



FortiGate Log Message Reference Guide

FortiGate Log Message Reference Guide

Version 2.80 MR10

15 August 2005

01-28010-0105-20050815

© Copyright 2005 Fortinet Inc. All rights reserved.

No part of this publication including text, examples, diagrams or illustrations may be reproduced, transmitted, or translated in any form or by any means, electronic, mechanical, manual, optical or otherwise, for any purpose, without prior written permission of Fortinet Inc.

FortiGate Log Message Reference Guide

Version 2.80 MR10

15 August 2005

01-28010-0105-20050815

Trademarks

Products mentioned in this document are trademarks or registered trademarks of their respective holders.

Regulatory Compliance

FCC Class A Part 15 CSA/CUS

Table of Contents

Introduction	5
About FortiGate logging	5
About this document	6
Document conventions	6
Fortinet documentation	7
Fortinet Knowledge Center	7
Comments on Fortinet technical documentation	8
Customer service and technical support.....	8
Logging Configuration Overview	9
Log config	9
Log setting options.....	9
Configuring log settings	10
Alert email options	10
Configuring alert email	11
Log filter options.....	11
Configuring log filters	12
Enabling traffic logging.....	12
Log access.....	13
Disk log file access	13
Viewing log messages	14
Choosing columns.....	15
Searching log messages.....	15
Log formats	17
Log header.....	17
Log types and sub-types.....	18
Logging severity levels.....	19
Log header format variations	19
Local disk or memory buffer log header format.....	19
WebTrends log header format	19
Remote Syslog log header format.....	19
Log body	20
Traffic log body	20
Event log body	21
Content archive body	21
HTTP.....	21
FTP	22

SMTP, POP3, and IMAP	22
Antivirus log body	22
Attack log body	22
Web filter log body	22
Spam filter log body	23

Log messages 25

Traffic log messages.....	25
Allowed	25
Violation	26
Event log messages.....	26
System	26
IPSec	39
DHCP	41
PPP	41
Admin	44
HA	56
Auth.....	57
Chassis	58
Antivirus log messages.....	60
Infected	60
Attack log messages.....	61
Signature.....	61
Anomaly	61
Web filter log messages.....	61
Urlblock	61
Urlexempt.....	63
Catblock	63
Spam filter log messages.....	64
SMTP	64
POP3	66
IMAP	67
Content archive messages	69
HTTP.....	69
FTP	69
SMTP	69
POP3	69
IMAP	70



FortiGate Log Message Reference Guide Version 2.80 MR10

Introduction

This chapter introduces you to FortiGate logging and the following topics:

- [About FortiGate logging](#)
- [About this document](#)
- [Document conventions](#)
- [Fortinet documentation](#)
- [Customer service and technical support](#)

About FortiGate logging

You can configure the FortiGate unit to record various types of logs to one or more locations. You can also configure alert email to notify administrators of specified events. This guide describes the basics of FortiGate logging configuration. For more information on configuring logging please see the Log & Report chapter in the *FortiGate Administration Guide* for your unit.

You can configure the FortiGate unit to record six types of logs:

- Traffic logs record all the traffic to and through the FortiGate interfaces. You can configure logging for traffic controlled by firewall policies and for traffic between any source and destination addresses.
- Event logs record management and administration events, such as when a configuration has changed or a routing gateway has been added.
- Attack logs record attack signatures and anomalies detected by the FortiGate unit.
- Antivirus logs record virus incidents in web, FTP, and email traffic, such as when the FortiGate unit detects an infected file, blocks a file type, blocks an oversized file or email, or passes a fragmented email.
- Web filter logs record HTTP content and URL blocking events and URL exemption events.
- Spam filter logs record blocking of address patterns and content in IMAP and POP3 traffic.

About this document

This document provides an overview of FortiGate logging configuration, describes the format of FortiGate log messages, explains each message, and recommends actions for you to take in response to the messages, if any.

This document contains the following chapters:

- [Logging Configuration Overview](#) - provides a general overview of configuring logging and alert email.
- [Log formats](#) - provides information on the format of the log messages.
- [Log messages](#) - is an extensive listing of all log messages from the FortiGate unit.

Document conventions

This guide uses the following conventions to describe the structure of log messages.

- angle brackets `< >` to indicate variable keywords

For example:

```
user= <administrator_name>  
radvd receive signal=<value_signal>
```

- vertical bar and curly brackets `{|}` to separate alternative, mutually exclusive required keywords

For example:

```
status={enable | disable}
```

The log message may contain a setting that is set to `enable` or `disable`.

Fortinet documentation

The most up-to-date publications and previous releases of Fortinet product documentation are available from the Fortinet Technical Documentation web site at <http://docs.forticare.com>.

The following [FortiGate product documentation](#) is available:

- *FortiGate QuickStart Guide*
Provides basic information about connecting and installing a FortiGate unit.
- *FortiGate Installation Guide*
Describes how to install a FortiGate unit. Includes a hardware reference, default configuration information, installation procedures, connection procedures, and basic configuration procedures. Choose the guide for your product model number.
- *FortiGate Administration Guide*
Provides basic information about how to configure a FortiGate unit, including how to define FortiGate protection profiles and firewall policies; how to apply intrusion prevention, antivirus protection, web content filtering, and spam filtering; and how to configure a VPN.
- *FortiGate online help*
Provides a context-sensitive and searchable version of the *Administration Guide* in HTML format. You can access online help from the web-based manager as you work.
- *FortiGate CLI Reference Guide*
Describes how to use the FortiGate CLI and contains a reference to all FortiGate CLI commands.
- *FortiGate Log Message Reference Guide*
Describes the structure of FortiGate log messages and provides information about the log messages that are generated by FortiGate units.
- *FortiGate High Availability Guide*
Contains in-depth information about the FortiGate high availability feature and the FortiGate clustering protocol.
- *FortiGate IPS Guide*
Describes how to configure the FortiGate Intrusion Prevention System settings and how the FortiGate IPS deals with some common attacks.
- *FortiGate VPN Guide*
Explains how to configure VPNs using the web-based manager.
- *FortiGate VLANs and VDOMs Guide*
Describes how to configure VLANs and VDOMs in both NAT/Route and Transparent mode. Includes detailed examples.

Fortinet Knowledge Center

Additional Fortinet technical documentation is available from the Fortinet Knowledge Center. The knowledge center contains troubleshooting and how-to articles, FAQs, technical notes, and more. Visit the Fortinet Knowledge Center at <http://kc.forticare.com>.

Comments on Fortinet technical documentation

Please send information about any errors or omissions in this document, or any Fortinet technical documentation, to techdoc@fortinet.com.

Customer service and technical support

For antivirus and attack definition updates, firmware updates, updated product documentation, technical support information, and other resources, please visit the Fortinet technical support web site at <http://support.fortinet.com>.

You can also register FortiGate Antivirus Firewalls from <http://support.fortinet.com> and modify your registration information at any time.

Fortinet email support is available from the following addresses:

amer_support@fortinet.com For customers in the United States, Canada, Mexico, Latin America and South America.

apac_support@fortinet.com For customers in Japan, Korea, China, Hong Kong, Singapore, Malaysia, all other Asian countries, and Australia.

eu_support@fortinet.com For customers in the United Kingdom, Scandinavia, Mainland Europe, Africa, and the Middle East.

For information on Fortinet telephone support, see <http://support.fortinet.com>.

When requesting technical support, please provide the following information:

- Your name
- Company name
- Location
- Email address
- Telephone number
- FortiGate unit serial number
- FortiGate model
- FortiGate FortiOS firmware version
- Detailed description of the problem

Logging Configuration Overview

This chapter provides a general overview of configuring logging and alert email. For more information about logging please see the Log & Report chapter of the *FortiGate Administration Guide* for your FortiGate unit.

This chapter describes how to configure the following options:

- [Log config](#)
- [Log access](#)

Log config

Use Log Config to configure log storage settings, log filters and alert email.

Log setting options

You can enable storing log messages to one or more of the following locations:

- Remote Syslog Server** A remote computer running a syslog server.
- WebTrends Server** A remote computer running a NetIQ WebTrends firewall reporting server. FortiGate log formats comply with WebTrends Enhanced Log Format (WELF) and are compatible with NetIQ WebTrends Security Reporting Center 2.0 and Firewall Suite 4.1.
- Local Disk** The FortiGate local disk (if the FortiGate unit has one).
- Memory Buffer** The FortiGate system memory. The FortiGate system memory has a limited capacity and only displays the most recent log entries. Traffic and content archives cannot be stored in the memory buffer. When the memory is full, the FortiGate unit begins to overwrite the oldest messages. All log entries are deleted when the FortiGate unit restarts.
- FortiLog Device** A FortiLog device. The FortiLog device is a log analyzer and manager that can combine the log information from various FortiGate units and other firewall units. You can also use the FortiLog device to generate reports based on the content of the log files.
- Alert E-mail** An alert email is sent to the recipients listed in **Log&Report > Log Config > Alert Email**.

When you enable a logging location you need to configure any required settings, such as IP addresses for remote servers, and log roll rules for logging to memory. You must also select a logging severity level for each location.

For descriptions of the settings for each log location please see the Log & Report chapter of the *FortiGate Administration Guide*. For a description of the logging severity levels see [“Logging severity levels” on page 19](#).

Configuring log settings

Log setting configuration is organized by log location. Configure log settings for each location to which you want to record logs. If you want to log traffic, you must also enable traffic logging for specific interfaces and firewall policies.

To configure Log Setting

- 1 Go to **Log&Report > Log Config > Log Setting**.
- 2 Select a check box to enable logging to that location.
- 3 Select the blue arrow beside the location.
The setting options appear for that location.
- 4 Enter the IP address if logging to a remote location.
- 5 Enter the port number if logging to a remote syslog server.
- 6 Select the logging severity level.
- 7 Configure the log roll settings if logging to the local disk.
- 8 Repeat steps 2 through 8 to configure other logging locations.
- 9 Select Apply.

Alert email options

You can configure the FortiGate unit to send alert email up to three recipients when selected events occur. Use the following settings to configure alert email:

Authentication Enable	Selecting the Authentication Enable check box enables SMTP authentication.
SMTP Server	The name/address of the SMTP server for email.
SMTP User	The SMTP user name.
Password	The SMTP password.
Email To	Enter one to three email recipients for alert email. You can send a test alert email using the Test button.
Level	The FortiGate unit sends alert email for all messages at and above the logging severity level you select.
Emergency	The interval to wait before sending an alert email for emergency level log messages. See “Logging severity levels” on page 19 .
Alert	The interval to wait before sending an alert email for alert level log messages. See “Logging severity levels” on page 19 .
Critical	The interval to wait before sending an alert email for critical level log messages. See “Logging severity levels” on page 19 .
Error	The interval to wait before sending an alert email for error level log messages. See “Logging severity levels” on page 19 .
Warning	The interval to wait before sending an alert email for warning level log messages. See “Logging severity levels” on page 19 .
Notification	The interval to wait before sending an alert email for notification level log messages. See “Logging severity levels” on page 19 .
Information	The interval to wait before sending an alert email for information level log messages. See “Logging severity levels” on page 19 .



