# Firewall Configuration Guide

## Security Reporting Center

**June 15, 2006**

# Notice

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 Firewall Configuration Guide provides information about how to configure supported firewalls, proxy servers, and security devices to work with Security Reporting Center. It describes where log files are located, how to retrieve them, and how to make sure that they use a format that can be read and analyzed by Security Reporting Center. It also includes information about configuring both Security Reporting Center and your firewall to produce the most useful reports.

## Intended Audience

This book provides information for firewall administrators and security personnel in charge of firewall configuration and Security Reporting Center administration.

## Other Information in the Library

The library provides the following information resources:

*Evaluation Guide*

Provides general information about the product and guides you through the trial and evaluation process.

*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.

# 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<br>• Technical terms, when introduced |
| *Italics* | • Book and CD-ROM titles<br>• Variable names and values<br>• Emphasized words |
| `Fixed Font` | • File and folder names<br>• Commands and code examples<br>• Text you must type<br>• 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* \| *value2* | • Exclusive parameters. Choose one parameter. |

# About Marshal

Marshal delivers a complete email and Web security solution to a variety of Internet risks. The Marshal solution provides 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 Web site. If you cannot contact your partner, please contact our Technical Support team.

| | |
|---|---|
| **Telephone:** | +44 (0) 1256 848 080 (EMEA)<br>+1 404 459 2890 (Americas)<br>+ 64 9 984 5700 (Asia-Pacific)) |
| **Sales Email:** | info@marshal.com |
| **Support:** | www.marshal.com/support |
| **Web Site:** | www.marshal.com |

# Chapter 1
# Configuring Supported Firewalls and Logs

This chapter describes the supported firewalls and log formats for Security Reporting Center and helps you configure your firewall and Security Reporting Center to create meaningful reports based on your logs.

# BorderWare Firewall Server

## Versions Supported

BorderWare Firewall Server versions 5.*x* and 6.*x*

## Obtaining Log Information

To create a firewall profile for use with Security Reporting Center, you must specify the log file location.

The BorderWare Firewall Server maintains several log files.

Using FTP, move the connections logs and messages logs from the `root/logs` directory on the BorderWare Firewall server.

When you create a profile, select the FTP retrieval method and specify both the name of the connections log and the name of the messages log in the **Log File Path** text box. Use a vertical bar (|) to separate the two files.

# Check Point VPN-1/FireWall-1 v4.*x*

## Versions Supported

Check Point™ VPN-1® v 4.*x*

Check Point FireWall-1® v4.*x*

## Obtaining Log Information

You must specify the location of the Check Point firewall log file when you create a profile in Security Reporting Center. For step-by-step instructions on creating a profile, see the *User Guide* for Security Reporting Center.

Security Reporting Center supports two methods for accessing a Check Point firewall log file:

- OPSEC™ LEA (recommended). You can access the logs directly by using OPSEC LEA with an unauthenticated LEA connection.

  **Note**
  Because of changes to the Check Point SDK, authenticated connections are no longer supported for Check Point VPN-1/Firewall-1 v4.*x*. If you need an authenticated LEA connection, we recommend upgrading to Check Point VPN-1/Firewall-1 vNG.

- Exported logs. You can export the logs to text files.

## Configuring an Unauthenticated Connection

The following sections describe how to create a connection between Security Reporting Center and OPSEC LEA.

**Note**
To finish setting up a Check Point LEA connection, you must configure the connection using the Check Point LEA Connections options in Security Reporting Center. For more information about Check Point LEA Connections options, see the Help or the *User Guide* for Security Reporting Center.

**To configure your Check Point firewall for OPSEC LEA:**

1. Confirm that you have defined a firewall rule that enables the `Any` or `FW_LEA` protocol. This lets computers connect to the firewall using the LEA protocol.
2. If necessary, create the rule based on the following criteria:

| | |
|---|---|
| **Source** | The Security Reporting Center system or subnet |
| **Destination** | The internal or external network interface of the firewall, or the Management Console where logs are collected. |
| **Service** | `fw_lea` or `ANY` |
| **Method** | `Accept` |

## Configuring an Unauthenticated Connection

**To set up an unauthenticated LEA connection:**

1. In the `FWDIR\conf` directory on the computer where the Check Point Management Server is installed, edit the `fwopsec.conf` file to include the following line:

   ```
   lea_server  port 18184
   ```

2. Restart the firewall service.
3. Make sure that there are no `.C` files in the `modules\leaservice\config` directory.

**Note**
If the `authkeys.C` file is present, Security Reporting Center attempts to make an authenticated connection. If you have been using authenticated connections and switch to using unauthenticated connections, delete this file.

4. On the computer where the NetIQ LEA Service is installed, edit the `lea.conf` file to include the following lines:

```
lea_server     port    18184
lea_server     ip      fw1_host_ip
```

5. Use the Check Point LEA Connections options in Security Reporting Center to finish creating the connection. For more information, see "Security Reporting Center Configuration" on page 5.

6. Restart the NetIQ LEA Service.

## Security Reporting Center Configuration

To finish setting up a Check Point LEA connection, you must configure the connection in Security Reporting Center using the Check Point LEA Connections options. These options allow you to:

- Provide server-side information to the NetIQ LEA Service
- Specify where to store information generated by the NetIQ LEA Service.
- Manage multiple LEA connections
- Track the status of each LEA connection

To access the Check Point LEA Connections options, open a Reporting module and click **Options > Check Point LEA Connections**. Use the Help for each panel to guide you through connection setup.

For more information about the Check Point LEA Connections options, see the *User Guide* for Security Reporting Center.

## Managing Check Point LEA Log Files

Security Reporting Center retrieves the Check Point OPSEC LEA log data and stores the files on the local system in the Security Reporting Center installation directory. Any profile that points to this firewall uses that directory, for example:

*SRC installation directory*`\leacache\192.168.0.26.dat\`

After the log files are created, they are rotated daily and accumulate indefinitely. To remove log files, delete the files or back them up.

After you configure the firewall for Check Point OPSEC LEA, specify the IP address of the firewall in the Log Files panel when you create a Security Reporting Center firewall profile.

## Exporting Check Point Logs

Check Point stores log files in a proprietary binary format that is not directly accessible. In order to analyze these files and create reports, you must export them to an ASCII text file using the log export utility supplied by Check Point.

Check Point maintains two types of log files: `fw.log` and `fw.alog`.

- The `fw.log` file contains all the information required for reports, except for bandwidth data.
- The `fw.alog` file contains bandwidth data.

When you create the Check Point security policy, set the tracking option to create `.log` files, or to create both `.log` and `.alog` files. For more information, see "Special Firewall Configuration" on page 7.

**Note**
Always use the command line to export Check Point log files. Security Reporting Center cannot parse data that has been exported using the Check Point user interface.

**To export Check Point log files:**

1. On the computer where the firewall is installed, open a command prompt.
2. Switch to the directory where the `fw.exe` file is located..
   - For version 4.0: `\winnt\fw\bin`
   - For version 4.1: `\winnt\fw1\4.1\bin`
3. Export the log files:
   - To export the `fw.log` file, type:

     ```
     fw logexport -d ; -i fw.log -o log_path\fw.log
     ```

   - To export the `fw.alog` file, type:

     ```
     fw logexport -d ; -i fw.alog -o log_path\fw.alog
     ```

   Make sure that Security Reporting Center can access the log files. Either map a drive to the firewall from the computer running Security Reporting Center, or copy the log files to another computer accessible to Security Reporting Center.

# Special Firewall Configuration

You can configure your firewall in ways that will enhance reports.

## Logging Options

When associating a logging option with rules in the Check Point Management Console, we recommend that you select either **Long** or **Account**.

Long creates a `.log` file, which contains all the data Security Reporting Center requires to create useful report except for bandwidth information.

Accounting adds bandwidth information to the logs and creates both `.alog` and `.log` files.

## Defining Services

Check Point lets you define services as protocols. If you change the protocols associated with services, you must specify the changes in the Security Reporting Center Protocol options. Otherwise, Security Reporting Center cannot recognize the protocols in the log files and reports any unrecognized services as "other."

For more information about protocol settings, see the *User Guide* for Security Reporting Center.

## Load Balancing

You must have a separate license for each firewall or proxy server in a cluster, but the cluster can log to a single file. If your cluster logs to separate log files, combine them into a single file by using wildcards in the log file path.

## Fault-Tolerant Systems

Each Security Reporting Center license works for a specified number of firewall IP addresses, which you specify in your profile setup. If your fault-tolerant system logs to a different IP address than the one(s) specified, Security Reporting Center cannot recognize it. Make sure that you set up your fault-tolerant system to log to the same IP address.

**To determine the version of Check Point that you are running:**

Use this command:

```
$FWDIR/bin/fw ver
```

where `$FWDIR` is the directory where Check Point is installed.

## Special LEA Service Configuration

You can modify your Check Point LEA connection settings in several ways that can improve performance. For example, you can change the level of debug logging and set LEA to log the IP address of the Check Point firewall rather than a text name. In earlier versions of Security Reporting Center, these settings were controlled by the `leaservice.ini` configuration file. You can now modify them using the Security Reporting Center user interface.

For more information about these settings, see the *User Guide* for Security Reporting Center.

# Check Point VPN-1/Firewall-1 NG

## Versions Supported

Check Point Firewall-1 vNG

Check Point™ VPN-1 vNG

**Note**
This section applies only to Security Reporting Center installations. Firewall Suite users should use the instructions in the *Firewall Configuration Guide* for Firewall Suite, Firewall Appliance Analyzer, and Firewall Reporting Center. You can find this version of the *Configuration Guide* on the World Wide Web at www.marshal.com/support.

## Obtaining Log Information

You must specify the location of the Check Point firewall log file when you create a profile in Security Reporting Center. The log file location is described below. For step-by-step instructions on creating a profile, see the *User Guide* for Security Reporting Center.

Security Reporting Center supports two methods for accessing a Check Point NG firewall log file:

- OPSEC™ LEA (recommended). You can access the logs directly by using OPSEC LEA. By default, Check Point NG uses an authenticated connection with sslca. We strongly recommend using this secure configuration.

  **Note:**
  To run the NetIQ LEA Service on Solaris 8, you must patch your operating system to the level required for Check Point vNG with Feature Pack 3. For more information, see the Check Point documentation. The NetIQ LEA Service does not run on Solaris 7.

- Exported logs. You can export the logs to text files.

# Using OPSEC LEA

There are many possible configurations for collecting Check Point log records using an OPSEC LEA connection. We provide configuration instructions for two types of connections:

- A secure authenticated connection using sslca. For more information, see "Configuring an sslca Connection" on page 12.
- A clear connection with no authentication or encryption. For more information, see "Configuring a Clear Connection" on page 16.

We recommend using sslca, the default connection method, because it is an extremely secure method.

To use a connection method not documented in this Guide, refer to the Check Point documentation or contact Check Point technical support.

## Configuring an sslca Connection

The following information describes the settings for using the default connection, using sslca. sslca is a 3DES encryption scheme that uses certificate-based authentication. To create an sslca connection, configure the Check Point firewall using the Check Point Policy Editor, request a certificate from the Check Point computer, and then use the Check Point Connections panel in Security Reporting Center to finish configuring the connection.

**To set up an authenticated connection using sslca:**

1. Open the Check Point Policy Editor and select **Network Objects** from the Manage menu.

**Note:**
If you previously used OPSEC LEA with Firewall Suite or Firewall Reporting Center, you must comment out modifications to the `fwopsec.conf` file. The `fwopsec.conf` file resides in the *`installation directory`*`\FW1\NG\conf` directory. Comment out all the lines in `fwopsec.conf`.

2. Click **New** and select **Node > Host** from the list.
3. Type a name (for example `hostname01`) and the IP address for the computer where the NetIQ LEA Service is installed. The information you type in this dialog box defines the computer as a network object. The name is case-sensitive.
4. Click **Close**.
5. Select **OPSEC Applications** from the Manage menu

**Note:**
You can type either a reference name or the computer host name.

6. Click New and select **Opsec Application** from the list to define Security Reporting Center as an OPSEC application. In the **Name** text box, type a name for the connection such as `lea`. The name you type here is the same name you specify as the LEA object in Step **21**. The string is case-sensitive.
7. From the Host list, select the object you created in Step **3**.

**Note**
Type a name other than `SRC` or `src`. These names are already in use.

8. Under Client Entities, select the **LEA** check box.
9. Click **Communication** to set up the SIC (Secure Internal Communication) certificate.
10. In the **Authentication Key** text box, type a text string to authenticate the connection. Write down the string. This string you type here is the same string you specify as the text string in Step **21**. The string is case-sensitive.
11. Retype the authentication key.

12. Click **Initialize**.

13. Click **Close**.

14. Under Secure Internal Communication in the OPSEC Application Properties dialog box, write down the DN number for the LEA connection. A DN number uses a format like this:

    ```
    lea_server opsec_entity_sic_name
    "cn=cp_mgmt,o=hostname.company.com.i3yyym"
    ```

    If the DN number is long, it may extend off the screen.

15. Click **OK**.

16. Click **Close**.

17. Select **Network Objects** from the Manage menu.

    **Note:**
    When the certificate is created, the Trust State field displays Initialized but trust not established. This messages means that the certificate has been created, but the client computer has not yet requested and received it. When the certificate is received, the Trust State displays Trust established.

18. Select the network object for the computer where the Check Point Management Server is installed and click Edit.

19. Under Secure Internal Communication, write down the DN number for the Check Point Management Server object.

20. On the computer where you installed the NetIQ LEA Service, open a command prompt and go to the following directory:

    ```
    installation directory\modules\leaservice\config
    ```

21. Type the following command to request the certificate:

    ```
    opsec_pull_cert -h check point IP -n LEA object -p text string
    ```

where Check Point IP is the IP address of the Check Point Management Server, LEA object is the name of the OPSEC application you created for the OPSEC LEA computer in Step **6**, and text string is the authentication key you used to create the certificate in Step **10**. Typing this command creates the `opsec.p12` file, which is the certificate.

22. Place the p12 file in the directory where you will store the log files the LEA Service generates. By default, Security Reporting Center stores these files in the *`installation directory`*`\modules\leaservice\lealogs\connection name` directory.

23. Restart the NetIQ LEA Service. If you experience any problems with communication between the Check Point Management Server and the NetIQ LEA Service, restart the computers where both are installed.

