp-server write-enable
!
!
track 123 rtr 3 reachability
!
crypto isakmp keepalive 10 periodic
!
!
crypto ipsec client ezvpn backup_profile_vpn3k
 connect auto
 group hw_client_groupname key password123
 mode client
 peer 10.0.0.5
 username user1 password  password123
crypto ipsec client ezvpn hw_client_vpn3k
 connect auto
 group hw_client_groupname key password123
 backup backup_profile_vpn3k track 123
 mode client
 peer 10.0.0.5
 username user1 password password123
!
!
interface Loopback0
 ip address 10.40.40.50 255.255.255.255
!
interface Loopback1
 ip address 10.40.40.51 255.255.255.255
!
interface Loopback2
```

```
 no ip address
!
interface FastEthernet0
 description Primary Link to 10.0.0.2
 ip address 10.0.0.10 255.255.255.0
 duplex auto
 speed auto
 no cdp enable
 crypto ipsec client ezvpn hw_client_vpn3k
!
interface FastEthernet1
 no ip address
 duplex full
 speed 100
 no cdp enable
!
interface FastEthernet2
 no ip address
 no cdp enable
!
interface FastEthernet3
 no ip address
 no cdp enable
!
interface FastEthernet4
 no ip address
 no cdp enable
!
interface Vlan1
 ip address 10.0.0.1 255.255.255.0
 crypto ipsec client ezvpn backup_profile_vpn3k inside
 crypto ipsec client ezvpn hw_client_vpn3k inside
!
interface Async1
 description Backup Link
 no ip address
 ip nat outside
 ip virtual-reassembly
 encapsulation ppp
 no ip route-cache cef
 dialer in-band
 dialer pool-member 1
 dialer-group 1
 async default routing
 async mode dedicated
!
interface Dialer1
 ip address 10.30.0.1 255.255.255.0
 encapsulation ppp
 no ip route-cache cef
 dialer pool 1
 dialer idle-timeout 60
 dialer string 102
 dialer hold-queue 100
 dialer-group 1
 crypto ipsec client ezvpn backup_profile_vpn3k
!
ip local policy route-map policy_for_rtr
ip classless
ip route 0.0.0.0 0.0.0.0 faste0 track 123
ip route 0.0.0.0 0.0.0.0 Dialer1 240
no ip http server
no ip http secure-server
!
!
ip access-list extended dummy1
 permit ip host 10.0.0.2 host 10.3.0.1
ip access-list extended important_traffic
 permit ip 10.0.0.0 0.0.0.255 10.0.0.2 0.0.0.255
 permit ip 10.0.0.0 0.0.0.255 10.0.0.3 0.0.0.255
ip access-list extended important_traffic_2
 permit ip 10.0.0.0 0.0.0.255 10.0.0.3 0.0.0.255
access-list 112 permit icmp any host 10.0.10.2 echo
```

```
dialer-list 1 protocol ip permit
no cdp run
!
route-map policy_for_rtr permit 10
 match ip address 112
 set interface Null0
 set ip next-hop 10.0.10.2
!
!
control-plane
!
rtr 2
 type echo protocol ipIcmpEcho 10.0.0.2 source-ipaddr 10.0.0.3
 timeout 10000
 threshold 1000
 frequency 11
rtr schedule 2 life forever start-time now
rtr 3
 type echo protocol ipIcmpEcho 10.0.0.2 source-interface FastEthernet0
 timeout 10000
 threshold 1000
 frequency 11
rtr schedule 3 life forever start-time now
!
line con 0
 exec-timeout 0 0
line 1
 modem InOut
 modem autoconfigure discovery
 transport input all
 autoselect ppp
 stopbits 1
 speed 115200
 flowcontrol hardware
line aux 0
line vty 0 4
 password lab
!
```

DHCP Configured on Primary Interface and PPP Async as Backup

The following example shows that a Cisco 1711 router has been configured so that DHCP is configured on the primary interface and PPP asynchronous mode is configured as the backup:

```
Router# show running-config
Building configuration...
Current configuration : 3427 bytes
!
version 12.3
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname ph4_R5
!
boot-start-marker
boot-end-marker
!
no logging buffered
!
username ph4_R8 password 0 cisco
username ph4_R7 password 0 lab
mmi polling-interval 60
no mmi auto-configure
no mmi pvc
mmi snmp-timeout 180
aaa new-model
!
!
aaa session-id common
ip subnet-zero
```

```
!
!
no ip domain lookup
ip cef
ip ids po max-events 100
ip dhcp-client default-router distance 1
no ftp-server write-enable
!
!
track 123 rtr 3 reachability
!
crypto isakmp keepalive 10 periodic
!
!
crypto ipsec client ezvpn backup_profile_vpn3k
 connect auto
 group hw_client_groupname key password123
 mode client
 peer 10.0.0.5
 username user1 password  password123
crypto ipsec client ezvpn hw_client_vpn3k
 connect auto
 group hw_client_groupname key password123
 backup backup_profile_vpn3k track 123
 mode client
 peer 10.0.0.5
 username user1 password  password123
!
!
interface Loopback0
 ip address 10.40.40.50 255.255.255.255
!
interface Loopback1
 ip address 10.40.40.51 255.255.255.255
!
interface Loopback2
 no ip address
!
interface FastEthernet0
 description Primary Link to 10.0.0.2
 ip dhcp client route track 123
 ip address dhcp
 duplex auto
 speed auto
 no cdp enable
 crypto ipsec client ezvpn hw_client_vpn3k
!
interface FastEthernet1
 no ip address
 duplex full
 speed 100
 no cdp enable
!
interface FastEthernet2
 no ip address
 no cdp enable
!
interface FastEthernet3
 no ip address
 no cdp enable
!
interface FastEthernet4
 no ip address
 no cdp enable
!
interface Vlan1
 ip address 10.0.0.1 255.255.255.0
 crypto ipsec client ezvpn backup_profile_vpn3k inside
 crypto ipsec client ezvpn hw_client_vpn3k inside
!
interface Async1
 description Backup Link
 no ip address
```

```
 ip nat outside
 ip virtual-reassembly
 encapsulation ppp
 no ip route-cache cef
 dialer in-band
 dialer pool-member 1
 dialer-group 1
 async default routing
 async mode dedicated
!
interface Dialer1
 ip address 10.0.0.3 255.255.255.0
 encapsulation ppp
 no ip route-cache cef
 dialer pool 1
 dialer idle-timeout 60
 dialer string 102
 dialer hold-queue 100
 dialer-group 1
 crypto ipsec client ezvpn backup_profile_vpn3k
!
ip local policy route-map policy_for_rtr
ip classless
ip route 0.0.0.0 0.0.0.0 Dialer1 240
no ip http server
no ip http secure-server
!
!
ip access-list extended dummy1
 permit ip host 10.10.0.2 host 10.0.0.1
ip access-list extended important_traffic
 permit ip 10.0.0.0 0.0.0.255 10.0.0.2 0.0.0.255
 permit ip 10.0.0.0 0.0.0.255 10.0.0.3 0.0.0.255
ip access-list extended important_traffic_2
 permit ip 10.0.0.0 0.0.0.255 10.0.0.3 0.0.0.255
access-list 112 permit icmp any host 10.0.0.2 echo
dialer-list 1 protocol ip permit
no cdp run
!
route-map policy_for_rtr permit 10
 match ip address 112
 set interface Null0
 set ip next-hop 10.0.0.2
!
!
control-plane
!
rtr 2
 type echo protocol ipIcmpEcho 10.0.0.2 source-ipaddr 10.0.0.3
 timeout 10000
 threshold 1000
 frequency 11
rtr schedule 2 life forever start-time now
rtr 3
 type echo protocol ipIcmpEcho 10.0.0.2 source-interface FastEthernet0
 timeout 10000
 threshold 1000
 frequency 11
rtr schedule 3 life forever start-time now
!
line con 0
 exec-timeout 0 0
line 1
 modem InOut
 modem autoconfigure discovery
 transport input all
 autoselect ppp
 stopbits 1
 speed 115200
 flowcontrol hardware
line aux 0
line vty 0 4
```

```
 password lab
!
```

Web-Based Activation Example

The following example shows that HTTP connections from the user are to be intercepted and that the user can do web-based authentication (192.0.0.13 is the VPN client device and 192.0.0.1 is the server device):

```
crypto ipsec client ezvpn tunnel22
  connect manual
  group tunnel22 key 22tunnel
  mode client
  peer 192.168.0.1
  xauth userid mode http-intercept
!
!
interface Ethernet0
  ip address 10.4.23.15 255.0.0.0
  crypto ipsec client ezvpn tunnel22 inside!
interface Ethernet1
  ip address 192.168.0.13 255.255.255.128
  duplex auto
  crypto ipsec client ezvpn tunnel22
!
```

Easy VPN Remote with Virtual IPsec Interface Support Configuration Examples

The following examples indicate that Virtual IPsec Interface Support has been configured on the Easy VPN remote devices.

Virtual IPsec Interface Generic Virtual Access

The following example shows an Easy VPN remote device with virtual-interface support using a generic virtual-access IPsec interface.

```
!
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname Router
!
boot-start-marker
boot-end-marker
!
!
no aaa new-model
!
resource policy
!
clock timezone IST 0
ip subnet-zero
no ip dhcp use vrf connected
!
!
crypto ipsec client ezvpn ez
 connect manual
 group easy key cisco
 mode client
 peer 10.3.0.2
 virtual-interface
 xauth userid mode interactive
```

```
!
!
interface Ethernet0/0
 ip address 10.1.0.2 255.255.255.0
 no keepalive
 no cdp enable
 crypto ipsec client ezvpn ez inside
!
interface Ethernet1/0
 ip address 10.2.0.1 255.255.255.0
 no keepalive
 no cdp enable
 crypto ipsec client ezvpn ez
!
ip classless
ip route 0.0.0.0 0.0.0.0 10.2.0.2 2
no ip http server
no ip http secure-server
!
!
line con 0
line aux 0
line vty 0 4
 login
!
end
```

Virtual IPsec Interface Virtual Access Derived from Virtual Template

The following example shows an Easy VPN remote device with virtual-interface support using a virtual-template-derived virtual-access IPsec interface:

```
!
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname Router
!
boot-start-marker
boot-end-marker
!
!
no aaa new-model
!
resource policy
!
clock timezone IST 0
ip subnet-zero
no ip dhcp use vrf connected
!
!
crypto ipsec client ezvpn ez
 connect manual
 group easy key cisco
 mode client
 peer 10.3.0.2
 virtual-interface 1
 xauth userid mode interactive
!
!
interface Ethernet0/0
 ip address 10.1.0.2 255.255.255.0
 no keepalive
 no cdp enable
 crypto ipsec client ezvpn ez inside
!
interface Ethernet1/0
 ip address 10.2.0.1 255.255.255.0
```

```
 no keepalive
 no cdp enable
 crypto ipsec client ezvpn ez
!
interface Virtual-Template1 type tunnel
 no ip address
 tunnel mode ipsec ipv4
!
!
ip classless
ip route 0.0.0.0 0.0.0.0 10.2.0.2 2
no ip http server
no ip http secure-server
!
!
line con 0
line aux 0
line vty 0 4
 login
!
end
```

When the Tunnel Is Down

The result of a virtual-interface configuration on an Easy VPN profile is the creation of a virtual-access interface. This interface provides IPsec encapsulation. The output below shows the configuration of a virtual-access interface when Easy VPN is “down.”

```
Device# show running-config interface virtual-access 2
Building configuration...
Current configuration : 99 bytes
!
interface Virtual-Access2
 no ip address
 tunnel source Ethernet1/0
 tunnel mode ipsec ipv4
end
```

A virtual-interface configuration results in the creation of a virtual-access interface. This virtual-access interface is made automatically outside the interface of the Easy VPN profile. The routes that are added later when the Easy VPN tunnels come up point to this virtual interface for sending the packets to the corporate network. If **crypto ipsec client ezvpn name outside** (**crypto ipsec client ezvpn name** command and **outside** keyword) is applied on a real interface, that interface is used as the IKE (IPsec) endpoint (that is, IKE and IPsec packets use the address on the interface as the source address).

```
Device# show crypto ipsec client ezvpn
Easy VPN Remote Phase: 5
Tunnel name : ez
Inside interface list: Ethernet0/0
Outside interface: Virtual-Access2 (bound to Ethernet1/0)
Current State: CONNECT_REQUIRED
Last Event: TRACKED OBJECT UP
Save Password: Disallowed
Current EzVPN Peer: 10.3.0.2
```

Because a virtual interface, or for that matter any interface, is routable, routes act like traffic selectors. When the Easy VPN tunnel is “down,” there are no routes pointing to the virtual interface, as shown in the following example:

```
Device# show ip route
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
```

```
       o - ODR, P - periodic downloaded static route
Gateway of last resort is 10.2.0.2 to network 0.0.0.0
     10.0.0.0/24 is subnetted, 2 subnets
C       10.2.0.0 is directly connected, Ethernet1/0
C       10.1.0.0 is directly connected, Ethernet0/0
S*   0.0.0.0/0 [2/0] via 10.2.0.2
```

When the Tunnel Is Up

In the case of client or network plus mode, Easy VPN creates a loopback interface and assigns the address that is pushed in mode configuration. To assign the address of the loopback to the interface, use the **ip unnumbered** command (**ip unnumbered loopback**). In the case of network extension mode, the virtual access will be configured as **ip unnumbered ethernet0** (the bound interface).

```
Router# show running-config interface virtual-access 2
Building configuration...
Current configuration : 138 bytes
!
interface Virtual-Access2
 ip unnumbered Loopback0
 tunnel source Ethernet1/0
 tunnel destination 10.3.0.2
 tunnel mode ipsec ipv4
end
Router# show crypto ipsec client ezvpn
Easy VPN Remote Phase: 5
Tunnel name : ez
Inside interface list: Ethernet0/0
Outside interface: Virtual-Access2 (bound to Ethernet1/0)
Current State: IPSEC_ACTIVE
Last Event: SOCKET_UP
Address: 10.5.0.2
Mask: 255.255.255.255
DNS Primary: 10.6.0.2
NBMS/WINS Primary: 10.7.0.1
Default Domain: cisco.com
Using PFS Group: 2
Save Password: Disallowed
Split Tunnel List: 1
       Address    : 10.4.0.0
       Mask       : 255.255.255.0
       Protocol   : 0x0
       Source Port: 0
       Dest Port  : 0
Current EzVPN Peer: 10.3.0.2
```

When the tunnels come up, Easy VPN adds either a default route that points to the virtual-access interface or adds routes for all the split attributes of the subnets that point to the virtual-access interface. Easy VPN also adds a route to the peer (destination or concentrator) if the peer is not directly connected to the Easy VPN device.

The following **show ip route** command output examples are for virtual IPsec interface situations in which a split tunnel attribute was sent by the server and a split tunnel attribute was not sent, respectively.

Split Tunnel Attribute Has Been Sent by the Server

```
Router# show ip route
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route
Gateway of last resort is 10.2.0.2 to network 0.0.0.0
     10.0.0.0/8 is variably subnetted, 5 subnets, 2 masks
```

```
C       10.2.0.0/24 is directly connected, Ethernet1/0
S       10.3.0.2/32 [1/0] via 10.2.0.2, Ethernet1/0  <<< Route to
 peer (EzVPN server)
C       10.1.0.0/24 is directly connected, Ethernet0/0
C       10.5.0.2/32 is directly connected, Loopback0
S       10.4.0.0/24 [1/0] via 0.0.0.0, Virtual-Access2  <<< Split
tunnel attr sent by the server
S*   10.0.0.0/0 [2/0] via 10.2.0.2
```

Split Tunnel Attribute Has Not Been Sent by the Server

All networks in the split attribute should be shown, as in the following example:

```
Router# show ip route
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route
Gateway of last resort is 0.0.0.0 to network 0.0.0.0
     10.0.0.0/8 is variably subnetted, 4 subnets, 2 masks
C       10.2.0.0/24 is directly connected, Ethernet1/0
! The following line is the route to the peer (the Easy VPN server).
S       10.3.0.2/32 [1/0] via 10.2.0.2, Ethernet1/0
C       10.1.0.0/24 is directly connected, Ethernet0/0
C       10.5.0.3/32 is directly connected, Loopback0
! The following line is the default route.
S*   10.0.0.0/0 [1/0] via 10.0.0.0, Virtual-Access2
```

Dual Tunnel Configuration Example

The following is an example of a typical dual-tunnel configuration:

```
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname Router
!
boot-start-marker
boot-end-marker
!
enable password lab
!
no aaa new-model
!
resource policy
!
clock timezone IST 0
ip subnet-zero
!
!
username lab password 0 lab
!
!
crypto ipsec client ezvpn ezvpn1
 connect manual
 group easy key cisco
 mode network-extension
 peer 10.75.1.2
 virtual-interface 1
 xauth userid mode interactive
crypto ipsec client ezvpn ezvpn2
 connect manual
 group easy key cisco
```

```
 mode network-extension
 peer 10.75.2.2
 virtual-interface 1
 xauth userid mode interactive
!
!
interface Ethernet0/0
 ip address 192.168.1.1 255.255.255.255
 no keepalive
 crypto ipsec client ezvpn ezvpn1 inside
 crypto ipsec client ezvpn ezvpn2 inside
!
interface Ethernet0/1
 no ip address
 shutdown
!
interface Ethernet0/2
 no ip address
 shutdown
!
interface Ethernet0/3
 no ip address
 shutdown
!
interface Ethernet1/0
 ip address 10.76.1.2 255.255.255.0
 no keepalive
 crypto ipsec client ezvpn ezvpn1
 crypto ipsec client ezvpn ezvpn2
!
interface Serial2/0
 ip address 10.76.2.2 255.255.255.0
 no keepalive
 serial restart-delay 0
!
interface Virtual-Template1 type tunnel
 no ip address
 tunnel mode ipsec ipv4
!
!
ip classless
ip route 10.0.0.0 10.0.0.0 10.76.1.1 2
no ip http server
no ip http secure-server
!
!
no cdp run
!
!
line con 0
 exec-timeout 0 0
line aux 0
line vty 0 4
 login local
!
end
```

Dual Tunnel Show Output Examples

The following **show** command examples display information about three phases of a dual tunnel that is coming up:

- First Easy VPN tunnel is up
- Second Easy VPN tunnel is initiated
- Both of the Easy VPN tunnels are up

Before the EzVPN Tunnels Are Up

```
Router# show crypto ipsec client ezvpn
Easy VPN Remote Phase: 6
Tunnel name : ezvpn1
Inside interface list: Ethernet0/0
Outside interface: Virtual-Access2 (bound to Ethernet1/0)
Current State: CONNECT_REQUIRED
Last Event: TRACKED OBJECT UP
Save Password: Disallowed
Current EzVPN Peer: 10.75.1.2
Tunnel name : ezvpn2
Inside interface list: Ethernet0/0
Outside interface: Virtual-Access3 (bound to Serial2/0)
Current State: CONNECT_REQUIRED
Last Event: TRACKED OBJECT UP
Save Password: Disallowed
Current EzVPN Peer: 10.75.2.2
Router# show ip route
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route
```

The gateway of last resort is 10.76.1.1 to network 0.0.0.0.

```
10.0.0.0/24 is subnetted, 2 subnets
C       10.76.2.0 is directly connected, Serial2/0
C       10.76.1.0 is directly connected, Ethernet1/0
C    192.168.1.0/24 is directly connected, Ethernet0/0
S*   0.0.0.0/0 [2/0] via 10.76.1.1
```

Note The metric of the default route should be greater than 1 so that the default route that is added later by Easy VPN takes precedence and the traffic goes through the Easy VPN virtual-access interface.

Easy VPN "ezvpn2" Tunnel Is Up

```
Router# show crypto ipsec client ezvpn
Easy VPN Remote Phase: 6
Tunnel name : ezvpn1
Inside interface list: Ethernet0/0
Outside interface: Virtual-Access2 (bound to Ethernet1/0)
Current State: CONNECT_REQUIRED
Last Event: TRACKED OBJECT UP
Save Password: Disallowed
Current EzVPN Peer: 10.75.1.2
Tunnel name : ezvpn2
Inside interface list: Ethernet0/0
Outside interface: Virtual-Access3 (bound to Serial2/0)
Current State: IPSEC_ACTIVE
Last Event: SOCKET_UP
DNS Ezvpn1: 10.6.0.2
NBMS/WINS Ezvpn1: 10.7.0.1
Default Domain: cisco.com
Save Password: Disallowed
Current EzVPN Peer: 10.75.2.2
Router# show ip route
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
```

```
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route
```

The gateway of last resort is 0.0.0.0 to network 0.0.0.0.

```
10.0.0.0/8 is variably subnetted, 3 subnets, 2 masks
! The next line is the Easy VPN route.
S       10.75.2.2/32 [1/0] via 10.76.1.1
C       10.76.2.0/24 is directly connected, Serial2/0
C       10.76.1.0/24 is directly connected, Ethernet1/0
C    192.168.1.0/24 is directly connected, Ethernet0/0
! The next line is the Easy VPN route.
S*   0.0.0.0/0 [1/0] via 0.0.0.0, Virtual-Access3
```

One default route and one route to the peer is added as shown above.

Easy VPN "ezvpn2" Is Up and Easy VPN "ezvpn1" Is Initiated

```
Router# crypto ipsec client ezvpn connect ezvpn1
Router# show crypto ipsec cli ent ezvpn

Easy VPN Remote Phase: 6
Tunnel name : ezvpn1
Inside interface list: Ethernet0/0
Outside interface: Virtual-Access2 (bound to Ethernet1/0)
Current State: READY
Last Event: CONNECT
Save Password: Disallowed
Current EzVPN Peer: 10.75.1.2
Tunnel name : ezvpn2
Inside interface list: Ethernet0/0
Outside interface: Virtual-Access3 (bound to Serial2/0)
Current State: IPSEC_ACTIVE
Last Event: SOCKET_UP
DNS Ezvpn1: 10.6.0.2
NBMS/WINS Ezvpn1: 10.7.0.1
Default Domain: cisco.com
Save Password: Disallowed
Current EzVPN Peer: 10.75.2.2
Router# show ip route
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route
```

The gateway of last resort is 10.0.0.0 to network 10.0.0.0.

