

# Novell Client Firewall



2.0

USER GUIDE

[www.novell.com](http://www.novell.com)

October 20, 2003



Novell®

## Legal Notices

Novell, Inc. makes no representations or warranties with respect to the contents or use of this documentation, and specifically disclaims any express or implied warranties of merchantability or fitness for any particular purpose. Further, Novell, Inc. reserves the right to revise this publication and to make changes to its content, at any time, without obligation to notify any person or entity of such revisions or changes.

Further, Novell, Inc. makes no representations or warranties with respect to any software, and specifically disclaims any express or implied warranties of merchantability or fitness for any particular purpose. Further, Novell, Inc. reserves the right to make changes to any and all parts of Novell software, at any time, without any obligation to notify any person or entity of such changes.

You may not export or re-export this product in violation of any applicable laws or regulations including, without limitation, U.S. export regulations or the laws of the country in which you reside.

Copyright © 2003 Novell, Inc. Portions Copyright (C) 1999-2003 Agnitum Ltd. All rights reserved. No part of this publication may be reproduced, photocopied, stored on a retrieval system, or transmitted without the express written consent of the publisher.

U.S. Patent No. 5,349,642; 5,572,528; 5,608,903; 5,671,414; 5,677,851; 5,719,786; 5,758,069; 5,758,344; 5,781,724; 5,784,560; 5,818,936; 5,828,882; 5,832,275; 5,832,483; 5,832,487; 5,870,561; 5,870,739; 5,873,079; 5,878,415; 5,884,304; 5,913,025; 5,933,503; 5,933,826; 5,946,467; 5,956,718; 5,983,234; 5,991,810; 6,016,499; 6,029,247; 6,061,740; 6,065,017; 6,081,900; 6,092,200; 6,105,062; 6,105,132; 6,108,649; 6,112,228; 6,115,039; 6,119,122; 6,167,393; 6,219,676; 6,275,819; 6,286,010; 6,308,181; 6,330,605; 6,345,266; 6,345,266; 6,424,976; 6,459,809; 6,519,610; 6,539,381; 6,542,967; 6,578,035; 6,615,350; 6,629,132. Patents Pending.

Novell, Inc.  
1800 South Novell Place  
Provo, UT 84606  
U.S.A.

[www.novell.com](http://www.novell.com)

Novell Client Firewall 2.0 User Guide

[October 20, 2003](#)

**Online Documentation:** To access the online documentation for this and other Novell products, and to get updates, see [www.novell.com/documentation](http://www.novell.com/documentation).

**Novell Trademarks**

Novell is a registered trademark of Novell, Inc. in the United States and other countries.

**Third-Party Trademarks**

All third-party trademarks are the property of their respective owners.



# Contents

- About the Guide** **7**
  
- 1 Understanding the Internet and NCF** **9**
  - Introduction . . . . . 9
  - How the Internet Works. . . . . 9
  - Internet Dangers . . . . . 10
  - NCF Capabilities . . . . . 10
  - Minimum System Requirements . . . . . 12
  
- 2 Installing Novell Client Firewall** **13**
  - Installing NCF. . . . . 13
  - Starting NCF . . . . . 15
  - Stopping NCF. . . . . 15
  - Automatic Update. . . . . 15
  - Uninstalling NCF . . . . . 16
  
- 3 User Interface Orientation** **17**
  - System Tray Icon . . . . . 17
  - NCF Main Window . . . . . 18
  - Panels . . . . . 19
  - Toolbar . . . . . 22
  
- 4 Setting Up Novell Client Firewall** **25**
  - Basic Information . . . . . 25
  - Initial Settings. . . . . 26
  - Selecting a Policy. . . . . 27
  - Application Level Filtering . . . . . 29
  
- 5 Plug-Ins** **33**
  - Introduction . . . . . 33
  - Active Content Filtering. . . . . 34
  - Ad Blocking . . . . . 35
  - Attachments Filtering . . . . . 37
  - Attack Detection . . . . . 39
  - Content Blocking . . . . . 40
  - Domain Name System Cache (DNS). . . . . 42
  
- 6 Advanced Settings** **45**
  - Saving and Loading Configurations . . . . . 45
  - Setting a Password . . . . . 46
  - Creating Rules for Applications. . . . . 47
  - System Level Filtering . . . . . 48
  - Settings for a Home or Office Network . . . . . 49
  
- 7 The View Menu** **53**
  - Layout . . . . . 53
  - Filter by Time . . . . . 54

Columns . . . . .	54
Group By . . . . .	56
<b>8 The NCF Log System</b>	<b>59</b>
Introduction . . . . .	59
NCF Log Viewer Main Window . . . . .	60
Displaying Logs . . . . .	62
Working with Logs and Filters . . . . .	64
<b>A Message and Menu Descriptions</b>	<b>69</b>
ICMP Messages . . . . .	69
NCF Main Menu Options . . . . .	70
<b>B Novell Client Firewall FAQs</b>	<b>73</b>
General Issues . . . . .	73
When I run NCF, some applications fail to work. Why? . . . . .	73
My attack detection event log gives information about a portscan event. What should I do? . . . . .	73
Certain areas on the web pages I browse display the terms AD_IMG, AD_SIZE, and AD. What do they mean? . . . . .	73
After installing NCF, I tried to ping the machine from outside, but it is not accessible. Why? . . . . .	74
I tried to block certain sites using the content filtering option, but NCF fails to block the content. Why? . . . . .	74
I get a very delayed response while accessing some http:// sites, why is this? . . . . .	74
What should I do when the message 'Handle is Invalid' pops up? . . . . .	74
Sometimes, at the Startup, my system fails to communicate with the network. Is this NCF related? . . . . .	74
For no apparent reason, my system runs out of hard disk space. Is this NCF related? . . . . .	75
Issues Related to Windows NT . . . . .	75
While installing NCF, I receive messages titled 'Overwrite Protection' or 'Error Executing the Specified Program'. What should I do? . . . . .	75
What should I do if Auto-configuration of network settings fail? . . . . .	75
Windows FTP client is not working even though an application rule is present. How will I resolve this? . . . . .	75

# About the Guide

This guide provides the information that you need to configure and use the Novell® firewall software.

The guide is divided into the following sections:

- ◆ Chapter 1, “Understanding the Internet and NCF,” on page 9
- ◆ Chapter 2, “Installing Novell Client Firewall,” on page 13
- ◆ Chapter 3, “User Interface Orientation,” on page 17
- ◆ Chapter 4, “Setting Up Novell Client Firewall,” on page 25
- ◆ Chapter 5, “Plug-Ins,” on page 33
- ◆ Chapter 6, “Advanced Settings,” on page 45
- ◆ Chapter 7, “The View Menu,” on page 53
- ◆ Chapter 8, “The NCF Log System,” on page 59
- ◆ Appendix A, “Message and Menu Descriptions,” on page 69
- ◆ Appendix B, “Novell Client Firewall FAQs,” on page 73

## Documentation Updates

For the most recent version of the Novell Client Firewall 2.0 User Guide, see the [Novell online documentation \(http://www.novell.com/documentation/lg/nbm38/index.html\)](http://www.novell.com/documentation/lg/nbm38/index.html).

## Documentation Conventions

In Novell documentation, a greater-than symbol (>) is used to separate actions within a step and items in a cross-reference path.

In this documentation, a trademark symbol ®, ™, etc.) denotes a Novell trademark. An asterisk (\*) denotes a third-party trademark.

When a single pathname can be written with a backslash for some platforms or a forward slash for other platforms, the pathname is presented with a backslash. Users of platforms that require a forward slash, such as UNIX\*, should use forward slashes as required by your software.





# 1

## Understanding the Internet and NCF

This chapter provides a brief overview of the following networking concepts that you need to understand for using Novell® Client Firewall (NCF):

- ♦ “Introduction” on page 9
- ♦ “How the Internet Works” on page 9
- ♦ “Internet Dangers” on page 10
- ♦ “NCF Capabilities” on page 10
- ♦ “Minimum System Requirements” on page 12

### Introduction

A *Firewall* is the technical name for a barrier between your computer and the rest of the Internet. It is like the locks on the doors of your home. Most of your neighbors can probably be trusted not to walk into your home and vandalize it or steal from you. Usually only a small number of your neighbors are untrustworthy. But, if you live in heavily populated area, there are a greater number of dishonest people around.

The Internet is similar except that your immediate neighborhood consists of hundreds of millions of people. Even the small percentage of those people who have a destructive bent is a large number of people.

Novell Client Firewall (NCF) not only locks your computer's doors, it makes your computer invisible on the Internet. Your computer normally lets other Internet users know its address. It is like the address sign of your home or the license plate of your car. Your computer's address is plainly visible. NCF prevents your computer from broadcasting its address unless specifically authorized. Hackers are not just kept out; they cannot even find out that your computer is connected to the Internet.

### How the Internet Works

The Internet is a network of networks. There are two fundamental types of computers on the Internet, servers and clients. A server is a computer specifically set up to serve its files (make its files available for viewing or download) to client computers. A client is any computer you use to access the Internet: desktop, laptop, handheld, cell phone, etc. The files a server makes available to your computer can be Web pages, videos, sounds, images, etc. For your home computer to be able to receive files or any data from a server, your computer must request this information. This happens when you enter an URL in your browser or when you receive an e-mail.

Any computer can be set up as a server or a client. Without proper safeguards, anyone can access the files on your personal computer when it is connected to the Internet. This is why a firewall

should be used. A firewall is simply a way to protect your computer from having its files accessed without your permission. There are many kinds of firewalls and they have different capabilities.

## Internet Dangers

We have all heard of the dangers of the Internet and Cyberspace. Although some of these have been greatly exaggerated, it does not alter the fact that a computer connected to the Internet is susceptible to very real attacks. Unfortunately, there are people who feel compelled to use their knowledge about computers and how to access files remotely in illegal and unethical ways. Subsequently, they make life difficult for others. They are called *hackers* or *crackers*. To keep them out of our systems, we need to use a strong firewall.

Here are the main dangers associated with the Internet:

- ◆ Unauthorized applications can be delivered to your computer and executed without your knowledge or control (for example, ActiveX or Java\* applets embedded in a Web page you browse). These programs can perform any operation on your computer, including transferring files containing your private information to other computers or simply erasing all the files on your system.
- ◆ If your system is not properly configured, other computers can access your files directly without someone having to surreptitiously load special software on your computer.
- ◆ Some information (in the form of cookies or referrers) can be placed on your computer, which enables advertisers and others to track the sites you visit and what your interests are.
- ◆ *Trojan horses* can be placed on your computer. Trojans are programs used by hackers (crackers) that open the door to your private information, such as passwords, banking data, and credit card numbers. One of the fundamental differences between a Trojan and a virus is that a virus on your computer executes autonomously, whereas a Trojan horse is constructed to be used directly by a remote intruder.
- ◆ *Internet worms* can get to your computer as attachments to e-mail messages. Some e-mail programs open attachments without asking for permission. Some users, unaware of threats, open all attachments manually. When opened, the worm executes and rapidly infects your system.
- ◆ Unnecessary data in the form of banners and other advertisements use up your bandwidth. Although these objects cannot directly access or damage the data on your computer, they can significantly slow your connection, especially on a dial-up.
- ◆ Spyware is in many ways similar to Trojans. These programs gather information about you and your interests (such as your surfing habits, what other software you have on your computer, etc.) without your knowledge or consent. Spyware is mostly used by online or software corporations for marketing purposes.

## NCF Capabilities

NCF provides an easy-to-use interface. To effectively use NCF, you do not need to know the inner workings of Windows\*. The default settings are configured for you. However, you can change any of these many settings at any time. These are covered later in this manual.

A tremendous strength of NCF is its modular organization. NCF's capabilities are implemented as special modules called plug-ins, files with the .ofp extension. Each module is independent and can easily be added to an installed system.

Following are the major benefits of NCF:

- ◆ Protects you against the full spectrum of security threats from privacy issues to data leaks and exploits.
- ◆ Can be used immediately after installation without any customization.
- ◆ Can be auto-configured for best protection, or will let you easily create your custom secure configuration very quickly using system prompts and default settings without interrupting your work.
- ◆ Performs very complicated adjustments to the security of your system with just a few keystrokes.
- ◆ Can be used to restrict network access both to your computer and from your applications. Advanced users can also adjust service protocols and create special security facilities as required.
- ◆ Has a stealth mode that makes your computer invisible to hackers while letting you browse the Internet as usual.
- ◆ Has a modular system structure that lets you add new protective modules in the form of plug-ins.
- ◆ Is compatible with all versions of Windows 98/2000/ME/NT/XP.
- ◆ Has minimal system requirements.
- ◆ Can restrict a list of applications having access to the network and specify acceptable protocols, ports, and directions of access (incoming or outgoing) for each of these applications.
- ◆ Can block or restrict nonrequested information being sent to your computer, such as the following in particular:
  - ◆ Banner advertisements
  - ◆ Pop-up windows on Web pages
  - ◆ Inappropriate content data from specific Web pages
- ◆ Can restrict or prohibit the action of program components built into Web pages, such as Java applets, ActiveX scripts, and JavaScript\*.
- ◆ Can restrict or prohibit the use of cookies.
- ◆ Specify a zone of friendly IP addresses (your own LAN, for example). In this zone, NCF does not control or restrict network exchange.
- ◆ Can quarantine e-mail attachments to protect your system from Internet worms.
- ◆ Can warn of any indication of someone attempting an attack on your computer from any other computer and instantly prevent access.
- ◆ Has an advanced database-driven log system that supports custom queries for data mining tasks.
- ◆ Is successful with all known leak-tests.

# Minimum System Requirements

The minimum system requirements needed for NCF to operate are given below:

Processor	166 MHz Intel* Pentium* or compatible CPU
RAM	128 MB
Operating System	Windows NT Service Pack 6, Windows 2000 Professional, Windows XP, Windows XP Home Edition, or Windows Me
Hard disk space	512 MB

**NOTE:** There is no special network card or modem, and there are no special configuration settings of these boards needed for the normal operation of the software.

# 2

## Installing Novell Client Firewall

This chapter provides you with the following information on how to install Novell® Client Firewall (NCF):

- ♦ “Installing NCF” on page 13
- ♦ “Uninstalling NCF” on page 16
- ♦ “Starting NCF” on page 15
- ♦ “Stopping NCF” on page 15
- ♦ “Automatic Update” on page 15

### Installing NCF

**HINT:** We recommend that you use the default settings when the installation utility asks to confirm its choices, if you are not an advanced user.

- 1** Uninstall any other firewall software on your computer and reboot.

This is in order to prevent a system conflict of different firewalls fighting to control network access.

- 2** Close all open applications.

- 3** On the Windows task bar, Click Start > Run.

- 4** Type the full path to the setup program file (NCFInstall.exe) in the Open field.

For example, if the setup program is on D: in the ncf folder under downloads you would type  
D:\downloads\ncf\NCFInstall.exe

- 5** Click OK.

The setup procedure is arranged in several steps. The installation begins with choosing the language for the NCF interface in the Choose Setup Language window.

- 6** Select a language from the drop-down list, then click OK.

The Welcome section of the wizard is displayed. This screen reminds you to exit all Windows programs and guides you through the entire process.

The installation screens have the following buttons:

- ♦ Next—Takes you to the next step of the procedure.
- ♦ Back—Returns you to the previous step.
- ♦ Cancel—Aborts the entire setup procedure.

- 7** Click Next.

The License Agreement section is displayed. Read the agreement carefully before proceeding.

**8** Click Yes to proceed if the license agreement is acceptable to you.

The Destination Directory section is displayed.

**9** Click Yes. Or, if you prefer a different destination, click Browse and change the path.

The Select Program Folder section is displayed.

**10** (Optional). Type a new folder name or select one from the Existing Folders List.

This is the last step before the actual installation of the software. If you decide to change any of the choices you made, click Back.

**11** Click Next.

The Setup Status section of the screen appears displaying the installation progress. After the installation is completed, the Auto-configuration section of the wizard is displayed.

**12** Click Next. Or, if you do not want to auto-configure, click Skip.

NCF scans your hard disk for selected applications that might use the Internet. NCF offers specific rules for each application it detects. The rules are created for optimum performance and security of these applications. When the search is completed, the Application Rules section is displayed asking you to apply the auto-configured rules for the applications.

**IMPORTANT:** We strongly recommend that you let NCF auto-configure the rules and network settings for your system.

**13** Do one of the following:

- ◆ To remove auto-configured rules for any application, click Details, uncheck the box next to the application component name, then click OK.

We strongly recommend that you apply the auto-configured rules until you are an advanced user and would like to create some rules manually.

- ◆ To apply the auto-configured rules, check the Apply the Auto-configured Rules.

**14** Click Next.

NCF auto-detects your network settings and displays the Network settings window.

**15** (Optional) Click Details to view the details of network settings.

You can change these settings at any time while using NCF. We strongly recommend that you accept the auto-configured rules for your Network.

**16** Check Apply the Auto-configured Rules, then click Next.

**17** Click Next to read the Readme file, then exit and proceed with the installation.

**NOTE:** Uncheck the View Read Me File option to skip the Readme.

**18** Click Next.

The Reboot section of the wizard is displayed. This section prompts you to restart your computer.