24. Use the Check Point LEA Connections panel in Security Reporting Center to finish creating the connection.

## Resetting the Certificate

**To reset the certificate for LEA communication:**

1. In the Check Point Management Server, select the OPSEC LEA object you created and click **Edit**.

2. Click **Communication**.

3. Click **Reset**.

4. Reinstall the policies.

## Configuring a Clear Connection

The following instructions describe how to configure a clear connection between the Check Point NG firewall and the NetIQ LEA Service. To create a clear connection, configure the Check Point firewall using the Check Point Policy Editor, configure the **`fwopsec.conf`** file on the Check Point computer and then use the Check Point LEA Connections panel in Security Reporting Center to finish creating the connection.

---

**Note:**
We recommend using a clear connection only if you are unable to use sslca. To set up a clear connection:

---

1. On the computer where Check Point NG is installed, locate the *`installation directory`*`\fw1\ng\conf` directory.
2. Edit the `fwopsec.conf` file to include the following lines:

```
lea_server      auth_type      none
lea_server      auth_port      0
lea_server      port           18184
```

   OPSEC LEA uses 18184 as the default port.

3. Use the Check Point LEA Connections options in Security Reporting Center to finish creating the connection. For more information, see "Security Reporting Center Configuration" on page 16.

## Security Reporting Center Configuration

To finish setting up a Check Point LEA connection, you must configure the connection in Security Reporting Center using the Check Point LEA Connections options. These options allow you to:

- Provide server-side information to the NetIQ LEA Service
- Specify where to store information generated by the NetIQ LEA Service.
- Manage multiple LEA connections
- Track the status of each LEA connection

To access the Check Point LEA Connections options, open a Reporting module and click **Options > Check Point LEA Connections**. Use the help for each panel to guide you through connection setup.

For more information about the Check Point LEA Connections options, see the *User Guide* for Security Reporting Center.

## Using Exported Log Files

Check Point stores log files in a proprietary binary format that is not directly accessible. In order to analyze these files and create reports, you must export them to an ASCII text file using the log export utility supplied by Check Point. When you create the Check Point security policy, set the tracking option to create `.log` files, or to create both `.log` and `.alog` files.

**Note**
Always use the command line to export Check Point log files. Security Reporting Center cannot parse data that has been exported using the Check Point user interface.

**To export Check Point log files:**

1. On the computer where the firewall is installed, open a command prompt.
2. Switch to the `\winnt\fw1\NG\bin` directory where the `fw.exe` file is located.
3. Export the log files using the following command:

   ```
   fwm logexport -i (input file) -o (output file)
   ```

   If you do not specify an input file, Check Point exports the current log.
4. Make sure that Security Reporting Center can access the log files. Either map a drive to the firewall from the computer(s) running Security Reporting Center Reporting agents, or copy the log files to another computer accessible to the agent(s).

## Configuring log files for HTTP, SMTP, and FTP

Check Point VPN-1/FireWall-1 vNG does not automatically log HTTP, SMTP, and FTP connections. Configuring Check Point to log these connection types may slightly affect firewall performance.

After you follow the steps for configuring logging for these protocols, you need to create new rules for http, ftp, and smtp resource objects.

**To configure HTTP reporting:**

1. Click **Resources** on the Firewall Manage page.
2. Click **New** and select **URL**.
3. Enter all the necessary information. Do not select **Optimize URL Logging**.
4. Select the Match tab

> **Note:**
> The delimiter between fields in exported log files must be a semi-colon.

5. Select all the check boxes under Schemes.
6. Type an asterisk (*) in the **Other** text box.
7. Select all the check boxes under Methods.
8. Type an asterisk (*) in the **Other** text box.
9. Type an asterisk (*) in the **Host**, **Path**, and **Query** text boxes.
10. Click **OK**.

**To configure SMTP reporting:**

1. Click **Resources**.
2. Click **New** and select **SMTP**.
3. Enter all the necessary information.
4. Select the Match tab.

5. Type an asterisk (*) in the **Sender** and **Recipient** text boxes.
6. Click **OK**.

**To configure FTP reporting:**

1. Click **Resources**.
2. Click **New** and select **FTP**.
3. Enter all the necessary information.
4. Select the Match tab.
5. Type an asterisk (*) in the **Path** text box.
6. Select the **Get** and **Put** check boxes under Methods.
7. Click **OK**.

# Special Firewall Configuration

You can configure your firewall in ways that will enhance reports.

## Defining Services

Check Point lets you define services as protocols. If you change the protocols associated with services, you must specify the changes in the Security Reporting Center Protocol options. Otherwise, Security Reporting Center cannot recognize the protocols in the log files and reports any unrecognized services as "other."

For more information about protocol settings, see the *User Guide* for Security Reporting Center.

## Load Balancing

You must have a separate license for each firewall or proxy server in a cluster, but the cluster can log to a single file. If your cluster logs data to separate log files, combine them into a single file by using wildcards in the log file path.

### Fault-Tolerant Systems

Each Security Reporting Center license works for a specified number of firewall IP addresses, which you specify in your profile setup. If your fault-tolerant system logs to a different IP address than the one(s) specified, Security Reporting Center cannot recognize it. Make sure that you set up your fault-tolerant system to log to the same IP address.

## Special LEA Service Configuration

You can modify your Check Point LEA connection settings in several ways that can improve performance. For example, you can change the level of debug logging and set LEA to log the IP address of the Check Point firewall rather than a text name. In earlier versions of Security Reporting Center, these settings were controlled by the `leaservice.ini` configuration file. You can now modify them using the Security Reporting Center user interface.

For more information about these settings, see the *User Guide* for Security Reporting Center.

# CimTrak Web Security Edition

## Versions Supported

CimTrak Web Security Edition v1.3.2.0

## Reports for CimTrak

CimTrak is not a firewall or proxy server, but Security Reporting Center can create reports using the security information that it logs. CimTrak creates log files in WebTrends Enhanced Log Format (WELF), which is compatible with Security Reporting Center. For more information about WELF format, see "WebTrends Enhanced Log Format" on page 119. Create a profile for CimTrak as you would for a firewall or proxy server.

## Obtaining Log Information

To create a profile for use with Security Reporting Center, you must specify the log file location. Select **CimTrak WSE (WELF)** log file format.

Log files are stored in the `/wtlogs` directory on the computer where the Server component of CimTrak is installed. This location cannot be changed.

# Cisco Content Engine

## Versions Supported

ACNS v5.*x*

## Obtaining Log Information

Cisco Content Engine can generate logs in three formats: Squid, Extended Squid, and Apache (or NCSA Common). To produce logs that Security Reporting Center can read, we recommend using the default log format, Squid. You should also configure the Content Engine to generate transaction logs and automatically send them to an accessible log repository using FTP.

## Configuring ACNS

The Cisco Web site describes how to create Squid-format transaction logs and automatically move them to a log repository where Security Reporting Center can access them. For detailed instructions, see the following Web page:

`http://www.cisco.com/univercd/cc/td/doc/product/webscale/uce/acns50/cnfg50/logging.htm`

---

**Note**
Like other devices that log data in Squid format, the Content Engine logs firewall data in UTC, or Greenwich Mean Time. By default, Security Reporting Center reports show firewall events in terms of the time zone where Security Reporting Center analyzes the data. For example, if the Firewall Suite computer is in New York, where the time is GMT minus five hours, an event logged at GMT 08:00 is displayed as 03:00.

---

# Cisco IOS Firewall and Router

## Versions Supported

Cisco IOS Firewall version 11.3 or later.

## Obtaining Log Information

To create a firewall profile for use with Security Reporting Center, you must specify the log file location. Because Cisco IOS does not export log files, we recommend using the NetIQ Syslog Service. Refer to the User Guide for Security Reporting Center for information about the NetIQ Syslog Service.

## Configuring Cisco IOS for the NetIQ Syslog Service

Security Reporting Center supports the analysis of log files created by a Cisco IOS router in two possible configurations:

- A router using access control lists (ACLs).
- A Cisco IOS log file made by a firewall or router using the Firewall Feature Set.

To find out if your router uses access control lists as the basis of its security, look for the following section in the configuration. The following code is created by the access-list command:

```
access-list 112 permit udp any host 192.168.27.3 eq domain
access-list 112 permit tcp any host 192.168.27.3 eq domain
access-list 112 permit tcp any host 192.168.27.3 eq www
access-list 112 permit tcp any host 192.168.27.3 eq ftp
access-list 112 permit tcp any host 192.168.27.3 eq smtp
```

Another way of seeing what type of system you are using is to look at the log files:

- Records based on ACLs contain `%SEC`.

- Records based on the Firewall Feature will contain %FW.

**To enable firewall logging for the Cisco IOS router:**

1. Telnet to the router or log in to the console port.

**Note**
Alerts are automatically enabled if the associated inspection rule is active.

2. Turn on audit trail (SESS_AUDIT_TRAIL). By default, audit trail is off. In configuration mode, type:

```
ip inspect audit-trail
```

3. Enable logging. In configuration mode, type:

```
logging on
logging trap debugging
logging facility local5
logging history size 16
logging xxx.xxx.xxx.xxx
```

where `xxx.xxx.xxx.xxx` is the IP address of the Security Reporting Center computer where the Syslog Service is enabled.

4. Add inspection rules for each protocol for which you want log details. For example, inspection rules like the following are typically found in the configuration file:

```
ip subnet-zero
ip inspect audit-trail
ip inspect name qafw ftp
ip inspect name qafw http
ip inspect name qafw smtp
ip inspect name qafw realaudio
```

Add the inspection rule to whatever interfaces the traffic is going through. For example, interfaces like the following are found in the configuration file:

```
interface Ethernet0
```

```
ip address 192.168.0.1 255.255.0.0
  no ip directed-broadcast
  ip nat outside
  ip inspect qafw out
```

For additional details, refer to the Cisco Technical Assistance Center.

# Cisco PIX Firewall

## Versions Supported

Cisco PIX Firewall versions 4.*x*, 5.*x*, and 6.*x*.

## Obtaining Log Information

To create a firewall profile for use with Security Reporting Center, you must specify the log file location. Because the Cisco PIX firewall does not create a log file, a syslog server is required. We recommend using the built-in NetIQ Syslog Service. Refer to the User Guide for Security Reporting Center for more information about the NetIQ Syslog Service.

## Configuring Cisco PIX for the NetIQ Syslog Service

Because the NetIQ Syslog Service uses the UDP protocol to make the syslog connection, verify that the Security Reporting Center computer can access port 514 on the firewall. You may need to make a rule specific to this situation before Security Reporting Center can connect to the firewall.

### Configuring Versions Earlier than Version 4.2(2)

**To configure Cisco PIX for Security Reporting Center:**

1. Telnet to the PIX firewall.
2. Type:

   ```
   syslog facility 20.7
   ```

   where `facility 20` is the function that you want to perform and `7` is the log detail level or debug level of messages you want sent to the NetIQ Syslog Service.

Level 7 sends the most data. Lower levels can be used, but Security Reporting Center will produce less detailed information, especially in incoming and outgoing reports.

3. Type:

```
syslog host SRC_machine_IP
```

where `SRC_machine_IP` is the IP address of the computer where the NetIQ Syslog Service is installed. For more information, see your Cisco PIX firewall documentation.

## Configuring Version 4.2(2) and Later

**To configure Cisco PIX for Security Reporting Center:**

1. Telnet to the PIX firewall.
2. Type:

```
logging on
logging facility 20
logging trap informational
logging host interface_name SRC_machine_IP
```

where `SRC_machine_IP` is the IP address of the computer where the NetIQ Syslog Service is installed.

In this example:

```
logging host inside 10.0.0.2
```

`inside` is the interface name and the `10.0.0.*` subnet is on the inside of the PIX.

Different trap levels can be used, but Security Reporting Center produces less detailed information, especially in incoming and outgoing reports.

For more information, see your Cisco PIX firewall documentation.

# Clavister Firewall

## Versions Supported

Clavister Firewall v8.*x* and higher

## Getting Log Information

To create a log that Security Reporting Center can analyze, the Clavister log must be converted to WebTrends Enhanced Log Format, or WELF. For more information about WELF, see "WebTrends Enhanced Log Format" on page 119. We recommend that you set up log conversion so it takes place as part of event pre-processing each time Security Reporting Center creates a new report.

To perform Clavister log conversion, you use the command line to execute `FWLogQry`. `FWLogQry` uses the parameters specified in `firewall-query.txt` to collect records from Clavister's compressed logs and write the log data in a standard output format. The `gawk.exe` utility then uses the script `convert.awk` to parse the log data and output it in WELF format.

**To set up Clavister log conversion:**

1. Download and configure the Clavister log conversion scripts and supporting files. For more information, see "Configuring Clavister Log Conversion Scripts" on page 30.
2. Create a Security Reporting Center profile that points to the location where you plan to store the converted logs. For more information, see "Configuring Security Reporting Center" on page 32.

3. Do one of the following:

   – Configure Security Reporting Center to run the conversion on the command line as part of event pre-processing. For more information, see "Configuring Security Reporting Center" on page 32.

   – Manually run the conversion on the command line.

## Configuring Clavister Log Conversion Scripts

**To pre-configure the conversion scripts for WELF conversion:**

1. Create a folder for the conversion scripts on a computer accessible to your Security Reporting Center installation.

   **Note**
   The folder name should not contain spaces.

2. Download the `FWLogQry` utility from `www.clavister.com/support/utilities/fwlogqry-win32-1.01.03.exe` to the scripts folder you created in Step **1** and rename the file `fwlogqry.exe`. `FWLogQry` searches the compressed log files generated by the Clavister Log Receiver and extracts the log entries you specify.

3. Download the conversion scripts from `http://www.clavister.com/support/webtrends/webtrends-files.zip` and extract them to the scripts folder you created in Step **1**. The `.zip` archive contains the following files:

   – `gawk.exe` (the executable file for GNU AWK 3.03) parses the file produced by `FWLogQry` so that Security Reporting Center can read it.

   – `convert.awk` (the Clavister WebTrends parser script) interprets Clavister log data and converts it to WELF.

   – `firewall-query.txt` contains a pre-defined query with the correct output parameters.

**Note**
You can download an MD5 check sum at
`www.clavister.com/support/webtrends/webtrends-files.zip.md5`.

4. Edit the `firewall-query.txt` file as follows:
   - Replace `GW-YOURGW-HERE` with the correct host name for your firewall.
   - Change the `last full days` value from `1` to the number of days you want to analyze.
5. To set the directory where `FWLogQry` should access log files generated by the Clavister Log receiver, open a command line, navigate to your scripts folder, and type `fwlogqry –s` plus the path to the log location: For example, type:

   ```
   fwlogqry -s "c:\path\to\fwlogger"
   ```

   or

   ```
   fwlogqry -s "\\servername\path\to\fwlogger"
   ```

## Special VPN Configuration

If you run a VPN gateway or a VPN-enabled firewall, you can modify `convert.awk` for your VPN settings:

**To customize convert.awk for your VPN:**

1. In lines 10-12 of `convert.awk`, define the names of your virtual VPN interfaces as entered in the Interfaces\VPN Tunnels section of the Clavister Firewall Manager.