Note: If more than one log message is collected before an interval is reached, the messages are combined and sent out as one alert email.

You can select specific events to trigger alert email. The log settings in Alert E-mail Configuration are filters used for determining alert email content.

The filters are the same as those used for configuring Log Setting (but without traffic logging), and are described in [“Log setting options” on page 9](#).

Configuring alert email



Note: Before configuring alert email make sure you configure at least one DNS server. The FortiGate unit uses the SMTP server name to connect to the mail server, and must look up this name on your DNS server.

To configure alert email

- 1 Go to **Log&Report > Log Config > Alert E-mail**.
- 2 Select Enable to enable SMTP Authentication if required.
- 3 Configure the SMTP server, user, and password information if required.
- 4 Type one or more email addresses.
- 5 Select the logging severity level for which you want to send alert email.
- 6 Configure the time limit in which to send email for each logging severity level.
- 7 Select Apply.
- 8 Go to **Log&Report > Log Config > Log Filter** to select the desired log types for sending alert email.

Log filter options

For each logging location you enable, you can create a customized log filter based on the log types described in the Log & Report chapter of the *FortiGate Administration Guide*.



Note: Log locations must be enabled in Log Setting to be available for selection in the Log Filter.

Figure 1: Example traffic and event log filter settings

Log Filter							
	Check all	Fortilog	Disk	Memory	Syslog	WebTrends	Alert E-mail
▶ Traffic Log	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
▶ Event Log	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
▼ Anti-virus Log	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Virus infected	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Filename blocked	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
File oversized	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
▼ Web Filter Log	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Content block	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
URL block	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
URL exempt	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Blocked category ratings	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Monitored category ratings	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Category rating errors	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
▶ Attack Log	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
▼ Spam Filter Log	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
SMTP	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
POP3	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
IMAP	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Configuring log filters

Configure log filters for each location to which you are saving logs.

To configure log filters

- 1 Go to **Log&Report > Log Config > Log Filter**.
- 2 Enable the logging type for each location to which you want to log messages.
- 3 Select the specific log sub-types to log for each location.
- 4 Select Apply.

Enabling traffic logging

To enable traffic logging for an interface or VLAN subinterface

You can enable traffic logging for an interface or VLAN subinterface (if available). All connections to and through the interface are recorded in the traffic log.

- 1 Go to **System > Network > Interface**.
- 2 Select the Edit icon for an interface.
- 3 Select Log.
- 4 Select OK.
- 5 Repeat steps 1 through 4 for each interface for which you want to enable logging.

To enable traffic logging for a firewall policy

You can enable traffic logging for a firewall policy. All connections accepted by the firewall policy are recorded in the traffic log.

- 1 Go to **Firewall > Policy**.
- 2 Select the Edit icon for a policy.
- 3 Select Log Traffic.
- 4 Select OK.

Log access

Log Access provides access to log messages saved to the FortiGate disk or to the memory buffer. Not all FortiGate units include a hard disk drive.



Note: FortiGate units do not save some types of logs to memory. You can view these log messages with Log Access only if your FortiGate unit contains a hard disk drive.













On its disk, the FortiGate unit saves log messages in files. To view log messages, you must first select the file to open. You can also delete a file, clear (remove the log messages from) a file, or download a file in either plain text or CSV format.

You can view the log messages in a memory buffer simply by accessing the buffer. You cannot delete or download log messages from the memory buffer.

Disk log file access

You can view, navigate, and download log files saved to the FortiGate disk.

Figure 2: Sample list of log files stored on the FortiGate disk

Type: Disk			
File name	Size	Last access time	
elog	6656	Tue Jan 13 08:44:17 2004	  
elog.1	9216	Thu Jan 8 15:58:47 2004	  
elog.2	12800	Tue Dec 23 12:45:52 2003	  
elog.3	1414656	Mon Dec 15 10:05:32 2003	  

To access log files on the FortiGate disk

- 1 Go to **Log&Report > Log Access**.
- 2 Select the log type you wish to access.
- 3 Select Disk from the Type list.
- 4 You can clear or delete, download, or view the log files by selecting the corresponding icon.

When downloading a log file, you can save the log in plain text or CSV format.

To download log files from the FortiGate disk

- 1 Go to **Log&Report > Log Access**.
- 2 Select the log type you wish to access.
- 3 Select Disk from the Type list.
- 4 Select the Download icon for the file you wish to download.
- 5 Select Download file in normal or CSV format.
- 6 Select Open to view the log file or Save to save the log file to your computer.

Viewing log messages

You can view and navigate log messages saved to FortiGate hard disk drive or to the memory buffer.

Figure 3: Viewing log messages

#	Date	Time	Level	User Interface	Action	Message
1	2004-07-27	12:01:33	information	GUI(172.20.120.51)	login	User admin login successfully from GUI(172.20.120.51)
2	2004-07-27	12:01:31	information	GUI(172.20.120.51)	logout	GUI session timeout from GUI(172.20.120.51)
3	2004-07-27	11:41:59	information	GUI(172.20.120.51)	login	User admin login successfully from GUI(172.20.120.51)
4	2004-07-27	11:41:57	information	GUI(172.20.120.51)	logout	GUI session timeout from GUI(172.20.120.51)
5	2004-07-27	11:41:56	information	GUI(172.20.120.51)	logout	GUI session timeout from GUI(172.20.120.51)
6	2004-07-27	11:29:06	information	GUI(172.20.120.51)	login	User admin login successfully from GUI(172.20.120.51)
7	2004-07-27	11:29:03	information	GUI(172.20.120.51)	logout	GUI session timeout from GUI(172.20.120.51)
8	2004-07-27	11:29:03	information	GUI(172.20.120.51)	logout	GUI session timeout from GUI(172.20.120.51)
9	2004-07-27	11:21:37	information	GUI(172.20.120.51)	login	User admin login successfully from GUI(172.20.120.51)
10	2004-07-27	11:21:34	information	GUI(172.20.120.51)	logout	GUI session timeout from GUI(172.20.120.51)
11	2004-07-27	11:12:34	information	GUI(172.20.120.51)	login	User admin login successfully from GUI(172.20.120.51)
12	2004-07-27	11:12:31	information	GUI(172.20.120.51)	logout	GUI session timeout from GUI(172.20.120.51)
13	2004-07-27	11:01:33	information	GUI(172.20.120.51)	login	User admin login successfully from GUI(172.20.120.51)

To view log messages in the FortiGate memory buffer

- 1 Go to **Log&Report > Log Access**.
- 2 Select the log type you wish to view.
- 3 Select Memory from the Type list.
The log messages are displayed.

You can change the displayed columns or see the raw log messages, go to the previous or next log page, or search the log by selecting the corresponding icon.

To view log messages in FortiGate disk drive files

- 1 Go to **Log&Report > Log Access**.
- 2 Select the log type you wish to view.
- 3 Select Disk from the Type list.
The log files are displayed.
- 4 Select the View icon for the log file you want to open.
The log messages are displayed.

You can change the displayed columns or see the raw log messages, go to the previous or next log page, or search the log by selecting the corresponding icon.

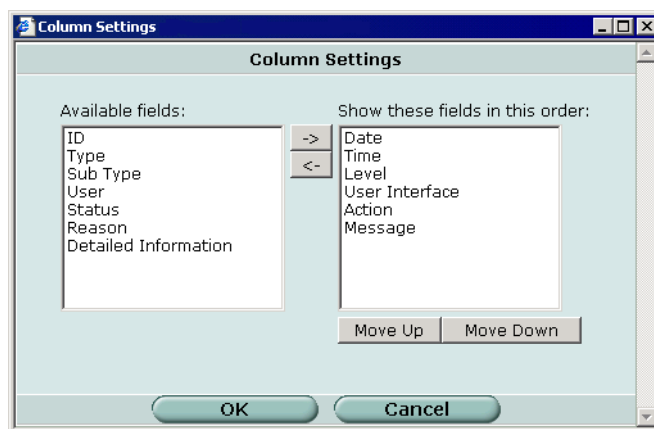
Choosing columns

You can customize your log messages display using the Column Settings window. The column settings apply only when the formatted (not raw) display is selected.

To change the columns in the log message display

- 1 While viewing log messages, select the Column Settings icon.

Figure 4: Column settings for viewing log messages



- 2 To add fields, select them in the Available fields list and select the right arrow button.
- 3 To remove fields, select them in the Show these fields list and select the left arrow button.
- 4 To change the position of a column, select the field in the Show these fields list and then select Move Up or Move Down as necessary.
- 5 Select OK.



Note: The Detailed Information column provides the entire raw log entry and is not needed unless the log contains information not available in any of the other, more specific columns.

Searching log messages

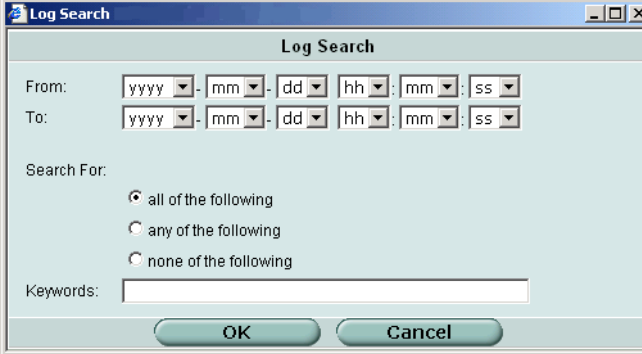
There are two ways to search log messages: a simple keyword search or an advanced search that enables you to use multiple keywords and specify a time range.

To perform a simple keyword search

- 1 Display the log messages you want to search. For more information, see [“Viewing log messages” on page 14](#).
- 2 In the Search field, type a keyword and select Go.
The log message list shows only the logs containing the keyword.

To perform an advanced search

- 1 Display the log messages you want to search. For more information, see [“Viewing log messages” on page 14](#).
- 2 Select Advanced Search.

Figure 5: Log search window

The screenshot shows a 'Log Search' dialog box with the following fields and options:

- From:** yyyy - mm - dd hh : mm : ss
- To:** yyyy - mm - dd hh : mm : ss
- Search For:**
 - all of the following
 - any of the following
 - none of the following
- Keywords:** [Text input field]
- Buttons:** OK, Cancel

- 3** If you want to search for log messages in a particular date range, select the From and To dates.
- 4** Select one of the following options:

all of the following	The message must contain all of the keywords
any of the following	The message must contain at least one of the keywords
none of the following	The message must contain none of the keywords
- 5** In the Keywords field, type the keywords for the search.
- 6** Select OK.
The log message list shows only the logs that meet your log search criteria.

