



# Firewall Configuration Guide

Firewall Suite

August 1, 2003



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, NETIQ CORPORATION 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 STATES 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 NetIQ Corporation, 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 NetIQ Corporation. 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. NetIQ Corporation may make improvements in or changes to the software described in this document at any time.

© 1995-2003 NetIQ Corporation, all rights reserved.

U.S. Government Restricted Rights: If the software and documentation are being acquired by or on behalf of the U.S. Government or by a U.S. Government prime contractor or subcontractor (at any tier), in accordance with 48 C.F.R. 227.7202-4 (for Department of Defense (DOD) acquisitions) and 48 C.F.R. 2.101 and 12.212 (for non-DOD acquisitions), the government's rights in the software and documentation, including its rights to use, modify, reproduce, release, perform, display or disclose the software or documentation, will be subject in all respects to the commercial license rights and restrictions provided in the license agreement.

Check Point, FireWall-1, and Provider-1 are trademarks or registered trademarks of Check Point Software Technologies Ltd.

ActiveAgent, ActiveAnalytics, ActiveAudit, ActiveKnowledge, ActiveReporting, ADcheck, AppAnalyzer, Application Scanner, AppManager, AuditTrack, AutoSync, Chariot, ClusterTrends, CommerceTrends, Configuration Assessor, ConfigurationManager, the cube logo design, DBTrends, DiagnosticManager, Directory and Resource Administrator, Directory Security Administrator, Domain Migration Administrator, End2End, Exchange Administrator, Exchange Migrator, Extended Management Pack, FastTrends, File Security Administrator, Firewall Appliance Analyzer, Firewall Reporting Center, Firewall Suite, Ganymede, the Ganymede logo, Ganymede Software, Group Policy Administrator, Intergreat, Knowledge Scripts, Migrate.Monitor.Manage, Mission Critical Software, Mission Critical Software for E-Business, the Mission Critical Software logo, MP3check, NetIQ, the NetIQ logo, the NetIQ Partner Network design, NetWare Migrator, OnePoint, the OnePoint logo, Operations Manager, PentaSafe, PSAudit, PSDetect, PSPasswordManager, PSSecure, Qcheck, RecoveryManager, Security Analyzer, Security Manager, Security Reporting Center, Server Consolidator, SQLcheck, VigilEnt, Visitor Mean Business, Vivinet, W logo, WebTrends, WebTrends Analysis Suite, WebTrends for Content Management Systems, WebTrends Intelligence Suite, WebTrends Live, WebTrends Log Analyzer, WebTrends Network, WebTrends OLAP Manager, WebTrends Report Designer, WebTrends Reporting Center, WebTrends Warehouse, Work Smarter, WWWorld, and XMP are trademarks or registered trademarks of NetIQ Corporation or its subsidiaries in the United States 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 .....	ix
Conventions .....	x
About NetIQ Corporation .....	xi
<b>Configuration Instructions</b> .....	<b>1</b>
AltaVista Firewall .....	2
Versions Supported .....	2
Obtaining Log Information .....	2
AXENT Raptor Firewall .....	4
BorderWare Firewall Server .....	5
Versions Supported .....	5
Obtaining Log Information .....	5
Check Point VPN-1/FireWall-1 v4.x .....	6
Versions Supported .....	6
Obtaining Log Information .....	6
OPSEC LEA (Server-Side Configuration) .....	6
Managing Check Point OPSEC LEA Log Files .....	7
Exporting Check Point Log Files .....	8
Special Firewall Configuration .....	9
Special LEA Service Configuration .....	10
Determining the Check Point Version Number .....	11
Check Point VPN-1/FireWall-1 vNG .....	12
Supported Firewalls .....	12
Obtaining Log Information .....	12
Using OPSEC LEA .....	12
Using Exported Log Files .....	20
Special Firewall Configuration .....	23
Special LEA Service Configuration .....	24

CimTrak Web Security Edition .....	26
Versions Supported .....	26
Firewall Suite and CimTrak .....	26
Obtaining Log Information .....	26
Cisco Content Engine .....	27
Version Supported .....	27
Obtaining Log Information .....	27
Configuring ACNS .....	27
Cisco IOS Firewall and Router .....	28
Versions Supported .....	28
Obtaining Log Information .....	28
Configuring Cisco IOS for the WebTrends Syslog Service .....	28
Cisco PIX Firewall .....	31
Versions Supported .....	31
Obtaining Log Information .....	31
Configuring Cisco PIX for the WebTrends Syslog Service .....	31
CyberGuard Firewall .....	33
Versions supported .....	33
Obtaining Log Information .....	33
Fortinet FortiGate Network Protection Gateways .....	36
Versions Supported .....	36
Obtaining Log Information .....	36
Configuring the Fortinet FortiGate Network Protection Gateway .....	37
GTA Firewall Family .....	38
Versions Supported .....	38
Obtaining Log Information .....	38
Configuring the GnatBox Firewall .....	38
Inktomi Traffic Server .....	40
Versions Supported .....	40
Obtaining Log Information .....	40
Internet Dynamics Conclave .....	43
Versions Supported .....	43
Obtaining Log Information .....	43

iPrism Web Filtering Appliance .....	44
Versions supported .....	44
Obtaining Log Information .....	44
Lucent Managed Firewall .....	46
Version Supported .....	46
Obtaining Log Information .....	46
Lucent VPN Firewall .....	47
Versions Supported .....	47
Obtaining Log Information .....	47
Converting LSMS Logs to WELF .....	47
Microsoft ISA Server 2000 .....	49
Version Supported .....	49
Obtaining Log Information .....	49
Special ISA Server Configuration .....	50
Microsoft Proxy Server .....	51
Versions Supported .....	51
Obtaining Log Information .....	51
Special Proxy Server Configuration .....	52
Netasq Firewall .....	53
Versions Supported .....	53
Obtaining Log Information .....	53
Configuring Netasq for the WebTrends Syslog Service .....	54
Configuring Netasq to Create Log Files .....	54
Netopia S9500 Security Appliance .....	56
Versions Supported .....	56
Obtaining Log Information .....	56
Configuring Netopia using the Web Administration Interface .....	56
Configuring Netopia using the Command-Line Interface (CLI) .....	57
Netscape Proxy Server .....	60
Versions Supported .....	60
Obtaining Log Information .....	60
Special Firewall Configuration .....	60

NetScreen Firewall .....	61
Versions Supported .....	61
Obtaining Log Information .....	61
Configuring with Netscreen Web Administration Interface .....	61
Configuring with Netscreen Command-line Interface .....	62
Network Associates Gauntlet Firewall for UNIX .....	65
Versions Supported .....	65
Obtaining Log Information .....	65
Setting up Gauntlet for the WebTrends Syslog Service .....	66
Configuring Version 6.x .....	67
Network Associates Gauntlet Firewall for Windows NT .....	69
Versions Supported .....	69
Obtaining Log Information .....	69
Configuring Versions 2.1 and 5.0 .....	70
Configuring Version 5.5 .....	72
Network-1 CyberwallPLUS .....	75
Versions Supported .....	75
Obtaining Log Information .....	75
Configuring CyberwallPLUS to Create WELF Logs .....	75
Configuring CyberwallPLUS for the WebTrends Syslog Service .....	76
Special Configuration Issues .....	76
Novell BorderManager Firewall Services .....	77
Versions Supported .....	77
Obtaining Log Information .....	77
RapidStream .....	79
Software Versions Supported .....	79
Obtaining Log Information .....	79
Configuring RapidStream .....	80
Recourse ManHunt .....	81
Versions Supported .....	81
Obtaining Log Information .....	81

Secure Computing Sidewinder .....	82
Versions Supported .....	82
Obtaining Log Information .....	82
Configuring Sidewinder .....	82
SecureSoft SUHOSHIN .....	85
Versions Supported .....	85
Obtaining Log Information .....	85
How to Retrieve the Log .....	85
SonicWALL Internet Security Appliance .....	87
Versions Supported .....	87
Obtaining Log Information .....	87
Sun Microsystems SunScreen .....	89
Versions Supported .....	89
Obtaining Log Information .....	89
Symantec Enterprise Firewall .....	90
Versions Supported .....	90
Obtaining Log Information .....	90
Special Firewall Configuration .....	92
3Com Firewalls .....	93
Versions Supported .....	93
Obtaining Log Information .....	93
TopLayer AppSwitch 3500 .....	95
Versions Supported .....	95
Obtaining Log Information .....	95
Configuring AppSwitch Components .....	96
Identifying Protocols in AppSwitch Log Files .....	96
WatchGuard Technologies Firebox .....	97
Versions Supported .....	97
Obtaining Log Information .....	97

<b>Glossary</b>	<b>103</b>
<b>Index</b>	<b>105</b>

---

# 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 Firewall Suite. 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 Firewall Suite. It also includes information about configuring both Firewall Suite 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 Firewall Suite administration.

