Before You Install Cisco Centri Firewall

Introduction

To install Cisco Centri Firewall, you must have the required hardware and software, your target computer must be configured appropriately, and you must have the answers to the questions that you will be asked by the Centri Setup program.

Caution The actual liscense registration scheme may differ from the documented procedures. Pease see the "Read Me First" insert to learn about the license agreement and to activate your license key.

This chapter explains what you need to know and do before install Cisco Centri Firewall. It includes the following information:

- what the hardware and software requirements are for the firewall server and the remote administrative computer;
- how Windows NT should be configured for the firewall server and for the remote administrative computer;
- how to make a back-up copy of the Centri License disk; and
- what information you should know before starting the install, as well as what information you must provide the Centri Setup program during the install.

Before you install Cisco Centri Firewall, you should verify that each computer targeted for the product meets the minimum hardware and software requirements for running the edition type that you plan to install. The next section of this guide describes the minimum hardware and software requirements and defines the procedures that you should follow to prepare the target computer.

Preparing the Target Computer

The computer on which you plan to install Cisco Centri Firewall must be properly configured for Centri to operate efficiently and securely. Preparing the computer intended for Centri installation may involve performing up to seven tasks, depending on how the computer is currently configured and depending on which configuration tasks you allow the Centri Setup program to perform for you:

1. Remove or disable all user accounts other than Administrator and rename the Administrator account.
2. Install and configure at least two network adapter cards.
3. Install and configure the TCP/IP network stack.
4. Remove all network protocols and network services that are not required.
5. Disable all services that are not required.
6. Verify that the TCP/IP network stack is configured and operating correctly.
7. Verify that the boot settings of the target computer are configured correctly.

Before you begin preparing the target Centri server, you should read the next section, entitled “Recommendations for Your Firewall Computer.” It defines which operating system you should use and draws your attention to special details of the operating system.

Recommendations for Your Firewall Computer

Cisco Systems, Inc. recommends specific hardware and software settings for the computer on which you plan to install Cisco Centri Firewall. If these recommended settings are not followed or are modified in any way, your Centri computer may not be secure. The hardware and software requirements depend on whether you are installing the full Cisco Centri Firewall or the Remote Administrative Interface.

To install the full Cisco Centri Firewall, the target computer must meet the following hardware and software requirements:

- a 90+ MHz Pentium-based computer
- 32+ MB RAM
- 2+ GB hard disk

- a SVGA-compatible video card with resolution support of at least 800 x 600 and 8-bit color support
- a SVGA-compatible display
- a CD-ROM drive
- a 1.44 MB 3.5" floppy disk drive
- at least two network adapter cards
- Microsoft Windows NT Server, Version 4.0 running the Windows NT file system (NTFS), must be installed, configured, and operating correctly

The Windows NT Server on which you are installing the Full Firewall Install must be configured as follows:

- The server must be partitioned using NTFS—not FAT.
- The server should be set up as a stand-alone server—not as a primary or secondary domain controller.
- The server must have Service Pack 2 (Service Packs are the means by which Windows NT updates are distributed) and the RPC patch installed and configured properly.
- At least two network adapter cards must be installed, configured, and operating correctly. You should install one network adapter card for the external network and one adapter card for each internal network that you intend to support with the firewall server.
- Network software for at least one network adapter card driver must be installed, configured, and operating correctly.
- The Microsoft TCP/IP components must be installed, configured, and operating correctly.
- The server should not lease any of its IP addresses from a DHCP server.
- Only one user account should exist on this computer. This account should have administrative privileges and should be used to install and administer Cisco Centri Firewall.
- Cisco Systems, Inc. recommends that you do not install any network protocols other than the TCP/IP protocol suite on the computer where you plan to install Cisco Centri Firewall. If your security policy does not require that you use any other protocols on this computer, you should remove them.

