User Guide

Firewall Suite

August 1, 2003

MARSHAL™

THIS DOCUMENT AND THE SOFTWARE DESCRIBED IN THIS DOCUMENT ARE FURNISHED UNDER AND ARE SUBJECT TO THE TERMS OF A LICENSE AGREEMENT OR A NON-DISCLOSURE AGREEMENT. EXCEPT AS EXPRESSLY SET FORTH IN SUCH LICENSE AGREEMENT OR NON-DISCLOSURE AGREEMENT, MARSHAL LIMITED PROVIDES THIS DOCUMENT AND THE SOFTWARE DESCRIBED IN THIS DOCUMENT "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. SOME JURISDICTIONS DO NOT ALLOW DISCLAIMERS OF EXPRESS OR IMPLIED WARRANTIES IN CERTAIN TRANSACTIONS; THEREFORE, THIS STATEMENT MAY NOT APPLY TO YOU.

This document and the software described in this document may not be lent, sold, or given away without the prior written permission of Marshal, except as otherwise permitted by law. Except as expressly set forth in such license agreement or non-disclosure agreement, no part of this document or the software described in this document may be reproduced, stored in a retrieval system, or transmitted in any form or by any means, electronic, mechanical, or otherwise, without the prior written consent of Marshal. Some companies, names, and data in this document are used for illustration purposes and may not represent real companies, individuals, or data. This document could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein. These changes may be incorporated in new editions of this document. Marshal may make improvements in or changes to the software described in this document at any time.

U.S. Government Restricted Rights: The software and the documentation are commercial computer software and documentation developed at private expense. Use, duplication, or disclosure by the U.S. Government is subject to the terms of the Marshal standard commercial license for the software, and where applicable, the restrictions set forth in the Rights in Technical Data and Computer Software clauses and any successor rules or regulations.

Marshal, MailMarshal, the Marshal logo, WebMarshal, Security Reporting Center and Firewall Suite are trademarks or registered trademarks of Marshal Limited or its subsidiaries in the United Kingdom and other jurisdictions. All other company and product names mentioned are used only for identification purposes and may be trademarks or registered trademarks of their respective companies.

Contents

Chapter 1

Installation 1

Chapter 2

Getting Started 9

Chapter 3

Firewall Profiles 27

Chapter 4

Alerting and Monitoring 103

Scheduling Reports 241

Chapter 8

Monitoring Activity 281

Chapter 9

Options 287

About This Book and the Library

The *User Guide* provides conceptual information about the NetIQ Firewall Suite product (Firewall Suite). This book defines terminology and various related concepts.

Intended Audience

This book provides information for individuals responsible for understanding Firewall Suite concepts.

Other Information in the Library

The library provides the following information resources:

Firewall Configuration Guide

Provides information about configuring your firewall to work with NetIQ firewall security applications

Help

Provides context-sensitive information and step-by-step guidance for common tasks, as well as definitions for each field on each window.

Conventions

The library uses consistent conventions to help you identify items throughout the documentation. The following table summarizes these conventions.

Convention	Use
Bold	• Window and menu items • Technical terms, when introduced
Italics	• Book and CD-ROM titles • Variable names and values • Emphasized words
`Fixed Font`	• File and folder names • Commands and code examples • Text you must type • Text (output) displayed in the command-line interface
Brackets, such as [value]	• Optional parameters of a command
Braces, such as {value}	• Required parameters of a command
Logical OR, such as value1 | value 2	• Exclusive parameters. Choose one parameter.

About Marshal

Marshal's Content Security products (MailMarshal for SMTP, MailMarshal for Exchange , WebMarshal, Security Reporting Center and Firewall Suite) deliver a complete email and Web security solution to a variety of Internet risks. They provide comprehensive protection by acting as a gateway between an organization and the Internet. It allows organizations to restrict, block, copy, archive, and automatically manage the sending and receiving of messages.

Marshal Products

Marshal's Content Security solution, which includes MailMarshal SMTP, MailMarshal for Exchange and WebMarshal, delivers a complete email and Web security solution to these risks by acting as a gateway between your organization and the Internet. The products sit behind your firewall but in front of your network systems to control outbound documents and their content. By providing anti-virus, anti-phishing and anti-spyware protection at the gateway, Marshal's Content Security solution offers you a strategic, flexible and scalable platform for policy-based filtering that protects your network, and as a result, your reputation.

Contacting Marshal

Please contact us with your questions and comments. We look forward to hearing from you. For support around the world, please contact your local partner. For a complete list of our partners, please see our Web site. If you cannot contact your partner, please contact our Technical Support team.

Telephone:	+44 (0) 1256 848 080 (EMEA)
	+1 404 759 2890 (Americas)
	+ 64 9 984 5700 (Asia-Pacific)

Sales Email: info@marshal.com
Support: www.marshal.com/support
Web Site: www.marshal.com

Chapter 1
Installation

For security and performance reasons, we recommend that you install Firewall Suite on a workstation other than the one running the firewall or proxy server software. We also recommend that you do not install Firewall Suite on a Primary Domain Controller (PDC) or Backup Domain Controller (BDC).

This chapter covers topics related to installing your Firewall Reporting solution, including:

- System requirements
- Steps for installing and uninstalling the software
- Considerations when installing the Alerting and Monitoring module
- Product license and registration
- Addition of firewall licenses

System Requirements

The following is a list of *minimum* system requirements for the computer running Firewall Suite:

- Microsoft Windows NT 4.*x*, Windows 2000, or Windows XP
- 1.0 GB available disk space
- 512 MB RAM

  More disk space and memory may be required to analyze large log files. Contact your Product Support representative for more information.
- Microsoft Office 97 or later (if you plan to use Microsoft Word or Excel reports)
- Internet Explorer 4.0 and higher or Netscape Navigator 4.5 and higher

Installing Firewall Suite

Note
Although you do not need to provide license information to install Firewall Suite, you must do so before you can run the application. See "License and Registration" on page 5 for details.

The installation uses a straightforward setup program. Choose the procedure that best suits your needs.

Installing from the Autorun

Use this procedure if your system is set up to run CD-ROMs automatically when you place them in the drive

To install Firewall Suite:

1. Insert the program CD into your CD-ROM drive to launch the setup program.
2. Follow the on-screen instructions to install the program.

Installing from the Run Dialog Box

Use this procedure to start the installation program manually.

To install Firewall Suite:

1. Insert the program CD into your CD-ROM drive, and then choose **Run** from the File or Start menu.
2. In the Run dialog box, type:

   ```
   d:\setup
   ```

   where *d:* is the letter of your CD-ROM drive.
3. Follow the on-screen instructions to install the program.

Software License Agreement

Before the program files are copied to your system, the Software License Agreement is presented.

- ***If you agree to the stated terms***, click **Accept**.
- ***If you do not agree***, click **Cancel** to exit the setup program without installing.

Registering your Software

If you installed Firewall Suite from a CD-ROM you purchased, you can register your product online. If you purchased the product online, your registration is recorded automatically. Registration allows you to access technical support and ensures that you receive information about new releases of the product and other benefits.

To register your product:

1. Install Firewall Suite and then start it from either the **Start > Programs** menu or your WebTrends Firewall Suite desktop shortcut icon. Instructions for installing the product accompany the installation wizard.
2. From the Help menu of the product Main Console, select **Registration**. The product will start your Web browser, then connect to the NetIQ customer service Web site.
3. Complete the registration information requested at the site.

Note
If you do not register when you install Firewall Suite, you can register later by opening the Help menu and selecting Registration.

Uninstalling Firewall Suite

You can uninstall the program from the Windows Control Panel.

License and Registration

When you download Firewall Suite from the Web site and run Setup for the first time, choose one of the following options in the first installation wizard panel:

- *Install a free time-limited trial.* During a limited trial, you may use the product free of charge to create profiles and run reports on your own log files for a period of 14 days. After that period expires, you must purchase the product to continue to create profiles or run reports. If you do not, the product runs in a limited demonstration mode, which restricts you to creating reports only for the sample profiles provided.
- You will need to register for a trial code in order to use Firewall Suite in its trial mode. See “Trial Mode” on page 5 for details.
- *Install purchased software.* Purchasing the product gives you a license to create profiles and run reports on your own log files without restrictions. You will need to supply purchase information online, via telephone or fax, or by mail. NetIQ will issue you a product serial number, which you can use to enable a full license for the product. See “Purchasing Firewall Suite” on page 6 for details.
- *Upgrade current product.* If you have a previous version of Firewall Suite installed on your system, use this option to install a current product version. Setup will detect any previous product licenses you have, or you may enter a product serial number during installation.

Trial Mode

If you selected the **Install a free time limited trial** option in the first wizard installation panel and then completed the remaining installation steps, Setup starts Firewall Suite and displays the Product Licensing dialog box.

To run the product in trial mode:

1. Click **Register for a Trial Serial Number**. Firewall Suite opens the NetIQ customer service Web site.
2. Complete the Registration form, then click **Submit**. Your trial code is shown in the browser window and is sent to the email address you specify in the registration form.
3. Copy your trial code.
4. Return to the Product Licensing dialog box and paste the code you copied into the text box provided.
5. Click **Submit**. Your trial mode registration is complete.

Purchasing Firewall Suite

If you selected the **Install purchased software** option in the first wizard installation panel, but did not enter a product serial number in the next panel, Setup will install Firewall Suite without a serial number. When you next start the product, the Product Licensing dialog box opens.

To purchase the product you downloaded:

1. Click **Purchase Information**. Firewall Suite starts your Web browser, then connects you to the NetIQ customer service Web site.
2. Complete the purchase information required at the site. When you have finished, you will receive a serial number for Firewall Suite.
3. Copy the serial number.
4. Return to the Product Licensing dialog box, then paste the serial number you copied into the text box provided.
5. Click **Submit**. You can now run the product under a full license, without restrictions.

Adding More Firewall Licenses

The standard software license lets you install Firewall Suite on one system and report on one firewall. If you want to report on more than one firewall, you must purchase Firewall Add-Ons. For example, if you purchased a three-firewall Add-On, you could install Firewall Suite on one system and report on a total of four firewalls. You can purchase Firewall Add-Ons by contacting NetIQ or your reseller.

Chapter 2

Getting Started

This chapter tells you what capabilities Firewall Suite offers your organization. You will learn the components of the user interface and how to create your first firewall activity report by using a sample profile to generate a report. In addition, you will set up monitors and alerts and run reports based on these settings.

Creating Firewall Reports

Firewall Suite enables you to accomplish two basic reporting tasks:

- Produce firewall and Web activity reports that detail security violations, protocol usage distribution, bandwidth usage, employee Web surfing habits, incoming and outgoing traffic, FTP transfers and more.
- Set up monitors and alerts and report on them. When a device goes down or stops responding, or when a critical security event is detected at your firewall, Firewall Suite can alert you to these events. Customize alerts to notify you when the number of times an event occurs over a specific time period has exceeded your defined threshold.

Many other capabilities fall within these two high-level capabilities, but these more detailed features will be discussed in later chapters.

Producing Firewall and Web Activity Reports

Creating a firewall report requires that you:

1. Configure your firewall to produce log files that may be accessed and used by Firewall Suite.
2. Create a profile to define the information you want to capture in your report.
3. Generate a report either on-demand or by scheduling a reporting event.

The following section discusses these three steps in detail.

Configuring Your Firewall

Most firewalls generate log files that contain data about the activity occurring around the firewall. Firewall Suite uses these log files to capture, analyze and report on firewall activity; however, you need to configure your firewall properly to enable Firewall Suite to access and get the most from your firewall log files. The *Firewall Configuration Guide* provides this information on a firewall-by-firewall basis.

The configuration guide includes information about:

- Which versions of your firewall are supported by Firewall Suite
- Where the logs are located and how to retrieve or access them
- How to optimize your firewall log format to display the information you want in reports

The printed guide is included with your purchase, but you may also download and view it in Adobe® Acrobat® Reader version 4.0 or greater by visiting www.netiq.com\support. Make sure the cover of the guide you download specifies Firewall Suite.

Understanding Firewall Log Files

Depending on which application protocols your firewall is configured to handle, your firewall log files may contain a variety of different information. For example, it could contain information about users, the protocols they used, what activity they generated, their system platforms, the search engine they used, keywords on which they searched, date and time information and more. To create a profile and generate a meaningful report on your firewall activity, you must determine which type and version of firewall you have, how the activity information is recorded in the log file, and how you can retrieve that log file.

For example, if Firewall Suite relies on FTP, HTTP, or Syslog/LEA service access to retrieve log files, there will be an issue with firewalls that do not allow these types of access. If this issue is recognized ahead of time, a workaround can be developed, such as making a copy of the log file on another server for use with Firewall Suite.

The WebTrends Syslog Service

Many of the firewall log file formats supported by Firewall Suite support the WebTrends Syslog Service, a service that gets firewall log files in a consistent format that is usable by Firewall Suite. For more information, see the *Firewall Configuration Guide*.

Create a Profile

A profile is a group of settings that defines the location of your firewall log file and the type of information you wish to capture from it and include in reports. Specifically, it contains the information needed to import, process and store log files for analysis.

The three types of firewall and Internet activity profiles are:

- *General Firewall Activity profiles*. Let you produce reports on firewall and VPN security-related activity, including bandwidth and protocol usage, firewall rules, and firewall errors and warnings.
- *Incoming Firewall Activity profiles*. Help you analyze the Web activity coming through the firewall from external sources. Information in reports includes top requested pages; least requested pages; top paths through the site; and visitors by domain, geography, organization, browser, and operating system.
- *Outgoing Firewall Activity profiles*. Let you analyze the Web activity originating from within your network. Reports include bandwidth usage by user or department, Web sites visited by IP address, search engine keywords used, and authenticated user

Note
Different firewalls support different types of firewall and Web activity reporting. For more information, see the *Firewall Configuration Guide*.

Generate a Report

Firewall Suite lets you tailor the appearance of your reports by letting you choose the graphs and tables to include and the colors, fonts, layouts and text to use. Tables and graphs are organized under expandable categories in HTML. See “Working with Reports” on page 201 for information on generating and customizing reports.

Reports output to multiple HTML files, which allows for smaller file sizes—exactly how much smaller depends on the tables and graphs included. These smaller-sized files simplify printing and speed download times over slow connections.

You may also use the Scheduler to automate the generation of reports that you run regularly. See “Scheduling Reports” on page 241 for details.

Alerting and Monitoring

Firewall Suite's Alerting and Monitoring capability lets you:

- Monitor Web-related devices and services
- Send alerts when something goes wrong with a Web-related device or service
- Automatically restore Web-related devices and services when something goes wrong
- Run reports on the status and health of Web-related devices and services

The Alerting and Monitoring profiles you create define the devices and services you want to monitor and the type of response you want to occur when the status of a monitored device or service changes.

For more information, see "Alerting and Monitoring" on page 103.

Starting Firewall Suite

You can open the Main Console of Firewall Suite in any of these ways:

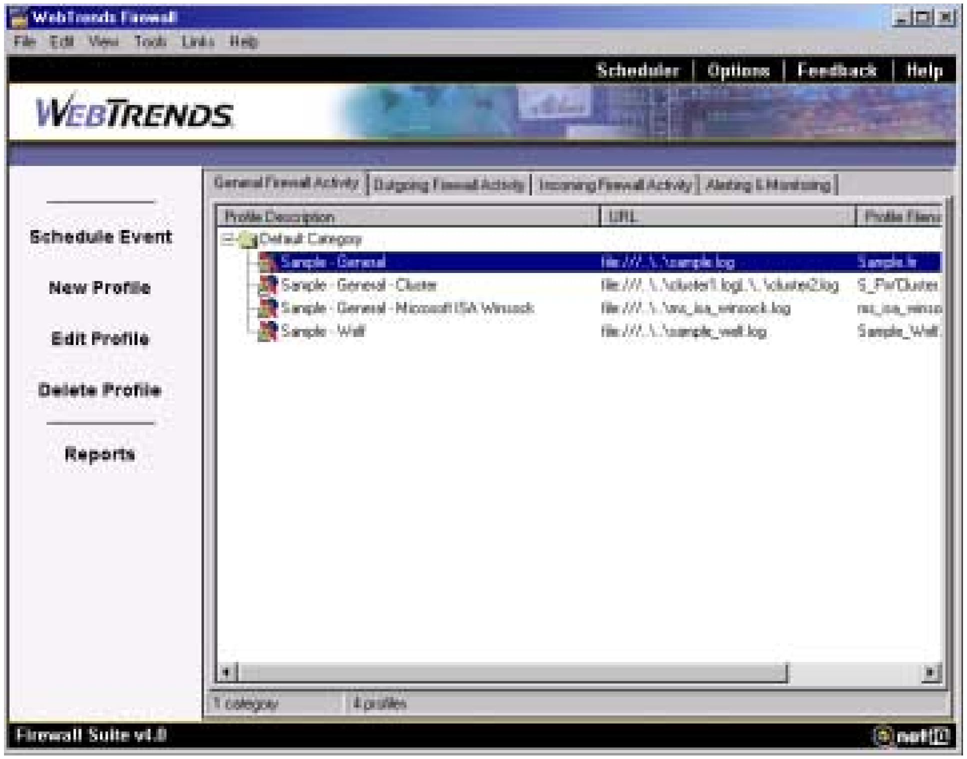
- Double-click the WebTrends Firewall Suite shortcut icon on your desktop
- Select **WebTrends Firewall Suite > WebTrends Firewall Suite** from the **Start > Programs** menu on your desktop
- Double-click `wt_firewall.exe` from the program group in the top level of Firewall Suite installation directory

The Main Console

The Main Console of Firewall Suite is the first window you see after starting the software. It contains five main areas:

- *Profile Description list*. Lists existing profiles, including sample profiles.
- *Tasks area*. Initiates common tasks such as profile creation and event scheduling.
- *Functions area*. Scheduler, Options, Feedback, and Help
- *Main menu*. File, Edit, etc.
- *Profile Type tabs*. General Firewall Activity, Outgoing Firewall Activity, etc.

The following figure shows the Main Console of Firewall Suite.


WebTrends Firewall
File Edit View Tools Links Help
Scheduler | Options | Feedback | Help
WEBTRENDS
Schedule Event
New Profile
Edit Profile
Delete Profile
Reports
General Firewall Activity
Outgoing Firewall Activity
Incoming Firewall Activity
Alerting & Monitoring
Firewall Suite v4.0
netIQ

Profile Description	URL	Profile Filena
Default Category		
Sample - General	file:///..\..\sample.log	Sample.fr
Sample - General - Cluster	file:///..\..\cluster1.log|..\..\cluster2.log	S_FwCluster
Sample - General - Microsoft ISA Winsock	file:///..\..\ms_isa_winsock.log	ms_isa_winso
Sample - Wall	file:///..\..\sample_wall.log	Sample_Wall.

1 category 4 profiles

Profile Description List

Click one of the four Profile Type tabs: General Firewall Activity, Outgoing Firewall Activity, Incoming Firewall Activity or Alerting & Monitoring. For each tab, you see a list of the profiles available for running reports. This list includes sample profiles for each profile type, and if you already created profiles for an earlier version of Firewall Suite, these are automatically placed in the Default Category folder of the appropriate profile type.

The list contains folders, called categories, containing profiles. Each profile has an associated Profile Description column and other columns, depending on the selected profile type. Click any column heading to sort the list in alphabetically and numerically descending order (A, B, C... and 1, 2, 3...) according to the heading clicked.

For example, if you click the Incoming Firewall Activity tab, you will see the Profile Description called “Sample - Incoming” in the Default Category folder along with any other previously created Incoming Firewall Activity profiles. Beyond sorting the list of Profile Descriptions, there are other tasks you can perform on the Profile Description list.

Hiding or Showing Columns

When a profile description is so long that it can’t display fully in the Profile Description column, you can hide the other columns to make room.

To hide or show columns:

1. Choose **Select Columns** from the View menu. The Select Columns dialog box displays.
2. Select a column check box to display the column, or clear the check box to hide the column. The Profile Description column cannot be hidden.
3. Click **OK**.

Organizing Profiles into Category Folders

You can organize your profiles using category folders. When you install Firewall Suite, the only category you have for each profile type is the Default Category. You can create, rename and delete these category folders as needed.

To create a new category:

1. Select **Category** from the File menu.
2. Type the new Category name and click **OK**.

To rename a category:

1. Select the category to rename.
2. Select **Rename** from the File menu.
3. Type the new Category name and click **OK**.

To delete a category:

1. Select the category to delete.
2. Select **Delete** from the Edit menu.
3. Type the new Category name and click **OK**.

Tasks Area

The tasks area, located along the left side of the Main Console, contains the features needed to manage, schedule an event for and generate reports on a selected profile.

- *Schedule Event*. Click this to open the Scheduler and the New Scheduled Event - Analysis wizard. The Scheduler displays profile reports that have been set up to run automatically. You can edit existing scheduled events in this window, or schedule automated events for additional profiles.
- *New Profile*. Click this to open the New Profile wizard and create a new profile in the selected profile type and category folder.
- *Edit Profile*. Click this to display a dialog box in which you can make changes to the selected profile.
- *Delete Profile*. Click this to delete the selected profile.
- *Reports*. Click this to open a list of available, pre-defined reports for the selected profile type. You can add, edit, rename or delete the available reports within this dialog box and you can choose what output format in which to create the report: HTML, Microsoft Word, Microsoft Excel, comma-delimited text, or text. You can also select a report and view a previously generated version of it or generate a report on-demand.

Main Menu

The Main menu contains the following items:

File Menu

- *Generate Report*. Accomplishes the same functionality as mentioned for Reports in the “Tasks Area” on page 17.
- *New Profile*. Accomplishes the same functionality as mentioned for New Profile in the “Tasks Area” on page 17.
- *New Category*. Lets you create a new category folder in the selected Profile Type and/or selected category folder by opening the Category Name dialog box.
- *New Report*. Opens up the New Report wizard, in which you define the report range, report format, location at which to save the report, report style and report content for a new report template. This template gets added to the list of available reports, and may be used with an appropriate profile.
- *Rename*. Lets you rename the selected category folder or profile.
- *Schedule Event for Profile*. Accomplishes the same functionality as mentioned for Schedule Event in the “Tasks Area” on page 17.
- *Open File/Saved Report*. Lets you open an existing report through a Windows Explorer-like interface.
- *Close*. Closes the program window, but the application continues to run, including any scheduled reports and real-time analysis.
- *Exit and Unload*. Shuts down the application and any automated processes, including the Scheduler and real-time analysis.

Notes

Many Main Menu tasks are also available through right-click functionality.

Edit Menu

- *Profile*. Accomplishes the same functionality as mentioned for Edit Profile in the “Tasks Area” on page 17.
- *Cut*. Allows you to cut a profile or category folder, which can later be pasted in another folder or directly under the root of the Profile Descriptions list.
- *Copy*. Allows you to copy a profile, which you can rename and edit as needed.
- *Paste*. Lets you paste a profile that was previously cut. This is useful if you want to move a profile from one folder to another within the Profiles Description list.
- *Delete*. Accomplishes the same functionality as mentioned for Delete Profile in the “Tasks Area” on page 17.

View Menu

- *Collapse All Categories*. Collapses category folders to show just the folders, not the profiles contained within them.
- *Expand All Categories*. Expands all category folders so that you can see the profiles in each.
- *Select Columns*. Lets you choose which columns to hide or show in the Profile Description list.
- *Align Columns*. Adjusts columns to show the maximum amount of information possible per column.
- *Auto Refresh Profile List*. Updates the profiles list with the most current information.
- *Print Profile List*. Prints the list of profiles as it appears on-screen (expanded or collapsed).

Tools Menu

- *Scheduler*. Opens the Event Scheduler main console.
- *Style Editor*. Opens the Style wizard, which lets you change the style of a selected available report style, or lets you create a new report style and add it to the list of available report styles. The Style Editor lets you change the colors, fonts, descriptive text, graph appearances and more for the reports you generate.
- *FastTrends Maintenance*. Lets you manage the contents of the FastTrends database associated with a given profile.
- *URL Categorization (Outgoing Firewall Activity profiles only)*. Opens the URL Categorization Databases dialog box, which lets you register or update the SurfControl databases available for use with Firewall Suite. Use these databases to track Web surfing activity of inappropriate Web content.
- Status of LEA Connections. Lets you check the status of connections between the WebTrends LEA Service and a Check Point Management Server.
- *Limit Memory Usage*. Lets you to limit the number of elements included in a specific section of a report to reduce memory consumption.
- *Department Management*. Lets you create, edit or delete departments by IP addresses. This feature allows you to later report on the activity for a specific department, or to break down activity by departments.
- *Options*. Opens the Options dialog box, which controls global options as well as options that affect only the Firewall Activity or the Alerting & Monitoring module.

Links Menu

- *GeoTrends Information*. Links you to a Web page from which you may download GeoTrends, an optional, free database that provides location information about Web visitors and companies for your reports.
- *Customer Feedback*. Opens a Web page in which you may enter your comments about NetIQ's WebTrends brand of products.
- *Contact Technical Support*. Links you to the technical support page, in which you may enter any technical questions you have about Firewall Suite.
- *Frequently Asked Questions*. Links to a page of the questions most commonly encountered by technical support.
- *Purchase Technical Support*. Opens a page on which you can learn about and compare our three technical support packages.
- *Purchase Additional Licenses*. Links to a page from which you can purchase additional licenses for Firewall Suite. You may also use the contact information to order from a WebTrends sales representative or reseller.

Help Menu

- *Contents*. Opens the Firewall Suite online Help.
- *Add Serial Numbers*. Opens the dialog box in which you may enter the serial number for a Maintenance Subscription or a Server Add-On License.
- Ch*eck for Product Updates*. Runs a utility that lets you know if your Firewall Suite version is most current available version. You must have registered your product for this utility to provide accurate information.
- *View Release Notes*. Opens the latest copy of the product Release Notes.
- *View Product License*. Displays the license agreement you accepted when you installed Firewall Suite.
- *About*. Displays information such as Firewall Suite Version number, the number of Firewall Add-Ons and more.

Functions Area

The Functions area contains the following items:

- *Scheduler*. Opens the Event Scheduler.
- *Options*. Opens the Options dialog box
- *Feedback*. Links to the Customer Feedback page (see “Links Menu” on page 21).
- *Help*. Opens the Firewall Suite online Help.

Profile Type Tabs

The Profile Type tabs include:

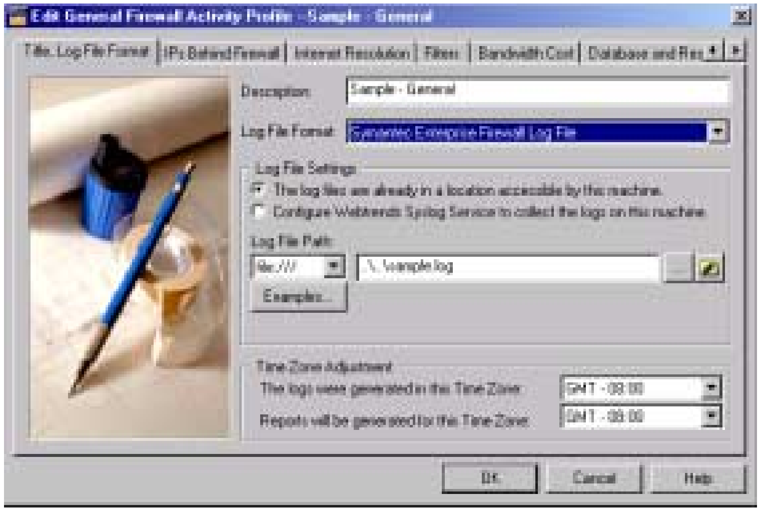
- *General Firewall Activity*. Report on security related issues including email activity, FTP transfers, and Telnet connections. You can also track bandwidth usage and VPN activity. Identify large data transfers, failed connection attempts by IP, the source that triggered firewall rules and other suspicious activity.
- *Outgoing Firewall Activity*. Pinpoint where the employees in your organization are going on the Internet and how much time they’re spending there. You can report on all the IP addresses to perform an organizational analysis, or focus on just one IP address to report on an individual’s activity.
- *Incoming Firewall Activity*. If your Web server is behind your firewall, use Incoming Web Activity profiles to report on traffic coming into your Web site, including the volume of activity on your site, where users are coming from, and what pages interest them most.
- *Alerting & Monitoring*. Monitor any networked or Internet-connected device or service and receive alerts whenever a device goes down or automate actions to take when specific events occur.

Reports Using a Sample Profile

In this section, you will use a sample profile included with the installation to create a report. Use the sample Incoming Firewall Activity profile called “Sample – Incoming”.

To create a report using the Sample – Incoming profile:

1. From the Main Console, click the **Incoming Firewall Activity** tab.
2. Select the profile called “Sample – Incoming”.
3. Review the profile’s settings by clicking **Edit > Profile** from the Main menu. The Edit Incoming Firewall Activity Profile dialog box opens.



Description: Sample - General

Log File Format: Symantec Enterprise Firewall Log File

Log File Settings

● The log files are already in a location accessible by this machine.

○ Configure Webtrends Syslog Service to collect the logs on this machine

Log File Path: file:/// .\..\sample.log

Time Zone Adjustment

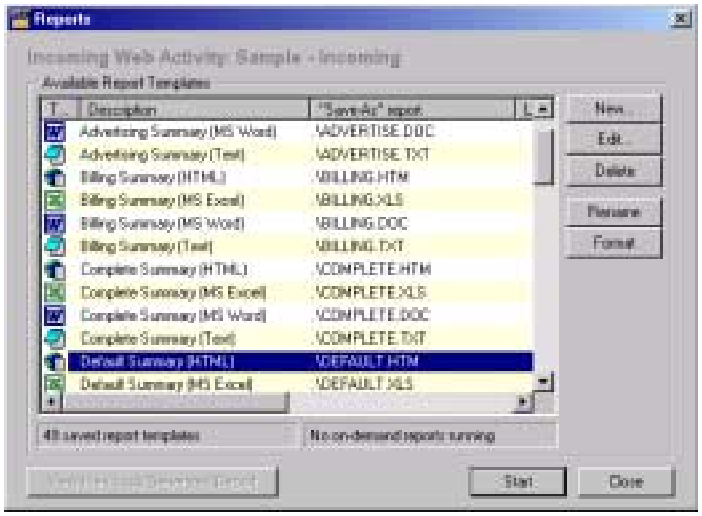
The logs were generated in this Time Zone: GMT -08:00

Reports will be generated for this Time Zone: GMT -08:00

4. Select any tab within the Edit Incoming Firewall Activity Profile dialog box to review the profile settings for the individual tabs. You can also modify profile settings within this dialog box. For more information about each setting in this dialog box, see “Firewall Profiles” on page 27.
5. Click **Cancel** to close the dialog box without making any changes.

6. Reselect the sample profile from the Profile Description list.

7. Generate a report for this profile by clicking **File > Generate Report** from the Main menu. The Reports dialog box opens.



Reports

Incoming Web Activity: Sample - Incoming

Available Report Templates

T...	Description	"Save-As" report
W	Advertising Summary (MS Word)	\ADVERTISE.DOC
	Advertising Summary (Text)	\ADVERTISE.TXT
	Billing Summary (HTML)	\BILLING.HTM
X	Billing Summary (MS Excel)	\BILLING.XLS
W	Billing Summary (MS Word)	\BILLING.DOC
	Billing Summary (Text)	\BILLING.TXT
	Complete Summary (HTML)	\COMPLETE.HTM
X	Complete Summary (MS Excel)	\COMPLETE.XLS
W	Complete Summary (MS Word)	\COMPLETE.DOC
	Complete Summary (Text)	\COMPLETE.TXT
	Default Summary (HTML)	\DEFAULT.HTM
X	Default Summary (MS Excel)	\DEFAULT.XLS

48 saved report templates

No on-demand reports running

For this example, just use the default settings for the report.

8. Click **Start** to generate the report. The report compiles and then opens.

Using Shortcuts

Firewall Suite includes a number navigational shortcuts.

Many Main Menu tasks are also available from the right-click menu. For example, to view a list of menu selections for a profile, select the profile in the Profile Description list and right-click. You can use right-click functionality to:

- Create a new category, profile, scheduled event or report.
- Edit a selected profile

- Generate a report
- Manage profiles.
- Collapse, expand, select, and align the columns in the Profile Description list.
- Print and refresh the profile list.
- Close or exit and unload the Firewall Suite application and its services.

In the Reports window, you can use right-click functionality to:

- Create, edit, rename, delete, start and format a report
- View a previously generated report
- Align and select columns
- Print a list of available reports

Chapter 3
Firewall Profiles

This chapter explains the various settings available for creating firewall and Web activity profiles. Firewall Suite produces a report on the data in your firewall or proxy server log files according to how these settings are configured. Profile settings specify:

- The hardware configuration of your firewall, which includes the firewall or proxy server and the computers behind your firewall.
- The location, format, and method for retrieving the log file data.
- The information from the log file you want to include in a report.
- The storage of log file analysis for future use.

Tables referenced in this chapter are included at the end of the chapter.

Alerting and Monitoring profiles use different settings. They are described in "Alerting and Monitoring" on page 103.

Notes

You may need to configure your firewall or proxy server before creating a firewall or Web activity profile. For more information, see the *Firewall Configuration Guide*.

Profile Types

The tabs in the Main Console correspond to the types of profiles you can create. These include:

- **General Firewall Activity**. Use these profiles to report on security-related issues, such as failed connection attempts by IP, firewall rules that were triggered, firewall warnings and errors and other suspicious activity. You can also track bandwidth usage, email activity, FTP transfers and Telnet connections.
- **Outgoing Firewall Activity**. Use these profiles to determine and generate reports on employee Internet surfing habits. In addition, these profiles let you report on all the IP addresses for an organization, or focus on just one IP address to report on an individual's activity.
- **Incoming Firewall Activity**. If your Web server is behind your firewall, use these profiles to report on traffic coming into your Web site from the outside, including the volume of activity on your site, where users are coming from and what pages interest them most.

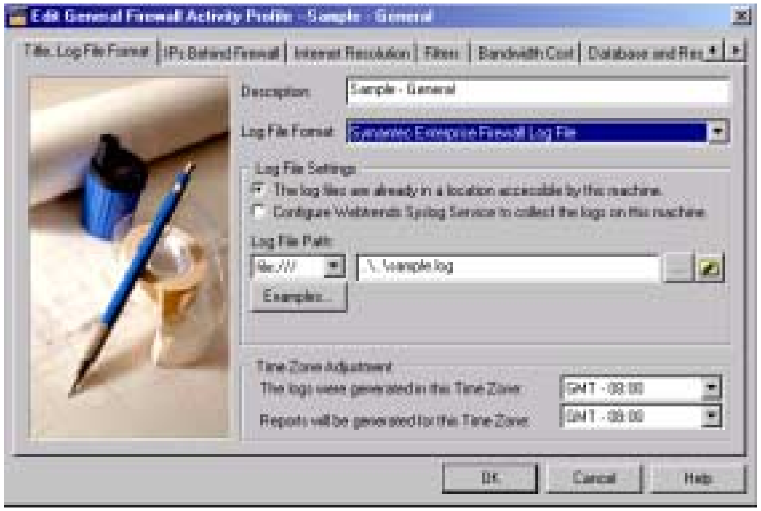
Viewing a Sample Profile

Firewall profiles have numerous settings. Before creating a profile for the first time, it may be helpful to look at the settings for some of the sample firewall activity profiles included in your Firewall Suite installation.

- *Sample - General*, a General Firewall Activity profile for a firewall on a single computer.
- *Sample - General - Cluster*, a General Firewall Activity profile for a firewall configuration spread across multiple computers.
- Sample - Outgoing, an Outgoing Firewall Activity profile or a firewall on a single computer.
- *Sample - Incoming*, an Incoming Firewall Activity profile for a firewall on a single computer.

To view a sample profile:

1. On the Main Console, select any of the three firewall activity tabs, **General Firewall Activity**, **Outgoing Firewall Activity** or **Incoming Firewall Activity**.
2. Select the profile that you wish to view from the Profile Description list.
3. From the Edit menu, click **Profile**. The Edit Firewall Profile dialog box opens. Use this dialog box to review or make changes to the selected profile's settings by selecting the individual tabs associated with each profile.



Description: Sample - General

Log File Format: Symantec Enterprise Firewall Log File

Log File Settings

● The log files are already in a location accessible by this machine.

○ Configure Webtrends Syslog Service to collect the logs on this machine.

Log File Path: file:/// ..\..\sample.log

Time Zone Adjustment

The logs were generated in this Time Zone: GMT -08:00

Reports will be generated for this Time Zone: GMT -08:00

Choosing a Firewall Profile Type

You need two pieces of information when deciding which of the three Firewall profile types to use to create the report you want.

- *The profile types supported by your firewall or proxy server.*

  Note
  Some firewalls and proxy servers do not support all the capabilities available with Firewall Suite. For more information about your firewall or proxy server, see the Firewall Configuration Guide.

  For detailed information on designing Firewall Activity profiles, see “Designing Firewall Profiles” on page 99.

- *The log file information that you want to include in the report.* See “Report Content” on page 99 for more information about what content can be included in a report, how that information can be reported, and the profile type you should use to generate the report.

Creating a Firewall Profile

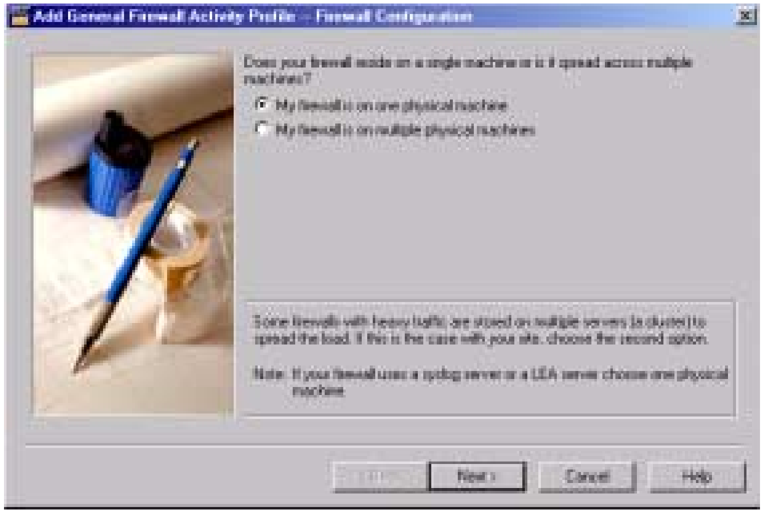
This procedure describes the sequence of panels in the New Profile wizard for creating a firewall profile. It describes the information required in each panel to set up a firewall profile. Refer to the online help in each panel for more information.

To create a new firewall profile using the New Profile wizard:

1. Select a firewall profile type from the profile type tabs on the Main Console. Make your decision based on the type of firewall you have, and the type of information on which you wish to report.
2. From the File menu or the Tasks area select **New Profile**. The New Profile wizard opens to the Firewall Configuration dialog box.

Firewall Configuration Dialog Box

The Firewall Configuration dialog box lets you specify whether your firewall is on one computer or distributed across multiple computers. A firewall or firewalls may be spread across multiple computers to distribute the work load for sites that experience high traffic volumes.


Add General Firewall Activity Profile -- Firewall Configuration
< Back
Next >
Cancel
Help

Does your firewall reside on a single machine or is it spread across multiple machines?

● My firewall is on one physical machine

○ My firewall is on multiple physical machines

Some firewalls with heavy traffic are stored on multiple servers (a cluster) to spread the load. If this is the case with your site, choose the second option.

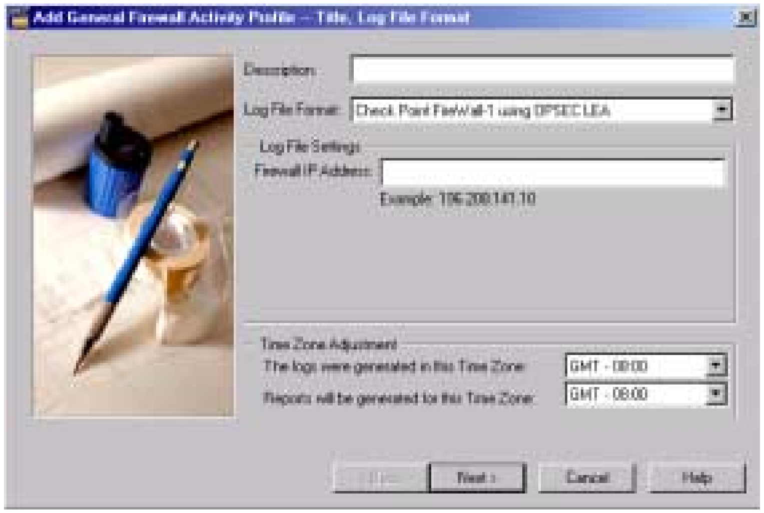
Note: If your firewall uses a syslog server or a LEA server choose one physical machine.

To specify your firewall configuration:

1. Choose one of the following two options depending on your circumstances:
   - ***If your firewall resides on one computer***, select **My firewall is on one physical machine**.
   - ***If your firewall resides on multiple computers***, select **My firewall is on multiple machines**.
2. Click **Next**. Depending on the selection you made in Step **1**, the Title, Log File Format or the List of Servers dialog box opens. The next set of instructions will continue with creating a profile for a firewall on a single computer.
3. To continue creating a profile for a firewall on multiple computers, see “List of Servers Dialog Box” on page 40.

Title, Log File Format Dialog Box

If your firewall is on a single computer, use the Title, Log File Format dialog box to name the profile and specify the log file format and path. You also have the opportunity to use the built-in WebTrends Syslog Service, a Windows service that makes firewall log files accessible by converting them into a consistent log file format. For more information about the WebTrends Syslog Service, see “About the WebTrends Syslog Service” on page 37.



Add General Firewall Activity Profile -- Title, Log File Format

Description:

Log File Format: Check Point FireWall-1 using OPSEC LEA

Log File Settings

Firewall IP Address:

Example: 196.208.141.10

Time Zone Adjustment

The logs were generated in this Time Zone: GMT - 08:00

Reports will be generated for this Time Zone: GMT - 08:00

To specify the profile log file settings for a firewall on a single computer:

1. In the **Description** text box, enter the name you wish to call your profile.
2. In the **Logs were generated in this Time Zone** dropdown list, select the time zone, in comparison to Greenwich Mean time (GMT), in which the log files are generated. For example, if your firewall is located in the Pacific Time Zone, select **GMT -08:00** because this zone is eight hours behind Greenwich Mean Time.
3. In the **Reports will be generated for this Time Zone** dropdown list, select the time zone for which reports for this profile will be generated. For example, while you may work in the Pacific Time Zone, the reports you generate may be destined for your Paris offices. Because Paris is one hour ahead of GMT, select **GMT +01:00**.
4. In the **Log File Format** area, which lists the firewalls supported by the selected Profile Type tab, select the firewall type and the format of your firewall's log files.

   Note
   The options and fields available in the lower half of the dialog box vary depending on the format you select.

5. ***If you selected a Check Point firewall with OPSEC LEA***, skip to "Check Point LEA Instructions" on page 36.
6. ***If you are using any other firewall or log file format***, continue with the following steps.

7. ***If you want to use logs that are accessible by the Firewall Suite computer***:

   a. Select **The log files are already in a location accessible by this machine**.

   b. Select the firewall log file retrieval method from the dropdown list in the Log File Path area. For firewalls on a single computer, Firewall Suite supports `file:\\\`, `ftp:\\` or `http:\\`. For more information on selecting the appropriate retrieval method, see “Log File Retrieval Methods” on page 38.

   c. Enter or browse to the location of your log file in the text box to the right of the log retrieval method. For more information on using Firewall Suite’s browse features, see “Specifying a Single Log File” on page 82 and “Specifying Multiple Log Files” on page 82.

8. *If you want to use the WebTrends Syslog Service to collect your firewall log files*, use the following steps:

   a. Enter the IP address of your firewall in the **Firewall IP Address** text box.

   b. Enter or browse to the location in which the WebTrends Syslog Service should save the collected log files in the **Save Log Files To** text box.

Check Point LEA Instructions

If you selected Check Point LEA, you must choose a Check Point OPSEC LEA connection to collect the data. Check Point LEA Connections are configured using the LEA Connection options under General Firewall Activity Options. Before you can configure a LEA connection, you must configure your Check Point firewall to work with OPSEC LEA. For more information,see the *Firewall Configuration Guide*.

If you are using a Check Point firewall with OPSEC LEA:

1. Make sure you selected the correct Check Point firewall type from the Log File Format list.
2. ***If no connections have been configured***, click **Create or Manage Connections** to open the Manage Connections dialog box, and follow the instructions for creating a new OPSEC LEA connection on page “LEA Connections Dialog Box” on page 334.
3. ***If one or more connections have been configured***, select a connection from the list.

About the WebTrends Syslog Service

Your firewall must be configured to use the WebTrends Syslog Service. Refer to the *Firewall Configuration Guide* for information about configuring your firewall.

Note
Because the WebTrends Syslog Service runs as a Windows service, you must run Firewall Suite on a Windows NT, Windows 2000, or Windows XP system and you must have administrator rights to configure Firewall Suite as a Windows service.

To make firewall log files accessible in a consistent log file format, the Syslog daemon of the WebTrends Syslog Service collects firewall log data from the firewall. The daemon then writes a log file in a usable format to an IP address on the computer running Firewall Suite. The log files created by the WebTrends Syslog Service are stored locally on the computer running Firewall Suite, and log files created by the firewall remain there.

The WebTrends Syslog Service standardizes the prefix of the firewall log records. In the following example, the part of the firewall record that is formatted by WebTrends Syslog Service appears in bold:

```
WTsyslog [2001-11-01 00:31:41 ip=192.168.9.1 pri=6] 304001
192.168.10.20 accessed URL 192.9.24.116:template/sunstyle.css
```

By default, the WebTrends Syslog Service is bound to the IP address on the computer running Firewall Suite where it writes log data. If the computer running Firewall Suite has more than one IP address, WebTrends Syslog Service binds to all IP addresses by default. We recommend that you do not bind the WebTrends Syslog Service to a single IP address unless absolutely necessary.

You can select the frequency with which log files are rotated in the Syslog dialog box of the General Firewall Activity section of the Options window. Log files are rotated when the current log file is archived and a new log is started.

Because the WebTrends Syslog Service collects data in real time, up-to-date logs are available for reporting. If the WebTrends Syslog Service is not running, however, any log data generated is lost.

When you create a profile that uses the WebTrends Syslog Service, the server is configured to start whenever the computer running Firewall Suite is started. The WebTrends Syslog Service will continue to run as long as the computer is running.

Log File Retrieval Methods

Firewall Suite supports the following retrieval methods:

- **file:///** (file retrieval). Select this option if you have a drive mapped to your firewall server. You can identify single, multiple, and compressed log files in one of three ways:
  - Type the complete log file path in the **Log File URL Path** text box.

    To specify multiple log files, use wildcards or use a vertical bar (|) between log file path names. For more information, see “Specifying Log Paths” on page 351.
  - Click **Normal Browse** to browse to the location of a single file.

  - Click **Extended Browse** to open the Selected Logfiles dialog box and specify multiple log files. See “Specifying a Single Log File” on page 82 and “Specifying Multiple Log Files” on page 82 for instructions and examples.

- **ftp://** (FTP retrieval). Select this option to retrieve your log file using FTP.

  a. Type the path and file name in the **Log File URL Path** text box, or click **Browse** to navigate to the log file location.When you specify an FTP URL, you must type the full path from the root of the FTP server.

  b. Type your user name and password for the FTP site.

- **http://** (HTTP retrieval). Select this option to retrieve your Web server log file over the Internet using HTTP.

  a. Type the path and file name in the **Log File URL Path** text box.

  b. If you are accessing a secure Web site, type the user name and password information. This is usually not required to access a Web server.

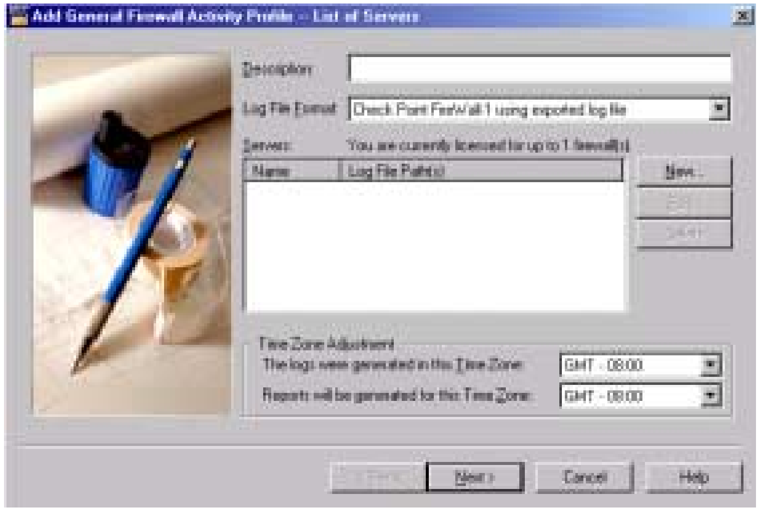
  See “Specifying a Single Log File” on page 82 and “Specifying Multiple Log Files” on page 82 for detailed instructions on using the browse features associated with each log retrieval method.

Note

ftp and http retrieval are only available for firewalls that use single servers. Clustered servers are assumed to have log files aggregated and stored in a single file location.

List of Servers Dialog Box

The settings in the List of Servers dialog box parallel the Title, Log File Format dialog box for firewalls on single servers, only they pertain to firewall configurations that have firewalls and log files on multiple servers. This may occur when network traffic is heavy, and firewalls need to spread the workload to multiple computers.



Description:

Log File Format: Check Point FireWall-1 using exported log file

Servers: You are currently licensed for up to 1 firewall(s)

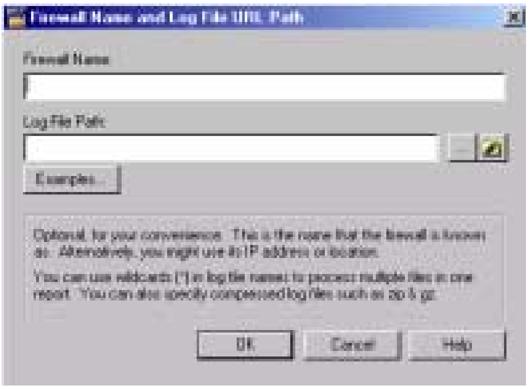
Time Zone Adjustment

The logs were generated in this Time Zone: GMT - 08:00

Reports will be generated for this Time Zone: GMT - 08:00

To specify the profile log file settings for a firewall on multiple computers:

1. In the **Description** text box, type the name you wish to call your profile.
2. In the **Logs originate in Time Zone GMT** dropdown list, select the time zone, in comparison to Greenwich Mean time (GMT), in which the log files are generated. For example, if your firewall is located in the Pacific Time Zone, this setting is eight hours behind Greenwich Mean Time, so you would select **GMT -08:00**.
3. In the **Report in GMT** dropdown list, select the time zone for which reports for this profile will be generated. For example, while you may work in the Pacific Time Zone, the reports you generate may be destined for your Paris offices, which is one hour ahead of GMT. Therefore, select **GMT +01:00**.
4. In the **Log File Format** area, which lists the firewalls supported by the selected Profile Type tab, select the firewall and log file type of your firewall configuration.
5. Click **New**, to add a server and the path to a log file or files for that server. The Firewall Name and Log File Path dialog box opens.



Optional, for your convenience. This is the name that the firewall is known as. Alternatively, you might use its IP address or location.

You can use wildcards (*) in log file names to process multiple files in one report. You can also specify compressed log files such as zip & gz.

6. In the **Firewall Name** text box, type the name for your firewall.

7. In the **Log File Path** text box, either type or browse to the location of the log file(s) for that firewall.

Note
Use wildcards (*) in log file names to process multiple log files in one report. You can also specify compressed log files such as zip or gzip.

8. Click **OK** to return to the List of Servers dialog box. The new server and path is added to the Servers list.
9. Click **Next**. The IPs Behind Firewalls dialog box opens.

Editing the Server List

To edit a server in the list:

1. In the **Server** list, select the server you wish to edit.
2. Click **Edit**. The Firewall Name and Log File URL Path dialog box opens.
3. Edit the server settings as needed and click **OK**.

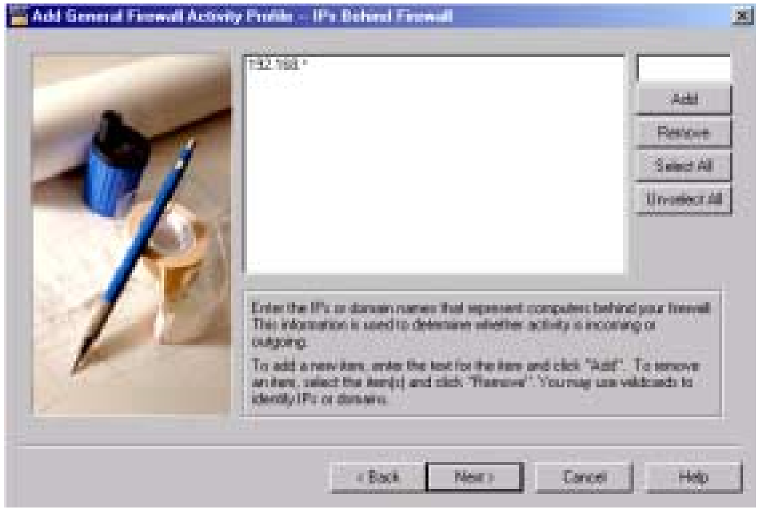
Deleting a Server from the List

To delete a server from the list:

1. In the **Server** list, select the server you wish to delete.
2. Click **Delete**. A confirmation message displays.
3. Click **Yes** to confirm the deletion. The selected server is deleted from the list.

IPs Behind Firewall Dialog Box

The IPs Behind Firewall dialog box allows you to specify the IP addresses or domains of computers located behind your firewall. The information in this dialog box tells Firewall Suite which computers are behind your firewall so it can distinguish between activity that originates inside the firewall (in other words, from within your organization) and activity that originates outside.


Add General Firewall Activity Profile -- IPs Behind Firewall
Add
Remove
Select All
Un-select All
< Back
Next >
Cancel
Help

192.168.*

Enter the IPs or domain names that represent computers behind your firewall. This information is used to determine whether activity is incoming or outgoing.

To add a new item, enter the text for the item and click "Add". To remove an item, select the item(s) and click "Remove". You may use wildcards to identify IPs or domains.

Adding an IP Address

To add an IP address to the list:

1. Enter an IP address or domain name in the text box above the **Add** button.

Note
You can use wildcards (*) to specify a group of IP addresses or domain names. For example, type `192.168.*` to indicate that all addresses that begin with `192.168.` are behind the firewall. Type the domain name `*.webtrends.com` to add all computers on the `webtrends.com` domain to the list. Adding `*.webtrends.com` includes all computers on `internal.webtrends.com` and `pdx.webtrends.com`.

2. Click **Add**. The contents of the text box are added to the list.
3. Click **Next**. The DNS Lookup dialog box opens.

Removing an IP Address

To remove an IP address or domain name from the list:

1. Select an IP address or domain name in the list.
2. Click **Remove**. The selected item is deleted from the list.

Selecting or De-selecting an IP Address

To select or de-select all IP addresses or domain names from the list:

- Click **Select All** to select all items in the list
- Click **Un-select All** to deselect any selected items in the list.

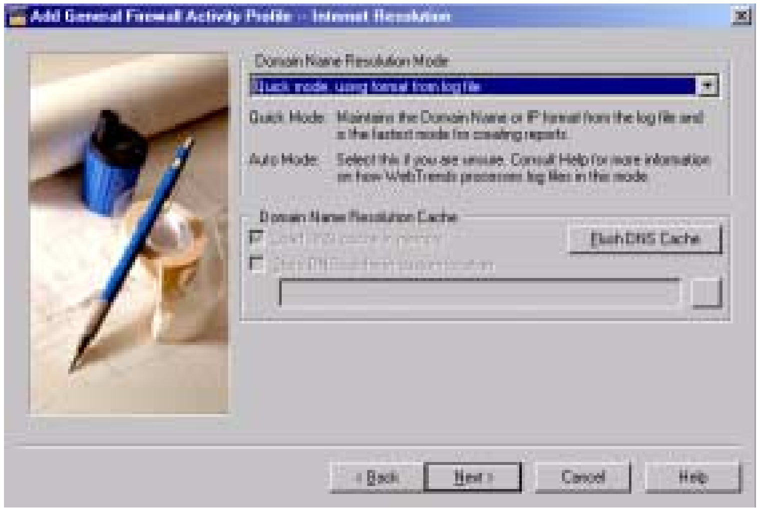
Internet Resolution Dialog Box

DNS lookup is the process of translating numeric IP addresses into domain names. Most users consider domain names more useful for analysis and reports than IP addresses; however, IP resolution can be a slow process, and for this reason, you may choose to not use this capability.

In general, DNS lookups are performed more efficiently by the firewall or proxy server as the log is created, rather than during log file analysis by Firewall Suite. If your firewall or proxy server does not perform DNS lookups or your administrator has disabled that capability, Firewall Suite can do it for you.

The Internet Resolution dialog box allows you to choose whether or not to perform DNS lookup for the current profile. Resolving IP addresses into domain names takes a large amount of processing power the first time, but once resolution has occurred, the results are stored in a profile-specific DNS cache that is readily and quickly accessed for future analyses with the profile.

Note
If multiple profiles refer to the same IP address, they may all share the same DNS cache rather than perform the same DNS resolution for each profile.



Add General Firewall Activity Profile -- Internet Resolution

Domain Name Resolution Mode

Quick mode, using format from log file

Quick Mode: Maintains the Domain Name or IP format from the log file and is the fastest mode for creating reports.

Auto Mode: Select this if you are unsure. Consult Help for more information on how WebTrends processes log files in this mode.

Domain Name Resolution Cache

☑ [illegible]

☐ [illegible]

Specifying Settings for DNS Lookup

Depending on the Resolution mode and/or cache settings you choose, you may be required to fill in or choose additional settings.

To specify settings for DNS lookup:

1. In the **Domain Name/IP Resolution Mode** dropdown list, select one of the following options:

   – **Quick mode**. Uses the format from the log file. In this mode, Firewall Suite does not perform DNS lookups, but maintains the address in its original state in the log file. This is the fastest method for creating reports. If you select this mode, **Cache Control** is grayed out in the dialog box.

   – **Resolve mode**. Does a lookup for all numeric IP addresses. Select this option if your firewall or proxy does not perform DNS lookups and you need geographic or other domain-related information.

   – **Auto mode**. This is the best method to use if you don't know whether you log file contains IP addresses or domain names, but you want domain names in your analyses. In Auto mode, Firewall Suite examines the first record in the log. If the first record contains an IP address, it attempts to translate all IP addresses. If the first record contains a domain name, it turns on Quick mode.

2. In the **Cache Control** area, select how and where you want the results of the IP address resolution to be stored. Cache Control settings allow you to load the DNS cache in the Firewall Suite default location and/or store it in a custom location of your choice. Choose one of the following two options:

   - **Load DNS cache in memory**. Places the DNS cache in a profile-specific default location. The DNS cache is made up of two files, dnscache.din and dnscache.dtx. The default storage location uses the profile's file name when creating the storage path for these two files. For example, with the profile:

     install_dir`\wtm_FirewallOther\datfiles\0000dc.fir`

     the DNS cache files are:

     install_dir`\wtm_FirewallOther\datfiles\0000dc.dns\dnscache.din`

     install_dir`\wtm_FirewallOther\datfiles\0000dc.dns\dnscache.dtx`

   - **Store DNS Cache in custom location**. Places the DNS cache files in a location of your choice. Type or browse to the location.