## Other Information in the Library

The library provides the following information resources:

### *User Guide*

Provides conceptual information about Firewall Suite. This book also provides an overview of the Firewall Suite 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
<b>Bold</b>	<ul style="list-style-type: none"><li>• Window and menu items</li><li>• Technical terms, when introduced</li></ul>
<i>Italics</i>	<ul style="list-style-type: none"><li>• Book and CD-ROM titles</li><li>• Variable names and values</li><li>• Emphasized words</li></ul>
Fixed Font	<ul style="list-style-type: none"><li>• File and folder names</li><li>• Commands and code examples</li><li>• Text you must type</li><li>• Text (output) displayed in the command-line interface</li></ul>
Brackets, such as [value]	<ul style="list-style-type: none"><li>• Optional parameters of a command</li></ul>
Braces, such as {value}	<ul style="list-style-type: none"><li>• Required parameters of a command</li></ul>
Logical OR, such as value1   value 2	<ul style="list-style-type: none"><li>• Exclusive parameters. Choose one parameter.</li></ul>

---

# About NetIQ Corporation

NetIQ Corporation is a leading provider of eBusiness infrastructure management software solutions that enable organizations to optimize the performance and availability of their Windows NT and Windows 2000 systems and applications. The company develops and markets products that provide simpler, less costly, and more secure administration and operation of corporate and service provider networks. More than 2000 customers and more than 50 of the Fortune 100 companies use NetIQ products. NetIQ Corporation - a Microsoft Premier Independent Software Vendor, a Microsoft Certified Solution Provider, ADSI Partner, and Microsoft Security Partner - is headquartered in Santa Clara, California with offices throughout the United States, Canada, Europe, and Asia.

## NetIQ Products

NetIQ Corporation provides a wide selection of enterprise products to help you manage and secure all your essential platforms, including Windows, Unix, Linux, and iSeries. These products provide the in-depth expertise you need to consolidate your management systems today, and manage the next generation of applications for tomorrow. NetIQ Corporation offers the following solutions:

### **Extensive Systems Management**

These products allow you to manage, analyze, and report on the health, performance, and availability of your mission critical Windows, Unix, and Linux applications and servers. For example, you can manage all your Exchange and Voice over IP (VoIP) essentials before, during, and after deployment. With these products, you can pinpoint network problems and resolve them quickly and effectively. You can also predict the impact of network changes, such as adding users or new applications. These products integrate with other NetIQ solutions to ensure optimal availability and performance, seamless migration, secure administration, and in-depth analysis.

### **Integrated Security Management**

These products provide real-time security event consolidation, policy enforcement, host-based intrusion detection, centralized incident management, vulnerability assessment and prevention, firewall log analysis and reporting, and security administration. This comprehensive security management covers many platforms, including Windows, Unix, Linux, NetWare, and iSeries. With the Windows security administration products, you can also manage group policy, administration workflows, and permissions on vital assets throughout your enterprise.

### **Web Analytics and Management**

These products deliver important insight into every element of Web site visitor activity, as well as improved Web site performance and availability. These solutions enhance your e business performance, resulting in higher returns on infrastructure and marketing investments and improved visitor to customer conversion rates.

## **Contacting NetIQ Corporation**

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.

**Sales:** 713-548-1700  
888-323-6768 (only in the United States and Canada)

**Sales Email:** [info@netiq.com](mailto:info@netiq.com)

**Support:** [www.netiq.com/support](http://www.netiq.com/support)

**Web Site:** [www.netiq.com](http://www.netiq.com)

# Configuration Instructions

The following sections describe how to configure each supported firewall, proxy server, and security device to work with WebTrends Firewall Suite. Each section covers the location of log files, any necessary format conversions, and the method(s) used to provide access to the log files before they can be analyzed. Where applicable, we provide information about how to configure the firewall and Firewall Suite to produce more useful and readable reporting.

# AltaVista Firewall

## Versions Supported

AltaVista Firewall 97

AltaVista Firewall 98

## Obtaining Log Information

To create a firewall profile for use in your WebTrends firewall application, you must specify the log file location.

### Log File Locations

The AltaVista Firewall maintains separate logs for every protocol, each having a .log extension. You can create a single report based on all of these log files by specifying \*.log to identify the logs as a set.

All log files, except outgoing web activity logs for the current day, are stored in the root directory of your firewall installation, for example

*fw\_install\_dir\\*.log.*

Log files older than the current day are located in a dated subdirectory such as

*fw\_install\_dir\log\19980725\\*.log.*

All Outgoing Web Activity logs, including the log for the current day, are stored in the wwwlog directory, a subdirectory of your firewall installation directory, such as *fw\_install\_dir\wwwlog\hs{date].log.*

### How to Access the Logs

AltaVista Firewall lets you map a drive from a computer to the firewall. To access the log files directly, it is recommended that you create a mapped drive from the computer running Firewall Suite to the firewall.

For example, if you create a firewall profile for today's activity and map the f: drive to the firewall from the Firewall Suite computer, the log file path URL in your profile looks like this:

```
file:///f:\dfw\*.log
```

The log file path URL for a report on yesterday's activity looks like this:

```
file:///f:\dfw\log\%Date-1%%YYYY%%MM%%DD%\*.log
```

The log file path URL for a report on last month's activity looks like this:

```
file:///f:\dfw\log\%%YYYY%%MM\*.log
```

If you create a profile showing Outgoing Web activity, and map the f: drive to the firewall from the Firewall Suite computer, your log file path URL looks like this:

```
file:///f:\dfw\wwwlog\*.log
```

Since log files for both the current day and previous days are located in the same directory, specifying \*.log accesses all the firewall logs as a set.

For more information about using date macros, see the *User Guide* for Firewall Suite.

# AXENT Raptor Firewall

See “Symantec Enterprise Firewall” on page 90

# 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 Firewall Suite, you must specify the log file location.

### 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 the pipe character (|) to separate the two files.

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

## Versions Supported

- Check Point™ VPN-1®/FireWall-1® versions 4.0 and 4.1.

## Obtaining Log Information

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

Firewall Suite 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.
- *Exported logs*. You can export the logs to text files.

## OPSEC LEA (Server-Side Configuration)

### 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 Firewall Suite 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

3. Modify the firewall's LEA configuration to use an unauthenticated connection.

---

**Note**

If you switch from using an authenticated OPSEC LEA connection with a previous version of Firewall Suite, remove all profiles associated with the authenticated connection.

---

## Setting Up or Modifying Connections

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

### 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. Use the LEA Connections options to finish creating the connection.

## Managing Check Point OPSEC LEA Log Files

Firewall Suite retrieves the Check Point OPSEC LEA log data where configured. Any profile that points to this LEA connection, for example,

```
SRC_Install_Dir\leacache\192.168.0.26.dat\
```

uses that directory.