Log formats

FortiGate log messages have two parts:

- [Log header](#)
- [Log body](#)

In the following example of an event log message, the log header is marked in bold.

```
2004-05-22 19:32:56 log_id=0420073001 type=ips subtype=anomaly  
pri=critical attack_id=100663399 src=10.10.1.2 dst=10.10.1.4  
src_port=2000 dst_port=21 interface=external src_int=n/a  
dst_int=n/a status=clear_session proto=6 service=ftp  
msg="anomaly: syn_fin[Reference: http://www.fortinet.com/ids/  
ID100663399]"
```

Log header

The log header may contain the following information:

```
date time log_id log_type subtype severity virtual_domain  
session_number
```

Date	The year, month, and day when the event occurred in the format yyyy-mm-dd.
Time	The hour, minute, and second when the event occurred in the format hh:mm:ss.
Log ID (message ID)	log_id= a ten digit number. The first two digits represent the log type and the following two digits represent the log subtype. The last 5 digits are the message ID, which you can use to search for message descriptions in this guide.
Log type	type= the section of the system where the event occurred. The log types are traffic, event, attack, antivirus, web filter, and spam filter. See “Log types and sub-types” on page 18 .
Subtype	subtype= the subtype for each message. See “Log types and sub-types” on page 18 .
Severity	pri= the severity level (priority) of the event. There are seven logging severity levels, from Information up to Emergency. See “Logging severity levels” on page 19 .
virtual_domain	vd= the virtual domain in which the traffic was logged.
session_number	Traffic log messages only. SN= the session number referenced in a traffic log message.

Log types and sub-types

FortiGate log messages are divided into the following types and sub-types which correspond to the settings you selected when configuring the Log Setting.

Table 1: Log message types and sub-types

Log type	Category Number	Sub-type	Sub-type number
traffic (Traffic Log)	00	allowed – Policy allowed traffic	22
		violation – Policy violation traffic	23
event (Event Log)	01	system – System activity event	00
		ipsec – IPSec negotiation event	01
		dhcp – DHCP service event	02
		ppp – L2TP/PPTP/PPPoE service event	03
		admin – admin event	04
		ha – HA activity event	05
		auth – Firewall authentication event	06
		pattern – Pattern update event	07
		chassis – FortiGate-4000 and FortiGate-5000 series chassis event	30
contentarchive (Content Archive)	06	HTTP – Virus infected	25
		FTP – FTP content meta-data	26
		IMAP – IMAP content meta-data	29
		POP3 – POP3 content meta-data	28
		SMTP – SMTP content meta-data	27
virus (Antivirus Log)	02	infected – Virus infected	11
		filename – Filename blocked	12
		oversize – File oversized	13
webfilter (Web Filter Log)	03	content – content block	14
		urlblock – URL block	15
		urlexempt – URL exempt	16
		catblock – Blocked category ratings; ;	17
		Monitored category ratings	18
		Category rating errors	19
ids (Attack Log)	04	signature – Attack signature	20
		anomaly – Attack anomaly	21
emailfilter (Spam Filter Log)	05	SMTP	08
		POP3	09
		IMAP	10

Logging severity levels

The FortiGate unit logs all messages at and above the logging severity level you select. For example, if you select Error, the unit logs Error, Critical, Alert and Emergency level messages.

[Table 2](#) lists and describes the logging severity levels.

Table 2: Logging severity levels

Level name	Description
Emergency	The system has become unusable.
Alert	Immediate action is required. Alert level log messages include attack signature detections.
Critical	Functionality is affected. Critical level log messages include virus detection, out of memory, out of range, and routing problem messages.
Error	An error condition exists and functionality is probably affected.
Warning	Functionality might be affected. Warning level log messages include packet timer, and interface problem messages, limit messages, and major configuration change messages.
Notification	Information about normal events. Notification level log messages include messages about minor configuration changes and HA events that require little or no action.
Information	General information about system operations. Information level log messages include messages about very minor configuration changes and other events that require little or no action.

Log header format variations

The log header format varies depending on the log location to which it is sent. For information about log locations, see [“Log setting options” on page 9](#).

Local disk or memory buffer log header format

If you configure logging to the local disk or memory buffer, the log header format is similar to the following example:

```
2004-05-23 16:23:46 log_id=0100030101 type=event subtype=admin
pri=information
```

WebTrends log header format

If you configure logging to a remote NetIQ WebTrends firewall reporting server, the log header format is similar to the following example:

```
id=firewall time="2004-05-21 14:01:01" fw=FGT4002801021089
pri=6 log_id=0100030101 type=event subtype=admin
```

Remote Syslog log header format

If you configure logging to a remote Syslog server, you can enable or disable CSV format.

In CSV format, the log header format is similar to the following example:

```
2004-05-21, time=14:01:01, device_id=FGT4002801021089,
pri=information, log_id=0100030101, type=event, subtype=admin
```

In normal format, the log header format is similar to the following example:

```
date=2004-05-21 time=14:01:01 device_id=FGT4002801021089
pri=information log_id=0100030101 type=event subtype=configure
```

Log body

The log body contains details about the event or activity, such as IP addresses and status information. Except for the traffic log, the log entries may also contain user messages at the end of the log body, as in the following example:

```
user=admin ui=GUI(192.168.110.141) action=switch_mode
status=success msg="System has been changed to Transparent mode
by user admin via GUI(192.168.110.141)"
```

Traffic log body

With traffic logging enabled, the FortiGate unit records all the traffic to and through the FortiGate interfaces. For information on how to enable traffic logging, see [“Enabling traffic logging” on page 12](#).

An example traffic log body contains the following information:

```
rule=<value_webtrend> policyid=<value_policyid>
proto=<protocol> service=<network_service> status={accept |
deny} src=<ip_address> srcname={<ip_address> | <domain_name>}
dst=<ip_address> dstname={<ip_address> | <domain_name>}
src_int=<interface_name> dst_int=<interface_name>
sent=<value_bytes> rcvd=<value_bytes> sent_pkt=<value_packets>
rcvd_pkt=<value_packets> src_port=<port_num>
dst_port=<port_num> vpn={<vpn_name> | n/a} tran_ip=<ip_address>
tran_port=<port_num> dir_disp={org | replay} tran_disp={noop |
snat | dnat}
```

rule	Same as policyid below. Required by WebTrends message format.
policyid	The ID number of the firewall policy that applies to the session or packet.
proto	The protocol that applies to the session or packet.
service	The IP network service that applies to the session or packet. The services displayed correspond to the services configured in the firewall policies.
status	The status can be either deny or accept, depending on the applicable firewall policy.
src	The source IP address.
srcname	The source name or IP address.
dst	The destination IP address.
dstname	The destination name or IP address.

src_int	The interface through which the traffic comes in. For outgoing traffic originating from the firewall it will be "unknown".
dst_int	The interface through which the traffic goes out. For incoming traffic to the firewall it will be "unknown".
sent	The total number of bytes sent.
rcvd	The total number of bytes received.
sent_pkt	The total number of packets sent during the session.
rcvd_pkt	The total number of packets received during the session.
src_port	The source port number of TCP and UDP traffic. The src_port is 0 (zero) for other types of traffic.
dst_port	The destination port number of TCP and UDP traffic. The dst_port is 0 (zero) for other types of traffic.
vpn	The name of the VPN tunnel used by the traffic. "n/a" is displayed if VPN is not applicable.
tran_ip	The translated IP in NAT mode. For transparent mode, it is "0.0.0.0".
tran_port	The translated port number in NAT mode. For transparent mode, it is "0".
dir_disp	The packet is either "org" (original) or "replay".
tran_disp	The packet is source NAT translated or destination NAT translated.

For descriptions of traffic log messages, see ["Traffic log messages" on page 25](#).

Event log body

Event logs record system activity, IPSec, DHCP, PPP, administration, high availability (HA) and firewall related events.

Each event log message records the date and time of the event and a description of the event.

The following example shows an event log message body:

```
user=admin ui=GUI(192.168.110.44) action=download
status=success msg="Logging file has been downloaded by user
admin via GUI(GUI(192.168.110.44))"
```

For descriptions of event log messages, see ["Event log messages" on page 26](#).

Content archive body

Content archives record meta-data about the content for a particular protocol (HTTP, FTP, IMAP, POP3, and SMTP).

Each content archive message records the date and time and a description of the content.

HTTP

An example HTTP content archive body contains the following information:

```
<ContLogVersionNo>:<SessionNo>:<clientIP>-><serverIP>:
<infectionStatus>:<RequestSize>:<ResponseSize>:<HTTPrequest>
```

FTP

An example FTP content archive body contains the following information:

```
<ContLogVersionNo>:<SessionNo>:<clientIP><-><serverIP>:
<infectionStatus>:<RequestSize>:<ResponseSize>:<FTPcommand>
```

SMTP, POP3, and IMAP

An example email content archive body contains the following information:

```
<ContLogVersionNo>:<SessionNo>:<clientIP><-><serverIP>:
<infectionStatus>:<SizeSent>:<from/to>:
<attachment(1=yes, 0=no)>
```

For descriptions of content archive messages, see [“Content archive messages” on page 69](#).

Antivirus log body

Each virus log message records the date and time at which the virus was detected, the type of virus, and the source and destination IP addresses of the infected traffic.

A virus log body contains the following information:

```
src=<ip_address> dst=<ip_address> src_int=<interface_name>
dst_int=<interface_name> service= {http | smtp | pop3 | imap |
ftp} status={blocked | passthrough} from=<email_address>
to=<email_address> msg="<string>"
```

For descriptions of virus log messages, see [“Antivirus log messages” on page 60](#).

Attack log body

Attack logs record attacks detected by the FortiGate intrusion prevention and detection systems. Each attack log message records the date and time at which the attack was made, the type of attack, and the source and destination IP addresses of the attack.

The following example shows an attack log message body:

```
2004-05-09 08:13:17 ids-detec-alert: attack_id=102891683
src=192.155.122.73 dst=192.155.48.21 src_port=1066 dst_port=80
status=detected proto=006 service=http msg="Web-Misc. whisker
HEAD with large datagram"
```

For descriptions of attack log messages, see [“Attack log messages” on page 61](#).

Web filter log body

Each web filter log message records the date and time at which content was blocked, a URL was blocked, or a URL was exempted, and the source and destination IP addresses of the HTTP traffic.

