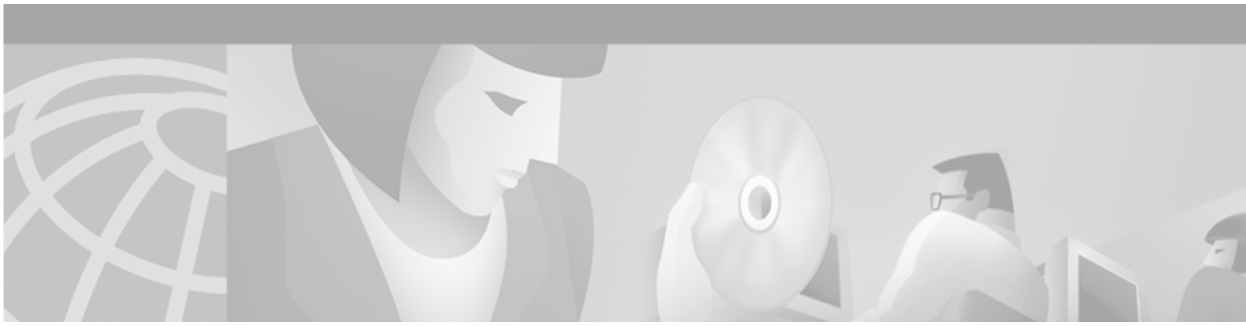


Cisco Easy VPN Client for the Cisco 1700 Series Routers

This document provides information on configuring and monitoring the Cisco Easy VPN client feature to support the Cisco 1700 series routers as IPSec clients of the VPN 3000 series concentrator. The following topics are included:

- Feature Overview
- Restrictions
- Related Documents
- Prerequisites
- Configuration Tasks
- Configuration Examples
- Simultaneous Client Server Functionality
- Obtaining Documentation
- Obtaining Technical Assistance

Feature Overview

Routers and other broadband devices provide high-performance connections to the Internet, but many applications also require the security of virtual private network (VPN) connections that perform a high level of authentication and that encrypt the data between two particular endpoints. However, establishing a VPN connection between two routers can be complicated, and it typically requires tedious coordination between network administrators to configure the two routers' VPN parameters.

The Cisco Easy VPN Client feature eliminates much of this tedious work by implementing Cisco's Unity Client protocol, which allows most VPN parameters to be defined at a VPN 3000 series concentrator acting as an IPSec server.

Cisco Systems

Corporate Headquarters:
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

The Cisco Easy VPN client feature can be configured in one of two modes: client mode or network extension mode. Client mode is the default configuration and allows only devices at the client site to access resources at the central site. Resources at the client site are unavailable to the central site. Network extension mode allows users at the central site (where the VPN 3000 series concentrator is located) to access network resources on the client site.

After the IPSec server has been configured, a VPN connection can be created with minimal configuration on an IPSec client, such as a supported Cisco 1700 series router. When the IPSec client initiates the VPN tunnel connection, the IPSec server pushes the IPSec policies to the IPSec client and creates the corresponding VPN tunnel connection.

Note Note that Cisco 1700 series routers are supported as IPSec clients of VPN 3000 series concentrators.

The following policies are pushed from the VPN concentrator to the Cisco Easy VPN client-enabled 1700 series router:

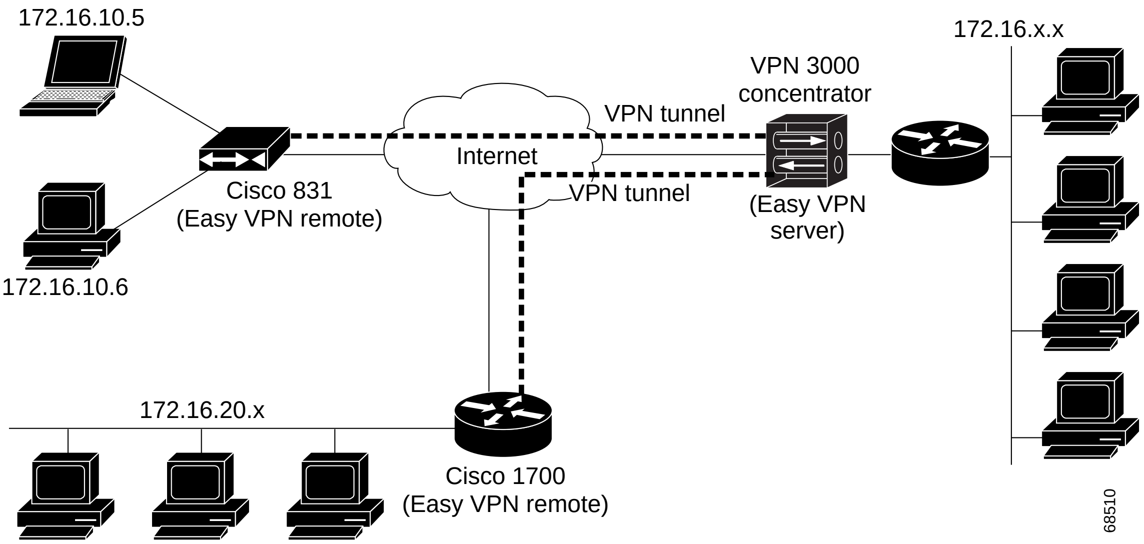
- Internal IP address
- WINS server address
- DHCP address
- Internal subnet mask
- Split tunneling flag

