



Exam Topics Discussed in This Chapter

This chapter covers the following topics, which you need to master in your pursuit of certification as a Cisco Certified Security Professional:

- 9** Overview of remote access using preshared keys
- 10** Initial configuration of the Cisco VPN 3000 Concentrator Series for remote access
- 11** Browser configuration of the Cisco VPN 3000 Concentrator Series
- 12** Configuring users and groups
- 13** Advanced configuration of the Cisco VPN 3000 Concentrator Series
- 14** Configuring the IPSec Windows Client

Configuring Cisco VPN 3000 for Remote Access Using Preshared Keys

From a procedural perspective, it is easier to configure the Cisco VPN 3000 Concentrator Series for remote access using preshared keys. While the alternative method is to use the services of a Certificate Authority (CA), that method entails additional steps. Using preshared keys, the client only needs to know the address of the VPN concentrator and the shared secret key.

While VPN configuration is relatively easy with preshared keys, this manual process does not scale well for large implementations. The VPN administrator must provide the password and implementation instructions to prospective users. This could be accomplished by preconfiguring client software on a floppy disk or CD-ROM, but even that process can be labor intensive in large implementations.

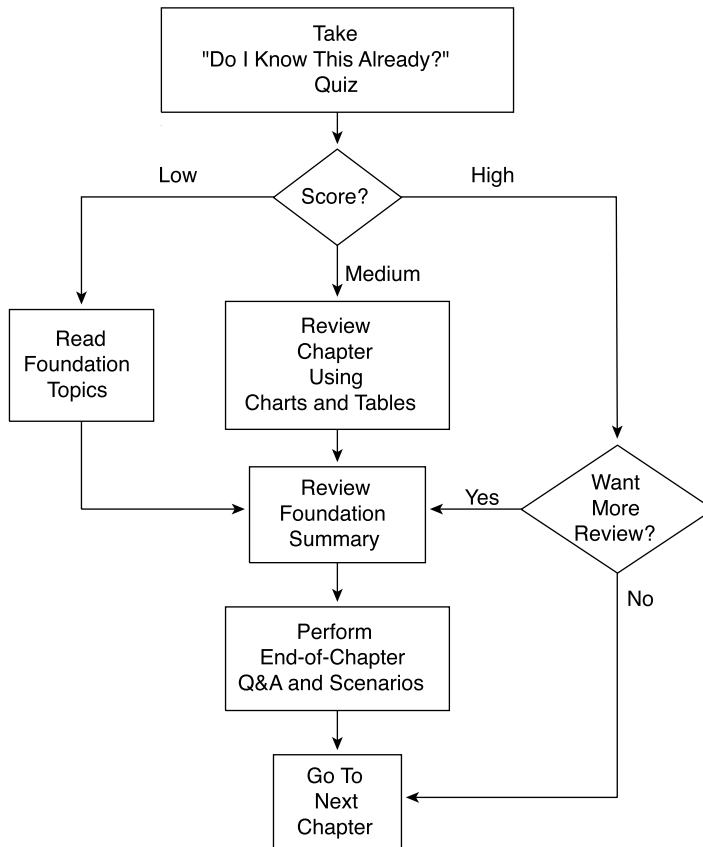
Once all of your users have successfully configured their remote systems with the current shared key, the process of changing passwords periodically, as every good security plan requires, would require notifying all users of the new password and providing modification instructions. You can imagine how it would be easy to forget about this important security consideration.

While scaling VPN implementations can be better handled by using CA support and digital certificates, preshared keys are easy to implement and can be used in many applications. This chapter discusses the process of implementing Internet Protocol Security (IPSec) using preshared keys on the Cisco VPN 3000 Series Concentrators. The clever graphical user interface (GUI) makes the implementation process easy.

How to Best Use This Chapter

By taking the following steps, you can make better use of your time:

- Keep your notes and answers for all your work with this book in one place for easy reference.
- Take the “Do I Know This Already?” quiz, and write down your answers. Studies show retention is significantly increased through writing facts and concepts down, even if you never look at the information again.
- Use the diagram in Figure 4-1 to guide you to the next step.

Figure 4-1 *How to Use This Chapter*

“Do I Know This Already?” Quiz

The purpose of the “Do I Know This Already?” quiz is to help you decide what parts of the chapter to use. If you already intend to read the entire chapter, you do not need to answer these questions now.

This 24-question quiz helps you determine how to spend your limited study time. The quiz is sectioned into six smaller “quizlets,” which correspond to the six major topic headings in the chapter. Figure 4-1 outlines suggestions on how to spend your time in this chapter based on your quiz score. Use Table 4-1 to record your scores.

Table 4-1 *Score Sheet for Quiz and Quizlets*

Quizlet Number	Foundations Topics Section Covering These Questions	Questions	Score
1	Overview of remote access using preshared keys	1–4	
2	Initial configuration of the Cisco VPN 3000 Concentrator Series for remote access	5–8	
3	Browser configuration of the Cisco VPN 3000 Concentrator Series	9–12	
4	Configuring users and groups	13–16	
5	Advanced configuration of the Cisco VPN 3000 Concentrator Series	17–20	
6	Configuring the IPSec Windows Client	21–24	
All questions		1–24	

1 What methods can you use for user authentication on the Cisco VPN 3000 Series Concentrators?

2 What methods can you use for device authentication between VPN peers?

3 What are the three types of preshared keys?

4 What is a unique preshared key?

- 5 When you boot up a Cisco VPN 3000 Concentrator with the default factory configuration, what happens?

- 6 What information do you need to supply in the command-line interface (CLI) portion of Quick Configuration?

- 7 Which interface do you need to configure using the browser-based VPN Manager?

- 8 What is the default administrator name and password for VPN concentrators?

- 9 How do you get your web browser to connect to the VPN concentrator's Manager application?

- 10 What is the default administrator name and password for the GUI VPN Manager?

11 What are the three major sections of the VPN Manager system?

12 What hot keys are available in the standard toolbar of the VPN Manager?

13 From where do users inherit attributes on the VPN concentrator?

14 How many groups can a user belong to in the VPN concentrator's internal database?

15 What is an external group in the VPN Manager system?

16 When reviewing the list of attributes for a group, what does it mean when an attribute's Inherit? box is checked?

17 What are the nine subcategories under the Configuration | System option in the VPN Manager's table of contents?

18 Where would you configure information for Network Time Protocol (NTP) and Dynamic Host Configuration Protocol (DHCP) servers within the VPN Manager?

19 What tunneling protocol can you configure on the VPN concentrator to support the Microsoft Windows 2000 VPN Client?

20 What dynamic routing protocols are available on the VPN 3000 Concentrators?

21 What Microsoft Windows operating systems can support the Cisco VPN Client?

22 How do you start the Cisco VPN Client on a Windows system?

23 How do you start the Cisco VPN Client installation process?

24 What variables can you supply during the installation process of the Cisco VPN Client?

The answers to this quiz are listed in Appendix A, “Answers to the “Do I Know This Already?” Quizzes and Q&A Sections.” The suggestions for your next steps, based on quiz results, are as follows:

- **2 or less score on any quizlet**—Review the appropriate parts of the “Foundation Topics” section of this chapter, based on Table 4-1. Then proceed to the section, “Foundation Summary,” the section, “Q&A,” and the scenarios at the end of the chapter.
- **12 or less overall score**—Read the entire chapter, including the “Foundation Topics” and “Foundation Summary” sections, the “Q&A” section, and the scenarios at the end of the chapter.
- **13 to 18 overall score**—Begin with the section, “Foundation Summary,” continue with the section, “Q&A,” and read the scenarios. If you are having difficulty with a particular subject area, read the appropriate section in the “Foundation Topics” section.
- **19 or more overall score**—If you feel you need more review on these topics, go to the “Foundation Summary” section, then to the “Q&A” section, then to the scenarios. Otherwise, skip this chapter and go to the next chapter.

Foundation Topics

Using VPNs for Remote Access with Preshared Keys

9 Overview of remote access using preshared keys

For site-to-site VPN connections, peer devices must authenticate one another before IPSec communications can occur. In addition to requiring device authentication, remote access VPN connections require user authentication to make certain that the user is permitted to use the applications that are protected by the IPSec connection.

User authentication can be handled in a variety of ways. You can configure Remote Authentication Dial-In User Service (RADIUS), NT Domain, and Security Dynamics International (SDI) authentication on most Cisco devices, and the VPN 3000 Concentrators have the additional ability to authenticate users through an internal database.

If you want to use internal authentication, create a username and password for each user and assign the users to the group that is to be used for IPSec device authentication. Once the devices have established the IPSec tunnel, the user is prompted to enter a username and password to continue. Failure to authenticate causes the tunnel to drop. A similar login prompt is displayed if you are using RADIUS, NT Domain, or SDI authentication.

You can establish device authentication by using either preshared keys or digital certificates. (For more information, see Chapter 5, “Configuring Cisco VPN 3000 for Remote Access Using Digital Certificates.”) With preshared keys, the system administrator chooses the key and then shares that key with users or other system administrators. Combining a preshared key with some other metric establishes three different uses for preshared keys, as follows:

- Unique
- Group
- Wildcard

The following sections describe each type of preshared key in more detail.

Unique Preshared Keys

When a preshared key is tied to a specific IP address, the combination makes the preshared key unique. Only the peer with the correct IP address can establish an IPSec session using this key. Ideal for site-to-site VPNs where the identity of the peer devices is always known, unique preshared keys are not recommended for remote access VPNs. Unique preshared keys scale particularly poorly because each new user requires a new key and the administrative burden that entails.

While this type of preshared key is the most secure of the three types, it is not practical for remote access applications, where users are typically connecting through a commercial Internet service provider (ISP). Most users are not willing to pay for the luxury of a permanently assigned IP address from their ISP and are assigned an IP address from an available pool of addresses when they connect to the service. If you had a large installed base of VPN users, keeping up with these dynamically assigned IP addresses to provide this level of security would be a maintenance nightmare.

Group Preshared Keys

If you begin using unique preshared keys, at some point you can decide to just use the same password for discrete groups of users. If you decide to do that, and shed the association with the IP address, you have begun to use the next type of preshared key, the group preshared key. A group preshared key is simply a shared key that is associated with a specific group. In a VPN 3000 Concentrator configuration, the group can be the Base Group or any other group that you define.

A group preshared key is well suited for remote access VPNs and is the method used by Cisco VPN 3000 Concentrators. It is good practice to use groups to establish Internet Key Exchange (IKE) and IPSec settings and to provide other capabilities that are unique to a specific set of users. If you choose to use the Cisco VPN 3000 Concentrator's internal database for user authentication, you can assign your users to specific groups, making the process of managing preshared keys much easier.

Wildcard Preshared Keys

The final type of preshared key classification is the wildcard preshared key. This type of key does not have an IP address or group assigned to it and can be used by any device holding the key to establish an IPSec connection with your VPN concentrator. When you set up your concentrator to use wildcard preshared keys, every device connecting to the concentrator must also use preshared keys. If any device is compromised, you must change the key for all the devices in your network. This type of key is also open to man-in-the-middle attacks and should not be used for site-to-site applications.

NOTE

Man-in-the-middle attacks happen when an intruder has access to data packets that are in transit between connection endpoints. The intruder can then modify information within the packets in an attempt to gain access to the endpoints or for some other nefarious purpose. The intruder might just extract information from the packets. Obtaining a wildcard preshared key this way would permit an attacker to establish a VPN connection to the host from any other system.

VPN Concentrator Configuration

- 10 Initial configuration of the Cisco VPN 3000 Concentrator Series for remote access
- 11 Browser configuration of the Cisco VPN 3000 Concentrator Series
- 12 Configuring users and groups
- 13 Advanced configuration of the Cisco VPN 3000 Series Concentrator

Three major categories of activities that should be performed on network devices are configuration, administration, and monitoring. The browser-based VPN 3000 Concentrator Series Manager was designed with those functions in mind. The remainder of this chapter focuses on the configuration capabilities of the VPN concentrator.

Remote access VPNs can be established with minimal equipment. Most of your users connect through the Internet, so their infrastructure costs are minimal. While you should place the concentrator behind or in parallel with a firewall, you could establish a robust VPN network with just a border router and your concentrator.

Administration requirements for the Cisco VPN 3000 Concentrator Series are fairly standard. You could configure the concentrators completely from the CLI using either a directly connected console monitor or by Telnetting to the concentrator. However, the best option for configuring this series of concentrators is through the GUI that you access through a web browser.

Microsoft Internet Explorer version 4.0 or higher is the recommended browser to use, but you can also use Netscape Navigator/Communicator version 4.0 or higher. You must enable the use of JavaScript and cookies in the browser application in order for the Cisco VPN 3000 Concentrator Manager to work properly. Nothing needs to be installed on your workstation other than the browser software.

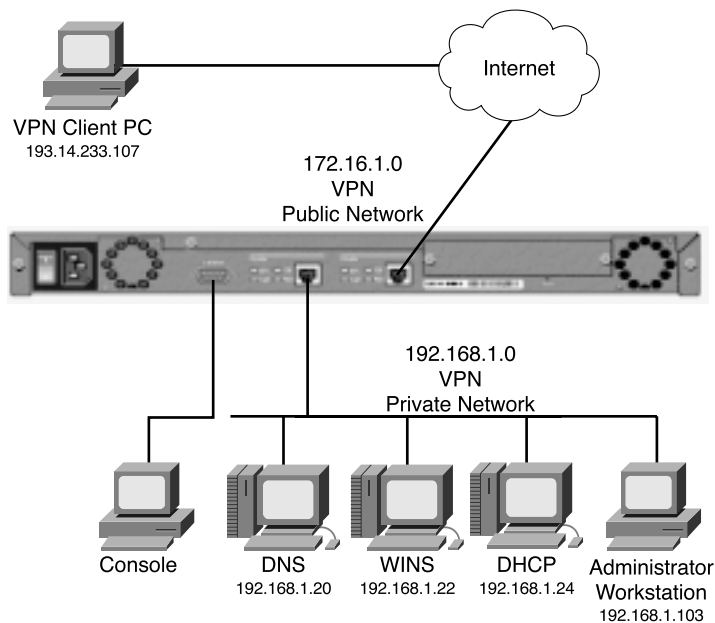
This section covers the following topics:

- Cisco VPN 3000 Concentrator configuration requirements
- Cisco VPN 3000 Concentrator initial configuration
- Configuring IPSec with preshared keys through the VPN 3000 Concentrator Series Manager
- Advanced configuration of the VPN concentrator

Cisco VPN 3000 Concentrator Configuration Requirements

Figure 4-2 shows a typical VPN concentrator configuration using a Cisco VPN 3005 Concentrator. The Public interface connects to the Internet through a security device such as a firewall or border router (not shown in this diagram). The Private interface connects to the local network, in this case supporting Domain Name System (DNS), Windows Internet Naming Service (WINS), and DHCP servers. On those models that have a third interface, you can establish a demilitarized zone (DMZ), which could contain some of these elements and, most likely, your Internet server. Connection to the Public and Private 10/100-Mbps Ethernet interfaces is done using UTP/STP CAT-5 cabling with RJ-45 connectors.

Figure 4-2 *VPN 3005 Concentrator Configuration*



You need to attach a console for the initial configuration. The console port takes a standard straight-through RS-232 serial cable with a female DB-9 connector, which Cisco supplies with the system. Once the Private interface has been configured, you can access the concentrator from your administrator workstation using a web browser such as Internet Explorer or Netscape Navigator.

In addition to the physical connections, you also need to plan your IKE phase 1 and phase 2 settings. If you are going to be using preshared keys, you must select that key as well. The

following is a list of the data values you need to obtain to completely configure your Cisco VPN 3000 Series Concentrator:

- Private interface IP address, subnet mask, speed, and duplex mode.
- Public interface IP address, subnet mask, speed, and duplex mode.
- VPN concentrator's device or system name.
- System date and time of day.
- VPN tunnel protocol that you will use, either IPSec, PPTP, or L2TP.
- Your local DNS server's IP address.
- Your registered domain name.
- The IP address or host name for the concentrator's default gateway.
- (Optional) Additional interfaces (for example, for a DMZ, on models 3015–3080 only), IP addresses, subnet masks, speed, and duplex mode.
- (Optional) IP address or host name of your DHCP server, if your concentrator will be using DHCP to assign addresses to remote users.
- (Optional) A pool of IP addresses if the VPN concentrator will be assigning addresses to remote users.
- (Optional) For external RADIUS user authentication, the IP address or host name, port number, and server secret or password for the RADIUS server.
- (Optional) For external Windows NT Domain user authentication, the IP address, port number, and Primary Domain Controller (PDC) host name for your domain.
- (Optional) For external SDI user authentication, the IP address and port number for the SDI server.
- (Optional) For internal VPN concentrator user authentication, the username and password for each user. If you specify per-user address assignment, you also need the IP address and subnet mask for each user.
- (Optional) For the IPSec tunneling protocol, a name and password for the IPSec tunnel group.

