

# WatchGuard® System Manager Reference Guide

---

WatchGuard System Manager v8.3



---

## Notice to Users

---

Information in this guide is subject to change without notice. Companies, names, and data used in examples herein are fictitious unless otherwise noted. No part of this guide may be reproduced or transmitted in any form or by any means, electronic or mechanical, for any purpose, without the express written permission of WatchGuard Technologies, Inc.

## Copyright, Trademark, and Patent Information

---

Copyright© 1998 - 2006 WatchGuard Technologies, Inc. All rights reserved.

Complete copyright, trademark, patent, and licensing information can be found in the WatchGuard System Manager User Guide. A copy of this book is automatically installed into a subfolder of the installation directory called Documentation. You can also find it online at:  
<http://www.watchguard.com/help/documentation/>

All trademarks or trade names mentioned herein, if any, are the property of their respective owners.

Software Version: WSM 8.3

Document Version: Reference-8.3-352-2672-001

---

### ADDRESS:

505 Fifth Avenue South  
Suite 500  
Seattle, WA 98104

### SUPPORT:

[www.watchguard.com/support](http://www.watchguard.com/support)  
[support@watchguard.com](mailto:support@watchguard.com)  
U.S. and Canada +877.232.3531  
All Other Countries +1.206.613.0456

### SALES:

U.S. and Canada +1.800.734.9905  
All Other Countries +1.206.521.8340

### ABOUT WATCHGUARD

WatchGuard is a leading provider of network security solutions for small- to mid-sized enterprises worldwide, delivering integrated products and services that are robust as well as easy to buy, deploy and manage. The company's Firebox X family of expandable integrated security appliances is designed to be fully upgradeable as an organization grows and to deliver the industry's best combination of security, performance, intuitive interface and value. WatchGuard Intelligent Layered Security architecture protects against emerging threats effectively and efficiently and provides the flexibility to integrate additional security functionality and services offered through WatchGuard. Every WatchGuard product comes with an initial LiveSecurity Service subscription to help customers stay on top of the security landscape with vulnerability alerts, software updates, expert security instruction and superior customer care. For more information, please call (206) 521-8340 or visit [www.watchguard.com](http://www.watchguard.com).

# Contents

---

CHAPTER 1 Internet Protocol Reference .....	1
Internet Protocol Header .....	1
<i>IP header number list</i> .....	2
Internet Protocol Options .....	4
Transfer Protocols .....	5
<i>UDP</i> .....	5
<i>TCP</i> .....	6
<i>ICMP</i> .....	6
<i>Other protocols</i> .....	6
Standard Ports and Random Ports .....	6
CHAPTER 2 MIME Content Types .....	7
CHAPTER 3 Services and Ports .....	19
Ports Used by WatchGuard Products .....	19
Ports Used by Microsoft Products .....	20
Well-Known Services List .....	21
CHAPTER 4 Log Messages .....	27
Introduction to Logging .....	27
Traffic Logs .....	28
<i>Packet Filter Logs</i> .....	28
<i>Proxy Logs</i> .....	30
Alarm Logs .....	36
Event Logs .....	41
<i>Event Log Messages</i> .....	43
Firebox Log File XML DTD and Schema .....	55
Firebox® X Edge Log Messages .....	56
CHAPTER 5 WebBlocker Content .....	69
Searching for Blocked Sites .....	69

---

WebBlocker Categories .....	69
CHAPTER 6 Resources .....	75
Publishers .....	75
Books .....	76
<i>Non-Fiction</i> .....	76
<i>Fiction</i> .....	76
White Papers & Requests for Comments .....	76
Mailing Lists .....	77
General IT and Security Web Sites .....	77
White Hat Web Sites .....	79
Grey Hat Sites .....	80
Other Web Sites .....	81
Dictionaries of Computer Terminology .....	82
RSS Feeds .....	82
<i>Security Feeds</i> .....	82
<i>IT Related Feeds</i> .....	83
<i>Fun Feeds</i> .....	83

---

Internet Protocol (IP) sets the format of packets and the address pattern for sending data through the Internet. It operates as a postal system, and allows you to address a package and drop it into the system. But, there is no direct link between you and the recipient. In other words, there is no package.

Most networks mix IP with higher level protocols such as Transmission Control Protocol (TCP). TCP/IP makes a connection between two host servers. Then, they can send messages to each other. TCP/IP supplies the “packaging.”

## Internet Protocol Header

---

Internet Protocol (IP) is an Internet standard that enables the sending of datagrams — packets of information that include an address and instructions on how to send the datagram to its destination. IP prepends a header to each datagram. The IP header contains a minimum of 12 properties, and other optional properties.

Property	Size	Description
Version	4 bits	IP format number (Current version = 4)
IHL	4 bits	Header length in 32-bit words (Minimum = 5)
TOS	8 bits	Type of service sets routing priorities. It is usually not used because not many application layers can set it.
Tot_Len	16 bits	Total length of packet measured in octets. It is used to assemble fragments.
ID	16 bits	Packet ID, used to assemble fragments.
Flags	3 bits	Miscellaneous flags
Frag_Off	13 bits	Identifies fragment part for this packet.
TTL	8 bits	Time to live. It sets the maximum time the datagram remains alive in the system.
Protocol	8 bits	IP protocol number. Indicates which of TCP, UDP, ICMP, IGMP, or other Transport protocol is inside.

Property	Size	Description
Check	16 bits	Checksum for the IP header
Sour_Addr	32 bits	Source IP address
Dest_Addr	32 bits	Destination IP address
Options	24 bits	IP Options (Present if IHL is 6)

## IP header number list

The IP Protocol header contains an 8-bit field that identifies the protocol for the transport layer for the datagram.

Keyword	Number	Protocol
	0	Reserved
ICMP	1	Internet Control Message
IGMP	2	Internet Group Management
GGP	3	Gateway-to-Gateway
IP	4	IP-within-IP (encapsulation)
ST	5	Stream
TCP	6	Transmission Control Protocol
UCL	7	UCL
EGP	8	Exterior Gateway Protocol
IGP	9	Any private interior gateway
BBN-RCC-MON	10	BBN RCC Monitoring
NVP-II	11	Network Voice Protocol
PUP	12	PUP
ARGUS	13	ARGUS
EMCON	14	EMCON
XNET	15	Cross Net Debugger
CHAOS	16	Chaos
UDP	17	User Datagram Protocol
MUX	18	Multiplexing
DCN-MEAS	19	DCN Measurement Subsystems
HMP	20	Host Monitoring
PRM	21	Packet Radio Measurement
XNS-IDP	22	XEROX NS IDP
TRUNK-1	23	Trunk-1
TRUNK-2	24	Trunk-2
LEAF-1	25	Leaf-1
LEAF-2	26	Leaf-2
RDP	27	Reliable Data Protocol
IRTP	28	Internet Reliable Transaction
ISO-TP4	29	ISO Transport Protocol Class 4
NETBLT	30	Bulk Data Transfer Protocol

Keyword	Number	Protocol
MFE-NSP	31	MFE Network Services Protocol
MERIT-INP	32	MERIT Internodal Protocol
SEP	33	Sequential Exchange Protocol
3PC	34	Third Party Connect Protocol
IDPR	35	Inter-Domain Policy Routing Protocol
XTP	36	XTP
DDP	37	Datagram Delivery Protocol
IDPR-CMTP	38	IDPR Control Message Transport Protocol
TP++	39	TP++ Transport Protocol
IL	40	IL Transport Protocol
SIP	41	Simple Internet Protocol
SDRP	42	Source Demand Routing Protocol
SIP-SR	43	SIP Source Route
SIP-FRAG	44	SIP Fragment
IDRP	45	Inter-Domain Routing Protocol
RSVP	46	Reservation Protocol
GRE	47	General Routing Encapsulation
MHRP	48	Mobile Host Routing Protocol
BNA	49	BNA
ESP	50	Encapsulated Security Payload
AH	51	Authentication Header
I-NLSP	52	Integrated Net Layer Security TUBA
SWIPE	53	IP with Encryption
NHRP	54	NBMA Next Hop Resolution Protocol
	55-60	Unassigned
	61	Any host internal protocol
CFTP	62	CFTP
	63	Any local network
SAT-EXPAK	64	SATNET and Backroom EXPAK
KRYPTOLAN	65	Kryptolan
RVD	66	MIT Remote Virtual Disk Protocol
IPPC	67	Internet Pluribus Packet Core
	68	Any distributed file system
SAT-MON	69	SATNET Monitoring
VISA	70	VISA Protocol
IPCV	71	Internet Packet Core Utility
CPNX	72	Computer Protocol Network Executive
CPHB	73	Computer Protocol Heart Beat
WSN	74	Wang Span Network
PVP	75	Packet Video Protocol
BR-SAT-MON	76	Backroom SATNET Monitoring

---

## Internet Protocol Options

Keyword	Number	Protocol
SUN-ND	77	SUN NDPROTOCOL-Temporary
WB-MON	78	WIDEBAND Monitoring
WB-EXPAK	79	WIDEBAND EXPAK
ISO-IP	80	ISO Internet Protocol
VMTP	81	VMTP
SECURE-VMTP	82	SECURE-VMTP
VINES	83	VINES
TTP	84	TTP
NSFNET-IGP	85	NSFNET-IGP
DGP	86	Dissimilar Gateway Protocol
TCF	87	TCF
IGRP	88	IGRP
OSPFIGP	89	OSPFIGP
SPRITE-RPC	90	Sprite RPC Protocol
LARP	91	Locus Address Resolution Protocol
MTP	92	Multicast Transport Protocol
AX.25	93	AX.25 Frames
IPIP	94	IP-within-IP Encapsulation Protocol
MICP	95	Mobile Internetworking Control Protocol
SCC-SP	96	Semaphore Communications Security Protocol
ETHERIP	97	Ethernet-within-IP Encapsulation
ENCAP	98	Encapsulation Header
	99	Any private encryption scheme
GMTP	100	GMTP
	101-254	Unassigned
	255	Reserved

---

## Internet Protocol Options

Internet Protocol (IP) options are additions to the standard IP header that can be of different lengths. Enabling IP options can be dangerous. Hackers can use them to create routing that helps them get access to your network. Because most software applications make it very difficult to use IP options, they are not frequently used.

There are different types of IP options:

### *Security*

These options control the routing of IP packets that transmit sensitive data. Security options are not frequently supported.

### *Stream ID (SID)*

The stream ID option is not frequently supported.

### *Source Routing*

The loose source route option and the strict source route option enable the source of an Internet packet to give routing information. Source routing options can be very dangerous, because an attacker could use them to masquerade as a different user. But, loose source route option and the traceroute tool can also help debug some unusual routing problems.

### *Record Route*

The record route option was first used to do tests on the Internet. But, record route can record only ten IP addresses. On the current Internet, a typical connection can include 20 or 30 different routers, making the record route option out of date.

### *Time Stamp*

The time stamp option measures the time for a packet to make one full cycle (source --> destination --> source). Higher level time protocols or time stamp messages do this task better than the time stamp option.

---

## Transfer Protocols

---

The Internet Protocol (IP) includes information kept in the transport layer. The transport layer has different protocols that tell how to transmit data between software applications: for example, UDP, TCP, ICMP, and others.

### UDP

User Datagram Protocol (UDP) is a datagram protocol that does not use connections. It is a very fast protocol, and it does not use much bandwidth or CPU. But, you cannot trust that datagrams will get to their destination. A software application that uses UDP must make sure that the full message gets to its destination in the correct sequence.

Characteristics of UDP include:

- Frequently used for services that include the exchange of small quantities of data where sending a datagram more than one time is not a problem.
- Used for services such as time synchronization in which a missing packet does not have an effect on continued operation. Many systems using UDP send packets again at a constant rate to tell other systems about unusual events.
- Frequently used on LANs. Because of its low system and bandwidth requirements, it gives a large performance advantage to Network File System (NFS) services users. Network File System is a popular TCP/IP service for supplying shared file systems over a network.
- Gives supports to broadcasts.
- Gives abstraction of ports. A connection is made of its source and destination ports and its source and destination IP addresses. In typical use, port numbers less than 1024 are saved for well-known services (destinations). The client side can use ports higher than 1023 for the source of the connection. But, this rule has many exceptions: NFS (port 2049) and Archie (port 1525) use server ports at numbers higher than 1024. Some services use the same source and destination port for server to server connections. Examples include DNS (53), NTP (123), syslog (514), and RIP (520).

## TCP

Transmission Control Protocol (TCP) enables two hosts to make a connection and send streams of data to each other. TCP makes sure that the data that is sent gets to its destination. It also makes sure that packets are put in the same sequence as when they were sent.

TCP manages connections with properties that control the condition of a connection. Three very important properties of TCP packets are the SYN, ACK, and FIN bits. The SYN bit is set only on the first packet sent in each direction for a given connection. The ACK bit is set when the other side gets the data. The FIN bit is set when the source or destination closes the connection.

## ICMP

The Internet Control Message Protocol (ICMP) is most frequently used to supply error information about other services. It operates using the same method as UDP. That is, it does not use connections and does not make sure that packets get to their destination. One dangerous ICMP packet is the ICMP redirect packet, which can change routing information on the devices that receive it.

## Other protocols

Most traffic on the Internet uses TCP, UDP, or ICMP protocols. Some other protocols are as follows:

*IGMP (Internet Group Multicast Protocol)*

A protocol used for hosts on multicast access networks to tell locally attached routers the group they are a member of.

*IPIP (IP-within-IP)*

An encapsulation protocol used to assemble virtual networks on the Internet.

*GGP (Gateway-Gateway Protocol)*

A routing protocol used between different systems.

*GR*

A protocol used for PPTP.

*ES*

An encryption protocol used for IPSec.

---

## Standard Ports and Random Ports

UDP and TCP use encapsulation of information contained in the application layer. The software application procedures are specified by source and destination port numbers. These port numbers, together with the source and destination IP addresses, supply a unique connection on the Internet.

For example, you can have two telnet sessions from one host to a different host. Since telnet uses a well-known service port number of 23, something must be different between these two connections. The other port in these conditions is a port that is usually larger than 1023. The operating system on the client side assigns this port number automatically.

Random ports can cause problems if they match a well-known service on a port higher than 1023. If some client computer assigns a random port of 2049, no connection can be made. This type of problem frequently occurs with the X Window and Archie services.

Usually, most operating systems assign port numbers between 1024 and 2100. Because of this, this problem does not occur frequently.

# MIME Content Types

Software applications use content type headers to identify the type of data they receive. Content type headers tell the software application how to correctly identify and display video clips, images, sound, or other data. Usually, people are most familiar with the MIME content types used in e-mail.

The WatchGuard HTTP proxy can use content type headers to know if it must allow or deny HTTP traffic. Use Policy Manager to configure an HTTP proxy policy to allow or deny content types. Content types are also used in the SMTP and FTP proxies. This chapter contains a list of the MIME content types included in a WatchGuard configuration file.

You can use wildcards to select all subtypes of a type, and thus deny all or allow all of that MIME type. For example, to allow all content types that are text (including text/enriched, text/plain, and others), use the content type `text/*`.

New, registered MIME content types appear regularly. WatchGuard recommends frequent checks of an online source for the most current list. One source of current MIME types is:

[www.iana.org/assignments/media-types/](http://www.iana.org/assignments/media-types/)

Note that software applications can use incorrect content types, or content types that are not registered,

To make a request to add a new content type in the WatchGuard list, send an e-mail to:

[manual@watchguard.com](mailto:manual@watchguard.com)

Type	Subtype	Reference (where available)
application	*	
application	activemessage	Shapiro
application	andrew-inset	Borenstein
application	applefile	Falstrom
application	astound	
application	atomicmail	Borenstein
application	cals-1840	RFC 1895
application	commonground	Glazner
application	cybercash	Eastlake
application	dca-rft	Campbell
application	dec-dx	Campbell

Type	Subtype	Reference (where available)
application	eshop	Katz
application	hyperstudio	Domino
application	iges	Parks
application	mac-binhex40	Falstrom
application	macwriteii	Lindner
application	marc	RFC 2220
application	mathematica	Van Nostern
application	ms-excel	
application	mspowerpoint	
application	msword	Lindner
application	news-message-id	RFC 1036, Spencer
application	news-transmission	RFC 1036, Spencer
application	octet-stream	RFC 2045, RFC 2046
application	oda	RFC 2045, RFC 2046
application	olescript	
application	pdf	RFC 3778
application	pgp-encrypted	RFC 3156
application	pgp-keys	RFC 3156
application	pgp-signature	RFC 3156
application	pkcs10	RFC 2311
application	pkcs7-mime	RFC 2311
application	pkcs7-signature	RFC 2311
application	postscript	RFC 2045, RFC 2046
application	prs.alvestrand.titrax-sheet	Alvestrand
application	prs.cww	Rungchavalnont
application	prs.nprend	Doggett
application	realnetworksupgrade	
application	remote-printing	RFC 1486, Rose
application	riscos	Smith
application	rtf	Lindner
application	set-payment	Korver
application	set-payment-initiation	Korver
application	set-registration	Korver
application	set-registration-initiation	Korver
application	sgml	RFC 1874
application	sgml-open-catalog	Grosso
application	slate	
application	vis5d	
application	vnd.3M.Post-it-Notes	O'Brien
application	vnd.FloGraphIt	Floersch
application	vnd.acucobol	Lubin

Type	Subtype	Reference (where available)
application	vnd.anser-web-certificate-issue-initiation	Mori
application	vnd.answer-web-funds-transfer-initiation	Mori
application	vnd.audiograph	Slusanschi
application	vnd.businessobjects	Imoucha
application	vnd.claymore	Simpson
application	vnd.commerce-battelle	Applebaum
application	vnd.commonspace	Chandhok
application	vnd.cosmocaller	Dellutri
application	vnd.cybank	Helmee
application	vnd.dna	Searcy
application	vnd.dxr	Duffy
application	vnd.ecdis-update	Buettgenbach
application	vnd.ecowin.chart	Olsson
application	vnd.ecowin.filerequest	Olsson
application	vnd.ecowin.fileupdate	Olsson
application	vnd.ecowin.series	Olsson
application	vnd.ecowin.seriesrequest	Olsson
application	vnd.ecowin.seriesupdate	Olsson
application	vnd.enliven	Santinelli
application	vnd.epson.quickanime	Gu
application	vnd.epson.salt	Nagatomo
application	vnd.fdf	Zilles
application	vnd.ffmpeg	Holstage
application	vnd.framemaker	Wexler
application	vnd.fujitsu-oasys	Togashi
application	vnd.fujitsu-oasys2	Togashi
application	vnd.fujitsu-oasys3	Okudaira
application	vnd.fujitsu-oasysgp	Sugimoto
application	vnd.fujitsu-oasysprs	Ogita
application	vnd.fujixerox.docuworks	Taguchi
application	vnd.fut-misnet	Pruulmann
application	vnd.hp-HPGL	Pentecost
application	vnd.hp-PCL	Pentecost
application	vnd.hp-PCLXL	Pentecost
application	vnd.hp-hps	Aubrey
application	vnd.ibm.MiniPay	Herzberg
application	vnd.ibm.modcap	Hohensee
application	vnd.intercon.formnet	Gurak
application	vnd.intertrust.digibox	Tomasello
application	vnd.intertrust.nncp	Tomasello
application	vnd.intu-qbo	Scratchley

Type	Subtype	Reference (where available)
application	vnd.is-xpr	Natarajan
application	vnd.japannet-directory-service	Fujii
application	vnd.japannet-jpnstore-wakeup	Yoshitake
application	vnd.japannet-payment-wakeup	Fujii
application	vnd.japannet-registration	Yoshitake
application	vnd.japannet-registration-wakeup	Fujii
application	vnd.japannet-setstore-wakeup	Yoshitake
application	vnd.japannet-verification	Yoshitake
application	vnd.japannet-verification-wakeup	Fujii
application	vnd.loan	Cole
application	vnd.lotus-1-2-3	Wattenberger
application	vnd.lotus-approach	Wattenberger
application	vnd.lotus-freelance	Wattenberger
application	vnd.lotus-organizer	Wattenberger
application	vnd.lotus-screencam	Wattenberger
application	vnd.lotus-wordpro	Wattenberger
application	vnd.meridian-slideshow	Wedel
application	vnd.mif	Wexler
application	vnd.minisoft-hp3000-save	Bartram
application	vnd.mitsubishi.misty-guard.trustweb	Tanaka
application	vnd.ms-artgalry	Slawson
application	vnd.ms-asf	Fleischman
application	vnd.ms-powerpoint	Gill
application	vnd.ms-project	Gill
application	vnd.ms-tnef	Gill
application	vnd.ms-works	Gill
application	vnd.ms.wms-hrd.asfv1	Gill
application	vnd.music-niff	Butler
application	vnd.musician	Adams
application	vnd.netfpx	Mutz
application	vnd.noblenet-directory	Solomon
application	vnd.noblenet-sealer	Solomon
application	vnd.noblenet-web	Solomon
application	vnd.novadigm.EDM	Swenson
application	vnd.novadigm.EDX	Swenson
application	vnd.novadigm.EXT	Swenson
application	vnd.osa.netdeploy	Klos
application	vnd.powerbuilder6	Guy
application	vnd.powerbuilder6-s	Guy
application	vnd.publishare-delta-tree	Ben-Kiki
application	vnd.rapid	Szekely

