Debug crypto isakmp *Command Output (Continued)*

```
000579: Mar 26 21:00:28.904: ISAKMP:(1005):Input = IKE_MESG_FROM_AAA, IKE_AAA_GROUP_ATTR
000580: Mar 26 21:00:28.904: ISAKMP:(1005):Old State = IKE_CONFIG_AUTHOR_AAA_AWAIT  New
  State = IKE_P1_COMPLETE


000581: Mar 26 21:00:28.904: ISAKMP:(1005):Input = IKE_MESG_INTERNAL, IKE_PHASE1_COMPLETE
000582: Mar 26 21:00:28.904: ISAKMP:(1005):Old State = IKE_P1_COMPLETE  New State =
  IKE_P1_COMPLETE


000583: Mar 26 21:00:28.916: ISAKMP (0:1005): received packet from 172.16.1.40 dport 500
  sport 500 Global (R) QM_IDLE
000584: Mar 26 21:00:28.916: ISAKMP: set new node 1682961045 to QM_IDLE
000585: Mar 26 21:00:28.916: ISAKMP:(1005): processing HASH payload. message ID =
  1682961045
000586: Mar 26 21:00:28.916: ISAKMP:(1005): processing SA payload. message ID = 1682961045
000587: Mar 26 21:00:28.916: ISAKMP:(1005):Checking IPsec proposal 1
! - Begin IPSec process and check against proprosal 1
000588: Mar 26 21:00:28.916: ISAKMP: transform 1, ESP_AES
000589: Mar 26 21:00:28.916: ISAKMP:   attributes in transform:
000590: Mar 26 21:00:28.916: ISAKMP:      authenticator is HMAC-MD5
000591: Mar 26 21:00:28.916: ISAKMP:      key length is 256
000592: Mar 26 21:00:28.916: ISAKMP:      encaps is 1 (Tunnel)
000593: Mar 26 21:00:28.916: ISAKMP:      SA life type in seconds
000594: Mar 26 21:00:28.916: ISAKMP:      SA life duration (VPI) of  0x0 0x20 0xC4 0x9B
000595: Mar 26 21:00:28.916: ISAKMP:(1005):atts are acceptable.
000596: Mar 26 21:00:28.916: ISAKMP:(1005):Checking IPsec proposal 1
000597: Mar 26 21:00:28.916: ISAKMP:(1005):transform 1, IPPCP LZS
000598: Mar 26 21:00:28.916: ISAKMP:   attributes in transform:
000599: Mar 26 21:00:28.916: ISAKMP:      encaps is 1 (Tunnel)
000600: Mar 26 21:00:28.916: ISAKMP:      SA life type in seconds
000601: Mar 26 21:00:28.916: ISAKMP:      SA life duration (VPI) of  0x0 0x20 0xC4 0x9B
000602: Mar 26 21:00:28.916: ISAKMP:(1005):atts are acceptable.
000603: Mar 26 21:00:28.916: ISAKMP:(1005): IPsec policy invalidated proposal with error
  256
! - No match, check second proposal
000604: Mar 26 21:00:28.916: ISAKMP:(1005):Checking IPsec proposal 2
000605: Mar 26 21:00:28.916: ISAKMP: transform 1, ESP_AES
000606: Mar 26 21:00:28.916: ISAKMP:   attributes in transform:
000607: Mar 26 21:00:28.916: ISAKMP:      authenticator is HMAC-SHA
000608: Mar 26 21:00:28.916: ISAKMP:      key length is 256
000609: Mar 26 21:00:28.916: ISAKMP:      encaps is 1 (Tunnel)
000610: Mar 26 21:00:28.916: ISAKMP:      SA life type in seconds
000611: Mar 26 21:00:28.916: ISAKMP:      SA life duration (VPI) of  0x0 0x20 0xC4 0x9B
000612: Mar 26 21:00:28.916: ISAKMP:(1005):atts are acceptable.
000613: Mar 26 21:00:28.916: ISAKMP:(1005):Checking IPsec proposal 2
000614: Mar 26 21:00:28.916: ISAKMP:(1005):transform 1, IPPCP LZS
000615: Mar 26 21:00:28.916: ISAKMP:   attributes in transform:
000616: Mar 26 21:00:28.916: ISAKMP:      encaps is 1 (Tunnel)
000617: Mar 26 21:00:28.916: ISAKMP:      SA life type in seconds
```

Example 16-3 **debug crypto isakmp** *Command Output (Continued)*

```
000618: Mar 26 21:00:28.916: ISAKMP:      SA life duration (VPI) of  0x0 0x20 0xC4 0x9B
000619: Mar 26 21:00:28.916: ISAKMP:(1005):atts are acceptable.
000620: Mar 26 21:00:28.920: ISAKMP:(1005): IPsec policy invalidated proposal with error
  256
! - No match, check third proposal
000736: Mar 26 21:00:28.924: ISAKMP:(1005):Checking IPsec proposal 3
000737: Mar 26 21:00:28.924: ISAKMP: transform 1, ESP_3DES
000738: Mar 26 21:00:28.924: ISAKMP:   attributes in transform:
000739: Mar 26 21:00:28.924: ISAKMP:      authenticator is HMAC-SHA
000740: Mar 26 21:00:28.924: ISAKMP:      encaps is 1 (Tunnel)
000741: Mar 26 21:00:28.924: ISAKMP:      SA life type in seconds
000742: Mar 26 21:00:28.924: ISAKMP:      SA life duration (VPI) of  0x0 0x20 0xC4 0x9B
000743: Mar 26 21:00:28.924: ISAKMP:(1005):atts are acceptable.
! - Match.  Begin SA process.
000744: Mar 26 21:00:28.924: ISAKMP:(1005): processing NONCE payload. message ID =
  1682961045
000745: Mar 26 21:00:28.924: ISAKMP:(1005): processing ID payload. message ID = 1682961045
000746: Mar 26 21:00:28.924: ISAKMP:(1005): processing ID payload. message ID = 1682961045
000747: Mar 26 21:00:28.924: ISAKMP:(1005):QM Responder gets spi
000748: Mar 26 21:00:28.924: ISAKMP:(1005):Node 1682961045, Input = IKE_MESG_FROM_PEER,
  IKE_QM_EXCH
000749: Mar 26 21:00:28.924: ISAKMP:(1005):Old State = IKE_QM_READY  New State =
  IKE_QM_SPI_STARVE
000750: Mar 26 21:00:28.928: ISAKMP:(1005): Creating IPsec SAs
000751: Mar 26 21:00:28.928:         inbound SA from 172.16.1.40 to 172.16.0.4 (f/i)  0/ 0
        (proxy 172.16.1.191 to 0.0.0.0)
000752: Mar 26 21:00:28.928:         has spi 0xF38581A8 and conn_id 0
000753: Mar 26 21:00:28.928:         lifetime of 2147483 seconds
000754: Mar 26 21:00:28.928:         outbound SA from 172.16.0.4 to 172.16.1.40 (f/i) 0/0
        (proxy 0.0.0.0 to 172.16.1.191)
000755: Mar 26 21:00:28.928:         has spi  0x7065A45A and conn_id 0
000756: Mar 26 21:00:28.928:         lifetime of 2147483 seconds
000757: Mar 26 21:00:28.928: ISAKMP:(1005): sending packet to 172.16.1.40 my_port 500
  peer_port 500 (R) QM_IDLE
000758: Mar 26 21:00:28.928: ISAKMP:(1005):Node 1682961045, Input = IKE_MESG_INTERNAL,
  IKE_GOT_SPI
000759: Mar 26 21:00:28.928: ISAKMP:(1005):Old State = IKE_QM_SPI_STARVE  New State =
  IKE_QM_R_QM2
000760: Mar 26 21:00:28.932: ISAKMP (0:1005): received packet from 172.16.1.40 dport 500
  sport 500 Global (R) QM_IDLE
000761: Mar 26 21:00:28.932: ISAKMP:(1005):deleting node 1682961045 error FALSE reason "QM
  done (await)"
000762: Mar 26 21:00:28.936: ISAKMP:(1005):Node 1682961045, Input = IKE_MESG_FROM_PEER,
  IKE_QM_EXCH
000763: Mar 26 21:00:28.936: ISAKMP:(1005):Old State = IKE_QM_R_QM2  New State =
  IKE_QM_PHASE2_COMPLETE
000764: Mar 26 21:00:30.884: %CRYPTO-4-RECVD_PKT_INV_SPI: decaps: rec'd IPSEC packet has
  invalid spi for destaddr=172.16.0.4, prot=50, spi=0x94040000(2483290112),
  srcaddr=172.16.1.40
000765: Mar 26 21:00:30.888: ISAKMP: set new node -189570038 to QM_IDLE
```

continues

Example 16-3 **debug crypto isakmp** *Command Output (Continued)*

```
000766: Mar 26 21:00:30.888: ISAKMP:(1005): sending packet to 172.16.1.40 my_port 500
  peer_port 500 (R) QM_IDLE
000767: Mar 26 21:00:30.888: ISAKMP:(1005):purging node -189570038
000768: Mar 26 21:00:30.888: ISAKMP:(1005):Input = IKE_MESG_FROM_IPSEC, IKE_PHASE2_DEL
000769: Mar 26 21:00:30.888: %CRYPTO-4-RECVD_PKT_NOT_IPSEC: Rec'd packet not an IPSEC
  packet.
        (ip) vrf/dest_addr= /10.250.1.10, src_addr= 172.16.1.191, prot= 1
000770: Mar 26 21:00:30.888: ISAKMP:(1005):Old State = IKE_P1_COMPLETE  New State =
  IKE_P1_COMPLETE
```

The highlighted portions show that each policy is offered in hopes of finding one in common. The process continues until one is acceptable to both sides. Upon acceptance of the transform set, the connection parameters are uploaded to the client as shown by the highlighted text once again. Once those parameters are uploaded, the IPsec portion of the connection begins and, once again, policies are negotiated. It is clear that the order of input of the policies for both ISAKMP and IPsec can have some bearing on the processing and response time for the connection.

Example 16-3 was performed using only local authentication. In cases where RADIUS and TACACS+ servers are used, or any AAA model in fact, the process of authentication can be monitored using the appropriate command or combination of commands, as follows:

- **debug aaa authentication**
- **debug aaa authorization**
- **debug radius**

Foundation Summary

The Easy VPN Server functionality is, as the name implies, quite straightforward in its configuration and function. The polices, preshared keys, DNS/WINS servers, DNS domain(s), and IP address pools all need to be preconfigured in the group policy to facilitate VPN Client connections.

The Easy VPN Server provides a mechanism for IT organizations to better and more effectively support the teleworker in the small office/home office (SOHO) and on the road. This allows IT organizations to provide to teleworkers a common experience through access to identical applications and services as are available to those workers located in central and/or headquarters sites.

Table 16-2 revisits the aspects of VPN connectivity managed by Cisco Easy VPN.