A web filter log body contains the following information:

```
src=<ip_address> dst=<ip_address> src_int=<interface_name>  
dst_int=<interface_name> service=http status={blocked |  
passthrough} dstname=<domain_name> arg=<url_path>  
msg="<string>"
```

For descriptions of web filter log messages, see [“Web filter log messages” on page 61](#).

Spam filter log body

Each spam filter log message records the date and time at which an IP address, email address, or a banned word was blocked, and the source and destination IP addresses of the IMAP or POP3 traffic.

A spam filter log body contains the following information:

```
src=<ip_address> dst=<ip_address> src_int=<interface_name>  
dst_int=<interface_name> service= {http | smtp | pop3 | imap |  
ftp} status={blocked | passthrough} from=<email_address>  
to=<email_addr> msg="<string>"
```

For descriptions of spam filter log messages, see [“Spam filter log messages” on page 64](#).

Log messages

This chapter describes the following log messages.

- [Traffic log messages](#)
- [Event log messages](#)
- [Antivirus log messages](#)
- [Attack log messages](#)
- [Web filter log messages](#)
- [Spam filter log messages](#)



Note: You can search for a specific message using the message ID, which is the last 5 digits of the log_id from the log message. For example, if you are looking for a message with log_id=0104032006, search for “32006”.

Traffic log messages

Allowed

The following traffic log messages are generated by policy allowed traffic.

Message ID:	10001
Severity:	Notification
Message:	SN=<session_num> duration=<value_seconds> rule=<value_webtrend> policyid=<value_policyid> proto=<protocol> service=<network_service> status=accept src=<ip_address> srcname={<ip_address> <domain_name>} dst=<ip_address> dstname={<ip_address> <domain_name>} src_int=<interface_name> dst_int=<interface_name> sent=<value_bytes> rcvd=<value_bytes> sent_pkt=<value_packets> rcvd_pkt=<value_packets> src_port=<port_num> dst_port=<port_num> vpn={<vpn_name> n/a} tran_ip=<ip_address> tran_port=<port_num> dir_disp={org replay} tran_disp={noop snat dnat}
Meaning:	See “Traffic log body” on page 20 for a description of the traffic log message fields.

Violation

The following traffic log messages are generated by policy violation traffic.

Message ID:	13001
Severity:	Notification
Message:	SN=<session_num> duration=<value_seconds> rule=<value_webtrend> policyid=<value_policyid> proto=<protocol> service=<network_service> status=deny src=<ip_address> srcname={<ip_address> <domain_name>} dst=<ip_address> dstname={<ip_address> <domain_name>} src_int=<interface_name> dst_int=<interface_name> sent=<value_bytes> rcvd=<value_bytes> sent_pkt=<value_packets> rcvd_pkt=<value_packets> src_port=<port_num> dst_port=<port_num> vpn={<vpn_name> n/a} tran_ip=<ip_address> tran_port=<port_num> dir_disp={org replay} tran_disp={noop snat dnat}
Meaning:	See “Traffic log body” on page 20 for a description of the traffic log message fields.
Action:	As required to resolve traffic violation.

Event log messages

System

The following event log messages are generated by system activity events.

Message ID:	20001
Severity:	Information
Message:	gateway=<gateway_ip_address> interface={internal external dmz <other> ... } status={up down}
Meaning:	Routing information has changed because the gateway is up/down
Action:	Check gateway status.

Message ID:	20001
Severity:	Information
Message:	modem: unable to open modem device - check hardware
Meaning:	Problem contacting the modem.
Action:	Verify modem connections and settings.

Message ID: 20001
Severity: Information
Message: modem: Redial limit exceeded... giving up
Meaning: The FortiGate unit has attempted to redial the ISP from the modem and could not connect.
Action: Reset the modem to attempt to the connection.

Message ID: 20002
Severity: Notification
Message: user=system ui=system action=<action> status=failure msg="Can't resolve the IP address of <email_address>"
Meaning: The domain name configured for an alert email recipient cannot be resolved.
Action: Verify the email addresses configured for alert emails.

Message ID: 20031
Severity: Critical
Message: Out of memory in <memory_sector>
Meaning: The FortiGate flash memory is full in the specified sector.
Action: Delete logs stored to local disk, perform other maintenance to free memory space.

Message IDL 20032
Severity: Critical
Message: Interface <interface_name> not found in <memory_sector>
Meaning: The FortiGate unit cannot find the specified interface.
Action: Check configuration of the interface and check any physical connections.

Message ID: 20033
Severity: Information
Message: using Mobile IPv6 extensions
Meaning: An interface uses Mobile IPv6 extensions.

Message ID: 20034
Severity: Critical
Message: MinRtrAdvInterval for <interface_name> must be between <start_range_seconds> and <end_range_seconds>
Meaning: The minimum time allowed between sending unsolicited multicast router advertisements from the specified interface (using Mobile IPv6 extensions) must be configured within the specified range. Range is specified in seconds.
Action: Reconfigure router according to MinRtrAdvInterval.

Message ID: 20035
Severity: Critical
Message: MinRtrAdvInterval must be between <start_range_seconds> and <end_range_seconds> for <interface_name>
Meaning: The minimum time allowed between sending unsolicited multicast router advertisements from the specified interface must be configured within the specified range. Range is specified in seconds.
Action: Reconfigure router according to MinRtrAdvInterval.

Message ID: 20036
Severity: Critical
Message: MaxRtrAdvInterval for <interface_name> must be between <start_range_seconds> and <end_range_seconds>
Meaning: The maximum time allowed between sending unsolicited multicast router advertisements from the specified interface (using Mobile IPv6 extensions) must be configured within the specified range. Range is specified in seconds.
Action: Reconfigure router according to MaxRtrAdvInterval.

Message ID: 20037
Severity: Critical
Message: MaxRtrAdvInterval must be between <start_range_seconds> and <end_range_seconds> for <interface_name>
Meaning: The maximum time allowed between sending unsolicited multicast router advertisements from the specified interface must be configured within the specified range. Range is specified in seconds.
Action: Reconfigure router according to MaxRtrAdvInterval.

Message ID: 20038
Severity: Critical
Message: AdvLinkMTU must be zero or between <start_range_bytes> and <end_range_bytes> for <interface_name>
Meaning: The value to be placed in MTU options sent by the router must be either zero or between the specified range for the specified interface. A value of zero indicates that no MTU options are sent.
Action: Reconfigure router according to range.

Message ID: 20039
Severity: Critical
Message: AdvLinkMTU must be zero or greater than <value_bytes> for <interface_name>
Meaning: The value to be placed in MTU options sent by the router must be either zero or greater than the specified value for the specified interface. A value of zero indicates that no MTU options are sent.
Action: Reconfigure router according to range.

Message ID: 20040
Severity: Critical
Message: AdvReachableTime must be less than <value> for <interface_name>
Meaning: The value to be placed in the Reachable Time field in the Router Advertisement messages sent by the router must be less than the specified value for the specified interface. A value of zero means unspecified (by this router).
Action: Reconfigure router according to specified value.

Message ID: 20041
Severity: Critical
Message: AdvCurHopLimit must not be greater than <value_hop_limit> for <interface_name>
Meaning: The default value to be placed in the Cur Hop Limit field in the Router Advertisement messages sent by the router must not be greater than the specified value for the specified interface.
Action: Reconfigure router according to specified value.

Message ID: 20042
Severity: Critical
Message: AdvDefaultLifetime for <interface_name> must be zero or between <start_range_seconds> and <end_range_seconds>
Meaning: The value to be placed in the Router Lifetime field of Router Advertisements sent from the interface, in seconds, must be either zero or between the specified range. A value of zero indicates that the router is not to be used as a default router.
Action: Reconfigure router according to specified range.

Message ID: 20043
Severity: Critical
Message: HomeAgentLifetime must be between <value> and <value> for <interface_name>
Meaning: HomeAgentLifetime in Router Advertisement packet is out of range.
Action: Reconfigure router according to specified range.

Message ID: 20044
Severity: Critical
Message: AdvHomeAgentFlag must be set with HomeAgentInfo
Meaning: AdvHomeAgentFlag HomeAgentLifetime in Router Advertisement packet must be set with HomeAgentInfo.
Action: As above.

Message ID: 20045
Severity: Critical
Message: invalid prefix length for <string>
Meaning: Prefix length is too long
Action: Adjust packet prefix length.

Message ID: 20046
Severity: Critical
Message: AdvValidLifetime must be greater than AdvPreferredLifetime for <string>
Meaning: The value to be placed in the Valid Lifetime in the Prefix Information option, in seconds, must be greater than the AdvPreferredLifetime.
Action: As above.

Message ID:	20047
Severity:	Critical
Message:	can't create socket(AF_INET6): <string>
Meaning:	The IPv6 router advertisement daemon failed to create an IPv6 socket.

Message ID:	20048
Severity:	Critical
Message:	setsockopt(IPV6_PKTINFO): <string>
Meaning:	The IPv6 router advertisement daemon failed to set IPV6_PKTINFO option.

Message ID:	20049
Severity:	Critical
Message:	setsockopt(IPV6_CHECKSUM): <string>
Meaning:	The IPv6 router advertisement daemon failed to set IPV6_CHECKSUM option.

Message ID:	20050
Severity:	Critical
Message:	setsockopt(IPV6_UNICAST_HOPS): <string>
Meaning:	The IPv6 router advertisement daemon failed to set IPV6_UNICAST_HOPS option.

Message ID:	20051
Severity:	Critical
Message:	setsockopt(IPV6_MULTICAST_HOPS): <string>
Meaning:	The IPv6 router advertisement daemon failed to set IPV6_MULTICAST_HOPS option.

Message ID:	20052
Severity:	Critical
Message:	setsockopt(IPV6_HOPLIMIT): <string>
Meaning:	The IPv6 router advertisement daemon failed to set IPV6_HOPLIMIT option.

Message ID:	20053
Severity:	Critical
Message:	setsockopt(ICMPV6_FILTER): <string>
Meaning:	The IPv6 router advertisement daemon failed to set ICMPV6_FILTER option.

Message ID: 20054
Severity: Information
Message: radvd receive signal=<value_signal>\n
Meaning: The IPv6 router advertisement daemon received the specified signal and is going to exit.

Message ID: 20055
Severity: Critical
Message: Can not create query to interface at <string>:<string>:<value>!
Meaning: The IPv6 router advertisement daemon cannot create query to interface by using cmf_query_create().

Message ID: 20056
Severity: Critical
Message: Internal error in cmf_query_for_each()!
Meaning: The IPv6 router advertisement daemon occurs an internal error when it uses cmf_query_for_each().

Message ID: 20057
Severity: Critical
Message: Interface <string>:<value> not found in the list!
Meaning: The IPv6 router advertisement daemon failed to find a virtual interface by interface index.

