CHAPTER 2

Installing Cisco Centri Firewall

Install Process Overview

Before you begin the install process, you must read Chapter 1, “Installing Cisco Centri Firewall.” It explains what you need to know and do before installing Cisco Centri Firewall and specifies the hardware and software requirements.

The Centri install process contains two phases. During Phase 1, you must install the latest version of the Microsoft Internet Explorer web browser that lets you view the HTML Reference Help and the HTML-base reports generated from within the Cisco Centri Firewall user interface. During Phase 2, you must install the Cisco Centri Firewall software. This chapter explains how to complete these two phases of the Cisco Centri Firewall install process.

Phase 1: Installing Microsoft Internet Explorer

Phase 1 requires that you install the Microsoft Internet Explorer web browser. Cisco Centri Firewall utilizes this program to display reports and HTML-based documentation. The latest Windows NT versions of this program are provided on the Cisco Centri Firewall Installation CD-ROM.

Before you install Internet Explorer, you must determine whether you want to install supplemental programs with the browser. Two different setup programs are provided: the minimal install and the full install. Cisco Centri Firewall requires the minimal install only. The following table identifies the file names of the different setup programs, as well as the components that each setup provides.

Table 2-1 Versions of Microsoft Internet Explorer

Operating System	Filename	Description
Windows NT	Msie302mnt.exe	*Full Installation.* Includes Internet Explorer 3.02, Java, and Internet Mail and News.
	Msie302.exe	*Minimum Installation.* Includes Internet Explorer 3.02 and Java only.

Once you have installed Internet Explorer, you must reboot your computer for the changes to take effect. When you complete this installation and reboot your computer, continue with the "Phase 2: Installing Cisco Centri Firewall" section. During Phase 2 of the install process, you will install the Cisco Centri Firewall software.

Phase 2: Installing Cisco Centri Firewall

Once you complete the preparatory procedures presented in Chapter 1, "Installing Cisco Centri Firewall," and Phase 1 (the previous section), you are ready to install Cisco Centri Firewall. The Centri Setup program guides you through the install process step by step, prompting you to make decisions about how and where you want to install the security system.

We strongly recommend that you exit all Windows programs before continuing this Setup program. Press **Alt+Tab** to switch to any running applications, and close them. To cancel the install process at any time, click **Cancel**.

To install Cisco Centri Firewall:

Step 1 Insert the CD-ROM disk labeled "Cisco Centri Firewall" into the local CD-ROM drive on the target computer.

The Centri Setup program starts automatically, and the Welcome panel displays. At this time, you may cancel the install process or continue with the Centri Setup program.

Note If you have disabled the Auto insert notification option on your local CD-ROM drive, locate and double-click **Setup.exe** on the CD-ROM disk.

Step 2 To continue installing Cisco Centri Firewall, click **Next**.

The Centri License Disk Location panel displays.

Step 3 Insert your backup copy of the Centri License Key disk into the local floppy drive, and type the drive letter that corresponds to this drive. To continue, Click **Next**.

The Centri License Key disk must contain the key file named `license.dsk`. This file identifies the edition of Cisco Centri Firewall that you purchased.

The License Authentication panel displays.

Step 4 In the provided box, type the pass phrase that corresponds to the license key. To continue, click **Next**.

The pass phrase verifies that you have permission to access the contents of the Centri License disk. Chapter 2, "Before You Install Cisco Centri Firewall," provides instructions for obtaining this pass phrase from Cisco Systems, Inc.

The Installation Type panel displays.

Step 5 Click the installation type of Cisco Centri Firewall that you would like to install. To continue, Click **Next**.

You can select the Full Firewall Install, the Remote Administrative Interface Install, or the Functional Demo Install.

The Select Administrative Account Type panel displays.

Step 6 Under **Administrative Account Type**, click the type of administrative account under which you want to install the product. To continue, Click **Next**.

To install Cisco Centri Firewall, you must be logged into Windows using an account that is a member of the Administrators group. If you plan to apply security policies to Windows NT Domains and Group and User accounts, you must be logged into a Windows NT Domain. Otherwise, you can install using an account on the local computer.

The Select Administrative Account for Install panel displays.

Step 7 To specify which administrative account to use to install this product, select an account from the list.

This screen lists the user accounts that are already defined for the Windows NT domains that are accessible from this computer, as well as those defined for the local computer. The user account that you select is used to install Cisco Centri Firewall, and it must be a member of the Administrators group either within a Windows NT domain or on the local computer.

Note For security reasons, we strongly recommend that you select and then rename the Administrator account. We recommend Administrator account because it cannot be removed or disabled; however, it can be renamed.

We also recommend that you disable all other user accounts and delete any other accounts that are members of the Administrator group on the local computer. By following these guidelines, you reduce the risk of attacks on well-known user accounts, such as Administrator and Guest.