   The unmodified script looks like this:

   ```
   #
   # VPN List
   #
   ```

   Define each interface using the following format:

   ```
   vpn["RoamVPN"] = 1;
   ```

For example, if you have two configured VPN connections named `RoamVPN` and `GBGNet`, type:

```
#
# VPN List
vpn["RoamVPN"] = 1;
vpn["GBGNet"] = 1;
#
```

To temporarily disable a VPN interface in your firewall, set the interface value to `0` or delete the line.

2. Optionally, reset the following priority levels:

| | |
|---|---|
| 0 | emergency |
| 1 | alert |
| 2 | critical |
| 3 | error |
| 4 | warning |
| 5 | notice |
| 6 | information |
| 7 | debug |

## Configuring Security Reporting Center

To analyze Clavister logs, create a Security Reporting Center profile that points to the Clavister log in your scripts folder. To automate log conversion as part of Security Reporting Center reporting (recommended), create an event that runs the conversion scripts as part of log pre-processing.

You can also convert logs manually using the command line. However, you must reconvert the log each time Clavister generates new data. For more information about converting logs manually, see “Converting Logs Manually” on page 33.

**To configure Security Reporting Center for Clavister log conversion:**

1. When you create a profile for your Clavister logs, select **Webtrends Enhanced Log Format (WELF)** and specify the path to `logfile.log` in the scripts folder you created to store your Clavister log conversion scripts.
2. When you create an event, choose the following settings on the Pre-Processing panel:
   - Select the **Enable Pre-Processing** check box.
   - In the **Application** text box, type the path to the `CMD.EXE` file. `CMD.EXE` is typically located in the `\System32` folder.
   - In the **Working Folder** text box, specify the scripts folder you created to store your Clavister log conversion scripts.
   - In the **Command Arguments** text box, type the following command as a single line:

     ```
     "c:\scripts_directory\fwlogqry -f
     c:\scripts_directory\firewall-query.txt |
     c:\scripts_directory\gawk -f c:\scripts_directory\convert.awk >
     c:\scripts_directory\logfile.log"
     ```

     where *`c:\scripts_directory`* is the scripts directory you created to store your Clavister log conversion scripts.

To verify that the script extracted data and converted it correctly, check `logfile.log` in the scripts folder.

## Converting Logs Manually

If you do not want to use the Security Reporting Center pre-processing settings, you can convert Clavister logs manually using the command line. Keep in mind that if you want Security Reporting Center reports to reflect the latest information, you must reconvert the log each time Clavister logs new data.

**To convert logs manually:**

1. At a command line, type the following command as a single line:

   ```
   "c:\scripts_directory\fwlogqry -f
   c:\scripts_directory\firewall-query.txt |
   c:\scripts_directory\gawk -f c:\scripts_directory\convert.awk >
   c:\scripts_directory\logfile.log"
   ```

   where *c:\scripts_directory* is the scripts directory you created to store your Clavister log conversion scripts.

2. To verify that the script extracted data and converted it correctly, check `logfile.log` in the scripts folder.

# CyberGuard Firewall

## Versions Supported

CyberGuard for UnixWare Systems version 4.1 with product service update (PSU) 4 or later installed

CyberGuard for UnixWare Systems versions 4.2, 4.3, and 5.*x*.

**Note**
CyberGuard for UnixWare Systems version LX 5.0 is NOT supported.

## Obtaining Log Information

To create a firewall profile for use with Security Reporting Center, you must specify the log file location.

Once the firewall log files are generated, copy them to a computer accessible to Security Reporting Center. Specify this location when you create a profile in Security Reporting Center.

## Configuring CyberGuard

CyberGuard supports two methods for generating log files:

- Audit log files contain session information for a specified time period
- Configurable log files provide information about the firewall activity in real time using syslog facilities. The types of records that can be included in configurable log files include:
  - Session information
  - Addition of packet filtering rules
  - Alerts, which are suspicious or critical events.
  - Audit Log Files

**To configure CyberGuard Firewall to generate audit log files:**

1. Click **Reports** on the control panel of the CyberGuard Firewall console, and select **WebTrends Audit Reports**. The Report Generation window opens.
2. Specify the start time, end time, and a filename to which the data can be written. The default filename is `/var/audit_logs/webtrends.log`.
3. Click **Apply**.

**To configure CyberGuard Firewall to generate configurable log files:**

1. On the control panel of the CyberGuard Firewall console, click **Configuration**.
2. Select **Alerts and Activities**.
3. In the WebTrends setup frame on the Activities page, specify that records be written to the system log file or to a local log file.
4. To write activity records to the system log file in compatible format:
   a. Select a level (problem severity). The default is Notice Message Priority.
   b. Type the IP address to which CyberGuard should write the syslog information.
5. To write activity records to a local log file:
   a. Select **Log Activities to a File (WebTrends format)**. The location of the log file is `var/audit_logs/WebTrends`.
   b. Select the **Alerts** page, and select the check boxes for the events you want to monitor..
   c. View the records generated by the selected alerts and activities.
   d. Click Reports, and select Activity Reports.
6. Do one of the following:
   - For version 4.1: In the **Report On** text box, select **WebTrends Report on All Activity**.
   - For version 4.2: Click **Refresh**.

The real-time data in the file `/var/audit_logs/WebTrends` is displayed. This data is used for Security Reporting Center reports.

# Fortinet FortiGate Network Protection Gateways

## Versions Supported

FortiGate-50

FortiGate-100

FortiGate-200

FortiGate-300

FortiGate-400

FortiGate-500

FortiGate-2000

**Note**
Firmware v2.26 or higher is required.

## Obtaining Log Information

To create a Security Reporting Center firewall profile, you must specify the log file location. Because Fortinet FortiGate does not export log files, a syslog server is required. We recommend using the built-in NetIQ Syslog Service. For more information about the NetIQ Syslog Service, see the *User Guide* for Security Reporting Center. Fortinet Fortigate logs in WebTrends Enhanced Log Format, or WELF. For more information about WELF format, see "WebTrends Enhanced Log Format" on page 119.

Use the following log file settings when creating a Security Reporting Center firewall profile:

- Select **Fortinet FortiGate (WELF)**.
- Select **Use Syslog** to have the NetIQ Syslog Service collect the log files.

– In the **Firewall IP address** text box, type the IP address of the computer where Fortinet FortiGate is installed.

## Configuring the Fortinet FortiGate Network Protection Gateway

**To configure Fortinet FortiGate to send log file data to the NetIQ Syslog Service:**

1. Log into the Fortinet FortiGate Web interface.
2. Select **Firewall > Policy**.
3. Choose a rule for which you want to log traffic and click **Edit**. You can configure any traffic to be logged separately if it is acted upon by a specific rule.
4. Select the **Log Traffic** check box.
5. Click **OK**, then click **Apply**.
6. Repeat for all rules for which you want to log traffic.
7. Select **Log & Reports > Log Setting**.
8. Click **Log to WebTrends** and enter the IP address of the NetIQ Syslog Service.
9. Make sure that the **Log All Events** check box is selected.
10. Click **Apply**.

# GTA Firewall Family

## Versions Supported

GNAT Box System Software v3.3.0 and higher

## Getting Log Information

To create a Security Reporting Center firewall profile, you must specify the log file location. Because the GTA firewall family does not export a compatible log file, a syslog server is required. We recommend using the built-in NetIQ Syslog Service. For more information about the NetIQ Syslog Service, refer to the *User Guide* for Security Reporting Center. GTA Firewall Family logs in WebTrends Enhanced Log Format, or WELF. For more information about WELF format, see "WebTrends Enhanced Log Format" on page 119.

**Use the following log file settings when creating a Security Reporting Center firewall profile:**

1. Select **GTA Firewall Family (WELF)**.
2. Select **Use Syslog** to have the NetIQ Syslog Service collect the log files.
3. In the **Firewall IP address** text box, type the IP address of the computer where the GNAT Box system is installed.

## Configuring the GNAT Box Firewall

**To configure the GNAT Box to send data in WELF format to the NetIQ Syslog Service:**

1. Log on to the firewall using either the Web interface or the GBAdmin interface.
2. From the Services menu, select **Remote Logging**.

3. Select the **Enable remote logging** check box.
4. In the **Syslog server IP Address** text box, type the IP address of the computer where the NetIQ Syslog Service is installed.
5. In the **Port** text box, use the default port, `514`.
6. Clear the **Use old log format** check box if it is selected.
7. Set both the Network Address Facility and the WWW Pages Accessed Facility to **local7**.
8. Set all the Priority settings to **5-notice**.
9. Before you exit the current page, save the section.

# Ingate Systems Firewall

## Versions Supported

| Hardware Versions | Software Versions |
|---|---|
| Ingate Firewall 1200 | 3.1.0 |
| Ingate Firewall 1400 | 3.1.1 |
| Ingate Firewall 1800 | 3.1.3 |
| Ingate Firewall 1880 | 3.1.4 |
| | 3.2 |
| | 3.2.1 |

## Getting Log Information

To create a Security Reporting Center firewall profile, you must specify the log file location. To create a log that Security Reporting Center can analyze, configure the Ingate firewall to export a log file in WebTrends Enhanced Log Format, or WELF. For more information about WELF, see "WebTrends Enhanced Log Format" on page 119.

**To export the log in WELF format:**

1. Make sure the Ingate firewall is correctly configured and connected to the network.
2. Log in to the firewall.
3. Click the Logging tab.
4. At the bottom of the Logging tab, next to the **Export Log** button, select **WELF** from the list of file formats.
5. In the text box, type the maximum size in MB for the exported log file.
6. Click **Export Log**.

7. Click **Save** to download the log file to a local computer.

**Note**
Save the file in a location where all components of your Security Reporting Center installation have access to it.

# Inktomi Traffic Server

## Versions Supported

Traffic Server version 3.5.2 and later

## Getting Log Information

To create a firewall profile for use with Security Reporting Center, you must specify the log file location. The log file location is equivalent to the configuration variable `proxy.config.log2.logfile_dir`, which is located in the `records.config` file. Inktomi Traffic Server logs in WebTrends Enhanced Log Format, or WELF. For more information about WELF, see "WebTrends Enhanced Log Format" on page 119.

The name of the log file you should use depends on the configuration of the Traffic Server. By default, the log file is called `welf.log`. However, it can be renamed.

## Proxy Server Configuration

The Traffic Server can output access logs in several built-in formats (squid, Netscape common, extended, and extended2) or in user-defined custom formats. Use the custom log facility to generate logs in WELF format. For more information, see "Understanding Traffic Server Logs" in the *Inktomi Traffic Server Administrator's Guide* v3.5 or "Working with Log Files" in the *Inktomi Traffic Server Administrator's Guide* v4.0.

Before you can use Traffic Server's custom log facility, you must perform the following operations:

- You must define a custom format.
- You must activate custom logging.

### Defining the WELF Custom Logging Format

The Traffic Server provides two ways of defining a custom format. One is the "traditional" style, using the configuration file `logs.config`. While this style is very

simple to use, it is not particularly flexible. The second way to define a custom format involves a more powerful and flexible XML-based style that uses the `logs_xml.config` file.

If you are using a Traffic Server version earlier than 4.0, support for the WELF format is limited to the traditional style. However, versions 4.0 and later support both the traditional and the XML-based styles.

## Activating Custom Logging (Versions Earlier than 4.0)

To activate custom logging, you must manually define an entry for WELF in the `logs.config` file.

**To manually define an entry:**

1. Open the `logs.config` file in a text editor.
2. Insert the following text, making sure that it all goes onto a single line:

```
format:enabled:1:welf:id=firewall time="%<cqtd> %<cqtt>" fw=%<phn>
pri=6 proto=%<cqus> duration=%<ttmsf> sent=%<psql> rcvd=%<cqhl>
src=%<chi> dst=%<shi> dstname=%<shn> user=%<caun> op=%<cqhm>
arg="%<cqup>" result=%<pssc> ref="%<{Referer}cqh>" agent="%<{user-
agent}cqh>" cache=%<crc>:welf:ASCII:# INKTOMI WELF
```

3. If you are using any other custom format in the `logs.config` file, change the `1` in this portion of the code:

   ```
   format:enabled:1
   ```

   to any number that is not used by one of the other formats. Each format should have a unique identifier.

## XML Log Customization (Version 4.0 and Higher)

Traffic Server versions 4.0 and higher support WELF using the XML-based custom configuration format as well as in the traditional custom log format. These versions have predefined entries for the WELF in both the `logs.config` and `logs_xml.config` files, so you do not have to configure them manually.

# iPrism Web Filtering Appliance

## Versions Supported

iPrism Version 3.200 and later

## Getting Log Information

To create a firewall profile for use with Security Reporting Center, you must specify the log file location. Because iPrism exports logs using the syslog protocol, a syslog server is required. We recommend using the built-in NetIQ Syslog Service. For more information about the NetIQ Syslog Service, see the *User Guide* for Security Reporting Center. iPrism logs use the WebTrends Enhanced Log Format, or WELF. For more information about WELF, see "WebTrends Enhanced Log Format" on page 119.

Use the following settings to create a firewall profile:

- Select **WebTrends Enhanced Log File (WELF)** log file format.
- Specify that you want the NetIQ Syslog Service to collect the log files.
- In the **Firewall IP address** text box, type the IP address of the iPrism. This is the address you configured iPrism to use in the setup wizard.

## Configuring iPrism for WELF

**To configure iPrism to generate log records in WELF format:**

1. Attach to the iPrism administrative interface via a browser or application.
2. Click the **System** button.
3. Select the Reports tab.
4. In the **Syslog Host** field, type the IP address of the computer where the NetIQ Syslog Service is installed.
5. Select the **WELF** check box to use WELF format.

6. Security Reporting Center requires activity to be assigned to a single URL category. To avoid logging activity under multiple categories, which can cause confusing reports, select the **WELF single category output** check box.

7. Exit the iPrism interface and save your changes.

# Lucent Managed Firewall

## Versions Supported

Lucent Managed Firewall v3.*x* and v4.*x*

## Getting Log Information

To create a Security Reporting Center firewall profile, you must specify the log file location.

Lucent Managed Firewall maintains one type of log file that is rotated daily. The logs have a .log extension.