**19** Click Finish to complete the installation procedures.

**IMPORTANT:** Do not launch NCF manually using the Start button or Windows Explorer right after installing it. To protect your system, you must reboot your computer before starting NCF.

## Starting NCF

After installed, NCF starts automatically when Windows loads. In this way, NCF starts protecting your computer immediately before other programs can compromise your system.

If you have chosen auto-configured rules during installation, services or applications detected by NCF during installation will be allowed. For any new traffic, NCF pops up a dialog box (as no rule is defined) asking you to select an appropriate action for that traffic. See “[Selecting a Policy](#)” on [page 27](#) for details.

When NCF starts, its icon  is displayed in the system tray, on the right-side of the Windows task bar.

If, for some reason, NCF does not start when Windows loads, you can start it by following these steps:

- 1 In the Windows task bar, click Start > Programs.
- 2 Click Novell Client Firewall > Novell Client Firewall.

When NCF is running, its icon is displayed in the system tray. If you do not see the NCF icon in the system tray, then you know that NCF is not protecting your computer unless you specifically set it up to run in background mode.

## Stopping NCF

Closing the main window of NCF does not shut down the firewall. Its icon remains in the system tray.

There are two ways to shut down NCF:

- ♦ Right-click its icon in the system tray, then click Exit and Shutdown Novell Client Firewall.
- ♦ In the main NCF window, click File > Exit and Shutdown.

Both ways close the interface and stop the firewall, which means NCF is no longer protecting your system.

When NCF is shut down, its icon disappears from the system tray indicating that the firewall is no longer protecting your computer.

## Automatic Update

With Automatic Update, you never have to be concerned about the latest Internet threats. NCF provides you with a convenient way of keeping itself updated via the Internet. Each day, Automatic Update checks for newer components and plug-ins and, if it finds any, it retrieves them for you.

If, for some reason, you would like to check for newer components manually, you could run the Update procedure by clicking the Update button  on the NCF toolbar.

The Update wizard lets you choose how to update NCF by selecting one of the following:

- ♦ **Automatic**—The system finds all the components that have an update available and updates them together. We recommend this option.
- ♦ **Custom**—You specify each component to be updated. Only advanced users should use this option, for debug purposes.

With either Automatic or Custom, components are updated only if updates are available for them.

Clicking the Settings button in the wizard displays the Settings dialog box with the following options:

- ◆ **Auto Detect**—Uses the proxy settings already specified in Microsoft\* Internet Explorer.
- ◆ **User Proxy Server**—Lets you specify the parameters of the proxy server that is to be used by NCF's Automatic Update. The Server and Port fields become visible when you choose this option. Specify the name of your proxy server and its port number (port 8080 is the default). If your proxy server requires authorization, check the appropriate check box and type your username and password. If you are unsure what type of proxy you use or you do not know your username and password, consult your system administrator.
- ◆ **Do Not Use Proxy Server**—Select this if your system is not connected to the Internet through a proxy server.

If you select Custom update, the wizard asks you to select the components for update.

Any line in the components list that starts with a plus sign (+) is a grouping of components. You can see the listing of these components by clicking on the plus sign.

A red check is a component that must be updated for NCF to avoid compatibility problems between modules and other selected components.

Select (check) the components you want to update. Deselect (uncheck) the components you do not want to update. We recommend that you update all components unless you are an advanced user and have some reason not to.

**NOTE:** When this dialog box first appears, all the components are checked by default.


After all the components to be updated are selected, click Next. After the download is complete, you will be prompted to restart the system. Restart your computer as soon as possible to take advantage of the increased protection afforded by the updated components you just downloaded.

Once the download is complete, you will be prompted to restart the system. Restart your computer as soon as possible to take advantage of the increased protection afforded by the updated components you just downloaded.

**NOTE:** The NCF version is changed only after a reboot of your computer. If you simply restart NCF, it will be the same version. To see what version is active, click Help > About Novell Client Firewall.

## Uninstalling NCF

Before installing a newer version of NCF, you *must* uninstall any earlier version and reboot.

- 1** Right-click the NCF system tray icon , then click Exit and Shutdown Novell Client Firewall.
- 2** On the Windows task bar, click Start > Programs.
- 3** Click Novell Client Firewall > Uninstall Novell Client Firewall.

The system starts uninstalling NCF immediately and a dialog box displays the progress of uninstall process.

- 4** After the uninstalling is complete, restart the system as prompted.

To avoid software conflicts, restart your system immediately after the uninstall process.



# 3

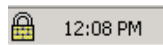
## User Interface Orientation

This chapter discusses the basic features of the Novell® Client Firewall (NCF) user interface:

- ♦ [“System Tray Icon” on page 17](#)
- ♦ [“NCF Main Window” on page 18](#)
- ♦ [“Panels” on page 19](#)
- ♦ [“Toolbar” on page 22](#)

### System Tray Icon






The NCF icon in the Windows task bar system tray looks like this:



This icon is one of the primary ways you can access NCF's many controls, settings, and logs. This icon changes along with each of NCF's major modes. Therefore, you can see which mode is being used to protect your system at any time by checking the icon.

The following table lists the icons and the modes they represent.

Table 1 Icon Modes

Icon	Mode	Description
	Stop All	All network connections are blocked.
	Block Most	All network connections are blocked except those you explicitly allowed.
	Rules Wizard	Determines how an application will interact with the network the first time each application is run.
	Allow Most	All network connections are allowed except those you explicitly blocked.
	Disable	All network connections are allowed.

These modes are covered in detail in [“Selecting a Policy” on page 27](#).

Right-click the NCF system tray icon to display its context-sensitive menu, which contains the following options:

- ◆ **Show Novell Client Firewall**—Displays the NCF main window.
- ◆ **Policy**—Opens a submenu where you can change the NCF policy to Disable mode, Allow Most mode, Rules Wizard mode, Block Most mode, or Stop All mode.
- ◆ **Options**—Displays the Options dialog box.
- ◆ **Always on Top**—When selected, keeps the current window on top of all other windows.
- ◆ **About**—Shows the current version of NCF and lists all modules in the package and their individual versions.
- ◆ **Exit**—Closes the NCF GUI but leaves the firewall running in memory, blocking connections and banners.
- ◆ **Exit and Shutdown Novell Client Firewall**—Closes the GUI and disables the firewall. This means NCF is no longer protecting your system.

## NCF Main Window

The main window is your central control panel of NCF. It is used to monitor the network operations of the computer and to modify the firewall settings.

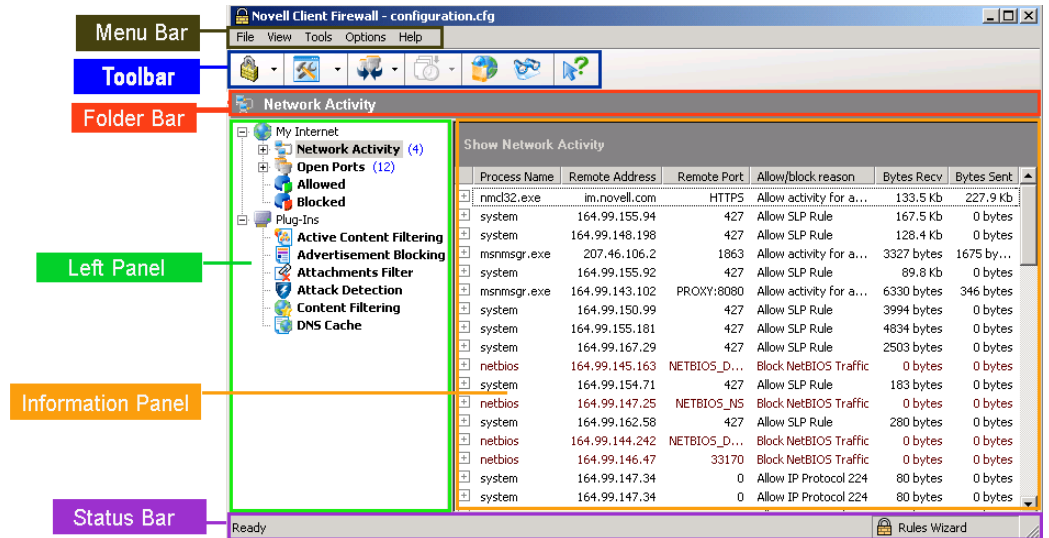
To display the NCF main window:

- 1** Right-click the NCF icon in the system tray.
- 2** From the menu, select Show Novell Client Firewall.

The main window contains the following areas, as shown in [Figure 1 on page 19](#):

- ◆ Menu bar
- ◆ Toolbar
- ◆ Folder bar
- ◆ Left panel
- ◆ Information panel
- ◆ Status bar

Figure 1 Novell Client Firewall Main Window

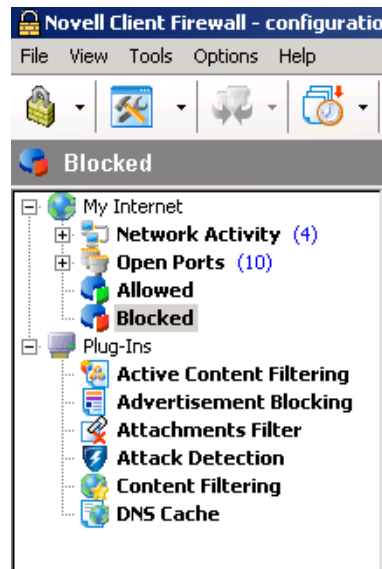


## Panels

The Left panel and Information panel are similar to the left and right panels of Windows\* Explorer. The Left panel is a listing of the components secured by NCF on your computer and the Information panel gives specific data about any component selected in the Left panel.

### Left Panel

Figure 2 Left Panel



### Under My Internet

- ◆ **Network Activity**—Lists every application and protocol that currently has an active connection to the Internet or LAN as well as other network activity.
- ◆ **Open Ports**—Lists your system's open ports.

- ◆ **Allowed**—Shows the event log stats for all the applications and connections that NCF allowed. You can view the stats filtered for the current session, current day, or all times.
- ◆ **Blocked**—Shows the event log stats for all the applications and connections that NCF blocked. You can view the stats filtered for the current session, current day, or all times.
- ◆ **Reported**—Is the event log of all the attempts by applications and connections to access the Internet or LAN that you specified NCF should report to you.

Although the details of the logs are intended for advanced users, the above items are important when you need to see the statistics on established connections or bytes sent and received. To view the logs in more detail, click the Show Detailed Log button located on the Information Panel of Allowed, Blocked, and Reported items. (For more details, refer to [Chapter 8, “The NCF Log System,” on page 59.](#)) You can also use these lists to make certain that NCF is correctly configured and is doing the job you need and want.

### Under Plug-ins

Plug-ins are independent from the primary NCF engine and you can install or uninstall any or all of them. You can even get third-party plug-ins from other developers and Web sites. (For more details, refer to [Chapter 5, “Plug-Ins,” on page 33.](#))

Each plug-in has its own icon in the Left panel and the log of its activity is displayed in the Information panel. When NCF is first installed, the Plug-Ins list contains the following modules:

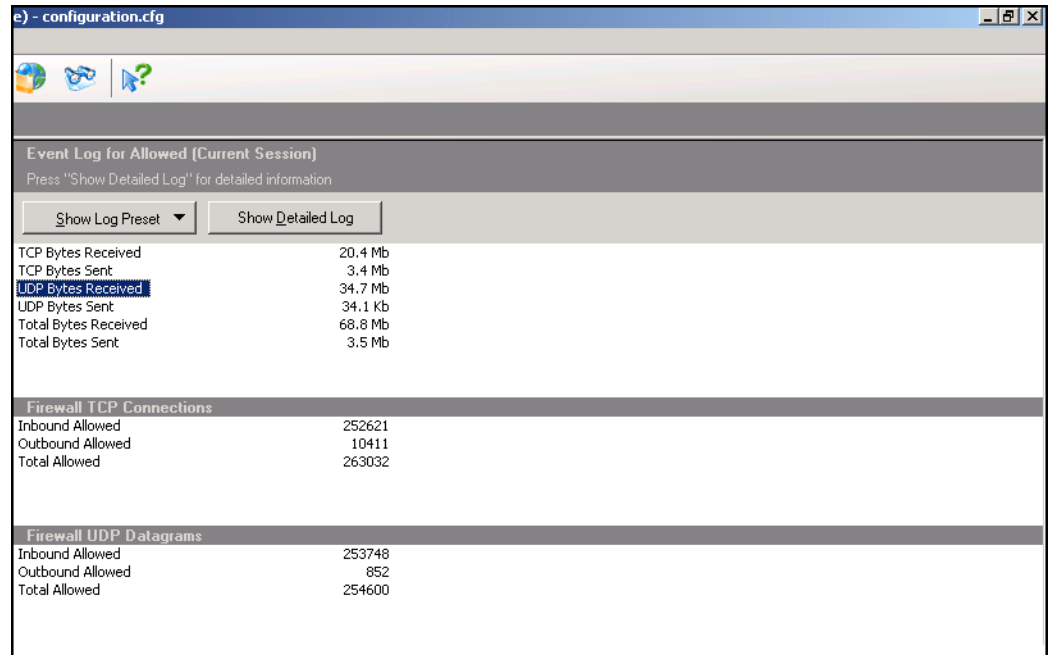
- ◆ **Active Content**—Displays the event log of the sites that had some of their active content blocked based on the settings for Java, VB Script, Active X\*, and other active content elements.
- ◆ **Ads**—Displays the event log of all the ads that were blocked.
- ◆ **Attachments Filter**—Displays the event log of all the e-mail file attachments that were neutralized and quarantined from your computer.
- ◆ **Attack Detection**—Displays the event log of any suspected attacks on your computer from the Internet, the ports involved, and where the attacks are from.
- ◆ **Content**—Displays the event log of all the Web sites or pages that were blocked and the reason for it.
- ◆ **DNS Cache**—Displays the event log of the Web addresses cached by NCF to speed up your Internet connection to those sites.

Each of the components is preceded by a plus sign (+) except the one selected, which has a minus sign (-) and is expanded to show its individual data. To hide this extra data, click the category's minus sign. A component without a plus or minus sign preceding it has no extra data to be shown or hidden.

## Information Panel

The following figure is an example of the Information panel and some of the data it displays:

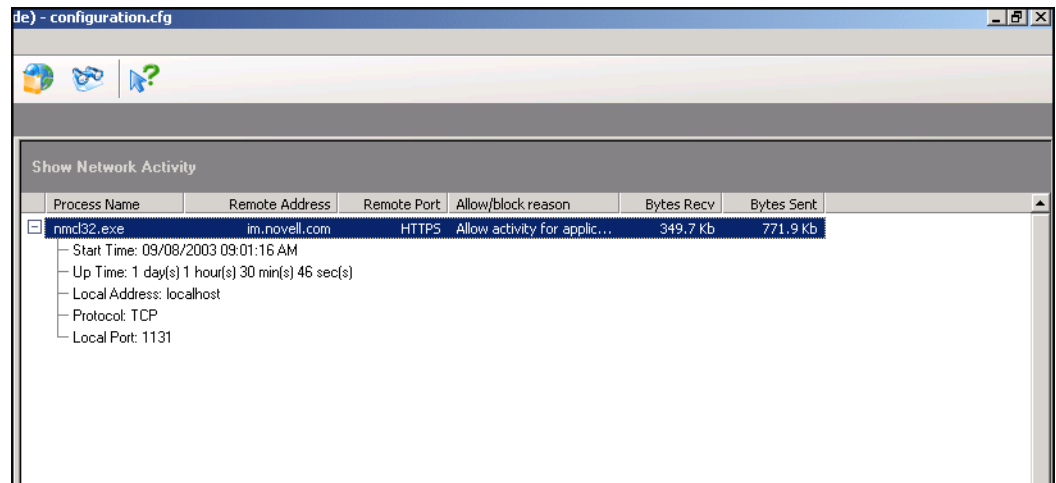
**Figure 3** Information Panel



For information about customizing the Information panel, see [“Columns” on page 54](#).

As with most elements of NCF, a right-click in the Information panel produces a context-sensitive menu. In the figure below, the menu is pertinent to the selected line. If no line is selected and the right-click is made over some of the white space below the lines, then none of the menu items is applicable and so all are grayed out.

**Figure 4** Right-click in the Information Panel



The Welcome screen of NCF is displayed in the Information panel if you select My Internet in the Left panel. You can directly access the Application and System settings, Plug-ins, Log Viewer, and

Help from this screen. For this, click the required feature from the list on the right-hand side of the screen.

## Toolbar


The toolbar is situated at the top of the main window.



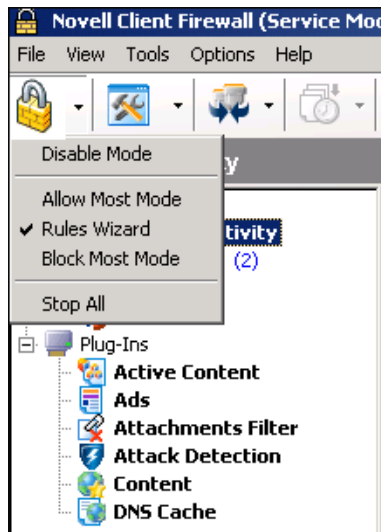
Only some of these buttons are active at any one time, depending on what is selected in the Left panel or the Information panel.