3. Click **Next**. If this profile is for:

   - General Firewall Activity, the Filters dialog box opens.
   - Outgoing Firewall Activity, the Categories dialog box opens.
   - Incoming Firewall Activity, the Home Page dialog box opens.

Clearing the DNS Cache

You can clear the DNS cache for the current profile to dispose of unresolved or out-dated entries. The cache repopulates when the next DNS lookup is performed.

To clear the DNS cache:

Click the **Flush DNS Cache** button.

Sharing the DNS Cache

You can share a DNS cache among multiple profiles by choosing the **Storing the DNS cache in custom location** option, and pointing each profile to that custom location.

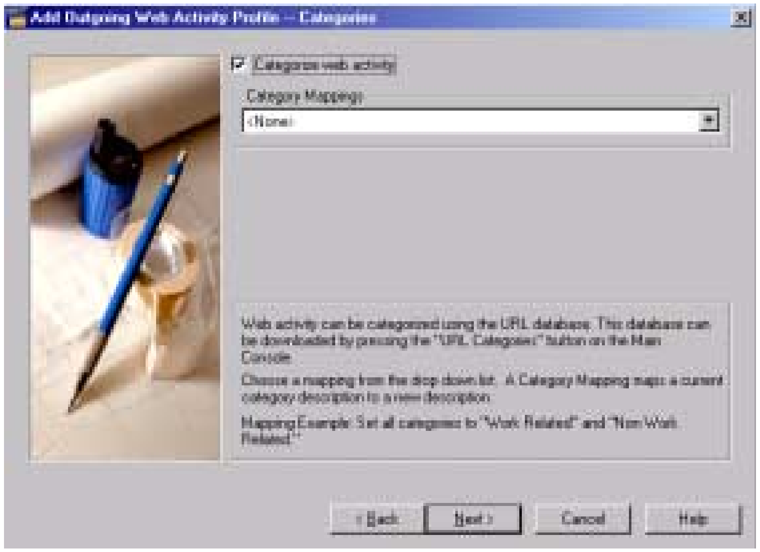
URL Categorization

With Outgoing Firewall Activity profiles, Firewall Suite provides access to databases from SurfControl. These databases list Internet URLs that may expose the organization to legal liability, detract from employee productivity, or waste bandwidth. Firewall Suite uses a modifiable `.ini` file to map these Internet URLs to categories such as Hate Speech or General News. The software can then track and report on the categories of Internet content that individuals in your organization access to ensure that employees do not visit inappropriate Web sites.

The Firewall Suite software includes the SurfControl categorization engine that licenses and accesses the categorization databases. Once you have downloaded the databases and activated URL Categorization, you can create profiles with filters to track the scope and nature of Internet usage in your organization.

Because Web sites change and new Web sites are continually being added, you can update the database periodically to obtain access to the most current list of sites.

Use the Categories dialog box to enable categorization and assign either the default category mapping, or a custom mapping you have created.



Add Outgoing Web Activity Profile -- Categories

☑ Categorize web activity

Category Mapping: <None>

Web activity can be categorized using the URL database. This database can be downloaded by pressing the "URL Categories" button on the Main Console.

Choose a mapping from the drop down list. A Category Mapping maps a current category description to a new description.

Mapping Example: Set all categories to "Work Related" and "Non Work Related"

Choosing Settings for Categories

To choose settings for Categories:

1. In the Categories dialog box, click **Categorize web activity** to enable URL categorization.
2. In the **Category Mappings** dropdown list, select the type of category mapping you wish to use.
3. Click **Next**. The Filters dialog box opens.

Note
You can create your own categories by assigning the existing categories new names and associating them with one of the two major category types, Core or General. See “Mapping URL Categories” on page 57 for information about creating your own category names.

Category Types

The Firewall Suite installation includes a Core Categories database. Core Categories include Web sites that contain objectionable content that may result in liability issues. You can purchase a separate license to download a General categories database that contains content believed to reduce employee productivity.

Core Categories

The Core categories database includes URLs of Web sites with the following types of content:

- ·Adult/Sexually Explicit
- Criminal Skills
- Drugs, Alcohol & Tobacco
- Gambling
- Hacking
- Hate Speech
- Violence
- Weapons

General Categories

Firewall Suite’s General Categories database contains the following additional categories of URLs that, while not objectionable, reduce employee productivity:

- Advertisements
- Arts & Entertainment
- Chat
- Computing & Internet
- Education
- Finance & Investment
- Food & Drink
- Games
- Glamour & Intimate Apparel
- Government & Politics
- Health & Medicine
- Hobbies & Recreation
- Hosting Sites
- Job Search & Career Development
- Kids Sites
- Lifestyle & Culture
- Motor Vehicles
- News
- Personals & Dating
- Photo Searches
- Real Estate
- Reference
- Religion
- Remote Proxies
- Search Engines
- Shopping
- Sports
- Streaming Media
- Travel
- Usenet News
- Web-based Email
- Sex Education

Updating the URL Categorization Database

Because the database is frequently updated to provide more relevant reports, use the URL Categorization Database dialog box to check the status of your database and update it when necessary. A good rule of thumb is to update the database monthly.

Note
If you are accessing the Internet through a proxy server, you must provide your proxy connection settings before you can update the database. See “Proxy Server Settings” on page 59.

To determine whether your database needs updating:

1. Select **URL Categorization** from the Tools menu. The URL Categorization dialog box opens.
2. Review the information in the **Database Information** area at the bottom of the dialog box. The Status tells you whether or not the database is up to date.

To update your database:

1. Select **URL Categorization** from the Tools menu. The URL Categorization dialog box opens.
2. Click **Update Database**. The Update URL Database dialog box opens.
3. Click **Get Update**.

Incorrect Categorization of IP Addresses

When a single IP address hosts multiple sites, visits to any site hosted by that address can be mis-categorized. For example, the same IP address may host both a sexually explicit site and a news site. If a person visited the news site, reports may incorrectly categorize the visit as one to a sexually explicit site. You can avoid this problem of mis-categorization by not categorizing IP addresses.

To disable categorization of IP addresses:

1. Select **URL Categorization** from the Tools menu. The URL Categorization Databases dialog box opens.
2. Select the **Do not categorize IPs** check box.

System Performance and URL Categorization

URL categorization will categorize all file types unless you specify otherwise. In most cases, you only need to categorize document file types, which you specified in the File Types dialog box. These typically include files with `.htm`, `.html`, `.asp`, `.txt`, and similar extensions. Access the File Types dialog box by clicking **Tools > Options> General Firewall Activity > File Types**.

By only categorizing document file types, you significantly improve system performance because Firewall Suite does not have to categorize every file.

To improve system performance for URL categorization:

1. Select **URL Categorization** from the Tools menu. The URL Categorization dialog box opens.
2. Select the **Only categorize documents** check box.

Licensing the URL Categorization Database

When you install Firewall Suite, you install a sample database. A full Firewall Suite license lets you update the database as many times as you like.

Mapping URL Categories

You can create new mappings for your standard URL categories to create URL categories that help your reports answer the questions you need to answer. For example, to see whether employee Web surfing activity is for work-related or non-work-related purposes, you can use the pre-defined Work Mappings setting, which assigns the pre-defined categories to either the Work-Related or Non-Work-Related mapping. Individual categories such as Sexually Explicit or Hate are not shown, but visits to these categories are shown under the mapped categories.

Each category is made up of two elements:

- *Category Type*. Core or General. Reports are broken down by Core or General categories. For example, among the many URL categorization reports possible, you can generate a Most Popular Core Categories graph and table, a Users Visiting Most Popular Core Categories table and a General Categories Visited by Most Active Users table.
- *Category Name*. For example, Sexually Explicit, Hate Speech, Entertainment, General News. These names can be changed into names that are more meaningful for the user's or organization's reports.

Note
For a complete list of Category Names, see "Core Categories" on page 53 and "General Categories" on page 54.

Category mappings are defined in the `urlcatmap.ini` file, which is located in the f*`install_dir`*`\wtm_FirewallWebOut`directory. If this file is empty, no mappings are available in the Category Mappings list.

An Example of Mapped Categories

Firewall Suite includes one preconfigured alternate mapping called *Work Mappings*, which can be selected from the Category Mappings dropdown list. View this mapping by navigating to and opening the `urlcatmap.ini` file from the above location. Firewall Suite includes one pre-defined category mapping, Work Mappings. By default, this mapping maps all SurfControl categories to the category type "General" and the category "Non Work Related." You can modify this mapping in the `urlcatmap.ini` file to change the way it maps categories.

Remapping Syntax

Add new mappings to the `URLcatmap.ini` file. Each mapping must be a separate block of code from any other mapping code. You can add it at the top of the `.ini` text file or at the very end of any text in the `.ini` file. The order of the mappings in the .ini file determines their order in the Category Mappings dialog box.

Each new mapping must have a new mapping name. For example, the Work Mappings settings are initiated by the mapping heading:

```
[Work Mappings]
```

Category type and name changes can be assigned as follows:

```
Category Type, Category Name = New Category Name, Reassigned Category
Type
```

or

```
Category Type, Category Name = New Category Name
```

The order of Category Type and Name are reversed on the right side of the equals sign in syntax example 1. In example 2, the Category Type will not be reassigned, only the Category Name will be changed--an example of this is shown in the

```
General, Chat = Non Work Related
```

mapping on the second line of the sample mapping excerpt from the `URLcatmap.ini` file.

Reporting with URL Categorization

The reports that you generate can include tables and graphs showing the most active authenticated users, non-authenticated users, and host names or IP addresses connecting to the proxy server. Of the categorized sites most visited, you can list the number of users that visit a site; the names of the categories of visited sites; the number of hits on each site; the number of user sessions; the amount of time visitors spent at a site; and the amount of data (in KB) that was downloaded

You can generate a report for all activity related to categorized sites, or you can create filters to limit reports to specific categories or category mappings. For instruction on including or excluding categories of outgoing activity, see “Filters Dialog Box” on page 66, “Working with Filters” on page 160, and “Category” on page 169.

Proxy Server Settings

If you connect to the Internet via a proxy server, you will need to provide your proxy connection settings in order to update the database.

To provide your proxy connection settings:

1. On the Main Console, select **Tools > Options** from the Configure menu or click **Options** in the Functions area.
2. Click **Main Options**.
3. Select the **Access to Internet** option.
4. Select the **Connect through a Proxy Server** check box and type the address of the proxy server and the port.
5. Choose one of the following options:
   - ***If your access requires authentication***, select the **HTTP access requires a User Name/Password** and type the user name and password for your proxy server.

- *If your access does not require authentication*, clear the check box.

6. Click **OK**.

Category Names

The Category Mappings choice selected in the URL Categorization Databases dialog box determines which Category Names are available for the selected profile. You can see which Category Names are available from the Include Filter and Exclude Filter dialog boxes.

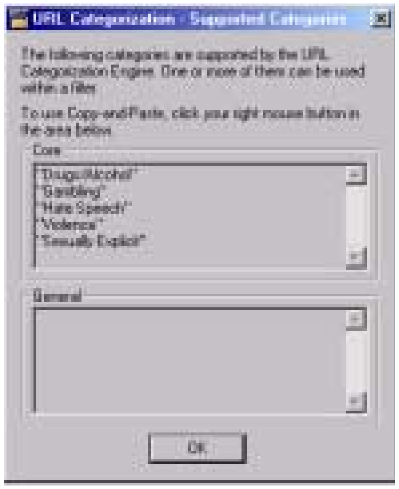
For instruction on including or excluding categories of outgoing activity, see “Filters Dialog Box” on page 66, “Working with Filters” on page 160 and “Category” on page 169.

To view the category names available for a selected profile:

1. While editing an existing profile or creating a new one, open the Filters dialog box.
2. Either edit an existing filter or create a new one
3. Select **Include/Exclude activity based upon**.
4. Choose one of the following:
   - *If you are editing an existing filte*r, select the **Category** check box and select the **Category** tab.

- ***If you are creating a new filter***, click **Next**. The Category dialog box opens.

5. Click **Examples** to see a list of available Category Names available for using with category filters.



The following categories are supported by the URL Categorization Engine. One or more of them can be used within a filter.

To use Copy-and-Paste, click your right mouse button in the area below.

"Drugs/Alcohol"
"Gambling"
"Hate Speech"
"Violence"
"Sexually Explicit"

Interpreting Categorization Reports

The categorization feature is powerful, and the reports, when interpreted properly, can point to Web abuse and possibly head off potential litigious issues. However, there are some aspects to Internet technology that require caution when interpreting categorization reports.

Some Internet providers and Web hosting services host several Web sites on a single server. These Web sites are referred to as virtual Web sites. For such sites there are at least two host names: the host name of the virtual Web site itself and the host name of the server. The host name used for URL Categorization depends on how your firewall or proxy server records this information. If both are recorded, the virtual host name is categorized and the server host name is understood to belong to that category. This may mean that a server computer can trigger a “core category” ranking because it hosts a virtual Web site that is registered as objectionable. Thus, a visit to an innocuous site on that server will also trigger the “core category” ranking.

Ads or other embedded objects on a page may be served up by a totally different site from the page itself. The page may be registered as an objectionable site when it is the site serving up the ad that is objectionable. This is complicated when ads come from sites on virtual servers.

Note

The table “Core Categories Visited by Active Users” can be misinterpreted. It does not list the top offenders of the Core Categories, but rather lists a breakdown of the Core sites visited by the Most Active Users.

With page title retrieval turned on, the analyzing host may register as hitting the objectionable sites found by the analysis.

To maximize the usefulness of the information in reports, look carefully at the KB transferred, at the number of hits, and of course, visit pages to judge the content for yourself.

Before any action is taken to warn an employee about potential misuse, it is highly recommended that the URLs in question be double-checked for their content and appropriateness.

Home Page Dialog Box

With Incoming Firewall Activity profiles, you can use the Home Page dialog box to obtain accurate data about hits to your home page(s). Home pages are the pages a Web server defaults to when the user requests a URL without a specific file name. For example, if a user requests:

`http://www.webtrends.com/`

and `index.htm` is the home page for the uppermost level of the site, the Web server delivers:

`http://www.webtrends.com/index.htm`

Similarly, if the user requests:

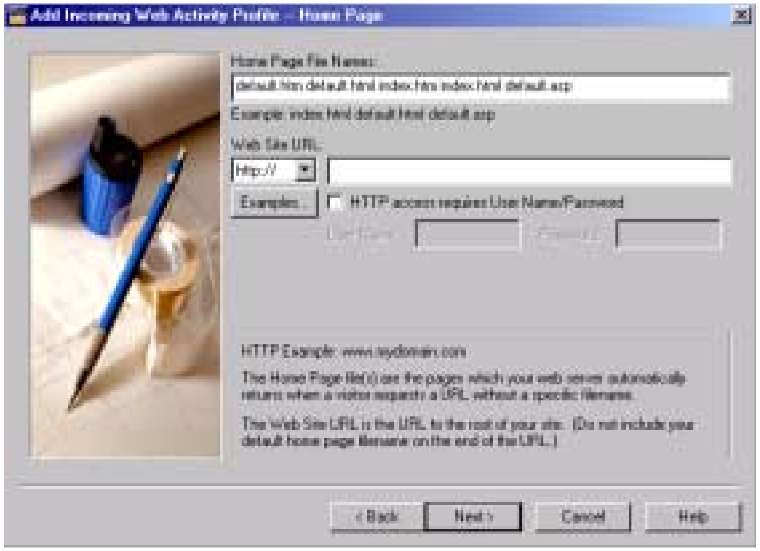
`http://www.webtrends.com/reports/incoming`

and `default.htm` is the home page for that directory, the Web server delivers:

`http://www.webtrends.com/reports/incoming/default.htm`

Both `index.htm` and `default.htm` are home pages for the site (though for different directories), so if you wish to accurately count the number of hits to home pages, specify any file names used as home pages for the entire site. The specified paths and file names are shown in Firewall Suite reports.

You may also wish to specify multiple home page file names when a home page file name changes, but you still want to perform analysis on log files created before and after the name change. For example, if the home page for www.webtrends.com, `default.htm`, was changed to `index.htm`, but you wanted to report on hits to both the new and old home page file names.



Add Incoming Web Activity Profile -- Home Page

Home Page File Names: default.htm default.html index.htm index.html default.asp

Example: index.html default.html default.asp

Web Site URL: http://

□ HTTP access requires User Name/Password

HTTP Example: www.mydomain.com

The Home Page file(s) are the pages which your web server automatically returns when a visitor requests a URL without a specific filename.

The Web Site URL is the URL to the root of your site. (Do not include your default home page filename on the end of the URL.)

To specify the home page:

1. In the **Home Page File Names** text box of the Home Page dialog box, type the home page file names that the Web server defaults to when a visitor requests a URL without a specific file name. The most common filenames are provided by default.

   – Separate multiple file names with spaces.

   – You can type up to 255 characters.

2. Specify your Web site URL using the entire path from the root of your site. Do not include your default home page file name.

   – ***If you access your Web site from a mapped drive or by using a Universal Naming Convention (UNC) name to identify a shared file***, select **file:///** from the dropdown list and type the URL path or browse to it. For example, type `c:\inetpub\wwwroot\`.

   – ***If you access your Web site by FTP***, select **ftp://** and type or browse to the location of the site. For example, type `ftp.isp.com/~user`. If required, provide a user name and password.

   – ***If yours is an HTTP site***, select **http://** and type your Web site URL, for example `www.domain.com/`. If authentication is required, click **HTTP access requires User Name and Password** and provide user name and password. This is not usually required.

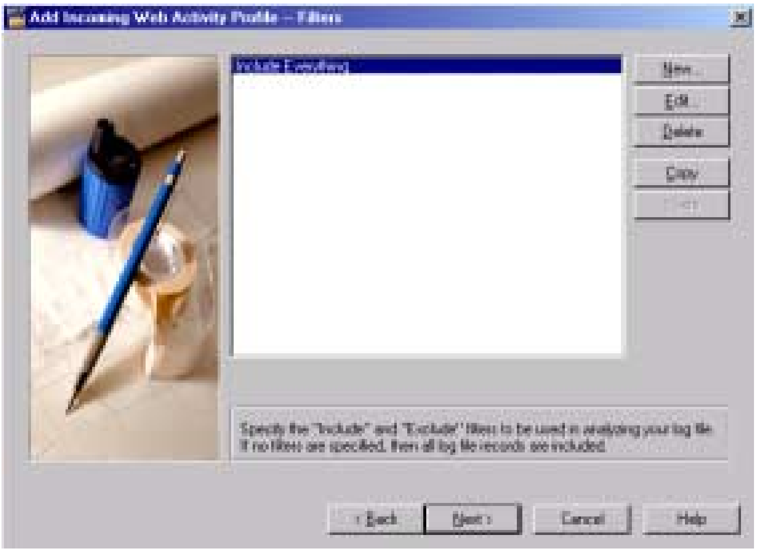
3. Click **Next**. The Filters dialog box opens.

Filters Dialog Box

Filters focus the contents of a report by including only the data you want to analyze. You can use filters that include data based on defined criteria, and you can use filters to exclude data based on defined criteria. Because filters are such a powerful tool, they are discussed in their own chapter. See “Filtering for Focused Reports” on page 157 for detailed information about filters, and how to add, delete, edit, copy and combine them.

You can create a profile without using any filters. By default, this means that all log file data is included in the log file analysis.

Use the Filters dialog box to create, edit, copy and delete filters.

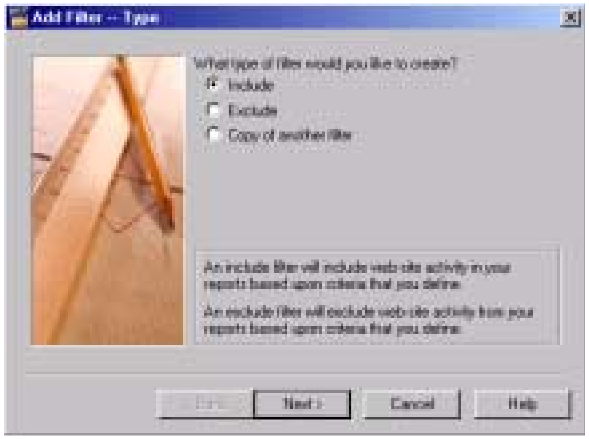


Specify the "Include" and "Exclude" filters to be used in analyzing your log file. If no filters are specified, then all log file records are included.

Creating a Filter

To create a filter:

1. In the Filters dialog box, click **New** to create a new filter using the New Filter wizard.



What type of filter would you like to create?

● Include

○ Exclude

○ Copy of another filter

An include filter will include web site activity in your reports based upon criteria that you define.

An exclude filter will exclude web site activity from your reports based upon criteria that you define.

2. Select one of the following options:
   - **Include** to include Web site activity that meets the selected criteria in your analysis and reports.
   - **Exclude** to exclude the Web site activity that meets the selected criteria in your analysis and reports.
   - **Copy of another filter** to copy an existing filter from a list of existing filters for the selected profile type and edit it as needed.
3. Click **Next**.
4. ***If you selected*** *Copy of another filter,* select the filter you wish to copy and click **Next**.
5. ***If you selected*** *Include or Exclude*, type a name for the filter in the text box and click **Next**.

6. Click **Include/Exclude activity based upon**.
7. Select any filter elements you wish to include or exclude from your log file analysis and reports.
8. Click **Next**. The dialog box for the first filter element you selected opens.
9. Fill in the settings for the filter element dialog box.
10. Click **Next** and continue to fill in the settings for the remaining selected filter elements. For more information, review “Filter Basics” on page 157.
11. Click **Next**. The Database and Real-Time dialog box opens.

Editing a Filter

To edit a filter:

1. In the Filters dialog box, select the filter you wish to edit from the filters list.
2. Click **Edit** and edit the filter as needed. See “Filter Elements” on page 164 for a list of filter elements. See“Filter Element Descriptions” on page 166 for a full description of each filter element.
3. Click **OK**.

Deleting a Filter

To delete a filter:

1. In the Filters dialog box, select the filter you wish to delete from the filters list.
2. Click **Delete**. A confirmation message displays.
3. Click **Yes** to confirm the deletion. The filter is now deleted.

Copying and Pasting a Filter

To copy and paste a filter:

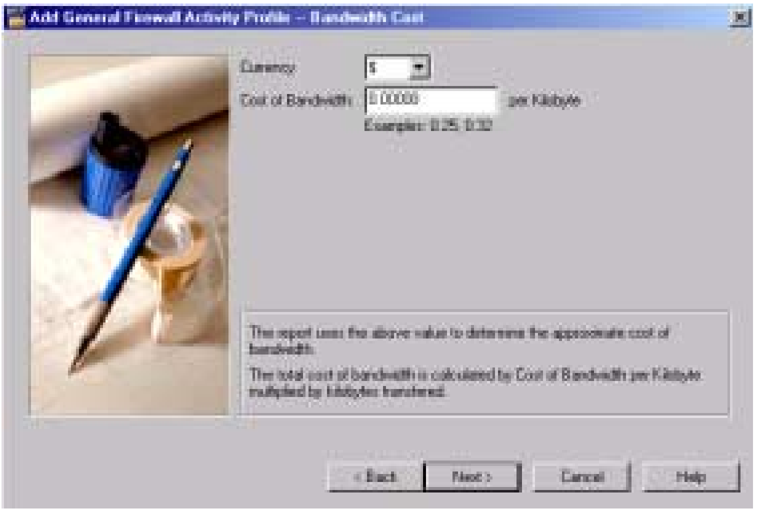
1. In the Filters dialog box, select the filter you wish to copy from the filters list.
2. Click **Copy**.
3. Click **Paste**. A copy of the filter is placed in the list with the name “Copy of filter name”.
4. Select and edit the copied filter as needed.

Bandwidth Cost Dialog Box

Use the Bandwidth Cost dialog box to specify the cost of service for each kilobyte of data transferred for General Firewall Activity profiles. The information collected in the Bandwidth Usage report chapter includes the number of events, the percent of total events, the kilobytes transferred, and the cost of bandwidth used by top user addresses, outgoing protocols, and incoming protocols.

Firewall Suite calculates and reports the cost of bandwidth usage for all types of incoming and outgoing Internet activity. Bandwidth cost is calculated by multiplying the Cost of Bandwidth per Kilobyte you supplied by the number of kilobytes transferred. All firewall events that log a value for kilobytes transferred are included. Typically, firewalls log this value for events associated with a protocol.

To report on bandwidth cost accounting, you must include the graphs and tables for Top Users by Bandwidth Utilization, Outgoing Protocol Usage and Incoming Protocol Usage.



Currency: $

Cost of Bandwidth: 0.00000 per Kilobyte

Examples: 0.25, 0.32

This report uses the above value to determine the approximate cost of bandwidth.

The total cost of bandwidth is calculated by Cost of Bandwidth per Kilobyte multiplied by kilobytes transferred.

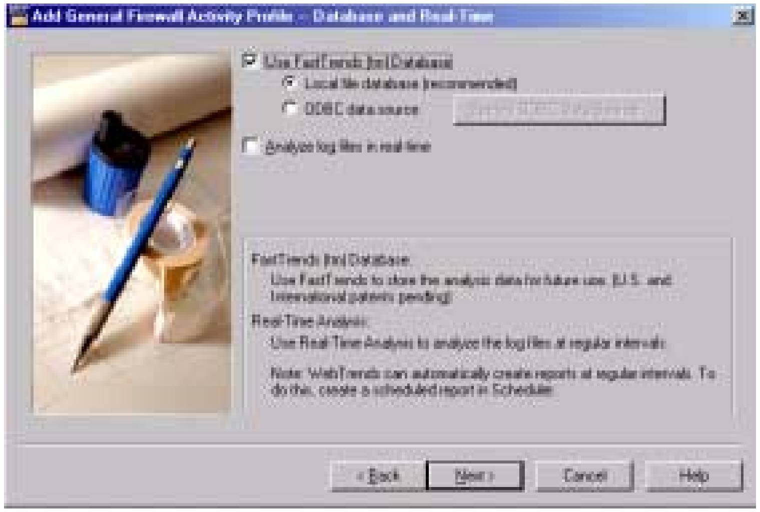
Specifying Bandwidth Cost

To specify the bandwidth cost:

1. In the **Currency** dropdown list of the Bandwidth Cost dialog box, select the currency to use when calculating bandwidth cost.
2. In the **Cost of Bandwidth per Kilobyte** text box, enter the cost per kilobyte transferred.

Database and Real-Time Dialog Box

The Database and Real-Time dialog box allows you to activate the FastTrends™ database and use real-time analysis when analyzing that data. Both features are useful for speeding up analysis and reporting, especially if your firewall generates large amounts of data.



Add General Firewall Activity Profile -- Database and Real-Time

☑ Use FastTrends [tm] Database

● Local file database (recommended)

○ ODBC data source

□ Analyze log files in real-time

FastTrends [tm] Database:
Use FastTrends to store the analysis data for future use. (U.S. and International patents pending)

Real-Time Analysis:
Use Real-Time Analysis to analyze the log files at regular intervals.

Note: WebTrends can automatically create reports at regular intervals. To do this, create a scheduled report in Scheduler.

FastTrends Database

Using the FastTrends database allows Firewall Suite to store analysis results in a cache. Because the cached data is more accessible, Firewall Suite can perform more efficient future analysis and report generation on the current profile. For example, if you activate the FastTrends database option and generate a report on Monday, Firewall Suite stores the data in the FastTrends database. If you run a report on the same profile for Monday *and* Tuesday, only the data for Tuesday needs to be analyzed.

Real-Time Analysis

Firewall Suite's real-time analysis feature can keep your log file analysis as current as possible. Real-time analysis enables Firewall Suite to monitor log files at regular intervals and check for any new activity. If new activity is found, then FastTrends analyzes the new data in the background, and stores the analysis results in the FastTrends database.

Real-time analysis is useful if your firewall generates unusually large amounts of data and initial analysis of an entire log file would take a significant amount of time. By collecting and analyzing log file information at regular intervals, when an analysis and reporting event kicks off, only the new log file records will need to undergo analysis before a report can be generated.

To specify settings for the FastTrends database and real-time analysis:

1. To store the results of log file analysis in a database to use for future reports, select the Use FastTrends Database checkbox. . The default location of the FastTrends database is InstallDir\wtm_FirewallOther\datfiles\profile_name.dat.

   Use the Advanced FastTrends tab (enabled when you activate FastTrends) to specify a location for the database different from the default location

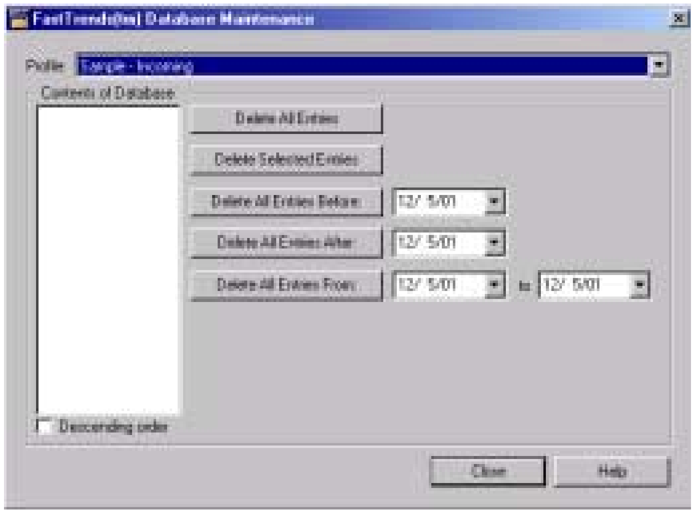
2. Select or clear the **Analyze log files in real-time** check box to determine whether log files are analyzed in real time. For more information on real-time analysis, see "Advanced FastTrends Dialog Box" on page 76.

Maintaining the FastTrends Database

You may need to manage the amount of data in your FastTrends database to free up available space.

To maintain the FastTrends database:

1. On the Main Console, select the profile type tab containing the profile for which you want to perform FastTrends database maintenance.
2. On the Main Console, select **Tools > FastTrends Maintenance**. The FastTrends Database Maintenance dialog box opens.



Profile: Sample - Incoming

Delete All Entries Before: 12/ 5/01

Delete All Entries After: 12/ 5/01

Delete All Entries From: 12/ 5/01 to 12/ 5/01

□ Descending order

3. From the **Profile** dropdown list, select the profile for which you want to perform FastTrends database maintenance. The **Contents of Database** list shows all the FastTrends database entries by date.

   The **Contents of Database** list may be sorted in ascending or descending order. Select the **Descending order** check box to sort in descending order. Clear the check box to sort in ascending order.

4. Delete entries from the list using one of the following buttons:

- Click **Delete All Entries** to delete all entries in the list.
- Click **Delete Selected Entries** to delete a selected entry from the list.
- Click **Delete All Entries Before** to delete all entries before a specified date.
- Click **Delete All Entries After** to delete all entries after a specified date.
- Click **Delete all Entries From** to delete all entries between two user-specified dates

5. Click **Close**.

Notes

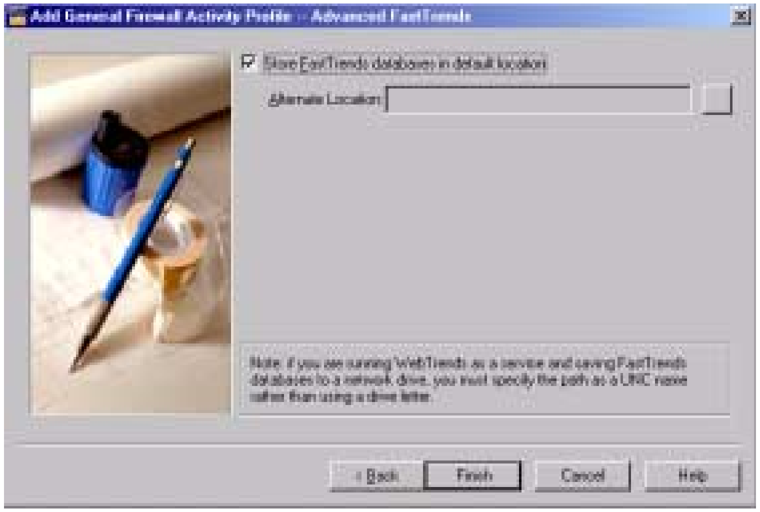
If you make changes to a profile, for example by using a different log file, changing DNS Lookup settings, or modifying the filters, clear the database and rerun the analysis to store the correct data in the database.

If you turn off FastTrends, clear the database to free up disk space.

Advanced FastTrends Dialog Box

This dialog box is shown only if you activated FastTrends database in the Database and Real-Time dialog box. The Advanced FastTrends dialog box lets you specify a database location other than the default location.

Storing FastTrends data in a location other than the default can save space on your local computer; however, it can slow down processing.



Add General Firewall Activity Profile -- Advanced FastTrends

☑ Store FastTrends databases in default location

Alternate Location:

Note: if you are running WebTrends as a service and saving FastTrends databases to a network drive, you must specify the path as a UNC name rather than using a drive letter.

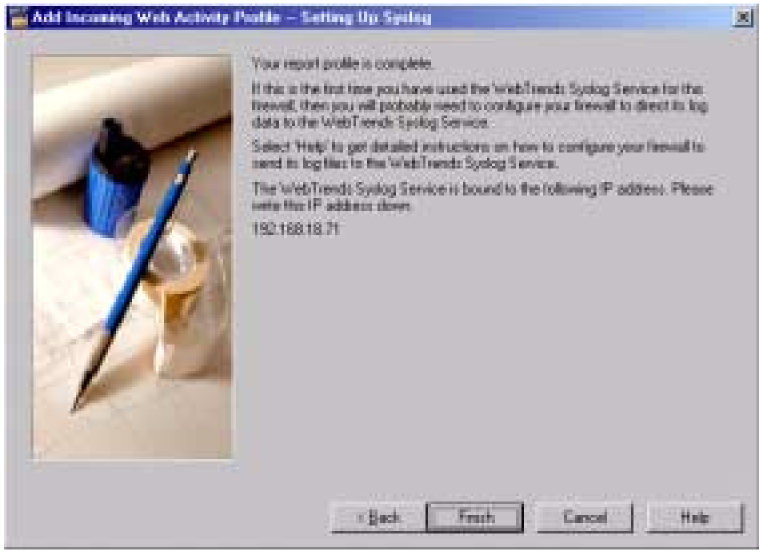
To specify an alternate data storage location:

1. Clear the **Store FastTrends databases in default location** check box.
2. Type the path and directory for the new location in the **Alternate Location** text box, or use the browse button to navigate to the new location.
3. Click **Finish**.

Setting Up Syslog Dialog Box

The Setting Up Syslog dialog box is the last dialog box you will see when setting up a profile that uses the WebTrends Syslog Service.

If you have not already configured your firewall to send its log files to the WebTrends Syslog Service, you will need to do so. The *Firewall Configuration Guide* contains specific information for your firewall.



Add Incoming Web Activity Profile – Setting Up Syslog

Your report profile is complete.

If this is the first time you have used the WebTrends Syslog Service for the firewall, then you will probably need to configure your firewall to direct its log data to the WebTrends Syslog Service.

Select 'Help' to get detailed instructions on how to configure your firewall to send its log files to the WebTrends Syslog Service.

The WebTrends Syslog Service is bound to the following IP address. Please write this IP address down.

192.168.18.71

To finish setting up your profile:

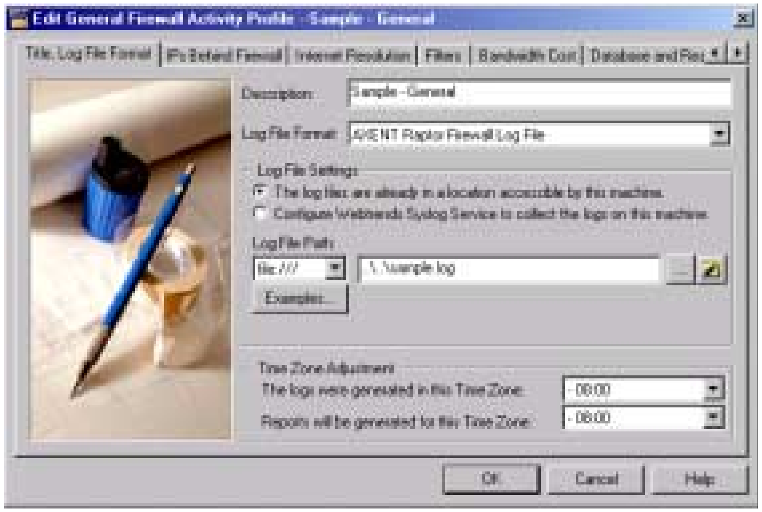
1. Write down the IP Address or addresses you find at the bottom of the Setting Up Syslog dialog box. These are the addresses on the computer running Firewall Suite to which the WebTrends Syslog Service is bound.
2. Click **Finish**.

Editing a Profile

You can edit an existing profile in the Edit profile window.

To edit an existing profile:

1. On the Main Console, select the profile that you want to change in the Profile Description list.
2. Select **Edit > Profile** from the Main menu, or **Edit Profile** on the Tasks area. The Edit Firewall Activity Profile window opens.



Description: Sample - General

Log File Format: AXENT Raptor Firewall Log File

Log File Settings

● The log files are already in a location accessible by this machine.

○ Configure WebTrends Syslog Service to collect the logs on this machine.

Log File Path: file:/// ..\..\sample.log

Time Zone Adjustment

The logs were generated in this Time Zone: -08:00

Reports will be generated for this Time Zone: -08:00

3. View the current settings for the profile by selecting the tabs at the top of the window to open the associated dialog box. The tabs correspond to the dialog boxes used in the New Profile wizard. See “Creating a Firewall Profile” on page 31 for more information on the settings for each tab. Make any needed changes to the settings.
4. Click **Cancel** to close the window without saving any changes, or click **OK** to save your changes and close the window.

Copying a Profile

You can create a new profile based on existing profile settings. This may be useful if many of the settings in the existing profile are needed in the new profile.

To copy a profile:

1. On the Main Console, select the profile you want to copy and modify from the Profile Description list.
2. Select **Edit > Copy Profile** from the Main menu. The Edit Firewall Activity Profile window opens.
3. Select the **Title, Log File Format** or **List of Servers** tab, and then type a name for your new profile in the Description text.
4. Select other tabs as needed, making any necessary changes. Use the scroll arrows in the upper-right corner of the window to access all of the tabs
5. Click **OK** to save the new profile and its settings.

Deleting a Profile

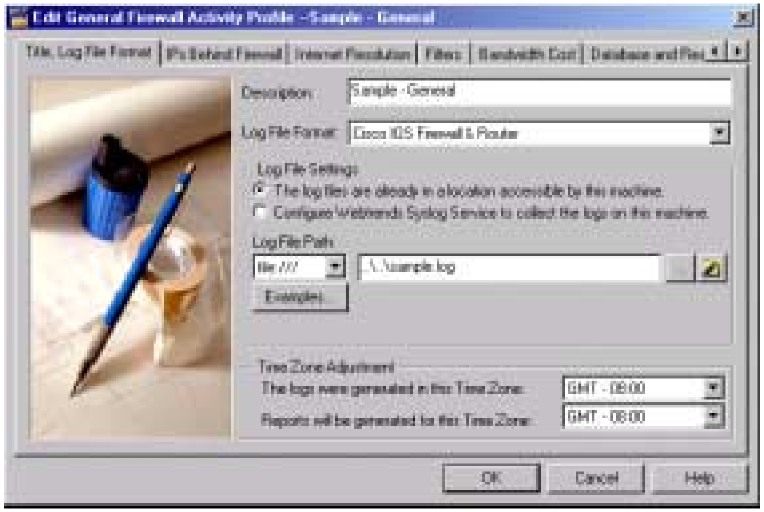
If you have profiles that are no longer needed, you can delete them.

To delete a profile:

1. On the Main Console, select the profile that you want to delete from the Profile Description list.
2. Click **Edit > Delete** from the Main menu or **Delete Profile** from the Tasks area. A confirmation message displays.
3. Click **Yes** to confirm the deletion. The profile is deleted.

Specifying Log Files

When creating or editing a profile, you can specify single or multiple log files using the browse buttons in the Log File Path section of the Title, Log File Format dialog box. This section discusses how to browse for log files and how to specify multiple logs using date macros or wildcards. For most firewalls, you will see the dialog box shown below.



Description: Sample - General

Log File Format: Cisco IOS Firewall & Router

Log File Settings

● The log files are already in a location accessible by this machine.

○ Configure Webtrends Syslog Service to collect the logs on this machine.

Log File Path: file:/// ..\..\sample.log

Time Zone Adjustment

The logs were generated in this Time Zone: GMT - 08:00

Reports will be generated for this Time Zone: GMT - 08:00

Specifying a Single Log File

To specify a single log file:

1. In the Title, Log File Format dialog box, click the browse button ▭.
2. Navigate to the directory with the log file.
3. Select the file, and click **Open**.

> **Note**
> You can specify compressed logs, such as `.zip` or `.gz` files.

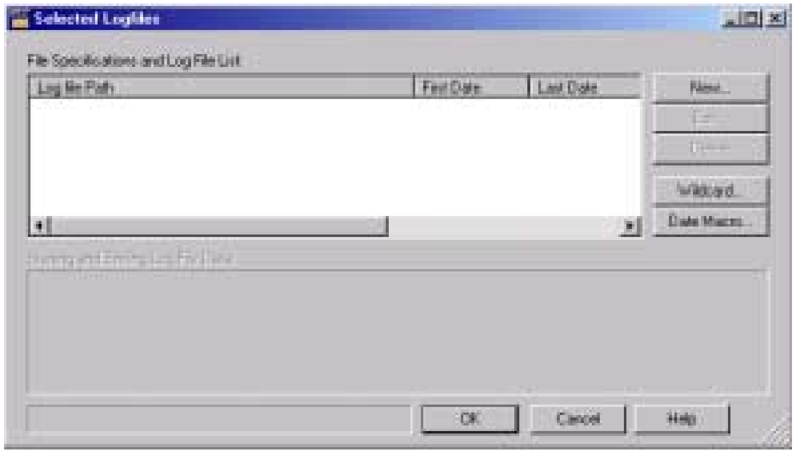
4. Click **Next**.

Specifying Multiple Log Files

Firewall Suite provides you with a number of ways to select multiple log files:

- Using a browser
- Using wildcards to select log files with similar names
- Using date macros to select log files that have dates as names

Multiple log files are specified using the Selected Log Files dialog box.



To add files using the browser:

1. Choose one of the following two options:

   – **Firewall on single machine**. Click the extended browse button on the Title, Log File Format dialog box. The Selected Logfiles dialog box opens.

   – **Firewall on multiple machines**:

   a. Click New in the List of Servers dialog box to open the Firewall Name and Log File URL Path dialog box.

   b. Click the extended browse button. The Selected Logfiles dialog box opens.

2. Click **New**.

3. Navigate to the directory that contains the log file. Select the log file.

4. Click **OK** to add the file to the File Specification and Log File List.

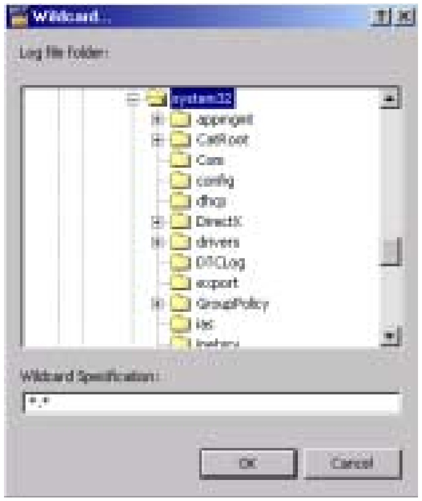
5. Repeat to add additional files.

6. Click **OK** to return to the Title, Log File Format dialog box.

To add files using wildcards:

1. On the Title, Log File Format dialog box, click the extended browse button . The Selected Logfiles dialog box opens.

2. Click **Wildcard**. The Wildcard dialog box opens.



Wildcard Specification: *.*

3. Select the directory that contains the log files.

4. In the **Wildcard Specification** text box, type the log file path names or file names using * or ?. See “Specifying Log Paths” on page 351 for examples.

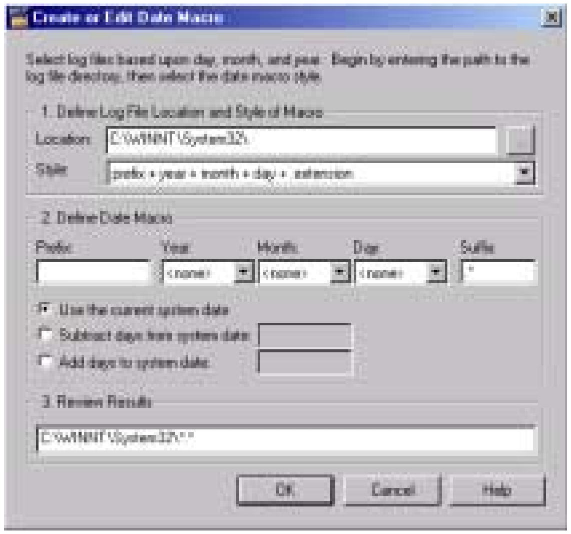
5. Click **OK** to add the files to the File Specification and Log File List.

6. Click **OK** again to return to the Title, Log File Format dialog box.

To add files using date macros:

1. On the Title, Log File Format dialog box, click ▣. The Selected Logfiles dialog box opens.

2. Click **Date Macro**. The Create or Edit Date Macro dialog box opens.



Create or Edit Date Macro

Select log files based upon day, month, and year. Begin by entering the path to the log file directory, then select the date macro style.

1. Define Log File Location and Style of Macro

Location: C:\WINNT\System32\

Style: prefix + year + month + day + .extension

2. Define Date Macro

Prefix	Year	Month	Day	Suffix
	<none>	<none>	<none>	.*

☒ Use the current system date

☐ Subtract days from system date

☐ Add days to system date

3. Review Results

C:\WINNT\System32\*.*

3. In the **Location** text box, type the path to the log file or browse to the directory.

4. In the **Style** text box, use the dropdown list to specify the way in which the date is arranged in the file name.

5. In the various **Log File Name** text boxes, specify the following:

   - **Prefix**: Type any text that precedes the date.
   - **Year**: If the file name contains the year, select a year format from the dropdown list.
   - **Month**: If the file name contains a month, select a month format from the dropdown list.

     The three-character text abbreviations for the month are case sensitive. Select the case desired.
   - **Day**: If the file name contains a day, select a day format from the dropdown list.
   - **Suffix**: Type the log file extension.

6. Make any necessary adjustments to the system date:

   - Select **Use the current system date** to make no changes to the system date.
   - Select **Subtract this many days from the system date** to subtract days, then type the number of days to be subtracted into the text box.
   - Select **Add this many days to the system date** to add days, then type the number of days to be added into the text box.

7. The resulting macro is displayed in the **Review Results** text box. Click **OK** to close the dialog box.

   Note
   You can also use macros in the Log File URL path as well as the Save As paths of the Scheduler and the Create Report dialog boxes.

8. Click **OK** to return to the Title, Log File Format dialog box.

To remove log files from the File Specifications and Log File List:

1. On the Title, Log File Format dialog box, click . The Selected Logfiles dialog box opens.
2. Select the log files in the list.
3. Click **Delete**. A confirmation message displays.
4. Click **Yes** to confirm. The log file is removed from the list.

Using Date Macros

If your firewall maintains a separate log file for each day named by the date, and you would like to define a log profile which incorporates only the previous day’s firewall activity, type a line like the following in the **Log File Path** text box in the Title, Log File Format dialog box, or use the Create or Edit Date Macro dialog box.

```
C:\WEBSRVR\LOGFILES\%DATE-1%%mm%%dd%%yy%.log
```

If your firewall maintains a separate log file for each day named by the date, and you would like to specify the previous three days’ worth of log files, type a line like the following in the **Log File Path** text box in the Title, Log File Format dialog box, or use the Create or Edit Date Macro dialog box.

```
C:\WEBSRVR\LOGFILES\%DATE-3%%mm%%dd%%yy%.log|%DATE-
2%%mm%%dd%%yy%.log|%DATE-1%%mm%%dd%%yy%.log
```

Using Firewall Add-On Support for Clusters

The Firewall Add-On analyzes the multiple log files created by firewalls, VPNs, or proxy servers hosted on multiple servers or server clusters. Using WebTrends ClusterTrends technology, it automatically consolidates the data to provide an accurate analysis of firewall activity. While Firewall Suite offers accurate, sophisticated reporting for log files for a single firewall, the Firewall Add-On support for clusters provides additional reporting capability for firewalls hosted by multiple servers. Firewall Add-On addresses the problem of overlapping log files.

A firewall cluster is a group of firewalls, VPNs, or proxy servers cooperating to provide high bandwidth and reliable access. The simplest and most common form of a firewall cluster includes multiple servers and a load balancing device or redirector. Each server has identical firewall content and usually runs mirroring software to maintain the duplicate content across all the firewalls in the cluster.

Activity through the firewall is distributed among all the firewalls, VPNs, or proxy servers in the cluster by a redirector device. The redirector achieves a balanced load for each server in the cluster.

Firewall clusters provide the following benefits:

- *High bandwidth capabilitie*s. Because of the load balancing hardware or software that distributes the requests, you can achieve greater bandwidth than with a single server configuration.
- *Reliability*. Because an identical firewall is on each server, if one server is down because of software or hardware problems, the other servers can continue to handle activity.
- *Maintenance*. You can upload changes to one firewall server while others are still available for access. Once uploaded, changes are copied to other servers in the cluster.

However, the individual log files from the firewalls in the cluster yield inaccurate data because they are logging only part of the activity.

To remedy this issue, the Firewall Add-On time-stamps firewall activity, and records it in sequence, even though the activity may be directed to and logged on different firewalls in the cluster. Using the time stamp, the Firewall Add-On collects all of the data from each server, reorders it, and analyzes it to produce accurate and complete results for the firewall. You must purchase a Firewall Add-On to implement this technology.

Using Department Management

You may wish to configure your profile using the Department Management feature. This feature provides a more detailed break-down of your organization's domain name into groups of users using their IP address or domain names. You can configure Firewall Suite to report on domain activity by department including the following:

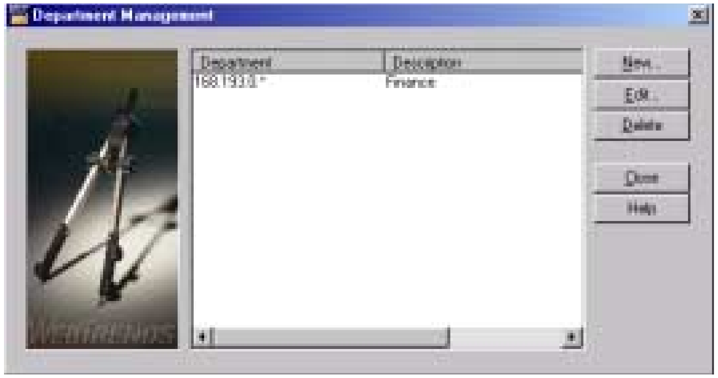
- Which pages users access, and how much time they spend on them.
- Which departments access your intranet and when that access occurs.
- Where your users and departments are located.
- Which operating systems are used most widely within the your organization.
- Which browsers are used.
- Which days and times are the most active and inactive.
- Which forms users submit.
- Which scripts run and when they run.

Once you have set up departments, this information is automatically included in General and Outgoing Firewall Activity reports. You can also use the Departments filter element to report on just the ones you are interested in. See "Departments" on page 172.

Defining a Department

To set up departments to be included in reports or used in filters:

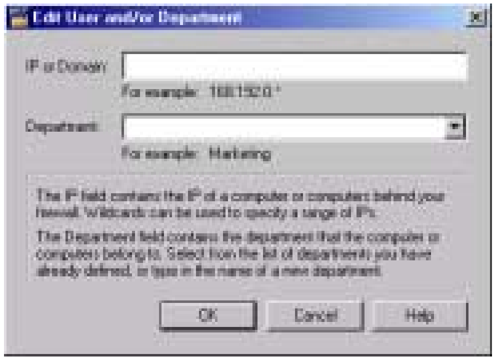
1. On the Main Console, select **Tools > Department Management**. The Department Management dialog box appears.



Department	Description
168.193.3.*	Finance

A list of departments that have been defined appears in the list window.

2. Click **New**. The Edit User and/or Department dialog box opens.



IP or Domain:

For example: 168.192.0.*

Department:

For example: Marketing

The IP field contains the IP of a computer or computers behind your firewall. Wildcards can be used to specify a range of IPs.

The Department field contains the department that the computer or computers belong to. Select from the list of departments you have already defined, or type in the name of a new department.

3. In the **IP or Domain** text box, type an IP address, IP address range, or domain name.

   - You can type a subnet using CIDR format. For example:

     ```
     206.13.01.48/26
     ```

     where /26 indicates the number of bits used to identify the network.

   - You can use wildcards to specify a range of addresses. For example, type:

     ```
     255.255.255.*
     ```

     to specify an entire Class C subnet, or type:

```
255.255.*
```

     to specify a Class B subnet, or type

```
255.*
```

     to specify a Class A subnet.

     You *cannot* list IP addresses or domain names separated by spaces or commas.

4. Do one of the following:

   - Select a previously-defined department from the **Departmen**t dropdown list.
   - In the **Department** text box, type a new department name as you want it to appear in reports.

5. Click **OK**.

Editing a Department

You can make changes to the departments and the IP addresses or domains associated with the departments within the Department Management dialog box.

To edit a department:

1. On the Main Console, click **Tools > Departments**. The Department Management dialog box opens.
2. In the Department Management dialog box, select the department definition that you want to change, and click **Edit**. The Edit User and/or Department dialog box opens.
3. In the **IP or Domain** text box, type an IP address, IP address range, or domain name.
4. Do one of the following:
   - Select a previously-defined department from the **Department** dropdown list.
   - In the **Department** text box, type a new department name as you want it to appear in reports.
5. Click **OK** to save your changes, or click **Cancel** to return to the Department Management dialog box without saving your changes.

Running Firewall Activity Profiles from the Command Line

You can run any profile from the command line. To prevent collisions, the Scheduler handles command-line processing. When you run a profile, it is placed in the Scheduler queue until it can be processed.

Basic Information

Command-Line Help

Get help for any command by typing:

```
unknown
```

Files

Each profile type is referred to as a *cartridge*. The command syntax for running a profile specifies three files:

- The cartridge application extension
- The profile configuration
- The memorized report.

Following each command-line component section is a table that lists the files and their locations.

Syntax

The syntax for running a profile is:

"`runevent` *`cartridge profile memorized report distribution`*"

Note
The distribution option is not required.

Command-Line Components

The following sections provide descriptions of each component. You can use the name of the component, its file name, or its complete path and file name.

Cartridge

Use the following command to specify the cartridge:

```
/c="cartridge filename"
```

where *`cartridge filename`* is the cartridge application extension file name.

Cartridge	File name	Location
General	`wtm_FirewallOther.dll`	`\WebTrends Firewall Suite`
Incoming	`wtm_FirewallWebIn.dll`	`\WebTrends Firewall Suite`
Outgoing	`wtm_FirewallWebOut.dll`	`\WebTrends Firewall Suite`

Profile

Use `/p` or `/pf` to identify the profile. For example:

`/p=`*`profile description`*

or

`/pf=`*`profile file name`*

where *`profile description`* is the value of the Description parameter in the profile configuration file (or the profile description from the Main Console) and *`profile file name`* is the name of the profile configuration file.

Note
When you use the user interface to create profiles, the corresponding configuration files are named numerically beginning with `00000001.fir`. You can rename them.

The following table shows profile configuration file extensions.

Cartridge	File name	Location
General	`*.fir`	`\WebTrends Firewall Suite\wtm_FirewallOther\datfiles`
Incoming	`*.fwi`	`\WebTrends Firewall Suite\wtm_FirewallWebIn\Datfiles`
Outgoing	`*.fwo`	`\WebTrends Firewall Suite\wtm_FirewallWebOut\Datfiles`

Memorized Report

If you are running a report, use `/m` or `/mf` to specify the memorized report. For example, type

`/m=`*`memorized report description`*

or

`/mf=`*`memorized report file name`*

where *`memorized report description`* is the value of the Description parameter in the memorized report configuration file (or the memorized report name in the Create Report window of the user interface) and *`memorized report file name`* is the file name of the memorized report configuration file.

The following table shows memorized report file extensions.

Cartridge	File Name	Location
General	.mss	\WebTrends Firewall Suite\wtm_FirewallOther\datfiles
Incoming	.mss	\WebTrends Firewall Suite\wtm_FirewallWebIn\Datfiles
Outgoing	.mss	\WebTrends Firewall Suite\wtm_FirewallWebOut\Datfiles

Distribution Method

If you are running a report, use /s to specify how the report is saved or distributed. You can save a report to a file, transfer it using FTP, or send it as an email attachment.

Note

Using /s overrides the distribution method in the memorized report.

In this example:

```
/s="path and report name"
```

path and report name is the complete path of the location where you want to save the report and the file name for the report.

In this example:

```
/s="ftp://ftp site/path and report name
/username=username /password=password"
```

ftp site is the domain name of the FTP site; *path and report name* is the path from the root directory of the site and the file name for the report; *username* and *password* are the login name and password required to access the FTP site.

In this example:

```
/s="mailto:user@domain.com/c:\directory\report.html"
```

`user@domain.com` is the recipient of the report, and `c:\directory\report.html` is the directory and file name for saving the report. Note that there is no space between the recipient and the `/save-to` directory path.

Command-Line Examples

In these examples, the options and their values are displayed on separate lines. Each command is on a single line, with a single space preceding each option.

This example uses the profile and the memorized report descriptions for the General Firewall Activity cartridge. The report is saved to a local directory.

```
"runevent /c="wtm_FirewallOther.dll"
/p="General Firewall Activity"
/m="Default Summary (HTML)"
/s="c:\reports\report.htm""
```

This example uses file names for the General Firewall Activity cartridge to identify the cartridge, profile, and memorized report. This report is sent via email:

```
"runevent /c="wtm_FirewallOther.dll"
/pf="sample.fir"
/mf="DEFAULT_htm.mss"
/s="mailto:administrator@webtrends.com/c:\reports\report.html""
```

Designing Firewall Profiles

This section contains information that will help you design a Firewall or Web Activity Profile.

Report Content

The following table shows which type of profile you should use to get the report content you need.

To Report On	Using These Criteria	Use This Profile Type
Bandwidth	Users, by protocol	General Firewall Activity
	Users, by day of week	Incoming Firewall Activity
	Users, through proxy server	Incoming Firewall Activity
Categories	Categories of Web sites accessed by organization user	Outgoing Firewall Activity
Directories	Most accessed	Incoming Firewall Activity
Email	Top senders by direction, largest messages by direction	General Firewall Activity
Files	Files downloaded by an external user by type	Incoming Firewall Activity
	Files downloaded most by an internal user	Outgoing Firewall Activity
FTP	Upload activity, download activity, largest uploads/ downloads	General Firewall Activity

To Report On	Using These Criteria	Use This Profile Type
Geographic Information	By country, by North America, by city for external users	Incoming Firewall Activity
	Countries accessed by internal users	Outgoing Firewall Activity
Incoming Activity Summary	Activity by day, by hour	Incoming Firewall Activity
Incoming Activity Details	Activity by day, by hour	Incoming Firewall Activity
Organizations	Visited by internal users	Outgoing Firewall Activity
	Visited by external users	Incoming Firewall Activity
Outgoing Web Activity Summary	Activity by hour, by day	Outgoing Firewall Activity
Outgoing Web Activity Details	Activity by hour, by day	Outgoing Firewall Activity
Pages	Most/least requested pages, top entry pages, top exit pages, single access pages, paths through sites	Incoming Firewall Activity
Rules	By internal address, by external address, by protocol	General Firewall Activity
Telnet	Top telnet users by direction, largest telnet sessions	General Firewall Activity
Traffic	By direction, by time of day, by day of week	General Firewall Activity

To Report On	Using These Criteria	Use This Profile Type
Users	By region, organization, paths through site	Incoming Firewall Activity
	email senders, telnet sessions, FTP activity, users triggering firewall rules	General Firewall Activity
VPNs	IP addresses, events	General Firewall Activity

Chapter 4
Alerting and Monitoring

This chapter explains how to create and use profiles for the Alerting and Monitoring module. Firewall and Web Activity profiles are covered in “Firewall Profiles” on page 27.