Refer to the document at the following URL to obtain instructions on configuring the DHCP server pool, and to see the Easy VPN client profile required for implementing Easy VPN. This document contains configuration examples for the Cisco 1700 router.

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t13/ftezvpcm.htm

Figure 1 shows the network extension mode of operation. In this example, the Cisco 1700 series router and a Cisco 831 cable access router both act as Easy VPN clients, connecting to a VPN 3000 series concentrator. The PCs and hosts attached to the two routers have IP addresses that are in the same address range as that of the destination enterprise network; this results in a seamless extension of the remote network.

Figure 1 Network Extension Mode



Restrictions

The Cisco Easy VPN client feature supports configuration of only one destination peer. If your application requires creation of multiple VPN tunnels, you must manually configure the IPSec VPN and Network Address Translation/Peer Address Translation (NAT/PAT) parameters on both the client and the server.

Related Documents

This section lists other documentation related to the configuration and maintenance of the supported routers and the Cisco Easy VPN client feature.

Platform Documentation

The following documents provide information for specific Cisco routers:

- *Cisco 1700 Series Router Software Configuration Guide*
- *Cisco 1710 Security Router Hardware Installation Guide*
- *Cisco 1710 Security Router Software Configuration Guide*
- *Cisco 1720 Series Router Hardware Installation Guide*

- *Cisco 1750 Series Router Hardware Installation Guide*
- *Cisco 1751 Router Hardware Installation Guide*
- *Cisco 1751 Router Software Configuration Guide*

IPsec and VPN Documentation

For general information about IPsec and VPNs, see the following information in the product literature and the IP technical tips sections on Cisco.com:

- *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.
- *Certificate Authority Support for IPsec Overview*—Describes the concept of digital certificates and tells how they are used to authenticate IPsec users.
- *An Introduction to IP Security (IPsec) Encryption*—Provides step-by-step instructions for configuring IPsec encryption.

The following technical documents, available on Cisco.com and on the Documentation CD-ROM, also provide more in-depth configuration information:

- *Cisco IOS Security Configuration Guide, Cisco IOS Release 12.2*—Provides an overview of Cisco IOS security features.
- *Cisco IOS Security Command Reference, Cisco IOS Release 12.2*—Provides a reference for each of the Cisco IOS commands used to configure IPsec encryption and related security features.
- *Cisco IOS Software Command Summary, Cisco IOS Release 12.2*—Summarizes the Cisco IOS commands used to configure all Release 12.1 security features.

Prerequisites

The following conditions must exist in order to use the Cisco Easy VPN client feature on the Cisco 1700 series routers:

- The Cisco 1700 series router must be running Cisco IOS Release 12.2(4)XM or later, configured as an Easy VPN IPSec client.
- Another Cisco router or VPN concentrator that supports the Remote Access VPN Server Support feature or the Unity Client protocol must be configured as an IPSec server.

Configuration Tasks

The following sections describe the tasks for configuring the Cisco Easy VPN client feature:

- Configuring the DHCP Server Pool (Required for Client Mode)
- Verifying the DHCP Server Pool
- Configuring and Assigning the Cisco Easy VPN Client Profile
- Verifying the Cisco Easy VPN Configuration
- Configuring the VPN 3000 Series Concentrator

Configuring the DHCP Server Pool (Required for Client Mode)

The local router uses the DHCP protocol to assign IP addresses to the PCs or other hosts that are connected to the router's LAN interface. This requires creating a pool of IP addresses for the router's onboard DHCP server. The DHCP server then assigns an IP address from this pool to each PC or other host when it connects to the router.