Each button has a help tip and you can see what each button does by holding your cursor over it for a second or so.

Except for the Update and Help buttons, each button on the toolbar is a shortcut to a menu item. The buttons are simply an easy and direct path to their functions rather than your having to go through several different menus or windows to access these same functions.



The icon  - at the left end of the toolbar shows the current NCF policy. Click on this icon to view a menu with options to quickly change usage modes.






**Figure 5 Policy Menu**



The following table lists and explains the different toolbar buttons.

**Table 2 NCF Toolbar Buttons**

Button	Function	Corresponding Menu Path
	Changes the NCF policy.	Options > Policy
	Accesses the Options window.	Options

Button	Function	Corresponding Menu Path
	Changes the listed item grouping.	View > Group By
	Narrows a log listing to events within a specified time.	View > Filter by Time
	Checks for an update of NCF plug-ins or components.	To have NCF automatically check for updates whenever Windows starts, use Tools > Automatically Check for Update
	Opens a viewer that displays the logs.	Tools > Log Viewer
	Displays NCF Help topics.	Help > Context and Index





# 4

## Setting Up Novell Client Firewall

This chapter discusses the following information about setting up the Novell® Client Firewall (NCF):

- ♦ “Basic Information” on page 25
- ♦ “Initial Settings” on page 26
- ♦ “Selecting a Policy” on page 27
- ♦ “Application Level Filtering” on page 29

### Basic Information

A firewall for your computer is like the lock on a door of your house. You usually lock the front door of your house when you leave to prevent other people from snooping, stealing, or causing any other kind of damage.

The Internet is similar. Most Web sites are unobtrusive and benign. Only a small percentage holds any threat to our privacy. However, because there are such a huge number of Internet users, even a small percentage of them with an impulse to vandalize adds up to a very significant number of people. For this reason, you need to provide protection for your computer.

Novell Client Firewall (NCF) is engineered to detect a suspicious connection. When NCF alerts you to a suspicious connection request from an application on your computer or from the Internet, it gives you some information about the request (such as the DNS or IP address of the remote computer), the application making the request, and other data to help you decide if you want to allow the connection or not. If in doubt, simply disallow the connection this one time. See what happens. If you are prevented from doing something you wanted to do, then try doing it again and this time allow the connection when prompted. In this way, you can learn what your applications are doing and which ones you need to be careful of or even uninstall completely from your system. NCF will also alert you to the presence of a Trojan horse.

**NOTE:** A good rule of thumb when using NCF is to keep the settings NCF suggests if you do not have a particular reason or the knowledge to change them. If you have any doubt or confusion about changing any default setting, we recommend that you save or record the setting before changing it.

In NCF, an access setting is basically a rule that you set regulating how much of your information you want to let other computers access or how much information you want to allow other computers to send to yours.

NCF uses various security settings to keep your computer protected from unwanted access from other computers on the Internet or any type of network connection. It also restricts the flow of information coming into your computer as you see fit. You might set a rule about file sharing, for example, so that your computer shares your files only with other computers you trust on your local network. A common use for a firewall is to restrict the amount of information your computer gives out while it is connected to the Internet.


**HINT:** If you are unfamiliar with how firewalls work, we recommend that you keep the firewall in Rules Wizard mode for several days of use.

# Initial Settings

This section gives a brief overview on how to customize the system. You can change these settings at any time.

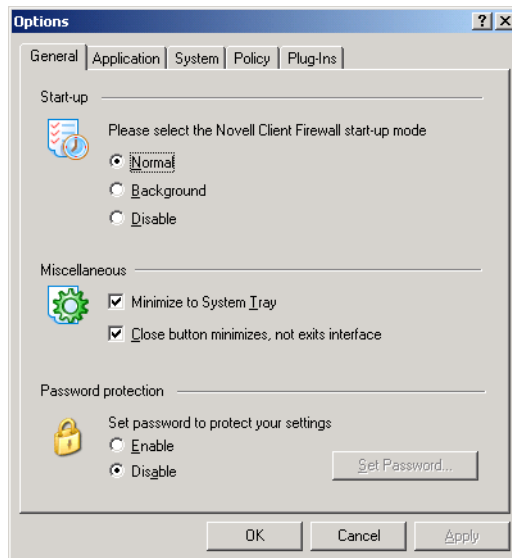
NCF is ready for operation as soon as it is installed. Its default settings are more than adequate for most purposes and we recommend using them until you become fully acquainted with how NCF operates. After you are familiarized with it, you can customize NCF in many ways to best suit your particular needs.

To display the NCF settings window:

- 1 Right-click the NCF system tray icon .
- 2 Click Options.

The settings window opens:

**Figure 6 Options Dialog Box (General Tab)**



The General tab contains Start-up, Miscellaneous, and Password Protection settings.

## Start-up

- ◆ **Normal**—This is the default startup mode, which loads NCF automatically at startup and displays its icon in the system tray.
- ◆ **Background**—This is the invisible mode, without its system tray icon or any of its dialog boxes. This option is provided for two reasons: to save system resources and for a parent or Systems Administrator to block unwanted traffic or content in a way that's completely hidden from a user.
- ◆ **Disable**—Disables auto-loading of NCF at startup.

## Miscellaneous

- ◆ **Minimize to System Tray**—When selected, a button is *not* placed on the task bar for NCF's main window whenever it is minimized. To see NCF's main window, simply double-click NCF's system tray icon, or right-click it and then click Show Novell Client Firewall.
- ◆ **Close Button Minimizes, Not Exits Interface**—When selected, this ensures that whenever you click the Close button, only NCF's dialog box will be closed, not the firewall. To shutdown NCF, right-click NCF's system tray icon and then click Exit and Shutdown NCF.

## Password

- ◆ **Enable**—Protects your firewall settings with a password. Click Set Password to create a password for your settings.
- ◆ **Disable**—Leaves your firewall settings unprotected so that anyone can change them.

If you choose to have your NCF settings protected by password, only you can change its configuration.

## Selecting a Policy

One of the most useful and important features of NCF is its usage modes. The different modes are described in [Table 1, “Icon Modes,” on page 17](#).

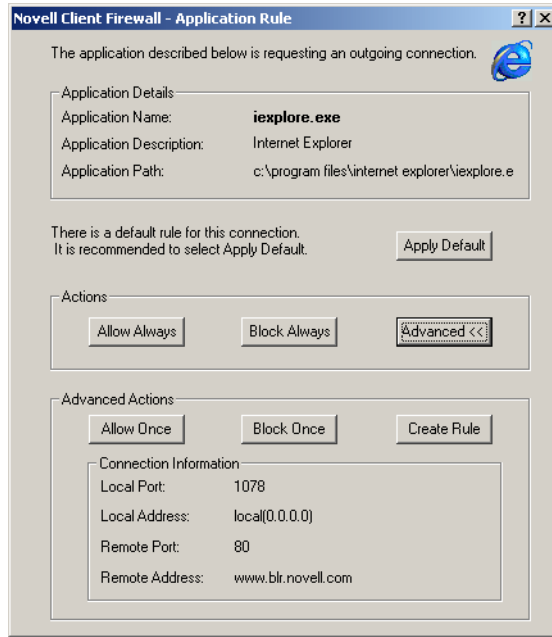
The icon shown for each mode is what is displayed in the system tray as the NCF icon. You can tell at a glance what mode NCF is in by looking at its system tray icon.

When NCF is installed, the default mode is Rules Wizard mode. This mode helps you decide whether an application should be allowed a network connection. Rules Wizard facilitates the specifying of applicable network parameters for each type of application.

Although, during the installation process, NCF creates the rules for applications already installed on your system, it might miss a few uncommon programs. In this case Rules Wizard mode makes your life a little easier. Instead of your having to create a new and often complex rule each time a new application is run, Rules Wizard does the work for you by basing its presets on all well-known applications. Rules Wizard even recommends the best selection for you.

Whenever a new application requests a network connection, the Application Rule window is displayed:

**Figure 7 Application Rule Window**



NCF has a database of the more commonly used applications, and it optimizes the settings for each type of application so the decisions you have to make are very few.

The NCF system divides applications into three categories:

- ◆ **Blocked**—Distrusted applications for which all connections are blocked.
- ◆ **Partially Allowed**—Applications granted limited network access by having their protocols, ports, and directions specified by policies (rules).
- ◆ **Trusted**—Applications for which all connection requests are allowed.

In [Figure 7](#) above, you can see what application is requesting an outgoing connection, what manner of access is being attempted, the basic parameters of the connection, and your options concerning the request.

The options you can choose from in Rules Wizard mode are as follows:

Option	Purpose	Result
Apply Default	For pre-defined rules	Connections will be allowed according to the pre-defined rules.
Allow Always	For applications you trust completely.	All network requests by this application are allowed and the application is given the status Trusted Application.
Block Always	For applications that should not be allowed network access.	All network activities for this application are disabled. The application is given the status Blocked Application.
Allow Once	For applications that you are doubtful of but want to see what they do with the connection.	This network connection is allowed this time. The next time this application tries to establish a network connection, this same dialog box appears. No rule is created for the application.

Option	Purpose	Result
Block Once	For applications that you do not trust but do not want to block totally.	This network connection is blocked this time. The next attempt by this application to establish a network connection results in this same dialog box. No rule is created for the application.
Create Rule	For applications that can obtain network access under specific protocols, via specific ports, etc.	Limits network access to specific ports and protocols using presets that are optimum for most purposes. The application is given the status Partially Allowed Application.

Use the Advanced button in the Actions section to choose advanced actions.

NCF detects most of the applications that regularly access the network after working a day or so in Rules Wizard mode. After NCF has registered most of your applications, you can switch to Block Most mode.

You can also create your own rule for an application rather than select one of the presets. To create a rule, select Create Rules Using Preset, select Other from the drop-down list, and then click OK. This opens the Rules dialog box where you can create any rule for this application.

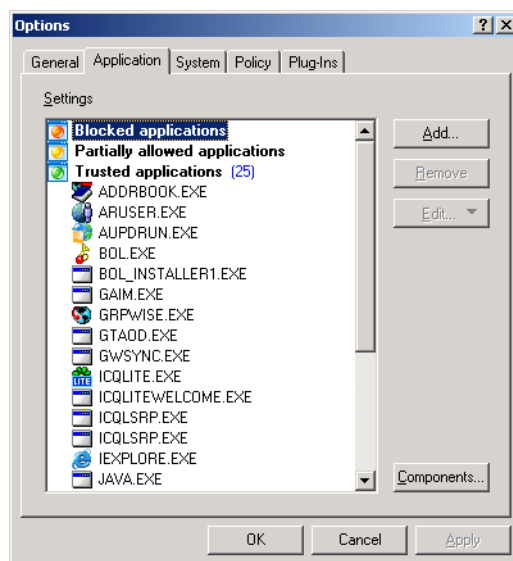
**NOTE:** The Allow Once and Block Once buttons are available only for some connections (outgoing TCP connections). When these functions are unavailable, their buttons are grayed out.

## Application Level Filtering

One of the most important NCF features is application-level filtering. This lets you decide which applications should have access and which should not.

The dialog box used to control applications can be accessed by right-clicking the system tray icon and then clicking Options > Application. You can also access it from the main window using the Options > Application menu path.

Figure 8 Options (Application Tab)



NCF divides applications into three categories:

- ◆ **Blocked**—All activities of this group are blocked. We recommend that you add to this group all applications that do not need Internet access, such as text editors, calculators, etc.
- ◆ **Partially Allowed**—NCF allows access to the Internet for these applications based on the rules that were created by you manually or from presets. Only specified application activity is allowed. We recommend that you put most of your applications in this group.
- ◆ **Trusted**—All activities for these applications are allowed. We do not recommend that you include an application in this group unless you trust it absolutely.

There is no need to add your applications to these groups manually. Rules Wizard automatically does this for you.

You can change an application's status at any time. Applications can simply be dragged-and-dropped from one category to another.

You can also directly add an application by either of the following methods:

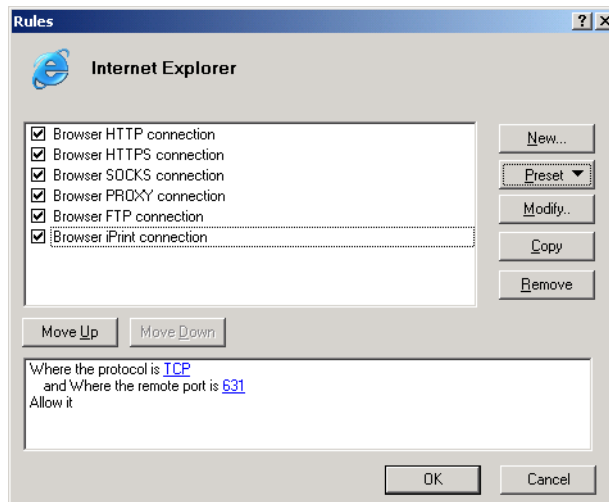
- ◆ Drag the application's icon from Windows Explorer or your desktop into the Options > Application dialog box.
- ◆ Click Add, browse to the location of the application's .exe file, then click Open.

If the same application is already listed in another category, it will be deleted from that other category.

To change any of the detailed settings for the selected application, click Edit.

Whenever an application is dragged to the Partially Allowed applications category of the Options > Application tab, or is in any other way added to this category, the Rules dialog box is displayed.

**Figure 9** Rules Dialog Box

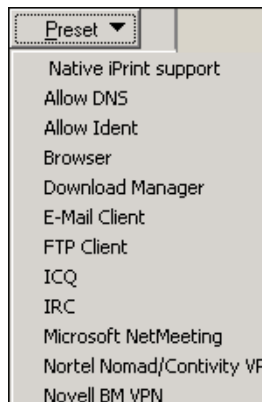


Using this dialog box, you have full control of any of the different protocol settings by selecting it and then clicking Modify. For details, see [“Creating Rules for Applications” on page 47](#).

A simpler approach is to use the Preset button to select the general type of application that best applies. The settings for these presets are optimized for most purposes. We recommend that even advanced users use these presets and then modify their settings later as needed.

It is possible to create several different rules for the same application. However, NCF uses the first instance of a rule having criteria that matches the application's activity and ignores all subsequent ones. The rules in the firewall rules list are processed in the order in which they are listed. When a rule matches, searching of the rules list stops. In other words, any other rules that match this type of communication are ignored if they are further down the list than the first rule that matches. You can use the Move Up and Move Down buttons to change the sequence of rules and determine which NCF will use. If no rule is found, NCF displays the Rules Wizard dialog box or simply blocks the connection, depending on whether you are running NCF in Rules Wizard or Block Most mode. An empty check box in the list of rules means that rule will not be applied.

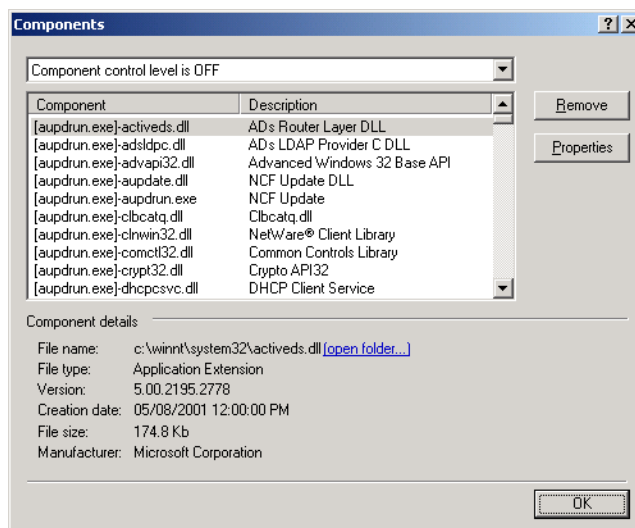
Clicking the Preset button displays a drop-down list similar to the following:



For more information about rule creation, see [“Creating Rules for Applications” on page 47](#).

NCF not only monitors applications but also monitors the components of each application. So, when a component of an application has changed and the application is about to establish a connection, NCF will ask you to allow or permit this. The purpose of the Component Control is to make sure those components are not fake and malicious. Some Trojan horses can be injected as a module of a legitimate application (for example, your browser) and thereby gain the privileges needed to go online. NCF allows you to view the components it monitors for each application by clicking the Components button in the Applications dialog box, which displays the following window:

**Figure 10 Components Window**



You can view the details of any component by selecting it. You can remove a component from the list by selecting it and then clicking Remove.

You can also select one of the Component Control levels by clicking the drop-down menu at the top of the window:

- ◆ **Normal**—Monitors all new and updated components and remembers the legitimate ones.
- ◆ **Maximum**—Monitors all components.
- ◆ **Off**—Switches off the Component Control.



