Text Part Number: 78-4670-07

Cisco Centri Firewall Version 4.0.5 Release Notes

August 1999

These release notes describe the features and caveats for Cisco Centri Firewall version 4.0 up to and including version 4.0.5(171). The following topics are discussed:

- "Product Documentation," page 1
- "Platform Support," page 2
- "Memory Requirements," page 2
- "New Hardware Features," page 2
- "New Software Features," page 2
- "Installation Issues," page 6
- "Y2K Operating System Requirements," page 7
- "Important Notes," page 7
- "Version 4.0.5(171) Caveats," page 8
- "Centri Firewall Code Revision History," page 13
- "Cisco Connection Online," page 18
- "Documentation CD-ROM," page 19

Product Documentation

The Cisco Centri Firewall documentation set includes the following documents:

- *Securing Your Network with the Cisco Centri Firewall*, Text Part Number 78-4632-01
- *Cisco Centri Firewall Installation Guide*, Text Part Number 78-4634-01
- Online Help (Select **Help Topics** or **What's This?** on the **Help** menu in the Centri Firewall user interface)
- HTML Reference Documentation (Select **HTML Help Browser** on the **Help** menu in the Centri Firewall user interface)

Corporate Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA

Platform Support

This release supports single-processor, Pentium and higher, Intel-based microcomputers running the Microsoft Windows NT 4.0 operating system and Service Pack 3 (English and Japanese versions).

Note Do not use a Service Pack other than those specified for your version of the Windows NT 4.0 operating system.

Memory Requirements

This release requires a minimum of 32 MB of RAM.

New Hardware Features

This section defines the new hardware supported by Centri Firewall version 4.0.2(142) and later.

Network Adapter Cards

Centri Firewall version 4.0.2(142) and later now supports Token Ring networks and network adapter cards. In addition, only one known restriction exists for supported Ethernet network adapter cards. Previously, only a select set of Ethernet network adapters were supported.

The following Ethernet network adapter does not work with Centri Firewall:

- SMC 16 EZ

The following Token Ring network adapter has been tested with Centri Firewall version 4.0.2(142):

- Madge Smart 16/4 PCI Ring Node

The following Token Ring network adapter does not work with Centri Firewall:

- IBM PCI Token Ring

Network adapter incompatibility symptoms include a system lockup after installing the firewall on an operational network host. If you see these symptoms, please contact the Cisco Technical Assistance Center (TAC). [CSCdk09496]

New Software Features

This section defines the new software features provided by Centri Firewall version 4.0.1(110) and later.

Centri Firewall 4.0.5(171) Software Features

This release of Centri Firewall is year 2000 compliant. The only changes made to the system ensured that the product is Y2K compliant.

Centri Firewall 4.0.4(170 and later) Software Features

Pager-Based Notifications

To make numeric pager notifications work in Centri Firewall 4.0.4, you must perform the following tasks:

- Edit the Windows NT Registry to specify the correct key and values
- Specify the timeout setting in the Modem Properties dialog box under Control Panel
- Enter the numeric pager number and message for the audit event about which you want to be notified. For more information about defining notifications, refer to the *Cisco Centri Firewall Frequently Asked Questions* document located at the following URL: **http://www.cisco.com/warp/public/458/centrifaq1.html**

Note The pager-based notifications only work for numeric pagers. Alphanumeric pager systems are not supported.

To specify the correct key and values in the Windows NT Registry, perform the following procedure:

Step 1 To start the Registry editor, click **Run** on the **Start** menu and type **regedt32**. Press **Enter**.

Step 2 Create the following Registry key under the HKEY_LOCAL_MACHINE key:

SOFTWARE\Cisco Systems\Centri\Pager

Step 3 Under the **Pager** key, create the following Registry values under the HKEY_LOCAL_MACHINE key:

Value Name	Value Type	String Value
Port	REG_SZ	This value represents the port on which the modem is installed on the firewall server. For example, COM1.
Timeout	REG_SZ	This value represents the number of seconds that can occur between the time the message is sent to the modem and the time that the modem hangs up on the call. This value may vary depending on your paging service. For example, 60.

To specify the timeout setting in the Modem Properties dialog box, perform the following steps:

Step 1 Click **Start**, point to **Settings**, and then click **Control Panel**.

Result: Control Panel appears.

Step 2 In **Control Panel**, double-click **Modems**.

Result: The Modem Properties applet appears.

Step 3 To view the properties, select the correct modem from the list, and then click **Properties**.

Result: The properties dialog box for the selected modem appears.

Step 4 To view the connection settings, click the **Connection** tab.

Step 5 To specify the timeout setting, type the value in the **Cancel the call if not connected within** box.

This value should match the value that you previously assigned to the Timeout value in the Registry.