Type	Subtype	Reference (where available)
application	vnd.rn-realplayer	
application	vnd.seemail	Webb
application	vnd.shana.informed.formdata	Selzler
application	vnd.shana.informed.formtemplate	Selzler
application	vnd.shana.informed.interchange	Selzler
application	vnd.shana.informed.package	Selzler
application	vnd.street-stream	Levitt
application	vnd.svd	Becker
application	vnd.swiftview-ics	Widener
application	vnd.truedoc	Chace
application	vnd.uplanet.alert	Martin
application	vnd.uplanet.alert-wbxml	Martin
application	vnd.uplanet.bearer-choi-wbxml	Martin
application	vnd.uplanet.bearer-choice	Martin
application	vnd.uplanet.cacheop	Martin
application	vnd.uplanet.cacheop-wbxml	Martin
application	vnd.uplanet.channel	Martin
application	vnd.uplanet.channel-wbxml	Martin
application	vnd.uplanet.list	Martin
application	vnd.uplanet.list-wbxml	Martin
application	vnd.uplanet.listcmd	Martin
application	vnd.uplanet.listcmd-wbxml	Martin
application	vnd.uplanet.signal	Martin
application	vnd.visio	Sandal
application	vnd.webturbo	Rehem
application	vnd.wrq-hp3000-labelled	Bartram
application	vnd.wt.stf	Wohler
application	vnd.xara	Matthewman
application	vnd.yellowriver-custom-menu	Yello
application	vnd.wita	
application	vnd.workperfect5.1	
application	write	
application	x-alpha-form	
application	x-asap	
application	x-bcpio	
application	x-chat	
application	x-cpio	
application	x-sch	
application	x-cu-seemee	
application	x-demoshield	
application	x-director	

Type	Subtype	Reference (where available)
application	x-dvi	
application	x-framemaker	
application	x-gtar	
application	x-ica	
application	x-installshield	
application	x-javascript	
application	x-koan	
application	x-latex	
application	x-mif	
application	x-msaddr	
application	x-mms-framed	
application	x-mswallet	
application	x-net-install	
application	x-nokia-9000-add-on-software	
application	x-ns-proxy-autoconfig	
application	x-oleobject	
application	x-olescript	
application	x-p3d	
application	x-pcn	
application	x-pdf	
application	x-perl	
application	x-pn-realaudio	
application	x-pn-realmedia	
application	x-pointplus	
application	x-rad-powermedia	
application	x-sh	
application	x-shar	
application	x-shockwave-flash	
application	x-sprite	
application	x-stuffit	
application	x-tar	
application	x-tcl	
application	x-tex	
application	x-texinfo	
application	x-troff	
application	x-troff-man	
application	x-troff-me	
application	x-troff-ms	
application	x-ustar	
application	x-wais-source	
application	x-watchguard-cloaked	

Type	Subtype	Reference (where available)
application	x-webbasic	
application	x-wintalk	
application	x-wls	
application	x-wms-LogStats	
application	x400-bp	
application	xml	RFC 3023
application	zip	Lindner
audio	*	
audio	32kadpcm	RFC 2421, RFC 2422
audio	basic	RFC 2045, RFC 2046
audio	echospeech	
audio	vnd.qcelp	
audio	voxware	
audio	x-aiff	
audio	x-mpeg	
audio	x-mpeg-2	
audio	x-wav	
chemical	*	
chemical	x-cdx	
chemical	x-cif	
chemical	x-chem3d	
chemical	x-cmdf	
chemical	x-cml	
chemical	x-daylight-smiles	
chemical	x-csml	
chemical	x-galactic-spc	
chemical	x-gaussian-input	
chemical	x-gaussian-cube	
chemical	x-isostar	
chemical	x-jcamp-dx	
chemical	x-kinemage	
chemical	x-mdl-molfile	
chemical	x-mdl-rxnfile	
chemical	x-macmolecule	
chemical	x-macromode1-input	
chemical	x-mopac-input	
chemical	x-pdb	
chemical	x-xyz	
chemical	x-vmd	

Type	Subtype	Reference (where available)
drawing	*	
drawing	x-dwf	
graphics	*	
graphics	x-inventor	
image	*	
image	cgm	Francis
image	fif	
image	g3fax	
image	gif	RFC 2045, RFC 2046
image	ief	RFC 1314
image	jpeg	RFC 2045, RFC 2046
image	naplps	Ferber
image	png	Randers-Pehrson
image	prs.btif	Simon
image	tiff	
image	vnd.dwg	Moline
image	vnd.dxf	Moline
image	vnd.fastbidsheet	Becker
image	vnd.fpx	Spencer
image	vnd.net-fpx	Spencer
image	vnd.svf	Moline
image	vnd.xiff	S. Martin
image	wavelet	
image	x-cals	
image	x-cmu-raster	
image	x-cmx	
image	x-dwg	
image	x-dxf	
image	x-mgx-dsf	
image	x-ms-bmp	
image	x-photo-cd	
image	x-pict	
image	x-png	
image	x-portable-anymap	
image	x-portable-bitmap	
image	x-portable-graymap	
image	x-portable-pixmap	
image	x-rgb	

Type	Subtype	Reference (where available)
image	x-svf	
image	x-xbitmap	
image	x-xwindowdump	
image	xpm	
message	*	
message	delivery-status	RFC 1894
message	disposition-notification	RFC 2298
message	external-body	RFC 2045, RFC 2046
message	http	RFC 2616
message	news	RFC 1036, H. Spencer
message	partial	RFC 2045, RFC 2046
message	rfc822	RFC 2045, RFC 2046
model	*	
model	iges	Parks
model	mesh	RFC 2077
model	vnd.dwf	Pratt
model	vrml	RFC 2077
multipart	*	
multipart	alternative	RFC 2045, RFC 2046
multipart	appledouble	Falstrom
multipart	byteranges	RFC 2068
multipart	digest	RFC 2045, RFC 2046
multipart	encrypted	RFC 1847
multipart	form-data	RFC 2388
multipart	header-set	Crocker
multipart	mixed	RFC 2045, RFC 2046
multipart	parallel	RFC 2045, RFC 2046
multipart	related	RFC 2387
multipart	report	RFC 1982
multipart	signed	RFC 1847
multipart	voice-message	RFC 2421, RFC 2423
text	*	
text	css	RFC 2318
text	enriched	RFC 1896
text	html	RFC 2854
text	javascript	
text	plain	RFC 2046, RFC 3676

Type	Subtype	Reference (where available)
text	richtext	RFC 2045, RFC 2046
text	sgml	RFC 1874
text	tab-separated-values	Lindner
text	uri-list	RFC 2483
text	vbscript	
text	vnd.abc	Allen
text	vnd.fmiflexstor	Hurta
text	vnd.in3d.3dml	Powers
text	vnd.in3d.spot	Powers
text	vnd.latex-z	Lubos
text	x-setext	
text	x-speech	
text	xml	RFC 3023
video	*	
video	mpeg	RFC 2045, RFC 2046
video	mpeg-2	
video	quicktime	Lindner
video	vdo	
video	vivo	Wolfe
video	vnd.motorola.video	McGinty
video	vnd.motorola.videop	McGinty
video	vnd.vivo	
video	x-ms-asf	
video	x-msvideo	
video	x-sgi-movie	
workbook	*	
workbook	formulaone	
x-conference	x-cooltalk	
x-form	x-openscape	
x-model	x-mesh	
x-music	x-midi	
x-script	x-wfxclient	
x-world	*	

---

<b>Type</b>	<b>Subtype</b>	<b>Reference (where available)</b>
x-world	x-3dmf	
x-world	x-svr	
x-world	x-vream	
x-world	x-vrml	
x-world	x-vrt	
x-world	x-wvr	



---

Well-known services are a mixture of port number and transport protocol for specified, standard software applications. This chapter contains tables that list service names, port number, protocol, and description.

## Ports Used by WatchGuard Products

---

The WatchGuard Firebox, management station, and WatchGuard Security Event Processor use specified ports during usual operations.

Port #	Protocol	Purpose
4100	TCP	Authentication service
4107 4115	TCP	WatchGuard Log Server
4103 4105 4117 4118	TCP	WatchGuard Firebox configuration and management
4110 4112 4113	TCP	WatchGuard Management Server
4109	TCP	Secure access to SOHO and Edge Fireboxes with a web browser
5003	TCP and UDP	WebBlocker

## Ports Used by Microsoft Products

Port #	Protocol	Purpose
137, 138	UDP	Browsing
67, 68	UDP	DHCP Lease
135	TCP	DHCP Manager
138 139	UDP TCP	Directory Replication
135	TCP	DNS Administration
53	UDP	DNS Resolution
139	TCP	Event Viewer
139	TCP	File Sharing
137, 138 139	UDP TCP	Logon Sequence
138	UDP	NetLogon
137, 138 139	UDP TCP	Pass Through Validation
139	TCP	Performance Monitor
1723 47	TCP IP	PPTP
137, 138 139	UDP TCP	Printing
139	TCP	Registry Editor
139	TCP	Server Manager
137, 138 139	UDP TCP	Trusts
139	TCP	User Manager
139	TCP	WinNT Diagnostics
137, 138 139	UDP TCP	WinNT Secure Channel
42	TCP	WINS Replication
135	TCP	WINS Manager
137	TCP	WINS Registration

Port(s)	Protocol	Purpose
135	TCP	Client/Server Communications
135	TCP	Exchange Administrator
143	TCP	IMAP
993	TCP	IMAP (SSL)
389	TCP	LDAP
636	TCP	LDAP (SSL)
102	TCP	MTA - X.400 over TCP/IP
110	TCP	POP3
995	TCP	POP3 (SSL)

Port(s)	Protocol	Purpose
135	TCP	RCP
25	TCP	SMTP
137	UDP	SMB
138	UDP	SMB
139	TCP	SMB
445	TCP/UDP	MS-DS (Directory Services)
119	TCP	NNTP
563	TCP	NNTP (SSL)

## Well-Known Services List

In addition to the ports used by services described above, WatchGuard supplies a list of well-known services. Because software companies regularly add new services, this is not a full list of all possible services. For more information, refer to:

[www.iana.org/assignments/port-numbers](http://www.iana.org/assignments/port-numbers)

To recommend additions to this list, send an e-mail to: [manual@watchguard.com](mailto:manual@watchguard.com).

Service Name	Port #	Protocol	Description
tcpmux	1	TCP/UDP	TCP Port Service Multiplexer
compressnet	2,3	TCP/UDP	Management Utility
rje	5	TCP/UDP	Remote Job Entry
echo	7	TCP/UDP	Echo
discard	9	TCP/UDP	Discard
systat	11	TCP/UDP	Active Users
daytime	13	TCP/UDP	Daytime
qotd	17	TCP/UDP	Quote of the Day
misp	18	TCP/UDP	Message Send Protocol
chargen	19	TCP/UDP	Character Generator
ftp-data	20	TCP/UDP	File Transfer [Default Data]
ftp	21	TCP/UDP	File Transfer [Control]
ssh	22	TCP/UDP	SSH Remote Login Protocol
telnet	23	TCP/UDP	Telnet
smtp	25	TCP/UDP	Simple Mail Transfer
nsw-fe	27	TCP/UDP	NSW User system FE
msg-icp	29	TCP/UDP	MSG ICP
msg-auth	31	TCP/UDP	MSG Authentication
dsp	33	TCP/UDP	Display Support Protocol
time	37	TCP/UDP	Time
rap	38	TCP/UDP	Route Access Protocol
rlp	39	TCP/UDP	Resource Location Protocol

---

**Well-Known Services List**

<b>Service Name</b>	<b>Port #</b>	<b>Protocol</b>	<b>Description</b>
graphics	41	TCP/UDP	Graphics
nameserver	42	TCP/UDP	Host Name Server
nicname	43	TCP/UDP	whois
mpm-flags	44	TCP/UDP	MPM Flags
mpm	45	TCP/UDP	MPM
mpm-snd	46	TCP/UDP	MPM Send
ni-ftp	47	TCP/UDP	NI FTP
auditd	48	TCP/UDP	Digital Audit Daemon
tacacs	49	TCP/UDP	Login Host Protocol (TACACS)
re-mail-ck	50	TCP/UDP	Remote Mail Checking Protocol
la-maint	51	TCP/UDP	IMP Logical Address Maintenance
xns-time	52	TCP/UDP	XNS Time Protocol
domain	53	TCP/UDP	Domain Name Server
xns-ch	54	TCP/UDP	XNS Clearinghouse
isi-gl	55	TCP/UDP	ISI Graphics Language
xns-auth	56	TCP/UDP	XNS Authentication
xns-mail	58	TCP/UDP	XNS Mail
ni-mail	61	TCP/UDP	NI MAIL
acas	62	TCP/UDP	ACA Services
whois++	63	TCP/UDP	whois++
covia	64	TCP/UDP	Communications Integrator (CI)
tacacs-ds	65	TCP/UDP	TACACS-Database Service
sql*net	66	TCP/UDP	Oracle SQL*NET
bootps	67	TCP/UDP	Bootstrap Protocol Server
bootpc	68	TCP/UDP	Bootstrap Protocol Client
tftp	69	TCP/UDP	Trivial File Transfer
gopher	70	TCP/UDP	Gopher
netrjs-1	71	TCP/UDP	Remote Job Service
netrjs-2	72	TCP/UDP	Remote Job Service
netrjs-3	73	TCP/UDP	Remote Job Service
netrjs-4	74	TCP/UDP	Remote Job Service
deos	76	TCP/UDP	Distributed External Object Store
vettcp	78	TCP/UDP	vettcp
finger	79	TCP/UDP	Finger
www-http	80	TCP/UDP	World Wide Web HTTP
hosts2-ns	81	TCP/UDP	HOSTS2 Name Server
xfer	82	TCP/UDP	XFER utility
mit-ml-dev	83	TCP/UDP	MIT ML device
ctf	84	TCP/UDP	Common Trace Facility
mit-ml-dev	85	TCP/UDP	MIT ML device
mfcobol	86	TCP/UDP	Micro Focus Cobol

Service Name	Port #	Protocol	Description
kerberos	88	TCP/UDP	Kerberos
sug-mit-tug	89	TCP/UDP	SU/MIT Telnet gateway
dnsix	90	TCP/UDP	DNSIX Secure Application Token Map
mit-dov	91	TCP/UDP	MIT Dover Spooler
npp	92	TCP/UDP	Network Printing Protocol
dcp	93	TCP/UDP	Device Control Protocol
objcall	94	TCP/UDP	Tivoli Object Dispatcher
supdup	95	TCP/UDP	SUPDUP
dixie	96	TCP/UDP	DIXIE Protocol Specification
swift-rvf	97	TCP/UDP	Swift Remote Virtual File Protocol
tacnews	98	TCP/UDP	TAC News
metagram	99	TCP/UDP	Metagram Relay
newacct	100	TCP	[unauthorized use]
hostname	101	TCP/UDP	NIC Host Name Server
iso-tsap	102	TCP/UDP	ISO-TSAP
gppitnp	103	TCP/UDP	Genesis Point-to-Point Trans Net
acr-nema	104	TCP/UDP	ACR-NEMA Digital Imag. Comm. 300
cso	105	TCP/UDP	CCSO name server protocol
csnet-ns	105	TCP/UDP	Mailbox Name Nameserver
3com-tsmux	106	TCP/UDP	3COM-TSMUX
rtelnet	107	TCP/UDP	Remote Telnet Service
snagas	108	TCP/UDP	SNA Gateway Access Server
pop2	109	TCP/UDP	Post Office Protocol - Version 2
pop3	110	TCP/UDP	Post Office Protocol - Version 3
sunrpc	111	TCP/UDP	SUN Remote Procedure Call
mcidas	112	TCP/UDP	McIDAS Data Transmission Protocol
auth(ident)	113	TCP/UDP	Authentication Service
audionews	114	TCP/UDP	Audio News Multicast
sftp	115	TCP/UDP	Simple File Transfer Protocol
ansanotify	116	TCP/UDP	ANSA REX Notify
uucp-path	117	TCP/UDP	UUCP Path Service
sqlserv	118	TCP/UDP	SQL Services
nntp	119	TCP/UDP	Network News Transfer Protocol
cfdpkt	120	TCP/UDP	CFDPKT
erpc	121	TCP/UDP	Encore Expedited RPC
smakynet	122	TCP/UDP	SMAKYNET
nntp	123	TCP/UDP	Network Time Protocol
ansatrader	124	TCP/UDP	ANSA REX Trader
locus-map	125	TCP/UDP	Locus PC-Interface Net Map
unitary	126	TCP/UDP	Unisys Unitary Login
locus-con	127	TCP/UDP	Locus PC-Interface Conn Server

---

**Well-Known Services List**

<b>Service Name</b>	<b>Port #</b>	<b>Protocol</b>	<b>Description</b>
gss-xlicen	128	TCP/UDP	GSS X License Verification
pwdgen	129	TCP/UDP	Password Generator Protocol
cisco-fna	130	TCP/UDP	cisco FNATIVE
cisco-tna	131	TCP/UDP	cisco TNATIVE
cisco-sys	132	TCP/UDP	cisco SYSMaint
statsrv	133	TCP/UDP	Statistics Service
ingres-net	134	TCP/UDP	INGRES-NET Service
epmap	135	TCP/UDP	DCE-RPC Endpoint resolution
profile	136	TCP/UDP	PROFILE naming system
netbios-ns	137	TCP/UDP	NETBIOS Name Service
netbios-dgm	138	TCP/UDP	NETBIOS Datagram Service
netbios-ssn	139	TCP/UDP	NETBIOS Session Service
imap	143	TCP/UDP	Internet Message Access Protocol
news	144	TCP/UDP	NewS
jargon	148	TCP/UDP	Jargon
sql-net	150	TCP/UDP	SQL-NET
bftp	152	TCP/UDP	Background File Transfer
sgmp	153	TCP/UDP	SGMP
sqlsrv	156	TCP/UDP	SQL Service
pcmail-srv	158	TCP/UDP	PCMail Server
sgmp-traps	160	TCP/UDP	SGMP-TRAPS
snmp	161	TCP/UDP	SNMP
snmptrap	162	TCP/UDP	SNMPTRAP
cmip-man	163	TCP/UDP	CMIP/TCP Manager
cmip-agent	164	TCP	CMIP/TCP Agent
smip-agent	164	UDP	CMIP/TCP Agent
namp	167	TCP/UDP	NAMP
rsvd	168	TCP/UDP	RSVD
send	169	TCP/UDP	SEND
xyplex-mux	173	TCP/UDP	Xyplex MUX
xdmcp	177	TCP/UDP	X Display Manager Control Protocol
NextStep	178	TCP/UDP	NextStep Window Server
bgp	179	TCP/UDP	Border Gateway Protocol
unify	181	TCP/UDP	Unify
irc	194	TCP/UDP	Internet Relay Chat Protocol
at-rtmp	201	TCP/UDP	AppleTalk Routing Maintenance
at-nbp	202	TCP/UDP	AppleTalk Name Binding
at-3	203	TCP/UDP	AppleTalk Unused
at-echo	204	TCP/UDP	AppleTalk Echo
at-5	205	TCP/UDP	AppleTalk Unused
at-zis	206	TCP/UDP	AppleTalk Zone Information

Service Name	Port #	Protocol	Description
at-7	207	TCP/UDP	AppleTalk Unused
at-8	208	TCP/UDP	AppleTalk Unused
qmtip	209	TCP/UDP	Quick Mail Transfer Protocol
z39.50	210	TCP/UDP	ANSI Z39.50 (WAIS)
ipx	213	TCP/UDP	IPX
imap3	220	TCP/UDP	Interactive Mail Access Protocol v3
fln-spx	221	TCP/UDP	Berkeley rlogind with SPX auth
rsh-spx	222	TCP/UDP	Berkeley rshd with SPX auth
backweb	371	UDP	BackWeb
ulistserv	372	TCP/UDP	Unix Listserv
netware-ip	396	TCP/UDP	Novell Netware over IP
biff	512	UDP	Used by mail system to notify users
exec	512	TCP	Remote process execution
login	513	TCP/UDP	Login Host Protocol
who	513	UDP	Maintains databases showing who's who
cmd	514	TCP	Like exec, but automatic
syslog	514	UDP	logging facilities
printer	515	TCP/UDP	Spooler
talk	517	TCP/UDP	Talk protocol
ntalk	518	TCP/UDP	another Talk
utime	519	TCP/UDP	Unixtime
router	520	UDP	RIP local routing process (on site)
timed	525	TCP/UDP	Timeserver
tempo	526	TCP/UDP	Newdate
courier	530	TCP/UDP	Rpc
conference	531	TCP/UDP	Chat
netnews	532	TCP/UDP	Readnews
netwall	533	TCP/UDP	For emergency broadcasts
uucp	540	TCP/UDP	Uucpd
uucp-rlogin	541	TCP/UDP	Uucp-rlogin Stuart Lynne
klogin	543	TCP/UDP	Kerberos (v4/v5)
kshell	544	TCP/UDP	krcmd Kerberos (v4/v5)
dhcpv6-client	546	TCP/UDP	DHCPv6 Client
dhcpv6-server	547	TCP/UDP	DHCPv6 Server
cybercash	551	TCP/UDP	Cybercash
remotefs	556	TCP/UDP	Rfs server
9pfs	564	TCP/UDP	Plan 9 file service
whoami	565	TCP/UDP	Whoami
msn	569	TCP	Microsoft Network
doom	666	TCP/UDP	Doom Id Software
kerberos-adm	749	TCP/UDP	Kerberos administration

---

**Well-Known Services List**

<b>Service Name</b>	<b>Port #</b>	<b>Protocol</b>	<b>Description</b>
webster	765	TCP/UDP	Network dictionary
phonebook	767	TCP/UDP	Phone
socks	1080	TCP/UDP	Socks
hermes	1248	TCP/UDP	Hermes
lotusnote	1352	TCP/UDP	Lotus Notes
netware-csp	1366	TCP/UDP	Novell NetWare Comm Service Platform
novell-lu6.2	1416	TCP/UDP	Novell LU6.2
netopia	1419 8000	UDP TCP	Netopia Virtual Office
ms-sql-s	1433	TCP/UDP	Microsoft-SQL-Server
ms-sql-m	1434	TCP/UDP	Microsoft-SQL-Monitor
winframe	1494	TCP	WinFrame
watcom-sql	1498	TCP/UDP	Watcom-SQL
ingreslock	1524	TCP/UDP	Ingres
groupwise	1677	TCP	GroupWise
nfs	2049	TCP/UDP	Network File Server
www-dev	2784	TCP/UDP	World Wide Web - development
Squid	3128	TCP/UDP	Web proxy/caching service -- frequently scanned for vulnerabilities
ccmail	3264	TCP/UDP	Cc:mail/lotus
ICQ	2109 4000	TCP UDP	Used for chat
Firstclass	3000 30004	TCP	FirstClass (ftp channel on 510 TCP)
compuserve	4144	TCP	CompuServe Online
rfe	5002	TCP/UDP	Radio free ethernet
aol	5190	TCP	America Online
x11	6000	TCP/UDP	X Window System (through 6063)
font-service	7100	TCP/UDP	X Font Service
nas	8000	TCP/UDP	NCD Network Audio Server
iphone	6670	TCP	for connecting to the phone server
iphone	22555	UDP	for audio
iphone	25793	TCP	for the address server, in 4.x and 5.0
iphone	1490	TCP	for the conference engine in 4.x and 5.0

---

Understanding the log messages the Firebox sends to the log file is a critical function for a Firebox administrator. The log messages give you important information about the flow of traffic through your network. The log messages are also a key component in troubleshooting problems that occur in your network.