Table 16-2 *Easy VPN Automated Tasks*

Task	Description
Tunnel parameter negotiation	Tunnel addresses, algorithms, and duration
Tunnel establishment	Creation of tunnel connection between its source and destination
NAT/PAT/ACL	Automatic creation of NAT and PAT tables as well as ACL generation
Security key management	Encryption and decryption key management
Tunneled data handling	Encryption, decryption, and authentication

Cisco Easy VPN Client functions in one of three modes, as summarized in Table 16-3.

Table 16-3 *Cisco Easy VPN Client Modes*

Mode	Description
Client	Specifies that NAT and/or PAT is used and that end stations on the client side of the connection do not use IP addressing from the address space of the VPN Server side
Network Extension	Client-side end stations use IP addressing from the address space of the VPN Server so that they form a single internetwork
Network Extension Plus	Similar to Network Extension mode with the added capability of being able to request an IP address via mode configuration and assign it to an available loopback interface

Q&A

The questions and scenarios in this book are designed to be challenging and to make sure that you know the answer. Rather than allowing you to derive the answers from clues hidden inside the questions themselves, the questions challenge your understanding and recall of the subject.

Hopefully, mastering these questions will help you limit the number of exam questions on which you narrow your choices to two options, and then guess.

You can find the answers to these questions in Appendix A. For more practice with exam-like question formats, use the exam engine on the CD-ROM.

1. Easy VPN Remote feature supports a two-stage process for client/server authentication. Describe both stages.
2. One of the key concepts necessary to properly understand VPN connectivity is the step-by-step method of VPN tunnel establishment. List the steps in order of completion.
3. Describe Xauth and why it is beneficial in VPN connections.
4. Why is the RRI important to the VPN connection?
5. Describe the options available for Group Authorization configuration of an Easy VPN Server.
6. In the selection of a transform set for a given VPN connection, by what process is the transform set chosen?
7. List the modes of operation for Easy VPN Remote and provide a brief description of each.
8. To ensure secure tunnel connections, the Cisco Easy VPN Remote feature does not support certain transform set configurations. In what circumstance(s) would this be the case?

Exam Topic List

This chapter covers the following topics that you need to master for the CCNP ISCW exam:

- **Cisco VPN Client Installation and Configuration Overview**—Describes the purpose of the Cisco VPN Client and provides an overview of the installation and configuration process.

- **Cisco VPN Client Installation**—Describes the process of installing the Cisco VPN Client on a client PC.

- **Cisco VPN Client Configuration**—Describes the necessary configuration steps for the Cisco VPN Client.

CHAPTER 17

Implementing the Cisco VPN Client

A core piece of the teleworker or road warrior battle chest is certainly the ability to connect back to the corporate network to access company resources such as e-mail, file shares, documents, and other resources.

The Cisco VPN Client allows Microsoft Windows-based PCs, Apple Macintosh OS X computers, and Linux clients to connect remotely over any IP-based network connection in order to create a secure connection over Internet or dialup infrastructure.

"Do I Know This Already?" Quiz

The purpose of the "Do I Know This Already?" quiz is to help you decide whether you really need to read the entire chapter. If you already intend to read the entire chapter, you do not necessarily need to answer these questions now.

The 6-question quiz, derived from the major sections in the "Foundation Topics" portion of the chapter, helps you to determine how to spend your limited study time.

Table 17-1 outlines the major topics discussed in this chapter and the "Do I Know This Already?" quiz questions that correspond to those topics.

Table 17-1 *"Do I Know This Already?" Foundation Topics Section-to-Question Mapping*

Foundation Topics Section	Questions Covered in This Section	Score
Cisco VPN Client Installation and Configuration Overview	1	
Cisco VPN Client Installation	2	
Cisco VPN Client Configuration	3–6	
Total Score		

CAUTION The goal of self-assessment is to gauge your mastery of the topics in this chapter. If you do not know the answer to a question or are only partially sure of the answer, you should mark this question wrong for purposes of self-assessment. Giving yourself credit for an answer that you correctly guess skews your self-assessment results and might provide you with a false sense of security.

1. From which source is the Cisco VPN Client Software obtained?
   a. Cisco.com with a CCO ID
   b. CD shipped with VPN devices
   c. Local software retailer
   d. Bundled with client PC
2. Which of the following is the default installation location of the Cisco VPN Client Software?
   a. C:\Cisco\VPN Client
   b. C:\Program Files\Cisco Systems\VPN Client
   c. C:\Cisco VPN Client
   d. C:\Cisco Systems\VPN Client
3. To use Group Authentication for a connection entry, which of the following is required?
   a. Root certificate
   b. IPsec over UDP
   c. TCP transport
   d. VPN dialup
4. Which is the default transport for a new connection entry?
   a. IPsec over TCP port 10000
   b. IPsec over UDP port 10000
   c. IPsec over TCP port 4500
   d. IPsec over UDP port 4500

5. To provide for VPN server resilience, which is typically provided by network administrators to the VPN Clients?
   a. Authentication mechanism
   b. Backup server name or address
   c. Transport mechanism
   d. Personal firewall
6. Which of the following connection entry options allows the use of a PSTN connection to provide VPN access?
   a. Mutual group authentication
   b. IPsec over TCP transport
   c. Dial-Up tab configuration options
   d. Backup server configuration

The answers to the "Do I Know This Already?" quiz are found in Appendix A, "Answers to the 'Do I Know This Already?' Quizzes and Q&A Sections." The suggested choices for your next step are as follows:

- **2 or fewer overall score**—Read the entire chapter. This includes the "Foundation Topics," "Foundation Summary," and "Q&A" sections.
- **3 or 4 overall score**—Begin with the "Foundation Summary" section, and then go to the "Q&A" section.
- **5 or more overall score**—If you want more review on these topics, skip to the "Foundation Summary" section, and then go to the "Q&A" section. Otherwise, move to the next chapter.

Foundation Topics

Cisco VPN Client Installation and Configuration Overview

The installation of the Cisco VPN Client Software is a very straightforward process. A number of tasks must be completed to establish connectivity to a VPN head-end, which can consist of a VPN Concentrator or IOS Router. These include

- Installation of the Cisco VPN Client on a user PC
- Creation of a new connection entry in the software
- Configuration of the client authentication properties
- Configuration of transparent tunneling
- Enabling and adding of backup servers
- Configuration of a connection to the Internet via dialup networking

The Cisco VPN Client Software can be downloaded from Cisco.com. A registered Cisco Connection Online (CCO) ID is required to access the software download area on Cisco.com. Cisco recommends that users maintain an up-to-date version of the software. In the absence of a CCO ID, it is possible to use the Microsoft IPsec client that is bundled with Microsoft Windows.

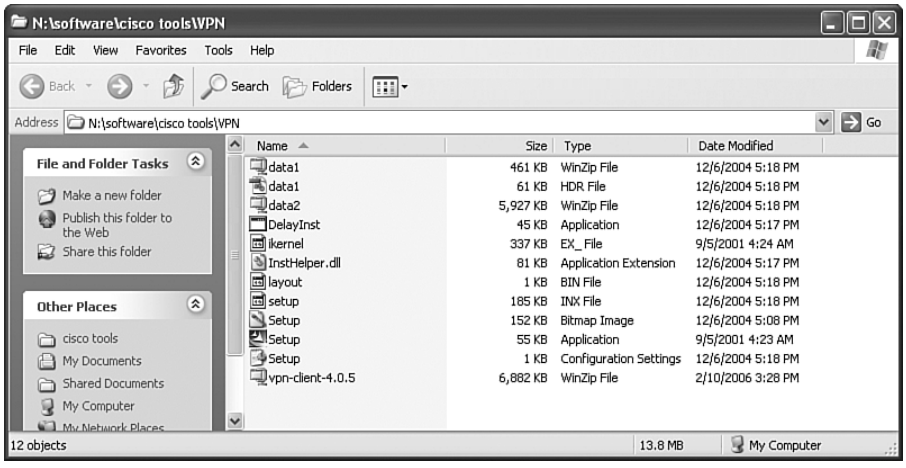
Before installing a new version of the software, it is recommended that existing connection entries (profiles) be exported to a temporary directory and the software be uninstalled. Once the setup process has begun, an installation wizard will step through the entire process to its completion.

After the software is installed, it should be launched so that connection entries can be imported back into the client or new connection entries can be created. Any created connections should be tested for functionality and reconfigured as needed to establish the needed connectivity.

Cisco VPN Client Installation

After the Cisco VPN Client Software has been downloaded from Cisco.com and saved to a working directory on the target hard disk, double-click the self-extracting executable file to begin the installation process. This initial step simply extracts the included files to the same working directory on the PC's hard disk (the extraction location depends on the WinZip settings). Once all files are extracted, double-click the setup.exe file in the directory where all the files have been extracted to begin the installation process. Figure 17-1 lists the files extracted from the downloaded archive file.

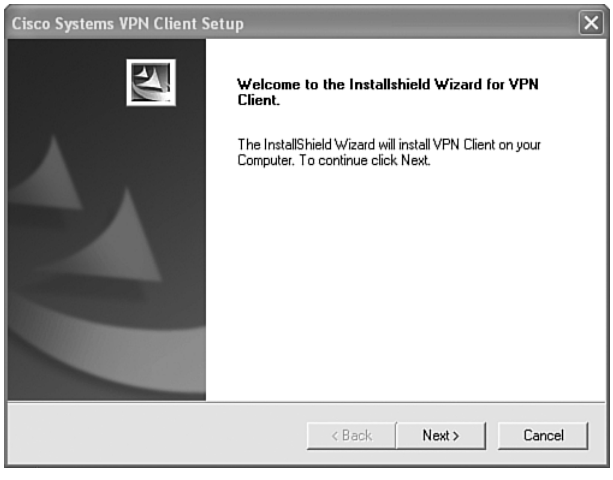
Figure 17-1 *Cisco VPN Client Files*



The bottom file in the listing is the one that was actually downloaded from Cisco.com. When the file extraction occurred, the additional files were placed in the same directory.

The installation wizard is launched by double-clicking the setup.exe file. This process first checks to see whether an older version of the Cisco VPN Client is already installed. If a previous version is already installed, the existing software must first be uninstalled. Click the **OK** button on the warning screen to exit the installation. Uninstall the previous version either from the Windows **Settings > Control Panel > Add or Remove Programs**, or by navigating to **Start > All Programs > Cisco System VPN Client > Uninstall VPN Client**. Once the older version has been removed, the machine will require a reboot. If no previous version of the VPN Client is detected, the Welcome screen will be presented, as shown in Figure 17-2.

Figure 17-2 *Cisco VPN Client Welcome Screen*

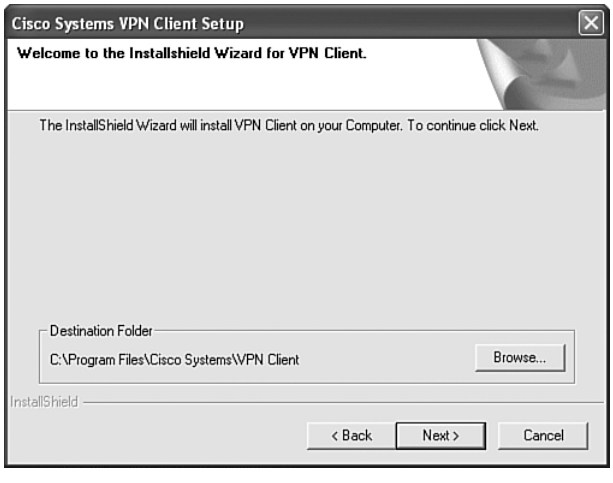


Click **Next** on the Welcome screen to progress the installation wizard to the License Agreement screen, shown in Figure 17-3. If all terms and conditions of the Software Licensing Agreement are acceptable to the user, click **Yes** to continue the installation process.