The Alerting and Monitoring module keeps tabs on a number of different types of networked objects such as Web sites, files, event logs, services, ODBC database servers, and devices identified with an (IP) address—networked objects in your organization that must be running and available. If an event or a change of state occurs with a monitored object, the module can notify you, start recovery actions, or do both.

The module can also generate reports that help you track how reliable each monitored device or object is and determine how the software responded when any device failed. You can tailor your reports to see which objects tend to fail, when they do so, and for how long. You can also automate status reports that find the data you need and make it available when you need it most.

Alerting and Monitoring Profiles

Much like the firewall activity modules, you must first create a profile to take advantage of the features available with the Alerting and Monitoring module. Once you’ve created a profile, you can generate reports of response activity for that profile. See “Working with Reports” on page 201.

Use alerting and monitoring profiles to:

- Monitor Web-related devices and services for changes in state. For a complete list of devices you can monitor, see “Monitor Types” on page 148.
- Send and receive alerts when the state of a device changes or a particular event triggers an alert.
- Set up recovery actions to automatically restore devices and services that have stopped operating.
- Run alerting reports that contain information about the status of monitored devices and services.
- Create automated status reports.

How Alerting and Monitoring Works

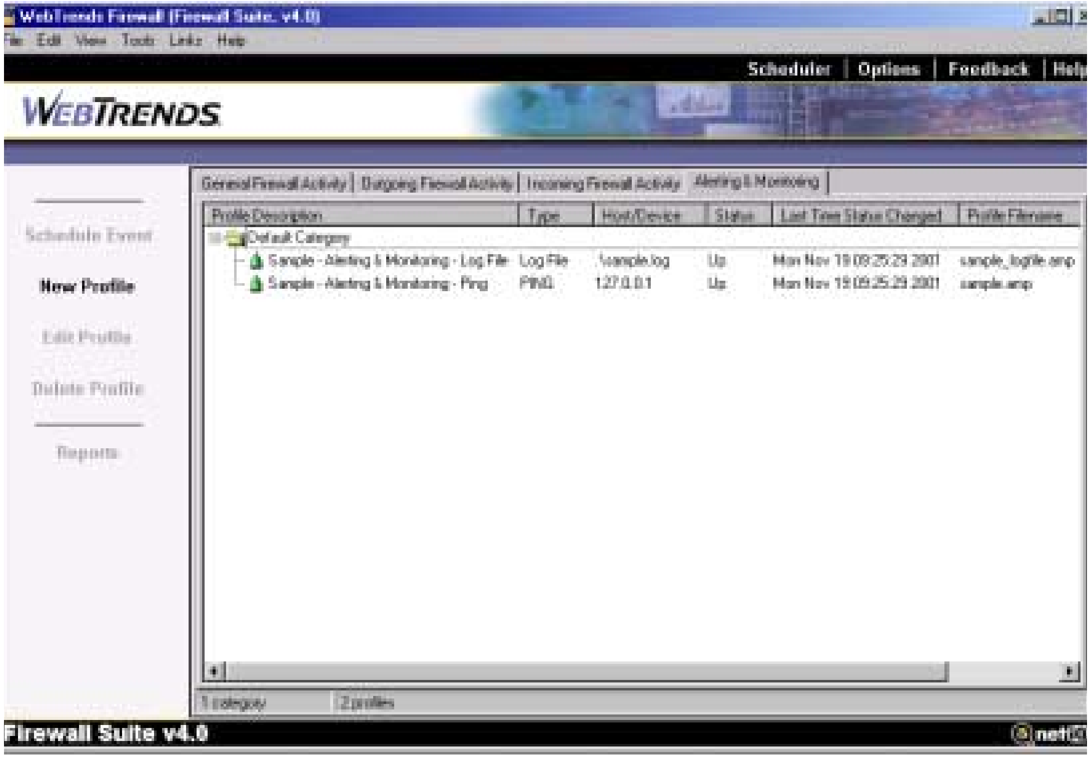
A *state* is a condition that can be repeatedly tested. For example, a network device that is operating is considered to be in an *up* state, while a device that is not operating is in a *down* state. The Alerting and Monitoring module functions by polling a target object—that is, using a Ping utility to repeatedly query the object about its state at user-specified intervals.

In contrast, an *event* is a unique occurrence. For example, an NT Event error that is entered in your Web server log a single time is an event. In addition to monitoring an object’s state, the module can watch for certain events that might occur.

When an object’s status varies from a certain preset state, or when a trigger event occurs, the Alerting and Monitoring module uses a pre-programmed method to alert you and takes a course of pre-determined recovery actions to respond to the event or return the object to its initial state.

Sample Alerting and Monitoring Profiles

It may be helpful to view a sample profile as you review the next section, “Alerting and Monitoring Profile Settings” on page 106. Two sample alerting and monitoring profiles are provided in the profile description list of the Main Console under the **Alerting & Monitoring** tab. In one sample, the profile specifies a network device to be monitored using the Ping utility, the response configuration specifies a single-phase response, and the response action profile specifies an audio alert.



WebTrends Firewall (Firewall Suite. v4.0)
File Edit View Tools Links Help
Scheduler | Options | Feedback | Help
WEBTRENDS
General Firewall Activity | Outgoing Firewall Activity | Incoming Firewall Activity | Alerting & Monitoring
Schedule Event
New Profile
Edit Profile
Delete Profile
Reports
1 category
2 profiles
Firewall Suite v4.0
netIQ

Profile Description	Type	Host/Device	Status	Last Time Status Changed	Profile Filename
Default Category					
Sample - Alerting & Monitoring - Log File	Log File	.\sample.log	Up	Mon Nov 19 09:25:29 2001	sample_logfile.amp
Sample - Alerting & Monitoring - Ping	PING	127.0.0.1	Up	Mon Nov 19 09:25:29 2001	sample.amp

To view the sample Alerting and Monitoring profile:

1. Select the **Alerting & Monitoring** tab on the Main Console.
2. Select the profile called "Sample - Alerting & Monitoring - Ping".
3. Click **Edit > Profile** from the Main menu. The sample profile opens.
4. Select the various tabs in the Edit Alerting & Monitoring Profile dialog box to view the settings specified for the profile.

Alerting and Monitoring Profile Settings

When creating an alerting and monitoring profile, you must define which device or object to monitor, when to monitor the device, what event or change in state for that device should trigger a response, and what action or actions should occur when the response is triggered. These elements are discussed in the following sections.

Configuring some of these elements requires drilling down several dialog boxes deep. To familiarize you with these dialog boxes and their settings, instructions for creating an alerting and monitoring profile follow this section.

Device or Object Being Monitored

When first creating an alerting and monitoring profile, you must specify which device to monitor and point to the device so that the Alerting and Monitoring module can access it. For a complete list of devices you can monitor, see “Monitor Types” on page 148.

Monitoring Schedule

The monitoring schedule specifies when the alerting and monitoring profile should actively monitor the specified device or object by polling it with the Ping utility. The monitoring schedule also includes the frequency with which to poll the device, and the amount of time to wait after a failure occurs before initiating a response.

Response Settings

The combination of settings and dialog boxes in which you specify:

- The device state change or event that triggers a response. Use the Response Settings dialog box to make these selections.
- The schedule for applying the response. Use the Edit Response Schedule dialog box to specify these settings.
- The set of actions that constitute the response, the order in which to apply those actions, and how many times to apply each action. Use the Select Response Configuration, Response Configuration Settings, and the Response Profile Phase Settings dialog boxes as needed to specify these settings.
- The specific configurations for each action that constitutes the response. Use the Select Response Actions dialog boxes and the individual configuration dialog boxes for each possible action to specify the appropriate settings.

Response Schedule

The response schedule specifies how and when to apply response configurations in reaction to an event or change of state in a monitored device. You can create new response schedules, or you can edit, copy, or link to existing response schedules.

Once you have created and saved a response schedule, you can use it for other monitoring and alerting profiles.

Response Configuration

A response configuration specifies the response or responses you want to occur for a given time period when a state changes or an event occurs. This includes any response actions and those actions' settings, and if applicable, the settings that specify when to escalate from one phase to the next.

Once you have created and saved a response configuration, it can be used in multiple response schedules.

A response can be either of two types: single phase or multi phase.

Single-phase applies any assigned actions simultaneously. For example, when a server goes down, a pager alert could be sent to the server administrator, while simultaneously, the module could attempt to reboot the server.

Note

A response phase can consist of a single action or multiple actions.

Multi-phase applies to an assigned action or actions in phases. With the previous example, when the server goes down, the computer could first try rebooting. This would be the first phase. Then, if the computer does not come back up (change state) for a specified amount of time or number of attempts at rebooting, a second phase could be initiated, in which the server administrator is sent an email message and is also paged.

With a multi-phase response, you can set each phase to:

- Wait a specified number of seconds before repeating the response action.
- Repeat a phase a specified number of times before escalating to the next phase of response action.
- Repeat a phase until the profile state changes, which causes the response profile to reset itself.

Response Actions

A single action, such as a pager alert, a system reboot, or an audio alert that can be configured to occur in a specified manner when an event or a change of state for a device or object triggers a response. Once the settings for a response action have been configured, they can be used within either a single or multi phase response.

Possible response actions include:

- Sending an audio or email alert
- Broadcasting an alert to a pager
- Passing an SNMP trap
- Running a program
- Running a group of responses
- Rebooting a device
- Restarting a Windows service

A response action can initiate a single action or, in the case of running a group of responses, can initiate multiple successive actions. You can use the same response action with different response configurations.

Creating an Alerting and Monitoring Profile

This procedure describes the sequence of panels in the New Profile wizard for creating an alerting and monitoring profile. It describes the information required in each panel to set up the profile. Refer to the online help in each panel for more information.

Note
You can create an unlimited number of alerting and monitoring profiles.

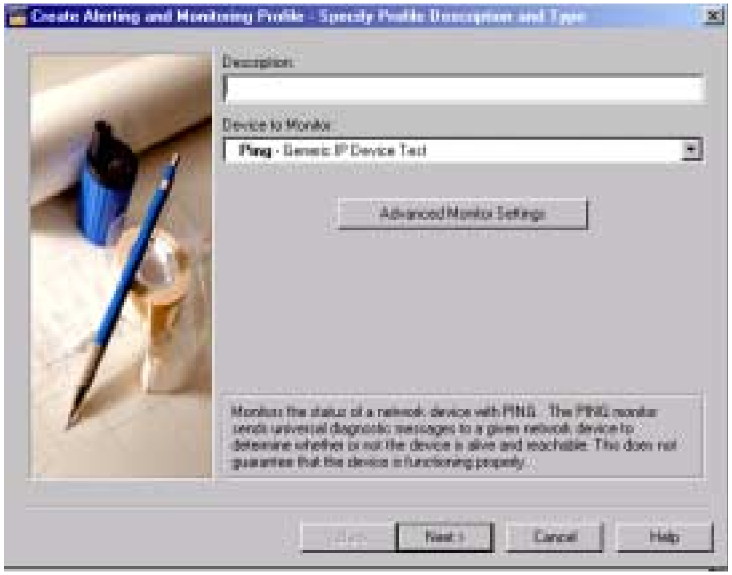
To create a new alerting and monitoring profile:

1. Select the **Alerting & Monitoring** profile type tab on the Main Console.
2. From the File menu or the Tasks area select **New Profile**. The New Profile wizard opens to the Specify Profile Description and Type dialog box.

Specify Profile Description and Type

In this dialog box, you specify a name for the alerting and monitoring profile, select a device to monitor, and specify any dependencies the profile you are creating has on other profiles. See “Defining Advanced Monitor Options” on page 144 for more information on dependencies.

Note
You can create an unlimited number of alerting and monitoring profiles.


Create Alerting and Monitoring Profile - Specify Profile Description and Type
Advanced Monitor Settings
< Back
Next >
Cancel
Help

Description:

Device to Monitor: **Ping** - Generic IP Device Test

Monitors the status of a network device with PING. The PING monitor sends universal diagnostic messages to a given network device to determine whether or not the device is alive and reachable. This does not guarantee that the device is functioning properly.

To specify the profile name and device to monitor:

1. Type a name for the profile in the **Description** text box. The description identifies the profile in the Profile Description list in the Main Console and is used as a sub-heading for reports.
2. Select the device you want to monitor with this profile from the **Device to Monitor** dropdown list.

   Note
   The list is sorted by device type: IP Device, NT System Monitors, SNMP Monitors, LAN Computer Monitors, Disk and File Monitors. For a list of monitors with descriptions, see “Monitor Types” on page 148.

3. *If you wish to set dependencies on other profiles*:

   a. Click **Advanced Monitor Settings** to set dependencies on other profiles monitoring other objects. The Advanced Monitor Settings dialog box opens. See “Defining Advanced Monitor Options” on page 144.

   b. In the Monitor Profiles list, select the check boxes of any profiles that the current profile depends on.

      Notes
      The current profile is enabled only when the devices for the profiles you select here are active. If one of these profiles goes down, the current profile is disabled.

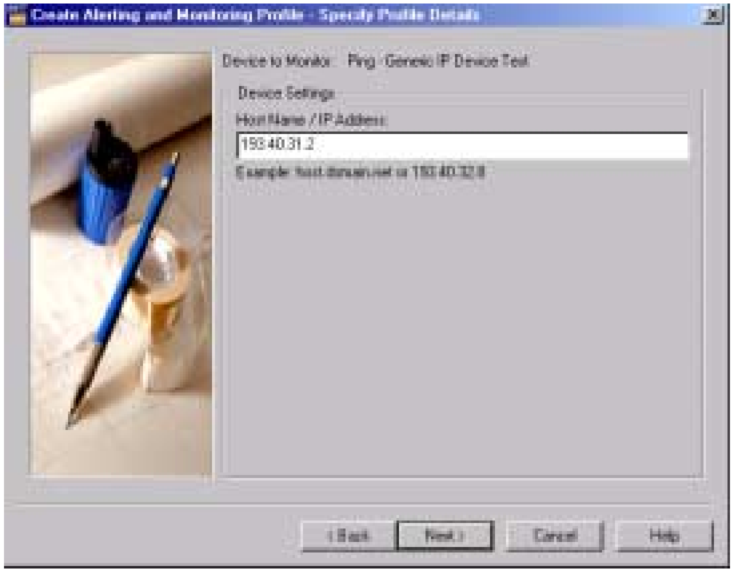
      If you are editing an existing profile, click **Flush Log File** in this dialog box to delete the profile’s log data. Use this option only after you have created the reports you need.

   c. Click **OK** to return to the Specify Profile Description and Type dialog box.

4. Click **Next**. The Specify Profile Details dialog box opens.

Specify Profile Details

Use this dialog box to enter the location of the device to be monitored and settings relevant to the selected device. The fields that appear in this dialog box vary according to the device selected.


Create Alerting and Monitoring Profile - Specify Profile Details
< Back
Next >
Cancel
Help

Device to Monitor: Ping - Generic IP Device Test

Device Settings

Host Name / IP Address:

193.40.31.2

Example: host.domain.net or 193.40.32.8

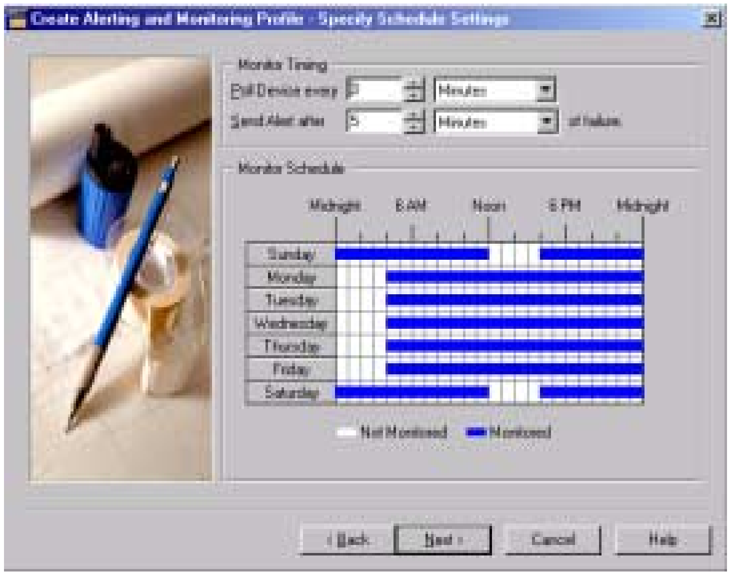
To specify profile details:

1. Fill in the fields in this dialog box, clicking the **Help** button in the dialog box to get device-specific information.

2. Click **Next**. The Specify Schedule Settings dialog box opens.

Specify Monitoring Schedule Settings

Use this dialog box to enter the frequency with which you want to poll the monitored device and specify how long to wait after a device fails before sending an alert. Then set up a weekly monitoring schedule using the monitor schedule. For more information, see “Monitoring Schedule” on page 107.



Poll Device every [illegible] Minutes

Send Alert after 5 Minutes of failure

To specify the monitor schedule settings:

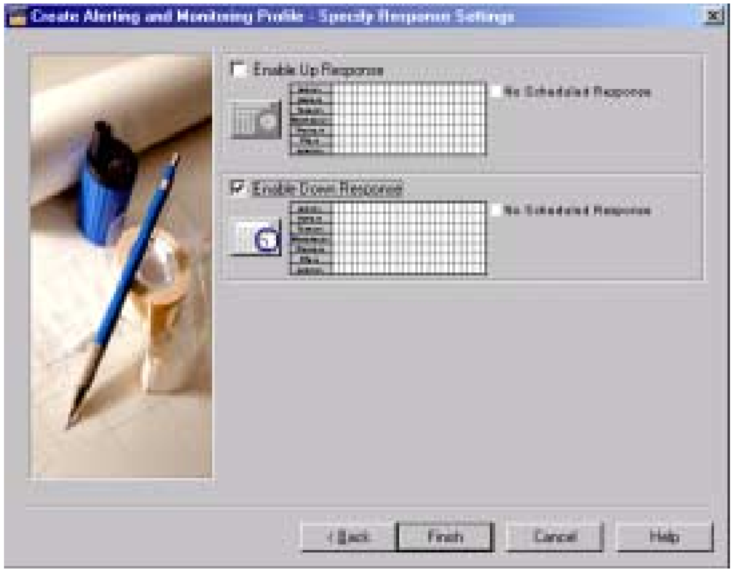
1. Enter the frequency with which you want the Ping utility to poll the monitored device by typing or scrolling to a number to set the **Poll Devices every** values in the Monitor Timing area and in the dropdown box. Select either Seconds or Minutes as the time unit.
2. Enter the amount of time after a device has failed to initiate a response by typing or scrolling to a number in the **Send Alert after... of failure** values in the Monitoring area and in the dropdown box. Select either Seconds or Minutes as the time unit.

3. Set the Monitor Schedule by clicking on or off individual grid squares or by clicking and dragging vertically or horizontally to select or un-select days and hours. The areas in blue indicate the times that this profile will actively monitor the device.

4. Click **Next**. The Specify Response Settings dialog box opens.

Specify Response Settings

What you see in this dialog box depends on which device you have chosen to monitor. Some devices allow you to monitor for an “up” state or a “down” state—that is, whether the device is functional or accessible to the Alerting and Monitoring module. Other devices allow you to monitor an additional state particular to the device. You can choose to create a response schedule for any or all of the states available with that device. You can also create and reuse response schedules with different monitoring profiles.


Create Alerting and Monitoring Profile - Specify Response Settings
< Back
Finish
Cancel
Help

☐ Enable Up Response

☐ No Scheduled Response

☑ Enable Down Response

☐ No Scheduled Response

Choosing Response Options

To create a response schedule for the device you want to monitor, select the state or states to which you want the module to respond. You can specify more than one state by creating multiple schedules. For example, if you want to be notified when a server is down and when it comes back up, create response schedules for both states.

- **Enable Up Response**. Select this option if you want to receive notification and/or trigger a response when the monitored object or device is "up," as indicated by its ability to respond to the module's polling request. You would choose this option if the normal state for the object is down or inaccessible, or if the object you want to monitor does not yet exist and you want notification when it becomes available, active, or accessible.

  For example, if you want to be alerted when your Web server has created and saved a new log file for processing, configure the alerting and monitoring module to poll the directory where the log file is crated. Ordinarily, that file will not exist until the server creates it, so its state will be "down." Once the server creates the file, however, its state will change to "up," and the module can notify you.

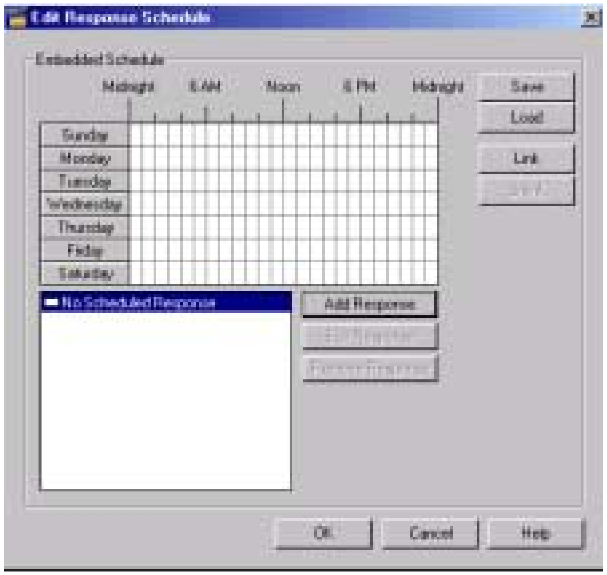
- **Enable Down Response**. Select this option if you want to receive notification and/or trigger a response when the monitored object or device goes "down," which means that it no longer responds to the module's polling request. Choose this option if the monitored object or device is normally active, available, or accessible and you want notification when that state changes.

  For example, if you want to monitor the state of your Web server to ensure its availability, you would have the module poll it periodically to check its state. If the server fails to respond to the polling request, after a specified time period of non-responsiveness, the module could notify you that the server is down and initiate the response action you have programmed into your response profile for that condition.

- **Enable [other] Response**. Select this option if you want to receive notification and/or trigger a response when the monitored object or device changes its state from an expected state. What happens to change the state from the expected state to a different state depends on the nature of the object or device property you want to monitor.

To specify response settings in the response schedule:

1. In the Specify Response Settings dialog box, select one or more response states to configure, for example Enable Up Response, or Enable Down Response.
2. Click the button located below the check box for a selected response state to open the Edit Response Schedule dialog box.



3. In this dialog box, specify which actions the module should take when the monitored device changes state. Using this dialog box you can:

   - *Create a new response schedule* by clicking **Add New** and defining new response configurations and their response actions. If you choose to save the response schedule, you can use it later with another monitoring profile. For more information, see “To create a response schedule:” on page 119.
   - *Edit an existing response that is already associated with the profile* by selecting a response schedule in the list of response schedules and clicking **Edit New**.
   - *Dissociate an existing response schedule from the current profile* by selecting a response schedule in the list of response schedules and clicking **Remove Response**.
   - *Load an existing response schedule* by clicking **Load**, then altering and saving it to suit the current monitoring profile. A loaded schedule is a standalone copy of the original response schedule. If you make changes to the loaded (copied) schedule, changes to it only affect the monitoring profile to which it is attached. When you modify the response schedule, you are asked to give it a new name. The schedule is identified by this name when loading or linking to it from other monitoring profiles.
   - *Link to an existing response schedule* by clicking **Link** to apply its settings to the current monitoring profile. Because the monitoring profile is only linked by reference to the response schedule, changes made to the schedule affect *every* monitoring profile linked to it. Typically, you link to a schedule if several monitoring profiles need to have the same response schedule applied and you do not want to re-enter the settings for each profile.

     Conversely, you can unlink from an existing profile by clicking **Unlink** to dissociate the current monitoring profile from a linked response schedule.

- *Save a response schedule* by clicking **Save** to save the response schedule settings. Once saved, you can use a loaded or new response schedule with other profiles. If you made changes to a linked profile, saving these changes affects all other profiles to which the response schedule is linked.

4. If necessary, add another response schedule for the current response state, or add a response schedule for another state.

Note
You can add more than one response schedule for a given response state.

5. Click **Finish** to complete your Alerting and Monitoring profile. It now appears in your Profile Description list in the Main Console.

Adding a Response Schedule

You can create a response schedule:

- While creating a new Monitoring and Alerting profile in the Specify Response Settings dialog box.
- While editing an existing Alerting and Monitoring profile using the **Response Settings** tab.

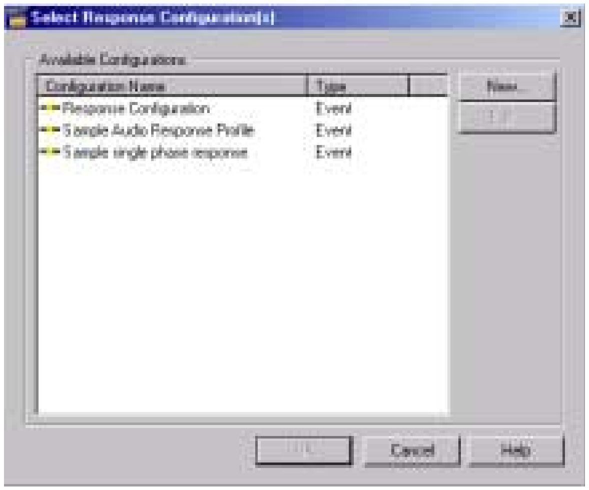
When a response schedule is complete, its name appears in the Available Schedules list in the Select a Response Schedule dialog box. You can use this response schedule with the current or other profiles by selecting it from this list.

If the response schedule appears in the Edit Response Schedule dialog box's list, then it is active for the current Alerting and Monitoring profile.

The following procedure follows the steps for creating a response schedule while editing an existing Alerting and Monitoring profile. This procedure could be followed just as well when creating a new profile.

To create a response schedule:

1. Select an Alerting and Monitoring profile from the Profile Description list in the Main Console.
2. Click **Edit** on the toolbar and select the **Response Settings** tab.
3. Click the button located below the check box for a selected response state to open the Edit Response Schedule dialog box.
4. Click **Add Response**. The Select Response Configuration(s) dialog box opens.



Configuration Name	Type
Response Configuration	Event
Sample Audio Response Profile	Event
Sample single phase response	Event

5. *To use an existing response configuration*, select an existing response configuration from the list at the bottom of the dialog box and click **OK** to exit.
6. *To edit an existing response configuration*, select an existing response configuration and click **Edit**. Skip to Step **8**.
7. *To create a new response configuration*, click **New**.

8. Type a name for the Response Profile. This name will appear in the list of Response profiles. You can select it for other Alerting and Monitoring profiles.

9. Select one of the following response types:

   – **This is a single phase Event Response Profile**. Select this option to create a response configuration that triggers all of its component response actions once, simultaneously, before resetting.

   – **This is a multi phase Escalating State Response Profile**. Select this option if the condition that originally triggered the response persists for a set time, and you wish to escalate to a new phase that has new or different response actions.

10. Choose one of the following options:

    – **New Phase** (only available if you selected multi phase). Choose this to add a new phase of response actions that will be applied according to the settings. See “Adding or Editing a New Phase” on page 120 to continue this procedure.

    – **Edit Phase**. Select an existing phase from the Response Details list, and click **Edit Phase** to open the Response Profile Phase Settings dialog box.

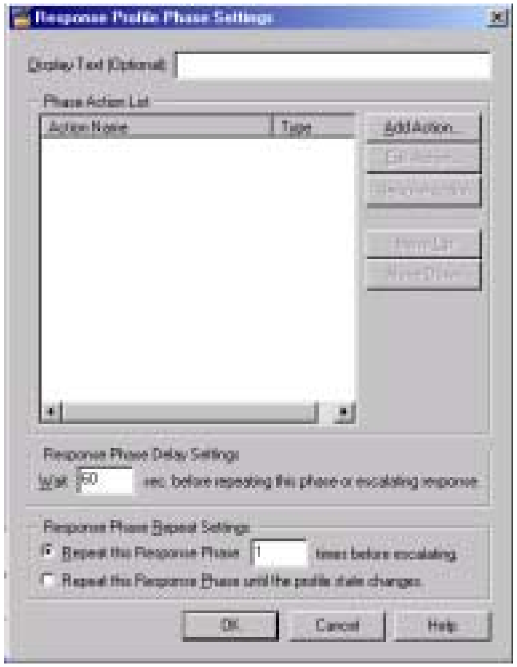
11. Click **OK**.

Adding or Editing a New Phase

With a single phase response configuration, you can edit the existing phase (there will always be a default phase called "Single Phase" with no actions configured for it). With a multi phase response configuration, you can add new phases or edit existing phases. This procedure assumes the Response Configuration Settings dialog box is already open.

To add or edit a new phase:

1. Click **New Phase** or select an existing phase and click **Edit Phase**. The Response Profile Phase Settings dialog box opens.



Display Text (Optional):

Response Phase Delay Settings

Wait: 60 sec. before repeating this phase or escalating response

Response Phase Repeat Settings

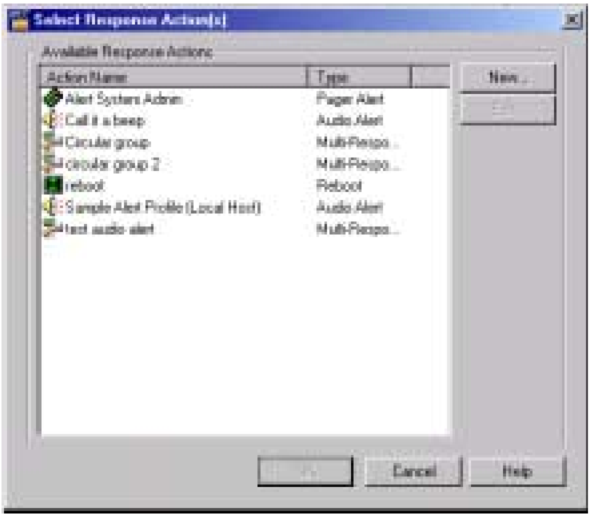
● Repeat this Response Phase 1 times before escalating

○ Repeat this Response Phase until the profile state changes

2. Enter a descriptive name in the **Display Text (Optional)** text box, or edit the existing name. This name will appear in the Response Details list.

3. Select from among the following options:

- Add a new action. Click **Add Action** to open the Select Response Action(s) dialog box, in which you may add and configure an action using the steps that follow.



Action Name	Type
Alert System Admin	Pager Alert
Call it a beep	Audio Alert
Circular group	Multi-Respo...
circular group 2	Multi-Respo...
reboot	Reboot
Sample Alert Profile (Local Host)	Audio Alert
test audio alert	Multi-Respo...

- Click **New** to configure a new action and make it available in the Available Response Actions List. See “Adding and Configuring Response Actions” on page 123 for detailed instructions on configuring the various types of available response actions.
- Select an action from the Available Response Actions List and click **Edit** to change the settings for the selected response action. Make changes to the selected response action as needed. See “Adding and Configuring Response Actions” on page 123 for detailed instructions on configuring the various types of available response actions.

- Remove an action. Select an action in the Phase Action List, then click **Remove Action** to remove the action from the list.
- Reorder the action list. Select an action in the Phase Action List, then click **Move Up** or **Move Down** to specify the order in which you want the actions to be applied. Although the actions occur almost simultaneously, they are applied in the order in which they appear in the Phase Action List.

4. *If the* ***Wait N sec. before repeating this phase or escalating response*** *field is available* (for multi phase responses only), type a number of seconds to wait before repeating this phase or escalating to the next phase.

5. *If the Response Phase Repeat settings are available* (for multi phase responses only), do one of the following:

- If you want a specific number of repetitions, select **Repeat this Response Phase N times before escalating** and type a number of times to repeat.
- If you want the phase repeated until the profile state changes, select **Repeat this Response Phase until the profile state changes**.

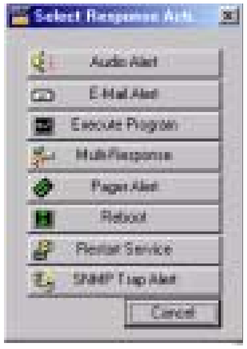
6. Click **OK**.

Adding and Configuring Response Actions

You can add and configure a response action from the Select Response Action(s) dialog box. You can access this dialog box while editing a profile, or while creating a new profile using the New Profile wizard. You can get to this dialog box by following the instructions up through Step **3** for “Adding or Editing a New Phase” on page 120.

To add and configure a response action profile:

1. In the Select Response Actions dialog box, click **New**. The Select Response Action dialog box opens with all possible response actions available.



2. Select a response action and the configuration dialog box for that action opens.
   - **Audio Alert**: See “Creating an Audio Alert” on page 125.
   - **E-mail Alert**: See “Creating an Email Alert” on page 126.
   - **Execute Program**: See “Creating an Execute Program Response Action” on page 128.
   - **Multi-Response**: See “Creating a Multi-Response Action” on page 129.
   - **Pager Alert**: See “Creating a Pager Alert” on page 130.
   - **Reboot**: See “Creating a Reboot Response Action” on page 138.
   - **Restart Service**: See “Creating a Restart Service Response Action” on page 140.
   - **SNMP Trap Alert**: See “Creating an SNMP Trap Alert” on page 141.
3. Complete the settings for the response action, and click **OK**. You return to the Select Response Action(s) dialog box with the newly configured response action appearing in the list of Available Response Actions.
4. Click **OK**. You return to the Response Profile Phase Settings dialog box.

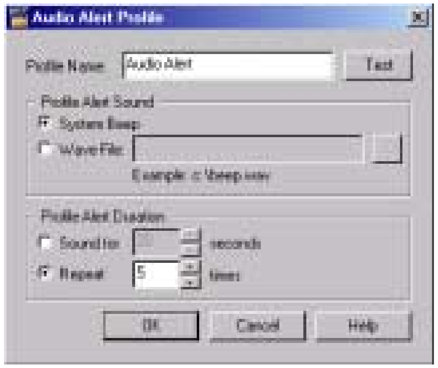
Creating an Audio Alert

An Audio Alert plays a system sound, such as a beep, when the Alerting and Monitoring module detects a change in state of the monitored object or device.

See “Adding and Configuring Response Actions” on page 123 for the steps to access the Select Response Action(s) dialog box.

To create an audio alert:

1. Click **New** to open the Select Response Action (type) dialog box.
2. Select **Audio Alert**. The Audio Alert Profile dialog box opens.



Audio Alert Profile

Profile Name: Audio Alert

Profile Alert Sound

● System Beep

○ Wave File:

Example: c:\beep.wav

Profile Alert Duration

○ Sound for 30 seconds

● Repeat 5 times

3. Type a name for the audio configuration in the **Profile Name** text box.

   It may be useful to name this profile something like Audio Alert. Whenever you need an audio alert, you can select it by name to use with other response phases for this or other Response profiles.

4. Select the sound to use:

   – **System Beep** plays a predefined beep.

   – **Wave File** plays a `.WAV` file. Click **Browse** to specify the exact location of the file.

5. Specify the duration by choosing one of the following options:

   - **Sound for** sets the number of seconds that the sound will play. Select the number of seconds to play the sound.
   - **Repeat** specifies the number of times to repeat the sound.

6. Click **Test** to make sure your alert works.

7. Click **OK**.

Creating an Email Alert

An E-mail Alert sends an email message to the address you specify when the Alerting and Monitoring module detects a change in state of the monitored object or device.

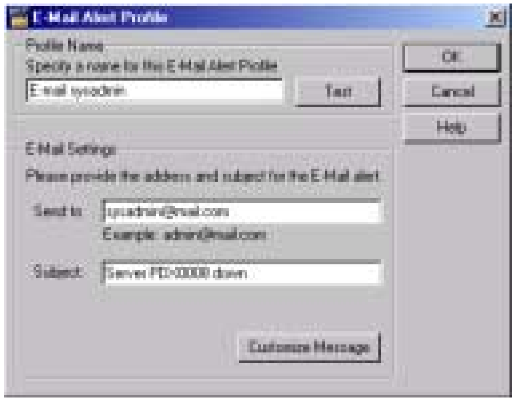
Note

You must configure your email server settings in the General Options dialog box for email alerts to work.

See “Adding and Configuring Response Actions” on page 123 for the steps to access the Select Response Action(s) dialog box.

To create an email alert:

1. Click **New** to open the Select Response Action (type) dialog box.
2. Select **E-Mail Alert** from the Select Response Action dialog box. The E-Mail Alert Profile dialog box opens.



Specify a name for the E-Mail Alert Profile

E-mail sysadmin

Please provide the address and subject for the E-Mail alert

Send to: sysadmin@mail.com

Example: admin@mail.com

Subject: Server PID>00000 down

3. Type a description for this alert in the **Profile Name** text box.
4. Type the email address to which you wish to send the alert in the **Send To** text box.
5. Type the text that you want to appear on the subject line of the message in the **Subject** text box.
6. Click **Customize Message** to change the message sent for the alert. See “Customizing Text Messages” on page 142 for details.
7. Click **Test** to make sure your alert works.
8. Click **OK**.

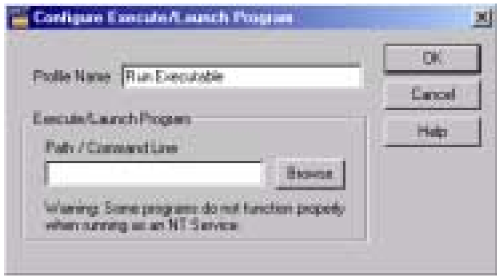
Creating an Execute Program Response Action

The Execute Program response launches a specified program when the Alerting and Monitoring module detects a change in state of the monitored object or device.

See “Adding and Configuring Response Actions” on page 123 for the steps to access the Select Response Action(s) dialog box.

To create a response action:

1. Click **New** to open the Select Response Action (type) dialog box.
2. Select **Execute Program** from the Select Response Action dialog box. The Configure Execute/Launch Program dialog box opens.



Profile Name: Run Executable

Warning: Some programs do not function properly when running as an NT Service

3. Type a name in the **Profile Name** text box.
4. Type the path to the executable file or command line in the **Path/ Command Line** text box. If desired, click **Browse** to navigate to an executable file.
5. Click **OK**.

Creating a Multi-Response Action

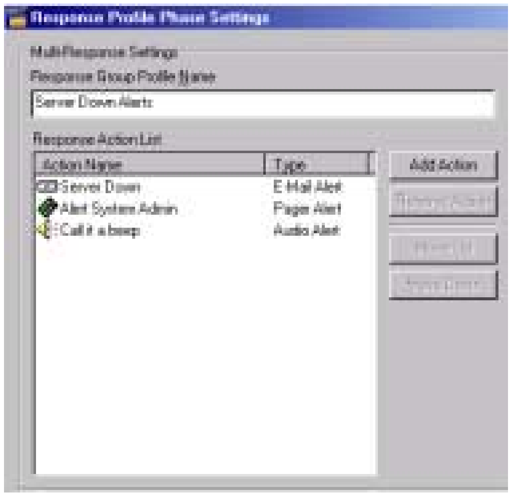
A multi-response action carries out a series of response actions when the Alerting and Monitoring module detects a change in state for the monitored object or device. Response actions can include one or more of the existing response action types such as audio alert or pager alert. A response action can also consist of another multi-response action.

See “Adding and Configuring Response Actions” on page 123 for more information about accessing the Select Response Action(s) dialog box.

To configure a multi-response action:

1. Click **New** to open the Select Response Action (type) dialog box.
2. Select **Multi-Response** from the Select Response Action dialog box. The Response Profile Phase Settings dialog box for a multi-response action opens.
3. In the **Response Group Profile Name** text box, type a name for this group of response actions.
4. Click **Add Action** to open the multi-response version of the Select Response Action(s) dialog box, which lists the available configured actions you can select and add to your multi-response action.

5. Select an existing action in the list and click **Select**. You return to the Response Profile Phase Settings dialog box, and the selected item appears in the Response Action List.



Response Group Profile Name: Server Down Alerts

Response Action List

Action Name	Type
Server Down	E-Mail Alert
Alert System Admin	Pager Alert
Call it a beep	Audio Alert

6. Add more actions as needed by repeating Steps 2 and 3.

7. Click **OK**. You return to the Select Response Action(s) dialog box, and the new multi-response alert is added to the Available Response Actions list.

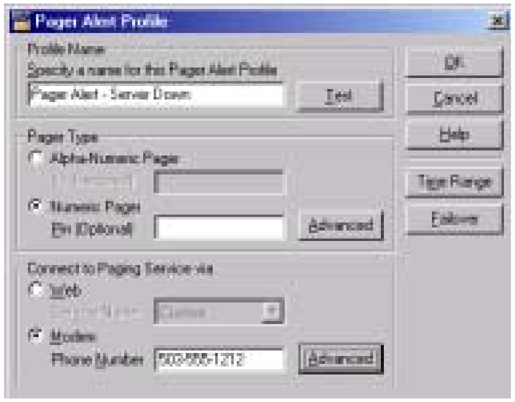
Creating a Pager Alert

A pager alert sends a page when the Alerting and Monitoring module detects a change in state of the monitored object or device.

See “Adding and Configuring Response Actions” on page 123 for the steps to access the Select Response Action(s) dialog box.

To create a pager alert:

1. Click **New** to open the Select Response Action (type) dialog box.
2. Select **Pager Alert** from the Select Response Action dialog box. The Pager Alert Profile dialog box opens.



Pager Alert Profile

Profile Name

Specify a name for this Pager Alert Profile: Pager Alert - Server Down

Pager Type

○ Alpha-Numeric Pager

● Numeric Pager

Pin (Optional):

Connect to Paging Service via

○ Web

● Modem

Phone Number: 503-555-1212

3. In the **Profile Name** field, type a description for this alert.
4. In the Pager Type section, specify the type of pager:
   - – Select Alpha-Numeric Pager if the pager accepts messages with either letters or numbers. Specify the ID number needed to send the page in the **ID** field.
   - – Click **Advanced** if you need to further define the pager settings. See “Defining Alpha-Numeric Pager Settings” on page 132 for details.
   - – Select Numeric Pager if the pager accepts only messages with numbers. If your paging service requires a PIN, type it in the **PIN** text box.
   - – Click **Advanced** if you need to further define the pager settings. See “Defining Numeric Pager Settings” on page 134 for details.

5. Specify how your pager can be accessed:

   - Select **Web** if your paging service supports Web paging, then select your paging service from the list.
   - If your service doesn't appear in the list, select the Custom list item, and click **Advanced** to set up your paging service options. "Defining Custom Web Paging Settings" on page 134 for details.
   - Select **Modem** to access your pager through a modem connection, then type the complete telephone number in the **Phone Number** text box. Click **Advanced** to display the Modem Settings dialog box if you need to modify the default modem settings. See "Changing the Modem Settings" on page 136.

6. Click **Test** to make sure your alert works.

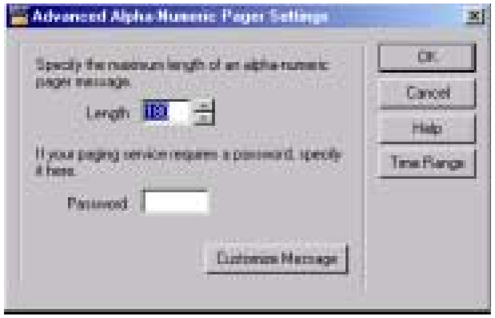
7. Click **OK**.

Defining Alpha-Numeric Pager Settings

Use the Advanced Alpha-Numeric Pager Settings dialog box to define a message length or password for alpha-numeric paging.

To define settings:

1. In the Pager Alert Profile dialog box, select **Alpha-Numeric Pager** in the Pager Type area.
2. Click **Advanced** in the Pager Type area. The Advanced Alpha-Numeric Pager Settings dialog box opens.



Specify the maximum length of an alpha-numeric pager message.

Length: 180

If your paging service requires a password, specify it here.

Password:

3. Use the **Length** list box to define the length of the message your pager will accept.

   Most alpha numeric pager will accept messages with up to 180 characters. Some have a higher restriction on the number of characters for each message. If this is the case for your pager, use this setting to specify the maximum length of the message sent by Firewall Suite your pager will accept. Select or type the maximum number of characters that may be sent to this alpha-numeric pager.

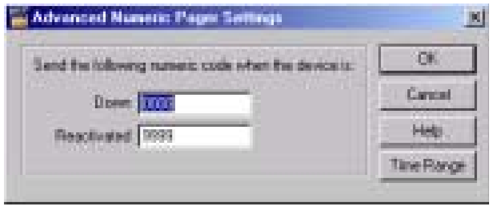
4. If your service requires a password, type the pager's password in the **Password** text box.
5. Click **Customize Message** to tailor the message that is sent for the alert. See “Customizing Text Messages” on page 142 for details.
6. Click **Time Range** to open the Edit Schedule dialog box in which you can specify when you want the alert enabled.

Defining Numeric Pager Settings

You can modify the pager message sent when the device goes down, and the message sent if the device has recovered.

To define settings:

1. In the Pager Alert Profile dialog box, select **Numeric Pager** in the Pager Type area.
2. Click **Advanced** in the Pager Type area. The Advanced Numeric Pager Settings dialog box opens



Advanced Numeric Pager Settings

Send the following numeric code when the device is:

Down: 0000

Reactivated: 9999

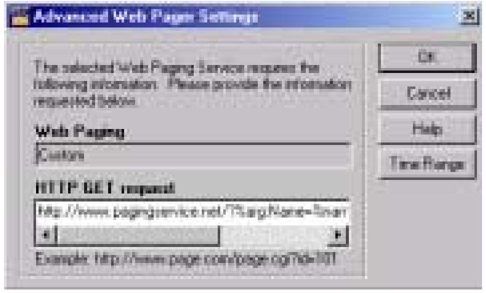
3. In the **Down** text box, type the message to be sent when the device is down. The default message is 0000.
4. In the **Reactivated** text box, type the message to be sent when the device is reactivated. The default alert is 9999.
5. Click **Time Range** to open the Edit Schedule dialog box in which you can specify when you want the alert enabled.

Defining Custom Web Paging Settings

Use these settings if your paging service supports Web paging, but your service doesn't appear in the **Service Name** dropdown list.

To define custom Web paging settings:

1. In the Pager Alert Profile dialog box, select **Web** in the Connect to Paging Service via area,
2. In the **Service Name** dropdown list, select **Custom**.
3. Click **Advanced** in the Connect to Paging Service via area. The Advanced Web Pager Settings dialog box appears.



The selected Web Paging Service requires the following information. Please provide the information requested below.

Web Paging: Custom

HTTP GET request: http://www.pagingservice.net/?arg:Name=%nan

Example: http://www.page.com/page.cgi?id=101

4. In the **HTTP Get Request** text box, copy the URL from the paging service Web page that provides a paging form. The URL should specify the Get request, and look something like this:

   ```
   http://www.pagingservice.net?arg:Date=%date%&To=%id%&Message=%msg%
   ```

   In this example, you would type values for *date*, *id*, and *msg*. The arguments and the data you use vary according to paging service. See “Custom Web Paging Variables” on page 136 for details on using variables to include user defined values.

5. Click **Time Range** to open the Edit Schedule dialog box in which you can specify when you want the alert enabled.
6. Click **OK** to save your changes and close the dialog box.

Custom Web Paging Variables

If your paging service doesn't appear in the Web paging service list in the Pager Alert dialog box, you can set it up using a custom Web paging alert. You can use any of the variables listed below in your custom Web paging settings.

The following table shows the supported variables.

This variable:	Does this:

`%arg:`*`title=`*
`default value``%`
	Adds a field to the Advanced Web Pager Alert dialog box displaying the default value you specify.

`%id%`	Includes the paging ID specified in the Pager Alert dialog box.
`%msg%`	Includes the pager alert message. For numeric pagers, this is the alert specified in the Advanced Numeric Pager settings dialog box.
`%num%`	Includes the phone number used in the Pager dialog box.

`??`*`post data`*	Indicates that the preceding URL is an HTTP post. For example:
	`http://www.pagingservice.net??arg:Date=`
	`%date%&To=%id%&Message=%msg%`

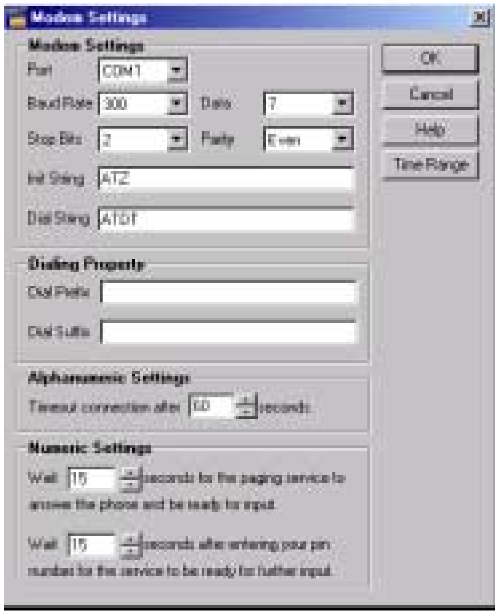
Changing the Modem Settings

If you need to modify the modem default settings for your pager alert, you can do so in the Modem Settings dialog box.

To change modem settings:

1. In the Pager Alert Profile dialog box, select **Modem** in the Connect to Paging Service via area.
2. Enter the complete phone number (area code + number) in the **Phone Number** text box.

3. Click **Advanced** in the Connect to Paging Service via area. The Modem Settings dialog box opens.



Modem Settings

Modem Settings

Port: COM1

Baud Rate: 300

Data: 7

Stop Bits: 2

Parity: Even

Init String: ATZ

Dial String: ATDT

Dialing Property

Dial Prefix:

Dial Suffix:

Alphanumeric Settings

Timeout connection after 60 seconds

Numeric Settings

Wait 15 seconds for the paging service to answer the phone and be ready for input.

Wait 15 seconds after entering your pin number for the service to be ready for further input.

4. Make any needed changes to the following settings:

- **Port**. Select the port used by the modem.
- **Baud Rate**. Select the rate of data transmittal (bps).
- **Data**. Select the number of bits in a data word.

  The default is `7`, which is usually right for pager services. The pager service provider can give you a description of the service's settings. It looks something like `[Data][Parity][Stop]`. For example, `8N1`, `7E2`, `7E1`.
- **Stop Bits**. Select the number of stop bits terminating each data word (either 1 or 2). This option defaults to the most common setting.
- **Parity**. Select the type of data checking that you want to use (odd, even or none).

- **Init String**. Type any necessary modem initialization string.
- **Dial String**. Type the command that tells the modem to start dialing.
- **Dial Prefix**. Type any prefix that must be entered before dialing the phone number. For example, type 9 if you are required to enter 9 before dialing the phone number.
- **Dial Suffix**. If you must enter a suffix such as a dialing code or an extension number, type the number here.

Note
You can select the number of seconds that Firewall Suite should wait before entering the suffix. Use commas to specify the number of seconds to wait. One comma is equal to 2 seconds of delay.

- **Timeout connection after *x* seconds**. Select the number of seconds to wait before ending an attempted transmission.
- **Wait**. Select the number of seconds for each waiting period. If your connection doesn’t require a waiting period, leave the text box empty.

5. Click **Time Range** to open the Edit Schedule dialog box in which you can specify when you want the alert enabled.
6. Click **OK** to save your settings.

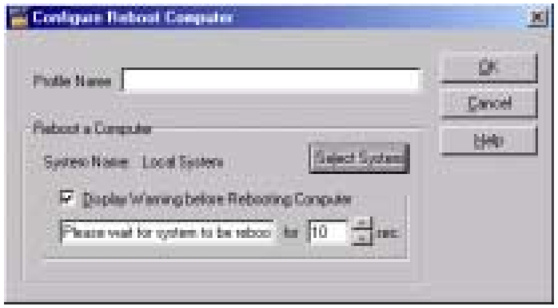
Creating a Reboot Response Action

A reboot response action reboots the system when the Alerting and Monitoring module detects a change in state of the monitored object or device.

See “Adding and Configuring Response Actions” on page 123 for the steps to access the Select Response Action(s) dialog box.

To create a reboot response action:

1. Click **New** to open the Select Response Action (type) dialog box.
2. Select **Reboot** from the Select Response Action dialog box. The Configure Reboot Computer dialog box opens.



Profile Name

Reboot a Computer

System Name Local System

☑ Display Warning before Rebooting Computer

Please wait for system to be reboo for 10 sec

3. Type a name in the **Profile Name** text box.
4. Choose **Select System** to open the Select System dialog box.
5. Navigate to and select the system to reboot. This selection populates the **System Name** text box.
6. If required, type the **User Name** and **Password** for the system.
7. Click **OK** to return to the Configure Reboot Computer dialog box.
8. Select the **Display Warning before Rebooting Computer** check box to set the response.
9. Type the message to display into the text box, and select the number of minutes to display the message.
10. Click **OK**.

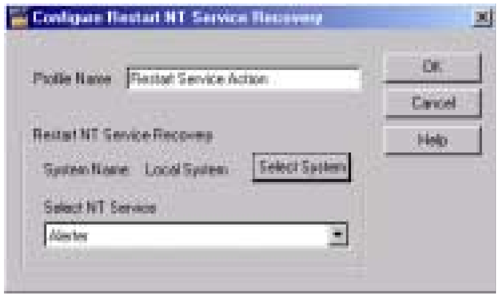
Creating a Restart Service Response Action

A restart service response action restarts a Microsoft Windows service when the Alerting and Monitoring module detects a change in state of the monitored object or device.

See “Adding and Configuring Response Actions” on page 123 for the steps to access the Select Response Action(s) dialog box.

To create a restart service response action:

1. Click **New** to open the Select Response Action (type) dialog box.
2. Select **Restart Service** from the Select Response Action dialog box. The Configure Restart NT Service Recovery dialog box opens.



Configure Restart NT Service Recovery

Profile Name: Restart Service Action

Restart NT Service Recovery

System Name: Local System

Select NT Service: Alerter

3. Type a name in the **Profile Name** text box.
4. Choose **Select System** to open the Select System dialog box.
5. Navigate to and select the system to reboot. This selection populates the **System Name** text box.
6. If required, type the **User Name** and **Password** for the system.
7. Click **OK** to return to the Configure Restart NT Service Recovery dialog box.
8. Select a service from the **Select NT Service** dropdown list.
9. Click **OK**.

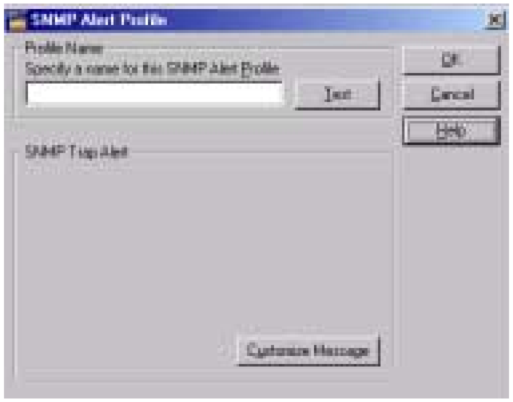
Creating an SNMP Trap Alert

If you have an SNMP Management console and the WebTrends SNMP Agent is activated, you can have an SNMP trap sent if the device you are monitoring fails.

See “Adding and Configuring Response Actions” on page 123 for the steps to access the Select Response Action(s) dialog box.

To create an alert:

1. Click **New** to open the Select Response Action (type) dialog box.
2. Select **SNMP Trap Alert** from the Select Response Action dialog box. The SNMP Alert Profile dialog box opens.



3. Type a name for the SNMP Alert profile in the **Specify a name for this SNMP Alert Profile** text box.
4. Click **Test** to make sure your alert works. See “Configuring Options” on page 291 for details on enabling the WebTrends SNMP Agent.

5. To create a custom alert message, click **Customize Message**. See "Customizing Text Messages" on page 142 for more information about this feature.

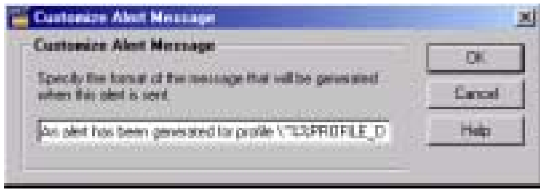
6. Click **OK**.

Customizing Text Messages

Many of the alerting dialog boxes have a Customize Alert Message feature which enables you to change the message used for the alert.

To change the message:

1. Click **Customize Message** in the dialog box you're working in (such as the E-mail Alert Profile dialog box). A Customize Alert Message dialog box appears.



Customize Alert Message

Customize Alert Message

Specify the format of the message that will be generated when this alert is sent.

An alert has been generated for profile \"%PROFILE_D

2. Type the new message. You can include any of the variables described in the table below in your message.

3. Click **OK**..

The following table shows the variables you can use to customize your messages.

Variable	Result
%%PROFILE_DESC%%	Includes the text from the profile's **Description** field.
%%HOST_NAME%%	If a host name or IP address has been defined, it is included.
%%PORT%%	If a port number for the device has been defined, as it is for the HTTP monitor, the port is included.
%%MONITOR_DEVICE%%	Includes the device specified in the profile.
%%MONITOR_TYPE%%	Includes the monitor type specified in the Device to Monitor list.
%%MONITOR_STATE%%	Includes the state of the device, such as down.
%%MONITOR_STATE_TIME%%	Includes the length of time that the monitor has been in the current state.
%%MONITOR_EVENT%%	Includes the last event that was logged for the profile.
%%MONITOR_EVENT_TIME%%	Includes the time that the last event occurred.
%%MONITOR_EVENT_MESSAGE%%	Includes additional information about the event.
%%RECOVERY_STAGE%%	Includes the number of the most recent recovery attempt (first, second, or third).
%%RECOVERY_ATTEMPT%%	Includes the number of the most recent retry for the current recovery attempt.

Formatting the Message

Use `\"` to put quotation marks around a word or phrase. This example:

```
\"%%MONITOR_EVENT_MESSAGE%%\"
```

puts quotation marks around the results of the event message variable in the message sent.

Use `\r\n` to insert a paragraph return.

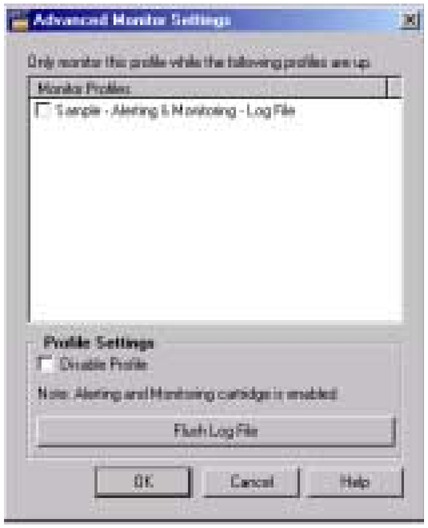
Defining Advanced Monitor Options

Define the dependencies of the current profile on others, disable the current profile, and flush the logs for the current profile.