This chapter explains the types of log messages the Firebox generates. It gives examples of traffic and alarm log messages and a list of available event logs for Fireboxes using Fireware appliance software. You can get access to the Fireware XML log DTD and schema using through the FAQs available at [www.watchguard.com/support](http://www.watchguard.com/support).

## Introduction to Logging

---

The WatchGuard Firebox X Core and Firebox X Peak send log messages to a WatchGuard log server. They can also send log messages to a syslog server or keep logs locally on the Firebox. It is your decision to send logs to any or all of these locations.

You can see log messages in real time using the WatchGuard System Manager Traffic Monitor. You can also show the logs in the LogViewer. The log messages are kept in an XML file with a .wgl.xml extension in the WatchGuard directory on the log server. If it becomes necessary, you can open this file using any XML tool to see log messages.

The Firebox sends four types of log messages:

- Traffic logs
- Alarm logs
- Event logs
- Diagnostic logs

### Traffic logs

The Firebox sends traffic logs as it applies packet filter and proxy rules to traffic passing through the Firebox.

### Alarm logs

Alarm logs are sent when an alarm condition is met. The Firebox sends the alarm to the Traffic Monitor and Log Server and triggers the specified action.

Some alarms are set in your Firebox configuration. For example, you can use Policy Manager to configure an alarm to occur when a certain threshold is met. Other alarms are set by default. The Firebox sends an alarm log when a network connection on one of the Firebox interfaces fails. This cannot be changed in your configuration. The Firebox never sends more than 10 alarms in 15 minutes for the same set of conditions.

There are eight categories of alarm logs: System, IPS, AV, Policy, Proxy, Probe, Denial of service, and Traffic.

### Event logs

Event logs are created because of Firebox user activity. Events that cause event logs include:

- Firebox start up/shut down
- Firebox and VPN authentication
- Process start up/shut down
- Problems with the Firebox hardware components
- Any task done by the Firebox administrator

### Diagnostic logs

Diagnostic logs are more detailed log messages sent by the Firebox that you can use to help troubleshoot problems. You can select the level of diagnostic logging to see in your traffic monitor, or write to your log file. You can configure the diagnostic log level from **Policy Manager > Setup > Logging > Advanced Diagnostics**. The available levels are off, low, medium, high, and advanced. We do not recommend that you set the logging level to advanced unless you are working with a technical support team to diagnose a problem, as it can cause the log file to fill up very quickly.

---

## Traffic Logs

Most of the logs shown in Traffic Monitor are traffic logs. Traffic logs show the traffic that moves through your Firebox and how the packet filter and proxy policies were applied. Traffic Monitor shows all of the log messages from the Firebox that are recorded in your log file.

### Packet Filter Logs

Packet filter logs contain a set number of fields. Here is an example of the XML output of a packet filter log message. The information will look different when you see the same log message in Traffic Monitor or LogViewer. Below the example, there is an explanation for each field that appears.

```
FWAllow d="2005-01-25T23:12:12" orig="HQFirebox" disp="Allow" pri="1" policy="SSH-outgoing-05" src_ip="192.168.130.59" dst_ip="10.10.171.98" pr="ssh" src_port="56952" dst_port="22" src_intf="1-Trusted" dst_intf="0-External" rc="100" msg="firewall pass, mss not exceeding 1460, idle time-out=43205 sec" pkt_len="60" ttl="63" log_type="tr"/
```

*FWAllow*

Each packet filter log message starts with FWDeny or FWAllow. This header shows whether the packet was allowed or denied by the Firebox.

*d="2005-01-25T23:12:12"*

The date and time the event occurred, adjusted according to the time zone setting in **Policy Manager > Setup > System**.

*orig="HQFirebox"*

The name or IP address (if no name is available) of the Firebox writing the log message.

*disp="Allow"*

The packet disposition. Can be deny or allow.

*pri="1"*

The priority of the log. The priority is used only for Net IQ reporting and is set to 1 (critical mode), 4 (warning mode), or 6 (normal allowed traffic).

*policy="ssh-outgoing-05"*

The name of the policy in Policy Manager that handled this packet.

*src\_ip="192.168.30.159"*

The source IP address of this packet.

*dst\_ip="10.10.171.98"*

The destination IP address for this packet.

*pr="ssh"*

The protocol used in this packet.

*src\_port="56952"*

The source port for this packet.

*dst\_port="22"*

The destination port for this packet.

*src\_intf="1-Trusted"*

The number of the source interface for this packet, and the name you have given the source interface for this packet (as defined in **Policy Manager > Network > Configuration**). A source interface of trusted indicates that this packet originated behind the trusted interface of the Firebox. A source interface of external shows that the packet has come from outside the Firebox.

*dst\_intf="0-External"*

The number of the destination interface for this packet, and the name you have given for the destination interface for this packet (as defined in **Policy Manager > Network > Configuration**).

*rc="100"*

Return code for the packet. This information is used in Historical Reporting.

*msg="firewall pass, mss not exceeding 1460, idle timeout=43205 sec"*

The message field.

*pckt\_len="60"*

The length of the packet, in bytes.

*ttl="63"*

The packet "time to live", in seconds.

*log\_type="tr"*

The type of log message. All traffic logs use the "tr" log type.

### **Traffic logs showing NAT**

A traffic log can also include fields that show how NAT (network address translation) was handled for this packet. An example log showing the ports the Firebox used to apply NAT to a packet is:

```
<FWAllow d="2005-02-02T09:46:53" orig="HQFirebox" disp="Allow" pri="1"
policy="WG-Firebox-Mgmt-outgoing-01" src_ip="192.168.1.15"
dst_ip="172.16.1.45" pr="WatchGuard" src_port="2154" dst_port="4105"
src_intf="1-Trusted" dst_intf="0-External" src_ip_nat="10.1.1.6"
src_port_nat="15013" rc="100" msg="firewall pass, mss not exceeding 1460,
idle timeout=43205 sec" pckt_len="48" ttl="128" log_type="tr"/>
```

### **Proxy Logs**

When the Firebox processes an event that is handled by a proxy, it writes more than one log message. The first entry shows the same information as a packet filter log, but includes two more fields:

*proxy\_act*

The name of the proxy action handling this packet. A proxy action is a set of rules for a proxy that can be applied to more than one policy.

*rule\_name*

The name of the specific proxy rule handling this packet.

*content\_type*

The type of content in the packet that is filtered by the proxy rule.

Other log messages that the Firebox writes when an event is handled by a proxy contain a variable number of fields. Here is an example of a group of log messages created by a user request handled by a proxy:

```
<ProxyMatch d="2005-02-01T23:35:16" orig="HQFirebox" proc_id="cfm[1497]"
disp="Allow" pri="6" policy="HTTP-proxy-01" src_ip="192.168.1.124"
dst_ip="66.35.250.151" pr="tcp/http" src_port="4345" dst_port="80"
src_intf="1-Trusted" dst_intf="0-External" src_ip_nat="250.168.43.6"
src_port_nat="13419" rc="590" msg="ProxyAllow: HTTP Header content type
match" proxy_act="HTTP-Client.2" rule_name="text/*" content_type="text/xml"
log_type="tr"/>
```

```
<ProxyHTTPRequest d="2005-02-01T23:35:16" orig="HQFirebox" proc_id="cfm[1497]"
disp="Allow" pri="6" policy="HTTP-proxy-01" src_ip="192.168.1.124"
dst_ip="66.35.250.151" pr="tcp/http" src_port="4345" dst_port="80"
src_intf="1-Trusted" dst_intf="0-External" src_ip_nat="250.168.43.6"
src_port_nat="13419" rc="525" msg="HTTP Request" proxy_act="HTTP-Client.2"
op="GET" dstname="politics.slashdot.org" arg="/politics.rss"
sent_bytes="345" rcvd_bytes="2727" log_type="tr"/>
```

```
<ProxyConnEnd d="2005-02-01T23:35:16" orig="HQFirebox" proc_id="cfm[1497]"
disp="Allow" pri="6" policy="HTTP-proxy-01" src_ip="192.168.1.124"
```

```
dst_ip="66.35.250.151" pr="tcp/http" src_port="4345" dst_port="80"
src_intf="1-Trusted" dst_intf="0-External" src_ip_nat="250.168.43.6"
src_port_nat="13419" rc="523" msg="Conn End" proxy_act="HTTP-Client.2"
log_type="tr"/>
```

Each proxy has its own set of messages. The tables here show the log messages each proxy can write to the log file, and the secondary fields for each log message.

## SMTP Proxy Traffic Log Messages

Text in Message Field <i>Associated Fields</i>	Message Meaning <i>Value that appears in associated field(s)</i>
SMTP GREETING <i>hostname</i> <i>rule_name</i>	There is an invalid message in HELO state <i>hostname sent in SMTP greeting</i> <i>name of rule matched in ruleset</i>
SMTP AUTH <i>authtype</i> <i>rule_name</i>	The AUTH type used matches a configured proxy rule <i>AUTH type used</i> <i>name of rule matched in ruleset</i>
SMTP HEADER <i>header</i>	The SMTP header matches a configured proxy rule. <i>header name</i>
SMTP FROM ADDRESS <i>address</i> <i>length</i> <i>response</i> <i>new_address</i> <i>header</i>	The sender e-mail address matches a configured proxy rule <i>the sender e-mail address (from envelope)</i> <i>length in bytes of address</i> <i>response code returned to client</i> <i>new address, if address rewrite used</i> <i>if header rewrite feature is used</i>
SMTP TO ADDRESS <i>address</i> <i>new_address</i> <i>length</i> <i>response</i>	The recipient e-mail address matches a configured proxy rule <i>recipient e-mail address (from envelope)</i> <i>new address, if address rewrite used</i> <i>length in bytes of address</i> <i>response code returned to client</i>
SMTP CONTENT TYPE <i>content_type</i> <i>rule_name</i> <i>sender</i> <i>recipient</i>	The content type matches a configured proxy rule <i>the content type found by the SMTP proxy</i> <i>name of rule matched in ruleset</i> <i>sender e-mail address (from envelope)</i> <i>recipient e-mail addresses (from envelope)</i>
SMTP Command <i>keyword</i> <i>response</i>	The full SMTP command as received from the SMTP client <i>values include EXPN, HELP, NOOP, etc.</i> <i>response code returned to client</i>
SMTP FILENAME <i>file_name</i> <i>rule_name</i> <i>sender</i> <i>recipients</i>	The filename matches a configured proxy rule <i>the file name</i> <i>name of rule matched in ruleset</i> <i>sender e-mail address (from envelope)</i> <i>recipient e-mail addresses (from envelope)</i>
SMTP TIMEOUT <i>timeout</i>	The connection idle timeout was reached <i>number of seconds configured to time-out</i>
SMTP AV VIRUS <i>virus</i> <i>filename</i> <i>content_type</i> <i>sender</i> <i>recipient</i>	The SMTP proxy found a virus <i>the name of the virus found</i> <i>the filename</i> <i>the content type of the virus found</i> <i>sender e-mail address (from envelope)</i> <i>recipient e-mail addresses (from envelope)</i>
SMTP AV TOO BIG <i>filename</i> <i>type</i>	An attachment was too big to scan <i>the filename</i> <i>the content type of the attachment</i>

### SMTP Proxy Traffic Log Messages

Text in Message Field <i>Associated Fields</i>	Message Meaning <i>Value that appears in associated field(s)</i>
SMTP AV ERROR  <i>filename</i> <i>error</i> <i>sender</i> <i>recipient</i>	The SMTP cannot finish an antivirus scan, usually because an attachment was encrypted  <i>file name</i> <i>description of error</i> <i>sender e-mail address (from envelope)</i> <i>recipient e-mail addresses (from envelope)</i>
SMTP REQ  <i>rcvd_bytes</i> <i>sent_bytes</i> <i>sender</i> <i>recipient</i>	Auditing information about an SMTP request  <i>size of message before proxying</i> <i>size of message after proxying</i> <i>sender e-mail address (from envelope)</i> <i>recipient e-mail addresses (from envelope)</i>
SMTP MESSAGE FORMAT  <i>header</i> <i>mime_error</i> <i>sender</i> <i>recipients</i>	The SMTP header uses a format that is not correct  <i>header with improper format</i> <i>description of format error</i> <i>sender e-mail address (from envelope)</i> <i>recipient e-mail addresses (from envelope)</i>
SMTP IPS MATCH  <i>ips_msg</i> <i>signature_id</i>	The SMTP proxy found an IPS signature match  <i>description of the signature that matched</i> <i>the signature ID of the rule that matched</i>
SMTP TOO MANY RECIPIENTS  <i>num_recipients</i>	The number of e-mail addresses in the TO field is larger than the configured limit  <i>number of recipients</i>
SMTP RESPONSE SIZE TOO LONG  <i>headers_size</i>	The SMTP server sent a response that is too long  <i>total size of message headers (up to when log emitted; full headers can be larger)</i>
SMTP LINE LENGTH TOO LONG  <i>line_length</i>	The SMTP client or server has sent a line that is longer than the configured limit  <i>total size of header line (up to when log emitted; full line can be larger)</i>
SMTP MESSAGE SIZE TOO LONG  <i>size</i>	The SMTP client sent a message larger than the configured limit  <i>size in bytes of message received (up to when log emitted; full message can be larger)</i>
SMTP HEADERS SIZE TOO LONG  <i>headers_size</i>	The SMTP client sent a header section that is larger than the SMTP limit  <i>total size of message headers (up to when log emitted; full headers can be larger)</i>

### DNS Proxy Traffic Log Messages

Text in Message Field <i>Associated Fields</i>	Message Meaning <i>Value that appears in associated field(s)</i>
DNS INVALID NUMBER OF QUESTIONS	There is more than one RRs inquiry in one DNS request
DNS OVERSIZED QUERY NAME	The total DNS query frame size is larger than the DNS protocol limit
DNS COMPRESSED QUERY NAME	The client used a DNS compression scheme in the query name
DNS PARSE ERROR	The DNS request or response is not in the correct format.
DNS NOT INTERNET CLASS  <i>query_class</i>	The DNS query is not in IP protocol format  <i>name or number of its class</i>
DNS DENIED OPCODE  <i>rulename</i> <i>query_opcode</i>	The opcode matches a configured proxy rule  <i>name of rule matched in ruleset</i> <i>name of the denied opcode (IQUERY, STATUS, UPDATE)</i>
DNS DENIED QUERY TYPE  <i>rulename</i> <i>query_type</i>	The query type matches a configured proxy rule  <i>name of rule matched in ruleset</i> <i>name of denied type (a, MX, NS)</i>
DNS UNDERSIZED QUESTION	The name component of the DNS query is too small

## DNS Proxy Traffic Log Messages

<b>Text in Message Field</b> <i>Associated Fields</i>	<b>Message Meaning</b> <i>Value that appears in associated field(s)</i>
DNS OVERSIZED QUESTION	The name component of the DNS query is too large
DNS TIMEOUT	There is no response to a DNS query before the connection time-out occurred
DNS UNDERSIZED ANSWER	The DNS response is too small
DNS INVALID RESPONSE	The DNS response does not match the request
DNS QUESTION NOT ALLOWED <i>rulename</i> <i>query_type</i> <i>question</i>	The query type matches a configured proxy rule <i>name of rule matched in ruleset</i> <i>name of denied type (a, MX, NS)</i> <i>name in query</i>
DNS REQ <i>rulename</i> <i>query_type</i> <i>question</i>	Auditing information for the DNS proxy <i>name of rule matched in ruleset</i> <i>name of denied type (a, MX, NS)</i> <i>name in query</i>
DNS IPS MATCH <i>ips_msg</i> <i>signature_id</i>	The DNS proxy found an IPS signature match <i>description of the signature that matched</i> <i>the signature ID of the rule that matched</i>

## FTP Proxy Traffic Log Messages

<b>Text in Message Field</b> <i>Associated Fields</i>	<b>Message Meaning</b> <i>Value that appears in associated field(s)</i>
FTP USERNAME TOO LONG <i>length</i>	Username is longer than the configured limit <i>length of line</i>
FTP PASSWORD TOO LONG <i>length</i>	Password line is longer than the configured limit <i>length of line</i>
FTP FILENAME TOO LONG <i>length</i>	Filename line is longer than the configured limit <i>length of line</i>
FTP COMMAND TOO LONG <i>length</i>	Command line is longer than the configured limit <i>length of line</i>
FTP BAD COMMAND <i>rule_name</i> <i>command</i>	The command matched a configured proxy rule <i>name of rule matched in ruleset</i> <i>the command requested</i>
FTP BAD DOWNLOAD <i>rule_name</i> <i>file_name</i>	The file name or name pattern matches a configured proxy rule <i>name of rule matched in ruleset</i> <i>name of file being blocked</i>
FTP BAD UPLOAD <i>rule_name</i> <i>file_name</i>	The file name or name pattern matches a configured proxy rule <i>name of rule matched in ruleset</i> <i>name of file being blocked</i>
FTP TIMEOUT	There was no response to an FTP request before the IP-level idle connection time-out
FTP REQ <i>command</i>	Auditing information for the FTP proxy <i>the command requested</i>
FTP REQUEST FORMAT <i>command</i>	The command in the FTP request is not in the correct format <i>the command requested</i>
FTP IPS MATCH <i>ips_msg</i> <i>signature_id</i>	The FTP proxy found an IPS signature match <i>description of the signature that matched</i> <i>the signature ID of the rule that matched</i>

### HTTP Proxy Traffic Log Messages

Text in Message Field <i>Associated Fields</i>	Message Meaning <i>Value that appears in associated field(s)</i>
HTTP INTERNAL ERROR	
HTTP SERVER RESPONSE TIMEOUT	The HTTP server did not send a response before the configured time-out
HTTP CLIENT REQUEST TIMEOUT	The HTTP client did not send a request before the configured time-out
HTTP CLOSE COMPLETE TIMEOUT	The remote host did not promptly complete the closing of the TCP connection.
HTTP START LINE OVERSIZE	The first line of the HTTP request or response is larger than the configured limit (maximum header line length).
HTTP REQUEST LINE PARSE ERROR <i>line</i>	The first line of the HTTP request is not in the correct format.  <i>header line that caused error</i>
HTTP STATUS LINE PARSE ERROR <i>line</i>	The first line of the HTTP response is not in the correct format.  <i>status line that caused error</i>
HTTP HEADER LINE OVERSIZE <i>line</i>	The length of an individual header is greater than the configured limit.  <i>header line that exceeded the limit</i>
HTTP HEADER BLOCK OVERSIZE <i>line</i>	The total length of all headers for a request or response is greater than the configured limit.  <i>header line that exceeded the limit</i>
HTTP HEADER BLOCK PARSE ERROR	The HTTP header block is not in the correct format.
HTTP REQUEST URL PATH MISSING <i>line</i>	The HTTP request does not include a URL path.  <i>request line that caused error</i>
HTTP REQUEST URL MATCH  <i>rulename</i> <i>dstname</i> <i>arg</i>	The HTTP request includes a URL specified in the proxy ruleset.  <i>name of rule matched in ruleset</i> <i>host name from requested URL</i> <i>path and query-string from requested URL</i>
HTTP CHUNK SIZE LINE OVERSIZE <i>line</i>	The line setting the size of the next response data chunk has a value that is too big.  <i>request line that caused error</i>
HTTP CHUNK SIZE INVALID <i>line</i>	The line setting the size of the next response data chunk has an invalid value.  <i>request line that caused error</i>
HTTP CHUNK CRLF TAIL MISSING <i>line</i>	The "carriage-return/line-feed" (CRLF) at the end of a data chunk is not there.  <i>the line that caused the error</i>
HTTP FOOTER LINE OVERSIZE <i>line</i>	The length of an individual footer line is greater than the configured limit.  <i>request line that exceeded the limit</i>
HTTP FOOTER BLOCK OVERSIZE <i>line</i>	The total length of all footers for a request or response is greater than the configured limit..  <i>footer line that exceeded the limit</i>
HTTP FOOTER BLOCK PARSE ERROR	The HTTP footer block is not in the correct format.
HTTP BODY CONTENT TYPE MATCH <i>rulename</i>	The content type in the response body matches a type configured in the proxy rule set.  <i>name of rule matched in ruleset</i>
HTTP HEADER MALFORMED <i>line</i>	An individual HTTP header is not in the correct format.  the line with the malformed header
HTTP HEADER CONTENT LENGTH INVALID	The Content-Length response header value is not a valid number.