Message ID: 20058
Severity: Information
Message: Interface <string>:<value> reloaded!
Meaning: The IPv6 router advertisement daemon reloaded the specified interface.

Message ID: 20059
Severity: Warning
Message: received packet with no pkt_info!
Meaning: The IPv6 router advertisement daemon received a packet with no pkt_info.

Message ID: 20060
Severity: Warning
Message: received icmpv6 packet with invalid length: <value_bytes>
Meaning: The IPv6 router advertisement daemon received an ICMPv6 packet with invalid length.

Message ID:	20061
Severity:	Critical
Message:	icmpv6 filter failed
Meaning:	The IPv6 router advertisement daemon received an unwanted type of ICMPv6 packet.

Message ID:	20062
Severity:	Warning
Message:	received icmpv6 RA packet with invalid length: <value_bytes>
Meaning:	The IPv6 router advertisement daemon received an ICMPv6 RA packet with invalid length.

Message ID:	20063
Severity:	Warning
Message:	received icmpv6 RA packet with non-linklocal source address
Meaning:	The IPv6 router advertisement daemon received ICMPv6 RA packet with non-linklocal source address.

Message ID:	20064
Severity:	Warning
Message:	received icmpv6 RS packet with invalid length: <value_bytes>
Meaning:	The IPv6 router advertisement daemon received ICMPv6 RS packet with invalid length.

Message ID:	20065
Severity:	Warning
Message:	received icmpv6 RS/RA packet with invalid code: <value_code>
Meaning:	The IPv6 router advertisement daemon received ICMPv6 RS/RA packet with invalid code.

Message ID:	20066
Severity:	Warning
Message:	received RS or RA with invalid hoplimit <value_hops> from <interface_name>
Meaning:	The IPv6 router advertisement daemon received ICMPv6 RS/RA packet with wrong hoplimit.

Message ID: 20067
Severity: Warning
Message: our AdvCurHopLimit on <interface_name> doesn't agree with <interface_name>
Meaning: The AdvCurHopLimit on the specified FortiGate interface does not agree with the value on the specified remote interface. A value of zero means unspecified (by this router).
Action: Configure the interfaces with the same AdvCurHopLimit value.

Message ID: 20068
Severity: Warning
Message: our AdvManagedFlag on <interface_name> doesn't agree with <interface_name>
Meaning: The AdvManagedFlag value (True/False) on the specified FortiGate interface does not agree with the value on the specified remote interface.
Action: Configure the interfaces with the same AdvManagedFlag value.

Message ID: 20069
Severity: Warning
Message: our AdvOtherConfigFlag on <interface_name> doesn't agree with <interface_name>
Meaning: The AdvOtherConfigFlag value (True/False) on the specified FortiGate interface does not agree with the value on the specified remote interface.
Action: Configure the interfaces with the same AdvOtherConfigFlag value.

Message ID: 20070
Severity: Warning
Message: our AdvReachableTime on <interface_name> doesn't agree with <interface_name>
Meaning: The AdvReachableTime configured on the specified FortiGate interface does not agree with the value on the specified remote interface. A value of zero means unspecified (by this router). The value must be no greater than 3 600 000 seconds (1 hour).
Action: Configure the interfaces with the same AdvReachableTime value.

Message ID: 20071
Severity: Warning
Message: our AdvRetransTimer on <interface_name> doesn't agree with <interface_name>
Meaning: The AdvRetransTimer value on the specified FortiGate interface does not agree with the value on the specified remote interface. A value of zero means unspecified (by this router).
Action: Configure the interfaces with the same AdvRetransTimer value.

Message ID: 20072
Severity: Critical
Message: trailing garbage in RA on <interface_name> from <interface_name>
Meaning: The IPv6 router advertisement daemon found extra data in an RA packet from the specified source.

Message ID: 20073
Severity: Critical
Message: zero length option in RA on <interface_name> from <interface_name>
Meaning: The IPv6 router advertisement daemon found an RA packet with no option data from the specified source.

Message ID: 20074
Severity: Critical
Message: option length greater than total length in RA on <interface_name> from <interface_name>
Meaning: The option length is greater than the total length in an RA packet from the specified source.

Message ID: 20075
Severity: Warning
Message: our AdvLinkMTU on <interface_name> doesn't agree with <interface_name>
Meaning: The AdvLinkMTU value on the specified FortiGate interface does not agree with the specified remote interface. A value of zero indicates that no MTU options are sent.
Action: Configure the interfaces with the same AdvLinkMTU value.

Message ID: 20076
Severity: Warning
Message: our AdvValidLifetime on <interface_name> for <value> doesn't agree with <interface_name>
Meaning: The AdvValidLifetime value on the specified FortiGate interface does not agree with the value on the specified remote interface.
Action: Configure the interfaces with the same AdvValidLifetime value.

Message ID: 20077
Severity: Warning
Message: our AdvPreferredLifetime on <interface_name> for <value> doesn't agree with <interface_name>
Meaning: The AdvPreferredLifetime value on the specified FortiGate interface does not agree with the value on the specified remote interface.
Action: Configure the interfaces with the same AdvPreferredLifetime value.

Message ID: 20078
Severity: Critical
Message: invalid option <value_option> in RA on <interface_name> from <interface_name>
Meaning: The IPv6 router advertisement daemon found the specified invalid option in an RA packet from the specified source.

Message ID: 20079
Severity: Information
Message: radvd started\n.
Meaning: The IPv6 router advertisement daemon is ready to serve.

Message ID: 20080
Severity: Critical
Message: recvmmsg: <string>
Meaning: Recvmmsg() in the IPv6 router advertisement daemon failed.

Message ID: 20081
Severity: Critical
Message: received a bogus IPV6_HOPLIMIT from the kernel! len=<value_bytes>, data=<value>
Meaning: The IPv6 router advertisement daemon received a packet with a wrong IPV6_HOPLIMIT.

Message ID: 20082
Severity: Critical
Message: received a bogus IPV6_PKTINFO from the kernel! len=<value_bytes>, index=<value_index>
Meaning: The IPv6 router advertisement daemon received a packet with a wrong IPV6_PKTINFO.

Message ID: 20083
Severity: Warning
Message: problem checking all-routers membership on <interface_name>
Meaning: The IPv6 router advertisement daemon failed to check whether we've joined the all-routers multicast group.

Message ID: 20084
Severity: Warning
Message: sendmsg: <string>
Meaning: sendmsg () in the IPv6 router advertisement daemon failed.

Message ID: 20100
Severity: Critical
Message: FortiGuard category is updated
Meaning: FortiGuard category is updated.

Message ID: 20101
Severity: Notification
Message: act=upload status=<status> file=<file_name> user=<user_name>
server=<server_name> port=<port_number>
Meaning: Status of file upload.

Message ID: 20101
Severity: Variable
Message: act=upload error=<string> file=<file_name> user=<user_name>
server=<server_name> port=<port_number>
Meaning: File upload error.

Message ID: 20101
Severity: Critical
Message: Fortiguard license is expired
Meaning: Fortiguard license is expired.
Action: Renew FortiGuard license.

Message ID: 22001
Severity: Warning
Message: version-<agent_version_num> is not supported
Meaning: The specified version of the URL agent is not supported.

Message ID:	22002
Severity:	Warning
Message:	Other request - <request_type> than http is not supported
Meaning:	Only HTTP is supported.

Message ID:	22004
Severity:	Warning
Message:	Socket() failed: <string>
Meaning:	The system failed to create a socket or failed to create an HA socket.

Message ID:	22005
Severity:	Warning
Message:	failed to create a <value>/udp socket to receive URL request
Meaning:	The system failed to create a UDP socket to receive URL requests.

Message ID:	22005
Severity:	Warning
Message:	failed to create a <value>/udp socket to relay URL request
Meaning:	The system failed to create a UDP socket to receive URL requests.

Message ID:	22006
Severity:	Warning
Message:	Failed to register for cmdb events.
Meaning:	The system failed to register for cmdb events.

Message ID:	22009
Severity:	Warning
Message:	id=<user_group firewall_policy> status=failure msg="failed to find its AV protection profile"
Meaning:	The specified user group or firewall policy could not find its protection profile.

Message ID:	22010
Severity:	Error
Message:	<string> failed to send rating result
Meaning:	The url filter has failed to send the rating result back to http proxy. The http proxy has crashed.

Message ID: 22100
Severity: Critical
Message: The log disk is going to be full.
Meaning: The log disk is almost out of space.
Action: Clean up the hard disk to create more space.

Message ID: 22800
Severity: Critical
Message: msg="The system has entered conserve mode" conserve=on total=<value> free=<value> entermargin=<value> exitmargin=<value>
Meaning: Scan services entered conserve mode.

Message ID: 22801
Severity: Critical
Message: msg="The system exited conserve mode" conserve=exit total=<value> free=<value> entermargin=<value> exitmargin=<value>
Meaning: Scan services exited conserve mode.

IPSec

The following log messages are generated by IPSec negotiation events.

Message ID: 23001
Severity: Critical
Message: Fortigate report: replay packet is detected, <ip_address_source> -><ip_address_dest>, seq=%ld
Meaning: IPsec negotiation daemon has detected a replay packet from the specified source to the specified destination.
Action: Ensure replay packet is legitimate.

Message ID: 23002
Severity: Notification
Message: loc_ip=<ip_address> loc_port=<port_num> rem_ip=<ip_address> rem_port=<port_num> out_if=<string> vpn_tunnel=<vpn_name> action=negotiate status={success | failure} msg="<string>"
Meaning: IPSec generic negotiation report.

Message ID: 23003
Severity: Notification
Message: loc_ip=<ip_address> loc_port=<port_num> rem_ip=<ip_address> rem_port=<port_num> out_if=<string> vpn_tunnel=<vpn_name> status=negotiate_error msg="<string>"
Meaning: IPsec negotiation error report.

Message ID: 23004
Severity: Notification
Message: loc_ip=<ip_address> loc_port=<port_num> rem_ip=<ip_address>
rem_port=<port_num> out_if=<string> vpn_tunnel=<vpn_name>
action=negotiate init=<string> mode={aggressive | main}
stage=<value_ipsec_stage> dir={inbound | outbound} status={success | failure} msg="<string>"
Meaning: IPsec negotiation progress report.

Message ID: 23005
Severity: Notification
Message: loc_ip=<ip_address> loc_port=<port_num> rem_ip=<ip_address>
rem_port=<port_num> out_if=<string> vpn_tunnel=<vpn_name>
status=packet_replay, spi=<value_index>-.8x, seqno=%u msg="<string>"
Meaning: IPsec negotiation replay report.