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

## Exporting Check Point 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.

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

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

When you create the Check Point security policy, set the tracking option to create `.log` files, or to create both `.log` and `.a.log` files. For more information, see “Special Firewall Configuration” on page 9.

---

**Note**

A semicolon delimiter between fields is required in exported log files.

---

## Exporting Logs for Check Point VPN-1/FireWall-1 v4.x

### To export Check Point v4.x log files:

1. On the computer where the Check Point 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:

- a.** To export the `fw.log` file, type:

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

- b.** To export the `fw.a.log` file, type:

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

- 4.** Make sure that the Firewall Suite computer can access the log files. Either map a drive to the firewall from the computer running Firewall Suite, or copy the log files to an accessible computer.

## Special Firewall Configuration

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

### Tracking

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 Firewall Suite requires to create useful report except for bandwidth information.
- **Accounting** adds bandwidth information to the logs and creates both `.a.log` 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 Firewall Suite Protocol options. Otherwise, Firewall Suite 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 Firewall Suite.

## Load Balancing and Fault-Tolerant Systems

### 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 Firewall Suite 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, Firewall Suite 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 use the `webtrend.ini` file, located in the Firewall Suite installation directory, to change settings for the WebTrends LEA Service. Make sure the header `[LEA]` appears in the `webtrend.ini` file before the LEA settings.

### Debug Level

To change the level of debugging output that is written to the LEA Service log files, change the `debugLevel` value in the `webtrend.ini` file. The default value is 1. The LEA service supports values between 1 and 5 .

### Name Logging for Check Point LEA

By default, the WebTrends LEA Service logs the text name of the Check Point firewall. If you want the firewall name to be logged as an IP address, add the following line in the `webtrend.ini` file:

```
LogFWIP=1
```

To make the WebTrends LEA Service log the text name again, delete this line or set the `LogFWIP` value to 0.

## Determining the Check Point Version Number

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.

# Check Point VPN-1/FireWall-1 vNG

## Supported Firewalls

Check Point FireWall-1 vNG

Check Point™ VPN-1 vNG

For convenience, we refer to this firewall as Check Point NG in the rest of this chapter.

## Obtaining Log Information

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

Firewall Suite 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.
- *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 13.
- A clear connection with no authentication or encryption. For more information, see “Configuring a Clear Connection” on page 19.

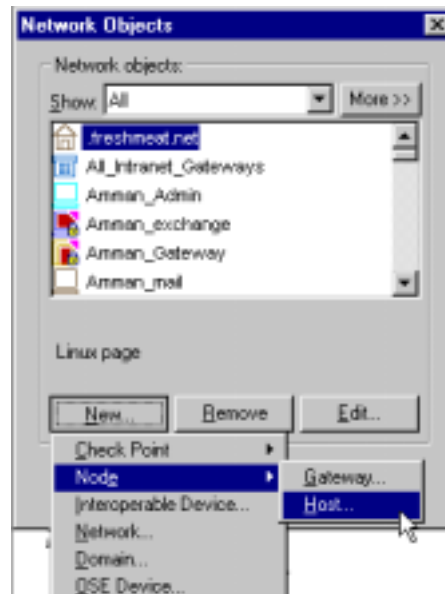
We recommend using `sslca`, the default connection method, because it is an extremely secure method. To use a connection method not documented in this *Guide*, refer to the Check Point documentation or contact Check Point technical support.

## **Configuring an `sslca` Connection**

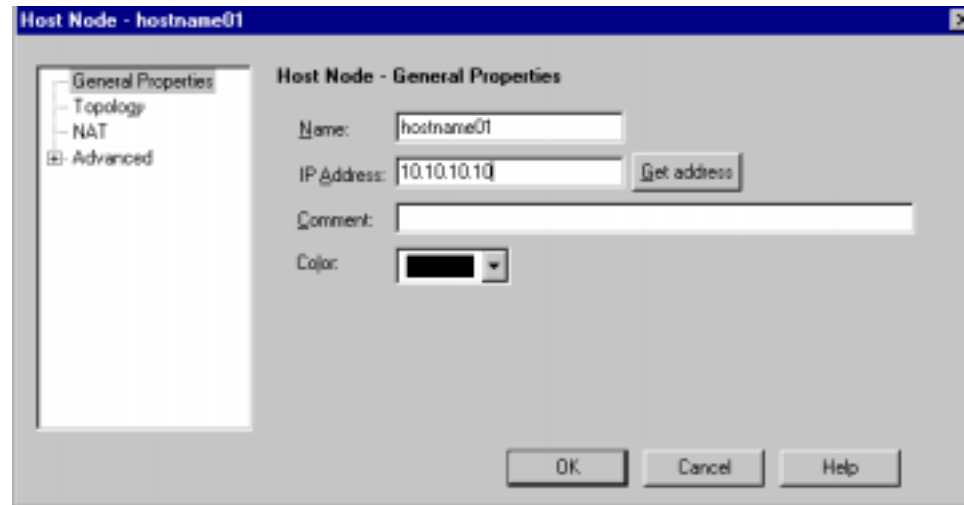
The following information describes the settings for using the default connection, using `sslca`. `sslca` is a 3DES encryption scheme that uses certificate-based authentication. To create an `sslca` connection, configure the Check Point firewall using the Check Point Policy Editor, request a certificate from the Check Point computer, and then use the LEA Connections options in Firewall Suite 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.



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 WebTrends LEA Service is installed. The information you type in this dialog box defines the computer as a network object. The name is case-sensitive.

---

**Note**

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

---

4. Click **Close**.

5. Select **OPSEC Applications** from the Manage menu

6. Click **New** and select **Opsec Application** from the list to define Firewall Suite as an OPSEC application.



In the **Name** field, 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.

---

**Note**

Type a name other than src or src. These names are already in use.

---

7. From the Host list, select the object you created in Step 3.

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. The 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**.

---

**Note**

When the certificate is created, the **Trust State** field displays `Initialized but trust not established`. 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."

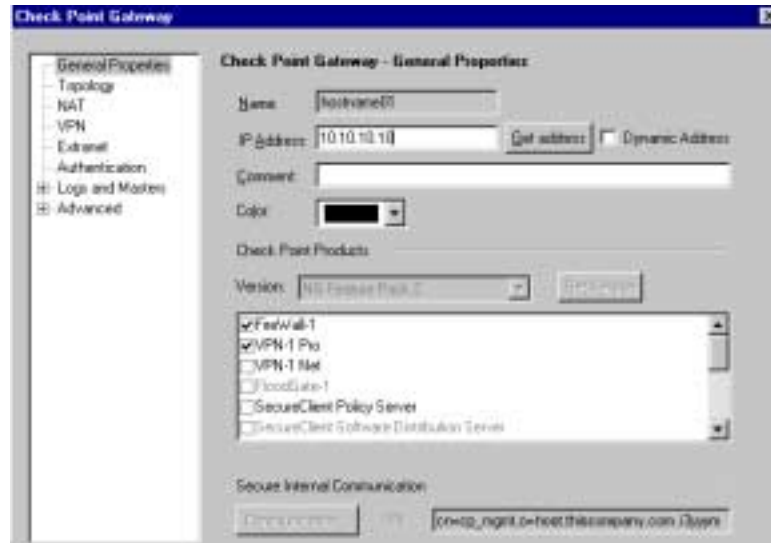
---

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.

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 Firewall Suite computer, 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 you point to in the Location dialog box of the Firewall Suite LEA Connection wizard.
23. Restart the WebTrends LEA Service. If you experience any problems with communication between the Check Point Management Server and the WebTrends LEA Service, restart the computers where both are installed.

## 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 WebTrends LEA Service. To create a clear connection, configure both the `fwopsec.conf` file on the Check Point Management Server and the `lea.conf` file on the computer where the WebTrends LEA Service is installed.