Step 6 To close the properties dialog box for the selected modem, click **OK**.

Result: The properties dialog box closes.

Step 7 To close the **Modem Properties** applet, click **Close**.

Result: The Modem Properties applet closes.

Centri Firewall 4.0.1(110 and later) Software Features

userauth Program

When you have applied a security policy to your domain, Centri Firewall ensures that any domain user trying to access services through the firewall has permission by enforcing out-of-band user authentication. For this reason, you need to configure all clients on the domain to start up a logon script, which is a batch or executable file that runs automatically when a user logs on. This logon script, which is invisible to the user, must start the *userauth* program included with Centri Firewall so that the required out-of-band user authentication works properly.

We recommend that you install *userauth* on the domain controller and that you configure a logon script for each user who needs to meet the out-of-band authentication requirement. If your domain incorporates multiple domain controllers, you must install the logon script on each domain controller and install *userauth* on the primary domain controller.

The command-line parameters for *userauth* are as follows:

userauth <*machine name of firewall*>

For example, if your firewall machine is named “Centri,” the command-line parameters are as follows:

userauth Centri

To configure *userauth* and a logon script for domain authentication, perform the following steps:

Step 1 On the domain controller, use Windows NT Explorer to create an executable directory (such as c:\firewall), copy userauth.exe from the **bin** directory of the firewall into that directory, and then share that directory as **Firewall**.

Step 2 Using a text editor such as Notepad, create a file named **Firewall.bat** in the **%systemroot%\system32\repl\import\scripts** directory of the domain controller.

Step 3 On the first line of the file, type **REM for firewall authentication**.

Step 4 On the second line of the file, type **start ***PDC***\Firewall\userauth.exe** *Centri*, where *PDC* is the name of the primary domain controller and *Centri* is the name of your firewall.

On the domain controller, you must then enable the logon script for each user who needs to meet the out-of-band authentication parameters. Perform the following steps:

Step 1 Click **Start**, point to **Programs** and then **Administrative Tools (Common)**, and click **User Manager**.

Result: The User Manager appears.

Step 2 In the list of users in the **User Manager**, double-click a username.

Result: The User Properties dialog box appears.

Step 3 In the **User Properties** box, click **Profile**.

Result: The User Environment Profile dialog box appears.

Step 4 In the **Logon Script Name** box, type **Firewall.bat**, and then click **OK** for both the **User Environment Profile** box and the **User Properties** box.

For more information about logon scripts, refer to your Windows NT documentation.

ODBC-Compliant Database Archival

Centri Firewall 4.0.4 (170) supports archival of session data via the Microsoft ODBC API. To configure Centri Firewall to archive session data to an ODBC-compliant database, you must install an ODBC driver and configure Centri Firewall to write data to that driver. The following procedures explain how to perform both of these tasks on the firewall server.

To install an ODBC driver and specify the data source path, perform the following steps:

Step 1 Click **Start**, point to **Settings**, and then click **Control Panel**.

Result: Control Panel appears.

Step 2 In **Control Panel**, double-click **ODBC**.

Result: The ODBC Data Source Administrator applet appears.

Step 3 To add a new data source, click **Add** on the **User DSN** tab.

Result: The Create New Data Source dialog box appears.

Step 4 Under **Name**, select the database type that you want to use to create the data source that Centri Firewall will use to archive session records.

Step 5 To create the new data source, click **Finish**.

Result: The ODDC Setup dialog box appears for that database type.

Step 6 In the **Data Source Name** box, type the name that you want to use to identify this data source, and then press **Tab**.

Step 7 In the **Description** box, type a description (if desired), and then press **Tab**.

Step 8 Depending on the type of driver that you selected, you must complete additional fields in this dialog box, including identifying the location of the database.

Step 9 When you complete all the fields in the **ODBC Setup** dialog box, click **OK**.

Result: The ODBC Setup dialog box closes.

Step 10 To close the **ODBC Data Source Administrator** applet, click **OK**.

Result: The ODBC Data Source Administrator applet closes.

To configure Centri Firewall to use the Data Source Name (defined in the previous procedure) for ODBC archival, perform the following steps:

Step 1 In the **Navigation** pane, click **Networks** to expand the tree.

Step 2 On the **Networks** tree, double-click **Centri Server**.

Result: The Security Knowledge Base property panel appears.

Step 3 Click the **Audit Record Archival** tab.

Step 4 Under **Purge Audit Records** in the **Retain audit records for** box, type the value that represents the number of days that you want the Security Knowledge Base to maintain audit records before they are purged.

Step 5 In the **Limit database size to** box, type the value that represents the maximum size that you want to allow for the Security Knowledge Base before the oldest audit records are automatically purged.

Step 6 In the **Examine database age / size every** box, type the number of minutes that should pass before the Security Knowledge Base is examined.