Figure 17-3 *Cisco VPN Client Licensing Agreement*

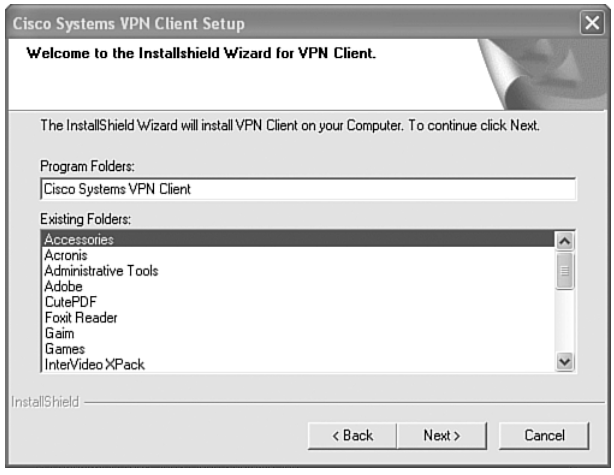
Upon acceptance of the Licensing Agreement, the next screen provides the option of altering or accepting the default program installation directory. As shown in Figure 17-4, the default installation directory is C:\Program Files\Cisco Systems\VPN Client.

Figure 17-4 *Cisco VPN Client Installation Directory*



Click **Browse** to select an alternative installation location. Otherwise, click **Next** to move the installation process to the Program Folders screen. This option provides the installer with the choice of how the Cisco VPN Client will be presented under the Windows Start menu. As shown in Figure 17-5, the default setting is to create a subfolder under the Programs folder called Cisco Systems VPN Client.

Figure 17-5 *Cisco VPN Client Program Folder*

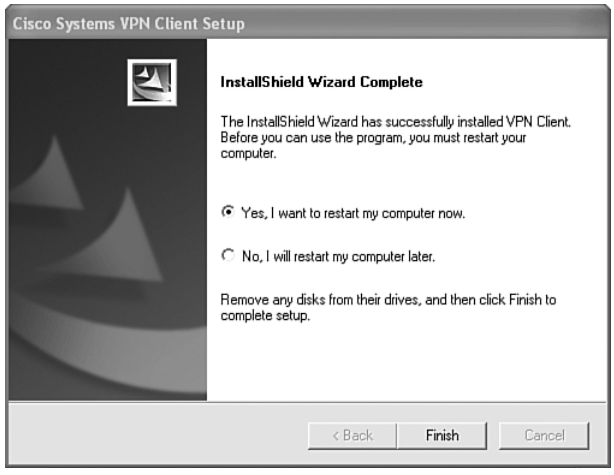


This entry can be deleted entirely to install the Cisco VPN Client Software shortcuts into the Programs folder directly, renamed, or accepted as is. Once the desired folder name is entered in the field, click **Next** to begin the file copy process.

This process is relatively short, and typically lasts less than a minute. While the files are copied and the settings are updated, the user is informed of the file copy process, as well as the installation of a new network adapter for the Cisco VPN Client.

After all the files are copied and settings have been updated and/or added, the installation process is complete. At this point, the PC must be rebooted to put all changes into effect and load the installed drivers. This announcement is shown in Figure 17-6.

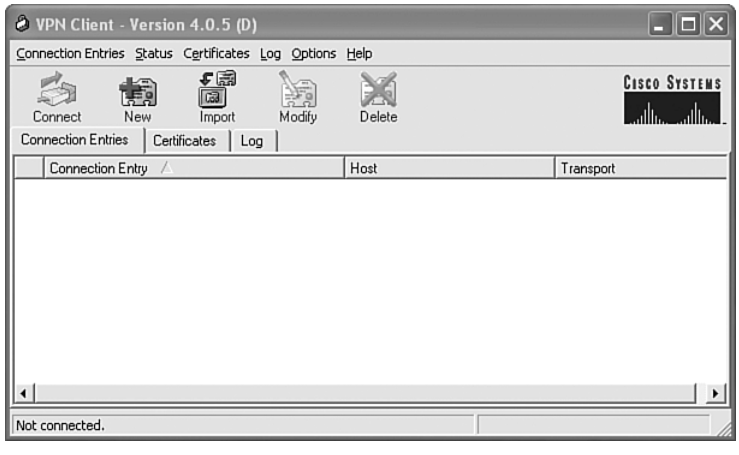
Figure 17-6 *Cisco VPN Client Install Complete*



Cisco VPN Client Configuration

With the installation complete and the PC rebooted, the Cisco VPN Client Software can be launched. The interface is quite simple, as shown in Figure 17-7. It consists of a number of connection entries that facilitate connectivity to various VPN sites as might be offered by a large enterprise corporation.

Figure 17-7 *Cisco VPN Client*



Initially, there are no connection entries, so they must be added to establish a connection via an IP connection to a VPN site.

Connection Entries

The Connection Entries screen is capable of holding multiple entries should multiple access sites and/or methodologies be available. Click the **New** button at the top of the screen to open the Create New VPN Connection Entry dialog box, shown in Figure 17-8.

Figure 17-8 *Cisco VPN Client New Connection Entry Dialog Box*

The Connection Entry field is simply a local name for the connection. It should be unique and allow the user to easily identify the site to which it connects. For added clarification, there is a Description field just below it as well.

The Host field is of key importance as it will contain the IP address or the Fully Qualified Domain Name (FQDN) of the host so that a Domain Name System (DNS) lookup can be performed to resolve the IP address of the target VPN device.

Next, the authentication options listed on the tabs in the bottom half of the Create New VPN Connection Entry dialog box must also be configured.

Authentication Tab

The three options (radio buttons) on the Authentication tab are as follows:

- **Group Authentication**—A username and password is necessary to complete the VPN profile. The password must be entered twice for confirmation (typo prevention).
- **Mutual Group Authentication**—A root certificate must be issued that is compatible with the Central Site VPN Concentrator. A network administrator can load root certificates on the system during the VPN Client installation. Such a certificate must be imported in this window when the Mutual Group Authentication radio button is selected.

- **Certificate Authentication**—After you click the radio button, a drop-down menu allows you to select the certificate to use in this connection. If you choose it and no certificate has been installed, the field reads No Certificates Installed. To use this authentication method, a certificate must be installed.

Transport Tab

The Transport tab allows the configuration of transparent tunneling as well as the choice of whether to use IPsec over UDP or TCP. Figure 17-9 shows the Transport tab.

Figure 17-9 *Cisco VPN Client Transport Tab*

Transparent tunneling allows secure transfer of packets between the VPN Client and a secure gateway through a router running firewall services. Typically, such a gateway is also running either Network Address Translation (NAT) or Port Address Translation (PAT). IPsec endpoints expect the target IP addresses to be globally reachable. In the vast majority of networks today, some form of NAT or PAT is used to extend the number of IP addresses available. Transparent tunneling permits the IPsec end points to operate in such an environment.

Transparent tunneling must use common configuration parameters on both the VPN client and the VPN gateway. Transparent tunneling encapsulates Protocol 50 (Encapsulating Security Payload [ESP]) traffic inside of TCP or UDP datagrams. It can allow both Internet Security Association and Key Management Protocol (ISAKMP) and ESP to be encapsulated inside a transport protocol before being sent through a NAT/PAT device. Virtually every home network sits behind a PAT device, because the home ISP typically gives out only a single IP address. Transparent tunneling is useful when accessing VPN services via a small office/home office (SOHO) router.

The decision to use either IPsec over UDP or IPsec over TCP depends on the configuration of the VPN gateway. Both TCP and UDP can properly deal with PAT environments. TCP tends to work better with multiple connections, and UDP does not operate well through stateful firewalls (because UDP is not connection oriented).

In the VPN Client Software, transparent tunneling is on by default. The Central Site VPN device must be configured to make use of it as well in order to support the connection. Ensure that the Central Site VPN device and the VPN client software are configured identically to ensure proper functionality.

The default Transparent Tunneling mode is IPsec over UDP. It normally uses UDP port 4500 to encapsulate packets before they reach the NAT/PAT device. The actual port number is negotiated during the establishment of the VPN tunnel. This encapsulation allows the VPN client to exist and operate behind a NAT or PAT device.

IPsec over TCP requires that the TCP port number used in VPN connections match on both ends. The default port number is 10000, but it can be changed (typically by policy at the central site). The use of IPsec over TCP also helps with NAT/PAT environments but adds support for stateful firewalls.

The final option on this tab is the Allow Local LAN Access checkbox. The LAN Access parameter provides access to the local network resources such as printers, faxes, shared files, and other resources. Both the client and the Central Site VPN device must be configured to permit this option. The central site informs the client that local LAN access is permitted, and all other traffic travels through the VPN. The client simply checks the Local LAN box. Local LAN is defined as the subnet (or subnets—up to 10) applied to the interface before the VPN connection (and the associated VPN subnet) is established.

For example, if a user initiates a VPN connection from home (where they have their own network-attached printer), this option would be necessary to permit the user to print to their home printer while connected to the VPN. The user could also access other shared resources at home; however, all local communication is possible only with IP addresses, not device names. All name resolution is sent through the VPN, which would not be aware of devices on the home network.

Typically, such configuration is not permitted by the central site because it could permit traffic from an unsecured interface into the VPN. When Local LAN access is not configured, all traffic is sent across the VPN connection and local resources are unreachable.

Backup Servers Tab

To ensure VPN availability, multiple VPN servers can be deployed in a given network model. From an architectural standpoint, this makes good sense if a significant number of employees use the VPN to facilitate their job functions day to day. The VPN client contains a Backup Servers tab to configure a single connection with the capability to connect to multiple servers. Should the primary server configured for the connection entry be unavailable, the client will automatically attempt to contact the servers configured in the Backup Servers tab. The search order for backup servers will be top-down. With this in mind, buttons have been added to this tab to facilitate reordering of Backup Server entries based on preference. Figure 17-10 shows the Backup Servers tab.