In a typical VPN connection, the PCs or other hosts connected to the router's LAN interface are assigned an IP address in a private address space. The router then uses NAT/PAT to translate those IP addresses into a single IP address that is transmitted across the VPN tunnel connection.

To configure the DHCP server pool, follow these steps:

	Command	Purpose
Step 1	Router(config)# **ip dhcp pool** *pool-name*	Creates a DHCP server address pool named *pool-name* and enters DHCP pool configuration mode.
Step 2	Router(dhcp-config)# **network** *ip-address* [*mask* | */prefix-length*]	Specifies the IP network number and subnet mask of the DHCP address pool that is to be used for the PCs connected to the router's local Ethernet interface. This network number and subnet mask must specify the same subnet as the IP address assigned to the Ethernet interface. The subnet mask can also be specified as a prefix length that specifies the number of bits in the address portion of the subnet address. The prefix length must be preceded by a forward slash (/).
Step 3	Router(dhcp-config)# **default-router** *address* [*address2 ... address8*]	Specifies the IP address of the default router for a DHCP client. You must specify at least one address. You can optionally specify additional addresses, up to a total of eight addresses per command. **Tip** The first IP address for the **default-router** option should be the IP address that is assigned to the router's Ethernet address.
Step 4	Router(dhcp-config)# **domain-name** domain	(Optional) Specifies the domain name for the client.
Step 5	Router(dhcp-config)# **import all**	(Optional) Imports available DHCP option parameters from a central DHCP server into the router's local DHCP database. **Note** This option requires that a central DHCP server be configured to provide the DHCP options. The central DHCP server should be on the same subnet as was configured using the **network** option. (On Cisco IOS routers, this is done using the **ip dhcp database** command.) If you are using the PPP/IPCP protocol on the WAN interface, or if the client on the WAN interface supports the Easy IP feature, then the central DHCP server can be on a different subnet or network.

	Command	Purpose
Step 6	Router(dhcp-config)# **dns-server** *address* [*address2 ... address8*]	(Optional, if you do not use the **import all** option) Specifies the IP address of a DNS server that is available to a DHCP client. You must specify at least one address. You can optionally specify additional addresses, up to eight addresses per command.
Step 7	Router(dhcp-config)# **netbios-name-server** *address* [*address2 ... address8*]	(Optional, if you do not use the **import all** option) Specifies the NetBIOS WINS server that is available to a Microsoft DHCP client. You must specify at least one address. You can optionally specify additional addresses, up to eight addresses per command.
Step 8	Router (dhcp-config)# **netbios-node-type** *type*	(Optional, if you do not use the **import all** option) Specifies the NetBIOS node type for a Microsoft DHCP client: • **0** to **FF**—Specifies the raw hexadecimal number for the node type. • **b-node**—Specifies a broadcast node. • **h-node**—Specifies a hybrid node (recommended). • **m-node**—Specifies a mixed node. • **p-node**—Specifies a peer-to-peer node.
	Note You should not specify the **dns-server**, **netbios-name-server**, and **netbios-node-type** options if you use the **import all** option because that would override the imported values.	
Step 9	Router(dhcp-config)# **lease** {*days* [*hours*][*minutes*] | **infinite**}	(Optional) Specifies the duration of the DHCP lease. The default is a one-day lease.
Step 10	Router(dhcp-config)# **exit**	Exits DHCP pool configuration mode.

Verifying the DHCP Server Pool

To verify that the DHCP server pool has been correctly configured, use the following procedure.

Step 1 Use the **show ip dhcp pool** command in privileged EXEC mode to display the server pools that have been created:

```
Router# show ip dhcp pool
Pool localpool :
 Current index        : 192.168.100.1
 Address range        : 192.168.100.1 - 192.168.100.254
Router#
```

Step 2 If you used the **import all** option when you created the DHCP server pool, use the **show ip dhcp import** command to display the options that have been imported from the central DHCP server:

```
Router# show ip dhcp import

Address Pool Name: localpool
Domain Name Server(s): 192.168.20.5
NetBIOS Name Server(s): 192.168.20.6
Router#
```

Step 3 To display the IP addresses that the DHCP server has assigned, use the **show ip dhcp binding** command:

```
Router# show ip dhcp binding

IP address    Hardware address    Lease expiration        Type
192.168.100.3 00c0.abcd.32de      Nov 01 2001 12:00 AM    Automatic
192.168.100.5 00c0.abcd.331a      Nov 01 2001 12:00 AM    Automatic
Router#
```

Configuring and Assigning the Cisco Easy VPN Client Profile

The router acting as the IPSec client must create an Easy VPN profile and assign it to the outgoing interface. To configure and assign the profile, use the following procedure:

	Command	Purpose
Step 1	`router(config)#` **`crypto ipsec client easy VPN`** *`profile-name`*	Creates an Easy VPN profile named *profile-name* and enters Easy VPN configuration mode.
Step 2	`router(config-crypto-easy VPN)#` **`group`** *`group-name`* **`key`** *`key-value`*	Specifies the IPSec group and IPSec key value to be associated with this profile. **Note** The *group-name* must match the group defined on the IPSec server with the **crypto isakmp client configuration group** and **crypto map dynmap isakmp authorization list** commands. **Note** The *key-value* must match the key defined on the IPSec server with the **crypto isakmp client configuration group** command.
Step 3	`router(config-crypto-easy VPN)#` **`peer`** `[`*`ip-address`* `|` *`hostname`*`]`	Specifies the IP address or host name for the destination peer. This is typically the IP address on the destination router's WAN interface. **Note** You must have a DNS server configured and available to use the *hostname* option.
Step 4	`router(config-crypto-easy VPN)#` **`mode`** `{`**`client`** `|` **`network-extension`**`}`	Specifies the type of VPN connection that should be made: • **client**—Specifies that the router is configured for VPN client operation, using NAT/PAT address translation. • **network-extension**—Specifies that the router is to become a remote extension of the enterprise network at the destination of the VPN connection.
Step 5	`router(config-crypto-easy VPN)#` **`exit`**	Exits Easy VPN configuration mode.
Step 6	`router(config)#` **`interface`** *`interface`*	Enters interface configuration mode for the desired interface.
Step 7	`router(config-if)#` **`crypto ipsec client easy VPN`** *`profile-name <outside>`*	Assigns the Easy VPN profile to the interface. The keyword <outside> is optional.
Step 8	`router(config-if)#` **`exit`**	Exits interface configuration mode.
Step 9	`router(config)#` **`interface`** *`interface`*	Enters interface configuration mode for the desired interface.
Step 10	`router(config)#` **`exit`**	Exits global configuration mode.

	Command	Purpose
Step 11	`router(config)#` **`crypto ipsec client ezvpn profile-name`** *`<inside>`*	Configures the inside interface. This automatically creates the necessary NAT/PAT translation parameters and initiates the VPN connection.
Step 12	`router(config)#` **`crypto ipsec client ezvpn connect`** *`<ezvpn-name>`* `|` *`<cr>`*`}`	Initiates the VPN connection on the interface. This command is required only if the Easy VPN configuration was configured for manual connection.

Verifying the Cisco Easy VPN Configuration

Follow these steps to verify that the Easy VPN profile has been correctly configured, that the profile has been assigned to an interface, and that the IPSec VPN tunnel has been established:

Step 1 To display the current state of the Cisco Easy VPN connection, use the **show crypto ipsec client Easy VPN** command:

```
R2#sh cry ip cl ez
Tunnel name :prof2
Inside interface list:FastEthernet0/0,Serial0/1
Outside interface:Serial0/0
Current State:IPSEC_ACTIVE
Last Event:SOCKET_UP
Address:100.0.1.2
Mask:255.255.255.255
R2#
```

Step 2 To display the NAT/PAT configuration that was automatically created for the VPN connection, use the **show ip nat statistics** command. The “Dynamic mappings” section of this display provides the details about the NAT/PAT translation that is occurring on the VPN tunnel.

```
Router# 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 198.1.1.90 end 198.1.1.90
        type generic, total addresses 1, allocated 0 (0%), misses 0\
Router#
```

Step 3 The NAT/PAT translation uses an access list that is also dynamically configured at the time the VPN tunnel is initiated. To display this access list, use the **show access-list** command:

```
Router# show access-list
Extended IP access list 198
    permit ip 192.1.1.0 0.0.0.255 any
Router#
```

Note In this example, the Easy VPN configuration creates access list 198 for the VPN tunnel NAT/PAT translation. The exact numbering of the access list can vary, depending on the other access lists that have been configured on the router. Do not assume that the VPN tunnel will use the same access list every time the connection is initiated.

Step 4 To display the destination IPSec peer and the key value being used, use the **show crypto isakmp key** command:

```
Router# show crypto isakmp key
Hostname/Address       Preshared Key
193.1.1.1              hw-client-password
Router#
```

Configuring the VPN 3000 Series Concentrator

Use the following guidelines to configure the Cisco VPN 3000 series concentrator for use with Cisco Easy VPN clients.

Note You must be using software release 3.5 or later for the Cisco VPN 3000 series concentrator to support Cisco Easy VPN clients.