To define advanced options:

1. On the Main Console, select a profile and click **Edit**.
2. Select the **General** tab.

3. Click **Advanced**. The Advanced Monitor Settings dialog box opens, with a list of all available Monitoring profiles.



Advanced Monitor Settings

Only monitor this profile while the following profiles are up

Monitor Profiles

□ Sample - Alerting & Monitoring - Log File

Profile Settings

□ Disable Profile

Note: Alerting and Monitoring cartridge is enabled

4. Select the check boxes of any profiles on which the current profile depends. The current profile is enabled only when the devices for the profiles you select here are active. If one of these profiles goes down, the current profile is disabled.

5. If desired, select the **Disable Profile** check box to disable the current profile.

6. If you no longer need existing log data for reports, click **Flush Log File** to delete the for the current profile. Use this option only after you have created the reports that you need.

7. Click **OK**.

Configuring Alerting and Monitoring as a Windows Service

If you are running Firewall Suite on a Windows NT, Windows 2000, or Windows XP system, Alerting and Monitoring installs as a service. You must configure your Windows NT, Windows 2000, or Windows XP system to give Firewall Suite the rights it needs.

Monitoring systems over multiple domains is possible as long as the proper trust relationships exist.

Setting up the Required Rights

To run Alerting and Monitoring as a service, the account you use must have the following privileges:

- Act as part of the operating system
- Log on as a service
- Log on locally

To monitor systems remotely, the account you use must also have:

- Administrative rights on the system doing the monitoring
- Administrative rights on each of the systems that are being monitored

To set up administrative rights:

1. Select **Start > Programs > Administrative Tools > User Manager**.
2. Select the **Policies, User Rights** command.
3. In the User Rights Policy dialog box, select the **Show Advanced User Rights** check box.
4. Select **Act as Part of the Operating System** from the Right list.

5. Click **Add** and select the account that Firewall Suite uses to run as a service.
6. Click **OK**.
7. Select **Log on Locally** from the Right list.
8. Click **Add** and select the account that Firewall Suite uses to run as a service.
9. Click **OK**.
10. Select **Log on as a Service** from the Right list.
11. Click **Add** and select the account that Firewall Suite uses to run as a service.
12. Click **OK**.
13. Click **OK** to close the User Rights dialog box.

Running the Service

To run Alerting and Monitoring as a service:

1. Close Firewall Suite.
2. Select **Start > Settings > Control Panel**.
3. Select **WebTrends Alerting and Monitoring for Firewall Suite**.
4. Click **Start Up**.
5. Select **This Account**.
6. Type a user name and password that meets the above criteria.
7. Stop and restart the service. Firewall Suite can be restarted.

Monitor Types

The following table lists the monitor types used by Firewall Suite, along with each monitor's default port and the monitoring method used.

Type	Purpose	Default port	Method
All device monitors, excluding DNS	Test connection	Various	All device monitors, excluding DNS, do a simple port connect test unless Advanced Protocol Monitoring is available and enabled.
IP device monitors			
BOOTP	Monitors a BOOTP server. BOOTP gives diskless client computers the information they need to start-up (or boot).	TCP 67	
DNS	Monitors a Domain Name System (DNS). DNS translates numeric IP addresses into domain names.	UDP 53	Alerting and Monitoring sends a DNS request to the DNS server at the specified address.
Echo	Monitors an Echo server. Echo is a basic server that sends the client the same message it received. This is useful for troubleshooting network communication problems where data is being corrupted.	7	If you use the Advanced Protocol Validation, Alerting and Monitoring will send a specific string to the port ("WebTrends Echo Test") and ensure that it receives the proper response.

Type	Purpose	Default port	Method
Finger	Monitors a finger daemon. A finger daemon provides information about users such as the last login time, terminal location and other information.	79	If you use the Advanced Protocol Validation, Alerting and Monitoring ensures that it receives a properly formatted finger response.
FTP	Monitors an FTP server, which provides users/visitors remote access to files.	21	If you use the Advanced Protocol Validation, Alerting and Monitoring ensures that it receives a successful banner.
Gopher	Monitors a Gopher server, which provides access to WAIS services similar to HTTP.	70	
HTTP	Monitors a Web server, which handles HTTP requests from browsers.	80	If you use the Advanced Protocol Validation, Alerting and Monitoring ensures that it receives a properly formatted HTTP response.
HTTPS	Monitors a secure Web server, which handles HTTP requests from browsers.	443	
IMAP3	Monitors an IMAP3 mail server, which enables user to manage remote mailboxes. This is a simple port connect test.	220	
IMAP4	Monitors an IMAP4 server, which uses SMTP to provide remote mailbox management.	143	If you use the Advanced Protocol Validation, Alerting and Monitoring ensures that it receives a successful banner.

Type	Purpose	Default port	Method
IRC	Monitors an Internet Relay Chat (IRC) server, which provides a system for “chatting” on the Internet.	6667	
Kerberos	Monitors a Kerberos server. Kerberos handles requests for those using the Kerberos data authentication system. Typically, it is used to verify the identity of a user to a host when using Telnet or FTP.	88	
NFS	Monitors an NFS server. NFS allows users to access shared files on remote computers as if they were stored locally.	2049	
NNTP	Monitors a Network News Transfer Protocol (NNTP) server that enables users to post or read messages on a newsgroup.	119	If you use the Advanced Protocol Validation, Alerting and Monitoring ensures that it receives a successful banner.
PING	Sends an ICMP PING request to the specified device and waits for a response.	ICMP	
POP2	POP2 is a client-side email protocol. A POP2 server stores incoming email for client retrieval.	109	If you use the Advanced Protocol Validation, Alerting and Monitoring ensures that it receives a successful banner.

Type	Purpose	Default port	Method
POP3	POP3 is a client-side email protocol. A POP3 server stores incoming email for client retrieval.	110	If you use the Advanced Protocol Validation, Alerting and Monitoring ensures that it receives a successful banner.
RLOGIN	Monitors an RLOGIN server, which handles requests for users accessing a remote computer. RLOGIN enables users to access local services.	221	If you use the Advanced Protocol Validation, Alerting and Monitoring ensures that it receives a properly formatted Rlogin response.
RPC	Monitors an (RPC) Remote Procedure Call used by programs and hidden to users.	530	
RSH	Monitors an Rshell server, which allows users to access to a Unix computer remotely.	222	
RWHOIS	Monitors a RWHOIS server, which can tell users about a second-level domain name and allows for recursive queries. An experimental form of WHOIS.	4321	
SMTP	Monitors an SMTP server. SMTP servers are used to transfer Internet email.	25	If you use the Advanced Protocol Validation, Alerting and Monitoring ensures that it receives a successful banner.
SPOP3	A secure version of the POP3 mail protocol.	995	

Type	Purpose	Default port	Method
Telnet	Monitors a TELNET host, which allows users to log on and use the host services.	23	If you use the Advanced Protocol Validation, Alerting and Monitoring ensures that it receives a login prompt and responds to telnet escape codes.
Time	Monitors a Time server, which is used to return the current date and time.	13	
UUCP	Monitors a server used to automatically copy files from one Unix computer to another.	540	
WHO	Monitors a WHO server which provides information about a domain.	513	
WHOIS	Monitors a WHOIS server, which can tell users about a second-level domain name, such as the owner of the domain.	43	
Windows NT system monitors			
NT Service	Monitors a Windows NT service. If you are monitoring remote computers, the Windows API uses the SMB and/or RPC requests to operate.	None/SMB	If the service has the status RUNNING, its Alerting and Monitoring status is UP. Otherwise, the Alerting and Monitoring status is DOWN.

Type	Purpose	Default port	Method
NT EventLog	Watches for new entries matching user specified criteria in the NT Event log. You select the system, event source, and type. If you are monitoring remote computers, the Windows API uses the SMB and/or RPC requests to operate.	None/SMB	
NT Performance Data	Monitors the Windows NT performance data. If you are monitoring remote computers, the Windows API uses the SMB and/or RPC requests to operate.	None/SMB	
SNMP monitors			
SNMP Get	Monitors the value of a SNMP get request variable.	161	The get request is sent in by the SNMP manager to the SNMP agent.
SNMP Trap	Monitors an SNMP trap, which is sent from the SNMP agent to the SNMP manager.	162	The trap is used to monitor the agent and when the predefined value is reached, the trap is sent.
LAN computer monitors			
Windows System	Monitors presence and/or accessibility of a Windows Networking computer on your local network.	SMB	Uses windows networking to determine whether a computer is present / accessible.

Type	Purpose	Default port	Method
Netware Server	Monitors presence and/or accessibility of a Netware server on your local network.	SMB	Uses windows networking to determine whether a computer is present / accessible. A valid Netware driver must be installed.
Disk and file monitors			
File	Monitors a file to which you have access. When the file size or date stamp changes (or does not change), a response is sent. If you are monitoring remote computers, the Windows API uses the SMB and/or RPC requests to operate.	None/SMB	

Type	Purpose	Default port	Method
Log File	Monitors a user specified log file for new entries matching user specified criteria. Generates an event when a new matching entry is found. This profile type can optionally register a down state when the specified log file is inaccessible. Many programs record relevant activity in a file called a log file. The application must allow other programs access to its log file between writes. Monitoring will not be possible if an application keep its log file(s) locked between writes.	None/SMB	

Type	Purpose	Default port	Method
ODBC	Monitors a remote ODBC database sources. SQL Server and other ODBC data sources can be configured for a wide variety of protocol options. Port activity depends on the local configuration.	Depends on ODBC data source	
Disk Space	Monitors a drive on a computer. A response is sent if the minimum disk space specified can not be verified on the specified drive. If you are monitoring remote computers, the Windows API uses the SMB and/or RPC requests to operate.	None/SMB	
URL	Monitors a specified Web page or ftp file for availability/content.	TCP 80/ TCP 21	

Chapter 5

Filtering for Focused Reports

This chapter explains how to use filters to make your reports include only the data you need, while excluding the data you don’t need. Filters are only available for General Firewall Activity, Incoming Firewall Activity, and Outgoing Firewall Activity profiles.

Filter Basics

When you configure a filter, you can specify one of two *filter types* and one or more *filter elements*.

Filter Types

There are two possible filter types: *Include* and *Exclude*. Include filters ensure that only activity in the log file that matches the criteria you have defined will be processed. Exclude filters ensure that all log file activity *except* the activity matching the criteria you specify will be processed.

For example, if you have a multi-home log file (one that crosses multiple domains) and you want to store activity for only one of its domains, you might create an include filter to include data for only one domain. If your multi-home log contains activity for three of your domains, and you want to store activity for two of them only, you might create an Exclude filter to exclude the domain you want to leave out.

Filter Elements

A filter element defines one of the criteria used for filtering.

For example, suppose the firewall log includes events for more than one firewall. If you wanted to filter the log file data to view only events related to one firewall, you could create an Include filter specifying that firewall. To do so, you would create an **Include** filter and select the **Firewall Name** filter element, specifying the name of the firewall you want to include.

You can find a complete list of available filter elements in “Filter Elements” on page 164. For a full description of each filter element, see “Filter Element Descriptions” on page 166.

Formatting Filter Element Criteria

Use a space to separate several entries.

Use quotation marks to enclose filter element criteria entries that contain spaces or commas. For example, the URL:

```
welcome to oregon.htm
```

looks like this as a filter element:

```
“welcome to oregon.htm”
```

Use wildcards to filter groups of items. For example, `*.gif` filters all files with a `.gif` extension, while `image*.gif` filters `image1.gif`, `image2.gif`, and so on.

Multi-Element Filters

You can also combine several filter elements in one filter. If Firewall Suite finds a match that meets all criteria, it returns the result to you and writes the result to the report.

For example, you can filter the data in the log files defined in the current profile for all activity related to the internal IP addresses you have defined, and at the same time, filter for the occurrence of a particular firewall rule.

In this case you would first select the Include filter type and the **Internal Address** filter element. You would then place an asterisk (*) in **the Internal Address** text box to indicate *all* internal addresses. See "Formatting Filter Element Criteria" on page 158. Next, you would select the **Rule** filter element. If Firewall Suite finds a match that meets both criteria, it returns the result to you and writes the result to the report.

When you select more than one filter element, Firewall Suite reads the elements as Boolean AND statements. For example, if Log File Activity matches Filter Element1 AND matches Filter Element2 AND... then include or exclude the result in the report.

Combining Multiple Filters

Firewall Suite lets you combine multiple filters in a profile. Multiple filters of the same type are processed with Boolean OR logic. This means that if the criteria of any one of the filters is met, the record is included in the report.

You can also combine include and exclude filters within a profile. The result of this combination is dependent on the sequence in which the filters are processed. Include filters are always processed first.

For example, you might want to look at all outgoing activity from your organization, except for that of users in the Finance department.

In this case, you would create an include filter that specifies to include all outbound activity using the **Traffic Direction** tab. You would then create a separate exclude filter that specifies to exclude the Finance department using the **Departments** tab. This assumes that you earlier defined the IP addresses associated with the Finance department of your organization. If Firewall Suite finds a match that meets both criteria, it returns the result to you and writes the result to the report.

The include filter selects all outgoing activity, and then the exclude filter filters out the Finance department users.

Tip
To create reports on a single log file using different sets of filters, you must use a separate profile for each set of filters. Use the Copy option on the File menu to copy a selected profile and modify it to specify the desired filter(s).

Working with Filters

This section provides step-by-step instructions for adding filters to profiles, modifying the settings for filters, and deleting filters.

Note
When you create a profile, the Include All filter is used by default. This filter processes and stores all log file data. To use your own filters, you must delete the Include All filter because it overrides all other filters.

Adding a Filter to a Profile

To create a more focused report, you can add one or more filters to any profile.

To define a filter for a profile:

1. Select the profile that you want to filter in the Profile Description list of the Main Console.
2. Click **Edit**.
3. Select the **Filters** tab in the Edit Profile dialog box.
4. Select the Include Everything filter, and click **Delete**.
5. The Include All filter is selected by default. It overrides all other filters. For a new filter to take effect, you must delete the Include All filter.
6. Click **Yes** to confirm the deletion.

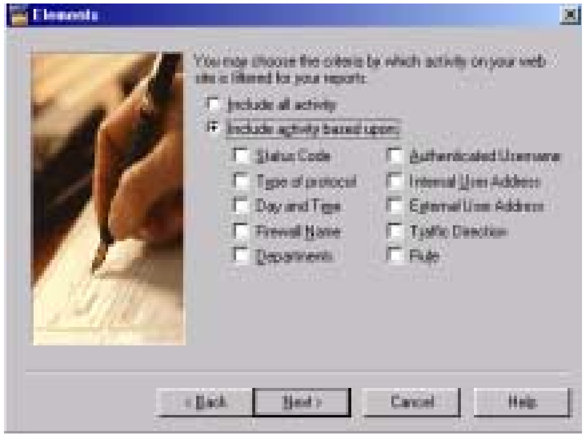
7. Click **New** to open the Type dialog box.

8. Choose whether to add an Include or Exclude filter.

9. Click **Next**. The Title dialog box opens.

10. In the **Name** text box, type a unique name to identify the filter in the **Filters** tab.

11. Click **Next**. The Elements dialog box opens.



You may choose the criteria by which activity on your web site is filtered for your reports.

○ Include all activity
● Include activity based upon:

□ Status Code
□ Type of protocol
□ Day and Time
□ Firewall Name
□ Departments
□ Authenticated Username
□ Internal User Address
□ External User Address
□ Traffic Direction
□ Rule

12. Select the **Include (Exclude) activity based upon** option.

13. Select the check box for each filter element you want to include in this filter. The specific filter elements available vary according to whether you are using a general, incoming, or outgoing profile.

14. Click **Next** to display the individual dialog boxes in which you may configure the filter elements you selected. Enter the criteria for the activity you want to filter in this profile. See “Filter Element Descriptions” on page 166 for details about each filter element.

15. After you have defined the filter criteria in the Filter Elements dialog boxes, the Summary dialog box opens. Click **Back** if you need to back up and make adjustments.

16. Click **Finish** to return to the Edit Profile window.

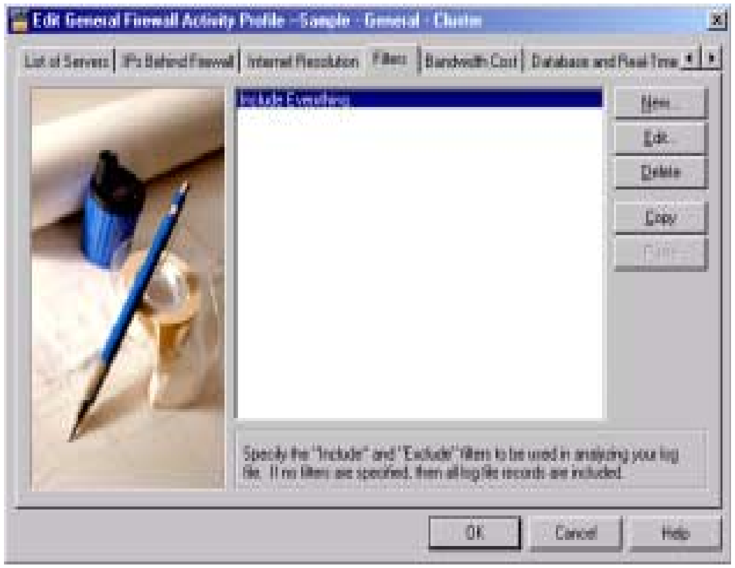
Modifying a Filter

You can change the filter criteria if you want to change the results.

To modify a filter:

1. In the Profile Description list of the Main Console, select the profile that has the filter that you want to modify.

2. Click **Edit**. The Edit Filter dialog box opens.



Edit General Firewall Activity Profile - Sample - General - Cluster

Include Everything

Specify the "Include" and "Exclude" filters to be used in analyzing your log file. If no filters are specified, then all log file records are included.

3. Select the **Filters** tab, then select the filter that you want to modify.

4. Click **Edit**. The Filter Properties dialog box opens with the **General** tab selected. Select and clear the check boxes to add or remove filter elements. A tab will appear for each filter element that you select.
5. Select the filter elements tabs to make changes to the criteria of specific elements.
6. When you have made your changes, click **OK**.

Note
If you are using FastTrends technology, clear the existing database and update it after editing a filter.

Deleting a Filter

Firewall Suite looks for data that matches all the criteria you have defined through your filters. You can remove a filter from a profile if you no longer want to use it.

To delete a filter:

1. In the Profile Description list of the Main Console, select the profile that has the filter that you want to delete.
2. Click **Edit**.
3. Select the **Filters** tab in the Edit Profile window.
4. Select the name of the filter that you want to delete in the list of existing filters.
5. Click **Delete**.
6. When you are prompted to confirm your action, click **Yes** to delete the selected filter or **No** to continue without deleting the selected filter.

Filter Elements

Overview

The table lists each filter element, along with a short description of the filter criteria and the profile types with which the filter can be used.

Filter element	**Specifies:**	**Profile types supported**
Actions	Firewall actions based on categorization. Only for firewalls using WELF format.	Actions
Authenticated Username	Authenticated users. This filter is useful if your Web site requires visitors to log on with a user names and password.	Authenticated Username
Browser	Spider or robot.	Browser
Category	Web site content.	Category
Day and Time	Hour of the day for each day of the week.	General Incoming Outgoing
Department	Departments in your organization, broken down by domain name.	General Outgoing
Directory	A particular directory on your Web site.	Incoming
External User Address	Specific domains or IP addresses coming from outside the firewall.	General
File	A particular file name or type on your Web site, for example `.gif`.	Incoming Outgoing
Firewall Actions	Check Point VPN-1/Firewall-1 actions. Actions can include responses to logon attempts or data transfers.	General (Check Point VPN-1/ Firewall-1 only)

Filter element	**Specifies:**	**Profile types supported**
Firewall Name	Activity for a specific firewall. This is useful if your firewall log file includes events for more than one firewall.	General
Internal User Address	Hits from specific domains or IP addresses behind the firewall.	General
Multi Homed Domain	Domains.	Incoming
Proxy Cache	Codes associated with the request.	Outgoing
Referrer	Entire user session coming from the specified referrers. Using this, you can establish the effectiveness of your Internet advertising.	Incoming
Return Code	Browser return codes. The log file records the results received from browsers, which are called return codes.	Incoming
Rule	Specific firewall rule. A rule identifies what activities and protocols are allowed through the firewall. They are usually identified by a number and vary from firewall to firewall.	General
Sites	A specific Web site or group of sites to include or exclude in your report (for example `*.edu`).	Outgoing
Status Codes	Status codes. These are numeric responses to attempts made to logon to the network to perform an activity or access a service.	General
Traffic Direction	Where the activity was initiated. This can be either *inbound* or *outbound*.	General

Filter element	Specifies:	Profile types supported
Type of Traffic	Protocols associated with traffic.	General
User Address or Country	Domains, IP addresses, or countries from the results of this profile.	Incoming
Users by IP	Activity of specific computers according to their IP address.	Outgoing

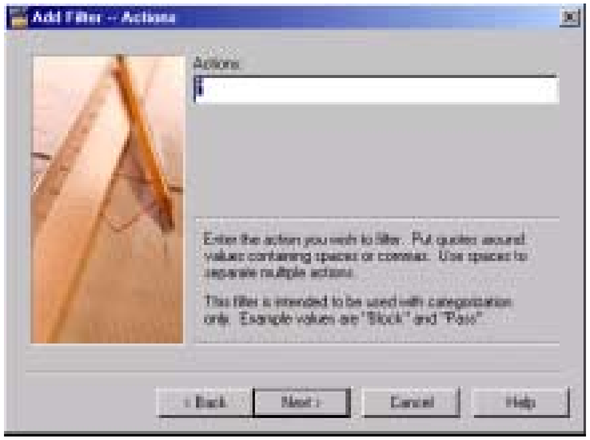
Filter Element Descriptions

Actions

The actions filter relates to URL categorization and is only available for firewalls using WELF format. Based on how a site is categorized, a firewall may block that site or allow access to it. The firewall logs the action of attempting to visit a blocked site as well as the action of visiting an approved (or passed) site.

The Actions filter element includes data on those firewall actions in the report, or excludes that data from the report.

Note
The Actions filter element is available only for firewalls using WELF format.



Enter the action you wish to filter. Put quotes around values containing spaces or commas. Use spaces to separate multiple actions.

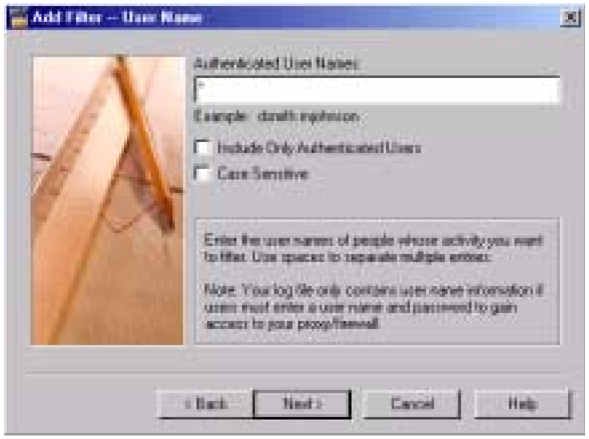
This filter is intended to be used with categorization only. Example values are "Block" and "Pass".

To add an Actions filter element:

1. The default includes both possible values (*) and reports all visits. If you do not want to accept the default, type one of the following:
   - – **Block** reports the attempts to visit blocked sites.
   - – **Pass** reports visits to all other sites, including non-categorized sites.
2. Click **Next**.

Authenticated Username

If you have a secure site that requires visitors to log on with a user name and password, you can use the Authenticated Username filter element to include or exclude authenticated users from the report. Use quotations mark around any authenticated user name that includes a space. For example, type `janesmith` to filter the authenticated user janesmith, but type “Jane Smith” to filter the authenticated user Jane Smith.



Enter the user names of people whose activity you want to filter. Use spaces to separate multiple entries.

Note: Your log file only contains user name information if users must enter a user name and password to gain access to your proxy/firewall.

To include or exclude all authenticated user names:

1. Select **Include** or **Exclude Only Authenticated Users**.
2. Click **Next**.

To include (exclude) specific authenticated user names:

1. In the **Authenticated Username** text box, type the names you want to filter. Put quotation marks around names that contain spaces. Separate individual entries with spaces. Select the **Case Sensitive** check box if you want to look for exact case matches. Most servers do not require case-sensitive matches.
2. Click **Next**.

Browser

Use the Browser filter element to either include or exclude a browser, spider or robot from the report. You can filter for any browser if you know how it appears in the `agent` field of the log file.

To define a Browser filter element:

1. In the **Browsers** text box, type the name of the browser you want to filter as it appears in the log file, or use the dropdown list to select common browsers, spiders, and robots. Use a space to separate multiple browsers. Use quotation marks to surround browser names that contain spaces. For example, type `"Microsoft Internet Explorer/4.`" to include or exclude any activity that matches Internet Explorer v4.*x*.

   Wildcards are not supported for Browser filters. Firewall Suite assumes that wildcards at either end of each browser entry when comparing it to the `agent` field in the log file.

   Note
   Filtering for Netscape Navigator may not return accurate results because many browsers identify themselves as Netscape Navigator.

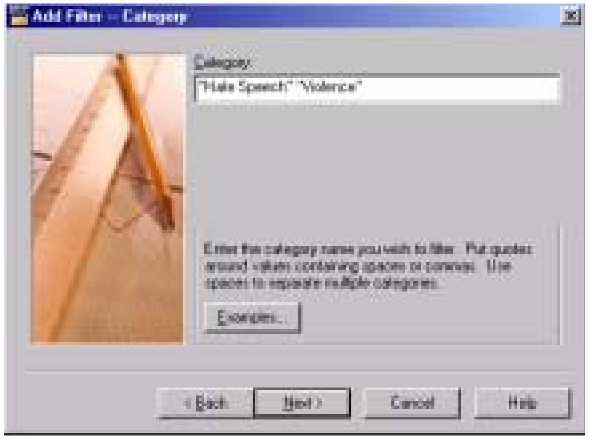
2. Click **Next**.

Category

Use the Category filter element to include or exclude information in your reports about sites visited by users from inside your organization. You can monitor Internet usage by category for bandwidth, productivity, and liability concerns.

The Category filter element lets you generate a report for all activity related to categorized sites, or limit the reports to specified categories.

Note
The categories available for filtering depend on the category databases that you download. Click **Examples** in the Add Filter—Category dialog box for a list.



Add Filter – Category

Category: "Hate Speech" "Violence"

Enter the category name you wish to filter. Put quotes around values containing spaces or commas. Use spaces to separate multiple categories.

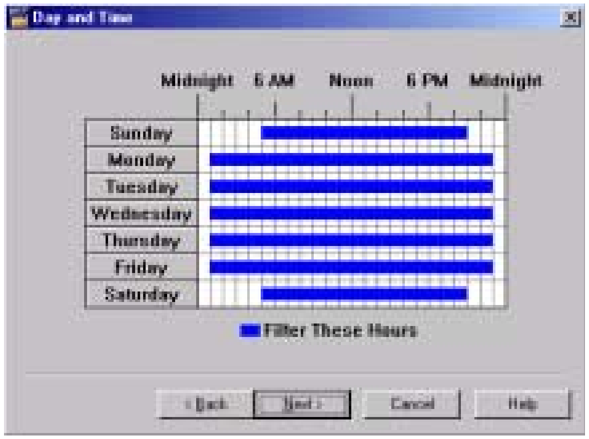
To define a Category filter element:

1. In the **Category** text box, type the names of the categories that you want to include or exclude in your reports. The default is to filter all categories
   - Separate categories with spaces.
   - Put quotation marks around categories that contain spaces or commas.
2. Click **Next**.

See “URL Categorization” on page 50 for more information about categories and category databases.

Day and Time

The Day and Time filter element includes or excludes activity according to the day of the week and the time of day.



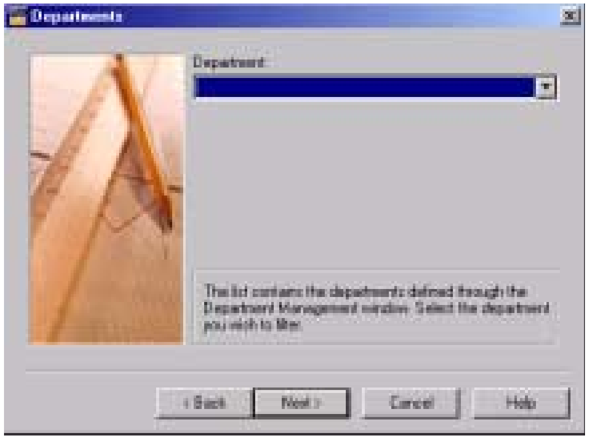
To define a Day and Time filter element:

1. Click on boxes, or drag rows or columns to select them. A blue box indicates an hour is selected. The figure shows Monday through Friday, 8:00 a.m. to 5:00 p.m. selected.

2. Click **Next**.

Departments

The Departments filter element includes or excludes departments from your analysis and reporting. For example, you can find out which department is using the Internet the most.



This list contains the departments defined through the Department Management window. Select the department you wish to filter.

To define a Departments filter element:

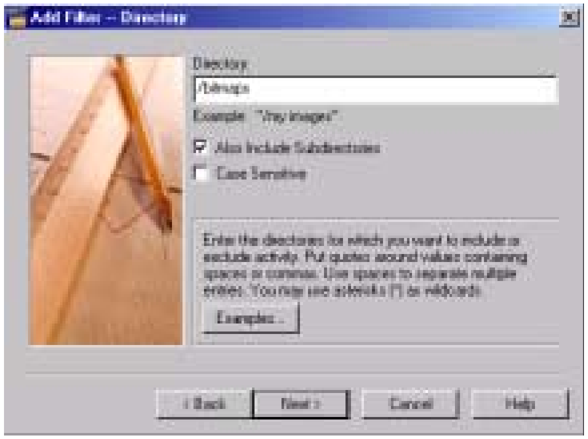
1. Use the **Department** dropdown list to select the department that you want to include or exclude.

   Any departments already defined using the Department Management dialog box appear in the dropdown list. See “Using Department Management” on page 90 for information about setting up departments.

2. Click **Next**.

Directory

Use the Directory dialog box to include or exclude the activity of a specific directory.



Directory
/bitmaps
Example: "/my images/"

☑ Also Include Subdirectories

□ Case Sensitive

Enter the directories for which you want to include or exclude activity. Put quotes around values containing spaces or commas. Use spaces to separate multiple entries. You may use asterisks (*) as wildcards.

To define a Directory filter element:

1. In the **Directory** text box, type the path for the directory to be filtered. Use wildcards to specify multiple directories. Separate directories with a space.Put quotation marks around directory names that contain spaces. For more information, see the table of Directory filter examples.

   By default, an include directory filter element includes all directories starting at the root directory, indicated by a slash (/) in the **Directory** text box. There is no default for an exclude directory filter.

2. If you do not want to include or exclude all subdirectories, clear the **Also Include/Exclude Subdirectories** check box. Otherwise, Firewall Suite will activates the subdirectories by default.

3. Select the **Case Sensitive** check box to look for exact case matches. Most servers do not require case-sensitive matches.

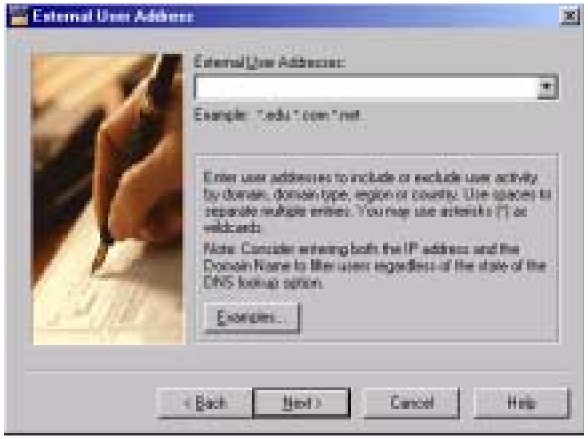
4. Click **Next**.

The following table shows examples of Directory filter definitions.

Example	**Result**
`/images`	Specifies the directory `/images` is to be included or excluded. If **Include Subdirectories** is selected, all subdirectories of /*images* will also be included or excluded.
`“/image files”`	Specifies the long directory `/image files`.
`“/image files” / intranet /graphics`	Specifies the directories `/image files`, `/intranet`, and `/graphics`.
`/*graphics`	Specifies any first-level directory whose name ends in `graphics`, such as `/bitmap graphics`, but not `/intranet/bitmap graphics`.
`/*/graphics`	Specifies all second-level directories named `/graphics`, such as `/home/graphics` and `/intranet/graphics`, but not `/home/sales/graphics`. Includes directories such as `/home/graphics/logos` only if **Include Subdirectories** is selected.
`/graphics /*/ graphics /*/*/ graphics`	Specifies all first-, second-, and third-level directories named graphics, such as `/graphics`, `/home/graphics`, and `/home/sales/graphics`. Includes subdirectories such as `/home/graphics/logos` and `/home/sales/graphics/logos/specials` only if **Include Subdirectories** is selected.
`/*graphics*/`	Specifies all first-level directories with names containing `graphics`, such as `/graphics`, `/graphics files`, and `/bitmap graphics`.

External User Address

Use the External User Address filter element to include or exclude activity from specific domains or IP addresses *outside* the firewall. For example, you can create a filter that includes activity from a questionable IP address if you think someone is trying to break into your firewall.



External User Address

External User Addresses:

Example: *.edu *.com *.net

Enter user addresses to include or exclude user activity by domain, domain type, region or country. Use spaces to separate multiple entries. You may use asterisks (*) as wildcards.

Note: Consider entering both the IP address and the Domain Name to filter users regardless of the state of the DNS lookup option.

To define an External User Address filter element:

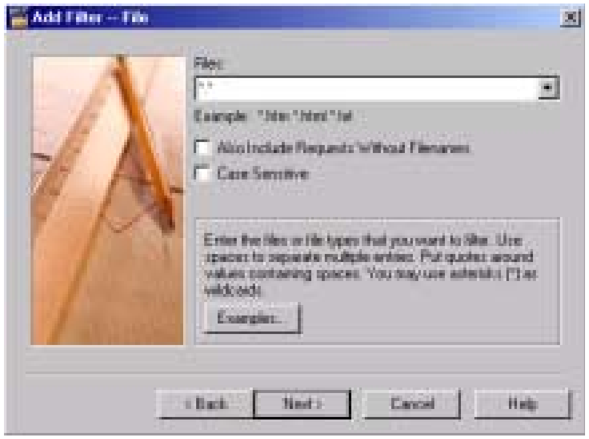
1. In the **External User Address** box, type the user addresses that you want to specify, or use the dropdown list to select a predefined user address. The default setting is All User Addresses (*).
2. Click **Next**.

The following table shows examples of how to specify user addresses.

Example	Result
`204.245.240.0-63`	Specifies all numeric IP addresses from 204.245.240.0 through 204.245.240.63
`204.245.240.0-204.245.240.64`	Specifies all numeric IP addresses from 204.245.240.0 through 204.245.240.64
`204.245.240.64/26`	CIDR notation. Specifies all addresses of the classless subnet: 204.245.240.64 - 204.245.240.127.
`111.92.76.0/26`	Specifies all subnet addresses from 111.92.76.0 through 111.92.76.63.
`*.WebTrends.com`	Only those addresses with a subdomain that appears to the left of this domain, for example www.WebTrends.com and ftp.WebTrends.com. Excludes addresses without a subdomain.
`*WebTrends.com`	Any address that includes the specified domain, with or without a subdomain, for example www.WebTrends.com, ftp. WebTrends.com, or WebTrends.com. **Tip:** You can specify IP addresses as well as domain names in filter text boxes if you are uncertain whether DNS lookups are being performed.
`*.edu *.com *.net`	All addresses that have the domain types `edu`, `com`, or `net`.
`*.de`	All addresses from Germany.
`www.*`	Only those addresses that have www as a subdomain.

File

Use the File filter element to include or exclude specific files.



Enter the files or file types that you want to filter. Use spaces to separate multiple entries. Put quotes around values containing spaces. You may use asterisks (*) as wildcards.

To define a File filter element:

1. In the **Files** text box, type the file name or extension, or select a file type from the dropdown list. Use wildcard characters to specify file names or extensions, such as all HTML files (`*.htm`) or all `GIF` files (`*.gif`). You can specify several file types at once by inserting a space between each file type.

   The default for an Include files filter element is to include all files, indicated by `*.*` in the **Files** text box. There is no default for an exclude filter.

2. Select the **Also Include Requests Without Filenames** check box to include activity in which no filenames are specified. For example, if a visitor to your site accesses `http://www.mydomain.com`, the Web server may log this hit without a file name, but return the file `http://www.mydomain.com.default.htm`.

   Note
   If you used the default setting for your filter, selecting the **Also Include Requests Without Filenames** check box has no effect.

3. Select the **Case Sensitive** check box to look for exact case matches. Most servers do not require case-sensitive matches.

4. Click **Next**.

The following table shows examples of how to specify files.

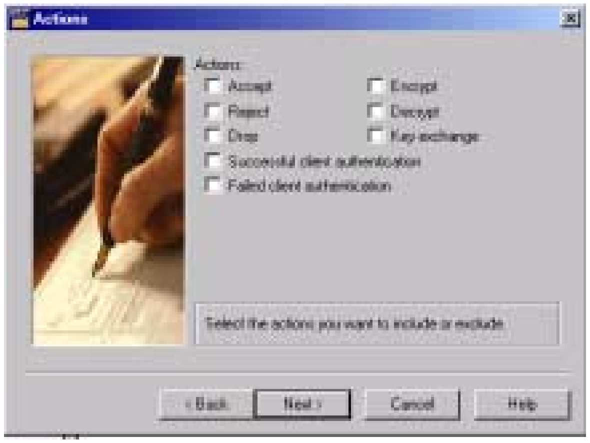
Example	Result
help.htm	Filters the file help.htm.
*.gif *.bmp	Filters bitmap (.bmp) and gif (.gif) files.
help*.html	Filters all html files whose name begin with help.
help*.*	Filters all files whose name begin with help, regardless of file type.
marketing.htm “marketing help.htm” “marketing leads.htm”	Filters the files marketing.htm, marketing help.htm, and marketing leads.htm.

Firewall Actions

Use the Firewall Actions filter element to include or exclude Check Point VPN-1/Firewall-1 actions such as responses to logon attempts or data transfers.

Note

Use the Firewall Actions filter element with Check Point VPN-1/Firewall-1 only. All other firewalls use the Status Codes filter.



Actions:

- □ Accept
- □ Reject
- □ Drop
- □ Encrypt
- □ Decrypt
- □ Key exchange
- □ Successful client authentication
- □ Failed client authentication

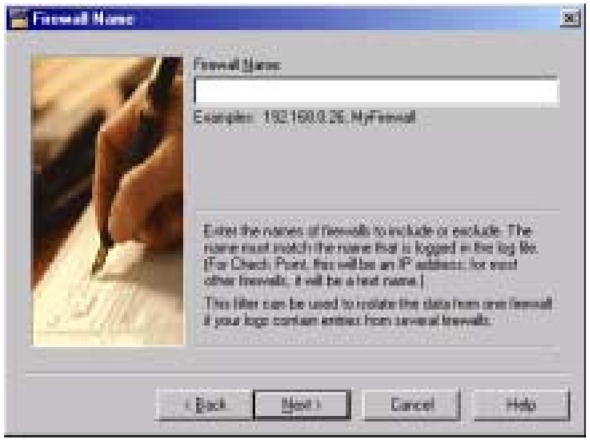
Select the actions you want to include or exclude

To define a Firewall Actions filter element:

1. Select the check box for each actions you want to include or exclude.
2. Click **Next**.

Firewall Name

The Firewall Name filter element includes or excludes activity for a specific firewall from analysis and reporting. If your firewall log file includes events for more than one firewall, you can use this element to look at the activity for a single firewall.



Examples: 192.168.0.26, MyFirewall

Enter the names of firewalls to include or exclude. The name must match the name that is logged in the log file. (For Check Point, this will be an IP address; for most other firewalls, it will be a text name.)

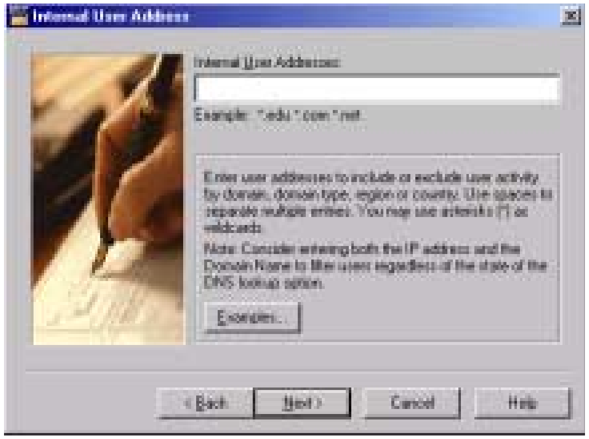
This filter can be used to isolate the data from one firewall if your logs contain entries from several firewalls.

To define a Firewall Name filter element:

1. In the **Firewall Name** text box, type the name of the firewall exactly as it is recorded in the log file. The name is either a text name or an IP address.
2. Click **Next**.

Internal User Address

The Internal User Address filter element includes or exclude hits from specific domains or IP addresses behind the firewall. You could use this filter element to focus your reports on the activity of one or more people. The default, All User Addresses, is indicated by an asterisk (*) in the text box.



Example: *.edu *.com *.net

Enter user addresses to include or exclude user activity by domain, domain type, region or country. Use spaces to separate multiple entries. You may use asterisks (*) as wildcards.

Note: Consider entering both the IP address and the Domain Name to filter users regardless of the state of the DNS lookup option.

To define an Internal User Address filter element:

1. In the **Internal User Address** text box, type the user addresses that you want to specify. Separate multiple addresses with spaces.Use a hyphen to indicate a range of addresses.Use an asterisk (*) as a wildcard.
2. Click **Next**.

The following table shows examples of internal user addresses.

Example	Result
`204.245.240.0-63`	Specifies all numeric IP addresses from 204.245.240.0 through 204.245.240.63.
`204.245.240.0-204.245.240.64`	Specifies all numeric IP addresses from 204.245.240.0 through 204.245.240.64.
`204.245.240.64/26`	CIDR notation. Specifies all addresses of this classless subnet: 204.245.240.64 - 204.245.240.127.
`111.92.76.0/26`	Specifies all subnet addresses from 111.92.76.0 through 111.92.76.63.
`*.WebTrends.com`	Only those addresses that have a subdomain that appears to the left of this domain, such as www. WebTrends.com, or ftp. WebTrends.com. Excludes addresses without a subdomain.
`*WebTrends.com`	Any address that includes the specified domain, with or without a subdomain, such as www. WebTrends.com, ftp. WebTrends.com, or WebTrends.com. **Tip:** You can specify IP addresses as well as domain names if you are uncertain whether DNS lookups are being performed.
`*.edu *.com *.net`	All addresses with the domain types `edu`, `com`, or `net`.
`*.de`	All addresses from Germany.
`www.*`	Only those addresses that have www as a subdomain.

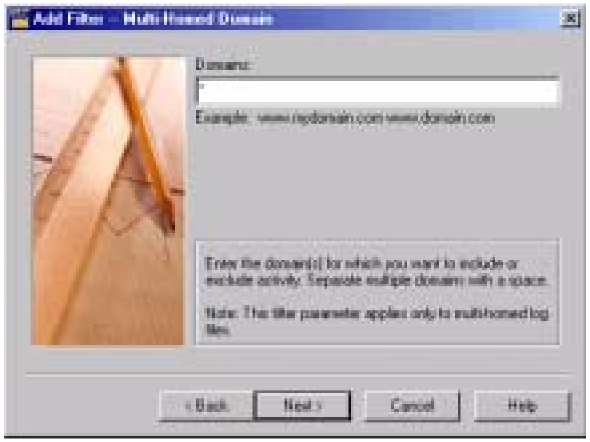
Multi-Homed Domain

Usually, there is only one Web site on a domain (they often have the same name). In some situations, however, a single IP address can host several Web sites and its log files contain entries related to all of them. An IP address owned by an Internet service provider is an example.

To create a report that analyzes data from only one or selected Web sites from a particular IP, use the Multi-Homed Domain filter. This filter element lets you specify the domains you want to include or exclude. For example, if your multi-homed log file contains activity from these domains:

```
www.abc.com
www.def.com
www.ghi.com
```

but you want to report only on `www.abc.com`, create an include filter and specify `www.abc.com`.



Add Filter – Multi-Homed Domain

Domains:

Example: www.mydomain.com www.domain.com

Enter the domain(s) for which you want to include or exclude activity. Separate multiple domains with a space.

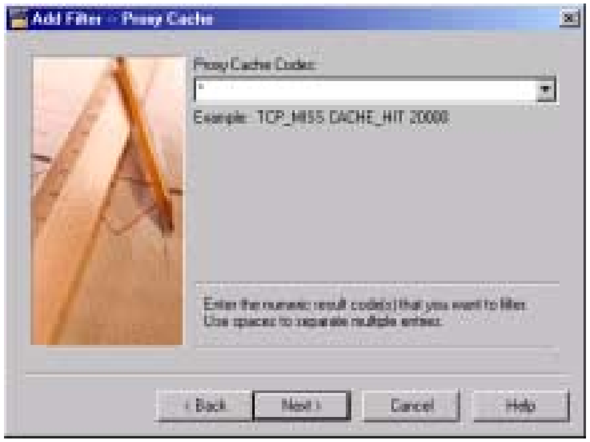
Note: This filter parameter applies only to multi-homed log files.

To define a Multi-Homed Domain filter element:

1. In the **Domains** text box, type the names of the domains you want to include or exclude. Put a space between domain names.
2. Click **Next**.

Proxy Cache

Use the Proxy Cache Codes filter element to include or exclude log records based on proxy cache codes. The default for an include filter element is All Proxy Status codes, indicated by an asterisk (*) in the Proxy Cache Codes box. There is no default for an exclude filter.



Add Filter - Proxy Cache

Proxy Cache Codes: *

Example: TCP_MISS CACHE_HIT 20000

Enter the numeric result code(s) that you want to filter.
Use spaces to separate multiple entries.

To define a Proxy Cache filter element:

1. In the **Proxy Cache Codes** text box, specify the codes you want to exclude or include, or select a set of codes from the dropdown list. Separate multiple entries with spaces.
2. Click **Next**.

The following table shows the definition of each proxy cache code.

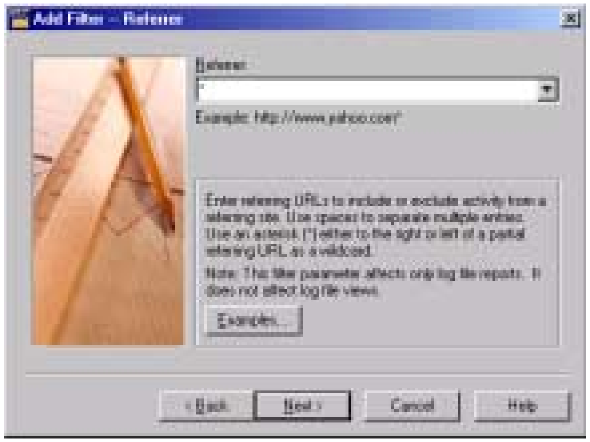
Option	Description
All Proxy Status Values	Includes or excludes records that have a proxy status value.
From the Internet (Summary)	Includes or excludes records that have a status value indicating that the file requested was downloaded from the Internet.
From the Cache (Summary)	Includes or excludes records that have a status value indicating that the file requested was downloaded from either the local proxy server's cache or from an upstream proxy server's cache.
Cache Unknown	Includes or excludes records that have a status value indicating that the cache is not known.
From the Internet, then cached (new)	Includes or excludes records that have a status value indicating that the file requested was downloaded from the Internet and then placed into the proxy server's cache for possible future use. It also indicates that the file was not present in the cache before downloading it.
From the Internet, then cached (updated file)	Includes or excludes records that have a status value indicating that the file requested was downloaded from the Internet and then placed into the proxy server's cache for possible future use. It also indicates that an older version of the file was in the cache before downloading it, and was updated by the newer version.
From the cache, verified by remote server	Includes or excludes records that have a status value indicating that the file requested was already present in the cache, and the proxy server contacted the remote server to verify that it was the newest version of the file.
From the cache, without verification	Includes or excludes records that have a status value indicating that the file requested was already present in the cache and the proxy server did not contact the remote server to verify that it was the newest version of the file.

Option	Description
Resource not cacheable	Includes or excludes records that have a status value indicating that the file requested was downloaded from the Internet and was not added to the proxy server’s cache.
Cache write aborted	Includes or excludes records that have a status value indicating that the file requested was downloaded from the Internet, and while the file was being added to the cache, something happened that caused the proxy server to cancel writing the file.
From the cache, no details	Includes or excludes records that have a status value indicating that the file requested was already in the cache. No other details were given.
Returned from array member cache	Includes or excludes records that have a status value indicating that the file requested was present in a proxy array member cache.
Returned from upstream cache	Includes or excludes records that have a status value indicating that the file requested was present in a proxy server’s cache upstream from the proxy server reported on.
From the Internet, no details	Includes or excludes records that have a status value indicating that the file requested was downloaded from the Internet. No other details were given.
Successful connection	Includes or excludes records that have a status value indicating that the client initiated a successful connection with the proxy server.
Connection rejected by proxy server	Includes or excludes records that have a status value indicating that the client attempted to initiate a connection and was rejected by the proxy server.
Normal connection termination	Includes or excludes records that have a status value indicating that the proxy server terminated a connection normally.
Abortive connection termination	Includes or excludes records that have a status value indicating that the proxy server terminated the connection abnormally.

Referrer

The Referrer filter helps you analyze the number and quality of users coming to your site from other sites or from a specific Internet advertisement link. With this filter you can establish the effectiveness of your Internet advertising.

Firewall Suite looks for exact case-insensitive matches.



Referrer: *

Example: http://www.yahoo.com*

Enter referring URLs to include or exclude activity from a referring site. Use spaces to separate multiple entries. Use an asterisk (*) either to the right or left of a partial referring URL as a wildcard.

Note: This filter parameter affects only log file reports. It does not affect log file views.

To define a Referrer filter element:

1. In the **Referrer** text box, type the referring URLs or select them from the dropdown list. Separate multiple referrers with a space.

   You can use an asterisk (*) as a wildcard at the beginning of the URL string to include all protocols. Append the asterisk wildcard if you want to specify all activity from a referrer. For example, type:

   `http://www.yahoo.com*.`

   By default, the include referrers filter element includes all hits with referring data regardless of site. The default for the exclude referrer filter element excludes only hits without any referring information.

2. Click **Next**.

The following table shows examples for filtering referrers

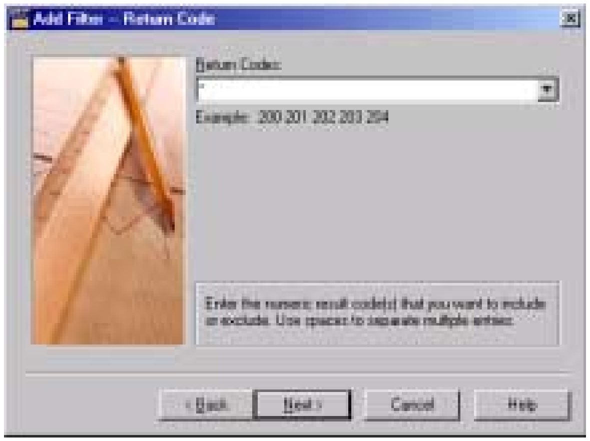
Examples	Result
`http://www.referrer.com*`	Filters any activity coming from http://www.referrer.com. Excludes hits from ftp://www.referrer.com.
`http://www.referrer.*`	Filters www.referrer.com, www.referrer.net, www.referrer.org, and other sites beginning with www.referrer.
`*.referrer.com*`	Filters ftp.referrer.com or www.referrer.com. Excludes sites such as www.referrer2.com and www.referrer.net.
`*referrer*`	Filters any site with referrer in the name, for example www.referrer.com, www.referrer.net, www.notreferrer.com, referrer.com, and referrer.
`http://www.referrer.com/page.htm`	Filters only references from page.htm at the www.referrer.com site.
`http://www.referrer.com/page.htm*`	Filters sites such as page.htm, page.html,or page.html2 from the root of the www.referrer.com domain.
`*.referrer.com/page.htm*`	Filters sites such as page.htm or page.html from referrer.com domains such as ftp.referrer.com and search.referrer.com.

The following table shows examples for filtering referrals from a single page.

Example	Result
`ad.html`	Filters only references from the page `ad.html`.
`*ad.*`	Filters hits referred from `ad.html`, `yippiedodad.htm`, `rad.gif`, and `mad.jpg`.
`*reports.html`	Specifies only the referring URLs originating from the `reports.html` pages.

Return Codes

The log file records browser activity in the form of return codes. You can include or exclude browser activity in reports by including or excluding the return codes.



Add Filter -- Return Code

Return Codes: *

Example: 200 201 202 203 204

Enter the numeric result code(s) that you want to include or exclude. Use spaces to separate multiple entries.

For example, if you want to report only on successful hits, select **Success Only** from the dropdown list. To find out about all hits that ended up with a 404 code, Failed Not Found, filter on the 404 return code. This would help you identify sites that have outdated references to material that you have removed from your site.

To define a Return Code filter element:

1. In the **Return Codes** text box, type one or more return codes, or use the dropdown list to select common return codes, or groups of return codes. Separate return codes by spaces. You cannot use wildcards. The default, indicated by an asterisk (*), is All Return Codes.

   See the table for a list of return codes and their descriptions.

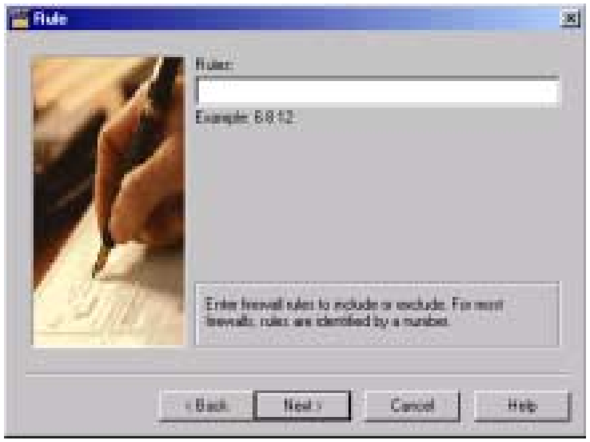
2. Click **Next**.

The following tables shows return codes that can be filtered.

Code	Description
*	All Return Values
200	Success, OK
201	Success, Created
202	Success, Accepted
203	Success, Partial Information
204	Success, No Response
300	Success, Redirected
301	Success, Moved
302	Success, Found
303	Success, New Method
304	Success, Not Modified
400	Failed, Bad Request
401	Failed, Unauthorized
402	Failed, Payment Required
403	Failed, Forbidden
404	Failed, Not Found
500	Failed, Internal Error
501	Failed, Not Implemented
502	Failed, Overloaded Temporarily
503	Failed, Gateway Timeout

Rule

The Rule filter element includes or excludes the analysis and reporting on a specific firewall rule. A rule identifies what activities and protocols are allowed through the firewall. They are usually identified by a number.



Example: 6 8 12

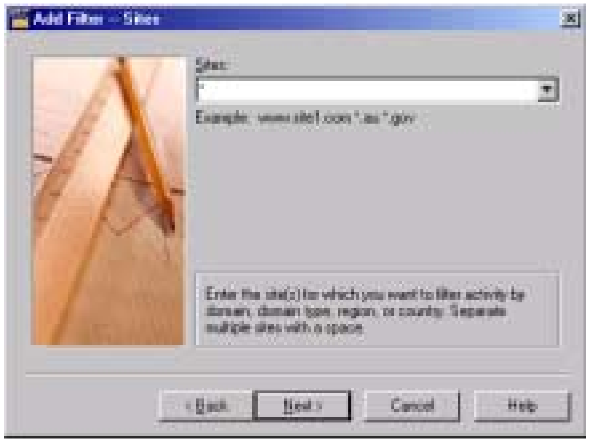
Enter firewall rules to include or exclude. For most firewalls, rules are identified by a number.

To define a Rule filter element:

1. In the **Rules** text box, type the firewall rules that you want to filter for. Separate multiple rules with spaces.
2. Click **Next**.

Sites

Use the Sites filter element to include or exclude a specific Web site or domain type for this analysis. For example, you might use the Sites filter element to report on the activity for your own intranet. Create an Include filter and specify the URL for your intranet, for example `www.intranet.company.com`. The resulting report shows only hits to your site.



Sites: *

Example: www.site1.com *.au *.gov

Enter the site(s) for which you want to filter activity by domain, domain type, region, or country. Separate multiple sites with a space.

To define a Sites filter element:

1. In the **Sites** text box, type the sites that you want to include or exclude, or use the dropdown list to select common domain and country extensions. Separate multiple entries with spaces. Specify multiple URLS by putting an asterisk (*) wildcard ahead of or trailing an entry. For example, to specify all sites with `.edu` in the domain name, type:

   ```
   *.edu
   ```

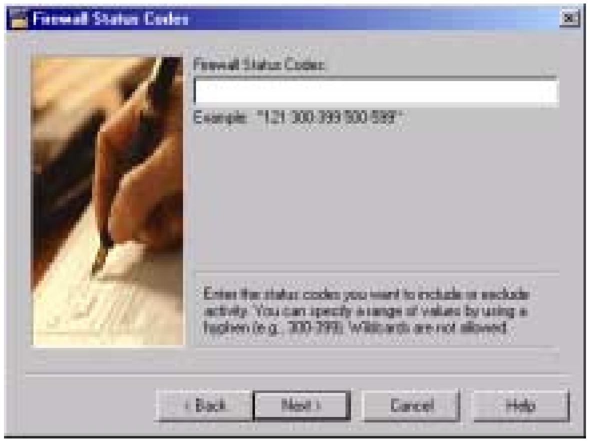
   Separate individual URLs with a vertical bar (|). For example, type:

   ```
   www.first.com|www.second.com
   ```

2. Click **Next**.

Firewall Status Code

Use the Firewall Status Codes filter element to include or exclude status codes from the analysis and reporting for this profile. Firewall status codes are numeric responses to attempts made to logon to the network. For example, status codes could indicate a problem on the network or someone abusing public space.



Example: "121 300-399 500-599"

Enter the status codes you want to include or exclude activity. You can specify a range of values by using a hyphen (e.g., 300-399). Wildcards are not allowed.

To define a Firewall Status Codes filter element:

1. In the **Firewall Status Codes** text box, type the status codes that you want to filter. Use spaces to separate the entries. Specify a code range by using a hyphen between the first and last codes in the range.Wildcards are not supported.

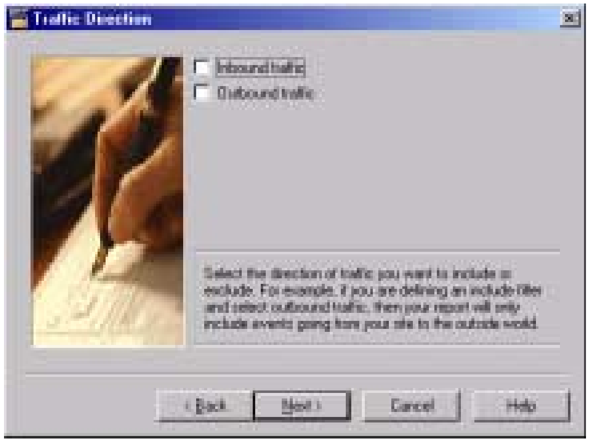
   Note
   Files listing status codes can be found in the root of your installation directory. These files are identified by firewall name, for example: `CiscoMessages.txt` and `Lucent Messages.txt`.