```
     10.0.0.0/8 is variably subnetted, 4 subnets, 2 masks
S       10.75.2.2/32 [1/0] via 10.76.1.1
! The next line is the Easy VPN router.
S       10.75.1.2/32 [1/0] via 10.76.1.1
C       10.76.2.0/24 is directly connected, Serial2/0
C       10.76.1.0/24 is directly connected, Ethernet1/0
C    192.168.1.0/24 is directly connected, Ethernet0/0
S*   10.0.0.0/0 [1/0] via 10.0.0.0, Virtual-Access3
```

The route to 10.75.1.2 is added before the Easy VPN "ezvpn1" tunnel has come up. This route is for reaching the Easy VPN "ezvpn1" peer 10.75.1.2.

Both Tunnels Are Up

```
Router# show crypto ipsec client ezvpn

Easy VPN Remote Phase: 6
Tunnel name : ezvpn1
Inside interface list: Ethernet0/0
Outside interface: Virtual-Access2 (bound to Ethernet1/0)
```

```
Current State: IPSEC_ACTIVE
Last Event: SOCKET_UP
DNS Ezvpn1: 10.6.0.2
NBMS/WINS Ezvpn1: 10.7.0.1
Default Domain: cisco.com
Save Password: Disallowed
Split Tunnel List: 1
       Address    : 192.168.3.0
       Mask       : 255.255.255.255
       Protocol   : 0x0
       Source Port: 0
       Dest Port  : 0
Current EzVPN Peer: 10.75.1.2
Tunnel name : ezvpn2
Inside interface list: Ethernet0/0
Outside interface: Virtual-Access3 (bound to Serial2/0)
Current State: IPSEC_ACTIVE
Last Event: SOCKET_UP
DNS Ezvpn1: 10.6.0.2
NBMS/WINS Ezvpn1: 10.7.0.1
Default Domain: cisco.com
Save Password: Disallowed
Current EzVPN Peer: 10.75.2.2
Router# show ip route
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route
```

The gateway of last resort is 10.0.0.0 to network 10.0.0.0.

```
     10.0.0.0/8 is variably subnetted, 4 subnets, 2 masks
! The next line is the Easy VPN router (ezvpn2).
S       10.75.2.2/32 [1/0] via 10.76.1.1
! The next line is the Easy VPN router (ezvpn1).
S       10.75.1.2/32 [1/0] via 10.76.1.1
C       10.76.2.0/24 is directly connected, Serial2/0
C       10.76.1.0/24 is directly connected, Ethernet1/0
C    192.168.1.0/24 is directly connected, Ethernet0/0
! The next line is the Easy VPN route (ezvpn1).
S    192.168.3.0/24 [1/0] via 0.0.0.0, Virtual-Access2
! The next line is the Easy VPN (ezvpn2).
S*   10.0.0.0/0 [1/0] via 10.0.0.0, Virtual-Access3
```

The route to split tunnel “192.168.3.0/24” that points to Virtual-Access2 is added for the Easy VPN “ezvpn”" tunnel as shown in the above **show** output.

Reactivate Primary Peer Example

The following show output illustrates that the default primary peer feature has been activated. The primary default peer is 10.3.3.2.

```
Router# show crypto ipsec client ezvpn

Easy VPN Remote Phase: 6
Tunnel name : ezc
Inside interface list: Loopback0
Outside interface: Ethernet0/0
Current State: IPSEC_ACTIVE
Primary EzVPN Peer: 10.3.3.2, Last Tried: Dec 30 07:21:23.071
Last Event: CONN_UP
Address: 10.7.7.1
Mask: 255.255.255.255
DNS Primary: 10.1.1.1
NBMS/WINS Primary: 10.5.254.22
Save Password: Disallowed
```

```
Current EzVPN Peer: 10.4.4.2
23:52:44: %CRYPTO-6-EZVPN_CONNECTION_UP(Primary peer):
        User: lab, Group: hw-client-g
        Client_public_addr=10.4.22.103, Server_public_addr=10.4.23.112
        Assigned_client_addr=10.7.7.1
```

Identical Addressing Support Configuration Example

In the following example, a Cisco router is configured for the Identical Addressing Support feature:

```
interface Virtual-Template1 type tunnel
 no ip address
 ip nat outside
!
crypto ipsec client ezvpn easy
 connect manual
 group easy key work4cisco
 mode network-extension
 peer 10.2.2.2
 virtual-interface 1
 nat allow
 nat acl 100
!
interface Ethernet1/0
 ip address 10.0.0.1 255.255.255.0
 ip nat outside
 crypto ipsec client ezvpn easy
!
interface Ethernet0/0
 ip address 10.0.1.1 255.255.255.0
 ip nat inside
!
interface Loopback0
 ip address 10.1.1.1 255.255.255.252
 ip nat enable
crypto ipsec client ezvpn easy inside
!
ip access-list 100 permit ip 10.0.0.0 0.0.0.255 any
!
ip nat inside source list 100 interface Loopback0 overload
```

cTCP on an Easy VPN Client (Remote Device) Examples

For configuration and troubleshooting examples, see the topic “cTCP on Cisco Easy VPN remote devices” in the cTCP on an Easy VPN Client (Remote Device) Examples, on page 94.

Easy VPN Server Configuration Examples

This section describes basic Cisco Easy VPN server configurations that support the Cisco Easy VPN remote configurations given in the previous sections. For complete information on configuring these servers, see Easy VPN Server for Cisco IOS Release 12.3(7)T, available on Cisco.com.

Cisco Easy VPN Server Without Split Tunneling Example

The following example shows the Cisco Easy VPN server that is the destination peer router for the Cisco Easy VPN remote network extension mode configurations shown earlier in this section. In addition to the other IPsec configuration commands, the **crypto isakmp client configuration group** command defines the attributes for the VPN group that was assigned to the Easy VPN remote router. This includes a matching key

value (easy vpn remote password), and the appropriate routing parameters, such as DNS server, for the Easy VPN remotes.

To support the network extension mode of operation, the **ip route** command instructs that incoming packets for the 172.168.0.0 network be directed from the cable modem interface to the Cisco Easy VPN remote. Other **ip route** commands might be needed, depending on the topology of your network.

Note This example shows a Cisco uBR925 cable access router, but typically the destination Easy VPN remote is a router, such as a Cisco VPN 3000 concentrator or a Cisco IOS router, that supports the Easy VPN Server feature.

```
version 12.2
no service pad
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
service internal
!
hostname uBR925Server
!
aaa new-model
!
!
aaa authorization network easy vpn remote-groupname local
aaa session-id common
!
!
clock timezone - 0 6
ip subnet-zero
!
ip ssh time-out 120
ip ssh authentication-retries 3
!
crypto isakmp policy 1
 authentication pre-share
 group 2
crypto isakmp client configuration address-pool local dynpool
!
crypto isakmp client configuration group easy vpn remote-groupname
 key easy vpn remote-password
 dns 172.16.0.250 172.16.0.251
 wins 172.16.0.252 172.16.0.253
 domain cisco.com
 pool dynpool
!
!
crypto ipsec transform-set transform-1 esp-des esp-sha-hmac
!
crypto dynamic-map dynmap 1
 set transform-set transform-1
 reverse-route
!
!
crypto map dynmap isakmp authorization list easy vpn remote-groupname
crypto map dynmap client configuration address respond
crypto map dynmap 1 ipsec-isakmp dynamic dynmap
!
!
interface Ethernet0
 ip address 172.16.0.129 255.255.255.128
!
interface cable-modem0
 no cable-modem compliant bridge
 crypto map dynmap
!
interface usb0
```

```
 no ip address
 arp timeout 0
!
ip local pool dynpool 172.16.0.65 172.16.0.127
ip classless
! Add the appropriate ip route commands for network-extension mode
ip route 172.16.1.0 255.255.255.248 cable-modem0
no ip http server
no ip http cable-monitor
!
snmp-server manager
!
line con 0
 exec-timeout 0 0
line vty 0 4
!
scheduler max-task-time 5000
```

Cisco Easy VPN Server Configuration with Split Tunneling Example

The following example shows a Cisco Easy VPN server that is configured for a split tunneling configuration with a Cisco Easy VPN remote. This example is identical to that shown in the "Cisco Easy VPN Server Without Split Tunneling Example, on page 94" except for access list 150, which is assigned as part of the **crypto isakmp client configuration group**command. This access list allows the Cisco Easy VPN remote to use the server to access one additional subnet that is not part of the VPN tunnel without compromising the security of the IPsec connection.

To support network extension mode, the **ip route** command instructs that incoming packets for the 172.168.0.0 network be directed from the cable modem interface to the Cisco Easy VPN remote. Other **ip route** commands might be necessary, depending on the topology of your network.

Note This example shows a Cisco uBR925 cable access router, but typically the destination Easy VPN remote will be a router, such as a VPN 3000 concentrator or a Cisco IOS router, that supports the Easy VPN Server feature.

```
version 12.2
no service pad
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
service internal
!
hostname uBR925Server
!
aaa new-model
!
!
aaa authorization network easy vpn remote-groupname local
aaa session-id common
!
!
clock timezone - 0 6
ip subnet-zero
!
ip ssh time-out 120
ip ssh authentication-retries 3
!
crypto isakmp policy 1
 authentication pre-share
 group 2
crypto isakmp client configuration address-pool local dynpool
!
```

```
crypto isakmp client configuration group easy vpn remote-groupname
 key easy vpn remote-password
 dns 172.16.0.250 172.16.0.251
 wins 172.16.0.252 172.16.0.253
 domain cisco.com
 pool dynpool
 acl 150

!
!
crypto ipsec transform-set transform-1 esp-des esp-sha-hmac
!
crypto dynamic-map dynmap 1
 set transform-set transform-1
 reverse-route
!
!
crypto map dynmap isakmp authorization list easy vpn remote-groupname
crypto map dynmap client configuration address respond
crypto map dynmap 1 ipsec-isakmp dynamic dynmap
!
!
interface Ethernet0
 ip address 172.16.0.129 255.255.255.255
!
interface cable-modem0
 no cable-modem compliant bridge
 crypto map dynmap
!
interface usb0
 no ip address
 arp timeout 0
!
ip local pool dynpool 172.16.0.65 172.16.0.127
ip classless
! Add the appropriate ip route commands for network-extension mode
ip route 172.16.1.0 255.255.255.255 cable-modem0

no ip http server
no ip http cable-monitor
!
access-list 150 permit ip 172.16.0.128 0.0.0.127 any

snmp-server manager
!
line con 0
 exec-timeout 0 0
line vty 0 4
!
scheduler max-task-time 5000
end
```

Cisco Easy VPN Server Configuration with Xauth Example

The following example shows a Cisco Easy VPN server configured to support Xauth with the Cisco Easy VPN Remote feature. This example is identical to that shown in the "Cisco Easy VPN Server Configuration with Split Tunneling Example, on page 96" except for the following commands that enable and configure Xauth:

- **aaa authentication login userlist local—**Specifies the local username database for authentication at login time. You could also specify the use of RADIUS servers by first using the **aaa authentication login userlist group radius** command and then by specifying the RADIUS servers using the **aaa group server radius** command.
- **crypto isakmp xauth timeout—**Specifies the amount of time, in seconds, that the user has to enter the appropriate username and password to authenticate the session.

- **crypto map dynmap client authentication list userlist—**Creates a crypto map named "**dynmap**" that enables Xauth.
- **username cisco password 7 cisco—**Creates an entry in the local username database for a user with the username of "**cisco**" and an encrypted password of "**cisco**." This command should be repeated for each separate user that accesses the server.

The following commands, which are also present in the non-Xauth configurations, are also required for Xauth use:

- **aaa authorization network easy vpn remote-groupname local—**Requires authorization for all network-related service requests for users in the group named "**easy vpn remote-groupname**" using the local username database.
- **aaa new-model—**Specifies that the router should use the new AAA authentication commands.
- **aaa session-id common—**Specifies that a unique and common session ID should be used for AAA sessions.
- **crypto map dynmap 1 ipsec-isakmp dynamic dynmap—**Specifies that IKE should be used to establish the IPsec SAs, using the crypt map named "dynmap" as the policy template.
- **crypto map dynmap client configuration address respond—**Enables IKE negotiation, accepting requests from any requesting peers.
- **crypto map dynmap isakmp authorization list easy vpn remote-groupname—**Configures the crypto map named "**dynmap**" to use IKE Shared Secret using the group named "**easy vpn remote-groupname**."

Tip This configuration shows the server configured for split tunneling, but Xauth can also be used with nonsplit tunnel configurations as well.

Note This example shows a Cisco uBR925 cable access router, but typically the destination Easy VPN server is a router such as a VPN 3000 concentrator or a Cisco IOS router that supports the Easy VPN Server feature.

```
version 12.2
no service pad
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
service internal
!
hostname uBR925Server
!
aaa new-model

!
!
aaa authentication login userlist local

aaa authorization network easy vpn remote-groupname local
aaa session-id common
!
username cisco password 7 cisco

!
```

```
!
clock timezone - 0 6
ip subnet-zero
!
ip ssh time-out 120
ip ssh authentication-retries 3
!
crypto isakmp policy 1
 authentication pre-share
 group 2
crypto isakmp client configuration address-pool local dynpool
crypto isakmp xauth timeout 60

!
crypto isakmp client configuration group easy vpn remote-groupname
 key easy vpn remote-password
 dns 172.16.0.250 172.16.0.251
 wins 172.16.0.252 172.16.0.253
 domain cisco.com
 pool dynpool
 acl 150
!
!
crypto ipsec transform-set transform-1 esp-des esp-sha-hmac
!
crypto dynamic-map dynmap 1
 set transform-set transform-1
 reverse-route
!
!
crypto map dynmap client authentication list userlist

