Evaluation Guide

Security Reporting Center

June 15, 2006

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.

© 2006 MARSHAL LIMITED, ALL RIGHTS RESERVED.

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

About This Book and the Library

The Evaluation Guide for Security Reporting Center provides a hands-on introduction to the Marshal Security Reporting Center product (Security Reporting Center). This book includes instructions to help you install Security Reporting Center and evaluate the primary features and benefits.

Intended Audience

This book provides information for individuals responsible for evaluating and reviewing Security Reporting Center. It explains how to use Security Reporting Center to assess activity around your firewall and generate reports containing valuable information about security on your network.

Other Information in the Library

The library provides the following information resources:

User Guide

Provides conceptual information about Security Reporting Center. This book also provides an overview of the Security Reporting Center user interface and the Help.

Firewall Configuration Guide

Explains how to configure each supported firewall, proxy server, or security device to work with Security Reporting Center.

Help

Provides context-sensitive information and step-by-step guidance for common tasks as well as conceptual background on using Security Reporting Center.

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 SMTP, MailMarshal 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 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 website. If you cannot contact your partner, please contact our Technical Support team.

Telephone: +44 (0) 1256 848 080 (EMEA)
+1 404 459 2890 (Americas)
+ 64 9 984 5700 (Asia-Pacific)

Sales Email: info@marshal.com

Support: www.marshal.com/support

Website: www.marshal.com

Chapter 1
Introduction

Given the volume and diversity of activity on networks today, firewalls, proxy servers, and security devices are increasingly essential to business operations. You are probably familiar with the simple security functions of a firewall. But not everyone knows that firewall logs contain a wealth of information about the traffic that flows through firewalls and proxy servers from both sides. Your logs contain vital data about activity on your network, for example:

- Who is trying to break into your network
- Who is sending information outside the network
- When maximum Web, FTP, and email activity take place
- Who is downloading information from the Internet

Unfortunately, most of this data cannot be read efficiently from the logs due to its volume and complexity. Most firewall vendors do not provide tools to help you decode log data. A firewall log in a large network can easily generate several hundred megabytes of log file data per day. A given log file may contain billions of records.

Security Reporting Center decodes the information in your firewall logs, transforming unwieldy log entries into valuable reports that give a detailed picture of network activity and the state of security. Security Reporting Center provides more than 200 readable, browser-based report pages showing information about data such as the following:

- security events
- bandwidth usage and cost
- protocol activity
- most active users
- proxy cache status
- Web content accessed by users inside the firewall.

Security Reporting Center can help you understand security & bandwidth baselines, forecast and plan for firewall and bandwidth requirements, summarize critical and non-critical events on your network, manage employee Internet usage, and assess the activity that passes through your firewall.

What Is Security Reporting Center?

Security Reporting Center is a reporting tool that provides security consultants, corporate security teams, IT departments, and system administrators with detailed analyses of firewall, proxy server, and security device log files. The scalable, browser-based reporting architecture makes it suitable for deployment in small networks as well as networks with large numbers of firewalls. You can install Reporting agents on multiple computers and on both Windows and Solaris platforms for efficient processing. A central administration console, accessible from any computer with a browser, controls configuration, report scheduling and report generation. This console provides secure access to reports and configuration through a multi-level system of user permissions.

These features work together to make Security Reporting Center a powerful, flexible, highly customizable application with the following capabilities:

- Provides detailed reports wherever and whenever you want them
- Handles logs of any size and many types
- Tracks multiple firewalls and devices through one convenient interface
- Accommodates thousands of users securely

What Does Security Reporting Center Analyze?

Security Reporting Center analyzes the log data generated by more than 35 firewalls, proxy servers, and security devices, including the following:

- Arkoon Firewall
- Aventail Extranet Center
- AXENT Raptor Firewall
- 3Com Firewalls
- BorderWare Firewall Server
- Check Point VPN-1/FireWall-1
- CimTrak Web Security Edition
- Cisco IOS for the NetIQ Syslog Service
- Cisco PIX Firewall
- Clavister Firewall
- CyberGuard Firewall
- Fortinet FortiGate
- Gauntlet Firewall for UNIX
- Gauntlet Firewall for Windows NT
- Inktomi Traffic Server
- Lucent Managed Firewall
- Microsoft Proxy Server
- Microsoft ISA Server 2000
- Neoteris IVE
- Netasq Firewall
- Netscape Proxy Server

- Netscreen Firewall
- Netopia S9500 Security Appliance
- Network Appliance NetCache
- Network-1 CyberwallPLUS
- Novell BorderManager
- Recourse ManHunt
- RapidStream Firewall
- Secure Computing Sidewinder
- SecureSoft SUHOSHIN
- SonicWALL Internet Security Appliance
- Squid Internet Object Cache
- Sun Microsystems SunScreen
- Symantec Enterprise Firewall
- TopLayer AppSwitch
- WatchGuard Firewall

Support is not limited to these firewalls. Many firewall manufacturers, including some in the preceding list, voluntarily use logs that meet the WebTrends Enhanced Logging Format (WELF) standard. The WELF standard was originally created by WebTrends (the legacy developer of Ssecurity Reporting Center) to produce logs that can be easily mined for information. This standard ensures that logs are fully readable by Security Reporting Center, or can be converted to WELF using a simple script provided by the manufacturer.

What Does Security Reporting Center Report?

Security Reporting Center provides specialized reporting modules that assess important security and productivity concerns. The Firewall Reporting module generates reports focused on security and incoming and outgoing activity around the firewall. The Proxy Reporting module generates reports focused on employee Web and FTP usage.

Firewall Report Content

Security Reporting Center provides the following standard report chapters in a complete Firewall report:

Summary
Provides an overview of the data in all report chapters.

Firewall Management
Contains reports about the firewall rules that were triggered and which internal and external clients and servers were responsible for triggering them.

Bandwidth
Contains reports about the volume and cost of incoming and outgoing bandwidth, categorized by incoming and outgoing traffic, as well as the top users of bandwidth.

Security
Contains reports about remote management events, critical events, informational events, and warnings on the firewall.

VPN
Contains report about VPN usage, clients, and events.

Web
Contains reports about Web usage, including client and server hits and traffic by department.

Email
Contains reports about email usage, including client and server hits and traffic by department.

FTP
Contains reports about FTP usage, including client and server hits and traffic by department.

Telnet
Contains reports about Telnet usage, including internal and external client and server hits and traffic by department.

Internal

Contains reports about outgoing traffic and security, including critical events and outgoing protocol usage by client.

External

Contains reports about incoming traffic and security, including critical events and incoming protocol usage by client.

Departments

Contains reports about activity broken down by organizational department (such as Accounting or Development) and protocol.

Servers

Contains reports about hits to internal and external servers.

Proxy Report Content

Security Reporting Center provides the following standard report chapters in a complete Proxy report:

General Statistics

Provides an overview of the data in all report chapters.

Visited Sites

Contains reports about the Web and FTP sites most often visited by users on your network, categorized by user and authenticated user.