Cisco VPN 3000 Concentrator Initial Configuration

When the Cisco VPN 3000 Concentrator is powered on for the first time, it boots up the factory default configuration, which offers a Quick Configuration option. The data requested by the Quick Configuration mode are enough to make the concentrator operational. Once you have the basic configuration entered through this mode, you can fine-tune the configuration through normal menu options.

The Quick Configuration can be accomplished from the CLI, but the HTML version of the concentrator manager provides a more intuitive tool for performing the essential configuration of the concentrator. The Quick Configuration steps are as follows:

- Step 1** CLI: Set the system time, date, and time zone.
- Step 2** CLI: Enable network access for your web browser by setting the Private interface's IP address, subnet mask, speed, and duplex mode.
- Step 3** Browser: Configure the Public interface and any other Ethernet or WAN interfaces of the concentrator. To do that, you need to set the IP address, subnet mask, speed, and duplex mode for each of these interfaces.
- Step 4** Browser: Identify the system by supplying system name, date, time, DNS, domain name, and default gateway.
- Step 5** Browser: Select the tunneling protocol to use and the encryption options.
- Step 6** Browser: Identify the method the concentrator is to use for assigning IP addresses to clients as a tunnel is established.
- Step 7** Browser: Select the type of user authentication to use, and provide the identity of the authentication server. You can choose to authenticate from the internal server, RADIUS, NT Domain, or SDI.
- Step 8** (Optional) Browser: When using the internal authentication server, populate the internal user database with group and user identities.
- Step 9** (Optional) Browser: When using IPsec as the tunneling protocol, assign a name and password to the IPsec tunnel group.
- Step 10** (Optional, but recommended) Browser: Change the admin password for security.
- Step 11** Browser: Save the configuration settings.

Quick Configuration Using the CLI

The VPN 3000 Concentrator enters into Quick Configuration mode the first time it is powered up. Quick Configuration is a configuration wizard that guides you through the initial configuration settings. To begin performing the 11 steps outlined above from the CLI, connect your console to the concentrator and power on the concentrator. As the system boots, various information is displayed on the console screen. After the system has performed the boot functions, you should see the login prompt. When prompted, supply the default administrator login name of **admin** and the default password, which is also **admin**. Note that the password is not displayed on the console screen as you type it, as shown in the following CLI output.

```
Login: admin
Password:
```

Once you have entered the correct login name and password, the concentrator displays a welcome screen, as shown in Example 4-1.

Example 4-1 *Quick Configuration Welcome Screen*

```
                Welcome to
                Cisco Systems
                VPN 3000 Concentrator Series
                Command Line Interface
                Copyright (C) 1998-2001 Cisco Systems, Inc.

-- : Set the time on your device. The correct time is very important,
-- : so that logging and accounting entries are accurate.

-- : Enter the system time in the following format:
-- :      HH:MM:SS. Example 21:30:00 for 9:30 PM

> Time

Quick -> [ 08:57:13 ]
```

Setting the System Time, Date, and Time Zone

At this point, the concentrator is waiting for you to verify the current time by pressing Enter or to type in a new time, as shown in Example 4-2. Notice that the system prompt changes to Quick -> to indicate that the system is waiting for you to confirm or enter data. The following example also shows the entries that are required (in boldface type) to complete the configuration of the date, time zone, and daylight-savings time support information.

Example 4-2 *Setting the System Time and Date*

```
Quick -> [ 08:57:13 ] 08:15:22

-- : Enter the date in the following format.
-- : MM/DD/YYYY Example 06/12/1999 for June 12th 1999.

> Date

Quick -> [ 03/29/2002 ] 09/01/2002

-- : Set the time zone on your device. The correct time zone is very
-- : important so that logging and accounting entries are accurate.

-- : Enter the time zone using the hour offset from GMT:
-- : -12 : Kwajalein  -11 : Samoa    -10 : Hawaii    -9 : Alaska
-- :  -8 : PST       -7 : MST      -6 : CST       -5 : EST
-- :  -4 : Atlantic  -3 : Brasilia -2 : Mid-Atlantic -1 : Azores
```

Example 4-2 *Setting the System Time and Date (Continued)*

```

-- : 0 : GMT          +1 : Paris    +2 : Cairo      +3 : Kuwait
-- : +4 : Abu Dhabi   +5 : Karachi   +6 : Almaty     +7 : Bangkok
-- : +8 : Singapore  +9 : Tokyo     +10 : Sydney    +11 : Solomon Is.
-- : +12 : Marshall Is.

> Time Zone

Quick -> [ 0 ] -6

1) Enable Daylight Savings Time Support
2) Disable Daylight Savings Time Support

Quick -> [ 1 ] 2

```

Configuring the Private LAN Interface

The next phase of the CLI Quick Configuration steps is to configure the Private LAN interface. This is simply a matter of setting the IP address and subnet mask information and then specifying the speed and duplex mode to use for the interface. Those steps are shown in the output in Example 4-3, which is displayed as soon as you enter your preference for daylight-savings support.

Example 4-3 *Configuring the Private Interface*

```

This table shows current IP addresses.

  Intf          Status          IP Address/Subnet Mask          MAC Address
-----
Ether1-Pri|Not Configured|      0.0.0.0/0.0.0.0          |
Ether2-Pub|Not Configured|      0.0.0.0/0.0.0.0          |
-----

DNS Server(s): DNS Server Not Configured
DNS Domain Name:
Default Gateway: Default Gateway Not Configured

** An address is required for the private interface. **

> Enter IP Address

Quick Ethernet 1 -> [ 0.0.0.0 ] 192.168.1.3

Waiting for Network Initialization...

> Enter Subnet Mask

Quick Ethernet 1 -> [ 255.255.255.0 ]

1) Ethernet Speed 10 Mbps

```

continues

Example 4-3 *Configuring the Private Interface (Continued)*

```
2) Ethernet Speed 100 Mbps
3) Ethernet Speed 10/100 Mbps Auto Detect

Quick Ethernet 1 -> [ 3 ] 2

1) Enter Duplex - Half/Full/Auto
2) Enter Duplex - Full Duplex
3) Enter Duplex - Half Duplex

Quick Ethernet 1 -> [ 1 ] 2

1) Modify Ethernet 1 IP Address (Private)
2) Modify Ethernet 2 IP Address (Public)
3) Save changes to Config file
4) Continue
5) Exit
```

In Example 4-3, the administrator wanted to use a 24-bit subnet mask. When he entered a Class C IP address for the interface, the system automatically brought up the 24-bit Class C default subnet mask. The administrator simply pressed Enter to accept this subnet mask setting. Also notice that the administrator explicitly set the speed of the interface to 100 Mbps and to Full Duplex rather than accepting the default automatic detection settings.

From the menu displayed at the end of the previous output display, you can see that you have the option of also configuring the Public interface. If the hardware configuration had additional interfaces, you would see menu options for configuring those interfaces, too.

The browser-based manager is the configuration tool of choice for the VPN 3000 Concentrator. The CLI is used only to enable network connectivity so that you can communicate with the concentrator through the network from your administration workstation. Configuration of additional interfaces and all remaining concentrator settings is accomplished through the browser-based manager.

To finish the CLI initial configuration of the VPN concentrator, simply save your changes to the Config file and then exit the Quick Configuration mode. Those steps are shown in the output in Example 4-4.

Example 4-4 *Saving Configuration Settings and Exiting the CLI*

```
1) Modify Ethernet 1 IP Address (Private)
2) Modify Ethernet 2 IP Address (Public)
3) Save changes to Config file
4) Continue
5) Exit

Quick -> 3

1) Modify Ethernet 1 IP Address (Private)
```

Example 4-4 *Saving Configuration Settings and Exiting the CLI (Continued)*

```

2) Modify Ethernet 2 IP Address (Public)
3) Save changes to Config file
4) Continue
5) Exit

Quick -> 5

```

The concentrator only presents the Quick Configuration process upon initial bootup using the default configuration. After you have configured the concentrator, the normal CLI menus look as follows:

Model 3005 menu:

```

1) Modify Ethernet 1 IP Address (Private)
2) Modify Ethernet 2 IP Address (Public)
3) Configure Expansion Cards
4) Save changes to Config file
5) Continue
6) Exit

Quick -> _

```

Model 3015–3080 menu:

```

1) Modify Ethernet 1 IP Address (Private)
2) Modify Ethernet 2 IP Address (Public)
3) Modify Ethernet 3 IP Address (External)
4) Configure Expansion Cards
5) Save changes to Config file
6) Continue
7) Exit

Quick -> _

```

If you need to go through the Quick Configuration again for any reason, simply select the **Reboot with Factory/Default Configuration** option from the **Administration | System Reboot** menu in the VPN 3000 Concentrator Manager.

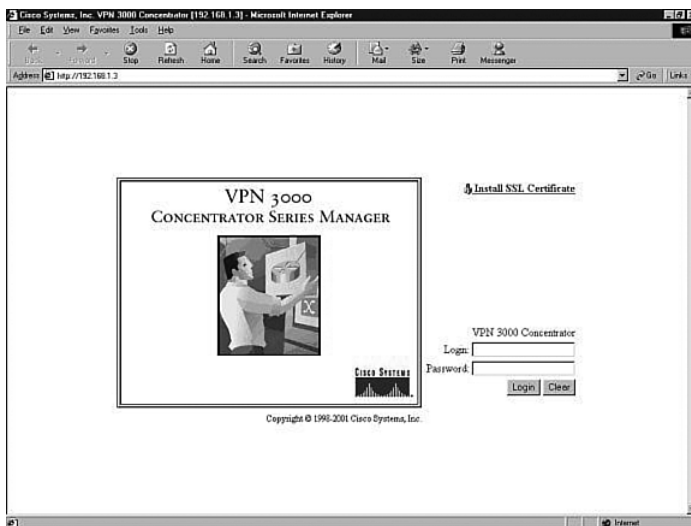
This finishes the CLI configuration steps. The remainder of the configuration steps are completed using the Cisco VPN 3000 Concentrator Manager application that is resident on each VPN concentrator and is accessible using the web browser on your administrator PC.

Quick Configuration Using the Browser-Based Manager

Now that you have configured the Private interface on the VPN concentrator, make sure that your workstation has an IP address on the same subnet as the concentrator and verify that you can reach the concentrator by pinging to it from the workstation. Once you have verified connectivity, open your web browser application and connect to the concentrator by entering the IP address of the concentrator in the Address field of the browser, as shown in Figure 4-3.

Figure 4-3 *HTTP Addressing for VPN 3000 Concentrator Series Manager*

The browser connects to the VPN concentrator and presents the initial login screen, as shown in Figure 4-4.

Figure 4-4 *VPN 3000 Concentrator Series Manager Login Screen*

Notice the hotlink option on the screen labeled Install SSL Certificate. You can use Secure Sockets Layer (SSL) encryption to establish a secure session between your management workstation and the concentrator. Using this secure session capability encrypts all VPN Manager communications with the concentrator at the IP socket level. SSL uses the HTTPS protocol and uses `https://` addressing on the browser. You might want to use SSL if your VPN Manager workstation connects to the concentrator across a public network. There can be a slight performance penalty when using SSL, depending on the capability of the administration workstation, but it should not be a serious consideration for management functions.

When the VPN concentrator boots for the first time, it generates a self-signed SSL server certificate. To use SSL with your browser, install this server certificate into the browser. If you have multiple concentrators, you must install the certificate from each of the concentrators into your browser, but you only need to do that once for each concentrator. Once the SSL server certificate is installed, you can begin using HTTPS for communications with the concentrator.

Clicking the Install SSL Certificate hotlink takes you to the browser's certificate installation wizard. Netscape and Microsoft browsers have slightly different installation routines, but in either case, accept the default settings presented, supply a nickname for the certificate if requested, and continue through the installation process by clicking Next or Finish. You can then immediately connect to the concentrator using HTTPS once the installation wizard has finished.

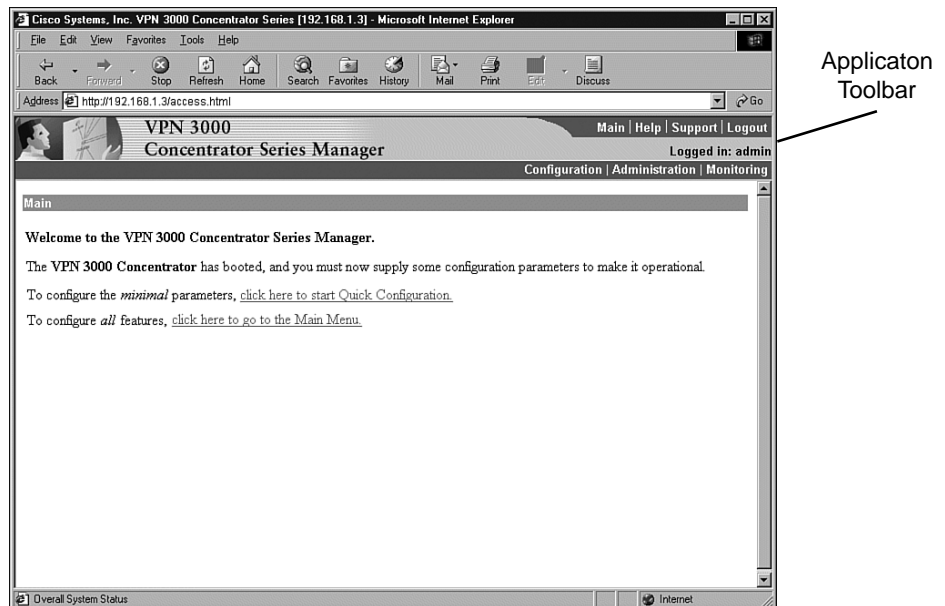
To continue with the Quick Configuration that you started from the CLI, log in with the administrator login name and password. Using the login screen shown in Figure 4-4, follow these steps:

- Step 1** Position your cursor in the Login field.
- Step 2** Type **admin** and the press Tab.
- Step 3** With the cursor in the Password field, type **admin** again. The window displays *****.
- Step 4** Click the **Login** button to initiate the login process.

If you make a mistake, click on the **Clear** button to refresh the screen so that you can start over.

After the VPN concentrator has accepted your administrator login, the screen shown in Figure 4-5 is displayed in your browser window.

Figure 4-5 *First-Time Quick Start Option Menu*



The top portion of the screen is the application toolbar, and it is displayed on every other manager screen. Because this is a consistent header, it is not shown in subsequent screen displays.

On the right-hand portion of the header, you see the standard toolbar, which contains the following elements:

- Hotlinks to the following items:
 - Main menu
 - Manager's Help system
 - A support page that provides web addresses and phone numbers to Cisco support sites
 - Logout, so that you can exit the system or log in as a different user
- Information on the login name of the current user
- Hotlinks to the Main Menu screen for the three major sections of the VPN 3000 Concentrator Manager system:
 - Configuration
 - Administration
 - Monitoring

The first time that you enter the VPN Manager after booting from the default configuration, you are presented with a screen that allows you to enter the Quick Configuration mode to continue the process that you started at the CLI. Figure 4-5 shows this screen.

If you click here to start Quick Configuration, the VPN Manager leads you through a series of screens to complete the 11 initial configuration steps. This is a continuation of the Quick Configuration wizard that was started at the CLI. You only have this opportunity once.

If you click here to go to the Main Menu, you can configure the same settings, but you must select the configuration windows from the table of contents. After you have completed the Quick Configuration, this screen is not displayed again, and the system boots into the standard VPN Manager window.

Configuring Remaining Interface Settings

When you click to start Quick Configuration, the VPN Manager displays the IP Interfaces screen. If your system is a 3005 series with only two fixed interfaces, the screen looks like that shown in Figure 4-6. Notice that the screen's title bar shows the complete path to this screen (Configuration | Quick | IP Interfaces), as it would be shown if you had worked down to this screen through the table of contents. This 3005 display shows that the Private interface is configured and operational and that the Public interface is not yet configured.

Figure 4-6 3005 Concentrator—Configuration / Quick / IP Interfaces

Configuration | Quick | IP Interfaces Save

Configure VPN 3000 Concentrator Series interfaces.

- Ethernet 1 (Private) = the interface to your private network (internal LAN).
- Ethernet 2 (Public) = the interface to the public network.
- WAN Interface Ports A and B = optional WAN interfaces, usually to the public network.

If you modify the interface that you are currently using to connect to this device, you will break the connection, and you will have to restart from the login screen.

Interface	Status	IP Address	Subnet Mask
Ethernet 1 (Private)	UP	192.168.1.3	255.255.255.0
Ethernet 2 (Public)	Not Configured		

Figure 4-7 shows the IP Interfaces screen for the Model 3015–3080 VPN Concentrator. This system has two unconfigured Ethernet interfaces and two unconfigured WAN interfaces. The listings in the Interface column are hotlinks to the configuration screen for each of the interfaces.

Figure 4-7 3015–3080 Concentrator—Configuration / Quick / IP Interfaces

Configuration | Quick | IP Interfaces Save

Configure VPN 3000 Concentrator Series interfaces.