   ---

2. Click **Next**.

Traffic Direction

Use the Traffic Direction filter element to include or exclude activity according to where the activity was initiated.



Select the direction of traffic you want to include or exclude. For example, if you are defining an include filter and select outbound traffic, then your report will only include events going from your site to the outside world.

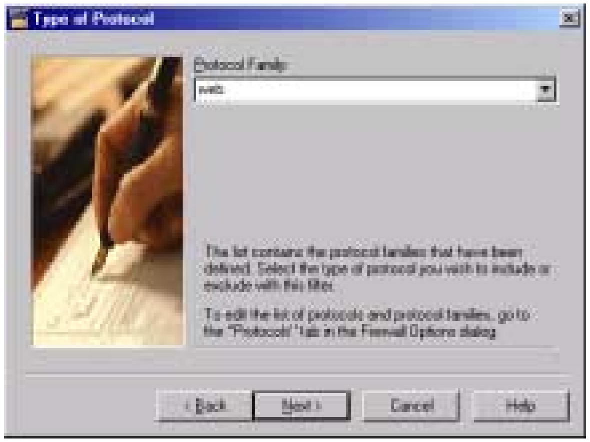
To define a Traffic Direction filter element:

1. Select a check box for each traffic direction you want to include or exclude.
   - **Inbound Traffic** filters traffic that is initiated by someone on the outside of the firewall.
   - **Outbound Traffic** filters traffic that is initiated by someone on the inside of the firewall (within your organization).
2. Click **Next**.

Protocol Family

Use the Protocol Family filter element to include or exclude a particular type of traffic from the analysis and reporting for this profile. Use the Protocols dialog box in the General Firewall Activity options to create and manage the Protocol Families you select for this filter element.

Note
Only one Protocol Family filter can be used in a profile. Create separate profiles to filter different protocol types.



Type of Protocol

Protocol Family: web

This list contains the protocol families that have been defined. Select the type of protocol you wish to include or exclude with this filter.

To edit the list of protocols and protocol families, go to the "Protocols" tab in the Firewall Options dialog.

To define a Protocol Family filter element:

1. Select the protocol that you want to filter from the **Protocol Family** dropdown list.
   - **web** filters the log file for Internet/Intranet activity.
   - **e-mail** filters the log file for email activity.
   - **ftp** filters the log file for FTP (File Transfer Protocol) activity.

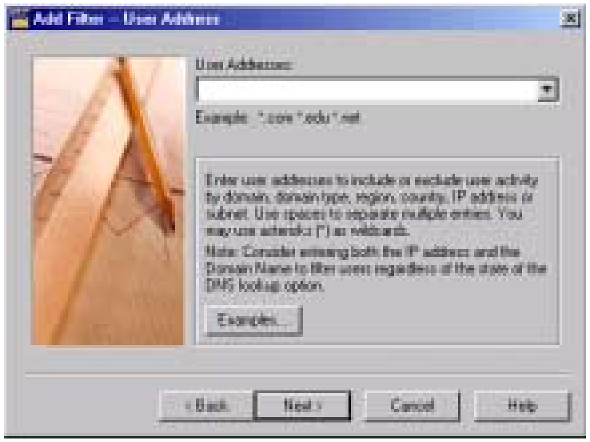
- **telnet** filters the log file for Telnet activity.
- **realaudio** filters the log file for RealAudio activity.

Any additional protocol families that you set up in the Protocols dialog box appear in the list as well.

2. Click **Next**.

User Address

Use the User Address filter element to include or exclude domains, IP addresses, or countries from the results of this profile. For example, if you create an exclude filter and you specify your own domain, the report would not include any activity from your domain.



Example: *.com *.edu *.net

Enter user addresses to include or exclude user activity by domain, domain type, region, country, IP address or subnet. Use spaces to separate multiple entries. You may use asterisks (*) as wildcards.

Note: Consider entering both the IP address and the Domain Name to filter users regardless of the state of the DNS lookup option.

To define a User Address filter element:

1. In the **User Addresses** text box, type the user addresses that you want to specify, or use the dropdown list to select predefined user addresses. Separate multiple entries with spaces. You can use asterisks (*) as wildcards. The default, All User Addresses, is indicated by an asterisk (*) in the text box. See the table for examples of User Address filters.

   Note
   Country information is not always accurately reported by Web sites.

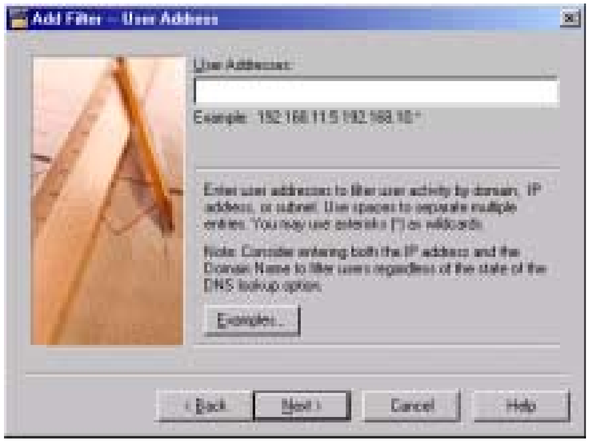
2. Click **Next**.

The following table shows examples of how to specify user addresses.

Example	Result
`* *.WebTrends.com`	Only those addresses with a subdomain to the left of this domain, such as www.WebTrends.com, or ftp.WebTrends.com. Excludes addresses without a subdomain.
`* *WebTrends.com`	Any address that includes the specified domain, with or without a subdomain, such as www.WebTrends.com, ftp. WebTrends.com, or WebTrends.com.
`* *.edu *.com *.net`	All addresses with the domain type `edu`, `com`, or `net`.
`* *.de`	All addresses from Germany.
`* www.*`	Only those addresses with www as a subdomain.

User (IP)

Use the User IP Address filter element to include or exclude activity from specific domains, subnets, or IP addresses. For example, you might use the user address filter element to focus on the activity of a specific user.



Example: 192.168.11.5 192.168.10.*

Enter user addresses to filter user activity by domain, IP address, or subnet. Use spaces to separate multiple entries. You may use asterisks (*) as wildcards.

Note: Consider entering both the IP address and the Domain Name to filter users regardless of the state of the DNS lookup option.

To define a User (IP) filter element:

1. In the **User Addresses** text box, type the IP addresses, subnets, or domains that you want to include or exclude. Separate multiple addresses with spaces. You can use asterisks (*) as wildcards to specify a set of IP addresses. The default for an include filter element is All User Addresses (*). The table shows User IP address examples.
2. Click **Next**.

The following table shows examples of how to specify IP address ranges.

Example	Result
`204.245.240.0-63`	Specifies all numeric IP addresses from 204.245.240.0 through 204.245.240.63.
`204.245.240.0 – 204.245.240.64`	Specifies all numeric IP addresses from 204.245.240.0 through 204.245.240.64.
`204.245.240.64/26`	CIDR notation. Specifies all addresses of the classless subnet: 204.245.240.64 – 204.245.240.127.
`111.92.76.0/26`	Specifies all subnet addresses from 111.92.76.0 through 111.92.76.63.

Chapter 6

Working with Reports

Once you have configured your firewall and created a profile, you can start working with reports. With Firewall Suite, you can create a variety of reports, modify report settings, memorize report settings for future use, add new report styles, and automate report generation.

Note

The sample profiles include report settings for both Firewall Activity Reports and Alerting and Monitoring Reports. For more information on Alerting and Monitoring Reports, see “Alerting and Monitoring” on page 103.

Firewall Reports

Firewall Activity Profiles can generate reports in a variety of formats. Most of these reports can be viewed and printed in HTML, Microsoft Word, or Microsoft Excel formats.

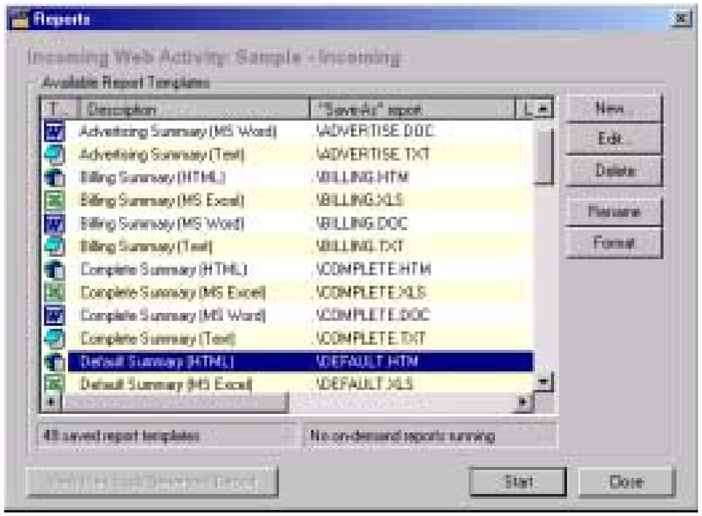
To see the report formats, select a General, Outgoing, or Incoming Firewall Activity profiles and click **Report** to open the Reports dialog box.

Generating Firewall Activity Reports

To generate a firewall report:

1. On the Main Console, select a profile from one of the Firewall Activity profile lists.
2. Click **Report** to open the Reports dialog box.

.



Incoming Web Activity: Sample - Incoming

Available Report Templates

T	Description	"Save As" report	L
W	Advertising Summary (MS Word)	\ADVERTISE.DOC	
	Advertising Summary (Text)	\ADVERTISE.TXT	
	Billing Summary (HTML)	\BILLING.HTM	
X	Billing Summary (MS Excel)	\BILLING.XLS	
W	Billing Summary (MS Word)	\BILLING.DOC	
	Billing Summary (Text)	\BILLING.TXT	
	Complete Summary (HTML)	\COMPLETE.HTM	
X	Complete Summary (MS Excel)	\COMPLETE.XLS	
W	Complete Summary (MS Word)	\COMPLETE.DOC	
	Complete Summary (Text)	\COMPLETE.TXT	
	Default Summary (HTML)	\DEFAULT.HTM	
X	Default Summary (MS Excel)	\DEFAULT.XLS	

48 saved report templates

No on-demand reports running

3. Select a report from the **Available Report Templates** list.

   An Available Report Template is a collection of saved report settings that you can use when creating or scheduling a report. See “Memorized Report Settings” on page 203.

4. Click **Start** to generate the report.

Once the data is collected, Firewall Suite launches your browser and loads the report. If you are generating a Microsoft Word or Excel report, Firewall Suite launches the appropriate program.

Reports and Color Depth

To properly display reports, your operating system color palette must be set to a minimum color depth of 16 bits. Settings below 16 bits may result in graphs where individual pixels can be seen.

To change color depth:

Right-click on your desktop, then select **Properties > Settings > Colors**. Make sure the color depth is at least 16 bit.

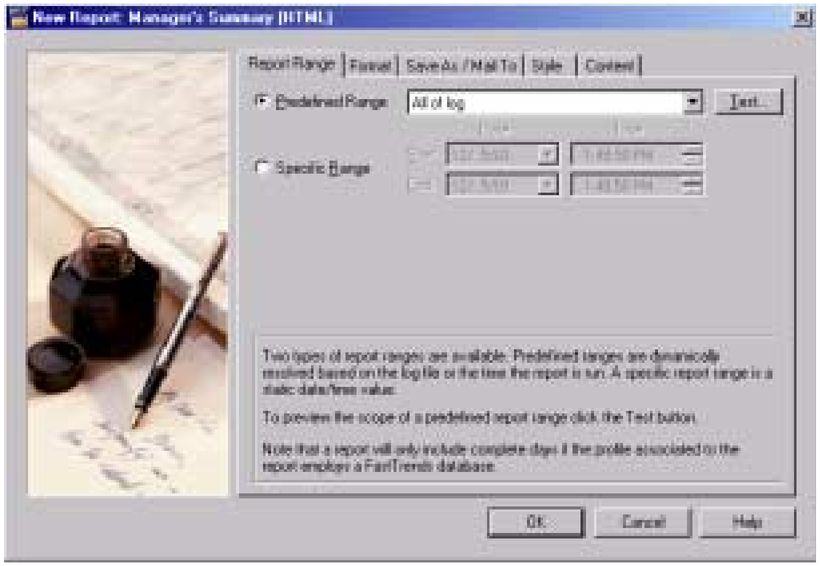
Memorized Report Settings

When you create a Firewall report, Firewall Suite lets you save the settings so that you can apply them to other reports at a later time.

To create a new memorized report setting:

1. On the Main Console, select any Firewall or Web Activity profile.
2. Click **Report** to open the Reports dialog box.
3. Click **New**. The Report Description dialog box opens.
4. Enter a descriptive name for the report setting you are creating.
5. Click **OK**. The New Report window opens.

6. Select the **Report Range** tab to open the Report Range dialog box.



● Predefined Range: All of log

○ Specific Range

Two types of report ranges are available. Predefined ranges are dynamically resolved based on the log file or the time the report is run. A specific report range is a static date/time value.

To preview the scope of a predefined report range click the Test button.

Note that a report will only include complete days if the profile associated to the report employs a FastTrends database.

7. Do one of the following:

– Select a pre-defined range from the dropdown list. You can add a pre-defined range to the list in the Report Ranges dialog box of the Options window. For more information, see “Report Range Definitions” on page 230.

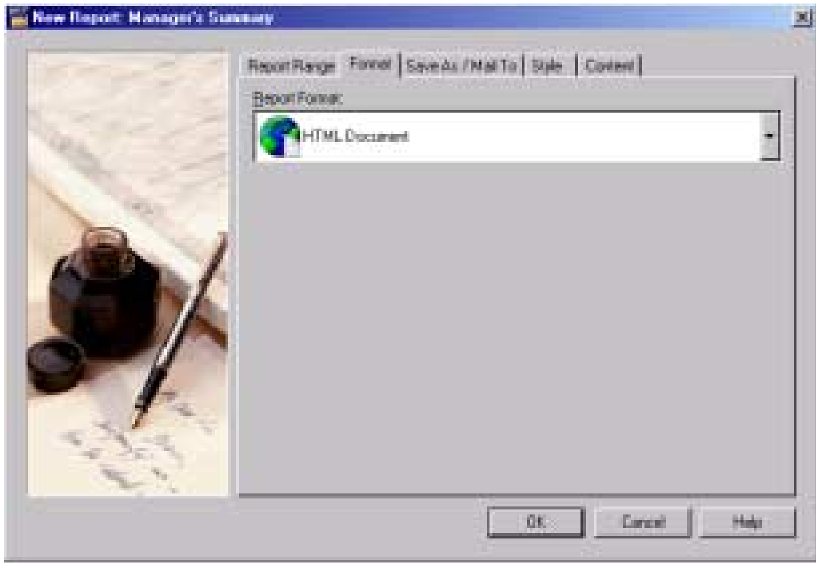
– Select **Specific Range** and type a start and end date and time to set up your own time range. “Report Range Definitions” on page 230 shows the options available. Make sure the date range you specify corresponds to existing dates in the log file.

Notes

Use the format `mm/dd/yyyy` in the **Date** text box. Use 24-hour time format, including seconds (`hh:mm:ss`) for the **Time** fields. To correctly enter the format, it may be easiest to use the dropdown calendar interface for the **Date** text box. To enter the correct format for the **Time** text box, you may also scroll.

If you access your log file remotely via FTP or HTTP, the Date/Time ranges read N/A.

8. Select the **Format** tab. The Format dialog box opens.



Report Format: HTML Document

9. Select one of the following report formats from the list:

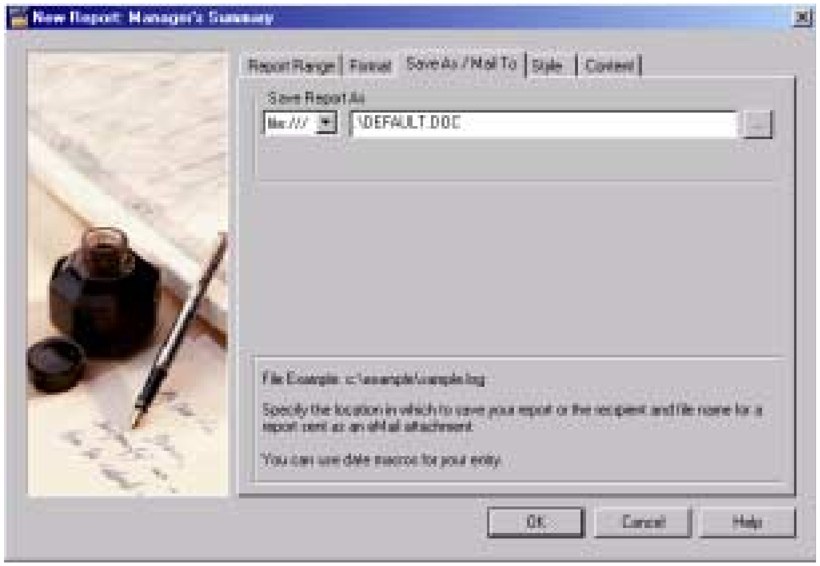
- HTML Document
- Microsoft Word Document
- Microsoft Excel Document

Note
To generate reports in the Microsoft Word or Microsoft Excel formats, You must have Microsoft Office 95 or 97 installed on your computer. Stand-alone versions of Word and Excel do not provide the macro language necessary to create these reports.

- Comma-delimited Document
- ASCII Text Document

The HTML report is the quickest to create. All other reports are based on the HTML report.

10. Select the **Save As/Mail To** tab to open the Save As/Mail To dialog box, in which you identify the destination and name for saved reports. This dialog box varies in appearance, depending on which **Save Report As** option you select.



Save Report As: file:/// \DEFAULT.DOC

File Example: c:\example\sample.log

Specify the location in which to save your report or the recipient and file name for a report sent as an eMail attachment.

You can use date macros for your entry.

11. Choose from one of the following Save Report As methods:

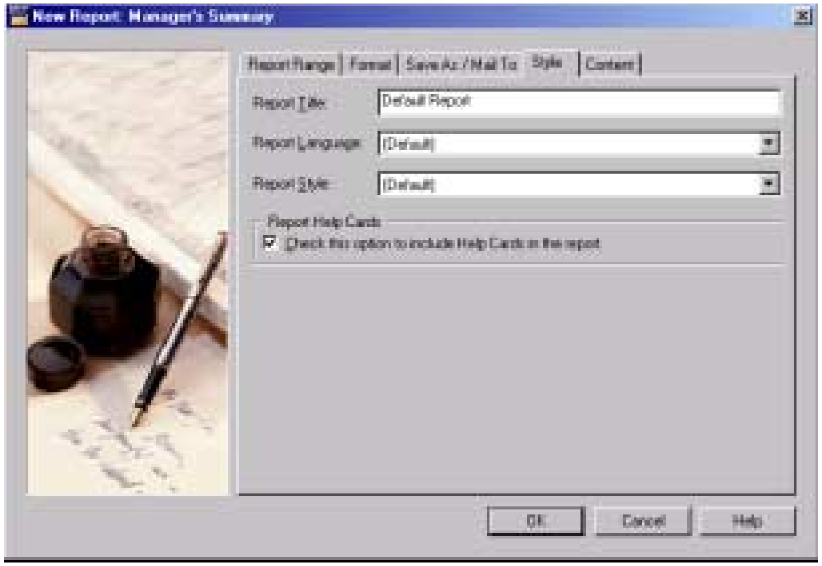
- To save the file on a local drive or a drive mapped to your computer, select **file:///** and type a path or browse to the directory where you want to save the report.
- To upload the file using ftp, select **ftp://** and type a path or browse to the directory where you want to save the report. If your ftp server requires a login, type the login name and password.
- To send the file an email attachment to the addresse(s) you specify and save a copy of the report on a mapped or local drive, select **mailto:**, browse to the location where you want to save the report, and type the email address(es) where you want to send the report.

Notes

You can use date macros to specify the names for saved reports. See "Date Macros" on page 353

To send reports as email attachments, you must define email server settings. See "E-Mail dialog box settings" on page 296 for details.

12. Select the **Style** tab.



Report Title: Default Report

Report Language: (Default)

Report Style: (Default)

Report Help Cards

☑ Check this option to include Help Cards in the report

13. In the **Report Title** text box, type the title that you want to appear at the top of your report above the log profile description.

14. Use the **Report Language** dropdown list to select the language that you want to use for the report.

    Report languages are among the Options made available to all profiles of one type. A language can be English, French, German, or Spanish, but specific text phrases and titles are also included in the concept of a language. The text of titles for tables and graphs that appear in reports, for example, are configured as a part of a language.

    You can change report titles to meet the needs of your organization. Create a custom language for your report that includes the preferred text for tables and graphs. For more information on defining Report Language Settings, see “Language dialog box settings (firewall activity profiles only)” on page 310.

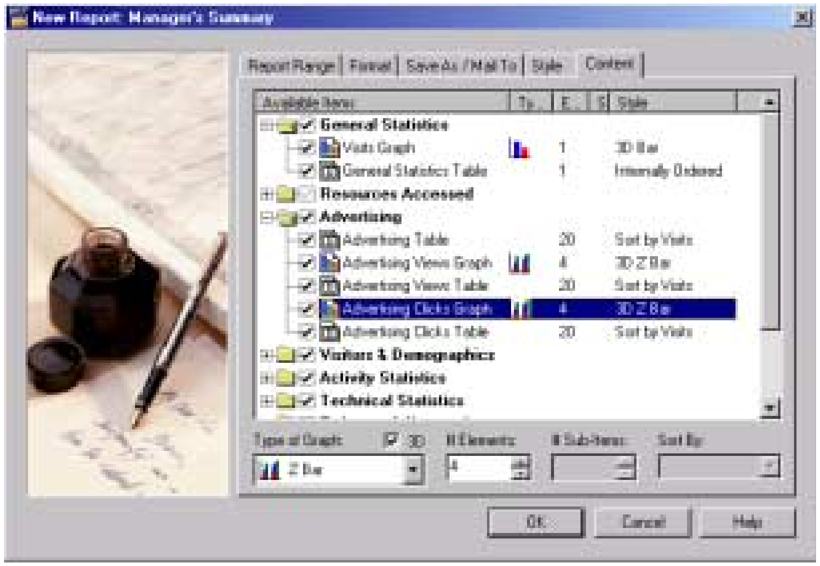
15. Use the **Report Style** dropdown list to select a style from the dropdown list.

    Style identifies the colors, fonts, table borders, and other criteria of report appearance. You can create a style that uses your organization's colors and logo. Some style selections affect report output. For example, you can output one file per section, which creates smaller files and shortens printing or download time. You can choose a style that eliminates the table of contents, or one that includes the long descriptions of each table and graph.

    For more information about creating your own style to add to this dropdown list, see “Adding or Editing Report Styles” on page 219.

16. Select **Report Help Cards** if you wish to append a description and explanation of the various report components to the bottom of the report. Report Help Cards can help you gain an understanding of how to use the reports when you are just starting out, or may provide helpful information to people receiving the reports.

17. Select the **Content** tab. The Content dialog box opens. Select the check box for each report item you want to include in this report. Report Items are groups of related tables and graphs.



Available Items	Ty..	E..	S	Style
☑ General Statistics				
☑ Visits Graph		1		3D Bar
☑ General Statistics Table		1		Internally Ordered
□ Resources Accessed				
☑ Advertising				
☑ Advertising Table		20		Sort by Visits
☑ Advertising Views Graph		4		3D Z Bar
☑ Advertising Views Table		20		Sort by Visits
☑ Advertising Clicks Graph		4		3D Z Bar
☑ Advertising Clicks Table		20		Sort by Visits
☑ Visitors & Demographics				
☑ Activity Statistics				
☑ Technical Statistics				

Type of Graph: Z Bar ☑ 3D # Elements: 4 # Sub-Items: Sort By:

18. Expand the Available Items, and select the individual tables and graphs to include.

For each individual graph:

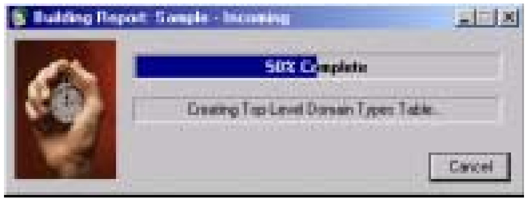
- Select a **Type of Graph** from the dropdown list. Not all graph types are available for all graphs. The choices may include: stack bar, standard bar, Z-bar, pie chart, area graph, line graph, side bar, and side stack bar.
- Select **3D**, to generate a 3-dimensional graph or de-select 3D to generate a 2-dimensional graph. These options are not available for all graphs.
- Enter the **# Elements** if this option is available. You can increase or decrease the number of elements to include in your graph (for example, the number of bars for bar charts or slices in a pie chart).

  - Enter the **# Sub-Items** if this option is available. You can increase or decrease the number of sub-items or elements to include. These are detailed data associated with each element item.
  - Select the criteria by which to sort the data in the **Sort By** dropdown list if this option is available.

19. Click **OK** to save the report settings. You return to the Reports dialog box.

20. Select the report template you just created and click **Start** to activate the settings you have defined and to generate the report. A Building Report progress window opens and shows you the status of your report generation.

Note
While the report is being generated, you can click **Cancel** to end the report generation.



Creating Top-Level Domain Types Table...

After the data is collected, Firewall Suite launches your browser and loads the report. If you are generating a Microsoft Word or Microsoft Excel report, Firewall Suite launches the appropriate program.

Notes
See "Alerting and Monitoring Reports" on page 213 for details on modifying report style and content.

Select any Available Report Template from the list and click **View Previously Generated Report** to quickly view the report if it has been previously generated. When you use this option, you access the report from a file rather than analyzing the data and completely rebuilding the report.

Alerting and Monitoring Reports

There are three types of Alerting and Monitoring reports:

- The *Short* report provides a basic activity information for the device specified, including how long the device was down and the total up and down times for the reporting period.
- The *Complete* report provides a complete report on the specified device. Each alerting event is described in detail, including date and time of the event, event type, and a description of the responses sent.
- The *Summary* report provides the current state of every monitored device.

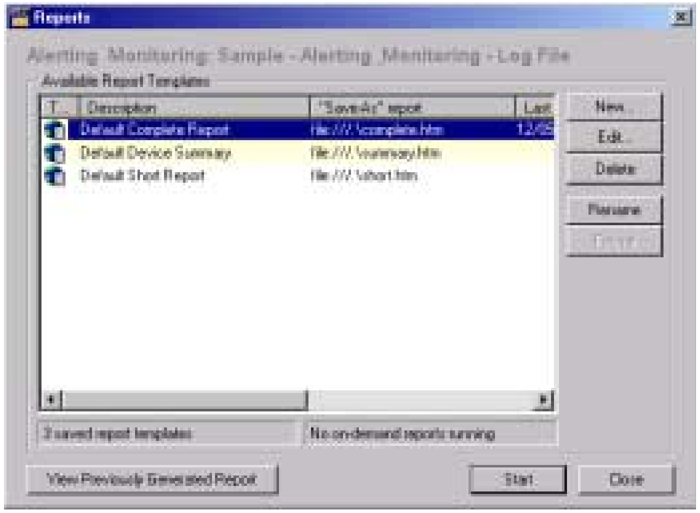
A default setting for each report type is provided in the **Memorized Report** dropdown list in the Create Report dialog box. To see the three defaults, select an Alerting and Monitoring profile and select **Report**.

You can override the settings of any memorized report (including the default reports) by changing the values in the text boxes of each tab in the report dialog box. *The overrides affect only the current report*. For a description of the report settings to use to override memorized report settings or to create a new memorized report, see “Memorized Report Settings” on page 203.

Creating Alerting and Monitoring Reports

To create an alerting and monitoring report:

1. In the Main Console, select the Alerting and Monitoring profile you want to use for the report from the Profile Description list.
2. Click **Report**. The Reports dialog box opens.



Alerting Monitoring: Sample - Alerting Monitoring - Log File

Available Report Templates

T...	Description	"Save-As" report	Last
	Default Complete Report	file:///.\complete.htm	12/0
	Default Device Summary	file:///.\summary.htm	
	Default Short Report	file:///.\short.htm	

3 saved report templates

No on-demand reports running

3. Select the report you want to use from the **Available Report Templates** list.
4. Click **Start** to run the report.

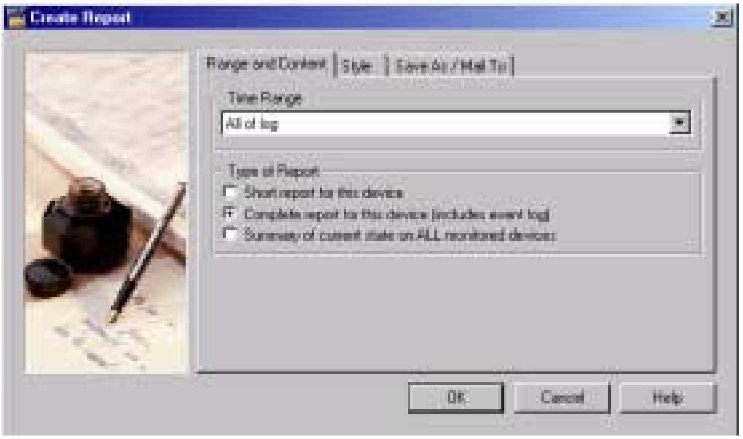
   Once the data is collected, Firewall Suite launches your browser and loads the report. If you are generating a Microsoft Word or Microsoft Excel report, Firewall Suite launches the appropriate program.

Memorized Alerting and Monitoring Report Settings

You can save new memorized settings for a report. Complete the following steps, click **Memorize**, and name the new group of settings to make them available in the memorized report dropdown list.

To create a new memorized report setting for alerting and monitoring reports:

1. Select any alerting and monitoring profile and click **Report** to open the Reports dialog box.
2. Click the **Range and Content** tab to display the Range and Content dialog box.



Time Range

All of log

Type of Report

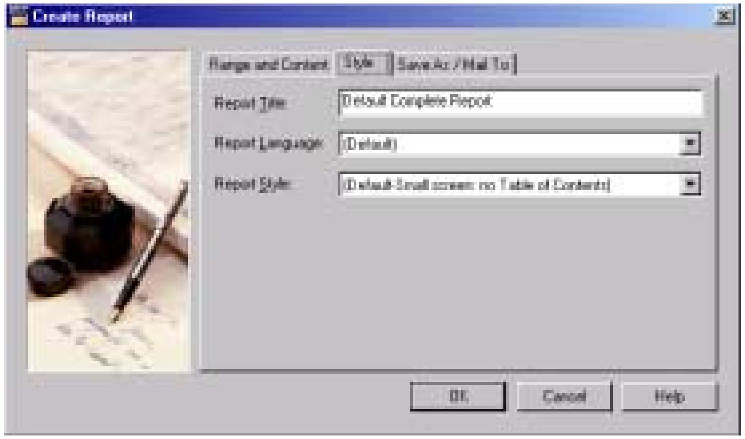
☐ Short report for this device

☑ Complete report for this device (includes event log)

☐ Summary of current state on ALL monitored devices

3. By default, all alerting activity in the log is included in the report, but you can specify a range in the **Time Range** dropdown list.
4. Select the type of alerting and monitoring report that you want to create (short report, complete report, or summary report).

5. Select the **Style** tab to open the Style dialog box.



Report Title: Default Complete Report

Report Language: (Default)

Report Style: (Default-Small screen: no Table of Contents)

6. In the **Report Title** text box, type the title that you want to appear at the top of your report above the log profile description.

7. Use the **Report Language** dropdown list to select the language that you want to use for the report.

   Report languages are among the General Options made available to all profiles of one type. A language can be English, French, German, or Spanish, but specific text phrases and titles are also included in the concept of a language. The text of titles for tables and graphs that appear in reports, for example, are configured as a part of a language.

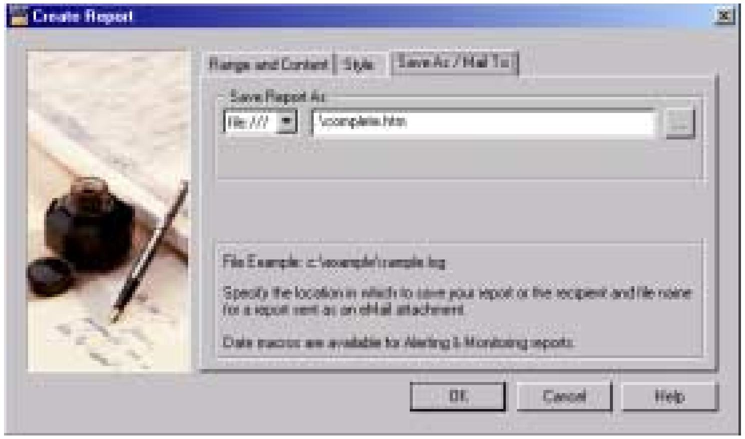
   You can change report titles to meet the needs of your organization. Create a custom language for your report that includes the preferred text for tables and graphs. See “Alerting & Monitoring - General dialog box settings” on page 331.

8. Use the **Report Style** dropdown list to select a style from the dropdown list.

Style identifies the colors, fonts, table borders, and other criteria for report appearance. You can create a style that uses your organization’s colors and logo. Some style selections affect report output. For example, you can output one file per section, which creates smaller files and shortens printing or download time. You can choose a style that eliminates the table of contents, or one that includes the long descriptions of each table and graph.

For more information about creating your own style to add to this dropdown list, See “Adding or Editing Report Styles” on page 219.

9. Click the **Save As/Mail To** tab to open the Save As/Mail To dialog box.



Save Report As: file:/// \complete.htm

File Example: c:\example\sample.log

Specify the location in which to save your report or the recipient and file name for a report sent as an eMail attachment.

Date macros are available for Alerting & Monitoring reports.

10. Choose how you want to distribute the report.

    - To save the file on a local drive or a drive mapped to your computer, select **file:///** and type a path or browse to the directory where you want to save the report.
    - To upload the file using ftp, select **ftp://** and type a path or browse to the directory where you want to save the report. If your ftp server requires a login, type the login name and password.

- To send the file an email attachment to the addresse(s) you specify and save a copy of the report on a mapped or local drive, select **mailto:**, browse to the location where you want to save the report, and type the email address(es) where you want to send the report.

Notes
You can use date macros to specify the names for saved reports. See “Date macros” on page 362

To send reports as email attachments, you must define email server settings. See “E-Mail dialog box settings” on page 296 for details.

11. Click **OK** to save your settings and return to the Reports dialog box.
12. Click **Start** to activate the settings you have defined and to generate the report.

Note
While the report is generating, you can click Stop Here to create the report with the data collected so far, or click Cancel to halt report generation.

Once the data is collected, Firewall Suite launches your browser and loads the report. If you are generating a Microsoft Word or Microsoft Excel report, Firewall Suite launches the appropriate program.

Note
See “Alerting and Monitoring Reports” on page 213 for details on modifying report style and content.

Customizing Reports

Firewall Suite provides report editors for tailoring your reports:

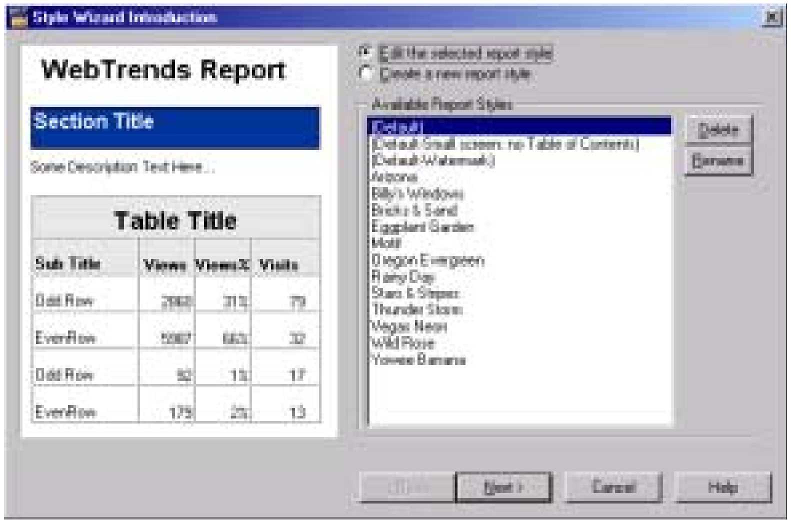
- The Style Editor modifies the colors, fonts, table frames, and logos used in HTML reports. You can create multiple combinations, save them, and apply them to different reports. For more information, see “Adding or Editing Report Styles” on page 219.
- The Language Editor customizes reports with terminology common to your organization or creates foreign language versions of your reports. For more information on the language editor, see “Adding or Editing Report Languages” on page 228.
- The Content Editor specifies the tables and graphs included in each table. For more information, see “Modifying Report Content” on page 229.

Adding or Editing Report Styles

Style Editor styles apply only to Firewall Suite reports generated as HTML files. Reports generated as Microsoft Word or Microsoft Excel documents *must* be edited using those programs.

To add or edit a style:

1. On the Main Console, select **Tools > Style Editor** to access the Style Wizard Introduction dialog box. The steps of the Style Wizard take you through the process of creating or changing a report style.



WebTrends Report

Section Title

Some Description Text Here...

Table Title			
Sub Title	Views	Views%	Visits
Odd Row	2968	31%	79
EvenRow	5987	66%	32
Odd Row	92	1%	17
EvenRow	175	2%	13

● Edit the selected report style
○ Create a new report style

Available Report Styles

- (Default)
- (Default-Small screen, no Table of Contents)
- (Default-Watermark)
- Arizona
- Billy's Windows
- Bricks & Sand
- Eggplant Garden
- Motif
- Oregon Evergreen
- Rainy Day
- Stars & Stripes
- Thunder Storm
- Vegas Neon
- Wild Rose
- Yowee Banana

2. The Introduction dialog box displays a list of report styles on the right side, while on the left, the dialog box shows a sample of the selected style.

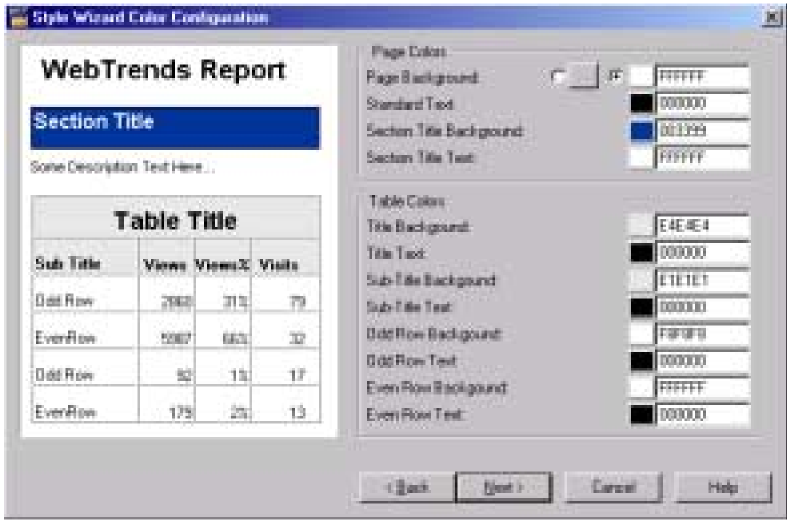
3. This dialog box lets you do a number of tasks related to styles:

   – Modify an existing style. Select a style in the Available Report Styles list, then select **Edit the Selected Report Style**. You can give the modified style a new name in the last dialog box of the wizard sequence to save it, and you can retain the unmodified style as well.

   – Define a new style. Select **Create New Report Style** to define a new style.

- Rename an existing style. Select a style in the Existing Styles list, and click the **Rename** button. Type a new name for the style.
- Delete a style. Select a style in the Existing Styles list, and click the **Delete** button. The style is deleted.

4. Click **Next**. The Color Configuration dialog box opens.



Page Colors

Page Background	○ ... ● FFFFFF
Standard Text	000000
Section Title Background	003399
Section Title Text	FFFFFF

Table Colors

Title Background	E4E4E4
Title Text	000000
Sub-Title Background	E1E1E1
Sub-Title Text	000000
Odd Row Background	F8F8F8
Odd Row Text	000000
Even Row Background	FFFFFF
Even Row Text	000000

5. Select a background image for your report pages.

a. Select the first **Page Background** radio button and click the **...** button. The Open a File dialog box appears.

b. Browse to the desired GIF or JPEG file and select it.

c. Click **Open**.

6. Select a color for a page background.

a. Select the second **Page Background** radio button. The color sample buttons display the currently selected color

b. Click the color sample button.

c. When the dialog box opens, select the desired color.

– Select a color for other page elements and for table elements.

Click the color sample button for each of the desired elements.

7. Click **Next**. The Font Selection dialog box opens.

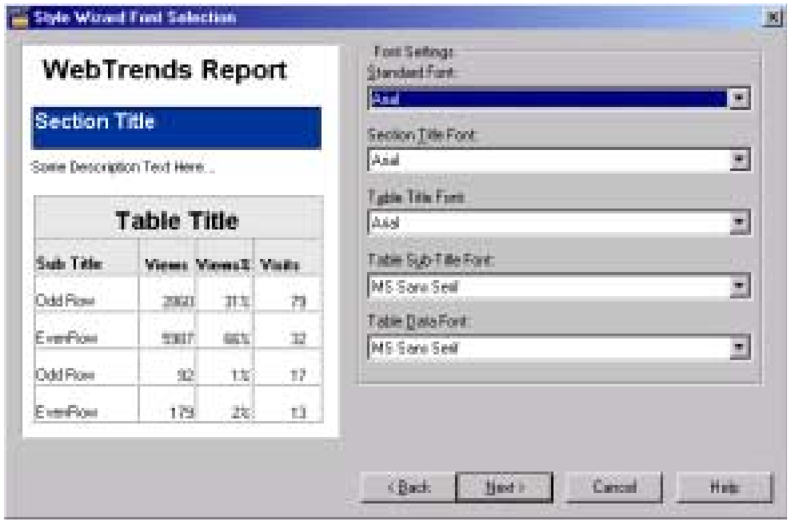


Table Title			
Sub Title	Views	Views%	Visits
Odd Row	2802	31%	79
Even Row	5907	66%	32
Odd Row	92	1%	17
Even Row	179	2%	13

Standard Font: Arial

Section Title Font: Arial

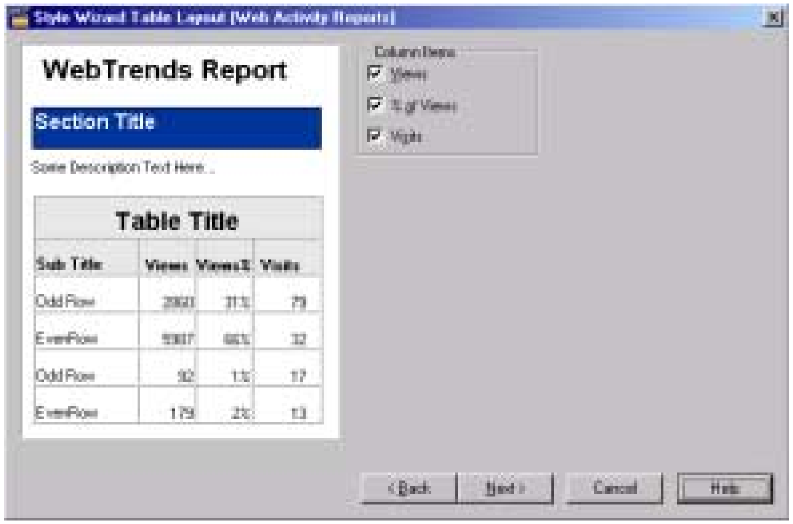
Table Title Font: Arial

Table Sub-Title Font: MS Sans Serif

Table Data Font: MS Sans Serif

8. Use the dropdown lists to identify the fonts for each report section. As you change fonts, the sample on the left displays your selections.

9. Click **Next**. The Table Layout (for Web Activity Reports) dialog box opens.



WebTrends Report

Section Title

Some Description Text Here...

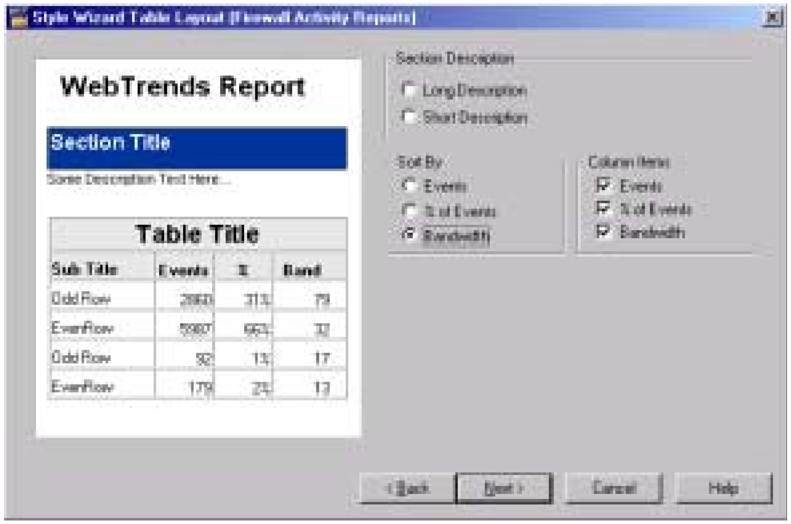
Table Title			
Sub Title	Views	Views%	Visits
Odd Row	2860	31%	79
EvenRow	5907	66%	32
Odd Row	92	1%	17
EvenRow	179	2%	13

Column Items
☑ Views
☑ % of Views
☑ Visits

This dialog box lets you modify report features for Incoming Web Activity and Outgoing Web Activity reports.

10. In the Column Items area of the dialog box, select the columns that will be included in report tables.

11. Click **Next**. The Table Layout (Firewall Activity Reports) dialog box opens.



Style Wizard Table Layout (Firewall Activity Reports)

WebTrends Report

Section Title

Some Description Text Here...

Table Title			
Sub Title	Events	%	Band
Odd Row	2860	31%	79
EvenRow	5987	66%	32
Odd Row	92	1%	17
EvenRow	179	2%	13

Section Description

○ Long Description

○ Short Description

Sort By

○ Events

○ % of Events

● Bandwidth

Column Items

☑ Events

☑ % of Events

☑ Bandwidth

This dialog box lets you modify report settings for General Firewall Activity reports.

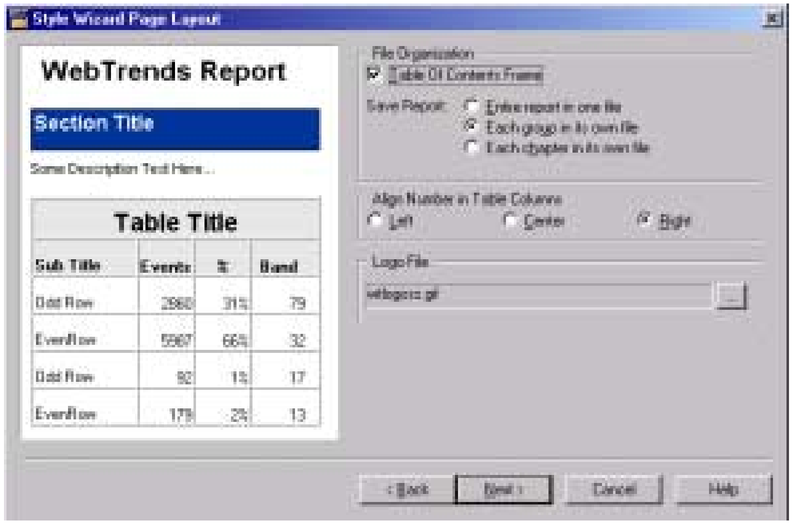
12. In the Section Description area of the dialog box, you can include long or short descriptions of each of the tables in the reports. These descriptions are defined in the Languages dialog boxes of the Options window. For more information, see “Language dialog box settings (firewall activity profiles only)” on page 310 and “Language dialog box settings (alerting and monitoring profiles)” on page 337.

13. In the Sort By area of the dialog box, you can choose to order the columns of your tables in ascending order by:

   - *Events*. An action recorded by the firewall and stored in the firewall log file.
   - *Percentage of Events*. The percentage of the total number of events that an item represents.
   - *Bandwidth*. The amount of activity coming through and leaving the firewall, measured in KB transferred.

14. In the Column Items area of the dialog box, select the columns that will be included in report tables.

15. Click **Next**. The Page Layout dialog box opens.



Style Wizard Page Layout

WebTrends Report

Section Title

Some Description Text Here...

Table Title

Sub Title	Events	%	Band
Odd Row	2960	31%	79
EvenRow	5967	66%	32
Odd Row	92	1%	17
EvenRow	179	2%	13

File Organization

☑ Table Of Contents Frame

Save Report: ○ Entire report in one file
● Each group in its own file
○ Each chapter in its own file

Align Number in Table Columns

○ Left ○ Center ● Right

Logo File

wtlogo.gif

16. Select the **Table of Contents Frame** check box to include a framed table of contents in HTML reports.

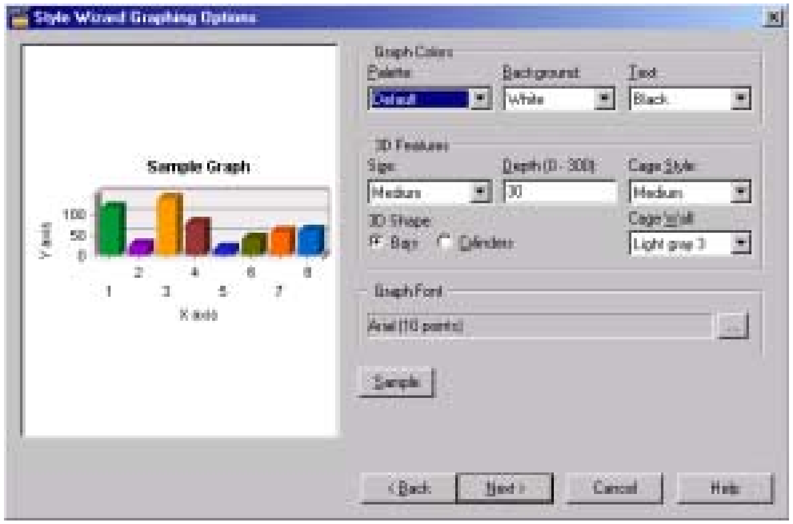
17. Select the way that the report will be saved.

   - **Entire report in one file** saves the entire report in a single file.
   - **Each group in its own file** saves each group (for example, General Statistics, Bandwidth Usage) in a separate file.
   - **Each chapter in its own file** saves each chapter (for example, the General Firewall Statistics chapter in the General Statistics group) in a separate file.

18. In the Align Number in Table Columns area of the dialog box, choose whether to center, left-justify, or right-justify the data in table report cells.

19. Click the browse button to specify the location of a logo for all of your reports. This logo file appears at the bottom of the last page of your report.

20. Click **Next**. The Graphing Options dialog box opens.



Style Wizard Graphing Options

Graph Colors
Palette: Default
Background: White
Text: Black

3D Features
Size: Medium
Depth (0 - 300): 30
Cage Style: Medium
3D Shape: ● Bars ○ Cylinders
Cage Wall: Light gray 3

Graph Font
Arial (10 points)

This dialog box lets you select colors, fonts, and 3-D features for the report graphs.

21. Use the dropdown lists to select colors for:

- *Palette*. Select the color scheme applied to the graph itself.
- *Background*. Select the color behind the graph and behind the legends.
- *Text*. Select the color of text for headings and labels.

22. Select the 3D features. Click **Test** to see what your 3D feature selections will look like.

- **Size**. Select the size in which you want the graph elements to appear
- **Depth**. Select the three-dimensional depth of the "cage" (the x and y backdrop).
- **Cage style**. Select the thickness of the cage walls for your graph.
- **Cage wall**. Select the color of the cage walls.

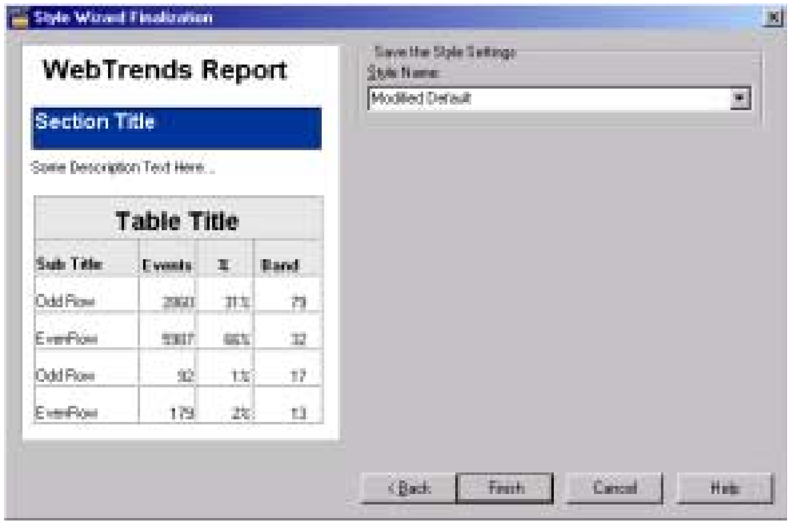
23. Select the Graph Font settings. Click **Sample** to see what your font selections will look like.

a. Use the **Font** dropdown list to select the font face applied to all text: Times Roman, Swiss or Modern.

b. Select the check box for the **Font Style** you want: **Bold**, **Italic**, or **Underline**. Leave the check boxes clear for Regular font style.

c. Use the **Size** dropdown list to select a font size.

24. Click **Next**. The Finalization dialog box opens.



WebTrends Report

Section Title

Some Description Text Here...

Table Title			
Sub Title	Events	%	Band
Odd Row	2860	31%	79
EvenRow	5907	66%	32
Odd Row	92	1%	17
EvenRow	179	2%	13

Save the Style Settings

Style Name: Modified Default

25. Type a name for the report style into the **Style Name** text box, or use the dropdown list to select an existing name.

26. Click **Finish** to save your settings and exit the Style Editor.

Adding or Editing Report Languages

Use the **Language** settings in the Options window to modify the default languages or to customize the words and phrases that appear in reports.

- For Firewall and Proxy Server profiles, use the language editor in the General Options dialog box. See "Language dialog box settings (firewall activity profiles only)" on page 310.

- For Alerting and Monitoring reports, use the language editor in the Alerting and Monitoring Options dialog box. See "Language dialog box settings (alerting and monitoring profiles)" on page 337.

Modifying Report Content

The **Content** tab in the Edit Report window lets you modify the content of sections included in a report.

Note
The tables and graphs available vary according to profile and firewall type.

---

1. On the Main Console, select the profile with the report you wish to modify,
2. Click **Report**. The Reports dialog box opens.
3. In the Available Report Templates list, Click **Edit**. The Edit Report dialog box opens.
4. Select the **Content** tab in the Edit Report window to open the Content dialog box.
5. Use the **Available Items** list to select the tables and graphs to be included in the report. Select the check box next to an item to include it; clear the check box to leave it out.
6. Use the **Graph Type** dropdown list to choose the type of graph to be used. The list shows a thumbnail for each graph type.
7. Once you have selected a graph type, select **2D** to use the two-dimensional version of the graph, or **3D** to use the three-dimensional version.
8. Use the **Elements** list to select the number of elements in the selected graph or the number of items in the selected table.
9. If you have selected a table that includes secondary information (such as Top Search Keywords with Engine Detail) use the **Sub-Items** list to specify the number of sub-items to be included.
10. Click **OK** to save your report settings. Once they are memorized, you can apply them when you are creating or scheduling a report.
11. Click **Start** to generate the report.

Report Range Definitions

When you generate a report, you can specify the date or time range to include in the report.

The following lost defines the predefined report range definitions.

All of Log
Reports on all data in the log file.

Specify Date/Time
Reports on the time frame from a specified Start Time and Date to a specified End Time and Date. Times use the 24-hour format. For 2:30 PM, type `14:30:00`. Dates use the `mm/dd/yyyy` format. For Europe, use `dd/mm/yyyy`. For Japan, use `yyyy/mm/dd`.

Last 15 minutes
Reports on the activity that has taken place in the last 15 minutes.

Last hour
Reports on the activity that has taken place in the last hour.

Last 12 hours
Reports on the activity that has taken place in the last 12 hours.

Today
Reports on activity for the current day from midnight to 11:59:59.

Yesterday
Reports on the activity for yesterday from midnight to 11:59:59.

This week
Reports on activity for the current calendar week, from Sunday up to the time when the report is started.

Last week
Reports on activity for the last calendar week, from Sunday to Saturday.

Last 7 days
Reports on activity for the seven calendar days that ended at 11:59 yesterday.

These 2 weeks

Reports on activity from Sunday of the previous calendar week up to the time when the report is started.

Last 14 days

Reports on activity for the 14 calendar days that ended at 11:59 p.m. yesterday.

Last 2 weeks

Reports on activity for the last two calendar weeks.

This month

Reports on activity from the first of the current calendar month until the time when the report is started.

Last full month

Reports on activity for the last calendar month. For example, selecting this range in mid-July will generate a report covering the month of June.

Last 30 days

Reports on activity for the last 30 days.

This quarter

Reports on activity for the current calendar quarter up to the time when the report is started.

Last quarter

Reports on activity for the last calendar quarter.

This 6 months

Reports on activity for the current six-month period, either January–June or July–December.

Last 6 months

Reports on the activity for the six-month period previous to the current one. For example, selecting this range in March 2002 generates a report for July–December 2001.

This year (by equal 4-week periods)

Reports on activity from January 1 of the current year to the time when the report is started. Each bar in the graph represents a four-week period.

This year (by months)

Reports on activity from January 1 for the current year up to the time when the report is started. Each bar in the graph represents one month.

Last year (by equal 4-week periods)

Reports on activity for the last full calendar year. Each bar in the graph represents a four-week period.

Last year (by months)

Reports on activity for the last full calendar year. Each bar in the graph represents one month.

This year and last year (by months)

Reports on activity from January 1 of the current year to the time when the report was started plus the activity for the previous calendar year. Each bar in the graph represents one month.

Last day of log

Reports on all activity from midnight to 11:59:59 p.m. for the day that includes the very last entry in the log file.

Previous day of log

Reports on all activity from midnight to 11:59:59 p.m. for the day before the day that includes the very last entry in the log file.

Last week of log

Reports on activity from Sunday to Saturday for the week that includes the very last entry in the log file.

Previous week of log

Reports on activity from Sunday to Saturday for the calendar week previous to the week that includes the very last entry in the log file.

Last 7 days of log

Reports on activity for the last seven days of entries in the log file.

Last 2 weeks of log

Reports on activity from Sunday of the current week up to the last entry in the log file plus the activity for the calendar week previous to the current one.

Previous 2 weeks of log

Reports on activity from Sunday to Saturday for the last two full calendar weeks previous to the week that includes the very last entry in the log file.

Last 14 days of log

Reports on activity for the last 14 days of entries in the log file.

Last month of log

Reports on activity from the first day of the current calendar month up to the very last entry in the log file.

Previous month of log

Reports on activity from the first day through the last day of the calendar month previous to the month that includes the very last entry in the log file.

Last 30 days of log

Reports on activity for the last 30 days of entries in the log file.

Last quarter of log

Reports on activity from the first day of the current calendar quarter up to the very last entry in the log file.

Previous quarter of log

Reports on activity from the first day through the last day of the calendar quarter previous to the quarter that contains the very last entry in the log file.

Last year of log (by equal 4-week periods)

Reports on activity from January 1 of the current calendar year up to the very last entry in the log file. Each bar in the graph represents a four-week period.

Last year of log (by months)

Reports on activity from January 1 of the current calendar year to the very last entry in the log file. Each bar in the graph represents one month.