Pages and Files

Contains reports about the most frequently viewed pages, the most frequently viewed files and file types, and the most popular file downloads accessed by users on your network.

Users

Contains reports about the most active users on your network and the sites they visited most often.

URL Core Category

Contains reports about visits by users on your network to Web and FTP sites with potentially sensitive content, such as sexually explicit material or gambling.

URL General Category

Contains reports about internal users' visits to Web and FTP sites containing content that detracts from employee productivity, such as shopping and chat sites.

Demographics

Contains reports about the top-level domains and countries accessed by users on your network.

Activity

Contains reports about hits, visits, and bandwidth usage over time by users on your network.

Technical Statistics

Contains reports about proxy cache status and errors logged to clients and servers.

Browsers & Platforms

Contains reports about the browsers and platforms used to access the proxy server, as well as the search engines and terms used to find content on the Internet.

What Does Security Reporting Center Provide?

Security Reporting Center provides a central reporting and configuration console accessible from any browser, a multi-layered system of permissions, and customizable reports deliverable as on-demand interactive HTML, as static HTML documents, or as Microsoft Word documents. Security Reporting Center provides the information you need to manage security on your network in a form that is easily accessible, secure, customizable, and highly readable. Security Reporting Center provides the following types of information:

- Security baseline reports that identify vulnerabilities on your network.
- State-of-security reports that identify attempts to breach your firewall.
- Network bandwidth reports that show how your system resources are used ad the associated costs.

- Protocol-specific reports that indicate how much of your bandwidth is consumed by Web, email, and FTP traffic.
- Department-focused reports that tell you which users and departments are responsible for large amounts of traffic.
- Outgoing Web traffic reports that identify the most popular sites, page hits, and downloads in your company.
- URL categorization reports that show when company employees access sites with sensitive or non-business-related content on the Internet.

How Security Reporting Center Helps You

Using Security Reporting Center, your organization can benefit from reduced security risks, better overhead planning and network resources management, and improved network usage policy enforcement. Security Reporting Center provides the following key benefits:

- Protect company assets by tracking security.
- Baseline and predict Internet resource needs.
- Encourage productive Web usage with URL categorization.
- Distribute security data safely and efficiently.
- Manage any size network and most types of firewall installations.

Protect Company Assets by Tracking Security

Your firewall appears to be protecting your data, but you also need to know how hard it is working and how often your data is threatened? To manage security, you should be able to quantify the risks to your network, how your firewall is responding, and whether your security needs have changed over time.

Security Reporting Center provides high-level summary reports as well as detailed event-by-event analysis. You can view the security events on your firewall by hour, day, week, month, or year. Find out when firewall and VPN events occur, which client connections experience critical, warning, and informational events, and what percentage of each type of event occurs during a specified time period.

Baseline and Predict Internet Resource Needs

To manage network resources effectively and plan for future upgrades, you need to know the answers to questions like these ones:

- Which users, departments, and groups use the most resources?
- How much bandwidth does email consume?
- How much does it cost to provide bandwidth for email and Web usage?

Productive companies ensure the Internet is used to maximize company effort. The Firewall Reporting module offers a big-picture view of activity on your network that helps you identify times and places where network traffic is especially high. Detailed statistics categorized by user, department, protocol family, and traffic direction can help you decide whether particular users and groups are using the Internet inappropriately. Firewall reports also calculate the cost of bandwidth consumed, providing you with hard data about costs that you can use to justify upgrades to the network.

For example, Security Reporting Center reports make it simple to find out whether a sharp increase in bandwidth usage is due to increased email usage from Marketing. If the increase is the result of a new email campaign, bandwidth cost reports let you know how much the extra traffic is costing the company. If the increase comes from a single user, the Top Internal Addresses report identifies the source. You have clear evidence for addressing any suspected Internet usage policy violations.

Encourage Productive Web Usage with URL Categorization

The World Wide Web is a powerful business tool, but making sure it is used appropriately is a challenge. How can you find out whether your employees are using the vast range of content on the World Wide Web in ways that maximize productivity and minimize legal issues? The Security Reporting Center Proxy Reporting module addresses both these issues. Proxy reporting analyzes your proxy server logs to deliver comprehensive and detailed reports about both Web activity and the actual content users on your network access.

Proxy reporting categorizes Web traffic in order to provide you with lists of top users, top sites and pages accessed, and top files downloaded. It also offers powerful URL categorization functionality to give you insight into the actual content users are viewing. Security Reporting Center matches the URLs users request against comprehensive URL categorization databases, which identify Internet URLs that may expose the organization to legal liability, detract from employee productivity, and waste bandwidth. You can report as much or as little of this data as you prefer by creating your own URL categories.

Make Security Data Secure and Highly Accessible

Insightful report content is useless unless you can get reports on demand and distribute them efficiently to the people who need the information. You may need to show customers that the network is secure, convince remote managers to approve a hardware purchase, and give Human Resources on-demand access to Web-surfing statistics. Perhaps you need to email a summary report to your manager weekly, and Information Services needs up-to-the-minute firewall analysis in several locations. Security Reporting Center supports all of these requirements with its convenient browser-based architecture, scheduled reporting capability, and custom static report configuration.

On-demand HTML report access is available from any browser on the network. On-demand reports always contain the latest data and are fully interactive, including automatic translation into French, Spanish, and German. When a printed report is more appropriate, or when you want to distribute an HTML report without providing any application access, Security Reporting Center can save or email static reports in HTML or Microsoft Word format. All reports can run on a schedule or as a one-time custom event. You can format reports with any headers and images you specify. Security Reporting Center provides multiple levels of user rights to ensure that report users have exactly as much access to the application as you want.

Manage Any Size Network and Most Firewall Installations

Because networks vary in size and structure, each one has unique security requirements served by different firewall types and configurations. Whether you maintain one firewall or a hundred, Security Reporting Center can meet your reporting needs. Security Reporting Center can analyze more than 35 firewall log formats, including single firewalls or firewall clusters. A single installation can provide reports for any number of different firewalls and log formats. Just purchase additional licenses to create reports for more firewalls of any type. Security Reporting Center also offers a built-in syslog server and a Check Point LEA service for enhanced log data retrieval. For more information about how Security Reporting Center handles your firewall logs, see the *Firewall Configuration Guide*.

Large or multiple logs may require extra resources and database storage. Because you can install Security Reporting Center on multiple computers in a distributed environment, you can scale your installation to the requirements of the network by adding databases and analysis agents on additional computers. You can also give access to unlimited numbers of users and groups. However large it is, you can still manage your installation using a single central reporting and configuration console.

You can install Security Reporting Center on Microsoft Windows and Sun Solaris computers.