# 5

## Plug-Ins

This chapter discusses the following plug-ins for Novell® Client Firewall (NCF):

- ◆ “Introduction” on page 33
- ◆ “Active Content Filtering” on page 34
- ◆ “Ad Blocking” on page 35
- ◆ “Attachments Filtering” on page 37
- ◆ “Attack Detection” on page 39
- ◆ “Content Blocking” on page 40
- ◆ “Domain Name System Cache (DNS)” on page 42

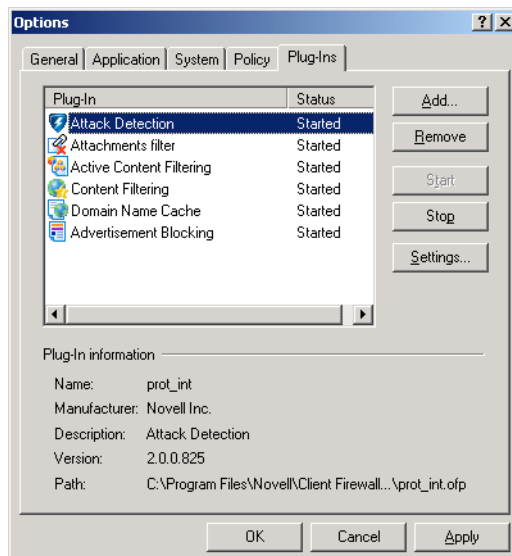
### Introduction

One of NCF's most useful and effective design strategies is the employment of plug-ins. These modules can be created by third-party developers and easily added to increase NCF's capabilities.


**NOTE:** Plug-ins are absolutely independent from each other and the main NCF module.

The Options window allows you to control these plug-ins. Right-click the system tray icon, then click Options > Plug-Ins. You can also access this window from the main window by clicking Options > Plug-Ins Setup.

**Figure 11** NCF Options Window (Plug-ins Tab)



The right-side buttons do the following:

- ◆ **Add**—Adds a new plug-in to NCF using the Windows File > Open Dialog box.
- ◆ **Remove**—Deletes the selected plug-in.
- ◆ **Start**—Starts the selected plug-in.
- ◆ **Stop**—Stops the selected plug-in from operating (but does not delete the plug-in from NCF).
- ◆ **Settings**—Modifies any of the settings for the selected plug-in. The types of settings vary with the different plug-ins. You can modify only the settings of the plug-ins that have the status Started. The Settings dialog box for any started plug-in can also be accessed by selecting that plug-in in the main window's Left panel, then clicking Properties. The Settings dialog box for each started plug-in can also be accessed using the  button on the toolbar of NCF's main window.

The lower half of the Plug-In Information section shows the most important properties of a selected plug-in and where, on your system, the plug-in's .ofp file is located.

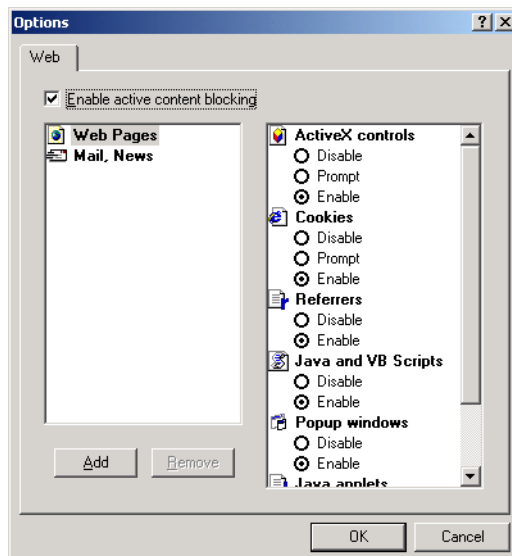
## Active Content Filtering

This plug-in controls the operation of the following active elements:

- ◆ ActiveX
- ◆ Java applets
- ◆ Programs based on JavaScript and VBScript
- ◆ Cookies
- ◆ Pop-up windows
- ◆ Referrers

This plug-in lets you independently allow or block any of these elements that might be contained in the Web pages you are browsing.

**Figure 12 Active Content Filtering Options Window (Web)**



Enable Active Content Blocking must be selected (checked) for this plug-in to function. After you have fully configured this plug-in, you can activate or deactivate it simply by checking or unchecking this check box.

You can individually set control of active elements for E-mail, News, or Web Pages. The right panel shows the settings for each selection:

- ◆ **Disable**—Blocks the element's action.
- ◆ **Prompt**—Asks you each time the element tries to activate.
- ◆ **Enable**—Allows the element to function.

When the system is installed, the use of all active elements is enabled by default for all Web pages.

Individual Web sites can be added to the listing in the left panel so that each site can be configured separately. To do this, select Web Pages and then click Add.

In the next dialog box, type the URL of the Web page you want to give individualized settings for its active content and then click OK. The use of all active elements is set to Enable for that site by default. To modify these settings, select the Web site in the left panel and change each element as desired.

To remove a site from the list of DNS addresses in the left panel, select it and click Remove.

**IMPORTANT:** Some sites require all or several active content elements to be active for their pages to display or function correctly. If you make very strict settings for all sites, you can experience the following problems: images not displayed, a Web page not displayed at all, a Web page displayed incorrectly, or some useful services contained in applets not working. If this happens, just change this plug-in's settings for all sites or that particular site.

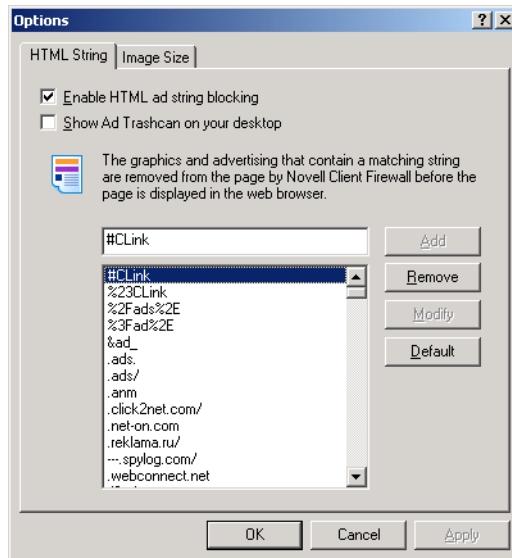
## Ad Blocking

More and more Web sites are getting crammed with ads. Generally, if you have a fast connection, ads do not create many problems. But often it is nice just to surf without the distraction of blinking, moving ads.

To change the settings of NCF's Ad Blocking plug-in, right-click the system tray icon and then click Options. In the Options window, select the Plug-Ins tab.

Select Advertisement Blocking from the Plug-In list, then click Settings.

**Figure 13 Ad-Blocking Options Window (HTML String Tab)**



NCF can block the display of banner ads from certain advertisers. NCF comes with a large list, as shown in the above figure. As you can see, all the entries in the list are single words, each having no spaces in them. These are the most common words in Internet advertisement URLs located in the HTML tags <IMG SRC= > and <A HREF= >. To add another word to the list, simply type it in the text field above the list, then click Add > OK. NCF replaces these banners with the text "AD-IMG".

The following options are available in the HTML String tab of the Options window:

- ◆ **Enable HTML Ad String Blocking**—Activates the Add and Modify buttons.
- ◆ **Show Ad Trashcan on Your Desktop**—Displays the Ad Trashcan on your desktop.
- ◆ **Add**—Adds a new entry to the list.
- ◆ **Remove**—Removes an entry from the list.
- ◆ **Modify**—Changes the entry you have made.
- ◆ **Default**—Resets the list of ad strings to default settings.

If you select Show Ad Trashcan on Your Desktop, the following Trashcan icon is placed on your desktop:

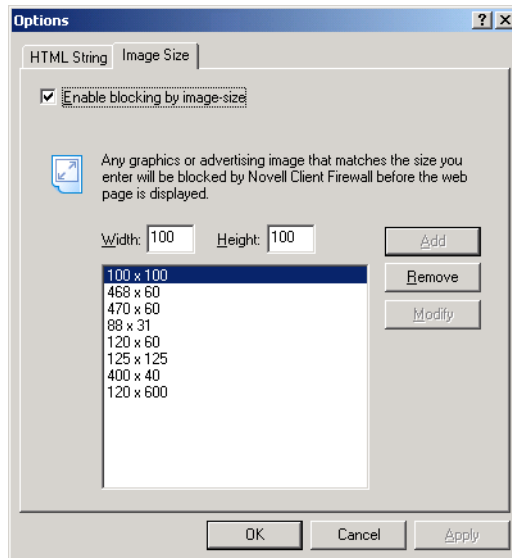


To completely remove an ad from the Web page you are viewing, simply drag the ad on top of the Ad Trashcan icon. In the Ad Trashcan dialog box that appears, do one of the following:

- ◆ To block the entire string, select the Whole String and click OK.
- ◆ To trim the URL down, select a Portion of the String and then click OK to save the ad's shortened URL into NCF.

NCF can also block all banner ads having standard sizes. To do this, select the Image Size tab in the Options window. The following window is displayed:

**Figure 14 Ad-Blocking Options Window (Image Size Tab)**



Immediately after installation, NCF is set to block all images with a link (images inside the <A> Tag) that have a size of 100 x 100, 125 X 125, 468 x 60, 470 x 60, 234 x 60, 120 x 80, or 88 x 31 pixels. NCF replaces the designated banners with the text "[AD-SIZE]" in the Web page.

To allow all graphics to be displayed on the screen, deselect Enable Blocking by Image Size.

To add to the list of image sizes to be blocked, select Enable Blocking by Image Size, type the width and height of the image to be blocked, then click Add > OK.

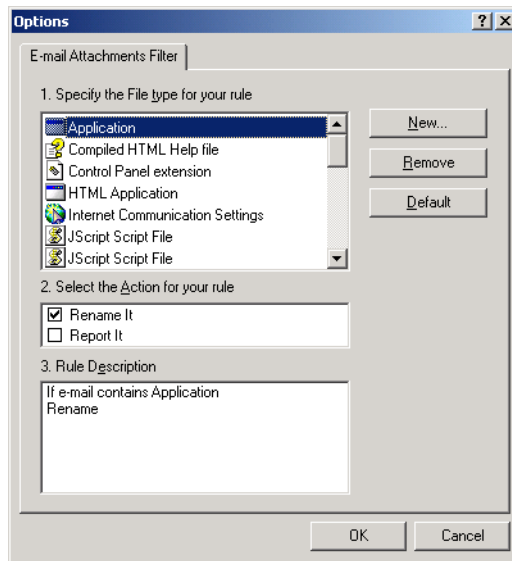
**IMPORTANT:** NCF blocks banner ads according to the settings you specify. Some legitimate images could be blocked if the setting is too strict, such as adding the word *image* to the list of blocked words. In addition, a few ads will not be blocked with this plug-in's default settings.

## Attachments Filtering

This plug-in checks the file attachments of e-mail arriving at your computer. With this plug-in, you can specify that attached files are to be quarantined so they cannot harm your computer and that you are alerted with appropriate messages. Different modes of file checking can be set with this plug-in according to the file type of each attachment.

The settings of this plug-in can be modified in its Options window:

**Figure 15 Attachments Filtering Options Window (E-mail Attachments Filter)**

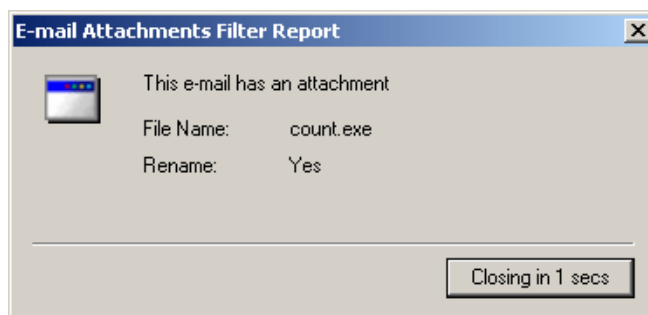


The most popular file types are configured by default. If you do not see the file type you want to set rules for, you can create a new rule for that file type by clicking New. This opens a window in which you can specify the extension of the file type. Its description is automatically supplied by NCF and added to the list.

Clicking OK brings you back to the plug-in's Options window where you will see the new file type and its description added to the list of file types NCF is set to monitor.

Check either Rename It or Report It, then click OK.

Following is an example of the message that is displayed by NCF whenever your computer receives an e-mail containing a file type that you specified to Rename It and Report It:



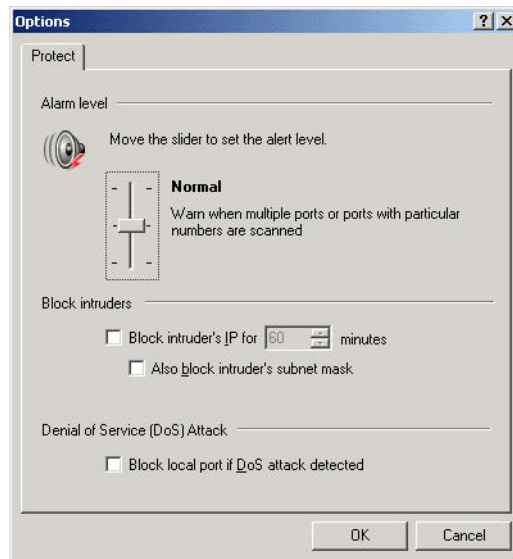
As you can see in the example, the message is displayed for a certain length of time, indicated on the button in the bottom-right corner of the message box. Clicking this button closes the message immediately.

# Attack Detection

This plug-in informs you of a possible attack on your computer from the Internet or the network your computer is connected to. It also recommends the steps to be taken in order to prevent damage to your computer.

The Attack Detection plug-in lets you specify the conditions in which a warning is to be displayed. It also has response settings that will be used if a specified security level is exceeded.

**Figure 16** Attack Detection Options Window (Protect)



In the Alarm Level section, move the slider up or down to set a higher or lower level of alarm:

- ◆ **Maximum**—A Port Scanned warning is displayed if even a single scanning of your port is detected.
- ◆ **Normal**—A Port Scanned warning is displayed if several ports are scanned or if a specific port is scanned that NCF recognizes as one that is commonly used in attacks.
- ◆ **Minimum**—A Port Scanned warning is displayed if a multiple attack is definitely detected.

The lower half of the window lets you specify the steps NCF is to follow if an attack on your computer is detected:

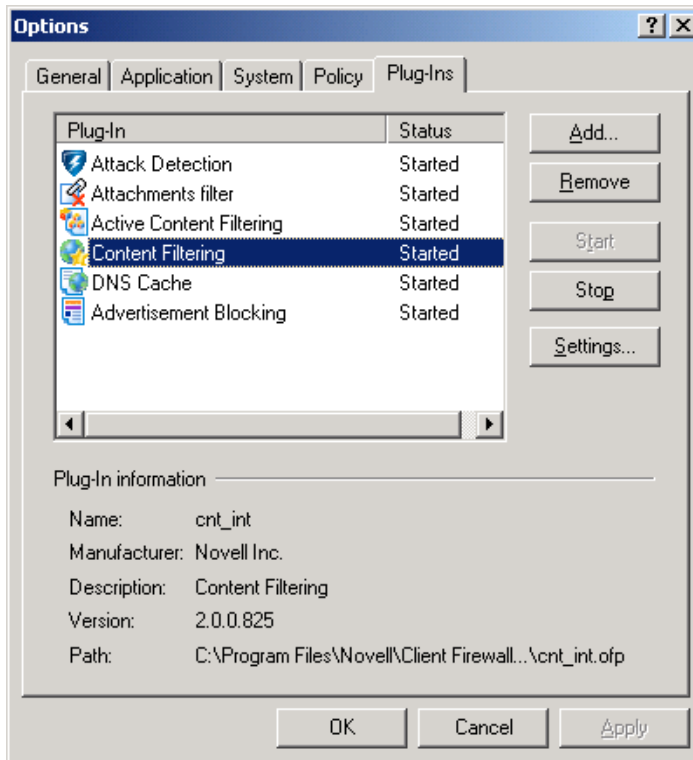
- ◆ **Block the Intruder's IP For**—Blocks all network exchanges from the computer attacking yours for the number of minutes you set (default = 60).
- ◆ **Also Block Intruder's Subnet**—Blocks all network exchanges from the entire subnet that the intruder belongs to.
- ◆ **Block Local Port If DoS Attack Is Detected**—Blocks the local port if a DoS (Denial of Service) attack is detected.

For more information about fine-tuning this plug-in, read the `install\protect.lst` file.