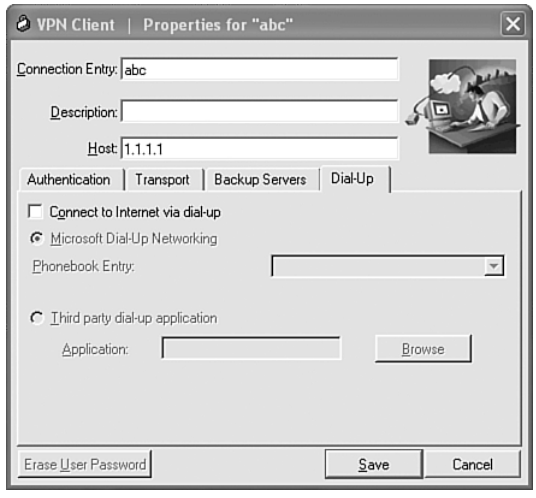
Figure 17-10 *Backup Servers Tab*

To enable the use of backup servers, check the Enable Backup Servers checkbox. Once checked, the options to add, remove, and reorganize (up/down arrows) become available. Additional servers are added by IP address only. All security parameters for the backup servers are already defined in the authentication tab.

Dial-Up Tab

Not all VPN servers are accessible via the Internet. If access to the central site requires that a dialup connection be made, the connection entry can be configured to do so. To enable the use of dialup, the Connect to Internet via Dial-up checkbox must be checked. This enables the options available on this page. The connection can use the Microsoft Dial-Up Networking phonebook or a specified third-party dialer application. Click the appropriate radio button to configure either option. Figure 17-11 shows the Dial-Up tab options.

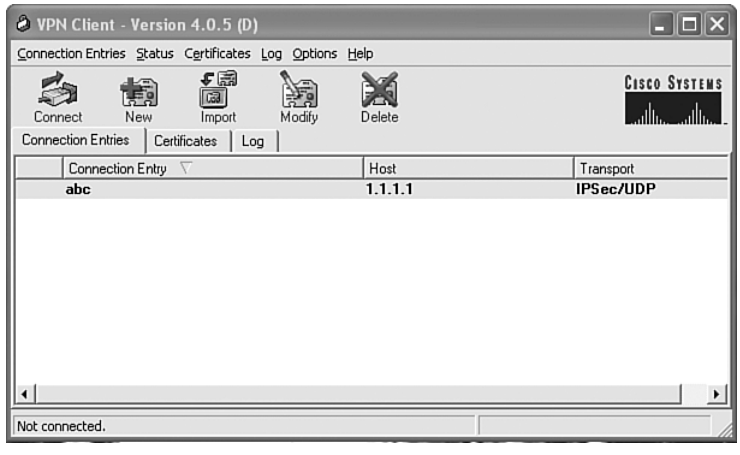
Figure 17-11 *Dial-Up Tab*



Finish the Connection Configuration

When all required options have been configured, click the **Save** button at the bottom of the Create window. All configurations are saved for this profile, and you are returned to the main VPN Client window. Figure 17-12 shows this window with the new profile added.

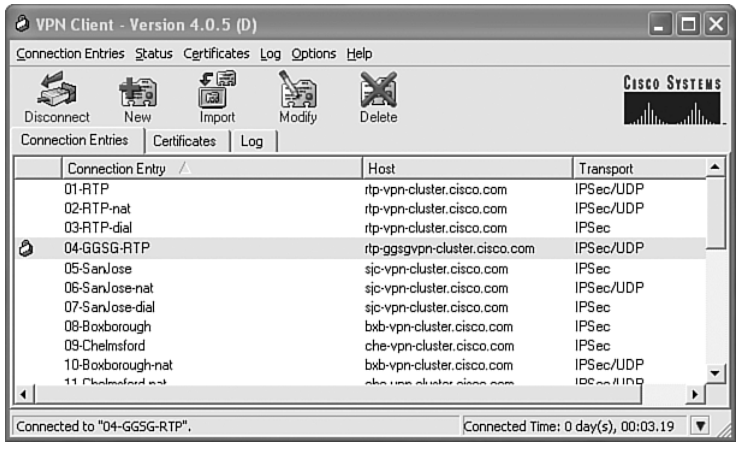
Figure 17-12 *New Profile Added*



From the main VPN Client window, you can establish a VPN connection by highlighting one of the profiles and clicking the **Connect** button at the top of the window. If the connection parameters

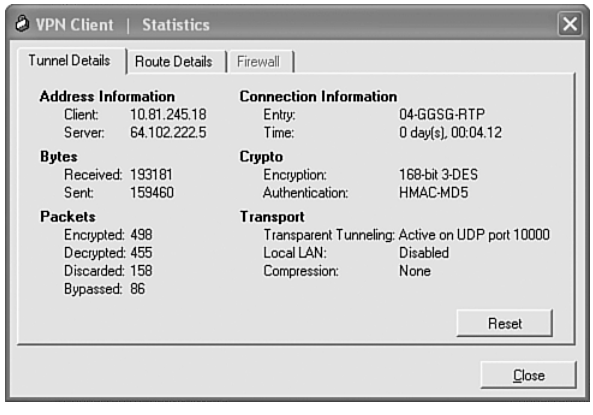
were properly configured, the VPN connection is successful. Figure 17-13 shows the VPN Client window with an established VPN tunnel.

Figure 17-13 *Established VPN*



After a VPN connection is established, various statistics about the connection are available. From the Status pull-down menu, select **Statistics**. This launches the Statistics window, as shown in Figure 17-14.

Figure 17-14 *Established VPN*



From this window, the Tunnel Details tab shows information about the current VPN connection. The Route Details tab shows which IP traffic is traveling through the VPN tunnel and which is considered local (this assumes that local LAN access was configured earlier).

Foundation Summary

A VPN connection is easily configurable to multiple sites based on geography or access methodology. The connection can be configured to take advantage of various encryption and/or authentication types as well as connectivity options relating to local resource availability, backup servers, and the use of dialup connections in order to establish a VPN session.

Table 17-2 reviews the configuration options available for a given connection entry in the VPN Client Software.

Table 17-2 *Connection Entry Options*

Parameter	Location	Purpose	Description
Connection Entry	Primary Connection Entry page	Specify a connection name	A unique name that will show in the Connection Entries page in the VPN Client
Host	Primary Connection page	Specify primary VPN server address	IP address or FQDN of the VPN server to be used for a given connection
Authentication	Authentication tab	Specify Group or Mutual Group Authentication	Method of authentication to the VPN server as well as name, password, and certificate specification
Transport	Transport tab	Specify transparent tunneling along with TCP- or UDP-based transport	Provide IPsec transport method and port number for a given connection as well as permit or deny local LAN access
Backup Server	Backup Servers tab	Configuration of additional VPN servers	Method of providing fallback server entries for a given connection should a primary VPN server be unavailable
Dial-Up	Dial-Up tab	Allow configuration of dialup parameters	Specify the use of dialup services for a particular connection entry along with Microsoft Dial-Up or third-party dialer application use

Q&A

The questions and scenarios in this book are designed to be challenging and to make sure that you know the answer. Rather than allowing you to derive the answers from clues hidden inside the questions themselves, the questions challenge your understanding and recall of the subject.

Hopefully, mastering these questions will help you limit the number of exam questions on which you narrow your choices to two options, and then guess.

You can find the answers to these questions in Appendix A. For more practice with exam-like question formats, use the exam engine on the CD-ROM.

1. A network administrator has provided the following information:

```
Entry: CorporateVPN
VPN Host: vpnserver1.mycompany.com
Connection Options:  Group Authentication, Transparent Tunneling, IPsec over UDP
Username: RoadWarrior
Password: cisco
Backup 1: vpnserver2.mycompany.com
```

   Assume that any options not provided herein are to be left disabled and that any necessary certificates have been provided previously.

   Describe the process of configuring the VPN Client to connect to the Central Site via a wired LAN connection.

2. What are the differences between IPsec over UDP and IPsec over TCP?
3. What are the purposes of configuring backup servers in the VPN Client?
4. What is Local LAN Access in the Cisco VPN Client?
5. When either creating or editing a VPN connection profile, which authentication method requires the use of a username and password?
6. Why would the Dial-Up tab be used to establish a VPN?

This part of the book covers the following ISCW exam topics:

Describe network security strategies.

- Describe and mitigate common network attacks (i.e., Reconnaissance, Access, and Denial of Service).
- Describe and mitigate Worm, Virus, and Trojan Horse attacks.
- Describe and mitigate application-layer attacks (e.g., management protocols).

Implement Cisco Device Hardening.

- Describe, configure, and verify AutoSecure/One-Step Lockdown implementations (i.e., CLI and SDM).
- Describe, configure, and verify AAA for Cisco Routers.
- Describe and configure threat and attack mitigation using ACLs.
- Describe and configure IOS secure management features (e.g., SSH, SNMP, SYSLOG, NTP, Role-Based CLI, etc.).

Implement Cisco IOS firewall.

- Describe the functions and operations of Cisco IOS Firewall (e.g., Stateful Firewall, CBAC, etc.).
- Configure Cisco IOS Firewall with SDM.
- Verify Cisco IOS Firewall configurations (i.e., IOS CLI configurations, SDM Monitor).

Describe and configure Cisco IOS IPS.

- Describe the functions and operations of IDS and IPS systems (e.g., IDS/IPS signatures, IPS Alarms, etc.).
- Configure Cisco IOS IPS using SDM.

Part IV: Device Hardening

Exam Topic List

This chapter covers the following topics that you need to master for the CCNP ISCW exam:

- **Router Vulnerability**—Identifies router services and interfaces that are vulnerable to network attack.
- **Using AutoSecure to Secure a Router**—Explains how to automate the process of locking down a Cisco router with the **auto secure** command.
- **Using SDM to Secure a Router**—Explains how to use the SDM web-based utility to configure, monitor, and secure a Cisco router as well as how to use the One-Step Lockdown mode of the Security Audit Wizard.

CHAPTER 18

Cisco Device Hardening

Many network devices have services enabled that create potential vulnerabilities. Such devices include desktop PCs, network servers, routers, and switches. Within an enterprise, most of these devices are protected by a firewall that sits at the perimeter of the network.

The firewall typically has Ethernet ports, and could be the edge device between the provider and the enterprise if an Ethernet service is offered from the provider. However, in many cases, an edge router sits outside of the firewall. This router is typically needed to perform media conversion from Ethernet (which is seen exclusively throughout most enterprises) to some WAN encapsulation for transport through a carrier network.

When a router is the edge device of a network, is it important to disable unnecessary services. Such services may be helpful and even important inside the enterprise, but offer attack vectors when exposed to the Internet. This chapter discusses how to disable unneeded services and secure a perimeter router.

"Do I Know This Already?" Quiz

The purpose of the "Do I Know This Already?" quiz is to help you decide whether you really need to read the entire chapter. If you already intend to read the entire chapter, you do not necessarily need to answer these questions now.

The 10-question quiz, derived from the major sections in the "Foundation Topics" portion of the chapter, helps you to determine how to spend your limited study time.

Table 18-1 outlines the major topics discussed in this chapter and the "Do I Know This Already?" quiz questions that correspond to those topics.

Table 18-1 *"Do I Know This Already?" Foundation Topics Section-to-Question Mapping*

Foundation Topics Section	Questions Covered in This Section	Score
Router Vulnerability	1–3	
Using AutoSecure to Secure a Router	4–7	
Using SDM to Secure a Router	8–10	
Total Score		

CAUTION The goal of self-assessment is to gauge your mastery of the topics in this chapter. If you do not know the answer to a question or are only partially sure of the answer, you should mark this question wrong for purposes of self-assessment. Giving yourself credit for an answer that you correctly guess skews your self-assessment results and might provide you with a false sense of security.