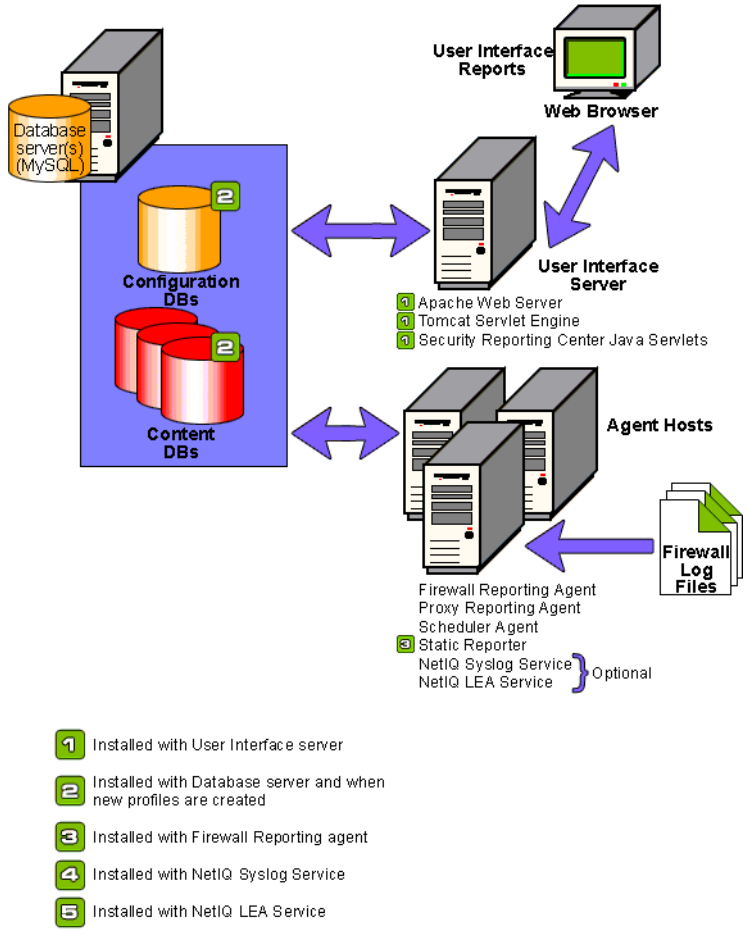
How Security Reporting Center Works

Security Reporting Center consists of the following core components, which can be installed on both Microsoft Windows and Sun Solaris computers:

- One or more Database servers built on MySQL. Each Database server stores information about scheduling and configuration as well as report content.
- A modular, browser-based user interface built on Apache Web server, which users access from any computer in the network.
- One or more Firewall Reporting agents. These agents analyze logs to produce Firewall reports.
- One or more Proxy Reporting agents. These agents analyze logs to produce Proxy reports.

Based on the information you provide about the firewall and the reporting schedule, the reporting agents collect the requested data from the log file and transfer it in compact form to an interim database. The data is then converted to report-ready format and exported to a permanent Content database, where the data can be quickly rendered into a report in HTML or Microsoft Word format when requested.

The following diagram illustrates the Security Reporting Center architecture:



Understanding the Evaluation Process

The remaining chapters in this book guide you through installing and evaluating Security Reporting Center. Following the steps in this book, you can quickly install Security Reporting Center and begin analyzing your own firewall log files.

When you complete this process, you should understand how to use Security Reporting Center to generate reports about firewall and Web activity on your network based on the data in your firewall or proxy server logs. You should also be familiar with many of the significant benefits Security Reporting Center can offer you and your organization.

Chapter 2
Installing Security Reporting Center

This chapter describes how to quickly install Security Reporting Center. For evaluation purposes, you should install all the components on a single computer.

System Requirements

Install Security Reporting Center using the requirements shown in the following tables.

Windows Requirements

Component	Minimum Requirements
Processor	Pentium III or higher **Recommended:** dual Pentium IV for typical installations
Disk Space	1GB free disk space. **Recommended:** SCSI
RAM	512 MB **Recommended:** 1 GB for typical installations
Operating System	Microsoft Windows 2000, Windows XP, and Windows 2003 Server
Database Application	MySQL

Solaris Requirements

Component	Minimum Requirements
Processor	**Single UltraSparc II** **Recommended:** Dual UltraSparc III for typical installations
Disk Space	1GB free disk space. **Recommended:** SCSI
RAM	512 MB **Recommended:** 1 GB for typical installations
Operating System	Sun Solaris 8 and 9
Database Application	MySQL

Browser Requirements

Security Reporting Center supports the following browsers on a Windows computer for accessing the java-based user interface as well as on-demand and

static HTML reports: Microsoft Internet Explorer 5.*x* or higher, or Netscape 6.*x* or higher. Netscape 6.0 is not supported.

Reports rely on Java, which is installed with most browsers. However, Java support is not included by default when installing Netscape 6.1. If you use Netscape 6.1, make sure you also install Java.

Installation Procedures for Windows

The following steps describe how to quickly install Security Reporting Center on Windows computers.

To install Security Reporting Center on a Windows computer:

1. Insert the CD-ROM in the CD-ROM drive.
2. Click **Install**.
3. Click **Next**.
4. To accept the terms of the license agreement, click **I accept the terms in the license agreement**, and then click **Next**.

> **Note**
> If you do not accept the terms of the license agreement, you cannot install Security Reporting Center.

5. Click **Next** to install all the components of Security Reporting Center in the default directory on this computer.
6. In the **Server** text box, use the auto-populated host name for the current computer.
7. In the **Port Number** text box, use the default port number, 3306. This port is used to communicate with the database.
8. In the **Username** text box, type a user name for your database. The user name you type in this dialog box is used internally to contact the database.

9. In the **Password** text box, type a password.
10. In the **Confirm Password** text box, type the password again.
11. Click **Next** to continue.
12. In the **Host Name** text box, use the auto-populated host name for the current computer.
13. In the **Port Number** text box, use the default port number, 9000. This port is used to communicate with the user interface.
14. In the **Login Name** text box, type the user name you will use to log in to the Security Reporting Center application.
15. In the **Password** text box, type a password for the user name.
16. In the **Confirm Password** text box, type the password again.
17. .Click **Next** to continue.
18. Click **Install** to begin installing the Security Reporting Center software. The installation may take several minutes.
19. Click **Finish** to exit the InstallShield Wizard.

Installation Procedures: Sun Solaris

The following steps describe how to quickly install Security Reporting Center on Solaris computers.Solaris installations require you to execute an installation script. Because all the installed services for Security Reporting Center will run under the same user account you are using when you run the script, you should switch to the appropriate user account before you begin installation.

Notes

Do not install Security Reporting Center as the root user.

To install Security Reporting Center, the installation user must have full rights to the installation directory

To install the NetIQ Syslog Service on a Solaris computer, you must first disable the Solaris syslog daemon.

To install Security Reporting Center on a Solaris computer:

1. Make sure you are logged in with the user account you want Security Reporting Center to run under.
2. From the Security Reporting Center CD-ROM, move one of the two compressed TAR files (`frs-solaris.sparc.tar.gz` and `frs-solaris.sparc.tar.z`) to a local directory, uncompress it, and unTAR it. This process creates a directory called `src-2.0`.
3. At a command prompt, type `install.src` to run the installation script.
4. Press **Enter** to install Security Reporting Center as the current user.
5. Press **Enter** to view the license agreement. You must read and accept the license agreement to continue your installation.
6. Type `accept` to accept the license agreement.
7. Press **Enter** to use the default directory. The default directory is `/usr/local/NetIQ`.
8. Type `Y` to confirm the installation directory.