- If you plan to use Cisco Centri Firewall to apply security polices to Windows NT Domains, Group, and User accounts, the server must be a member of one of the trusted domains in your network. In addition, the domain that you select must have appropriate trust relationships with all of the domains that you want to administer to ensure that it can access the User Database that is maintained for those domains.

Note Because each additional service and application that you install on the firewall server increases the likelihood of problems arising on the system, Cisco Systems, Inc. does not recommend that you run any additional Windows NT Services on the firewall server. These services include applications such as a Remote Access Services (RAS), other network protocol stacks, and web tools and servers, including FrontPage, Internet Information Server, FTP, and DNS.

To install the remote administrative interface**,** the computer must have either Windows NT Workstation 4.0 or Windows NT Server 4.0 installed, configured, and operating correctly. The computer must also have an SVGA video card with resolution support of at least 800 x 600 and 8-bit color support; an SVGA compatible display; a CD-ROM drive; a 1.44 MB 3.5" floppy disk drive; and at least one network adapter card.

Note You can install the Remote Administrative Interface on Windows NT Workstation or Windows NT Server 4.0.

The Windows NT Workstation or Server on which you are installing the Remote Administrative Interface must be configured as follows:

- The computer must have Service Pack 2 and the RPC patch installed and configured properly.
- At least one network adapter card must be installed, configured, and operating correctly.
- Network software for at least one network adapter card driver must be installed, configured, and operating correctly.

- The Microsoft TCP/IP components must be installed, configured, and operating correctly.
- The computer should not lease any of its IP addresses from a DHCP server.
- Cisco Systems, Inc. recommends that you do not install any network protocols other than the TCP/IP protocol suite on the computer where you plan to install Cisco Centri Firewall. If your security policy does not require that you use any other protocols on this computer, you should remove them.
- If you plan to use Cisco Centri Firewall to apply security polices to Windows NT Domains, Group, and User accounts, the computer must be a member of one of the trusted domains in your network. In addition, the domain that you select must have appropriate trust relationships with all of the domains that you want to administer to ensure that it can access the User Database that is maintained for those domains.

Removing User Accounts

As the point of focus between your internal network and the external network, the firewall computer must provide as few avenues of access as possible. An important step in reducing access to a computer is to remove any user accounts that are not required.

Note This task can be performed by the Centri Setup program. If this option is selected, the Setup program removes or disables all user accounts on the local computer except for the account that is used to install Cisco Centri Firewall.

The Centri Setup program also provides an option that allows you to rename the Administrator account. By renaming the administrator account, you greatly reduce any attacker’s ability to run password cracking programs against your firewall server because they can no longer target a well-known account. We strongly recommend that you rename this account during the install process.

When you install the Windows NT operating system, two user accounts are created by default: Administrator and Guest. At least one account that belongs to the Administrators group is required to install any network components, including Cisco Centri Firewall.

Using the User Manager found in the Administrative Tools program group on the Start menu, you can remove all user accounts other than Guest and Administrator. You should also disable the Guest account (you cannot remove it).

A disabled user account still exists and is listed in the User Manager window; however, logons to that account are not permitted. You can restore a disabled account at any time.

To disable a user account:

Step 1 In the **User Manager** window, click the user account that you want to disable.

The built-in Administrator account cannot be disabled; however, during the Centri Setup program, you can rename this account.

Step 2 On the **User** menu, click **Properties**.

Step 3 To prevent logons to the selected user account, select the **Accounts Disabled** check box, and click **OK**.

The next section defines the procedure for installing the requisite networking components. Cisco Centri Firewall requires that you have (at a minimum) two network adapter cards installed on the firewall server: at least one that communicates with the internal network and one that communicates with the external network. The next procedure assumes that you have these network adapter cards installed in the computer.

⚠ **Caution** Windows NT allows you to define multiple IP addresses for each network adapter card. This feature is not directly supported by Cisco Centri Firewall. During the install process, only the first IP address is detected and presented as a default value. However, you can assign multiple IP addresses to each network adapter card from within the Cisco Centri Firewall user interface.