Message ID: 23006
Severity: Notification
Message: loc_ip=<ip_address> loc_port=<port_num> rem_ip=<ip_address>
rem_port=<port_num> out_if=<string> vpn_tunnel=<vpn_name>
action=install_sa, in_spi=<value_index>-.8x out_spi=<value_index>-.8x
msg="<string>"
Meaning: An SA has been negotiated and installed successfully.

Message ID: 23007
Severity: Notification
Message: loc_ip=<ip_address> loc_port=<port_num> rem_ip=<ip_address>
rem_port=<port_num> out_if=<string> vpn_tunnel=<vpn_name>
action=delete_phase1_sa, spi=<string> msg="<string>"
Meaning: Deleted IPsec phase1 SA.

Message ID: 23008
Severity: Notification
Message: loc_ip=<ip_address> loc_port=<string> rem_ip=<ip_address>
rem_port=<port_num> out_if=<string> vpn_tunnel=<vpn_name>
action=delete_ipsec_sa, spi=<string> msg="delete ipsec sa"
Meaning: Deleted IPsec SA.

DHCP

The following log message is generated by a DHCP service event.

Message ID: 26001
Severity: Information
Message: dhcp_msg={Discover | Offer | Request | Ack | Release} dir={<sent> | <received>} mac=<mac_address> ip=<ip_address> lease=<lease_time> msg={A client broadcasts a DHCPDISCOVER message | Server responds with offer of configuration parameters | Client requests IP address/configuration parameters | Assigns IP address/configuration parameters to the client | Client relinquishes the IP address and cancelling remaining lease}
Meaning: DHCP requests and response log.

Message ID: 26002
Severity: Error
Message: No shared network for network <ip_address> (<ip_address>).
Meaning: No shared network found.

Message ID: 26002
Severity: Error
Message: Address range<ip_address> to <ip_address>, netmask %s spans %s!
Meaning: Address range spans multiple subnets.

Message ID: 26002
Severity: Error
Message: Address range %s to %s not on net %s/%s!
Meaning: Address range does not belong to the net.

PPP

The following log messages are generated by L2TP, PPTP, and PPPoE service events.

Message ID: 29001
Severity: Variable
Message: user=<user_name> local=<ip_address> remote=<ip_address> assigned=<ip_address> stat=""<string>" msg=""<string>"
Meaning: Pppd log message.

Message ID: 29002
Severity: Information
Message: msg="MGR: Manager process started"
Meaning: Manager process of PPTPd has started.

Message ID: 29003
Severity: Critical
Message: MGR: Couldn't create host socket
Meaning: PPTPd manager failed to create a socket for receiving PPTP requests.

Message ID: 29004
Severity: Warning
Message: MGR: the limit of pptp number has been reached - no more clients can connect!
Meaning: The maximum number of PPTP connections had been reached.

Message ID: 29005
Severity: Warning
Message: MGR: Error with manager select(!)
Meaning: PPTP server encountered an error during polling PPTP requests.

Message ID: 29006
Severity: Warning
Message: MGR: accept() failed
Meaning: PPTP server encountered an error while accepting a PPTP request. One of the likely reasons is that the firewall has run out of resources.

Message ID: 29009
Severity: Notification
Message: gateway_ip=<ip_address> assigned_ip=<ip_address> mtu=<value_bytes>
Meaning: PPPoE status report.

Message ID: 29011
Severity: Error
Message: Can't execute <program_name>: <string>.
Meaning: Pppd cannot execute the specified program.

Message ID: 29012
Severity: Error
Message: <string>
Meaning: PPPd has received the specified wrong option.

Message ID: 29013
Severity: Notification
Message: msg="pppd is started"
Meaning: The specified PPPd has been started.

Message ID: 29014
Severity: Information
Message: msg="pppd is exiting"
Meaning: PPPd is exiting.

Message ID: 29020
Severity: Critical
Message: vfid-<vdom_id> is bigger than the table-<value>\n
Meaning: The returned ID of the virtual domain is invalid.
Action: Ensure the virtual domain of that name is configured in the FortiGate unit.

Message ID: 29021
Severity: Information
Message: pptp of domain-<domain_name> is not configured
Meaning: PPTP for the specified domain is not configured.
Action: Ensure PPTP is configured with an IP address range and user group.

Message ID: 29022
Severity: Warning
Message: All IP address of pptp in domain-<domain_name> are assigned
Meaning: There are no more available IP addresses for the specified domain.
Action: Reassign IP addresses or increase the range.

Message ID: 29024
Severity: Warning
Message: failed to expand pptp config list
Meaning: There is not enough memory to expand the PPTP config list.

Admin

The following log messages are generated by administration events.

Message ID: 32001
Severity: Information
Message: user=LCD ui=LCD action=login status=success reason=none msg="Login from LCD successfully"
Meaning: A user has logged into the system successfully from the LCD.

Message ID: 32002
Severity: Information
Message: user=LCD ui=LCD action=login status=failure reason=passwd_invalid msg="Login from LCD failed"
Meaning: The specified user has failed to log in from the LCD because of an incorrect password.
Action: Ensure administrators and users have the correct passwords.

Message ID: 32005
Severity: Information
Message: user=<administrator_name> ui={GUI | CLI | console | LCD} action=login status=failure reason=<string> msg="User <administrator_name> login failed from {GUI | CLI | console | LCD}"
Meaning: An administrator has failed to log in.
Action: Ensure administrators and users have the correct login information.

Message ID: 32006
Severity: Information
Message: user=<administrator_name> ui={GUI | CLI | console | LCD} action=login status=success reason=none msg="User <administrator_name> login accepted from {GUI | CLI | console | LCD}"
Meaning: The specified administrator has logged in to the system successfully.

Message ID: 32007
Severity: Information
Message: user=<administrator_name> ui={GUI | CLI | console | LCD} action=logout status=success reason=timeout msg="GUI session timeout from <interface_name>"
Meaning: The GUI session of the specified administrator has been dropped because of inactivity (timeout limit reached).

Message ID:	32009
Severity:	Information
Message:	user=<administrator_name> ui={GUI CLI console LCD} action=login status=failure reason=<string> msg=\"User <administrator_name> login failed from {GUI CLI console LCD}\"
Meaning:	The specified administrator has failed to log in after three attempts from either a network address or via a console connection. After five failed login attempts, the Fortinet device automatically terminates the connection.
Action:	Ensure administrators have the correct login information.

Message ID:	32085
Severity:	Warning
Message:	user=LCD ui=LCD action=<action> status=success msg=\"System has been reset to factory default by user LCD via LCD\"
Meaning:	System has been reset to factory default by user LCD via the LCD.

Message ID:	32086
Severity:	Warning
Message:	user=LCD ui=LCD action=<action> status=success msg=\"System has been changed to transparent mode LCD via LCD\"
Meaning:	System has been changed to transparent mode by user LCD via the LCD.

Message ID:	32087
Severity:	Warning
Message:	user=LCD ui=LCD action=<action> status=success msg=\"System has been changed to NAT mode LCD via LCD\"
Meaning:	System has been changed to NAT mode by user LCD via the LCD.

Message ID:	32095
Severity:	Warning
Message:	user=<administrator_name> ui={GUI CLI console LCD} action= {reboot shutdown reload backup factory_reset restore upgrade switch_mode download upload clear_mlog del_log update downgrade del_session bootup} status={success failure} msg=\"<action> by user <administrator_name> via GUI<ip_address>\"
Meaning:	The specified administrator has performed one of the following actions on the firewall via the GUI: reboot, shutdown, reload, backup, factory reset, restore (all types of configuration files), firmware upgrade, switch mode, download (all types of configuration files), upload, clear log in memory buffer, delete log, update virus or IPS signatures, downgrade firmware, delete session, or bootup.

Message ID: 32101
Severity: Notification
Message: user=<administrator_name> ui=< LCD> msg="<string> by <string>"
Meaning: The specified administrator has changed the configuration from the LCD.

Message ID: 32102
Severity: Variable
Message: user=<administrator_name> ui={GUI | CLI | console | LCD}
module=<module_name> submodule=<submodule_name>
msg="<administrator_name> made a change from {GUI | CLI | console | LCD}: <string>"
Meaning: The specified administrator has changed the configuration for the specified sub-module.

Message ID: 32104
Severity: Critical
Message: <string> msg="Fortigate update failed"
Meaning: The FortiGate unit update has failed.
Action: Try the update again.

Message ID: 32120
Severity: Notification
Message: user=<administrator_name> ui={GUI | CLI | console | LCD}
intf=<interface_name> msg="User <administrator_name> added a new interface from {GUI | CLI | console | LCD}"
Meaning: A new interface was added by the specified administrator.

Message ID: 32121
Severity: Notification
Message: user=<administrator_name> ui={GUI | CLI | console | LCD} intf={internal | external | dmz | <other>...} field=ip old=<ip_address>:<ip_mask> new=<ip_address>:<ip_mask> msg="User <administrator_name> changed the setting of an interface from {GUI | CLI | console | LCD}"
user=<administrator_name> ui={GUI | CLI | console | LCD} intf={internal | external | dmz | <other>...} field=access old={HTTPS PING HTTP SSH SNMP TELNET} new={HTTPS PING HTTP SSH SNMP TELNET}
msg="User <administrator_name> changed the setting of an interface from {GUI | CLI | console | LCD}"
Meaning: The administrator changed the specified interface settings from "old" to "new".

Message ID:	32122
Severity:	Notification
Message:	user=<administrator_name> ui={GUI CLI console LCD} intf=<interface_name> msg="User <administrator_name> deleted a interface from {GUI CLI console LCD}"
Meaning:	The administrator deleted the specified interface.

Message ID:	32123
Severity:	Notification
Message:	user=<administrator_name> ui={GUI CLI console LCD} seq=<value_order> device={internal external dmz <other> ... } distance=<value_hops> dst=<ip_address> status={up down} msg="User <administrator_name> added a new static routing entry from {GUI CLI console LCD}{<ip_address>}"
Meaning:	The administrator added the specified static route entry.

Message ID:	32124
Severity:	Notification
Message:	user=<administrator_name> ui={GUI CLI console LCD} seq=<value_order> old_device={internal external dmz <other> ... } old_distance=<value_hops> old_dst=<ip_address> old_status={up down} new_device={internal external dmz <other> ... } new_distance=<value_hops> new_dst=<ip_address> new_status={up down} msg="User <administrator_name> changed the setting of a new static routing entry from {GUI CLI console LCD}"
Meaning:	The administrator made the specified changes to the static route entry.

Message ID:	32125
Severity:	Notification
Message:	user=<administrator_name> ui={GUI CLI console LCD} seq=<value_order> device={internal external dmz <other> ... } distance=<value_hops> dst=<ip_address> status={up down} msg="User <administrator_name> deleted a static routing entry from {GUI CLI console LCD}"
Meaning:	The administrator deleted the specified static route entry.