The Security Knowledge Base is examined to determine whether it contains audit records that are older than the value specified in Step 4 or it has exceeded the maximum size value specified in Step 5. The optimal value for this field is dependent on the number of audit records being generated and the amount of disk space that can be temporarily used by the Security Knowledge Base.

Step 7 To archive data to an ODBC-compliant database, click **Archive purged data** under **Target Archival Database**.

Step 8 In the **Data Source Name** box, type the name of the data source that you defined in the previous procedure.

This information is available in the ODBC Data Source Administrator applet in Control Panel.

Step 9 In the **Username** box, type the username of the account that will be used to connect to the database identified in the **Data Source Name** box.

Step 10 In the **Password** box, type the password that the database uses to authenticate the specified username.

Step 11 To close the **Centri Server** node, click **OK**.

Step 12 To save your changes, click **Save** on the **File** menu.

Installation Issues

For complete installation instructions, refer to the *Cisco Centri Firewall Installation Guide* document. The following list identifies issues that you should be aware of before attempting to install the product.

Caution When you install Centri Firewall, the Windows NT administrative account that you use to install the product must have a password that is not blank. If you attempt to install the product using an account with a blank password, Centri Firewall will not work.

- To use the HTML-based installation program, you *must* use the Microsoft Internet Explorer web browser. This installation program does not work properly with Netscape Navigator. [CSCgi01709]
- The Centri Setup program does *not* support pathnames that include spaces in the target installation directory, such as C:\Program Files\Centri\.
- The Centri Setup program does not check the new and confirmed passwords for case sensitivity. This bug exists within the InstallShield program and will be corrected in a later version. Be sure to use the same case to type and confirm the password.
- Install this product only on Windows NT 4.0, not Windows 95.

- The Centri Setup program does not support more than ten network adapter cards in the target computer.
- Multiple warning and message boxes may appear when bindings are calculated. These message boxes are benign. Click **OK** to close them and continue with the install process. [CSCgi01034]

Y2K Operating System Requirements

Centri 4.0.5 requires that you install Windows NT 4.0, Service Pack 4 and Internet Explorer 3.02 with the Y2K patch applied. You can download these patches from the Microsoft web site at the following URLs:

- http://www.microsoft.com/ntserver/nts/downloads/recommended/NT4SvcPk4/NT4SvcPk4.asp
- http://www.microsoft.com/ntserver/nts/downloads/recommended/NT4y2kpostSP4/default.asp
- http://www.microsoft.com/msdownload/iebuild/ie3y2k_win32/en/ie3y2k_win32.htm.

Important Notes

This section describes the issues that you should understand before using the Centri Firewall version 4.0.4 (170) software.

Windows NT Interoperation

Once Centri Firewall is installed, we strongly recommend that you do not use the Network applet in Control Panel to make modifications to the local network stack addresses. To make modifications to these addresses and any installed IP addresses, use the Centri Firewall user interface. [CSCgi01783]

Once Centri Firewall is installed, modifications to the routing rules on the firewall server made using the **route** command will have no effect on the system. To make modifications to the routing rules for the firewall server, use the Centri Firewall user interface.

If your Centri Firewall server stops sending traffic under high loads, the firewall server may be running low on Non-paged pool. To increase the Non-paged pool, perform the following procedure:

Step 1 To start the Registry editor, click **Run** on the **Start** menu and type **regedt32**. Press **Enter**.

Step 2 Select the following Registry entry from the HKEY_LOCAL_MACHINE key:

SYSTEM\CurrentControlSet\Control\Session Manager\Memory Management\NonPagedPoolSize

Step 3 Use the appropriate value in the following table to change the value of this entry. The radix (decimal or hex) that you use should match the installed physical memory in your firewall server. The maximum Non-paged pool allowed is 128 MB decimal or 8000000 hex.

Note If you change this value to one that is greater than the physical memory of the firewall server or greater than 128 MB, Windows NT will crash.

Physical Memory in Firewall Server	Decimal Radix	Hex Radix
32 MB	8388608	800000
64 MB	25165824	1800000

Physical Memory in Firewall Server	Decimal Radix	Hex Radix
96 MB	41943040	2800000
128 MB	58720256	3800000

System Backup

Do *not* use a remote administrative interface to back up the Centri Firewall Security Knowledge Base.

You should set up your system configuration, and then you should back up this information by clicking **Backup** on the **File** menu. Procedures for backing up and restoring the firewall system are provided in the online Help system (click **Help Topics** on the **Help** menu). [CSCgi01606]

Version 4.0.5(171) Caveats

Basic System Issues

The default security policies applied during the Centri Setup program do not include default inbound security policies. To enable incoming communications, such as e-mail addressed to your network users from the Internet, you must apply a security policy to the Internet node on the Networks tree.