# Content Blocking

You can block the display of any Web sites or pages. To do this, right-click the NCF icon in the system tray, then select Options to get the following dialog box:

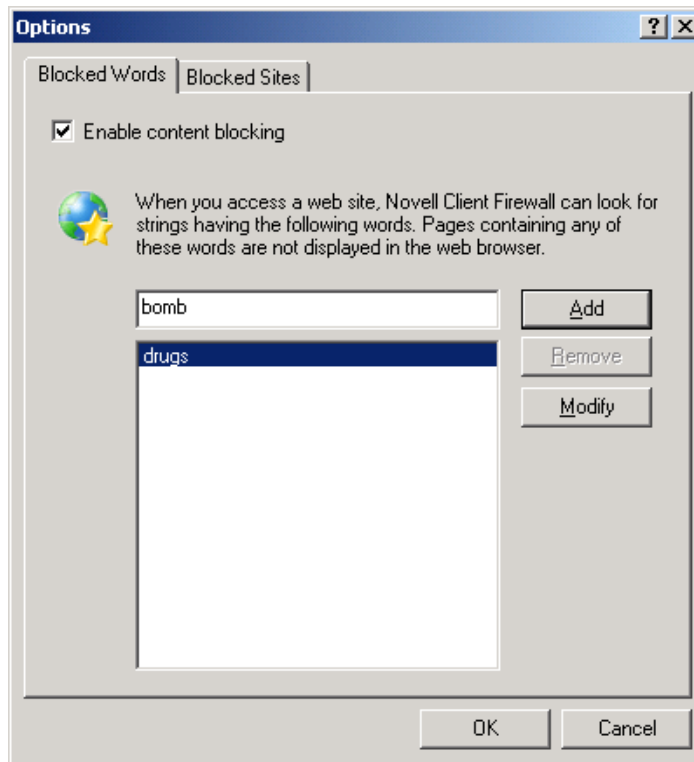
Figure 17 NCF Options Window (Plug-ins Tab)





Select Content Filtering, then click Settings. The following dialog box appears.

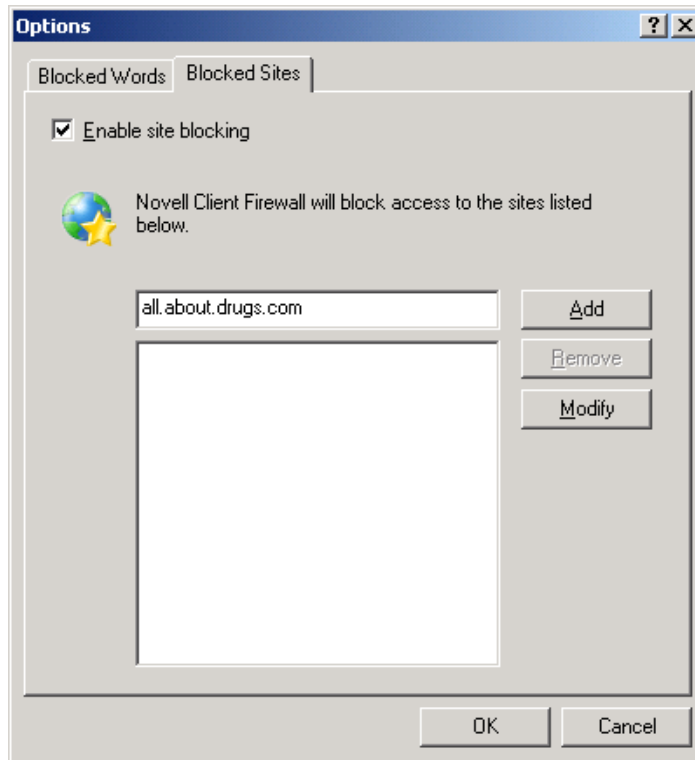
**Figure 18 Content Blocking Options Window (Blocked Words Tab)**



Check Enable Content Blocking, then type in the text field each word you want NCF to look for when blocking Web sites. As soon as you start typing, the Add button is activated. Click Add after you type each separate word or phrase. Any Web page containing any of the words on this list will not be displayed.

To list specific Web sites you do not want to be displayed on your computer, select the Blocked Sites tab.

Figure 19 Content Blocking Options Window (Blocked Sites Tab)



Check Enable Site Blocking, then type the URL or the part of the URL of the site you do not want displayed on your computer. As soon as you start typing, the Add button is activated. Click Add after URL you type. Then click OK to save the list.

## Domain Name System Cache (DNS)

The Internet works by assigning a series of numbers to each computer connected to it. This is called the computer's IP address. An example of an IP address is: 172.16.0.0. You can simply type this series of numbers into your browser's location field (near the top of your browser's window) and press Enter and your browser will go to that computer's Web pages.

Although these numerical IP addresses are easy for a computer to use, they are difficult for us humans to remember. So an address system was invented that uses words or letters called the DNS (Domain Name System). DNS is what you are probably more familiar with than IP numbers. An example of a DNS name is `www.novell.com`.

DNS names are much easier for us to remember, but our browsers still need to use the IP address to find and transfer files on the Internet. Therefore, there are databases throughout the Internet that keep track of what IP address goes with what DNS name. To find the IP address that corresponds to a DNS name, sometimes your browser has to consult several different databases located at different places on the Internet, and this often takes time.

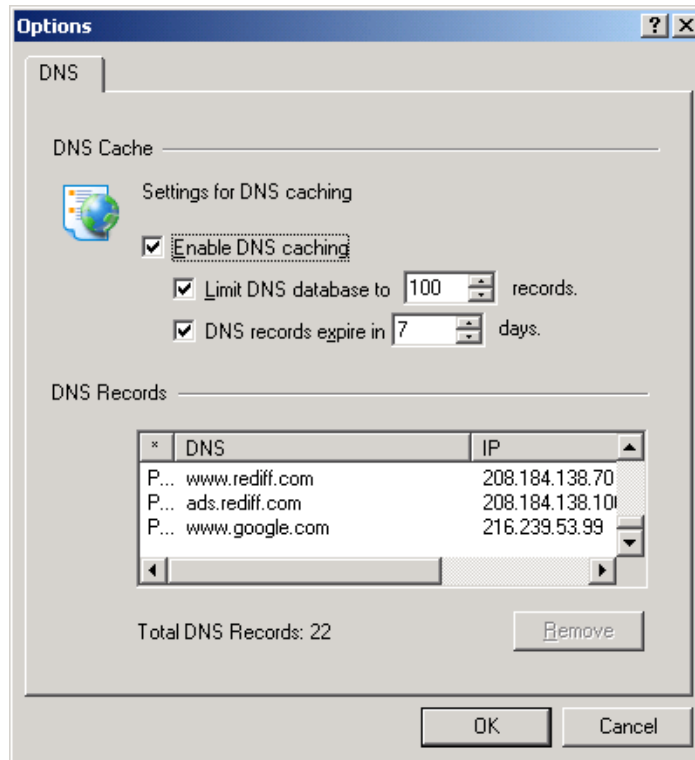
To speed things up, NCF provides a personalized look-up table of DNS addresses on your own computer. This is called a *domain name cache* and you can customize it however you like.

NCF maintains the DNS cache automatically within your specifications to include those addresses that are most recently used by you. The amount of time that a DNS address is saved in the DNS cache depends on the time you specify as one of the settings for this plug-in. It also depends on

how many DNS names you want NCF to keep track of. Only the most recently used names are kept, up to the maximum number of entries you specify.

To modify the settings of the DNS Cache plug-in, in the NCF main window click Options > Plug-Ins Setup, select DNS Cache, and then click Settings. Another way to get this same settings window is to right-click DNS Cache in the main window, then click Properties.

**Figure 20** DNS Cache Options Window (DNS)



The Enable DNS caching option must be selected (checked) for NCF to provide this speed-up. You can limit the DNS database to a specific number of entries and have them be automatically deleted if they are not used within a certain number of days. To not limit the database to only those entries that are used within a certain number of days, uncheck the DNS Records Expire check box.

We strongly recommend that you do not increase the limits of the DNS database, change the expiry period, or limit the database by unchecking any of these check boxes.

You can delete particular DNS entries from the list by selecting the line and then clicking the Remove.

The list of entries can be sorted by DNS name or IP address by clicking either of these column names. The total number of DNS entries is shown just below the list.



# 6

## Advanced Settings

Novell® Client Firewall (NCF) is designed to be effectively used in its preconfigured state even by computer novices who need not know about network protocols to safeguard their computer system against malicious applications or Web sites.

However, NCF is also fully configurable for advanced users who understand networking technology.

This chapter provides the following information so that advanced users can effectively tweak NCF and learn about its most powerful features:

- ◆ “Saving and Loading Configurations” on page 45
- ◆ “Setting a Password” on page 46
- ◆ “Creating Rules for Applications” on page 47
- ◆ “System Level Filtering” on page 48
- ◆ “Settings for a Home or Office Network” on page 49

**HINT:** A good rule of thumb when using NCF is to keep the suggested settings if you do not have a particular reason and the knowledge to change them.

## Saving and Loading Configurations

NCF has very many settings. Being able to save several different configurations of these settings lets you

- ◆ Create different configurations for you and your family or colleagues.
- ◆ Prevent your children from accessing unwanted sites (sex, games, bomb-making), playing online games, or chatting.
- ◆ Switch, using one mouse click, between Work, Rest, I am away, Block Everything, and Children configurations.
- ◆ Back up your configurations.

A configuration is the state NCF is in at any time. To create a new configuration, first save your current configuration. Then change whatever settings you want, go to the File menu, select Save Configuration As..., then specify the name you want to give the new configuration. The File menu item New Configuration is simply the default settings that NCF had when first installed. This is given for your convenience when making new configurations, but you need not use it while creating a new configuration.

The default configuration file NCF uses is named configuration.cfg, located in the directory. You can create several different configuration files simply by giving each a different name.

A configuration file can be protected by password. To do this, click Options > General, then click Enable in the Password Protection section of the dialog box.

To change to a new configuration, click File > Load Configuration and then select the configuration file you want or select the configuration name from the File menu between Save Configuration As and Exit.

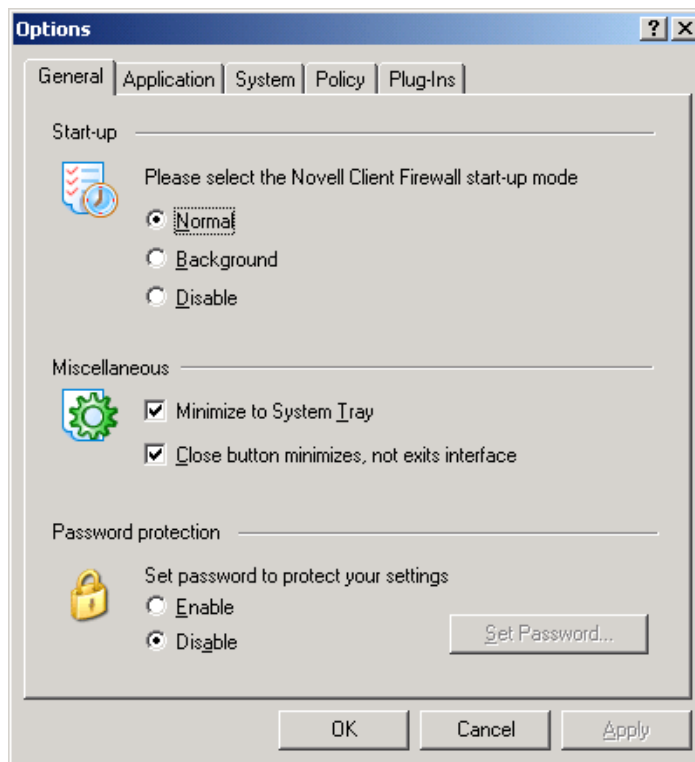
When exiting NCF, the configuration file that is currently in use is saved and it will be automatically loaded the next time NCF is started.

## Setting a Password

You can safeguard the settings you give NCF by selecting a password. This prevents all the data you entered into NCF from being changed. You can, for example, block access to objectionable sites for your children and ensure that your settings cannot be tampered with.

To set a password or change an old one, right-click the NCF icon in the system tray and then click Options. You will see this dialog box:

**Figure 21** NCF Options Window (General Tab)



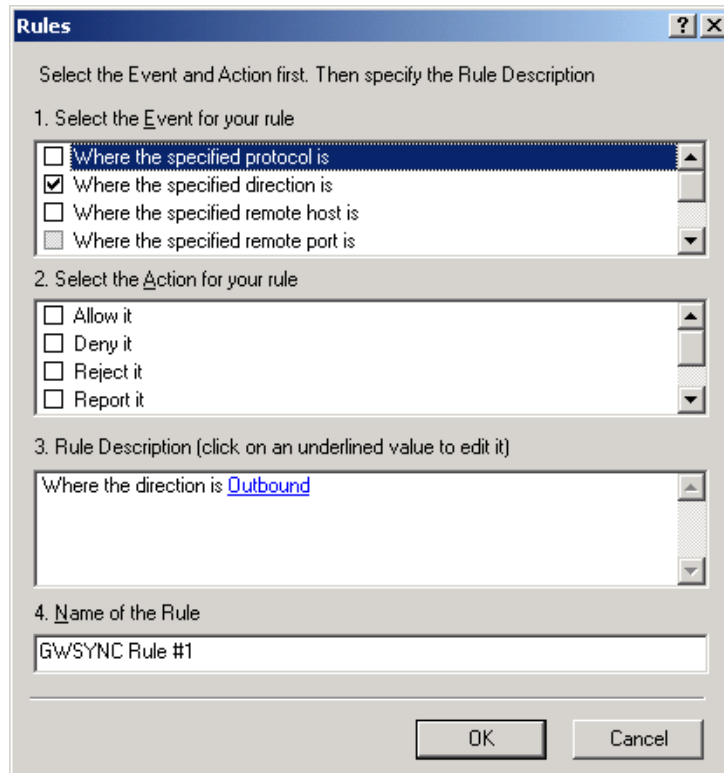
Select Enable under Set Password to protect your settings. This brings up a small window in which you can type the password you want, then click OK. Then on the General tab, click Set Password.

**IMPORTANT:** Remember your password!

# Creating Rules for Applications

This section is an extension of what was covered in “Application Level Filtering” on page 29. The rules for applications can be set in the following Rules dialog box accessed by clicking Options > Application, selecting an application on the list, then clicking Modify.

Figure 22 Rules Window



**IMPORTANT:** We recommend that only people who understand networking protocols use this dialog box.

First, describe the Event to which the rule applies. You can select from the following criteria for your rule in the Select the Event section:

- ◆ Protocol
- ◆ Direction
- ◆ Remote host and port
- ◆ Local host and port
- ◆ Time interval

Checking an event’s check box adds its message to the Rules Description field. If a rule is listed as undefined, you should click it and select one of its options.

Then select one of the following actions for your rule in the Action section:

- ◆ **Allow It**—Allows this communication.
- ◆ **Deny It**—Drops the packet. The source is not notified, so it appears that the packet never arrived at the destination.

- ◆ **Reject It**—Drops the packet and sends "The host (or port) unreachable" message to the source.
- ◆ **Report It**—Displays a message box when a rule is triggered.
- ◆ **Run Application**—Runs any application when a rule is triggered.
- ◆ **Stateful Inspection**—Turns on "stateful inspection" for this application. If activated after an application connects to a remote server, all incoming communications from that server to a port opened by the application will be allowed.

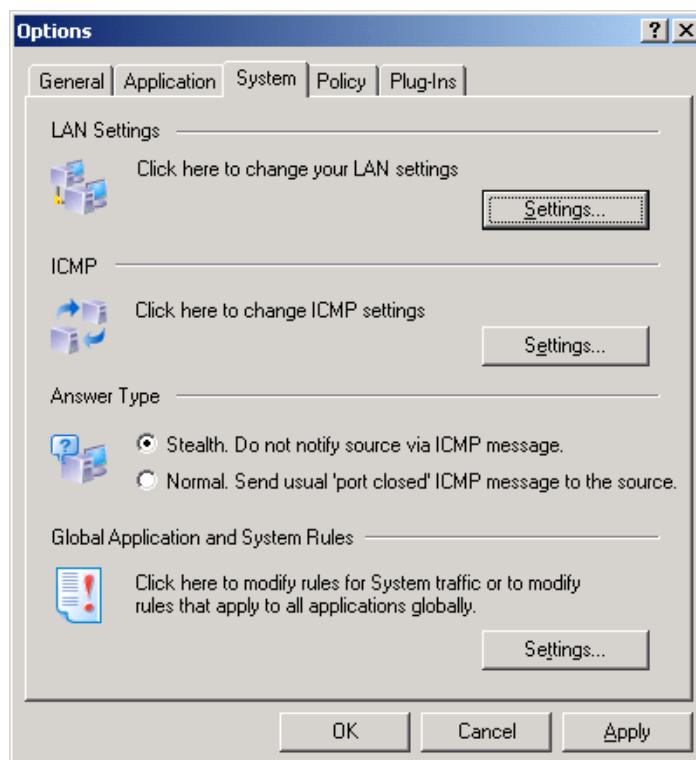
The final step is to assign a name to the rule. We recommend that you give a logical name to the rule, so it will be easy for you or others to recognize it in the future. In addition, the name you give your rule appears in the Allowed or Blocked log as the reason for allowing or blocking this communication.

**HINT:** Here is a quick summary of how Rules for Applications and Global Application and System Rules are used in NCF. When an application tries to go online, NCF checks if there are any rules for that application in the Application Rules list and, if so, NCF uses those rules and ignores the Global Application and System Rules. Otherwise, NCF checks for rules matching the activity of the application in the Global Applications and System Rules list and uses any that apply.