## HTTP Proxy Traffic Log Messages

Text in Message Field <i>Associated Fields</i>	Message Meaning <i>Value that appears in associated field(s)</i>
HTTP HEADER TRANSFER ENCODING INVALID	The response header includes illegal or unsupported transfer encoding.
HTTP HEADER TRANSFER ENCODING MATCH <i>rulename</i> <i>encoding</i>	The response header includes transfer encoding that matches the configured proxy rule set. <i>name of rule matched in ruleset</i> <i>Transfer-Encoding header value</i>
HTTP HEADER CONTENT TYPE MISSING	The Content-Type response header, which sets the response body MIME type, is missing or has an empty value.
HTTP HEADER CONTENT TYPE MATCH <i>rulename</i> <i>content_type</i>	The Content-Type response header, which sets the response body MIME type, matches the configured proxy rule set. <i>name of rule matched in ruleset</i> <i>value of content-type header</i>
HTTP REQUEST VERSION MATCH <i>rulename</i> <i>line</i>	The request protocol version (such as HTTP/1.1) matches the configured proxy rule set. <i>name of rule matched in ruleset</i> <i>request line that caused error</i>
HTTP REQUEST METHOD MATCH  <i>rulename</i> <i>method</i>	The HTTP request method matches the configured proxy rule set. <i>name of rule matched in ruleset</i> <i>request method that caused error</i>
HTTP HEADER MATCH  <i>rulename</i> <i>header</i>	The individual HTTP header (name and value) matches the configured proxy rule set. <i>name of rule matched in ruleset</i> <i>header line that matched</i>
HTTP HEADER COOKIE DOMAIN MATCH  <i>rulename</i> <i>domain</i>	The domain included in the Set-Cookie response header, or if none, then the host set in the request, matches the configured proxy rule set. (This feature is used to prevent cookies from a specified Web site.) <i>name of rule matched in ruleset</i> <i>domain parameter from Set-Cookie response header or (if not present in cookie) hostname in requested URL</i>
HTTP REQUEST HOST MISSING	The server host name is not included in the request line or in the "host" request header.
HTTP HEADER AUTH SCHEME MATCH  <i>rulename</i> <i>scheme</i>	The WWW-Authenticate response header includes an authentication scheme that matches the configured proxy rule set. <i>name of rule matched in ruleset</i> <i>scheme parameter from WWW-Authenticate response header</i>
HTTP REQUEST METHOD UNSUPPORTED  <i>method</i>	The request includes a method not currently supported. This can result from the use of an HTTP-based protocol with additional non-HTTP methods. <i>request method that caused error</i>
HTTP REQUEST PORT MISMATCH	The destination TCP port of the connection does not match the TCP port used in the header. Can indicate an attempt to get access to an outside proxy server.
HTTP REQUEST CATEGORIES  <i>cats</i> <i>dstname</i> <i>arg</i>	An HTTP request was denied by WebBlocker.  <i>comma delimited list of WebBlocker categories which match host name from requested URL path and query-string from requested URL</i>
HTTP SERVICE UNAVAILABLE  <i>service</i> <i>details</i>	The WebBlocker server is not responding. <i>name of ProtocolHandler Helper</i> <i>explanation of problem</i>
HTTP REQUEST URL PATH OVERSIZE	The URL component of the HTTP request start line is too big.

### HTTP Proxy Traffic Log Messages

Text in Message Field <i>Associated Fields</i>	Message Meaning <i>Value that appears in associated field(s)</i>
HTTP REQ <i>op</i> <i>dstname</i> <i>arg</i>	Auditing information about an HTTP request. <i>HTTP request method</i> <i>hostname from requested URL</i> <i>path and query-string from requested URL</i>
HTTP HEADER IPS MATCH <i>ips_msg</i> <i>signature_id</i>	The HTTP header matches an IPS signature. <i>description of the signature that matched</i> <i>the signature ID of the rule that matched</i>
HTTP BODY IPS MATCH <i>ips_msg</i> <i>signature_id</i>	The HTTP body matches an IPS signature. <i>description of the signature that matched</i> <i>the signature ID of the rule that matched</i>
HTTP BYTECOUNT UPDATE	Auditing information for an HTTP request that has a very large response.

### TCP Proxy Traffic Log Messages

Text in Message Field <i>Associated Fields</i>	Message Meaning <i>Value that appears in associated field(s)</i>
TCP REQ <i>outgoing_msg</i>	<i>the mode the handler is in.</i>
TCP IPS MATCH <i>ips_msg</i> <i>signature_id</i>	TCP proxy found an IPS signature match. <i>description of the signature that matched</i> <i>the signature ID of the rule that matched</i>

---

## Alarm Logs

Alarm logs are sent when an alarm condition is met. The Firebox sends the alarm log to the Traffic Monitor and Log Server and triggers the specified action.

Some alarms are set in your Firebox configuration. For example, you can use Policy Manager to configure an alarm to occur when a certain threshold is met. Other alarms are set by default. The Firebox sends an alarm log when a network connection on one of the Firebox interfaces fails. This cannot be changed in your configuration. The Firebox never sends more than 10 alarms in 15 minutes for the same set of conditions.

There are eight categories of alarm logs: System, IPS, AV, Policy, Proxy, Probe, Denial of service, and Traffic. There is a table below for each category of alarms, showing the format of the alarm log messages in each category.

## Policy Alarms

Default Name	Message Format	Example Message	Caused By
Policy	alarm_name="WGRD_PM_BP_Alarm", alarm id, timestamp, message, policy name, source IP, destination IP, protocol, source port, destination port, source interface, destination interface, log_type="al"	alarm_name="WGRD_PM_BP_Alarm" alarm_id="4001" time="Wed Mar 2 07:41:21 2005 (PST)" msg="Block" policy="WGRD_PM_BP_Policy" src_ip="24.56.20.79" dst_ip="192.168.30.164" pr="tcp/sun-rpc" src_port="1727" dst_port="111" src_intf="0-External" dst_intf="2-Optional-1" log_type="al"/	These alarms are caused by events associated with each policy.

## Proxy Alarms

Default Name	Message Format	Example Message	Caused By
Proxy	alarm_name="Proxy", alarm_id, time, message, source IP, destination IP, protocol, source port, destination port, source interface destination interface, log_type="al"	alarm_name="Proxy" alarm_id="6001" time="Tue Aug 3 00:49:35 2004 (PST)" msg="ProxyAllow/HTTP Request method match" src_ip="192.168.1.102" dst_ip="16.0.0.107" pr="tcp/smtp" src_port="1384" dst_port="25" src_intf="PPTP" dst_intf="1-Trusted" log_type="al"/	These alarms are caused by events associated with each proxy action.

## System Alarms

Default Name	Message Format	Example Message	Caused By
System	<i>alarm_name</i> detected, <i>message_string</i> .	System detected. [1401-0512@H] user abc failed to log in from 192.168.228.226.  System detected. [1401-0202@H] Number of IPSec tunnels 2500 reaches max IPSec tunnels allowed.	These alarms are triggered by system events.

### Denial of Service (DoS) Alarms

Default Name	Message Format	Example Message	Caused By
DOS	<i>alarm_name</i> detected. <i>message_string</i> .	NOTE: The content of this alarm message is based on what DOS event triggered it. See the examples below.	These alarms are triggered by any DOS events.
SYN-Attack	<i>alarm_ame</i> detected. TCP SYN attack detected on interface <i>interface_number</i> ."	SYN-Attack detected. TCP SYN attack detected on interface 1.	These alarms are triggered by SYN attacks.
UDP-Flood	<i>alarm_name</i> detected. UDP Flood attack detected on interface <i>interface_number</i> .	UDP-Flood detected. UDP Flood attack detected on interface 1.	These alarms are triggered by UDP Flood attacks.
ICMP-Flood	<i>alarm_name</i> detected. ICMP Flood attack detected on interface <i>interface_number</i> .	ICMP-Flood detected. ICMP Flood attack detected on interface 1.	These alarms are triggered by ICMP Flood attacks.
Ping-of-Death	<i>alarm_name</i> detected, PING-OF-DEATH attack detected on interface <i>interface_number</i> .	Ping-of-Death detected. PING-OF-DEATH attack detected on interface 1.	These alarms are triggered by Ping-of-Death attacks.
Source-Route	<i>alarm_name</i> detected. SOURCE-ROUTE attack detected on interface <i>interface_number</i> .	Source-Route detected. SOURCE-ROUTE attack detected on interface 1.	These alarms are triggered by Source-Route attacks.
IPSec-Flood	<i>alarm_name</i> detected. IPSEC Flood attack detected on interface <i>interface_number</i> .	IPSec-Flood detected. IPSEC Flood attack detected on interface 1.	These alarms are triggered by high severity level and IPSec Flood attacks.
IKE-Flood	<i>alarm_name</i> detected. IKE Flood attack detected on interface <i>interface_number</i> .	IKE-Flood detected. IKE Flood attack detected on interface 1.	These alarms are triggered by IKE Flood attacks.
DDOS-Attack-Src	<i>alarm_name</i> detected. Denial-of-Service attacks (> <i>threshold</i> ) from source <i>IP address/subnet</i> mask detected on interface <i>interface_number</i> .	DDOS-Attack-Src detected. Denial-of-Service attacks (.50) from source 192.168.226.226/255.255.255.255 detected on interface 1.	These alarms are triggered by Distributed Denial of Service Source attacks.
DDOS-Attack-Dest	<i>alarm_name</i> detected. Denial-of-Service attacks (> <i>threshold</i> ) for destination <i>IP address/subnet</i> mask detected on interface <i>interface_number</i> .	DDOS-Attack-Src detected. Denial-of-Service attacks (.50) for destination 192.168.226.226/255.255.255.255 detected on interface 1.	These alarms are triggered by Distributed Denial of Service Destination attacks.

## Denial of Service (DoS) Alarms

Default Name	Message Format	Example Message	Caused By
Port-Scan	<i>alarm_name</i> detected. <i>message_string</i> .	Port-Scan detected. Port scan threshold 300 reached, 300 ports scanned by 192.168.228.226 in 10 seconds.	These alarms are triggered by Port Space Probe attacks.
IP-Scan	<i>alarm_name</i> detected. <i>message_string</i> .	IP-Scan detected. IP scan threshold 300 reached, 300 IPs scanned by 192.168.228.226 in 10 seconds.	These alarms are triggered by Address Space Probe attacks.
IP-Spoofing	<i>alarm_name</i> detected. <i>message_string</i> .	IP-Spoofing detected. IP source spoofing detected, src_intf=30, src_ip=192.168.228.226.	These alarms are triggered by IP Spoofing attacks.
Tear-Drop	<i>alarm_name</i> detected. TEAR-DROP attack detected on interface <i>interface_number</i> .	Tear-Drop detected. TEAR-DROP attack detected on interface 1.	These alarms are triggered by Tear-Drop attacks.

## Traffic Alarms

Default Name	Message Format	Example Message	Caused By
Traffic	<i>alarm_name</i> detected, <i>message_string</i> .	NOTE: The content of this alarm message is based on what traffic event triggered the alarm. See the examples below.	These alarms are triggered by any traffic events.
ESP-Auth-Error	<i>alarm_name</i> detected. ESP Authentication error, policy_id= <i>policy_id_number</i> , local_ip= <i>local_IP_address</i> , peer_ip= <i>peer_IP_address</i> , spi= <i>spi</i> , sa_id= <i>ID_of_SA</i> , interface= <i>interface_number</i> , the first (x) bytes are <i>list_of_first x number of bytes</i> .	ESP-Auth-Error detected. ESP Authentication error, policy_id=2, local_ip=10.10.10.10, peer_ip=192.168.228.226, spi=12345678, sa_id=1000, interface=1, the first 80 bytes are A0 B1 C2.....	These alarms are triggered by the traffic event "ESP-AUTH_ERR".
AH-Auth-Error	<i>alarm_name</i> detected. AH Authentication error, policy_id= <i>policy_id_number</i> , local_ip= <i>local_IP_address</i> , peer_ip= <i>peer_IP_address</i> , spi= <i>spi</i> , sa_id= <i>ID_of_SA</i> , interface= <i>interface_number</i> , the first (x) bytes are <i>list_of_first x number of bytes</i> .	AH-Auth-Error detected. AH Authentication error, policy_id=2, local_ip=10.10.10.10, peer_ip=192.168.228.226, spi=12345678, sa_id=1000, interface=1, the first 80 bytes are A0 B1 C2.....	These alarms are triggered by the traffic event "AH-AUTH_ERR".

**Traffic Alarms**

Default Name	Message Format	Example Message	Caused By
ESP-Replay-Error	<i>alarm_name</i> detected. ESP replay error, <i>policy_id=policy_id_number</i> , <i>local_ip=local_IP_address</i> , <i>peer_ip=peer_IP_address</i> , <i>spi=spi</i> , <i>sa_id=ID_of_SA</i> , <i>interface=interface_number</i> , the first (x) bytes are <i>list_of_first x number of bytes</i> .	ESP-Replay-Error detected. ESP replay error, <i>policy_id=2</i> , <i>local_ip=10.10.10.10</i> , <i>peer_ip=192.168.228.226</i> , <i>spi=12345678</i> , <i>sa_id=1000</i> , <i>interface=1</i> , the first 80 bytes are A0 B1 C2.....	These alarms are triggered by the traffic event "ESP_REPLAY_ERROR".
AH-Replay-Error	<i>alarm_name</i> detected. AH replay error, <i>policy_id=policy_id_number</i> , <i>local_ip=local_IP_address</i> , <i>peer_ip=peer_IP_address</i> , <i>spi=spi</i> , <i>sa_id=ID_of_SA</i> , <i>interface=interface_number</i> , the first (x) bytes are <i>list_of_first x number of bytes</i> .	AH-Replay-Error detected. AH replay error, <i>policy_id=2</i> , <i>local_ip=10.10.10.10</i> , <i>peer_ip=192.168.228.226</i> , <i>spi=12345678</i> , <i>sa_id=1000</i> , <i>interface=1</i> , the first 80 bytes are A0 B1 C2.....	These alarms are triggered by the traffic event "AP_REPLAY_ERROR".
Invalid-SPI	<i>alarm_name</i> detected. Invalid SPI <i>%d(0x%x)</i> detected on interface <i>interface_number</i> , the first (x) bytes are <i>list_of_first x number of bytes</i> .	Invalid-SPI detected. Invalid SPI 12345678 (0xBC614E) detected on interface 1, the first 80 bytes are A0 B1 C2.....	These alarms are triggered by the traffic event "INVALID_SPI".
Other-Policy-Error	<i>alarm_name</i> detected. Policy error detected on interface <i>interface_number</i> , the first (x) bytes are <i>list_of_first x number of bytes</i> .	Other-Policy-Error detected. Policy error detected on interface 1, the first 80 bytes are A0 B1 C2.....	These alarms are triggered by the traffic event "OTHER_AUTH_ERROR".

**Probe Alarms**

Default Name	Message Format	Example Message	Caused By
AnyProbe Alarm	<i>Operator</i> [Probe <i>probe_name</i> : <i>probe_value</i> (value) <i>alarm_cond_op_name threshold</i> (threshold)]	NOTE: The content of this alarm message is based on the event that triggered the alarm. See the examples below.	These alarms are triggered by counter values.
Link-Down		[Probe Link Status: 0.00 (value) becomes 0.00 (threshold)] OR [Probe Link Status: 1.00 (value) becomes 0.00 (threshold)] OR [Probe Link Status: 0.00 (value) becomes 0.00 (threshold)]	These alarms are triggered by interface counters..

## Gateway AntiVirus Service Alarms

Default Name	Message Format	Example Message	Caused By
AV	alarm_name="AV" alarm id, timestamp, message, source IP, destination IP, protocol, source port, destination port, source interface, destination interface, virus name, sender, log_type="al"	alarm_name="AV" alarm_id="6001" time="Mon Aug 2 22:20:44 2004 (PST)" msg="SMTP Filename" src_ip="192.168.1.102" dst_ip="16.0.0.107" pr="tcp/smtp" src_port="1384" dst_port="25" src_intf="PPTP" dst_intf="1-Trusted" virus="Eicar-Test-Signature" sender="phillip@sjcqa.com" log_type="al"/	These alarms are caused by events associated with each AV rule of the SMTP proxy action.

## Intrusion Prevention Service Alarms

Default Name	Message Format	Example Message	Caused By
IPS	alarm_name="IPS", alarm id, timestamp, message, source IP, destination IP, protocol, source port, destination port, source interface, destination interface, IPS message, signature category, signature ID, log_type="al"	alarm_name="IPS" alarm_id="3001" time="Wed Aug 4 00:58:33 2004 (PST)" msg="IPS" src_ip="16.0.0.1" dst_ip="16.0.1.107" pr="tcp/http" src_port="4110" dst_port="80" src_intf="1-Trusted" dst_intf="0-External" ips_msg="WEB-ATTACKS kill command attempt" signature_cat="http-request" signature_id="1335" log_type="al"/	These alarms are caused by different protocol types.

## Event Logs

Event logs are created because of Firebox user activity. Events that cause event logs include:

- Firebox start up/shut down
- Firebox and VPN authentication
- Process start up/shut down
- Problems with the Firebox hardware components
- Any task done by the Firebox administrator

On a Firebox using Fireware appliance software, there are seven product components, including 27 different log modules, that create event and diagnostic log messages to send to the log server. The function of each log module is shown in the table that follows.

## Description of Log Modules

Product Component	Log Module	Function
VPN	IKE	Internet Key Exchange daemon. Diagnose the configuration and operation of VPN tunnels.
	PPTP	Point to Point Tunneling Protocol daemon. Diagnose the daemon that manages PPTP for VPN tunnels.
High Availability	VRRP	Virtual Router Redundancy Protocol daemon. Diagnose the module that manages the virtual router for High Availability.
	HAM	High Availability Manager. Diagnose the module that manages High Availability operations.
	TPDAEMON	Transport (HA) Protocol. Diagnose the module that manages the High Availability transport protocol.
Dynamic IP	DHCLIENT	DHCP client. Diagnose the module that gets IP addresses for DHCP clients.
	DHCPD	DHCP server. Diagnose the module that DHCP servers use to give IP addresses to clients.
	DHCRELAY	DHCP relay. Diagnose the module that relays DHCP requests to another server.
	PPP	Point to Point protocol daemon. Diagnose the daemon that gives you PPP protocol support for PPPoE and PPTP.
	PPPoE (shows in the log file as ADSL)	Point to Point Protocol over Ethernet daemon. Diagnose the daemon that manages PPPoE.
Proxy	CFM	Connection Framework Manager. Diagnose the service that manages proxy protected connections.
	SM	Session Manager. Diagnose the module that converts network packet streams into TCP connections and UDP connections.
	HTTP	Hypertext Transfer Protocol proxy. Diagnose the process that analyzes HTTP connections.
	SMTP	Simple Mail Transfer Protocol proxy. Diagnose the process that analyzes SMTP connections.
	FTP	File Transfer Protocol proxy. Diagnose the process that analyzes FTP connections.
	DNS	Domain Name Service proxy. Diagnose the analysis service for DNS connections.
	WEBBLOCKER	WebBlocker Server daemon. Diagnose the module that gives you the list of Web sites to block.
	AV	AntiVirus Server. Diagnose the server that supports AV detection.
Management	CMM	Configuration Maintenance Manager. Diagnose the module that manages device configuration.
	SNMP	Simple Network Management Protocol daemon. Diagnose the module that can query for SNMP MIB and can send SNMP traps to the user.
	MA	Monitoring Agent. Diagnose Alarm Manager, the module that collects alarms and determines the alarm response.
	MIA	Management Information Agent. Diagnose the module that captures appliance statistics.

## Description of Log Modules

Product Component	Log Module	Function
	MONITOR	Monitor daemon. Diagnose the daemon that monitors the network link.
	Webs (GOAHEAD)	Web server. Diagnose the device Web server that supports Web authentication and WSM.
	DVCPD	Dynamic VPN Control Protocol Client daemon. Diagnose the daemon that manages devices under DVCP control.
Packet Filter	PMM	Policy Management Module. Diagnose the module that manages and controls packet filter policies.
Authentication	ADM	Authentication Domain Manager. Diagnose the module that authenticates packet filters and VPN tunnels.

## Event Log Messages

This table includes the messages for most event logs generated by a Firebox using Fireware appliance software, divided by log module.