crypto map dynmap isakmp authorization list easy vpn remote-groupname
crypto map dynmap client configuration address respond
crypto map dynmap 1 ipsec-isakmp dynamic dynmap
!!
!
interface Ethernet0
 ip address 172.16.0.129 255.255.255.128
!
interface cable-modem0
 no cable-modem compliant bridge
 crypto map dynmap
!
interface usb0
 no ip address
 arp timeout 0
!
ip local pool dynpool 172.16.0.65 172.16.0.127
ip classless
ip route 172.16.1.0 255.255.255.248 cable-modem0
no ip http server
no ip http cable-monitor
!
access-list 150 permit ip 172.16.0.128 0.0.0.127 any
snmp-server manager
!
line con 0
 exec-timeout 0 0
line vty 0 4
!
scheduler max-task-time 5000
end
```

Easy VPN Server Interoperability Support Example

For information about this feature, see “General information on IPSec and VPN” in the section “Additional References, on page 100” (*Managing VPN Remote Access*).

Additional References

Related Documents

Related Topic	Document Title
Cisco 800 series routers	• Cisco 800 Series Routers • Cisco 806 Router and SOHO 71 Router Hardware Installation Guide • Cisco 806 Router Software Configuration Guide • Cisco 826, 827, 828, 831, 836, and 837 and SOHO 76, 77, 78, 91, 96, and 97 Routers Software Configuration Guide • Cisco 826 and SOHO 76 Router Hardware Installation Guide • Cisco 827 and SOHO 77 Routers Hardware Installation Guide • Cisco 828 and SOHO 78 Routers Hardware Installation Guide • Cisco 837 ADSL Broadband Router
Cisco uBR905 and Cisco uBR925 cable access routers	• Cisco uBR925 Cable Access Router Hardware Installation Guide • Cisco uBR905 Hardware Installation Guide • Cisco uBR905/uBR925 Cable Access Router Software Configuration Guide • Cisco uBR905 Cable Access Router Subscriber Setup Quick Start Card • Cisco uBR925 Cable Access Router Subscriber Setup Quick Start Card • Cisco uBR925 Cable Access Router Quick Start User Guide

Related Topic	Document Title
Cisco 1700 series routers	• Cisco 1700 Series Router Software Configuration Guide • Cisco 1710 Security Router Hardware Installation Guide • Cisco 1710 Security Router Software Configuration Guide • Cisco 1711 Security Access Router • Cisco 1720 Series Router Hardware Installation Guide • Cisco 1721 Access Router Hardware Installation Guide • Cisco 1750 Series Router Hardware Installation Guide • Cisco 1751 Router Hardware Installation Guide • Cisco 1751 Router Software Configuration Guide • Cisco 1760 Modular Access Router Hardware Installation Guide Also see the Cisco IOS release notes for Cisco IOS Release 12.2(4)YA: • SOHO 70 and Cisco 800 Series--Release Notes for Release 12.2(4)YA • Release Notes for Cisco uBR905 and Cisco uBR925 Cable Access Routers for Cisco IOS Release 12.2 YA • Cisco 1700 Series--Release Notes for Release 12.2(4)YA

Related Topic	Document Title
Cisco 2600 series, Cisco 3600 series, and Cisco 3700 series routers	• Cisco 2600 Series Multiservice Platforms • Cisco 2600 Series Routers Hardware Installation Guide • Cisco 3600 Series Multiservice Platforms • Cisco 3600 Series Hardware Installation Guide • Cisco 3700 Series Multiservice Access Routers • Cisco 3700 Series Routers Hardware Installation Guide • Cisco 2600 Series, 3600 Series, and 3700 Series Regulatory Compliance and Safety Information on Cisco.com
802.1x authentication	• Configuring Cisco IOS Easy VPN Remote with 802.1X Authentication (white paper) • VPN Access Control Using 802.1X Local Authentication
Access Control Lists Configuration	IP Access List Overview
Configuration information (additional in-depth)	• Cisco IOS Security Command Reference—Provides a reference for each of the Cisco IOS commands used to configure IPsec encryption and related security features. • SSL VPN—Provides information about SSL VPN.
cTCP on Cisco Easy VPN remote devices	EFT Deployment Guide for Cisco Tunnel Control Protocol on Cisco EasyVPN
Dead peer detection	IPSec Dead Peer Detection Periodic Message Option
DHCP configuration	*Configuring the Cisco IOS DHCP Client*
Digital certificates (RSA signature support)	Easy VPN Remote RSA Signature Support
DNS, configuration	Configuring DNS on Cisco Routers

Related Topic	Document Title
Easy VPN Server feature, which provides Cisco Unity client support for the Cisco Easy VPN Remote feature	• Easy VPN Server • Cisco Easy VPN • Configuring NAC with IPsec Dynamic Virtual Tunnel Interface
Encrypted Preshared Key feature	Encrypted Preshared Key
IPsec and VPN, general information	• Deploying IPsec—Provides an overview of IPsec encryption and its key concepts, along with sample configurations. Also provides a link to many other documents on related topics. • Configuring Authorization and Revocation of Certificates in a PKI—Describes the concept of digital certificates and how they are used to authenticate IPsec users. • Configuring Authentication Proxy • An Introduction to IP Security (IPsec) Encryption—Provides a step-by-step description of how to configure IPsec encryption. • Configuring VPN Settings—Provides information about configuring a PIX firewall to operate as a Cisco Secure VPN client. • Configuring Security for VPNs with IPsec—Provides information about configuring crypto maps. • IPSec Virtual Tunnel Interface—Provides information about IPsec virtual tunnel interfaces. • IP technical tips sections on Cisco.com.
Object tracking	Reliable Static Routing Backup Using Object Tracking
Recommended cryptographic algorithms	Next Generation Encryption

MIBs

MIBs	MIBs Link
• CISCO-IPSEC-FLOW-MONITOR-MIB—Contains attributes describing IPsec-based VPNs (Internet Engineering Task Force (IETF) IPSec Working Group Draft). • CISCO-IPSEC-MIB—Describes Cisco implementation-specific attributes for Cisco routers implementing IPsec VPNs. • CISCO-IPSEC-POLICY-MAP-MIB—Extends the CISCO-IPSEC-FLOW-MONITOR-MIB to map dynamically created structures to the policies, transforms, cryptomaps, and other structures that created or are using them.	To locate and download MIBs for selected platforms, Cisco IOS software releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

Technical Assistance

Description	Link
The Cisco Support and Documentation website provides online resources to download documentation, software, and tools. Use these resources to install and configure the software and to troubleshoot and resolve technical issues with Cisco products and technologies. Access to most tools on the Cisco Support and Documentation website requires a Cisco.com user ID and password.	http://www.cisco.com/cisco/web/support/index.html

Feature Information for Easy VPN Remote

Table 4: Feature Information for Easy VPN Remote

Feature Name	Releases	Feature Information
Easy VPN Remote	12.2(4)YA Cisco IOS XE Release 2.1	Support for Cisco Easy VPN Remote (Phase I) of this feature was introduced for Cisco 806, Cisco 826, Cisco 827, and Cisco 828 routers; Cisco 1700 series routers; and Cisco uBR905 and Cisco uBR925 cable access routers. In Cisco IOS XE Release 2.1, support for this feature was introduced on Cisco ASR 1000 Series Routers.
	12.2(13)T	Cisco Easy VPN Remote was integrated into Cisco IOS Release 12.2(13)T.
	12.2(8)YJ	Support for Cisco Easy VPN Remote (Phase II) of this feature was introduced for Cisco 806, Cisco 826, Cisco 827, and Cisco 828 routers; Cisco 1700 series routers; and Cisco uBR905 and Cisco uBR925 cable access routers.
	12.2(15)T	The Cisco Easy VPN Remote (Phase II) feature was integrated into Cisco IOS Release 12.2(15)T. Support for the Cisco 2600 series, Cisco 3600 series, and Cisco 3700 series routers was added.
	12.3(2)T	The Type 6 Password in the IOS Configuration feature was added.
	12.3(4)T	The Save Password and Multiple Peer Backup features were added.
	12.3(7)T	The following feature was introduced in this release:

Feature Name	Releases	Feature Information
	12.3(7)XR	The following features were introduced: Dead Peer Detection with Stateless Failover (Object Tracking with Easy VPN)--Backup Server List Local Configuration and Backup Server List Auto Configuration, Management Enhancements, Load Balancing, VLAN Support, Multiple Subnet Support, Traffic-Triggered Activation, Perfect Forward Secrecy (PFS) Via Policy Push, 802.1x Authentication, Certificate (PKI) Support, Easy VPN Remote and Server on the Same Interface, and Easy VPN Remote and Site to Site on the Same Interface. **Note** Cisco 800 series routers are not supported in Cisco IOS Release 12.3(7)XR. **Note** These features are available only in Cisco Release 12.3(7)XR2.
	12.3(7)XR2	The features in Cisco IOS Release 12.3(7)XR were introduced on Cisco 800 series routers.
	12.3(8)YH	The Dial Backup, Traffic-Triggered Activation, and Web-Based Activation features were introduced on the Cisco 1812 router.
	12.3(11)T	Except for the Dial Backup and Traffic-Triggered Activation features, all features introduced in Cisco IOS Releases 12.3(7)XR and 12.3(7)XR2 were integrated into Cisco IOS Release 12.3(11)T.
	12.3(14)T	Dial Backup and Traffic-Triggered Activation features were integrated into Cisco IOS Release 12.3(14)T. In addition, the Web-Based Activation feature was integrated into this release.

Feature Name	Releases	Feature Information
	12.3(8)YI	The Dial Backup, Traffic-Triggered Activation, and Web-Based Activation features were introduced on the Cisco 1800 series fixed configuration routers.
	12.3(8)YI1	The Dial Backup, Traffic-Triggered Activation, and Web-Based Activation features were introduced on the Cisco 870 series routers.
	12.4(2)T 12.2(33)SXH	The following features were added in this release: Banner, Auto-Update, and Browser-Proxy Enhancements.
	12.4(4)T 12.2(33)SXH	The following features were added in this release: Dual Tunnel Support, Configuration Management Enhancements (Pushing a Configuration URL Through a Mode-Configuration Exchange), Reactivate Primary Peer, and Virtual IPsec Interface Support. In addition, the **flow allow acl** command was added so that traffic can be blocked when a tunnel is down.
	12.2(33)SRA	Cisco Easy VPN Remote was integrated into Cisco IOS Release 12.2(33)SRA.
	12.4(11)T	The following feature was added in this release: • Identical Addressing Support
	12.4(20)T	The following features were added in this release: • cTCP Support on Easy VPN Clients The following commands were introduced or modified for this feature: **crypto ctcp**, **ctcp port**

Glossary

AAA --authentication, authorization, and accounting. Framework of security services that provide the method for identifying users (authentication); for remote access control (authorization); and for collecting and sending security server information used for billing, auditing, and reporting (accounting).

aggressive mode --Mode that eliminates several steps during Internet Key Exchange (IKE) authentication negotiation between two or more IPsec peers. Aggressive mode is faster than main mode but is not as secure.

authorization --Method for remote access control, including one-time authorization or authorization for each service; per-user account list and profile; user group support; and support of IP, IPX, ARA, and Telnet. AAA authorization works by assembling a set of attributes that describe what the user is authorized to perform. These attributes are compared to the information contained in a database for a given user and the result is returned to AAA to determine the actual capabilities and restrictions of the user. The database can be located locally on the access server or router, or it can be hosted remotely on a RADIUS or TACACS+ security server. Remote security servers, such as RADIUS and TACACS+, authorize users for specific rights by associating attribute-value (AV) pairs, which define those rights, with the appropriate user. All authorization methods must be defined through AAA.

CA --certificate authority. An entity in a network that issues and manages security credentials and public keys (in the form of X509v3 certificates) for message encryption. As part of a public key infrastructure (PKI), a CA checks with a registration authority (RA) to verify information provided by the requestor of a digital certificate. If the RA verifies the information of the requestor, the CA can then issue a certificate. Certificates generally include the public key of the owner, the expiration date of the certificate, the name of the owner, and other information about the public key owner.

CRWS --Cisco Router Web Setup Tool. Tool that provides web interface capabilities.

cTCP --Cisco Tunneling Control Protocol. When cTCP is enabled on a remote device (client) and headend device, IKE and ESP (Protocol 50) traffic is encapsulated in the TCP header so that the firewalls in between the client and the headend device permits this traffic (considering it the same as TCP traffic).

DPD --dead peer detection. Queries the liveliness of the Internet Key Exchange (IKE) peer of a router at regular intervals.

DSLAM --digital subscriber line access multiplexer. A device that connects many digital subscriber lines to a network by multiplexing the DSL traffic onto one or more network trunk lines.

IKE --Internet Key Exchange. Key management protocol standard that is used in conjunction with the IP Security (IPsec) standard. IPsec is an IP security feature that provides robust authentication and encryption of IP packets. IPsec can be configured without IKE, but IKE enhances IPsec by providing additional features, flexibility, and ease of configuration for the IPsec standard. IKE is a hybrid protocol that implements the Oakley key exchange and Skeme key exchange inside the Internet Security Association and Key Management Protocol (ISAKMP) framework. ISAKMP, Oakley, and Skeme are security protocols implemented by IKE.

IPsec --IP Security Protocol. Framework of open standards that provides data confidentiality, data integrity, and data authentication between participating peers. IPsec provides these security services at the IP layer. IPsec uses IKE to handle negotiation of protocols and algorithms based on local policy and to generate the encryption and authentication keys to be used by IPsec. IPsec can be used to protect one or more data flows between a pair of hosts, between a pair of security gateways, or between a security gateway and a host.

main mode --Mode that ensures the highest level of security when two or more IPsec peers are negotiating IKE authentication. It requires more processing time than aggressive mode.

MIB --Management Information Base. Database of network management information that is used and maintained by a network management protocol, such as Simple Network Management Protocol (SNMP) or

Common Management Information Protocol (CMIP). The value of a MIB object can be changed or retrieved using SNMP or CMIP commands, usually through a graphical user interface (GUI) network management system (NMS). MIB objects are organized in a tree structure that includes public (standard) and private (proprietary) branches.

peer --Router or device that participates as an endpoint in IPsec and IKE.

preshared key --Shared, secret key that uses IKE for authentication.

QoS --quality of service. Capability of a network to provide better service to selected network traffic over various technologies, including Frame Relay; Asynchronous Transfer Mode (ATM); Ethernet; and 802.1 networks, SONET, and IP-routed networks that may use any or all of these underlying technologies.

RADIUS --Remote Authentication Dial-In User Service. Distributed client or server system that secures networks against unauthorized access. RADIUS clients run on Cisco routers and send authentication requests to a central RADIUS server that contains all user authentication and network service access information.

SA --security association. Instance of security policy and keying material applied to a data flow. Both IKE and IPsec use SAs, although SAs are independent of one another. IPsec SAs are unidirectional, and they are unique in each security protocol. An IKE SA is used by IKE only, and unlike the IPsec SA, it is bidirectional. IKE negotiates and establishes SAs on behalf of IPsec. A user can also establish IPsec SAs manually.

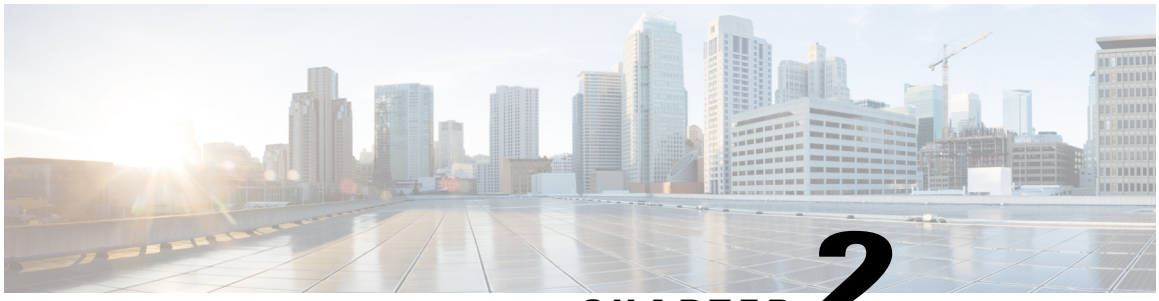
A set of SAs are needed for a protected data pipe, one per direction per protocol. For example, if you have a pipe that supports encapsulating security payload (ESP) between peers, one ESP SA is required for each direction. SAs are uniquely identified by destination (IPsec endpoint) address, security protocol (AH or ESP), and security parameter index (SPI).

SDM --Security Device Manager. Web interface manager that enables you to connect or disconnect a VPN tunnel and that provides a web interface for extended authentication (Xauth).

SNMP --Simple Network Management Protocol. Application-layer protocol that provides a message format for communication between SNMP managers and agents.

trap --Message sent by an SNMP agent to a network management system, console, or terminal to indicate the occurrence of a significant event, such as a specifically defined condition or a threshold that was reached.

VPN --Virtual Private Network. Enables IP traffic to travel securely over a public TCP/IP network by encrypting all traffic from one network to another. A VPN uses tunnels to encrypt all information at the IP level.



CHAPTER 2

Easy VPN Remote RSA Signature Support

The Easy VPN Remote RSA Signature Support feature provides support for the Rivest, Shamir, and Adleman (RSA) signatures on Easy VPN remote devices. The support is provided through RSA certificates that can be stored on or off the remote devices.

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table at the end of this module.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Prerequisites for Easy VPN Remote RSA Signature Support

- You must have a Cisco Virtual Private Network (VPN) remote device and be familiar with configuring the device.
- You must have a certification authority (CA) available to your network before you configure this interoperability feature. The CA must support the public key infrastructure (PKI) protocol of Cisco Systems, which is the Simple Certificate Enrollment Protocol (SCEP) (formerly called certificate enrollment protocol [CEP]).

- You should be familiar with IP Security (IPsec) and PKI and with configuring RSA key pairs and CAs.

Restrictions for Easy VPN Remote RSA Signature Support

- This feature should be configured only when you configure both IPsec and Internet Key Exchange (IKE) on your network.
- Easy VPN does not support RSA signature and preshared key authentication at the same time. A router can have one or more RSA signature-authenticated Easy VPN tunnels or preshared key-authenticated Easy VPN tunnels. However, only tunnels with the same authentication method are up at any time.
- Cisco IOS software does not support CA server public keys that are greater than 2048 bits.

Information About Easy VPN Remote RSA Signature Support

Easy VPN Remote RSA Signature Support Overview

The Easy VPN Remote RSA Signature Support feature allows you to configure RSA signatures on your Easy VPN remote device. The signatures can be stored on or off your remote device.

How to Configure Easy VPN Remote RSA Signature Support

Configuring Easy VPN Remote RSA Signature Support

To enable the RSA signatures, when you are configuring the Easy VPN remote and assigning the configuration to the outgoing interface, you must omit the **group** command. The content of the first Organizational Unit (OU) field will be used as the group. For information about configuring Cisco Easy VPN remote devices, refer to the Cisco Easy VPN Remote module.

Troubleshooting Easy VPN RSA Signature Support

To troubleshoot your Easy VPN remote RSA signature configuration, you can use the following **debug** commands. The **debug** commands can be used in any order or individually.

SUMMARY STEPS

1. **enable**
2. **debug crypto ipsec client ezvpn**
3. **debug crypto isakmp**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**debug crypto ipsec client ezvpn** **Example:** `Router# debug crypto ipsec client ezvpn`	Displays information about the VPN tunnel as it relates to the Easy VPN remote configuration.
Step 3	**debug crypto isakmp** **Example:** `Router# debug crypto isakmp`	Displays messages about IKE events.

Additional References

Related Documents

Related Topic	Document Title
Cisco IOS commands	Cisco IOS Master Commands List, All Releases
Security commands	Cisco IOS Security Command Reference
Configuring Internet Key Exchange for IPsec VPNs	Configuring Internet Key Exchange for IPsec VPNs
Deploying RSA keys	Deploying RSA Keys Within a PKI
Certificate Authorities	• Easy VPN Server • Cisco IOS PKI Overview: Understanding and Planning a PKI • Deploying RSA Keys Within a PKI • Configuring Certificate Enrollment for a PKI
Configuring a Cisco Easy VPN remote device	Cisco Easy VPN Remote

Standards

Standard	Title
None	--

MIBs

MIB	MIBs Link
None	To locate and download MIBs for selected platforms, Cisco software releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

RFCs

RFC	Title
None	--

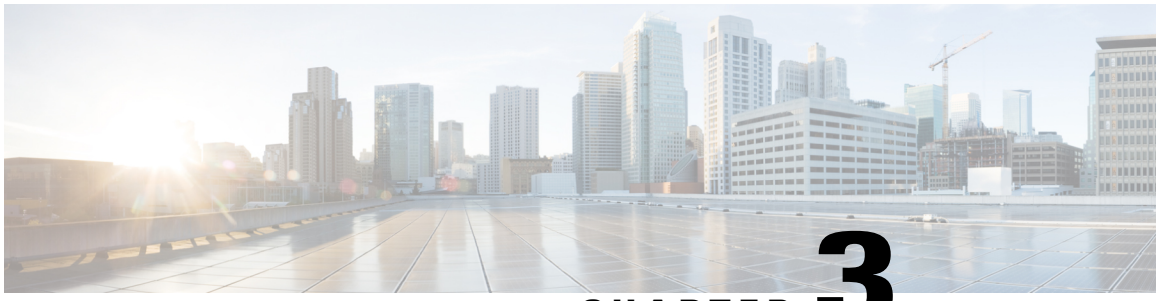
Technical Assistance

Description	Link
The Cisco Support and Documentation website provides online resources to download documentation, software, and tools. Use these resources to install and configure the software and to troubleshoot and resolve technical issues with Cisco products and technologies. Access to most tools on the Cisco Support and Documentation website requires a Cisco.com user ID and password.	http://www.cisco.com/cisco/web/support/index.html

Feature Information for Easy VPN Remote RSA Signature Support

Table 5: Feature Information for Easy VPN Remote RSA Signature Support

Feature Name	Releases	Feature Information
Easy VPN Remote RSA Signature Support	12.3(7)T1 12.2(33)SRA 12.2(33)SXH	The Easy VPN Remote RSA Signature Support feature provides for the support of Rivest, Shamir, and Adleman (RSA) signatures on Easy VPN remote devices. The support is provided through RSA certificates that can be stored on or off the remote device. The following sections provide information about this feature: The following commands were introduced or modified: **debug crypto ipsec client ezvpn**, **debug crypto isakmp**.



CHAPTER 3

Easy VPN Server

The Easy VPN Server feature allows a remote end user to communicate using IP Security (IPsec) with any Cisco IOS VPN gateway. Centrally managed IPsec policies are "pushed" to the client device by the server, thereby minimizing end-user configurations.

Note Security threats, as well as the cryptographic technologies to help protect against them, are constantly changing. For more information about the latest Cisco cryptographic recommendations, see the Next Generation Encryption (NGE) white paper.

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table at the end of this module.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Restrictions for Easy VPN Server

Unsupported Protocols

The table below outlines IPsec protocol options and attributes that are not supported by Cisco VPN clients. These options and attributes should not be configured on the device for these clients.

Table 6: Unsupported IPsec Protocol Options and Attributes

Options	Attributes
Authentication types	• Authentication with public key encryption • Digital Signature Standard (DSS)
Diffie-Hellman (DH) groups	1
IPsec protocol identifier	IPSEC_AH
IPsec protocol mode	Transport mode
Miscellaneous	• Manual keys • Perfect Forward Secrecy (PFS)

Cisco Secure VPN Client 1.x Restrictions

When used with the Easy VPN Server feature, the Cisco Secure VPN Client 1.x has the following restrictions:

- It does not support dead peer detection (DPD) or any other keepalive scheme.
- It does not support initial contact.
- This feature cannot use per-group attribute policy profiles such as IP addresses and Domain Name Service (DNS). Thus, customers must continue to use the existing, globally defined parameters for the IP address assignment, Windows Internet Naming Service (WINS), DNS, and preshared keys.

Multicast and Static NAT

Multicast and static Network Address Translation (NAT) are supported only for Easy VPN servers using dynamic virtual tunnel interfaces (DVTIs).

Virtual IPsec Interface Restrictions

The Virtual IPsec Interface Support feature works only with a Cisco software VPN Client version 4.x or later and an Easy VPN remote device that is configured to use a virtual interface.

Cisco Tunnel Control Protocol Restrictions

- If a port is being used for Cisco Tunnel Control Protocol, the port cannot be used for other applications.
- Cisco Tunnel Control Protocol can be used on only ten ports at a time.
- Cisco Tunnel Control Protocol is supported on only Easy VPN servers.
- If a Cisco Tunnel Control Protocol connection is set up on a port, Cisco Tunnel Control Protocol cannot be disabled on that port because doing so causes the existing connection to stop receiving traffic.
- High Availability of Cisco Tunnel Control Protocol is not supported on the Easy VPN server.

Universal Client Mode

The Easy VPN Server feature does not support universal client mode using Dynamic Host Configuration Protocol (DHCP).

Information About Easy VPN Server

Easy VPN Server Operation

When the client initiates a connection with a Cisco IOS VPN device, the "conversation" that occurs between the peers consists of device authentication via Internet Key Exchange (IKE), followed by user authentication using IKE Extended Authentication (Xauth), VPN policy push (using Mode Configuration), and IPsec security association (SA) creation. An overview of this process is as follows:

- The client initiates IKE Phase 1 via aggressive mode (AM) if a preshared key is to be used for authentication; the client initiates main mode (MM) if digital certificates are used. If the client identifies itself with a preshared key, the accompanying group name entered in the configuration GUI (ID_KEY_ID) 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 group profile.

Note Because the client may be configured for preshared key authentication, which initiates IKE AM, Cisco recommends that the administrator change the identity of the Cisco IOS VPN device via the **crypto isakmp identity hostname** command. This client configuration will not affect certificate authentication via IKE MM.

- The client attempts to establish an IKE SA between its public IP address and the public IP address of the Cisco IOS VPN device. It is proposed that every combination of encryption, hash algorithms, authentication methods and D-H group sizes must be used to reduce the amount of manual configuration on the client.
- Depending on its IKE policy configuration, the Cisco IOS VPN device will determine which proposal is acceptable to continue negotiating Phase 1.

Tip IKE policy is global for the Cisco IOS VPN device and can consist of several proposals. In the case of multiple proposals, the Cisco IOS VPN device will use the first match, so you should always list your most secure policies first.

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

- After the IKE SA is successfully established, and if the Cisco IOS VPN 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 AAA protocols such as RADIUS and TACACS+. Token cards may also be used via AAA proxy. During Xauth, a user-specific attribute may be retrieved if the credentials of that user are validated via RADIUS.

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

- If the Cisco IOS VPN device indicates that authentication was successful, the client requests further configuration parameters from the peer. The remaining system parameters (for example, the IP address, DNS, and split tunnel attributes) are pushed to the client at this time using 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 parameters in a group profile; all other parameters are optional.

- After each client is assigned an internal IP address via Mode Configuration, the Cisco IOS VPN device must know how to route packets through the appropriate VPN tunnel. Reverse route injection (RRI) will ensure that a static route is created on the Cisco IOS VPN device for each client internal IP address.

  Note Cisco recommends that you enable RRI on the crypto map (static or dynamic) for the support of VPN clients unless the crypto map is being applied to a generic routing encapsulation (GRE) tunnel that is already being used to distribute routing information.

- After the configuration parameters have been successfully received by the client, IKE quick mode is initiated to negotiate the IPsec SA establishment.
- After IPsec SAs are created, the connection is complete.

RADIUS Support for Group Profiles

Group policy information is stored in a profile that can be defined locally in the device configuration or on a RADIUS server that is accessible by the Cisco IOS VPN device. If RADIUS is used, you must configure access to the server and allow the Cisco IOS VPN device to send requests to the server.

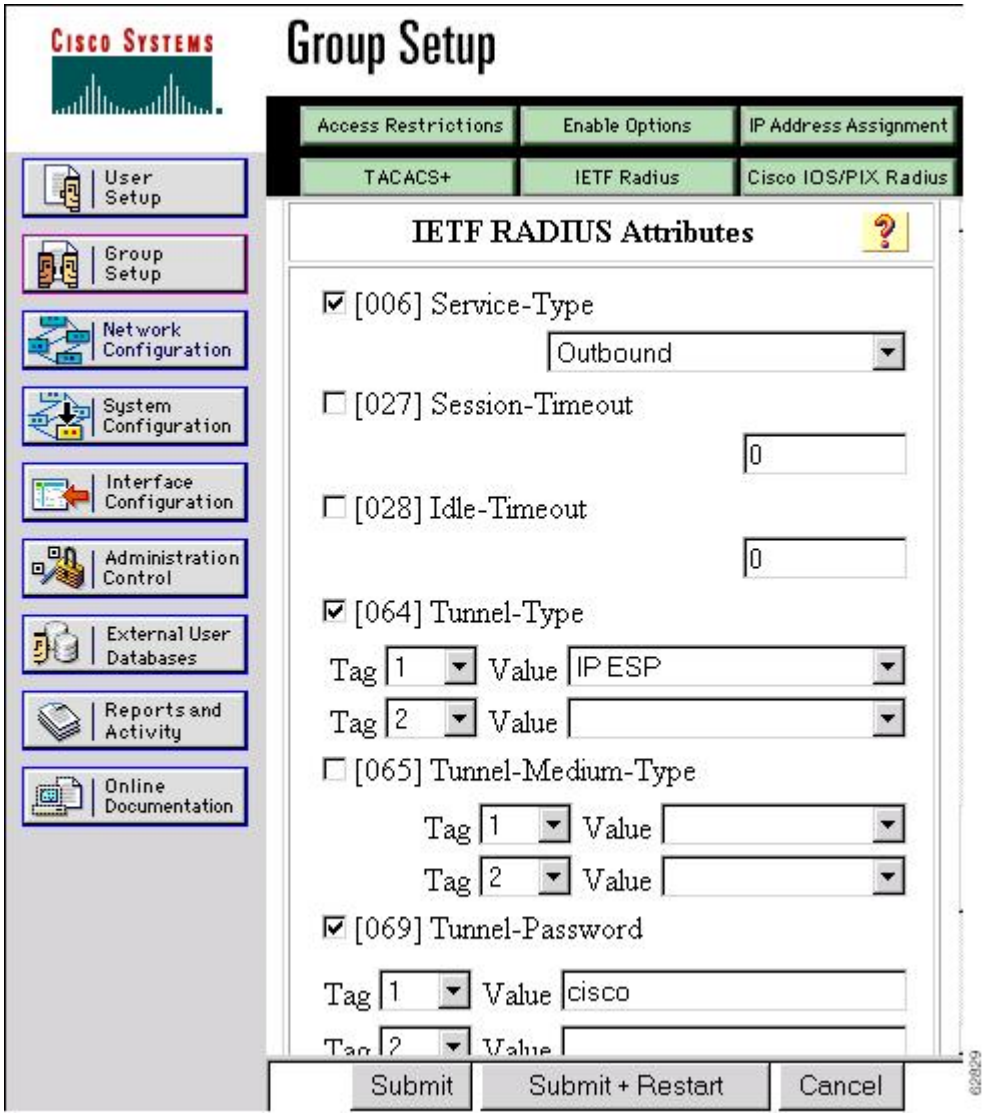
To define group policy attributes for RADIUS, you must perform the following task on your RADIUS server: Define a user that has a name equal to the group name as defined in the client GUI. For example, if users will be connecting to the Cisco IOS VPN device using the group name “sales,” you will need a user whose name is “sales.” The password for this user is “cisco,” which is a special identifier that is used by the device for RADIUS purposes. The username must then be made a member of a group in which the correct policy is defined. For simplicity, Cisco recommends that the group name be the same as the username.

For a Cisco Secure Access Control Server

If you are using a Cisco Secure access control server (ACS), you may configure your remote access VPN group profiles on this server. To perform this task, you must ensure that IETF RADIUS attributes are selected for group configuration as shown in the figure below. (This figure also shows the compulsory attributes required for a remote access VPN group.) All values must be entered except the Tunnel-Password attribute,

which is actually the preshared key for IKE purposes; if digital certificates are preferred, this attribute may be omitted.

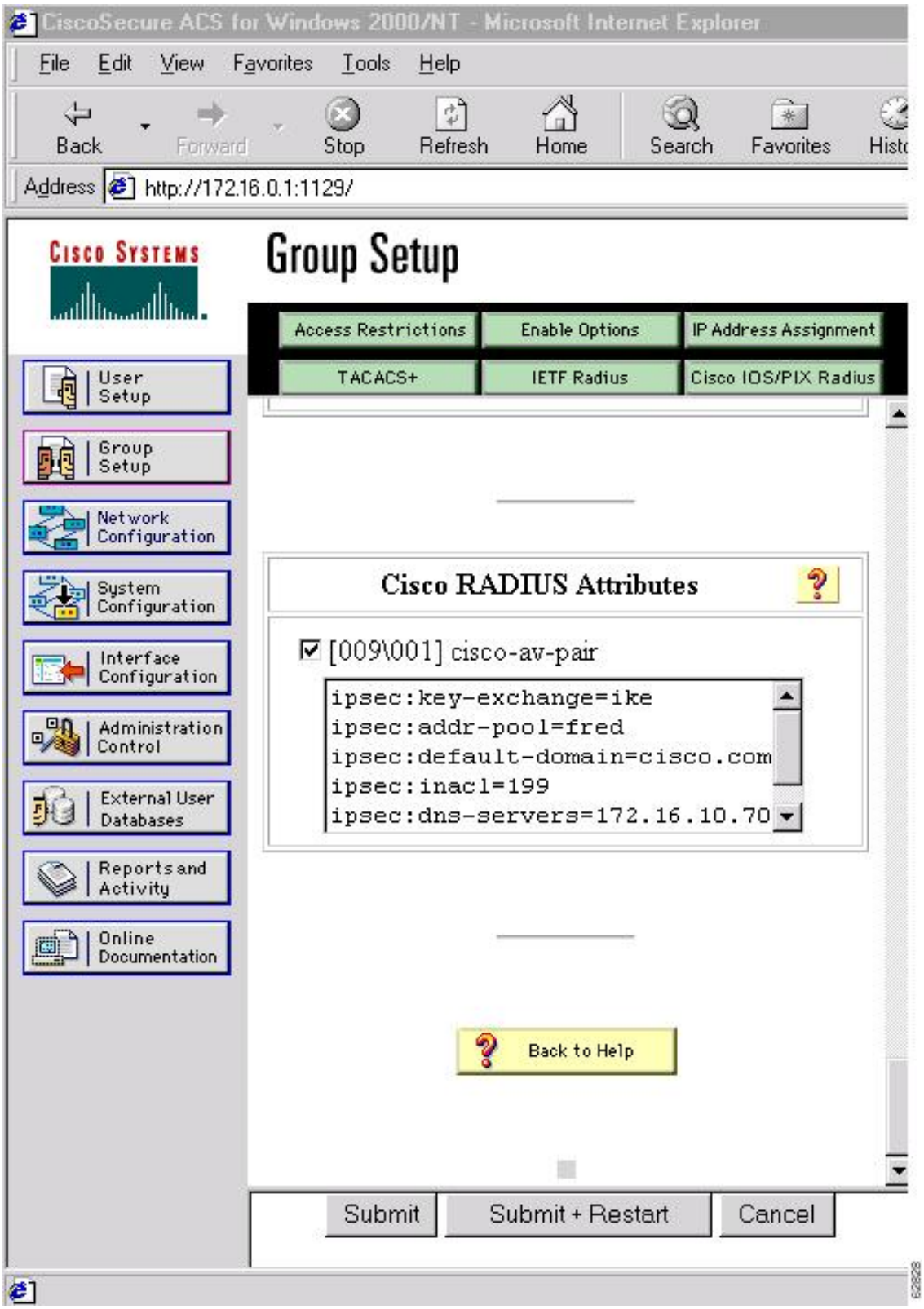
Figure 13: IETF RADIUS Attributes Selection for Group Configuration



In addition to the compulsory attributes shown in the figure, other values can be entered that represent the group policy that is pushed to the remote client via Mode Configuration. The figure below shows an example of a group policy. All attributes are optional except the addr-pool, key-exchange=preshared-key, and key-exchange=ike attributes. The values of the attributes are the same as the settings used if the policy is

defined locally on the device rather than in a RADIUS server (These values are explained in the "Defining Group Policy Information for Mode Configuration Push" section).

Figure 14: Cisco Secure ACS Group Policy Setup


CiscoSecure ACS for Windows 2000/NT - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Forward Stop Refresh Home Search Favorites
Address http://172.16.0.1:1129/
Cisco Systems
Group Setup
Access Restrictions
Enable Options
IP Address Assignment
TACACS+
IETF Radius
Cisco IOS/PIX Radius
User Setup
Group Setup
Network Configuration
System Configuration
Interface Configuration
Administration Control
External User Databases
Reports and Activity
Online Documentation
Cisco RADIUS Attributes
[009\001] cisco-av-pair
ipsec:key-exchange=ike
ipsec:addr-pool=fred
ipsec:default-domain=cisco.com
ipsec:inacl=199
ipsec:dns-servers=172.16.10.70
Back to Help
Submit
Submit + Restart
Cancel

After the group profile is created, a user who is a member of the group should be added. (Remember that the defined username maps to the group name as defined on the remote client, and the password defined for the username in the RADIUS database must be “cisco.”) If digital certificates are the preferred method of IKE authentication, the username should reflect the OU field in the certificate presented by the remote client.

For All Other RADIUS Servers

Ensure that your RADIUS server allows you to define attribute-value (AV) pairs. (For an example, see the “Example: Configuring Cisco IOS Software for Easy VPN Server” section.)

Note If digital certificates are used, the username defined in RADIUS must be equal to the OU field of the DN of the certificate of the client.

RADIUS Support for User Profiles

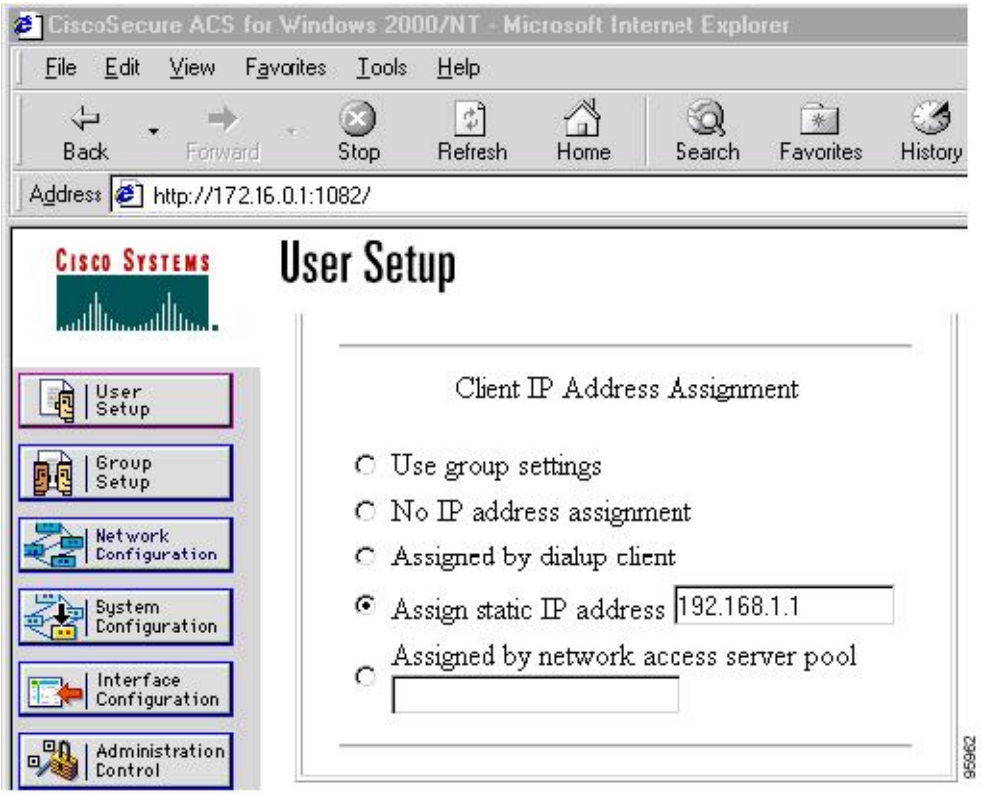
Attributes may be applied on a per-user basis. If you apply attributes on a per-user basis, you can override a group attribute value with an individual user attribute. The attributes are retrieved at the time that user authentication via Xauth occurs. The attributes are then combined with group attributes and applied during Mode Configuration.

User-based attributes are available only if RADIUS is being used for user authentication.

To define user policy attributes for RADIUS, you must perform the following task on your RADIUS server: Define a user or add attributes to the existing profile of a user in your RADIUS database. The password for the user will be used during Xauth user authentication, or you may proxy to a third-party server, such as a token card server.

The figure below shows how Cisco Secure ACS may be used for user authentication and for the assignment of a Framed-IP-Address attribute that may be pushed to the client. The presence of this attribute means that the local address pool defined for the group to which that user belongs will be overridden.

Figure 15: Cisco Secure ACS User Profile Setup



For All Other RADIUS Servers

Ensure that your RADIUS server allows you to define AV pairs. (See "Example: Configuring Cisco IOS Software for Easy VPN Server" section.)

Easy VPN Server Supported Protocols

The table below outlines supported IPsec protocol options and attributes that can be configured for this feature. (See the Unsupported Protocols section in the *Restrictions for Easy VPN Server* for unsupported options and attributes.)

Table 7: Supported IPsec Protocol Options and Attributes

Options	Attributes
Authentication algorithms	• Hashed Message Authentication Codes with message digest algorithm 5 (HMAC-MD5) • HMAC-Secure Hash Algorithm 1 (HMAC-SHA1)
Authentication types	• Preshared keys • RSA digital signatures
D-H groups	• 2 • 5
Encryption algorithms (IKE)	• Data Encryption Standard (DES) • Triple Data Encryption Standard (3DES)
Encryption algorithms (IPsec)	• DES • 3DES • NULL
IPsec protocol identifiers	• Encapsulating Security Payload (ESP) • IP Lempel-Ziv-Stac compression (IPCOMP-LZS)
IPsec protocol mode	Tunnel mode

Table 8: AAA protocols and services supported by Easy VPN Server

AAA Service	Database Type		
	RADIUS	TACACS+	Local
Authentication	Yes	Yes	Yes
Authorization	Yes	Yes	Yes
Accounting	Yes	Yes	No

We recommend choosing RADIUS over TACACS+. Easy VPN does not support other AAA protocols such as LDAP and Kerberos.

Functions Supported by Easy VPN Server

Mode Configuration Version 6 Support

Mode Configuration Version 6 is supported for more attributes (as described in an IETF draft submission).

Xauth Version 6 Support

Cisco software supports XAuth version 6. Xauth for user authentication is based on an IETF draft submission.

Internet Key Exchange (IKE) Dead Peer Detection (DPD)

The client implements a keepalive scheme—IKE DPD.

DPD allows two IPsec peers to determine whether the other is still “alive” during the lifetime of a VPN connection. DPD is useful because a host may reboot, or the dialup link of a remote user may disconnect without notifying the peer that the VPN connection has gone away. When an IPsec host determines that a VPN connection no longer exists, the host can notify a user, attempt to switch to another IPsec host, or clean up valuable resources that were allocated for the peer that no longer exists.

A Cisco VPN device can be configured to send and reply to DPD messages. DPD messages are sent if no other traffic is being passed through the VPN tunnel. If a configured amount of time has elapsed since the last inbound data was received, DPD will send a message (“DPD R-U-THERE”) the next time it sends outbound IPsec data to the peer. DPD messages are unidirectional and are automatically sent by Cisco VPN clients. DPD must be configured on the device only if the device wants to send DPD messages to the VPN client to determine the health of the client.

Split Tunneling Control

Remote clients can support split tunneling, which enables a client to have intranet and Internet access at the same time. If split tunneling is not configured, the client will direct all traffic through the tunnel, even traffic destined for the Internet.

Note The split tunnel access control list (ACL) has a limit of 50 access control entries (ACEs). If more than 50 ACEs are configured in a split tunnel ACL, only the first 50 ACEs are considered. These ACEs are sent to the client during Mode Configuration.

Initial Contact

If a client is suddenly disconnected, the gateway may not be notified. Consequently, removal of connection information (IKE and IPsec SAs) for that client will not immediately occur. Thus, if the client attempts to

reconnect to the gateway, the gateway will refuse the connection because the previous connection information is still valid.

To avoid such a scenario, Cisco introduced a new capability called initial contact that is supported by all Cisco VPN products. If a client or device is connecting to another Cisco gateway for the first time, an initial contact message is sent that tells the receiver to ignore and delete any old connection information that has been maintained for that newly connecting peer. Initial contact ensures that connection attempts are not refused because of SA synchronization problems, which are often identified via invalid security parameter index (SPI) messages and which require devices to have their connections cleared.

Group-Based Policy Control

Policy attributes such as IP addresses, DNS, and split tunnel access can be provided on a per-group or per-user basis.

User-Based Policy Control

Attributes may be applied on a per-user basis. You can override a group attribute value with an individual user attribute. The attributes are retrieved at the time that user authentication via XAuth occurs. They are then combined with group attributes and applied during Mode Configuration.

Effective with Cisco IOS Release 12.3(4)T, attributes can be applied on a per-user basis after the user has been authenticated. These attributes can override any similar group attributes. User-based attributes are available only if RADIUS is used as the database.

Framed-IP-Address

To select the Framed-IP-Address attribute for CiscoSecure for NT, under the user profile choose the “use this IP address” option under addressing and manually enter the address. (You should check the method of configuring a framed IP address with your own RADIUS server because this procedure will vary.)

Note If a framed IP address is present, and a local pool address is also configured for the group that the user belongs to, the framed IP address will override the local pool setting.

DHCP Client Proxy

Easy VPN servers assign an IP address to a remote device using either a local pool that is configured on another device or the framed IP address attribute that is defined in RADIUS. Effective with Cisco IOS Release 12.4(9)T, the DHCP Client Proxy feature provides the option of configuring an Easy VPN server to obtain an IP address from a DHCP server. The IP address is pushed to the remote device using Mode Configuration.

Note This feature does not allow the DHCP server to push the DNS, WINS server, or domain name to the remote client.

To configure DHCP Client Proxy, see the “Configuring an Easy VPN Server to Obtain an IP Address from a DHCP Server.”

Benefits of DHCP Client Proxy

- This feature helps in creating dynamic Domain Name System (DDNS) entries when a DNS server exists in conjunction with the DHCP server.
- The user is not restricted to IP address pools.

User-Save-Password

As per the group description, the User-Save-Password attribute can be received in addition to the group variant (Save-Password) attribute, but if it is received it will override the value asserted by the group.

The following is an output example of a RADIUS AV pair for the User-Save-Password attribute:

```
ipsec:user-save-password=1
```

User-Include-Local-LAN

As per the group description, the User-Include-Local-LAN attribute can be received in addition to the group variant (Include-Local-LAN), but if it is received, it will override the value asserted by the group.

The following is an output example of a RADIUS AV pair for the User-Include-Local LAN attribute:

```
ipsec:user-include-local-lan=1
```

User-VPN-Group

The User-VPN-Group attribute is a replacement for the group lock attribute. It allows support for both the preshared key and the RSA signature authentication mechanisms such as certificates.

If you need to check that the group a user is attempting to connect to is indeed the group the user belongs to, use the User-VPN-Group attribute. The administrator sets this attribute to a string, which is the group that the user belongs to. The group the user belongs to is matched against the VPN group as defined by the group name (ID_KEY_ID) for preshared keys or by the OU field of a certificate. If the groups do not match, the client connection is terminated.

This feature works only with AAA RADIUS. Local XAuth authentication must still use the Group-Lock attribute.

The following is an output example of a RADIUS AV pair for the User-VPN-Group attribute:

```
ipsec:user-vpn-group=cisco
```

Group-Lock

If you are using preshared keys (no certificates or other RSA signature authentication mechanisms) with RADIUS or local AAA, you can continue to use the Group-Lock attribute. If you are using preshared keys (no certificates or other RSA signature authentication mechanisms) with RADIUS only, you can either continue to use the Group-Lock attribute or you can use the User-VPN-Group attribute.

Group Lock Feature Operation

The group lock feature, introduced in Cisco IOS 12.2(13)T, allows you to perform an extra authentication check during Xauth. With this feature enabled, the user must enter a username, group name, and user password during Xauth to authenticate. The username and group name can be entered in any of the following formats: “username/group name,” “username\group name,” “username%group name,” or “username group name.” The server compares the group name entered during Xauth with the group name sent for preshared key device

authentication. If they do not match, the server denies the connection. To enable this feature, use the **group-lock** command for the group.

Cisco software does not strip the @group from the Xauth username, so the username user@group must exist in the local or external AAA database pointed to by the Internet Security Association Key Management Protocol (ISAKMP) profile selected at Phase 1 (machine group authentication).

Caution Do not use the Group-Lock attribute if you are using RSA signature authentication mechanisms such as certificates. Use the User-VPN-Group attribute instead. The User-VPN-Group attribute is recommended regardless of whether preshared keys or the RSA signature is used as the method of authentication when an external AAA database is used.

Session Monitoring for VPN Group Access

It is possible to mimic the functionality provided by some RADIUS servers for limiting the maximum number of connections to a specific server group and also for limiting the number of simultaneous logins for users in that group. After user-defined thresholds are defined in each VPN group, connections will be denied until counts drop below these thresholds.

If you use a RADIUS server, such as CiscoSecure ACS, Cisco recommends that you enable this session control on the RADIUS server if the functionality is provided. In this way, usage can be controlled across a number of servers by one central repository. When this feature is enabled on the device, only connections to groups on that specific device are monitored. Load-sharing scenarios are not accurately accounted for.

To configure session monitoring using CLI, use the **crypto isakmp client configuration group** command and the **max-users** and **max-logins** commands.

The following is an output example of RADIUS AV pairs that have been added to the relevant group:

```
ipsec:max-users=1000
ipsec:max-logins=1
```

Virtual IPsec Interface Support on a Server

The Virtual IPsec Interface Support on a Server feature allows you to selectively send traffic to different Easy VPN concentrators (servers) and to the Internet.

Before Cisco IOS Release 12.4(4)T, at the tunnel-up/tunnel-down transition, attributes that were pushed during the mode configuration had to be parsed and applied. When such attributes resulted in the configurations being applied on the interface, the existing configuration had to be overridden.

With the Virtual IPsec Interface Support on a Server feature, the tunnel-up configuration can be applied to separate interfaces, making it easier to support separate features at tunnel-up. Features that are applied to the traffic going into the tunnel can be separate from the features that are applied to traffic that is not going through the tunnel (for example, split-tunnel traffic and traffic leaving the device when the tunnel is not up). When the Easy VPN negotiation is successful, the line protocol state of the virtual-access interface gets changed to up. When the Easy VPN tunnel goes down because the SA expires or is deleted, the line protocol state of the virtual access interfaces changes to down.

Note The Virtual IPsec Interface Support on a Server feature does not support multicast.

For more information about this feature, see the "Cisco Easy VPN Remote" module. (This feature is configured on the Easy VPN remote device.)

For information about the IPsec Virtual Tunnel Interface feature, see the "IPsec Virtual Tunnel Interface" module in the *Security for VPNs with IPsec Configuration Guide*.

Virtual Tunnel Interface per-User Attribute Support

Effective with Cisco IOS Release 12.4(9)T, the Virtual Tunnel Interface feature provides per-user attribute support for Easy VPN servers.

For more information about this feature, see the "IPsec Virtual Tunnel Interface" module in the *Security for VPNs with IPsec Configuration Guide* .

Banner, Auto-Update, and Browser Proxy

The following sections describe support for attributes that aid in the management of the Cisco Easy VPN remote device:

Banner

An Easy VPN server can be configured to push the banner to the Easy VPN remote device. A banner is needed for the web-based activation feature. The banner is displayed when the Easy VPN tunnel is up on the Easy VPN remote console or as an HTML page in the case of web-based activation.

Auto-Update

An Easy VPN server can be configured to provide an automated mechanism for software and firmware upgrades on an Easy VPN remote device.

Browser Proxy

An Easy VPN server can be configured so that an Easy VPN remote device can access resources on the corporate network. Using this feature, the user does not have to manually modify the proxy settings of the web browser when connecting to the corporate network using the Cisco IOS VPN Client or manually revert the proxy settings upon disconnecting.

Configuration Management Enhancements

Pushing a Configuration URL Through a Mode-Configuration Exchange

When remote devices connect to a corporate gateway for creating an IPsec VPN tunnel, some policy and configuration information has to be applied to the remote device when the VPN tunnel is active to allow the remote device to become a part of the corporate VPN.

The Pushing a Configuration URL Through a Mode-Configuration Exchange feature provides a mode-configuration attribute that "pushes" a URL from the concentrator (server) to the Cisco IOS Easy VPN remote device. The URL contains the configuration information that the remote device has to download and apply to the running configuration, and it contains the Cisco IOS CLI listing. (For more information about

Cisco IOS CLI listing, see Cisco IOS documentation for the **configuration url** command.) The CLI for this feature is configured on the concentrator.

The configuration that is pushed to the remote device is persistent by default. That is, the configuration is applied when the IPsec tunnel is “up,” but it is not withdrawn when the IPsec tunnel goes “down.” However, a section of the configuration can be written that is transient in nature, in which case the configuration of the section is reverted when the tunnel is disconnected.

There are no restrictions on where the configuration distribution server is physically located. However, Cisco recommends that a secure protocol such as Secure HTTP (HTTPS) be used to retrieve the configuration. The configuration server can be located in the corporate network, and because the transfer happens through the IPsec tunnel, insecure access protocols (HTTP) can be used.

Regarding backward compatibility, the remote device asks for the CONFIGURATION-URL and CONFIGURATION-VERSION attributes. Because the CONFIGURATION-URL and CONFIGURATION-VERSION attributes are not mandatory attributes, the server sends them only if it has them configured for the group. There is no built-in restriction to push the configuration, but bootstrap configurations (such as for the IP address) cannot be sent because those configurations are required to set up the Easy VPN tunnel, and the CONFIGURATION-URL comes into effect only after the Easy VPN tunnel comes up.

After the Configuration Has Been Acquired by the Easy VPN Remote Device

After the configuration has been acquired by the Easy VPN remote device, the remote device sends a new ISAKMP notification to the Easy VPN server. The notification contains several manageability information messages about the client (remote device). The Easy VPN server takes two actions when this information is received:

- The Easy VPN server caches the information in its peer database. The information can be displayed by using the **show crypto isakmp peer config** command. This command output displays all manageability information that is sent by the client (remote device).
- If accounting is enabled, the Easy VPN server sends an accounting update record that contains the manageability information messages about the remote device to the accounting RADIUS server. This accounting update is later available in the accounting log of the RADIUS server.

How to Configure This Feature

The commands that are used to configure this feature and the CONFIGURATION-URL and CONFIGURATION-VERSION attributes are described in the **crypto isakmp client configuration group** command documentation.

Per-User AAA Policy Download with PKI

With the Support of Per-User AAA Policy Download with PKI feature, user attributes are obtained from the AAA server and pushed to the remote device through Mode Configuration. The username that is used to get the attributes is retrieved from the remote device certificate.

Per-User Attribute Support for Easy VPN Servers

The Per-User Attribute Support for Easy VPN Servers feature provides users with the ability to support per-user attributes on Easy VPN servers. These attributes are applied on the virtual access interface.

Local Easy VPN AAA Server

For a local Easy VPN AAA server, the per-user attributes can be applied at the group level or at the user level using the CLI.

To configure per-user attributes for a local Easy VPN server, see "Configuring Per-User Attributes on a Local Easy VPN AAA Server."

Remote Easy VPN AAA Server

Attribute value (AV) pairs can be defined on a remote Easy VPN AAA server as shown in the following example:

```
cisco-avpair = "ip:outacl#101=permit tcp any any established
```

Per-User Attributes

The following per-user attributes are defined in the AAA server and are applicable to IPsec:

- inacl
- interface-config
- outacl
- policy-route
- prefix
- route
- rte-fltr-in
- rte-fltr-out
- sub-policy-In
- sub-policy-Out

Syslog Message Enhancements

Syslog messages were added for Easy VPN in Cisco IOS Release 12.4(4)T. The syslog messages can be enabled on your server by using the CLI. The format of the syslog messages is as follows:

```
timestamp: %CRYPTO-6-VPN_TUNNEL_STATUS: (Server)  <event message>  User=<username>
Group=<groupname>  Client_public_addr=<ip_addr> Server_public_addr=<ip addr>
```

For an authentication-passed event, the syslog message looks like the following:

```
Jul 25 23:33:06.847: %CRYPTO-6-VPN_TUNNEL_STATUS: (Server) Authentication PASS
ED User=blue Group=Cisco1760group Client_public_addr=10.20.20.1 Server_public_addr=10.20.20.2
```

Three of the messages (Max users, Max logins, and Group do not exist) are authorization issues and are printed only with the group name in the format because the authorization check occurs before mode configuration.

Therefore, the peer information is not yet present and cannot be printed. The following is an example of a "Group does not exist" message.