Installing the Networking Components

To install Cisco Centri Firewall, the computer must have a properly configured and operational TCP/IP protocol stack, as well as specific components that provide support for Microsoft Networking. This section defines the procedures that you must perform to install TCP/IP and these supporting components. Once you have installed these components, you will need to test the TCP/IP protocol stack to ensure that it is operating correctly.

To test the network configuration, you can use the TCP/IP connectivity utilities that are automatically installed with TCP/IP. These utilities include FINGER, FTP, RCP, rexec, rsh, TELNET, and TFTP. These utilities are also installed automatically with TCP/IP: ARP, hostname, ipconfig, nbtstat, netstat, ping, and route.

If you did not install TCP/IP when you installed Windows NT, you can do so using the following procedures. If you did install TCP/IP during the Windows NT install process, then go to the “Understanding Network Protocols and Services” section.

For TCP/IP to operate correctly, you must configure the IP addresses, subnet mask, and default gateway settings for both network adapter cards. To configure these settings, you must have the following information available:

- Two unused IP addresses (one for the external network and one for the internal network) and the subnet masks for both networks
- One or more IP addresses for the default gateways (one for the external IP router and additional ones for the internal IP routers, if applicable)

Note Assuming that your external network adapter card is connected to the Internet, the IP address should be a legal IP address assigned to your site by the Internet Network Information Center (InterNIC). This organization is responsible for registering and assigning IP addresses to those who wish to connect to the Internet. Also, you must be logged on as a member of the Administrator group to install and configure TCP/IP and its components.

The easiest way to ensure that you install all of the network protocols, services, and adapter drivers that are required by Cisco Centri Firewall is to delete all of the networking components and reboot the computer. Once the computer is rebooted, you can select the Network icon in the Control Panel to initiate the Network Setup Wizard. This wizard guides you through the process of setting up your networking components. In addition, it allows you to select on the options that you need. The following procedures explain how to configure the TCP/IP protocol and associated networking components. The first procedure in this section explains how to remove all of the networking components. The second procedure walks you through the Network Wizard and identifies the components that you should install.

To remove all networking components:

Step 1 On the desktop, right-click **Network Neighborhood**.

The Network dialog box displays.

If the you did not have a network adapter card installed when you performed the Windows NT install, a Network Configuration dialog box may display asking you if you want to set up Windows NT networking. If this dialog box displays, continue the next procedure to install the requisite networking components.

Step 2 Click the **Services** tab.

Step 3 For each service presented in the **Network Services** list, click the service and then click **Remove**.

A confirmation dialog box displays. Click **Yes** to remove all of the services in this list.

Step 4 Click the **Protocols** tab.

Step 5 For each protocol presented in the **Network Protocols** list, click the protocol and then click **Remove**.

A confirmation dialog box displays. Click **Yes** to remove all of the protocols in this list.

Step 6 Click the **Adapters** tab.

Step 7 For each network adapter card presented in the **Network Adapters** list, click the adapter and then click **Remove**.

A confirmation dialog box displays. Click **Yes** to remove all of the adapters in this list.

Step 8 Once you have removed all of the network services, protocols, and adapters, click **Close**.

When you close the Network property sheet, you must reboot your computer for the changes to take effect.

When you complete this procedure and reboot your computer, continue with the next procedure to install the requisite networking components.

To install the requisite networking components using the Network Setup Wizard:

Step 1 On the desktop, right-click **Network Neighborhood**.

The Network Configuration dialog box displays asking you if you want to set up Windows NT networking.

Step 2 To begin installing the networking components, click **Yes.**

The Network Setup Wizard displays. At this point, you can either select your network adapter in a list of supported network adapters or allow the wizard to automatically detect the adapter. This procedure assumes that you will select the network adapter manually.

Step 3 Click **Select from list**.

The Select Network Adapter dialog box displays.