- Ethernet 1 (Private) = the interface to your private network (internal LAN).
- Ethernet 2 (Public) = the interface to the public network.
- Ethernet 3 (External) = the interface to an additional LAN.
- WAN Interface Ports A and B = optional WAN interfaces, usually to the public network.


If you modify the interface that you are currently using to connect to this device, you will break the connection, and you will have to restart from the login screen.

Interface	Status	IP Address	Subnet Mask
Ethernet 1 (Private)	UP	192.168.1.3	255.255.255.0
Ethernet 2 (Public)	Not Configured		
Ethernet 3 (External)	Not Configured		
WAN Interface in slot 2, port A	Not Configured		
WAN Interface in slot 2, port B	Not Configured		

If you click the hotlink to Ethernet 1 (Private), the configuration screen for Ethernet 1 appears, as shown in Figure 4-8. You can select to disable the interface, to obtain addressing from a DHCP server, or to assign static IP addressing.

Figure 4-8 Configuration / Quick / IP Interfaces / Ethernet 1

Configuration / Quick / IP Interfaces / Ethernet 1

 You are modifying the interface you are using to connect to this device. If you make any changes, you will break the connection and you will have to restart from the login screen.

Configuring Ethernet Interface 1 (Private).

General Parameters			
Sel	Attribute	Value	Description
<input type="radio"/>	Disabled		Select to disable this interface.
<input type="radio"/>	DHCP Client		Select to obtain the IP Address, Subnet Mask and Default Gateway via DHCP (System Name may be required for DHCP).
	System Name	<input type="text"/>	
<input checked="" type="radio"/>	Static IP Addressing		Select to configure the IP Address and Subnet Mask. Enter the IP Address and Subnet Mask for this interface.
	IP Address	<input type="text" value="192.168.1.3"/>	
	Subnet Mask	<input type="text" value="255.255.255.0"/>	
	Public Interface	<input type="checkbox"/>	Check to make this interface a "public" interface.
	MAC Address	00.90.A4.00.00.13	The MAC address for this interface.
	Filter	<input type="text" value="--None--"/>	Select the filter for this interface.
	Speed	<input type="text" value="100 Mbps"/>	Select the speed for this interface.
	Duplex	<input type="text" value="Full-Duplex"/>	Select the duplex mode for this interface.

NOTE If you disable the Private interface, you lose your browser connection to the concentrator.

The Speed and Duplex settings were configured from the CLI in this example. The default settings for these two fields are 10/100 Auto and Auto, respectively, allowing the systems to negotiate speed and duplex mode.

When you have completed entering the configuration settings for an interface, click the Apply button to save the settings and return to the IP Interfaces screen. Once you have configured all the interfaces, click the Continue button to proceed to the next Quick Configuration screen.

Configuring System Information

The System Info screen is the next screen displayed. Figure 4-9 shows this screen. The date and time settings were entered during the CLI configuration steps. You can enter a system name here along with DNS server, domain name, and default gateway information.

Figure 4-9 Configuration / Quick / System Info

Configuration Quick System Info	
Assign a system name/hostname to this device. This may be required if you use DHCP to obtain an address.	
System Name	<input type="text" value="vpn01"/> Enter a hostname for the system; e.g. vpn01.
Set the time on your device. The correct time is very important, so that logging and accounting entries are accurate.	
The current time on this device is Friday, 29 March 2002 08:53:29.	
New Time	<input type="text" value="8"/> : <input type="text" value="57"/> : <input type="text" value="34"/> <input type="text" value="March"/> <input type="text" value="29"/> / <input type="text" value="2002"/> <input type="text" value="(GMT-06:00) CST"/>
<input checked="" type="checkbox"/> Enable DST Support	
Specify a DNS server, which lets you enter hostnames rather than IP addresses in subsequent Manager fields.	
DNS Server	<input type="text" value="192.168.1.20"/> Enter the IP address of your local DNS server.
Domain	<input type="text" value="cisco.com"/> Enter your Internet domain name; e.g. yourcompany.com.
Default Gateway	<input type="text" value="172.16.1.1"/> Enter your default gateway. Leave at 0.0.0.0 for no default gateway.
<input type="button" value="Back"/> <input type="button" value="Continue"/>	

Configuring the Tunneling Protocol

Clicking the Continue button takes you to the Protocols screen, as shown in Figure 4-10. You can select all protocols, if you like. The configuration described in this chapter works with IPSec only, so that is the only protocol selected on this screen.

Figure 4-10 Configuration / Quick / Protocols

Configuration Quick Protocols	
Select the tunneling protocols and encryption options that you want to enable.	
<input type="checkbox"/> PPTP	<input type="radio"/> Require Encryption (Clients without encryption will not gain access. Requires MSCHAP.) <input checked="" type="radio"/> Don't Require Encryption (Clients may optionally use encryption.)
<input type="checkbox"/> L2TP	<input type="radio"/> Require Encryption (Clients without encryption will not gain access. Requires MSCHAP.) <input checked="" type="radio"/> Don't Require Encryption (Clients may optionally use encryption.)
<input checked="" type="checkbox"/> IPSec	Check to enable remote user connections via IPSec. LAN-to-LAN configurations are done outside of Quick Configuration.
<input type="button" value="Back"/> <input type="button" value="Continue"/>	

Configuring Address Assignment Method

After you have selected the protocol to use, you must select the method the VPN concentrator is to use to assign an address to clients as they establish tunnels with the concentrator. The method of address assignment selected in Figure 4-11 is to use a DHCP server. You could select multiple methods; the concentrator tries each method in order until it is successful in assigning an address to the client.

Figure 4-11 Configuration / Quick / Address Assignment

Configuration | Quick | Address Assignment

Select at least one method of assigning IP addresses to clients as a tunnel is established. The methods are tried in the order listed.

- Client Specified This method lets the client specify its own IP address.
- Per User This method assigns IP addresses on a per-user basis. If you use an authentication server (which you configure next) that has IP addresses configured, we recommend selecting this method.
- DHCP Specify Server
 - Range Start
 - Range End
- Configured Pool This method uses this device to assign IP addresses.

Back Continue

Configuring User Authentication Method

Next, you determine how users connecting over the VPN tunnel are to be authenticated. Figure 4-12 shows the selection screen. Users can be authenticated from RADIUS servers, NT Domain controllers, external SDI servers, and the concentrator's internal server. The option you select brings up the appropriate next screen so that you can continue configuring user authentication.

Figure 4-12 Configuration / Quick / Authentication

Configuration | Quick | Authentication

Specify how to authenticate users under PPTP, L2TP or IPsec. You can use the internal server or an external authentication server. If you select the *Internal Server*, you must configure the internal user database. You may configure additional servers using System Configuration.

Server Type Selecting *Internal Server* will let you add users to the internal user database.

Back Continue

Configuring Users for Internal Authentication

The example shown in Figure 4-12 has selected the Internal Server option and brings up the User Database screen, shown in Figure 4-13, so that you can enter the usernames and passwords. This screen also requests an IP address and subnet mask because, in this case, the concentrator's administrator selected Per User address assignment on the screen displayed in Figure 4-11.

Figure 4-13 Configuration | Quick | User Database

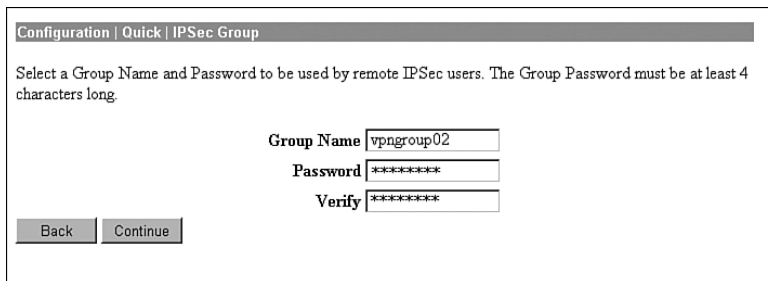
There is a maximum combined number of groups and users that you can configure on a VPN 3000 Concentrator. The number varies by concentrator model, as shown in Table 4-2.

Table 4-2 Maximum Number of Combined Groups and Users per VPN Model

Model	Maximum Combined Number of Groups and Users
3005	100
3015	100
3030	500
3060	1000
3080	1000

Configuring the IPSec Tunnel Group

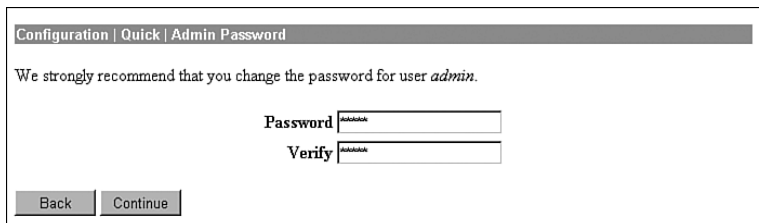
When you select IPSec as the tunneling protocol from the screen shown in Figure 4-10, the concentrator prompts you to define a group during the Quick Configuration phase. This group is used by every user unless you change the association later from the standard configuration section of the VPN Manager. Figure 4-14 shows the configuration information for the IPSec group. The password for this group becomes the preshared key for remote access users.

Figure 4-14 Configuration / Quick / IPsec Group

The screenshot shows a web-based configuration interface for an IPsec group. At the top, a breadcrumb trail reads "Configuration | Quick | IPsec Group". Below this, a message states: "Select a Group Name and Password to be used by remote IPsec users. The Group Password must be at least 4 characters long." There are three input fields: "Group Name" containing "vpngroup02", "Password" containing "*****", and "Verify" containing "*****". At the bottom left, there are two buttons: "Back" and "Continue".

Configuring the Admin Password

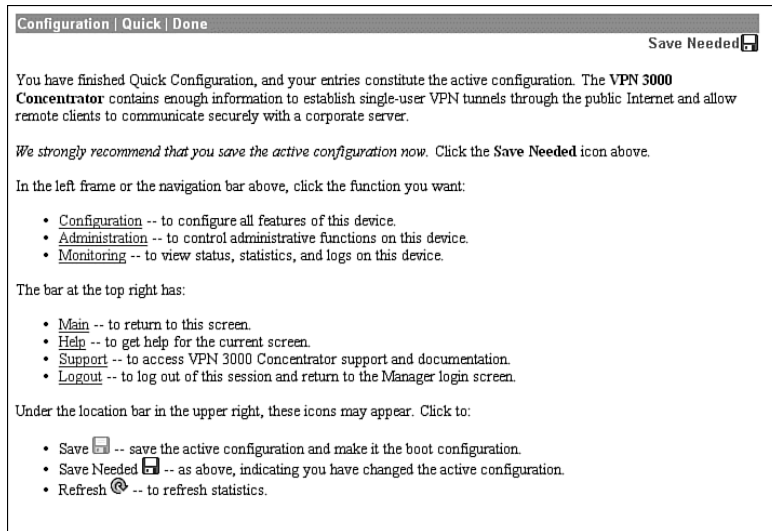
The final setting that you should configure during the Quick Configuration is the password for the admin user. Figure 4-15 shows the Quick Configuration screen for completing this task and displays the message that strongly recommends changing the admin password. For maximum password security, select a password containing at least eight characters that are a mixture of uppercase and lowercase letters, numbers, and special characters.

Figure 4-15 Configuration / Quick / Admin Password

The screenshot shows a web-based configuration interface for setting the admin password. At the top, a breadcrumb trail reads "Configuration | Quick | Admin Password". Below this, a message states: "We strongly recommend that you change the password for user *admin*." There are two input fields: "Password" containing "*****" and "Verify" containing "*****". At the bottom left, there are two buttons: "Back" and "Continue".

Saving Configuration Settings

When you click the Continue button after changing the admin password, the VPN Manager presents you with the Quick Configuration Done screen, as shown in Figure 4-16. At this point, you have configured the system information, LAN and WAN interfaces, users, and IPsec group, completing the basic configuration of the VPN concentrator.

Figure 4-16 Configuration | Quick | Done

Notice the Save Needed icon in the upper-right corner of the main screen. Click that icon to save the active configuration changes you have made to the boot configuration. As you continue with additional configuration steps, this icon appears from time to time. As you can see from Figure 4-16, the icon can display Save, Save Needed, or Refresh depending on the type of screen you are on and whether you have made modifications to the active configuration.

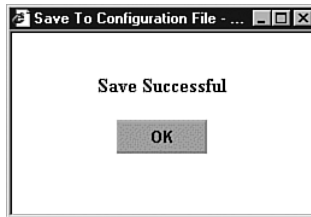
As with most Cisco products, configuration changes are done to the active configuration and take effect immediately. To ensure that your changes are still in effect after a system reboot, you must copy the active configuration to the boot configuration. The VPN Manager's Save Needed reminder is a nice touch, providing a gentle reminder and an easy method of execution.

Clicking the Save Needed icon executes the requested save and provides you with a status screen. Figure 4-17 shows the screen that is returned upon the completion of a successful save. After you clear this screen by clicking the OK button, VPN Manager displays the Main Menu.

In addition to the Save, Save Needed, and Refresh options, the Configuration | Quick | Done screen shows Configuration, Administration, and Monitoring in the upper-left corner (refer to Figure 4-16). These three keys are the primary navigation tools for the daily VPN Manager functions. Similar to a directory display from a product such as Microsoft Windows Explorer,

the plus sign indicates that the indicated function has subfunctions. Clicking the plus sign displays an indented list of the subfunctions, and clicking the option takes you to the window for that function.

Figure 4-17 *Save Successful Message*



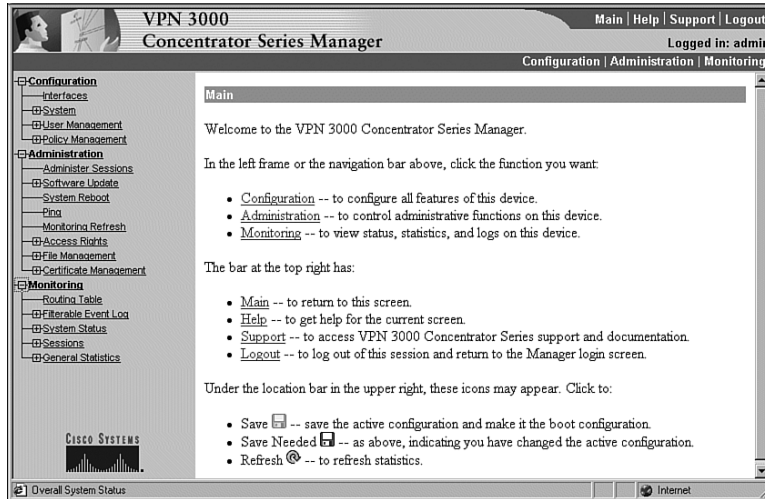
Configuring IPSec with Preshared Keys Through the VPN 3000 Concentrator Series Manager

The Quick Configuration allows you to configure the basic operational settings of the concentrator, but the IPSec settings have not been established yet. Those settings are made using features in the Configuration portion of the Cisco VPN 3000 Concentrator Manager.

Figure 4-18 shows the Main screen that appears after you log in to the concentrator through VPN Manager. Normally the root Configuration, Administration, and Monitoring levels are the only options displayed in the table of contents. In this case, each of those major sections has been opened to the first layer of subfunctions. You can see the following major subfunctions under the Configuration option:

- **Interfaces**—Ethernet interfaces and power supplies
- **System**—System-wide parameters: servers, address assignment, tunneling protocols, IP routing, management protocols, events, and identification
- **User Management**—Groups and users
- **Policy Management**—Access hours, network lists, rules, security associations, filters, and NAT

Figure 4-18 IPsec Configuration



The interfaces have already been configured using the Quick Configuration option. If you chose to use internal authentication, the Quick Configuration wizard then asked you to enter usernames and passwords and then requested a group name to use for IPsec traffic.

Recall from previous chapters that there is a hierarchy to the way groups are used on the Cisco VPN 3000 Concentrator. The following basic rules govern group usage:

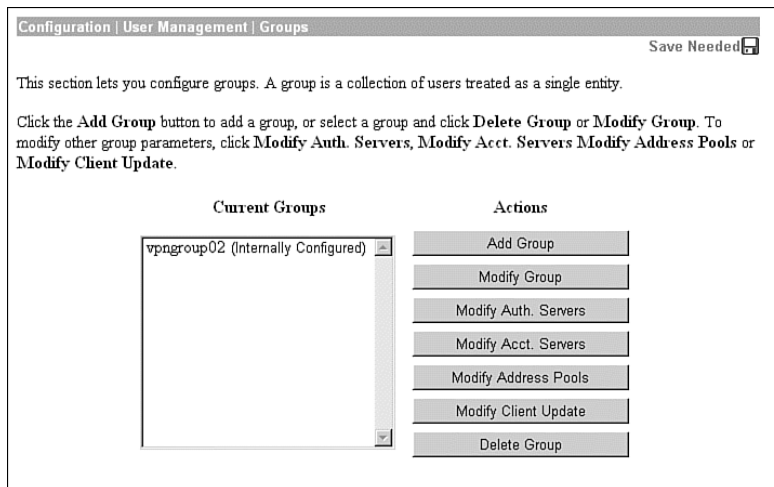
- Groups and users have attributes that can be modified to control how they can use the services of the concentrator.
- Users are always members of groups, and groups are always members of the Base Group. The Base Group is a default group that cannot be deleted but which can be modified.
- Inheritance rules state that, by default, users inherit rights from groups, and groups inherit rights from the Base Group.
- A user can only be a member of one concentrator group and, if not explicitly assigned to a different group, is a member of the Base Group by default.
- Users and groups have names and passwords.
- If you change the attributes of a group, it affects all group members.
- If you delete a group, user membership reverts to the Base Group.

