CHAPTER 4

Remote Access VPN Business Scenario

This chapter explains the basic tasks for configuring an IP-based, remote access Virtual Private Network (VPN) on a Cisco IOS VPN gateway. In the remote access VPN business scenario, a remote user running VPN client software on a PC establishes a connection to the headquarters gateway.

Note The configurations in this chapter utilize a Cisco 7100 series VPN gateway. If you have a Cisco IOS VPN gateway model other than the Cisco 7100 series VPN gateway, your configurations will differ slightly, most notably in the port slot numbering. Please refer to your model configuration guide for detailed configuration information. Please refer to the "Obtaining Documentation" section on page xviii for instructions about locating product documentation.

Note This chapter describes basic features and configurations used in a remote access VPN scenario. Some Cisco IOS security software features not described in this document can be used to increase performance and scalability of your VPN. For up-to-date Cisco IOS security software features documentation, refer to the *Cisco IOS Security Configuration Guide* and the *Cisco IOS Security Command Reference*. To access these documents, go to Cisco.com, and select

the following links under "Service and Support": **Technical Documents**: **Cisco IOS Software**: **Cisco IOS Release 12.2**: **Configuration Guides and Command References**.

This chapter includes the following sections:

Note Throughout this chapter, there are numerous configuration examples and sample configuration outputs that include unusable IP addresses. Be sure to use your own IP addresses when configuring your Cisco VPN gateway.

Scenario Description

Figure 4-1 shows a headquarters network providing a remote user access to the corporate intranet. In this scenario, the headquarters and remote user are connected through a secure tunnel that is established over an IP infrastructure (the Internet). The remote user is able to access internal, private web pages and perform various IP-based network tasks.

Figure 4-1 Remote Access VPN Business Scenario

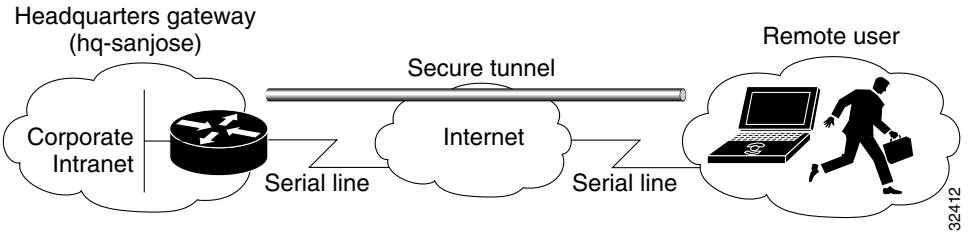
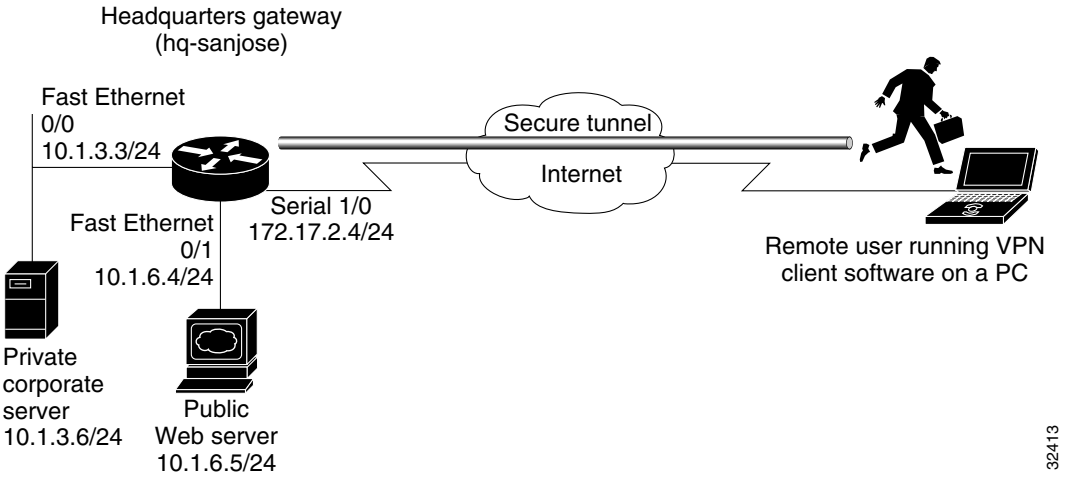