Lucent Managed Firewall log files reside on the management server in the `\users\isms\mf\log\sessions\date.log` directory.

Because Lucent is managed by a dedicated PC (the SMS) that is not a part of the network, you must copy the log file to an external device such as a SyJet, Zip, or Jaz drive, and then transfer the file to the computer running Security Reporting Center.

# Lucent VPN Firewall

## Versions Supported

Lucent Security Management Server v6.*x* and higher

Lucent VPN Firewall Brick - Models 201, 20, 300

## Getting Log Information

Logs for the Lucent VPN Firewall reside in a directory on the Lucent Security Management Server (LSMS). To create compatible logs, pre-configure the LSMS FTP logs feature to move the session logs to an accessible location. Then use the `Log2WELF.jar` utility to convert the logs to WebTrends Enhanced Log Format (WELF), a format compatible with Security Reporting Center. For more information about WELF, see "WebTrends Enhanced Log Format" on page 119.

## Converting LSMS Logs to WELF

To run `Log2WELF.jar` your environment must meet the following requirements:

- Java v1.3 must be installed on the computer running `Log2WELF.jar`.
- The Directory containing the Java executable must be in your `PATH`.
- The utility must run on the same computer that contains the exported LSMS log files.

**Use the following steps to run `Log2WELF.jar`:**

1. **F**rom the LSMS 6.*x* CD, copy `Tools\Reports\Log2WELF.jar` to a local directory.
2. Add the full path to `Log2WELF.jar` to your `CLASSPATH`.
   - ***If you are using Windows NT***, click **System Properties > Environment**.
   - ***If you are using Windows 2000***, click **System Properties >Advanced > Environment Variables**.

– ***If you are using Sun Solaris***, see the Solaris documentation for more information about changes to the `CLASSPATH`.

3. At a command prompt, change to the directory containing `Log2WELF.jar` and type the following:

```
" java  -DLSMSDIR= LSMS log directory  -DWELFDIR= WELF log
directory LogFileMonitor "
```

This command converts the files in the source directory to WELF and copies them to the specified target directory. You may want automate this process using local file and event scheduling utilities. You can also run this utility as part of the pre-processing phase of a scheduled event. See the *User Guide* for Security Reporting Center for more information about configuring event pre-processing tasks.

# Microsoft ISA Server 2000

## Versions Supported

Microsoft Internet Security and Acceleration Server 2000, version 3.*x*

## Getting Log Information

To create a Security Reporting Center firewall profile, you must specify the log file location. Access Microsoft ISA Server log files using either file access, FTP, or HTTP.

Microsoft ISA Server maintains three log files:

- CERN Proxy log files (used to track outgoing Web activity).
- Winsock log files.
- Packet filter log files.

The log file name is user-defined. For more information, see "Special ISA Server Configuration" on page 53.

The default location for log files is `c:\program files\Microsoft ISA Server\ISALogs`. You can verify the location in the Properties window.

## Special ISA Server Configuration

To get the most complete reports, you must verify the ISA server log format.

**To set the Microsoft ISA Server logging format:**

1. In the Microsoft ISA Server Administration console, select **Your_Server_Array > Monitoring Configuration > Logs**.
2. Right-click on CERN Proxy (or Winsock), and select **Properties**.
3. Select the **File** option.

4. From the drop-down list of logging formats, select either **ISA File Format** or **W3C File Format**.

---

**Note**
The format you select must match the format you select when creating a Security Reporting Center reporting profile.

---

5. If desired, specify the location of the log file in the **Directory** text box.
6. Indicate log file rollover frequency.

---

**Note**
The log file name is specified in the display area below the **Log File Directory** text box.

---

# Microsoft Proxy Server

## Versions Supported

Microsoft Proxy Server version 1.*x* and 2.*x*.

Microsoft Winsock version 2.*x*

## Getting Log Information

To create a Security Reporting Center firewall profile, you must specify the log file location.

Microsoft Proxy Server maintains three log files, one for each proxy (Web, Winsock, and Socks). Use the Web proxy server log file for the Security Reporting Center firewall profile. The log file name is user-defined. For more information, see "Special Proxy Server Configuration" on page 55. If you have a drive mapped to your proxy server, access your log through file access.

The default location for log files is:

```
c:\winnt\system32\msplogs\
```

You can verify the location in the Properties window. For more information, see "Special Proxy Server Configuration" on page 55.

## Special Proxy Server Configuration

To get the most complete report, you must verify the proxy server logging format.

**To set the proxy server logging format:**

1. In the Microsoft Proxy Administration console, select **Web Proxy**.
2. Right-click and select **Properties**.
3. Select the **Logging** tab. Make sure that the **Enable Logging** check box is selected..

4. In the drop-down list of logging formats, make sure that **Verbose** is selected.

5. (Optional) Specify a location in the **Log File Directory** text box.

**Note**
The log file name is specified in the display area below the **Log File Directory** text box.

# Neoteris IVE

## Versions Supported

Neoteris IVE v4.*x* and higher

## Getting Log Information

To create a Security Reporting Center profile, you must specify the log file location.

Neoteris can generate logs in Webtrends Enhanced Log Format (WELF). For more information about WELF, see "WebTrends Enhanced Log Format" on page 119. Store the converted logs in a location accessible to all the components of your Security Reporting Center installation.

## Configuring Neoteris

**To configure Neoteris to generate logs in WELF format:**

1. Log into the Admin interface using following URL:

   `https://`*`ive hostname`*`/admin/`

   where *`ive hostname`* is the host name of the Neoteris IVE.

2. Under Log/Monitoring, click the User Access tab.

3. Select **Filters**.

4. ***If you want to use the default WELF filter***, select the **WELF** check box. The default WELF log uses the following syntax:

```
id=firewall time="%date% %time%" pri=%syslogcode% fw=%localip%
vpn=%node% user=%user% realm="%realm%" roles="%roles%"
proto=%protocol% src=%sourceip% dst=%remoteip%
dstname=%remotehost% type=vpn op=%method% arg="%uri%"
result=%result% sent=%sbytes% rcvd=%rbytes% agent="%agent%"
duration=%duration% msg="%id%: %msg%"
```

5. ***If you want to create a custom WELF filter that specifies a query string and a time range***:

   **a.** Click **New Filter**.

   **b.** Select the query parameters you prefer.

   **c.** Under Export Format, click **WELF**.

   **d.** Click **Save** to save the filter.

6. To apply the filter to your logs, return to the Log menu, select the filter, from the View By Filter menu, and click **Update**.

7. To export the log, click **Save Log As**. Store the log in a location where Security Reporting Center can access it.

# Netasq Firewall

## Getting Log Versions Supported

Netasq F10-10

Netasq F10-30

Netasq F10-Unlimited

Netasq F100-2

Netasq F100-3

Netasq F100-C (all versions)

## Getting Log Information

To create a firewall profile for use with Security Reporting Center, you must specify the log file location.

By default, Netasq Firewall saves logs on its hard drive. You can move these logs to another computer using Netasq Remote Firewall Manager. However, we strongly recommend using the built-in NetIQ Syslog Service to collect log file information in a compatible format. For more information about the NetIQ Syslog Service, see the *User Guide* for Security Reporting Center. Netasq logs use the WebTrends Enhanced Log Format, or WELF. For more information about WELF, see "WebTrends Enhanced Log Format" on page 119.

When you create a firewall profile, use the following settings in the Log Files panel:

- In the **Log File Format** list, select **Netasq Log File (WELF)**.
- In the Log File Configuration area, do one of the following:
  - **a.** If you do not want to use the NetIQ Syslog Service, specify that your log files are already in a location accessible by Security Reporting Center.

**b.** If you want to use the NetIQ Syslog Service, specify that you want the NetIQ Syslog Service to collect the log

## Configuring Netasq for the NetIQ Syslog Service

The following instructions explain how to configure Netasq to send log records to the NetIQ Syslog Service.

**To configure Netasq to send log records to the NetIQ Syslog Service, use the following steps:**

1. From the Configuration menu, select **Logs**. The Log dialog box opens.
2. Select the **Forward log to an external syslog server** check box.
3. In the **Host (IP)** text box, type the IP address of the computer where the NetIQ Syslog Service is installed.
4. In the **Port** text box, type 514.
5. From the **Log facility** drop-down list, select the facility your firewall will use to send data.
6. Select all three of the log type check boxes.
7. Click **Send** to send the configuration information to the firewall.

## Configuring Netasq to Create Log Files

To configure Netasq to create its own log files, create and save the log files.

**Use the following steps to have Netasq create log files:**

1. From the Logs menu, select the log type. For example, select:
   - **File > Alarm** to create an Alarm log file
   - **File > Web** to create a Web log file
   - **File > GUI history** to create a GUI history log file.

2. After selecting the log type, select a time range such as "Last Month" from the Selection drop-down menu.

3. Click **Save**. You are prompted for a location.

4. Enter the location where the log should be saved.

5. To save your changes, click **Enregistrer**. To exit without saving your changes, click **Annuler**.

# Netopia S9500 Security Appliance

## Versions Supported

Netopia version 1.60 and later

## Getting Log Information

To create a Security Reporting Center firewall profile, you must specify the log file location.

Netopia S9500 Security Appliance does not export log files, so you must use a syslog server to collect them. We recommend using the built-in NetIQ Syslog Service. For more information about the NetIQ Syslog Service, see the *User Guide* for Security Reporting Center. Netopia logs use the WebTrends Enhanced Log Format, or WELF. For more information about WELF, see "WebTrends Enhanced Log Format" on page 119.

**Use the following settings to create a firewall profile for Netopia:**

- In the **Log File Format** drop-down list, select **Netopia S9500 Security Appliance (WELF)**.
- In the Log File Configuration area, specify that you want the NetIQ Syslog Service to collect the logs .
- In the Firewall IP address text box, type the firewall IP address of the Netopia system (the IP address used for the management of the Netopia unit) that is sending data to the NetIQ Syslog Service.

## Configuring Netopia using the Web Administration Interface

**To set up Netopia for the NetIQ Syslog Service:**

1. On the Netopia Appliance, click **Admin**.
2. Select the **Syslog** tab.

3. Set the host IP address. This is the address of the computer where the NetIQ Syslog Service is installed. It should be on the trusted side of your Netopia system.
4. Use the default host port (514) for the NetIQ Syslog Service.
5. Select the **Enable WebTrends Message** text box.

## Configuring Netopia using the Command-Line Interface (CLI)

To use the Netopia command-line interface, you must have:

- A serial cable connecting the serial line port on the firewall appliance to an empty serial port on a client computer
- A program that communicates between the firewall appliance and the client computer. This program must have the following properties:
  - Bits per second: 9600
  - Data bits: 8
  - Parity: None
  - Stop bits: 1
  - Flow control: None
- An administrator username and password.

**To set up Netopia for the NetIQ Syslog Service:**

1. Connect to the firewall appliance and log in.
2. In the Netopia CLI, type:

   ```
   get conf
   ```

   The following firewall device configuration is shown:

   ```
   set url server 0.0.0.0 15868 10
   set url message “Netopia and NetPartners WebSENSE have been set to
   block this site.”
   ```

```
set url msg-type 1
set url config disable
...
unset firewall land
set firewall default-deny
set policy outgoing “Inside Any” “Outside Any” “ANY” Permit log
count
set syslog webtrends ip 172.16.0.2
set syslog webtrends enable
```

3. Find this line in the configuration:

```
set policy outgoing “Inside Any” “Outside Any” “ANY” Permit log
count
```

As shown, this line lets all traffic from outside the firewall go to the inside, and all traffic from the inside go to the outside. Usually, more restrictive policies are defined using multiple lines.

**Note**
By default, syslog uses UDP port 514.

4. Modify all set policy lines to allow syslog traffic from the firewall appliance to the computer where Security Reporting Center is running.

**Note**
Make sure that all instances of the set policy line defined in the configuration contain the options log and count.

5. Modify the line:

```
set syslog webtrends ip 172.16.0.2
```

to indicate the IP address of the network location where syslog traffic is to be sent.

6. To find the IP address of the reporting computer, type:

```
ipconfig
```

at a command line. The reporting computer is the computer where Security Reporting Center is installed.

On a Solaris computer, type

```
ifconfig -a
```

7. In the Netopia CLI, ping this computer to verify the network connection.
8. Modify the line:

   ```
   set syslog webtrends enable
   ```

   to enable the WebTrends Enhanced Log Format for the firewall appliance logs instead of using the Netopia proprietary format. WELF format is required to generate reports.
9. Save the changes to your firewall appliance configuration. At the CLI prompt, type:

   ```
   save
   ```
10. Restart the device. Type:

    ```
    reset
    ```

# Netscape Proxy Server

## Versions Supported

Netscape Proxy Server versions 1.*x*, 2.*x*, and 3.*x*

## Getting Log Information

To create a firewall profile for use with Security Reporting Center, you must specify the log file location.

Netscape Proxy Server maintains two logs, an access log and an error log. Use the access log file for Security Reporting Center analysis. If you have a drive mapped to the Netscape Proxy server, you can access your log files directly.

The default location for logs is `c:/Netscape/SuiteSpot/admin-server/logs/access`.

## Special Firewall Configuration

**To change the log file location:**

1. In the Server Admin window, click **Admin Preference**.
2. In the **Access Log** text box, specify the location of your log files.

# NetScreen Firewall

## Versions Supported

NetScreen Firewall version 1.60 and later

## Getting Log Information

To create a Security Reporting Center firewall profile, you must specify the log file location. Because NetScreen does not export log files, a syslog server is required. We recommend using the built-in NetIQ Syslog Service. For more information about the NetIQ Syslog Service, see the *User Guide* for Security Reporting Center. NetScreen logs use the WebTrends Enhanced Log Format, or WELF. For more information about WELF, see "WebTrends Enhanced Log Format" on page 119.

Use the following log file settings when creating a firewall profile:

- Select **NetScreen Log File (WELF)** log file format.
- Specify that you want the NetIQ Syslog Service to collect the log files.
- In the **Firewall IP address** text box, type the IP address of the NetScreen system (the IP address used for the management of the NetScreen unit) that is sending data to the NetIQ Syslog Service.

## Configuring with NetScreen Web Administration Interface

**To set up NetScreen Firewall for the NetIQ Syslog Service:**

1. On the NetScreen Firewall, click **Admin**.
2. Select the **Syslog** tab.
3. Set the Host IP address. This IP address is the address of the Windows NT host where Security Reporting Center is installed. It should be on the trusted side of your NetScreen system.