Because the Base Group had not been modified before Quick Configuration set up the new group for IPSec use, that new group has default settings that it inherited from the Base Group. Additionally, all the users that you created were placed in this single group. That might be adequate for your organization. The final step you need to perform to set up the concentrator for remote access using preshared keys is to validate the entries that were placed in the IPSec group.

NOTE The discussions in this chapter assume that you would be performing the configuration on a new concentrator. You could be setting up remote access services on a concentrator that has been used for other purposes, such as LAN-to-LAN VPNs. In that case, you would start at this point in the configuration process. While this discussion looks at modifying the group that was established through Quick Configuration, you would simply need to add a new group from the Configuration | User Management | Groups screen.

To modify the settings for the IPSec group previously created, work down to the Configuration | User Management | Groups screen (see Figure 4-19). In this screen, you find the `vpngroup02` group listed in the Current Groups window. There are internal and external groups. External groups are those that would be used with external authentication servers such as RADIUS or NT Domain. The `vpngroup02` group is an internal group and is to be used with internal database users.

Figure 4-19 Configuration | User Management | Groups



Modify Groups—Identity Tab

To modify the group, click the group to highlight it, and then click the **Modify Group** button. The screen shown in Figure 4-20 shows the Modify screen for an internal group. Internal groups have multiple tabs. External groups only have the Identity tab. The information in this screen should match the data you entered during Quick Configuration. If not, you can correct it here. When everything looks correct, click the **General** tab.

Figure 4-20 Configuration | User Management | Groups | Modify > Identity

Configuration | User Management | Groups | Modify vpngroup02

This section lets you add a group. Check the **Inherit?** box to set a field that you want to default to the base group value. Uncheck the **Inherit?** box and enter a new value to override base group values.

Identity | General | IPSec | Client Config | Client FW | HW Client | PPTP/L2TP

Identity Parameters		
Attribute	Value	Description
Group Name	vpngroup02	Enter a unique name for the group.
Password	*****	Enter the password for the group.
Verify	*****	Verify the group's password.
Type	Internal	External groups are configured on an external authentication server (e.g. RADIUS). Internal groups are configured on the VPN 3000 Concentrator's Internal Database.

Add Cancel

Modify Groups—General Tab

Figure 4-21 depicts the General tab for the group's Modify function. Notice that each attribute listed has a Value, Inherit?, and Description column. If the Inherit? box is checked, that attribute's value is inherited from the Base Group, regardless of what you enter into the Value field. To change the value for an attribute, uncheck the Inherit? box.

The following information is shown on the General tab:

- **Access Hours**—Selected from the drop-down menu, this attribute determines when the concentrator is open for business for this group. Currently set to No Restrictions, you could also select Never, Business Hours (9 a.m. to 5 p.m., Monday through Friday), or named access hours that you created elsewhere in the VPN Manager.
- **Simultaneous Logins**—Default is 3. Minimum is 0. There is no upper limit, but you should limit this value to 1 for security purposes.
- **Minimum Password Length**—The allowable range is 1 to 32 characters. A value of 8 provides a good level of security for most applications.
- **Allow Alphabetic-Only Passwords**—Notice that the Inherit? box has been unchecked. The default is to allow alphabetic-only passwords, which is not a good idea. This value has been modified.
- **Idle Timeout**—A value of 30 minutes is good here. The minimum allowable value is 1 and the maximum is a value that equates to over 4000 years! 0 disables idle timeout.

- **Maximum Connect Time**—0 disables maximum connect time. The range here is again 1 minute to over 4000 years.
- **Filter**—Filters determine whether IPSec traffic is permitted or denied for this group. There are three default filters: Public, Private, and External. You can select from those or from any that you can define in the drop-down box. The default None option permits IPSec to handle all traffic.
- **Primary/Secondary DNS/WINS**—These have been modified from the Base Group's default settings.
- **SEP Card Assignment**—Some models of the VPN concentrator can contain up to four Scalable Encryption Processing (SEP) modules that handle encryption functions. This attribute allows you to steer the IPSec traffic for this group to specific SEPs to perform your own load balancing.
- **Tunneling Protocols**—IPSec has been selected, but you could allow the group to use Point-to-Point Tunneling Protocol (PPTP), Layer 2 Tunneling Protocol (L2TP), and L2TP over IPSec as well.
- **Strip Realm**—The default operation of the VPN concentrator verifies users against the internal database using a combination of the username and realm qualifier, as in *username@group*. The *@group* portion is called the realm. You can have the VPN concentrator use name only by checking the value for this attribute.

Figure 4-21 Configuration | User Management | Groups | Modify > General

Configuration | User Management | Groups | Modify vpngroup02

This section lets you add a group. Check the **Inherit?** box to set a field that you want to default to the base group value. Uncheck the **Inherit?** box and enter a new value to override base group values.

Identity | General | IPSec | Client Config | Client FW | HW Client | PPTP/L2TP

General Parameters			
Attribute	Value	Inherit?	Description
Access Hours	-No Restrictions	<input checked="" type="checkbox"/>	Select the access hours assigned to this group.
Simultaneous Logins	3	<input checked="" type="checkbox"/>	Enter the number of simultaneous logins for this group.
Minimum Password Length	8	<input checked="" type="checkbox"/>	Enter the minimum password length for users in this group.
Allow Alphabetic-Only Passwords	<input type="checkbox"/>	<input type="checkbox"/>	Enter whether to allow users with alphabetic-only passwords to be added to this group.
Idle Timeout	30	<input checked="" type="checkbox"/>	(minutes) Enter the idle timeout for this group.
Maximum Connect Time	0	<input checked="" type="checkbox"/>	(minutes) Enter the maximum connect time for this group.
Filter	-None-	<input checked="" type="checkbox"/>	Enter the filter assigned to this group.
Primary DNS	192.168.1.20	<input type="checkbox"/>	Enter the IP address of the primary DNS server.
Secondary DNS	192.168.34.20	<input type="checkbox"/>	Enter the IP address of the secondary DNS server.
Primary WINS	192.168.1.22	<input type="checkbox"/>	Enter the IP address of the primary WINS server.
Secondary WINS	192.168.34.22	<input type="checkbox"/>	Enter the IP address of the secondary WINS server.
SEP Card Assignment	<input checked="" type="checkbox"/> SEP 1 <input checked="" type="checkbox"/> SEP 2 <input checked="" type="checkbox"/> SEP 3 <input checked="" type="checkbox"/> SEP 4	<input checked="" type="checkbox"/>	Select the SEP cards this group can be assigned to.
Tunneling Protocols	<input type="checkbox"/> PPTP <input type="checkbox"/> L2TP <input checked="" type="checkbox"/> IPSec <input type="checkbox"/> L2TP over IPSec	<input type="checkbox"/>	Select the tunneling protocols this group can connect with.
Strip Realm	<input type="checkbox"/>	<input checked="" type="checkbox"/>	Check to remove the realm qualifier of the user name during authentication.

Add Cancel

Modify Groups—IPSec Tab

Clicking the IPSec tab brings up the screen shown in Figure 4-22. The attributes on this screen are as follows:

- **IPSec SA**—For remote access clients, you must select an IPSec Security Association (SA) from this list of available combinations. If you have created additional SA types, those are also displayed here as selection options. The client and server negotiate an SA that governs authentication, encryption, encapsulation, key management, and so on based on your selection here.

The following are the default selections supplied by the VPN concentrator:

- **None**—No SA is assigned.
- **ESP-DES-MD5**—This SA uses DES 56-bit data encryption for both the IKE tunnel and IPSec traffic, ESP/MD5/HMAC-128 authentication for IPSec traffic, and MD5/HMAC-128 authentication for the IKE tunnel.
- **ESP-3DES-MD5**—This SA uses Triple-DES 168-bit data encryption and ESP/MD5/HMAC-128 authentication for IPSec traffic, and DES-56 encryption and MD5/HMAC-128 authentication for the IKE tunnel.
- **ESP/IKE-3DES-MD5**—This SA uses Triple-DES 168-bit data encryption for both the IKE tunnel and IPSec traffic, ESP/MD5/HMAC-128 authentication for IPSec traffic, and MD5/HMAC-128 authentication for the IKE tunnel.
- **ESP-3DES-NONE**—This SA uses Triple-DES 168-bit data encryption and no authentication for IPSec traffic, and DES-56 encryption and MD5/HMAC-128 authentication for the IKE tunnel.
- **ESP-L2TP-TRANSPORT**—This SA uses DES 56-bit data encryption and ESP/MD5/HMAC-128 authentication for IPSec traffic (with ESP applied only to the transport layer segment), and it uses Triple-DES 168-bit data encryption and MD5/HMAC-128 for the IKE tunnel. Use this SA with the L2TP over IPSec tunneling protocol.
- **ESP-3DES-MD5-DH7**—This SA uses Triple-DES 168-bit data encryption and ESP/MD5/HMAC-128 authentication for both IPSec traffic and the IKE tunnel. It uses Diffie-Hellman Group 7 (ECC) to negotiate Perfect Forward Secrecy. This option is intended for use with the movianVPN client, but you can use it with other clients that support D-H Group 7 (ECC).
- **IKE Peer Identity Validation**—This option applies only to VPN tunnel negotiation based on certificates. This field enables you to hold clients to tighter security requirements.

- **IKE Keepalives**—Monitors the continued presence of a remote peer and notifies the remote peer that the concentrator is still active. If a peer no longer responds to the keepalives, the concentrator drops the connection, preventing hung connections that could clutter the concentrator.
- **Tunnel Type**—You can select either LAN-to-LAN or Remote Access as the tunnel type. If you select LAN-to-LAN, you do not need to complete the remainder of this screen.
- **Group Lock**—Checking this field forces the user to be a member of this group when authenticating to the concentrator.
- **Authentication**—This field selects the method of user authentication to use. The available options are as follows:
 - **None**—No user authentication occurs. Use this with L2TP over IPsec.
 - **RADIUS**—Uses an external RADIUS server for authentication. The server address is configured elsewhere.
 - **RADIUS with Expiry**—Uses an external RADIUS server for authentication. If the user's password has expired, this method gives the user the opportunity to create a new password.
 - **NT Domain**—Uses an external Windows NT Domain system for user authentication.
 - **SDI**—Uses an external RSA Security, Inc., SecurID system for user authentication.
 - **Internal**—Uses the internal VPN concentrator authentication server for user authentication.
- **IPComp**—This option permits the use of the Lempel Zif Stac (LZS) compression algorithm for IP traffic developed by Stac Electronics. This can speed connections for users connecting through low-speed dial-up circuits.
- **Reauthentication on Rekey**—During IKE phase 1, the VPN concentrator prompts the user to enter an ID and password. When you enable reauthentication, the concentrator prompts for user authentication whenever a rekey occurs, such as when the IKE SA lifetime expires. If the SA lifetime is set too short, this could be an annoyance to your users, but it provides an additional layer of security.
- **Mode Configuration**—During SA negotiations, this option permits the exchange of configuration parameters with the client. To pass configuration information to the client, such as DNS or WINS addresses, you must enable this option. If you check this box, you need to continue to the Mode Config tab to complete the selection of attributes there.

Figure 4-22 Configuration | User Management | Groups | Modify > IPsec

Configuration | User Management | Groups | Modify vpngroup02

This section lets you add a group. Check the **Inherit?** box to set a field that you want to default to the base group value. Uncheck the **Inherit?** box and enter a new value to override base group values.

Identity | General | **IPSec** | Client Config | Client FW | HW Client | PPTP/L2TP

IPSec Parameters			
Attribute	Value	Inherit?	Description
IPSec SA	ESP-3DES-MD5	<input checked="" type="checkbox"/>	Select the group's IPSec Security Association.
IKE Peer Identity Validation	If supported by certificate	<input checked="" type="checkbox"/>	Select whether or not to validate the identity of the peer using the peer's certificate.
IKE Keepalives	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Check to enable the use of IKE keepalives for members of this group.
Tunnel Type	Remote Access	<input checked="" type="checkbox"/>	Select the type of tunnel for this group. Update the Remote Access parameters below as needed.
Remote Access Parameters			
Group Lock	<input type="checkbox"/>	<input checked="" type="checkbox"/>	Lock users into this group.
Authentication	Internal	<input checked="" type="checkbox"/>	Select the authentication method for members of this group. This parameter does not apply to Individual User Authentication .
IPComp	None	<input checked="" type="checkbox"/>	Select the method of IP Compression for members of this group.
Reauthentication on Rekey	<input type="checkbox"/>	<input checked="" type="checkbox"/>	Check to reauthenticate the user on an IKE (Phase-1) rekey.
Mode Configuration	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Check to initiate the exchange of Mode Configuration parameters with the client. This must be checked if version 2.5 (or earlier) of the Altiga/Cisco client is being used by members of this group.

Add Cancel

Modify Groups—Client Config Tab

The Client Config tab screen is shown in Figure 4-23. Configuration of the attributes on this screen is only necessary if you selected Mode Configuration from the IPSec tab screen. The attributes on this page have the following meanings:

- **Banner**—You can enter up to a 510-character greeting banner that is displayed to IPSec software clients each time they log in to the system.
- **Allow Password Storage on Client**—This option allows the client PC to store the user's password. For security reasons, this is not a good policy. The default is to have this capability disabled.
- **IPSec over UDP**—This option permits clients to connect to the VPN concentrator via UDP through a firewall or router using NAT.
- **IPSec over UDP Port**—This attribute lets you set the port to use through the firewall. The default is 10,000.

- **IPSec Backup Servers**—This attribute is used on Cisco VPN 3002 Hardware Clients and is not required for remote access users.
- **Intercept DHCP Configure Message**—Enable DHCP intercept to permit Microsoft Windows XP clients to perform split tunneling with the VPN concentrator. When you enable this field, the VPN concentrator replies to the Microsoft Windows XP client DHCP Inform message. This capability allows the VPN concentrator to provide the client with a subnet mask, domain name, and classless static routes for the tunnel IP address when a DHCP server is not available.
- **Subnet Mask**—Enter a valid subnet mask for Microsoft Windows clients requesting DHCP services.
- **Split Tunneling Policy**—This option, disabled by default, permits clients to specify some types of traffic as not requiring IPSec protection. This traffic is sent in clear text. The options within this attribute are as follows:
 - **Tunnel everything**—All data use the secure IPSec tunnel.
 - **Allow networks in list to bypass the tunnel**—All data use the secure IPSec tunnel except for data being sent to addresses on the network list. This option gives users who have elected to tunnel all traffic the ability to access devices such as printers on their local networks without having that traffic encrypted.
 - **Only tunnel networks in list**—Uses the secure IPSec tunnel for data sent to addresses on the network list. All other traffic is sent as clear text. This option allows remote users to access public networks without requiring IPSec tunneling through the corporate network.
- **Split Tunneling Network List**—If you select the Allow networks in list to bypass the tunnel option, then this list is an exclusion list, allowing traffic to pass over the network without going through IPSec. If you select the Only tunnel networks in list option, then this list is an inclusion list that determines which traffic is handled via IPSec. You can establish these lists elsewhere in the concentrator, or you can use the VPN Client Local LAN option.
- **Default Domain Name**—If you supply a domain name here, the concentrator passes this name to the client. Fully qualified domain names sent over the IPSec tunnel have this domain name appended to the end.
- **Split DNS Names**—Enter a list of domain names that you want the VPN concentrator's internal DNS server to resolve for traffic going over the tunnel. This option is useful in split-tunneling connections, permitting the internal DNS server to resolve domain names for traffic through the tunnel. The ISP-assigned DNS servers resolve DNS requests that travel in the clear to the Internet.

Figure 4-23 Configuration | User Management | Groups | Modify > Client Config

Configuration | User Management | Groups | Modify vpngrp02

This section lets you add a group. Check the **Inherit?** box to set a field that you want to default to the base group value. Uncheck the **Inherit?** box and enter a new value to override base group values.