Message ID:	32126
Severity:	Notification
Message:	user=<administrator_name> ui={GUI CLI console LCD} seq=<order_number> msg="User <administrator_name> added a new firewall policy from {GUI CLI console LCD}"
Meaning:	The administrator added a new firewall policy.

Message ID:	32127
Severity:	Notification
Message:	user=<administrator_name> ui={GUI CLI console LCD} old_sintf=<interface_name> old_dintf=<interface_name> old_saddr=<ip_address> old_daddr=<ip_address> old_schd=<schedule_name> old_svr=<network_service> old_act=<string> old_nat=<string> old_log=<string> new_sintf=<interface_name> new_dintf=<interface_name> new_saddr=<ip_address> new_daddr=<ip_address> new_schd=<schedule_name> new_svr=<network_service> new_act=<string> new_nat=<string> new_log=<string> msg="User <administrator_name> changed a firewall policy from {GUI CLI console LCD}"
Meaning:	The administrator made the specified changes to a firewall policy.

Message ID:	32128
Severity:	Notification
Message:	user=<administrator_name> ui={GUI CLI console LCD} seq=<policy_id> sintf=<interface_name> dintf=<interface_name> saddr=<ip_address> daddr=<ip_address> schd=<schedule_name> svr=<network_service> act=<string> nat=<string> log=<string> msg="User <administrator_name> deleted a firewall policy from {GUI CLI console LCD}"
Meaning:	The administrator deleted a firewall policy.

Message ID:	32129
Severity:	Notification
Message:	user=<administrator_name> ui={GUI CLI console LCD} name=<administrator_name> status={enable disable} msg="User <administrator_name> added a local user from {GUI CLI console LCD}"
Meaning:	The administrator added a new local administrator.

Message ID:	32130
Severity:	Notification
Message:	user=<administrator_name> ui={GUI CLI console LCD} name=<administrator_name> old_status=<string> new_status=<string> passwd=<password> msg="User <administrator_name> changed a local user's setting from {GUI CLI console LCD}"
Meaning:	The administrator changed the specified settings for a local administrator.

Message ID:	32131
Severity:	Notification
Message:	user=<administrator_name> ui={GUI CLI console LCD} name=<administrator_name> status=<string> msg="User <administrator_name> deleted a local user from {GUI CLI console LCD}"
Meaning:	The administrator deleted the specified local administrator from the system.

Message ID:	32132
Severity:	Notification
Message:	user=<administrator_name> ui={GUI CLI console LCD} name=<server_name> server=<server_address> msg="User <administrator_name> added a radius user from {GUI CLI console LCD}"
Meaning:	The administrator added a RADIUS server to the server list.

Message ID:	32133
Severity:	Notification
Message:	user=<administrator_name> ui={GUI CLI console LCD} name=<administrator_name> old_server=<server_address> new_server=<server_address> secret=<server_secret> msg="User <administrator_name> changed a radius' setting user from {GUI CLI console LCD}"
Meaning:	The administrator made the specified changes to the RADIUS server entry.

Message ID:	32134
Severity:	Notification
Message:	user=<administrator_name> ui={GUI CLI console LCD} name=<administrator_name> server=<server_address> msg="User <administrator_name> deleted a radius user from {GUI CLI console LCD}"
Meaning:	The administrator deleted the RADIUS server from the server list.

Message ID:	32135
Severity:	Notification
Message:	user=<administrator_name> ui={GUI CLI console LCD} name=<server_name> server=<server_address> msg="User <administrator_name> added a ldap user from {GUI CLI console LCD}"
Meaning:	The administrator added a new LDAP server to the list.

Message ID:	32136
Severity:	Notification
Message:	user=<administrator_name> ui={GUI CLI console LCD} name=<administrator_name> old_server=<server_address> old_port=<port_num> old_cn=<value_cn> old_dn="<dn_name> new_server=<server_address> new_port=<port_num> new_cn=<value_cn> new_dn="<dn_name>" msg="User <administrator_name> changed a ldap user's setting from {GUI CLI console LCD}"
Meaning:	The administrator made the specified changes to an LDAP server entry.

Message ID: 32137
Severity: Notification
Message: user=<administrator_name> ui={GUI | CLI | console | LCD}
name=<administrator_name> server=<server_address> msg="User
<administrator_name> deleted a ldap user from {GUI | CLI | console | LCD}"
Meaning: The administrator deleted the LDAP server from the list.

Message ID: 32138
Severity: Critical
Message: user=<administrator_name> ui={GUI | CLI | console | LCD | ha_daemon}
action=reboot msg="\User <administrator_name> rebooted the device from
{GUI | CLI | console | LCD}"
user=<administrator_name> ui={GUI | CLI | console | LCD}
action=shutdown msg="\User <administrator_name> shut down the device
from {GUI | CLI | console | LCD | ha_daemon}"
Meaning: The administrator rebooted the FortiGate unit.
The administrator shut down the FortiGate unit.
Action: None.

Message ID:	32139
Severity:	Critical
Message:	<pre> user=<administrator_name> ui={GUI CLI console LCD} action=factory- reset msg=\"User <administrator_name> reset to the factory settings from {GUI CLI console LCD}\" user=<administrator_name> ui={GUI CLI console LCD} action=format- disk msg=\"User <administrator_name> formatted the log disk from {GUI CLI console LCD}\" user=<administrator_name> ui={GUI CLI console LCD} action=restore- image msg=\"User <administrator_name> restored the image from {GUI CLI console LCD}\" user=<administrator_name> ui={GUI CLI console LCD} action=restore- configuration msg=\"User <administrator_name> restored the configuration from {GUI CLI console LCD}\" user=<administrator_name> ui={GUI CLI console LCD} action=import- certificate msg=\"User <administrator_name> imported the certificate from {GUI CLI console LCD}\" user=<administrator_name> ui={GUI CLI console LCD} action=restore- all-configuration msg=\"User <administrator_name> restored all the configuration from {GUI CLI console LCD}\" user=<administrator_name> ui={GUI CLI console LCD} action=update msg=\"User <administrator_name> updated the firmware from {GUI CLI console LCD}\" user=<administrator_name> ui={GUI CLI console LCD} action=loaded- image msg=\"User <administrator_name> loaded an image from {GUI CLI console LCD}, the new image has an invalid RSA signature.\" user=<administrator_name> ui={GUI CLI console LCD} action=loaded- image msg=\"User <administrator_name> loaded an image from {GUI CLI console LCD}, the new image does have a valid RSA signature with new public key.\" user=<administrator_name> ui={GUI CLI console LCD} action=loaded- image msg=\"User <administrator_name> loaded an image from {GUI CLI console LCD}, the new image does have a valid RSA signature.\" user=<administrator_name> ui={GUI CLI console LCD} action=loaded- image msg=\"User <administrator_name> loaded an image from {GUI CLI console LCD}, the new image does not have a valid RSA signature. user=<administrator_name> ui={GUI CLI console LCD} action=loaded- image msg=\"User <administrator_name> loaded the image from {GUI CLI console LCD}, the new image has RSA signature with new key.\" </pre>
Meaning:	<p>The administrator performed a reset to factory default settings.</p> <p>The administrator formatted the local disk.</p> <p>The administrator restored the firmware image.</p> <p>The administrator restored a backed up configuration.</p> <p>The administrator imported a certificate.</p> <p>The administrator restored a complete configuration.</p> <p>The administrator updated the firmware.</p> <p>The administrator uploaded an image with an invalid RSA signature.</p> <p>The administrator uploaded an image with a valid RSA signature and new public key.</p> <p>The administrator uploaded an image with a valid RSA signature.</p> <p>The administrator uploaded an image that does not have a valid RSA signature.</p> <p>The administrator uploaded an image that contains a RSA signature with a new key.</p>
Action:	None.

Message ID: 32140
Severity: Notification
Message: user=<administrator_name> ui={GUI | CLI | console | LCD} field=mode | virtual-domain | hostname | ip-overlap | auth-timeout | detection-interval old_value=<value_ip_overlap> new_value=<value> msg="User <administrator_name> changed global setting from {GUI | CLI | console | LCD}"
Meaning: The administrator has changed the global setting specified in the 'field' field.

Message ID: 32141
Severity: Variable
Message: id=<id_value> msg=<message_string>
Meaning: DHCPD log information.

Message ID: 32142
Severity: Critical
Message: user=<administrator_name> ui={GUI | CLI | console | LCD} action=backup msg="User <administrator_name> backed up the configuration from {GUI | CLI | console | LCD}"
Meaning: The administrator backed up the current configuration to a file.

Message ID: 32143
Severity: Critical
Message: user=<administrator_name> ui={GUI | CLI | console | LCD} action=loaded-image msg="User <administrator_name> loaded a wrong image from {GUI | CLI | console | LCD}."
Meaning: The administrator loaded the wrong image type.

Message ID: 32144
Severity: Notification
Message: user=<administrator_name> ui={GUI | CLI | console | LCD} iff=<incoming_interface> src=<ip_address> dst=<ip_address> proto=<protocol_num> ports=<port_range> off=<outgoing_interface> qw=<gateway_ip_address> msg="User <administrator_name> added a policy routing entry."
Meaning: An administrator added a policy routing entry.

Message ID:	32145
Severity:	Notification
Message:	user=<administrator_name> ui={GUI CLI console LCD} iff=<something> src=<ip_address> dst=<ip_address> proto=<protocol_num> ports=<port_range> off=<something> qw=<gateway_ip_address> msg="User <administrator_name> deleted a policy routing entry."
Meaning:	An administrator deleted a policy routing entry.

Message ID:	32146
Severity:	Notification
Message:	user=<administrator_name> ui={GUI CLI console LCD} old_pattern=<url_address> old_status={enable disable} new_pattern=<url_address> new_status={enable disable} msg="User <administrator_name> changed a url pattern entry."
Meaning:	An administrator changed a web block url pattern.

Message ID:	32147
Severity:	Notification
Message:	user=<administrator_name> ui={GUI CLI console LCD} old_pattern=<url_address> pattern=<url_address> status={enable disable} msg="User <administrator_name> added a url pattern entry."
Meaning:	An administrator added a web block url pattern.

Message ID:	32148
Severity:	Notification
Message:	user=<administrator_name> ui={GUI CLI console LCD} old_pattern=<url_address> pattern=<url_address> status={enable disable} msg="User <administrator_name> deleted a url pattern entry."
Meaning:	An administrator deleted a web block url pattern.

Message ID:	32149
Severity:	Notification
Message:	user=<administrator_name> ui={GUI CLI console LCD} old_url=<url_address> old_status={enable disable} new_url<url_address> new_status={enable disable} msg="User <administrator_name> changed a url block entry."
Meaning:	An administrator changed a url block entry.