## System Level Filtering

**WARNING:** The System Tab settings are for advanced users only. If any are incorrectly changed for your system or network, it could result in your firewall not working as expected.

Figure 23 Options Dialog Box (System Tab)





The System tab of the NCF Options dialog box includes the following settings:

**LAN Settings**—Lets you change the settings for your local area network (LAN) and NetBIOS protocol and lets you add or remove trusted IP ranges. NetBIOS is what Windows uses as the protocol for transferring shared files between computers or printers on a network. NetBIOS is useful on a LAN with trusted computers, but it can leave your computer open to attack if it is allowed for general Internet connections.

**ICMP**—Lets you specify the types and directions of ICMP messages allowed. We recommend that you do not change the ICMP settings unless you are certain that you are making the right changes. The Default button in the ICMP Settings dialog box resets all the ICMP settings to what they were when NCF was first installed.

**Answer Type**—Switches stealth mode on or off. Normally, when your computer receives a connection request from another computer, it lets that computer know that this port is closed. In stealth mode, your computer will not respond, making it seem like it is not turned on or not connected to the Internet. We recommend that you keep NCF in stealth mode unless you have some very good reason not to.

**Global Application and System Rules**—Lets you specify global rules for each of the following:

- ◆ DNS Resolving
- ◆ Outgoing DHCP
- ◆ Inbound Identification
- ◆ Broadcast/Multicast
- ◆ Inbound/Outbound Loopback
- ◆ GRE Protocol
- ◆ PPTP Control Connection
- ◆ Remote Procedure Call (RPC)
- ◆ Server Message Block (SMB) Protocol

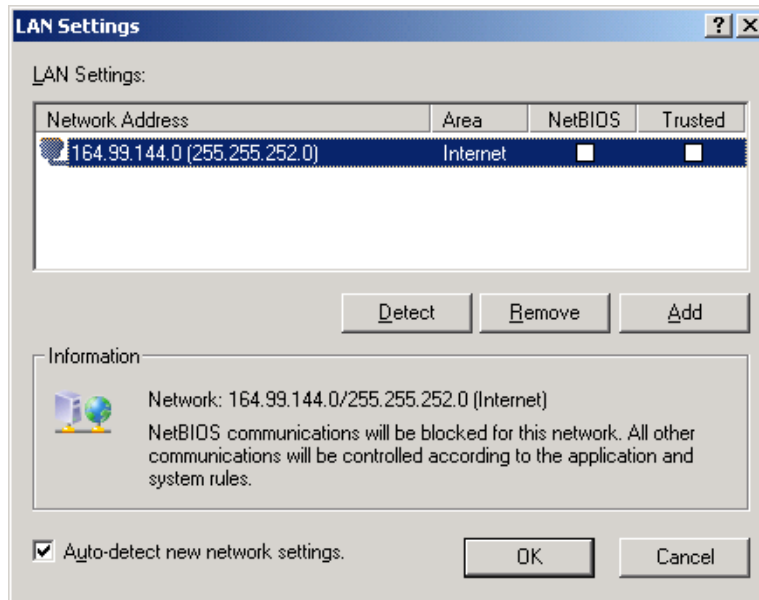
You can also create system rules by clicking the Settings button; this is very similar to how application-based rules are created. (See [“Creating Rules for Applications” on page 47.](#))

## Settings for a Home or Office Network

A fundamental difference between a local area network (LAN) and the Internet is the level of trust you can have in each. A LAN used in the home or an office is generally comprised of "friendly" computers, computers belonging to or operated by other family members or coworkers. Computers on a LAN can be called a Trusted Zone.

To check or reconfigure your network settings, click Settings in the LAN Settings section in the System tab of the NCF Options dialog box:

**Figure 24 LAN Settings Dialog Box**



Normally you will see your network address in the LAN Settings dialog box that opens. But if you deselected Auto-configure Network Settings during the NCF installation process and removed all detected networks, then no address will be listed. To detect your network automatically, click Detect.

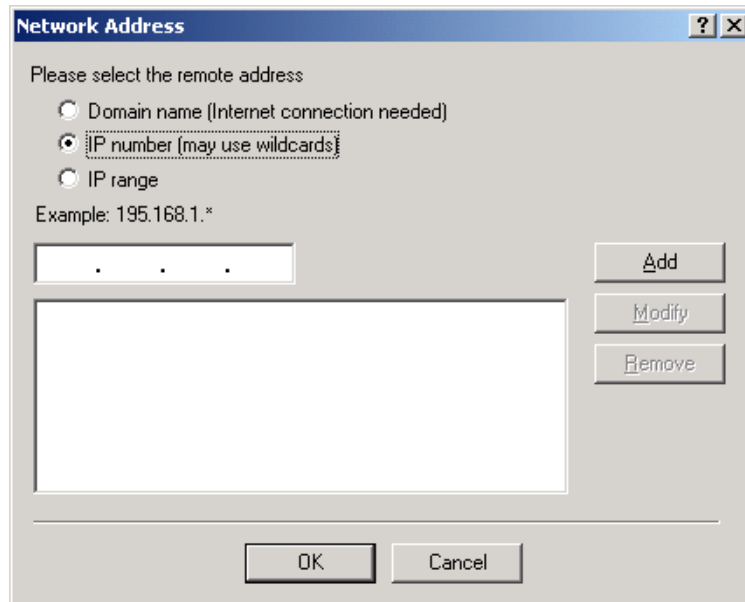
We also recommend that you keep Auto-detect New Network Settings checked, so NCF will automatically detect any new networks and you will not have to add them manually.

If you want to allow all connections for a particular network, check the corresponding check box in the Trusted column to add this network address to the Trusted Zone. Otherwise, if you want to remove the network address from the Trusted Zone, uncheck its check box.

If you want to allow all NetBIOS communications to and from a network address, check the corresponding check box in the NetBIOS column. To disallow all communications with the network, uncheck the NetBIOS and Trusted Zone check boxes.

You can also add a custom remote network address to the Trusted Zone by clicking Add to display the following dialog box:

**Figure 25 Network Address Dialog Box**



Select one of the remote address types and add data about the address into the field. An active Internet connection is required for Domain Name because the IP address needs to be looked up directly over the Internet. The IP address is saved along with the domain name you specify and it is mostly this IP address that is used by NCF.

To add your entry to the Trusted Zone list, click Add.

An entry in this list can be modified at any time by selecting it and clicking Modify.

To remove an entry, select it and click Remove.

Note that plug-ins are independent from the Trusted Zone settings. For example, even if you add `www.novell.com` to the Trusted network addresses, NCF plug-ins will still block banners, active content, and other things from this site.

**IMPORTANT:** Remember that Trusted Zone rules are given the highest priority possible. Even restricted applications can communicate with Trusted Zone hosts. We advise you to put *only* your absolutely trusted computers into this zone. If you need only file and printer sharing, use NetBios Settings rather than Trusted Zone.



# 7

## The View Menu

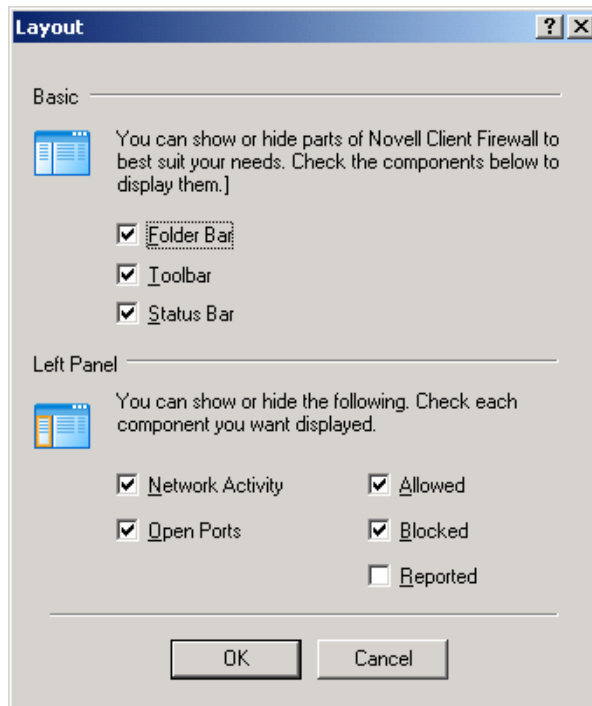
This chapter explains the following features of the Novell® Client Firewall (NCF) View menu:

- ◆ “Layout” on page 53
- ◆ “Filter by Time” on page 54
- ◆ “Columns” on page 54
- ◆ “Group By” on page 56

### Layout

This feature lets you choose to not display the folder bar, tool bar, or status bar in order to increase the amount of viewing space of the Information panel.

Figure 26 Layout Dialog Box



The Left Panel section of the dialog box lists the categories that can be displayed or hidden in the Left panel's listing by selecting or deselecting them:


- ◆ **Network Activity**—All objects with a network activity.
- ◆ **Open Ports**—All objects with an open port for a network connection.

- ◆ **Allowed**—The event log for all applications with a protocol that is supported and allowed for network operation.
- ◆ **Blocked**—The event log for all applications with network connection attempts that were blocked.
- ◆ **Reported**—The event log for all applications for which a report on their network operations must be made according to NCF's settings.

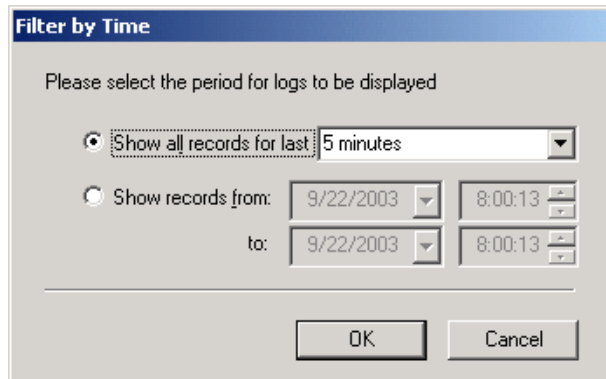
**NOTE:** The same object can appear in multiple lists.

## Filter by Time

This feature lets you filter out the data normally displayed that you are not interested in. It limits the event log display to the Allowed, Blocked, and Reported items of the Left panel.

Aside from the View menu, an alternate way to access the Filter by Time dialog box is from the NCF toolbar. The Filter by Time button  and menu options are available only when one of the Left panel's Allowed, Blocked, or Reported items is selected.

**Figure 27** Filter by Time Dialog Box



Filter by Time lets you choose from three options:

- ◆ **Current Session**—The event log for the current session of NCF.
- ◆ **Today**—The event log for the current date.
- ◆ **All**—The entire event log from the time you started using NCF

For information about filtering NCF Log Viewer logs, refer to [Chapter 8, “The NCF Log System,” on page 59](#).

## Columns

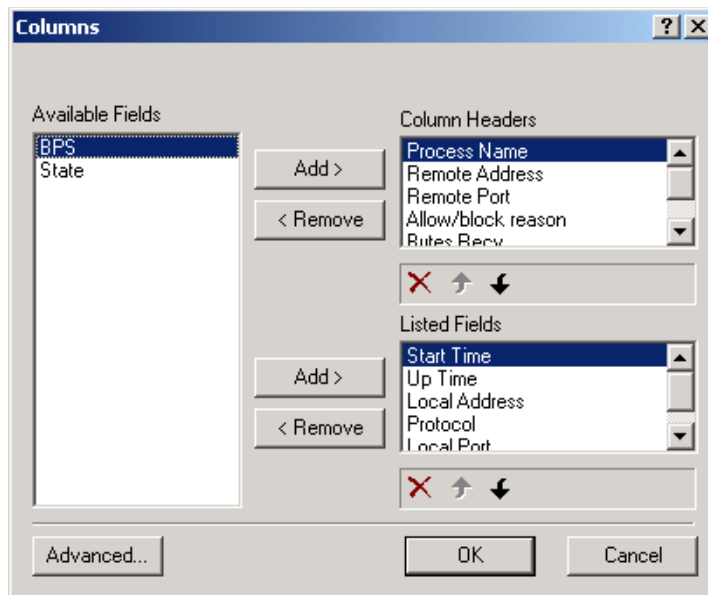
This feature lets you configure NCF to display only the data you are interested in.

**NOTE:** The Columns menu is available for Network Activity and Open Ports items only.

The Columns menu is available for Network Activity and Open Ports items only.

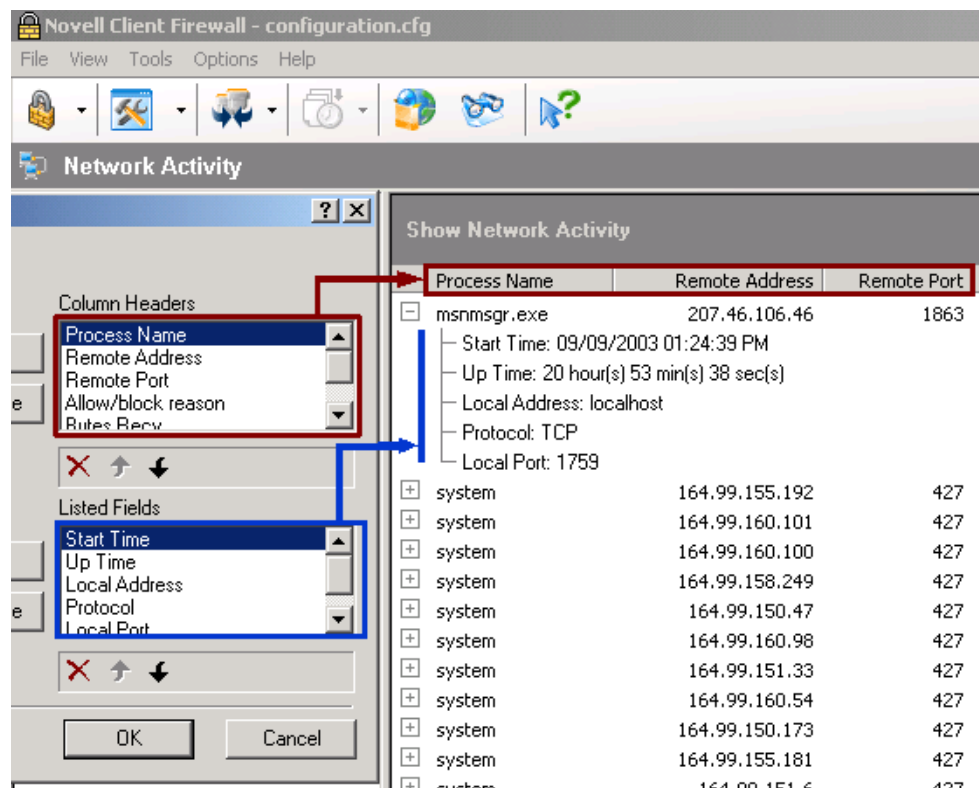
After clicking View > Columns, the Columns dialog box is displayed:

Figure 28 Columns Window Dialog Box



The dialog box can also be accessed by selecting an element in the Information panel and right-clicking it to get its context-sensitive menu. The Column Headers and Listed Fields correspond to those in the Information panel, as shown in the following figure:

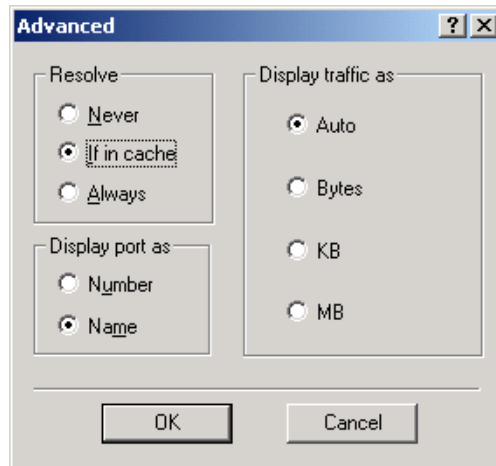
Figure 29 Column Headers and Listed Fields



You can customize the listings by removing an item from the list using the Remove button or by adding a previously removed item back to the list using the Add button.

Clicking the Advanced button in the lower-left corner of the Columns dialog box displays the Advanced dialog box:

**Figure 30** Advanced Dialog Box



The Resolve section gives you options for displaying network addresses as DNS (for example, `www.novell.com`):

- ◆ **Never**—Always displays these addresses as IP addresses (for example, `172.16.0.0`).
- ◆ **If in Cache**—Converts these to their DNS addresses if the information for the address conversion is stored in the DNS Cache module.
- ◆ **Always**—Always converts and displays these addresses as DNS addresses. However, we do not recommend this because it can result in a great number of DNS requests.

The Display Port As section lets you display the local port (on your computer) and remote port values as either of the following:

- ◆ **Number**—Ports are displayed as numbers.
- ◆ **Name**—Ports are displayed as names describing their task, if the information is available in the system for that port (for example, "www" rather than "80").

The Display Traffic As section lets you specify the base measure of the amount of transferred information in the Sent and Received fields as any of the following:

- ◆ **Auto**—Displays traffic in the most suitable measurement.
- ◆ **Bytes**—Displays traffic in number of bytes sent or received.
- ◆ **KB**—Displays traffic in kilobytes.
- ◆ **MB**—Displays traffic in megabytes.