Identity | General | IPsec | Client Config | Client FW | HW Client | PPTP/L2TP

Client Configuration Parameters

Cisco Client Parameters			
Attribute	Value	Inherit?	Description
Banner	<input type="text"/>	<input checked="" type="checkbox"/>	Enter the banner for this group. Only software clients see the banner.
Allow Password Storage on Client	<input type="checkbox"/>	<input checked="" type="checkbox"/>	Check to allow the IPsec client to store the password locally.
IPsec over UDP	<input type="checkbox"/>	<input checked="" type="checkbox"/>	Check to allow a client to operate through a NAT device using UDP encapsulation of ESP.
IPsec over UDP Port	<input type="text" value="10000"/>	<input checked="" type="checkbox"/>	Enter the UDP port to be used for IPsec through NAT (4001 - 49151, except port 4500, which is reserved for NAT-T).
IPsec Backup Servers	Use Client Configured List <input type="text"/>	<input checked="" type="checkbox"/>	<ul style="list-style-type: none"> Select a method to use or disable backup servers. Enter up to 10 IPsec backup server addresses/names starting from high priority to low. Enter each IPsec backup server address/name on a single line.
Microsoft Client Parameters			
Intercept DHCP Configure Message	<input type="checkbox"/>	<input checked="" type="checkbox"/>	Check to use group policy for clients requesting Microsoft DHCP options.
Subnet Mask	<input type="text" value="255.255.255.255"/>	<input checked="" type="checkbox"/>	Enter the subnet mask for clients requesting Microsoft DHCP options.
Common Client Parameters			
Split Tunneling Policy	<input checked="" type="radio"/> Tunnel everything <input type="checkbox"/> Allow the networks in list to bypass the tunnel <input type="radio"/> Only tunnel networks in the list	<input checked="" type="checkbox"/>	Select the method and network list to be used for Split Tunneling. Tunnel Everything: Send all traffic through the tunnel. Allow the networks in the list to bypass the tunnel: The VPN Client may choose to send traffic to addresses in this list to the client's LAN. Send all other traffic through the tunnel. NOTE: This setting only applies to the Cisco VPN Client.
Split Tunneling Network List	<input type="text" value="--None--"/>	<input checked="" type="checkbox"/>	Tunnel networks in the list: Send traffic to addresses in this list through the tunnel. Send all other traffic to the client's LAN.
Default Domain Name	<input type="text"/>	<input checked="" type="checkbox"/>	Enter the default domain name given to users of this group.
Split DNS Names	<input type="text"/>	<input checked="" type="checkbox"/>	Enter the set of domains, separated by commas without spaces, to be resolved through the Split Tunnel.

Add Cancel

That is all that you need to configure on the VPN concentrator. Click the Modify button to save your work to the active configuration and return to the Groups screen shown in Figure 4-19. Be sure to click the Save Needed icon to save your configuration changes to the boot configuration. To configure the client firewall capability or hardware client features, or if you are using either the PPTP or L2TP tunneling protocols, continue configuring the group settings using the Client FW, HW Client, and PPTP/L2TP tabs discussed in the following sections.

Modify Groups—Client FW Tab

The Client FW tab permits you to configure firewall options for Cisco VPN Clients running on a Microsoft Windows platform. Client firewall support is disabled by default but can be enabled on this tab. A stateful firewall is built into the VPN Client, but other commercially available firewalls can be used and operate as a separate application that runs on the Windows platform. Firewalls inspect each inbound and outbound packet to determine if the packet should be forwarded toward its destination or whether the packet should be dropped. These decisions are made using rules defined in firewall policies. Firewalls provide an extra measure of protection to systems and corporate networks, especially when split tunneling is used.

The VPN concentrator can support client firewalls in three different ways:

- Each client can individually manage its own personal firewall policy.
- The VPN concentrator can push a centralized firewall policy to each client.
- A separate, standalone firewall server can be used to manage and enforce firewall policy usage on VPN Client devices.

Figure 4-24 shows the configuration options that are available on the Client FW tab for these three types of firewall management. The following bulleted items discuss the options shown on the Client FW tab screen:

- **Firewall Setting**—This attribute is used to enable or disable firewall support for the users connecting through this group. The available settings are as follows:
 - **No Firewall**—This is the default setting for a new group. When this option is checked, the VPN concentrator ignores VPN Client firewall settings.
 - **Firewall Required**—When this option is checked, every VPN Client peer that connects through this group must use the firewall specified for this group. If the peer is not using the correct firewall, the VPN concentrator drops the connection and notifies the VPN Client of the mismatch.
 - **Firewall Optional**—Setting the firewall to optional can be used when all your VPN Client users are not currently running firewalls on their systems. Choosing this option lets users without firewalls connect, giving them a warning message. Those users with firewalls installed must be using the correct firewall; the VPN concentrator and VPN Client then manage the firewall policy according to the settings contained on this Client FW tab.

- **Firewall**—Select the firewall that members of the group are to use. The available options are as follows:
 - **Cisco Integrated Client Firewall**—The stateful firewall built into the VPN Client.
 - **Network ICE BlackICE Defender**—The Network ICE BlackICE Agent or Defender personal firewall.
 - **Zone Labs ZoneAlarm**—The Zone Labs ZoneAlarm personal firewall.
 - **Zone Labs ZoneAlarm Pro**—The Zone Labs ZoneAlarm Pro personal firewall.
 - **Zone Labs ZoneAlarm or ZoneAlarm Pro**—Either the Zone Labs ZoneAlarm personal firewall or the Zone Labs ZoneAlarm Pro personal firewall.
 - **Zone Labs Integrity**—The Zone Labs Integrity Client.
 - **Custom Firewall**—This option is primarily for future use. Choose this option when you cannot use any of the previous options or when you want to combine two or more of these options. When you choose this option, you must detail your firewall selection(s) in the Custom Firewall attribute settings.
- **Custom Firewall**—All the supported options are currently selectable from the list available in the Firewall attribute setting. In the future, additional options might be available. At that time, you could use this section to identify those new firewalls.
 - **Vendor ID**—You can only enter one vendor ID code in this field. Currently, the available vendor codes are Cisco Systems (Vendor ID 1), Zone Labs (Vendor ID 2), and Network ICE (Vendor ID 3).
 - **Product ID**—For the vendor selected, you can enter multiple product ID codes in this field. When entering multiple code numbers, separate them with a comma or use a hyphen to designate a range, such as 1-3 for Zone Labs. To use all available products for a given vendor, enter 255 as the Product ID. Table 4-3 shows the current product codes.

Table 4-3 *Custom Firewall Product Codes*

Vendor	Product	Product Code
Cisco	Cisco Integrated Client (CIC)	1
Zone Labs	Zone Alarm	1
	Zone Alarm Pro	2
	Zone Labs Integrity	3
Network ICE	BlackIce Defender/Agent	1

- **Description**—You can enter an optional description for your custom firewall in this field.

- **Firewall Policy**—You can select from three different methods for administering the firewall policy for your VPN Client systems. Those methods are as follows:
 - **Policy Defined by Remote Firewall (AYT)**—The user of the VPN Client system has established firewall policy settings for a personalized firewall that runs on the user’s system. That firewall can be a third-party firewall that works with the Cisco VPN Client and VPN concentrator. The VPN Client uses the Are You There (AYT) enforcement mechanism to periodically poll the firewall. If the firewall doesn’t respond to the periodic “Are you there?” messages, the VPN Client drops the connection to the VPN concentrator. A system administrator can initially configure and install the firewall for these users, but each user is allowed to configure his or her own policies beyond the initial settings. This option is available for use with the Network ICE BlackIce Defender, Zone Labs ZoneAlarm, and Zone Labs ZoneAlarm Pro firewall products.
 - **Policy Pushed (CPP)**—When a corporation’s security policy mandates that all VPN Clients use the same firewall policy, the system administrator can configure the VPN concentrator to push a centralized, standardized firewall policy to each VPN Client, which then passes the policy on to the local firewall for enforcement. The administrator creates a set of traffic management rules on the VPN concentrator, associates the rules with a filter, and designates the filter as the firewall policy from the drop-down window for this attribute. This type of firewall policy management is called *push policy* or *Central Protection Policy (CPP)*. This option is available for use with the Cisco Integrated Client Firewall, Zone Labs ZoneAlarm, and Zone Labs ZoneAlarm Pro firewall products.
 - **Policy from Server**—You can use the Zone Labs Integrity Server (IS), a stand-alone firewall server, to manage firewall policy management and enforcement through the VPN Client. A centralized firewall policy is maintained on the IS. The IS then pushes this policy to each monitored VPN Client host and then monitors the use of the policy on those hosts. The Zone Labs IS also communicates with the VPN concentrator to manage connections and share session, user, and status information. This option is only available for the Zone Labs Integrity Server firewall product.

Modify Groups—HW Client Tab

Cisco VPN 3002 Hardware Clients provide additional authentication capabilities for peer and user authentication. The VPN 3002 Hardware Client communicates with the VPN concentrator to establish the tunnel and the user systems connect to the hardware client via Ethernet connections. The user systems do not require the VPN Client.

Figure 4-24 Configuration | User Management | Groups | Modify > Client FW

Configuration | User Management | Groups | Modify vpngroup02

This section lets you add a group. Check the **Inherit?** box to set a field that you want to default to the base group value. Uncheck the **Inherit?** box and enter a new value to override base group values.

Identity | General | IPsec | Client Config | **Client FW** | HW Client | PPTP/L2TP

VPN Client Firewall Policy			
Attribute	Value	Inherit?	Description
Firewall Setting	<input checked="" type="radio"/> No Firewall <input type="radio"/> Firewall Required <input type="radio"/> Firewall Optional		Select whether or not to require that the client firewall specified below be installed and active. Refer to the client documentation for details about using this feature.
Firewall	Custom Firewall		Select the firewall vendor and product required for clients in this group. For client firewalls not listed, select Custom Firewall and enter the vendor and product IDs.
Custom Firewall	Vendor ID: <input type="text"/> Product ID: <input type="text"/> Description: <input type="text"/>	<input checked="" type="checkbox"/>	Separate multiple product IDs with commas. To indicate all products by a particular vendor, enter product ID 255. The product description is optional.
Firewall Policy	<input checked="" type="radio"/> Policy defined by remote firewall (AYT) <input type="radio"/> Policy Pushed (CPP): --None-- <input type="radio"/> Policy from Server		Select the policy for the protection provided by the client firewall.

Add Cancel

When you configure the VPN 3002 Hardware Client for the IPsec tunneling protocol, you enter the IPsec group name and password that you configured on the VPN concentrator onto the Configuration | System | Tunneling Protocols | IPsec screen of the VPN 3002 Hardware Client. You must also enter a single username and password on that same screen, which are used to establish user authentication for all users connected to the VPN 3002 Hardware Client. Both the group name and username must be valid to establish the IPsec tunnel. Once the VPN 3002 Hardware Client and the VPN concentrator have established the VPN tunnel, any users connected to the hardware client can use the secure tunnel.

To provide additional security, you can enable interactive authentication for the establishment of the IPsec tunnel and for interactive user authentication. The HW Client tab, shown in Figure 4-25, permits you to enable the following authentication features:

- Require Interactive Hardware Client Authentication**—When this field is checked, the username and password that were configured on the VPN 3002 Hardware Client are ignored. The first user connected to the VPN 3002 Hardware Client that wants to begin using secure IPsec communications is prompted to enter a valid username and password. The method of authentication was selected earlier on the group's IPsec tab. Once the initial user establishes the IPsec tunnel, no other users are prompted for the tunnel authentication username and password.

- **Require Individual User Authentication**—You can also require all other users connected to the VPN 3002 Hardware Client to authenticate before using the IPSec tunnel by checking this attribute box. Each user is prompted for a username and password and is authenticated using whatever method the IPSec group requires.
- **User Idle Timeout**—The default idle timeout for a user’s connection is 30 minutes. The smallest idle timeout period you can use is 1 minute. You can enter 0 to tell the concentrator to never drop an idle connection. When a user’s connection has been idle for the period of time specified by the idle timeout period, the concentrator drops the connection.
- **Cisco IP Phone Bypass**—Checking this field tells the VPN concentrator not to negotiate individual user authentication for IP phones.
- **Allow Network Extension Mode**—You can configure the VPN 3000 Concentrator to support Network Extension mode with VPN 3002 Hardware Clients in site-to-site networks by checking this field. The VPN 3002 Hardware Client must also be configured to support network extension mode, or the two devices can never connect to one another. The default connection mode is Port Address Translation (PAT).

Figure 4-25 Configuration / User Management / Groups / Modify > HW Client

Configuration | User Management | Groups | Modify vpngroup02

This section lets you add a group. Check the **Inherit?** box to set a field that you want to default to the base group value. Uncheck the **Inherit?** box and enter a new value to override base group values.

Identify | General | IPSec | Client Config | Client FW | **HW Client** | PPTP/L2TP

Hardware Client Parameters			
Attribute	Value	Inherit?	Description
Require Interactive Hardware Client Authentication	<input type="checkbox"/>	<input checked="" type="checkbox"/>	Check to require the hardware client to be interactively authenticated at each connection attempt.
Require Individual User Authentication	<input type="checkbox"/>	<input checked="" type="checkbox"/>	Check to require users behind a hardware client to be authenticated.
User Idle Timeout	30	<input checked="" type="checkbox"/>	Enter the session idle timeout in minutes. Use 0 for no timeout.
Cisco IP Phone Bypass	<input type="checkbox"/>	<input checked="" type="checkbox"/>	Check to allow Cisco IP Phones to bypass Individual User Authentication behind a hardware client.
Allow Network Extension Mode	<input type="checkbox"/>	<input checked="" type="checkbox"/>	Check to allow hardware clients using Network Extension Mode to connect.

Add Cancel

Modify Groups—PPTP/L2TP Tab

If you selected PPTP, L2TP, or L2TP over IPSec as an allowable tunneling protocol to be used for VPN connections, you might need to make adjustments to the attributes displayed on the PPTP/L2TP Tab, shown in Figure 4-26. Client and VPN concentrator settings must match during VPN tunnel negotiations, or the tunnel is not established. The following attributes are shown on this screen:

- **Use Client Address**—You can allow clients to supply their own address for the client end of the VPN tunnel. This is not a good idea from a security perspective, so be careful about

enabling this capability. The default mode for this attribute is disabled, forcing the VPN concentrator to supply the address through one of the various means available to the concentrator.

- **PPTP Authentication Protocols**—During tunnel negotiation, prospective peers generally authenticate one another through some mechanism. By checking none of the available options, you can permit the tunnel to be negotiated with no authentication, but you should only use that for test purposes. The available authentication protocols are as follows:
 - **PAP**—The Password Authentication Protocol (PAP) passes the username and password in clear text and is therefore not secure. Although this is the default setting, it is not a recommended choice for a secure environment. PAP does not provide data encryption.
 - **CHAP**—The Challenge-Handshake Authentication Protocol (CHAP) is also permitted by default, but is also not particularly secure. In response to a challenge from the server, the client encrypts the challenge plus password and returns that to the server along with the clear text username. CHAP does not provide data encryption.
 - **MSCHAPv1**—The Microsoft Challenge-Handshake Authentication Protocol version 1 (MSCHAPv1) is more secure than CHAP because the server only stores and compares encrypted passwords. MSCHAPv1 can encrypt data using the Microsoft Point-to-Point Encryption (MPPE) Protocol.
 - **MSCHAPv2**—The Microsoft Challenge-Handshake Authentication Protocol version 2 (MSCHAPv2) is a step up from MSCHAPv1 because it requires mutual client-server authentication. MPPE can also be used here for data encryption using keys that are unique for each session. MSCHAPv2 also uses different keys for the send and receive functions.
 - **EAP Proxy**—The Extensible Authentication Protocol (EAP) Proxy lets the VPN concentrator offload the authentication process to an external RADIUS server, providing additional authentication services such as EAP/MD5, Smartcards and certificates (EAP/TLS), and RSA SecurID (EAP/SDI). EAP Proxy does not support encryption.
- **PPTP Encryption**—Select the type of PPTP encryption that you want to use from these options:
 - **Required**—If you select this option, clients must use MPPE encryption. This means that you can only select MSCHAPv1 and MSCHAPv2 as the allowable authentication protocols when using this option. You must also select either 40-bit and/or 128-bit encryption in this category.
 - **Require Stateless**—Under this encryption scheme, the encryption key is changed with each packet transferred.

- **40-bit**—Clients can use the RSA RC4 encryption algorithm using a 40-bit key when this option is checked.
- **128-bit**—Clients can use the RSA RC4 encryption algorithm using a 128-bit key when this option is checked.
- **PPTP Compression**—If many of your clients connect via dial-up connections, you might want to enable PPTP compression to decrease the amount of data being transferred. If you enable compression, the Microsoft Point-to-Point Compression (MPPC) algorithm is used.
- **L2TP Authentication Protocols**—L2TP authentication protocol options are the same as the PPTP options previously discussed.
- **L2TP Encryption**—L2TP encryption options are the same as the PPTP options previously discussed.
- **L2TP Compression**—L2TP compression options are the same as the PPTP options previously discussed.

Figure 4-26 Configuration | User Management | Groups | Modify > PPTP/L2TP

Configuration | User Management | Groups | Modify vpngroup02

This section lets you add a group. Check the **Inherit?** box to set a field that you want to default to the base group value. Uncheck the **Inherit?** box and enter a new value to override base group values.