Step 4 In the list of network adapters, click one of the adapters installed in this computer and click **OK**.

The network adapter that you select is listed in the Network Adapters box of the wizard. For each network adapter that you want to add, repeat Step 3 and Step 4.

Step 5 To continue installing the networking components, click **Next**.

The wizard displays the list of available network protocols.

Step 6 In the **Network Protocols** list, verify that the TCP/IP Protocol option is selected.

Step 7 Click **Next**.

The wizard displays the list of available network services.

Step 8 Click **Next**.

The wizard states that it is now ready to install the selected components.

Step 9 Click **Next**.

The Windows NT Setup dialog box displays and prompts you for the full path to the Windows NT distribution files.

Step 10 In the **Location of the distribution files** box, type the location of the distribution files and click **Continue**.

The wizard begins installing the networking components. A dialog box displays asking you if you want to use DHCP to dynamically provide an IP address. You do *not* want to assign IP addresses using DHCP on the firewall server.

Step 11 In the **TCP/IP Setup** dialog box, click **No**.

The wizard continues installing the networking components. The Microsoft TCP/IP Properties property sheet displays.

Step 12 In the **IP Address** box of the IP Address tab, type the IP address assigned to this network adapter card.

Step 13 In the **Subnet Mask** box, type the subnet mask for the network to which this network adapter card is attached.

Step 14 In the **Default Gateway** box, type the IP address of the default gateway.

If you are configuring the external network adapter card, the default gateway is the IP router through which the firewall computer will deliver packets to networks for which the firewall does not have a route defined. If you are configuring the internal network adapter card, the internal IP router is the default gateway. If your firewall configuration does not include an internal router, you should leave this box empty.

Step 15 To identify the DNS servers on your network, click the **DNS** tab.

Step 16 In the **Host Name** box, type the host name for this computer.

The host name allows some utilities to authenticate the local computer using its name. By default, this value is the Windows NT computer name, but you can assign another host name without affecting the computer name. Names are stored on DNS servers in a table. This table maps the host names to the IP addresses.

Step 17 In the **Domain** box, type the name of your DNS domain.

A DNS domain is not the same as a Windows NT or LAN Manager domain. This name is usually an organization name followed by a period and an extension that indicates the type of organization, such as cisco.com.

This Domain Name is used with the host name to create a fully qualified domain name (FQDN) for that computer. The FQDN is the host name followed by a period (.) followed by the domain name. For example, this computer’s FQDN could be firewall.gi.net, where firewall is the host name and gi.net is the domain name. During DNS queries, the local domain name is appended to host names.

Step 18 Verify that the **Domain Suffix Search Order** box is empty.

Step 19 On the **IP Address** tab, verify that the **Obtain IP address from a DHCP server** check box is *not* selected.

Step 20 On the **Routing** tab, verify that the **Enable IP forwarding** check box is *not* selected.

Step 21 To save your TCP/IP settings, click **Close**.

A dialog box displays notifying you that at least one network adapter has an empty primary WINS address.

Step 22 Click **Yes**.

The wizard continues and displays the binding information for all services.

Step 23 Click **Next**.

The wizard states that it is ready to start the network.

Step 24 Click **Next**.

The wizard prompts you for information about which Windows NT domain you want to join.

Step 25 If you plan to use Cisco Centri Firewall to apply security policies to Windows NT Domains, Group, and User accounts, specify the domain name. Otherwise, type a name for the Workgroup to which this computer will belong. To continue, click **Next**.

Step 26 To complete the networking component setup, click **Finish**.

When you complete the wizard, you must reboot your computer for the changes to take effect. When you complete this procedure and reboot your computer, continue with the “Understanding Network Protocols and Services” section.

Understanding Network Protocols and Services

Cisco Systems, Inc. recommends that you remove all network protocols other than the TCP/IP protocol suite. Any additional protocols can be installed, but they will not function.