```
*Jun 30 18:02:58.107: %CRYPTO-6-VPN_TUNNEL_STATUS: Group: group_1 does not exist
```

Supported Easy VPN Syslog Messages

Both ezvpn_connection_up and ezvpn_connection_down were already supported in a previous release of syslog messages. The enhancements in Cisco IOS Release 12.4(4)T follow the same format, but new syslogs are introduced. The added syslogs are as follows:

- ACL associated with Ezvpn policy but NOT defined (hence, no split tunneling possible)
- Authentication Failed (AAA Not Contactable)
- Authentication Passed
- Authentication Rejected
    - Access restricted via incoming interface
    - Group does not exist
    - Group Lock Enabled
    - Incorrect Username or Password
    - Max Users exceeded/Max Logins exceeded
    - Number of Retries exceeded
- Incorrect firewall record being sent by Client (incorrect vendor, or product, or capability)
- IP Pool Not present/No Free IP Address available in the pool
- Save password Turned ON

Network Admission Control Support for Easy VPN

Network Admission Control was introduced in Cisco IOS Release 12.3(8)T as a way to determine whether a PC client should be allowed to connect to the LAN. Network Admission Control uses Extensible Authentication Protocol over UDP (EAPoUDP) to query the Cisco trust agent on the PC and allows a PC to access the network if the client status is healthy. Different policies can be applied on the server to deny or limit access of PCs that are infected.

Effective with Cisco IOS Release 12.4(4)T, Network Admission Control can be used to also monitor the status of remote PC clients. After the Easy VPN tunnel comes up and the PC starts to send traffic, the traffic is intercepted at the Easy VPN server, and the posture validation process starts. The posture validation process consists of sending an EAPoUDP request over the Easy VPN tunnel and querying the Cisco trust agent. The authentication server is configured inside the trusted network, behind the IPsec aggregator.

The configuration of an Easy VPN server that has Network Admission Control enabled is shown in the output in "Example: Network Admission Control."

Central Policy Push Firewall Policy Push

The Easy VPN server supports Central Policy Push (CPP) Firewall Policy Push feature, which allows administrators to push policies that enforce security to the Cisco Easy VPN Client and related firewall software.

A split tunnel enables access to corporate networks, but it also allows a remote device to be exposed to attacks from the Internet. The Central Policy Push (CPP) Firewall Policy Push feature enables the server to determine whether to allow or deny a tunnel if the remote device does not have a required firewall, thereby reducing exposure to attacks.

The following firewall types are supported:

- Cisco-Integrated-firewall (central-policy-push)
- Cisco-Security-Agent (check-presence)
- Zonelabs-Zonealarm (both)
- Zonelabs-ZonealarmPro (both)

The server can be used either to check the presence of a firewall on the client (remote device) using the check-presence option or to specify the specifics of the firewall policies that must be applied by the client using the central-policy-push.

Note The **policy check-presence** command and keyword, which are used with this feature, replace the **firewall are-u-there** command functionality that was supported before Cisco IOS Release 12.4(6)T. The **firewall are-u-there** command is supported for backward compatibility.

For information on enabling this feature, see the "Defining a CPP Firewall Policy Push Using a Local AAA Server" and "Applying a CPP Firewall Policy Push to the Configuration Group."

Syslog Support for CPP Firewall Policy Push

Syslog support can be enabled using the **crypto logging ezvpn** command on your device. CPP syslog messages will be printed for the following error conditions:

- If a policy is configured on a group configuration (using the **firewall policy** command), but a global policy with the same name is not defined (using the **crypto isakmp client firewall** command), the syslog message is as follows:
  ```
  Policy enabled on group configuration but not defined
  ```
  Tunnel setup proceeds as normal (with the firewall).
- If an incorrect firewall request (vendor/product/cap incorrect order) is received, the syslog message is as follows:
  ```
  Incorrect firewall record received from client
  ```
- If a policy mismatch occurs between the Cisco VPN Client and the server, the syslog is as follows:
  ```
  CPP policy mismatch between client and headend
  ```

Password Aging

Prior to Cisco IOS Release 12.4(6)T, EasyVPN remote devices (clients) sent username and password values to the Easy VPN server, which in turn sent them to the AAA subsystem. The AAA subsystem generated an

authentication request to the RADIUS server. If the password had expired, the RADIUS server replied with an authentication failure. The reason for the failure was not passed back to the AAA subsystem. The user was denied access due to authentication failure, but did not know that the failure was due to password expiration.

Effective with Cisco IOS Release 12.4(6)T, if you have configured the Password Aging feature, the EasyVPN client is notified when a password has expired, and you are prompted to enter a new password. To configure the Password Aging feature, see the section "Configuring Password Aging, on page 164."

For more information about the Password Aging feature, see the "Related Documents" section.

Split DNS

Effective with Cisco IOS Release 12.4(9)T, split DNS functionality is available on Easy VPN servers. This feature enables the Easy VPN hardware client to use primary and secondary DNS values to resolve DNS queries. These values are pushed by the Easy VPN server to the Easy VPN remote device. To configure this feature on your server, use the **split-dns** command (see the "Defining Group Policy Information for Mode Configuration Push, on page 139"). Configuring this command adds the split-dns attribute to the policy group. The attribute will include the list of domain names that you configured. All other names will be resolved using the public DNS server.

For more information about configuring split DNS, see the document "Configuring Split and Dynamic DNS on the Cisco VPN 3000 Concentrator."

Cisco Tunneling Control Protocol

The Cisco Tunneling Control Protocol (cTCP) feature can be used for situations in which an Easy VPN remote device is operating in an environment in which standard IPsec does not function or does not function transparently without modification to existing firewall rules. These situations include the following:

- Small or home office device performing Network Address Translation (NAT) or Port Address Translation (PAT)
- PAT-provided IP address behind a larger device (for example, in a corporation)
- Non-NAT firewall (packet filtering or stateful)
- Proxy server

The firewall should be configured to allow the headend to accept Cisco Tunneling Control Protocol connections on the configured Cisco Tunneling Control Protocol port. This configuration is enabled on the Easy VPN server. If the firewall is not configured, the Cisco Tunneling Control Protocol traffic is not allowed.

Note Cisco Tunneling Control Protocol traffic is actually TCP traffic. Cisco Tunneling Control Protocol packets are IKE or Encapsulating Security Payload (ESP) packets that are being transmitted over TCP.

The Cisco Tunneling Control Protocol server sends a gratuitous ACK message to the client whenever the data received from the client over the established cTCP session reaches 3 kilobytes (KB) in size. A similar procedure is followed by the client. By default, this gratuitous ACK message is sent to keep the NAT or firewall sessions between the Cisco Tunneling Control Protocol server and Cisco Tunneling Control Protocol client alive. The data size at which gratuitous ACK messages are sent is not configurable.

Keepalives that are sent by a client or server do not keep the sessions alive when the server or client sends data at a high speed.

The Cisco Tunneling Control Protocol server sending ACK message ensures that NAT or firewall sessions do not drop packets when there is one-way traffic and the data is lengthy. It also ensures that an acknowledgment is provided from the device receiving the data.

VRF Assignment by a AAA Server

To assign VPN Routing and Forwarding (VRF) to Easy VPN users, enable the following attributes on a AAA server:

```
Cisco-avpair “ip:interface-config=ip vrf forwarding example1”
Cisco-avpair “ip:interface-config=ip unnumbered loopback10”
```

How to Configure Easy VPN Server

Enabling Policy Lookup via AAA

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **aaa new-model**
4. **aaa authentication password-prompt** *text-string*
5. **aaa authentication username-prompt** *text-string*
6. **aaa authentication login** [*list-name method1*] [*method2...*]
7. **aaa authorization network** *list-name* **local group radius**
8. **username** *name* **password** *encryption-type encrypted-password*
9. **exit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**aaa new-model** **Example:** `Device(config)# aaa new-model`	Enables AAA.

	Command or Action	Purpose
Step 4	**aaa authentication password-prompt** *text-string* **Example:** `Device(config)# aaa authentication password-prompt "Enter your password now:"`	(Optional) Changes the text displayed when users are prompted for a password.
Step 5	**aaa authentication username-prompt** *text-string* **Example:** `Device(config)# aaa authentication username-prompt "Enter your name here:"`	(Optional) Changes the text displayed when users are prompted to enter a username.
Step 6	**aaa authentication login** [*list-name method1*] [*method2...*] **Example:** `Device(config)# aaa authentication login userlist local group radius`	Sets AAA authentication at login. • A local and RADIUS server may be used together and will be tried in order. **Note** This command must be enabled to enforce Xauth.
Step 7	**aaa authorization network** *list-name* **local group radius** **Example:** `Device(config)# aaa authorization network grouplist local group radius`	Enables group policy lookup. • A local and RADIUS server may be used together and will be tried in order.
Step 8	**username** *name* **password** *encryption-type encrypted-password* **Example:** `Device(config)# username server_r password 7 121F0A18`	(Optional) Defines local users for Xauth if RADIUS or TACACS+ is not used. **Note** Use this command only if no external validation repository will be used.
Step 9	**exit** **Example:** `Device(config)# exit`	Exits global configuration mode and returns to privileged EXEC mode.

Defining Group Policy Information for Mode Configuration Push

Although users can belong to only one group per connection, they may belong to specific groups with different policy requirements. Thus, users may decide to connect to the client using a different group ID by changing their client profile on the VPN device. To define the policy attributes that are pushed to the client via Mode Configuration, perform the following steps.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **crypto isakmp client configuration group** {*group-name* | **default**}
4. **key** *name*
5. **dns** *primary-server secondary-server*
6. **wins** *primary-server secondary-server*
7. **domain** *name*
8. **pool** *name*
9. **netmask** *name*
10. **acl** *number*
11. **access-restrict** *interface-name*
12. Do one of the following:
    - **policy check-presence**
    - **firewall are-u-there**
13. **group-lock**
14. **include-local-lan**
15. **save-password**
16. **backup-gateway**
17. **pfs**
18. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**crypto isakmp client configuration group** {*group-name* | **default**} **Example:** `Device(config)# crypto isakmp client configuration group group1`	Specifies the policy profile of the group that will be defined and enters ISAKMP group configuration mode. • If no specific group matches and a default group is defined, users will automatically be given the policy of the default group.

	Command or Action	Purpose
Step 4	**key** *name* **Example:** `Device(config-isakmp-group)# key group1`	Specifies the IKE preshared key for the group policy attribute definition. **Note** This command must be enabled if the client identifies itself with a preshared key.
Step 5	**dns** *primary-server secondary-server* **Example:** `Device(config-isakmp-group)# dns 10.2.2.2 10.3.3.3`	(Optional) Specifies the primary and secondary DNS servers for the group.
Step 6	**wins** *primary-server secondary-server* **Example:** `Device(config-isakmp-group)# wins 10.10.10.10 10.12.12.12`	(Optional) Specifies the primary and secondary WINS servers for the group.
Step 7	**domain** *name* **Example:** `Device(config-isakmp-group)# domain example.com`	(Optional) Specifies the DNS domain to which a group belongs.
Step 8	**pool** *name* **Example:** `Device(config-isakmp-group)# pool pool1`	Defines a local pool address. • Although a user must define at least one pool name, a separate pool may be defined for each group policy. **Note** This command must be defined and refer to a valid IP local pool address or the client connection will fail.
Step 9	**netmask** *name* **Example:** `Device(config-isakmp-group)# netmask 255.255.255.255`	(Optional) Specifies that a subnet mask be downloaded to the client for local connectivity. **Note** Some VPN clients use the default mask for their particular classes of address. However, for a device, the host-based mask is typically used (/32). If you want to override the default mask, use the **netmask** command.
Step 10	**acl** *number* **Example:** `Device(config-isakmp-group)# acl 199`	(Optional) Configures split tunneling. • The *number* argument specifies a group of access control list (ACL) rules that represent protected subnets for split tunneling purposes.
Step 11	**access-restrict** *interface-name* **Example:** `Device(config-isakmp-group)# access-restrict fastethernet0/0`	Restricts clients in a group to an interface.

	Command or Action	Purpose

Step 12	Do one of the following:
	• **policy check-presence**
	• **firewall are-u-there**
	Example:
	`Device(config-isakmp-group)# policy check-presence`
	Example:
	`Device(config-isakmp-group)# firewall are-u-there`
		(Optional) Denotes that the server should check for the presence of the specified firewall (as shown as the firewall type on the client).
		or
		Adds the firewall are-u-there attribute to the server group if your PC is running the Black Ice or Zone Alarm personal firewalls.
		Note The **policy** command and **check-presence** keyword were added in Cisco IOS Release 12.4(6)T. Cisco recommends that the **policy** command be used instead of the **firewall are-u-there** command because the **policy** command is supported in local AAA and remote AAA configurations. The **firewall are-u-there** command can be figured only locally and is supported for backward compatibility.

Step 13	**group-lock** **Example:** `Device(config-isakmp-group)# group-lock`	Enforces the group lock feature.
Step 14	**include-local-lan** **Example:** `Device(config-isakmp-group)# include-local-lan`	(Optional) Configures the Include-Local-LAN attribute to allow a nonsplit-tunneling connection to access the local subnetwork at the same time as the client.
Step 15	**save-password** **Example:** `Device(config-isakmp-group)# save-password`	(Optional) Saves your Xauth password locally on your PC.
Step 16	**backup-gateway** **Example:** `Device(config-isakmp-group)# backup-gateway`	(Optional) Pushes a list of backup gateways to the client device. • These gateways are tried sequentially when the previous gateway fails. The gateways may be specified using IP addresses or hostnames.
Step 17	**pfs** **Example:** `Device(config-isakmp-group)# pfs`	(Optional) Notifies the client of the central-site policy regarding whether Password Forward Secrecy (PFS) is required for any IPsec SA. • Because the client device does not have a user interface option to enable or disable PFS negotiation, the server will notify the client device of the central site policy using this parameter. The Diffie-Hellman (D-H) group that is proposed for PFS will be the same that was negotiated in Phase 1 of the IKE negotiation.
Step 18	**end** **Example:** `Device(config-isakmp-group)# end`	Exits ISAKMP group configuration mode and returns to privileged EXEC mode.

Enabling VPN Session Monitoring

If you want to restrict the maximum number of connections to the device per VPN group and the maximum number of simultaneous logins per user, perform this task.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **crypto isakmp client configuration group** *group-name*
4. **exit**
5. **max-logins** *number-of-logins*
6. **max-users** *number-of-users*
7. **exit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**crypto isakmp client configuration group** *group-name* **Example:** `Device(config)# crypto isakmp client configuration group group1`	Specifies the policy profile of the group that will be defined and enters ISAKMP group configuration mode. • *group-name*—Group definition that identifies which policy is enforced for users.
Step 4	**exit** **Example:** `Device(config-isakmp-group)# exit`	Exits ISAKMP group configuration mode.
Step 5	**max-logins** *number-of-logins* **Example:** `Device(config)# max-logins 10`	(Optional) Limits the number of simultaneous logins for users in a specific server group.

	Command or Action	Purpose
Step 6	**max-users** *number-of-users* **Example:** `Device(config)# max-users 1000`	(Optional) Limits the number of connections to a specific server group.
Step 7	**exit** **Example:** `Device(config)# exit`	Exits global configuration mode and returns to privileged EXEC mode.

Verifying a VPN Session

SUMMARY STEPS

1. **enable**
2. **show crypto session group**
3. **show crypto session summary**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**show crypto session group** **Example:** `Device# show crypto session group`	Displays groups that are currently active on the VPN device.
Step 3	**show crypto session summary** **Example:** `Device# show crypto session summary`	Displays groups that are currently active on the VPN device and the users that are connected for each of those groups.

Applying Mode Configuration and Xauth

Mode Configuration and Xauth must be applied to a crypto map to be enforced. To apply Mode Configuration and Xauth to a crypto map, perform the following steps.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **crypto map** *tag* **client configuration address** [**initiate** | **respond**]
4. **crypto map** *map-name* **isakmp authorization list** *list-name*
5. **crypto map** *map-name* **client authentication list** *list-name*
6. **exit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**crypto map** *tag* **client configuration address** [**initiate**	**respond**] **Example:** `Device(config)# crypto map dyn client configuration address initiate`	Configures the device to initiate or reply to Mode Configuration requests. **Note** Cisco clients require the **respond** keyword to be used; however, if the Cisco Secure VPN Client 1.x is used, the **initiate** keyword must be used; the **initiate** and **respond** keywords may be used.
Step 4	**crypto map** *map-name* **isakmp authorization list** *list-name* **Example:** `Device(config)# crypto map ikessaaamap isakmp authorization list ikessaaalist`	Enables IKE querying for group policy when requested by the client. • The *list-name* argument is used by AAA to determine which storage source is used to find the policy (local or RADIUS) as defined in the **aaa authorization network** command.
Step 5	**crypto map** *map-name* **client authentication list** *list-name* **Example:** `Device(config)# crypto map xauthmap client authentication list xauthlist`	Enforces Xauth. • The *list-name* argument is used to determine the appropriate username and password storage location (local or RADIUS) as defined in the **aaa authentication login** command.

	Command or Action	Purpose
Step 6	**exit** **Example:** `Device(config)# exit`	Exits global configuration mode and returns to privileged EXEC mode.

Enabling Reverse Route Injection (RRI) for the Client

To enable RRI on the crypto map (static or dynamic) for VPN client support, perform the following steps.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. Do one of the following:
   - **crypto dynamic** *map-name seq-num*
   - **crypto map** *map-name seq-num* **ipsec-isakmp**
4. **set peer** *ip-address*
5. **set transform-set** *transform-set-name*
6. **reverse-route**
7. **match address**
8. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	Do one of the following: • **crypto dynamic** *map-name seq-num* • **crypto map** *map-name seq-num* **ipsec-isakmp**	Creates a dynamic crypto map entry and enters crypto map configuration mode. or

	Command or Action	Purpose

	Example:
	`Device(config)# crypto dynamic mymap 10`
	
	Example:
	`Device(config)# crypto map yourmap 15 ipsec-isakmp`
		Adds a dynamic crypto map set to a static crypto map set and enters crypto map configuration mode.

Step 4	**set peer** *ip-address* **Example:** `Device(config-crypto-map)# set peer 10.20.20.20`	Specifies an IPsec peer IP address in a crypto map entry. • This step is optional when configuring dynamic crypto map entries.
Step 5	**set transform-set** *transform-set-name* **Example:** `Device(config-crypto-map)# set transform-set dessha`	Specifies which transform sets are allowed for the crypto map entry. • Lists multiple transform sets in the order of priority (highest priority first). **Note** This list is the only configuration statement required in dynamic crypto map entries.
Step 6	**reverse-route** **Example:** `Device(config-crypto-map)# reverse-route`	Creates source proxy information.
Step 7	**match address** **Example:** `Device(config-crypto-map)# match address`	Specifies an extended access list for a crypto map entry. • This step is optional when configuring dynamic crypto map entries.
Step 8	**end** **Example:** `Device(config-crypto-map)# end`	Exits crypto map configuration mode and returns to privileged EXEC mode.

Enabling IKE Dead Peer Detection

To enable a Cisco IOS VPN gateway (instead of the client) to send IKE DPD messages, perform the following steps.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **crypto isakmp keepalive** *seconds retries*
4. **exit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**crypto isakmp keepalive** *seconds retries* **Example:** `Device(config)# crypto isakmp keepalive 20 10`	Allows the gateway to send DPD messages to the device. • The *seconds* argument specifies the number of seconds between DPD messages (the range is from 1 to 3600). • The *retries* argument specifies the number of seconds between retries if DPD messages fail (the range is from 2 to 60).
Step 4	**exit** **Example:** `Device(config)# exit`	Exits global configuration mode and returns to privileged EXEC mode.

Configuring RADIUS Server Support

To configure access to the RADIUS server and allow the Cisco IOS VPN device to send requests to the server, perform the following steps.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **radius server host** *ip-address* [**auth-port** *port-number*] [**acct-port** *port-number*] [**key** *string*]
4. **exit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**radius server host** *ip-address* [**auth-port** *port-number*] [**acct-port** *port-number*] [**key** *string*] **Example:** `Device(config)# radius server host 192.168.1.1. auth-port 1645 acct-port 1646 key XXXX`	Specifies a RADIUS server host. **Note** This step is required if you choose to store group policy information in a RADIUS server.
Step 4	**exit** **Example:** `Device(config)# exit`	Exits global configuration mode and returns to privileged EXEC mode.

Verifying Easy VPN Server

To verify your configurations for this feature, perform the following steps.

SUMMARY STEPS

1. **enable**
2. **show crypto map** [**interface** *interface* | **tag** *map-name*]

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.

	Command or Action	Purpose
Step 2	**show crypto map** [**interface** *interface* | **tag** *map-name*] **Example:** `Device# show crypto map interface ethernet 0`	Displays the crypto map configuration.

Configuring a Banner

To configure an Easy VPN server to push a banner to an Easy VPN remote device, perform the following steps.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **crypto isakmp client configuration group** *group-name*
4. **banner c** *banner-text* **c**
5. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**crypto isakmp client configuration group** *group-name* **Example:** `Device(config)# crypto isakmp client configuration group Group1`	Specifies to which group a policy profile will be defined and enters ISAKMP group configuration mode.
Step 4	**banner c** *banner-text* **c** **Example:** `Device(config-isakmp-group)# banner c The quick brown fox jumped over the lazy dog c`	Specifies the text of the banner.

	Command or Action	Purpose
Step 5	**end** **Example:** `Device(config-isakmp-group)# end`	Exits ISAKMP group configuration mode and returns to privileged EXEC mode.

Configuring Auto Upgrade

To configure an Easy VPN server to provide an automated mechanism to make software and firmware upgrades automatically available to an Easy VPN remote device, perform the following steps.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **crypto isakmp client configuration group** *group-name*
4. **auto-update client** *type-of-system* **url** *url* **rev** *review-version*
5. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**crypto isakmp client configuration group** *group-name* **Example:** `Device(config)# crypto isakmp client configuration group Group2`	Specifies to which group a policy profile will be defined and enters ISAKMP group configuration mode.
Step 4	**auto-update client** *type-of-system* **url** *url* **rev** *review-version* **Example:** `Device(config-isakmp-group)# auto-update client Win2000 url http:www.example.com/newclient rev 3.0.1(Rel), 3.1(Rel)`	Configures autoupdate parameters for an Easy VPN remote device.

	Command or Action	Purpose
Step 5	**end** **Example:** `Device(config-isakmp-group)# end`	Exits ISAKMP group configuration mode and returns to privileged EXEC mode.

Configuring Browser Proxy

To configure an EasyVPN server so that the Easy VPN remote device can access resources on the corporate network when using Cisco IOS VPN Client software, perform the following steps. With this configuration, the user does not have to manually modify the proxy settings of the web browser when connecting and does not have to manually revert the proxy settings when disconnecting.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **crypto isakmp client configuration browser-proxy** *browser-proxy-name*
4. **proxy** *proxy-parameter*
5. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**crypto isakmp client configuration browser-proxy** *browser-proxy-name* **Example:** `Device(config)# crypto isakmp client configuration browser-proxy bproxy`	Configures browser-proxy parameters for an Easy VPN remote device and enters ISAKMP browser proxy configuration mode.

	Command or Action	Purpose
Step 4	**proxy** *proxy-parameter* **Example:** `Device(config-ikmp-browser-proxy)# proxy auto-detect`	Configures proxy parameters for an Easy VPN remote device.
Step 5	**end** **Example:** `Device(config-ikmp-browser-proxy)# end`	Exits ISAKMP browser proxy configuration mode and returns to privileged EXEC mode.

Configuring the Pushing of a Configuration URL Through a Mode-Configuration Exchange

To configure an Easy VPN server to push a configuration URL through a Mode-Configuration exchange, perform the following steps.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **crypto isakmp client configuration group** *group-name*
4. **configuration url** *url*
5. **configuration version** *version-number*
6. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.

	Command or Action	Purpose
Step 3	**crypto isakmp client configuration group** *group-name* **Example:** `Device(config)# crypto isakmp client configuration group Group1`	Specifies to which group a policy profile will be defined and enters ISAKMP group configuration mode.
Step 4	**configuration url** *url* **Example:** `Device(config-isakmp-group)# configuration url http://10.10.88.8/easy.cfg`	Specifies the URL the remote device must use to get the configuration from the server. • The URL must be a non-NULL-terminated ASCII string that specifies the complete path of the configuration file.
Step 5	**configuration version** *version-number* **Example:** `Device(config-isakmp-group)# configuration version 10`	Specifies the version of the configuration. • The version number will be an unsigned integer in the range 1 through 32767.
Step 6	**end** **Example:** `Device(config-isakmp-group)# end`	Exits ISAKMP group configuration mode and returns to privileged EXEC mode.

Configuring Per-User AAA Download with PKI—Configuring the Crypto PKI Trustpoint

To configure a AAA server to push user attributes to a remote device, perform the following steps.

Before You Begin

Before configuring a AAA server to push user attributes to a remote device, you must have configured AAA. The crypto Public Key Infrastructure (PKI) trustpoint must also be configured. Preferably the trustpoint configuration should contain the **authorization username** command.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **crypto pki trustpoint** *name*
4. **enrollment url** *url*
5. **revocation-check none**
6. **rsakeypair** *key-label*
7. **authorization username subjectname** *subjectname*
8. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**crypto pki trustpoint** *name* **Example:** `Device(config)# crypto pki trustpoint ca-server`	Declares the trustpoint that your device should use and enters CA-trustpoint configuration mode.
Step 4	**enrollment url** *url* **Example:** `Device(config-ca-trustpoint)# enrollment url http://10.7.7.2:80`	Specifies the URL of the certification authority (CA) server to which to send enrollment requests.
Step 5	**revocation-check none** **Example:** `Device(config-ca-trustpoint)# revocation-check none`	Checks the revocation status of a certificate.
Step 6	**rsakeypair** *key-label* **Example:** `Device(config-ca-trustpoint)# rsakeypair rsa-pair`	Specifies which key pair to associate with the certificate.

	Command or Action	Purpose
Step 7	**authorization username subjectname** *subjectname* **Example:** `Device(config-ca-trustpoint)# authorization username subjectname commonname`	Specifies the parameters for the different certificate fields that are used to build the AAA username.
Step 8	**end** **Example:** `Device(config-ca-trustpoint)# end`	Exits CA-trustpoint configuration mode and returns to privileged EXEC mode.

Configuring the Actual Per-User AAA Download with PKI

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **crypto isakmp policy** *priority*
4. **group** {**1** | **2** }
5. **exit**
6. **crypto isakmp profile** *profile-name*
7. **match certificate** *certificate-map*
8. **client pki authorization list** *listname*
9. **client configuration address** {**initiate** | **respond**}
10. **virtual-template** *template-number*
11. **exit**
12. **crypto ipsec transform-set** *transform-set-name transform1* [*transform2*] [*transform3*] [*transform4*]
13. **crypto ipsec profile** *name*
14. **set transform-set** *transform-set-name*
15. **exit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.

	Command or Action	Purpose
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**crypto isakmp policy** *priority* **Example:** `Device(config)# crypto isakmp policy 10`	Defines an IKE policy and enters ISAKMP policy configuration mode.
Step 4	**group** {**1** | **2** } **Example:** `Device(config-isakmp-policy)# group 2`	Specifies the Diffie-Hellman group identifier within an IKE policy.
Step 5	**exit** **Example:** `Device(config-isakmp-policy)# exit`	Exits ISAKMP policy configuration mode.
Step 6	**crypto isakmp profile** *profile-name* **Example:** `Device(config)# crypto isakmp profile ISA-PROF`	Defines an ISAKMP profile, audits IPsec user sessions, and enters ISAKMP profile configuration mode.
Step 7	**match certificate** *certificate-map* **Example:** `Device(config-isakmp-profile)# match certificate cert_map`	Assigns an ISAKMP profile to a peer on the basis of the contents of arbitrary fields in the certificate.
Step 8	**client pki authorization list** *listname* **Example:** `Device(config-isakmp-profile)# client pki authorization list usrgrp`	Specifies the authorization list of AAA servers that will be used for obtaining per-user AAA attributes on the basis of the username constructed from the certificate.
Step 9	**client configuration address** {**initiate** | **respond**} **Example:** `Device(config-isakmp-profile)# client configuration address respond`	Configures IKE configuration mode in the ISAKMP profile.
Step 10	**virtual-template** *template-number* **Example:** `Device(config-isakmp-profile)# virtual-template 2`	Specifies the virtual template to clone virtual access interfaces.

	Command or Action	Purpose
Step 11	**exit** **Example:** `Device(config-isakmp-profile)# exit`	Exits ISAKMP profile configuration mode.
Step 12	**crypto ipsec transform-set** *transform-set-name transform1* [*transform2*] [*transform3*] [*transform4*] **Example:** `Device(config)# crypto ipsec transform-set trans2 esp-aes esp-sha-hmac1`	Defines a transform set—an acceptable combination of security protocols and algorithms.
Step 13	**crypto ipsec profile** *name* **Example:** `Device(config)# crypto ipsec profile IPSEC_PROF`	Defines the IPsec parameters that are to be used for IPsec encryption between two IPsec devices.
Step 14	**set transform-set** *transform-set-name* **Example:** `Device(config)# set transform-set trans2`	Specifies the transform sets to be used with the crypto map entry.
Step 15	**exit** **Example:** `Device(config)# exit`	Exits global configuration mode and returns to privileged EXEC mode.

Configuring Per-User Attributes on a Local Easy VPN AAA Server

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **aaa attribute list** *list-name*
4. **attribute type** *name value* [**service** *service*] [**protocol** *protocol*]
5. **exit**
6. **crypto isakmp client configuration group** *group-name*
7. **crypto aaa attribute list** *list-name*
8. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**aaa attribute list** *list-name* **Example:** `Device(config)# aaa attribute list list1`	Defines a AAA attribute list locally on a device and enters attribute list configuration mode.
Step 4	**attribute type** *name value* [**service** *service*] [**protocol** *protocol*] **Example:** `Device(config-attr-list)# attribute type attribute xxxx service ike protocol ip`	Defines an attribute type that is to be added to an attribute list locally on a device.
Step 5	**exit** **Example:** `Device(config-attr-list)# exit`	Exits attribute list configuration mode.
Step 6	**crypto isakmp client configuration group** *group-name* **Example:** `Device(config)# crypto isakmp client configuration group group1`	Specifies the group to which a policy profile will be defined and enters ISAKMP group configuration mode.
Step 7	**crypto aaa attribute list** *list-name* **Example:** `Device(config-isakmp-group)# crypto aaa attribute list listname1`	Defines a AAA attribute list locally on a device.
Step 8	**end** **Example:** `Device(config-isakmp-group)# end`	Exits ISAKMP group configuration mode and returns to privileged EXEC mode.

Enabling Easy VPN Syslog Messages

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **crypto logging ezvpn** [*group group-name*]
4. **exit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**crypto logging ezvpn** [*group group-name*] **Example:** `Device(config)# crypto logging ezvpn group group1`	Enables Easy VPN syslog messages on a server. • The **group** keyword and *group-name* argument are optional. If a group name is not provided, syslog messages are enabled for all Easy VPN connections to the server. If a group name is provided, syslog messages are enabled for that particular group only.
Step 4	**exit** **Example:** `Device(config)# exit`	Exits global configuration mode and returns to privileged EXEC mode.

Defining a CPP Firewall Policy Push Using a Local AAA Server

To define a CPP firewall policy push on a server to allow or deny a tunnel on the basis of whether a remote device has a required firewall for a local AAA server, perform the following steps.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **crypto isakmp client firewall** *policy-name* **required** | **optional** *firewall-type*
4. **policy** {**check-presence** | **central-policy-push access-list** {**in** | **out**} {*access-list-name* | *access-list-number*}}
5. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**crypto isakmp client firewall** *policy-name* **required**	**optional** *firewall-type* **Example:** `Device(config)# crypto isakmp client firewall hw-client-g-cpp required Cisco-Security-Agent`	Defines the CPP firewall push policy on a server and enters ISAKMP client firewall configuration mode. • *policy-name*—Uniquely identifies a policy. A policy name can be associated with the Easy VPN client group configuration of the server (local group configuration) or on the AAA server. • **required**—Policy is mandatory. If the CPP policy is defined as mandatory and is included in the Easy VPN server configuration, the tunnel setup is allowed only if the client confirms this policy. Otherwise, the tunnel is terminated. • **optional**—Policy is optional. If the CPP policy is defined as optional, and is included in the Easy VPN server configuration, the tunnel setup is continued even if the client does not confirm the defined policy. • *firewall-type*—Type of firewall (see the **crypto isakmp client firewall** command for a list of firewall types).
Step 4	**policy** {**check-presence** | **central-policy-push access-list** {**in** | **out**} {*access-list-name* | *access-list-number*}} **Example:** `Device(config-isakmp-client-fw)# policy central-policy-push access-list out acl1`	Defines the CPP firewall policy push. • **check-presence**—Denotes that the server should check for the presence of the specified firewall as shown by the value of the *firewall-type* argument on the client. • **central-policy-push**—The configuration following this keyword specifies the actual policy, such as the input and output access lists that have to be applied by the client firewall, which is of the type specified by the value of the *firewall-type* argument.

	Command or Action	Purpose
		• **access-list** {**in** | **out**}—Defines the inbound and outbound access lists. • *access-list-name* | *access-list-number*--Name or number of the access list.
Step 5	**end** **Example:** `Device(config-isakmp-client-fw)# end`	Exits ISAKMP client firewall configuration mode and returns to privileged EXEC mode.

What to Do Next

Apply the CPP firewall policy push to the configured group.

Applying a CPP Firewall Policy Push to the Configuration Group

After the CPP firewall policy push is defined, it must be applied to the configuration group.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **crypto isakmp client configuration group** *group-name*
4. **firewall policy** *policy-name*
5. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.

	Command or Action	Purpose
Step 3	**crypto isakmp client configuration group** *group-name* **Example:** `Device(config)# crypto isakmp client configuration group hw-client-g`	Specifies to which group a policy profile will be defined and enters ISAKMP group configuration mode.
Step 4	**firewall policy** *policy-name* **Example:** `Device(config-isakmp-group)# firewall policy hw-client-g-cpp`	Specifies the CPP firewall push policy name for the crypto ISAKMP client configuration group on a local authentication AAA server.
Step 5	**end** **Example:** `Device(config-isakmp-group)# end`	Exits ISAKMP group configuration mode and returns to privileged EXEC mode.

Defining a CPP Firewall Policy Push Using a Remote AAA Server

The steps to define a CPP firewall policy push using a remote AAA server is similar to defining a CPP firewall policy push using a local AAA server. See the section Defining a CPP Firewall Policy Push Using a Local AAA Server.

What to Do Next

After defining the CPP firewall policy push, you should add the Vendor Specific Attributes (VSA) CPP policy under the group definition.

Adding the VSA CPP-Policy Under the Group Definition

To add the Vendor-Specific Attributes (VSA) CPP policy under the group definition that is defined in RADIUS, perform the following step.

SUMMARY STEPS

1. Add the VSA “cpp-policy” under the group definition that is defined in RADIUS.

DETAILED STEPS

	Command or Action	Purpose
Step 1	Add the VSA “cpp-policy” under the group definition that is defined in RADIUS. **Example:** `ipsec:cpp-policy=“Enterprise Firewall”`	Defines the CPP firewall push policy for a remote server.

Verifying CPP Firewall Policy Push

SUMMARY STEPS

1. **enable**
2. **debug crypto isakmp**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**debug crypto isakmp** **Example:** `Device# debug crypto isakmp`	Displays messages about IKE events.

Configuring Password Aging

To configure the Password Aging feature so that the Easy VPN client is notified if the password has expired, perform the following steps.

Note The following restrictions apply to the Password Aging feature:

- It works only with VPN software clients. It does not work with VPN client hardware.
- It works only with RADIUS servers.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **aaa new-model**
4. **aaa authentication login** *list-name* **password-expiry** *method1* [*method2...*]
5. **radius-server host** *ip-address* **auth-port** *port-number* **acct-port** *port-number* **key** *string*
6. **crypto isakmp profile** *profile-name*
7. **client authentication list** *list-name*
8. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**aaa new-model** **Example:** `Device(config)# aaa new-model`	Enables AAA.
Step 4	**aaa authentication login** *list-name* **password-expiry** *method1* [*method2...*] **Example:** `Device(config)# aaa authentication login userauth password-expiry group radius`	Configures the authentication list so that the Password Aging feature is enabled.
Step 5	**radius-server host** *ip-address* **auth-port** *port-number* **acct-port** *port-number* **key** *string*	Configures the RADIUS server.

	Command or Action	Purpose
	Example: `Device(config)# radius-server host 172.19.217.96 255.255.255.0 auth-port 1645 acct-port 1646 key cisco radius-server vsa send authentication`	
Step 6	**crypto isakmp profile** *profile-name* **Example:** `Device(config)# crypto isakmp profile ISA-PROF`	Defines an ISAKMP profile and enters ISAKMP profile configuration mode.
Step 7	**client authentication list** *list-name* **Example:** `Device(config-isakmp-profile)# client authentication list userauth`	Configures IKE extended authentication (Xauth) in an ISAKMP profile and includes the authentication list defined in Step 4.
Step 8	**end** **Example:** `Device(config-isakmp-profile)# end`	Exits ISAKMP profile configuration mode and returns to privileged EXEC mode.

Configuring Split DNS

Before You Begin

Before the Split DNS feature can work, the following commands must be configured on the Easy VPN remote:

- **ip dns server**
- **ip domain-lookup**

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **crypto isakmp client configuration group** {*group-name* | **default**}
4. **dns** *primary-server secondary-server*
5. **split-dns** *domain-name*
6. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**crypto isakmp client configuration group** {*group-name* | **default**} **Example:** `Device(config)# crypto isakmp client configuration group group1`	Specifies the policy profile of the group that will be defined and enters ISAKMP group configuration mode. • If no specific group matches and a default group is defined, users will automatically be given the policy of a default group.
Step 4	**dns** *primary-server secondary-server* **Example:** `Device(config-isakmp-group)# dns 10.2.2.2 10.3.3.3`	Specifies the primary and secondary DNS servers for the group.
Step 5	**split-dns** *domain-name* **Example:** `Device(config-isakmp-group)# split-dns example.com`	Specifies a domain name that must be tunneled or resolved to the private network.
Step 6	**end** **Example:** `Device(config-isakmp-group)# end`	Exits ISAKMP group configuration mode and returns to privileged EXEC mode.

Verifying Split DNS

To verify a split DNS configuration, perform the following steps (the **show** commands can be used one at a time or together).

SUMMARY STEPS

1. **enable**
2. **show ip dns name-list** [*name-list-number*]
3. **show ip dns view** [**vrf** *vrf-name*] [**default** | *view-name*]
4. **show ip dns view-list** [*view-list-name*]

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**show ip dns name-list** [*name-list-number*] **Example:** `Device# show ip dns name-list 1`	Displays information about DNS name lists.
Step 3	**show ip dns view** [**vrf** *vrf-name*] [**default**	*view-name*] **Example:** `Device# show ip dns view default`	Displays information about DNS views.
Step 4	**show ip dns view-list** [*view-list-name*] **Example:** `Device# show ip dns view-list ezvpn-internal-viewlist`	Displays information about DNS view lists.

Monitoring and Maintaining Split DNS

SUMMARY STEPS

1. **enable**
2. **debug ip dns name-list**
3. **debug ip dns view**
4. **debug ip dns view-list**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**debug ip dns name-list** **Example:** `Device# debug ip dns name-list`	Enables debugging output for Domain Name System (DNS) name-list events.
Step 3	**debug ip dns view** **Example:** `Device# debug ip dns view`	Enables debugging output for DNS view events.
Step 4	**debug ip dns view-list** **Example:** `Device# debug ip dns view-list`	Enables debugging output for DNS view-list events.

Configuring an Easy VPN Server to Obtain an IP Address from a DHCP Server

The Easy VPN server selects the method for address assignment in the following order of precedence:

1. Selects the Framed IP address
2. Uses the IP address from the authentication server (group/user)
3. Uses the global IKE address pools
4. Uses DHCP

Note To enable the Easy VPN server to obtain an IP address from a DHCP server, remove other address assignments.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **crypto isakmp client configuration group** *group-name*
4. **dhcp server** {*ip-address* | *hostname*}
5. **dhcp timeout** *seconds*
6. **dhcp giaddr** *scope*
7. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**crypto isakmp client configuration group** *group-name* **Example:** `Device(config)# crypto isakmp client configuration group group1`	Specifies to which group a policy profile will be defined and enters ISAKMP group configuration mode where you specify characteristics for the group policy.
Step 4	**dhcp server** {*ip-address* | *hostname*} **Example:** `Device(config-isakmp-group)# dhcp server 10.10.1.2`	Specifies a primary (and backup) DHCP server to allocate IP addresses to users entering a particular public data network (PDN) access point.
Step 5	**dhcp timeout** *seconds* **Example:** `Device(config-isakmp-group)# dhcp timeout 6`	Sets the wait time in seconds before the next DHCP server on the list is tried.
Step 6	**dhcp giaddr** *scope* **Example:** `Device(config-isakmp-group)# dhcp giaddr 10.1.1.4`	Specifies the gigabit address for the DHCP scope.

	Command or Action	Purpose
Step 7	**end** **Example:** `Device(config-isakmp-group)# end`	Exits ISAKMP group configuration mode and returns to privileged EXEC mode.

Verifying DHCP Client Proxy

To verify your DHCP client proxy configuration, perform the following steps (use the **show** commands one at a time or together).

SUMMARY STEPS

1. **enable**
2. **show dhcp lease**
3. **show ip dhcp pool**
4. **show ip dhcp binding**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**show dhcp lease** **Example:** `Device# show dhcp lease`	Displays information about the DHCP address pools. **Note** Use this command when an external DHCP is used.
Step 3	**show ip dhcp pool** **Example:** `Device# show ip dhcp pool`	Displays information about the DHCP address pools. **Note** This command is applicable only when the Easy VPN server is also the DHCP server (generally not the case because the DHCP server usually is an external server).
Step 4	**show ip dhcp binding** **Example:** `Device# show ip dhcp binding`	Displays address bindings on the DHCP server. **Note** This command is applicable only when the Easy VPN server is also the DHCP server (generally not the case because the DHCP server usually is an external server).

Monitoring and Maintaining DHCP Client Proxy

To monitor and maintain your DHCP client proxy configuration, perform the following steps (use the **debug** commands one at a time or together).

SUMMARY STEPS

1. **enable**
2. **debug crypto isakmp**
3. **debug dhcp**
4. **debug dhcp detail**
5. **debug ip dhcp server events**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**debug crypto isakmp** **Example:** `Device# debug crypto isakmp`	Displays messages about Internet Key Exchange (IKE) events.
Step 3	**debug dhcp** **Example:** `Device# debug dhcp`	Reports server events such as address assignments and database updates.
Step 4	**debug dhcp detail** **Example:** `Device# debug dhcp detail`	Displays detailed DHCP debugging information.
Step 5	**debug ip dhcp server events** **Example:** `Device# debug ip dhcp server events`	Reports server events such as address assignments and database updates. **Note** This command is applicable only when the Easy VPN server is also the DHCP server (generally not the case because the DHCP server usually is an external server).

Configuring Cisco Tunneling Control Protocol

Before You Begin

Before configuring Cisco Tunneling Control Protocol, ensure that crypto IPsec is configured.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **crypto ctcp port** [*port-number*]
4. **exit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**crypto ctcp port** [*port-number*] **Example:** `Device(config)# crypto ctcp port 120`	Configures Cisco Tunneling Control Protocol encapsulation for Easy VPN. • Up to ten port numbers can be configured. • If the *port-number* argument is not configured, Cisco Tunneling Control Protocol is enabled on port 80 by default.
Step 4	**exit** **Example:** `Device(config)# exit`	Exits global configuration mode and returns to privileged EXEC mode.

Verifying Cisco Tunneling Control Protocol

To verify your Cisco Tunneling Control Protocol configuration, perform the following steps.

SUMMARY STEPS

1. **enable**
2. **show crypto ctcp** [**peer**]

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**show crypto ctcp** [**peer**] **Example:** `Device# show crypto ctcp peer`	Displays information about a specific Cisco Tunneling Control Protocol peer.

Monitoring and Maintaining a Cisco Tunneling Control Protocol Configuration

To monitor and maintain your Cisco Tunneling Control Protocol configuration, perform the following steps.

SUMMARY STEPS

1. **enable**
2. **debug crypto ctcp**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**debug crypto ctcp** **Example:** `Device# debug crypto ctcp`	Displays information about a Cisco Tunneling Control Protocol session.

Clearing a Cisco Tunneling Control Protocol Configuration

To clear a Cisco Tunneling Control Protocol configuration, perform the following steps.

SUMMARY STEPS

1. **enable**
2. **clear crypto ctcp** [**peer** *ip-address*]

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**clear crypto ctcp** [**peer** *ip-address*] **Example:** `Device# clear crypto ctcp peer 10.76.23.21`	Displays information about a Cisco Tunneling Control Protocol session.

Troubleshooting a Cisco Tunneling Control Protocol Configuration

To troubleshoot a Cisco Tunneling Control Protocol configuration, perform the following steps.

SUMMARY STEPS

1. To ensure that the Cisco Tunneling Control Protocol session is in the CTCP_ACK_RECEIVED state, use the **show crypto ctcp** command.
2. If the Cisco Tunneling Control Protocol session is not in the CTCP_ACK_RECEIVED state, enable the **debug crypto ctcp** command and then try using the **show crypto ctcp** command again.
3. If no Cisco Tunneling Control Protocol bugs are seen, ensure that the firewall is allowing the Cisco Tunneling Control Protocol packets to get to the server (check the firewall configuration).
4. If the firewall configuration is correct, debugging is enabled, and you do not see any Cisco Tunneling Control Protocol debugs on your console, you must find out why the Cisco Tunneling Control Protocol port on the device is not receiving packets. If you do not see any Cisco Tunneling Control Protocol debugs and a Cisco Tunneling Control Protocol session has not been set up, Cisco Tunneling Control Protocol packets that are actually TCP packets could have been delivered to a TCP stack instead of to the Cisco Tunneling Control Protocol port. By enabling the **debug ip packet** and **debug ip tcp packet** commands, you may be able to determine whether the packet is being given to the TCP stack.

DETAILED STEPS

Step 1 To ensure that the Cisco Tunneling Control Protocol session is in the CTCP_ACK_RECEIVED state, use the **show crypto ctcp** command.

Step 2 If the Cisco Tunneling Control Protocol session is not in the CTCP_ACK_RECEIVED state, enable the **debug crypto ctcp** command and then try using the **show crypto ctcp** command again.

Step 3 If no Cisco Tunneling Control Protocol bugs are seen, ensure that the firewall is allowing the Cisco Tunneling Control Protocol packets to get to the server (check the firewall configuration).

Step 4 If the firewall configuration is correct, debugging is enabled, and you do not see any Cisco Tunneling Control Protocol debugs on your console, you must find out why the Cisco Tunneling Control Protocol port on the device is not receiving packets. If you do not see any Cisco Tunneling Control Protocol debugs and a Cisco Tunneling Control Protocol session has not been set up, Cisco Tunneling Control Protocol packets that are actually TCP packets could have been delivered to a TCP stack instead of to the Cisco Tunneling Control Protocol port. By enabling the **debug ip packet** and **debug ip tcp packet** commands, you may be able to determine whether the packet is being given to the TCP stack.

Configuration Examples for Easy VPN Server

Example: Configuring Cisco IOS Software for Easy VPN Server

The following example shows how to define group policy information locally for mode configuration. In this example, a group name is named “cisco” and another group name is named “default.” The policy is enforced for all users who do not offer a group name that matches “cisco.”