- IPSec Tunnel Protocol—Enable the IPSec tunnel protocol so that it is available for users. This is configured on the VPN 3000 concentrator by clicking the **General** tab on the Configuration | User Management | Base Group screen.
- IPSec group—Configure the VPN 3000 series concentrator with a group name and password that match the values configured for the Cisco Easy VPN client profile on the router. These values are configured on the router with the **group** *group-name* **key** *key-value* command, and they are configured on the VPN 3000 series concentrator using the Configuration | User Management | Groups screen.
- IKE Proposals—Release 3.5 of the Cisco VPN 3000 series concentrator is preconfigured with a default Internet Key Exchange (IKE) proposal, CiscoVPNClient-3DES-MD5, that can be used with Cisco Easy VPN clients. This IKE proposal supports preshared keys with extended authentication (XAUTH) using the MD5/HMAC-128 algorithm, and Diffie-Hellman Group 2.

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

  Note You can also use the default IKE proposals IKE-DES-MD5 and IKE-3DES-MD5, but they do not include XAUTH support, and they are not recommended.

- A new IPSec Security Association—Cisco Easy VPN clients use a security association with the following parameters:
  - Authentication Algorithm: ESP/MD5/HMAC-128
  - Encryption Algorithm: DES-56 or 3DES-168 (recommended)
  - Encapsulation Mode: Tunnel

  - Digital Certificate: None (use preshared keys)
  - IKE Proposal: CiscoVPNClient-3DES-MD5 (preferred)

Release 3.5 of the Cisco VPN 3000 series concentrator is preconfigured with several default security associations, but they do not meet the IKE proposal requirements. To use an IKE proposal of CiscoVPNClient-3DES-MD5, copy the ESP/IKE-3DES-MD5 security association. Then modify it to use CiscoVPNClient-3DES-MD5 as its IKE proposal. This is configured on the VPN 3000 series concentrator using the Configuration | Policy Management | Traffic Management | Security Associations screen.

Configuration Examples

This section includes the followng configuration examples:

- Cisco 1700 Router Configured as a VPN Client
- VPN Concentrator Configured as an IPsec Server

Cisco 1700 Router Configured as a VPN Client

The following example configures a Cisco 1700 series router as an IPSec client using the Cisco Easy VPN feature in the client mode of operation. This example shows the following components of the Cisco Easy VPN Client configuration:

- DHCP server pool—The **ip dhcp pool** command creates a pool of IP addresses to be assigned to the PCs connected to the router’s Ethernet1 interface. 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 router’s Ethernet interface.
- Easy VPN client configuration—The **crypto ipsec client Easy VPN hw-client** command (global configuration mode) creates an Easy VPN client configuration named **hw-client**. This configuration specifies a group name of **hw-client-groupname** and a shared key value of **hw-client-password**, and it sets the peer destination to the IP address 188.185.0.5, which is the address assigned to the interface connected to the Internet on the destination peer router. The Easy VPN configuration is configured for the default operations mode, which is the client mode.

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

- The second **crypto ipsec client Easy VPN hw-client** command (interface configuration mode) assigns the Easy VPN client configuration to the ATM 0 interface, so that all traffic received and transmitted on that interface is sent through the VPN tunnel.

```
Current configuration :1308 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
!
ip audit notify log
ip audit po max-events 100
!
crypto ipsec client ezvpn hw3
 connect auto
 group ez key ez
 mode client
 peer 7.7.7.1
crypto ipsec client ezvpn hw1
 connect manual
 group ezvpn key ezvpn
 mode client
 peer 6.6.6.1
!
interface FastEthernet0/0
 ip address 5.5.5.2 255.255.255.0
 speed auto
 crypto ipsec client ezvpn hw3 inside
!
interface Serial0/0
 ip address 4.4.4.2 255.255.255.0
 no ip route-cache
 no ip mroute-cache
 no fair-queue
 crypto ipsec client ezvpn hw1 inside
!
interface Serial0/1
 ip address 3.3.3.2 255.255.255.0
 crypto ipsec client ezvpn hw1 inside
!
interface Serial1/0
 ip address 6.6.6.2 255.255.255.0
 clockrate 4000000
 crypto ipsec client ezvpn hw1
!
interface Serial1/1
 ip address 7.7.7.2 255.255.255.0
 no keepalive
 crypto ipsec client ezvpn hw3
!
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

1760#sh crypto ipsec client ezvpn

Tunnel name :hw1
Inside interface list:Serial0/0, Serial0/1,
Outside interface:Serial1/0
```

```
Current State:IPSEC_ACTIVE
Last Event:SOCKET_UP
Address:8.0.0.5
Mask:255.255.255.255
Default Domain:cisco.com

Tunnel name :hw3
Inside interface list:FastEthernet0/0,
Outside interface:Serial1/1
Current State:IPSEC_ACTIVE
Last Event:SOCKET_UP
Address:9.0.0.5
Mask:255.255.255.255
Default Domain:cisco.com
```