If your firewall services heavy traffic loads, you should reduce the level of audit records maintained in the Security Knowledge Base. Under sustained heavy loads, detailed audit records can overload the Security Knowledge Base, which can cause throughput problems that lead to slower performance.

Network services and applications that require dynamic port assignments (negotiated ports) to set up a session do not work unless a kernel proxy has been provided, such as FTP. Also, the TCP and UDP proxies do not allow this feature. Currently, only FTP supports this feature.

Default network services are not defined for NetBIOS and many frequently used network services in the Microsoft networking environment. [CSCgi01940]

You should review the disk space requirement in the Centri Server node of the Networks tree. Otherwise, the firewall server may run out of disk space and shut down. The default value is 488 MB.

If you use an exposed service to communicate to an FTP server, you cannot perform FTP queries from the client that resides on the same site as the FTP server. Instead, the clients should communicate directly to that FTP server rather than passing through the Centri Firewall server. [CSCgi01485]

During system boot, the domain controller cannot be found initially. This lack of connectivity is normal; once the firewall services are started, you can connect to the domain controller normally. [CSCgi01536, CSCgi01703]

Do *not* define routing rules for the local stack. The routing rules for the local stack are defined by the firewall. If you change or define new routing rules for the local stack, the firewall may cease to function.

If you are running the network services in proxy mode and you have services that typically deal with multiple network services, such as HTTP using FTP and SLL, these additional services are controlled by security policies that enforce specific rules for those services. In other words, a

security policy that would handle each of these additional services must include a separate set of rules for each of these services (such as FTP and SLL) or else another security policy should be used to control communications using these additional network services.

Note This solution is only required for network services running in proxy mode that use additional network services.

If you change the name of the computer (Windows NT computer name) after you install Centri Firewall or you remove the user account that you used to install the Centri Firewall, you cannot remove the software automatically. To remove the software after you change the computer name, you must use a user account with administrative privileges to remove the files and Registry entries manually. The following procedure identifies this process:

Step 1 Delete the Centri root directory and all files listed in that directory.

Step 2 Delete the **fw.sys** file located at **%SystemRoot%/system32/drivers/**.

Step 3 Delete the following Registry keys found under the HKEY_LOCAL_MACHINE key:

/SOFTWARE/Cisco Systems/Centri

/SYSTEM/CurrentControlSet/Services/Fw

/SYSTEM/CurrentControlSet/Services/FwAdapter

/SOFTWARE/Microsoft/Windows/CurrentVersion/App Paths/Cat.exe

/SOFTWARE/Microsoft/Windows/CurrentVersion/Uninstall/Centri v4.0

Step 4 In addition, from the **Network** applet in Control Panel, click the **Bindings** tab to force a recalculation of the network bindings. You must reboot your computer when this recalculation is completed.

HTTP Kernel Proxy

S/Key authentication is not supported by the HTTP kernel proxy. [CSCgi01874]

Gopher is not supported in HTTP proxy mode.

If you add a rule to the HTTP filter list, it quickly takes effect. However, if you remove a rule from the filter list, the time to take effect varies up to several hours. The size of the list and the speed of your DNS lookups are directly proportional to the time required for a removed rule to take effect.

If the HTTP authentication setting is “strict” and a user requests a page on *WebServerA* that makes requests to *WebServerB*, the user will be required to authenticate twice, once for *WebServerA* and once for *WebServerB*. [CSCgi01877]

FTP Kernel Proxy

In proxy mode, the deny message does not appear.

Centri Firewall does not deal with passive mode FTP. [CSCgi01933]

Telnet Kernel Proxy

Currently, the command set does not include support for blank entries that do not display the help information, as well as several control key options that support word and line erasures and quitting. [CSCgi01452]

In proxy mode, the welcome and prompt strings do not appear.

Security Policies

If you apply any security policies to a Windows NT domain, User account, or Group account and the firewall server cannot contact the domain controller or it is unavailable, communication requests relying on those security policies are not processed by the firewall server. Once communication is re-established with the domain controller, domain-based security policy communications through the firewall resume. [CSCgi01936]

If you design a security policy that does not contain a network service (e.g., *if (time condition) then Accept* or *if (destination = X) then Accept*), the security kernel automatically assigns a "Reject" security policy because it cannot determine which kernel proxies to start. The fact that it is automatically rejected is not reflected in the Policy Builder control. [CSCgi01216]

Reporting and Monitoring

By default, no audit records are stored (including detailed statistics). You must enable the logging of audit records before you can use the reporting features. You should enable only those audit records that are required by your organization's security policy.