Figure 4-2 shows the physical elements of the scenario. The Internet provides the core interconnecting fabric between the headquarters and remote user. The headquarters is using a Cisco IOS VPN gateway (either a Cisco 7100 series with an Integrated Service Module (ISM) or VPN Accelerator Module (VAM), a Cisco 7200 series with an Integrated Service Adaptor (ISA) or VAM, or a Cisco 3600 series concentrator), and the remote user is running VPN client software on a PC.

The tunnel is configured on the first serial interface in chassis slot 1 (serial 1/0) of the headquarters and remote office routers. Fast Ethernet interface 0/0 of the headquarters router is connected to a corporate server and Fast Ethernet interface 0/1 is connected to a web server.

Figure 4-2 Remote Access VPN Scenario Physical Elements



The configuration steps in the following sections are for the headquarters router. Comprehensive configuration examples for the headquarters router are provided in the "Comprehensive Configuration Examples" section on page 4-18. Table 4-1 lists the physical elements of the scenario.

Table 4-1 Physical Elements

Headquarters Network			Remote User		
Site Hardware	**WAN IP Address**	**Ethernet IP Address**	**Site Hardware**	**WAN IP Address**	**Ethernet IP Address**
hq-sanjose	Serial interface 1/0: 172.17.2.4 255.255.255.0	Fast Ethernet Interface 0/0: 10.1.3.3 255.255.255.0 Fast Ethernet Interface 0/1: 10.1.6.4 255.255.255.0	PC running VPN client software	Dynamically assigned	—
Corporate server	—	10.1.3.6	—	—	—
Web server	—	10.1.6.5			

Configuring a Cisco IOS VPN Gateway for Use with Cisco Secure VPN Client Software

Using Cisco Secure VPN Client software, a remote user can access the corporate headquarters network through a secure IPSec tunnel. Although Cisco IOS VPN gateways support Cisco Secure VPN Client software, this guide does not explain how to configure your gateway for use with it. For detailed information on configuring client-initiated VPNs using Cisco Secure VPN Client software, refer to the *Cisco Secure VPN Client Solutions Guide* publication. You can access the publication by logging on to Cisco.com and selecting **Technical Documents**: **Network Security**: **Cisco Secure VPN Client**: **Cisco Secure VPN Client Solutions Guide**.

Configuring a Cisco IOS VPN Gateway for Use with Microsoft Dial-Up Networking

Using Microsoft Dial-Up Networking (DUN), available with Microsoft Windows 95, Microsoft Windows 98, Microsoft Windows NT 4.0, and Microsoft Windows 2000, a remote user can use Point-to-Point Tunneling Protocol (PPTP) with Microsoft Point-to-Point Encryption (MPPE) to access the corporate headquarters network through a secure tunnel.

Employing PPTP/MPPE, users can use any Internet service provider (ISP) account and any Internet-routable IP address to access the edge of the enterprise network. At the edge, the IP packet is detunneled and the IP address space of the enterprise is used for traversing the internal network. MPPE provides an encryption service that protects the datastream as it traverses the Internet. MPPE is available in two strengths: 40-bit encryption, which is widely available throughout the world, and 128-bit encryption, which may be subject to certain export controls when used outside the United States.

Note PPTP/MPPE is built into Windows DUN1.2 and above. However, 128-bit encryption and stateless (historyless) MPPE is only supported in Windows DUN1.3 or later versions. PPTP/MPPE only supports Cisco Express Forwarding (CEF) and process switching. Regular fast switching is not supported.