1. Which interfaces should be disabled (shut down) in a router?
   a. Ethernet interfaces
   b. WAN interfaces
   c. Loopback interfaces
   d. Active interfaces
   e. Unconnected interfaces
2. Which of the following services are typically not seen in modern networks (select all that apply)?
   a. MOP
   b. FTP
   c. TFTP
   d. PAD
   e. NTP
3. How can SNMP be secured in a router (select all that apply)?
   a. SNMP is inherently secure.
   b. SNMPv3 offers security features that should be used.
   c. SNMP should be disabled at all times.
   d. Use ACLs to restrict SNMP access to the router.
   e. Wait until SNMPv4 is available.
4. Which of the following Cisco IOS features are enabled by AutoSecure to secure the forwarding plane (select all that apply)?
   a. AAA
   b. CEF
   c. uRPF
   d. SSH
   e. CBAC

5. Which of the following are interface-related security issues that AutoSecure addresses (select all that apply)?

   a. CEF

   b. IP proxy ARP

   c. Banner

   d. IP unreachables

   e. uRPF

6. Which of the following statements are true about the Cisco IOS command **auto secure** (select all that apply)?

   a. **auto secure** is a complete security solution, and no user input is required or possible.

   b. **auto secure** offers both an interactive mode and an automatic mode.

   c. **auto secure** creates a report for the router administrator, who then applies the necessary security configurations.

   d. **auto secure** enables a variety of security features, but only **auto secure** appears in the configuration file.

   e. **auto secure** can perform a complete security adjustment or correct individual portions of the router.

7. Which **auto secure** command option enables automatic mode?

   a. mode-automatic

   b. automatic

   c. no-interact

   d. full

   e. interact

8. Which of the following are security wizards offered by SDM (select all that apply)?

   a. Security Audit

   b. AutoSecure

   c. One-Step Lockdown

   d. Security Lockdown

   e. One-Step AutoSecure

9. Which of the following statements accurately describe the SDM Security Audit (select all that apply)?

   a. The user can define which security features are audited.

   b. The user can determine which security vulnerabilities must be corrected.

   c. SDM uses a predefined list of security settings for audit.

   d. The security audit automatically corrects all vulnerabilities discovered.

   e. The security audit only reports on vulnerabilities discovered and cannot correct issues.

10. Which of the following statements accurately describe the SDM One-Step Lockdown (select all that apply)?

   a. The One-Step Lockdown only secures parameters that are first identified by the user.

   b. A security audit must be run before the One-Step Lockdown to determine current vulnerabilities.

   c. There are no user-configurable options in the One-Step Lockdown.

   d. There are no reports of "vulnerabilities to be corrected" in the One-Step Lockdown.

   e. The One-Step Lockdown process asks the user for confirmation of each corrective measure before execution.

The answers to the "Do I Know This Already?" quiz are found in Appendix A, "Answers to the 'Do I Know This Already?' Quizzes and Q&A Sections." The suggested choices for your next step are as follows:

- **6 or fewer overall score**—Read the entire chapter. This includes the "Foundation Topics," "Foundation Summary," and "Q&A" sections.

- **7 or 8 overall score**—Begin with the "Foundation Summary" section, and then go to the "Q&A" section.

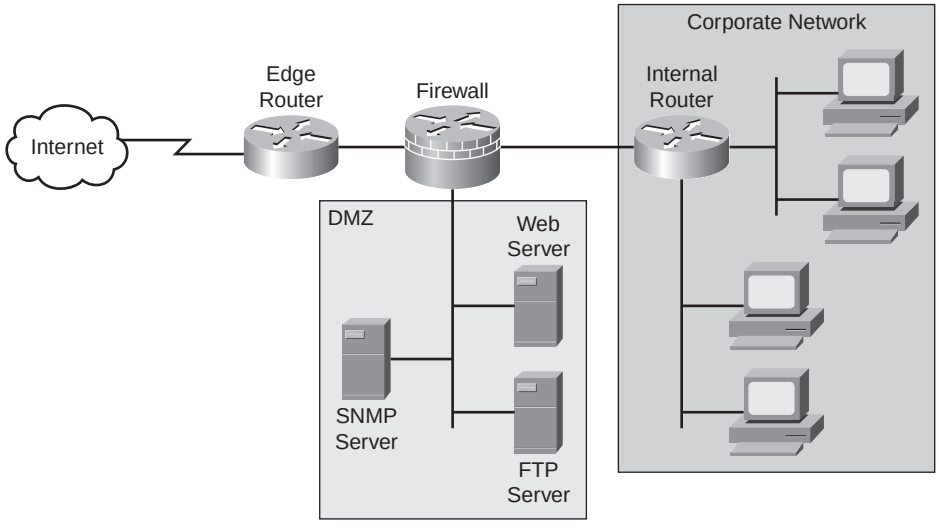
- **9 or more overall score**—If you want more review on these topics, skip to the "Foundation Summary" section, and then go to the "Q&A" section. Otherwise, move to the next chapter.

Foundation Topics

Router Vulnerability

A Cisco IOS router, like many other network devices, has a variety of services enabled by default. Such services help with network management and maintenance. The exposure of such services is normally protected by a perimeter firewall. However, devices that sit outside of the firewall are exposed and vulnerable to attack. Figure 18-1 shows a typical corporate network.

Figure 18-1 *Corporate Network*



The corporate network and demilitarized zone (DMZ) shown in Figure 18-1 is protected from Internet threats by the firewall. Normally, additional services are permitted onto the DMZ, and access to the corporate network itself is more restricted. Assuming that sufficient policies are configured on the firewall, the corporate network should be sheltered. The internal network contains a multitude of routers, switches, user workstations, and servers.

The DMZ offers services to the public Internet. Devices in the DMZ are behind the firewall, but are purposely more accessible than those in the corporate network. The firewall permits particular ports to specific devices in the DMZ, and additional security is provided by the server/host operating systems.

Although the edge router might be physically similar to any of the internal routers, its location outside of the firewall makes it the first device visible to attackers. Many of the Cisco IOS services that are enabled by default to ease management create vulnerabilities in this circumstance. Such services should be disabled to enhance overall network security.

Vulnerable Router Services

There are a number of router services that are considered security threats. To simplify the list, the services are grouped into categories. Each of these categories is expanded in greater detail later in the chapter.

- **Unnecessary services and interfaces**—Services that are generally not needed
- **Common management services**—Services that assist in network management of the router
- **Path integrity mechanisms**—Services that can affect the forwarding plane in the router
- **Probes and scans**—Services that may return excessive information to an attacker
- **Terminal access security**—Services that help protect the router
- **Gratuitous and proxy ARP**—Services that help identify devices on a segment

Within each of these categories are a number of services. The following sections describe what the services are, how they are normally used, and whether they should remain active in a Cisco IOS router.

Disabling so many services on every network device can be a very tedious process. At a minimum, such services should be disabled on the perimeter routers. Because of the sheer volume of necessary adjustments, such services are typically left enabled on many routers, and the network is at risk.

It is important to realize that most of these services should be disabled to avoid any vulnerabilities. The sections that follow describe each service and how to disable it.

Unnecessary Services and Interfaces

This category of services is by far the largest one. Many services in this category are used to transfer configuration files and Cisco IOS images to the router. As such, these services can be exploited if left unattended. Table 18-2 provides a description of these unnecessary services, their default configuration, and how to disable them.

Table 18-2 *Router Vulnerability: Unnecessary Services and Interfaces*

Service	Description	Default	Disable
Router interfaces	Provide packet access in to and out of the router. It is possible that a connection is severed by removing the cable from an active interface. In this case, it is important to also logically disable the interface. This action prevents the interface from becoming active if a cable is accidentally or maliciously connected.	Disabled (in a Cisco router with no user configuration)	(config-if)# **shutdown**
BOOTP server	This service permits the router to act as a BOOTP server for other network devices. Such a service is rarely needed in modern networks, and should be disabled.	Enabled	(config)# **no ip bootp server**
Cisco Discovery Protocol (CDP)	CDP periodically advertises information between Cisco devices, such as the type of device and Cisco IOS version. Such information could be used to determine vulnerabilities and launch specific attacks. Unless needed inside the network, this service should be disabled globally or disabled on unnecessary interfaces.	Enabled (globally and interface)	(config)# **no cdp run** (config-if)# **no cdp enable**
Configuration auto-loading	This service permits a router to automatically load a configuration file from a network server upon boot. This service should remain disabled when not needed.	Disabled	(config)# **no service config**
FTP server	This service permits the router to act as an FTP server for specific files in flash memory. It should remain disabled when not needed.	Disabled	(config)# **no ftp-server enable**
TFTP server	This service permits the router to act as a TFTP server for specific files in flash memory. It should remain disabled when not in use.	Disabled	(config)# **no tftp-server** *file-sys*:*image-name*
NTP service	This service both receives a time-of-day clock from an NTP server and allows the router to act as an NTP server to NTP clients. Correct time is necessary for accurate time stamps when logging messages. This service should be disabled if not needed, or restricted to only devices that require NTP services.	Disabled	(config)# **no ntp server** *ip-address*

continues

Table 18-2 *Router Vulnerability: Unnecessary Services and Interfaces (Continued)*

Service	Description	Default	Disable
Packet assembler/ disassembler (PAD) service	This service allows access to X.25 PAD commands in an X.25 network. Such a service is rarely needed in modern networks, and should be disabled.	Enabled	(config)# **no service pad**
TCP and UDP minor services	These services execute small servers (daemons) in the router, typically used for diagnostics. They are rarely used and should be disabled.	Enabled (before 11.3) Disabled (11.3 and greater)	(config)# **no service tcp-small-servers** (config)# **no service udp-small-servers**
Maintenance Operation Protocol (MOP) service	This service is a Digital Equipment Corporation (DEC) maintenance protocol. Such a service is rarely needed in modern networks, and should be disabled.	Enabled (most Ethernet interfaces)	(config-if)# **no mop enabled**

Common Management Services

Services in this category are used to transfer configuration files and Cisco IOS images to the router. As such, these services can be exploited if left unattended. Table 18-3 provides a description of these common management services, their default configuration, and how to disable them.

Table 18-3 *Router Vulnerability: Common Management Services*

Service	Description	Default	Disable
Simple Network Management Protocol (SNMP)	This service permits the router to respond to queries and configuration requests. If not used, this service should be disabled. If needed, restrict access to the router via access control lists (ACL), and use SNMPv3 for additional security features.	Enabled	(config)# **no snmp-server enable**
HTTP Configuration and Monitoring	This service allows the router to be monitored and configured from a web browser. SDM uses secure HTTP (HTTPS). If not used, this service should be disabled. If needed, restrict access to the router via ACLs, and use HTTPS for encrypted data transfer.	Device dependent	(config)# **no ip http server** (config)# **no ip http secure-server**
Domain Name Service (DNS)	Cisco routers use 255.255.255.255 as the default address to reach a DNS server for name resolution. If not used, this service should be disabled. If needed, explicitly set the address of the DNS server.	Enabled (client service)	(config)# **no ip domain-lookup**

Path Integrity Mechanisms

Services in this category are used to transfer configuration files and Cisco IOS images to the router. As such, these services can be exploited if left unattended. Table 18-4 provides a description of these path integrity mechanisms, their default configuration, and how to disable them.