---

### Note:

We recommend using a clear connection only if you are unable to use `sslca` or another secure connection type.

---

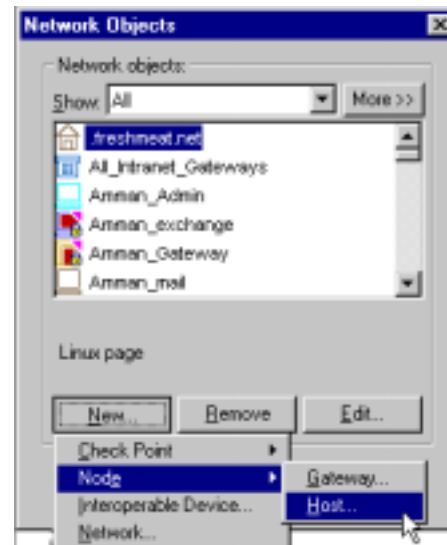
### To set up a clear connection:

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. Open the Policy Editor on the Check Point Management Server.
4. Ensure that the rule set allows OPSEC LEA communication between the firewall and the WebTrends LEA service.



## 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. For more information, see “Special Firewall Configuration” on page 23.

---

**Note**

The delimiter between fields in exported log files must be a semi-colon.

---

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 Firewall Suite can access the log files. Either map a drive to the firewall from the computer running Firewall Suite, or copy the log files to another computer accessible to Firewall Suite.

## 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.

### To configure HTTP reporting:

1. Click **Resources** on the Firewall Manage page.
2. Click **New** and select **URL**.
3. Type 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. Under Schemes, select all the check boxes.
6. Type an asterisk (\*) in the **Other** text box.
7. Under Methods, select all the check boxes.
8. Type an asterisk (\*) in the **Other** text box.
9. Type an asterisk (\*) in the **Host** text box, the **Path** text box, and the **Query** text box.
10. Click **OK**.

**To configure SMTP reporting:**

1. Click **Resources**.
2. Click **New** and select **SMTP**.
3. Type all the necessary information.
4. Select the Match tab.
5. Type an asterisk (\*) in the **Sender** text box and the **Recipient** text box.
6. Click **OK**.

**To configure FTP reporting:**

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

5. Type an asterisk (\*) in the Path box.
6. Select the **Get** check box and the **Put** check box under Methods.
7. Click **OK**.

After you follow these steps, create new rules for http, ftp, and smtp resource objects.

## Special Firewall Configuration

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

### Tracking

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 Firewall Suite requires to create useful report except for bandwidth information.
- **Accounting** adds bandwidth information to the logs.

### 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 Firewall Suite Protocol options. Otherwise, Firewall Suite 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 Firewall Suite.

## Load Balancing and Fault-Tolerant Systems

### 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 Firewall Suite 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, Firewall Suite 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 use the `webtrend.ini` file, located in the Firewall Suite installation directory, to change settings for the WebTrends LEA Service. Make sure the header `[LEA]` appears in the `webtrend.ini` file before the LEA settings.

### Debug Level

To change the level of debugging output that is written to the LEA Service log files, change the `debugLevel` value in the `webtrend.ini` file. The default value is 1. The LEA service supports values between 1 and 5.

### Download Time Lag

By default, the NetIQ LEA Service downloads log records for Check Point vNG only after they have aged for 3000 seconds (50 minutes). For example, the LEA Service does not download a record time-stamped 2:30 until 3:20. Because Check Point does not log bandwidth statistics for an individual connection until it closes, this time lag ensures that a connection has closed and bandwidth data is available.

To adjust the time lag before downloading records, change the `LagwindowSec` value in the `webtrend.ini` file. Specify a higher value to create a longer lag time and increase the likelihood of collecting bandwidth statistics. The minimum `LagwindowSec` value is 30 seconds. The maximum value is 86400 seconds.

## Time Between Sessions

During each LEA session, the NetIQ LEA Service initiates a connection, downloads all available records, and then closes the connection. By default, the LEA service waits 300 seconds (5 minutes) before starting another session.

To adjust the elapsed time between LEA sessions for Check Point vNG firewalls, change the `sessionSuspendTimeSec` value in the `webtrend.ini` file. Specify a smaller value to force more frequent downloads. The minimum `sessionSuspendTimeSec` value is 30 seconds. The maximum value is 300 seconds.

## Name Logging for Check Point LEA

By default, the WebTrends LEA Service logs the text name of the Check Point firewall. If you want the firewall name to be logged as an IP address, add the following line in the `webtrend.ini` file:

```
LogFWIP=1
```

To make the WebTrends LEA Service log the text name again, delete this line or set the `LogFWIP` value to 0.

# CimTrak Web Security Edition

## Versions Supported

CimTrak Web Security Edition v1.3.2.0

## Firewall Suite and CimTrak

CimTrak is not a firewall or proxy server, but Firewall Suite can create reports using the security information that it logs. CimTrak creates log files in the WebTrends Enhanced Log Format (WELF), which is compatible with Firewall Suite. Create a profile for CimTrak as you would for a firewall or proxy server.

## Obtaining Log Information

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

### Log File Location

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

## Version 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 readable by Firewall Suite, we recommend using the default log format, Squid. You should also configure the Content Engine to generate transaction logs and automatically send them to a Firewall Suite-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 Firewall Suite 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, Firewall Suite reports show firewall events in terms of the time zone where Firewall Suite 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 Firewall Suite, you must specify the log file location. Because Cisco IOS does not export log files, we recommend using the WebTrends Syslog Service. Refer to the *User Guide* for Firewall Suite for information about the WebTrends Syslog Service.

## Configuring Cisco IOS for the WebTrends Syslog Service

Firewall Suite 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. This 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 will 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 Firewall Suite 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
```

5. 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 Firewall Suite, 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 WebTrends Syslog Service. Refer to the *User Guide* for Firewall Suite for more information about the WebTrends Syslog Service.

## Configuring Cisco PIX for the WebTrends Syslog Service

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

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

#### To configure Cisco PIX for Firewall Suite:

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 WebTrends Syslog Service.

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

**3. Type:**