Alternatively, a remote user with client software bundled into Microsoft Windows 2000 can use Layer 2 Tunneling Protocol (L2TP) with IPSec to access the corporate headquarters network through a secure tunnel.

Because L2TP is a standard protocol, enterprises can enjoy a wide range of service offerings available from multiple vendors. L2TP implementation is a solution that provides a flexible, scalable remote network access environment without compromising corporate security or endangering mission-critical applications.

Note L2TP is only supported in Microsoft Windows 2000.

This section includes the following topics:

- Configuring PPTP/MPPE
- Verifying PPTP/MPPE
- Configuring L2TP/IPSec

Configuring PPTP/MPPE

PPTP is a network protocol that enables the secure transfer of data from a remote client to a private enterprise server by creating a VPN across TCP/IP-based data networks. PPTP supports on-demand, multiprotocol, virtual private networking over public networks, such as the Internet.

MPPE is an encryption technology developed by Microsoft to encrypt point-to-point links. These PPP connections can be over a dialup line or over a VPN tunnel. MPPE works as a subfeature of Microsoft Point-to-Point Compression (MPPC).

MPPE uses the RC4 algorithm with either 40- or 128-bit keys. All keys are derived from the cleartext authentication password of the user. RC4 is stream cipher; therefore, the sizes of the encrypted and decrypted frames are the same size as the original frame. The Cisco implementation of MPPE is fully interoperable with that of Microsoft and uses all available options, including historyless mode. Historyless mode can increase throughput in high-loss environments such as VPNs.

Note The VAM, which is available for Cisco 7100 and 7200 series gateways, does not support MPPE.

Note Windows clients must use Microsoft Challenge Handshake Authentication Protocol (MS-CHAP) authentication for MPPE to work. If you are performing mutual authentication with MS-CHAP and MPPE, both sides of the tunnel must use the same password.

This section contains basic steps to configure PPTP/MPPE and includes the following tasks:

- Configuring a Virtual Template for Dial-In Sessions
- Configuring PPTP
- Configuring MPPE

Configuring a Virtual Template for Dial-In Sessions

Using virtual templates, you can populate virtual-access interfaces with predefined customized configurations. To configure your Cisco IOS VPN gateway to create virtual-access interfaces from a virtual template for incoming PPTP calls, use the following commands beginning in global configuration mode:

	Command	Purpose
Step 1	`hq-sanjose(config)# interface virtual-template` *number*	Creates the virtual template that is used to clone virtual-access interfaces.
Step 2	`hq-sanjose(config-if)# ip unnumbered` *interface-type number*	Specifies the IP address of the interface the virtual-access interfaces uses.
Step 3	`hq-sanjose(config-if)# ppp authentication ms-chap`	Enables MS-CHAP authentication using the local username database. All windows clients using MPPE need to use MS-CHAP.
Step 4	`hq-sanjose(config-if)# ip local pool default` *first-ip-address last-ip-address*	Configures the default local pool of IP addresses that will be used by clients.
Step 5	`hq-sanjose(config-if)# peer default ip address pool {default|name}`	Returns an IP address from the default pool to the client.

	Command	Purpose
Step 6	`hq-sanjose(config-if)# ip mroute-cache`	Disables fast switching of IP multicast.
Step 7	`hq-sanjose(config-if)# ppp encrypt mppe {auto | 40 | 128} [passive | required] [stateful]`	(Optional) Enables MPPE encryption on the virtual template[1] if you are not using an ISM with your Cisco IOS VPN gateway. If you are using an ISM with a Cisco 7100 series router, see the "Configuring MPPE" section on page 4-9.

1. Stateful MPPE encryption changes the key every 255 packets. Stateless (historyless) MPPE encryption generates a new key for every packet. Stateless MPPE is only supported in recent versions of Dial-Up Networking (DUN1.3).