4. Use the default syslog port, 514.

5. Select the **Enable WebTrends Message** check box.

## Configuring with NetScreen Command-line Interface

To use the NetScreen command-line interface (CLI), you must have:

- A serial cable connecting the serial line port on the firewall appliance to an empty serial port on a client computer
- A program that communicates between the firewall appliance and the client computer. This program must have the following properties:
  - Bits per second: 9600
  - Data bits: 8
  - Parity: None
  - Stop bits: 1
  - Flow control: None
- An administrator user name and password

**To set up NetScreen Firewall for the NetIQ Syslog Service:**

1. Connect to the firewall appliance and log in.

2. In the NetScreen CLI, type:

   ```
   get conf
   ```

   The following firewall device configuration is displayed:

   ```
   set url server 0.0.0.0 15868 10
   set url message "NetScreen and NetPartners WebSENSE
     have been set to block this site.”
   set url msg-type 1
   set url config disable
   ...
   unset firewall land
   ```

```
set firewall default-deny
set policy outgoing "Inside Any" "Outside Any" "ANY"
Permit log count
set syslog webtrends ip 172.16.0.2
set syslog webtrends enable
```

3. Find this line in the configuration:

   ```
   set policy outgoing "Inside Any" "Outside Any" "ANY" Permit log
   count
   ```

   As shown, this line lets allows traffic from outside the firewall to go inside, and all traffic from the inside to go outside. More restrictive policies are typically defined using multiple lines.

**Note**
By default, syslog uses UDP port 514.

4. Modify all "set policy" lines to allow syslog traffic from the firewall appliance to go to the computer where the NetIQ Syslog Service is running.

**Note**
Make sure all instances of the "set policy" line defined in the configuration contain the options log and count.

5. Modify the line:

   ```
   set syslog webtrends ip 172.16.0.2
   ```

   to use the IP address of the Security Reporting Center computer where syslog traffic will be sent. To obtain the IP address of the reporting computer, type `ipconfig` at a command line for a Windows computer. On a Solaris computer, type `ifconfig` –a.

6. In the NetScreen CLI, use PING to verify the network connection for this computer.

7. Modify the line:

   ```
   set syslog webtrends enable
   ```

to enable WebTrends Enhanced Log Format. This enables the WELF format for the firewall appliance logs, rather than for the NetScreen proprietary format. WELF format is required to generate reports.

8. Save the changes to your firewall appliance configuration. At the CLI prompt, type:

```
save
```

9. Restart the device. Type:

```
reset
```

# Network Appliance NetCache

## Versions Supported

NetCache v3.3 and higher

## Getting Log Information

To create a Security Reporting Center firewall profile, you must specify the log file location. To generate logs that Security Reporting Center can analyze, configure your NetCache appliance to log in W3C, squid, or NCSA format. Store the logs in a location where all Security Reporting Center components have access to them.

# Network Associates Gauntlet Firewall for UNIX

## Versions Supported

NAI Gauntlet Firewall for UNIX versions 4.*x*, 5.*x*, and 6.*x*

## Getting Log Information

To create a Security Reporting Center firewall profile, you must specify the log file location.

You can send the firewall logs to the reporting computer via FTP (using the Gauntlet computer as the FTP client and the Security Reporting Center computer as the FTP server), or you can use the NetIQ Syslog Service to collect the logs.

Because Gauntlet Firewall versions 4.*x* and 5.*x* may not export log files, we recommend using the built-in NetIQ Syslog Service to collect them. See "Configuring Gauntlet for Syslog" on page 74. Refer to the *User Guide* for Security Reporting Center for more information about the NetIQ Syslog Service.

Use the following log file settings when creating a firewall profile:

- If you are using PDK format (`http-pdk proxy`), select **NAI Gauntlet Firewall for UNIX Type 2**.
- If you are using GW format (`http_gw`), select **NAI Gauntlet Firewall for UNIX**.

## Configuring Gauntlet for Syslog

**To set up Gauntlet Firewall 4.*x* and 5.*x* to use the NetIQ Syslog Service:**

1. Edit the `/etc/syslog.conf` file on the firewall.
2. Make a copy of the last line and paste it at the end of the file so that you have two of the same line. The following line logs events to `/var/log/messages`:

   ```
   *.notice;kern.debug;mail,lpr,auth.info var/log/messages
   ```

In your copy, replace `/var/log/` with:

```
@<your NetIQ Syslog Service IP address>
```

Make sure a tab separates the items to be logged and the @ symbol.

3. To kill the syslog process, type:

```
kill -HUP <syslog process id>
```

## Sample syslog.conf File

The following sample shows how your `syslog.conf` file appears after completing the steps in the previous section.

```
# BSDI    $Id: syslog.conf,v2.1 1995/02/03 05:54:44
   salmon Exp $
# user@domain.com modified for gauntlet
#TAG=OSI
*.emerg;*.err;kern.debug;auth.notice;mail.crit
   /dev/console
*.emerg;*.err;kern.debug;auth.notice;mail.crit
   /var/log/syslog
*.notice;kern.debug;mail,lpr,auth.info
   /var/log/messages
*.notice;kern.debug;mail,lpr,auth.info
   @NetIQ Syslog Service IP address
```

For more information about the NetIQ Syslog Service, see the *User Guide* for Security Reporting Center.

**To configure Gauntlet Firewall 6.x:**

1. Open the Gauntlet Firewall user interface and log in.
2. Open the Services menu and select **HTTP**.
3. Select the configuration you want, and click **Modify**.
4. Verify that you are using Adaptive Proxy, and not Content Scanning.

5. Click **Operations**, and turn on logging for FTP requests and HTTP requests.
6. Click **OK** to save the operations changes.
7. Click **OK** again to save the configuration changes.
8. Click **Advanced**, then select **Enable Logging**.
9. Click **OK** to save your changes.
10. Open the Services menu and select **FTP**.
11. Select the configuration you want, and click **Modify**.
12. Verify that you are using Adaptive Proxy, and not Content Scanning.
13. Click **Operations**, and turn on logging for FTP requests and HTTP requests.
14. Click **OK** to save the operations changes.
15. Click **OK** again to save the configuration changes.
16. Click **OK** to save your changes.
17. Turn on logging for any other service you are interested in. It is especially useful to log activity for the Telnet, POP3, and SMTP services.
18. Save these new settings and restart the firewall services. At this point, meaningful data will begin to accumulate in the `/var/log/messages` directory.

---

**Note**

Because the year is not logged inside an exported Gauntlet log file, Security Reporting Center parses the year based on the name of the exported file. By default, Gauntlet uses one of the following date formats to name log files:

```
messages.mm.dd.yyyy

messages.dd.mm.yy
```

We strongly recommend that you use the default file names for your exported logs. If you use a file name other than the default, Security Reporting Center determines the year based on the current system date. This can lead to reporting errors.

---

# Network Associates Gauntlet Firewall for Windows NT

## Versions Supported

Gauntlet Firewall for Windows NT versions 2.*x*, 5.0, and 5.5

## Getting Log Information

To create a Security Reporting Center firewall profile, you must specify the log file location.

The most recent log file is called `gauntlet-log`.

All log files are in plain-text format or compressed `.gz` format. Log files are typically rotated according to the firewall configuration. Log file rotation is the process of naming the file (usually basing the name on the date or the day of the week), saving it, and then starting a new log file.

Gauntlet Firewall for Windows NT stores log files in a directory called `FW_Install_Dir\Logs`. A typical installation directory is `c:\Gauntlet\Logs`.

Use any of the following methods to access the log file, depending on your firewall configuration:

- Map a drive on the computer where the Reporting agent(s) are installed to the firewall, and use Security Reporting Center to browse to the appropriate log file.
- Browse to the log file using Network Neighborhood and then point Security Reporting Center to the appropriate log file.
- Use an FTP client to move the log off the firewall onto an FTP server running on a computer other than the firewall.

- Manually copy the log file to an external device such as a SyJet, Zip, or Jaz drive, and then transfer it to your reporting computer.

## Configuring Versions 2.1 and 5.0

The following logging options must be set in order to fully support firewall reports for these logs.

**To set logging options for Gauntlet Firewall:**

1. Open the Gauntlet Firewall Manager and select the Proxy tab.
2. Open the HTTP Proxy configuration window and click **Advanced**.
3. In the Advanced window, select the **Log Use** check box for every option.
4. Click **OK** to close the Advanced configuration window.
5. Click **OK** again to close the HTTP Proxy configuration window.
6. Open the FTP Proxy configuration window and click **Advanced**.
7. In the Advanced window, select the **Log Use** check box for every option.
8. Click **OK** to close the Advanced configuration window.
9. Click **OK** again to close the FTP Proxy configuration window.
10. Click **OK** to close the Proxy tab.
11. Specify Trusted policies:
12. Open the Policies tab, and open the Trusted Policy window.
13. Select **HTTP** and click **Customize**.
14. In the Customize window, click **Advanced**.
15. In the Advanced configuration window, select the **Log Use** check box for every option.
16. Click **OK** to close the Advanced configuration window.

17. Click **OK** again to close the Customize HTTP window.
18. Click **OK** to close the HTTP window.
19. In the Trusted Policy window, repeat Steps 13-18 for FTP.
20. Click OK to close the Trusted Policy window.
21. Specify Untrusted policies
22. Open the Policies tab and the Untrusted Policy window.
23. Select **HTTP** and click **Customize**.
24. When the Customize window opens, click **Advanced**.
25. In the Advanced window, make sure that all possible **Log Use** check boxes are selected.
26. Click **OK** to close the Advanced window.
27. Click **OK** again to close the Customize window.
28. Click **OK** to close the HTTP window.
29. On the Policies tab, select **FTP** and click **Customize**.
30. Repeat Steps 13-18.
31. Click **OK** to close the Untrusted Policy window.
32. Click **OK** to close the Policies tab.
33. On the toolbar, click **Apply** to save your changes.

## Configuring Version 5.5

The following logging options must be set for Security Reporting Center to fully support reporting on these logs.

**To set logging options for Gauntlet Firewall:**

1. Open the Gauntlet Firewall Manager, and select the Proxy tab.

2. Open the HTTP Proxy configuration window and click **Advanced**.
3. In the Advanced window, select the **Log Use** check boxes for HTTP, FTP, HTTPS, GOPHER, and WAIS. Do not select any other options.
4. Click **OK** to close the Advanced window.
5. Click **OK** again to close the HTTP Proxy configuration window.
6. Open the FTP Proxy window and click **Advanced**.
7. In the Advanced window, make sure that all possible **Log Use** check boxes are selected.
8. Click **OK** to close the Advanced Configuration window.
9. Click **OK** again to close the HTTP Proxy configuration window.
10. Click **OK** to close the Proxy tab.
11. Specify Trusted policies.
12. Select the Policies tab and open the Trusted Policy window.
13. Select **HTTP** and click **Customize**.
14. When the Customize window opens, click **Advanced** (if possible).
15. In the Advanced window, select the **Log Use** check boxes for HTTP, FTP, HTTPS, GOPHER, and WAIS. Do not select any other options.
16. Click **OK** to close the Advanced window.
17. Click **OK** again to close HTTP window.
18. On the Policies tab, select **FTP** and click **Customize**.
19. In the Customize window, click **Advanced** (if possible).
20. In the Advanced window, select the **Log Use** check boxes for HTTP, FTP, HTTPS, GOPHER, and WAIS. Do not select any other options.
21. Click **OK** to close the Advanced Configuration window.

22. Click **OK** again to close the Customize window.
23. Click **OK** to close the HTTP window.
24. Specify Untrusted policies.
25. On the Policies tab, open the Untrusted Policy window.
26. Select **HTTP** and click **Customize**.
27. In the Customize window, click **Advanced** (if possible).
28. In the Advanced window, select the **Log Use** check boxes for HTTP, FTP, HTTPS, GOPHER, and WAIS. Do not select any other options.
29. Click **OK** to close the Advanced window.
30. Click **OK** again to close the Customize window.
31. Click **OK** to close HTTP window.
32. On the Policies tab, select **FTP** and click **Customize**.
33. In the Customize window, click **Advanced** (if possible).
34. In the Advanced window, select the **Log Use** check boxes for all possible options.
35. Click **OK** to close the Advanced Configuration window.
36. Click **OK** again to close the Customize window.
37. Click **OK** to close the FTP window.
38. Click **OK** to close the Policies tab.
39. On the toolbar, click **Apply** to save your changes.

# Network-1 CyberwallPLUS

## Versions Supported

CyberwallPLUS 7.0*x*

## Getting Log Information

To create a Security Reporting Center firewall profile, you must specify the log file location.

CyberwallPLUS can be configured to create logs in WebTrends Enhanced Log Format (WELF), or to send log information to the built-in NetIQ Syslog Service. For more information about the NetIQ Syslog Service, see the *User Guide* for Security Reporting Center. For more information about WELF, see "WebTrends Enhanced Log Format" on page 119.

When you create a firewall profile, use the following settings in the Log Files panel:

- In the Log File Format drop-down list, select **CyberwallPLUS (WELF).**
- In the Log File Configuration area, do one of the following:
  - If you do not want to use the NetIQ Syslog Service, specify that your log files are already in a location accessible by Security Reporting Center
  - If you want to use the NetIQ Syslog Service, specify that you want the NetIQ Syslog Service to collect the logs.

## Creating WELF Logs

**To configure CyberwallPLUS to generate log files in the WELF format, use the following steps:**

1. From the User Interface, stop the Filter Engine before you make any changes.
2. Select **Logs > Log Management**.

3. Under Log Management, enable **CyberwallPLUS native** and **WebTrends WELF**.
4. Save your settings.
5. Start the Filter Engine. Given a typical installation, log files are stored in the `Program Files\Network-1\CyberwallPLUS\Logs directory`.

## Configuring CyberwallPLUS for Syslog

**To set up CyberwallPLUS to send data to the NetIQ Syslog Service:**

1. From the User Interface, stop the Filter Engine before you make any changes.
2. Select **Logs > Log Management**.
3. Under Log Management, enable **CyberwallPLUS native**, **WebTrends WELF**, and **Syslog to remote server**.
4. Enter the IP address of the computer where the NetIQ Syslog Service is running.
5. Save your changes and start CyberwallPLUS.

## Special Configuration Issues

CyberwallPLUS log files use proprietary protocols. In order for Security Reporting Center to recognize the protocols and report them, you must define the protocols using the Security Reporting Center Protocols options. For more information about protocols, see the CyberwallPLUS Rules Properties.