Table 18-4 *Router Vulnerability: Path Integrity Mechanisms*

Service	Description	Default	Disable
ICMP Redirects	This service causes the router to send an ICMP redirect message when a packet is forwarded out the interface it arrived on. An attacker can use such information to redirect packets to an untrusted device. This service should be disabled when not needed.	Enabled	(config)# **no ip icmp redirect** (config-if)# **no ip redirects**
IP Source Routing	This service allows the sender to control the route that a packet travels through a network. Such a service can permit an attacker to bypass the normal forwarding path and security mechanisms in a network. Because most network devices should not attempt to dictate their preferred path through the network, this service should be disabled.	Enabled	(config)# **no ip source-route**

Probes and Scans

Services in this category can be used to glean information for reconnaissance attacks. As such, these services can be exploited if left unattended. Table 18-5 provides a description of these probes and scans, their default configuration, and how to disable them.

Table 18-5 *Router Vulnerability: Probes and Scans*

Service	Description	Default	Disable
Finger service	The finger protocol (port 79) retrieves a list of users from a network device, which includes the line number, connection name, idle time, and terminal location. Such information is also seen in the **show users** Cisco IOS command, and can be used for reconnaissance attacks. This service should be disabled when not needed.	Enabled	(config)# **no service finger**
ICMP unreachable notification	This service notifies a sender of invalid destination IP subnets or specific addresses. Such information can be used to map a network. This service should be disabled.	Enabled	(config-if)# **no ip unreachables**

continues

Table 18-5 *Router Vulnerability: Probes and Scans (Continued)*

Service	Description	Default	Disable
ICMP mask reply	This service sends the IP subnet mask when it is requested. Such information can be used to map a network. This service should be disabled on interfaces to untrusted networks.	Disabled	(config-if)# **no ip mask-reply**
IP directed broadcasts	A directed broadcast can be used to probe or deny service to (via a DoS attack) an entire subnet. The directed broadcast packet is unicast until it reaches the router that is responsible for the segment. At that time, the packet becomes a broadcast for the specified segment. This service should be disabled.	Enabled (Cisco IOS Software releases prior to 12.0) Disabled (Cisco IOS Software Release 12.0 and later)	(config-if)# **no ip directed-broadcast**

Terminal Access Security

Services in this category can be used to gather information about router users or to launch DoS attacks. As such, these services can be exploited if left unattended. Table 18-6 provides a description of these terminal access security services, their default configuration, and how to disable them.

Table 18-6 *Router Vulnerability: Terminal Access Security Services*

Service	Description	Default	Disable/Enable
IP identification service	The identification protocol (RFC 1413) reports the identity of the TCP connection initiator. Such information can be used in reconnaissance attacks. This service should be disabled.	Enabled	To disable this service, enter (config)# **no ip identd**.
TCP keepalives	TCP keepalives help clean up TCP connections when a remote host has stopped processing TCP packets (such as after a reboot). This service should be enabled to help prevent certain DoS attacks.	Disabled	To enable this service, enter (config)# **service tcp-keepalives-in**. (config)# **service tcp-keepalives-out**

Gratuitous and Proxy ARP

Services in this category can be used to gather information about router users or to launch DoS attacks. As such, these services can be exploited if left unattended. Table 18-7 provides a

description of these gratuitous and proxy ARP services, their default configuration, and how to disable them.

Table 18-7 *Router Vulnerability: Gratuitous and Proxy ARP Services*

Service	Description	Default	Disable
Gratuitous ARP	This service is the primary means used in ARP poisoning attacks. Unless needed, this service should be disabled.	Enabled	(config)# **no ip arp gratuitous**
Proxy ARP	This service permits the router to resolve Layer 2 addresses. This feature is only useful if the router is acting as a Layer 2 bridge. Because this is unlikely in modern networks, this service should be disabled.	Enabled	(config)# **no ip arp proxy**

Using AutoSecure to Secure a Router

Due to the number of CLI commands needed to manually disable services in an attempt to make the router more secure, some routers might not be as protected as they should be. Also, as new features and services become available, additional configurations are necessary to protect against new threats. To combat the mountain of manual configuration statements, Cisco introduced the AutoSecure feature.

AutoSecure helps router administrators secure Cisco IOS Software by automatically performing a variety of functions. AutoSecure is available in Cisco IOS Software Release 12.3 and later. AutoSecure can execute automatically or interactively. In automatic mode, default settings are applied to all security settings. With interactive mode, the user is permitted to select options and features individually.

AutoSecure performs a variety of Cisco IOS router functions. It was shown earlier how to disable many unnecessary features. In addition to disabling unneeded functions, AutoSecure also enables additional Cisco IOS security parameters. The following router functions are performed with AutoSecure:

- **Management plane services and functions**—Include finger, PAD, UDP and TCP small servers, password encryption, TCP keepalives, CDP, BOOTP, HTTP, source routing, gratuitous ARP, proxy ARP, IMCP redirects, ICMP mask replies, directed broadcast, MOP, and banner.
- **Forwarding plane services and functions**—Include CEF and ACLs, which affect every packet flowing through the router.
- **Firewall services and functions**—Include Cisco IOS firewall inspection for common protocols, which permits deep packet inspection on data flows through the IOS router.

- **Logging functions**—Include event logging and password security to keep track of events (attempted attacks) on your network devices.
- **NTP**—Ensures that NTP is securely configured to prevent abuse of the NTP information.
- **SSH access**—Prefer encrypted SSH access compared to clear-text Telnet to prevent packet sniffers from capturing telnet session data.
- **TCP intercept services**—Prevent TCP SYN-flooding attacks, which are a form of DoS attack.

AutoSecure is enabled with the following privileged mode (not configuration mode) Cisco IOS command:

```
Router# auto secure [management | forwarding] [no-interact | full] [login | ntp | ssh |
  firewall | tcp-intercept]
```

full is the default option of this command. This means that the user is prompted (interactively) for input to all security features. **no-interact** induces automatic mode, which applies default configurations to all security parameters without user involvement.

If individual options are selected (**login**, **ntp**, **ssh**, **firewall**, or **tcp-intercept**), only **management** or **forwarding** can be secured at any given time, and only one of **login**, **ntp**, **ssh**, **firewall**, or **tcp-intercept** can be secured at a time. You can run the **auto secure** Cisco IOS command many times to configure a different feature each time, or select the **full** option for all features. Each time the command is executed, the user has the choice of automatic mode (**no-interact**) or interactive mode (no option specified).

When **auto secure full** privileged-mode IOS command is executed, the following steps are performed in sequence:

1. **Identify the outside interface(s)**—Select the Internet-facing interfaces.
2. **Secure the management plane**—Enable and/or disable services and functions mentioned earlier.
3. **Create a security banner**—Configure a message that is displayed when the router is accessed. Remember that a banner is at best a warning, and does not actually prevent an attack.
4. **Configure passwords, AAA, and SSH**—Configure secure modes/features to access the router to include minimum password length, login failure tolerance, AAA, and enable SSH instead of telnet.
5. **Secure the interfaces**—Disable various features mentioned earlier, such as **no ip redirects**, **no ip proxy-arp**, **no ip unreachables**, **no ip directed-broadcast**, **no ip mask-reply**, and **no mop enabled** (on Ethernet interfaces).

6. **Secure the forwarding plane**—Enable CEF, uRFP (if possible), and CBAC (router firewall feature).

The default commands applied by AutoSecure are shown for reference in the "AutoSecure Default Configurations" section at the end of this chapter.

AutoSecure creates a series of Cisco IOS commands and applies them to the running configuration of the router (all "behind the scenes"). As with any configuration opportunity, there is a chance that the procedure could fail before completion. This procedure executes without any notification to the administrator. A failure in the middle of AutoSecure would mean that the router is not as protected as originally thought.

There are two ways to mitigate the failure of the AutoSecure process:

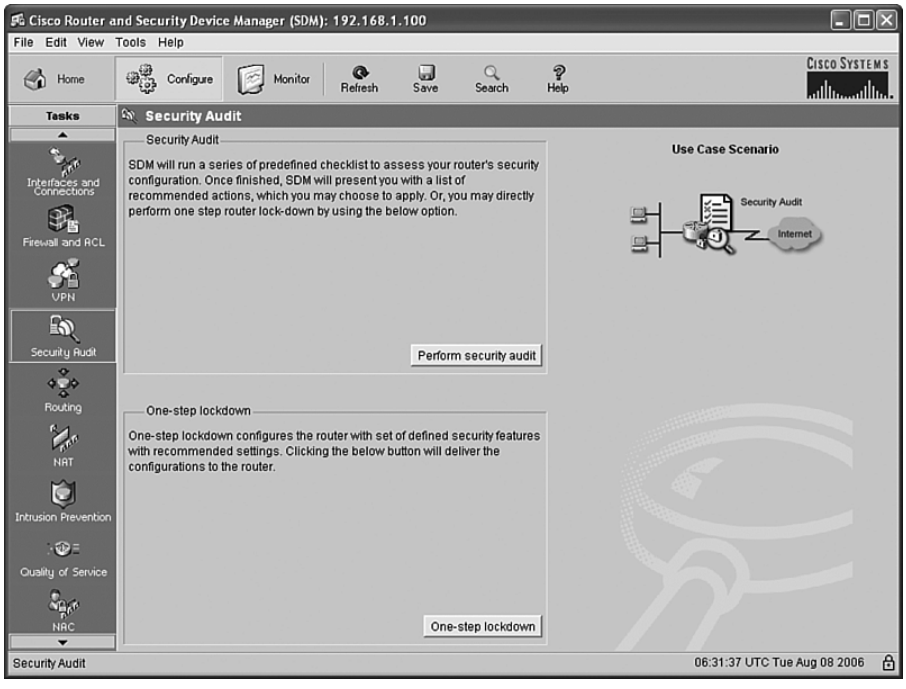
- As should be done before any configuration modification, manually save the running configuration to either NVRAM, flash, or a network server prior to starting the AutoSecure process. Should AutoSecure only install a partial configuration, you can revert to your copy of the untouched configuration file.
- Starting with Cisco IOS Software Release 12.3(8)T, AutoSecure creates a copy of the running configuration file for you as part of the AutoSecure process. A snapshot of the running configuration file is saved in flash as pre_autosec.cfg. If this file is needed, it can be restored with the command **configure replace flash:pre_autosec.cfg**.

Using SDM to Secure a Router

As seen in Chapter 13, "Site-to-Site VPN Operations," SDM is a web-based utility used to configure, monitor, and secure a Cisco router. Manually configuring the router to safeguard against many possible threats is an arduous task. In the CLI, the **auto secure** command automates the overall security process of the router.