## Group By

This feature lets you retrieve the information you need very quickly. Normally, the information is grouped by application, which is generally the most useful grouping of information. For example, you can Group by Application and select the application you are investigating from the Left panel,



and then NCF lists all the connections of this particular application and nothing more. Another example is if you run a Web or FTP server, you can Group by Local Port and select the port name from the Left panel ("www," for example), and then the Information panel shows you how your computer is exactly connected to your server.

If you are looking for applications sending data to a particular computer on the Internet, you can do this almost immediately if you use the Group By option in the View menu.

Group By can be used on the following Left panel items:

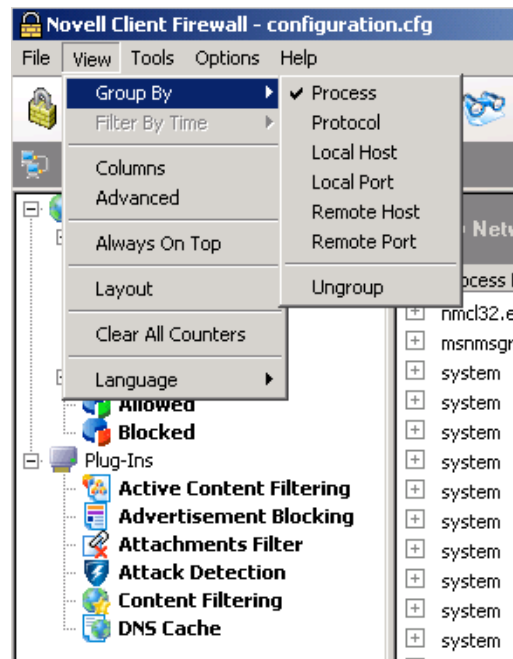
- ◆ Network Activity
- ◆ Open Ports

Group By changes the type of objects shown in a listing to any of the following:

- ◆ Process
- ◆ Protocol
- ◆ Local Host (your computer)
- ◆ Local Port (on your computer)
- ◆ Remote Host (computer other than yours)
- ◆ Remote Port (on the other computer)

To use the Group By feature, select one of the Left panel items listed above and then click View > Group By to see the following:

**Figure 31 Group By Menu Options**



Clicking an item in the Group By menu selects that item to be listed. This moves the check from the previously selected item to the one just selected.



# 8

## The NCF Log System

This chapter discusses the following information about the Novell® Client Firewall (NCF) log system:

- ◆ [“Introduction” on page 59](#)
- ◆ [“NCF Log Viewer Main Window” on page 60](#)
- ◆ [“Displaying Logs” on page 62](#)
- ◆ [“Working with Logs and Filters” on page 64](#)

### Introduction

NCF performs many different functions as it protects your computer from attacks. Each action it takes is referred to as an event, and every event is logged.

The NCF Log Viewer makes it easy for you to view these event logs. The event logs show you the history of every operation NCF performed, including the following:

- ◆ Every application and connection that was allowed or blocked by NCF.
- ◆ The specific activities of each NCF plug-in.
- ◆ The start of every program and all changes made to policies, configuration settings, and passwords.

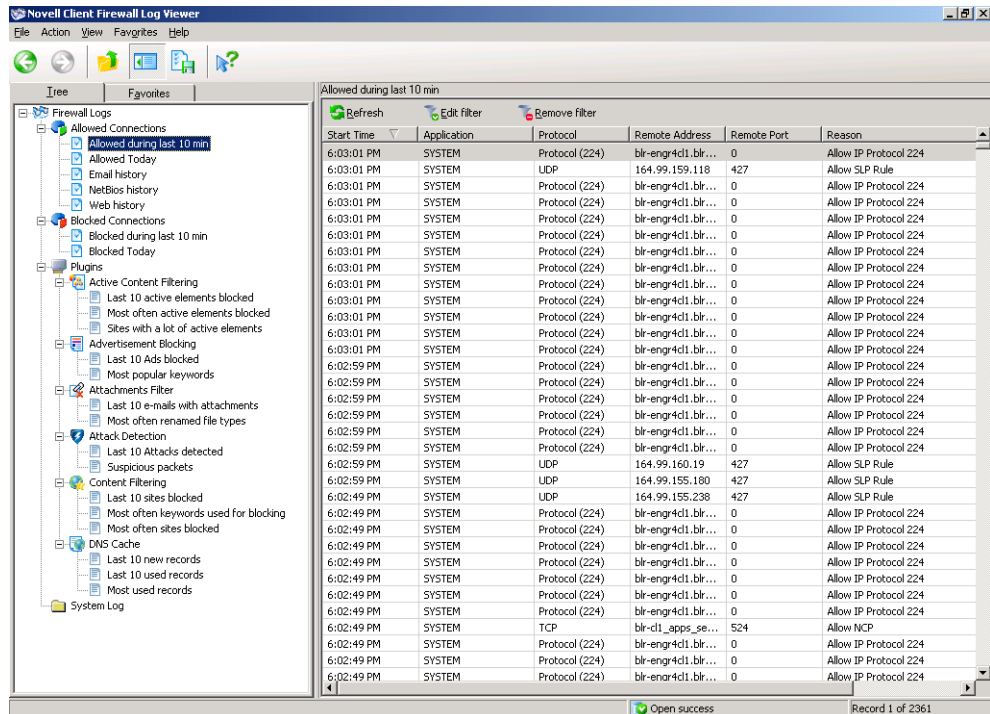
The following are the main features of the NCF log system:

- ◆ One mouse click to view the entire log or a selection of specific events. For details, see [“Displaying Logs” on page 62](#).
- ◆ Customized display of the logs. You can view only the information you need by selecting columns and limiting their parameters or by sorting by any parameter.
- ◆ Preset selections of events can be displayed. You can easily switch between connections blocked during the last ten minutes, for instance, or all connections allowed today. You can also create, edit, and remove selections of events to be displayed. For details, see [“Working with Logs and Filters” on page 64](#).
- ◆ Filters can be added to organize the data displayed.
- ◆ Logs can be copied or exported according to presets, filters, or selected records.
- ◆ Log files can be cleared to save hard drive space.
- ◆ Customized SQL queries can be created for specific monitoring purposes.
- ◆ Logs can also be browsed via the Microsoft Management Console (MMC) snap-in.

# NCF Log Viewer Main Window

The main window of the NCF Log Viewer is for viewing and working with the logs. To access this window, click Tools > Novell Client Firewall Log Viewer.

Figure 32 Log Viewer Main Window



## Console Tree

The Console tree is a listing of filters. It consists of two tabs: Tree and Favorites.

On the Tree tab, there are four groups of logs:

- ◆ **Allowed Connections**—A listing of every application and connection that NCF allowed.
- ◆ **Blocked Connections**—A listing of every application and connection that NCF blocked.
- ◆ **Plug-Ins**—Each plug-in has its own log. Active Content displays the sites that had some of its active content blocked based on the settings for Java, JavaScript, VB Script, ActiveX, and other active content elements.
  - ◆ **Ads** displays a list of all the ads that were blocked.
  - ◆ **Attachments Filter** shows all the e-mail file attachments that were neutralized and quarantined from your computer.
  - ◆ **Attack Detection** shows every suspicious activity and attack on your computer from the Internet, the ports involved, and where the attacks originated.
  - ◆ **Content** lists all the Web sites or pages that were blocked due to their content.
  - ◆ **DNS Cache** displays the Web addresses saved by NCF to speed up your Internet connection to those sites.
- ◆ **System Log**—A record of every program start and every change made to the firewall policies, program options, and configuration settings.

## Information Panel







The Information panel shows the details of whatever filter you select in the Console tree. The information is arranged in a table. The columns of this table represent the various log parameters, such as Application, Start Time, and Protocol. Each log has its own set of parameters. For details, see “[Displaying Logs](#)” on page 62.

## NCF Viewer Toolbar

The NCF Viewer toolbar is near the top of the NCF Viewer window.

When working with NCF Viewer, you can see a pop-up explaining what each button does by holding your cursor over it for a second or so.

Table 3 NCF Viewer Buttons

Button	Function
	Goes back to the previous selected item.
	Goes forward to the next selected item.
	Goes up one level.
	Shows or hides the Console Tree.
	Exports the selected log.
	Displays Help.

## Description Bar

The Description bar is right above the Information panel in the NCF Viewer window, and it displays a description of the filter selected in the Console tree.

Blocked Today

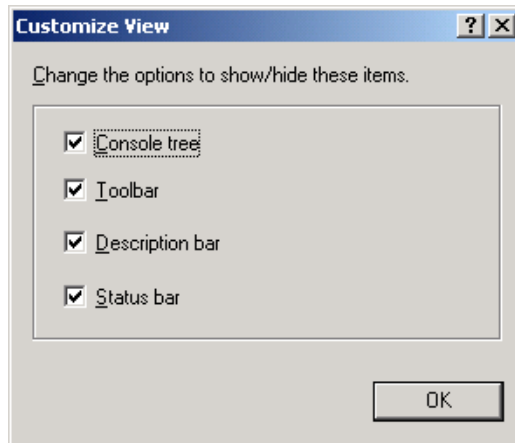
## Status Bar

The Status bar is at the bottom of the NCF Viewer window, and it consists of two sections that display the following information:


- ◆ The result of attempting to open the selected log
- ◆ The number of the record being viewed and the total number of records in that log

You can very often locate data more easily by hiding specific parts of the NCF Viewer window that you do not care to view. To customize the Viewer's layout, click Tools > Novell Client Firewall Log Viewer > View > Layout.

**Figure 33 Customize View Dialog Box**



Check the elements you want to display and uncheck those you want to hide.




**HINT:** To show or hide the Console tree, you can also use the  button on the NCF Viewer Toolbar

## Displaying Logs

To view NCF logs, click Tools > Novell Client Firewall Log Viewer. Then select the items of interest in the Console tree as described below, or switch to the Favorites tab.

The Console tree and Information panel are similar to the left and right panels of Windows Explorer. The Console tree is a listing of the filters and the Information panel gives detailed data about whatever filter is selected in the Console tree.

As with Windows Explorer, any line that starts with a plus sign (+) can be expanded to show each of its subcategories. Any line starting with a minus sign (-) shows that the line has already been expanded. By clicking the minus sign, all of its subcomponents can be hidden so only the name of the component is displayed to conserve screen space.

- ◆ To expand or collapse all the items of a log or plug-in, right-click it in the Console tree, then click Expand All or Collapse All.
- ◆ To go back to the previously selected item, click the  button on the NCF Viewer toolbar.
- ◆ To go forward to the next selected item, click the  button on the toolbar.
- ◆ To go up one level, click the  button on the toolbar.
- ◆ To see a filter:
  - ◆ In the left panel of the NCF main window, select the component you want to view (Allowed, Blocked, or one of the plug-ins).
  - ◆ Click the Show Detailed Log button if you want to see the entire log. To view a part of the log, select a preset or filter from the drop-down list using the Show Log Preset button.

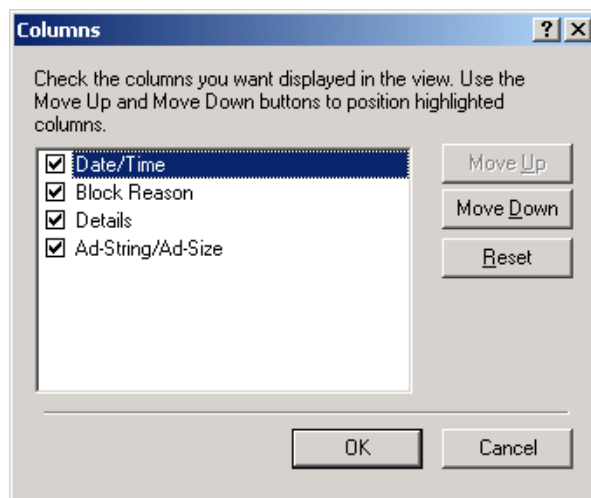
The NCF Viewer shows the details of the log, and the Console tree shows the preset or filter being viewed.

Content in the NCF Viewer changes quickly; therefore, to display the latest data in the Information panel, refresh it occasionally by first selecting the log, preset, or filter you want to refresh in the Console tree and then clicking the Refresh button in the Information panel.

The history of NCF activity is displayed in the NCF Viewer Information panel as a table. Every log has its own set of columns. You can configure the NCF Viewer to show only the columns you are interested in and in any sequence you like.

To select the columns you want displayed for the selected log, open the log as described above. Then right-click anywhere in the Information panel and then click Columns. Alternatively, you can click View > Add/Remove Columns on the Menu bar.

**Figure 34 Columns Dialog Box**



In the Columns dialog box, check the names of the parameters (columns) you want displayed in the Information panel.

To change the sequence of columns in your log, simply click-and-drag the columns in the Information panel to arrange them in whatever order you want. This can also be done in the Columns dialog box by selecting a column and then clicking the Move Up or Move Down button. To revert to the default order, click Reset.

To resize a column, open the log as described above. Position your cursor over the border of the column's caption. The cursor changes to a double-headed arrow. Click the left mouse button and keep it pressed while moving the cursor. Release the button when the column has reached the size you want.

NCF Log Viewer also lets you sort the records of a log by the values of any column in descending or ascending order. Click the header of the column you would like to use to sort the records. If the header shows an arrow pointing upwards, the records will be sorted in ascending order (1, 2, 3...). To reverse the order, repeat the click. The header now shows a downward arrow and the records will be in descending order (...3, 2, 1).

To make it easier to locate specific data in a log, you can show or hide records containing the same data in any displayed columns. Select a record in the Information panel, then right-click in the cell that contains the data of interest. From the context menu, select Include Selection to show the

records with similar data or Exclude Selection to hide them. If there are other records that have the same data in a cell, you can add that also. To show all records again, select Show All from the context menu.

For example, to view data on connections established by a certain application at a particular time, select the Allowed Connections log, right-click the cell containing the information record for the application in the Application column, then click Include Selection. Then right-click the required date and time in the Start Time column and click Include Selection again. The Information panel will now display all the records of the selected date related to the selected application.

This operation can be done so quickly that there is no reason to save the configuration. To create a permanent selection of records under complex conditions, create a filter.

**NOTE:** Include Selection and Exclude Selection commands are not available for some logs.

## Working with Logs and Filters

There are several useful tasks you can perform with logs:

- ◆ Create filters.
- ◆ Clear logs.
- ◆ Copy logs, filters, presets, or particular records to the Windows clipboard.
- ◆ Export logs, filters, presets, or records to text files.
- ◆ Add logs, filters, or presets to Favorites.

### Creating, Modifying, and Removing Filters

A filter is a way of selecting specific logged events; it filters out only the data you want in a log. A filter is named to show the data it presents and it appears as a separate item in the Console tree. The conditions (rules) of filtering are specified by the user. The rules are based on each column (type of data) that is in a log. Filtering out only the data that you are interested in is a powerful and flexible feature. With filters, you can narrow your search to only the data within a specific time span or only the data about a particular application, port, etc.

To create a filter:

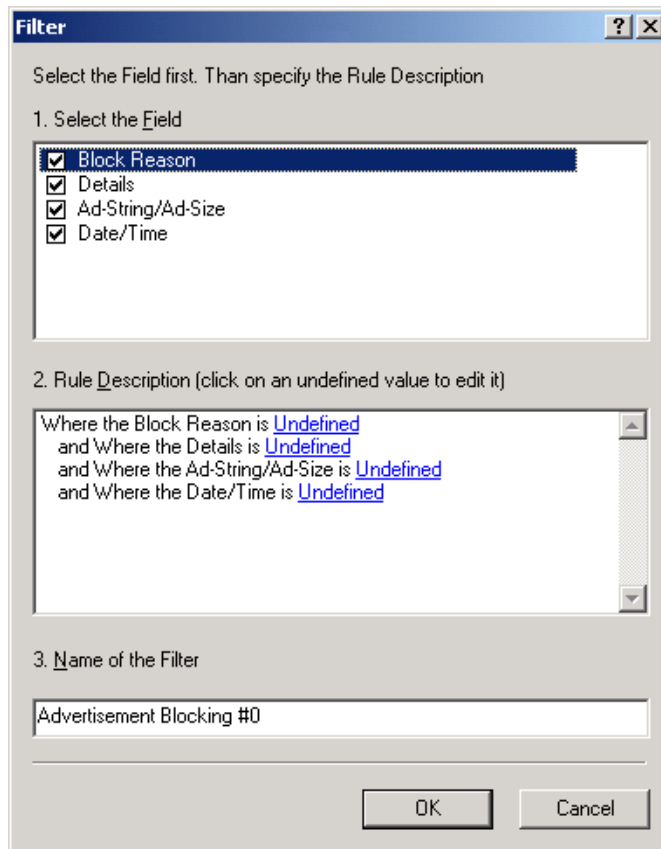
- 1** Open the log of interest as described in [“Displaying Logs” on page 62](#).
- 2** Click the Add Filter button in the Information panel.

This command is also available on the NCF Viewer Menu Bar under Actions > Add Filter and in the context menu of each log in the Console tree.