### Event Log Message Catalog

Log Module	Log Message ID	Message
ADM	1000	The ADM daemon started
ADM	1001	The ADM daemon stopped
ADM	1002	The ADM set the event/trace level to %d/%d
ADM	1003	Is this message necessary?
ADM	1004	ADM cannot allocate memory
ADM	1005	ADM authentication server %s:%d did not respond
ADM	1006	ADM authentication is using this server %s:%d
ADM	1007	This ADM authentication server %s:%d is not available
ADM	1008	This ADM authentication server %s:%d is available
ADM	1009	Need more information about the ADM auth user [%s@%s]
ADM	1010	ADM authentication switched to this secondary server %s:%d
ADM	1011	ADM domain configuration contains an incorrect entry <%s>
ADM	1012	ADM auth %s user [%s@%s] accepted
ADM	1013	ADM auth %s user [%s@%s] from %s rejected
ADM	1014	ADM auth %s user [%s@%s] Server Challenge
ADM	1015	ADM auth %s user [%s@%s] rejected, exceeded login limit
ADM	1016	ADM auth %s user [%s@%s] error, reason - %s
ADM	1017	ADM auth %s user [%s@%s] error, RADIUS auth method %s not supported
ADSL	100	Your IP addresses are mismatched. Do a check to make certain that the IP addresses are correct.
ADSL	101	The ADSL connection on %s is on
ADSL	102	The ADSL link on %s ended
ADSL	201	A signal stopped the ADSL daemon

**Event Log Message Catalog**

Log Module	Log Message ID	Message
ADSL	2015	PPP Authentication failed. Either Auth Server is down or user account information is incorrect!
ADSL	2016	Unable to establish PPP session.
ADSL	2017	PPP link is available. System will be ready.
ADSL	2018	Inactive Timeout (%s minutes)! Bring down PPP session.
ADSL	2019	Received on demand request for PPP session. Establishing PPP..
ADSL	2020	PPP session (ON_DEMAND) is ready
ADSL	2021	Exceed max auth retry period (%sk). PPP Authentication failed.
CFM	001	event high '%s'
CFM	002	event low '%s'
CFM	003	worker=[%d] ready
CFM	005	worker=[%d] exiting
CFM	006	exiting
CFM	010	error in options parsing
CFM	016	skip loading of SM
CFM	025	unable to load SM
CFM	040	worker=[%d] quitting
CFM	040	CFM crashed!
CFM	041	%s
CFM	085	unable to initialize SM
CFM	097	unable to load config for worker PID[%d]
CFM	101	unable to find worker with PID [%d]
CFM	155	invalid UDS command='%s' from '%s' id=[%d]
CFM	001	internal error
CFM	001	unable to lock connection table: %s
CFM	002	unable to unlock connection table: %s
CFM	003	no more available connections
CFM	004	unable to extract proxy action from hash: %s
CFM	005	no pointer in payload
CFM	006	unable to read %lu from SM: %s
CFM	007	received a read event with no data waiting: %s
CFM	008	unable to get channel info
CFM	009	unable to drop timer
CFM	010	unable to flush input
CFM	011	unable to unblock input mode
CFM	012	unable to connect a new session: %s
CFM	013	connect requested for active connection
CFM	014	failed to create event type: '%s' channel: %s
CFM	015	unable to close session: %s

## Event Log Message Catalog

Log Module	Log Message ID	Message
CFM	016	unable to abort session: %s
CFM	018	unable to queue payload
CFM	019	unable to append to payload
CFM	020	unable to write data: %s
CFM	021	unable to add timer at %u ticks
CFM	022	unable to get number of ticks remaining
CFM	023	request to queue an empty payload
CFM	024	request to write an empty payload
CFM	025	output requested with an invalid output scheme
CFM	026	no callback registered: proxy action %s
CFM	027	proxy action %s is disabled. Not allowing new connection.
CFM	028	proxy action %s will be deleted. Not allowing new connections.
CFM	029	proxy action %s reached %lu connections. Not allowing any new connections.
CFM	030	protocol handler %s has reached %lu connections. Not allowing any new connections.
CFM	031	received session connected with unknown proxy action: %s
CFM	032	unknown connection event type: %s
CFM	033	unable to process CONNECTED for dynamic chaining
CFM	034	unable to process new connection for dynamic chaining
CFM	035	not handling connection refused
CFM	036	received an invalid connection ID: %c:%u:%u
CFM	037	received write event for session with no data queued: %s
CFM	038	unable to get events: %s
CFM	039	unable to add timer group
CFM	040	unable to redirect connection to CFM %d: %s
CFM	041	unable to register %s
CFM	042	not given a connection table
CFM	043	unable to open current directory
CFM	044	unable to change to parent directory
CFM	045	unable to open %s SM device: %s
CFM	046	unable to change to previous directory
CFM	047	unable to get SM library file descriptor: %s
CFM	048	unable to add a listener
CFM	049	unable to create timer
CFM	050	unable to start timer
CFM	051	unable to create shared memory: too big (%lu > %lu)
CFM	052	unable to create shared memory (%s): %s
CFM	053	unable to set counter shared memory functions
CFM	054	unable to initialize counter context
CFM	055	unable to clean up child processes

## Event Log Message Catalog

Log Module	Log Message ID	Message
CFM	056	unable to initiate handler for proxy action %s
CFM	057	unable to start SM: %s
CFM	058	unable to find %p handler for signal %d
CFM	100	dropping %lu bytes of input data buffered for %s: %d
CFM	101	dropping %lu bytes of output data queued for %s: %d
CFM	102	%lu connection events read (max: %u)
CFM	103	%lu I/O events read (max: %u)
CFM	001	received %s with an active connection at index %lu (%s)
CFM	002	received %s with another worker ID [%u] instead of [%u]
CFM	003	received %s with no active connection at index %lu
CFM	004	received %s event with a payload
CFM	005	no %s callback defined
CFM	006	callback failed for %s event in %s handler using %s proxy action
CFM	007	handler stuck in CALL NEXT loop. Stopping after %d iterations
CFM	008	data queued for input
CFM	009	invalid input mode: %d
CFM	010	unable to duplicate view
CFM	011	unable to seek view
CFM	012	unable to set view length
CFM	013	unable to cut view
CFM	014	unable to concat view
CFM	015	unable to register %s variable
CFM	001	unable to append payload
CFM	002	unable to copy data from payload
CFM	003	unable to rewind payload
CFM	004	unable to send response
CFM	005	unable to close channel
CFM	006	unknown variable type: %u
CFM	007	name already exists: %s
CFM	100	internal error
CFM	201	Failed to load IPS signatures name='%s'
CMM	512	%s failed to log in from %s
CMM	512	%s failed to log in
CMM	513	%s attempted to log in
CMM	514	%s logged in
CMM	515	%s logged in from %s
CMM	516	%s logged out
CMM	517	User session %s timed out because of inactivity
CMM	518	%s account is disabled

## Event Log Message Catalog

Log Module	Log Message ID	Message
CMM	520	%s logged out %s user %s
CMM	528	%s failed to update password
CMM	529	%s updated password
CMM	530	%s failed to restore to factory default configuration
CMM	535	%s upgrade failed. Error = %s
CMM	537	%s upgrade complete
CMM	538	%s changed operational mode to %s
CMM	539	%s changed login limit
CMM	540	%s unlocked all disabled accounts
CMM	541	%s unlocked this disabled account: %s
CMM	542	%s backup failed. Error = %s
CMM	551	Peer Firebox updated %s configuration
CMM	552	%s updated %s configuration
CMM	553	Peer Firebox updated %s to %s
CMM	554	%s updated %s to %s
CMM	555	%s imported a certificate
CMM	556	%s imported a CRL
CMM	557	%s removed a certificate
CMM	558	%s failed to install the license
CMM	559	%s added %d license(s) in bulk license
CMM	559	%s retrieved licenses
CMM	568	%s rebooted the Firebox
CMM	569	%s restarted the Firebox
CMM	570	%s shut down the Firebox
CMM	574	%s saved the configuration
CMM	575	%s failed to restore the configuration
CMM	576	%s restored the configuration
CMM	578	%s restored to factory default status
CMM	649	Successfully committed policy
CMM	664	%s failed to cancel policy changes
CMM	665	%s canceled policy changes
CMM	682	%s upgraded model number to X%d
CMM	683	License %s expires soon
CMM	684	%s feature will expire in %s. Please contact WatchGuard LiveSecurity to renew your subscription.
CMM	685	%s feature expired. Please contact WatchGuard LiveSecurity to renew your subscription.
CMM	687	%s forced a failover
CMM	688	%s recovered this Firebox
CMM	689	%s recovered the peer HA Firebox
CMM	690	HA is disabled. The error is %s

## Event Log Message Catalog

Log Module	Log Message ID	Message
CMM	691	%s synchronized configuration to peer HA Firebox
CMM	692	%s failed to discover peer Firebox. Error=%s
CMM	693	%s failed to synchronize configuration to peer HA Firebox. Error=%s
CMM	700	%s failed to change policy related configuration. Error=%s
CMM	725	%s failed to import XML file. Error=%s
CMM	726	%s failed to update system settings after importing XML file. Error=%s
CMM	727	%s imported an XML file
CMM	728	%s exported an XML file
CMM	729	%s deleted system log files
CMM	731	%s user added %s %s
CMM	733	<b>%s user</b> updated %s %s
CMM	734	<b>%s user</b> deleted %s %s
CMM	736	<b>%s'</b> moved by user '%s' from '%d' to '%d'
CMM	749	%s. Please contact WatchGuard LiveSecurity for licensing service.
CMM	750	<b>%s user</b> changed %s
CMM	751	%s license expired
CMM	752	%s configuration error. Error=%s
CMM	753	%s daemon started
CMM	754	%s daemon stopped
DHCPC	200	%s
DHCPD	100	DHCPD starts
DHCPD	200	%s
DHCPR	200	%s
DVCPCD	1000	Starting up...
DVCPCD	1001	Exiting...
DVCPCD	1010	Start to initialize
DVCPCD	1011	Failed to initialize
DVCPCD	1013	Initialization completed
DVCPCD	1014	No DVCP servers configured
DVCPCD	1020	Contacting server %s in %d seconds
DVCPCD	1021	Contacting DVCP server %s with client id %s
DVCPCD	1022	Cannot connect to DVCP server %s: %s
DVCPCD	1023	Cannot get status from server %s, %s
DVCPCD	1024	There is no configuration update from server %s
DVCPCD	1025	Waiting for the read/write privilege
DVCPCD	1040	Submitting certificate request to DVCP server %s

## Event Log Message Catalog

Log Module	Log Message ID	Message
DVCPCD	1041	The Firebox cannot get certificates from this server %s, %s
DVCPCD	1042	The Firebox is importing the CA certificate
DVCPCD	1043	The Firebox cannot import the CA certificate
DVCPCD	1044	The Firebox imported the CA certificate
DVCPCD	1045	The Firebox is importing the VPN certificate
DVCPCD	1046	Cannot import the VPN certificate
DVCPCD	1047	Successfully imported the VPN certificate
DVCPCD	1050	Cannot load configuration (export xml config)
DVCPCD	1051	Requesting new configuration from server %s
DVCPCD	1052	Cannot download configuration from server %s, %s
DVCPCD	1053	Cannot save this new configuration: %s
DVCPCD	1054	The new configuration was saved
HAM	0	The HA manager is initialized and enabled
HAM	2	The Firebox is now in active mode
HAM	4	The Firebox starts with HA disabled
HAM	7	Firebox restart completed and HA is now ready
HAM	20	The Configuration manager sets HA manager with invalid HA type: %d
HAM	107	HA: The Firebox did not complete the secure transport channel process (error: %s)
HAM	108	Secure channel is dropped! (error:%s)
HAM	110	TCP connection was broken! (error:%s)
HAM	214	HA: Received a fail notification from peer (error:%s)
HAM	218	HA: Start the forced failover process (error:%s)
HAM	222	HA:The hotsync procedure failed (error:%s)
HAM	231	HA: The secure channel was not set (rc=%d)
HAM	232	HA: Mismatched HA peer information (error:%s)
HAM	233	HA: The peer Firebox is upgrading. Need to takeover!
HAM	234	HA event monitor is enabled and the system starts from the WAITADMIN state
HAM	301	HA: The HA link is down on port %d
HAM	302	HA: The Firebox is missing the MIA heartbeat
HAM	304	HA: The Firebox will failover because (%s). Info=%d
HAM	307	HA: The Firebox is now active because of peer restarts or because peer is unavailable
HAM	308	HA: The Firebox is in standby mode
HAM	310	HA: Process the forced failover command
IKE	0	There is no CA Certificate available for the certificate payload build
IKE	1	Cannot convert the CA name from DER to X509
IKE	2	Certificate chain forming failure because there is no matching certificate

## Event Log Message Catalog

Log Module	Log Message ID	Message
IKE	3	Certificate chain forming failure because the size is too large
IKE	4	Certificate chain forming failure: %s
IKE	5	Certificate validation failure: %s
IKE	6	Certificate validation failed because the Firebox cannot retrieve the public key
IKE	7	Cannot validate peer ID in certificate (idType %d)
IKE	8	Cannot retrieve private key in certificate (id %d)
IKE	1000	IKE full policy loading complete
IKE	1002	IKE ready to have trace level %d and event level %d
IKE	1003	IKE is set to use LDAP server (%s)
IKE	1005	IKE daemon is starting
IKE	1006	IKE daemon stopped
IKE	1007	IKE uses software crypto
IKE	1008	IKE uses hardware crypto card for the public key cipher
IKE	1600	Try primary RADIUS server %s
IKE	1601	Backup RADIUS server (%s) is not responding
IKE	1602	Backup RADIUS server (%s) is not responding. Switch to primary server %s
IKE	1603	Primary RADIUS server (%s) is not responding
IKE	1604	Primary RADIUS server (%s) is not responding. Switch to backup RADIUS server %s.
IKE	1605	Primary RADIUS server (%s) is not responding. No backup RADIUS server configured.
IKE	9007	IKE is terminated by SIGBUS (%d). System may be out of memory.
IKE	9011	IKE is terminated by SIGSEGV (%d). System may become unstable.
MA	1000	received SIGTERM, MA daemon is shutting down
MIA	100	eth%d is up.
MIA	101	eth%d is down
MIA	201	The number of allowed IPSec tunnels %d is at 90% of its limit
MIA	202	The current number of IPSec tunnels %d is at its limit.
MIA	203	The number of %s exceeds its high water mark %lu.
MIA	204	The number of %s is at its limit %lu.
MIA	301	Deleted tunnel to peer %s.
MIA	302	The system's cooling fan failed.
MIA	303	The system's supply power failed.
MIA	304	The system's cooling fan recovered.
MIA	305	The system's supply power recovered.
MIA	306	This load balancing server %s recovered.
MIA	307	The load balancing server %s does not respond.
MIA	308	Heartbeats lost.

## Event Log Message Catalog

Log Module	Log Message ID	Message
MIA	309	Heartbeats recovered.
MIA	310	Received SIGTERM, MIA daemon is shutting down.
MIA	401	Added MUVPN user group %s (%d).
MIA	402	Deleted MUVPN user group %s (%d).
MIA	403	Updated MUVPN user group %s (%d).
MIA	404	Phase 1 SA %d set for MUVPN user %d.
MIA	405	Phase 1 rekey for MUVPN user %d.
MIA	406	MUVPN user %s logged in from %s.
MIA	407	MUVPN user %s (login from %s) logged out.
MIA	408	Cannot add a tunnel %d to MUVPN user %s because the phase 1 SA %d does not exist or is expired
MIA	409	Add tunnel %d to MUVPN user %s. The phase 1 SA is %d.
MONITORD	100	%s is connected
MONITORD	101	%s is disconnected
MONITORD	102	Response from gateway %s on %s received
MONITORD	103	No response from gateway %s on %s
MONITORD	201	The intermodule connection does not work
MONITORD	202	LNKMON cannot activate this service socket: %d
PMM	1	Firewall user %s from %u.%u.%u.%u logged out due to idle timeout
PMM	2	%s
PMM	3	policy="\%s\" %s%s%s%s%s rc="\%d\" msg="\%s%s%s%s\" pckt_len="\%s\" ttl="\%s\"
PMM	4	policy="\%s\" %s rc="\%d\" msg="\%s\"
PMM	5	policy="\%s\" src_ip="\\" dst_ip="\\" pr="\\" src_port="\\" dst_port="\\" src_intf="\%s\" dst_intf="\\" rc="\%d\" msg="\%s\"
PMM	6	Firewall user %s from %u.%u.%u.%u logged in.
PMM	7	Firewall user %s from %u.%u.%u.%u logged out.
PMM	100	Failed to open %s: %s.
PMM	101	Failed to update run time %s.
PMM	102	%s is %s %s by unknown module.
PMM	103	%s is %s %s by %s
PPTP	1000	Starting up pptpd
PPTP	2001	PPTP CHAP authentication OK for peer %s
PPTP	2002	PPTP CHAP authentication failed for peer %s
PPTP	2003	PPTP connection up for %s
PPTP	2004	PPTP connection down for %s
PPTP	2005	PPTP authentication server %s:%d not responding

## Event Log Message Catalog

Log Module	Log Message ID	Message
SM	003	SM already running
SM	003	SM start failed
SM	010	Unsupported IP version (%u)
SM	011	Fragment discarded
SM	012	Short IP header (%u)
SM	013	IP options discarded
SM	014	Invalid parameter
SM	015	Invalid CID
SM	016	Invalid packet
SM	017	No channel in %s (%c:%u:%u)
SM	018	Unsupported protocol (%u)
SM	019	Protocol error
SM	020	Null state in %s (%c:%u:%u)
SM	021	Alloc failed
SM	022	Free failed
SM	023	PMM and SM CID mismatch in %s (%c:%u:%u %c:%u:%u)
SM	024	Queue append failed
SM	025	Tblmap set failed
SM	026	Tblmap unset failed
SM	027	Connection mask not set
SM	028	Event bit set but no event
SM	029	Channel not in the CFM
SM	030	Failed to initiate CONNECT
SM	031	Channel already CLOSED (%c:%u:%u)
SM	032	Unsupported ICMP type %u
SM	033	Setting mask failed
SM	034	Data written after close (%c:%u:%u)
SM	035	Internal error
SM	036	Acquire failed
SM	037	Connection table full
SM	038	Destroy failed (%d)
SM	039	Push failed
SM	043	freeing entry in PMM (%c:%u:%u)
SM	044	deleted previously (%c:%u:%u)
SM	050	Reserve failed
SM	051	Release failed
SM	052	Timeout failed
SM	053	Abort failed
SM	054	Close failed
SM	055	Read failed

## Event Log Message Catalog

Log Module	Log Message ID	Message
SM	056	Pre-connect failed
SM	057	Connect failed
SM	058	Write failed
SM	059	Refuse failed
SM	080	Unknown command %u
SM	081	Invalid arguments %u
SM	082	Invalid address %u
SM	100	ACK transmit failed
SM	101	FIN transmit failed
SM	102	RST transmit failed
SM	103	Data transmit failed
SM	104	SYN failed
SM	105	SYN+ACK failed
SM	106	Probe failed
SM	120	ACK past FIN
SM	121	ACK past sent data (%u)
SM	122	Maximum retransmits reached
SM	123	Non-SYN packet (%s%s%s%s%s%s)
SM	124	Connection reset in %s (%c:%u:%u)
SM	125	Invalid sequence in embedded header (%u)
SM	126	RST out-of-order
SM	150	Connection aborted (%c:%u:%u)
TPDAEMON	202	No Keep Alive message received from any HA port
TPDAEMON	203	HA%d port is down because it is missing the keep alive message
TPDAEMON	205	The active HA port is changing from HA%d to HA%d
VRRP	511	VR %d being enabled
VRRP	512	VR %d being disabled
VRRP	513	MIA is not responding
VRRP	514	VRRP router restart grace period expired
VRRP	515	RCE Lost HeartBeat
VRRP	516	RCE HeartBeat Received
VRRP	517	RCE Link Down on port %d
VRRP	518	MIA is responding again
VRRP	519	VR %d starts in master state
VRRP	520	VR %d shuts down to initialize state
VRRP	521	VR %d pauses to backup state
VRRP	522	VR %d becomes master because of resume event
VRRP	523	VR %d changes to backup

## Event Log Message Catalog

Log Module	Log Message ID	Message
VRRP	524	VR %d becomes master because old master died.
VRRP	525	VR %d becomes master
CLAM	901	internal error
CLAM	902	unable to allocate memory
CLAM	903	unable to open temporary file %d
CLAM	904	unable to read temporary file %d
CLAM	905	cannot start scand
SMTP	901	internal error
SMTP	902	unable to allocate memory
SMTP	903	unable to open temporary file %d
SMTP	904	unable to read temporary file %d
SMTP	905	unable to write to temporary file %d
SMTP	248	unable contact AV helper '%s'
SMTP	206	ruleset '%s' lookup failed
HTTP	100	internal error
HTTP	205	unable to init protocol handler
HTTP	232	unable to load proxy action '%s'
WEBBLOCKER	100	internal error
WEBBLOCKER	700	Restarting worker, too many invalid internal events
WEBBLOCKER	1000	server=[IP address]: [port]/[protocol] down after response timeout
WEBBLOCKER	1001	server=[IP address]: [port]/[protocol] is now active
<b>MISCELLANEOUS</b>		
SHELL	1000	wglog for shell scripts %s
SHELL	2023	<user> deleted <filename> system log file
SHELL	2024	<user> deleted <filename> support log file
SHELL	3001	%s %s signature update completed
SHELL	3002	%s %s signature update failed: %s
SHELL	5001	%s - system upgrade success
SHELL	5002	%s - system upgrade failure
KERNEL	1001	%s
INIT	1031	%s
INIT	1032	%s
PSTACK	2002	Process <process name> crashed (pid=%s)
PSTACK	2022	#%s %s -<pstack crash detail lines>

## **Firebox Log File XML DTD and Schema**

---

XML Document Type Definition (DTD) and schemas define and order the elements and attributes used in an XML document. We provide a DTD and a schema for the Firebox XML log file in the FAQ section of [www.watchguard.com/support](http://www.watchguard.com/support). The information can help you use the data in the log file with third-party reporting or analysis tools.

## Firebox® X Edge Log Messages

The Firebox® X Edge sends log messages to an internal event log stored in RAM. You can also send these messages to a remote log host, such as a WatchGuard Log Server or a syslog server.

Each log message contains the name of the module that generated the message, a timestamp, and the message text. When shown through the embedded web site event log page, the module name field is color coded to indicate the message type. The log messages below are shown in alphabetical order by module type.