# Novell BorderManager Firewall Services

## Versions Supported

BorderManager Firewall Services versions 2.*x* and 3.*x*

BorderManager Firewall Enterprise Edition 3.5

## Getting Log Information

To create a Security Reporting Center firewall profile, you must specify the log file location.

The proxy logs are stored on the file system as delimited text files. Set up the type of log you want—either common or extended—and specify the location of the log in `NWADMIN` in the BM server object `/HTTP/Proxy/Details/Logging`.

**Note**
Security Reporting Center does not support indexed logs.

### How to Retrieve the Log

You can access the log file in several different ways, depending on your firewall's configuration:

- Map a drive on the Security Reporting Center Reporting agent computer to the firewall, and use Security Reporting Center to browse to the appropriate log file.
- Browse to the log file using Network Neighborhood and then configure Security Reporting Center to point to the appropriate log file.
- Use an FTP client to move the log off the firewall onto an FTP server running on a computer other than the firewall.
- Manually copy the log file to an external device such as a SyJet, Zip, or Jaz drive, and then transfer it to your reporting computer.

# RapidStream

## Versions Supported

RapidStream Manager 3.0.*x*

## Getting Log Information

To create a firewall profile for use with Security Reporting Center, you must specify the log file location. You can use the log files generated by RapidStream, or alternately you can use a syslog server. If you choose to use a syslog server, we recommend using the built-in NetIQ Syslog Service. Refer to the User Guide for Security Reporting Center for more information.

Use the following log file settings when creating a Security Reporting Center firewall profile:

- Select **RapidStream Log File (WELF)**.
- If you want to have RapidStream generate log files that can be exported and analyzed by Security Reporting Center, specify that the firewalls are in a location accessible by Security Reporting Center.
- If you want RapidStream to send log file data to the NetIQ Syslog Service, specify that you want the NetIQ Syslog Service to collect the log files.
- In the **Firewall IP address** text box, type the private IP address of the RapidStream firewall.

## Configuring RapidStream

**To generate log files that can be exported and analyzed by Security Reporting Center:**

1. In the Log Manager, select the Log Archiving tab, and click **Settings**.
2. Turn off Remote Logging.

3. Click **Apply**. All new log records are now available for exporting to a text file for analysis.

4. On the **Log Archiving** tab, select the **Traffic** check box.

5. Select a directory to save to and click **Archive Now**.

**To send log records to the NetIQ Syslog Service:**

1. In the Log Manager, select the Log Archiving tab and click **Settings**.

2. Turn on Remote Logging.

3. Enter the IP address of the computer where the NetIQ Syslog Service is installed.

4. Click **Apply**. All records after you click **Apply** are sent to the NetIQ Syslog Service, and cannot be exported to a text log file.

# Secure Computing Sidewinder

## Versions Supported

Sidewinder version 5.0.0.02 and higher

## Getting Log Information

To create a Security Reporting Center firewall profile, you must specify the log file location. Sidewinder can export firewall data to a computer accessible to Security Reporting Center.

## Configuring Sidewinder

You must export Sidewinder audit data in WELF format to a computer where it can be accessed by Security Reporting Center. This computer can reside either on a trusted network protected by Sidewinder or on the Internet.

### Sidewinder v6.*x*

**To format and export firewall audit data:**

1. Log in to the firewall
2. To switch to the admin role, type:

   ```
   srole
   ```

3. To configure the export utility, type:

   ```
   cf export add type=wt name=entry_name host=hostname user=username
   password=password targetdir=destination
   ```

where *entry_name* is the name you want to apply to this configuration entry, *hostname* is the host name or IP address of the computer to which you are exporting the files, *username* and *password* are the user name and password for FTP authentication to the destination computer, and *destination* is the directory on the destination computer where you want to save the exported files.

## Sidewinder v5.3 and earlier

To format and export the WELF files, run the Sidewinder Export Data script. This script does the following:

- Converts the raw audit data collected by Sidewinder to WELF format.
- Saves the converted data to an export file.
- Creates a cron script, which automatically initiates an FTP script. The FTP script transfers the WELF export file to a host that can be accessed by Security Reporting Center. The cron script automatically initiates a separate FTP script to transfer the WELF file once every 24 hours. See "To change the time and frequency of the format and FTP process"on page 95 for more information.

You must define an access control rule that gives permission for the FTP job to transfer the file to the specified host. If you install the default FTP access control rule on your system, it may or may not work. See Chapter 3 of the *Secure Computing Sidewinder Administration Guide* for instructions.

The FTP proxy must also be enabled. See the *Secure Computing Sidewinder Administration Guide* for more information.

**To run the Export Data script:**

1. Log into Sidewinder, then switch to the admin role:

   ```
   /usr/bin/srole admin
   ```

2. Initiate the Export Data script:

   ```
   /usr/sbin/config_exp_data -r wt
   ```

   The `-r wt` options cause the script to write the file in WELF format.

3. Type the IP address of the host to which the data will be exported. If DNS is operational you can enter the host name rather than the IP address.
4. Type the user name and password needed to log into the host computer.
5. Type the name of the directory on the host that will be used to store the WELF-formatted data file.

After the Export Data script has been initiated, Sidewinder continues to automatically format and send the WELF data once a day (usually at 2:00 a.m.) using FTP.

**To change the time and frequency of the format and FTP process:**

Edit the `/etc/crontab` file. The `crontab` file contains an entry like this:

```
# FTP the report data for third party reporting tool using
FTP_export_data.py
58 1 * * * root Admin /usr/libexec/FTP_export_data -h 111.222.333.44
-u guest -p guest -r /usr/home/guest/jane -f wt
```

These two commands specify the parameters of the FTP process. The only fields you should modify, however, are the first few fields, which specify when and how often the FTP job runs. Set all other parameters by running the `config_exp_data` script.

For example, to change the command so that the FTP process runs every two hours, change `58 1 * * *` to `0 */2 * * *`. For more information about editing this file, type:

```
man crontab
```

at the UNIX command prompt.

**To stop Sidewinder from automatically exporting the raw audit files to a separate host:**

1. Log into Sidewinder and switch to the admin role by typing:

   ```
   /usr/bin/srole/admin
   ```

2. Terminate the export data process by typing:

   ```
   /usr/sbin/config_exp_data -u
   ```

The `-u` option stops the raw audit files from being reformatted and saved to an export file.

# SonicWALL Internet Security Appliance

## Versions Supported

SonicWALL Internet Security Appliance versions 4.1 and 5.*x*

SonicWALL PRO-VX

SonicWALL PRO

SonicWALL XPRS2 or XPRS

SonicWALL DMZ

SonicWALL SOHO2 or SOHO

SonicWALL TELE2 or TELE

## Getting Log Information

You must specify the location of the syslog server file when you create a Security Reporting Center firewall profile. For step-by-step instructions on creating a profile, see the *User Guide* for Security Reporting Center.

SonicWALL does not create a log file. Instead, the firewall directs a log stream to a syslog server which writes the log information to a file. Refer to the User Guide for Security Reporting Center for more information about the NetIQ Syslog Service.

---

**Note**
The logging preferences in SonicWALL version 6.0.0.0 differ from previous versions. There are now two logging formats: WELF format and standard format. In the standard format, the source (src) and destination (dst) fields contain port number and link (i.e., WAN, LAN, DMZ) information. This information is not included in the WELF format.

---

**To configure SonicWALL to direct a log stream to the NetIQ Syslog Service:**

1. Log onto the SonicWALL appliance.

2. Click **Log** on the left side of the browser window.
3. Select the Log Settings tab.
4. Type the IP address of the computer where the NetIQ Syslog Service is installed in the **Syslog Server** text box.
5. Click **Update** at the bottom of the browser window and restart the SonicWALL appliance.

**To configure SonicWALL to direct a log stream to another syslog server:**

1. Log onto the SonicWALL.
2. Click **Log** on the left side of the browser window.
3. Select the Log Settings tab.
4. Type the IP address of the computer running the syslog server in the **Syslog Server** text box.
5. Click **Update** at the bottom of the browser window and restart the SonicWALL appliance.

# Squid

## Versions Supported

Squid Object Internet Caching Server v1.1 to v2.4

Other devices can also log Squid format.

## Getting Log Information

To create a Security Reporting Center firewall profile, you must specify the log file location.

We recommend the default Native format for squid logs. Specify the desired location for the log file in the Squid configuration file using the `cache_access_log` tag. This tag specifies the path of the `access.log` file, which logs client requests.

The following example shows the supported format:

```
time elapsed remotehost code/status bytes method URL rfc931
peerstatus/peerhost type
```

# Sun Microsystems SunScreen

## Versions Supported

SunScreen EFS 3.0b

SunScreen Secure Net 3.1

SunScreen 3.1 Lite

## Getting Log Information

You must indicate the location of the SunScreen log file when you create a profile Security Reporting Center. The process for exporting the log file to a specific location is described below.

SunScreen provides the `welfmt` utility to translate binary SunScreen log files (generated by `ssadm log get` or `ssadm log get_and_clear`) to WebTrends Enhanced Log File (WELF) format.

**To use the welfmt utility:**

1. Download the `welfmt` utility onto the SunScreen Firewall. Type the following at a command prompt to get the log from the SunScreen firewall and save it:

   ```
   # ssadm log get > bin_logfile
   ```

2. Run the `welfmt` utility by typing the following at a command prompt.

   ```
   # ./welfmt -f firewall_name -i bin_logfile > output_file
   ```

## Exporting Logs

When you create a Security Reporting Center firewall profile, designate `output_file` as the log file location.

# Symantec Enterprise Firewall

## Versions Supported

Symantec Enterprise v6.5 and v7.*x*.

AXENT Raptor Eagle versions 3.*x* and 4.*x*

AXENT Raptor versions 5.*x* and 6.*x*

## Getting Log Information

To create a Security Reporting Center firewall profile, you must specify the log file location. Log files are kept on the computer where Symantec Enterprise Firewall is installed. The exact directory path varies from version to version. Consult the Symantec documentation for the location of your log files.

By default, log files are rotated daily at 12:01 a.m. The current day's log file is called `logfile`. Logs generated before the current day are located in a separate directory at `\sg\oldlogs\logfile.date`.

**Note**
Symantec Enterprise Firewall provides a log file formatting utility called Flatten that can be used to make your log file more readable. If you use this utility, make sure that you point Security Reporting Center to the original un-flattened log files.

### Retrieving Logs on Windows

The log files created by Symantec Enterprise for Windows are text logs, which are readable by Security Reporting Center. Because Symantec Enterprise Firewall prevents you from mapping a drive to the firewall, or from running an FTP service on the firewall, you have the following options for accessing the log file.

- Use Symantec utilities to retrieve the log files. This method is recommended.

- Manually copy the log file to an external device such as a SyJet, Zip, or Jaz disk, and transfer it to a computer accessible by Security Reporting Center.

### Retrieving Log Files with Symantec Utilities

Symantec provides the following system tools, which can be used to retrieve log files.

- `Rempass.exe`
- `RemoteLogDir.exe`
- `RemoteLogFile.exe`

`Rempass.exe` is used on both the firewall computer and the computer running Security Reporting Center. `Rempass.exe` enables an authenticated and encrypted communication between the two computers and specifies which remote computer is allowed to retrieve log files remotely.

`RemoteLogDir.exe` can be run remotely after Rempass.exe has been used to allow remote log retrieval. It gives a directory listing for the directory where the firewall creates its log files.

After `RemoteLogDir.exe` determines which files are needed, `RemoteLogFile.exe` is used to retrieve specific log files.

After the log files are retrieved from the Symantec firewall, Security Reporting Center can analyze them.

For specific instructions about using these tools, see to the Symantec Enterprise Firewall and Symantec Enterprise VPN Reference Guide, which can be downloaded from the World Wide Web at
`ftp://ftp.symantec.com/public/english_us_canada/products/symantec_enterprise_firewall/nt_2000/6.5/manuals/refguidew2k65.pdf`.

## Retrieving the Log on UNIX

UNIX Symantec Enterprise requires the use of the UNIX syslog utility for Security Reporting Center to collect the logging information.

Start the syslog service on the Symantec Enterprise firewall. Set up rules that give the computer where the NetIQ Syslog Service is installed access to logging via port 514. Refer to your firewall documentation for instructions.

Create a profile in Security Reporting Center, and select the option to obtain logging data from a remote computer using the NetIQ Syslog Service. Type the IP address of the firewall where the syslog data is posted.

## Special Firewall Configuration

Symantec Enterprise Firewall lets you define generic services using GSP (Generic Service Passer) which replaces the functionality available from built-in proxy server applications.

The firewall logs limit information on the HTTP, HTTPS, or FTP protocols if your firewall is set up to use GSP instead of proxy server applications. Any detail on these protocols—for example, incoming or outgoing Web activity—may be missing from the report.

# 3Com Firewalls

## Versions Supported

3Com Officeconnect Internet Firewall 25 versions 4.1.0 and 5.*x*

3Com Officeconnect Firewall DMZ versions 4.1.0 and 5.*x*

3Com SuperStack 3 version 5.*x*

## Getting Log Information

To create a Security Reporting Center firewall profile, you must specify the log file location.

3Com firewalls do not create a log file. Instead, they direct a log stream to a syslog server which writes the log information to a file. Refer to the User Guide for Security Reporting Center for more information about the NetIQ Syslog Service.

**To configure a 3Com firewall to use the NetIQ Syslog Service (recommended):**

1. Log onto the 3Com firewall.
2. Click **Log** on the left side of the browser window.
3. Select the Log Settings tab.
4. Type the IP address of the Security Reporting Center system in the **Syslog Server** text box.
5. Click **Update** at the bottom of the browser window and restart the 3Com firewall. The 3Com firewall directs a log stream to the NetIQ Syslog Service.

**To configure a 3Com firewall to use another syslog server:**

1. Log onto the 3Com Firewall.

2. Click **Log** on the left side of the browser window.

3. Select the Log Settings tab.

4. Type the IP address of the system running the syslog server in the **Syslog Server** text box.

5. Click **Update** at the bottom of the browser window and restart the 3Com firewall. The 3Com firewall directs a log stream to the syslog server.

# TopLayer AppSwitch 3500

## Versions Supported

SecureWatch v2.1.

Also required:

TopView Network Management Utility v3.50.017

Java 2 SDK Standard Edition v1.3.1

TopFlow Data Collector Utility v3.40

## Getting Log Information

To create a firewall profile for use with a Security Reporting Center, you must specify the log file location. Because AppSwitch does not export log files, a syslog server is required. We recommend using the built-in NetIQ Syslog Service. For more information about the NetIQ Syslog Service, see the *User Guide* for Security Reporting Center.