In SDM, there are two separate wizards that help secure the router. Both are accessed by going to the Configure page and choosing Security Audit in the Tasks bar. Figure 18-2 shows how to access the two different wizards.

Figure 18-2 *SDM Security Audit*



The first wizard is the Security Audit Wizard. This wizard scans the router configuration and reports both good and bad findings. Any or all of the shortcomings can be corrected at the end of the wizard. The second wizard is the One-Step Lockdown. This wizard applies a series of configurations to the router to secure against many vulnerabilities. The execution of this wizard is similar to the **full** option of the **auto secure** CLI command. The sections that follow explore each of these wizards in greater detail.

SDM Security Audit Wizard

As previously described, you access the SDM Security Audit Wizard by choosing the Security Audit task on the Configure page. The upper box on this window (see Figure 18-2) discusses the security audit process. You launch the audit and the wizard by clicking the **Perform Security Audit** button.

The first screen of the Security Audit Wizard is the Welcome to the Security Audit Wizard page. The page explains that the security audit will do the following:

- Check the router's running configuration against a list of predefined security configuration settings

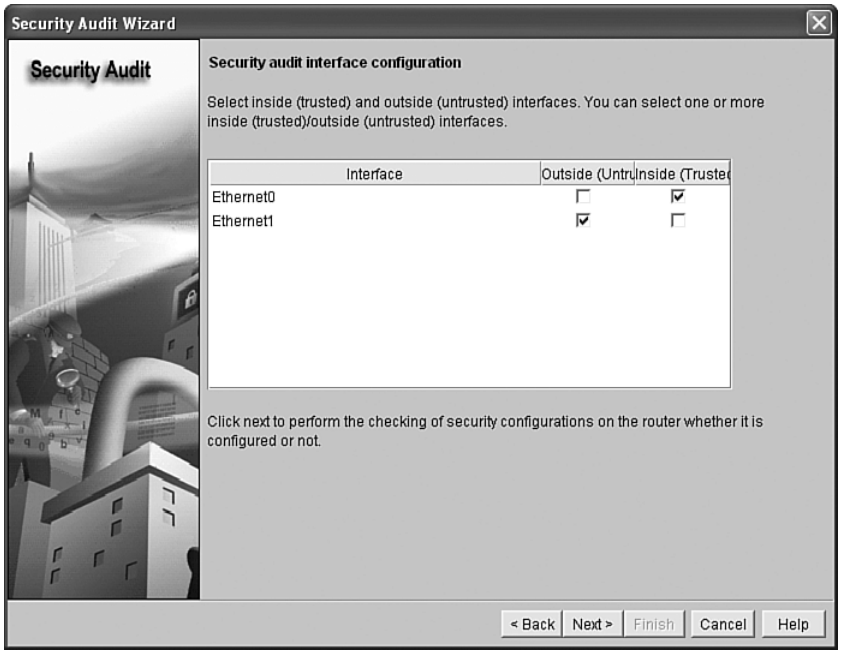
- List identified problems, and then provide recommendations for fixing them
- Allow the user to choose which identified problem(s) to fix, and then display the appropriate user interface for fixing them
- Configure the router with the user-chosen security configuration

At the bottom of this screen, click **Next>** to continue to the wizard, or click **Cancel** to return to the Security Audit Configure page.

The next step in the Security Audit Wizard is the Security Audit Interface Configuration page. This page lists all the active interfaces in the router, and enables you to configure each interface as either an outside (untrusted) or inside (trusted) interface. If an interface is not listed here, you must first enable and configure it by using the Interfaces and Connections Configure task (not detailed in this book).

Figure 18-3 shows the Security Audit Interface Configuration page.

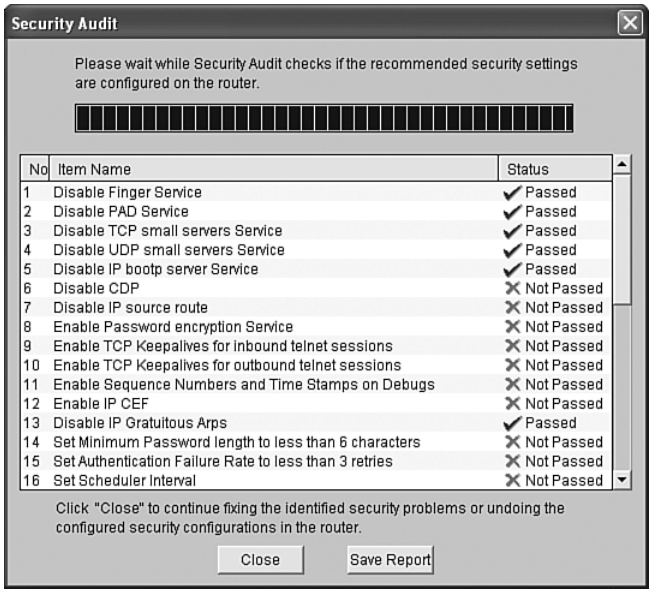
Figure 18-3 *SDM Security Audit Interface Configuration Page*



This page starts with all check boxes empty. In Figure 18-3, Ethernet0 has been selected as the Inside (Trusted) interface, and Ethernet1 has been chosen as the Outside (Untrusted) interface. Once all active interfaces of the router have been properly categorized, click **Next>**.

Now that SDM knows which interfaces are Inside and Outside, it compares the current configuration with an extensive list (more than 30 items) of appropriate security configurations. Figure 18-4 shows the results of this interface security validation.

Figure 18-4 *SDM Security Audit Security Report*

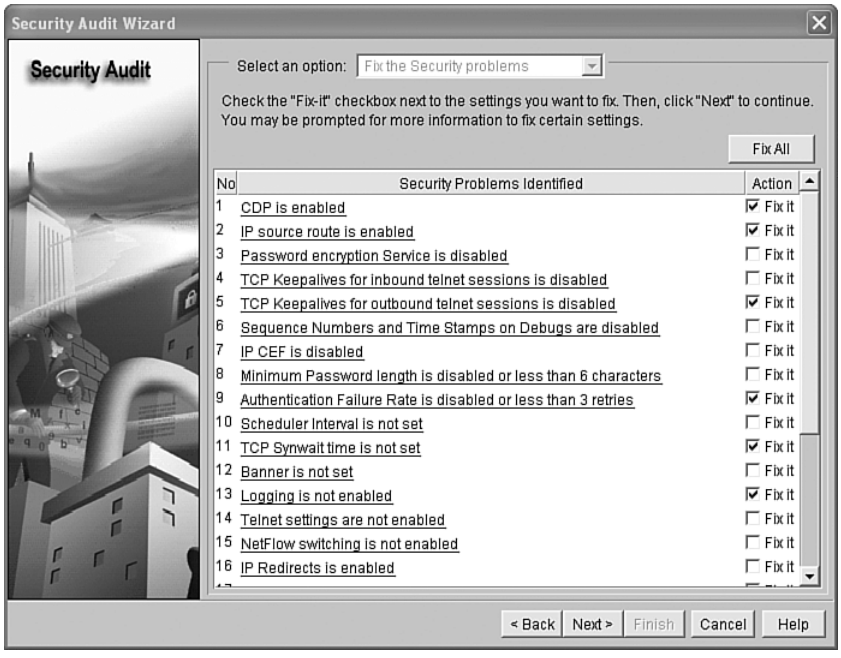


The SDM security audit checks numerous security settings on the router. Figure 18-4 shows only a portion of the security report. The remainder of the report can be viewed by dragging the scroll bar down. The report indicates a Passed or Not Passed status for each of the criteria evaluated. From this page, you have the option of saving the report to the local hard drive. Click **Close** to advance to the final action of the security audit.

The last action in the security audit is to correct the Not Passed issues that were displayed in the security report. Figure 18-5 shows this final page.

If the Security Problems Identified list is lengthy, you might need to use the scroll bar to see all the problems. Clicking the **Fix All** button at the top of the page checks each individual Fix it box in the list. You can also select check boxes individually for correction. Once you have checked the appropriate Fix it boxes, click **Next>** to apply the corrections to the router. Note that the <Back button on this page, although active, does not work. The entire security audit process must be run again to return to the security report.

Figure 18-5 *SDM Security Audit Fix-It Page*



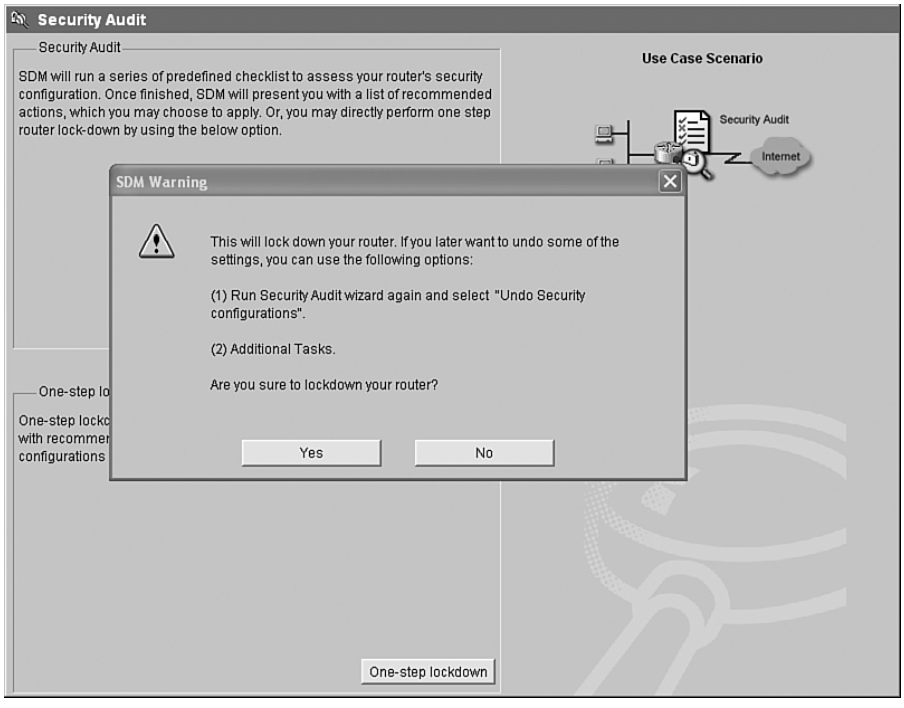
Application of the features is a two-step process. The first screen (after clicking **Next>**) is a summary screen of the features that will be applied. This list corresponds to the Fix it list from the previous screen. It is possible to return to the previous screen with the **<Back** button. This might be necessary to select additional corrective measures or remove selected corrective measures. Click **Finish** to cause SDM to push the appropriate configurations to the router. Click **OK** on the Command Delivery Status window to confirm the corrective actions and exit the Security Audit Wizard.

Once the wizard is finished, you are returned to the Security Audit Configure page, where you can run another security audit or perform the One-Step Lockdown.