Identity | General | IPsec | Client Config | Client FW | HW Client | **PPTP/L2TP**

PPTP/L2TP Parameters			
Attribute	Value	Inherit?	Description
Use Client Address	<input type="checkbox"/>	<input checked="" type="checkbox"/>	Check to accept and use an IP address received from the client.
PPTP Authentication Protocols	<input type="checkbox"/> PAP <input checked="" type="checkbox"/> CHAP <input checked="" type="checkbox"/> MSCHAPv1 <input type="checkbox"/> MSCHAPv2 <input type="checkbox"/> EAP Proxy	<input checked="" type="checkbox"/>	Check the authentication protocols allowed by this group. The choices available are determined by base group settings. Refer to the online help for authentication protocol dependencies. Unchecking all options means that no authentication is required.
PPTP Encryption	<input type="checkbox"/> Required <input type="checkbox"/> Require Stateless <input checked="" type="checkbox"/> 40-bit <input checked="" type="checkbox"/> 128-bit	<input checked="" type="checkbox"/>	Select the allowed encryption methods for PPTP connections for this group.
PPTP Compression	<input type="checkbox"/>	<input checked="" type="checkbox"/>	Check to enable compression for PPTP connections for this group.
L2TP Authentication Protocols	<input type="checkbox"/> PAP <input checked="" type="checkbox"/> CHAP <input checked="" type="checkbox"/> MSCHAPv1 <input type="checkbox"/> MSCHAPv2 <input type="checkbox"/> EAP Proxy	<input checked="" type="checkbox"/>	Check the authentication protocols allowed by this group. The choices available are determined by base group settings. Refer to the online help for authentication protocol dependencies. Unchecking all options means that no authentication is required.
L2TP Encryption	<input type="checkbox"/> Required <input type="checkbox"/> Require Stateless <input checked="" type="checkbox"/> 40-bit <input checked="" type="checkbox"/> 128-bit	<input checked="" type="checkbox"/>	Select the allowed encryption methods for L2TP connections for this group.
L2TP Compression	<input type="checkbox"/>	<input checked="" type="checkbox"/>	Check to enable compression for L2TP connections for this group.

Add Cancel

Advanced Configuration of the VPN Concentrator

The previous sections of this chapter looked at a small part of the Configuration portion of the VPN Manager. There is much more to the Manager than installing groups, users, or system identification. This section looks at the other aspects of the Configuration portion of the VPN Manager.

Configuration | System

The functions that fall under the Configuration | System section have to do with configuring parameters for system-wide functions in the VPN concentrator. The following subcategories under System let you control the VPN concentrator:

- Configuration | System | Servers
- Configuration | System | Address Management
- Configuration | System | Tunneling Protocols
- Configuration | System | IP Routing
- Configuration | System | Management Protocols
- Configuration | System | Events
- Configuration | System | General
- Configuration | System | Client Update
- Configuration | System | Load Balancing Cisco VPN Clients
- Configuration | User Management
- Configuration | Policy Management

The following sections describe each subcategory in more detail.

Configuration | System | Servers

The Configuration | System | Servers section of the VPN Manager allows you to configure the various types of servers that communicate with the concentrator. Those servers include the following:

- **Authentication Servers**—Used for user authentication
- **Accounting Servers**—Used for RADIUS user accounting
- **DNS Servers**—Domain Name System address lookup functions
- **DHCP Servers**—Dynamic Host Configuration Protocol to assign IP addresses for client connections
- **Firewall Servers**—Firewall enforcement by means of the Zone Labs Integrity Server

- **NTP Servers**—Network Time Protocol to ensure that all systems use the same time for ease of synchronizing log entries
- **Internal Authentication**—Used for user authentication

Configuration | System | Address Management

When an IPSec tunnel is established between a VPN concentrator and client, a new set of IP addresses is required to identify the endpoints of the tunnel. This section of the VPN Manager allows you to define how these addresses are managed.

The Assignment portion of Address Management allows you to select the methods that can be used to assign addresses. Quick Configuration used this portion as part of its setup steps.

The Pools portion of Address Management allows you to define a pool of internal addresses that the concentrator draws from when assigning addresses to clients.

Configuration | System | Tunneling Protocols

Cisco VPN 3000 Concentrators are capable of establishing tunnels using the three most popular VPN tunneling protocols:

- PPTP
- L2TP
- IPSec

To provide support for the Microsoft Windows 2000 VPN client, the VPN concentrators also support L2TP over IPSec.

This section of the VPN Manager allows you to configure the parameters that are associated with each of these protocols.

Configuration | System | IP Routing

Cisco VPN 3000 Concentrators have the ability to act as routers for IP traffic. This allows the concentrator to communicate with other routers in the network to determine the best path for traffic to take. This section of the VPN Manager allows you to configure the following:

- **Static Routes**—Manually configured routing tables
- **Default Gateways**—Routes for traffic for which routes cannot be determined
- **OSPF**—Open Shortest Path First routing protocol
- **OSPF Areas**—Subnet areas within the OSPF domain
- **DHCP**—Dynamic Host Configuration Protocol global parameters

- **Redundancy**—Virtual Router Redundancy Protocol parameters
- **Reverse Route Injection**—Reverse Route Injection global parameters

Routing Information Protocol (RIP) and interface-specific OSPF parameters are configured on the network interfaces. You access the interfaces to make those configurations through the Configuration | Interfaces screen.

Configuration | System | Management Protocols

The Configuration | System | Management Protocols portion of the VPN Manager allows you to control various management protocols and servers. These utilities can be an asset to you in managing your total network. Those management protocols are as follows:

- **FTP**—File Transfer Protocol
- **HTTP/HTTPS**—Hypertext Transfer Protocol and HTTP over SSL (Secure Sockets Layer) protocol
- **TFTP**—Trivial File Transfer Protocol
- **Telnet**—Terminal emulation protocol and Telnet over SSL
- **SNMP**—Simple Network Management Protocol
- **SNMP Community Strings**—Identifiers for valid SNMP clients
- **SSL**—Secure Sockets Layer Protocol
- **SSH**—Secure Shell
- **XML**—Extensible Markup Language

Configuration | System | Events

Significant occurrences within or that could affect a VPN 3000 Concentrator are classified as events. Typical events include alarms, traps, error conditions, network problems, task completions, breaches of threshold levels, and status changes. Events are stored in an event log in nonvolatile memory. Events can also be sent to a backup server via FTP or to Syslog servers. Events can be identified to trigger console messages, send e-mail messages, or send SNMP system traps.

Event attributes include class and severity level, as follows:

- **Event Class**—Specifies the source of the event and refers to a specific hardware or software subsystem within the VPN concentrator.
- **Event Severity Level**—Indicates how serious or significant the event is. Level 1 is the most significant.

Configuration | System | General

The General section of the VPN Manager enables you to configure these general VPN concentrator parameters:

- **Identification**—System name, contact person, system location
- **Time and Date**—System time and date
- **Sessions**—The maximum number of sessions
- **Authentication**—General authentication parameters

Configuration | System | Client Update

You can configure the Cisco VPN 3000 Concentrators to manage client updates for VPN Client and VPN 3002 Hardware Clients. In the case of the software clients, the concentrator notifies the clients of the acceptable client versions and provides the location where the appropriate versions can be obtained. For VPN 3002 Hardware Clients, the concentrator pushes the correct version to the client via TFTP.

This section of the VPN 3000 Concentrator Manager lets you configure the client update feature, as follows:

- **Enable**—Enables or disables client update
- **Entries**—Configures updates by client type, acceptable firmware and software versions, and their locations

Configuration | System | Load Balancing Cisco VPN Clients

When you have two or more VPN 3000 Concentrators on the same subnet handling remote access VPN services, you can group those devices together to perform load balancing across the devices. The private and public subnets are grouped into a virtual cluster. One of the concentrators acts as the cluster master and directs incoming calls to the device that has the smallest load, including itself. If, for any reason, the master fails, one of the other concentrators in the cluster takes over the role.

Clients first connect to the virtual IP address of the cluster. The cluster master intercepts the call and sends the client the public IP address of the least-loaded available concentrator. The client then uses that IP address to initiate the VPN tunnel with the concentrator. If a concentrator in the cluster fails, the terminated clients immediately try to reconnect with the virtual IP, and the cluster master reassigns them to available devices.

After you have made certain that the public and private interfaces have been fully configured and are operational, you use this section of the VPN 3000 Concentrator Manager to define the load-sharing cluster.

Configuration | User Management

Configuration | User Management is the section that you used in the “Configuring IPSec with Preshared Keys Through the VPN 3000 Concentrator Series Manager” section of this chapter to configure the group for remote access with preshared keys. In addition to working with specific groups, this section is used to configure the Base Group and to manage user accounts for the internal authentication database.

With the default settings, new groups inherit the attributes of the Base Group. Those attributes can be individually overridden for each group so that you can have a variety of groups with different properties. You could have a group using L2TP, one using IPSec with preshared keys, another using IPSec with digital certificates, another using RADIUS for user authentication, and still another using the concentrator’s internal database for user authentication.

If you are using the concentrator for internal authentication and have defined your groups, this section of the VPN Manager also allows you to create and manage user accounts. User accounts inherit the attributes of their group, and user accounts can only belong to one group. If you do not explicitly assign a user account to a group, it inherits the attributes of the Base Group.

Configuration | Policy Management

Policies control the actions of users as they connect to the VPN concentrator. User management determines which users are allowed to use the device. Policy management determines when users can connect, from where they can connect, and what kind of data are permitted in the tunnels. The section of the VPN Manager established filters that determine whether to forward or drop packets and whether to pass the traffic through a tunnel or to send it in the clear. Filters are applied to interfaces, groups, and users.

The Policy Management section contains the following sections:

- **Access Hours**—Establishes when remote users can access the VPN concentrator.
- **Traffic Management**—Controls what data traffic can flow through the VPN concentrator. Traffic Management is further divided into the following configuration sections:
 - **Network Lists**—Allows you to group lists of networks together as single objects.
 - **Rules**—Provides detailed parameters that let you specify the handling of data packets.
 - **SAs**—Lets you choose the options to be used in establishing IPSec Security Associations. This is where you set the authentication, encryption, encapsulation, and SA lifetime. You can modify predefined SAs or create your own.
 - **Filters**—Lets you combine the network lists, rules, and SAs into single packages that you can then apply to interfaces, groups, and users.
 - **NAT**—The Cisco VPN 3000 Concentrators can perform Network Address Translation, which you would configure in this section.

Installing and Configuring the VPN Client

14 Configuring the IPsec Windows Client

The Cisco VPN Client is packaged with every VPN concentrator sold by Cisco. The VPN Client can be installed on several different operating systems, including Linux, Sun Solaris, Apple MAC OS X, and Microsoft Windows. This section looks at the Microsoft Windows version of the VPN Client.

The following topics are covered in this section:

- Overview of the VPN Client
- VPN Client features
- VPN Client installation
- VPN Client configuration

Overview of the VPN Client

The Microsoft Windows version of the VPN Client runs on Windows 95, 98, 98 SE, Me, NT, 2000, and XP platforms. The client is designed to work as a remote access client connecting through a secure data tunnel to an enterprise network over the Internet. This permits remote users to access the services of a private network as though the users were attached directly to the network, with the security of encrypted communications between the client and the host.

To use the VPN Client after it has been installed, the user first connects to the Internet and then starts the VPN Client to negotiate a tunnel with the VPN host. For remote access services, that host is most commonly a VPN concentrator, but it could be a router or firewall, or some other network device.

To start the VPN Client from a Windows-based PC, select **Start, Programs, Cisco Systems VPN Client**, and then select one of the following programs:

- **Certificate Manager**—Manage digital certificates for the client to be used when authenticating with VPN devices.
- **Help**—View the complete online manual with full instructions on using the VPN Client application.
- **Log Viewer**—View events from the log file.
- **Set MTU**—Control the maximum transmission unit (MTU) size that the VPN Client is to use to communicate with the host.

- **Uninstall VPN Client**—Uninstall the application. You can choose to retain connection and certificate information.
- **VPN Dialer**—Manage connection information and start a connection with a VPN host device. This poorly named function is the main functional area of the VPN Client.

You can use the VPN Client with dial-up, ISDN, cable, or DSL modems as well as with direct LAN connections. How you get to the Internet does not matter to the VPN Client. The only requirement is that the client device can “see” the host device using TCP/IP.

VPN Client Features

The VPN Client is a feature-packed application. Most of the functions of the client are handled automatically and require little configuration. This section describes the important features of the Cisco VPN Client.

Program features include the following:

- Browser-based, context-sensitive HTML help
- VPN 3000 Series Concentrator support
- Command-line interface to the VPN Dialer application
- Access to local LAN resources while connected through a secure VPN
- Automatic VPN Client configuration option
- Log Viewer application to collect, view, and analyze events
- Ability to set the MTU size
- Application launcher
- Automatic connection via Microsoft Dial-Up Networking and other third-party dialers
- Software update notifications from the connecting VPN device
- Launch software update site from update notification

NT features include the following:

- Password expiration information from RADIUS authentication servers
- Start Before Logon, providing the ability to establish a VPN connection before logging on to a Windows NT platform
- Automatic disconnect disable when logging off to allow for roaming profile synchronization

IPSec features include the following:

- IPSec tunneling protocol
- Transparent tunneling
- IKE key management protocol

- IKE keepalives
- Split tunneling
- LZS data compression

Authentication features include the following:

- User authentication via the following:
 - VPN concentrator internal database
 - RADIUS
 - NT Domain (Windows NT)
 - RSA (formerly SDI) SecurID or SoftID
- Certificate Manager to manage client identity certificates
- Ability to use Entrust Entelligence certificates
- Ability to authenticate using smart cards with certificates

Firewall features include the following:

- Support for Cisco Secure PIX Firewall platforms
- Support for the following personal firewalls:
 - Cisco Integrated Firewall (CIF)
 - ZoneAlarmPro 2.6.3.57
 - ZoneAlarm 2.6.3.57
 - BlackIce Agent and BlackIce Defender 2.5
- Centralized Protection Policy provides support for firewall policies pushed to the VPN Client from the VPN 3000 Concentrator.

VPN Client IPSec attributes include the following:

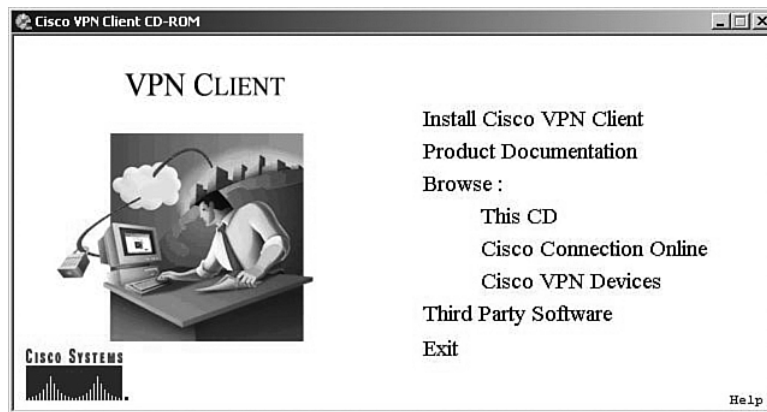
- Main and aggressive modes for negotiating phase 1 of establishing ISAKMP Security Associations
- Authentication algorithms:
 - HMAC (Hashed Message Authentication Coding) with MD5 (Message Digest 5) hash function
 - HMAC with SHA-1 (Secure Hash Algorithm) hash function
- Authentication modes:
 - Preshared keys
 - X.509 Digital Certificates
- Diffie-Hellman Groups 1, 2, and 5

- Encryption algorithms:
 - 56-bit DES
 - 168-bit Triple-DES
- Extended Authentication (XAUTH)
- Mode Configuration (also known as ISAKMP Configuration Method)
- Tunnel Encapsulation Mode
- IP compression (IPCOMP) using LZS

VPN Client Installation

Installing the VPN Client is a simple task. System requirements call for 10 MB of hard drive space and up to 64 MB of RAM for Windows 2000 systems. Once you have confirmed those requirements, simply insert the Cisco VPN Client CD-ROM into the system and allow the Autorun program to start, as shown in Figure 4-27.

Figure 4-27 *Cisco VPN Client Autorun*



Click the option to **Install Cisco VPN Client**. The system might respond with a message like the one shown in Figure 4-28, stating that the installer needs to disable the IPSec Policy Agent. Simply click the **Yes** button to continue the installation process.

Figure 4-28 *Initial Warning Message*



The Welcome screen appears, as shown in Figure 4-29. Click **Next** to continue.