Configuring PPTP

To configure a Cisco IOS VPN gateway to accept tunneled PPP connections from a client, use the following commands beginning in global configuration mode:

	Command	Purpose
Step 1	`hq-sanjose(config)# vpdn-enable`	Enables virtual private dialup networking on the router.
Step 2	`hq-sanjose(config)# vpdn-group 1`	Creates VPDN group 1.
Step 3	`hq-sanjose(config-vpdn)# accept dialin`	Enables the tunnel server to accept dial-in requests.
Step 4	`hq-sanjose(config-vpdn-acc-in)# protocol pptp`	Specifies that the tunneling protocol will be PPTP.
Step 5	`hq-sanjose(config-vpdn-acc-in)# virtual-template` *template-number*	Specifies the number of the virtual template that will be used to clone the virtual-access interface.
Step 6	`hq-sanjose(config-vpdn-acc-in)# exit` `hq-sanjose(config-vpdn)# local name` *localname*	(Optional) Specifies that the tunnel server will identify itself with this local name. If no local name is specified, the tunnel server will identify itself with its host name.

Configuring MPPE

Note The VAM, which is available for Cisco 7100 and 7200 series gateways, does not support MPPE.

To configure MPPE on your Cisco IOS VPN gateway, use the following commands beginning in global configuration mode:

	Command	Purpose
Step 1	`hq-sanjose(config)# controller isa` *slot/port*	Enter controller configuration mode on the ISM card.
Step 2	`hq-sanjose(config-controller)# encryption mppe`	Enables MPPE encryption.

Verifying PPTP/MPPE

After you complete a connection, enter the **show vpdn tunnel** command or the **show vpdn session** command to verify your PPTP and MPPE configuration.The following example contains typical output:

```
hq-sanjose# show vpdn tunnel | show vpdn session
PPTP Tunnel Information (Total tunnels=1 sessions=1)

LocID RemID Remote Name     State    Remote Address  Port  Sessions
22    22    172.16.230.29  estabd    172.16.230.29   1374  1
```

Configuring L2TP/IPSec

L2TP is an extension of the Point-to-Point (PPP) Protocol and is often a fundamental building block for VPNs. L2TP merges the best features of two other tunneling protocols: Layer 2 Forwarding (L2F) from Cisco Systems and PPTP from Microsoft. L2TP is an Internet Engineering Task Force (IETF) emerging standard.

Note For information on IPSec, see the "Step 3—Configuring Encryption and IPSec" section on page 3-20.

This section contains basic steps to configure L2TP/IPSec and includes the following tasks:

- Configuring a Virtual Template for Dial-In Sessions
- Configuring L2TP
- Configuring Encryption and IPSec

Configuring a Virtual Template for Dial-In Sessions

To configure your Cisco IOS VPN gateway to create virtual-access interfaces from a virtual template for incoming L2TP calls, refer to the "Configuring a Virtual Template for Dial-In Sessions" section on page 4-7.

Note When configuring a virtual template for use with L2TP/IPSec, do not enable MPPE.

Configuring L2TP

To configure a Cisco IOS VPN gateway to accept tunneled L2TP connections from a client, use the following commands beginning in global configuration mode:

	Command	Purpose
Step 1	`hq-sanjose(config)# vpdn-enable`	Enables virtual private dialup networking on the router.
Step 2	`hq-sanjose(config)# vpdn-group 1`	Creates VPDN group 1.
Step 3	`hq-sanjose(config-vpdn)# accept dialin`	Enables the tunnel server to accept dial-in requests.
Step 4	`hq-sanjose(config-vpdn-acc-in)# protocol l2tp`	Specifies that the tunneling protocol will be L2TP.

	Command	Purpose
Step 5	`hq-sanjose(config-vpdn-acc-in)#` **`virtual-template`** *`template-number`*	Specifies the number of the virtual template that will be used to clone the virtual-access interface.
Step 6	`hq-sanjose(config-vpdn-acc-in)#` **`exit`** `hq-sanjose(config-vpdn)#` **`local name`** *`localname`*	(Optional) Specifies that the tunnel server will identify itself with this local name. If no local name is specified, the tunnel server will identify itself with its host name.