Previous year of log (by equal 4-week periods)

Reports on activity from January 1 to December 31 for the last full calendar year. Each bar in the graph represents a four-week period.

Previous year of log (by months)

Reports on activity from January 1 to December 31 for last full calendar year. Each bar in the graph represents one month.

First day of log

Reports on activity from midnight to 11:59:59 p.m. of the calendar day that includes the very first entry in the log file.

First week of log

Reports on activity from Sunday to Saturday for the calendar week that includes the very first entry in the log file.

First 2 weeks of log

Reports on activity from Sunday to Saturday for each of the calendar weeks in the two-week period that includes the very first entry in the log file.

First month of log

Reports on activity for the calendar month that includes the very first entry in the log file.

First quarter of log

Reports on activity for the calendar quarter that includes the very first entry in the log file.

First year of log (by equal 4-week periods)
Reports on activity from January 1 to December 31 of the calendar year that includes the very first entry in the log file. Each bar in the graph represents a four-week period.

First year of log (by months)
Reports on activity from January 1 to December 31 of the calendar year that includes the very first entry in the log file. Each bar in the graph represents one month.

Specifying a Distribution Method

You can save reports locally, transfer them using FTP, or send them by email. These methods are specified on the **Save As/Mail To** tab in the Create Report dialog box.

To save a report locally:

1. In the Main Console, select the profile you want to use for the report from the Profile Description list.
2. Click **Report**. The Reports dialog box opens.
3. Select the report for which you wish to specify a distribution method and click **Edit.**
4. Select the **Save As/Mail To** tab to open the Save As/Mail To dialog box.
5. Select **file:///** from the dropdown list.
6. In the **Save Report As** text box, type the file path where you want to save the report. If you don't know the location, click the browse button to navigate to the exact directory.
7. Select another tab or click **OK** to save your settings.

To transfer the report using FTP:

1. In the Main Console, select the profile you want to use for the report from the Profile Description list.
2. Click **Report**. The Reports dialog box opens.
3. Select the report for which you wish to specify a distribution method and click **Edit.**
4. Select the **Save As/Mail To** tab to open the Save As/Mail To dialog box.
5. Select **ftp://** from the dropdown list.
6. In the **Save Report As** text box, type the complete path from the root of the FTP server.
7. If the FTP server requires authentication, enter the **User Name** and **Password**.
8. Select another tab or click **OK** to save your changes.

To send the report by email:

1. In the Main Console, select the profile you want to use for the report from the Profile Description list.
2. Click **Report**. The Reports dialog box opens.
3. Select the report for which you wish to specify a distribution method and click **Edit.**
4. Select the **Save As/Mail To** tab to open the Save As/Mail To dialog box.
5. Select **mailto:** from the dropdown list.
6. If you want to save a copy of the report locally, type a file path in the **Save To** text box or browse to the location.

7. In the **Save Report As** text box, type the email address where the report should be sent.

Tip
If you routinely send a report to the same group of people, create an alias to a list of their email addresses rather than re-typing each address separately each time you send the report.

---

8. Select another tab or click **OK** to save your changes.

Limiting Memory Used by Reports

All entries in a log file must be included in the analysis so that accurate statistics can be calculated. The database for some categories of data can become quite large.

Determining Memory Usage

To determine which tables are using large amounts of memory, include the Debug Statistics table in each report. This table specifies the amounts of memory used by each table in the report.

To include the Debug Statistics table in a report:

1. In the Main Console, select the profile you want to use for the report from the Profile Description list.
2. Click **Report**. The Reports dialog box opens.
3. Select the report for which you wish to include the Debug Statistics table and click **Edit.**
4. When the Edit Report window appears, select the **Contents** tab.
5. Select the **Debug Statistics Table** check box.

Limiting Memory Usage

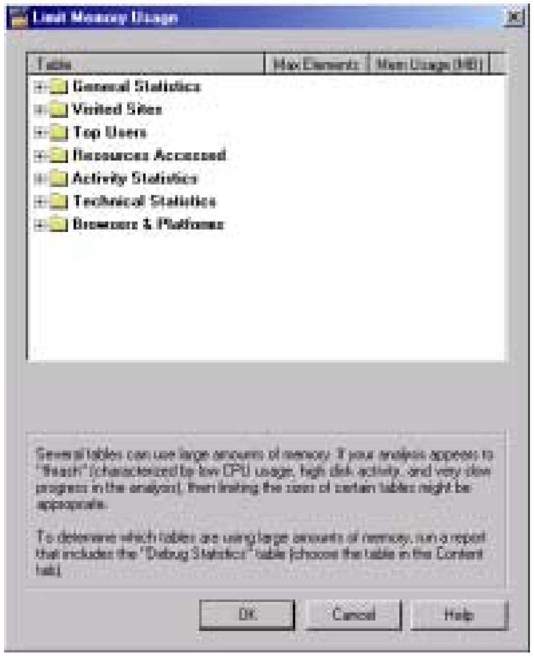
Note
This feature is available for firewall activity reports only.

If you have limited system resources or you are analyzing very large log files, you can limit the size of some tables to improve performance. This is an especially good idea if your analysis appears to “thrash”—a condition characterized by low CPU usage, high hard-disk activity, and slow progress in the analysis. In this case, you may want to limit the size of very large tables.

Use the Debug Statistics table to determine which tables are using large amounts of memory, then limit that usage by reducing the number of elements stored for that category.

To limit the memory used by tables:

1. On the Main Console, select the firewall activity profile used to generate the report in Profile Description list.
2. Select **Tools > Limit Memory Usage**. The Limit Memory Usage dialog box opens.



Several tables can use large amounts of memory. If your analysis appears to "thrash" (characterized by low CPU usage, high disk activity, and very slow progress in the analysis), then limiting the sizes of certain tables might be appropriate.

To determine which tables are using large amounts of memory, run a report that includes the "Debug Statistics" table (choose the table in the Content tab).

Because there are different sections and tables for each profile type, the Limit Memory Usage dialog box has different items available for each profile type, as a result, this dialog box will vary depending on the profile type you have selected.

3. Use the up- and down-arrows to adjust the maximum number of elements (in thousands) shown in each of the list boxes in the Max Elements column. The amount of memory (in MB) shown in the Mem Usage column will change to reflect the new number of elements.

   For example, in an incoming profile type, you can limit the number of users (elements) included in the report.

4. Click **OK**.

Chapter 7
Scheduling Reports

This chapter explains how to use the Scheduler to automate processing for:

- Profiles that are set up to run automatically
- On-demand reports that are generated through the Reports window
- Reports that are launched from the command line
- Real-time Analysis profiles

The Scheduler is launched when you start Firewall Suite, and a Scheduler icon is added to your system tray.

Open the Scheduler by clicking **Scheduler** on the Functions area, or by double-clicking the Scheduler icon in the system tray.

The Scheduler

The tabs in the Scheduler window let you work with events (any scheduled profile is referred to as an *event)*, monitor activity, and customize the way the Scheduler works.

Tabs

- *Scheduled Events* lets you maintain a list of all profiles that are processed by the Scheduler.
- *Schedule Log* provides a record of daily Scheduler activity.
- *Performance Analysis Log* provides a record of your system's performance for scheduled events and other system processes if you are running the program on Windows NT, and the Scheduler Performance feature is activated.

Functions Area

The following items are available in the upper right portion of the Scheduler Main window for all three Scheduler tabs.

- *Options* lets you change configuration settings for the Scheduler.
- *Remote* activates the Remote Scheduling server so that you can monitor activity and kick off reports remotely.
- *Service* lets you run the Scheduler as a Windows service.
- *Help* opens online help for the Scheduler.

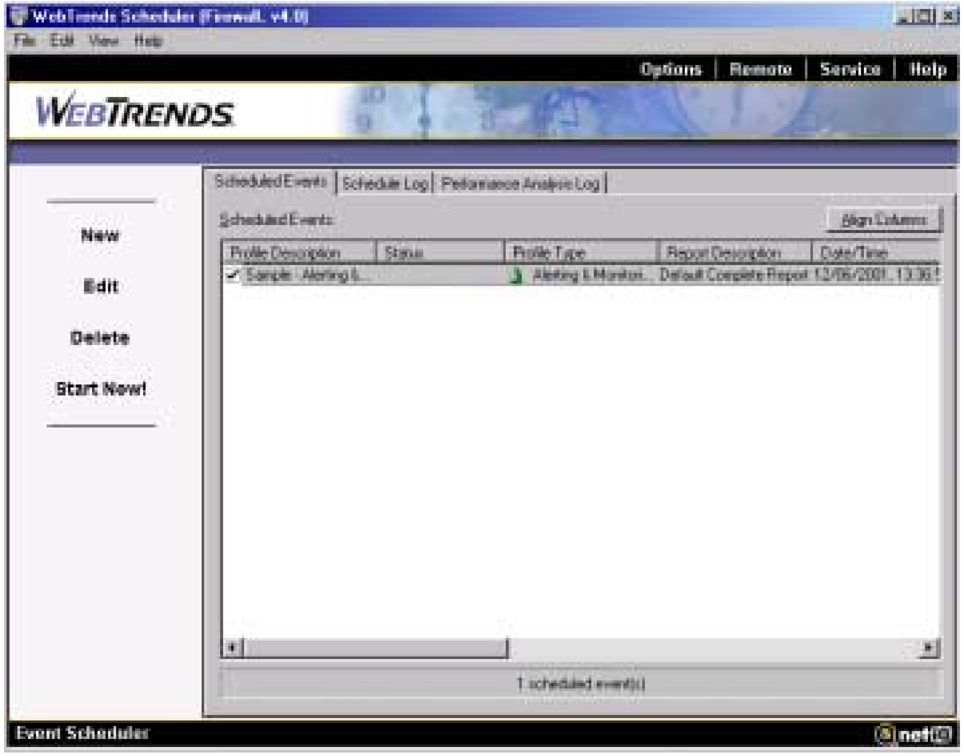
The Scheduler takes advantage of multi-processing and runs independently from other Firewall Suite processes. This design lets you set up events to run simultaneously, while keeping the main Firewall Suite application available for other tasks while reports are running.

Scheduling and Running Events

Scheduling a New Event

To schedule an event:

1. On the Main Console, click **Scheduler** to open the Scheduler Main window.
2. Select the **Scheduled Events** tab. (The **Scheduled Events tab** is the default.)

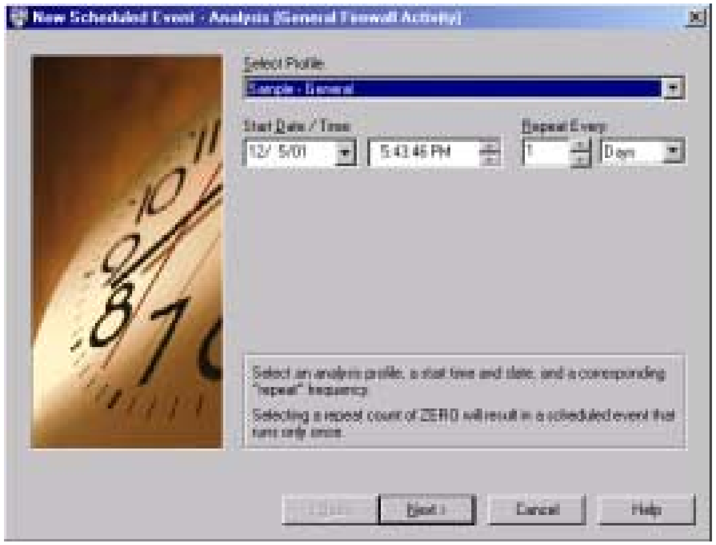


Profile Description	Status	Profile Type	Report Description	Date/Time
✓ Sample - Alerting &...		Alerting & Monitori...	Default Complete Report	12/06/2001, 13:36:!

Add a Scheduled Event

3. Click **New**. The Select Profile Type dialog box opens.

4. Select the profile type you are scheduling. The New Scheduled Event wizard opens to the Analysis dialog box.



New Scheduled Event - Analysis (General Firewall Activity)

Select Profile: Sample - General

Start Date / Time: 12/ 5/01 5:43:46 PM

Repeat Every: 1 Days

Select an analysis profile, a start time and date, and a corresponding "repeat" frequency.

Selecting a repeat count of ZERO will result in a scheduled event that runs only once.

5. In the **Start Date/Time** text boxes, type the date and time when you want the analysis to start. You can also select a date using the arrow buttons.

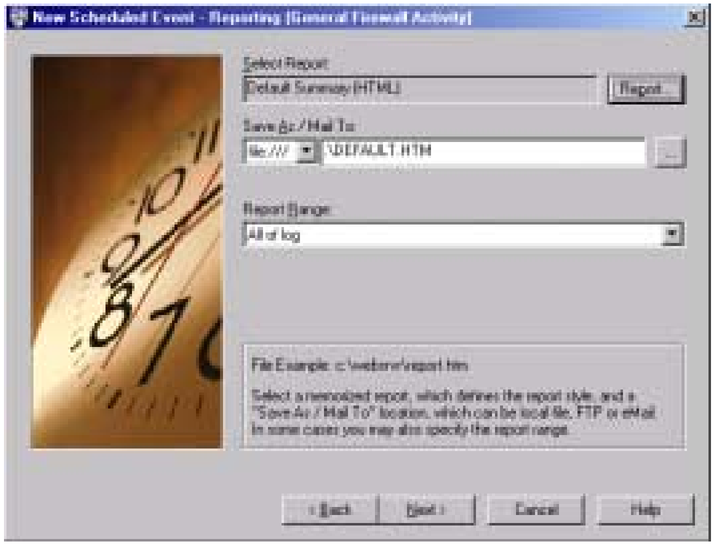
- If you type the time, use 24-hour clock format, including seconds (`hh:mm:ss`).
- If you type the date in the second text box, use the `dd/mm/yyyy` format. For example, type `07/31/2000`.

6. In the **Repeat Every** text boxes, select the interval at which to repeat the analysis and report.

Note
You can run reports simultaneously by scheduling them to run at the same time, or you can run them a minute apart if you want a specific order. The Scheduler Options window defines the number of events that can be processed at once.

---

7. Click **Next**. The Reporting dialog box opens.



New Scheduled Event - Reporting [General Firewall Activity]

Select Report: Default Summary (HTML)

Save As / Mail To: file:/// \DEFAULT.HTM

Report Range: All of log

File Example: c:\webroot\report.htm

Select a memorized report, which defines the report style, and a "Save As / Mail To" location, which can be local file, FTP or eMail. In some cases you may also specify the report range.

Set up the Report

8. Click **Report** to open the Reports dialog box and select a report. See “Memorized Report Settings” on page 217 for additional information.

9. In the **Save As/Mail To** text box, select a method for saving or delivering the report.

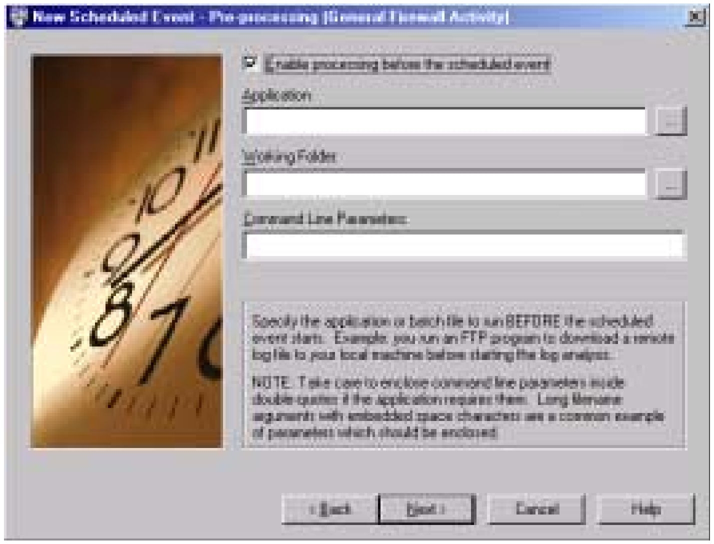
You can save the report locally, transfer it via FTP, or send it as an email attachment. See “Specifying a Distribution Method” on page 252 for details.

10. Use the **Report Range** dropdown list to select the range of time to be covered by the report. See “Report range definitions” on page 240 for more information.

Note
Make sure that the range you specify corresponds to existing dates in the log file.

---

11. Click **Next** and the Pre-Processing dialog box opens.



☑ Enable processing before the scheduled event

Specify the application or batch file to run BEFORE the scheduled event starts. Example: you run an FTP program to download a remote log file to your local machine before starting the log analysis.

NOTE: Take care to enclose command line parameters inside double quotes if the application requires them. Long filename arguments with embedded space characters are a common example of parameters which should be enclosed.

Set up Pre-Processing

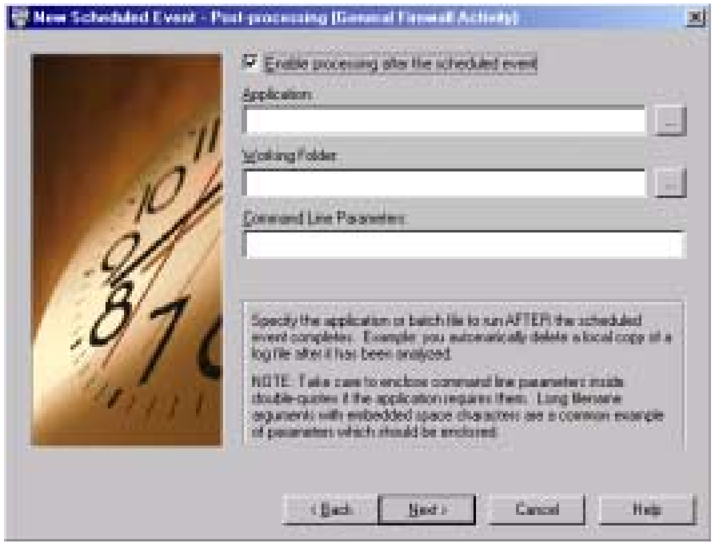
12. To run an application or batch file before the scheduled event is processed, select the **Enable processing before the scheduled event** check box.

13. In the **Application** text box, type the path for the application or batch file, or browse to its directory.

14. In the **Working Folder** text box, type the path for the directory where the application should run, or browse to its directory.

15. If the program requires any command-line parameters, type them in the **Command-line parameters** text box.

16. Click **Next**, and the Post-processing dialog box opens.



New Scheduled Event - Post-processing (General Firewall Activity)

☑ Enable processing after the scheduled event

Specify the application or batch file to run AFTER the scheduled event completes. Example: you automatically delete a local copy of a log file after it has been analyzed.

NOTE: Take care to enclose command line parameters inside double-quotes if the application requires them. Long filename arguments with embedded space characters are a common example of parameters which should be enclosed.

Set up Post-Processing

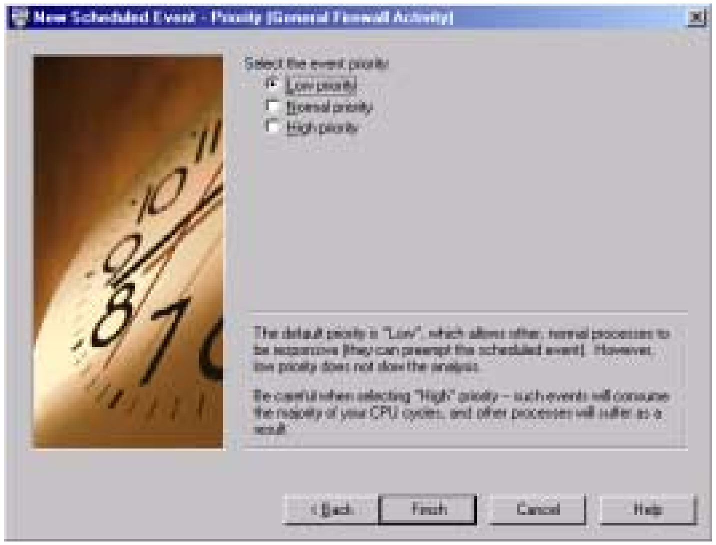
17. To run an application or batch file after the scheduled event is processed, select the **Enable processing after the scheduled event** check box.

18. In the **Application** text box, type the path for the application or batch file, or browse to its directory.

19. In the **Working Folder** text box, type the path for the directory where the application should run, or browse to its directory.

20. If the program requires any command-line parameters, type them in the **Command-line parameters** text box.

21. Click **Next**, and the Priority dialog box opens.



New Scheduled Event - Priority [General Firewall Activity]

Select the event priority:

● Low priority

○ Normal priority

○ High priority

The default priority is "Low", which allows other, normal processes to be responsive (they can preempt the scheduled event). However, low priority does not slow the analysis.

Be careful when selecting "High" priority -- such events will consume the majority of your CPU cycles, and other processes will suffer as a result.

Set the Processing Priority

22. Select the processing priority for this profile.

   – **Low priority** should be used for real-time events—those that are designed to run in the background because they are updated frequently.

   – **Normal priority** should be used for most profiles. This is the default setting.

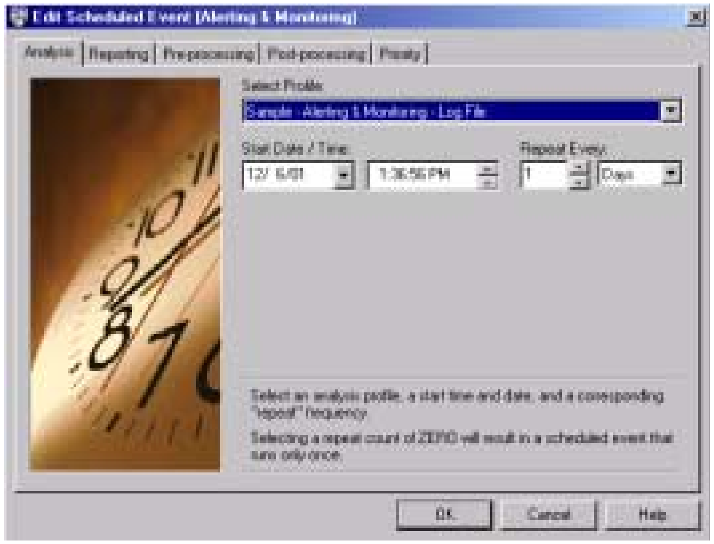
   – **High priority** should be used for critical reports only.

23. Click **Finish** to save the event and return to the Scheduler Main window.

Editing a Scheduled Event

To edit a scheduled event:

1. On the Main Console, click **Scheduler**.
2. When the Scheduler window appears, select the **Scheduled Events** tab.
3. Select the scheduled event that you want to edit, and click **Edit**. The Edit Scheduled Event window opens.



Select Profile: Sample - Alerting & Monitoring - Log File

Start Date / Time: 12/ 6/01 1:36:56 PM

Repeat Every: 1 Days

Select an analysis profile, a start time and date, and a corresponding "repeat" frequency.

Selecting a repeat count of ZERO will result in a scheduled event that runs only once.

These tabs in this window match the dialog box used when adding a new scheduled event.

– The **Analysis** tab lets you modify the profile name and schedule for running the profile.

– The **Reporting** tab lets you modify settings used when generating the report.

– The **Pre-Processing** tab lets you modify the application or batch file run before the event is processed.

- The **Post-Processing** tab lets you modify the application or batch file run after the event is processed.
- The **Priority** tab lets you modify the profile's processing priority.

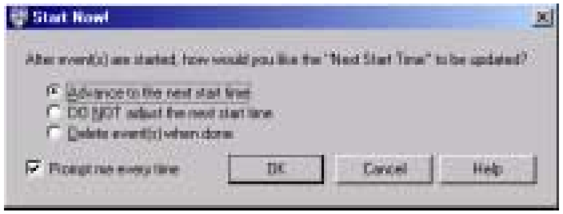
4. When you have made all necessary changes, click **OK** to save the event and return to the Scheduler window.

Running a Scheduled Event on Demand

Firewall Suite lets you run an event without waiting for the next scheduled time. For example, if you have scheduled a report to be generated every Monday morning, you can preview the report on Friday afternoon with the information to date.

To run a scheduled event on demand:

1. On the Main Console, click **Scheduler**.
2. When the Scheduler window appears, select the **Scheduled Events** tab.
3. Select the event that you want to run, then click **Start Now**. The Start Now dialog box appears.



After event(s) are started, how would you like the "Next Start Time" to be updated?

● Advance to the next start time
○ DO NOT adjust the next start time
○ Delete event(s) when done

☑ Prompt me every time

4. Select one of the following options:

   – **Advance to the next start time**. Leave this option selected if you want a scheduled event to run immediately *instead* of at the next scheduled time.

   – **DO NOT adjust the next start time**. Select this option to run an event immediately *and* at the next scheduled time.

   – **Delete event(s) when done**. Select this option to run an event once and then delete it.

5. If you prefer not to be prompted when this event is run, clear the **Prompt me every time** check box.

6. Click **OK.** The event is put in the queue to be processed. The Status column on the Scheduler window now shows the time left before processing.

Stopping an Event from Processing

At installation, the Scheduler is configured to stop processing when you exit the application using **Exit and Unload**. Scheduled events (except for on-demand events) will resume when you restart Firewall Suite.

While a scheduled event is running, you cannot disable it. You can “kill” it, however. Unless subsequently disabled, a killed event will resume at its next scheduled date and time.

To kill a scheduled event:

1. On the Main Console, click **Scheduler**.
2. When the Scheduler window appears, select the **Scheduled Events** tab.
3. Select the event that you want to stop.
4. Right-click and select **Kill** from the menu that appears. The processing for the selected event stops.

Specifying a Distribution Method

Firewall Suite lets you save reports locally, transfer them using FTP, or send them as email attachements.

To save a report locally:

1. On the Main Console, click **Scheduler**.
2. When the Scheduler window appears, select the **Scheduled Events** tab.
3. Select a profile and click **Edit**. The Edit Scheduled Event dialog box appears.
4. Select the **Reporting** tab.
5. Select **file:///** from the **Save As/Mail To** dropdown list.
6. In the text box, type the file path where you want to save the report, or click **Browse** to navigate to the location.
7. Click **OK**.

To transfer the report using FTP:

1. On the Main Console, click **Scheduler**.
2. When the Scheduler window appears, select the **Scheduled Events** tab.
3. Select a profile and click **Edit**. The Edit Scheduled Event dialog box appears.
4. Select the **Reporting** tab.
5. Select **ftp://** from the **Save As/Mail To** dropdown list.
6. In the text box, type the complete path from the root of the FTP server. If you are required to authenticate to access the server, enter the user name and password to use.
7. Click **OK**.

To send the report via email:

1. On the Main Console, click **Scheduler**.
2. When the Scheduler window appears, select the **Scheduled Events** tab.
3. Select a profile and click **Edit**. The Edit Scheduled Event dialog box appears.
4. Select the **Reporting** tab.
5. Select **mailto:** from the **Save As/Mail To** dropdown list.
6. To save a copy of the report locally, type the file path in the **Save To** text box.
7. In the **eMail address** text box, type the email address where the report should be sent.

   Tip
   To send the report to many people, create an alias rather than typing several email addresses.

8. Click **OK**.

Date Macros

Firewall Suite provides built-in macros that you can use to define file or directory names that represent the current date. If the log file name for 30 December, 1999 looks like this:

```
30121999.log
```

If you want to schedule the previous day’s activity, the Log File URL path for the profile would look like this:

```
c:\logfiles\%date-1%%dd%%mm%%yyyy%.log
```

The following table shows the content returned by date macros

Macro	Dates Returned
`%dd%`	Day
`%mm%`	2-digit month
`%Mon%`	Abbreviated month This macro is case sensitive: %Mon% returns Jan, mon returns jan, MON returns JAN
`%yy%`	2-digit year
`%yyyy%`	4-digit year
`%date-n%`	Subtracts *n* days from the current system date
`%date+n%`	Adds *n* days to current system date
`%mm-n%`	Subtracts *n* months from current month
`%mm+n%`	Adds *n* months to current month
`%yy-n%`	Subtracts *n* years from current year
`%yy+n%`	Adds *n* years to current year
`%yyyy-n%`	Subtracts *n* years from current year
`%yyyy+n%`	Adds *n* years to current year
`%dy%`	Day of the year, 001–366
`%wy%`	Week of the year, 00–53
`%dw%`	Day of the week, 0–6
`%wm%`	Week of the month, 0–5

Managing Scheduled Events

Scheduled events may be managed through the Scheduled Events windows available through the three Scheduler tabs:

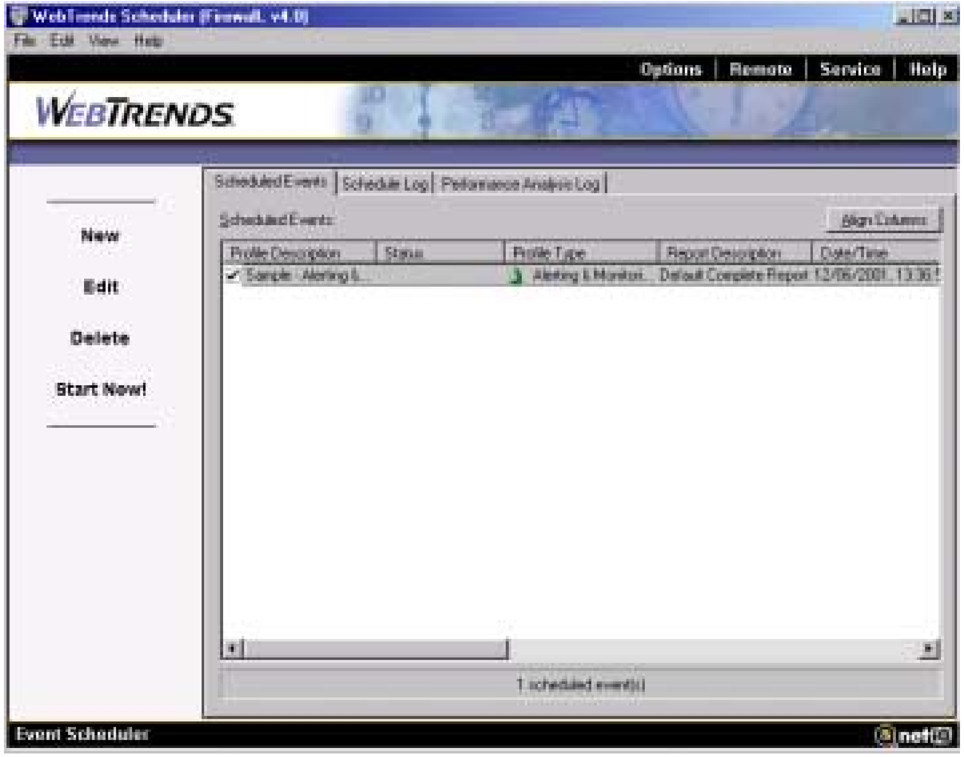
- Scheduled Events tab
- Schedule Log
- Performance Analysis Log

Once events have been scheduled, the Scheduler is minimized to an icon in your computer's system tray (located in the lower, right-hand corner of the screen). To view the Scheduler window, double-click the icon .

Note
If **Hide** is selected in any of the Scheduler tabs, the Scheduler icon appears on the system task bar.

Scheduled Events Tab Elements

Elements specific to the Scheduled Events tab include the Tasks area, the Scheduled Events list, and the Scheduled Events shortcut menu.


WebTrends Scheduler (Firewall, v4.0)
File Edit View Help
Options | Remote | Service | Help
WEBTRENDS
New
Edit
Delete
Start Now!
Scheduled Events | Schedule Log | Performance Analysis Log
Scheduled Events:
Align Columns
Event Scheduler
net

Profile Description	Status	Profile Type	Report Description	Date/Time
✓ Sample - Alerting &...		Alerting & Monitori...	Default Complete Report	12/06/2001, 13:36

1 scheduled event(s)

Tasks Area

The Tasks area is located on the left side of the Scheduler Main window and varies according to the selected tab. You can perform the following activities using the Tasks area of the Scheduled Events tab:

- **New** lets you add a new scheduled event for a specific profile type.
- **Edit** lets you edit a selected scheduled event.
- **Delete** lets you delete a selected scheduled event from the Scheduled Events list.
- **Start Now** lets you process the selected scheduled event immediately.

Scheduled Events List

The Scheduled Events list displays information for each of the events currently scheduled. The following fields are shown for each list entry:

- **Profile Description** displays the profile used for this event.
- **Status** shows the number of seconds until the analysis begins are displayed. When a profile is next in line for analysis, this column displays “Next.” When the analysis begins, the status changes to “Running.”
- **Profile Type** specifies the type of profile analyzed.
- **Report Description** displays the memorized report name for this event.
- **Date/Time** shows when the profile will be analyzed next. If the profile was scheduled to run once (the **Repeat Every** text box is set to 0), this field displays the date and time the event was scheduled to run. If the profile was scheduled to run repeatedly, this field displays the date and time of the next analysis.
- **Event Type** displays Scheduled Event, On-demand Event or Real-Time Analysis Event.
- **Repeat Every** specifies the interval between each analysis.

- **Save As Path** varies according to the selected distribution method:
  - If the report is to be saved locally, this field specifies the directory for the report.
  - If the report is transferred using FTP, this field specifies the path to the FTP server.
  - If the report is sent by email, this field specifies the recipients.
- **Schedule Filename** specifies the file name and location for the scheduled event file. This file contains all the settings for the event.

Scheduler Status

The lowest portion of the Scheduler window displays the total number of scheduled events.

Scheduled Events Shortcut Menu

Right-clicking anywhere in the Scheduled Events window opens a shortcut menu containing these commands:

- **New** starts the New Scheduled Event wizard, which allows you to create a scheduled event.
- **Edit** opens the Edit Scheduled Event dialog box so that you can modify the selected event.
- **Copy** copies the selected scheduled event and allows you to modify the copy in the Edit Scheduled Event dialog box.
- **Start Now!** kicks off the selected scheduled event immediately.
- **Delete** lets you delete the selected event.
- **Kill** allows you to kill processing for the selected event once it has begun.
- **Details** opens the Scheduled Events Details window, which displays profile, report, event, and file information about the selected event.

- **Set Priority** opens the Set Priority Level dialog box, in which you choose the processing priority for this event.
- **Update all security checksums**
- **Show Scheduled Events for all profile types** shows all scheduled events for all profile types.
- **Show Scheduled Events for only one profile type** allows you to display the scheduled events for a single profile type.
- **Align Columns** adjusts column widths so that the contents of every column is completely visible.
- **Select Columns** hides or shows a Scheduled Event detail column. Click to clear the Available Column check box next to the column you want to hide. By default all the Available Column boxes are checked.
- **Print** prints the Scheduled Events list.
- **Select All** selects all the items in the list
- **De-select All** deselects all selected items in the list.

You can select multiple events by holding the `Ctrl` key and selecting each event in turn. For example, you can add, edit, or delete several events at once by selecting them, right-clicking, and selecting the appropriate command.

Using the Scheduled Events Tab

The **Scheduled Events** tab lists all scheduled events.

To disable or enable an event:

Select or clear the check box next to the event name. Disabling an event does not stop the analysis once it has begun. See “Stopping an Event from Processing” on page 251 for instruction on “killing” an event while it is being processed.

To access the Scheduled Event Command menu:

Move the cursor to anywhere in the Scheduled Events window, then right-click to open a shortcut menu.

To access the command menu for a particular event:

Select an event in the Scheduled Events window and right-click to open a shortcut menu.

Managing the Scheduled Events List

You can sort the events in the Scheduled Events list and align the columns in the list to view the information optimally.

To sort the events by column type:

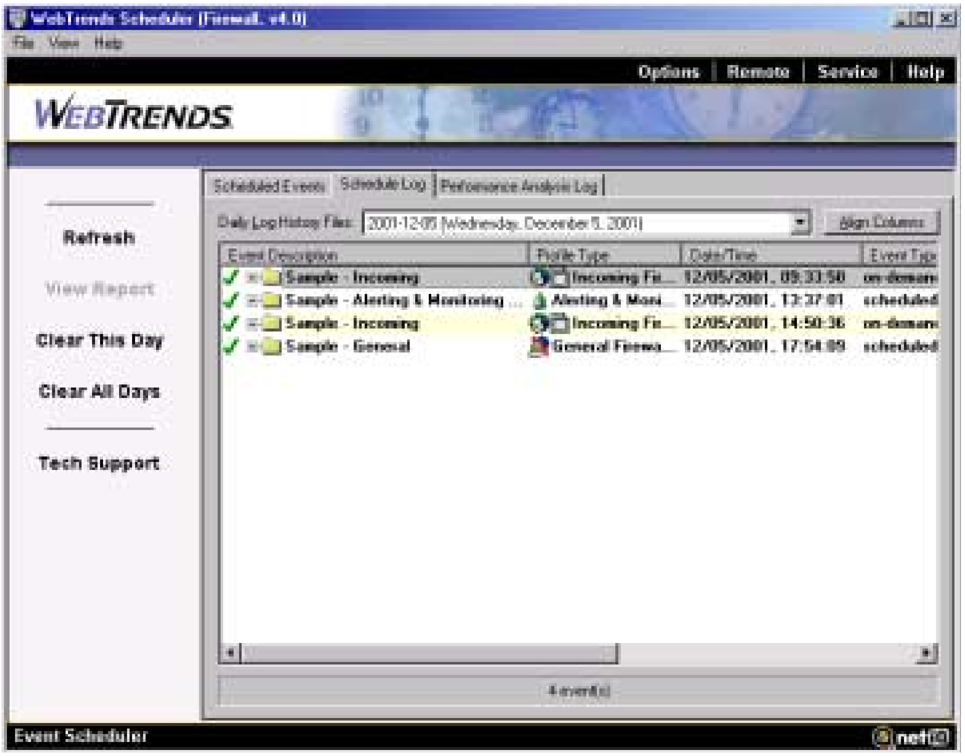
Select the desired column heading. The list is sorted on the basis of that column.

To change column alignment and view long entries:

Hold the cursor to the right of the column heading you wish to expand until the cursor changes into a double arrow. Manually adjust column width by clicking and dragging the right edge of the column heading.

Schedule Log Tab Elements

The **Schedule Log** tab provides a history of all scheduled events for a selected date, including details about their status. Events are listed in the order they were scheduled.



Daily Log History Files: 2001-12-05 (Wednesday, December 5, 2001)

Event Description	Profile Type	Date/Time	Event Typ
✓ Sample - Incoming	Incoming Fi...	12/05/2001, 09:33:50	on-deman
✓ Sample - Alerting & Monitoring ...	Alerting & Moni...	12/05/2001, 13:37:01	scheduled
✓ Sample - Incoming	Incoming Fi...	12/05/2001, 14:50:36	on-deman
✓ Sample - General	General Firewa...	12/05/2001, 17:54:09	scheduled

Use the + ahead of each item to expand and collapse items in the Event Description tree.

Tasks Area

The Tasks area is located on the left side of the Scheduler Main window and varies according to the selected tab. You can perform the following activities using the Tasks area of the Schedule Log tab:

- **Refresh** lets you update the scheduled event list.
- **View Report** lets you view the report associated with the selected scheduled event.
- **Clear This Day** clears out the log history data for the currently selected day (selected in the **Daily Log History Files** dropdown list).
- **Clear All Days** clears out all the log history data.
- **Tech Support** opens the eMail Diagnostic Data dialog box, which you can use to send diagnostic information to NetIQ Technical Support.

Schedule Log List

The following information is shown for each list entry of the Schedule Log tab:

- **Event Description** shows the name of the profile.
- **Profile Type** displays the type of profile.
- **Date/Time** displays the date and time the event took place.
- **Event Type** displays Scheduled Event, On-demand Event, or Real-Time Analysis Event.
- **Additional Messages** displays any information about the event, such as problems encountered.
- **Next Event** displays the time the next event is scheduled to take place.
- **Repeat Every** specifies how often the event is scheduled to take place.

Schedule Log Shortcut Menu

Right-clicking anywhere in the **Schedule Log** tab opens a shortcut menu containing these commands:

- **View Report** lets you view the report associated with the selected scheduled event.
- **Show all events** shows every event generated by the log, regardless of whether or not the event was successful.
- **Show error events** only displays only the error events generated.
- **Show All Profile Types** displays the log history information for all profile types.
- **Show One Profile Type Only** displays the log history information for a profile type you select.
- **Clear This Day** clears out the log history data for the currently selected day (selected in the Daily Log History Files dropdown list).
- **Clear All Days** clears out all the log history data.
- **Align Columns** adjusts column widths so that the contents of every column is completely visible.
- **Select Columns** hides or shows a Schedule Log Available Column. Click to clear the Available Column check box next to the column you want to hide. By default all the Available Column boxes are checked.
- **Print** prints the Schedule Log list.
- **Collapse** all collapses the listed items to just show the top-level folders.
- **Expand all** expands the list to show all folders and sub-items in folders.

Using the Schedule Log

When you select the **Schedule Log** tab, the schedule log for the current day is displayed.

To select history files:

Use the **Daily Log History Files** dropdown list to select the date of Schedule Log History files.

To sort the events by column type:

Select the desired column heading. The list is reorganized on the basis of that column.

To change column alignment and view long entries:

Hold the cursor to the right of the column heading you wish to expand until the cursor changes into a double arrow. Manually adjust column width by clicking and dragging the right edge of the column heading.

To clear the Schedule Log:

Remove *all schedule logs* by clicking **Clear All Days**, or click **Clear This Day** to remove the schedule logs for the day selected in the **Daily Log History Files** dropdown list.

Note
A schedule log is created for each day. By default, two weeks worth of schedule logs (14 logs) are maintained.

To refresh the Schedule Log:

Click **Refresh** in the Tasks area. By default, it is updated every two minutes. You can change the refresh rate in the Options tab.

To view a report for the selected event:

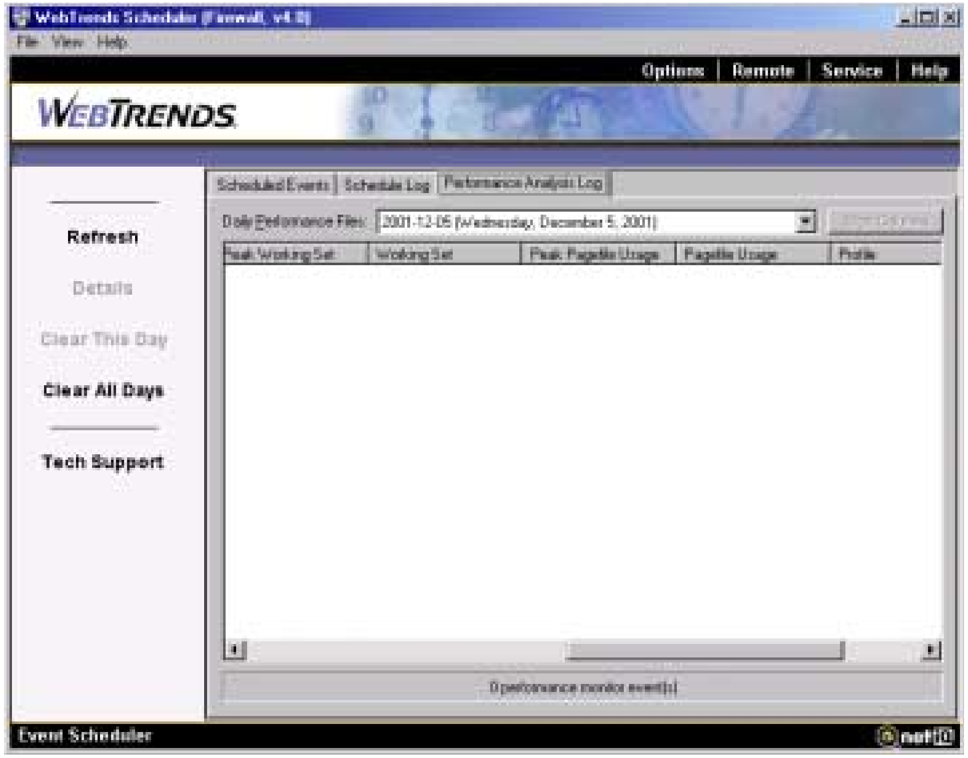
Click **View Report** in the Tasks area to display the report generated by the selected event

Performance Analysis Log Tab Elements

The **Performance Analysis Log** tab provides a breakdown of your system's performance by event, including processing time, memory usage, and the other processes.

The **Performance Analysis Log** tab is useful for troubleshooting. If an event takes longer than usual to run, you can determine which other processes were running and how much memory was available. If your computer consistently runs out of memory, consider increasing the physical memory.

To view computer details for a performance record, select it, right-click, and select **Details**. This feature is available only on systems running Microsoft Windows NT 4.0. You must configure the Performance settings in the Scheduler **Options** tab to get this information.



WebTrends Scheduler (Firewall, v4.0)

Daily Performance Files: 2001-12-05 (Wednesday, December 5, 2001)

0 performance monitor event(s)

Tasks Area

The Tasks area is located on the left side of the Scheduler Main window and varies according to the selected tab. You can perform the following activities using the Tasks area of the Schedule Log tab:

- **Refresh** updates the **Performance** tab with any new activity. By default, it is updated every five minutes. You can change the refresh rate in the Options tab under Performance analysis, How often
- **Details** shows information about the selected performance analysis log item.
- **Clear This Day** deletes the performance file for the selected day.
- **Clear All Days** deletes all performance files.
- **Tech Support** opens the eMail Diagnostic Data dialog box, which you can use to describe your technical support issue in an email message to NetIQ Technical Support.

Performance Analysis Log List

The following information is shown for each list entry:

- **Application Name/Cartridge** displays the name of the program or cartridge.
- **Total Execution Time** specifies the length of time since the process was started, although not necessarily the amount of time it took to run. For example, some applications start when you log on, but only run when called.
- **Time in Kernel Mode** shows the length of time that the process was given priority processing time in kernel mode. This gives you a good indication of actual processing time.
- **Time in User Mode** shows the length of time that the process was given processing time in user mode, a slightly lower priority than kernel mode.

- **Page Faults** shows the number of page faults that occurred during processing. Page faults occur when the process requires more physical memory than is available.
- **Peak Working Set (MB)** specifies the most memory used by the application or event. Pay close attention if the peak working memory exceeds the physical memory because this is when swapping occurs. You may need more physical memory if your computer runs out of memory often.
- **Working Set (MB)** specifies the memory used by this application or event when the performance was recorded.
- **Peak Pagefile Usage** specifies the most memory that was swapped to disk for this application or event. If it requires more memory than was available, it must be swapped to the paging file.
- **Pagefile Usage** specifies the memory that was being swapped for the application or event when the performance was recorded.
- **Profile** displays the profile used.
- **Report** displays the memorized report name.

Performance Analysis Log Shortcut Menu

- **Details** shows information about the selected performance analysis log item.
- **Clear This Day** deletes the performance file for the selected day.
- **Clear All Days** deletes all performance files.
- **Align Columns** adjusts column widths so that the contents of every column is completely visible.
- **Select Columns** hides or shows an Available Column of the Performance Analysis Log. Click to clear the Available Column check box next to the column you want to hide. By default all the Available Column boxes are checked.
- **Print** prints the Performance Analysis Log list.

- **Collapse all** collapses the listed items to just show the top-level folders.
- **Expand** all expands the list to show all folders and sub-items in folders.

Using the Performance Analysis Log Tab

When you select the **Performance Analysis Log** tab, the current day is displayed.

To select performance files:

Use the dropdown list to select the date of performance files.

To sort the events by column type:

Select the desired column heading. The list is reorganized on the basis of that column.

To change column alignment and view long entries:

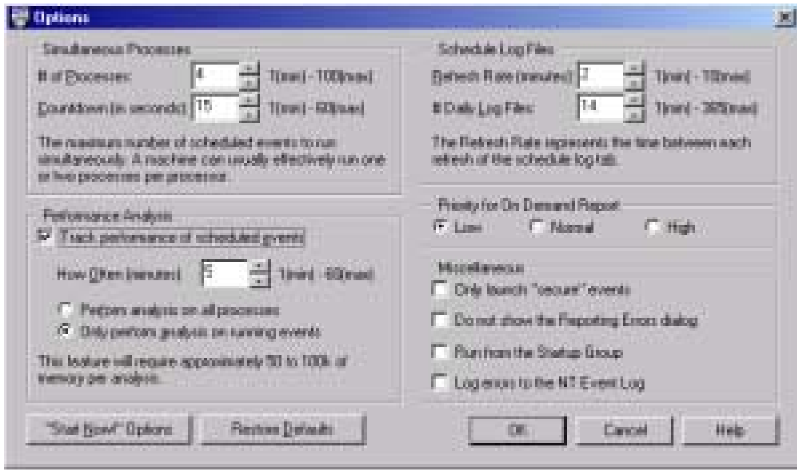
Hold the cursor to the right of the column heading you wish to expand until the cursor changes into a double arrow. Manually adjust column width by clicking and dragging the right edge of the column heading.

Using the Options Tab

The **Options** tab provides settings that affect how scheduled events are processed.The following areas are available:

- Simultaneous Processes
- Schedule Log Files
- Performance Analysis

- Priority for On Demand Report
- Miscellaneous



Options

Simultaneous Processes

# of Processes: 4 1(min) - 100(max)

Countdown (in seconds): 15 1(min) - 60(max)

The maximum number of scheduled events to run simultaneously. A machine can usually effectively run one or two processes per processor.

Performance Analysis

☑ Track performance of scheduled events

How Often (minutes): 5 1(min) - 60(max)

○ Perform analysis on all processes

● Only perform analysis on running events

This feature will require approximately 50 to 100k of memory per analysis.

Schedule Log Files

Refresh Rate (minutes): 2 1(min) - 10(max)

Daily Log Files: 14 1(min) - 365(max)

The Refresh Rate represents the time between each refresh of the schedule log tab.

Priority for On Demand Report

● Low ○ Normal ○ High

Miscellaneous

□ Only launch "secure" events

□ Do not show the Reporting Errors dialog

□ Run from the Startup Group

□ Log errors to the NT Event Log

Simultaneous Processes

- **# of Processes** lets you specify the maximum number of events that you wish to run at the same time. The default is 4.

  Typically, you can run two scheduled events for each processor on the computer. If you have more than two processors operating on your computer, you may want to increase this setting.

- **Countdown (in seconds)** lets you specify the number of seconds to be visually counted off in the status column before running a scheduled event.

Schedule Log Files

Schedule Log Files lets you specify how often to refresh your log files and lets you specify how many daily log files you want to save.

- **Refresh Rate (minutes)** lets you specify how often the **Schedule Log** tab is updated. At installation, this option is set to two minutes.
- **# Daily Log Files** lets you specify the maximum number of Schedule Log files saved.

  You can save up to a year’s worth of files.One Schedule Log file is created for each day. When the limit specified by this option is reached, the oldest file is deleted and replaced with the Schedule Log for the current day.

Performance Analysis

Performance analysis lets you capture the state of the computer at regular intervals (if you’re running Firewall Suite on Windows NT 4.0 or later).

- **Track performance of scheduled events** enables the Scheduler to track the performance of processes and display a breakdown of the data in the **Performance Analysis Log** tab.
- **How Often (minutes)** lets you specify how frequently, in minutes, a performance snap-shot is taken of the Firewall Suite computer. By default, the Performance dialog box is updated every five minutes, but you can change it to anything from between one and sixty minutes.
  - **Perform Analysis on all processes** monitors system performance for all applications and events. In addition to Firewall Suite scheduled events, all other processes running on your system are recorded.
  - **Only perform analysis on running events** monitors system performance only for events that are running.

Performance for On Demand Report

Lets you specify **Low**, **Normal**, or **High** priority for processing on demand reports relative to other events.

Low (the default setting) ensures that on-demand reports do not interfere with other processes. Use this setting for most, if not all, on-demand reports.

Miscellaneous

- **Only launch "secure" events** launches only schedule event that include an encrypted checksum. All scheduled events that are created through the user interface have this checksum, which ensures the file was created by Firewall Suite and not by someone who has accessed your computer via the Internet or your network.

Note
Do not use this option if you create events through batch file processing.

- **Do not show the reporting errors dialog box** turns off the reporting errors popup.
- **Run from the Startup Group** loads and runs the Scheduler at system startup.
- **Log Errors to the NT Event Log** logs errors the Windows NT event log. This option is available only if you are running Windows NT.

Commands

Performance tab commands are accessed using the following buttons:

- Start Now! Options opens the Start Now! dialog box, in which you can specify:
  - **Advance to the next start time**. Leave this option selected if you want a scheduled event to run immediately *instead* of at the next scheduled time.
  - **DO NOT adjust the next start time**. Select this option to run an event immediately *and* at the next scheduled time.
  - **Delete event(s) when done**. Select this option to run an event once and then delete it.
- **Restore Defaults** restores settings to the original defaults.
- **OK** saves your settings and close the Options dialog box.
- **Cancel** closes the Options dialog box without saving your settings.
- **Help** opens Help for the Scheduler options.

Using the Remote Scheduling Tab

Use the **Remote** option in the Functions area (top right of the Scheduler Main window) to set up the Remote Scheduling Server. With the Remote Scheduling Server, you can access Scheduler features through a browser. For example, you can look at the Schedule Log to monitor Scheduler activity or view reports that have been generated. Or, you can check the details of reports.

Note

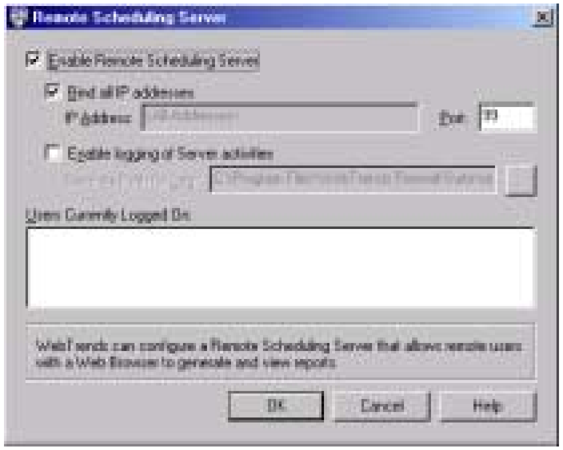
The Scheduler must either be running on its host system or running as a service to access the Remote Scheduling Server.

Setting up the Remote Scheduling Server

Use the Remote Scheduling Server dialog box to specify the location where the Remote Scheduling Server will run.

To set up the Remote Scheduling Server:

1. On the Scheduler Main window, select **Remote**. The Remote Scheduling Server dialog box opens.



Remote Scheduling Server

☑ Enable Remote Scheduling Server

☑ Bind all IP addresses

IP Address: (All Addresses) Port: [illegible]

☐ Enable logging of Server activities

[illegible]: C:\Program Files\WebTrends\Firewall Suite\[illegible]

Users Currently Logged On:

WebTrends can configure a Remote Scheduling Server that allows remote users with a Web Browser to generate and view reports.

2. Select the **Enable Remote Reporting Server** check box.
3. Select the **Bind all IP Addresses** check box if the computer running Firewall Suite has multiple IP addresses, and you want to be able to access the Remote Scheduling Server using any of them.

   For example, the system might be assigned an IP that can only be accessed locally and an IP that can be accessed throughout the network. Rather than explicitly defining the IP, select the **Bind all IP Addresses** check box.

4. If you un-selected **Bind all IP Addresses**, type the IP address in the **IP Address** text box. You will use this if your computer has only one IP address, or if there are more than one IP but you want to access the Remote Scheduling Server with a specific IP.

   Note
   The primary IP address of the computer you are using appears as the default address.

5. Type the Port number in the **Port** text box that the Remote Scheduler will use. The default is 99 which you should be able to use as long as it is not used by another service.
6. Select **Enable logging of Server activities** option to maintain a log file in NCSA format for this remote reporting server. This file is named `remote.log`, and by default is stored in Firewall Suite's *install_dir*`\reports` directory. However, you can browse to and save this file to a new location.
7. Click **OK**.

Note
The logged-on users box displays the names of all currently logged-on users.

Configuring Your User Account for Remote Scheduling

In order to run the Remote Scheduler Server, the account that you use to run Firewall Suite must have the "act as part of the operating system" privilege.

To define the "Act as part of the operating system" privilege:

1. From the Start menu and select **Programs > Administrative Tools > User Manager**. The User Manager window opens.
2. Select yourself in the Username list.

3. From the Policies menu, select **User Rights**. The User Policy window opens.

4. Select the **Show Advanced User Rights** check box at the bottom left of the dialog box.

5. In the Right dropdown list, select **Act as Part of Operating System**.

6. Click **Add** and the Add Users and Groups dialog box opens.

7. Click **Show Users**.

8. Select your user name from the list of names and click **Add**. Your name appear in the Add Names list.

Accessing the Remote Scheduling Server

To access the Remote Scheduling Server:

1. Open your Web browser.

2. In the Address/URL box, type the IP address for your Firewall Suite host system and the port number that you defined in the **Remote Scheduling Server** dialog box. Use the following syntax:

   ```
   http://IP_address:port_number
   ```

   The Remote Scheduling Server Logon window opens.

3. Type your user name and password, and click **Logon**. The Remote Scheduling Server opens.

Schedule Log

To use the Schedule log:

1. From the Remote Scheduling Server, click **Schedule Log**.
2. Select the day that you want to look at from the dropdown list, and click **View Report**. You can access reports that are saved to the `*install_dir*\reports` directory and those that are saved using a UNC path.
3. After viewing the report, click **Main** to return to the Remote Scheduling Server main window. Without viewing a report, click your browser's **Back** button.

Using the Performance Log

To use the Performance log:

1. From the Remote Scheduling Server, click **Performance Log**.
2. Select the day's log from the **Performance Log History Files** dropdown list.
3. Click your browser's **Back** button to return to the Remote Scheduling Server main window.

Scheduled Events

Creating a scheduled event:

1. Click **New**.
2. Select a profile type (cartridge) from the dropdown list.
3. The Edit Scheduled Event dialog box opens. Select the profile for the scheduled event, and continue with the other boxes in the dialog box. Review "Using the Scheduled Events Tab" on page 259 for details.

Editing a scheduled event:

1. In the Scheduled Events window of the Remote Scheduling Server, select the event to edit.
2. Click **Edit**.
3. The Edit Scheduled Event dialog box opens. Make changes in the dialog box. Review “Using the Scheduled Events Tab” on page 259 for details.

Running Reports

To run reports for a scheduled event remotely

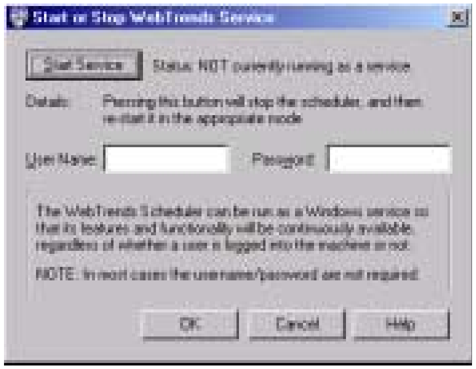
1. In the Scheduled Events window of the Remote Scheduling Server, select the event for the report that you want to run.
2. Click **Start Now** to place the selected event in the queue for priority processing.

The Start or Stop WebTrends Service Dialog Box

You can set up the Scheduler to run as a service. This ensures that scheduled events take place even if the system reboots accidentally.

To activate the service settings:

1. In the Schedule Main window, select **Service** from the Functions area in the upper right corner. The Start or Stop WebTrends Service dialog box opens.
2. Select the **Service** tab. The Start or Stop WebTrends Service dialog box opens.



Start or Stop WebTrends Service

Status: NOT currently running as a service

Details: Pressing this button will stop the scheduler, and then re-start it in the appropriate mode

User Name:

Password:

The WebTrends Scheduler can be run as a Windows service so that its features and functionality will be continuously available regardless of whether a user is logged into the machine or not.