9. The installation directory is created, and you are prompted to choose which components of Security Reporting Center will be installed.

10. Press **D** to install all the components on this computer.

11. Type a user name for the Database server. (This user name has no relationship to the Unix username.)

12. Type the host name of the computer where the Database server will run. The default is your local computer.

13. Type the name of the MySQL server socket. The default is `/tmp/mysql.sock`.

14. Type the port number for MySQL. The default port number is `3306`.

15. Press **Enter** to continue.

16. Type a user name for the User Interface server. (This user name has no relationship to the Unix user name.)

17. Type a password for the User Interface server.

18. Type a port number for the User Interface server. The default port number is `9000`.

19. Press **Enter** to install the User Interface server.

20. The Firewall Reporting agent is installed. Press **Enter** to continue.

21. Press **Enter** to install the Proxy Reporting agent.

22. Press **Enter** to install the NetIQ Check Point LEA service.

23. Press **Enter** to install the NetIQ Syslog Service.

24. Choose whether to copy the necessary scripts to `etc/init.d` so that Security Reporting Center can be launched during startup.

    - Type `n` to continue without copying the scripts.
    - Type `Y` to copy the scripts. When prompted, type the root password.

25. Type `Y` to start the User Interface server.

26. Go to the *`installpath`*`\common\bin` directory and execute `startallui.sh`.

27. Your installation is confirmed, and the URL you need to access the Security Reporting Center Console is displayed.

Starting and Stopping Components

If you need to start or stop any Security Reporting Center components, execute the start and stop scripts in the following locations:

User Interface Server	*`installpath`*`/common/bin/startallui.sh` *`installpath`*`/common/bin/stopallui.sh`
Database Server	*`installpath`*`/common/bin/mysql.server start` *`installpath`*`/common/bin/mysql.server stop`
Scheduler agent	*`installpath`*`/modules/agent/agent.sh -start` *`installpath`*`/modules/agent/agent.sh -stop`
NetIQ LEA Service	*`installpath`*`/modules/leaservice/wtlead -start` *`installpath`*`/modules/leaservice/wtlead -stop`
NetIQ Syslog Service	*`installpath`*`/modules/syslogservice /wtsyslogd -stop` *`installpath`*`/modules/syslogservice /wtsyslogd -start`
All Security Reporting Center services	*`installpath`*`/common/bin/stopallsrc.sh`

Starting Security Reporting Center

To start the user interface, use the URL `http://`*`hostname`*`:9000`, where *`hostname`* is the name of the computer where the User Interface server is installed.

To log in to Security Reporting Center and start using it, use the following steps:

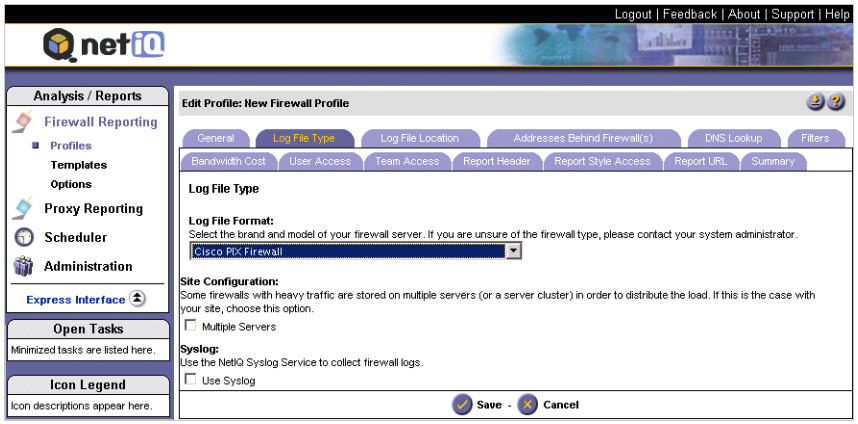
1. Open a browser.
2. Go to `http://`*`hostname`*`:9000.`
3. In the appropriate text boxes, type the login name and password you specified during installation for logging in to the user interface.
4. If you want to be logged in automatically when you open the program again, select the **Remember Me** check box.
5. Click **Log in**.
6. Type or paste a trial code or serial number into the text box at the bottom of the screen.
7. Click **Submit** to submit the code, or click **Cancel** to clear the text box.
8. Click **Done**. You can view the current serial numbers at any time by clicking **Administration > Licensing** in the left pane of Security Reporting Center.

Chapter 3
Quick Tour

This quick tour of Security Reporting Center walks you through the basic configuration steps to generate useful reports and explains the main functions of the four modules included in your product installation.

The User Interface

The Security Reporting Center user interface is a two-paned Web-based console. The left navigation pane shows a list of the currently available modules. It also shows a list of the configuration areas for the current module and an icon legend that tells you the meaning of any navigation icons.



The current content you selected is shown in the right-hand *panel*. To see a different panel, use the navigation buttons in the panel or choose another link from the left pane. If the panel contains a **Save**, **Next**, **Cancel**, or **Done** option, use one of these choices to move forward or backward in a sequence. Do not use the browser's back button to move to the previous panel.

Open Tasks

If you exit a panel during a configuration task without saving or canceling, the panel is added to the list of Open Tasks in the left pane below the module list. You can click on any open task to return to the configuration panel you left incomplete.

Using Help

Security Reporting Center provides several ways to access Help.

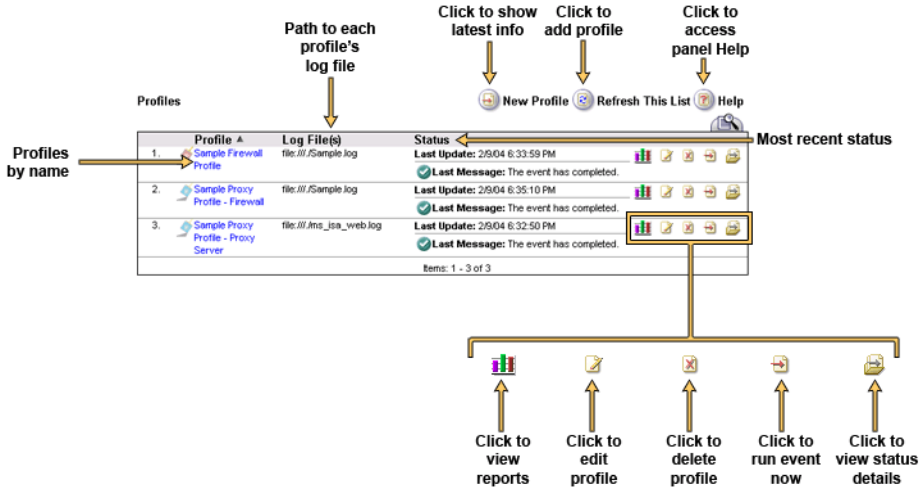
- Access context-sensitive Help for a configuration panel by clicking a **?** icon. Context-sensitive help supplies information and instructions directly related to the panel. You can access context-sensitive Help from any panel except the introductory and main Options panels. Click the icon at the top left of any context-sensitive Help topic to open the complete tri-pane Help system showing the Contents, Index and Search tabs for the current Help book.
- Click the **help** link in the Tools menu at the top of the panel to access the complete Help system, including the Table of Contents for the *User Guide* and *Firewall Configuration Guide*.
- Click the name of a module to see an orientation page that explains common tasks in that module. Descriptions are linked to related Help topics for quick review.