VPN Concentrator Configured as an IPsec Server

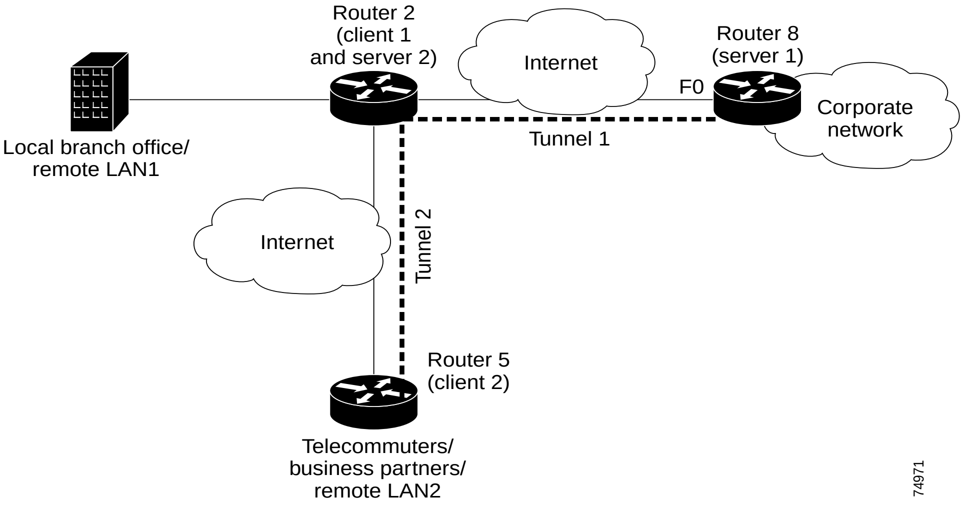
The following example shows a VPN concentrator configuration for a Cisco 7100 VPN concentrator.

```
7100-concentrator#sh running-config
Building configuration...

Current configuration :1131 bytes
!
version 12.2
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname 7100-concentrator
!
aaa new-model
!
aaa authentication login xauth local
aaa session-id common
!
memory-size iomem 15
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
!
crypto isakmp policy 1
 authentication pre-share
 group 2
!
crypto isakmp client configuration group ezvpn
 key ezvpn
 domain cisco.com
 pool dynpool
 acl 101
!
crypto ipsec transform-set proposal1 esp-des esp-sha-hmac
!
crypto dynamic-map foo 10
 set transform-set proposal1
!
crypto map foo isakmp authorization list ezvpn
crypto map foo client configuration address respond
crypto map foo 10 ipsec-isakmp dynamic foo
!
interface FastEthernet0/0
 no ip address
 shutdown
 speed auto
!
interface Serial0/0
 ip address 13.0.0.5 255.0.0.0
 no ip route-cache
 no ip mroute-cache
 crypto map foo
!
ip local pool dynpool 8.0.0.5
ip classless
no ip http server
ip pim bidir-enable
!
line con 0
line aux 0
line vty 0 4
!
end

7100-concentrator#
```

Simultaneous Client Server Functionality

A Cisco 1700 series router can simultaneouslyact as a Easy VPN client and server.The following figure shows a typical scenario, where a local branch office provides a secure VPN tunnel to telecommuters at the same time that they provide another secure tunnel to corporate headquarters.

Figure 2 Simultaneous Client Server Functionality Scenario



Server 1 Configuration Example

The following example shows a configuration for server 1, represented in the figure by router 8.

```
R8#sh running-config
Building configuration...

Current configuration :1283 bytes
!
version 12.2
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname R8
!
aaa new-model
!
aaa authorization network hw-client-group local
aaa session-id common
!
memory-size iomem 5
ip subnet-zero
!
no ip domain-lookup
!
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 hw-client-group
 key password
 dns 172.168.0.250 172.168.0.251
 wins 172.168.0.252 172.168.0.253
 domain cisco.com
 pool dynpool
!
crypto ipsec transform-set transform-1 esp-3des esp-md5-hmac
!
crypto dynamic-map dynmap 1
 set transform-set transform-1
!
crypto map dynmap isakmp authorization list hw-client-group
crypto map dynmap client configuration address respond
crypto map dynmap 1 ipsec-isakmp dynamic dynmap
!
interface Ethernet0
 ip address 200.0.1.5 255.0.0.0
 half-duplex
!
interface FastEthernet0
 ip address 30.0.0.5 255.0.0.0
 speed auto
 crypto map dynmap
!
ip local pool dynpool 100.0.1.65 100.0.1.70
ip classless
ip route 0.0.0.0 0.0.0.0 30.0.0.51
```

```
no ip http server
ip pim bidir-enable
!
line con 0
line aux 0
line vty 0 4
!
no scheduler allocate
end

R8#
```