While the following case can appear for any service under high loads, you will see it most often with HTTP. When you have high loads, warning messages are often generated stating that a session was denied. These warning messages appear to be attacks, though they are actually late arriving packets for an already closed/completed session. The symptoms of these warning messages include the source address for a valid server connecting to port 80, and the destination address for a valid internal client that can initiate an HTTP session.

All activities of non-HTTP protocols that operate over HTTP are reported as part of HTTP if running in proxy mode. If they are not in proxy mode, individual reports are generated for each network service, such as SSL. [CSCgi01954]

Summary reports behave differently from detailed reports. If you generate a summary report from one "hour" through "now" (the current time), the current hour's report is generated, even if the current hour has just begun. This attribute holds true for a time range of "1 day," which starts at 12:00 a.m. If the current time is 9:00 a.m. and if you requested a summary report for "1 day," you'll get summary of data between midnight until 9:00 a.m. If you want a summary report between yesterday 9:00 a.m. and the current time, use "24 hours" instead of "1 day." However, detailed reports do not round off to the beginning of the time interval (hour/day/week). A detailed report for "1 day" generates the same report as for "24 hours." [CSCgi01838]

To change the port on which the Centri Examining agent listens (by default, TCP port 8080), you must delete the Centri Examiner network service and create a new Centri Examiner service that requires a different port number. Once this network service is created, you must direct the built-in browser to the new port number by editing the value that is assigned in the HTML Report box on the Options dialog box, which is accessed by clicking **Options** on the **Tools** menu. A secondary effect of this issue occurs when you are trying to use the remote administrative interface. To get the correct information, you must direct the remote administrative interface to the firewall server (by clicking **Options** on the **Tools** menu), but you do not need to change the port on which the Centri Examiner service listens unless you have changed it on the firewall server due to a conflict of services.

However, you must configure Microsoft Internet Explorer on the Remote Administrative Interface computer to bypass the proxy server for local (intranet) addresses. This configuration ensures that requests to the Examining agent are processed correctly.

User Interface Issues

When you make changes in the user interface, you must click **OK** to commit the changes. Once the changes are committed, the view area grays out. Unless otherwise noted, you must also click **Save** on the **File** menu to save all committed changes.

Under very heavy loads, it is possible to start multiple instances of the user interface. If you start the user interface and see the hourglass for five seconds, it is possible that another instance of the user interface has been detected running on a remote computer. If the other instance cannot reset the appropriate lock due to a heavy load on the Security Knowledge Base, the second instance may be allowed to start. If you do not see the hourglass for five seconds and the user interface begins loading, another instance is *not* running. You should be aware of this possibility, because running multiple instances of the user interface could cause serious repercussions in your security policies. [CSCgi01938]

If you attempt to drag and drop a security policy onto an active network node that has its property sheet appearing in the View pane, the action will fail. You must deselect or close the active window before the drop operation will work.

If you rename an entry under the Services tree, any statistical data that you are generating for that service will be lost.

S/Key accounts cannot be extended using the Centri Firewall user interface. You must regenerate a new set of passwords. [CSCgi01378]

The use of Cut, Copy, and Paste is not consistent.

The Undo and Redo commands on the toolbar and in the **Edit** menu alter modifications to the Navigation pane only. They do not operate on activities performed within the View pane.

Printing support is limited to the Navigation pane of the user interface. Support is not provided for entries in the View pane. Also, Print Preview may not preview correctly if you zoom in and out repeatedly.

If the URL location specified in the **Options** box (available under the **Tools** menu) is invalid, the built-in browser control will crash. This problem exists within Microsoft Internet Explorer.

Some context-sensitive Help topics are unavailable or apply to multiple controls.

Unsupported Software

Remote Access Services (RAS) is *not* supported on the firewall server.

Because Progressive Network's RealPlayer requires the UDP connections (instead of the optional use of UDP in RealAudio), Cisco Systems, Inc. does not enable RealPlayer connections as part of the default security policy provided by the Centri Firewall Setup program. If you are using the Network Address Translation (NAT) feature, you will *not* be able to use RealPlayer.

Unsupported Hardware

This release has been tested only on single-processor computers (Intel-based). Multi-processor computers have *not* been tested.

Centri Firewall only supports Ethernet and Token Ring network adapter cards. No other network media are supported.

The following network adapters do not work with Centri Firewall:

- SMC 16 EZ (Ethernet)
- IBM PCI (Token Ring)

Network adapter incompatibility symptoms include a system lockup after installing the firewall on an operational network host. If you see these symptoms, please contact the Cisco Technical Assistance Center (TAC). [CSCdk09496]

Centri Firewall Code Revision History

This section describes the Centri Firewall code revision history.