Module	Message Type	Message Text	Description
Content Security	Error	Illegal value ([number]) for source port in FTP command. Possible FTP Bounce Attack	An FTP PORT command was sent with an illegal port value. It cannot be less than 1024.
Content Security	Error	Illegal value ([ip address]) for source address in FTP command. Possible FTP Bounce Attack	An FTP PORT command was sent with an IP address that is different from the source IP address. This could indicate an FTP bounce attack.
Content Security	Error	Unexpected FTP Data Channel from [ip address]:[number] to [ip address]:[number]. Possible FTP Attack	There was an attempt to open an unrequested FTP data channel. This could indicate an attempt to breach the firewall.
Day Time	Information	Synchronized Time [string] @ [string]	The system time was synchronized with the specified time source.
Day Time	Information	Synchronized Time [string] @ [number]ms since boot	The system time was synchronized with the specified time source (previous time in milliseconds since boot).
Day Time	Error	Timeout opening connection to time server	The time client was unable to contact the configured server.
Day Time	Warning	No reply from NTP server [string]	The NTP client did not receive a reply from the specified server.
DHCP	Warning	DHCP request discarded, server is disabled	The DHCP server discarded a request because it is disabled.
DHCP	Warning	Renewal Time-out	The DHCP client reached the renewing time-out.
DHCP	Information	Rebinding Time-out	The DHCP client reached the rebinding time-out.
DHCP	Warning	No reply	The DHCP client did not receive a response from the DHCP server.
DHCP	Error	Incorrect response received [string]	The DHCP client received an incorrect response from the DHCP server.
DHCP	Error	Write Error [number]	The DHCP client received an error when sending a request.
DHCP	Error	Open Error [number]	The DHCP client received an error when opening a connection to the server.
DHCP	Error	DHCP response is too short	The DHCP client received a response from the DHCP server that was too short.

Module	Message Type	Message Text	Description
DHCP	Error	DHCP response has incorrect id	The DHCP client received a response intended for another DHCP client.
DHCP	Error	DHCP response has incorrect opcode	The DHCP client received a response with an invalid opcode.
DHCP	Error	DHCP response has incorrect client hardware address	The DHCP client received a response with an incorrect hardware address.
DHCP	Information	Use Default Renewal Time [number]	The DHCP client did not receive a renewal value from the server. A default value will be used.
DHCP	Information	Renewal Time [number]	The DHCP client received the specified renewal time from the server..
DHCP	Information	Use Default Rebind Time [number]	The DHCP client did not receive a rebind value from the server. A default value will be used
DHCP	Information	Rebind Time [number]	The DHCP client received the specified renewal time from the server.
DHCP	Information	Lease Time [number]	The DHCP client received the specified lease time from the server.
DHCP	Error	NO SERVER ID	The DHCP client received an invalid response from the DHCP server.
DHCP	Error	DHCP NAK RECEIVED	The DHCP client received a NAK response from the DHCP server. The client will restart.
DHCP	Information	INIT_BOOT	The DHCP client entered the INIT-BOOT state.
DHCP	Information	SELECTING	The DHCP client entered the SELECTING state.
DHCP	Information	REQUESTING	The DHCP client entered the REQUESTING state.
DHCP	Information	REBINDING	The DHCP client entered the REBINDING state.
DHCP	Information	REBIND WAIT	The DHCP client entered the REBIND-WAIT state.
DHCP	Information	BOUND	The DHCP client received an IP address from the DHCP server.
DHCP	Information	RENEWING	The DHCP client reached the renewing timeout and will attempt to renew the current configuration.
DHCP	Information	RENEWING WAIT	The DHCP client entered the RENEW-WAIT state.
DHCP	Error	UNKNOWN	The DHCP client entered an unknown state. This is an internal error.
DHCP	Information	CLIENT STATE CHANGE [string]	The DHCP client changed to a new state.

Module	Message Type	Message Text	Description
DHCP	Information	DHCP server on [string] configured for [number] addresses	This message displays the size of the DHCP address pool for the specified network.
DHCP	Error	Config prop "[string]" has illegal format	The configuration of a reserved DHCP address is not in the proper format and was skipped.
DHCP	Error	Request received from [string] - DHCP server has no addresses available	The DHCP server received a request but had no addresses available. The request was ignored.
DHCP	Information	DHCP client disabled	The DHCP server was disabled.
DHCP	Error	DHCP relay enabled but no host specified - request processed locally	The DHCP server was configured to relay requests, but the address of the relay host was not specified.
DHCP	Error	Unable to open connection to relay host - request processed locally	The DHCP server cannot establish a connection to the DHCP relay host.
DHCP	Warning	DHCP max hop count exceeded - request discarded	The DHCP server received a request but cannot send it to the relay host because the maximum number of hops was exceeded.
DHCP	Error	DHCP relay reply received with unknown gateway address - reply discarded	The DHCP server could not determine which interface to which to send a reply. The request was discarded.
DHCP	Error	DHCP request with unknown message type - request discarded	The DHCP server received an unknown request from a client.
DHCP	Error	DHCP Lease Expired	The DHCP client reached the Lease timeout and must restart negotiations for a new address.
DHCP	Error	No reply from DHCP relay server, will process locally	The DHCP client did not receive a reply from the configured DHCP relay server.
DYNDNS	Error	HTTP error [number] received from DYNDNS server	The HTTP response from the Dynamic DNS server was not valid and was ignored.
DYNDNS		Sending request to dyndns server: [string]	This message shows the request sent to the Dynamic DNS server for diagnostic purposes
DYNDNS	Error	DYNDNS server returned an error ({string})	The specified error was received from the Dynamic DNS server.
DYNDNS	Error	DYNDNS client missing required config prop	The Dynamic DNS configuration is missing a username, password or a domain name.
DYNDNS	Error	Unable to contact DYNDNS server at [string]	Could not establish a connection to members.dyndns.org.
DYNDNS	Error	No reply from dyndns server	A request was sent to the Dynamic DNS server but no reply was received.
DYNDNS		DynamicDNS address updated ({string})	The updated address information was accepted by the Dynamic DNS server.

Module	Message Type	Message Text	Description
DYNDNS	Error	Not allowed to register a private address with dyndns ([ip address])	The Dynamic DNS service cannot register a private IP address.
DYNDNS	Information	Will update dyndns server in [number] days	This message indicates the number of days until the address stored by dynamic DNS must be updated.
DYNDNS	Information	Configuration has not changed, not updating dyndns	The external IP address was not modified since the last update of the dynamic DNS service, so an update will not occur.
FTP Server	Information	Denied access attempt to FTP server from [ip address]: invalid username or password	A connection to the FTP server from the trusted network was denied because access was disabled in the configuration file.
HTTP Server	Warning	BASIC authentication used when Digest was enabled.	The browser chose to use Basic instead of the more secure Digest authentication method.
IP	Warning	Discard	An IP packet was discarded for the specified reason.
IP	Warning	Fragment reassembly failed	Not all fragments of an IP packet were received and the packet was discarded.
IP	Information	[string] from [ip address] port [number] to [ip address] port [number] [string]	This is part of the string used for logging packet.
IP	Information	[string] from [ip address] to [ip address] protocol [number] [string]	This is part of the string used for logging packet.
IP	Information	Discard from [ip address] to [ip address] ICMP type ([number]) code ([number])	This is part of the log discarded packet message.
IP	Error	Packet from [ip address] discarded - unknown network on trusted	An IP packet was received on the trusted network, but the source address is not reachable on the trusted network. The packet will be discarded.
IP	Warning	Allowed from [ip address] port [number] to [ip address] port [number] [string] ([string])	A connection has been established from the external interface using the specified port forward rule.
IP	Information	ICMP type ([number]) code ([number]) received from [ip address]	An ICMP packet was received on the external interface.
IP	Information	Allowed	Part of the message generated when a packet is allowed to external and log all outgoing packets is enabled.
IP	Error	Routing table full, route not added	The routing table does not have enough room for the new route.
IP	Warning	IP header contains options - discard	Any IP packet with options specified in the header is discarded for security reasons.
IP	Warning	incorrect state	A packet for a port forward was discarded, because the connection was not fully established.

<b>Module</b>	<b>Message Type</b>	<b>Message Text</b>	<b>Description</b>
IP	Error	Bad IP address	A packet was discarded because the IP address in the header was not valid.
IP	Error	Error in filter	Because an internal error occurred in the packet filter, the disposition of the rule is not understood.
IP	Error	Error in SIP	An internal error occurred in the packet filter engine.
IP	Warning	SIP discarded	The packet was discarded at the request of the Application Level Gateway (ALG module).
IP	Warning	Port not available	The packet was discarded because it was addressed to a port that was not listening for connections.
IP	Warning	External not up	The packet was discarded because the public network is not up yet.
IP	Warning	Blocked Sites	The packet was discarded because the source IP address is on the blocked sites list.
IP	Warning	Maximum number of inbound sessions	The packet was discarded because the maximum number of forwarded connections was reached.
IP	Error	Spoofed source IP address	The source IP address does not route to the interface on which the packet was received (spoofed address).
IP	Error	Illegal IP packet - possible Land attack	The source and destination IP address are identical, which indicates a LAND attack.
IP	Error	Sequence number not within expected range, possible attack	The sequence number in the TCP connection was not in the expected range. This could indicate an attempt to interrupt an active TCP session.
IP	Error	Attempt to send TCP packet on an unopen port	The flags field in the TCP header was not valid. This could indicate an attempt to crash the firewall.
IP	Error	Error allocating port for NAT	There was an error during the Network Address Translation (NAT) process.
IP	Warning	Incorrect length in IP header	The length in the IP header was not correct and the packet was discarded.
IP	Warning	Non-version 4 IP packet	Only IP version 4 is supported. A packet with a different version was received and discarded.
IP	Error	Incorrect checksum in IP header	The IP header checksum was not correct. The packet may have been corrupted in transit.
IPSec	Information	IPSEC tunnel is active	Traffic was sent and received over an IPSEC tunnel.
IPSec	Information	IPSEC tunnel is active, but no data has been received	IKE negotiation is complete for a tunnel, traffic was sent, but no data was received.

Module	Message Type	Message Text	Description
IPSec	Information	IPSEC tunnel is not active	IKE negotiation is complete for a tunnel, but no traffic was sent or received.
LSS	Error	Unknown error [number]	The FTP client received an unknown error when retrieving a software update.
LSS	Error	Bad response from server	The FTP client received an unexpected response when retrieving a software update.
LSS	Error	Access denied by update server	The FTP client was denied access to the software update server.
LSS	Error	Unable to establish connection to update server	The FTP client was unable to contact the software update server.
LSS	Error	Error waiting for data channel to open	The FTP client was unable to receive files from the software update server.
LSS	Error	Network error [[number]] while downloading [string]	The FTP client encountered an error downloading files from the software update server.
LSS	Error	File verify failed on [string]	The files received from the software update server are corrupted.
MODEM	Information	Modem Connected: [string]	Displays the dial string sent to the modem and the connection response for diagnostic purposes.
MODEM	Error	Modem disconnected	The modem connection was terminated due to a dialing error.
MODEM	Error	Modem disconnected, no activity	The modem connection was terminated due to idle timeout.
MODEM	Error	Modem connection error	The modem disconnected because of a carrier loss. This could be noise on the telephone line or the other side terminated the call.
MODEM	Error	Modem initialization error	The modem rejected one of the commands in the initialization string.
MODEM	Error	Modem connection error: No carrier	The modem disconnected because of a NO CARRIER response. Check the phone number and connection.
MODEM	Error	Modem connection error: No dialtone	The modem disconnected because no dialtone was detected. Check the phone connection.
MODEM	Error	Modem connection error: Modem is busy	The modem could not connect because the telephone number is busy.
MONITOR	Information	The event log has been cleared	The event log has been cleared by an administrator.
MONITOR	Information	Start of Log	This is always the first message put into the log.
MONITOR	Information	IPSEC VPN is not installed	The IPSEC feature is not installed.

<b>Module</b>	<b>Message Type</b>	<b>Message Text</b>	<b>Description</b>
MONITOR	Error	Critical task failed to start	A thread failed to start due to an internal error. The Firebox is restarting.
MONITOR	Error	Critical task [string] unexpectedly terminated - device will reboot shortly	A thread has unexpectedly terminated. The Firebox is restarting.
MONITOR	Error	Out of Network Buffers	The network buffer pool is empty, the Firebox is restarting.
MONITOR	Warning	System memory pool is getting low	The amount of free memory is low, some functions may not operate properly.
MONITOR	Error	System memory pool exhausted	The system is out of memory, the Firebox is restarting.
MONITOR	Error	Timeout opening connection to log server	The secure logging client was unable to connect to the server.
MONITOR	Error	Error [[number]] opening connection to log server	The secure logging client had an error while connecting to the server.
MONITOR	Error	Error opening remote log ([string])	The secure logging client was denied access to the server. Check the server address and passphrase.
MONITOR	Information	Remote logging connection open to [ip address]	The secure logging client established a connection to the server.
MONITOR	Error	Remote log closed due to [string]	The secure logging client connection terminated.
MONITOR	Error	Error creating event log queue	The secure logging encountered an internal error during initialization.
MONITOR	Error	Too many consecutive alloc failures	The network buffer pool is empty. The Firebox is restarting.
MONITOR	Information	NrelbufR id	A network buffer is corrupted due to an internal error. The Firebox is restarting.
MONITOR	Information	Out of free space on fragment list	A fragmented IP packet was discarded because there was no space available to accept a new one.
MONITOR	Information	Fragment too large (max is [number] bytes) from [ip address]	A fragmented IP packet was discarded because the total size of the packet was too large.
MONITOR	Error	msgQReceive error [number]	The secure logging client had an internal error and will restart.
MONITOR	Error	sendLogKeepAlive returned error [number]	The secure logging client failed to receive a keep alive response from the server. The client will restart.
MONITOR	Error	sendLogData returned error [number]	The secure logging client had an error sending data to the server. The client will restart.
MONITOR	Error	Error [[number]] issuing log message to syslog host [ip address]	The syslog client was unable to open a connection the specified server.

<b>Module</b>	<b>Message Type</b>	<b>Message Text</b>	<b>Description</b>
MONITOR	Information	Syslog enabled to host at [ip address]	The syslog client established a connection to the server.
MONITOR	Information	Syslog for host at [ip address] disabled due to [string]	The syslog client terminated the connection to the server due to an error or it was disabled.
MONITOR	Error	Error creating event log queue for syslog	An internal error occurred during the initialization of the syslog client. Syslog logging is disabled.
MONITOR	Error	Error [[number]] processing event log queue for syslog	An internal error occurred in the syslog client. The connection will restart.
MONITOR	Information	Settings update	The syslog configuration changed - the client will restart.
MONITOR	Error	SOCKS Proxy Disabled	The socks 5 proxy module terminated due to configuration change.
MONITOR	Information	Config file updated	Any time the configuration file is updated this message is generated.
MONITOR	Warning	Remote Configuration Denied from [ip address]: invalid username or password	A connection was attempted to VPN Manager Access port (FBSH and was rejected due to an invalid passphrase.
MONITOR	Information	Remote Configuration Allowed from [ip address]	A connection was established to the VPN Manager Access port.
MONITOR	Information	Administrator access allowed from [ip address]	Access has been granted to the configuration page.
MONITOR	Information	With WSEP host at [ip address]	The time has been synchronized with the secure logging server.
MONITOR	Information	With browser (local time)	The time was synchronized with the browser.
MONITOR	Information	With user specified time	The time was set manually.
MONITOR	Error	Serial number is not valid	The serial number installed in the flash for this Firebox is not valid.
MONITOR	Error	Connection was unexpectedly terminated	The secure logging client connection to the server was terminated due to an error.
MONITOR	Warning	Switching external interface to [string]	This message indicates that the external connection failed over to a new interface.
MONITOR	Error	Critical task [string] suspended - device will reboot shortly	A thread unexpectedly stopped running. The Firebox will restart.
MONITOR	Error	Unable to save config file - wg_savebuf failed	An internal error occurred when trying to save the config file ( wg_savebuf failed .
MONITOR	Error	Unable to save config file - error opening /ram device	An internal error occurred when trying to access the RAM disk.
MONITOR	Warning	RAM disk low on space purging all temporary files	The RAM disk is running out of space. This could be caused by having debug logging enabled. The temporary log files will be removed if necessary.

<b>Module</b>	<b>Message Type</b>	<b>Message Text</b>	<b>Description</b>
MONITOR	Error	Unable to save config file - insufficient space on device	There is not enough space on the RAM drive to store the configuration file.
MONITOR	Error	Unable to store license file	An internal error occurred while storing the license key.
MONITOR	Error	[string] is disconnected from the network.	The specified port is no longer connected to the network.
MONITOR	Information	[string] is connected to the network at [number] Mbps [string] duplex.	The specified port is now connected to the network at the specified speed.
MONITOR	Error	No license has been installed so only 1 IP address is allowed to access the external network. Contact WatchGuard support to obtain a license for this device.	No license has been installed so only 1 IP address is allowed to access the external network. Contact WatchGuard support to obtain a license for this device.
MONITOR	Error	The license for the [string] feature has expired and has been disabled	The license for the specified feature has expired.
MONITOR	Error	No firmware updates are allowed because the LiveSecurity subscription has expired.	No firmware updates are allowed once the LiveSecurity subscription has expired.
NAT	Error	Translation pool exhausted	The maximum number of active connections through the firewall is at its limit.
NAT	Error	User count exceeded, packet dropped	The maximum number of users allowed through the firewall is at its limit.
NAT	Error	IPSEC packet with zero SPI discarded	An ESP IPSEC packet was discarded because of an illegal SPI value (zero).
NAT	Error	Discard IPSEC packet to [ip address] - still waiting for response for [ip address]	An IPSEC packet was discarded because another client is currently establishing a connection.
NAT	Information	IPSEC NAT timeout: gateway [ip address] client [ip address]	An established IPSEC connection ended because it timed out.
NAT	Information	IPSEC NAT IKE timeout: client [ip address]	A established NAT-d IPSEC connection timed out and was terminated.
NAT	Warning	Default	The packet was discarded because it did not match any of the existing NAT connections.
NAT	Warning	Session terminated by administrator for host [ip address]	An administrator terminated all NAT sessions via the GUI.
NAT	Warning	Session terminated by periodic automatic time-out for host [ip address]	All NAT sessions were terminated because the configured time was reached.
PPP	Error	PPP negotiation failed during LCP	PPP negotiation failed in the initial state (LCP).
PPP	Error	Authentication failure, verify username and password	The supplied username and password were rejected by the remote site.
PPP	Error	PPP server rejected static IP in IPCP negotiation	PPP server rejected static IP in IPCP negotiation.

Module	Message Type	Message Text	Description
PPP	Error	PPP IP configuration error	PPP negotiation failed in the IPCP state.
PPP	Information	Login Successful	The PPP connection was established.
PPP	Information	Negotiating IP settings	The PPP client is starting the IPCP phase.
PPP	Information	CHAP Authentication	The PPP client is starting CHAP authentication.
PPP	Information	PAP Authentication	The PPP client is starting PAP authentication.
PPP	Information	Starting login	The PPP client is starting the LCP phase.
PPP	Error	PPPOE started by packet	The packet was discarded because it was not for our current PPPOE session.
PPP	Error	Cannot start PPPOE until ppp configuration is updated	A new PPP connection cannot be established because the username and password were previously rejected by the server and were not updated.
PPPoE	Error	Unable to locate PPPoE server	A PADI request was sent to the PPPOE server, but received no reply.
PPPoE	Error	Timeout communicating with PPPoE server	A PADR request was sent to the PPPOE server, but received no reply.
PPPoE	Information	PPPoE service established	A PPPOE Session has been established.
PPPoE	Warning	Timeout locating PPPoE server, will retry	No reply was received by the PPPOE client. The request is being sent again.
PPPoE	Warning	Incorrect session number in PPPoE packet	A PPPOE packet was received for a different PPPOE client session .
PPPoE	Warning	PPPoE session terminated by remote	The PPPOE server terminated the current session.
PPPoE	Warning	PPPoE connection terminated, no activity	The PPPOE connection was idle for the configured limit and will be terminated.
PPPoE	Warning	PPPoE connection terminated, service unavailable	An LCP ECHO request was sent to the server but no reply was received. Restarting the link.
PPPoE	Warning	PPPOE response received with incorrect AC or ServiceName	A PADO packet from the server was ignored because of the service name did not match our name.
SMTP	Error	Unable to create message queue	There was an error adding a new message to the SMTP logging queue.
SMTP	Error	Unable to allocate memory for mail message	There was an error allocating memory for SMTP logging.
SMTP	Error	Missing required config props for SMTP	The SMTP logging client is missing required configuration information.
SMTP	Error	Unable to connect to SMTP host (error [number])	The SMTP logging client cannot establish a connection to the specified server.
SMTP	Error	Error reading from SMTP server (error [number])	The SMTP logging client had an error communicating with the specified server.