From the Network property sheet in the Control Panel, you should remove all components *except* for the following:

- **Network Adapter Card Driver(s)** (actual name varies). These drivers, located on the Adapters tab of the Network property sheet, map directly to the network adapters that you have installed on the firewall computer.
- **TCP/IP Protocol.** This service, located on the Protocols tab of the Network property sheet, provides communication across interconnected networks made up of computers with diverse hardware architectures and various operating systems. The TCP/IP protocol suite can be used with Windows NT alone, to communicate with devices using other Microsoft networking products, or to communicate with non-Microsoft computers. The TCP/IP protocol suite is used to communicate across the Internet.
- **Computer Browser.** This service is the Microsoft Network Browser service; it maintains an up-to-date list of computers and provides that list to requesting applications. It provides the list of computers displayed in the Select Computer and Select Domain dialog boxes. The TCP/IP protocol services are dependent on this service.
- **RPC Configuration.** This service, located on the Services tab of the Network property sheet, enables programs that use Remote Procedure Calls (RPCs) to perform procedures on multiple computers. It includes the endpoint mapper and other RPC services.
- **NetBIOS Interface.** This service, located on the Services tab of the Network property sheet, defines the software interface and naming convention for Microsoft Networking.
- **Server.** This service, located on the Services tab of the Network property sheet, is the Microsoft Windows Server service; it provides network connections and communications by installing the Server Message Block (SMB) protocol. The TCP/IP protocol services are dependent on this service.
- **Workstation.** This service, located on the Services tab of the Network property sheet, is the Microsoft Windows Workstation service; it provides network connections and communications by installing the client for the Server Message Block (SMB) protocol. The TCP/IP protocol services are dependent on this service.

Once you have removed non-required protocols, you should restart the computer and then test the TCP/IP networking component to verify that all drivers and services are functioning correctly.

Verifying that TCP/IP is Functioning Correctly

To install Cisco Centri Firewall, you must have a configured and functioning TCP/IP protocol stack. If you have installed Windows NT but have not tested the TCP/IP networking functionality, we strongly urge that you take the time to do so. You can test it in at least two ways: you can verify that the firewall server is able to communicate using TCP/IP, and you can verify that other computers on the network can communicate with the firewall server.

Caution You should not perform testing while connected to the external network. Because the firewall is not installed and configured, your network and firewall will be exposed to all users on the external network.

To verify that your TCP/IP connection settings are operating correctly:

Step 1 To verify that the server can communicate using TCP/IP, use the **ping** command to ping an IP address of a computer that you know has the network software installed correctly. To test each network adapter card, ping a computer on both networks.

Step 2 To verify that other computers can communicate with the firewall server, use the **ping** command to ping the firewall computer. To test each network adapter card, **ping** the firewall computer from a computer on each network.

You can only ping the firewall’s interface that is connected to that network. You cannot ping through the firewall to the other network. Once the underlying TCP/IP software and networking hardware are functioning correctly, the Centri installation procedures should proceed smoothly.

Verifying the Boot Settings

We strongly recommend that you set the startup time-out to zero seconds and that you load Windows NT by default.

To change the time-out setting to zero:

Step 1 In the **Control Panel**, double-click **System**.

Step 2 On the **Startup/Shutdown** tab, change the value of the **Show list for** box to zero.

Once you have prepared your target computer, you should make a backup copy of the Centri License disk. The next section defines the procedure for performing this task.

Making a Backup Copy of the Centri License Disk

To ensure that the original Cisco Centri Firewall License disk is not damaged during installation, you should make a working copy of the disk. To make a backup disk, you need a *formatted* blank disk and a label for each original disk that you received in the Centri package.

To make a backup copy of the original Centri License disk:

Step 1 Prepare a label for the disk that you intend to copy using the information that is provided on the original Cisco Centri Firewall disk's label.

Step 2 To get to a DOS prompt from within Windows NT, double-click the DOS Prompt icon located in the Main program group of the Program Manager.