The AppSwitch broadcasts the firewall log file to the computer running SecureWatch. The computer running SecureWatch can then be configured to send data to the NetIQ Syslog Service.

Use the following log file settings when creating a Security Reporting Center firewall profile:

- Select **TopLayer AppSwitch Log File (WELF)**.
- Specify that you want the NetIQ Syslog Service to collect the log files.
- In the **Firewall IP address** text box, type the IP address of the computer where SecureWatch is installed.

## Configuring AppSwitch Components

**Use the following steps to configure TopLayer to send data to the NetIQ Syslog Service:**

1. Make sure the SecureWatch system status is stopped.
2. Configure a Producer to direct log file data from the AppSwitch to the SecureWatch system.
3. Restart SecureWatch. Otherwise, the NetIQ Syslog Service will not receive any firewall data from the AppSwitch.

## Identifying Protocols in AppSwitch Log Files

Because AppSwitch log file data uses a unique set of activity identifiers, you must manually associate the identifiers with protocols so that Security Reporting Center can recognize protocol-specific activity in the log file.

Use the TopView Network Management Utility to view the application groups found in AppSwitch log files. Then use the Protocol configuration settings in Security Reporting Center to associate the log file text for each application group with a protocol.

# WatchGuard Technologies Firebox

## Versions Supported

WatchGuard Technologies Firebox MSS v2.*x* with SP1 or later

WatchGuard Technologies Firebox II v3.3

WatchGuard Technologies Firebox LSS v4.*x*

WatchGuard Technologies Firebox Systems v5.*x* and higher

WatchGuard Technologies Firebox Vclass

## Getting Log Information

To create a Security Reporting Center firewall profile, you must specify the log file location. For step-by-step instructions on creating a profile, see the *User Guide* for Security Reporting Center.

Because WatchGuard does not create an accessible log file, you have two choices for creating a file in WebTrends Enhanced Log Format, depending on what version of the Watchguard you are using:

- If you are using a WatchGuard Vclass firewall, use the NetIQ Syslog Service to collect the log records. The NetIQ Syslog Service is installed as part of your Security Reporting Center installation. For more information about the NetIQ Syslog Service, see the *User Guide* for Security Reporting Center.
- If you are using any other supported version of Watchguard, export the log file and convert it to WELF format. For more information about exporting log files and converting them to WELF format, see "Exporting Log Files" on page 112.

You must also add a proxy logging service such as SMTP proxy or HTTP proxy. In the proxy settings, enable **Log Accounting/Auditing Information**.

# Exporting Log Files

## LSS v4.1

This information is taken from the *WatchGuard Technologies Firebox LiveSecurity System User Guide*. Refer to that document for information about creating, editing, removing, scheduling, and running WatchGuard reports. The steps that follow focus on creating a log file that is exported in WebTrends Enhanced Log File (WELF) format.

The WatchGuard Historical Reports reporting tool creates summaries and reports of Firebox log activity. It generates these reports using the log files created by and stored on the LiveSecurity Event Processor. It also exports the log file in WELF format.

**To export WELF logs to Security Reporting Center:**

1. Start Historical Reports from the Control Center.
2. In the WatchGuard Reports dialog box, click **Add**. The Report Properties dialog box opens.
3. Type the Firebox IP address and log file name in the text boxes provided.
4. Use Output File to define the location of the generated log file. By default, the log file is saved in the WatchGuard installation directory.

   **Note**
   When you create a profile in Security Reporting Center, designate this location as the Log File URL Path.

5. Select **WebTrends Export** as the output type.
6. Follow the instructions in Chapter 16, "Generate Historical Reports," in the *WatchGuard LiveSecurity System User Guide*, or use the Help to complete the remaining fields.

## MSS Version 2.5

This information is taken from the WatchGuard Technologies *NOC Security Suite Operations Guide*. The WatchGuard for Manager Security System (MSS) Historical

Reports feature exports the currently loaded `logdb` file in WebTrends Enhanced Log File (WELF) format.

Security Reporting Center calculates information differently than WatchGuard Historical Reports. WatchGuard counts the number of transactions that occur on port 80. Security Reporting Center calculates the number of URL requests. These numbers vary because multiple URL requests may go over the same port 80 connection.

**To export WELF logs to Security Reporting Center:**

1. Start Historical Reports from the Control Center.
2. Select **File > Export > WebTrends File**. The Export Log File to WebTrends dialog box opens, displaying the default name and folder location.
3. If necessary, specify a text name and a location.

   **Note**
   When you create a profile in Security Reporting Center, designate this location as the Log File URL Path.

4. Click **Save**. The Export Properties dialog box opens.
5. Specify the time filter and the day of the report to export. Select or clear the **DNS Lookup** check box.

   **Note**
   Activating DNS lookup can considerably increase the time it takes Historical Reports to generate a report. Tailoring the report to a narrower time frame can reduce time.

6. Click **OK**. Historical Reports exports the specified parts of the log file to WELF format. The files appear in the directory designated in Step **3** with the designated name in `*.wts` format.

Refer to the *NOC Security Suite Operations Guide* for information about using information stored in the NOC workspace to develop a schedule configuration.

## SMS Version 3.3

WatchGuard SMS 3.3 ships with a utility called `WebTrendsExport.exe` that converts your `logdb` files into a format that Security Reporting Center can parse. The utility is located on your SMS administrative host in the `C:\Program Files\WatchGuard` directory.

You should also turn on logging for HTTP, FTP, Telnet, POP, and SMTP. These logs can all be exported and used by Security Reporting Center. Incoming and outgoing traffic should be explicitly logged, since WatchGuard may not be configured to do so. Doing this supplies the logging information required for all reports.

You can also choose to run DNS resolves. DNS resolves significantly extend the export time.

**To export WELF log files to Security Reporting Center using the WebTrends Update:**

1. From a command prompt, change to the directory where you installed SMS. (The default is the WatchGuard directory.)
2. To list the required parameters, type:

   ```
   WebtrendsExport
   ```

   The following parameters are shown:

   ```
   Usage:
   webtrendsexport
   [-dns] < > required [ ] = optional
   C:\Program Files\WatchGuard
   ```

3. Select the parameters to export the logs.
4. Create a profile pointing to these exported log files.

For more information, see the WatchGuard Web site.

## LSS v4.0, MSS v2.1 with SP1 and higher

The `WebtrendsExport.exe` functionality has been consolidated into `rep_cmd.exe`.

For these versions of WatchGuard, the WebtrendsExport.exe functionality has been consolidated into `rep_cmd.exe`.

Security Reporting Center calculates information differently than WatchGuard Historical Reports. WatchGuard counts the number of transactions that occur on port 80. Security Reporting Center calculates the number of URL requests. These numbers vary because multiple URL requests may go over the same port 80 connection.

You should also turn on logging for HTTP, FTP, Telnet, POP, and SMTP. These logs can all be exported and used by Security Reporting Center. Incoming and outgoing traffic should be explicitly logged, since WatchGuard may not be configured to do so. Doing this supplies the logging information required for all reports.

**To export log files to Security Reporting Center:**

1. From a command prompt, change to the directory where you installed LSS 4.0. (The default is the WatchGuard directory.)
2. To list the required parameters, type:

   ```
   rep_cmd
   ```

   The following parameters are shown:

   **Usage**

   ```
   rep_cmd <logdb file> <report type> <time interval>
   <start time> [filter] [other]
   ```

   **Required Fields**

   ```
   <logdb file> - full path of logdb file
   <report type> - [-exceptions | -urls | -time-series
   | -by-host | -by-service | -by-session | -by-user
   | -auth | -masquerade | -bytecount-by-host
   | -bytecount-by-user | -bytecount-by-email
   | -bytecount-time-series | -webtrends <file>
   | -export <file>
   <time interval> - [-annual | -monthly | -weekly | -daily]
   <start time> - -when [today | yesterday | "this week"
   | "last week" | "this month" | "last month"
   ```

```
| "this year" | "last year" | YYYY/MM/DD]
```

**Optional Fields**

```
[filter] - [-host <IP addr> | -service <port>
| -user <username>] [other] - [-dns]
```

3. Include the `-webtrends <file>` parameter to export the logs.

   For example, the following code:

   ```
   rep_cmd -logdb D:\logdb -locatlime -verbose -webtrends -annual -
   when "this year" -file logfile.log
   ```

   exports the log file `logdb` to a file called `logfile.log` in WebTrends Enhanced Log File (WELF) format. Create a profile pointing to these exported log files.

**Note**
For more information about `rep_cmd`, contact WatchGuard.

## WatchGuard Firewall Systems v4.x and higher

For these versions of WatchGuard, the `WebtrendsExport.exe` functionality has been consolidated into `rep_cmd.exe`.

Security Reporting Center calculates information differently than WatchGuard Historical Reports. WatchGuard counts the number of transactions that occur on port 80. Security Reporting Center calculates the number of URL requests. These numbers vary because multiple URL requests may go over the same port 80 connection.

You should also turn on logging for HTTP, FTP, Telnet, POP, and SMTP. These logs can all be exported and used by Security Reporting Center. Incoming and outgoing traffic should be explicitly logged, since WatchGuard may not be configured to do so. Doing this supplies the logging information required for all reports.

**To export log files to Security Reporting Center:**

1. Open Historical Reports.

2. In the Historical Reports dialog box, click **Add**.
3. In the Report Properties dialog box, select the Setup tab.
4. Select **WebTrends Export**. Do not change the directory settings.
5. Select the Firebox tab.
6. In the **Firewall IP or Name** text box, type a unique IP address or name, for example the name or IP address of the WatchGuard device.
7. Select the Time/Filters tab.
8. In the Time Span list, select **Entire Log**.
9. Select the Sections tab.
10. Click **Check All** to select all the check boxes.
11. Click **Filters** and add an Include filter that includes all data.
12. Click **OK**.
13. In the Historical Reports dialog box, select the check box for the report name and click **Run**. The Firebox creates a log file in the installation directory/logs directory.
14. Open a command prompt and navigate to the WatchGuard installation directory.
15. Run the following command:

    ```
    rep_cmd log path -firebox -webtrends outputfilename.log
    ```

    where `log path` is the path to the unconverted log file and `outputfilename.log` is the name you want to use for the generated WELF-format file. WatchGuard saves the file in the WatchGuard installation directory.

    **Note**
    The log path cannot contain spaces. If your directory paths contain spaces, use a relative path or use the ~ character to truncate the pathname.

16. Save the log file to a location where all Security Reporting Center components have access to it.

Chapter 2

# WebTrends Enhanced Log Format

This document defines the WebTrends Enhanced Log Format used by firewalls, proxy servers, and security devices. Any firewall, VPN system, proxy server, or device that uses this log format can generate logs that are compatible with Security (Firewall) Reporting Center v1.0 and later, as well as with WebTrends Firewall Suite v2.0 and later.

## Log File Format

A log file is made up of records. Each record is a single line in the file. Records are logged in chronological order, with the earliest record appearing first.

WebTrends Enhanced Log Format places no restrictions on log file names or log file rotation policies.

### Record Format

A log record is a single line terminated by the character sequence carriage return-line feed (`0x0D-0x0A`). There can be no carriage returns or line feeds within a single record.

Each log record is made up of fields. The record identifier field `(id=)` must be the first field in a record. After that, fields can be in any order.

A few fields must be present in every record, but most fields are optional. For example, fields referring to specific types of activity (for example the operation on an HTTP request) occur only in records describing that activity type.

Not all types of firewall servers log all fields. Log records that omit certain fields produce report tables that are partially incomplete. The description of each field includes notes about which tables rely on the presence of the field.

The following example shows a generalized sample record. In a log file, the record would be on a single line.

```
id=firewall time="1998-8-4 12:01:01" fw=192.168.0.238 pri=6 rule=3
proto=http src=192.168.0.23 dst=206.1.0.36 dstname=www.webtrends.com
arg=/index.htmlop=GET result=200 rcvd=1426
```

## Field Format

All fields except for `time` are terminated by spaces. If a field contains spaces, it must be enclosed in double quotes.

All fields use the form `key=value`. Fields are separated by spaces. If the value contains spaces, then it must be enclosed in double quotes. The key must use the form specified in this chapter. The value can contain any printable ASCII characters, with the following exceptions:

- The value for the fields `pri`, `duration`, `sent`, and `rcvd` must be a decimal number
- The value for `time` must use the format `yyyy-mm-dd hh:mm:ss`

# Identifying Users, Servers, and Sites

Many records, for example all records for Web, email, FTP, and Telnet activity, include a source and a destination. The source is the computer that originates the activity. The destination is the computer that receives the activity.

For example, for an internal user accessing an external Web site, the internal user is the source and the external Web site is the destination. If an external user sends an email message to an internal user, the external user is the source and the internal user is the destination.

The most basic level of source and destination information is an IP address. Reports are more meaningful when higher-level information is logged, for example resolved IP addresses or server names. Security Reporting Center can also report authenticated user names if users are authenticated through the firewall. The authenticated user field, if present, is assumed to identify an internal user.

Marshal firewall reporting applications generally use the most user-friendly identifier available to create tables and graphs. When reporting internal users, Security Reporting Center looks for the authenticated user field first, then for the user name field, and finally for the IP address. For external users, Security Reporting Center looks for the name field first and then for the IP address.

# Required Fields

Each record contains the five required fields shown in the following table.

| field | definition |
|---|---|
| id= | Record identifier |
| time= | Date/time |
| fw= | Firewall IP address or name |
| pri= | Priority of the record |
| proto= | Protocol |

The first two fields in each record must be `id=` and `time=`, in that order.

## id=

The `id` field identifies the type of record. In a WELF log, the `id` value is always `firewall`.

## time=

The `time` field shows the date and time of the event in the time zone where the event was logged. The form of the date/time field is shown below.

**Note**
Because this field contains spaces, it must be enclosed in double quotes.

The time log record uses the following format:

```
time="yyyy-mm-dd hh:mm:ss"
```

The value for year must use four digits. The values for month, day, hour, minute, and second can use either one or two digits. For example, a record for 6:00 am on January 1, 1998 can use either of the following formats:

```
time="1998-1-1 6:0:0"
time="1998-01-01 06:00:00"
```

The record for 6:00 pm on January 1, 1998 uses this format:

```
time="1998-01-01 18:00:00"
```

## fw=

The `fw` field identifies the firewall that generated the log record. Typically a firewalls is identified using an IP address or a host name. Security Reporting Center uses this field for licensing purposes to determine how many different firewalls you are currently analyzing. Licensing is simplified if the firewall is consistent in logging this field. In other words, a particular firewall should always log its IP address OR always log its machine name. If the firewall logs its IP address, it should always log the IP address of the internal network interface OR always log the IP address of the external network interface. If it logs the field inconsistently, Security Reporting Center may read the log as if it were generated by two different firewalls.