```
syslog host FWS_machine_IP
```

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

## Configuring Version 4.2(2) and Higher

### To configure Cisco PIX for Firewall Suite:

**1.** Telnet to the PIX firewall.

**2.** Type:

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

where `FWS_machine_IP` is the IP address of the computer where the WebTrends 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 Firewall Suite produces less detailed information, especially in incoming and outgoing reports.

For more information, see your Cisco PIX firewall documentation.

# 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 Firewall Suite, you must specify the log file location.

### How to Retrieve the Log

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

## Generating the Firewall Log

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**.

### Configurable Log Files

**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:
  - To write activity records to the system log file in compatible format:
    - a. Select **Send Activity Reports to Syslog (WebTrends format)**.
    - b. Select a facility (the system component generating the problem message). The default is **local7**.
    - c. Select a level (problem severity). The default is **Notice Message Priority**.
    - d. Type the IP address to which CyberGuard should write the syslog information.
  - To write activity records to a local log file, **Select Log Activities to a File (WebTrends format)**. The location of the log file is `/var/audit_logs/webTrends`.
4. Select the Alerts page, and select the check boxes for the events you want to monitor.
5. View the records generated by the selected alerts and activities.
  - a. Click **Reports**, and select **Activity Reports**.
  - b. 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**.
6. The real-time data in the file `/var/audit_logs/webTrends` is displayed. This data is used for Firewall Suite 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 later is required.

---

## Obtaining Log Information

To create a Firewall Suite 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 WebTrends Syslog Service. Refer to the Firewall Suite *User Guide* for information about the WebTrends Syslog Service.

### **Use the following log file settings when creating a Firewall Suite firewall profile:**

- 1. Select Fortinet FortiGate (WELF).**
- 2. Select Use Syslog** to have the WebTrends Syslog Service collect the log files.
- 3. 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 WebTrends 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 WebTrends Syslog Service.
9. Make sure that the **Log All Events** check box is selected.
10. Click **Apply**.

# GTA Firewall Family

## Versions Supported

GnatBox v3.3.0 or later

## Obtaining Log Information

To create a firewall profile, you must specify the log file location. Because the GTA firewall family does not export a WebTrends-compatible log file, a syslog server is required. We recommend using the built-in WebTrends Syslog Service. For more information about the WebTrends Syslog Service, refer to the *User Guide* for Firewall Suite.

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

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

## Configuring the GnatBox Firewall

**To configure the GnatBox to send data in WELF format to the WebTrends 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 WebTrends 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.

# Inktomi Traffic Server

## Versions Supported

Traffic Server version 3.5.2 and higher

## Obtaining Log Information

To create a firewall profile for use with Firewall Suite, you must specify the log file location.

### 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.

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.

### Special 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. Support for the WebTrends Extended Log File (WELF) format is achieved through the custom log facility. For details, see “Understanding Traffic Server Logs” in the Inktomi Traffic Server *Administrator’s Guide* 3.5, or “Working with Log Files” in the Inktomi Traffic Server *Administrator’s Guide* 4.0.

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 WebTrends Extended Log File format is limited to the traditional style. However, versions 4.0 and higher 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 the WELF in the `logs.config` file.

### To manually define an entry:

1. In a text editor, open the `logs.config` file in a text editor.
2. Insert the following, 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="%<cqh1> 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 the WELF format in 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.

# Internet Dynamics Conclave

## Versions Supported

Internet Dynamics Conclave version 2.10

## Obtaining Log Information

To create a Firewall Suite firewall profile, you must specify the log file location.

By default, Conclave logs are stored at *InstallDir\conclave\logs*. You can, however, define a different location for logs using the executable *r1.exe*.

You can retrieve Conclave logs by mapping a drive to the log directory on the Conclave machine, or by using FTP.

To FTP your logs, you must set up access filters on Conclave. Refer to the Conclave web site or documentation for instructions.

Firewall Suite retrieves the audit logs. Conclave audit logs are named:

*ADT-domain\_name-machine\_name-atomic\_time*

# iPrism Web Filtering Appliance

## Versions supported

iPrism Version 3.200 and higher

## Obtaining Log Information

To create a firewall profile for use with Firewall Suite, you must specify the log file location. Because iPrism exports WELF log file information via the syslog protocol, a syslog server is required. We recommend using the built-in WebTrends Syslog Service. For more information about the WebTrends Syslog Service, see the *User Guide* for Firewall Suite

Use the following settings to create a firewall profile:

- Select **Webtrends Enhanced Log File (WELF)** log file format.
- Specify that you want the WebTrends 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

**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 WebTrends Syslog Service is installed.
5. Select the **WELF** check box to use WELF format.

6. Firewall Suite 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

## Version Supported

Lucent Managed Firewall versions 3.x and 4.x

## Obtaining Log Information

To create a Firewall Suite firewall profile, you must specify the log file location.

### 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.

### How to Retrieve the Log

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 Firewall Suite.

# Lucent VPN Firewall

## Versions Supported

Lucent Security Management Server v6.0.471

Lucent VPN Firewall Brick - Models 201, 20, 300

## Obtaining Log Information

Logs for the Lucent VPN Firewall reside in a directory on the Lucent Security Management Server (LSMS). The administrator must pre-configure the LSMS FTP logs feature to move the session logs to an accessible location. The administrator can then use the `Log2WELF.jar` utility Logs to convert the logs locally to WebTrends Enhanced Log Format (WELF), a format compatible with Firewall Suite.

## 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:

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

4. *If you are using Windows 2000* click **System Properties >Advanced > Environment Variables**.
5. 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 Firewall Suite for more information about configuring event pre-processing tasks.

# Microsoft ISA Server 2000

## Version Supported

Microsoft Internet Security and Acceleration Server 2000

## Obtaining Log Information

To create a Firewall Suite firewall profile, you must specify the log file location.

### Which Log File to Use

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 50.

### Log File Location

The default location for log files is `c:\program files\Microsoft ISA Server\ISALogs`. You can easily verify the location in the Properties window. See “Special ISA Server Configuration” for details.

### Log File Retrieval

Access Microsoft ISA Server log files with file, FTP, and HTTP access.

## 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 Firewall Suite 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

## Obtaining Log Information

To create a Firewall Suite firewall profile, you must specify the log file location.

### Which Log File to Use

Microsoft Proxy Server maintains three log files, one for each proxy (Web, Winsock, and Socks). Use the Web proxy server log file for the Firewall Suite firewall profile. The log file name is user-defined. See “Special Proxy Server Configuration” on page 52 for details.

### Log File Location

The default location for log files is:

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

You can easily verify the location in the Properties window. See “Special Proxy Server Configuration” on page 52 for details.

### How to Retrieve the Log

If you have a drive mapped to your proxy server, access your log through file access.

## 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.

---

# Netasq Firewall

## Versions Supported

Netasq F10-10  
Netasq F10-30  
Netasq F10-Unlimited  
Netasq F100-2  
Netasq F100-3  
Netasq F100-C (all versions)

## Obtaining Log Information

To create a firewall profile for use with Firewall Suite, 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 WebTrends Syslog Service to collect log file information in a compatible format. Refer to the Firewall Suite *User Guide* for more information about the WebTrends Syslog Service.

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

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

## Configuring Netasq for the WebTrends Syslog Service

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

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

1. From the Configuration menu, select **Logs**. The Log dialog is shown.
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 WebTrends 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 higher

## Obtaining Log Information

To create a Firewall Suite 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 WebTrends Syslog Service. Refer to the *User Guide* for Firewall Suite for more information about the WebTrends Syslog Service.

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

1. In the Log File Format drop-down list, select **Netopia S9500 Security Appliance (WELF)**.
2. In the Log File Configuration area, specify that you want the WebTrends Syslog Service to collect the logs.
3. 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 WebTrends Syslog Service.

## Configuring Netopia using the Web Administration Interface

### To set up Netopia for the WebTrends 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 WebTrends Syslog Service is installed. It should be on the trusted side of your Netopia system.
4. Use the default host port (514) for the WebTrends 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 user name and password.

### To set up Netopia for the WebTrends 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 Firewall Suite 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.

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

```
ipconfig
```

at a command line. The reporting computer is the computer where Firewall Suite is installed.

On a Solaris computer, type

```
ifconfig -a
```

6. In the Netopia CLI, ping this computer to verify the network connection.

7. Modify the line:

```
set syslog webtrends enable
```

to enable the WebTrends Enhanced Log File (WELF) format for the firewall appliance logs instead of using the Netopia 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. Reboot the device. Type:

```
reset
```

# Netscape Proxy Server

## Versions Supported

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

## Obtaining Log Information

To create a firewall profile for use with Firewall Suite, 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 Firewall Suite 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 higher

## Obtaining Log Information

To create a Firewall Suite 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 WebTrends Syslog Service. Refer to the *User Guides* for Firewall Suite for information about the WebTrends Syslog Service.

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

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

## Configuring with Netscreen Web Administration Interface

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

1. On the Netscreen Firewall, click **Admin**, and select the Syslog tab.
2. Set the Host IP address. This IP address is the address of the Windows NT host where Firewall Suite is installed. It should be on the trusted side of your NetScreen system.
3. Use the default syslog port (514).
4. 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 WebTrends Syslog Service:

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

```
get conf
```

This displays the firewall device configuration shown here:

```
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 WebTrends 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
```

using the IP address of the network location where syslog traffic will be sent.

To get the IP address of the reporting computer, type `ipconfig` at a command line on a Windows computer where Firewall Suite is installed.

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 the WebTrends Enhanced Log File (WELF) 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. Reboot the device. Type:

```
reset
```

# Network Associates Gauntlet Firewall for UNIX

## Versions Supported

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

## Obtaining Log Information

To create a Firewall Suite 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 Firewall Suite computer as the FTP server), or you can use a syslog server to collect the logs.

Because Gauntlet Firewall versions 4.x and 5.x may not generate log files, we recommend using the built-in **WebTrends Syslog Service** to collect them. See “Setting up Gauntlet for the WebTrends Syslog Service” on page 66. Refer to the *User Guide* for Firewall Suite for more information about the WebTrends 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**.

# Setting up Gauntlet for the WebTrends Syslog Service

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

1. Edit the `/etc/syslog.conf` file on the firewall.
  - a. 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. This line logs events to `/var/log/messages`:

```
*.notice;kern.debug;mail,lpr,auth.info var/log/messages
```
  - b. In your copy, replace `/var/log/` with:

```
@<your webTrends syslog service IP address>
```

Make sure a tab separates the items to be logged and the `@` symbol.
2. To kill the syslog process, type:

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

## Sample syslog.conf File

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

```
# BSDI    $Id: syslog.conf,v 2.1 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
@webTrends Syslog Service IP address
```

Refer to the *User Guide* for Firewall Suite for information about the WebTrends Syslog Service.

## Configuring Version 6.x

### 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 a Gauntlet log file, Firewall Suite 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 logs. If you use a file name other than the default, Firewall Suite 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

## Obtaining Log Information

To create a Firewall Suite firewall profile, you must specify the log file location.

### Which Log Files to Use

The most recent log file is called `gauntlet-log`. Running reports on this file gives you the most recent data.

### Log File Location

All the log files are either kept in plain-text format or compressed in `.gz` format. The log files are usually rotated, and the rotation of the logs depends on 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`.

You can 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 Firewall Suite to browse to the appropriate log file.
- Browse to the log file using Network Neighborhood and then point Firewall Suite 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, then 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, then click **Advanced**.
7. In the Advanced window, select the **Log Use** check box on every option where it appears.
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:
  - a. Open the Policies tab, and open the Trusted Policy window.
  - b. Select **HTTP**, and click **Customize**.
  - c. When the Customize window opens, click **Advanced**.

- d.** In the Advanced configuration window, select the **Log Use** check box for every option.
  - e.** Click **OK** to close the Advanced configuration window.
  - f.** Click **OK** again to close the Customize HTTP window.
  - g.** Click **OK** to close the HTTP window.
  - h.** In the Trusted Policy window, repeat Steps **c** through **g** for FTP.
  - i.** Click **OK** to close the Trusted Policy window.
- 12.** Specify Untrusted policies
- a.** Open the Policies tab, and open the Untrusted Policy window.
  - b.** Select **HTTP**, and click **Customize**.
  - c.** When the Customize window opens, click **Advanced**.
  - d.** In the Advanced window, make sure that all possible **Log Use** check boxes are selected.
  - e.** Click **OK** to close the Advanced window.
  - f.** Click **OK** again to close the Customize window.
  - g.** Click **OK** to close the HTTP window.
  - h.** On the Policies tab, select **FTP** and click **Customize**.
  - i.** Repeat Steps **c** through **g**.
  - j.** Click **OK** to close the Untrusted Policy window.
- 13.** Click **OK** to close the Policies tab.
- 14.** On the toolbar, click **Apply** to save your changes.

## Configuring Version 5.5

The following logging options must be set for Firewall Suite 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, then 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.
  - a. Select the Policies tab, and open the Trusted Policy window.
  - b. Select **HTTP**, and click **Customize**.
  - c. When the Customize window opens, click **Advanced** (if possible).
  - d. In the Advanced window, select the **Log Use** check boxes for HTTP, FTP, HTTPS, GOPHER, and WAIS. Do not select any other options.
  - e. Click **OK** to close the Advanced window.
  - f. Click **OK** again to close HTTP window.

- g.** On the Policies tab, select **FTP** and click **Customize**.
  - h.** When the Customize window opens, click **Advanced** (if possible).
  - i.** In the Advanced window, select the **Log Use** check boxes for HTTP, FTP, HTTPS, GOPHER, and WAIS. Do not select any other options.
  - j.** Click **OK** to close the Advanced Configuration window.
  - k.** Click **OK** again to close the Customize window.
  - l.** Click **OK** to close the HTTP window.
- 12.** Specify Untrusted policies.
- a.** On the Policies tab, open the Untrusted Policy window.
  - b.** Select **HTTP**, and click **Customize**.
  - c.** When the Customize window opens, click **Advanced** (if possible).
  - d.** In the Advanced window, select the **Log Use** check boxes for HTTP, FTP, HTTPS, GOPHER, and WAIS. Do not select any other options.
  - e.** Click **OK** to close the Advanced window.
  - f.** Click **OK** again to close the Customize window.
  - g.** Click **OK** to close HTTP window.
  - h.** On the Policies tab, select **FTP** and click **Customize**.
  - i.** When the Customize window opens, click **Advanced** (if possible).
  - j.** In the Advanced window, select the **Log Use** check boxes for all possible options.

- k.** Click **OK** to close the Advanced Configuration window.
  - l.** Click **OK** again to close the Customize window.
  - m.** Click **OK** to close the FTP window.
- 13.** Click **OK** to close the Policies tab.
- 14.** On the toolbar, click **Apply** to save your changes.

# Network-1 CyberwallPLUS

## Versions Supported

CyberwallPLUS 7.0x

## Obtaining Log Information

To create a Firewall Suite firewall profile, you must specify the log file location.

CyberwallPLUS can be configured to create logs in the compatible WELF format, or to send log information to the built-in WebTrends Syslog Service. Refer to the Firewall Suite *User Guide* for more information about the WebTrends Syslog Service.

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

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

## Configuring CyberwallPLUS to Create WELF Logs

**To configure CyberwallPLUS to generate log files in the Firewall Suite-compatible 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 the WebTrends Syslog Service

### To set up CyberwallPLUS to send data to the WebTrends 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 WebTrends Syslog Service is running.
5. Save your changes and start CyberwallPLUS.

## Special Configuration Issues

CyberwallPLUS log files use proprietary protocols. In order for Firewall Suite to recognize the protocols and report them, you must define the protocols using the Firewall Suite 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

## Obtaining Log Information

To create a Firewall Suite firewall profile, you must specify the log file location.

### 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**

Firewall Suite 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 Firewall Suite Reporting agent computer to the firewall, and use Firewall Suite to browse to the appropriate log file.
- Browse to the log file using Network Neighborhood and then configure Firewall Suite 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

## Software Versions Supported

RapidStream Manager 3.0.x

## Obtaining Log Information

To create a firewall profile for use with Firewall Suite, 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 WebTrends Syslog Service. Refer to the *User Guide* for Firewall Suite for more information.

### **Use the following log file settings when creating a Firewall Suite firewall profile:**

Select **RapidStream Log File (WELF)**.

- If you want to have RapidStream generate log files that can be exported and analyzed by Firewall Suite, specify that the firewalls are in a location accessible by Firewall Suite.
- If you want RapidStream to send log file data to the WebTrends Syslog Service:
  - a. Specify that you want the WebTrends Syslog Service to collect the log files.
  - b. In the **Firewall IP address** text box, type the private IP address of the RapidStream firewall.

# Configuring RapidStream

## Using RapidStream Log Files

**To generate log files that can be exported and analyzed by Firewall Suite:**

1. In the Log Manager, select the Log Archiving tab, and click **Settings**.
2. Turn off Remote Logging.
3. Click **Apply**. At this point, all new log records will be 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**.

## Using the WebTrends 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 WebTrends Syslog Service is installed.
4. Click **Apply**. All records will be sent to the IP address specified, and will not be available for export to a text log file.

# Recourse ManHunt

## Versions Supported

ManHunt v1.2

## Obtaining Log Information

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

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

1. Select **Recourse ManHunt (WELF)**.
2. Specify that the log files are already in a location accessible by Firewall Suite.

ManHunt creates proprietary log files, which are stored in `/usr/manhunt/dbs`. These log files need to be converted to the WELF log file standard. Recourse provides scripts and an RPL to convert the log files to WELF format. For more information, consult the Recourse Web site at [www.recourse.com](http://www.recourse.com).

---

**Note**

ManHunt log files do not provide information about network traffic, so reports will not include information about bandwidth or activity type.

---

# Secure Computing Sidewinder

## Versions Supported

Sidewinder version 5.0.0.02 and higher

## Obtaining Log Information

To create a Firewall Suite firewall profile, you must specify the log file location.

Sidewinder can export firewall data to a computer accessible to Firewall Suite.

## Configuring Sidewinder

You must export Sidewinder audit data in WELF format to a workstation or host where it can be accessed by Firewall Suite. This workstation or host can be on a trusted network protected by Sidewinder, or it can be a host that resides somewhere on the Internet.

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 Firewall Suite. 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 83.

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 Chapter 4 of 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 similar to 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 details on 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:

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

2. Terminate the export data process:

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

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

# SecureSoft SUHOSHIN

## Versions Supported

SecureSoft SUHOSHIN versions 2.0 and 3.0

## Obtaining Log Information

You must specify the location of the log file when you create a profile. For step-by-step instructions on creating a profile, see the *User Guide* for Firewall Suite.

## How to Retrieve the Log

The SUHOSHIN logs are stored at the following locations, by report type:

- General Firewall Activity and Outgoing Web Activity reports are stored at:

`/opt/SUHOSHIN/web/yyyymmdd.cnx`

- Incoming Web Activity reports are stored at:

`/opt/SUHOSHIN/web/yyyymmdd.log`

These logs are in a proprietary format. However, SecureSoft provides a conversion utility that will produce log files that are compatible with Firewall Suite.

The conversion utility is a perl script named `ss2wt.pl`. It is shipped with the SUHOSHIN software, and is available directly from SecureSoft.

## Using the `ss2wt.pl` Conversion Utility

Use the following syntax:

```
ss2wt.pl options input_file output_file
```

where:

- *options* is one of the following:

`--help, -?, /?` Display help information.

`-v` Display version information.

`-p` Display progress information to STDERR. Progress information is not displayed unless both *input\_file* and *output\_file* are specified.

- *input file* is the SUHOSHIN log file to be converted.
- *output file* is the location for the converted log file.

If *input\_file* is not specified, `ss2wt.pl` takes input from `STDIN`.

If *input\_file* is specified but *output\_file* is not, `ss2wt.pl` prints all output to `STDOUT`.

# SonicWALL Internet Security Appliance

## Versions Supported

SonicWALL Internet Security Appliance versions 4.1, 5.x and 6.x

SonicWALL PRO-VX

SonicWALL PRO

SonicWALL XPRS2 or XPRS

SonicWALL DMZ

SonicWALL SOHO2 or SOHO

SonicWALL TELE2 or TELE

## Obtaining Log Information

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

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 Firewall Suite for more information about the WebTrends Syslog Service.

---

### Note

The logging preferences in SonicWALL version 6.0.0.0 differ from those of earlier 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 WebTrends 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 Firewall Suite system in the **Syslog Server** text box.
5. Click **Update** at the bottom of the browser window and restart the SonicWALL appliance for the change to take effect.

**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 system 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 for the change to take effect.

# Sun Microsystems SunScreen

## Versions Supported

SunScreen EFS 3.0b

SunScreen Secure Net 3.1

SunScreen 3.1 Lite

## Obtaining Log Information

You must indicate the location of the SunScreen log file when you create a profile Firewall Suite. For more information about exporting the log file to a specific location, see “Exporting Logs to Firewall Suite” on page 89.

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 to Firewall Suite

When you create a Firewall Suite firewall profile, designate `output_file` as the log file location.

# Symantec Enterprise Firewall

## Versions Supported

Symantec Enterprise v6.5 and v7.0

AXENT Raptor Eagle versions 3.x and 4.x

AXENT Raptor versions 5.x and 6.x

## Obtaining Log Information

To create a Firewall Suite firewall profile, you must specify the log file location.

### 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 Firewall Suite to the original un-flattened log files.

---

## Retrieving the Logs on Windows

The log files created by Symantec Enterprise for Windows are text logs, which are readable by Firewall Suite. 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 Firewall Suite.

### 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 Firewall Suite. `Rempass.exe` enables an authenticated and encrypted communication between the two computers and it specifies what 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.

Once the log files are retrieved from the Symantec firewall, Firewall Suite can be configured to analyze those log files.

For specific instructions about using these tools, refer 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](ftp://ftp.symantec.com/public/english_us_canada/products/symantec_enterprise_firewall/nt_2000/6.5/manuals/refguidew2k65.pdf).

## How to Retrieve the Log on UNIX

UNIX Symantec Enterprise requires the use of the UNIX syslog utility for Firewall Suite to collect the logging information.

1. Start the syslog service on the Symantec Enterprise firewall. Set up rules that give the computer where the WebTrends Syslog Service is installed access to logging via port 514. Refer to your firewall documentation for instructions.
2. Create a profile in Firewall Suite, and select the option to obtain logging data from a remote computer using the WebTrends Syslog Service. Type the IP address of the firewall where the syslog data is posted.

## Special Firewall Configuration

### GSP versus EagleNT Proxy Server applications

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

## Obtaining Log Information

To create a Firewall Suite 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 Firewall Suite for more information about the WebTrends Syslog Service.

### **To configure a 3Com firewall to use the WebTrends 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 Firewall Suite system in the **Syslog Server** text box.
5. Click **Update** at the bottom of the browser window and restart the 3Com firewall for the change to take effect. The 3Com firewall then directs a log stream to the WebTrends 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 for the change to take effect. 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

## Obtaining Log Information

To create a firewall profile for use with a Firewall Suite, 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 WebTrends Syslog Service. Refer to the *User Guide* for Firewall Suite for information about the WebTrends Syslog Service.

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 WebTrends Syslog Service.

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

- Select **TopLayer AppSwitch Log File (WELF)**.
- Specify that you want the WebTrends 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

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 WebTrends 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 Firewall Suite 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 Firewall Suite to associate the log file text for each application group with a protocol.

# WatchGuard Technologies Firebox

## Versions Supported

WatchGuard Technologies Firebox II version 3.3

WatchGuard Technologies Firebox LSS version 4.x

WatchGuard Technologies Firebox MSS version 2.x SP1 or later

## Obtaining Log Information

You must indicate the location of the WatchGuard Technologies Firebox log file when you create a Firewall Suite firewall profile. For more information about exporting the log file to a specific location, see “Exporting Log Files to Firewall Suite” on page 97. For step-by-step instructions on creating a profile, see the *User Guide* for Firewall Suite.

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 to Firewall Suite

### LSS Version 4.1

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 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 log files to Firewall Suite:

1. Start Historical Reports from the Control Center.
2. On the Control Center toolbar, click **Historical Reports**. The WatchGuard Reports dialog box opens. (You can also start Historical Reports from the WatchGuard installation directory by running `WGReports.exe`.)
3. In the WatchGuard Reports dialog box, click **Add**. The Report Properties dialog opens.
4. Type the Firebox IP address and log file name in the text boxes provided.
5. Use Output File to define the location of the generated log file. By default, the log file is generated into the WatchGuard installation directory.

---

**Note**

When you create a profile in Firewall Suite, designate this location as the Log File URL Path.

---

6. Select **WebTrends Export** as the output type.
7. 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.

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

**To export log files to Firewall Suite:**

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 location.

---

**Note**

When you create a profile in Firewall Suite, 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 Firewall Suite 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 Firewall Suite. 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 extends the export time.

**To export log files to Firewall Suite 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.

More documentation is available on the WatchGuard Web site.

## LSS Version 4.0, MSS Version 2.1 SP1 or Later

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

### To export log files to Firewall Suite:

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]
```