Icons

For a quick reference to the icons available in each panel, see the Icon Legend in the left navigation pane.

Accessing Sample Reports

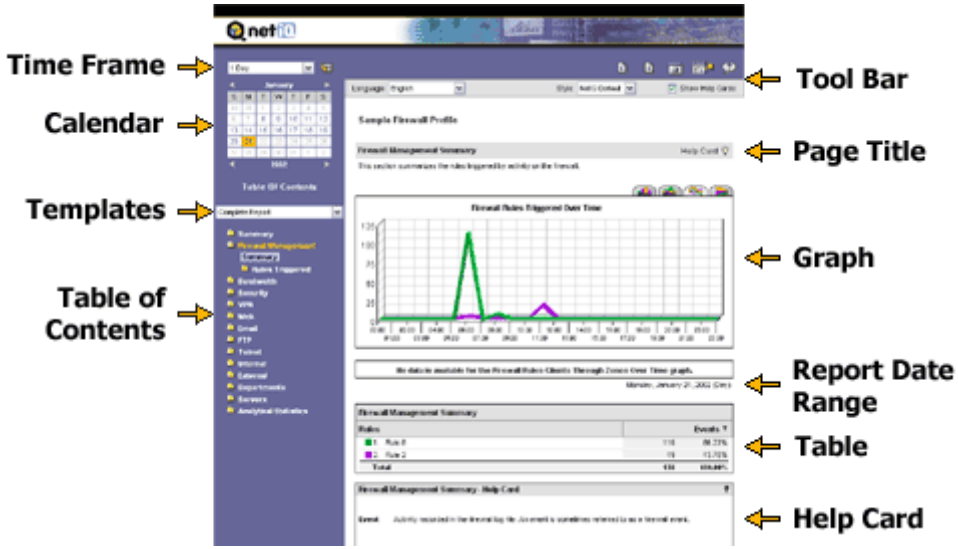
As soon as you first log in and add a serial number, Security Reporting Center creates reports based on sample data. The Express interface shows a list of all pending and available report jobs. A green check-mark icon next to a report shows that it has completed.



Reports pop up as soon as they are complete.

Using Reports

The following diagram shows the layout of a report and its configuration areas.



Choosing Report Chapters

Click the folder links at the left of any report to access specialized report chapters. For example, the Bandwidth report chapter shows a collection of report pages on bandwidth costs.

Choosing a Time Interval

By default, each report shows data for a single day. Use the list to view the data for a different time interval. For instance, if you want to see data presorted by month, select **1 Month**. To see all possible data in the report, select the largest possible time interval. If you selected the **1 Month** interval, for example, and no critical events were logged during the currently selected month, the Critical Events report chapter shows no data. Selecting **1 year** captures all data in the year. You can then drill down month by month to discover when critical events occurred.

To see a different interval (for example, a different week for a weekly report) use the report calendar. Unavailable intervals or dates indicate that there is no report data for that interval.

Choosing a Different Language

To see the report in a different language, choose a language from the list at the top of the report.

Converting a Report to Word

To convert any on-demand report to Microsoft Word format, click the **Word** icon at the top of the report. You are prompted to download the Document Utility and start the conversion.

Creating Reports

This section outlines the steps for using Security Reporting Center to create on-demand reports based on your log file data.

Creating a Report in Express Mode

The Express interface is designed to create on-demand reports with the simplest configuration options. If you are not already using the Express interface, click **Express Interface** on the left pane of Security Reporting Center to switch from Expanded to Express interface mode.

To create reports based on your logs:

1. Click **New Profile**.
2. Select the type of reports you want Security Reporting Center to create. If you want reports to focus on security, bandwidth, and other information about the traffic crossing your firewall, select **Firewall Reporting**. If you want reports to focus on the Web and FTP traffic generated by users in your network, select **Proxy Reporting**.
3. Click **Next**.
4. In the **Description** text box, type a distinctive name such as the name of your firewall. This description identifies the profile in list panels and in the database.
5. Click **Next**.
6. Select the type of log you want to analyze. In most cases, the log type is the brand and type of firewall server. However, you can also select a log type such as WELF or squid. The log type you select here determines the options available in this panel and subsequent configuration panels.
7. ***If your firewall resides on more than one computer***, select the **Multiple Servers** check box.
8. ***If you want to use the NetIQ Syslog Service to collect firewall records***, select the **Use Syslog** check box.
9. Click **Next**.

10. ***If you selected a Check Point firewall using OPSEC LEA***, click the **Check Point LEA Connections** link and create a connection to your Check Point Management Server. For more information about Check Point OPSEC LEA and Check Point LEA connections, see "Using Check Point LEA" on.

11. ***If you selected*** **Use Syslog**, provide the IP address of the Check Point Management Server and the location where you want the NetIQ Syslog Service to store log records.

12. ***If you selected Multiple Servers***, click **Add New Server** and browse to create a list of firewall servers.

13. ***If you selected any other firewall type***:

    a. Type the path to where your firewall logs are stored, or browse to select the log location. List each file path on a separate line.

    b. ***If you are accessing log files using FTP***, select absolute or relative FTP paths and provide login information if your FTP server requires it.

14. Click ***Next***.

15. Specify IP addresses inside the firewall you want to report on. This allows Security Reporting Center to distinguish incoming from outgoing traffic and report on internal users and groups.

16. Specify the cost of bandwidth per kilobyte on your network and the currency used to report on bandwidth cost. This allows Security Reporting Center to calculate how much the activity for various users and protocols costs your organization. If you do not know the cost of bandwidth, set the cost to `0`.

17. Click **Save** to save your settings. Security Reporting Center automatically creates and launches a report job or *event*. You report pops up as soon as Security Reporting center finishes analyzing the log and creating the report.

Tracking Report Jobs in Expanded Mode

If your report does not generate successfully, you may want to use the Expanded interface to explore the cause. You can track report and analysis jobs, or *events*, using the Scheduler module in the Expanded interface.

To track the progress of a report event:

1. Click **Expanded Interface** to switch interface modes.
2. Click **Scheduler > Scheduled Events** to view the list of events. The Scheduled Events list shows the most recent status logged for the event.
3. Click **Event Queue** in the left pane to see the event tasks that are currently running and the tasks that are waiting to run.
4. Click **Event Status** to see all the status messages generated by an event as it runs.