SDM One-Step Lockdown Wizard

The SDM One-Step Lockdown Wizard is a web-based solution that works similarly to the **auto secure** Cisco IOS command. To access the wizard, click the **One-step lockdown** button at the bottom of the Security Audit Configure page. Doing so results in the immediate display of a warning, as shown in Figure 18-6.

Figure 18-6 *SDM One-Step Lockdown Wizard*



There are no user-configurable options in the One-Step Lockdown Wizard. There are no reminders of what will be secured or what steps will be performed. The One-Step Lockdown Wizard performs every corrective action that was shown in the security report during the security audit. The complete list of correctable actions is shown later in this chapter. The list is not part of the certification test, but you should understand which actions will be taken before you decide to proceed with the lockdown.

AutoSecure Default Configurations

This section shows the default configurations that are applied with the **auto secure full** Cisco IOS command. This list of configuration commands is not part of the certification exam, but serves as a reference as to the scope of the **auto secure** command.

```
! disable several global services
no service finger
no service pad
no service udp-small-servers
no service tcp-small-servers
service password-encryption
service tcp-keepalives-in
service tcp-keepalives-out
no cdp run
```

```
no ip bootp server
no ip http server
no ip finger
no ip source-route
no ip gratuitous-arp
no ip identd

! banner provided by the user
banner # This banner is created by the user #

! log after ten failed login attempts
security authentication failure rate 10 log

! enable passwords provided by the user
enable secret 5 $1$6NpI$ClSvtL5Zs63fPpsQT5Dyq/
enable password 7 09674F04100916

! configure AAA and apply the lines
aaa new-model
aaa authentication login local-auth local
line con 0
 login authentication local-auth
 exec-timeout 5 0
 transport output telnet
line aux 0
 login authentication local-auth
 exec-timeout 10 0
 transport output telnet
line vty 0 4
 login authentication local-auth
 exec-timeout 10 0
 transport input telnet

! login security
login block-for 5 attempts 3 within 5

! hostname and domain-name are needed for key generation
hostname testrouter
ip domain-name company.com
crypto key generate rsa general-keys modulus 1024
ip ssh time-out 60
ip ssh authentication-retries 2

! add ssh to the vty lines
vty line 0 4
 transport input ssh telnet

! logging parameters
service timestamps debug datetime msec localtime show-timezone
service timestamps log datetime msec localtime show-timezone
service sequence-numbers
logging facility local2
logging trap debugging
logging console critical
logging buffered

! disable interface services
interface <something> 0/0
 no ip redirects
 no ip proxy-arp
 no ip unreachables
 no ip directed-broadcast
 no ip mask-reply
 no mop enabled (only on Ethernet interfaces)

! enable CEF
```

```
ip cef

! apply the BOGON ACL (actual ACL not shown) and configure uRPF to the outside interface
interface <outside> 0/0
 ip access-group autosec_complete_bogon in
exit
access-list 100 permit udp any any eq bootpc
interface <outside> 0/0
 ip verify unicast source reachable-via rx allow-default 100

! configure CBAC
ip inspect audit-trail
ip inspect dns-timeout 7
ip inspect tcp idle-time 14400
ip inspect udp idle-time 1800
ip inspect name autosec_inspect cuseeme timeout 3600
ip inspect name autosec_inspect ftp timeout 3600
ip inspect name autosec_inspect http timeout 3600
ip inspect name autosec_inspect rcmd timeout 3600
ip inspect name autosec_inspect realaudio timeout 3600
ip inspect name autosec_inspect smtp timeout 3600
ip inspect name autosec_inspect tftp timeout 30
ip inspect name autosec_inspect udp timeout 15
ip inspect name autosec_inspect tcp timeout 3600

! apply CBAC to the outside interface
ip access-list extended auto_firewall_acl
 permit udp any any eq bootpc
 deny ip any any
interface <outside> 0/0
 ip inspect autosec_inspect out
 ip access-group autosec_firewall_acl in
```

SDM One-Step Lockdown Default Configurations

This section shows the default configurations that are applied with the SDM One-Step Lockdown. This list of configuration features is not part of the certification exam, but serves as a reference as to the scope of the One-Step Lockdown Wizard.

- Disable:
  - Both TCP and UDP small servers service
  - CDP
  - Finger service
  - IP BOOTP server service
  - IP directed broadcast
  - IP gratuitous ARPs
  - IP identification service
  - IP mask reply
  - IP proxy ARP

- IP redirects
- IP source route
- IP unreachables on all interfaces
- MOP service
- PAD service
- SNMP

- Enable:
  - Firewall (CBAC) on outside interfaces
  - IP CEF
  - Password encryption service
  - Logging
  - NetFlow switching
  - Sequence numbers and time stamps on debugs
  - SSH for access to the router
  - TCP keepalives for both inbound and outbound Telnet sessions
  - Telnet settings
  - uRPF on outside interfaces
- Set:
  - Access class on HTTP server service and VTY lines
  - Authentication failure rate to less than three retries
  - Banner
  - Enable secret password
  - Minimum password length to greater than or equal to six characters
  - Scheduler interval and allocation
  - TCP SYN wait time
  - Users

Foundation Summary

Vulnerable router services include

- **Unnecessary services and interfaces**—Services that are generally not needed
- **Common management services**—Services that assist in network management of the router
- **Path integrity mechanisms**—Services that can affect the forwarding plane in the router
- **Probes and scans**—Services that may return excessive information to an attacker
- **Terminal access security**—Services that help protect the router
- **Gratuitous and proxy ARP**—Services that help identify devices on a segment

The unnecessary services and interfaces that should be disabled include

- Router interfaces
- BOOTP server
- CDP
- Configuration auto-loading
- FTP server
- TFTP server
- NTP server
- PAD
- TCP and UDP minor services
- MOP

The common management services that should be verified include

- SNMP
- HTTP access to the router
- DNS

The path integrity mechanisms that should be verified include

- ICMP redirects
- IP source routing

The services that permit probes and scans that should be disabled include

- Finger
- ICMP unreachables
- ICMP mask replies
- IP directed broadcasts

The terminal access security services that should be verified include

- IP identification
- TCP keepalives

The ARP services that should be disabled include

- Gratuitous ARP
- Proxy ARP

AutoSecure secures the following router functions:

- Management plane services and functions
- Forwarding plane services and functions
- Firewall services and functions
- Logging functions
- NTP protocol
- SSH access
- TCP intercept services

Management plane services and functions secured by AutoSecure include

- Finger
- PAD

- UDP and TCP small servers
- Password encryption
- TCP keepalives
- CDP
- BOOTP
- HTTP
- Source routing
- Gratuitous ARP
- Proxy ARP
- IMCP redirects
- ICMP mask replies
- Directed broadcast
- MOP
- Banner

Forwarding plane services and functions secured by AutoSecure include

- CEF
- ACLs

The privileged mode command used to invoke the AutoSecure process is

```
Router# auto secure [management | forwarding] [no-interact | full] [login | ntp | ssh |
  firewall | tcp-intercept]
```

full is the default option, which means that the user is prompted (interactively) for all security features.

When **full** mode is executed, the following steps are executed in sequence:

1. **Identify the outside interface(s)**—Select the Internet-facing interfaces.
2. **Secure the management plane**—Enable and/or disable services and functions mentioned earlier.
3. **Create a security banner**—Configure a message that is displayed when the router is accessed. Remember that a banner is at best a warning and does not actually prevent an attack.

4. **Configure passwords, AAA, and SSH**—Configure secure modes/features to access the router, including to include minimum password length, login failure tolerance, AAA, and enable SSH instead of telnet.
5. **Secure the interfaces**—Disable various features mentioned earlier, such as **no ip redirects**, **no ip proxy-arp**, **no ip unreachables**, **no ip directed-broadcast**, **no ip mastmask-reply**, and **no mop enabled** (on Ethernet interfaces).

AutoSecure creates a copy of the running configuration file in flash as pre_autosec.cfg.

The pre-AutoSecure configuration can be restored with the following command:

```
Router# configure replace flash:pre_autosec.cfg
```

In SDM, there are two separate wizards that help secure the router: the Security Audit Wizard and the One-Step Lockdown Wizard.

The SDM security audit does the following:

- Checks the router's running configuration against a list of predefined security configuration settings
- Lists identified problems and then provides recommendations for fixing them
- Allows the user to choose which identified problem(s) to fix and then displays the appropriate user interface for fixing them
- Configures the router with the user-chosen security configuration

The SDM Security Audit process consists of

- Determining inside and outside interfaces
- Performing an audit of various security options in the router
- Allowing the user to select which shortcomings must be corrected
- Creating a list of configurations to correct the indicated security vulnerabilities
- Applying the security configurations

Features of the SDM One-Step Lockdown process include

- No user-configurable options
- No reminders of what is secured
- Automatic security audit to determine vulnerabilities

Q&A

The questions and scenarios in this book are designed to be challenging and to make sure that you know the answer. Rather than allowing you to derive the answers from clues hidden inside the questions themselves, the questions challenge your understanding and recall of the subject.

Hopefully, mastering these questions will help you limit the number of exam questions on which you narrow your choices to two options, and then guess.

You can find the answers to these questions in Appendix A. For more practice with exam-like question formats, use the exam engine on the CD-ROM.

1. How should CDP be treated in a secure router?
2. What are some of the legacy protocols and services that should simply be disabled?
3. What are some of the ICMP features that should be disabled?
4. Which ARP features should be disabled?
5. What is an issue with manually configuring security options and features into a Cisco IOS router?
6. How can AutoSecure help secure a Cisco IOS router?
7. What is the Cisco IOS command to launch AutoSecure to automatically secure all options?
8. What AutoSecure option forces all security parameters to be properly configured?
9. What are the general sequential tasks that AutoSecure performs?
10. How is it possible to recover from a failed AutoSecure process?
11. What are the two security wizards offered by SDM?
12. What type of input does the user have in the Security Audit Wizard?
13. What type of input does the user have in the One-Step Lockdown Wizard?

Exam Topic List

This chapter covers the following topics that you need to master for the CCNP ISCW exam:

- **Router Access**—Examines the various physical and logical ways to access a Cisco router.
- **Password Considerations**—Describes the best way to construct passwords for network devices.
- **Set Login Limitations**—Describes how to limit the number of failed login attempts into the router.
- **Setup Mode**—Covers the script that performs basic router configuration, including passwords.
- **CLI Passwords**—Describes all password options that can be configured in the CLI.
- **Additional Line Protections**—Covers other IOS features to further protect the console, aux, and vty lines.
- **Password Length Restrictions**—Describes how longer passwords are more difficult to guess or break.
- **Password Encryption**—Describes how password encryption prevents password compromise if the configuration is compromised.
- **Create Banners**—Describes how to create banners which are used to warn others that the network is for authorized use only.
- **Provide Individual Logins**—Explains how each administrator can have an individual login to the router rather than a shared password.
- **Create Multiple Privilege Levels**—Describes the various customized privilege levels that can be created to limit access to CLI commands.
- **Role-Based CLI**—Explains how role-based CLI overcomes some of the shortcomings of privilege levels.
- **Prevent Physical Router Compromise**—Covers how physical security is sometimes forgotten.