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

The following code, for example:

```
rep_cmd -logdb D:\logdb -locatime -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.

---

---

# Glossary

**department** A designated group of IP or network addresses that defines a department or other subgroup found on the network.

**profile** A set of user-defined criteria that determines how firewall log file information will be collected.

**WebTrends Syslog Service** The built-in syslog server installed with Firewall Suite. Certain firewalls do not generate accessible log files. The WebTrends Syslog Service collects log records and writes them to a specified location.

**WebTrends LEA Service** The WebTrends service that retrieves log file records from a properly configured Check Point Management Server.

**WELF** WebTrends Expanded Log Format, a WebTrends-compatible standard log format that allows a variety of firewalls to produce readable log files.



---

# Index

## Numerics

- 3Com Firewalls
  - configuring to use other syslog servers 93
  - configuring to use the Webtrends Syslog Service 93
  - obtaining log information 93
  - versions supported 93

## A

- Alta Vista Firewall
  - accessing logs 2
  - obtaining log information 2
  - versions supported 2
- AXENT Raptor
  - versions supported 90

## B

- BorderManager
  - log file location 77
  - obtaining log information 77
  - retrieving the log 77
  - versions supported 77

- BorderWare
  - log file location 5
  - obtaining log information 5
  - versions supported 5

## C

- Check Point v4.x
  - determining version number 11
  - fault-tolerant systems 10
  - firewall name logging 10
  - LEA service configuration 10
  - LEA Service debug level 10
  - LEA unauthenticated connection 7
  - load balancing 10
  - obtaining log information 6
  - OPSEC LEA configuration 6–??
  - OPSEC LEA log file management 7
  - special configuration notes 9
  - troubleshooting 9
  - versions supported 6
- Check Point vNG
  - clear connection to LEA 19
  - collecting logs with OPSEC LEA 12
  - exported log files 20
  - fault-tolerant systems 24

- firewall name logging 25
- LEA download time lag 24
- LEA service configuration 24
- LEA Service debug level 24
- load balancing 24
- protocols logged 21
- special configuration issues 23
- sslca connection to LEA 13
- supported firewalls 12
- time between LEA sessions 25
- troubleshooting 23
- CimTrak Web Security Edition
  - and firewall analysis 26
  - obtaining log information 26
  - versions supported 26
- Cisco Content Engine
  - configuring ACNS 27
  - obtaining log information 27
  - versions supported 27
- Cisco IOS
  - configuring to use the WebTrends Syslog Service 28
  - obtaining log information 28
  - versions supported 28
- Cisco PIX
  - and WebTrends Syslog Service
    - configuring for version 4.2(2) and higher 32
    - configuring for versions earlier than 4.2(2) 31
  - configuring to use the Webtrends Syslog Service 31
  - obtaining log information 31
  - versions supported 31
- Conclave 43
  - obtaining log information 43
  - versions supported 43

- CyberGuard
  - generating audit log files 34
  - generating configurable log files 34
  - generating the firewall log 34
  - obtaining log information 33
  - retrieving the log 33
  - versions supported 33
- CyberwallPLUS firewall
  - configuring Firewall Suite 75

## F

- Firebox
  - exporting log files
    - from LSS version 4.0 101
    - from LSS version 4.1 97
    - from MSS version 2.1 SP1 or later 101
    - from MSS version 2.5 98
    - from SMS version 3.3 99
    - using the WebTrends update 100
  - obtaining log information 97
  - versions supported 97
- Fortinet FortiGate
  - configuring for the WebTrends Syslog Service 37
  - obtaining log information 36
  - versions supported 36

## G

- Gauntlet Firewall for UNIX
  - configuring to use the WebTrends Syslog Service 66
  - configuring version 5.5 72
  - configuring version 6.0 67

- obtaining log information 65
- sample syslog.conf file 66
- versions supported 65
- Gauntlet for Windows NT
  - configuring versions 2.1 and 5.0 70
  - log file location 69
  - obtaining log information 69
  - versions supported 69
  - which log files to use 69
- GnatBox. See GTA Firewall Family
- GSP
  - Symantec Enterprise 92
- GTA Firewall Family
  - configuring for the WebTrends Syslog Service 38
  - obtaining log information 38
  - versions supported 38

## I

- Inktomi Traffic Server
  - obtaining log information 40
  - special configuration for reports 40
    - activating custom logging 41
    - defining the WELF format 41
  - versions supported 40
- Internet Dynamics Conclave 43
- iPrism Web Filtering Appliance
  - configuring to generate WELF 44
  - multiple activity categories 44
  - obtaining log information 44
  - versions supported 44

## L

- Lucent Managed Firewall
  - how to retrieve log 46
  - log file location 46
  - obtaining log information 46
  - versions supported 46
- Lucent VPN Firewall
  - converting files to WELF 47
  - Log2welf.jar 47
  - obtaining log information 47
  - versions supported 47

## M

- Microsoft ISA Server 2000
  - how to retrieve the log 49
  - log file location 49
  - obtaining log information 49
  - special configuration for reports 50
  - versions supported 49
  - which log file to use 49
- Microsoft Proxy Server
  - how to retrieve the log 51
  - log file location 51
  - obtaining log information 51
  - special configuration for reports 52
  - versions supported 51
  - which log file to use 51

## N

- Netasq Firewall 53
  - configuring for Firewall Suite 53
  - configuring to create its own log file 54
  - configuring to use the Webtrends Syslog Service 54
  - obtaining log information 53

Netopia  
  configuring using command-line interface 57  
  configuring with user interface 56  
  obtaining log information 56  
  profile settings 56  
  versions supported 56

Netscape Proxy Server  
  log file location 60  
  obtaining log information 60  
  special configuration 60  
  versions supported 60  
  which log file to use 60

Netscape Proxy server  
  changing the log file location 60

NetScreen  
  configuring with command line 62  
  configuring with user interface 61  
  obtaining log information 61  
  profile settings 61, 65, 95  
  versions supported 61

Network Associates Gauntlet  
  See Gauntlet

## O

OPSEC LEA  
  configuration 6-??

## R

RapidStream  
  configuring  
    to generate readable files 80  
  configuring to use the WebTrends Syslog Service 80  
  monitoring syslog performance 81

  obtaining log information 79  
  profile settings 79, 81  
  versions supported 79

Raptor Firewall  
  See Axent Raptor.

Recourse ManHunt  
  obtaining log information 81  
  versions supported 81

## S

Sidewinder  
  configuring 82  
  obtaining log information 82  
  versions supported 82

SonicWALL  
  configuring to use other syslog servers 88  
  configuring to use the WebTrends Syslog Service 88  
  obtaining log information 87  
  versions supported 87

SUHOSHIN  
  converting log format 86  
  how to retrieve the log 85  
  obtaining log information 85  
  ss2wt.pl conversion utility 86  
  versions supported 85

SunScreen  
  exporting log files to Firewall Suite 89  
  obtaining log information 89  
  versions supported 89

Symantec Enterprise  
  how to retrieve the log 91  
  log file location 90  
  log retrieval utilities 91  
  obtaining log information 90

- special configuration 92
- UNIX syslog utility 92
- versions supported 90

## **T**

- TopLayer AppSwitch
  - configuring to use the WebTrends Syslog Service 96
  - obtaining log information 95
  - protocols 96
  - versions supported 95

## **W**

- WatchGuard
  - exporting log files to Firewall Suite 97
  - LSS version 4.0, MSS version 2.1 SP1 101
    - Export log files to WebTrends 102
  - SMS version 3.3 99