Figure 4-29 *VPN Client Install Setup Welcome*

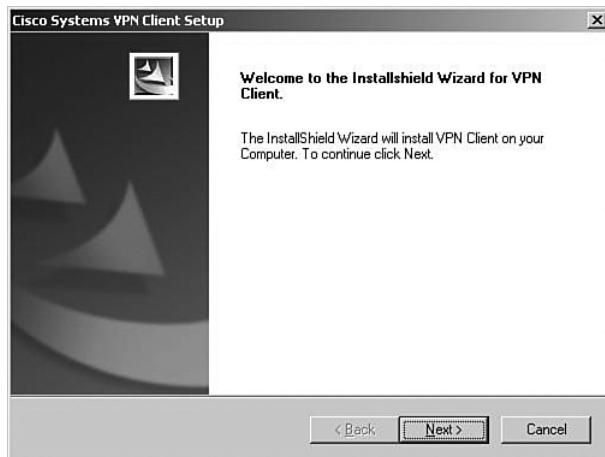
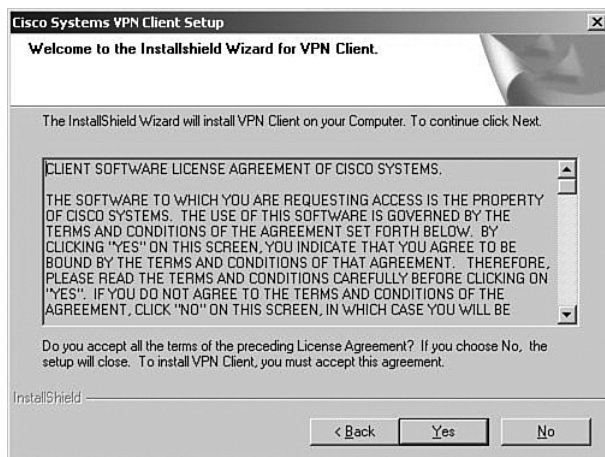


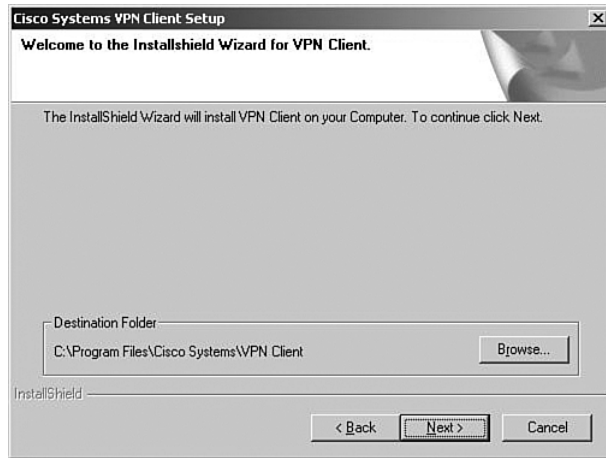
Figure 4-30 shows the next screen to be displayed, the license agreement screen. Scroll down through the agreement, and then click **Yes** to continue if you agree to the terms of the license agreement.

Figure 4-30 *VPN Client License Agreement*



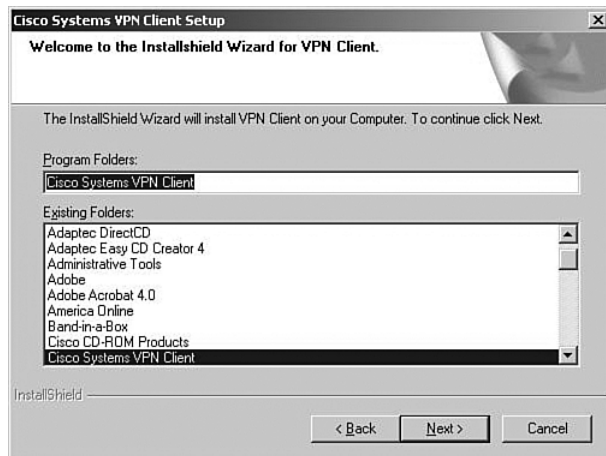
The file location screen is displayed, as shown in Figure 4-31. To accept the default location, click **Next**. If not, click **Browse** to select the folder where the installation wizard is to install the client application.

Figure 4-31 *VPN Client Install File Location*



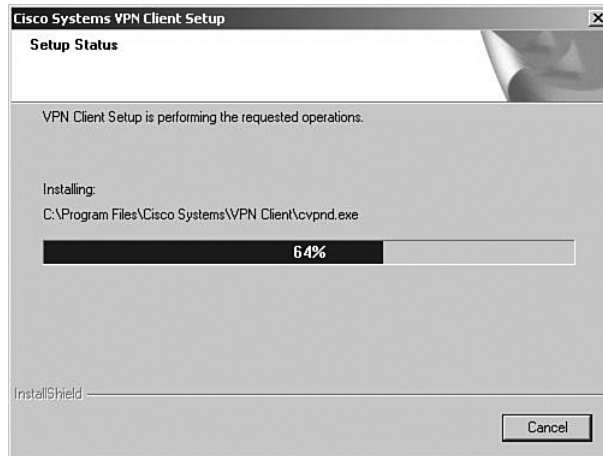
The next screen to be displayed, shown in Figure 4-32, asks you to select the Windows folder for the application. Click **Next** to accept the default, or select another location for the application.

Figure 4-32 *VPN Client Install Windows Folder Selection*



The installation wizard then copies the files from the CD to your system, as shown in Figure 4-33. This portion of the installation takes less than a minute.

Figure 4-33 *Cisco VPN Client Installation*



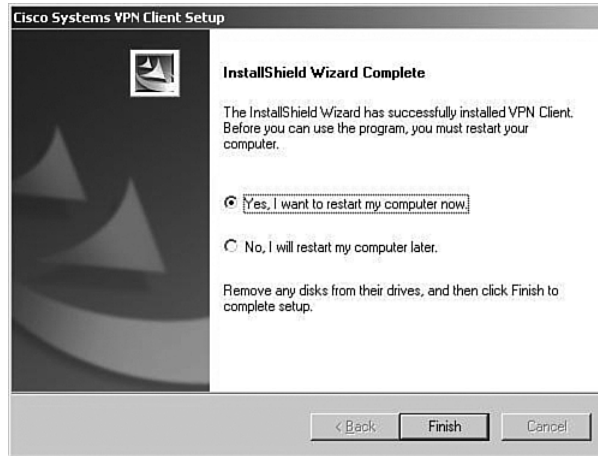
The installation wizard then updates the Windows Registry settings. While it does this, the wizard presents the message shown in Figure 4-34. While the message indicates that it can take several minutes, the wizard is, in fact, fast in accomplishing this task.

Figure 4-34 *VPN Client Install Network Settings*



The final screen of the installation process is shown in Figure 4-35. After the installation has been completed, you must reboot the Windows system. The completion screen gives you the option of rebooting when you click the Finish button or waiting until a later time to restart the system. Make your selection and click **Finish**.

This is a simple installation process. As a systems administrator, you could provide the application to your users with simple instructions, especially if you want them to use the default settings.

Figure 4-35 *VPN Client Installation Complete*

VPN Client Configuration

The configuration process is almost as easy as the installation process. The user must enter several pieces of information. Your installation instructions should provide all the entries that your users must make.

To start the configuration process, start the VPN Client application. From the Windows Desktop, choose **Start, Programs, Cisco Systems VPN Client** to display the Option menu shown in Figure 4-36. The next step is not self-evident. To start the client, click the **VPN Dialer** menu option.

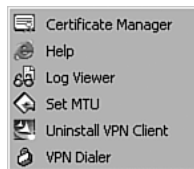
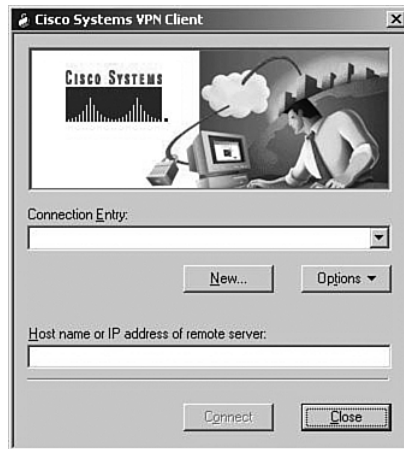
Figure 4-36 *Starting the Cisco VPN Client*

Figure 4-37 shows the main interface screen for the VPN Client. Notice that the Connection Entry window is blank, indicating that you have not yet configured the connection information. The Connect button is also grayed out and stays that way until you have a valid connection defined. Create the first connection entry; click **New** to begin that process.

Figure 4-37 *Connection Entry Screen*

The first screen of the creation process is shown in Figure 4-38. On this screen, you identify the connection by supplying a name and a brief description. The screen is initially blank. The name **CorpConnect** and the description **Connection to the Corporate Network via VPN** were added to describe the connection. Try to make the name fairly descriptive because it is used to make the connection. After you have entered a name and description, click **Next**.

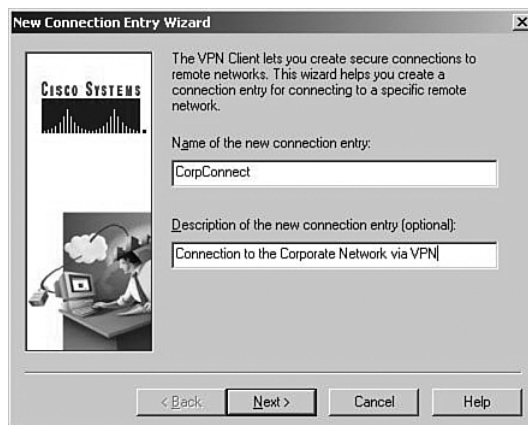
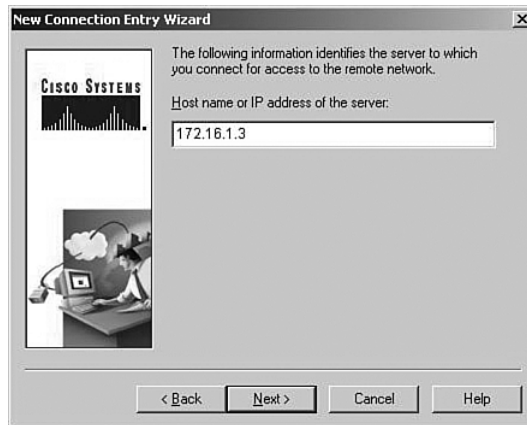
Figure 4-38 *Create New Connection*

Figure 4-39 shows the next screen to be displayed. This screen asks you to identify the VPN server to which you will be connecting. In this case, you are connecting to the VPN 3000 Concentrator that you configured in the “Configuring IPsec with Preshared Keys Through the

VPN 3000 Concentrator Series Manager” section of this chapter. Enter either the IP address of the device or the fully qualified domain name (FQDN), if you know it. The public IP address of the VPN concentrator is required, so enter 172.16.1.3 to reach the concentrator you configured earlier. Click **Next** after you have identified the host server.

Figure 4-39 *New Connection Address*



Because you have not yet installed any digital certificates onto your PC, the next screen presents only one option to use for authenticating the IPSec connection. In Figure 4-40 you can see that the Certificate option is grayed out. To configure the client to use a preshared key for the IPSec connection, simply enter the IPSec group name and password in the appropriate fields of the Group Access Information section.

Figure 4-40 *Entering the Preshared Key*



The group name that you established earlier was **vpngroup02**. Enter that in the Name field and the associated password into the Password and Confirm Password fields. The password for the IPSec group is the preshared key for the IPSec connection authentication. Click **Next** to continue.

That's all there is to it. Figure 4-41 shows that the new VPN connection, CorpConnect, has been successfully created. Notice that you did not enter any IKE or IPSec configuration information. Those values are pushed from the VPN concentrator during the initial connection.

Because anyone with the VPN Client and the correct group name and password can now create a secure connection to your VPN 3000 Concentrator, you can see how important the group password is to the security of the system. Be sure to use a strong password for this purpose, and exercise strict control over issuing the password. Also, consider changing the password frequently, even though your user community might object.

Click **Finish** to complete the creation process.

Figure 4-41 *New Connection Complete*



Clicking Finish returns you to the main VPN Client window, shown in Figure 4-42. Notice that CorpConnect now shows in the Connection Entry window and the IP address of the remote server shows in the lower window. Also notice that the Connect button is now active.

If you had additional connections defined to different servers or for different purposes (for example, stricter security), you could access those other connections by clicking the arrow to open the drop-down menu.

Figure 4-42 *Using the New VPN Connection*

To connect to the VPN 3000 Concentrator, simply click the Connect button. The client attempts to negotiate IKE and IPSec SAs with the concentrator. If that is successful, the IPSec tunnel is created and the client prompts you for your username and password. Once that has been authenticated, you can begin using the VPN Client for secure remote access to the VPN concentrator.

Foundation Summary

The Foundation Summary is a collection of tables and figures that provides a convenient review of many key concepts in this chapter. For those of you already comfortable with the topics in this chapter, this summary could help you recall a few details. For those of you who just read this chapter, this review should help solidify some key facts. For anyone doing his or her final preparation before the exam, these tables and figures are hopefully a convenient way to review the material the day before the exam.

Types of Preshared Keys

The types of preshared keys are as follows:

- **Unique**—Tied to a specific IP address
- **Group**—Tied to a group
- **Wildcard**—Not tied to anything

VPN 3000 Concentrator CLI Quick Configuration Steps

The steps to VPN 3000 Concentrator CLI Quick Configuration are as follows:

- Step 1** Boot the VPN concentrator with default configuration.
- Step 2** Login as admin/admin.
- Step 3** Set the system time.
- Step 4** Set the system date.
- Step 5** Set the time zone.
- Step 6** Set the daylight-savings time support.
- Step 7** Enter an IP address for the Private interface.
- Step 8** Enter a subnet mask for the Private interface.
- Step 9** Select the speed of the interface.
- Step 10** Select the duplex mode of the interface.
- Step 11** Save and exit the CLI.

VPN 3000 Concentrator Browser-Based Manager Quick Configuration Steps

The steps to the VPN 3000 Concentrator browser-based Manager Quick Configuration are as follows:

- Step 1** Ping the VPN concentrator from the administrator PC to verify connectivity.
- Step 2** Start the web browser.
- Step 3** Enter the address of the VPN concentrator (be sure to use https:// if you need to enable the VPN concentrator's SSL Certificate on your browser).
- Step 4** Log in as admin/admin.
- Step 5** Select **Click here to start Quick Configuration**.
- Step 6** Select hotlink to Ethernet 2 (Public) interface.
- Step 7** Enter the IP address, subnet mask, speed, and duplex mode.
- Step 8** Verify the system name, date, time, time zone, and DST support.
- Step 9** Enter the DNS server address.
- Step 10** Enter the domain name.
- Step 11** Enter the default gateway address.
- Step 12** Select the tunneling protocols to use—IPSec.
- Step 13** Select the methods of assigning IP address for the IPSec tunnel endpoints.
- Step 14** Choose the method for user authentication (Internal Server).
- Step 15** Add usernames and passwords.
- Step 16** Supply the IPSec group name and password.
- Step 17** Change the admin password.
- Step 18** Click the **Save Needed** icon to save the configuration changes.

VPN Client Installation Steps

The steps for installing the VPN Client are as follows:

- Step 1** Insert the Cisco VPN Client CD into your CD-ROM drive.
- Step 2** View the CD's menu after Autorun starts the CD.
- Step 3** Select **Install Cisco VPN Client**.

- Step 4** Click **Yes** to permit disabling IPSec Policy Agent (if asked).
- Step 5** Click **Next** on the Welcome screen.
- Step 6** Read and accept the license agreement.
- Step 7** Click **Next** to accept the default file location.
- Step 8** Click **Next** to accept the default application location.
- Step 9** Select the reboot option (now or later) and click **Finish**.

VPN Client Configuration Steps

The steps for configuring the VPN Client are as follows:

- Step 1** Choose **Start, Programs, Cisco Systems VPN Client, VPN Dialer** to start the application.
- Step 2** Click **New** to create a new connection.
- Step 3** Enter the connection name and description.
- Step 4** Enter the IP address or host name of the VPN concentrator.
- Step 5** Enter the IPSec group name and password that you created on the VPN concentrator.
- Step 6** Click **Finish** to complete the connection creation.

NOTE You can customize the installation process to suit different client configurations. See the Cisco website, www.cisco.com, for more information.

VPN Client Program Options

VPN Client program options include the following:

- Certificate Manager
- Help
- Log Viewer
- Set MTU
- Uninstall VPN Client
- VPN Dialer

Limits for Number of Groups and Users

Table 4-4 shows the maximum number of groups and users.

Table 4-4 *Maximum Combined Groups and Users per VPN Model*

Model	Maximum Combined Number of Groups and Users
3005	100
3015	100
3030	500
3060	1000
3080	1000

Complete Configuration Table of Contents

Table 4-5 shows the complete configuration table of contents (TOC).