```
! Enable policy look-up via AAA. For authentication and authorization, send requests to
! RADIUS first, then try local policy.
aaa new-model
aaa authentication login userlist group radius local
aaa authorization network grouplist group radius local
enable password XXXX
!
username cisco password 0 cisco
clock timezone PST -8
ip subnet-zero
! Configure IKE policies, which are assessed in order so that the first policy that
matches the proposal of the client will be used.
crypto isakmp policy 1
 group 2
!
crypto isakmp policy 3
 hash md5
 authentication pre-share
 group 2
crypto isakmp identity hostname
!
! Define “cisco” group policy information for mode config push.
crypto isakmp client configuration group cisco
 key cisco
 dns 10.2.2.2 10.2.2.3
 wins 10.6.6.6
 domain cisco.com
 pool pool1
 acl 199
```

```
! Define default group policy for mode config push.
crypto isakmp client configuration group default
 key cisco
 dns 10.2.2.2 10.3.2.3
 pool pool1
 acl 199
!
!
crypto ipsec transform-set dessha esp-des esp-sha-hmac
!
crypto dynamic-map mode 1
 set transform-set dessha
!
! Apply mode config and xauth to crypto map “mode.” The list names that are defined here
! must match the list names that are defined in the AAA section of the config.
crypto map mode client authentication list userlist
crypto map mode isakmp authorization list grouplist
crypto map mode client configuration address respond
crypto map mode 1 ipsec-isakmp dynamic mode
!
!
controller ISA 1/1
!
!
interface FastEthernet0/0
 ip address 10.6.1.8 255.255.0.0
 ip route-cache
 ip mroute-cache
 duplex auto
 speed auto
 crypto map mode
!
interface FastEthernet0/1
 ip address 192.168.1.28 255.255.255.0
 no ip route-cache
 no ip mroute-cache
 duplex auto
 speed auto
! Specify IP address pools for internal IP address allocation to clients.
ip local pool pool1 192.168.2.1 192.168.2.10
ip classless
ip route 0.0.0.0 0.0.0.0 10.6.0.1
!
! Define access lists for each subnet that should be protected.
access-list 199 permit ip 192.168.1.0 0.0.0.255 any
access-list 199 permit ip 192.168.3.0 0.0.0.255 any
!
! Specify a RADIUS server host and configure access to the server.
radius-server host 192.168.1.1 auth-port 1645 acct-port 1646 key XXXXX
radius-server retransmit 3
!
!
line con 0
 exec-timeout 0 0
 length 25
 transport input none
line aux 0
line vty 5 15
!
```

Example: RADIUS Group Profile with IPsec AV Pairs

The following is an example of a standard RADIUS group profile that includes RADIUS IPsec AV pairs. To get the group authorization attributes, “cisco” must be used as the password.

```
client_r Password = "cisco"
 Service-Type = Outbound
```

```
 cisco-avpair = "ipsec:tunnel-type*ESP"
 cisco-avpair = "ipsec:key-exchange=ike"
 cisco-avpair = "ipsec:tunnel-password=lab"
 cisco-avpair = "ipsec:addr-pool=pool1"
 cisco-avpair = "ipsec:default-domain=cisco"
 cisco-avpair = "ipsec:inacl=101"
 cisco-avpair = "ipsec:access-restrict=fastethernet 0/0"
 cisco-avpair = "ipsec:group-lock=1"
 cisco-avpair = "ipsec:dns-servers=10.1.1.1 10.2.2.2"
 cisco-avpair = "ipsec:firewall=1"
 cisco-avpair = "ipsec:include-local-lan=1"
 cisco-avpair = "ipsec:save-password=1"
 cisco-avpair = "ipsec:wins-servers=10.3.3.3 10.4.4.4"
 cisco-avpair = "ipsec:split-dns=example.com"
 cisco-avpair = "ipsec:ipsec-backup-gateway=10.1.1.1"
 cisco-avpair = "ipsec:ipsec-backup-gateway=10.1.1.2"
 cisco-avpair = "ipsec:pfs=1"
 cisco-avpair = "ipsec:cpp-policy="Enterprise Firewall"
 cisco-avpair = “ipsec:auto-update=”Win http://www.example.com 4.0.1”
 cisco-avpair = “ipsec:browser-proxy=bproxy_profile_A”
 cisco-avpair = "ipsec:banner=Xauth banner text here"
```

The following is an example of a RADIUS user profile that is set up for a group that has group-lock configured. The username is entered in the same format as the user@domain format.

```
abc@example.com Password = "abcll1111"
cisco-avpair = "ipsec:user-include-local-lan=1"
cisco-avpair = "ipsec:user-save-password=1"
Framed-IP-Address = 10.10.10.10
```

Example: RADIUS User Profile with IPsec AV Pairs

The following is an example of a standard RADIUS user profile that includes RADIUS IPsec AV pairs. These user attributes will be obtained during Xauth.

```
ualluall Password = "uall1234"
        cisco-avpair = "ipsec:user-vpn-group=unity"
        cisco-avpair = "ipsec:user-include-local-lan=1"
        cisco-avpair = "ipsec:user-save-password=1"
        Framed-IP-Address = 10.10.10.10
```

Example: Backup Gateway with Maximum Logins and Maximum Users

The following example shows that five backup gateways have been configured, that the maximum number of users has been set to 250, and that the maximum number of logins has been set to 2:

```
crypto isakmp client configuration group sdm
 key 6 RMZPPMRQMSdiZNJg`EBbCWTKSTi\d[
 pool POOL1
 acl 150
 backup-gateway 172.16.12.12
 backup-gateway 172.16.12.13
 backup-gateway 172.16.12.14
 backup-gateway 172.16.12.130
 backup-gateway 172.16.12.131
 max-users 250
 max-logins 2
```

Example: Easy VPN with an IPsec Virtual Tunnel Interface

The following output shows that Easy VPN has been configured with an IPsec virtual tunnel interface.

```
!
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname Router
!
boot-start-marker
boot-end-marker
!
!
aaa new-model
!
!
aaa authentication login default local
aaa authorization network default local
!
aaa session-id common
!
resource policy
!
clock timezone IST 0
ip subnet-zero
ip cef
no ip domain lookup
no ip dhcp use vrf connected
!
username lab password 0 lab
!
crypto isakmp policy 3
 authentication pre-share
 group 2
crypto isakmp xauth timeout 90
!
crypto isakmp client configuration group easy
 key cisco
 domain foo.com
 pool dpool
 acl 101
crypto isakmp profile vi
   match identity group easy
   isakmp authorization list default
   client configuration address respond
   client configuration group easy
   virtual-template 1
!
!
crypto ipsec transform-set set esp-3des esp-sha-hmac
!
crypto ipsec profile vi
 set transform-set set
 set isakmp-profile vi
!
!
interface Loopback0
 ip address 10.4.0.1 255.255.255.0
!
interface Ethernet0/0
 ip address 10.3.0.2 255.255.255.0
 no keepalive
 no cdp enable
interface Ethernet1/0
 no ip address
 no keepalive
```

```
 no cdp enable
!
interface Virtual-Template1 type tunnel
 ip unnumbered Ethernet0/0
 tunnel mode ipsec ipv4
 tunnel protection ipsec profile vi
!
ip local pool dpool 10.5.0.1 10.5.0.10
!
ip classless
ip route 10.2.0.0 255.255.255.0 10.3.0.1
no ip http server
no ip http secure-server
!
!
access-list 101 permit ip 10.4.0.0 0.0.0.255 any
no cdp run
!
!
line con 0
line aux 0
line vty 0 4
!
end
```

Example: Pushing a Configuration URL Through a Mode-Configuration Exchange

The following **show crypto ipsec client ezvpn** command output displays the mode configuration URL location and version:

```
Device# show crypto ipsec client ezvpn

Easy VPN Remote Phase: 5
Tunnel name : branch
Inside interface list: Vlan1
Outside interface: FastEthernet0
Current State: IPSEC_ACTIVE
Last Event: SOCKET_UP
Address: 172.16.1.209
Mask: 255.255.255.255
Default Domain: cisco.com
Save Password: Allowed
Configuration URL [version]: tftp://172.16.30.2/branch.cfg [11]
Config status: applied, Last successfully applied version: 11
Current EzVPN Peer: 192.168.10.1
```

The following **show crypto isakmp peers config** command output displays all manageability information that is sent by the remote device:

```
Device# show crypto isakmp peers config

Client-Public-Addr=192.168.10.2:500; Client-Assigned-Addr=172.16.1.209; Client-Group=branch;
 Client-User=branch; Client-Hostname=branch.; Client-Platform=Cisco 1711;
Client-Serial=FOC080210E2 (412454448); Client-Config-Version=11; Client-Flash=33292284;
Client-Available-Flash=10202680; Client-Memory=95969280; Client-Free-Memory=14992140;
Client-Image=flash:c1700-advipservicesk9-mz.ef90241;
Client-Public-Addr=192.168.10.3:500; Client-Assigned-Addr=172.16.1.121; Client-Group=store;
 Client-User=store; Client-Hostname=831-storerouter.; Client-Platform=Cisco C831;
Client-Serial=FOC08472UXR (1908379618); Client-Config-Version=2; Client-Flash=24903676;
Client-Available-Flash=5875028; Client-Memory=45298688; Client-Free-Memory=6295596;
Client-Image=flash:c831-k9o3y6-mz.ef90241
```

Example: Per-User AAA Policy Download with PKI

The following output from the **show running-config** shows that the Per-User AAA Policy Download with PKI feature has been configured on the Easy VPN server:

```
Device# show running-config

Building configuration...
Current configuration : 7040 bytes
!
! Last configuration change at 21:06:51 UTC Tue Jun 28 2005
!
version 12.4
no service pad
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname GEN
!
boot-start-marker
boot-end-marker
!
!
aaa new-model
!
!
aaa group server radius usrgrppki
 server 10.76.248.201 auth-port 1645 acct-port 1646
!
aaa authentication login xauth group usrgrppki
aaa authentication login usrgrp group usrgrppki
aaa authorization network usrgrp group usrgrppki
!
aaa session-id common
!
resource policy
!
ip subnet-zero
!
!
ip cef
!
!
ip address-pool local
!
!
crypto pki trustpoint ca-server
 enrollment url http://10.7.7.2:80
 revocation-check none
 rsakeypair rsa-pair
 ! Specify the field within the certificate that will be used as a username to do a per-user
 AAA lookup into the RADIUS database. In this example, the contents of the  commonname will
 be used to do a AAA lookup. In the absence of this statement, by default  the contents of
 the “unstructured name” field in the certificate is used for AAA lookup.
 authorization username subjectname commonname
!
!
crypto pki certificate map CERT-MAP 1
 subject-name co yourname
 name co yourname
!
crypto pki certificate chain ca-server
 certificate 02
  308201EE 30820157 A0030201 02020102 300D0609 2A864886 F70D0101 04050030
  14311230 10060355 04031309 63612D73 65727665 72301E17 0D303530 36323832
  30303731 345A170D 30363036 32383230 30373134 5A301531 13301106 092A8648
  86F70D01 09021604 47454E2E 30819F30 0D06092A 864886F7 0D010101 05000381
  8D003081 89028181 00ABF8F0 FDFFDF8D F22098D6 A48EE0C3 F505DD96 C0022EA4
```

```
  EAB95EE8 1F97F450 990BB0E6 F2B7151F C5C79391 93822FE4 DEE5B00C A03412BB
  9B715AAD D6C31F93 D8802658 AF9A8866 63811942 913D0C02 C3E328CC 1C046E94
  F73B7C1A 4497F86E 74A627BC B809A3ED 293C15F2 8DCFA217 5160F9A4 09D52044
  350F85AF 08B357F5 D7020301 0001A34F 304D300B 0603551D 0F040403 0205A030
  1F060355 1D230418 30168014 F9BC4498 3DA4D51D 451EFEFD 5B1F5F73 8D7B1C9B
  301D0603 551D0E04 1604146B F6B2DFD1 1FE237FF 23294129 E55D9C48 CCB04630
  0D06092A 864886F7 0D010104 05000381 81004AFF 2BE300C1 15D0B191 C20D06E0
  260305A6 9DF610BB 24211516 5AE73B62 78E01FE4 0785776D 3ADFA3E2 CE064432
  1C93E82D 93B5F2AB 9661EDD3 499C49A8 F87CA553 9132F239 1D50187D 21CC3148
  681F5043 2F2685BC F544F4FF 8DF535CB E55B5F36 31FFF025 8969D9F8 418C8AB7
  C569B022 46C3C63A 22DD6516 C503D6C8 3D81
  quit
 certificate ca 01
  30820201 3082016A A0030201 02020101 300D0609 2A864886 F70D0101 04050030
  14311230 10060355 04031309 63612D73 65727665 72301E17 0D303530 36323832
  30303535 375A170D 30383036 32373230 30353537 5A301431 12301006 03550403
  13096361 2D736572 76657230 819F300D 06092A86 4886F70D 01010105 0003818D
  00308189 02818100 BA1A4413 96339C6B D36BD720 D25C9A44 E0627A29 97E06F2A
  69B268ED 08C7144E 7058948D BEA512D4 40588B87 322C5D79 689427CA 5C54B3BA
  82FAEC53 F6AC0B5C 615D032C 910CA203 AC6AB681 290D9EED D31EB185 8D98E1E7
  FF73613C 32290FD6 A0CBDC40 6E4D6B39 DE1D86BA DE77A55E F15299FF 97D7C185
  919F81C1 30027E0F 02030100 01A36330 61300F06 03551D13 0101FF04 05300301
  01FF300E 0603551D 0F0101FF 04040302 0186301F 0603551D 23041830 168014F9
  BC44983D A4D51D45 1EFEFD5B 1F5F738D 7B1C9B30 1D060355 1D0E0416 0414F9BC
  44983DA4 D51D451E FEFD5B1F 5F738D7B 1C9B300D 06092A86 4886F70D 01010405
  00038181 003EF397 F4D98BDE A4322FAF 4737800F 1671F77E BD6C45AE FB91B28C
  F04C98F0 135A40C6 635FDC29 63C73373 5D5BBC9A F1BBD235 F66CE1AD 6B4BFC7A
  AB18C8CC 1AB93AF3 7AC67436 930E9C81 F43F7570 A8FE09AE 3DEA01D1 DA6BD0CB
  83F9A77F 1DFAFE5E 2F1F206B F1FDD8BE 6BB57A3C 8D03115D B1F64A3F 7A7557C1
  09B0A34A DB
  quit
!
!
crypto isakmp policy 10
 group 2
crypto isakmp keepalive 10
crypto isakmp profile ISA-PROF
   match certificate CERT-MAP
   isakmp authorization list usrgrp
   client pki authorization list usrgrp
   client configuration address respond
   client configuration group pkiuser
   virtual-template 2
!
!
crypto ipsec transform-set trans2 esp-3des esp-sha-hmac
!
crypto ipsec profile IPSEC_PROF
 set transform-set trans2
!
crypto ipsec profile ISC_IPSEC_PROFILE_1
 set transform-set trans2
!
!
crypto call admission limit ike sa 40
!
!
interface Loopback0
 ip address 10.3.0.1 255.255.255.255
 no ip route-cache cef
 no ip route-cache
!
interface Loopback1
 ip address 10.76.0.1 255.255.255.255
 no ip route-cache cef
 no ip route-cache
!
interface Ethernet3/0
 ip address 10.76.248.209 255.255.255.255
 no ip route-cache cef
 no ip route-cache
 duplex half
!
```

```
!
interface Ethernet3/2
 ip address 10.2.0.1 255.255.255.0
 no ip route-cache cef
 no ip route-cache
 duplex half
!
!
interface Serial4/0
 no ip address
 no ip route-cache cef
 no ip route-cache
 shutdown
 serial restart-delay 0
!
interface Serial4/1
 no ip address
 no ip route-cache cef
 no ip route-cache
 shutdown
 serial restart-delay 0
!
interface Serial4/2
 no ip address
 no ip route-cache cef
 no ip route-cache
 shutdown
 serial restart-delay 0
!
interface Serial4/3
 no ip address
 no ip route-cache cef
 no ip route-cache
 shutdown
 serial restart-delay 0
!
interface FastEthernet5/0
 ip address 10.9.4.77 255.255.255.255
 no ip route-cache cef
 no ip route-cache
 duplex half
!
interface FastEthernet6/0
 ip address 10.7.7.1 255.255.255.0
 no ip route-cache cef
 no ip route-cache
 duplex full
!
interface Virtual-Template1
 no ip address
!
interface Virtual-Template2 type tunnel
 ip unnumbered Loopback0
 tunnel source Ethernet3/2
 tunnel mode ipsec ipv4
 tunnel protection ipsec profile IPSEC_PROF
!
router eigrp 20
 network 172.16.0.0
 auto-summary
!
ip local pool ourpool 10.6.6.6
ip default-gateway 10.9.4.1
ip classless
ip route 10.1.0.1 255.255.255.255 10.0.0.2
ip route 10.2.3.0 255.255.0.0 10.2.4.4
ip route 10.9.1.0 255.255.0.0 10.4.0.1
ip route 10.76.0.0 255.255.0.0 10.76.248.129
ip route 10.11.1.1 255.255.255.0 10.7.7.2
!
no ip http server
no ip http secure-server
!
```

```
!
logging alarm informational
arp 10.9.4.1 0011.bcb4.d40a ARPA
!
!
radius-server host 10.76.248.201 auth-port 1645 acct-port 1646 key cisco
!
control-plane
!
!
gatekeeper
 shutdown
!
!
line con 0
 stopbits 1
line aux 0
 stopbits 1
line vty 0 4
!
!
end
```

Example: Per-User Attributes on an Easy VPN Server

The following example shows that per-user attributes have been configured on an Easy VPN server:

```
!
aaa new-model
!
!
aaa authentication login default local
aaa authentication login noAAA none
aaa authorization network default local
!
aaa attribute list per-group
 attribute type inacl "per-group-acl" service ike protocol ip mandatory
!
aaa session-id common
!
resource policy
!
ip subnet-zero
!
!
ip cef
!
!
username example password 0 example
!
!
crypto isakmp policy 3
 authentication pre-share
 group 2
crypto isakmp xauth timeout 90
!
crypto isakmp client configuration group PerUserAAA
 key cisco
 pool dpool
 crypto aaa attribute list per-group
!
crypto isakmp profile vi
 match identity group PerUserAAA
 isakmp authorization list default
 client configuration address respond
 client configuration group PerUserAAA
 virtual-template 1
!
!
```

```
crypto ipsec transform-set set esp-3des esp-sha-hmac
!
crypto ipsec profile vi
 set transform-set set
 set isakmp-profile vi
!
!
interface GigabitEthernet0/0
 description 'EzVPN Peer'
 ip address 192.168.1.1 255.255.255.128
 duplex full
 speed 100
 media-type rj45
 no negotiation auto
!
interface GigabitEthernet0/1
 no ip address
 shutdown
 duplex auto
 speed auto
 media-type rj45
 no negotiation auto
interface Virtual-Template1 type tunnel
 ip unnumbered GigabitEthernet0/0
 tunnel mode ipsec ipv4
 tunnel protection ipsec profile vi
!
ip local pool dpool 10.5.0.1 10.5.0.10
ip classless
!
no ip http server
no ip http secure-server
!
!
ip access-list extended per-group-acl
 permit tcp any any
 deny   icmp any any
logging alarm informational
logging trap debugging
!
control-plane
!
gatekeeper
 shutdown
!
line con 0
line aux 0
 stopbits 1
line vty 0 4
!
!
end
```

Example: Network Admission Control

The following is output for an Easy VPN server that has been enabled with Network Admission Control:

Note Network Admission Control is supported on an Easy VPN server only when the server uses IPsec virtual interfaces. Network Admission Control is enabled on the virtual template interface and applies to all clients that use this virtual template interface.