Exploring the Expanded Interface

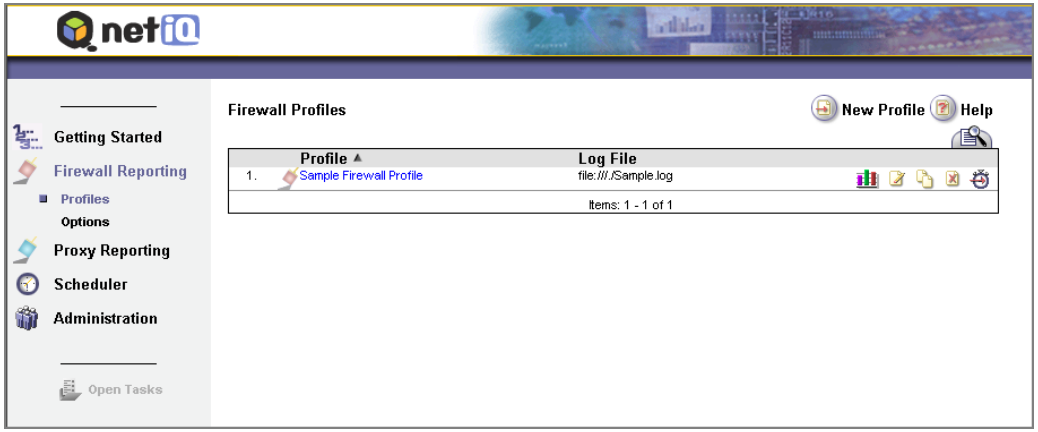
The Expanded interface shows the full range of configuration options.

The following sections provide an overview of the user interface modules installed with Security Reporting Center, and the common tasks you can perform in each module.

Firewall Reporting Module

The Firewall Reporting module creates profiles for the logs used to generate firewall reports. Firewall reports emphasize security, traffic across the firewall, and bandwidth.

Click **Firewall Reporting > Profiles** in the left pane to display the Firewall Profiles panel.



This window lets you create, edit, copy and delete profiles as well as view reports for each profile.

Each profile is a set of instructions that determines the log data collected, where that data is accessed, and how it is analyzed and presented in reports. For instance, a profile identifies the locations of your firewall log files, determines how IP addresses should be resolved, and indicates which users and teams can access reports. Profiles also allow you to choose filters that can narrow your data to the information you need most, saving time and resources.

The Firewall Reporting module also includes a range of Options panels for configuring data collection and reporting settings. The Options let you perform the following tasks:

Log Analysis options
Let you control how the Firewall Reporting module analyzes firewall logs.

Global Filter options
Let you define filters available for use with profiles. Add filters to profiles to specify which data to include or exclude during log file analysis.

FastTrends and Content Database Management options
Let you manage database content and locations.

Firewall Reporting options
let you control reporting by defining the list of protocols tracked in firewall reports, how many table rows should be exported to the Content database, how work hours are defined, and whether to limit memory usage for individual tables.

Report Styles options
Let you design visual styles for reports, including fonts, colors, and logos.

Department Management options
Let you group IP addresses in departments so Security Reporting Center can categorize activity by department.

Syslog options
Let you decide how to handle log file retrieval using the NetIQ Syslog Service.

Check Point LEA Connections options
Let you create connections between the NetIQ LEA Service and a Check Point Management Server.

Check Point LEA Performance options
Let you fine-tune Check Point LEA connections.

Cisco PIX Interfaces options

Let you specify custom interfaces logged by a Cisco PICX firewall so that Security Reporting Center can parse them correctly.

Log File Path Macros options

Let you create macros for specifying the path to your log files.

Currency options

Let you manage the list of currencies that can be used to represent bandwidth cost in reports.

DNS options

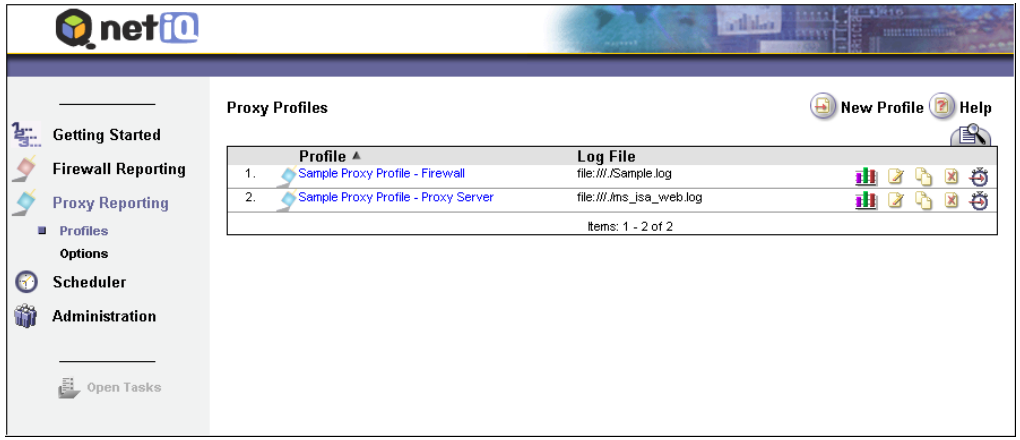
Let you fine-tune the way DNS lookups are handled.

Proxy Reporting Module

The Proxy Reporting module creates profiles for the logs used to generate proxy reports. Proxy reports focus on the Web-surfing habits of users inside the firewall, providing detailed information about how they surf and which Web sites they visit.

Each profile is a set of instructions that determines the log data is collected, where that data is accessed, and how it is analyzed and presented in reports. For instance, a profile identifies the locations of your firewall log files, determines how IP addresses should be resolved, and indicates which users and teams can access reports. Profiles also allow you to choose filters that can narrow your data to the information you need most, saving time and resources.

Click **Proxy Reporting > Profiles** in the left pane to display the Proxy Profiles panel.



The Proxy module also includes a range of Options panels for configuring data collection and reporting settings. The Options let you perform the following tasks:

URL Categorization options

Let you choose how URL categories are analyzed, create custom URL databases, manage third-party databases, and map categories to other categories for focused reporting.

Log Analysis options

Let you control how the Firewall Reporting module analyzes firewall logs.

Global Filter options

Let you define the data filters available for use with profiles.

FastTrends and Content Database Management options

Let you manage database content and locations.

Proxy Reporting options

Let you control reporting by defining which files count as download file types and page file types; which top-level domains are tracked in reports; whether to allocate system resources to retrieving HTML page titles; how a visitor session is defined; how many table rows should be exported to the Content database; whether to limit memory usage for individual tables; and how work hours are defined.

Report Styles options

Let you design visual styles for reports, including fonts, colors, and logos.

Department Management options

Let you group IP addresses in departments so Security Reporting Center can categorize activity by department.

Syslog options

Let you decide how to handle log file retrieval using the NetIQ Syslog Service.

Check Point LEA Connections options

Let you create connections between the NetIQ LEA Service and a Check Point Management Server.