Table 4-5 *Complete Expansion of the Configuration TOC*

Configuration	
>	Interfaces
>	System
>	Servers
>	> Authentication
>	> Accounting
>	> DNS
>	> DHCP
>	> NTP
>	> Parameters
>	> Hosts
>	Address Management
>	> Assignment
>	> Roots

continues

Table 4-5 Complete Expansion of the Configuration TOC (Continued)

Configuration (Continued)	
>	System (Continued)
>	Tunneling Protocols
>	PPTP
>	L2TP
>	IPSec
>	> LAN-to-LAN
>	> IKE Proposals
>	> IPSec over TCP
>	IP Routing
>	Static Routes
>	Default Gateways
>	OSPF
>	OSPF Areas
>	DHCP
>	Redundancy
>	Reverse Route Injection
>	Management Protocols
>	FTP
>	HTTP/HTTPS
>	TFTP
>	Telnet
>	SNMP
>	SNMP Communities
>	SSL
>	SSH
>	XML

Table 4-5 Complete Expansion of the Configuration TOC (Continued)

Configuration (Continued)	
>	System (Continued)
	> Events
	> General
	> FTP Backup
	> Classes
	> Trap Destinations
	> Syslog Servers
	> SMTP Servers
	> E-mail Recipients
	> General
	> Identification
	> Time and Date
	> Sessions
	> Authentication
	> Client Update
	> Enable
	> Entries
	> Load Balancing
>	User Management
	> Base Group
	> Groups
	> Users
>	Policy Management
	> Access Hours
	> Traffic Management
	> Network Lists
	> Rules
	> SAs

continues

Table 4-5 Complete Expansion of the Configuration TOC (Continued)

Configuration (Continued)	
>	Policy Management (Continued)
	> Traffic Management (Continued)
	> Filters
	> NAT
	> Enable
	> Rules

Complete Administration Table of Contents

Table 4-6 shows the complete administration table of contents (TOC).

Table 4-6 Complete Expansion of the Administration TOC

Administration	
>	Administer Sessions
>	Software Update
	> Concentrator
	> Clients
>	System Reboot
>	Ping
>	Monitoring Refresh
>	Access Rights
	> Administrators
	> Access Control List
	> Access Settings
	> AAA Servers
	> Authentication
>	File Management
	> Swap Config File
	> TFTP Transfer
	> File Upload
	> XML Export

Table 4-6 Complete Expansion of the Administration TOC (Continued)

Administration (Continued)	
>	Certificate Management
	> Enrollment
	> Installation

Complete Monitoring Table of Contents

Table 4-7 shows the complete monitoring table of contents (TOC).

Table 4-7 Complete Expansion of the Monitoring TOC

Monitoring	
>	Routing Table
>	Filterable Event Log
	> Live Event Log
>	System Status
>	Sessions
	> Protocols
	> Encryption
	> Top Ten Lists
	> Data
	> Duration
	> Throughput
>	Statistics
	> PPTP
	> L2TP
	> IPSec
	> HTTP
	> Events
	> Telnet
	> DNS
	> Authentication
	> Accounting
	> Filtering

continues

Table 4-7 Complete Expansion of the Monitoring TOC (Continued)

Monitoring (Continued)	
>	Statistics (Continued)
>	VRRP
>	SSL
>	DHCP
>	Address Pools
>	SSH
>	Load Balancing
>	Compression
>	Administrative AAA
>	NAT
>	MIP-II Stats
>	> Interfaces
>	> TCP/UDP
>	> IP
>	> RIP
>	> OSPF
>	> ICMP
>	> ARP Table
>	> Ethernet

Chapter Glossary

The following terms were introduced in this chapter or have special significance to the topics within this chapter.

cookie A piece of information sent by a web server to a web browser that the browser is expected to save and send back to the web server whenever the browser makes additional requests of the web server.

Extensible Markup Language (XML) A standard maintained by the World Wide Web Consortium (W3C). It defines a syntax that lets you create markup languages to specify information structures.

JavaScript Interpreted programming language from Netscape. Used on websites for such things as pop-up windows and image change during mouse rollover.

Network Time Protocol (NTP) Protocol built on top of TCP that ensures accurate local timekeeping with reference to radio and atomic clocks located on the Internet. This protocol is capable of synchronizing distributed clocks within milliseconds over long time periods.

Remote Authentication Dial-In User Service (RADIUS) Database for authenticating dial-up users and for tracking connection time.

Reverse Route Injection (RRI) Used to populate the routing table of an internal router running OSPF or RIP for remote VPN clients or LAN-to-LAN sessions.

Scalable Encryption Processing (SEP) VPN concentrator modules that perform hardware-based cryptographic functions, including random number generation, hash transforms (MD5 and SHA-1) for authentication, and encryption and decryption (DES and Triple-DES).

Security Dynamics International (SDI) authentication Third-party authentication services using token cards.

Secure Shell (SSH) Sometimes called Secure Socket Shell, a UNIX-based command interface and protocol for gaining access to a remote computer securely.

Secure Sockets Layer (SSL) Encryption technology for the web used to provide secure transactions, such as the transmission of credit card numbers for e-commerce.

Virtual Router Redundancy Protocol (VRRP) In installations of two or more VPN concentrators in a parallel, redundant configuration, VRRP provides automatic switchover to a backup system in case the primary system is out of service, thus ensuring user access to the VPN.

VPN concentrator Any of the Cisco VPN 3000 Series Concentrators.

VPN Manager Cisco VPN 3000 Concentrator Manager.

Q&A

As mentioned in Chapter 1, “All About the Cisco Certified Security Professional,” these questions are more difficult than what you should experience on the CCSP exam. The questions do not attempt to cover more breadth or depth than the exam; however, the questions are designed to make sure you know the answer. Rather than allowing you to derive the answer from clues hidden inside the question itself, your understanding and recall of the subject are challenged. Questions from the “Do I Know This Already?” quiz from the beginning of the chapter are repeated here to ensure that you have mastered the chapter’s topic areas. Hopefully, these questions will help limit the number of exam questions on which you narrow your choices to two options and guess!

You can find the answers to these questions in Appendix A, “Answers to the “Do I Know This Already” Quizzes and Q&A Sections.”

- 1 Where would you normally use unique preshared keys?

- 2 To use a web browser to access the VPN Manager application on VPN concentrators, what features must you enable on the browser?

- 3 What information is required to configure a LAN interface on the VPN concentrator?

- 4 What is the default administrator name and password for the GUI VPN Manager?

5 What options are available for addressing an IP interface on the IP Interfaces screen?

6 What is the maximum number of combined groups and users that can be supported on a VPN 3015 Concentrator?

7 What are the four subcategories under the Configuration option of the VPN Manager's TOC?

8 On the General tab of a group's Add screen, what options can you select for Access Hours?

9 What IPSec protocols are available from the default IPSec SA settings on the IPSec tab of the Group Add screen?

10 What are the nine subcategories under the Configuration | System option in the VPN Manager's table of contents?

11 Where does the VPN concentrator store system events?

12 What areas can be configured under the Traffic Management section of the Configuration | Policy Management section?

13 Where do you enter the preshared key so that a VPN Client can connect to a VPN concentrator?

14 What are the three types of preshared keys?

15 What types of interfaces are the Public and Private VPN interfaces?

16 Which interface do you need to configure using the browser-based VPN Manager?

- 17** What would you do if you needed to re-enter the Quick Configuration mode after you have completed the initial configuration of the VPN concentrator?

- 18** When the VPN Manager's Main window is displayed, how do you continue with the Quick Configuration that was started at the CLI?

- 19** What methods can be selected for assigning IP addresses to the tunnel endpoints from the Quick Configuration Address Assignment screen?

- 20** When using the VPN Manager, how can you tell that you have made changes to the active configuration?

- 21** What is an external group in the VPN Manager system?

- 22** What is the purpose of the SEP card assignment attribute on the General tab of the Group Add screen?

23 You would like to be able to pass DNS and WINS information from the VPN concentrator to the VPN Client. What Group option can you use to accomplish this?

24 What dynamic routing protocols are available on the VPN 3000 Concentrators?

25 What protocol does the VPN concentrator use to update software versions on Cisco VPN 3002 Hardware Clients?

26 How do you start the Cisco VPN Client installation process?

27 What methods can you use for user authentication on the Cisco VPN 3000 Series Concentrators?

28 What is a group preshared key?

- 29** When you boot up a Cisco VPN 3000 Concentrator with the default factory configuration, what happens?

- 30** If you supply an address of 144.50.30.24 and want to use a 24-bit subnet mask for the Private interface on a VPN concentrator, are you able to accept the default subnet mask offered by the VPN Manager?

- 31** What are the three major sections of the VPN Manager system?

- 32** The Quick Configuration system has displayed the System Info screen. What information, other than system date and time, can you enter on this screen?

- 33** What is the maximum number of combined groups and users that can be supported on a VPN 3060 Concentrator?

- 34** From where do users inherit attributes on the VPN concentrator?

35 What is the default number of simultaneous logins available to group members?

36 What is the purpose of IKE keepalives?

37 Where would you configure information for NTP and DHCP servers within the VPN Manager?

38 What is the most significant event severity level?

39 What Microsoft Windows operating systems can support the Cisco VPN Client?

40 What programs are available within the VPN Client installation?

41 What is a unique preshared key?

42 What type of cable does the console port require on VPN concentrators?

43 What is the default administrator name and password for VPN concentrators?

44 How do you get your web browser to connect to the VPN concentrator's manager application?

45 What is the first screen that appears when you click the **Click here to start Quick Configuration** option in the VPN Manager?

46 If you select Internal Server as the method of user authentication, what additional screen does the Quick Configuration system give you?

47 When do configuration changes become active on the Cisco VPN 3000 Series Concentrators?

48 When reviewing the list of attributes for a group, what does it mean when an attribute's Inherit? box is checked?

49 What is a realm in relation to user authentication?

50 What is split tunneling?

51 What management protocols can you configure on the VPN concentrator?

52 What is the process a VPN Client uses to connect to a VPN concentrator when load balancing is used between two or more VPN concentrators?

53 What variables can you supply during the installation process of the Cisco VPN Client?

54 What methods can be used for device authentication between VPN peers?

55 What is a wildcard preshared key?

56 What information do you need to supply in the CLI portion of Quick Configuration?

57 What is the last step you must take before moving from the CLI Quick Configuration mode to the browser-based Quick Configuration mode?

58 What hot keys are available in the standard toolbar of the VPN Manager?

59 What tunneling protocols does the VPN concentrator support?

60 When you select IPSec as the tunneling protocol, what screen does Quick Configuration present?

61 How many groups can a user belong to in the VPN concentrator's internal database?

62 What is the size range for user authentication passwords for internal users?

63 What does the Authentication option RADIUS with Expiry provide?

64 What tunneling protocol can be configured on the VPN concentrator to support the Microsoft Windows 2000 VPN client?

65 How does the VPN 3000 Concentrator handle software updates for VPN Software Clients?

66 How do you start the VPN Client on a Windows system?

Scenarios

The following scenarios and questions are designed to draw together the content of the chapter and exercise your understanding of the concepts. There might be more than one correct answer. The thought process and practice in manipulating each concept in the scenario are the goals of this section.

Scenario 4-1

Users at one of your small branch facilities dial in to your corporate access server for access to the Internet, e-mail, and other network services. This four-user group is one of your research and development teams, and each of the four users dials in to the access server using 56-kbps modems for network services. Their work is considered top secret by upper management. Because of the sensitive nature of their communications, you want to establish a VPN for them using IPsec.

At the same time, other users at other branch sites—your sales staff and other key personnel—frequently use laptops and home computers to connect to the corporate network through the Internet or through the access server. These users discuss sales figures and development projects and also require IPsec protection on their MS Exchange messaging and MS SQL database traffic.

You had considered using your router as a VPN server, but decided to use a Cisco VPN Concentrator because of its ability to authenticate users internally. You don't anticipate ever having more than 50 VPN clients active in your user community at any given time, and your employee base is stable.

As the senior security architect for your organization, how would you answer these questions?

- 1 Which VPN 3000 Concentrator would you purchase and install?
- 2 Would you use preshared keys or digital certificates for device authentication?
- 3 Would you depend on the internal authentication services of the VPN device, or would you use some other user authentication method?
- 4 How would you assign VPN addresses?
- 5 Would you permit split tunneling?
- 6 Would you use multiple IPsec groups? If so, why?
- 7 Which IPsec protocol would you use?
- 8 Which encryption protocol would you use?
- 9 Would you allow unrestricted access hours?
- 10 What would you set for idle timeout and maximum connect time?

Scenario 4-2

Your company sells donuts and has 60 shops located in a three-state area. These shops are each connected to the Internet using DSL circuits. You want to establish IPSec VPN connections from each shop through the Internet to the corporate network for sending/receiving e-mail, reporting sales, and ordering supplies.

You will be using a Cisco VPN 3030 Concentrator with no SEP modules. Device authentication is accomplished using preshared keys. User authentication is done through the NT Domain. The IP addresses of the DNS servers are 192.168.44.20 and 192.168.63.20. The IP addresses of the WINS servers are 192.168.44.25 and 12.168.63.25. No changes have been made to the default Base Group.

Create a group for the shops called DonutShops.

- 1 Indicate the settings that you would make on the group's General tab for each of the following attributes, and specify whether you would uncheck the Inherit? box.
 - Access Hours
 - Simultaneous Logins
 - Minimum Password Length
 - Allow Alphabetic-Only Passwords
 - Idle Timeout
 - Maximum Connect Time
 - Filter
 - Primary DNS
 - Secondary DNS
 - Primary WINS
 - Secondary WINS
 - SEP Card Assignment
 - Tunneling Protocols
 - Strip Realm
- 2 Indicate the settings that you would make on the group's IPSec tab for each of the following attributes, and specify whether you would uncheck the Inherit? box.
 - IPSec SA
 - IKE Peer Identity Validation
 - IKE Keepalives

- Reauthentication on Rekey
- Tunnel Type
- Group Lock
- Authentication
- IPComp
- Mode Configuration

Scenario Answers

The answers provided in this section are not necessarily the only correct answers. They merely represent one possibility for each scenario. The intention is to test your base knowledge and understanding of the concepts discussed in this chapter.

Should your answers be different (as they likely will be), consider the differences. Are your answers in line with the concepts of the answers provided and explained here? If not, reread the chapter, focusing on the sections that are related to the problem scenario.

Scenario 4-1 Answers

- 1 Concentrator model? The Cisco VPN 3005 Concentrator is probably adequate for this installation. If your company were growing quickly, you might opt for the 3015. It has about the same capabilities but is expandable, all the way to a 3080, if you ever needed the additional capacity.
- 2 Type of device authentication? Because this is a chapter on preshared keys, you would opt to use preshared keys. For this small user base, the maintenance for preshared keys should not be a big concern.
- 3 Authentication? Internal authentication was one of the reasons for choosing the concentrator over the router. The internal database keeps authentication on the same device and is flexible enough to meet the needs of this application.
- 4 Address assignment? Set aside a pool of 100 IP addresses and let the VPN concentrator assign the IP addresses from the pool. You could use DHCP, but that brings another network device into the picture. Keep it simple.
- 5 Split tunneling? Yes. The R&D group is going to need the Internet for research and the 56-kbps modems are going to be killers. Eliminate the need for encryption on trivial traffic to help this group out.
- 6 Multiple IPSec groups? It would make sense to use multiple IPSec groups. Some of your users might not need split tunneling, and you could use different rules for access time, idle timeout, or maximum connect times. You might want to set up functional groups such as R&D, Sales, Engineering, Accounting, Execs, and so on. You are only constrained by the 100 combined users and groups limitation on the concentrator.
- 7 IPSec protocol? ESP. AH is authentication only with no encryption. You would want to encrypt some of these data, especially for the R&D group.
- 8 Encryption? Probably Triple-DES. You could choose DES, but the extra security does not cost that much more in performance.

- 9 Unlimited access? This would be a group-by-group decision. Does the R&D team work around the clock or just during business hours? Do you need to set aside a regular maintenance window for network upgrades? Do the execs need unlimited access?
- 10 Idle timeout and maximum connect time? You probably want to drop connections after they have been idle for 20 to 30 minutes. There is no overpowering reason to establish limits on connect time. If you close the connection when it is idle, you should not have to worry about lengthy connections.

Scenario 4-2 Answers

- 1 General tab settings for the DonutShops group:
 - **Access Hours**—No Restrictions
 - **Simultaneous Logins**—1, uncheck Inherit?
 - **Minimum Password Length**—8
 - **Allow Alphabetic-Only Passwords**—No, uncheck Inherit?
 - **Idle Timeout**—30
 - **Maximum Connect Time**—0
 - **Filter**—None
 - **Primary DNS**—192.168.44.20, uncheck Inherit?
 - **Secondary DNS**—192.168.63.20, uncheck Inherit?
 - **Primary WINS**—192.168.44.25, uncheck Inherit?
 - **Secondary WINS**—192.168.63.25, uncheck Inherit?
 - **SEP Card Assignment**—You can leave these checked. Without SEP modules, this attribute has no effect.
 - **Tunneling Protocols**—Check only IPSec, uncheck Inherit?
 - **Strip Realm**—Leave unchecked. You will be using an external authentication service, so this field has no effect.
- 2 IPSec tab settings for the DonutShops group:
 - **IPSec SA**—ESP-3DES-MD5
 - **IKE Peer Identity Validation**—If supported by certificate
 - **IKE Keepalives**—Enabled
 - **Reauthentication on Rekey**—Enabled, uncheck Inherit?

- **Tunnel Type**—Remote access
- **Group Lock**—Disabled
- **Authentication**—NT Domain, uncheck Inherit?
- **IPComp**—None
- **Mode Configuration**—Enabled