NOTE: In most cases the username/password are not required.

3. By default, the Scheduler service logs on using the System Account. If you want to run the service by impersonating another user, type the user name and password that you want to use. You might do this in order to access log files stored on another system that the system account doesn't have access to.

   If you specify a user account, it must also have advanced privileges. See "Adding Privileges to your Windows User Account" on page 279 for details.

4. Click **Start Service** to start the Scheduler service. When the service starts successfully, a message is displayed in the lower portion of the window.
5. Click **OK** to save your selections, or click **Cancel** to exit the dialog box without saving your changes.

Configuring the Service Startup

In order to run the Scheduler as a service, the Schedule must be allowed to interact with the desktop.

To configure the startup:

1. From the system Start menu, select **Settings > Control Panel**.
2. Double-click **Services**. The Services window opens.
3. Select WebTrends Scheduler from the list, and click **Startup**.
4. Make sure the **Allow the service to Interact with the desktop** check box is selected.

Adding Privileges to your Windows User Account

In order to run the Scheduler as a service, the privileges for the account that you use to run Firewall Suite must allow it to do the following:

- Act as part of the operating system
- Log on as a service
- Log on locally

To add privileges:

1. Click the Start menu on your system.
2. Select **Programs > Administrative Tools > User Manager**. The User Manager window opens.
3. Select yourself in the Username list.
4. From the Policies menu, select **User Rights**. The User Policy window opens.
5. Select the **Show Advanced User Rights** check box at the bottom of the dialog box.

6. In the Right dropdown list, select **Act as Part of Operating System**.
7. Click **Add**. The Add Users and Groups dialog box opens.
8. Click **Show Users**.
9. Select your user name from the list of names, and click **Add**. Your name appears in the Add Names list.
10. In the Right dropdown list, select **Log on Locally**.
11. Click **Add**. The Add Users and Groups dialog box opens.
12. Click **Show Users**.
13. Select your user name from the list of names, and click **Add**. Your name appears in the Add Names list.
14. In the Right dropdown list, select **Log on as a Service**.
15. Click **Add**. The Add Users and Groups dialog box opens.
16. Click **Show Users**.

Select your user name from the list of names, and click **Add**. Your name appears in the Add Names list.

Chapter 8
Monitoring Activity

This chapter contains scenarios showing how you can use WebTrends Firewall Suite to do the following:

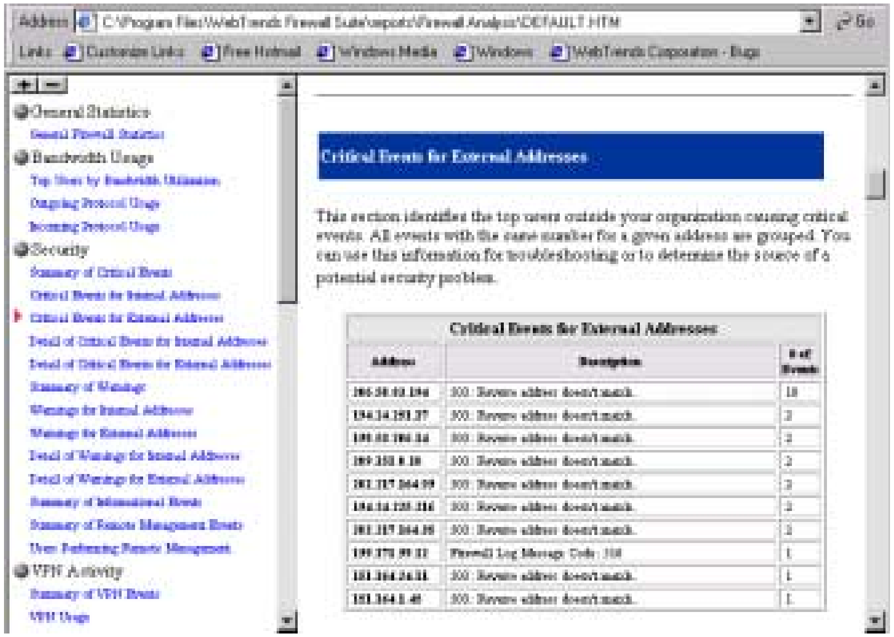
- Monitor Security Events
- Monitor Internet Searches
- Monitor Bandwidth Usage

Monitoring Security Events

In this scenario, we are trying to find the source of *critical events*. A critical event signals that you have potentially suspicious activity occurring on your network. Critical events are defined differently within each firewall. For example, an event is considered critical if it meets the following criteria:

- Gauntlet considers an event critical if it is logged as a “security alert.”
- Check Point considers an event critical if it is logged as “rejected.”
- Raptor considers an event critical if it has an error code of 500 or greater.

In this scenario you've noticed that for the last several days, the Critical Events table has reported a "503: Reverse address doesn't match" critical event being reported 10 times for the same IP address. Such activity may indicate a possible port scan and warrants further investigation.


Address
C:\Program Files\WebTrends Firewall Suite\reports\Firewall Analysis\DEFAULT.HTM
Go
Links
Customize Links
Free Hotmail
Windows Media
Windows
WebTrends Corporation - Bugs
+
−
General Statistics
General Firewall Statistics
Bandwidth Usage
Top Users by Bandwidth Utilization
Outgoing Protocol Usage
Incoming Protocol Usage
Security
Summary of Critical Events
Critical Events for Internal Addresses
Critical Events for External Addresses
Detail of Critical Events for Internal Addresses
Detail of Critical Events for External Addresses
Summary of Warnings
Warnings for Internal Addresses
Warnings for External Addresses
Detail of Warnings for Internal Addresses
Detail of Warnings for External Addresses
Summary of Informational Events
Summary of Remote Management Events
Users Performing Remote Management
VPN Activity
Summary of VPN Events
VPN Usage

Critical Events for External Addresses

This section identifies the top users outside your organization causing critical events. All events with the same number for a given address are grouped. You can use this information for troubleshooting or to determine the source of a potential security problem.

Critical Events for External Addresses

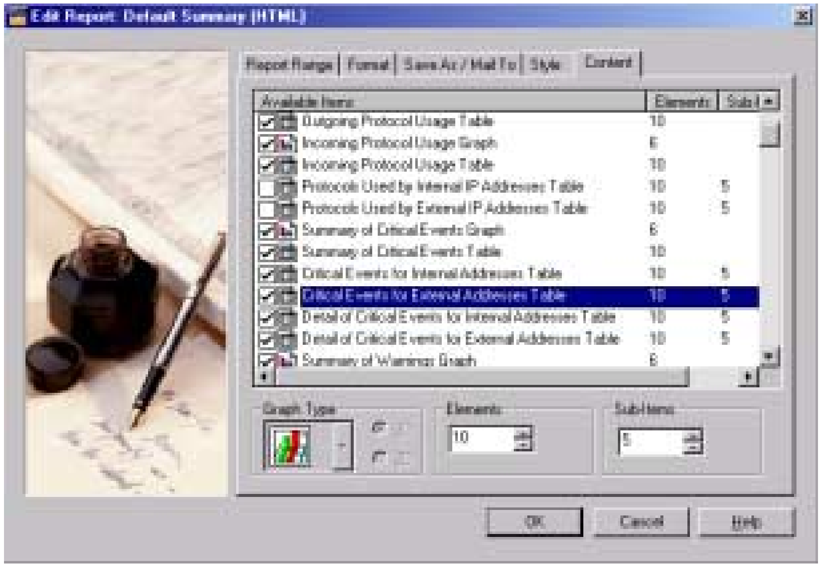
Address	Description	# of Events
205.38.12.194	503: Reverse address doesn't match.	10
134.24.193.27	503: Reverse address doesn't match.	2
195.32.196.24	503: Reverse address doesn't match.	2
209.252.8.10	503: Reverse address doesn't match.	2
161.227.164.59	503: Reverse address doesn't match.	2
194.24.125.216	503: Reverse address doesn't match.	2
161.227.164.95	503: Reverse address doesn't match.	2
199.172.99.22	Firewall Log Message Code: 318	1
151.164.24.21	503: Reverse address doesn't match.	1
151.164.1.45	503: Reverse address doesn't match.	1

You have visions of a disgruntled ex-employee persistently trying to break through your firewall. In order to make sure your firewall is secure, you want want to find out what else this person has been doing.

Finding the IP Addresses that Cause the Most Errors

To find the IP addresses:

1. Create a General Firewall Activity profile. See “Creating a Firewall Profile” on page 48.
2. Create a General Firewall Activity report by clicking **Report**.
3. Select the Default Summary (HTML) report from the list of Available Report Templates.
4. Click **Edit**. The Edit Report dialog box opens.
5. Select the **Content** tab and make sure the **Critical Events for External Addresses** check box is selected. You can also use the Security memorized report which is provided with Firewall Suite.



Available Items	Elements	Sub I
☑ Outgoing Protocol Usage Table	10	
☑ Incoming Protocol Usage Graph	6	
☑ Incoming Protocol Usage Table	10	
☐ Protocols Used by Internal IP Addresses Table	10	5
☐ Protocols Used by External IP Addresses Table	10	5
☑ Summary of Critical Events Graph	6	
☑ Summary of Critical Events Table	10	
☑ Critical Events for Internal Addresses Table	10	5
☑ Critical Events for External Addresses Table	10	5
☑ Detail of Critical Events for Internal Addresses Table	10	5
☑ Detail of Critical Events for External Addresses Table	10	5
☑ Summary of Warnings Graph	6	

Elements: 10

Sub-Items: 5

6. Once you’ve generated the report, determine the IP address that is causing the most errors.

Focusing on an IP Address

To look at a specific IP address

1. Create a new General Firewall Activity profile to determine the activity for this IP address. Delete the Include Everything filter, and create a new one based only upon the external address you want to report on. See “External user address (general)” on page 191 for details on how to do this.

Note
You can also create an Incoming Web Activity profile. This profile provides more in-depth information on any HTTP activity this IP address is generating.

2. Create a report on the profile you just created. Any activity recorded for this IP address is included in the report.

Note
Only tables and graphs for which there is data appear in the report.

Monitoring Internet Searches

The type of Internet content retrieved in the work environment is a cause of concern for many companies. Inappropriate content can cause harassment lawsuits, lost productivity, and damage to the organization. Your Firewall logs the keywords used for Internet searches. You can create a list of words that you want to filter for and produce a report that displays the top users of these keywords, which keywords they use, and the sites they visited. When combined with a User (by IP) filter, you can generate reports on the nature of the search being conducted by an individual.

To monitor Internet searches:

1. Create an Outgoing Web Activity profile to track Internet searches. See “Firewall Profiles” on page 27 for details.
2. Edit the Search Engine Keywords filter to contain only the keywords you want to search for. See “Filtering for Focused Reports” on page 173 for details.
3. Create a report based on the profile you’ve just created. It reports the users who entered the keywords and the sites they visited.
4. Create individual profiles for each IP address returned in the report results. Edit the Include Everything filter, and type the IP address in the **Users (by IP)** text box.
5. Create reports based on the Users by IP profile. These reports display all the activity for an IP address.

Note
If your organization requires users to log on to the firewall with a user name and password, you can create a similar report based on authenticated user data.

Monitoring Bandwidth Usage

One simple way to assess productivity in your organization is through Firewall Suite bandwidth tables and graphs. Bandwidth measures the amount of data transferred over the Internet. Firewall Suite breaks down bandwidth by protocol, telling you the type of activity conducted. Firewall Suite automatically looks for protocol activity and graphs it, but you can also report on a specific protocol or track an individual user’s bandwidth by protocol.

In this scenario, we determine which protocol uses the most bandwidth and which uses this protocol most often. We also determine what other activity this individual is generating.

To create a report showing bandwidth usage by protocol:

1. Create a General Firewall Activity profile using the steps described in "Creating a Firewall Profile" on page 48.

2. Create a General Firewall Activity report making sure the Bandwidth by Protocol element is selected in the **Content** tab. See "Modifying report content" on page 239 for details.

3. Once you've generated the report, determine the protocol that uses the most bandwidth.

Identifying High-Bandwidth Users

To create a report showing bandwidth usage by protocol and individual:

1. Create a new profile to find the individual who used the most bandwidth for this protocol. Edit the Include Everything filter to include only the Type of Traffic. In the **Type of Traffic** tab, select the protocol that uses the most bandwidth. See "Working with Filters" on page 175 for details.

2. Create a report based on the new profile. Check the Top Users by Bandwidth section to determine the individual who used the most bandwidth for this protocol.

To create a report showing an individual's activity:

1. Create a new profile to examine the activity of the top user of the protocol. Edit the Include filter to include just the Internal Address. This is the only filter element that you want to use because you want to assess all the user's activity, not just for a particular protocol.

2. Create a report based on this profile. This report breaks down the individual's activity.

Chapter 9
Options

This chapter explains how to modify your configuration settings to better suit your environment. Options are divided into three main areas:

- Main
- General Firewall Activity
- Alerting & Monitoring

The various settings you can configure within each main area are discussed in the following sections.

Main Options

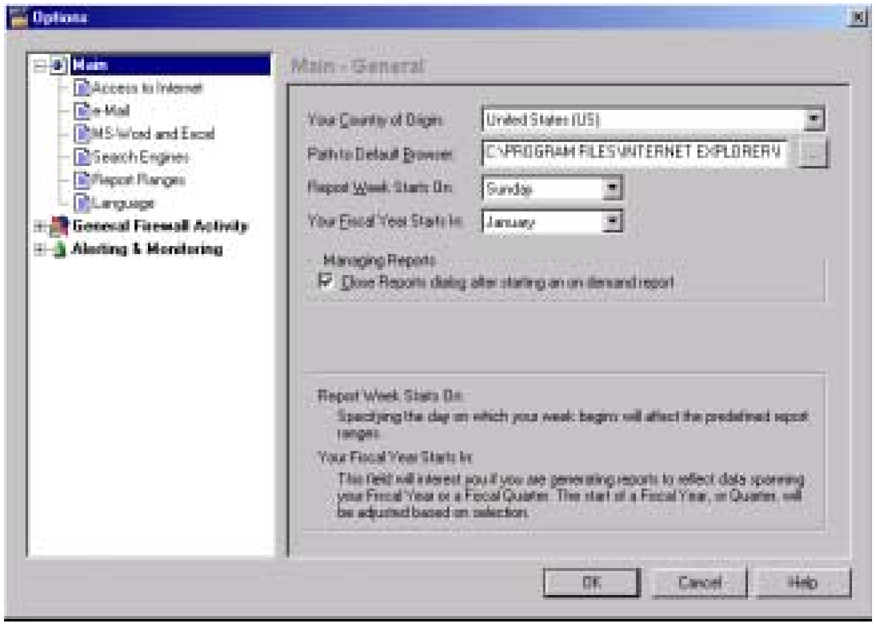
The Main Options settings apply to the entire program. These let you define:

- Your country of origin.
- The file path to your Web browser used for viewing HTML reports.
- The day that the report week starts on.
- The month in which your fiscal year begins.

- How you will access your network resources, including your firewall log file.
- Settings to send reports by email.
- Settings that allow your firewall reporting solution to generate reports in Microsoft Word and Excel.
- A list of search engines that you want your firewall reporting solution to identify in firewall log files.
- Report ranges that specify the time period a report can cover.
- Settings for accessing files through a proxy server.
- The language used in reports.

Main - General Dialog Box

The topics in this section cover the settings you may configure in the Main - General dialog box.



Your Country of Origin: United States (US)

Path to Default Browser: C:\PROGRAM FILES\INTERNET EXPLORER\

Report Week Starts On: Sunday

Your Fiscal Year Starts In: January

Managing Reports

☑ Close Reports dialog after starting an on demand report

Report Week Starts On:

Specifying the day on which your week begins will affect the predefined report ranges.

Your Fiscal Year Starts In:

This field will interest you if you are generating reports to reflect data spanning your Fiscal Year or a Fiscal Quarter. The start of a Fiscal Year, or Quarter, will be adjusted based on selection.

Identifying the Country of Origin

You have the option to identify the “source” country for your reports—what is considered “domestic.” For example, if you are in Italy and want Italian visitors to your site to be considered domestic and all others to be considered international, you should select Italy as your country of origin.

To specify the country of origin:

1. On the Main Console, click **Options** in the Functions area. The Options window opens.
2. In the left-side navigation area, click **Main**. The right side of the window opens to the Main - General dialog box.
3. In the **Your Country of Origin** dropdown list, select the country you wish to be considered domestic.
4. Click **OK** to save your selection.

Selecting a Web Browser

By default, your firewall reporting solution launches your default system browser, such as Microsoft Explorer or Netscape, for viewing your HTML reports. You can specify a different browser by modifying the default browser path that your firewall reporting solution uses.

To specify a different browser:

1. On the Main Console, click **Options** in the Functions area. The Options window opens.
2. In the left-side navigation area, click **Main**. The right side of the window opens to the Main - General dialog box.
3. In the **Path to Default Browser** text box, type the path to the browser that you wish to use, or click □ to search for a specific location.
4. Click **OK** to save your selection.

Defining the Week

Select the day you want to start your week. The day you choose will define the first day of the week in your reports. For example, if you choose Sunday as the day you want to start your week any report you create with a date range of **Last Week** will include information from Sunday through Saturday.

To change the start day for the week:

1. On the Main Console, click **Options** in the Functions area. The Options window opens.
2. In the left-side navigation area, click **Main**. The right side of the window opens to the Main - General dialog box.
3. In the **Report Week Starts On** dropdown list, select the day you wish to be considered as the first day of the week for your reports.
4. Click **OK** to save your selection.

Defining the Month

Select the month on which your fiscal year starts. The month you choose will determine how fiscal data is displayed in your reports. For example, if you choose January as the month you want your fiscal year to start, any report you create with the date range **Current Fiscal Year** will include information from January through the current date.

To change the start month for the fiscal year:

1. On the Main Console, click **Options** in the Functions area. The Options window opens.
2. In the left-side navigation area, click **Main**. The right side of the window opens to the Main - General dialog box.
3. In the **Your Fiscal Year Starts In** dropdown list, select the month you wish your reports to consider as the first month in the fiscal year when generating reports based on the fiscal year.
4. Click **OK** to save your selection.

Managing Reports

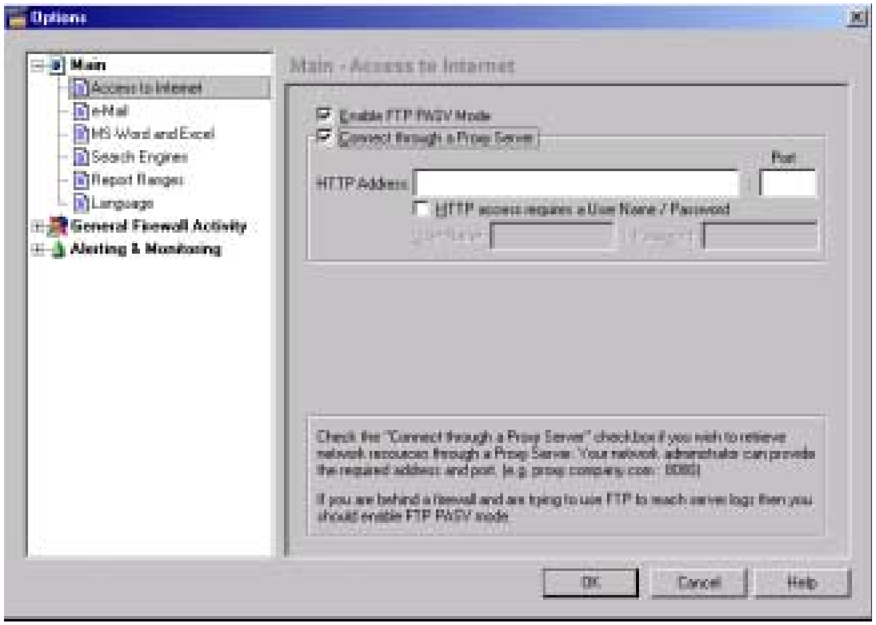
You may wish to close the Reports dialog box once you begin generating an on-demand report.

To close the Reports dialog box automatically when generating on-demand reports:

1. On the Main Console, click **Options** in the Functions area. The Options window opens.
2. In the left-side navigation area, click **Main**. The right side of the window opens to the Main - General dialog box.
3. Select the **Managing Reports** check box.
4. Click **OK** to save your selection.

Access to Internet Dialog Box

The topics in this section cover the settings you may configure in the Main - Access to Internet dialog box.



☑ Enable FTP PASV Mode

☑ Connect through a Proxy Server

HTTP Address:

☐ HTTP access requires a User Name / Password

Check the "Connect through a Proxy Server" checkbox if you wish to retrieve network resources through a Proxy Server. Your network administrator can provide the required address and port. (e.g. proxy.company.com : 8080)

If you are behind a firewall and are trying to use FTP to reach server logs then you should enable FTP PASV mode.

Enabling FTP PASV Mode

If you are behind a firewall and are using FTP to access your firewall log files, then you must enable FTP PASV mode.

To enable FTP PASV mode:

1. On the Main Console, click **Options** in the Functions area. The Options window opens.
2. In the left-side navigation area, expand the **Main** section and click **Access to Internet**. The Main - Access to Internet dialog box opens.
3. Select the **Enable FTP PASV Mode** check box.

Proxy Server Settings

If you access your firewall log files using HTTP via a proxy server, or if you register for and download a URL categorization database, you must define your proxy settings.

Note
If necessary, consult your network administrator for the address and port to use in this dialog box.

To set up the proxy server connection:

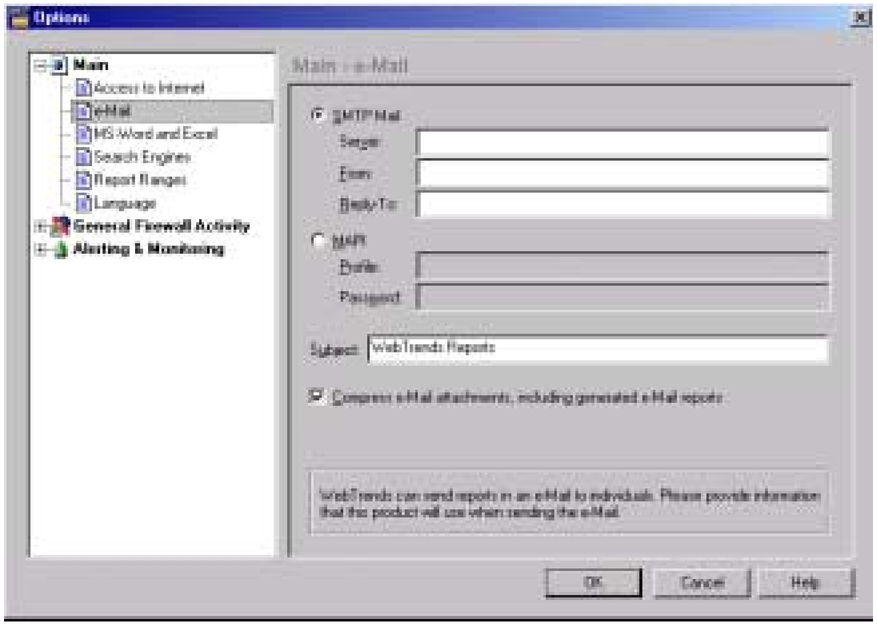
1. On the Main Console, click **Options** in the Functions area. The Options window opens.
2. In the left navigation area, expand the **Main** section and click **Access to Internet**. The Main - Access to Internet dialog box opens.
3. Select the **Connect through a Proxy Server** check box.
4. In the **HTTP Address** text box, type the HTTP address of the proxy server.
5. In the **Port** text box, type the port used by the proxy server.

6. If the proxy server is password-protected, select the **HTTP access requires a User Name/Password** check box and supply the user name and password used to log in to the proxy server in the text boxes provided.

7. Click **OK** to save your selection.

E-Mail Dialog Box

To send reports automatically by email, you must provide information about the type of email service your organization uses. Use the Main - e-Mail dialog box to specify these settings.



● SMTP Mail

Server:

From:

Reply-To:

○ MAPI

Profile:

Password:

Subject: WebTrends Reports

☑ Compress e-Mail attachments, including generated e-Mail reports

WebTrends can send reports in an e-Mail to individuals. Please provide information that this product will use when sending the e-Mail.

Sending Reports with SMTP Email

Simple Mail Transfer Protocol (SMTP) is used by most Internet mail programs (for example Eudora and Netscape). You can use SMTP email to send your reports.

To send reports using SMTP email:

1. On the Main Console, click **Options** in the Functions area. The Options window opens.
2. In the left-side navigation area, expand the **Main** section and click **e-Mail**. The Main - e-Mail dialog box opens.
3. Select the **SMTP Mail** check box
4. In the **Server** text box, type the host name or IP Address of your mail server.

   Note
   See your network administrator or refer to your email program configuration for this information.

5. In the **From** text box, type the email address that will be placed in the **From** field of the emailed report, for example `reports@webtrends.com`.
6. In the **Reply-To** text box, type the email address that any replies should go to. Usually this is the same as what's in the **From** text box, but in some cases it can be different.
7. In the **Subject** text box, type the text for the subject line that you want to appear on the report email.
8. Optionally compress email attachments by selecting the **Compress e-Mail attachments, including generated e-Mail reports** check box.
9. Click **OK** to save your selections.

Sending reports with MAPI email

Mail Application Programming Interface is an industry-wide standard for accessing large mail systems like Microsoft Mail and cc:Mail. You can use MAPI email to send your reports.

To send reports using MAPI email:

1. On the Main Console, click **Options** in the Functions area. The Options window opens.
2. In the left-side navigation area, expand the **Main** section and click **e-Mail**. The Main - e-Mail dialog box opens.
3. Select the **MAPI Mail** check box.
4. In the **Profile** text box, type the name of the profile to use for reports sent by email, for example Microsoft Outlook.

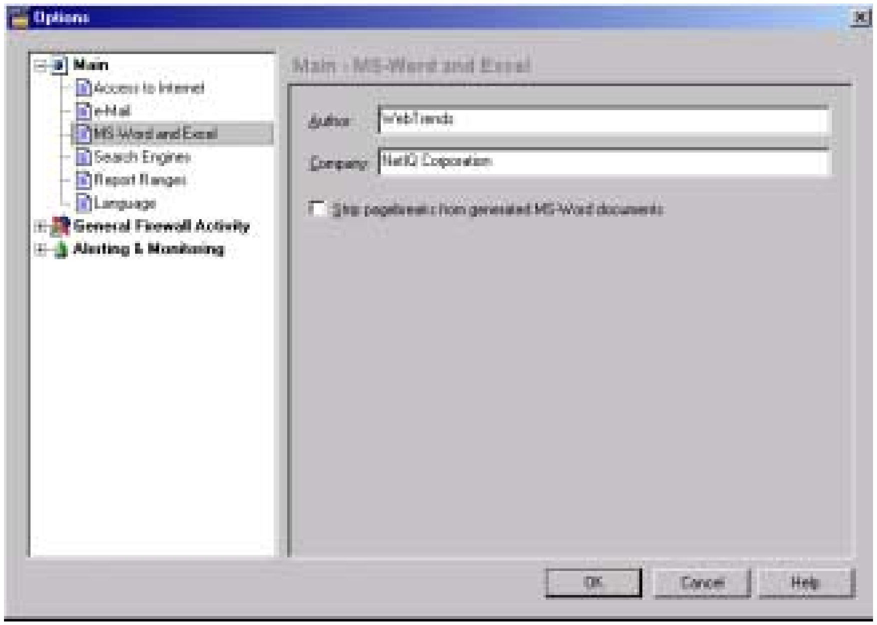
   Note
   See your network administrator or refer to your email program configuration for this information.

5. If applicable, type the password for the profile into the **Password** text box.
6. In the **Subject** text box, type the text for the subject line that you want to appear on the report email.
7. Optionally compress email attachments by selecting the **Compress e-Mail attachments, including generated e-Mail reports** check box.
8. Click **OK** to save your selections.

MS-Word and Excel Dialog Box

You can specify an author and company name to be included in reports generated in the Microsoft Word or Excel formats. By default, this information is taken from your system registry.

Note
You can generate reports in Microsoft Word or Excel formats only if you have Microsoft Office 95, Office 97, or Office 2000 installed on your system. Stand-alone versions of Microsoft Word and Excel do not provide the macro language necessary to create these reports.



Author: WebTrends

Company: NetIQ Corporation

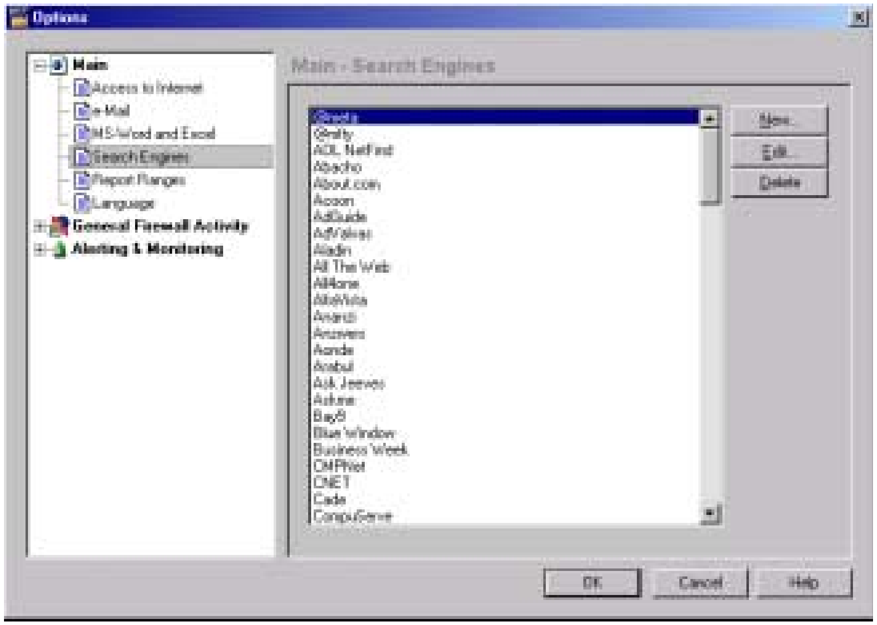
□ Strip pagebreaks from generated MS-Word documents

To specify MS-Word and Excel information:

1. On the Main Console, click **Options** in the Functions area. The Options window opens.
2. In the left-side navigation area, expand the **Main** section and click **MS-Word and Excel**. The Main - MS-Word and Excel dialog box opens.
3. In the **Author** text box, type the author name that you want to appear in reports.
4. In the **Company** text box, type the Company name as you want it to appear in reports.
5. Click **OK** to close the Options window.

Search Engines Dialog Box

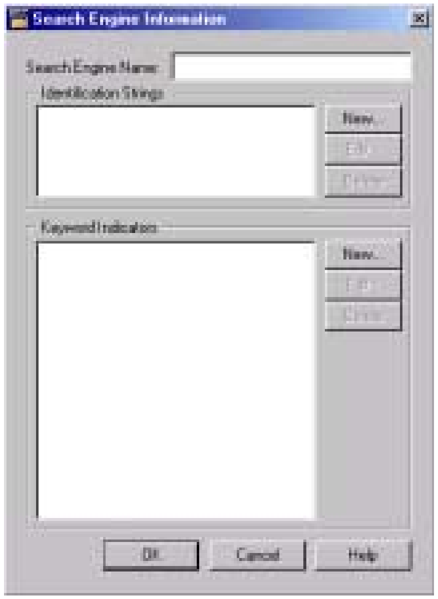
Firewall Suite can analyze a log file and pick out which search strings and which search engines visitors to your Web site used when they located and connected to your Web pages. The software already includes an extensive list of popular or common search engines it can identify and methods by which it can recognize keyword search terms. However, you can use the Main - Search Engines dialog box to add new search engines and keyword-recognition methods, change settings for search engines already in the list, or delete search engines from the list.



To add a new search engine:

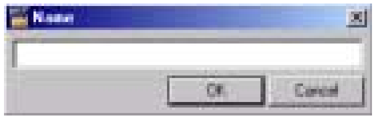
1. On the Main Console, click **Options** in the Functions area. The Options window opens.
2. In the left-side navigation area, expand the **Main** section and click **Search Engines**. The Main - Search Engines dialog box opens.

3. Click **New**. The Search Engine Information dialog box opens.



4. In the **Search Engine Name** text box, enter the name of the search engine you are adding.

5. In the Identification Strings area, click **New**. The Name dialog box opens.



6. Enter an identification string in the text box. These strings must correspond exactly to those that the search engine records in your firewall log file. Usually, you can spot the identification string by looking for a URL in the **Referrers** field and entering as much of it as you want Firewall Suite to look for when it analyzes the log file. Entering a single term such as "yahoo" will capture a broad selection of search engines that Yahoo! might use. Entering a more focused term such as "search.server1.yahoo.com" (a fictitious example), allows you to break down your report to identify specific engines.
7. Click **OK** to save the string and return to the Search Engine Information dialog box. You may repeat Steps **5** through **7** to add as many identification strings as needed.
8. In the Keyword Indicators area, click **New**. The Name dialog box opens.
9. Enter a keyword indicator in the text box. This allows you to determine which search terms visitors used to locate your Web site. You can use this information to adjust the keywords you use to identify your pages in the Meta tag or the keywords you used to register your site with search engines.

   The keyword indicators usually have a distinctive format and appear at the end of the URL that identifies the search engine in your log file. Be sure to enter only the indicator itself -- often, a character such as ? or & marks the start of the indicator, while a semicolon, an = sign, or other character can mark the end of the indicator.
10. Click **OK** to save the string and return to the Search Engine Information dialog box.
11. Repeat Steps **8** through **10** to add as many identification strings as you need.

To edit an existing search engine in the list:

1. On the Main Console, click **Options** in the Functions area. The Options window opens.
2. In the left-side navigation area, expand the **Main** section and click **Search Engines**. The Main - Search Engines dialog box opens.

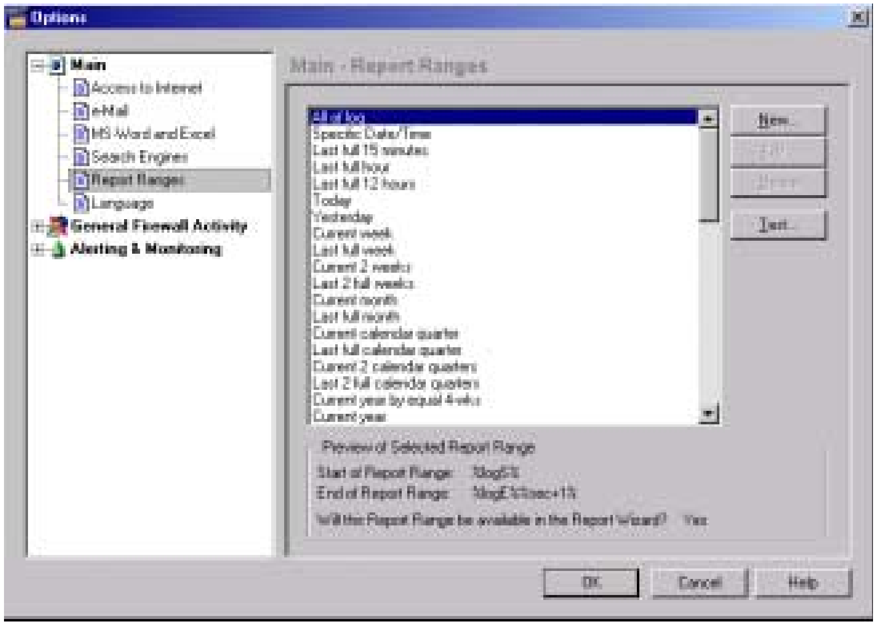
3. From the list, select the search engine you wish to edit.
4. Click **Edit**. The Search Engine Information dialog box opens.
5. Select an element that you wish to edit from the Identification Strings area or the Keyword Indicators area.
6. Click **Edit**. The Names dialog box opens.
7. Edit the string as needed and click **OK** to return to the Search Engine Information dialog box.
8. Repeat Steps **5** through **7** to edit as many items as needed.
9. Click **OK** to accept your changes and return to the Main - Search Engines dialog box.

To delete a search engine from the list:

1. On the Main Console, click **Options** in the Functions area. The Options window opens.
2. In the left-side navigation area, expand the **Main** section and click **Search Engines**. The Main - Search Engines dialog box opens.
3. From the list, select the search engine you wish to delete.
4. Click **Delete**. The selected search engine is removed from the list.

Report Ranges Dialog Box

Report ranges define the time period for which you want to generate reports. You can choose to report on the contents of the entire log file, or you can limit how much you report on by selecting a time period for which to generate reports. Your firewall reporting solution installs with many pre-defined report ranges, but you can add, edit, or delete report ranges as needed. Use the Main - Report Ranges dialog box to perform these actions.



All of log
Specific Date/Time
Last full 15 minutes
Last full hour
Last full 12 hours
Today
Yesterday
Current week
Last full week
Current 2 weeks
Last 2 full weeks
Current month
Last full month
Current calendar quarter
Last full calendar quarter
Current 2 calendar quarters
Last 2 full calendar quarters
Current year by equal 4-wks
Current year

Preview of Selected Report Range

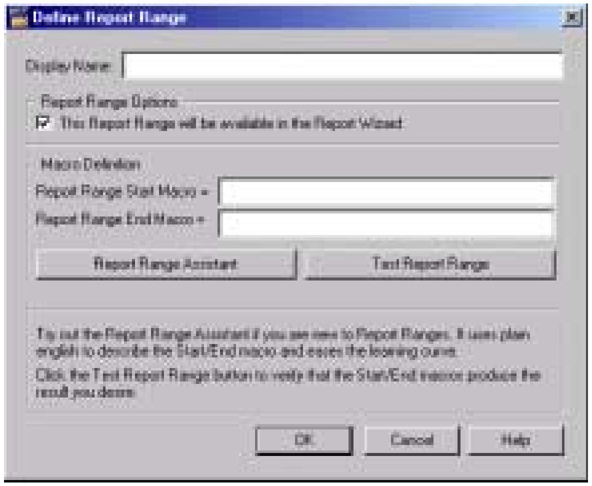
Start of Report Range: %logS%
End of Report Range: %logE%%sec+1%

Will this Report Range be available in the Report Wizard? Yes

To add a new report range:

1. On the Main Console, click **Options** in the Functions area. The Options window opens.
2. In the left-side navigation area, expand the **Main** section and click **Report Ranges**. The Main - Report Ranges dialog box opens.

3. Click **New**. The Define Report Range dialog box opens.



☑ This Report Range will be available in the Report Wizard

Try out the Report Range Assistant if you are new to Report Ranges. It uses plain english to describe the Start/End macro and eases the learning curve.

Click the Test Report Range button to verify that the Start/End macros produce the result you desire.

4. In the **Display Name** text box, enter a descriptive name for the report range you are defining. This name will appear in the list of report ranges in the Main - Report Ranges dialog box.

5. Select **This will be available in the Report Wizard** to have your report range listed in the **Pre-defined Range** dropdown menu in the Report Range tab. This tab appears either in the New Report or the Edit Report dialog box when you create or modify a report template.

6. Type the macros that you want to use to designate the start of your report range. Or click **Report Range Assistant** to specify the report range. To learn how to enter macros for this purpose, see “Using Macros to Define a Report Range” on page 306.

7. Enter the macros that designate the end of your report range. To learn how to do so, see “Using Macros to Define a Report Range” on page 306.

   If you want the software to guide you as you enter your macros in either provided text box, click **Report Range Assistant**.

8. Use the **Profile Type** dropdown list to select a profile type. Because the content of reports is different for each profile type, modifications to a “language” affect only the profile type that you select here.

9. In the Report Language pane, do one of the following:

   – Select an existing language to modify it.

   – Click **Add** to create a new language. When the Add New Report Language dialog box appears, type a name for your new report language, and select an existing language to base it on.

10. The Report Items pane displays a tree containing the report sections and corresponding text areas.

    – Click **Collapse All** to close all of the books and view only the top-level directories of the selected language tree.

    – Click **Expand All** to open all subdirectories and view the entire tree.

    – Click **Find** to access the Find/Replace dialog box, which lets you search for and replace text that appears in the reports.

11. When you select a report text string in Report Items, the text appears in the Content text box. Edit the text in this text box and click **Save**, or click **Restore** to revert to a previously saved text string (for the selected report item or the entire report language.

12. If desired, click **Set Default Language** to define the language that all new reports will use by default.

13. Click **Save** to keep your changes or **Restore** to return to the original settings.

14. Click **OK** to return to the Main Console.

To edit a report range:

1. Select the report range you wish to edit from the list.

2. Click **Edit**.

3. Edit any items in the dialog box and click **OK** to save your changes and return to the Main - Report Ranges dialog box.

To delete a report range:

1. Select the report range you wish to delete from the list.
2. Click **Delete**. A confirmation message appears
3. Click **Yes** to confirm that you wish to delete the report range.

Using Macros to Define a Report Range

To specify a report range, you need both a *reference point* and units of time that your firewall reporting solution can use to calculate the start and the end of the range. A reference point is a fixed point that your reporting solution uses to add to or subtract units of time from when defining the report range start and end times. The date and time of the first record in your file is one possible reference point.

See the following tables to learn more about each of the items available in the report range macro "vocabulary." The column labeled **What you enter** shows you the exact characters that you enter in the text boxes provided in the Define Report Range dialog box.

The following table defines macros that set reference points.

Macro Name	Macro text	Macro Resolution
Now	`%now%`	Sets the reference point to the time that you run your log analysis report
Start of log	`%logS%`	Sets the reference point equal to the date and time stamp for the first record captured in your log file
End of log	`%logE%`	Sets the reference point equal to the date and time stamp for the last record captured in your log file

The following table defines macros that set units of time.

Macro Name	Macro Text	Macro Resolution
Seconds	%sec%	Depending on its context, sets the beginning of the report range at the current second or at a particular second.
Minute	%min%	Depending on its context, sets the beginning of the report range at the first second of the current minute or at the first second of a particular minute.
Hour	%hr%	Depending on its context, sets the beginning of the report range at the first second of the current hour or at the first second of a particular hour.

Macro Name	Macro Text	Macro Resolution
Day	`%day%`	Depending on its context, sets the beginning of the report range at the exact point of midnight today or at the exact point of midnight on a particular day.
Week	`%wk%`	Depending on its context, sets the beginning of a report range at the exact point of midnight on the first day of the current week or on the first day of a particular week. The definition of the first day of the week depends on what you have specified in the Main Options page.
Four Week Period	`%4wk%`	Breaks the processed report into four-week periods, but does not otherwise affect the report range you specify with other macros. Use this macro at the end of the first macro string.
Month	`%mon%`	Depending on its context, sets the beginning of a report range at the exact point of midnight on the first day of the current month or of a particular month.

Macro Name	Macro Text	Macro Resolution
Calendar Quarter	`%cqtr%`	Depending on its context, sets the beginning of a report range at the exact point of midnight on the first day of the current calendar quarter, or at the exact point of midnight on the first day of a particular calendar quarter. A calendar quarter is a three-month period.
Fiscal Quarter	`%fqtr%`	Depending on its context, sets the beginning of a report range at the exact point of midnight on the first day of the current fiscal quarter, or at the exact point of midnight on the first day of a particular fiscal quarter. A fiscal quarter is a three-month period whose start depends on what you set in the Main Options dialog box as the start of your fiscal year.
Year	`%yr%`	Depending on its context, sets the beginning or a report range to the exact point of midnight on the first day of the current year, or at the exact point of midnight on the first day of a particular year.

Report Range Macros in Pre-Defined Reports

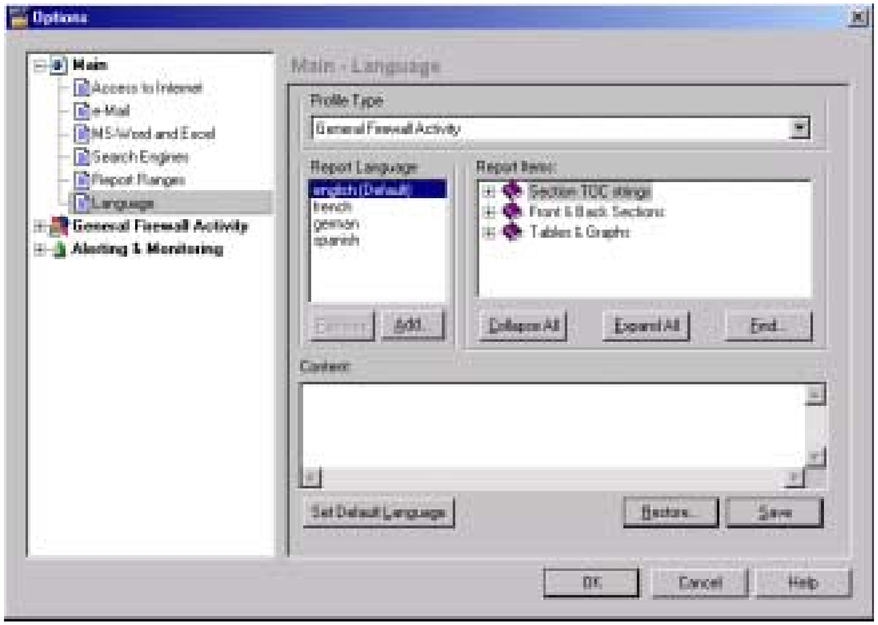
To see how the pre-defined reports available with your firewall reporting solutions use macros to specify their ranges, click on a report range in the Main - Report Ranges dialog box and examine the **Preview of Selected Report Range** area at the bottom of the dialog box.

The pre-defined reports available in the Create Report and Edit Report dialog boxes all use macros to specify their report ranges. Use these pre-defined reports as examples to guide you as you construct your own macro strings.

Language Dialog Box

The Main - Language dialog box allows you to specify the language options for firewall activity reports. Alerting and Monitoring language options are set separately in the Alerting and Monitoring section of the Options window.

Besides the available choices of English, French, German, and Spanish, this dialog box lets you define specific phrases and titles as a part of the "language" to use in reports. You can also modify an existing language to meet your reporting needs.



Profile Type: General Firewall Activity

Report Language: english (Default)

To define report language settings for firewall activity reports:

1. On the Main Console, click **Options** in the Functions area. The Options window opens.
2. In the left-side navigation area, expand the **Main** section and click **Language**. The Main - Language dialog box opens.

3. In the **Profile Type** dropdown list, select the profile type you wish to set language options for.

4. To use an existing language, select it from the list.

5. To add a new report language:

   a. Click **Add**. The Add New Report Language dialog box opens.

   b. In the **New Language Name** text box, type the name of the new language you are going to add to the list.

   c. Click **OK** to return to the Main - Languages dialog box.

6. In the **Report Items** list, select any item from the list that you wish to edit. The language associated with the selected item appears in the **Content** area below.

Note
Click **Collapse All** or **Expand All** to collapse or expand the items in the Report Items list. To locate a specific report item, click **Find**, and use the Find/Replace dialog box to search for and replace text that appears in the reports.

7. If you wish to change the text that appears in reports, replace the text in the **Content** area with the text you wish to see.

8. Click **Set Default Language** to define the language that will be used by default for all new reports.

9. Click **Save** to save your changes.

10. Click **OK** to save your selections and changes.

Restoring Language Settings

Within the Main - Language dialog box, you can revert back to the previously saved version of either the selected report item or the entire report language.

To restore language settings for a report item:

1. In the Main - Languages dialog box, select the report item you wish to restore.
2. Click **Restore**. The Content area should display the previously saved version of the selected item.
3. Click **OK** to save your changes.

To restore language settings for the entire report:

1. In the Main - Languages dialog box, click **Restore**.
2. Click **OK** to save your changes.

Specifying the Default Report Language

You can change which language to use as the default language for all reports.

To specify the default report language:

1. In the **Report Language** list of the Main - Languages dialog box, select the report language you wish to set as the default language.
2. Click **Set Default Language**.
3. Click **OK** to save your changes.

Report Date Format

Firewall Suite lets you display the date that appears in reports in several formats. By default, the date is written in `mm/dd/yy` format. Other available formats are `dd/mm/yy` and `yy/mm/dd`.

Note
The day of the week you select from the **Weeks Start** list on the **Locale** tab determines what constitutes a week in your reports. See “Selecting a Web Browser” on page 290 for details.

To select a report date format:

1. On the Main Console, click **Options** in the Functions area. The Options window opens.
2. In the left-side navigation area, expand the **Main** section and click **Language**. The Main - Language dialog box opens.
3. Select a profile type from the dropdown list. The date format change applies to all reports of this profile type.
4. ***If you are using an incoming profile*:**
   - **a.** Select a Report Language. The default is English.
   - **b.** In the Report Items area, expand Common Strings and expand Date and Local.
   - **c.** Select Report Date Format, and in the **Content** text box, type the format option you wish to use in your reports.

     Note

     You can also change the abbreviations for days and months, names for days and months, the Report Date delimiter, Report time delimiter, and hours designated as Work Hours and After Hours.

5. ***If you are using an outgoing profile:***

   a. Select a Report Language. The default is English.

   b. In the **Report Items** field, expand Tables and Graphs and expand Locale Variables (near the bottom of the list).

   c. Select **Report Date Format**, and in the **Content** text box, type the format option you wish to use in your reports.

   Note
   You can also change the Report Date delimiter, Report time delimiter, and hours designated as Work Hours and After Hours by entering them in the **Content** text box.

6. Click **Save**.

General Firewall Activity Options

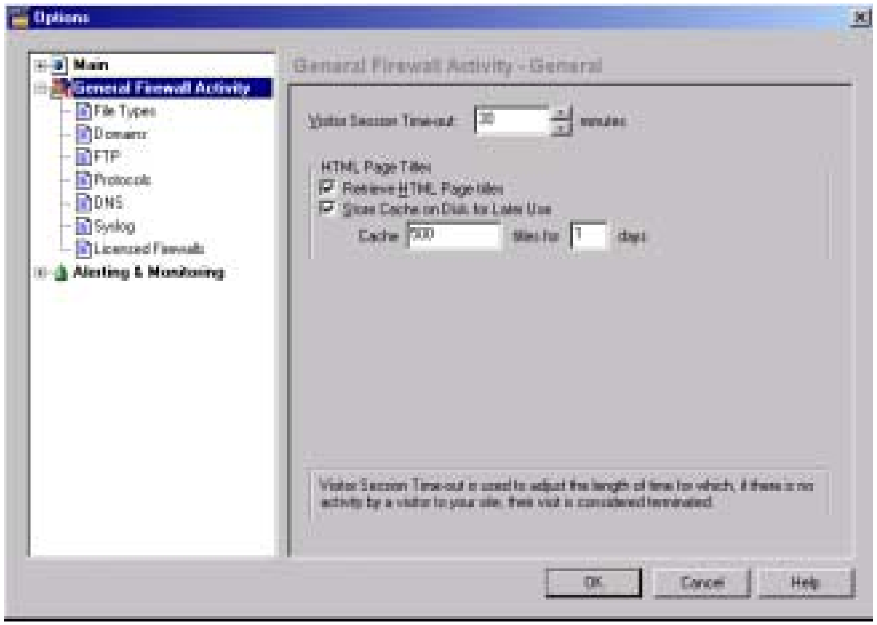
The settings in the General Firewall Activity Options window apply to how profiles and reports are processed. You can define a variety of settings including the following:

- The types of files and extensions to report on
- The types of domains to report on
- How often to retrieve the log file if accessed via HTTP or FTP
- The protocols logged by your firewall
- The size of the cache used for domain name (DNS) lookups
- How long to keep DNS lookups cached before deleting them

- How often to rotate WebTrends Syslog Service log files
- The Check Point LEA connections that can be selected when you create a profile that references a Check Point firewall with OPSEC LEA.
- The firewalls for which this product is licensed
- If you use a Cisco PIX firewall, which interfaces the firewall interacts with.

General Firewall Activity - General Options

The General Firewall Activity - General dialog box lets you control the DNS Cache size, set the frequency of the log file list refresh, specify the terminate user session interval, and define HTML report settings.



Visitor Session Time-out: 30 minutes

HTML Page Titles

☑ Retrieve HTML Page titles

☑ Store Cache on Disk for Later Use

Cache 500 titles for 1 days

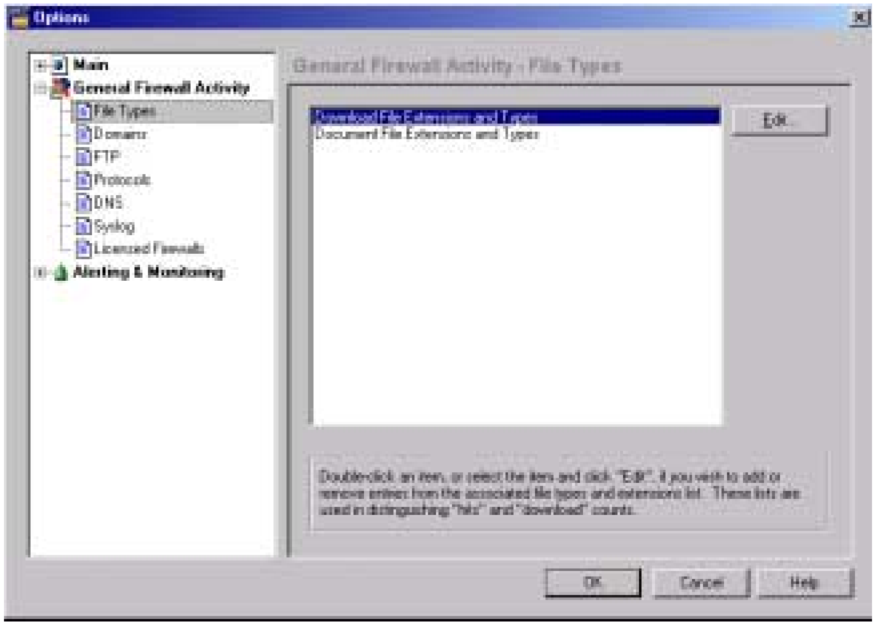
Visitor Session Time-out is used to adjust the length of time for which, if there is no activity by a visitor to your site, their visit is considered terminated.

To define General dialog box options:

1. On the Main Console, click **Options** in the Functions area. The Options window opens.
2. In the left-side navigation area, click **General Firewall Activity**. The General Firewall Activity - General dialog box opens.
3. In the **Visitor Session Time-Out** list, type or scroll to a number that to adjust the length of time for which, if there is no activity by a visitor to your site, his/her user session is considered terminated.
4. Optionally select **Retrieve HTML Page Titles** to display the page title of your Web site pages in related report tables. If this option is not selected, only the URL of the page appears
5. Optionally select **Store Cache on Disk for Later Use** and specify the maximum number of page titles to cache and the number of days to save them.
6. Click **OK** to save your changes.

File Types Dialog Box

The **General Firewall Activity - File Types** dialog box of the Options window lets you add or remove the file extensions that Firewall Suite includes in the relevant tables and graphs. These lists are used in distinguishing hits and download counts.



Download File Extensions and Types
Document File Extensions and Types

Double-click an item, or select the item and click "Edit", if you wish to add or remove entries from the associated file types and extensions list. These lists are used in distinguishing "hits" and "download" counts.

To define file types:

1. On the Main Console, click **Options** in the Functions area. The Options window opens.
2. In the left-side navigation area, expand the **General Firewall Activity** section and select the **File Types** option. The General Firewall Activity - File Types dialog box opens.

3. Select the file type that you want to modify:

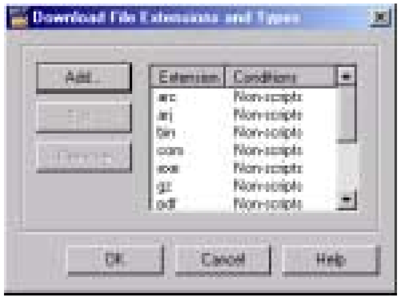
   – **Download File Extensions and Types** adds or removes the file types that are included in the Most Downloaded File Types table and graph.

   – **Document File Extensions and Types** adds or removes the file types included in report tables and graphs that track documents, for example Top and Least Requested Pages, Top Entry and Exit Pages, and Single Access Pages.

4. Click **Edit** to make changes to the selected list. If you selected:

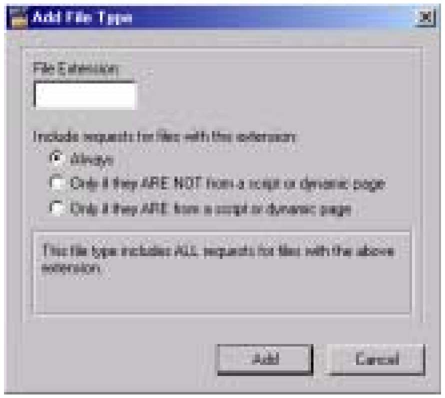
   – **Download File Extensions and Types**, the Download File Extensions and Types dialog box opens with a list of the file extensions and conditions.

   – **Document File Extensions and Types**, the Document File Extensions and Types dialog box opens with a list of the file extensions and conditions.



Extension	Conditions
arc	Non-scripts
arj	Non-scripts
bin	Non-scripts
com	Non-scripts
exe	Non-scripts
gz	Non-scripts
pdf	Non-scripts

5. *To add a file type*, click **Add** to open the Add File Type dialog box and do the following:



File Extension:

Include requests for files with this extension:

● Always
○ Only if they ARE NOT from a script or dynamic page
○ Only if they ARE from a script or dynamic page

This file type includes ALL requests for files with the above extension.

a. Enter the file extension for the new file type and select:

– **Always** if you wish to always include requests for this file type in your reports.

– **Only if they ARE NOT from a script or dynamic page** if you wish to include requests for this file type in your reports if they are not generated from a script or by a dynamic page.

– **Only if they ARE from a script or dynamic page** if you wish to include requests for this file type in your reports if they are generated from a script or by a dynamic page.

b. Click Add to add the new file extension.

6. *To edit a file type,* select an item from the list that you wish to edit and click **Edit**.

7. Enter the file extension for the new file type.

8. Do one of the following:

   - Select **Always** if you wish to always include requests for this file type in your reports.
   - Select **Only if they ARE NOT from a script or dynamic page** if you wish to include requests for this file type in your reports if they are not generated from a script or by a dynamic page.
   - Select **Only if they ARE from a script or dynamic page** if you wish to include requests for this file type in your reports if they are generated from a script or by a dynamic page.

9. Click **OK** to save your file extension edits.

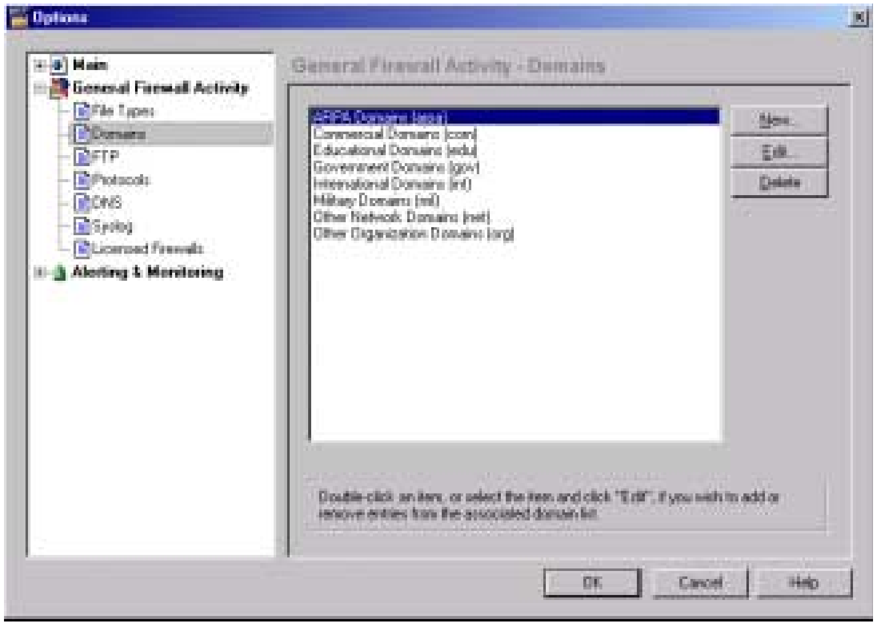
10. To remove a file type, select it from the list and click **Remove**.