Module	Message Type	Message Text	Description
SMTP	Error	Error writing to SMTP server (error [number])	An error occurred when the SMTP logging client sent the logs to the specified server.
SMTP	Error	SMTP server returned error ([number]) when connection established	The SMTP logging client did not understand the initial response from the server.
SMTP	Error	Sent HALO - server returned error ([number])	The SMTP logging client did not understand the response to the HELO command.
SMTP	Error	Sent MAIL From - server returned error ([number])	An error occurred when the SMTP logging client sent the mail message to the server.
SMTP	Error	Server did not like recipient - returned error ([number])	The SMTP server rejected the configured destination address.
SMTP	Error	Server returned error when sending data - returned error ([number])	An error occurred when the SMTP logging client sent the mail message body to the server.
TCP	Warning	Port not available [number]	No connection was available for an incoming TCP connection.
USERS	Warning	User not authorized	The specified user tried to perform an illegal action.
USERS	Warning	Unknown user	Traffic was discarded because no user logged in with the sending IP address.
USERS	Information	User [string] logged out from [IP address]	The specified user logged out.
USERS	Information	Session terminated by administrator for user [string] at host [IP address]	The administrator terminated the user session.
USERS	Warning	Session terminated for user [string] at host [IP address], idle time-out occurred	The specified user's session was terminated because of inactivity.
USERS	Warning	Session terminated for user [string] at host [IP address], maximum access time exceeded	The specified user session was terminated because it reached the configured maximum session time.
USERS	Warning	Session terminated for user [string] at host [IP address] periodic automatic time-out occurred	The configured time to log out all users was reached, so all active sessions were terminated.
USERS	Warning	User [string] authentication failed from [IP address]	An attempt to login failed due to an invalid username or password.
USERS	Warning	User [string] authentication failed from [IP address] via HTTPS	An attempt to login via HTTPS failed due to an invalid username or password.
USERS	Warning	User [string] authentication failed from [IP address] via HTTP	An attempt to login via HTTP failed due to an invalid username or password.
USERS		User [string] authentication failed from [IP address] via MUVPN	An attempt to login via MUVPN failed due to an invalid username or password.
USERS	Warning	User [string] authentication failed from [IP address] via wireless 802.1x	An attempt to login via 802.1x failed due to an invalid username or password.

Module	Message Type	Message Text	Description
USERS	Warning	User [string] authentication failed from [ip address] via FTP	An attempt to login via FTP failed due to invalid username or password.
USERS	Information	User [string] authenticated from [ip address]	The specified user successfully logged in.
USERS	Information	User [string] authenticated from [ip address] via HTTPS	The specified user has logged in successfully via HTTPS.
USERS	Information	User [string] authenticated from [ip address] via HTTP	The specified user successfully logged in via HTTP.
USERS	Information	User [string] authenticated from [ip address] via MUVPN	The specified user successfully logged in via MUVPN.
USERS	Information	User [string] authenticated from [ip address] via wireless 802.1x	The specified user successfully logged in via 802.1x.
USERS	Information	User [string] authenticated from [ip address] via FTP	The specified user successfully logged in via FTP.
USERS	Error	User [string] could not be authenticated, the LDAP server at [string] is unavailable	An attempt to login by an LDAP user failed because the LDAP server could be found.
USERS	Error	User [string] could not be authenticated, the request to the LDAP server at [string] timed out	An attempt to login by an LDAP user failed because the LDAP server did not respond within the configured time-out.
WebBlocker	Information	Full access granted to [ip address] for [number] minutes	A user supplied the override password and has unrestricted web access.
WebBlocker	Warning	Full access attempt by [ip address] was denied: invalid password	A user supplied an incorrect WebBlocker override password.
WebBlocker	Warning	Access to unacceptable web site at [ip address] denied to [ip address] [string] [string]	Access to the specified site was denied by WebBlocker because of the content type.
WebBlocker	Warning	Access to unacceptable web site [string] denied to [ip address] [string] [string]	Access to the specified site was denied by WebBlocker because of the content type.
WebBlocker	Error	Reply from wrong server [ip address], expected [ip address]	A WebBlocker response was received from an unexpected address and discarded.
WebBlocker	Error	No reply from WebBlocker server at [ip address]	The WebBlocker server failed to respond to a request. Check your DNS settings and the route to swb.watchguard.com.
Wireless	Error	Wireless hardware not detected	The wireless networking feature is enabled, but the required hardware was not detected.
Wireless	Information	Wireless access granted to mac address [hex]:[hex]:[hex]:[hex]:[hex]:[hex]	This message occurs when a wireless client has associated with the AP and has successfully sent data.
Wireless	Warning	Wireless access attempted from mac address [hex]:[hex]:[hex]:[hex]:[hex]:[hex]	This message occurs each time a wireless device associates with the access point.

---

**Firebox® X Edge Log Messages**

<b>Module</b>	<b>Message Type</b>	<b>Message Text</b>	<b>Description</b>
Wireless	Error	Attempted wireless access for unauthorized mac address [hex]:[hex]:[hex]:[hex]:[hex]	This message occurs when a device attempts to associate with the access point, but the MAC address is not in the list of allowed addresses.
Wireless	Error	Require MUVPN on Wireless Enabled	This message occurs when only MUVPN connections are allowed on the wireless network, and some other type of traffic is received.

---

WatchGuard® WebBlocker, together with the HTTP proxy, supplies Web filtering for the content of the Web pages your users open in their browsers. WebBlocker uses a URL database created and controlled by SurfControl.

## Searching for Blocked Sites

---

To see if WebBlocker is blocking a Web site as part of a category block, go to the Filter Testing and Submissions form on the SurfControl Web site.

- 1 Open a Web browser and go to:  
<http://mtas.surfcontrol.com/mtas/MTAS.asp>
- 2 Type the URL or IP address of the site to check.
- 3 Click **Test Site**.

The search engine tells you if the site is on the SurfControl list. You can also request that the URL be added to the SurfControl list.

## WebBlocker Categories

---

The WebBlocker database contains nine groups of categories with 40 individual categories. A Web site is added to a category when the contents of the Web site meet the correct criteria. Web sites that give opinion or educational material about the subject matter of the category are not included. For example, the drugs/drug culture category denies sites that tell how to use marijuana. They do not deny sites with information about the historical use of marijuana.

<b>Category</b>	<b>Description of Content</b>
Adult/Sexually Explicit	<ul style="list-style-type: none"> <li>• Sexually oriented or erotic full or partial nudity</li> <li>• Depictions or images of sexual acts, including inanimate objects used in a sexual manner</li> <li>• Erotic stories and textual descriptions of sex acts</li> <li>• Sexually exploitive or sexually violent text or graphic</li> <li>• Bondage, fetishes, genital piercing</li> <li>• Adult products including sex toys, CD-ROMs, and videos</li> <li>• Adult services including videoconferencing, escort services, and strip clubs</li> <li>• Explicit cartoons and animation</li> <li>• Child pornography/pedophilia</li> <li>• Online groups, including newsgroups and forums that are sexually explicit in nature</li> <li>• Naturist sites that feature nudity</li> <li>• Erotic or fetish photography which depicts nudity</li> </ul>
Advertise-ments	<ul style="list-style-type: none"> <li>• Banner Ad servers</li> <li>• Pop-up advertisements</li> <li>• Adware</li> </ul>
Arts & Entertainment	<ul style="list-style-type: none"> <li>• Television, movies, music, and video programming guides</li> <li>• Comics, jokes, movie, video, or sound clips</li> <li>• Performing arts (theatre, vaudeville, opera, symphonies, etc.)</li> <li>• Online magazines and reviews on the entertainment industry</li> <li>• Dance companies, studios, and training</li> <li>• Broadcasting firms and technologies (satellite, cable, etc.)</li> <li>• Book reviews and promotions, variety magazines, and poetry</li> <li>• Jokes, comics, comic books, comedians, or any site designed to be funny or satirical</li> <li>• Online museums, galleries, artist sites (including sculpture, photography, etc.)</li> <li>• Celebrity fan sites</li> <li>• Horoscopes</li> <li>• Online greeting cards</li> <li>• Amusement/theme parks</li> </ul>
Chat	<ul style="list-style-type: none"> <li>• Web-based chat</li> <li>• Instant Message servers</li> </ul>
Computing and Internet	<ul style="list-style-type: none"> <li>• Reviews, information, computer buyer's guides, computer parts and accessories, and software</li> <li>• Computer/software/Internet companies, industry news, and magazines</li> <li>• Pay-to-surf sites</li> <li>• Downloadable (non-streaming) movie, video, or sound clips</li> <li>• Downloadable mobile phone/PDA software, including themes, graphics, and ringtones</li> <li>• Freeware and shareware sites</li> <li>• Personal storage and backup</li> <li>• Clip art, fonts, and animated GIF pages</li> </ul> <p>Note: Does not include update sites for operating systems, anti-virus agents, or other business-critical programs.</p>
Criminal Skills	<ul style="list-style-type: none"> <li>• Advocating, instructing, or giving advice on performing illegal acts</li> <li>• Tips on evading law enforcement</li> <li>• Lock-picking and burglary techniques</li> <li>• Phishing</li> <li>• Phone service theft advice</li> <li>• Plagiarism and cheating, including the sale of research papers</li> </ul>

Category	Description of Content
Drugs, Alcohol, & Tobacco	<ul style="list-style-type: none"> <li>• Recipes, instructions, or kits for manufacturing or growing illicit substances, including alcohol, for purposes other than industrial usage</li> <li>• Glamorizing, encouraging, or instructing in the use of or masking the use of alcohol, tobacco, illegal drugs, and other substances that are illegal to minors</li> <li>• Alcohol and tobacco promotional Web sites</li> <li>• Information on “legal highs”: glue sniffing, misuse of prescription drugs, and abuse of other legal substances</li> <li>• Distributing alcohol, illegal drugs, or tobacco free or for a charge</li> <li>• Displaying, selling, or detailing the use of drug paraphernalia</li> </ul> <p>Note: SurfControl does not include sites that discuss medicinal drug use, industrial hemp use, or public debate on the issue of legalizing certain drugs. SurfControl also does not include sites sponsored by a public or private agency that provide educational information on drug use.</p>
Education	<ul style="list-style-type: none"> <li>• Educational institutions, including pre-, elementary, secondary, and high schools; universities</li> <li>• Educational sites: pre-, elementary, secondary, and high schools; universities</li> <li>• Distance education, trade schools, and online courses</li> <li>• Online teacher resources (lesson plans, etc.)</li> </ul>
Finance & Investment	<ul style="list-style-type: none"> <li>• Stock quotes, stock tickers, and fund rates</li> <li>• Online stock or equity trading</li> <li>• Online banking and bill-pay services</li> <li>• Investing advice or contacts for trading securities</li> <li>• Money management/investment services or firms</li> <li>• General finances and companies that advise thereof</li> <li>• Accountants, actuaries, banks, mortgages, and general insurance companies</li> </ul>
Food & Drink	<ul style="list-style-type: none"> <li>• Recipes, cooking instruction and tips, food products, and wine advisors</li> <li>• Restaurants, cafes, eateries, pubs, and bars</li> <li>• Food/drink magazines and reviews</li> </ul>
Gambling	<ul style="list-style-type: none"> <li>• Online gambling or lottery Web sites that invite the use of real money</li> <li>• Information or advice for placing wagers, participating in lotteries, gambling real money, or running numbers</li> <li>• Virtual casinos and offshore gambling ventures</li> <li>• Sports picks and betting pools</li> <li>• Virtual sports and fantasy leagues that offer large rewards or request significant wagers</li> </ul> <p>Note: Casino/hotel/resort sites that do not feature online gambling or provide gaming tips are categorized under Travel.</p>
Games	<ul style="list-style-type: none"> <li>• Game playing or downloading; game hosting or contest hosting</li> <li>• Tips and advice on games or obtaining cheat codes (“cheatz”)</li> <li>• Journals and magazines dedicated to online game playing</li> </ul>
Glamour & Intimate Apparel	<ul style="list-style-type: none"> <li>• Lingerie, negligee or swimwear modeling</li> <li>• Model fan pages; fitness models/sports celebrities</li> <li>• Fashion or glamour magazines online</li> <li>• Beauty and cosmetics</li> <li>• Modeling information and agencies</li> </ul>
Government & Politics	<ul style="list-style-type: none"> <li>• Government services such as taxation, armed forces, customs bureaus, and emergency services</li> <li>• Local government sites</li> <li>• Political debate, canvassing, election information, and results</li> <li>• Local, national, and international political sites</li> <li>• Conspiracy theorist and alternative government views that are not hate-based</li> </ul>

Category	Description of Content
Hacking	<ul style="list-style-type: none"> <li>• Promotion, instruction, or advice on the questionable or illegal use of equipment and/or software for purpose of hacking passwords, creating viruses, or gaining access to other computers and/or computerized communication systems</li> <li>• Sites that provide instruction or work-arounds for filtering software</li> <li>• Cracked software and information sites; "warez"</li> <li>• Pirated software and multimedia download sites</li> <li>• Computer crime</li> <li>• Sites that provide or promote information gathering or tracking that is unknown to, or without the explicit consent of, an end user or organization</li> <li>• Sites that distribute malicious executables or viruses</li> <li>• 3rd-party monitoring and other unsolicited commercial software</li> </ul>
Hate Speech	<ul style="list-style-type: none"> <li>• Advocating or inciting degradation of or attacks on specified populations or institutions based on associations such as religion, race, nationality, gender, age, disability, or sexual orientation</li> <li>• Promoting a political or social agenda that is supremacist in nature or exclusionary of others based on their race, religion, nationality, gender, age, disability, or sexual orientation</li> <li>• Holocaust revisionist/denial sites</li> <li>• Coercion or recruitment for membership in a gang* or cult**</li> <li>• Militancy, extremist</li> <li>• Flagrantly insensitive or offensive material, including lack of recognition or respect for opposing opinions or beliefs</li> </ul> <p>Note: SurfControl does not include news, historical, or press incidents that may include the above criteria in this category (except in graphic examples).</p> <p>*A gang is defined as: a group whose primary activities are the commission of felonious criminal acts, which has a common name or identifying sign or symbol, and whose members individually or collectively engage in criminal activity in the name of the group.</p> <p>**A cult is defined as: a group whose followers have been deceptively and manipulatively recruited and retained through undue influence such that followers' personalities and behavior are altered. Leadership is all-powerful, ideology is totalistic, the will of the individual is subordinate to the group, and the group is outside society.</p>
Health & Medicine	<ul style="list-style-type: none"> <li>• General health such as fitness and well-being</li> <li>• Alternative and complementary therapies, including yoga, chiropractic, and cranio-sacral</li> <li>• Medical information and reference about ailments, conditions, and drugs</li> <li>• Medical procedures, including elective and cosmetic surgery</li> <li>• Hospital, medical insurance</li> <li>• Dentistry, optometry, and other medical-related sites</li> <li>• General psychiatry and mental well-being sites</li> <li>• Promoting self-healing of physical and mental abuses, ailments, and addictions</li> <li>• Psychology, self-help books, and organizations</li> </ul>
Hobbies & Recreation	<ul style="list-style-type: none"> <li>• Recreational pastimes such as collecting, gardening, or kit airplanes</li> <li>• Outdoor recreational activities such as hiking, camping, rock climbing</li> <li>• Tips or trends focused on a specific art, craft, or technique</li> <li>• Online publications on a specific pastime or recreational activity</li> <li>• Online clubs, associations or forums dedicated to a hobby</li> <li>• Traditional (board, card, etc.) games and their enthusiasts</li> <li>• Animal/pet related sites, including breed-special sites, training, shows, and humane societies</li> <li>• Beauty and cosmetics</li> </ul>
Hosting Sites	<ul style="list-style-type: none"> <li>• Web sites that host business and individual Web pages (i.e. GeoCities, earthlink.net, AOL)</li> </ul>

Category	Description of Content
Job Search & Career Development	<ul style="list-style-type: none"> <li>• Employment agencies, contractors, job listings, career information</li> <li>• Career searches, career-networking groups</li> </ul>
Kids' Sites	<ul style="list-style-type: none"> <li>• Child-centered sites and sites published by children</li> </ul>
Lifestyle & Culture	<ul style="list-style-type: none"> <li>• Homelife and family-related topics, including weddings, births, and funerals</li> <li>• Parenting tips and family planning</li> <li>• Gay/lesbian/bisexual (non-pornographic) sites</li> <li>• Foreign cultures, socio-cultural information</li> <li>• Tattoo, piercing parlors (non-explicit)</li> </ul>
Motor Vehicles	<ul style="list-style-type: none"> <li>• Car reviews, vehicle purchasing or sales tips, parts catalogs</li> <li>• Auto trading, photos, discussion of vehicles including motorcycles, boats, cars, trucks, and RVs</li> <li>• Journals and magazines on vehicle modification, repair, and customization</li> <li>• Online automotive enthusiast clubs</li> </ul>
News	<ul style="list-style-type: none"> <li>• Newspapers online</li> <li>• Headline news sites, newswire services, and personalized news services</li> <li>• Weather sites</li> </ul>
Personals & Dating	<ul style="list-style-type: none"> <li>• Singles listings, matchmaking and dating services</li> <li>• Advice for dating or relationships; romance tips and suggestions</li> </ul>
Photo Searches	<ul style="list-style-type: none"> <li>• Sites that provide resources for photo and image searches</li> <li>• Online photo albums/digital photo exchange</li> <li>• Image hosting</li> </ul>
Real Estate	<ul style="list-style-type: none"> <li>• Home, apartment, and land listings</li> <li>• Rental or relocation services</li> <li>• Tips on buying or selling a home</li> <li>• Real estate agents</li> <li>• Home improvement</li> </ul>
Reference	<ul style="list-style-type: none"> <li>• Personal, professional, or educational reference</li> <li>• Online dictionaries, maps, and language translation sites</li> <li>• Census, almanacs, and library catalogs</li> <li>• Topic-specific search engines</li> </ul>
Religion	<ul style="list-style-type: none"> <li>• Churches, synagogues, and other houses of worship</li> <li>• Any faith or religious beliefs, including non-traditional religions such as Wicca and witchcraft</li> </ul>
Remote Proxies	<ul style="list-style-type: none"> <li>• Remote proxies or anonymous surfing</li> <li>• Web-based translation sites that circumvent filtering</li> <li>• Peer-to-peer sharing</li> </ul>
Search Engines	<ul style="list-style-type: none"> <li>• General search engines (Yahoo, AltaVista, Google)</li> </ul>
Sex Education	<ul style="list-style-type: none"> <li>• Pictures or text advocating the proper use of contraceptives, including condom use, the correct way to wear a condom, and how to put a condom in place</li> <li>• Sites related to discussion about the use of birth control pills, IUDs, and other types of contraceptives</li> <li>• Discussion sites on how to talk to your partner about diseases, pregnancy, and respecting boundaries</li> </ul> <p>Note: Not included in this category are commercial sites that sell sexual paraphernalia. These sites are filtered through the Adult category.</p>
Shopping	<ul style="list-style-type: none"> <li>• Department stores, retail stores, company catalogs, and other sites that allow online consumer shopping</li> <li>• Online auctions</li> <li>• Online downloadable product warehouses; specialty items for sale</li> <li>• Freebies or merchandise giveaways</li> </ul>

**WebBlocker Categories**

<b>Category</b>	<b>Description of Content</b>
Sports	<ul style="list-style-type: none"><li>• Team or conference Web sites</li><li>• National, international, college, or professional scores and schedules</li><li>• Sports-related online magazines or newsletters</li><li>• Fantasy sports and virtual sports leagues that are free or low-cost</li></ul>
Streaming Media	<ul style="list-style-type: none"><li>• Streaming media files or events (any live or archived audio or video file)</li><li>• Internet TV and radio</li><li>• Personal (non-explicit) Webcam sites</li><li>• Telephony sites that allow user to make calls via the Internet</li><li>• VoIP services</li></ul>
Travel	<ul style="list-style-type: none"><li>• Airlines and flight booking agencies</li><li>• Accommodation information</li><li>• Travel package listings</li><li>• City guides and tourist information</li><li>• Car rentals</li></ul>
Violence	<ul style="list-style-type: none"><li>• Portraying, describing, or advocating physical assault against humans, animals, or institutions</li><li>• Depictions of torture, mutilation, gore, or horrific death</li><li>• Advocating, encouraging, or depicting self-endangerment or suicide, including the use of eating disorders or addictions</li><li>• Instructions, recipes, or kits for making bombs and other harmful or destructive devices</li><li>• Sites promoting terrorism</li><li>• Excessively violent sports or games (including video and online games)</li><li>• Offensive or violent language, including through jokes, comics, or satire</li><li>• Excessive use of profanity or obscene gesticulation</li></ul> <p>Note: We do not block news, historical, or press incidents that may include the above criteria (except in graphic examples).</p>
Weapons	<ul style="list-style-type: none"><li>• Online purchasing or ordering information, including lists of prices and dealer locations</li><li>• Any page or site predominantly containing, or providing links to, content related to the sale of guns, weapons, ammunition, or poisonous substances</li><li>• Displaying or detailing the use of guns, weapons, ammunition or poisonous substances</li><li>• Clubs which offer training on machine guns, automatic guns, other assault weapons, and/or sniper training</li></ul> <p>Note: Weapons are defined as something (as a club, knife, or gun) used to injure, defeat, or destroy.</p>
Web-based E-mail	<ul style="list-style-type: none"><li>• Web-based e-mail accounts</li><li>• Messaging sites (SMS, etc)</li></ul>
Usenet/Forums	<ul style="list-style-type: none"><li>• Opinion or discussion forums</li><li>• Weblogs (blog) sites</li></ul>

---

There are many resources available to help you learn more about network security. This chapter gives different sources of information frequently used by WatchGuard's development and technical support teams to learn more about network security. The editorial comments included in this chapter are supplied to help you decide which resources would be most helpful to you. These comments are provided by the LiveSecurity editorial team. For more information like this, log in to the LiveSecurity site and look over the LiveSecurity archive at [www.watchguard.com/archive](http://www.watchguard.com/archive).

The types of resources included in this chapter are:

- Publishers
- Non-Fiction Books
- Fiction Books
- White Papers and Requests for Comments
- Mailing Lists
- General Information Technology and Security Web sites
- White Hat Sites
- Gray Hat Sites
- Other useful web sites
- Dictionaries of computer terminology
- RSS feeds

## Publishers

---

Some publishers focus on network security in their works.

*Addison-Wesley & Benjamin Cummings*

Publishes a computing series that includes some titles about networks and network security.

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

---

## Books

### *O'Reilly*

Publishes many books on network security.

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

---

## Books

### Non-Fiction

Zwicky, Elizabeth D. et al; Building Internet Firewalls. Sebastopol: O'Reilly & Associates, 2000. ISBN 1565928717.