Verifying L2TP

Enter the **show vpdn tunnel** command to verify your LT2P configuration.

```
hq-sanjose# show vpdn tunnel
L2TP Tunnel and Session Information (Total tunnels=5 sessions=5)

LocID RemID Remote Name   State  Remote Address  Port  Sessions
  10   8      7206b        est     10.0.0.1      1701      1

LocID RemID TunID Intf    Username    State  Last Chg Fastswitch
   4    6    10   Vi1      las         est   01:44:39   enabled
```

Configuring Encryption and IPSec

For detailed information on configuring encryption and IPSec, refer to the following sections of this guide:

- Configuring IKE Policies, page 3-22
- Verifying IKE Policies, page 3-30
- Creating Crypto Access Lists, page 3-34
- Verifying Crypto Access Lists, page 3-35
- Defining Transform Sets and Configuring IPSec Tunnel Mode, page 3-36
- Verifying Transform Sets and IPSec Tunnel Mode, page 3-37

Note When using IPSec with L2TP, do not configure IPSec tunnel mode.

- Creating Crypto Map Entries, page 3-39
- Verifying Crypto Map Entries, page 3-43
- Applying Crypto Maps to Interfaces, page 3-44
- Verifying Crypto Map Interface Associations, page 3-46

Note Although the configuration instructions in the listed sections refer to the "Extranet Scenario" section on page 3-5, the same configuration instructions apply to the remote access scenario described in the "Scenario Description" section on page 4-2.

Configuring Cisco IOS Firewall Authentication Proxy

Using the Cisco IOS firewall authentication proxy feature, network administrators can apply specific security policies on a per-user basis. Users can be identified and authorized on the basis of their per-user policy, and access privileges tailored on an individual basis are possible, in contrast with general policy applied across multiple users.

With the authentication proxy feature, users can log into the network or access the Internet via HTTP, and their specific access profiles are automatically retrieved and applied from an authentication server. The user profiles are active only when there is active traffic from the authenticated users.

The authentication proxy is compatible with Network Address Translation (NAT), Context-based Access Control (CBAC), IP Security (IPSec) encryption, and VPN client software.

This section contains basic steps to configure the Cisco IOS Firewall Authentication Proxy and includes the following tasks:

- Configuring Authentication, Authorization, and Accounting
- Configuring the HTTP Server
- Configuring the Authentication Proxy
- Verifying the Authentication Proxy

Configuring Authentication, Authorization, and Accounting

You must configure the authentication proxy for Authentication, Authorization, and Accounting (AAA) services. Use the following commands in global configuration mode to enable authorization and to define the authorization methods:

	Command	Purpose
Step 1	`hq-sanjose(config)# aaa new-model`	Enables the AAA functionality on the router.
Step 2	`hq-sanjose(config)# aaa authentication login default` *TACACS+ RADIUS*	Defines the list of authentication methods at login.
Step 3	`hq-sanjose(config)# aaa authorization auth-proxy default` [*method1* [*method2...*]]	Enables authentication proxy for AAA methods.
Step 4	`hq-sanjose(config)# tacacs-server host` *hostname*	Specifies an AAA server. For RADIUS servers, use the **radius server host** command.
Step 5	`hq-sanjose(config)# tacacs-server key` *sting*	Sets the authentication and encryption key for communications between the router and the AAA server. For RADIUS servers use the **radiusserverkey** command.
Step 6	`hq-sanjose(config)# access-list` *access-list-number* **permit** *tcp* **host** *source* **eq** *tacacs* **host** *destination*	Creates an ACL entry to allow the AAA server return traffic to the firewall. The source address is the IP address of the AAA server, and the destination address is the IP address of the router interface where the AAA server resides.