Centri Firewall 4.0.5(171) Modifications

Centri Firewall 4.0.5(171) fixes the following issues:

- WinFMS not reading parameters correctly. [CSCdm04834]
- GUI does not report version correctly. [CSCdm07563]
- Dates reported incorrectly. [CSCdm07567]
- Dates with MM-DD-YY or MM-DD-YYYY are invalid. [CSCdm07570]
- Invalid date entries generated 12/31/69. [CSCdm07577]
- Help reports invalid date format. [CSCdm07581]
- Date operation ranges differ. [CSCdm07588]
- Implicit century operations incorrect. [CSCdm07597]

Centri Firewall 4.0.4(170) Modifications

Centri Firewall 4.0.4(170) fixes the following issues:

- TCP proxy sends an RST in response to an ACK, when a SYN+ACK is expected. [CSCdk36774]
- The demo install does not work. [CSCdj50814]
- Remove benign warning and information messages in the NT Event Viewer. [CSCdj60478]
- Explain the Address Translation Error message. [CSCdj61865]
- UserAuth should report when a user logs off. [CSCdj62037]

Note This feature does not work if the userauth process is killed using the Windows NT Task Manager or a similar utility.

- Uninstall deletes the incorrect key in the Windows NT Registry. [CSCdj62421]
- If you select Print Preview and have not specified a default printer in the Printer Control Panel, the Centri user interface locks. [CSCdj73643]
- Pager notification does not work. [CSCdj85354]

Note Currently, only numeric paging works. Alphanumeric paging does not.

- Unauthorized users can access services enabled by security policies applied to Windows NT User and Group accounts. [CSCdj91845]
- Centri scheduled reports directory not fully functional. [CSCdj93575]
- The Centri Setup prompts the user for exposed server addresses and information when Network Address Translation (NAT) is not selected. [CSCdk00745]

- Summary reports broken when based on X through Y time periods. [CSCdk05177]

Note With this fix, Centri Firewall 4.0.4(170) is fully Y2K compliant.

- When a Windows NT Domain-based security policy is downloaded with proxy mode traffic, the firewall server blue screens. [CSCdk08442]
- IP address conflict causes infinite logging. [CSCdk08599]
- When an ICMP TTL expired message is destined through the firewall, it does not pass. [CSCdk08773]

Note If you allow ICMP in your policy, Windows NT **traceroute** can now traverse the firewall.

- Frame persistency bits reset. [CSCdk36776]

Centri Firewall 4.0.3(165) Modifications

Centri Firewall 4.0.3(165) fixes the following issues:

- Microsoft Internet Information Server (IIS) and PowerChute Plus do not run on the local firewall server with Centri Firewall. The Dr. Watson application log identifies a failed call to EnumProtocolsA. [CSCgi01016]
- Centri Firewall does not archive session data in ODBC-compliant databases. Instead, only raw event data is stored. [CSCdk04179]
- The warning reports generated by Centri Firewall are not Y2K compliant. [CSCdj45989]
- When using the HTTP kernel proxy with authentication (loose or strict), Centri Firewall does not process web browser cookies correctly. This problem is caused by failure of the firewall to determine which cookie is a proxy cookie. [CSCdk05056]
- FTP control channel does not explicitly clean up data sessions on exit, which causes firewall data channels to remain open. After time, no new sessions are allowed because resources are unavailable. [CSCdk06628]
- Race condition in the Security Knowledge Base. A thread can access and lock data that another thread has committed to deletion. [CSCdk06630]
- TCP may erroneously transition to the CLOSE_WAIT state. [CSCdk09539]
- Blue screen caused by applying the first security policy to a Windows NT Domain object. [CSCdk09543]
- Controlled Host Component performs expiration checks on permanent licences. [CSCdk10218]

Centri Firewall 4.0.2(156) Modifications

Centri Firewall 4.0.2(156) fixes the following issues:

- The Centri driver dependencies do not compute correctly for some network adapter cards, including some SMC network adapter cards. This problem causes the firewall server to hang as soon as network traffic occurs. [CSCdj90800]

- The Security Knowledge Base does not free and lock list elements correctly, causing a race condition. [CSCdj89353, CSCdj89354, CSCdj89356]
- Handles to the Security Knowledge Base are not released correctly, which consumes system resources in the form of a memory leak and then crashes the Security Knowledge Base. [CSCdj89355, CSCdj89357]
- Users experience frequent “connection is reset by peer” error messages when using the HTTP proxy in Centri Firewall. Connections seem to fail more often for high-traffic web servers that are running Microsoft Internet Information Server. The server sends out TCP resets when it is busy instead of dropping the SYN. [CSCdj87622]
- HTTP 1.1 traffic cannot pass through the firewall server. The HTTP proxy now permits HTTP 1.1 traffic to pass through it. [CSCdj49493]

Centri Firewall 4.0.2(150) Modifications

Centri Firewall 4.0.2(150) fixes the following issues:

- The Controlled Host Component incorrectly determines that the system license has expired and shuts down the firewall server. [CSCdj79222]
- If passwords are encoded before the data is transmitted, HTTP requests can fail, which results in a blue screen. [CSCdj78247]
- Group-based security polices do not work if the Centri administrator is not logged in as a Windows NT Domain administrator. [CSCdj82464]
- Allocation error in the Security Knowledge Base. [CSCdj82470]
- FMCompact fails due to access errors. [CSCdj82471]
- Possible race conditions exist in the Security Knowledge Base. [CSCdj82479]
- Browser cookies can cause HTTP requests to fail. [CSCdj82515]
- In Centri Firewall 4.0.1(122) and later, a session between a client and a server on the same site that passes through the firewall server using an exposed service rule does not work. [CSCdj82762]

Centri Firewall 4.0.2 Beta 2(142) Modifications

Centri Firewall 4.0.2(142) fixes the following issues:

- Centri Firewall has now been tested with the English version, as well as the Japanese version, of Windows NT Service Pack 3.
- Failure to support multi-ring Token Ring networks. [CSCdj50320]
- Failure to support network adapters from vendors other than 3Com, including SMC. [CSCdj60328]
- SYN attack causes lock up or blue screen. [CSCdj62195, CSCdj62181]
- Blue screen caused by failure to clean up initialized proxies. [CSCdj60050]
- Active content filtering is not always effective. [CSCdj52564]
- When logging in to FTP the first attempt fails, the second attempt causes Centri Firewall to blue screen. [CSCgi01979]
- Customer must reboot the firewall server twice when adding a network adapter. [CSCdj60334]
- Firewall server fails to notice IP address changes made in the Networks applet of Control Panel. [CSCdj01783]
- If the machine name changes, the firewall services do not start. [CSCdj60746]
- All changes made to the Registry for the local stack result in a new security policy being downloaded into the kernel. [CSCdj60848]
- Firewall does not notice, in real time, changes to the local stack IP address made from the Networks applet in Control Panel. [CSCdj71347]
- FMRestore and FMCompact fail to operate correctly. [CSCdj65372]
- Configuration tree lost if Security Knowledge Base crashes during a save operation. [CSCdj52600]

Centri Firewall 4.0.2 Beta 1(135) Modifications

Centri Firewall 4.0.2(135) fixes the following issue:

- Failure to support single-ring Token Ring networks. [CSCdj50320]

Centri Firewall 4.0.1(122) Modifications

Centri Firewall 4.0.1(122), available as centri40p4.exe, fixes the following issues:

- Macintosh FTP client software, FETCH, causes blue screen when session initiation is interrupted. [CSCdj70964]
- Proxy mode requests fail in build 120. [CSCdj73077]

Centri Firewall 4.0.1(120) Modifications

Centri Firewall 4.0.1(120), available as centri40p3.exe, fixes the following issues:

- Race condition in Domain-based security policies. [CSCdj64987]
- Proxy mode HTTP (and other kernel proxies) does not work with Domain-based security policies. [CSCdj66648]
- Blue screen caused when security policy is attached to a Domain-based network object. [CSCdj68926]
- Misleading logic in condition tree evaluation. [CSCdj69999]
- The Security Knowledge Base does not exit properly if a checkpoint fails. [CSCdj70228]
- The Security Knowledge Base corrupts if the firewall server crashes during a recovery. [CSCdj70229]
- A race condition causes the Security Knowledge Base to fail to save a new string table, to fail to reboot, and to consume all available processor time. [CSCdj70230]
- The Security Knowledge Base fails during install. [CSCdj70231]

Centri Firewall 4.0.1(116) Modifications

Centri Firewall 4.0.1(116), available as centri40p2.exe, fixes the following issues:

- IP plug proxies do not work. [CSCdj48647]
- Improved general performance of the Security Knowledge Base. [CSCdj52553, CSCdj52555]
- When address hiding is enabled, colliding ICMP requests cause blue screen. [CSCdj58409]
- Scheduled reports distributed via e-mail do not work. [CSCdj60495]
- The Reclamation Agent does not delete historical data properly. The Security Knowledge Base may corrupt during a checkpoint. [CSCdj62117]
- Improved checkpoint performance of the Security Knowledge Base. [CSCdj62120, CSCgi01967]
- When ARPing to a local address that also acts as a gateway and the gateway is disconnected, Centri Firewall freezes. [CSCdj62462]
- The Windows NT Service Manager displays an error message when it times out while waiting for the Security Knowledge Base to start during a recovery. [CSCgi01903]

- The Security Knowledge Base corrupts if the firewall server crashes during a recovery. [CSCgi01974]
- During uninstall, Centri Firewall files remain in the temporary directory. [CSCgi01993]