```
Device# show running-config

Building configuration...
Current configuration : 5091 bytes
```

```
!
version 12.4
!
hostname Router
!
aaa new-model
!
!
aaa authentication login userlist local
!
aaa authentication eou default group radius
aaa authorization network hw-client-groupname local
aaa accounting update newinfo
aaa accounting network acclist start-stop broadcast group radius
aaa session-id common
!
!
! Note 1: EAPoUDP packets will use the IP address of the loopback interface when sending
the EAPoUDP hello to the Easy VPN client. Using the IP address ensures that the returning
EAPoUDP packets come back encrypted and are associated with the correct virtual access
interface. The ip admission (ip admission source-interface Loopback10) command is optional.
 Instead of using this command, you can specify the IP address of the virtual template to
be an address in the inside network space as shown in the configuration of the virtual
template below in Note 2.
ip admission source-interface Loopback10
ip admission name test eapoudp inactivity-time 60
!
!
eou clientless username cisco
eou clientless password cisco
eou allow ip-station-id
eou logging
!
username lab password 0 lab
username lab@easy password 0 lab
!
!
crypto isakmp policy 3
  encr 3des
  authentication pre-share
  group 2
!
!
crypto isakmp key 0 cisco address 10.53.0.1
crypto isakmp client configuration group easy
  key cisco
  domain cisco.com
  pool dynpool
  acl split-acl
  group-lock
  configuration url tftp://10.13.0.9/Config-URL_TFTP.cfg
  configuration version 111
!
crypto isakmp profile vi
    match identity group easy
    client authentication list userlist
    isakmp authorization list hw-client-groupname
    client configuration address respond
    client configuration group easy
    accounting acclist
    virtual-template 2
!
crypto ipsec security-association lifetime seconds 120
crypto ipsec transform-set set esp-3des esp-sha-hmac
crypto ipsec transform-set aes-trans esp-aes esp-sha-hmac
crypto ipsec transform-set transform-1 esp-des esp-sha-hmac
crypto ipsec profile vi
  set security-association lifetime seconds 3600
  set transform-set set aes-trans transform-1
  set isakmp-profile vi
!
!
crypto dynamic-map dynmap 1
```

```
  set transform-set aes-trans transform-1
  reverse-route
!
interface Loopback10
  ip address 10.61.0.1 255.255.255.255
!
interface FastEthernet0/0
  ip address 10.13.11.173 255.255.255.255
  duplex auto
  speed auto
!
interface FastEthernet0/1
  ip address 10.55.0.1 255.255.255.255
  duplex auto
  speed auto
!
!
interface Virtual-Template2 type tunnel
! Note2: Use the IP address of the loopback10. This ensures that the EAPoUDP packets that
are attached to virtual-access interfaces that are cloned from this virtual template carry
 the source address of the loopback address and that response packets from the VPN client
come back encrypted.
!
  ip unnumbered Loopback10
! Enable Network Admission Control for remote VPN clients.
  ip admission test
  tunnel mode ipsec ipv4
  tunnel protection ipsec profile vi
!
!
ip local pool dynpool 172.16.2.65 172.16.2.70
ip classless
ip access-list extended ClientException
  permit ip any host 10.61.0.1
ip access-list extended split-acl
  permit ip host 10.13.11.185 any
  permit ip 10.61.0.0 255.255.255.255 any
  permit ip 10.71.0.0 255.255.255.255 any
  permit ip 10.71.0.0 255.255.255.255 10.52.0.0 0.255.255.255
  permit ip 10.55.0.0 255.255.255.255 any
!
ip radius source-interface FastEthernet0/0
access-list 102 permit esp any any
access-list 102 permit ahp any any
access-list 102 permit udp any any eq 21862
access-list 102 permit ospf any any
access-list 102 deny ip any any
access-list 195 deny ospf any any
access-list 195 permit ip 10.61.0.0 255.255.255.255 10.51.0.0 255.255.255.255
!
!
radius-server attribute 6 on-for-login-auth
radius-server attribute 8 include-in-access-req
radius-server host 10.13.11.185 auth-port 1645 acct-port 1646 key cisco
radius-server vsa send accounting
radius-server vsa send authentication
!
end
```

Example: Configuring Password Aging

The following example shows that password aging has been configured so that if the password expires the Easy VPN client is notified:

```
Current configuration : 4455 bytes
!
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
```

```
no service password-encryption
!
hostname xinl-gateway
!
boot-start-marker
boot system flash c2800nm-advsecurityk9-mz.124-7.9.T
boot-end-marker
!
!
aaa new-model
!
!
aaa authentication login USERAUTH passwd-expiry group radius aaa authorization network
branch local !
aaa session-id common
!
ip cef
username cisco privilege 15 secret 5 $1$A3HU$bCWjlkrEztDJx6JJzSnMV1 !
!
crypto isakmp policy 1
  encr 3des
  authentication pre-share
  group 2
crypto isakmp client configuration address-pool local dynpool !
crypto isakmp client configuration group branch
  key cisco
  domain cisco.com
  pool dynpool
!
!
crypto ipsec transform-set transform-1 esp-3des esp-sha-hmac !
crypto isakmp profile profile2
   client authentication list USERAUTH
   match identity group branch
   isakmp authorization list branch
   client configuration address respond
   virtual-template 1
crypto ipsec profile vi
  set transform-set transform-1
interface GigabitEthernet0/0
  description $ETH-LAN$$ETH-SW-LAUNCH$$INTF-INFO-GE 0/0$
  ip address 192.168.1.100 255.255.255.0
  duplex auto
  speed auto
  crypto map dynmap
!
interface GigabitEthernet0/1
  description $ES_LAN$
  ip address 172.19.217.96 255.255.255.0
  duplex auto
  speed auto
!
!interface Virtual-Template1 type tunnel
  ip unnumbered Ethernet0/0
  no clns route-cache
  tunnel mode ipsec ipv4
  tunnel protection ipsec profile vi
!
ip local pool dpool 10.0.0.1 10.0.0.3
!
radius-server host 172.19.220.149 auth-port 1645 acct-port 1646 key cisco radius-server vsa
 send authentication !
control-plane
!
!
end
```

Example: Split DNS

In the following example, the split tunnel list named “101” contains the 10.168.0.0/16 network. This network information must be included so that the DNS requests to the internal DNS server of 10.168.1.1 are encrypted.

```
crypto isakmp client configuration group home
 key abcd
 acl 101
 dns 10.168.1.1. 10.168.1.2
```

show Output

The following **show** command output example shows that www.example1.com and www.example2.com have been added to the policy group:

```
Device# show running-config
 | security group

 crypto isakmp client configuration group 831server
 key abcd
 dns 10.104.128.248
 split-dns www.example1.com
 split-dns www.example2.com
 group home2 key abcd
```

The following **show** command output example displays currently configured DNS views:

```
Device# show ip dns view

DNS View default parameters:
Logging is off
DNS Resolver settings:
  Domain lookup is enabled
  Default domain name: cisco.com
  Domain search list:
  Lookup timeout: 3 seconds
  Lookup retries: 2
  Domain name-servers:
    172.16.168.183
DNS Server settings:
  Forwarding of queries is enabled
  Forwarder addresses:
DNS View ezvpn-internal-view parameters:
Logging is off
DNS Resolver settings:
  Domain lookup is enabled
  Default domain name:
  Domain search list:
  Lookup timeout: 3 seconds
  Lookup retries: 2
  Domain name-servers:
    10.104.128.248
DNS Server settings:
  Forwarding of queries is enabled
  Forwarder addresses:
```

The following **show** command output example displays currently configured DNS view lists:

```
Device# show ip dns view-list

View-list ezvpn-internal-viewlist:
  View ezvpn-internal-view:
    Evaluation order: 10
    Restrict to ip dns name-list: 1
```

```
  View default:
    Evaluation order: 20
```

The following **show** command output displays DNS name lists:

```
Device# show ip dns name-list

ip dns name-list 1
    permit www.example1.com
    permit www.example2.com
```

Example: DHCP Client Proxy

The following examples display DHCP client proxy output information using **show** and **debug** commands.

show Output

Note Before you can use the **show ip dhcp** command, the DHCP server must be a Cisco IOS server.

The following **show ip dhcp pool** command output provides information about the DHCP parameters:

```
Device# show ip dhcp pool

Pool dynpool :
 Utilization mark (high/low)    : 100 / 0
 Subnet size (first/next)       : 0 / 0
 Total addresses                : 254
 Leased addresses               : 1
 Pending event                  : none
 1 subnet is currently in the pool:
 Current index    IP address range          Leased addresses
                  10.3.3.1 - 10.3.3.254     1
 No relay targets associated with class aclass
```

The following **show ip dhcp binding** command output provides information about the DHCP bindings:

```
Device# show ip dhcp binding

Bindings from all pools not associated with VRF:
IP address          Client-ID/                      Lease expiration      Type
                    Hardware address/User name
                    10.3.3.5  0065.7a76.706e.2d63.   Apr 04 2006 06:01 AM  Automatic
                6c69.656e.74
```

debug Output

The following example shows how the **debug crypto isakmp** and **debug ip dhcp server events** commands can be used to troubleshoot your DHCP client proxy support configuration:

```
*Apr  3 06:01:32.047: ISAKMP: Config payload REQUEST *Apr  3 06:01:32.047:
ISAKMP:(1002):checking request:
*Apr  3 06:01:32.047: ISAKMP:    IP4_ADDRESS
*Apr  3 06:01:32.047: ISAKMP:    IP4_NETMASK
*Apr  3 06:01:32.047: ISAKMP:    MODECFG_CONFIG_URL
*Apr  3 06:01:32.047: ISAKMP:    MODECFG_CONFIG_VERSION
*Apr  3 06:01:32.047: ISAKMP:    IP4_DNS
*Apr  3 06:01:32.047: ISAKMP:    IP4_DNS
*Apr  3 06:01:32.047: ISAKMP:    IP4_NBNS
*Apr  3 06:01:32.047: ISAKMP:    IP4_NBNS
*Apr  3 06:01:32.047: ISAKMP:    SPLIT_INCLUDE
*Apr  3 06:01:32.047: ISAKMP:    SPLIT_DNS
```

```
*Apr  3 06:01:32.047: ISAKMP:    DEFAULT_DOMAIN
*Apr  3 06:01:32.047: ISAKMP:    MODECFG_SAVEPWD
*Apr  3 06:01:32.047: ISAKMP:    INCLUDE_LOCAL_LAN
*Apr  3 06:01:32.047: ISAKMP:    PFS
*Apr  3 06:01:32.047: ISAKMP:    BACKUP_SERVER
*Apr  3 06:01:32.047: ISAKMP:    APPLICATION_VERSION
*Apr  3 06:01:32.047: ISAKMP:    MODECFG_BANNER
*Apr  3 06:01:32.047: ISAKMP:    MODECFG_IPSEC_INT_CONF
*Apr  3 06:01:32.047: ISAKMP:    MODECFG_HOSTNAME
*Apr  3 06:01:32.047: ISAKMP/author: Author request for group homesuccessfully sent to AAA
 *Apr  3 06:01:32.047: ISAKMP:(1002):Input = IKE_MESG_FROM_PEER, IKE_CFG_REQUEST
*Apr  3 06:01:32.047: ISAKMP:(1002):Old State = IKE_P1_COMPLETE  New State =
IKE_CONFIG_AUTHOR_AAA_AWAIT
*Apr  3 06:01:32.047: ISAKMP:(1002):attributes sent in message:
*Apr  3 06:01:32.047:         Address: 10.2.0.0
*Apr  3 06:01:32.047: Requesting DHCP Server0 address 10.3.3.3 *Apr  3 06:01:32.047: DHCPD:
 Sending notification of DISCOVER:
*Apr  3 06:01:32.047:   DHCPD: htype 1 chaddr aabb.cc00.6600
*Apr  3 06:01:32.047:   DHCPD: circuit id 00000000
*Apr  3 06:01:32.047: DHCPD: Seeing if there is an internally specified pool class:
*Apr  3 06:01:32.047:   DHCPD: htype 1 chaddr aabb.cc00.6600
*Apr  3 06:01:32.047:   DHCPD: circuit id 00000000
*Apr  3 06:01:34.063: DHCPD: Adding binding to radix tree (10.3.3.5) *Apr  3 06:01:34.063:
 DHCPD: Adding binding to hash tree *Apr  3 06:01:34.063: DHCPD: assigned IP address 10.3.3.5
 to client 0065.7a76.706e.2d63.6c69.656e.74.
*Apr  3 06:01:34.071: DHCPD: Sending notification of ASSIGNMENT:
*Apr  3 06:01:34.071:  DHCPD: address 10.3.3.5 mask 255.255.255.0
*Apr  3 06:01:34.071:   DHCPD: htype 1 chaddr aabb.cc00.6600
*Apr  3 06:01:34.071:   DHCPD: lease time remaining (secs) = 86400
*Apr  3 06:01:34.183: Obtained DHCP address 10.3.3.5 *Apr  3 06:01:34.183:
ISAKMP:(1002):allocating address 10.3.3.5 *Apr  3 06:01:34.183: ISAKMP: Sending private
address: 10.3.3.5 *Apr  3 06:01:34.183: ISAKMP: Sending subnet mask: 255.255.255.0
```

Example: Cisco Tunneling Control Protocol Session

The following **debug crypto ctcp** command output displays information about a cTCP session, including comments about the output:

```
Device# debug crypto ctcp

! In the following two lines, a cTCP SYN packet is received from the client, and the cTCP
connection is created.
*Sep 26 11:14:37.135: cTCP: Connection[648B50C0] 10.76.235.21:3519 10.76.248.239:10000:
created
*Sep 26 11:14:37.135: cTCP: SYN from 10.76.235.21:3519
! In the following line, the SYN acknowledgement is sent to the client.
*Sep 26 11:14:37.135: cTCP: Sending SYN(680723B2)ACK(100C637) to 10.76.235.21:3519
! In the following two lines, an acknowledgement is received, and connection setup is
complete. IKE packets should now be received on this newly created cTCP session.
*Sep 26 11:14:37.135: cTCP: Connection[648B50C0] 10.76.235.21:3519 10.76.248.239:10000:
found
*Sep 26 11:14:37.135: cTCP: ACK from 10.76.235.21:3519
*Sep 26 11:14:37.727: cTCP: Connection[648B50C0] 10.76.235.21:3519 10.76.248.239:10000:
found
*Sep 26 11:14:37.731: cTCP: updating PEER Seq number to 168288031
*Sep 26 11:14:37.731: cTCP: Pak with contiguous buffer
*Sep 26 11:14:37.731: cTCP: mangling IKE packet from peer: 10.76.235.21:500->3519
10.76.248.239:500->500
*Sep 26 11:14:37.731: cTCP: Connection[648B50C0] 10.76.235.21:3519 10.76.248.239:10000:
found
*Sep 26 11:14:37.799: cTCP: demangling outbound IKE packet: 10.76.248.239:500->500
10.76.235.21:3519->500
*Sep 26 11:14:37.799: cTCP: encapsulating IKE packet
*Sep 26 11:14:37.799: cTCP: updating LOCAL Seq number to 174529872701
! The above lines show that after the required number of IKE packets are exchanged, IKE and
 IPsec SAs are created.
*Sep 26 11:14:40.335: cTCP: updating PEER Seq number to 168304311
*Sep 26 11:14:40.335: cTCP: Pak with particles
*Sep 26 11:14:40.335: cTCP: encapsulating pak
```

```
*Sep 26 11:14:40.339: cTCP: datagramstart 0xF2036D8, network_start 0xF2036D8, size 112
*Sep 26 11:14:40.339: cTCP: Pak with contiguous buffer
*Sep 26 11:14:40.339:  cTCP: allocated new buffer
*Sep 26 11:14:40.339: cTCP: updating LOCAL Seq number to 17452995351
*Sep 26 11:14:40.339: IP: s=10.76.248.239 (local), d=10.76.235.21 (FastEthernet1/1), len
148, cTCP
! The above lines show that Encapsulating Security Payload (ESP) packets are now being sent
 and received.
```

Example: VRF Assignment by a AAA Server

The following output example shows that neither a VRF nor an IP address has been defined:

```
aaa new-model
aaa authentication login VPN group radius
aaa authorization network VPN group radius
!
ip vrf example1
 rd 1:1
!
crypto isakmp profile example1
 match identity group example1group
 client authentication list VPN
 isakmp authorization list VPN
 client configuration address respond
 virtual-template 10
!
crypto ipsec transform-set TS esp-3des esp-sha-hmac
!
crypto ipsec profile example1
 set transform-set TS
 set isakmp-profile example1
!
interface Virtual-Template10 type tunnel
! The next line shows that neither VRF nor an IP address has been defined.
 no ip address
tunnel mode ipsec ipv4
tunnel protection ipsec profile example1
```

Additional References

Related Documents

Related Topic	Document Title
Cisco IOS commands	Cisco IOS Master Commands List, All Releases
Security commands: complete command syntax, command mode, command history, defaults, usage guidelines, and examples	• Cisco IOS Security Command Reference Commands A to C • Cisco IOS Security Command Reference Commands D to L • Cisco IOS Security Command Reference Commands M to R • Cisco IOS Security Command Reference Commands S to Z

Related Topic	Document Title
Configuring and Assigning the Easy VPN Remote Configuration	*Cisco Easy VPN Remote*
General information on IPsec and VPN	• *IPsec VPN High Availability Enhancements* • Configuring NAC with IPsec Dynamic Virtual Tunnel Interface white paper
IPsec protocol options and attributes	*Configuring Internet Key Exchange for IPsec VPNs*
IPsec virtual tunnels	*IPsec Virtual Tunnel Interface*
Network Admission Control	*Network Admission Control*
Reverse route injection	*Reverse Route Injection*
Recommended cryptographic algorithms	Next Generation Encryption

Technical Assistance

Description	Link
The Cisco Support and Documentation website provides online resources to download documentation, software, and tools. Use these resources to install and configure the software and to troubleshoot and resolve technical issues with Cisco products and technologies. Access to most tools on the Cisco Support and Documentation website requires a Cisco.com user ID and password.	http://www.cisco.com/cisco/web/support/index.html

Feature Information for Easy VPN Server

Table 9: Feature Information for Easy VPN Server

Feature Name	Releases	Feature Information
Easy VPN Server	12.2(8)T	The Easy VPN Server feature introduces server support for the Cisco VPN Client Release 3.x and later software clients and Cisco VPN hardware clients (such as the Cisco 800, Cisco 900, Cisco 1700, VPN 3002, and PIX 501 devices). This feature allows a remote end user to communicate using IPsec with any Cisco IOS VPN gateway. Centrally managed IPsec policies are "pushed" to the client device by the server, thereby minimizing end-user configurations.
	12.3(2)T	RADIUS support for user profiles, user-based policy control, session monitoring for VPN group access, backup-gateway list, and PFS was added.
	12.3(7)T	The **netmask** command was integrated for use on the Easy VPN server.
	12.4(2)T 12.2(33)SXH	The Banner, Auto-Update, and Browser Proxy Enhancements feature was added in this release.
	12.4(6)T	The Central Policy Push Firewall Policy Push feature was added.
	12.2(33)SRA	This feature was integrated into Cisco IOS Release 12.2(33)SRA.

Feature Name	Releases	Feature Information
	12.4(9)T	The following features were added in this release: • Cisco Tunneling Control Protocol • DHCP Client Proxy • Per-User Attribute Support for Easy VPN Servers • Split DNS • Virtual Tunnel Interface Per-User Attribute Support for Easy VPN Servers • VRF Assignment by a AAA Server The following commands were introduced or modified: **crypto aaa attribute list**, **crypto isakmp client configuration group**, **debug ip dns**, **dhcp-server (isakmp)**, **dhcp-timeout**, **show ip dns name-list**, **show ip dns view**, **show ip dns view-list**.
DHCP Client Proxy Enhancements	12.4(11)T	The DHCP Client Proxy feature was updated to include manageability enhancements for remote access VPNs. The following commands were modified: **clear crypto session**, **crypto isakmp client configuration group**, **debug crypto condition**, **show crypto debug-condition**, **show crypto isakmp peers**, **show crypto isakmp profile**, **show crypto isakmp sa**, **show crypto session**.

Glossary

AAA—authentication, authorization, and accounting. Framework of security services that provides the method for identifying users (authentication), for remote access control (authorization), and for collecting and sending security server information used for billing, auditing, and reporting (accounting).

aggressive mode (AM)—Mode during Internet Key Exchange negotiation. Compared to main mode (MM), AM eliminates several steps, which makes it faster but less secure than MM. Cisco IOS software will respond in aggressive mode to an Internet Key Exchange (IKE) peer that initiates aggressive mode.

AV pair—attribute-value pair.

IKE—Internet Key Exchange. Hybrid protocol that implements Oakley key exchange and Skeme key exchange inside the ISAKMP framework. Although IKE can be used with other protocols, its initial implementation was with IPsec. IKE provides authentication of the IPsec peers, negotiates IPsec keys, and negotiates IPsec security associations.

IPsec—IP Security Protocol. Framework of open standards that provides data confidentiality, data integrity, and data authentication between participating peers. IPsec provides these security services at the IP layer. IPsec uses IKE to handle negotiation of protocols and algorithms based on local policy and to generate the encryption and authentication keys to be used by IPsec. IPsec can be used to protect one or more data flows between a pair of hosts, between a pair of security gateways, or between a security gateway and a host.

ISAKMP—Internet Security Association Key Management Protocol. Protocol framework that defines payload formats, the mechanics of implementing a key exchange protocol, and the negotiation of a security association.

MM—main mode. Mode that is slower than aggressive mode but more secure and more flexible than aggressive mode because it can offer an IKE peer more security proposals. The default action for IKE authentication (Rivest, Shamir, and Adelman signature (rsa-sig), RSA encryption (rsa-encr), or preshared) is to initiate main mode.

policy push—Allows administrators to push policies that enforce security to the Cisco Easy VPN (software) Client and related firewall software.

reverse route injection (RRI)—Simplified network design for VPNs on which there is a requirement for redundancy or load balancing. RRI works with both dynamic and static crypto maps.

In the dynamic case, as remote peers establish IPsec security associations with an RRI enabled device, a static route is created for each subnet or host protected by that remote peer. For static crypto maps, a static route is created for each destination of an extended access-list rule.

SA—security association. Description of how two or more entities will utilize security services to communicate securely. For example, an IPsec SA defines the encryption algorithm (if used), the authentication algorithm, and the shared session key to be used during the IPsec connection.

Both IPsec and IKE require and use SAs to identify the parameters of their connections. IKE can negotiate and establish its own SA. The IPsec SA is established either by IKE or by manual user configuration.

VPN—Virtual Private Network. Framework that consists of multiple peers transmitting private data securely to one another over an otherwise public infrastructure. In this framework, inbound and outbound network traffic is protected using protocols that tunnel and encrypt all data. This framework permits networks to extend beyond their local topology, while remote users are provided with the appearance and functionality of a direct network connection.

INDEX

E