In addition to configuring AAA on the firewall router, the authentication proxy requires a per-user access profile configuration on the AAA server. To support the authentication proxy, configure the AAA authorization service “auth-proxy” on the AAA server as outlined here:

- Define a separate section of authorization for **auth-proxy** to specify the downloadable user profiles. This does not interfere with other types of service, such as EXEC. The following example shows a user profile on a TACACS server:

```
default authorization = permit
key = cisco
user = newuser1 {
login = cleartext cisco
service = auth-proxy
{
priv-lvl=15
proxyacl#1="permit tcp any any eq 26"
proxyacl#2="permit icmp any host 60.0.0.2″
proxyacl#3="permit tcp any any eq ftp"
proxyacl#4="permit tcp any any eq ftp-data"
proxyacl#5="permit tcp any any eq smtp"
proxyacl#6="permit tcp any any eq telnet"
```

- The only supported attribute in the AAA server user configuration is **proxyacl#***n*. Use the **proxyacl#***n* attribute when configuring the access lists in the profile. The attribute **proxyacl#***n* is for both RADIUS and TACACS+ attribute-value (AV) pairs.
- The privilege level must be set to 15 for all users.
- The access lists in the user profile on the AAA server must have **permit** only access commands.
- Set the source address to **any** in each of the user profile access list entries. The source address in the access lists is replaced with the source address of the host making the authentication proxy request when the user profile is downloaded to the firewall.
- The supported AAA servers are CiscoSecure ACS 2.1.x for Window NT (where x is a number 0 to 12) and CiscoSecure ACS 2.3 for Windows NT, CiscoSecure ACS 2.2.4 for UNIX and CiscoSecure ACS 2.3 for UNIX, TACACS+ server (vF4.02.alpha), Ascend RADIUS server - radius-980618 (required avpair patch), and Livingston RADIUS server (v1.16).

Configuring the HTTP Server

To use the authentication proxy, you must also enable the HTTP server on the firewall and set the HTTP server authentication method to use AAA. Enter the following commands in global configuration mode:

	Command	Purpose
Step 1	`hq-sanjose(config)# ip http server`	Enables the HTTP server on the router. The authentication proxy uses the HTTP server to communicate with the client for user authentication.
Step 2	`hq-sanjose(config)# ip http authentication aaa`	Sets the HTTP server authentication method to AAA.
Step 3	`hq-sanjose(config)# ip http access-class` *access-list-number*	Specifies the access list for the HTTP server.

Configuring the Authentication Proxy

To configure the authentication proxy, use the following commands beginning in global configuration mode:

	Command	Purpose
Step 1	`hq-sanjose(config)# ip auth-proxy auth-cache-time` *min*	Sets the global authentication proxy idle timeout value in minutes. If the timeout expires, user authentication entries are removed, along with any associated dynamic access lists. The default value is 60 minutes.
Step 2	`hq-sanjose(config)# ip auth-proxy auth-proxy-banner`	(Optional) Displays the name of the firewall router on the authentication proxy login page. The banner is disabled by default.

	Command	Purpose
Step 3	`hq-sanjose(config)# ip auth-proxy name` *auth-proxy-name* **http** [**auth-cache-time** *min*] [**list** *std-access-list*]	Creates authentication proxy rules. The rules define how you apply authentication proxy. This command associates connection initiating HTTP protocol traffic with an authentication proxy name. You can associate the named rule with an access control list, providing control over which hosts use the authentication proxy feature. If no standard access list is defined, the named authentication proxy rule intercepts HTTP traffic from all hosts whose connection initiating packets are received at the configured interface. (Optional) The **auth-cache-time** option overrides the global authentication proxy cache timer. This option provides more control over timeout values for a specific authentication proxy rule. If no value is specified, the proxy rule assumes the value set with the **ip auth-proxy auth-cache-time** command. (Optional) The **list** option allows you to apply a standard access list to a named authentication proxy rule. HTTP connections initiated from hosts in the access list are intercepted by the authentication proxy.
Step 4	`hq-sanjose(config)# interface` *type*	Enters interface configuration mode by specifying the interface type on which to apply the authentication proxy.
Step 5	`hq-sanjose(config-if)# ip auth-proxy` *auth-proxy-name*	In interface configuration mode, applies the named authentication proxy rule at the interface. This command enables the authentication proxy rule with that name.