Centri Firewall 4.0.1(110) Modifications

Centri Firewall 4.0.1(110), available as centri40p1.exe, fixes the following issues:

- Failure to document the fact that Centri Firewall did *not* support Token Ring networks.
- Inaccurate release notes presented at the end of the Centri Setup program.
- Cannot install product in Windows NT domains that have more than 20 administrative accounts.
- Windows NT domain users are deleted from the end of the Users list in the Network tree.
- System instability caused by a bug in the TCP kernel proxy, noticed during heavy FTP and HTTP traffic loads.
- Cannot upgrade evaluation license key to a full license key.
- If you shut down the system cleanly, restart, and delete information, the changes do not take effect until the next reboot.
- User authentication does not work with Windows NT domains.
- If you have a trusted Windows NT domain defined in the Centri Firewall user interface, the Authenticator.exe consumes all memory and CPU time.
- The Reclamation Agent does not delete historical data properly.
- If you use the Site Wizard to set up an additional site beyond the Trusted Site and then try to move one of the existing Trusted Physical Networks into that new site, the existing hosts and new hosts that belong to that Trusted Physical Network fail validation processes/consistency checks (the hosts do not belong to a valid, trusted physical network).
- If you have two or more conditions connected with an OR operator, and you delete one of the conditions from that statement, attempting to select the **Change To** command for any remaining node causes an assert in the Policy Builder control.
- Active content filtering problems:

  In some cases, active content is not correctly filtered because the firewall determines that the content is binary and not appropriate to be filtered. This release includes a change whereby this detection of binary files is disabled and all files are filtered by the firewall. In other words, filtering will always be active; however, two side effects exist:

1. Performance degrades slightly, since binary files that previously would not have been filtered are now filtered.
2. In rare circumstances, binary files may be corrupted by the filter. It is possible for a binary file to contain strings that match that of active content. In such a case, that section of the binary file will be removed as if it were active content and the file corrupted. The workaround for this problem is to disable filtering, retrieve the file, and then restore filtering.

Cisco Connection Online

Cisco Connection Online (CCO) is Cisco Systems' primary, real-time support channel. Maintenance customers and partners can self-register on CCO to obtain additional information and services.

Available 24 hours a day, 7 days a week, CCO provides a wealth of standard and value-added services to Cisco's customers and business partners. CCO services include product information, product documentation, software updates, release notes, technical tips, the Bug Navigator, configuration notes, brochures, descriptions of service offerings, and download access to public and authorized files.

CCO serves a wide variety of users through two interfaces that are updated and enhanced simultaneously: a character-based version and a multimedia version that resides on the World Wide Web (WWW). The character-based CCO supports Zmodem, Kermit, Xmodem, FTP, and Internet e-mail, and it is excellent for quick access to information over lower bandwidths. The WWW version of CCO provides richly formatted documents with photographs, figures, graphics, and video, as well as hyperlinks to related information.

You can access CCO in the following ways:

- WWW: http://www.cisco.com
- WWW: http://www-europe.cisco.com
- WWW: http://www-china.cisco.com
- Telnet: cco.cisco.com
- Modem: From North America, 408 526-8070; from Europe, 33 1 64 46 40 82. Use the following terminal settings: VT100 emulation; databits: 8; parity: none; stop bits: 1; and connection rates up to 28.8 kbps.

For a copy of CCO's Frequently Asked Questions (FAQ), contact cco-help@cisco.com. For additional information, contact cco-team@cisco.com.

Note If you are a network administrator and need personal technical assistance with a Cisco product that is under warranty or covered by a maintenance contract, contact Cisco's Technical Assistance Center (TAC) at 800 553-2447, 408 526-7209, or tac@cisco.com. To obtain general information about Cisco Systems, Cisco products, or upgrades, contact 800 553-6387, 408 526-7208, or cs-rep@cisco.com.

Documentation CD-ROM

Cisco documentation and additional literature are available in a CD-ROM package, which ships with your product. The Documentation CD-ROM, a member of the Cisco Connection Family, is updated monthly. Therefore, it might be more current than printed documentation. To order additional copies of the Documentation CD-ROM, contact your local sales representative or call customer service. The CD-ROM package is available as a single package or as an annual subscription. You can also access Cisco documentation on the World Wide Web at http://www.cisco.com, http://www-china.cisco.com, or http://www-europe.cisco.com.

If you are reading Cisco product documentation on the World Wide Web, you can submit comments electronically. Click **Feedback** in the toolbar and select **Documentation**. After you complete the form, click **Submit** to send it to Cisco. We appreciate your comments.

This document is to be used in conjunction with the *Cisco Centri Firewall Installation Guide* and the *Securing Your Network with the Cisco Centri Firewall* publications.