Client 1 and Server 2 Configuration Example

The following example shows the configuration for the client 1 and server 2, represented in the figure by router 2.

```
R2#sh run
R2#sh running-config
Building configuration...

Current configuration :2040 bytes
!
version 12.2
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname R2
!
aaa new-model
!
!
aaa authorization network hw-server-group local
aaa session-id common
!
memory-size iomem 5
ip subnet-zero
!
no ip domain-lookup
!
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 hw-server-group
 key password
 dns 172.168.0.250 172.168.0.251
 wins 172.168.0.252 172.168.0.253
 domain cisco.com
 pool dynpool
!
crypto ipsec transform-set transform-1 esp-3des esp-md5-hmac
!
crypto ipsec client ezvpn prof3
 connect auto
 group hw-client-group key password
 mode client
 peer 30.0.0.5
!
crypto dynamic-map dynmap 1
 set transform-set transform-1
!
crypto map dynmap isakmp authorization list hw-server-group
crypto map dynmap client configuration address respond
crypto map dynmap 1 ipsec-isakmp dynamic dynmap
!
interface FastEthernet0/0
 ip address 5.0.0.1 255.0.0.0
 speed auto
 crypto ipsec client ezvpn prof3 inside
!
interface Serial0/0
 ip address 1.0.0.1 255.0.0.0
 no fair-queue
 crypto ipsec client ezvpn prof3
!
interface Serial0/1
 ip address 2.0.0.1 255.0.0.0
 crypto map dynmap  <--- to provide server functionality
 crypto ipsec client ezvpn prof3 inside  <-- to provide client functionality
!
! Note that the address range is in the same subnet as that of Serial 0/1
! This is required if the users attached to client2 need to access corporate network
behind server1
! If  the 2 tunnels need to be isolated then ip address pool has to be different from the
subnet on the inside interface serial0/1
ip local pool dynpool 2.0.0.3 2.0.0.100
ip classless
```

```
!
line con 0
line aux 0
line vty 0 4
!
no scheduler allocate
end

R2#
```

Client 2 Configuration Example

The following example shows a configuration for client 2, represented in the figure by router 5.

```
R5#sh running-config
Building configuration...

Current configuration :861 bytes
!
version 12.2
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname R5
!
ip subnet-zero
!
no ip domain-lookup
!
ip ssh time-out 120
ip ssh authentication-retries 3
!
crypto ipsec client ezvpn prof3
 connect auto
 group hw-server-group key password
 mode client
 peer 2.0.0.1
!
interface Loopback1
 ip address 10.0.0.1 255.0.0.0
!
interface FastEthernet0/0
 no ip address
 shutdown
 speed auto
!
interface Serial0/0
 ip address 3.0.0.1 255.0.0.0
 no fair-queue
 crypto ipsec client ezvpn prof3 inside
!
interface Serial0/1
 ip address 2.0.0.2 255.0.0.0
 clock rate 2000000
 crypto ipsec client ezvpn prof3
!
ip default-gateway 2.0.0.1
ip classless
ip route 0.0.0.0 0.0.0.0 2.0.0.1
```

```
no ip http server
ip pim bidir-enable
!
line con 0
line aux 0
line vty 0 4
!
no scheduler allocate
end

R5#
```

Obtaining Documentation

The following sections explain how to obtain documentation from Cisco Systems.

World Wide Web

You can access the most current Cisco documentation on the World Wide Web at the following URL:

http://www.cisco.com

Translated documentation is available at the following URL:

http://www.cisco.com/public/countries_languages.shtml

Documentation CD-ROM

Cisco documentation and additional literature are available in a Cisco Documentation CD-ROM package, which is shipped with your product. The Documentation CD-ROM is updated monthly and may be more current than printed documentation. The CD-ROM package is available as a single unit or through an annual subscription.