You will see the Filter dialog box with a listing of the columns in that log:

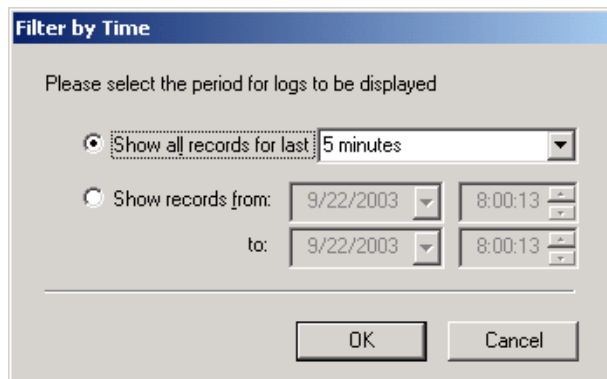
**Figure 35 Filter Dialog Box**



To specify a filtering rule, check each column of data in section 1 that you want to see. In the description field in section 2, the beginning part of the rule appears (such as Where the Start Time Is Undefined). To continue the rule, click Undefined.

In the dialog box that appears, you can specify various limitations for the selected column:

**Figure 36 Filter by Time Dialog Box**



After specifying the limitations, click OK. The rule will be completed according to the choice you have made. For example: Where the Start Time Is Last 5 Minutes.

- 3** Specify as many rules as you like, then specify the filter name and click OK.

The new filter will appear in the Console tree.

To edit an existing filter:

- 1** Click the Edit Filter button in the Information panel.
- 2** Edit all the settings of the filter.

To remove an unnecessary filter:

- 1** Select it in the Console Tree.
- 2** Click the Remove Filter button.

### Copying and Cleaning Logs

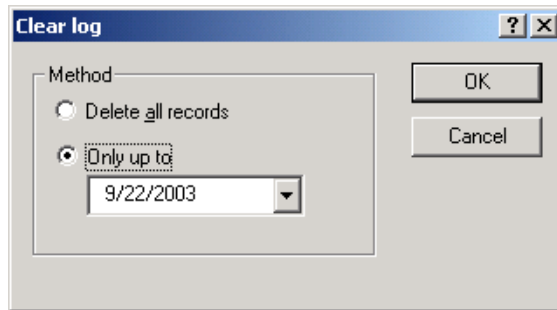
To save specific logged data to a text file or copy it to the clipboard (in order to paste it in other applications):

- 1** In the NCF main menu, click Tools > Novell Client Firewall Log Viewer.
- 2** In the Console tree, select the log you want.
- 3** Select the records you want to copy or export.
  - ◆ To select a group of records, click the first record, hold down the Shift key, then click the last record.
  - ◆ To select separate records, click each record while holding down the Ctrl key.
  - ◆ To make an advanced selection by using one or several columns, right-click a record and then click Include Selection or Exclude Selection.
- 4** Right-click a record, then click Export or Copy.
- 5** Specify the folder to export the data to and give the new file a name. If you are copying records, then remember to paste them into another file.
- 6** Click OK.

Logs are stored in a database that is automatically compressed to conserve space on your hard disk, so there is usually no need to clear these logs. However, if you want to clear them:

- 1** In the NCF main menu, click Tools > Novell Client Firewall Log Viewer.
- 2** Select the log you want in the Console tree
- 3** Right-click in the Information Panel.
- 4** Click Clear Log.

**Figure 37 Clear Log Dialog Box**



- 5 Either select Delete All Records or specify the date of the last record to be deleted.

### Using Favorites

The Console tree consists of two tabs: Tree and Favorites. Favorites is where you can keep things that you use often.

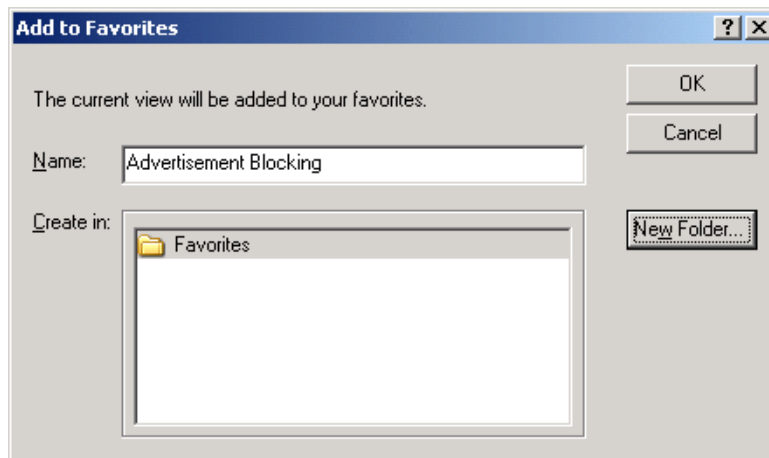
You can add logs, presets, or filters that you frequently use to the Favorites tab for convenient and quick access:

- 1 From the NCF main menu, click Tools > Novell Client Firewall Log Viewer.
- 2 In the Console tree, right-click the desired item (group of logs, log, log preset, or filter), then click Add to Favorites.

You can also select the item from the Favorites menu.

The Add to Favorites dialog box appears:

**Figure 38 Add to Favorites Dialog Box**



- 3 (Optional) Rename the item in the Name field.
- 4 Select a folder to place the item in or create a new one by clicking New Folder > OK.

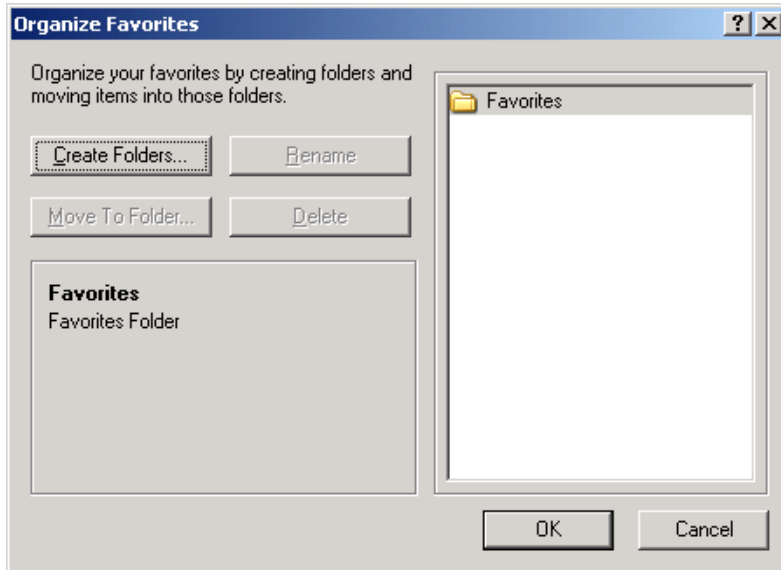
The item now appears on the Favorites tab in the specified folder.

To display an item you saved in Favorites, click Favorites in the Console tree and select the item.

To delete an item from Favorites, click the Favorites tab, right-click the item, then click Remove.

To rearrange the order of items in Favorites, select Favorites from the NCF Viewer menu, then click Organize Favorites to get this dialog box:

**Figure 39 Organize Favorites Dialog Box**

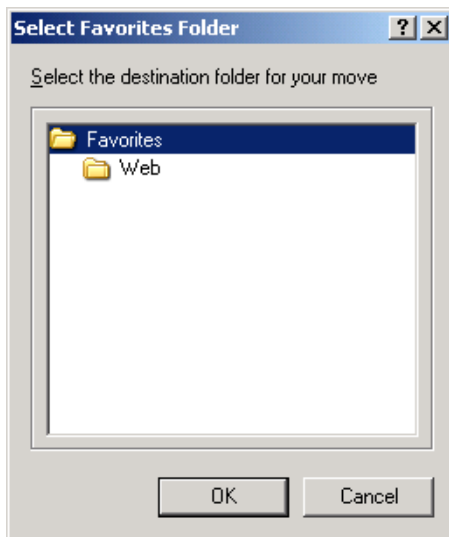


To create a new folder, click Create Folder.

To rename or delete an item, select the item and click Rename or Delete.

To move an item to another folder, click Move to Folder.

**Figure 40 Select Favorites Folder Dialog Box**



In the Select Favorites Folder, select the folder you want the item to be moved to, then click OK.

# A

## Message and Menu Descriptions

### ICMP Messages

Field Value	Message	Description
0	Echo Reply	One of the simplest methods of checking operating conditions of a network node. After an echo signal is received, any network node generates an echo reply and returns it to the source. If the source receives a reply to the echo request, this indicates that the main components of the traffic system are in good condition.
3	Destination Unreachable	Generated by a gateway when it cannot deliver an IP datagram. This is the unit of data, or packet, transmitted in a TCP/IP network. Each datagram contains source and destination addresses and data.
4	Source Quench	Transmitted from the node to the datagram source in the event that the input queue is overcrowded. In this case, the datagram is removed from the queue.
5	Redirect	Transmitted when a gateway detects that a nonoptimal route is being used. The gateway then sends a request for a change of route in the routing table.
8	Echo Request	One of the simplest methods of checking operating conditions of a network node. After an echo signal is received, any network node generates an echo reply and returns it to the source. If the source receives a reply to the echo request, this indicates that the main components of the traffic system are in good condition.
10	IP Announcement	Transmits a broadcast to announce its IP address.
11	Time Exceeded for Datagram	Sent when a datagram is transferred from one gateway to another more times than it is allowed (normally this indicates route cycling).
12	Parameter Problem on Datagram	Sent by a gateway if a problem occurs during the transmission of a specific datagram that is not in the range of the above messages. The datagram must be abandoned due to this error.
13	Timestamp Request	Used to synchronize the clocks in a network's nodes.
14	Timestamp Reply	Used to synchronize the clocks in a network's nodes.
15	Information Request	Obsolete. Was used earlier by network nodes to determine their internetwork addresses, but now considered outdated and should not be used.

Field Value	Message	Description
16	Information Reply	Obsolete. Was used earlier by network nodes to determine their internetwork addresses, but now considered outdated and should not be used.
17	Address Mask Request	Used to find out the mask of a subnet (what address bits define a network address). A local node sends an Address Mask Request to a gateway and receives an Address Mask Reply in answer.
18	Address Mask Reply	Used to find out the mask of a subnet (what address bits define a network address). A local node sends an Address Mask Request to a gateway and receives an Address Mask Reply in answer.

## NCF Main Menu Options

Menu	Menu Item	Description
File	New Configuration	Makes a new configuration of settings based on NCF default settings.
File	Load Configuration	Loads a previously saved file of configuration settings.
File	Save Configuration As	Saves the NCF current configuration to a file of your choosing.
File	Exit	Exits the NCF GUI but still protects your system by running NCF in the background (invisible to user).
File	Exit and Shutdown	Closes the interface and stop the firewall, so NCF is no longer protecting your system.
View	Group By	Specifies the types of connections in the Left pane.
View	Filter by time	Filters unwanted data from the display of a log file in the Information panel to help narrow a search for specific network activities.
View	Columns	Specifies the columns of data to be displayed and their sequence in the Information panel.
View	Advanced	Specifies how details are displayed in the Information panel of the Network Activity and the Open Ports items.
View	Always on Top	Keeps the NCF main window on top of all other windows.
View	Layout	Specifies the kind of elements in the My Internet list to be displayed in the Left panel.
View	Clear All Counters	Resets all general stats displayed in the Information panel for Allowed, Blocked, Reported, and plug-ins.
View	Language	Sets the language for the NCF interface.
View > Group By	Application	Groups by names of applications.

<b>Menu</b>	<b>Menu Item</b>	<b>Description</b>
View > Group By	Local address	Groups by names of local hosts.
View > Group By	Local port	Groups by names of local ports.
View > Group By	Direction	Groups by direction (listening, outbound, or open port).
View > Group By	Remote address	Groups by names of remote hosts.
View > Group By	Remote port	Groups by names of remote ports.
View > Group By	Ungroup	Does not group.
Tools	NCF Update	Clears all log information from NCF logs.
Tools	Automatically Check for Updates	Automatically updates NCF as updates become available.
Tools	Log Viewer	Opens the NCF Log Viewer so you can view detailed logs.
Options	General	Displays the System Settings window with the General tab activated.
Options	Application	Displays the System Settings window with the Application tab activated.
Options	System	Displays the System Settings window with the System tab activated.
Options	Policy	Displays the System Settings window with the Policy tab activated.
Options	Plug-Ins Setup	Displays the System Settings window with the Plug-Ins tab activated.
Help	Contents and Index	Displays the NCF main help files.
Help	Context Help	Displays help for a main window element.
Help	NCF on the Web	Displays the submenu of online support options.
Help	About NCF	Displays the version of NCF and each of its components.





# B

## Novell Client Firewall FAQs

### General Issues

#### When I run NCF, some applications fail to work. Why?

Check whether you have blocked the application unknowingly.

To do this:

- 1** From the NCF menu select Options > Application. The Application Tab is displayed.
- 2** Verify whether the application is in the Blocked Applications list.
- 3** (If so) Drag-and-drop it either to the list of Trusted Applications or Partially Allowed Applications.

#### My attack detection event log gives information about a portscan event. What should I do?

A portscan is initiated by a remote host to determine the open ports on the local system. Usually, this is done by malicious attackers prior to staging an attack on the local system or prior to hosting a distributed attack from the local system. NCF detects these portscans and filters them out.

However, at times it may suspect (incorrectly) a trusted host's connection request as an attack, also known as a false positive, and log the information in the Information Panel.

The pattern of port numbers scanned will help you to differentiate a false positive from a true alert. But a less familiar user may choose to either notify his network administrator about the alert, or simply ignore the logged information as the system is protected by NCF in any case.

#### Certain areas on the web pages I browse display the terms AD\_IMG, AD\_SIZE, and AD. What do they mean?

These are instances of removed advertisements using the Advertisement Blocking option in NCF. See [“Ad Blocking” on page 35](#). The space from where you have removed advertisements will show one of the above terms.

## After installing NCF, I tried to ping the machine from outside, but it is not accessible. Why?

By default your system is configured to the stealth mode. In order to ping, you have to enable In and Out options for both Echo Request and Echo Reply.

To do this:

- 1 From the NCF menu, select Options > System. Options dialog box is displayed.
- 2 Click Settings in the ICMP section. The ICMP window is displayed.
- 3 Keep In and Out options checked for both Echo Reply and Echo Request message types.

**WARNING:** Enabling In and Out options for both Echo Request and Echo Reply can expose the system identity to Internet.

## I tried to block certain sites using the content filtering option, but NCF fails to block the content. Why?

You will encounter this problem if you have typed *http://* along with the URL of the site you want to filter in the Options (Blocked Sites Tab) window. See “[Content Blocking](#)” on page 40 for details.

Type only the name of the site you are filtering.

Example: *http://www.abcdefg.com* (wrong)

*www.abcdefg.com* (right).

## I get a very delayed response while accessing some *http://* sites, why is this?

If the site is redirecting the request to *https://*, specify the *https://* URL directly instead of *http://* URL.

## What should I do when the message 'Handle is Invalid' pops up?

Exit and Shutdown NCF. Then restart it to resolve this.

After Restart, if the message continues to pop up, check whether your system meets the minimum memory requirements. See “[Minimum System Requirements](#)” on page 12 for details.

## Sometimes, at the Startup, my system fails to communicate with the network. Is this NCF related?

Check if this is related to NCF in the following ways:

- ◆ Verify if the NCF icon is missing in the system tray. If so, check whether NCF.exe is listed in the Process tab of Task Manager. If it is there, an error might have occurred during NCF startup. Restart NCF to solve this problem.
- ◆ Verify whether multiple instances of NCF are running on your system. To do this, go to the Process tab of the Task Manager. If there are multiple instances, select all ncf.exe processes and click End Process. Then Restart NCF.

## For no apparent reason, my system runs out of hard disk space. Is this NCF related?

Check if this is NCF related.

To do this, verify the size of the log database (op\_data.mdb). If it has taken a substantial amount of hard disk space (for example, more than 100MB) clear it.

To do this:

- 1** From the NCF main menu click Tools > Novell Client Firewall Log Viewer. Novell Client Firewall Log Viewer appears.
- 2** Select File > Repair Database. The Database Repair dialog box appears.
- 3** Click option Mark Database as "corrupt". On next OS startup delete file and create new.
- 4** Click OK.

## Issues Related to Windows NT

### While installing NCF, I receive messages titled 'Overwrite Protection' or 'Error Executing the Specified Program'. What should I do?

Note the path displayed in the error message and delete all files (in the directory) mentioned in the path.

After that, restart the installation.

### What should I do if Auto-configuration of network settings fail?

In this case you have to manually add network or host address.

### Windows FTP client is not working even though an application rule is present. How will I resolve this?

Add a system rule similar to the existing application rule for the Windows FTP client.

To do this:

- 1** From the NCF menu select Tools > Application. The Options menu is displayed.
- 2** Select the application and click the Edit button > Modify Rules.
- 3** In the Rules window, verify the Application Rules you have set.
- 4** Add the same rules in the System tab.

**NOTE:** For any other application, which faces similar problem, create a system rule.