Check Point LEA Performance options

Let you fine-tune Check Point LEA connections.

Cisco PIX Interfaces options

Let you specify custom interfaces logged by a Cisco PICX firewall so that Security Reporting Center can parse them correctly.

Log File Path Macros options

Let you create macros for specifying the path to your log files.

Currency options

Let you manage the list of currencies that can be used to represent bandwidth cost in reports.

DNS options

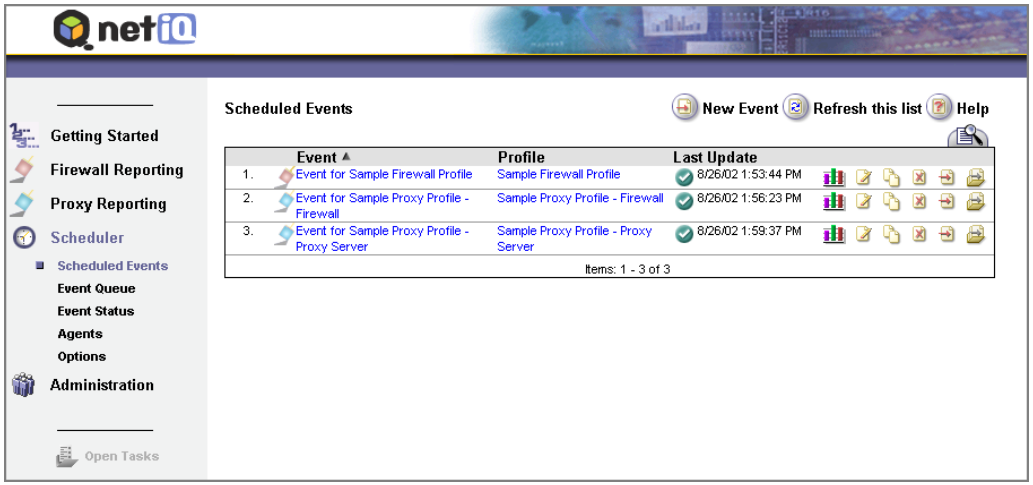
Let you fine-tune the way DNS lookups are handled.

Scheduler Module

The Scheduler module creates and monitors scheduled events. An event is an action scheduled by a Scheduler agent and performed by a Reporting agent. In Security Reporting Center, the Scheduler creates events that perform data analysis and report generation. When you create an event, you control the following settings:

- When and how often the event runs;
- What range of log file data is analyzed;
- What, if any, programs should be run before and after the event is run;
- What profile settings the event is based on.

Click **Scheduler > Scheduled Events** in the left pane to see the list of events in the Scheduled Events panel.



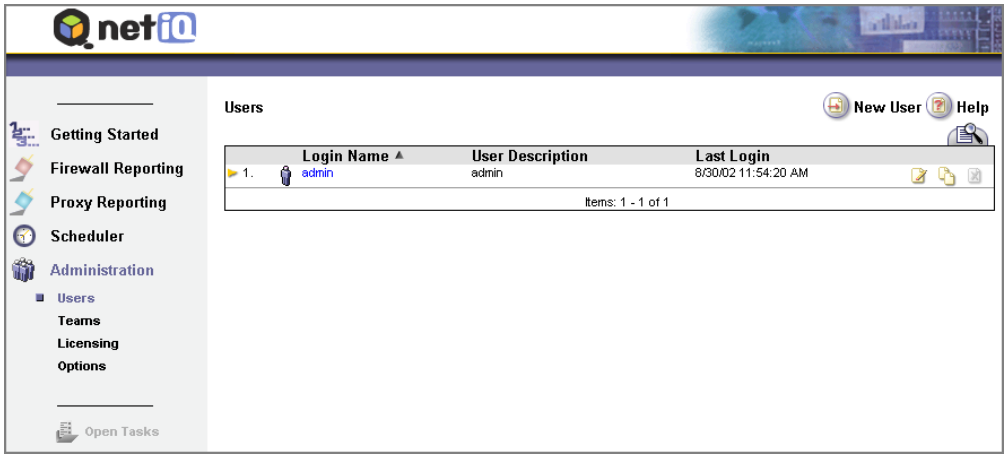
The Scheduler also includes the following panels, which help you track and troubleshoot events and manage the agents that run them.

Panel	Functions
Event Queue	Tracks events and tasks that are currently running and waiting to run.
Event Status	Shows status messages for each scheduled event and task.
Agents	Shows system statistics and status messages for each host computer where Security Reporting Center is installed.
Options	Sets default event characteristics, Scheduler polling frequency, and status message duration.

Administration Module

The Administration module controls access rights for users and teams and displays licensing information for your product installation. Using the **Users** and **Teams** panels in the Administration module, you can create lists of users and give them differing sets of access rights to profiles and events. You can also create and manage teams of users, who can be assigned differing rights within the team. Users and teams created in the Administration module can be given access to specific profiles using either of the Reporting modules.

Click **Administration > Users** in the left pane to access the Users panel.



The Administration module also includes the following panels, which provide information about the software you licensed and installed:

Panel	Functions
Licensing	Shows what tasks you are licensed to perform and which operating systems you are licensed to run them on, the number of firewalls you are licensed to monitor, and the serial numbers for the current installation. Lets you add new serial numbers.
Options	Shows the Security Reporting Center software components installed on each host computer, and the version of each software component. Controls global authentication options and the default time zone. Lets you select proxy server settings for downloading URL categorization databases.

Chapter 4
Evaluation Criteria Checklists

This chapter provides an evaluation criteria checklist to help you evaluate Security Reporting Center. Each item in the checklists identifies a Security Reporting Center feature.

Using a scale of 0 to 5, rate how important each feature is to your environment. Next, rate how well Security Reporting Center implements the feature compared to the other product. Then, calculate the weighted score for each feature by multiplying the *item significance* by the *product score*.

Security Event Tracking

Security Reporting Center tracks the frequency and source of firewall events to give

Item Description	Item significance score (0-5)	SRC score (0-5)	Other product score (0-5)	SRC weighted score	Other product weighted score
1. Quantifies and traces attempts on the firewall.					
2. Identifies users inside and outside the firewall who trigger events.					
3. Analyzes critical, warning, informational, and VPN events.					
4. Creates a detailed picture of security activity over time.					

Measurement and Baselining

Security Reporting Center provides comprehensive activity reporting that allows you to measure, baseline, analyze and predict network activity in order to efficiently manage human and network resources.

Item Description	Item significance score (0-5)	SRC score (0-5)	Other product score (0-5)	SRC weighted score	Other product weighted score
1. Analyzes bandwidth by day, hour, and week.					
2. Shows which users, departments, and protocols use the most bandwidth.					
3. Shows how much Internet traffic costs your organization, categorized by user, protocol, and traffic direction.					
4. Shows which internal clients and servers use the most bandwidth.					
5. Shows when the network is busiest and whether activity is approaching the limits of network resources.					
6. Identifies the users who generate the largest amount of email, Web, and FTP activity.					
7. Shows which users most frequently trigger warnings and other firewall events.					
8. Indicates whether large downloads are posing a risk to the network.					