Ordering Documentation

Cisco documentation is available in the following ways:

- Registered Cisco Direct Customers can order Cisco product documentation from the Networking Products MarketPlace:

  http://www.cisco.com/cgi-bin/order/order_root.pl

- Registered Cisco.com users can order the Documentation CD-ROM through the online Subscription Store:

  http://www.cisco.com/go/subscription

- Nonregistered Cisco.com users can order documentation through a local account representative by calling Cisco corporate headquarters (California, USA) at 408 526-7208 or, elsewhere in North America, by calling 800 553-NETS (6387).

Documentation Feedback

If you are reading Cisco product documentation on Cisco.com, you can submit technical comments electronically. Click **Leave Feedback** at the bottom of the Cisco Documentation home page. After you complete the form, print it out and fax it to Cisco at 408 527-0730.

You can e-mail your comments to bug-doc@cisco.com.

To submit your comments by mail, use the response card behind the front cover of your document, or write to the following address:

Cisco Systems
Attn: Document Resource Connection
170 West Tasman Drive
San Jose, CA 95134-9883

We appreciate your comments.

Obtaining Technical Assistance

Cisco provides Cisco.com as a starting point for all technical assistance. Customers and partners can obtain documentation, troubleshooting tips, and sample configurations from online tools by using the Cisco Technical Assistance Center (TAC) Web Site. Cisco.com registered users have complete access to the technical support resources on the Cisco TAC Web Site.

Cisco.com

Cisco.com is the foundation of a suite of interactive, networked services that provides immediate, open access to Cisco information, networking solutions, services, programs, and resources at any time, from anywhere in the world.

Cisco.com is a highly integrated Internet application and a powerful, easy-to-use tool that provides a broad range of features and services to help you to

- Streamline business processes and improve productivity
- Resolve technical issues with online support
- Download and test software packages
- Order Cisco learning materials and merchandise
- Register for online skill assessment, training, and certification programs

You can self-register on Cisco.com to obtain customized information and service. To access Cisco.com, go to the following URL:

http://www.cisco.com

Technical Assistance Center

The Cisco TAC is available to all customers who need technical assistance with a Cisco product, technology, or solution. Two types of support are available through the Cisco TAC: the Cisco TAC Web Site and the Cisco TAC Escalation Center.

Inquiries to Cisco TAC are categorized according to the urgency of the issue:

- Priority level 4 (P4)—You need information or assistance concerning Cisco product capabilities, product installation, or basic product configuration.
- Priority level 3 (P3)—Your network performance is degraded. Network functionality is noticeably impaired, but most business operations continue.
- Priority level 2 (P2)—Your production network is severely degraded, affecting significant aspects of business operations. No workaround is available.
- Priority level 1 (P1)—Your production network is down, and a critical impact to business operations will occur if service is not restored quickly. No workaround is available.

Which Cisco TAC resource you choose is based on the priority of the problem and the conditions of service contracts, when applicable.

Cisco TAC Web Site

The Cisco TAC Web Site allows you to resolve P3 and P4 issues yourself, saving both cost and time. The site provides around-the-clock access to online tools, knowledge bases, and software. To access the Cisco TAC Web Site, go to the following URL:

http://www.cisco.com/tac

All customers, partners, and resellers who have a valid Cisco services contract have complete access to the technical support resources on the Cisco TAC Web Site. The Cisco TAC Web Site requires a Cisco.com login ID and password. If you have a valid service contract but do not have a login ID or password, go to the following URL to register:

http://www.cisco.com/register/

If you cannot resolve your technical issues by using the Cisco TAC Web Site, and you are a Cisco.com registered user, you can open a case online by using the TAC Case Open tool at the following URL:

http://www.cisco.com/tac/caseopen

If you have Internet access, it is recommended that you open P3 and P4 cases through the Cisco TAC Web Site.

Cisco TAC Escalation Center

The Cisco TAC Escalation Center addresses issues that are classified as priority level 1 or priority level 2; these classifications are assigned when severe network degradation significantly impacts business operations. When you contact the TAC Escalation Center with a P1 or P2 problem, a Cisco TAC engineer will automatically open a case.

To obtain a directory of toll-free Cisco TAC telephone numbers for your country, go to the following URL:

http://www.cisco.com/warp/public/687/Directory/DirTAC.shtml

Before calling, please check with your network operations center to determine the level of Cisco support services to which your company is entitled; for example, SMARTnet, SMARTnet Onsite, or Network Supported Accounts (NSA). In addition, please have available your service agreement number and your product serial number.

Use this document in conjunction with your router installation and configuration guide, the regulatory compliance and safety information document for your router, and the Cisco IOS configuration guides and command references.