Step 8 To disable all user accounts that are defined on the local computer, click **Disable other local accounts**.

Step 9 To delete any user accounts that are a members of the Administrators group on the local computer, click **Delete other members of the Administrators Group**. To continue, click **Next**.

The Enter Windows NT Password panel displays, which prompts you to rename the selected user account and to provide its current password.

Step 10 Type the name to which you want to rename the selected account, and press **Tab**.

You are not required to rename this account; however, your goal should be to prevent any of Cisco Centri Firewall's services from running under the privileges of any well-known account.

Note If you did not log into Windows NT using the account that you have selected, you will be required to log off and log in using this account before continuing with the installation. You must restart the install process after you log in under the selected account.

To administer the product, you are *not* required to log in using a Windows NT account that is a member of the Administrator group. A specific account will be created later in the install process that you must use to log into Cisco Centri Firewall, which is a logon that is separate from the Windows NT logon.

Step 11 Type the password for the account that you selected on the previous panel. Press **Tab** and retype the password to confirm it. To continue, click **Next**.

You must type the exact password as defined for this account on the local computer or the Windows NT Domain controller.

The Security Knowledge Base Export Location panel displays.

Step 12 Insert a blank, formatted disk into the local floppy drive, and type the drive letter that corresponds to the drive. To continue, click **Next**.

This disk will be used to store the Centri Security Knowledge Base key. This disk is required whenever you want to install the Remote User Interface. Do not remove this disk until you complete the Centri Setup program.

The New Centri Administrative Account panel displays.

Step 13 In the Account Name and Password boxes, type the account name and password to use when logging into and administering Cisco Centri Firewall. To continue, click **Next**.

This information is used to define an administrative account within Cisco Centri Firewall. It does not have to conform to the account that you used to log into this computer.

Note This account is not a Windows NT account. It is used only for authenticating administrators to the Cisco Centri Firewall security system.

The Destination Path panel displays.

Step 14 The default destination directory is the `\Centri` directory. To install in this directory, click **Next**. To install in a different directory, click **Browse** and then select an alternate directory. To continue, click **Next**.

This directory, which *must* reside on an NTFS partition, is where Centri Setup will store the Cisco Centri Firewall files. If the selected directory does not exist, a confirmation dialog displays. If you want the Centri Setup program to create this directory for you, click **Yes.**

The Select Program Folder panel displays.

Step 15 To create the default **Centri Firewall** program folder, click **Next**. To install in a different program folder, select an alternate folder. To continue, click **Next**.

The Centri Firewall and the Remove icons can be found in this program folder, which is accessed from the Start menu on your desktop.

The Trusted Adapter(s) Selection panel displays.

Step 16 Select the network adapter card(s) that you consider trusted. To continue, click **Next**.

This panel lists the network adapter cards that are installed on this computer. A trusted network adapter card is one that is attached to a network over which you have administrative control. If this firewall server resides on an internal perimeter network, the trusted network adapter card(s) must be attached to the network(s) that you want to protect.

The Hide Addresses? dialog box displays.

Step 17 If you wish to perform network address translation for all communications originating from the selected trusted adapter(s), click **Yes**. If you do not want to perform network address translation, click **No**.

The Select an Adapter panel displays.

Step 18 Select the network adapter card to which you want to assign the Windows NT native network stack. To continue, click **Next**.

Because Cisco Centri Firewall treats the native Windows NT TCP/IP stack as a logical computer that resides on a trusted network, you must assign it to a network that is both trusted and resides within one of your internal networks.

The Collect Information for <*Network Adapter*> dialog displays.

Step 19 Type the IP address and subnetwork mask for the specified network adapter card. To continue, click **Next**.

This information identifies the network to which the specified adapter card is attached, and statically assigns an IP address that is valid for that network to the adapter card.

Step 20 You will be prompted to enter the information requested in Step 20 for each network adapter installed in this computer. If the network adapter is the network adapter that is attached to the external, untrusted network, you must specify an IP address and subnetwork mask that is registered with InterNIC.

If you chose to perform network address translation, you are prompted to type the IP address of the network adapter card that is exposed to untrusted and unknown networks, such as the Internet. If you answered “No” to the dialog in Step 17, then skip to Step 22 .

Step 21 In the **Exposed IP** box, type the IP address that you want to expose to untrusted and unknown networks. To continue, click **Next**.

To perform network address translation for the network to which the specified adapter is attached, you must enter an IP address that is registered with InterNIC.

Note If this firewall server resides on an internal perimeter network, the exposed address must be a valid IP address on the network to which an untrusted network adapter card is attached.

The Collect Information screen displays.

Step 22 Type the IP address for the native Windows NT network stack (the Local Stack). To continue, click **Next**.