Step 3 At the DOS prompt, enter the following command:

diskcopy *`a: a:`*

where *`a:`* is the drive letter of your 3.5" disk drive.

Example Result: The following message displays:

```
C:\diskcopy a: a:

Insert SOURCE diskette in drive A:

Press any key to continue . . .
```

Step 4 Insert the original Centri License disk into your 3.5" disk drive.

Step 5 To begin copying the disk in the 3.5" disk drive, press the Enter key.

Step 6 When you are prompted to `Insert TARGET diskette in drive A:`, insert a blank formatted disk into the 3.5" disk drive, and press the Enter key.

Step 7 Switch the disks as prompted until the following message displays:

```
Copy another diskette? [Y/N]
```

Step 8 Press **N** to quit.

Step 9 Remove the target disk from the drive, and place the label on the target disk that corresponds to the source disk that you just copied. Store the original disk in a safe, dry, cool location.

The next section identifies the information that you should gather before proceeding with Chapter 2, “Before You Install Cisco Centri Firewall.”

Things to Know Before Installing Centri

During the install process, you will be asked for information that you must supply to complete the installation successfully. This information includes the following.

- The network IP addresses of the following network objects:
  - your internal mail server
  - your internal DNS server
  - internal Web server
  - external router
  - registered IP address to expose to external users
- The section entitled “Pre-Installation Worksheet,” includes a worksheet to help you gather the information that you will be asked for during the install process.
- Your Centri License Key Password Phrase. Cisco Centri Firewall is designed to operate only with a valid enabling key. To obtain a valid key and to register your software, please refer to the Product Registration Form.

- Lastly, before installing the system you should have read *Securing Your Network With the Cisco Centri Firewall*, so you have a good understanding of the system and know how you want to configure the system. This guide provides information about the initial setup of your product and explains those concepts that you need to understand before you install the product. Fill out the worksheets in Chapter 6 of the guide so that you know and are able to configure your network's topology and your network security policies.

Pre-Installation Worksheet

The worksheet presented on the following pages identifies the information that you will be asked during the install process. Collecting this information beforehand ensures that you can complete the installation with a minimally configured firewall that securely provides access to your network users.

The next chapter provides step-by-step procedures for installing your Cisco Centri Firewall system.

Table 1-1 Pre-Installation Worksheet

Network Object	IP Address	Port	Description
External Router		N/A	The router on your outermost perimeter network.
External Adapter		N/A	The IP address to assign to the network adapter card attached to your outermost perimeter network.
Internal Router(s)		N/A	The router(s) on the internal perimeter network just inside the firewall server.
Internal Adapter(s)		N/A	The IP address(es) to assign to the trusted network adapter cards that connect the firewall server to internal network(s).
Exposed IP Address		N/A	The IP address that Cisco Centri Firewall will expose to untrusted and unknown networks.
Local Stack		N/A	The IP address to assign to the native Windows NT stack.
Internal DNS Server			The IP address and TCP port number of your internal DNS server that performs DNS zone transfers.
External DNS Server			The IP address and TCP port number that you want to expose for access to the server identified above.
Internal DNS Server			The IP address and UDP port number of your internal DNS server that performs DNS lookups for your network users.
External DNS Server			The IP address and UDP port number that you want to expose for access to the server identified above.
Internal Web Server			The IP address and TCP port number of your internal Web server that you want users on untrusted and unknown networks to be able to access through the firewall server.
External Web Server			The IP address and TCP port number that you want to expose for access to the server identified above.
Internal Mail Server			The IP address and TCP port number of your internal SMTP-based mail server that will deliver messages between your networks and untrusted and unknown networks.
External Mail Server			The IP address and TCP port number that you want to expose for access to the server identified above.
Account Name	**Password**		**Description**
			Account used to install Cisco Centri Firewall.
			Account used to administer Cisco Centri Firewall.