Verifying the Authentication Proxy

To check the current authentication proxy configuration, use the **show ip auth-proxy configuration** command in privileged EXEC mode. In the following example, the global authentication proxy idle timeout value is set to 60 minutes, the named authentication proxy rule is "pxy," and the idle timeout value for this named rule is 1 minute. The display shows that no host list is specified, meaning that all connections initiating HTTP traffic at the interface are subject to the authentication proxy rule:

```
router# show ip auth-proxy configuration
Authentication cache time is 60 minutes
Authentication Proxy Rule Configuration
Auth-proxy name pxy
http list not specified auth-cache-time 1 minutes
```

To verify that the authentication proxy is successfully configured on the router, ask a user to initiate an HTTP connection through the router. The user must have authentication and authorization configured at the AAA server. If the user authentication is successful, the firewall completes the HTTP connection for the user. If the authentication is unsuccessful, check the access list and the AAA server configurations.

Display the user authentication entries using the **show ip auth-proxy cache** command in privileged EXEC mode. The authentication proxy cache lists the host IP address, the source port number, the timeout value for the authentication proxy, and the state of the connection. If the authentication proxy state is HTTP_ESTAB, the user authentication was successful.

```
router# show ip auth-proxy cache
Authentication Proxy Cache
Client IP 192.168.25.215 Port 57882, timeout 1, state HTTP_ESTAB
```

Wait for one minute, which is the timeout value for this named rule, and ask the user to try the connection again. After one minute, the user connection is denied because the authentication proxy has removed the user authentication entry and any associated dynamic ACLs. The user is presented with a new authentication login page and must log in again to gain access through the firewall.

Comprehensive Configuration Examples

This section contains PPTP/MPPE, and L2TP/IPSec comprehensive sample configurations for the headquarters gateway.

PPTP/MPPE Configuration

```
hq-sanjose# show running-config

Current configuration
!
version 12.0
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname mp12
!
no logging console guaranteed
enable password lab
!
username tester41 password 0 lab41
!
ip subnet-zero
no ip domain-lookup
!
vpdn enable
!
vpdn-group 1
! Default PPTP VPDN group
accept-dialin
  protocol pptp
  virtual-template 1
local name cisco_pns
!
memory check-interval 1
!
controller ISA 5/0
encryption mppe
!
process-max-time 200
!
interface FastEthernet0/0
ip address 10.1.3.3 255.255.255.0
no ip directed-broadcast
```

```
duplex auto
speed auto
!
interface FastEthernet0/1
ip address 10.1.6.4 255.255.255.0
no ip directed-broadcast
duplex auto
speed auto
!
interface Serial1/0
no ip address
no ip directed-broadcast
shutdown
framing c-bit
cablelength 10
dsu bandwidth 44210
!
interface Serial1/1
no ip address
no ip directed-broadcast
shutdown
framing c-bit
cablelength 10
dsu bandwidth 44210
!
interface FastEthernet4/0
no ip address
no ip directed-broadcast
shutdown
duplex half
!
interface Virtual-Template1
ip unnumbered FastEthernet0/0
no ip directed-broadcast
ip mroute-cache
no keepalive
ppp encrypt mppe 40
ppp authentication ms-chap
!
ip classless
ip route 172.29.1.129 255.255.255.255 1.1.1.1
ip route 172.29.63.9 255.255.255.255 1.1.1.1
no ip http server
!
line con 0
exec-timeout 0 0
transport input none
line aux 0
```

```
line vty 0 4
login
!
aaa new-model
aaa authentication login default tacacs+ radius
!Set up the aaa new model to use the authentication proxy.
aaa authorization auth-proxy default tacacs+ radius
!Define the AAA servers used by the router
tacacs-server host 172.31.54.143
tacacs-server key cisco
radius-server host 172.31.54.143
radius-server key cisco
!
! Enable the HTTP server on the router:
ip http server
! Set the HTTP server authentication method to AAA:
ip http authentication aaa
!Define standard access list 61 to deny any host.
access-list 61 deny any
! Use ACL 61 to deny connections from any host to the HTTP server.
ip http access-class 61
!
!set the global authentication proxy timeout value.
ip auth-proxy auth-cache-time 60
!Apply a name to the authentication proxy configuration rule.
ip auth-proxy name HQ_users http
!
! Apply the authentication proxy rule at an interface.
interface e0
    ip address 10.1.1.210 255.255.255.0
    ip auth-proxy HQ_users
!
end
```