Cheswick, et al; Firewalls and Internet Security: Repelling the Wily Hacker. Reading, MA: Addison Wesley Longman, Inc., 2003. ISBN 020163466X.

Garfinkel and Spafford, Simson Garfinkel and Gene Spafford. Practical Unix and Internet Security. Sebastopol: O'Reilly & Associates, 2003. ISBN 0596003234.

McClure, Stewart; Scambray, Joel; and Kurtz, George. Hacking Exposed. Fourth Edition. McGraw-Hill Publishing, 2003. ISBN 0072227427.

Power, Richard. Tangled Web: Tales of Digital Crime from the Shadows of Cyberspace. Que; September 2000. ISBN 078973443x.

Schneier, Bruce. Applied Cryptography. Second Edition. New York: John Wiley & Sons, Inc., 1996. ISBN 0471117099.

Schwartau, Winn. Cybershock: Surviving Hacker, Phreakers, Identity Theives, Internet Terrorists and Weapons of Mass Disruption. New York: Thunder's Mouth Press, 2001. ISBN 156025307X.

Stevens, W. Richard. TCP/IP Illustrated. Reading MA: Addison Wesley Longman, Inc., 1994. ISBN 0201633469. (Note: This is a 3-volume set.)

Stoll, Cliff. Cuckoo's Egg. Pocket Books, 1995. ISBN 0671726889.

### Fiction

Stephenson, Neal. Cryptonomicon. New York, NY: HarperCollins Publishers, 1999. ISBN 0060512806.

---

## White Papers & Requests for Comments

[www.cis.ohio-state.edu/htbin/rfc/rfc1700.html](http://www.cis.ohio-state.edu/htbin/rfc/rfc1700.html)

Reynolds, J. and J. Postel, Assigned Numbers. Available at this Web site.

[www.cis.ohio-state.edu/hypertext/information/rfc.html](http://www.cis.ohio-state.edu/hypertext/information/rfc.html)

Internet Requests for Comments (RFC)

[www.watchguard.com/infocenter/whitepapers.asp](http://www.watchguard.com/infocenter/whitepapers.asp)

WatchGuard White Paper Library

## Mailing Lists

---

*wg-users@watchguard.com*

WatchGuard sponsors a listserv for our customers. For more information, see the Technical Support chapter in the User Guide.

*firewall-wizards@nfr.net*

Firewall gurus from around the world discuss and answer all types of questions.

*Full Disclosure*

When Symantec bought Security Focus and its lists, suspicious security experts and network administrators fled. Where did they go? Largely to FullDisclosure. **Pros:** Cannot be biased by any vendor because it's completely unmoderated. First choice for posting latest discoveries by some big-name researchers. Black-hat hackers like to harass this list, inadvertently providing useful perspective on the "script kiddie" mindset. **Con:** Because it's unmoderated, this high-volume list will drown you in 20 irrelevant flame-war e-mails for every on-topic comment. **Net:** You get what you pay for, and this list is free. Try it briefly to familiarize yourself with it, but use Outlook rules to divert Full Disclosure e-mails to a folder you can read at leisure.

*VulnWatch and VulnDiscuss*

These lists are, respectively, moderated and unmoderated. **Pro:** You can not only get security advisories from vendors, you can also see what the rest of the IT community thinks and feels about them. **Con:** Fairly large volume of highly technical alerts difficult for newcomers to understand. **Net:** While you wouldn't want this as your only source of security news, it provides a solid source for confirmation and alternate opinions on security trends.

*Secunia*

**Pro:** This list notifies on every vulnerability under the sun. **Con:** Secunia mostly reproduces vendor releases, without analysis or suggested remediation for IT beginners. And did I mention they report on everything under the sun? If you don't know Linux/Unix, you won't understand a lot of the bulletins. **Net:** High volume, but all on topic (unlike FullDisclosure). Try it to see if it's for you.

## General IT and Security Web Sites

---

First, a note to any intrepid beginner who is reading this: not all of these sites are sponsored by good guys. Some of them post malicious code that hackers use. Do not download or execute anything you do not fully understand.

*WatchGuard Frequently Asked Questions*

[www.watchguard.com](http://www.watchguard.com) (Click Support, Log into LiveSecurityService, click Knowledge Base, click FAQs)

*[www.cerias.purdue.edu/](http://www.cerias.purdue.edu/)*

The Center for Education and Research in Information Assurance and Security (CERIAS) is currently viewed as one of the world's largest centers for research and education in areas of information security that are crucial to the protection of critical computing and communication infrastructure. CERIAS is unique among such national centers in its multidisciplinary approach to the problems, ranging from purely technical issues (e.g., intrusion detection, network security, etc.) to ethical, legal, educational, communicational, linguistic, and economic issues, and the subtle interactions and dependencies among them.

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

The Computer Security Institute (CSI) is the world's leading membership organization specifically dedicated to serving and training the information, computer and network security professional. Since 1974, CSI has been providing education and aggressively advocating the critical importance of protecting information assets.

[www.cerias.purdue.edu/homes/spaf/](http://www.cerias.purdue.edu/homes/spaf/)

Dr. Eugene Spafford is a professor of computer sciences and electrical and computer engineering at Purdue University, where he has served on the faculty since 1987. He serves on a number of advisory and editorial boards, and is internationally-known for his writing, research, and speaking on issues of security and ethics. Spafford's current research interests are primarily in the areas of information security, computer crime investigation and information ethics. Spaf (as he is known to his friends, colleagues, and students) is Executive Director of the Purdue CERIAS (Center for Education and Research in Information Assurance and Security), and was the founder and director of the (superseded) COAST Laboratory. This is his homepage.

[project.honeynet.org](http://project.honeynet.org)

The Honeynet Project is a non-profit research organization of security professionals dedicated to information security. They have no products, services or employees, and all research is done on a volunteer basis. Their goal is to learn the tools, tactics, and motives of the blackhat community and share these lessons learned. Founded in October, 1999, all work is OpenSource and shared with the security community.

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

Information Security is the enterprise security and risk managers' leading source of critical, objective information on strategic and practical security issues. Information Security's team of veteran security journalists and experts break down the security problems challenging enterprises and provide practical resolutions.

[www.interhack.net/pubs/fwfaq](http://www.interhack.net/pubs/fwfaq)

This collection of Frequently Asked Questions and answers about Internet firewalls has been compiled over the years from fora such as Usenet, mailing lists, and Web sites. If you have a question, looking here to see whether it has been answered before posting your question is good form. Don't send your questions to the FAQ maintainers.

[www.cerias.purdue.edu/coast/firewalls](http://www.cerias.purdue.edu/coast/firewalls)

This site provides the comprehensive list of resources associated with Internet firewalls. The list is divided into sections to make finding information easier.

[www.microsoft.com/security](http://www.microsoft.com/security)

Microsoft's homepage for computer security resources.

[csrc.nist.gov](http://csrc.nist.gov)

National Institute of Standards and Technology, Computer Security Division.

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

Network Computing magazine, part of the tech web business technology network, features content covering general networking topics as well as specific security topics.

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

Formerly THE clearing house for security vulnerability announcements, Security Focus lost prestige after Symantec bought them (many readers assumed Symantec would bias the reporting). We haven't noticed any dramatic decline in quality, and we routinely use the site -- especially its acclaimed Bugtraq list -- for information about new vulnerabilities. **Pro:** Often the first place security researchers post their advisories. Has a great "Basics" reading room for IT

beginners. **Cons:** Advisories are posted in dense jargon difficult for beginners to comprehend. Poorly organized site can make finding a specific item tricky. **Net:** Authoritative, comprehensive, definitely a useful arrow in any sys admin's quiver.

#### *NewsNow*

NewsNow's UK-based spiders and bots automatically search over 15,000 news sources and return live links with the results, updated every five minutes. They offer dozens of newsfeeds (but do we really need to hear the latest on Michael Jackson every five minutes?). The feed you want is called "Security" (listed under "Internet" in the left column. Don't choose "Hacking;" you'll get countless articles about various hackers in legal trouble.) Pro: Comprehensive, up-to-the-minute survey of worldwide Internet security. **Con:** The same information repeats countless times as various online sources report it. **Net:** A great glimpse of security issues worldwide.

#### *The Register*

This is not the first place you'll learn of emerging threats, but when you hear of one, depend on The Reg for the most honest, no-hype summary of the issue. **Pro:** Plain-English writing style is great for IT beginners. Check out their "BOFH" series for hilariously bleak parodies of a network administrator's life. **Con:** Their scathing anti-Microsoft bias can get heavy-handed. **Net:** If you have to explain a new vulnerability to non-technical superiors, you'll appreciate The Register's style.

## White Hat Web Sites

American cinema of the 1930s, 40s, and early 50s, with their endless stream of big-city gangsters and singing cowboys, popularized the metaphorical idea that "good guys" wear white hats and "bad guys" reliably identify themselves by wearing black hats. Extending the tradition today, "white hat" computer security researchers find security holes in commercial software, but instead of telling everyone, they first inform the manufacturer of the flaw. Then they cooperate with the manufacturer in getting the flaw fixed before announcing their discovery to the public. We appreciate the efforts of these good guys.

#### *NTBugTraq*

Don't let the "NT" fool you: Russ Cooper's site tracks security vulnerabilities in every kind of Microsoft software that businesses typically use, from server software to Office. Russ's extraordinarily objective assessments neither bash Microsoft, nor cover their sometimes egregious security lapses. He has developed good relationships with key Microsoft personnel, and can often provide a straighter scoop on MS flaws than you can get through official MS channels.

#### *HackerIntel.com*

We like this site as a source of information about hacking and network security-related events. Administrators from educational institutions should consider bookmarking this site, because its multi-faceted coverage includes news accounts hard to find elsewhere about university networks being hacked.

#### *Crypto-Gram*

Bruce Schneier has two gifts you rarely see in one person: he is a bona fide cryptographic expert, and he can write in clear, everyday English. This free e-newsletter is not an alert service; rather, Schneier's insights on security issues will, over time, teach you how to think about security in general -- for example, how to assess whether a "cure" costs more than the risk it addresses, and how to resist falling for a great-sounding plan that doesn't actually provide added security.

### *Insecure.org*

Check out the online home of the well-known security researcher Fyodor, who authored nmap, the best port scanning tool available. From this site you can download nmap and 74 other security tools from others, many of them excellent. Insecure.org serves as a repository for numerous other security lists which may not have an archive of their own (such as FullDisclosure). If you don't want to junk up your Favorites with every security list (BugTraq, FullDisclosure, Pen Test, etc.) bookmark this one site and you can find them all from here.

### *Governmentsecurity.org*

Despite its name, this site is not sponsored by a government. Like many of the other sites we've recommended, it archives daily security news. But our favorite feature is the moderated security forums, where you can discuss relevant topics (ranging from general network security, to how to compile and run specific exploits) with other network administrators.

### *Microsoft TechNet*

IT professionals running a Windows network look here for the latest Microsoft security bulletins. **Pro:** Authoritative source for Microsoft security fixes. **Con:** Microsoft's alerts minimize the truly bad implications of some vulnerabilities, sometimes unfairly. Bring a suspicious mind to the part of each alert that talks about "mitigating factors" that supposedly reduce risk. **Net:** If you use Windows, you've got to visit here at least monthly.

### *CERT.org*

This government-funded source of security advisories describes itself as "a center to coordinate communication among experts during security emergencies and to help prevent future incidents." **Pro:** CERT does an excellent job of coordinating information when vulnerabilities are found in the most commonly-used Internet resources. **Con:** Because their work is "official" and because so many vendors can have a say in CERT's advisories, this is often the last entity to issue a security advisory. **Net:** Pretty much the final word on anything Internet-related and not owned by a private vendor. A must for your arsenal of resources.

---

## **Grey Hat Sites**

We characterize these security researchers as "grey hats" because, unlike white hats, they might not inform the appropriate manufacturer before publicly revealing their findings and posting exploit code (often passed off euphemistically as "proof of concept" code). Technically they're not breaking laws or acting maliciously, like "black hats." But announcing security holes before vendors can fix them is like giving an army a map of the castle they're attacking, with a big red arrow marking the secret entrance. Grey hats commonly claim their behavior contributes to overall security by making vendors watch themselves more diligently. Whether that is true is a battle we'll leave to someone else.

Nonetheless, "grey hat" sites are worth inspecting when you want to understand more about how a particular vulnerability works. These sites are often the first to reveal new vulnerabilities, much sooner than you'll get the info from the appropriate vendor. When trying to prioritize how urgently you need to patch flawed software on your network, flaws where the exploit code is publicly posted should go to the top of your list. To learn whether exploit code is publicly available, monitor our LiveSecurity alerts, and check some of the following sites.

### *Unpatched Internet Explorer Bugs*

Researchers have found numerous security flaws in Internet Explorer that Microsoft has not patched yet. Some holes are serious (for example, one enables a hacker who has lured you to his malicious Web site to silently install and execute code on your computer). Liu Die Yu's site

maintains a list of these unresolved flaws. Many of his descriptions include workarounds that minimize the vulnerability while we all wait for Microsoft's patch.

*Packetstormsecurity.org*

This site offers a repository of the Top 20 security tools, advisories, and exploits, updated throughout the week.

*K-otik.com*

This French site is usually the first place you'll find significant exploit code. They also archive notable white papers in various languages, so multilingual administrators can get a world of security instruction here.

*2600.com*

This Web site supplements the printed journal 2600, the seminal, well-known "hacker's quarterly," where programmers inform one another of new flaws, exploits, and attacks on everything from networks to phone systems. Worth a read so you can realistically assess the strength of your countermeasures.

---

**Other Web Sites**

---

*www.howstuffworks.com*

Simple explanations of how all kinds of things, including system and network components, work.

*www.zebra.org/zebra/index.html*

Online gnu zebra configuration document for Firebox users using dynamic routing protocols.

*www.watchguard.com/support/advancedfaqs/log\_sniffing.asp*

Check here for information on a useful Network Packet Analyzer.

*www.iana.org*

Look here for lists of protocol number assignments and TCP and UDP port numbers.

*www.telusplanet.com/public/sparkman/netcalc.htm*

A network calculator.

*www.winguides.com/registry/*

A good site for information about the Windows registry.

*www.watchguard.com/glossary/?nav=ic*

Online glossary of security terms.

*vmyths.com*

Some viruses you hear about are not real. Though each of virus vendor has a "virux hoax" page, when we have to prove to a hysterical user that a problem doesn't really exist, we like the write-ups here.

*slashdot.org*

For fun, no self-respecting geek should miss viewing science, pop culture, and the world of computers through the perspective of the IT-minded community (millions strong!) who contribute to Slashdot.

---

## Dictionaries of Computer Terminology

---

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

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

[info.astrian.net/jargon/](http://info.astrian.net/jargon/)

[www.techweb.com/encyclopedia/](http://www.techweb.com/encyclopedia/)

---

## RSS Feeds

---

Rich Site Summary (RSS) is an XML-based Web standard for easily distributing news and other information in syndication. In other words, RSS provides a format that delivers news from many sources directly to your desktop.

Furthermore, WatchGuard provides a free RSS feed, WatchGuard Wire, that covers many security topics and, when combined with LiveSecurity or LiveSecurity Informer, keeps you up-to-date with the latest breaking security news.

During a network administrator's hectic day, it's hard to find the time to browse the Web for all the latest IT and network security news. Yet, sometimes this news could help you save your network from the latest virulent worm. An RSS reader can provide you with a convenient, one-stop shop consolidating news from all your favorite sources. Try out RSS and WatchGuard Wire. They're free, and they'll keep you informed while saving you time.

Resources:

[www.watchguard.com/rss/Aboutrss.aspx](http://www.watchguard.com/rss/Aboutrss.aspx)

An introduction to the WatchGuard Wire RSS feed.

[www.watchguard.com/rss/list.aspx](http://www.watchguard.com/rss/list.aspx)

A Web archive of the latest WatchGuard Wire articles.

[www.sharpreader.net](http://www.sharpreader.net)

To download Sharpreader.

## Security Feeds

[www.watchguard.com/rss/watchguardwire.xml](http://www.watchguard.com/rss/watchguardwire.xml)

WatchGuard Wire

[www.securityfocus.com/rss/vulnerabilities.xml](http://www.securityfocus.com/rss/vulnerabilities.xml)

SecurityFocus Latest Vulnerabilities

[www.securityfocus.com/rss/news.xml](http://www.securityfocus.com/rss/news.xml)

SecurityFocus news

[www.f-secure.com/weblog/weblog.rdf](http://www.f-secure.com/weblog/weblog.rdf)

F-Secure Weblog

[www.sophos.com/virusinfo/infofeed/tenalerts.xml](http://www.sophos.com/virusinfo/infofeed/tenalerts.xml)

Sophos Ten Latest Virms

[www.sophos.com/virusinfo/infofeed/hoax.xml](http://www.sophos.com/virusinfo/infofeed/hoax.xml)  
Sophos Top Virus Hoaxes

[www.sophos.com/virusinfo/infofeed/topten.xml](http://www.sophos.com/virusinfo/infofeed/topten.xml)  
Sophos Top Virms Last Month

[www.microsoft.com/technet/security/bulletin/secrss.aspx](http://www.microsoft.com/technet/security/bulletin/secrss.aspx)  
Microsoft Security Bulletin Feed

[www.2600.com/rss.xml](http://www.2600.com/rss.xml)  
2600 (Hacker journal)

## IT Related Feeds

[slashdot.org/slashdot.rss](http://slashdot.org/slashdot.rss)

[news.com.com/2547-1\\_3-0-5.xml](http://news.com.com/2547-1_3-0-5.xml)  
CNET News Main News Feed

[news.com.com/2547-7343\\_3-0-5.xml](http://news.com.com/2547-7343_3-0-5.xml)  
CNET News Enterprise Software Feed

[news.com.com/2547-1001\\_3-0-5.xml](http://news.com.com/2547-1001_3-0-5.xml)  
CNET News Enterprise Hardware Feed

[news.com.com/2547-1009\\_3-0-5.xml](http://news.com.com/2547-1009_3-0-5.xml)  
CNET News Security Feed

[news.com.com/2547-1035\\_3-0-5.xml](http://news.com.com/2547-1035_3-0-5.xml)  
CNET News Networking Feed

## Fun Feeds

[www.wired.com/news/feeds/rss2/0,2610,,00.xml](http://www.wired.com/news/feeds/rss2/0,2610,,00.xml)  
Wired top stories

[www.wired.com/news/feeds/rss2/0,2610,3,00.xml](http://www.wired.com/news/feeds/rss2/0,2610,3,00.xml)  
Wired technology stories

[www.wired.com/news/feeds/rss2/0,2610,2,00.xml](http://www.wired.com/news/feeds/rss2/0,2610,2,00.xml)  
Wired culture stories

[www.wired.com/news/feeds/rss2/0,2610,4,00.xml](http://www.wired.com/news/feeds/rss2/0,2610,4,00.xml)  
Wired political stories

[dwtl.net/tapestry/dilbert.rdf](http://dwtl.net/tapestry/dilbert.rdf)  
Daily Dilbert.

[dwtl.net/tapestry/pa.rdf](http://dwtl.net/tapestry/pa.rdf)  
Penny Arcade.



# Index

---

## B

blocked sites, searching for 74

## C

content types  
and SMTP 7  
described 7  
MIME 7

## E

ESP 6

## G

Gateway-Gateway Protocol 6  
GGP 6  
GRE 6

## I

ICMP 6  
IGMP 6  
Internet Control Message Protocol 6  
Internet Group Multicast Protocol 6  
Internet Protocol  
described 1  
header 1  
header number list 2  
options 4  
IP  
described 1  
header 1  
header number list 2  
options 4  
IPIP 6

IP-within-IP 6

## M

MIME content types  
list of 7

## N

Network File System 5  
NFS 5

## P

ports  
random 6  
standard 6  
used by Microsoft products 20  
used by WatchGuard products 19  
protocols  
ESP 6  
GGP 6  
GRE 6  
ICMP 6  
IGMP 6  
Internet 1  
IPIP 6  
TCP 6  
UDP 5

## R

random ports 6

## S

services

---

well-known 19, 21  
standard ports 6  
SurfControl 69

## T

TCP 1, 6  
TCP/IP 1  
transfer protocols  
described 5  
ESP 6  
GGP 6  
GRE 6  
ICMP 6  
IGMP 6  
IPIP 6  
TCP 6  
UDP 5

Transmission Control Protocol 1, 6

## U

UDP 5  
User Datagram Protocol 5

## W

WebBlocker 69  
categories 69  
database 69  
searching for blocked sites 74  
well-known services 19, 21  
www.awl.com 75

---

### ADDRESS:

505 Fifth Avenue South  
Suite 500  
Seattle, WA 98104

### SUPPORT:

www.watchguard.com/support  
support@watchguard.com  
U.S. and Canada +877.232.3531  
All Other Countries +1.206.613.0456

### SALES:

U.S. and Canada +1.800.734.9905  
All Other Countries +1.206.521.8340

### ABOUT WATCHGUARD

WatchGuard is a leading provider of network security solutions for small- to mid-sized enterprises worldwide, delivering integrated products and services that are robust as well as easy to buy, deploy and manage. The company's Firebox X family of expandable integrated security appliances is designed to be fully upgradeable as an organization grows and to deliver the industry's best combination of security, performance, intuitive interface and value. WatchGuard Intelligent Layered Security architecture protects against emerging threats effectively and efficiently and provides the flexibility to integrate additional security functionality and services offered through WatchGuard. Every WatchGuard product comes with an initial LiveSecurity Service subscription to help customers stay on top of the security landscape with vulnerability alerts, software updates, expert security instruction and superior customer care. For more information, please call (206) 521-8340 or visit [www.watchguard.com](http://www.watchguard.com).