The following example shows how the field is logged using the IP address of the firewall:

```
fw=192.168.0.238
```

The following example shows how the field is logged using the host name of the firewall:

```
fw=ACME_FIREWALL
```

## pri=

The `pri` field shows the priority level for the event.

The following table shows the allowable values for the `pri` field.

| Value | Definition |
|---|---|
| `0` | emergency |
| `1` | alert |
| `2` | critical |
| `3` | error |
| `4` | warning |
| `5` | notice |
| `6` | information |
| `7` | debug |

Messages are allocated to report tables based on the priority value. Messages with priorities `0`, `1`, and `2` are placed in the critical error tables. Messages with priorities of `3` and `4` are placed in the errors and warnings tables. Messages with priorities of `5`, `6`, and `7` are placed in the informational message tables.

## proto=

The `proto` field logs the application-level protocols used by the event. Firewalls that do not log the protocol but do log the service should log the service in the `proto` field.

Marshal firewall applications track information at the application level, not the network level. Thus, the protocol field should contain information about application-level protocols such as `ftp` and `http`, not network-level protocols such as `tcp` and `udp`.

The following examples show how to log the protocol field:

```
proto=http
proto=ftp
proto=snmp
```

## Default Protocol Mappings

Security Reporting Center tracks a large number of protocols by default, including `web`, `ftp`, `http`, `80/tcp`, and `telnet`. See the Protocols panel in the Security Reporting Center application for a current list of the default protocols.

## Mapping New Protocols

If your log files contain protocols other than the default protocol mappings, you can configure Security Reporting Center to track them using the Protocols options. Unmapped protocols are tracked as a group under the protocol family `other`.

# Optional Fields

The following fields are optional:

- `rule=`
- `duration=`
- `sent=`
- `rcvd=`
- `src=`
- `srcname=`
- `dst=`
- `dstname=`
- `cat_site=`
- `cat_page=`
- `catlevel_site=`
- `catlevel_page=`
- `cat_action=`
- `user=`
- `op=`
- `arg=`
- `result=`
- `vpn=`
- `type=`
- `msg=`
- `ref=`
- `agent=`
- `cache=`

## rule=

The `rule` field logs the rule that triggered the log entry. Security Reporting Center uses this field to generate tables that help the user understand whether firewall rules are working as intended. The following report tables use the information logged in the rule field:

- Internal IP addresses triggering firewall rules
- External IP Addresses Triggering Firewall Rules
- Protocols Triggering Firewall Rules

Most firewalls log the `rule` field as an integer identifying a particular rule. However, some firewalls log rules as text names.

The following examples show how to define the rule variable.

```
rule=4
rule=deny
```

## duration=

The `duration` field shows the time required to perform the operation, in seconds. Although Marshal firewall applications track this field, it is not currently reported in any tables or graphs. However, if this information is available, we recommend logging it for use by future versions.

The following examples show two different ways to log an operation with a duration of three minutes:

```
duration=180.00
duration=180
```

## sent=

This field shows the number of bytes transferred from the source to the destination.

## rcvd=

This field shows the number of bytes transferred from the destination to the source.

## src=

This field shows the IP address that generated the event. For more information, see "Identifying Users, Servers, and Sites" on page 120.

## srcname=

The `srcname` field shows a user name or authenticated username for the source when available. This information is more detailed than the information in the `src` field. For more information, see "Identifying Users, Servers, and Sites" on page 120.

The following examples show how to log the `srcname` field.

```
srcname=mickm@webtrends.com
srcname=www.webtrends.com
srcname=JIMS_SYSTEM
```

## dst=

The `dst` field shows the IP address that received the event. For more information, see "Identifying Users, Servers, and Sites" on page 120.

## dstname=

The `dstname` field shows a user name or authenticated username for the destination when available. This information is more detailed than the information in the `dst` field. For more information, see "Identifying Users, Servers, and Sites" on page 120.

The following examples show how to log the `dstname` field.

```
dstname=WEBTRENDS_SERVER
dstname=www.webtrends.com
```

## cat_site=

For firewalls and proxy servers capable of categorizing Web sites, the `cat_site` field shows the category to which the accessed site belongs. For example, www.msnbc.com typically belongs to the General News category.

**Note**
If a field contains spaces, enclose the text in double quotes.

This field should only be present if the `dst=` or the `dstname=` field is also present. The following examples show how to log the `cat_site` field:

```
dst=www.msnbc.com cat_site=News
dst=www.msnbc.com cat_site="General News"
```

## cat_page=

For firewalls and proxy servers capable of categorizing Web pages, the `cat_page` field shows the category to which the accessed page belongs.

**Note**
If a field contains spaces, enclose the text in double quotes.

The `cat_page` field should only be present if the `arg` field is also present.

The following examples show how the `cat_page` field is logged.

```
arg=/investing/stocks.htm cat_page=”Investment”
arg=/counter-strike/newmaps.htm cat_page=”Entertainment”
```

## catlevel_site=

The `catlevel_site` field shows the category level for a Web site. The possible values for this field are `1` and `2`. Category level 1 records are used to create reports on Core category activity. Category level 2 records are used to create reports on General category activity.

Core categories (Category 1) include Drugs/Alcohol, Gambling, Hate Speech, Violence, and Sexually Explicit. General categories (Category 2) include Astrology and Mysticism, Entertainment, Games, General News, Glamour and Intimate Apparel, Hobbies, Investment, Job Search, Motor Vehicles, Personals and Dating, Real Estate, Shopping, Sports, Travel, Usenet News, and Web-based Chat.

The `catlevel_site` field should only be present if the `cat_site` field is also present.

The following examples show how to log the `catlevel_site` field:

```
dst=www.cars.com cat_site="Motor Vehicles" catlevel_site=2
cat_action=pass
dst=www.nudie.com cat_site="Sexually explicit" catlevel_site=1
cat_action=block
```

## catlevel_page=

The `catlevel_page` field shows the category level for a Web page. Possible values for this field are `1` and `2`. Category level 1 records are used to create reports on Core category activity. Category level 2 records are used to create reports on General category activity.

Core categories (Category 1) include Drugs/Alcohol, Gambling, Hate Speech, Violence, and Sexually Explicit. General categories (Category 2) include Astrology and Mysticism, Entertainment, Games, General News, Glamour and Intimate Apparel, Hobbies, Investment, Job Search, Motor Vehicles, Personals and Dating, Real Estate, Shopping, Sports, Travel, Usenet News, and Web-based Chat.

The `catlevel_page` field should only be present if the `cat_page` field is also present.

The following examples show how to log the `catlevel_page` field.

```
arg=/investing/stocks.htm cat_page="Investing" catlevel_page=2
cat_action=pass
arg=/counter-strike/newmaps.htm cat cat_page="Entertainment"
catlevel_page=2 cat_action=block
```

## cat_action=

The `cat_action` field shows the action the firewall or proxy server takes when a user requests a page or site belonging to a URL category. For example, the proxy server may block access when a user requests a gambling Web site.

The `cat_action` field should only be present if the `cat_site` or `cat_page` field is also present.

The possible values for this field are `block` and `pass`.

The following examples show how to log the `cat_action` field:

```
dst=www.gambling.com cat_site=Gambling cat_action=block
dst=www.msnbc.com cat_site=News cat_action=pass
```

## user=

The `user` field shows an authenticated user name. If users access sites through the firewall that require a user name and password, the authenticated user name can be logged in this field. For more information, see "Identifying Users, Servers, and Sites" on page 120.

The following examples show how to log the `user` field.

```
user=JohnB
user=MarySmith
```

## op=

The `op` field shows the operation associated with the logged activity. For example, `GET` and `POST` are associated with HTTP and FTP requests.

The following examples show how to log the `op` field.

```
op=GET
op=POST
```

## arg=

The `arg` field shows the URL requested in an HTTP or FTP transaction.

The following exampls show how to log the `arg` field:

```
arg=/PRODUCTS/WEBTREND/GIFS/IWAWARD2.gif
arg=/PRODUCTS/WEBTREND/download.htm?Product=Standard
```

## result=

The `result` field shows a standard result code for an HTTP request. For example, `200` is the result code for a successful file retrieval and `304` is the result code for a file returned from the cache.

## vpn=

The `vpn` field identifies a particular VPN. It is used to generate tables showing the most-used VPNs and the VPNs accessed by particular users.

The following examples show how to log the `vpn` field:

```
vpn="NY Branch VPN"
vpn=Sales
```

## type=

This field shows whether a particular event is a VPN event, a firewall management event, or both. It determines which tables will include the data for the event. To include a record in more than one category, separate the values with commas.

The following `type` values are supported:

| Value | Type |
|---|---|
| vpn | the record is a VPN event |
| mgmt | the record is a firewall management event |

The following examples show how to log the `type` value:

```
type=vpn
type=mgmt
type=vpn,mgmt
```

## msg=

The `msg` field determines the event summary tables where the data in a record will be shown  These tables classify the activity as one of the following: critical events, errors and warnings, VPN events, or firewall management events.If the user is logged using the `Src=`, `Srcname=`, `Dst=`, `Dstname`, or `User` field, Marshal firewall applications can also generate detailed tables associating users with events.

The following examples show how to log the `msg` field:

```
msg="VPN starting"
msg="Possible port scan detected"
msg="Firewall configuration changed"
```

## ref=

The `ref` field shows the referring site for incoming Web records.

## agent=

The `agent` field shows the agent (usually the browser) for incoming or outgoing Web records.

The following examples show how to log the `agent` field:

```
agent="SPRY_Mosaic/v8.32 (Windows 16-bit)”
agent="Microsoft Internet Explorer/4.40.308 (Windows 95)"
agent="Mozilla/3.0 (WinNT; I)"
```

## cache=

The `cache` field shows the proxy cache status for outgoing Web records and is used to create a report detailing proxy cache performance.

The following examples show how to log the `cache` field:

```
cache=TCP_MISS
cache=TCP_HIT
cache=Inet
```

# Sample Records

**Note**
In the following examples, records are broken up into multiple lines. In log files, each record is on one line

## Sample Web Records

The external user at IP address 132.0.92.91 requests a page from a Web site behind the firewall.

```
id=firewall time=”1998-8-4 12:01:01” fw=192.168.0.238 pri=6
rule=3 proto=http src=132.0.92.91
dst=192.168.0.36 dstname=www.webtrends.com arg=/index.html
```

```
op=GET result=200 sent=1426
```

The internal user at IP address 192.168.0.26 requests a page from a Web site outside the firewall:

```
id=firewall time="1998-8-4 12:01:01" fw=192.168.0.238 pri=6
rule=3 proto=http src=192.168.0.26
dst=192.168.0.36 dstname=www.yahoo.com arg=/index.html?abc
op=GET result=200 sent=10842
```

## Sample Email Records

The external user at IP address 203.61.93.90 sends an email message to the server www.webtrends.com:

```
id=firewall time="1998-8-4 12:01:01" fw=192.168.0.238 pri=6 rule=12
proto=smtp src=203.61.93.90 srcname=mail.sewl.com.au
dst=192.168.0.196 dstname=www.webtrends.com sent=23124
```

The internal user `webmaster@webtrends.com` sends an email message to the external address 205.229.190.12:

```
id=firewall time="1998-8-4 12:01:01" fw=192.168.0.238 pri=6 rule=12
proto=smtp user=webmaster@webtrends.com src=192.168.0.104
dst=205.229.190.12 dstname=mail.cx1.com sent=23124
```

## Sample Telnet Records

The user at IP address 192.168.0.26 initiates a telnet session with the computer at IP address 206.92.0.26:

```
id=firewall time="1998-8-4 12:01:01" fw=192.168.0.238 pri=6 rule=5
proto=telnet src=192.168.0.26 dst=206.92.0.11 sent=10842 rcvd=21222
duration=3201.32
```

## Sample FTP Records

The external user at IP address 206.92.0.11 uploads a file to `WebTrendsServer`. (Upload and download are determined by the `sent` or `rcvd` field.)

```
id=firewall time="1998-8-4 12:01:01" fw=192.168.0.238 pri=6 rule=8
proto=ftp src=206.92.0.11 dst=192.168.0.23 dstname=WebTrendsServer
sent=31124 duration=63.10
```

The external user at IP address 206.92.0.11 downloaded a file to `WebTrendsServer` (upload vs. download is determined by the `sent` or `rcvd` field):

```
id=firewall time="1998-8-4 12:01:01" fw=192.168.0.238 pri=6 rule=8
proto=ftp src=206.92.0.11 dst=192.168.0.23 dstname=WebTrendsServer
rcvd=31124 duration=63.10
```

## Sample RealAudio Records

```
id=firewall time="1998-8-4 12:01:01" fw=192.168.0.238 pri=6 rule=8
proto=RealAudio sent=431 rcvd=24184 duration=3600.00
src=192.168.0.242 dst=204.164.100.21
```

## Sample VPN Records

```
id=firewall time="1998-8-4 12:01:01" fw=192.168.0.238 pri=5
rule=6 src=122.110.1.1 type=vpn msg="VPN starting"
```

```
id=firewall time="1998-8-4 12:01:01" fw=192.168.0.238 pri=5
rule=6 src=122.110.1.1 type=vpn msg="VPN closing"
```

## Sample Management Records

```
id=firewall time="1998-8-4 12:01:01" fw=192.168.0.238 pri=5
rule=9 src=192.168.0.238 type=mgmt msg="Firewall starting"

id=firewall time="1998-8-4 12:01:01" fw=192.168.0.238 pri=5
rule=9 src=192.168.0.238 user=JohnSmith type=mgmt
msg="Firewall configuration changed"
```

## Sample Error Messages

```
id=firewall time="1998-8-4 12:01:01" fw=192.168.0.238 pri=3
rule=9 src=132.0.92.91
dst=192.168.0.36 msg="Possible port scan detected"

id=firewall time="1998-8-4 12:01:01" fw=192.168.0.238 pri=3
rule=9 dst=132.0.92.91 src=192.168.0.36 msg="Deny TCP out"
```

# Using WELF with the NetIQ Syslog Service

A firewall can use the WELF standard in conjunction with the NetIQ Syslog Service (formerly the WebTrends Syslog Service). The prefix to the syslog message is ignored when syslog log files are processed. Fields defined by WELF that might appear in the syslog prefix (for example the `pri` field) must also be present in the body of the syslog message and conform to the WELF standard.

# Index