Internet Usage Analysis

Security Reporting Center provides valuable insight into Internet usage patterns and the pages and files users request.

Item Description	Item significance score (0-5)	SRC score (0-5)	Other product score (0-5)	SRC weighted score	Other product weighted score
1. Analyzes Web usage to identify most active users and most popular sites.					
2. Distinguishes between dynamic HTML pop-ups and requested files or pages.					
3. Shows which sites each user visits and the length of each visit.					
4. Shows which files and file types are downloaded most frequently.					
5. Provides built-in registered access to the patented SurfControl categorization engine, which checks URLs against a database that categorizes content.					
6. Counts how frequently employees visit sites in 40 preconfigured categories, including legally sensitive content such as hate speech and time-wasting content such as online chat.					

Item Description	Item significance score (0-5)	SRC score (0-5)	Other product score (0-5)	SRC weighted score	Other product weighted score
7. Allows custom URL categorization for URLs not included in the standard databases.					
8. Allows grouping of existing categories to customize and simplify reporting.					

Secure, Customizable Reporting Access

Item Description	Item significance score (0-5)	SRC score (0-5)	Other product score (0-5)	SRC weighted score	Other product weighted score
1. Schedules reports to run every day, week, or month at a time of your choice, or schedule one-time custom reports for any time range.					
2. Reports on any range or interval of log data.					
3. Generates static reports in HTML, Microsoft Word, Microsoft Excel, PDF, or CSV format for easy distribution.					
4. Automatically saves reports to a network drive or auto-sends them as email attachments.					
5. Allows you to view or generate reports in French, Spanish, German, or English.					
6. Shows the latest data in one click.					
7. Provides instant report access only to the users and groups you choose.					
8. Lets you remotely view on-demand reports from any computer on the network.					

Support for Most Firewall Types and Formats

Item Description	Item significance score (0-5)	SRC score (0-5)	Other product score (0-5)	SRC weighted score	Other product weighted score
1. Supports all logs in WebTrends Enhanced File Format, the only standardized log format for firewall reporting.					
2. Supports logs for more than 35 firewalls, proxy servers, and security devices.					
3. Provides a built-in syslog server to access log data and create readable log files.					
4. Provides a built-in LEA service to access Check Point log data.					

Flexible, Scalable, and Centralized Architecture

Item Description	Item significance score (0-5)	SRC score (0-5)	Other product score (0-5)	SRC weighted score	Other product weighted score
1. Supports single-computer or distributed installation.					
2. Supports Microsoft Windows and Sun Solaris in single-platform or mixed installations.					
3. Reports on a single firewall, a firewall cluster, or many firewalls of different types.					
4. Allows simple license upgrade to cover more firewalls.					
5. Uses a central configuration console accessible from any computer on the network.					
6. Uses multiple levels of user rights to ensure easy report access and selective configuration access.					
7. Supports access by thousands of users and teams.					
8. Distributes HTML and Word-formatted reports to users with no application access.					

Chapter 5

Key Features at a Glance

This chapter highlights the important benefits Security Reporting Center provides and lists the key features that work together to offer these benefits. This list helps you quickly review the highlights of Security Reporting Center.

Monitors and Baselines Security

- Quantifies and traces attempts to breach the firewall.
- Identifies users inside and outside the firewall who cause critical, warning, informational, and VPN events.
- Creates a detailed picture of firewall events over time.
- Helps assess the need for firewall upgrades.

Extends Internet Usage Management

Bandwidth Management

- Analyzes bandwidth by hour, day, or week.
- Shows which users and departments use the most bandwidth.
- Shows how much Internet traffic costs your organization, categorized by user, protocol, and traffic direction.
- Shows which internal clients and servers use the most bandwidth.
- Tracks fluctuations in network traffic and shows whether traffic is overloading the network.

Internet Usage Policy Enforcement

- Shows which users are responsible for the largest amount of traffic.
- Identifies the users who generate the largest amount of email, Web, and FTP activity.
- Shows which users most frequently trigger warnings and other firewall events.
- Indicates whether large downloads pose a risk to the network.

Enhances Web Usage Analysis

Web and FTP Traffic Analysis

- Analyzes Web traffic to identify the most active users on your network and the Web and FTP sites they visit most frequently.
- Distinguishes between dynamic HTML pop-ups and requested files or pages.
- Shows which sites each user visits and the length of each visit.
- Shows which files and file types are downloaded most frequently.

Smart URL Categorization

- Provides built-in registered access to the patented SurfControl Categorization Engine, which checks the URLs requested by users on your network against a database categorized by content.
- Counts how frequently employees visit sites within 40 preconfigured categories, including both legally sensitive content, such as sexually explicit or drug-related material, and time-consuming content, such as Web chat and entertainment sites.
- Lets you create custom URL categories to categorize URLs not included in the standard databases.
- Lets you group existing categories for simplified reporting purposes using custom category mapping. For example, you can map several different categories into one custom category called Non-Work-Related Sites.

Provides Flexible Reporting Capabilities

Scheduled Reporting

- Schedules reports to run every day, week, or month at a time you choose.
- Schedules custom reports for any time range.
- Reports on any range or interval of log file data.
- Generates reports in HTML, Microsoft Word, Microsoft Excel, Adobe PDF, or CSV format for easy distribution.
- Automatically saves reports to a network drive or sends them as email attachments.
- Lets you generate and view reports in French, Spanish, German, English, or Japanese.
- Lets you create custom report groupings and design the report look, feel, and branding you prefer.

On-Demand Reporting

- Shows the latest data with one mouse click.
- Gives instant report access to only the users and groups you choose.
- Lets you view reports remotely.
- Lets you view any report in French, Spanish, German, English, and Japanese.
- Lets you select custom report groupings and apply the report look, feel, and branding you prefer.

Manages Any Size Network and Most Firewall Types

Scalable Architecture

- Supports all components installed on one computer or distributed among several computers.
- Supports both Microsoft Windows and Sun Solaris in single-platform or mixed installations.
- Creates reports for a single firewall, a cluster of firewalls, or many firewalls of different types.
- Allows simple license upgrade to cover more firewalls.

Broad Support for Firewalls and Proxy Servers.

- Supports the WebTrends Enhanced Log Format (WELF), the only standardized log format for firewall reporting.
- Supports over 35 firewalls, proxy servers, and security devices in multiple versions. For more information, see "What Does Security Reporting Center Analyze?" on page 3.
- Provides a built-in syslog server for accessing log data.
- Provides a built-in OPSEC LEA service for Check Point log data.

Centralized Reporting Accessible to Many Users

- Provides one central configuration console accessible from any computer on the network.
- Provides multiple levels of user rights to allow easy report access and selective configuration access.
- Allows report distribution in HTML, Microsoft Word, Microsoft Excel, Adobe PDF, or CSV format to users with no application access.
- Supports automated report distribution through email.
- Allows unlimited numbers of users.