L2TP/IPSec Configuration

```
hq-sanjose# show running-config

Current configuration:
 !
 version 12.0
 service timestamps debug uptime
 service timestamps log uptime
 no service password-encryption
 !
 hostname LNS
```

```
!
enable password ww
!
username LNS password 0 tunnelpass
username test@cisco.com password 0 cisco
ip subnet-zero
!
vpdn enable
!
vpdn-group 1
 accept dialin l2tp virtual-template 1 remote LAC
 local name LNS
!
crypto isakmp policy 1
 authentication pre-share
 group 2
 lifetime 3600
crypto isakmp key cisco address 172.1.1.1
!
crypto ipsec transform-set testtrans esp-des
!
 !
 crypto map l2tpmap 10 ipsec-isakmp
 set peer 172.1.1.1
 set transform-set testtrans
 match address 101
!
interface Ethernet 0/0
 ip address 10.1.3.3 255.255.255.0
 no ip directed-broadcast
 no keepalive
!
interface Ethernet 0/1
 no ip address
 no ip directed-broadcast
 shutdown
!
interface Virtual-Template1
 ip unnumbered Ethernet0
 no ip directed-broadcast
 no ip route-cache
 peer default ip address pool mypool
 ppp authentication chap
!
interface Serial 1/0
 ip address 172.17.2.4 255.255.255.0
 no ip directed-broadcast
 no ip route-cache
```

```
 no ip mroute-cache
 no fair-queue
 clockrate 1300000
 crypto map l2tpmap
!
interface Serial 0/0
 no ip address
 no ip directed-broadcast
 shutdown
!
ip local pool mypool 172.16.3.1 172.20.10.10
no ip classless
!
access-list 101 permit udp host 172.17.2.4 eq 1701 host 172.1.1.1 eq
1701
!
line con 0
 exec-timeout 0 0
 transport input none
line aux 0
line vty 0 4
 password cisco
 login
!
aaa new-model
aaa authentication login default tacacs+ radius
!Set up the aaa new model to use the authentication proxy.
aaa authorization auth-proxy default tacacs+ radius
!Define the AAA servers used by the router
tcacs-server host 172.31.54.143
tacacs-server key cisco
radius-server host 172.31.54.143
radius-server key cisco
!
! Enable the HTTP server on the router:
ip http server
! Set the HTTP server authentication method to AAA:
ip http authentication aaa
!Define standard access list 61 to deny any host.
access-list 61 deny any
! Use ACL 61 to deny connections from any host to the HTTP server.
ip http access-class 61
!
!set the global authentication proxy timeout value.
ip auth-proxy auth-cache-time 60
!Apply a name to the authentication proxy configuration rule.
ip auth-proxy name HQ_users http
!
```

```
! Apply the authentication proxy rule at an interface.
interface e0
   ip address 10.1.1.210 255.255.255.0
   ip auth-proxy HQ_users
!
end
```