    Warning
    The Remove function does not ask you to confirm the removal—the file type is removed immediately.

11. When the Firewall Types window reopens, click **OK** or select another tab.

Domains Dialog Box

The General Firewall Activity - Domains dialog box lets you add, edit, or remove the domain name suffixes that your firewall reporting solution includes in the listed domain name groupings, for example United States Domains, Government Domains, and Military Domains.



ARPA Domains (arpa)
Commercial Domains (com)
Educational Domains (edu)
Government Domains (gov)
International Domains (int)
Military Domains (mil)
Other Network Domains (net)
Other Organization Domains (org)

Double-click an item, or select the item and click "Edit", if you wish to add or remove entries from the associated domain list.

To add a domain grouping:

1. On the Main Console, click **Options** in the Functions area. The Options window opens.
2. In the left-side navigation area, expand the **General Firewall Activity** section and select the **Domains** option. The General Firewall Activity - Domains dialog box opens.
3. Click **New**.
4. Type the **Domain Name** and **Domain Type**.

5. In the text box to the right of the Domain Suffixes list, type the extension associated with your domain. For example, type `gov` for government domains.

6. Click **Add**. The extension is added to the list.

To edit a domain grouping:

1. On the Main Console, click **Options** in the Functions area. The Options window opens.

2. In the left-side navigation area, expand the **General Firewall Activity** section and select the **Domains** option. The General Firewall Activity - Domains dialog box opens.

3. Select a domain grouping from the list.

4. Click **Edit**.

5. *To add a domain extension to the list*:

   a. Enter the extension into the text box.

   b. Click **Add**.

6. *To remove an item from the list*.

   a. Select the domain extension(s) you wish to remove. Use the `Shift` and `Ctrl` keys to select multiple items.

   b. Click **Remove**. Any selected domain extensions are removed.

   Note
   Click **Select All** to select all items in the list. Click **Un-select All** to de-select any selected item in the list.

7. Click **OK** to save your changes.

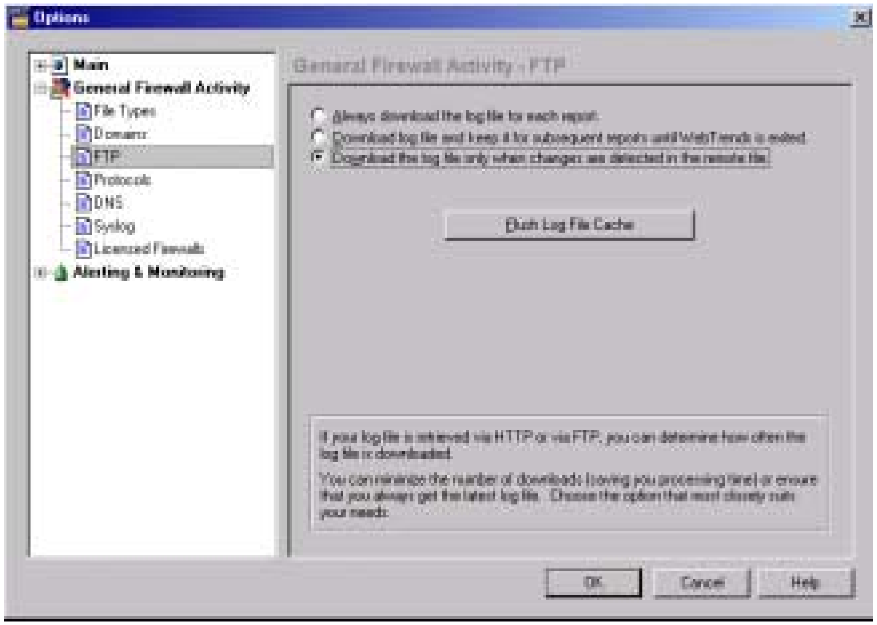
To delete a domain grouping:

1. On the Main Console, click **Options** in the Functions area. The Options window opens.
2. In the left-side navigation area, click **General Firewall Activity** and select the **Domains** option. The General Firewall Activity - Domains dialog box opens.
3. Select a domain grouping from the list.
4. Click **Remove**.
5. Click **OK**. The selected domain grouping is removed from the list.

FTP Dialog Box

If your firewall log file is retrieved by either HTTP or FTP, you can configure how frequently the log file is downloaded. More frequent downloads require more processing time, but ensure that your log file data is more current. Keep in mind that file access to your log file is quicker than either of these methods.

Note
Most firewalls do not allow you to download files via HTTP or FTP, but if yours does, these settings apply. If you only access the firewall log file through file retrieval, you don't need to define these settings.



General Firewall Activity - FTP

○ Always download the log file for each report.
○ Download log file and keep it for subsequent reports until WebTrends is exited.
● Download the log file only when changes are detected in the remote file.

If your log file is retrieved via HTTP or via FTP, you can determine how often the log file is downloaded.

You can minimize the number of downloads (saving you processing time) or ensure that you always get the latest log file. Choose the option that most closely suits your needs.

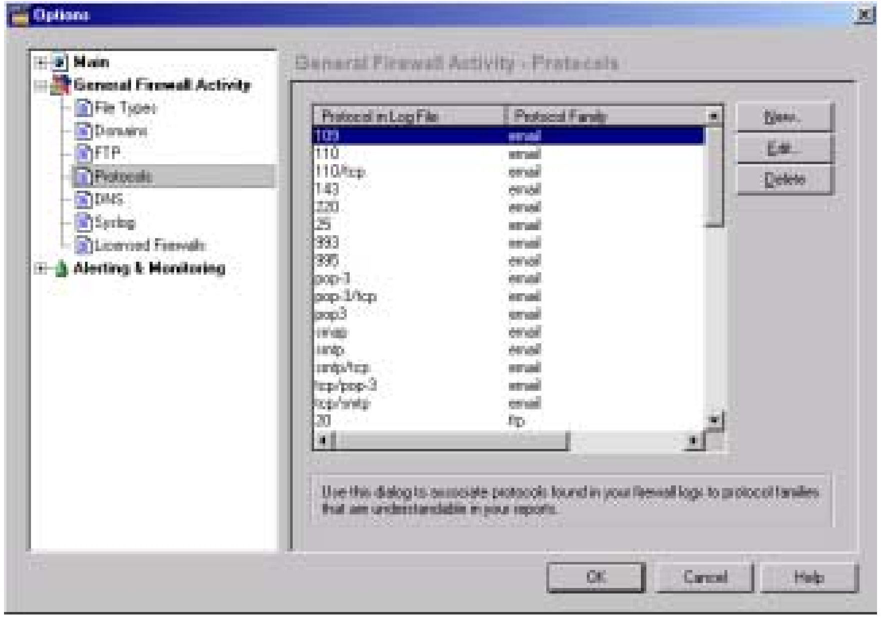
To specify how often to download the log file via HTTP or FTP:

1. On the Main Console, click **Options** in the Functions area. The Options window opens.
2. In the left-side navigation area, expand the **General Firewall Activity** section and select the **FTP** option. The General Firewall Activity - FTP dialog box opens.
3. Select one of the following options:
   - **Always download the log file for each report** if you wish to download the log file every time a new report is generated, regardless of whether there is any new activity.
   - **Download log file and keep it for subsequent reports until WebTrends is exited** if you wish to retrieve the log file only one time during each session, regardless of the number of reports generated on it or whether there has been any new activity. Use this option for best performance when creating several successive reports.
   - **Download the log file only when changes are detected in the remote file** if you wish to retrieve the log file only when new activity has been recorded. Each time you run a report, your firewall reporting solution determines whether the log file has changed since the last report was run and updates the log file only if it has changed.
4. To clear the entries in the log file cache and restore disk space, click **Flush Log File Cache**. Flushing the Log File Cache clears the cache for all profiles. However, when you report on a log file that is accessed via HTTP or FTP, the file must be downloaded until the entries are restored.

Protocols Dialog Box

General Firewall Activity reports include tables and graphs that provide a summary of protocol activity and details for a specific protocol in your log file.

For reporting purposes, protocols from your log file are associated with (or assigned to) a specific type of protocol (protocol family) in the General Firewall Activity - Protocols dialog box of the Options window. Types of protocols may include email, FTP, RealAudio, Telnet, or Web. You can associate protocols in groups that make the reports responsive to your needs. You can even create your own family of protocols.



Protocol in Log File	Protocol Family
109	email
110	email
110/tcp	email
143	email
220	email
25	email
993	email
995	email
pop-3	email
pop-3/tcp	email
pop3	email
imap	email
smtp	email
smtp/tcp	email
tcp/pop-3	email
tcp/smtp	email
20	ftp

Use this dialog to associate protocols found in your firewall logs to protocol families that are understandable in your reports.

The **Protocol in Log File** and **Type of Protocol** columns show how protocols are currently defined. The Protocol in Log File column identifies the protocol as it is recorded in the log file. The Type of Protocol column indicates how the associated Protocol in Log File has been set up to appear in reports.

Any protocol not included in the Protocol in Log File list or associated with a type of traffic is reported as “other.” The activity of these non-associated protocols is difficult to analyze.

Note

To determine if protocols are defined correctly, run a General Firewall Activity report, and view the Incoming Protocol Usage and Outgoing Protocol Usage tables. These tables display the protocols found in the log file. You can compare these protocols to those found in the Protocols dialog box. Any protocols not listed here that apply to one of the pre-defined categories should be added.

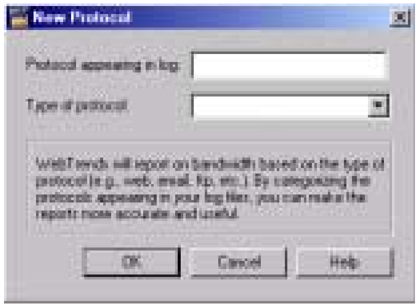
You can further refine the reports on protocols with the Protocol Family filter. See “Protocol Family” on page 195 for more information about filtering protocols.

You may want to add a new protocol that is present in your log file and assign its protocol type to determine how this new protocol will be analyzed and presented in reports.

To add a new protocol and assign its type:

1. On the Main Console, click **Options** in the Functions area. The Options window opens.
2. In the left-side navigation area, expand the **General Firewall Activity** section and select the **Protocols** option. The General Firewall Activity - Protocols dialog box opens.

3. Click **New**. The New Protocol dialog box opens.



WebTrends will report on bandwidth based on the type of protocol (e.g., web, email, ftp, etc.). By categorizing the protocols appearing in your log files, you can make the reports more accurate and useful.

4. In the **Protocol appearing in log** text box, type the protocol name as it appears in your firewall log,

5. Assign the protocol type by choosing one of the following options:

   – Select a protocol type from the **Type of Protocol** dropdown list.

   – Type a name in the **Type of Protocol** text box to create a new type of protocol. This new type will be available in the dropdown list from now on, unless you delete all protocol names assigned to it.

6. Click **OK** to return to the Protocols dialog box.

7. Click **OK** to save your changes.

To edit an existing protocol:

1. On the Main Console, click **Options** in the Functions area. The Options window opens.

2. In the left-side navigation area, expand the **General Firewall Activity** section and select the **Protocols** option. The General Firewall Activity - Protocols dialog box opens.

3. Select the protocol you wish to edit.

4. Click **Edit**. The Edit Protocol dialog box opens.

5. In the **Protocol appearing in log** text box, type the protocol name as it appears in your firewall log.

6. Assign the protocol type by choosing one of the following options:

   – Select a protocol type from the **Type of Protocol** dropdown list.

   – Type a name in the **Type of Protocol** text box to create a new type of protocol. This new type will be available in the dropdown list from now on, unless you delete all protocol names assigned to it.

7. Click **OK** to return to the Protocols dialog box.

8. Click **OK** to save your changes.

To delete an existing protocol:

1. On the Main Console, click **Options** in the Functions area. The Options window opens.

2. In the left-side navigation area, expand the **General Firewall Activity** section and select the **Protocols** option. The General Firewall Activity - Protocols dialog box opens.

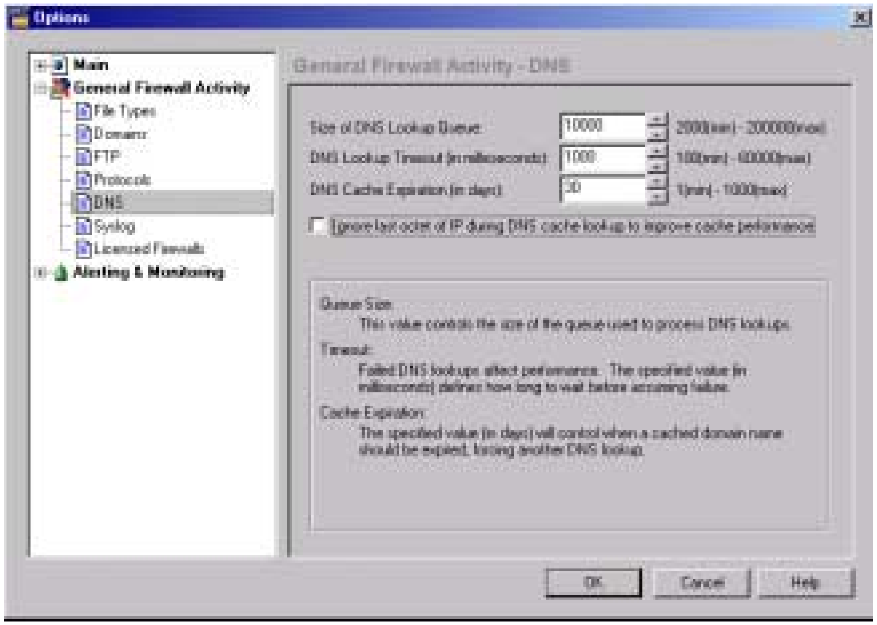
3. Select the protocol you wish to delete.

4. Click **Delete**. The selected protocol is deleted from the list.

DNS Dialog Box

When you create a Firewall activity profile, you can determine a Domain Name System (DNS) lookup method and the location of the DNS cache.

Use the DNS dialog box to optimize DNS lookups for the profiles when you've chosen to use either Resolve Mode or Auto Mode with the profile.



General Firewall Activity - DNS

Size of DNS Lookup Queue: 10000 2000(min) - 200000(max)

DNS Lookup Timeout (in milliseconds): 1000 100(min) - 60000(max)

DNS Cache Expiration (in days): 30 1(min) - 1000(max)

☐ Ignore last octet of IP during DNS cache lookup to improve cache performance

Queue Size:
This value controls the size of the queue used to process DNS lookups.

Timeout:
Failed DNS lookups affect performance. The specified value (in milliseconds) defines how long to wait before assuming failure.

Cache Expiration:
The specified value (in days) will control when a cached domain name should be expired, forcing another DNS lookup.

To specify DNS Lookup options:

1. On the Main Console, click **Options** in the Functions area. The Options window opens.
2. In the left-side navigation area, expand the **General Firewall Activity** section and select the **DNS** option. The General Firewall Activity - DNS dialog box opens.
3. In the **Size of DNS Lookup Queue** list, select the size of the queue used to process DNS lookups. The default is 10,000. Increasing the size of the queue can speed up processing, but it takes more memory.

4. In the **DNS Lookup Timeout** list, select the number of milliseconds that must elapse before DNS lookups time-out. If DNS lookup is unsuccessful within this time span, your firewall reporting solution assumes failure. The lookup for the IP is recorded in the cache as failed. No further DNS lookup is attempted until the cache expires.

5. In the **DNS Cache Expiration** list, select the number of days that a domain name will be retained in the cache. After this number of days passes for a given IP address, it is discarded from the cache. If the IP address is encountered at a later date, it is resolved and added to the cache the next time the profile is used.

6. If desired, select the **Ignore last octet of IP** check box to resolve to the network ID. This can speed up processing, but results may be less accurate because the last part of the IP address is ignored.

   For example, the following log entries:

   ```
   2000-01-01 10:48:02 195.52.225.44 - W3SVC7
     WEBSERVER - GET /default.htm…
   2000-01-01 10:48:04 195.52.225.45 - W3SVC7
     WEBSERVER - GET /loganalyzer/info.htm…
   2000-01-01 10:48:08 195.52.225.46 - W3SVC7
     WEBSERVER - GET /styles/style1.css…
   ```

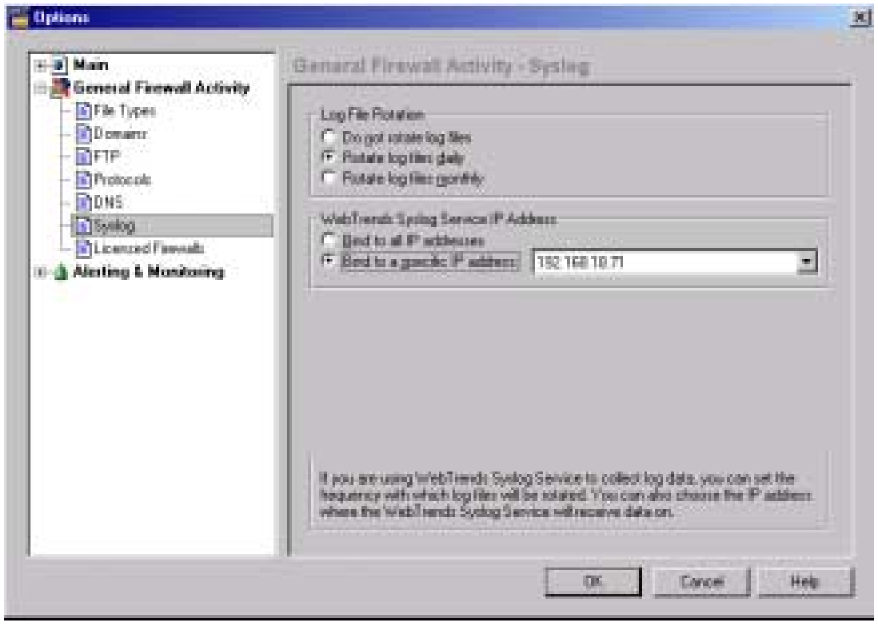
   would normally trigger three separate DNS lookups (195.52.225.44, 195.52.225.45, 195.52.225.46). With **Ignore last octet** enabled, only one lookup occurs (195.52.225.44). Since all three have the same first three parts, the first lookup is applied to the other two IP addresses.

7. Click **OK** to save your changes.

Syslog Dialog Box

Note
You must have Administrator rights on the Firewall Suite computer to be able to define the WebTrends Syslog Service settings.

Use the General Firewall Activity - Syslog dialog box to modify the settings for the WebTrends Syslog Service.



General Firewall Activity - Syslog

Log File Rotation

○ Do not rotate log files
● Rotate log files daily
○ Rotate log files monthly

WebTrends Syslog Service IP Address

○ Bind to all IP addresses
● Bind to a specific IP address: 192.168.10.71

If you are using WebTrends Syslog Service to collect log data, you can set the frequency with which log files will be rotated. You can also choose the IP address where the WebTrends Syslog Service will receive data on.

To define WebTrends Syslog Service settings:

1. On the Main Console, click **Options** in the Functions area. The Options window opens.
2. In the left-side navigation area, expand the **General Firewall Activity** section and select the **Syslog** option. The General Firewall Activity - Syslog dialog box opens.

3. In the Log File Rotation area, select how often you want the current log file archived and a new log started.

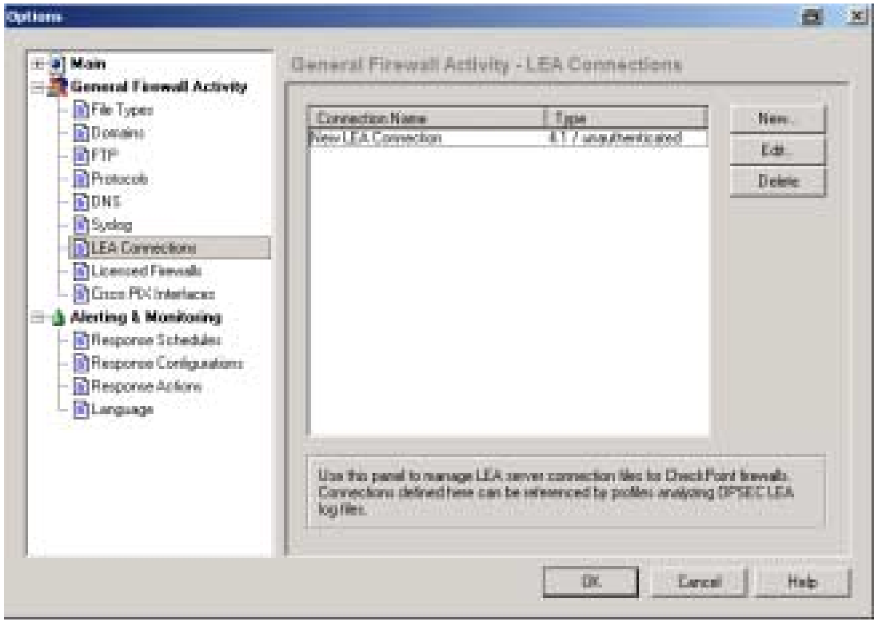
4. In the Syslog Server IP Address area, choose a binding method. Select:

   - **Bind to all IP addresses** to assure that all IP addresses respond to the Syslog Server. This is the default setting. Do not bind to a specific IP address unless absolutely necessary.
   - **Bind to a specific IP address** and select the address from the dropdown list.

5. Click **OK** to save your changes.

LEA Connections Dialog Box

The LEA Connections dialog box lists all currently configured connections between a Check Point firewall and the WebTrends LEA Service. A Check Point LEA connection is required for the WebTrends LEA Service to collect Check Point log data. Use this dialog box to create, edit, and delete LEA connections. When you create a profile that uses Check Point with OPSEC LEA, you select one of the LEA connections in the list to collect the log data.



General Firewall Activity - LEA Connections

Connection Name	Type
New LEA Connection	4.1 / unauthenticated

Use this panel to manage LEA server connection files for Check Point firewalls. Connections defined here can be referenced by profiles analyzing OPSEC LEA log files.

Before you add or edit connections, make sure you have configured your Check Point firewall to communicate with the WebTrends LEA Service. You need information about your Check Point configuration to create a LEA connection. For instructions on configuring Check Point firewalls, see the *Firewall Configuration Guide* or the Firewall Suite Help.

Note

You can fine-tune your LEA connection settings using the `Webtrend.ini` file in the Firewall Suite installation directory. For more information, see the *Firewall Configuration Guide*.

About User-Defined Connections

When you create a user-defined connection, you must manually create a `lea.conf` file to define the connection settings. User-defined connections can only be edited by changing the settings in this file. To troubleshoot user-defined connections, check the `leaservice.log` file in the Firewall Suite installation directory.

To manage Check Point connections:

1. On the Main Console, click **Options** in the Functions area. The Options window opens.
2. In the left-side navigation area, expand the **General Firewall Activity** section and click **LEA Connections**. The LEA Connections dialog box opens.
   - To add a LEA connection, click **New** and provide the required information in the New LEA Connection wizard.
   - To edit a LEA connection, select a connection and click **Edit** , then edit the information in the tabs on the Edit LEA Connection dialog box.

     You cannot edit a user-defined connection. For user-defined connections the **Edit** icon is grayed out.
   - To delete a LEA connection, select a connection and click **Delete**.

Creating a LEA Connection

To create a new LEA connection:

1. On the Main Console, click **Options** in the Functions area. The Options window opens.
2. In the left-side navigation area, expand the **General Firewall Activity** section and click **LEA Connections**. The LEA Connections dialog box opens.
3. Click **New**.
4. The General dialog box opens. In the **Name** text box, type a name that will identify this LEA connection when you select it in the Log Files dialog box. For example, depending on the number and type of firewalls in your configuration, you might use the host name or IP address of the Check Point Management Server, the version of the firewall (4.*x* or NG), or a connection type such as sslca or Unauthenticated.
5. Select the type of Check Point firewall you want to report on and the type of OPSEC LEA connections you want to configure. For more information about Check Point connection types, see the *Firewall Configuration Guide* or the Firewall Suite Help.
6. *If you selected Check Point vNG,* select **sslca**, **clear**, or **user-defined** from the list.

> **Note**
> Select **user-defined** only if you want to create a custom NG connection type by manually configuring the `lea.conf` configuration file, and only if you do not want to use any other connection type in the list. After they are created, user-defined connections cannot be edited using the Firewall Suite user interface. For more information, see “About User-Defined Connections” on page 335

7. To enable or disable the connection, clear or select the **Disable this connection** check box. When a connection is disabled, the WebTrends LEA Service cannot collect Check Point firewall data.

8. Click **Next**. The Location dialog box opens.

9. In the **Directory** text box, browse or type a path to the directory where you want the WebTrends LEA Service to store the Check Point firewall logs it collects. The path must be unique, because you cannot store logs for more than one LEA connection in the same directory.

10. In the **Host IP Address** text box, type the IP address of the computer where the Check Point Management Server is installed.

11. In the **Host Port** text box, type the port number the WebTrends LEA Service should use to communicate with the Check Point firewall. The default port is 18184.

12. Click **Next**.

13. *If you chose* **Check Point v4.x** *or* **Check Point NG with a clear connection** *in Step* **5**, use the **Back**, **Finish**, or **Cancel** button to return to the previous screen, save your connection settings, or cancel your connection settings and return to the LEA Connections dialog box. When you click **Finish**, Firewall Suite attempts to establish the connection.

14. *If you selected any other Check Point NG connection type in Step* **5**, the Type-Specific panel opens. Continue with Step **15**. Depending on the connection type you chose, not all the fields in this panel are enabled. For more information about how to obtain the information you need for the Type-Specific panel, see the *Firewall Configuration Guide* or the Firewall Suite Help.

15. In the **LEA SIC Name** text box, type the DN number for the OPSEC application you created in the Check Point Policy Editor. The DN number can be found under Secure Internal Communication in the OPSEC Application Properties dialog box.

16. In the **Management Server SIC Name** text box, type the DN number for the Check Point Management Server network object. The DN number can be found under Secure Internal Communication in the Object Properties dialog box.

17. In the **Certificate File Name** text box, type the name of the certificate file created using the `opsec_pull_cert` tool. The default name for the certificate file is `opsec.p12`.

18. Use the **Back**, **Finish**, or **Cancel** button to return to the previous screen, save your connection settings, or cancel your connection settings and return to the LEA Connections dialog box. When you click **Finish**, Firewall Suite attempts to establish the connection. To check the status of the connection, see "Check Point LEA Status" on page 338.

Check Point LEA Status

You can check on the status of LEA connections you create using the LEA Connection status dialog box.

To check LEA connection status:

1. Select **LEA Connection Status** from the Tools menu.

2. To monitor the status of a connection, check the Status column. The following table explains the meaning of each connection status.

Uninitialized	Connection information has been saved, but the connection has not yet been established.
Successful	The LEA service connected successfully and collected data with no errors.
Connection Error	An error was generated before, during or after connecting.
Critical Error	The LEA service itself generated an error, causing a connection failure.

3. To determine how much data was transferred, check the Log Size column.

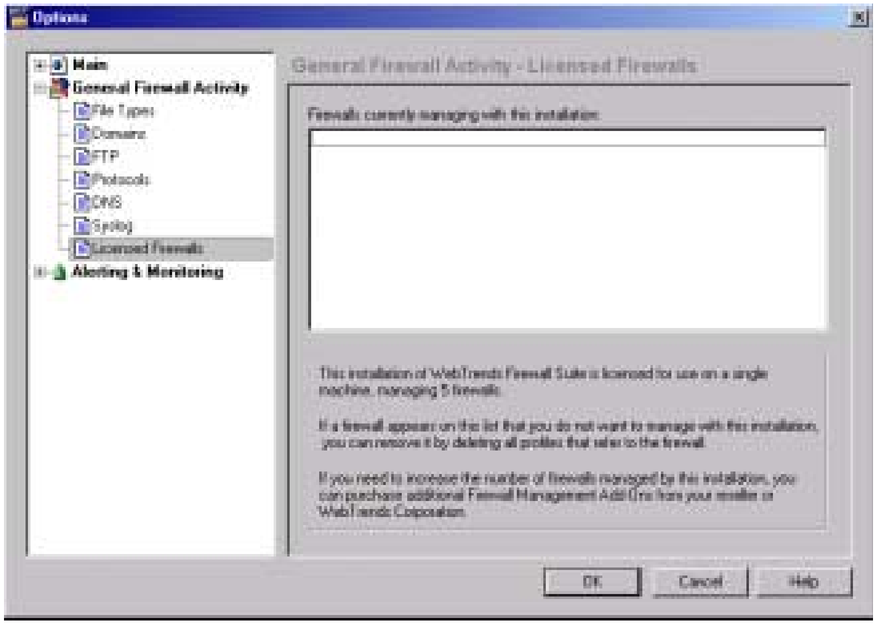
4. To disable a connection, select it in the list and click **Disable**.

5. To create, edit, or delete connections, click **Manage** to open the Manage LEA Connections dialog box.

Licensed Firewalls Dialog Box

The General Firewall Activity - Licensed Firewalls dialog box lists the licensed firewalls that are defined for your system. These licensed firewalls were specified when you created a profile.

The standard software license lets you install your firewall reporting solution on one system and report on one firewall. To report on more than one firewall, you must purchase Firewall Add-Ons. For example, a 3 Firewall Add-On license lets you install Firewall Suite on one system and report on a total of four firewalls. Contact NetIQ Corporation or your reseller to purchase add-ons.



Firewalls currently managing with this installation:

This installation of WebTrends Firewall Suite is licensed for use on a single machine, managing 5 firewalls.

If a firewall appears on this list that you do not want to manage with this installation, you can remove it by deleting all profiles that refer to the firewall.

If you need to increase the number of firewalls managed by this installation, you can purchase additional Firewall Management Add Ons from your reseller or WebTrends Corporation.

To view the list of licensed firewalls:

1. On the Main Console, click **Options** in the Functions area. The Options window opens.
2. In the left-side navigation area, expand the **General Firewall Activity** section and select the **Licensed Firewalls** option. The General Firewall Activity - Licensed Firewalls dialog box opens.
3. Review the list and click **OK** to exit the dialog box.

Cisco PIX Interfaces Dialog Box

The Cisco PIX Interfaces dialog box is used for Cisco PIX v6.2 and later only. Using this dialog box to map interfaces increases the usefulness of reports when the PIX firewall is configured in connection with more than one interface to a device or network. For example, the firewall may use an interface to a VPN device as well as to the network, or it may connect to more than one network. When you define these interfaces in the Cisco PIX Interfaces dialog box, Firewall Suite can parse the device names found in your log files and use them to report more effectively on the direction of traffic through the firewall.

To add or edit an interface:

1. Click **New**, or select an interface name and click **Edit**.
2. In the **Interface Name** text box, type the name of the device or interface as it appears in the log file.
3. Click **OK** to save your changes, or click **Cancel** to abandon them.
4. Click **OK** again to save the list of interfaces and exit the dialog box.

To delete an interface:

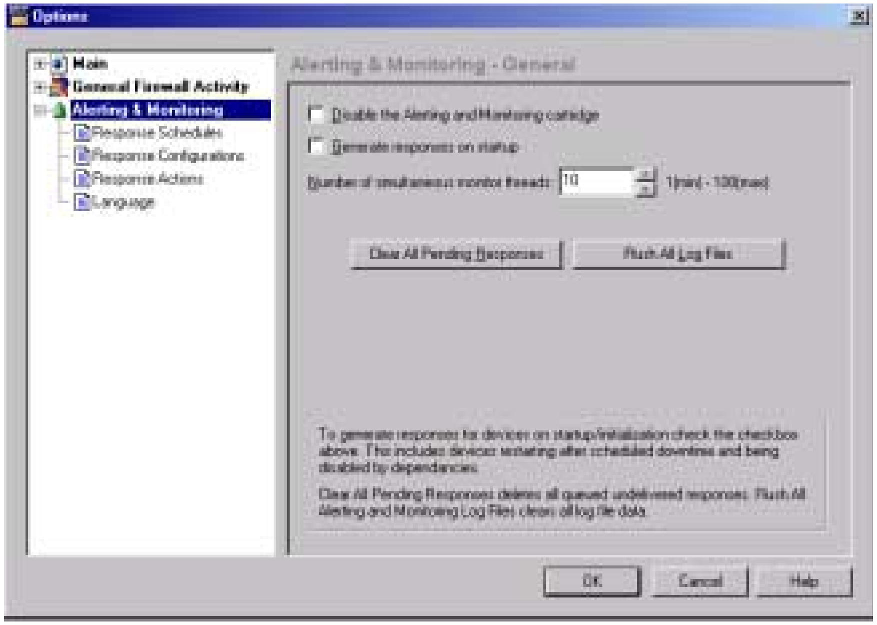
Select the interface in the list and click **Delete**.

Alerting and Monitoring Options

The Alerting and Monitoring options define settings that apply to Alerting and Monitoring profiles and reports, including report language settings and access to response schedules, configurations and actions.

Alerting & Monitoring - General Dialog Box

The General options affect the performance of Alerting and Monitoring. Here you can disable Alerting and Monitoring, reset the alert log, clear alerts, and define the number of threads you need for processing.



□ Disable the Alerting and Monitoring cartridge

□ Generate responses on startup

Number of simultaneous monitor threads: 10 1(min) - 100(max)

To generate responses for devices on startup/initialization check the checkbox above. This includes devices restarting after scheduled downtimes and being disabled by dependancies.

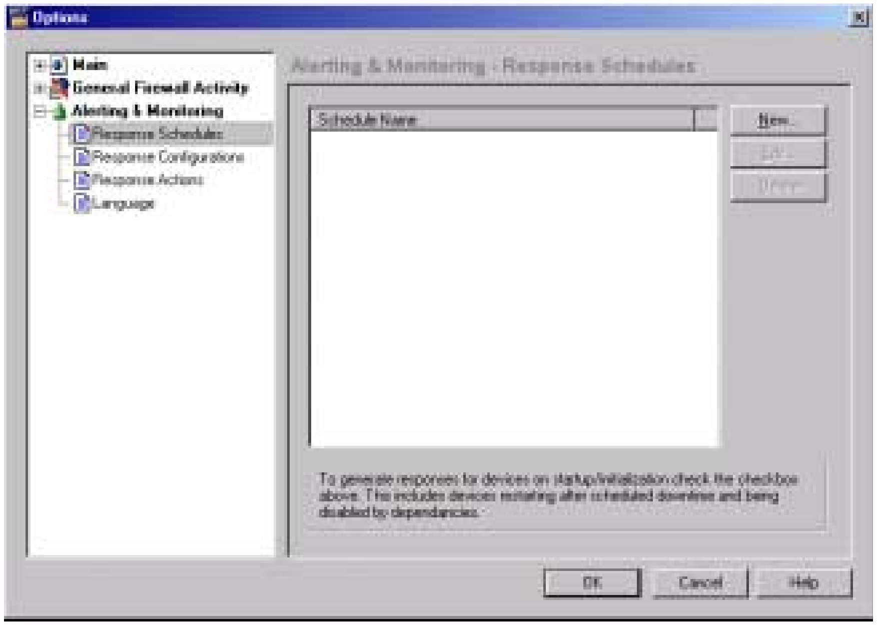
Clear All Pending Responses deletes all queued undelivered responses. Flush All Alerting and Monitoring Log Files clears all log file data.

To set General dialog box options:

1. On the Main Console, click **Options** in the Functions area. The Options window opens.
2. In the left-side navigation area, click **Alerting & Monitoring**. The Alerting & Monitoring - General dialog box opens.
3. Modify any of the following settings:
   - Select **Disable Alerting and Monitoring cartridge** to turn off Alerting and Monitoring. Devices are not monitored when Alerting and Monitoring is disabled.
   - Select **Generate Startup Responses** to send a response if a monitored device is down when Firewall Suite is started.
   - In the **Number of simultaneous monitor threads text box,** type or select the number of devices you will be monitoring. Each thread monitors one device.A maximum of 100 simultaneous threads is allowed.
   - Click **Clear All Pending Alerts** if you need to reset alerts while you are troubleshooting or repairing profile settings.
   - Click **Flush All Log Files** to delete the Alerting and Monitoring log file. If you find that you no longer need to report on the entire log file, and you want to purge the log files to start over, you can do so using this feature.
4. Click **OK** to save your changes.

Response Schedules Dialog Box

The Alerting & Monitoring - Response Schedules dialog box allows you to create, edit, and delete response schedules for the Alerting and Monitoring module. Configuring responses for Alerting and Monitoring profiles is discussed in-depth in “Alerting and Monitoring” on page 103.



To generate responses for devices on startup/initialization check the checkbox above. This includes devices restarting after scheduled downtime and being disabled by dependancies.

To add, edit or delete a response schedule:

1. On the Main Console, click **Options** in the Functions area. The Options window opens.
2. In the left-side navigation area, expand the **Alerting & Monitoring** section and click **Response Schedules**. The Alerting & Monitoring - Response Schedules dialog box opens.

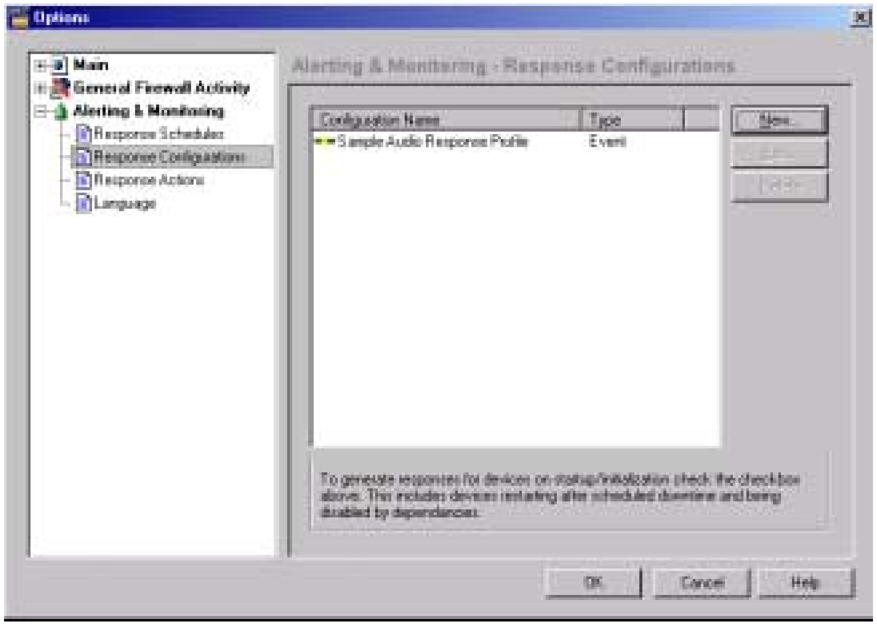
3. Choose one of the following three options:

   - Click **New**. The Edit Response Schedule dialog box opens. For more information, see “Alerting and Monitoring” on page 103.
   - Select a response schedule from the list and click **Edit**. The Response Configuration dialog box opens. For more information, see “Alerting and Monitoring” on page 103.
   - Select a response schedule from the list and click **Delete** to remove the response schedule from the list.

4. Click **OK** to save your changes.

Response Configurations Dialog Box

The Alerting & Monitoring - Response Configurations dialog box allows you to create, edit, and delete response configurations for the Alerting and Monitoring module. Configuring responses for Alerting and Monitoring profiles is discussed in-depth in “Alerting and Monitoring” on page 103.



Configuration Name	Type
Sample Audio Response Profile	Event

To generate responses for devices on startup/initialization check the checkbox above. This includes devices restarting after scheduled downtime and being disabled by dependancies.

To add, edit, or delete a response configuration:

1. On the Main Console, click **Options** in the Functions area. The Options window opens.
2. In the left-side navigation area, expand the **Alerting & Monitoring** section and click **Response Configurations**. The Alerting & Monitoring - Response Configurations dialog box opens.

3. Choose one of the following three options:

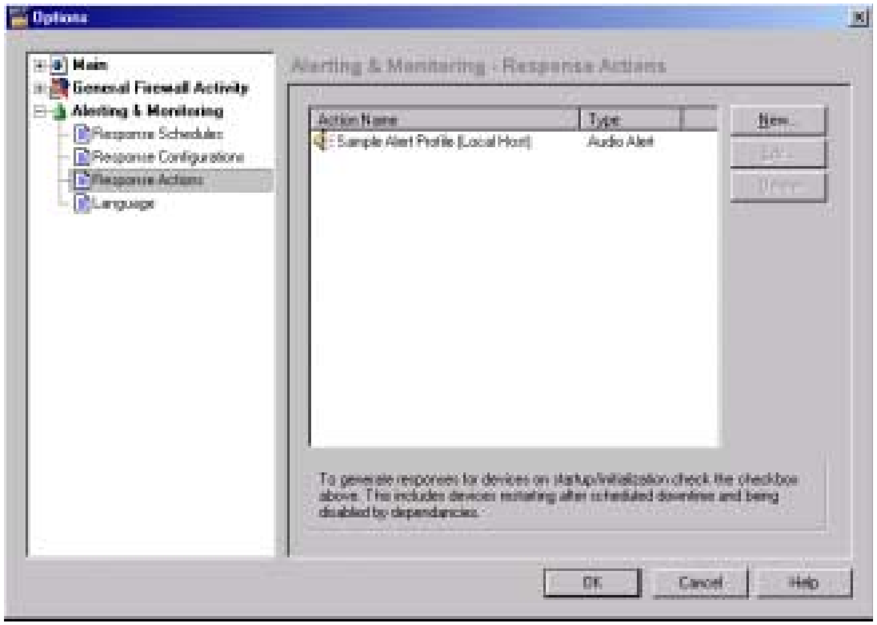
- Click **New**. The Response Configuration Settings dialog box opens. For more information, see “Alerting and Monitoring” on page 103.
- Select a response schedule from the list and click **Edit**. The Response Configuration Settings dialog box opens. For more information, see “Alerting and Monitoring” on page 103.
- Select a response configuration from the list and click **Delete** to remove the response configuration from the list.

4. Click **OK** to save your changes.

Response Actions Dialog Box

– The Alerting & Monitoring - Response Actions dialog box allows you to create, edit, and delete response actions for the Alerting and Monitoring module. Configuring responses for Alerting and Monitoring profiles is discussed in-depth in “Alerting and Monitoring” on page 103.

.



Action Name	Type
Sample Alert Profile (Local Host)	Audio Alert

To generate responses for devices on startup/initialization check the checkbox above. This includes devices restarting after scheduled downtime and being disabled by dependancies.

To create a response action for a response schedule:

1. On the Main Console, click **Options** in the Functions area. The Options window opens.
2. In the left-side navigation area, expand the **Alerting & Monitoring** section and click **Response Actions**. The Alerting & Monitoring - Response Actions dialog box opens.

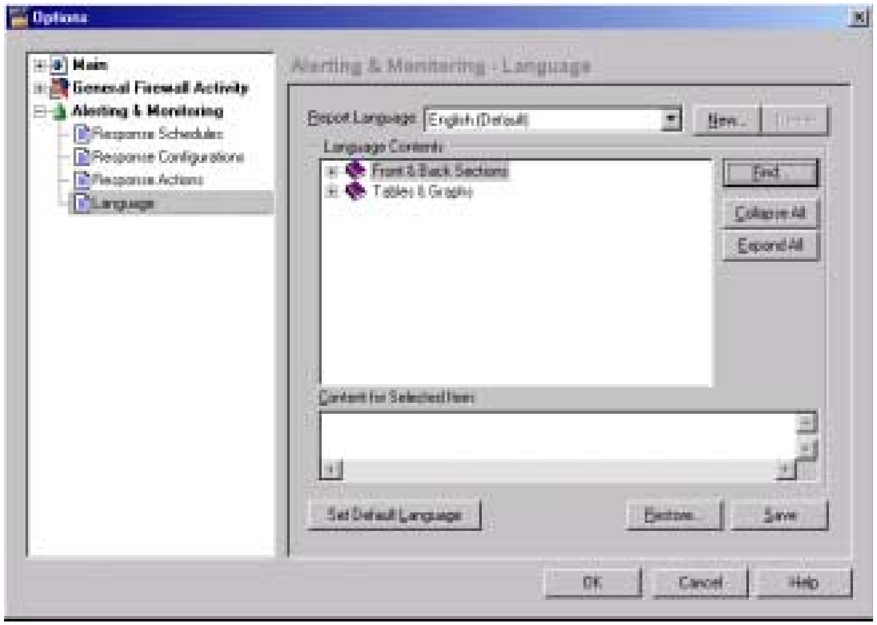
3. Choose one of the following three options:

   - Click **New**. The Edit Response Actions dialog box opens. For more information, see “Alerting and Monitoring” on page 103.
   - Select a response schedule from the list and click **Edit**. The Edit Response Actions dialog box opens. or more information, see “Alerting and Monitoring” on page 103.
   - Select a response action from the list and click **Delete** to remove the response action from the list.

4. Click **OK** to save your changes.

Language Dialog Box

Use the **Language** dialog box to define your own text to use in alerting and monitoring reports.The Language options for Firewall and Proxy Server reports are available in the Main - Language options. For more information, see “Language Dialog Box” on page 310.



Report Language: English (Default)

To set language options:

1. On the Main Console, click **Options** in the Functions area. The Options window opens.
2. In the left-side navigation area, expand the **Alerting & Monitoring** section and click **Language**. The Alerting & Monitoring - Language dialog box opens.

3. Under **Report Language**, *s*elect an existing language to modify from the dropdown list, or click **New** to open the Add New Report Language dialog box and specify a new language name.

4. Under **Language Contents**, you see a tree of the report sections and corresponding text areas.

   – Click **Collapse All** to close all of the books and view only the first directories of the selected language tree.

   – Click **Expand All** to open all subdirectories and view the entire tree.

   – Click **Find** to access the Find/Replace dialog box where you can search for text that appears in reports and replace it with your own text.

5. **Under Content for Selected Item**, selecting a report text area in the Report Items section displays the text in the Content section. Do one of the following:

   – Edit the text in this field and click **Save**.

   – Click **Restore** to revert to a previously saved version of text for the selected Report Item or the entire Report Language.

   – Select a language and click **Set Default Language** to define the default language to use for all new reports.

6. Click **OK** to save your changes.

Appendix A

Specifying Log Paths

Formatting Log File Path Entries

If you are having trouble specifying your log file location, the examples in this section may help.

Standard Examples

This path:	Specifies
`c:\logs\ex20000224.log`	a local file location.
`ftp.domain.com/logs/ex20000224.log`	a path to an FTP server.
`www.domain.com/logs/ex20000224.log`	an HTTP log file path.

Compressed Logs

This path:	Specifies
`c:\logs\ex20000224.zip`	the zipped log `ex20020224.zip`
`ftp.isp.com/logs/ex20000224.gz`	the compressed log `ex20020224.gz`, located in the `log` directory on the `isp.com` FTP server.

Wildcards

When you specify multiple files, use asterisks or question marks as wildcards in the file name only when using the `file:///`, `ftp://`, and `http://` retrieval methods. Do not use wildcards in the rest of the path when specifying ftp or http access. For example, type one of the following:

```
c:\logfiles\server 10\ex*.log
```

```
c:\logfiles\server20\ex200002*.log
```

```
c:\logfiles\server30\ex2000022?.log
```

You can use wildcards in the file name itself when you specify `file:///` retrieval method only. For example, type one of the following:

```
c:\logfiles\server??\ex20000224.log
```

```
c:\logfiles\*\*.log
```

You can also use a vertical bar (`|`) to separate entries. For example, type one of the following:

```
c:\logfiles\server 10\ex20000224.log|lex20000225.log
```

```
c:\logfiles\server10\*.log|\server20\*.log
```

```
c:\logfiles\*\20000224.log|d:\logfiles\*\20000224.log
```

Date Macros

Note
Date macros are case sensitive. For example, `%Mon%` returns Jan, `mon` returns jan, and `MON` returns JAN

The following table shows the information returned by date macros.

This date macro	Returns the following dates:
`%dd%`	Day
`%mm%`	Month (2-digit)
`%Mon%`	Month (Abbr)
`%yy%`	Year (2-digit)
`%YYYY%`	Year (4-digit)
`%Date-n%`	Subtract *n* days from the current system date
`%Date+n%`	Add *n* days to the current system date
`%mm-n%`	Subtract *n* days from the current system date
`%mm+n%`	Subtract *n* days from the current system date
`%yy-n%`	Subtract *n* days from the current system year
`%yy+n%`	Add *n* years to the current system year
`%yyyy-n%`	Subtract *n* years from the current system date
`%yyyy+n%`	Add *n* years to the current system date
`%dy%`	Day of year
`%wy%`	Week of year

This date macro	Returns the following dates:
%wm%	Week of month
%dw%	Day of week
%dm%	Day of month

Date Macro Examples

The following examples use 02/24/2000 as the current system date.

This macro:	Specifies this path
c:\winnt\system32\logfiles\ex%yyyy%%mm%%dd%.log	c:\winnt\system32\logfiles\ex20000224.log
c:\winnt\system32\logfiles\ex%yyyy%%mm%*.log	c:\winnt\system32\logfiles\ex200002*.log
c:\winnt\system32\logfiles\ex%Date-5%%yyyy%%mm%%dd%.log	c:\winnt\system32\logfiles\ex20000219.log
c:\winnt\system32\logfiles\access-%Mon%/%dd%/%yyyy%.log	c:\winnt\system32\logfiles\access-Feb/24/2000.log

IP Addresses

The following table shows how to specify ranges of IP addresses.

This IP address	Specifies
255.*	An entire Class A subnet
255.255.*	An entire Class B subnet
255.255.*	An entire Class C subnet

This IP address	Specifies
206.13.01.0/28	A classless subnet in CIDR format (where /28 indicates the number of bits used to identify the network)
206.13.01.0/26	Addresses 0–63 of a Class C address space that is divided into four subnets
206.13.01.64/26	Addresses 64–127 of a Class C address space that is divided into four subnets
206.13.01.128/26	Addresses 128–191 of a Class C address space that is divided into four subnets
206.13.01.192/26	Addresses 192–255 of a Class C address space that is divided into four subnets
206.13.01.0/25	Addresses 0–127 of a Class C address space that is divided into two subnets
206.13.01.128/25	Addresses 128–255 of a Class C address space that is divided into two subnets

Performance

A number of factors can affect how Firewall Suite performs. You can modify many of these options to suit your environment.

Using Filters to Optimize Performance

To maximize performance on your system and to create reports that focus on just the data you're interested in, consider adding a filter to your profiles. For more information, see "Filtering for Focused Reports" on page 157.

Running Reports Without DNS Lookup

Domain Name System (DNS) lookups translate the numeric IP address into a domain name. Most users consider domain names more useful for analysis than IP addresses, but DNS lookup (or *DNS resolution*) can be a slow process.

DNS lookups can be done either by the firewall or proxy server or by Firewall Suite when analyzing the log file. However, DNS lookups are performed more efficiently by the firewall or proxy server as the log is created—if this server option is available to you, you can optimize processing by using it.

If numeric IP addresses are adequate for your needs, do not do DNS lookups at all. Disable DNS lookups in the firewall or proxy server and use Quick mode for DNS lookups in Firewall Suite. For more information, see “Internet Resolution Dialog Box” on page 45.

Activating FastTrends

The FastTrends feature lets you collect data for the current profile in a database so that future reports can be generated more quickly.

To turn on FastTrends:

1. On the Main Console, select the profile for which you want to activate FastTrends.
2. Click **Edit** to display the Edit Profile dialog box.
3. Select the **Database and Real-Time** tab.
4. Select the **FastTrends database** check box.

For more information, see “Database and Real-Time Dialog Box” on page 72.

Accessing the Log File

The fastest way to access the log file for a site is through file retrieval. If you can access the log file locally, your analysis is quicker than it is when the log file is retrieved via HTTP or FTP.

Selecting the Report Type

HTML document reports are the fastest to create. All other report types (such as Microsoft Word or Excel) are based on this HTML report.

Alerting and Monitoring creates only HTML reports.

For firewall profiles, see “Memorized Report Settings” on page 203.

Zipping Archived Log Files

Firewall Suite can report on zipped log files, allowing you to save system space. Zip your archived log files using a tool such as WinZip or PKUnzip.

Appendix B
Silent Installation

Warning
An unattended or “silent” installation is for advanced users only. Do not attempt this procedure if you are unfamiliar with Firewall Suite or your network.

Disk Space

Make sure to check for available disk space. You will receive a warning message when 200 MB of disk space are left. The silent installation will abort at 50 MB.

Licensing Issues

Silent installations do not handle licensing for Firewall Suite. To add a license to these products, use the command-line executable wtlicense.exe.

Silent Installation for Windows NT, Windows 2000, and Windows XP

While some of the parameters described below are optional, others are required. Pay attention to the order as well as the case of the commands. Failure to follow the required order or use the correct case will cause problems with your Firewall Suite installation.

To run a silent installation:

Run the setup program with the following syntax:

`setup.exe /S` = Silent Install

`/NOSAMPLES` = No Sample Profiles

`/I` = destination path

Notes:
The parameters must be given in the order presented

The parameter `/DESTINATION` does not include quotes.

Installing as Administrator

To run a silent installation as administrator:

Run the setup program using the following syntax:

```
setup.exe /S /IDESTINATION=installation destination path
```

Please note the following:

Notes:
The parameters must be given in the order presented

The parameter `/DESTINATION` does not include quotes.

If you do not want to install sample files, you can use the /NOSAMPLES parameter with the following syntax:

```
setup.exe /S /NOSAMPLES /IDESTINATION=installation destination path.
```

Glossary

authentication Technique by which access to Internet or intranet resources requires users to identify themselves using a name and password.

bandwidth Measure (in kilobytes of data transferred) of the traffic on the site.

browser A program used to locate and view HTML documents (Netscape Navigator, Mosaic, Microsoft Explorer, for example).

category A category is a predefined grouping of URLs that have a common theme, such as Shopping, Games, and Personals/Dating.

client The browser used by a visitor to a Web site.

client error An error occurring due to an invalid request by the visitor's browser. Client errors are in the 400-range. See **Return Code**.

company database The proprietary database used by Firewall Suite to look up the company name, city, state, and country corresponding to a specific domain name.

connection A record of any protocol activity as recorded in the firewall logs. A unique user is determined by the IP address or domain name. Connection only applies to general profile reports. For example, for an ftp file download, both the request and the download are considered a single connection. An http connection would correspond to a single hit.

Core categories A set of URL categories that may present liability concerns, such as sex or gambling sites.

critical event In Firewall Suite reports, a firewall event that meets the following criteria:

- Gauntlet: The event is logged as a “security alert.”
- Check Point: The event is logged as “rejected.”
- Raptor: The event has an error code of 500 or greater.

domain name The text name corresponding to the numeric IP address of a computer on the Internet, for example www.webtrends.com.

Domain Name System (DNS) lookup The process of converting an numeric IP address into a text name. For example, 204.245.240.194 is converted to www.webtrends.com.

event A firewall activity recorded in a line of the firewall log file is usually referred to as a firewall event. A log analysis and reporting job in the Scheduler is also called an event. It is usually referred to as a scheduled event.

FastTrends database This patent-pending technology makes it possible to store the results of the log file analysis in a database to significantly speed future reports based on the same profile.

filter A means of narrowing the scope of a report by specifying the log file data that you want to include or exclude in a profile.

FTP Acronym for File Transfer Protocol, which is the way that most files are sent between computers over the Internet.

General Firewall Activity reporting A type of analysis that lets you analyze and report on general Web statistics, potential attacks on the firewall, and protocol usage.

home page The main page of a Web site. The home page usually provides visitors with an overview and links to the rest of the site. It often contains or links to a **table of contents for the site.**

HTTP Hyper Text Transfer Protocol, a standard method of transferring data between a Web server and a Web browser.

incoming activity In Firewall Suite, activity initiated on outside of the firewall, coming through the firewall, is considered incoming activity.

IP address An Internet Protocol address identifying a computer connected to the Internet.

IP spoofing An attack on a network that uses false IP addresses to imitate users with access rights.

Language Editor A Firewall Suite feature that lets you change the language available for reports. You can also create your own “language” by modifying the text that appears in Firewall Suite reports.

OPSEC LEA Check Point’s OPSEC Log Export API, a proprietary method of logging firewall data.

outgoing activity Any activity that is initiated behind the firewall and then goes through the firewall.

ping of death An attack executed by using an illegally large TCP/IP ping packet to halt a target computer by breaking down its buffers.

platform The operating system used by a visitor to a Web site.

profile A collection of settings used by Firewall Suite to create reports. A profile defines how to access the log file and where the log file resides. It also sets up IP resolution, filters, IP addresses behind the firewall, and, in the case of Incoming Web Activity profiles, the Web site’s home page. All reports are based on profiles.

Productivity categories A set of URL categories that may have a negative impact on an employee productivity but do not pose a legal risk to employers.

Protocol A set of rules used to send data over the Internet. Some common protocols are HTTP, FTP, and SMTP.

RealAudio An Internet sound technology developed by RealNetworks. Because RealAudio requires a great deal of bandwidth, many firewalls block RealAudio activity.

real-time analysis A technique that lets Firewall Suite continuously collect data in the background to speed up the creation of future reports based on the same log file.

referrer URL of an HTML page that refers to your Web site.

report A document created by Firewall Suite that presents the results of the log file analysis through tables and graphs. All reports are based on profiles.

report range The time range of the log file that you want to report on.

return code The return status of a transfer request which specifies whether the transfer was successful and why.

Rules A set of specifications configured on the firewall. Rules determine what users on the inside can do and where they can go, and what type of activity is allowed to come through the firewall from the outside.

SMTP Simple Mail Transfer Protocol, a protocol used by Internet mail programs such as Eudora and Netscape.

Style Editor A Firewall Suite feature that allows you to define the colors, fonts, and table and page layouts for HTML reports.

SYN flood An attack that bombards the firewall with requests to synchronize TCP connections, which causes the firewall to allocate all available buffer space to these requests. The firewall is then unable to accept any legitimate connections.

Sync Storm See Syn Flood.

TCP/IP Transmission Control Protocol/ Internet Protocol, a required Internet protocol.

Tunneling Using the Internet to create a private secure network.

UDP User Datagram Protocol, a protocol that can substitute for the TCP part of TCP/IP. Although UDP does not provide all the data that TCP does, it does provide port numbers to differentiate requests and can verify data arrival.

URL Uniform Resource Locator, a means of identifying an exact location on the Internet.

URL categorization A Firewall Suite feature that categorizes sites visited by their content.

URL database A database of URLs indexed by category.

User session A session of Web activity (all hits) as recorded in the firewall logs, including both FTP and HTTP activity. A unique user is determined by the IP address or domain name. By default, a user session is terminated when a user falls inactive for more than 30 minutes. User sessions only apply to incoming and outgoing profile reports.

VPN Virtual Private Network. A VPN uses the Internet to establish a secure connection using tunneling and data encryption.

Warning A firewall event that meets the following criteria:

- Gauntlet: The event is not logged as “security alert.”
- Check Point: The event is logged as “dropped.”
- Raptor: The event is logged with a code between 200–499.

Wildcard A symbol or combination of symbols that stands for a range of characters. In Firewall Suite, you can use wildcards to specify log file paths, URLs, filter entries, and the Save/As path for reports.

Index