This IP address *must* be a valid address on the internal network to which the network adapter card is attached; however, it *cannot* be the same address as the address that you assigned to the network adapter.

Note See Chapter 5, "Inside the Cisco Centri Firewall," of the *Securing Your Network With the Cisco Centri Firewall* guide for a discussion of the native stack and how it relates to Centri Firewall's custom dynamic stacks.

The Collect Information panel displays.

Step 23 Type the IP address of the default gateway for the firewall server. To continue, click **Next**.

If the gateway is your external router, which is responsible for forwarding all communications between untrusted and unknown networks and the firewall server, then the IP address must be an IP address that is registered with InterNIC. If this firewall server resides on an internal perimeter network, the address must be a valid IP address on the network to which an untrusted network adapter card is attached.

Step 24 To apply a default security policy to the users on your trusted network(s), click the preferred default security policy option. To continue, click **Next**.

While your network is fully protected between the time that you reboot your computer after installing Cisco Centri Firewall and the time you configure it, the Centri Setup program provides two additional default security policies that you can apply to all network objects on your trusted network(s). The default security policy is applied immediately upon completion of the install process and provides all of your network users with the same network services. You can modify this security policy or apply new security policies at any time.

You must select one of the three default security policies:

No policy assigned. This option applies the default security policy that is inherent in Cisco Centri Firewall — *Reject*. This security policy means that no communications are allowed to traverse the firewall server until an enabling security policy is applied to at least one network object.

Basic Web, Mail. This policy provides the following services:

- Allows your users to send SMTP-based e-mail to untrusted and unknown networks, such as the Internet.
- Allows your users to perform DNS lookups and allows internal DNS servers to update their lookup information.
- Allows your users to ping hosts outside of your network.
- Allows your users to browse the web using HTTP. However, they cannot download Java applets, ActiveX objects, or JavaScript and VBScript scripts. In addition, they cannot use their browsers to post messages or to connect to FTP servers. The users are not required to authenticate to the firewall server before browsing.
- Allows your users to use browsers to connect to SLL servers, which encrypts all traffic between the client and the server.

Web, Telnet, Mail. This policy provides the following services:

- Allows your users to send SMTP-based e-mail to untrusted and unknown networks, such as the Internet.
- Allows your users to perform DNS lookups and allows internal DNS servers to update their lookup information.
- Allows your users to ping hosts outside of your network.

- Allows your users to browse the web using HTTP with full access without first authenticating to the firewall server.
- Allows your users to use browsers to connect to SLL servers, which encrypts all traffic between the client and the server.
- Allows your users to use FTP and TELNET to connect to external, untrusted servers without first authenticating the firewall server.
- Allows users to read and post messages to News servers using NNTP.

The Exposed Network Servers panel displays.

Step 25 To expose internal network servers to untrusted and unknown networks, select the types of network server(s) that you want to expose, and click **Next**.

These network servers must reside on your internal, trusted network(s). Exposing your internal UDP DNS server allows it to provide name resolution for your trusted network(s). Exposing your internal TCP DNS server allows it to perform zone transfers for your trusted networks. Exposing your mail server will allow it to receive e-mail from and deliver e-mail to external users. Exposing a web server enables it to service requests from external users.

For each network server type that you selected, a Collect Information panel displays.

Step 26 For the specified server that you selected to expose to untrusted and unknown networks, type the actual and exposed IP addresses and the port numbers to which service requests should be directed. To continue, click **Next**.

The actual IP address is the network IP address assigned to that server; the exposed IP address is the one that will be shown to untrusted and unknown networks. The TCP or UDP port numbers are those that correspond to the service provided by the specified server.

A separate screen is displayed for each network server type that you selected.

Repeat Step 27 as needed.

The Start Copying Files panel displays.

Step 27 Verify that you have specified the correct settings in the Current Settings list box, and click **Next** to copy the files to the computer and perform the initial configuration of Cisco Centri Firewall.

The Copying Files dialog box displays, and the progress bar provides information about the status of the files being copied. When this dialog box closes, the Setup Complete panel displays.

Step 28 To complete the install, click **Finish**.

The Reboot Now? dialog displays.

Step 29 To reboot your computer and activate Cisco Centri Firewall, remove any disks from the local disk drive and click **Yes** and then click **OK** in the Confirmation dialog box that displays. To wait until a later time to activate Cisco Centri Firewall (it will automatically activate the next time you restart your computer), click **No** and then click **OK** in the Confirmation dialog box that displays.

Congratulations! You have successfully installed the Cisco Centri Firewall. Once the firewall server reboots, you can perform any custom modifications that are required by your site's policy using the Centri Firewall user interface. To start the user interface, click **Centri Firewall** on the Start menu.