Message ID:	32150
Severity:	Notice
Message:	user=<administrator_name> ui={GUI CLI console LCD} msg="User <administrator_name> added protection profile <protectin_profile_name>."
Meaning:	An administrator has added a new protection profile to the FortiGate unit.

Message ID:	32151
Severity:	Notice
Message:	user=<administrator_name> ui={GUI CLI console LCD} url=<url_address> status={enable disable} msg="User <administrator_name> deleted a url block entry."
Meaning:	An administrator has deleted a url block entry.

Message ID:	32152
Severity:	Notice
Message:	user=<administrator_name> ui={GUI CLI console LCD} old_url=<url_address> old_status={enable disable} new_url<url_address> new_status={enable disable} msg="User <administrator_name> changed an exempt url entry.
Meaning:	An administrator has deleted an exempt url entry.

Message ID:	32153
Severity:	Notification
Message:	user=<administrator_name> ui={GUI CLI console LCD} url=<url_address> status={enable disable} msg="User <administrator_name> added an exempt url entry.
Meaning:	An administrator added an exempt url entry.

Message ID:	32154
Severity:	Notification
Message:	user=<administrator_name> ui={GUI CLI console LCD} url=<url_address> status={enable disable} msg="User <administrator_name> deleted an exempt url entry.
Meaning:	An administrator deleted an exempt url entry.

Message ID:	32155
Severity:	Notification
Message:	user=<administrator_name> ui={GUI CLI console LCD} msg="User <administrator_name> changed a FortiGuard setting.
Meaning:	An administrator changed a FortiGuard configuration setting.

Message ID: 32156
Severity: Notification
Message: user=<administrator_name> ui={GUI | CLI | console | LCD} old_word=<word> old_lang=<language> old_type={wildcard | regular expression} old_satus={enable | disable} new_word=<word> new_lang=<language> new_type={wildcard | regular expression} new_satus={enable | disable} msg="User <administrator_name> changed a ban word entry."
Meaning: An administrator changed the settings for a banned word.

Message ID: 32157
Severity: Notification
Message: user=<administrator_name> ui={GUI | CLI | console | LCD} word=<word> lang=<language> type={wildcard | regular expression} satus={enable | disable} msg="User <administrator_name> added a ban word entry."
Meaning: An administrator added a word to the banned list.

Message ID: 32158
Severity: Notification
Message: user=<administrator_name> ui={GUI | CLI | console | LCD} word=<word> lang=<language> type={wildcard | regular expression} satus={enable | disable} msg="User <administrator_name> deleted a ban word entry."
Meaning: An administrator deleted a word to the banned list.

Message ID: 32200
Severity: Notification
Message: user=<administrator_name> ui={GUI | CLI | console | LCD} upload={url-exempt-list | url-block-list | word-block-list} num=<value> msg="User <administrator_name> uploaded URL block list from {GUI | CLI | console | LCD}"
Meaning: The administrator has uploaded the new web filter list specified in the 'upload' field.

Message ID: 32545
Severity: Critical
Message: user=<none> ui=<none> action=<reboot> msg="System will reboot due to scheduled daily restart. Current time is <hour>:<minute>"
Meaning: System restart.

HA

The following log messages are generated by high availability activity.

Message ID: 35001
Severity: Notification
Message: msg="HA group id changed to<value_ha_id>."
HA slave became master
HA move to standalone mode
HA move to work status
HA master became slave
HA move to standby state
Detected HA member dead
Detected new joined HA member
Meaning: As described in message.

Message ID: 35001
Severity: Warning
Message: HA monitored interface <interface_name> link failed
Meaning: The specified monitored interface on this cluster unit failed or was disconnected. This message is only displayed if an interface configured with a HA monitor priority fails or is disconnected.

Message ID: 35010
Severity: Critical
Message: msg="HA mode changed to standalone"
Meaning: HA mode changed to standalone.

Message ID: 35011
Severity: Critical
Message: msg="HA mode changed to A-A"
Meaning: HA mode changed to Active-Active.

Message ID: 35012
Severity: Critical
Message: msg="HA mode changed to A-P"
Meaning: HA mode changed to Active-Passive.

Message ID: 35013
Severity: Critical
Message: msg="HA mode changed to unknown"
Meaning: HA mode changed to unknown.

Auth

The following log messages are generated by firewall authentication events.

Message ID: 38001
Severity: Warning
Message: user=<administrator_name> service=<network_service> action=no
status=failure reason=timeout src=<ip_address> srcname=n/a
dst=<ip_address> dstname=n/a
Meaning: The specified administrator has failed to get authenticated before timeout occurred.
Action: Ensure administrators have the correct login information and have access to the FortiGate unit.

Message ID: 38002
Severity: Information
Message: user=<administrator_name> service=<network_service> action=<action>
status=success reason=none src=<ip_address> srcname=n/a
dst=<ip_address> dstname=n/a
Meaning: The specified administrator was authenticated successfully.

Message ID: 38003
Severity: Warning
Message: user=<administrator_name> service=<network_service> action=<action>
status=failure reason=<string> src=<ip_address> srcname=n/a
dst=<ip_address> dstname=n/a
Meaning: The specified administrator failed to get authenticated because of the specified reason.
Action: Ensure administrators have the correct login information and have access to the FortiGate unit.

Message ID: 42103
Severity: Notice
Message: msg="Fortigate updated successfully"
Meaning: Administrator has successfully updated FortiGate antivirus database.

Message ID: 42103
Severity: Notice
Message: msg="Fortigate updated successfully"
Meaning: Administrator has successfully updated FortiGate IDS database.

Chassis

The following log messages are generated by FortiGate-4000 and FortiGate-5000 series chassis events.

Message ID: 99503
Severity: Variable (Warning or Critical)
Message: Chassis fan anomaly: Fan %d, %d RPM Chassis fan anomaly
Meaning: The chassis fan is spinning at an RPM value outside of the operating range.

Message ID: 99504
Severity: Variable (Warning or Critical)
Message: Chassis temperature anomaly: T <celsius_integer> Celsius Chassis temperature anomaly
Meaning: The chassis temperature is outside of the operating range.

Message ID: 99505
Severity: Variable (Warning or Critical)
Message: Chassis voltage anomaly: <V3.3 | V5 | V12>, <voltage_integer> V Chassis voltage anomaly
Meaning: The chassis voltage level is outside of the operating range. The FortiGate unit reads 3 voltage points: 3.3V, 5V, and 12V.

Message ID: 99506
Severity: Variable (Warning or Critical)
Message: Blade fan anomaly: Blade <blade_integer>, <rpm_integer> RPM Blade fan anomaly
Meaning: The specified blade fan is spinning at an RPM value outside of the operating range.

Message ID: 99507
Severity: Critical
Message: Card 5001 in slot <slot_integer> has a temperature of <celsius_integer> Celsius.
Meaning: The 5001 blade has reached the indicated temperature outside of the operating range.

Message ID: 99507
Severity: Critical
Message: Card 5003 in slot <slot_integer> has {Baseboard | Top BRD | Bottom BRD | Center BRD} temperature of <celsius_integer> Celsius.
Meaning: The 5003 blade has reached the indicated temperature outside of the operating range.

Message ID: 99508
Severity: Critical
Message: Card 5001 in slot <slot_integer>, has voltage {1.5v | 1.8v | 2.5v | 3.3v | 5v} = <voltage_integer>.
Meaning: The 5001 blade is producing the indicated voltage outside of the indicated operating voltage range.

Message ID: 99508
Severity: Critical
Message: Card 5003 in slot <slot_integer>, has voltage {1.5v | 2.0v | 2.5v | 3.3v | 3.3VSB | 5VSB | 12v} = <voltage_integer>.
Meaning: The 5003 blade is producing the indicated voltage outside of the indicated operating voltage range.

Message ID: 99509
Severity: Notice
Message: chassisd failed to create the cmd pipe:
mkfifo(CHASSIS_CMD_PIPE_NAME) %s chassisd failed to create the cmd pipe
chassisd failed to open the cmd pipe: open(CHASSIS_CMD_PIPE_NAME) %s chassisd failed to open the cmd pipe
chassisd failed to create the shared memory segment:
shmget(CHASSIS_STATUS_SHM_KEY) %s chassisd failed to create the shared memory segment
chassisd failed to attach to the shared memory segment:
shmat(CHASSIS_STATUS_SHM_KEY) %s chassisd failed to attach to the shared memory segment
Meaning: As indicated. Software errors may prevent proper system monitoring.
Action: Reboot the FortiGate unit.

Antivirus log messages

Infected

The following log messages are generated by virus detections.

Message ID:	60001
Severity:	Warning
Message:	File <file name> is infected.
Meaning:	The specified file is infected with a virus detected by the FortiGate unit.
Action:	Ensure virus is cleaned and alerts issued.

Attack log messages

Signature

The following log message is generated when an attack signature is found.

Message ID:	70000
Severity:	Alert
Message:	attack_id=<value_attack_id> src=<ip_address> dst=<ip_address> src_port=<port_num> dst_port=<port_num> interface=<interface_name> src_int=<interface_name> dst_int=<interface_name> status={clear_session detected dropped reset drop_session pass_session reset_client reset_server} proto=<protocol_num> service=<network_service> msg="<string>"
Meaning:	Attack signature message providing the source and destination addressing information. Look up the attack ID in the Fortinet Attack Encyclopedia for more information about the signature.
Action:	Get more information about the attack and the steps to take from the Fortinet Attack Encyclopedia in the FortiProtect Center. Analyze logs as required.

Anomaly

The following log message is generated when an attack anomaly is detected.

Message ID:	73001
Severity:	Critical
Message:	attack_id=<value_attack_id> src=<ip_address> dst=<ip_address> src_port=<port_num> dst_port=<port_num> interface=<interface_name> src_int=<interface_name> dst_int=<interface_name> status={clear_session detected dropped reset drop_session pass_session reset_client reset_server} proto=<protocol_num> service=<network_service> msg="<string>"
Meaning:	Attack anomaly message providing the source and destination addressing information. Look up the attack ID in the Fortinet Attack Encyclopedia for more information about the anomaly.
Action:	Get more information about the attack and the steps to take from the Fortinet Attack Encyclopedia in the FortiProtect Center. Analyze logs as required.

Web filter log messages

Urlblock

The following log message is generated when a Web page is blocked because it is on the Web filter URL block list.

Message ID: 93001
Severity: Variable
Message: src=<ip_address> dst=<ip_address> src_int=<interface_name>
dst_int=<interface_name> service=<network_service> status=blocked
msg="<string>"
Meaning: The specified URL was blocked because it is in the URL blacklist.

Message ID: 93002
Severity: Notice
Message: user=<user_id> src=<ip_address> srcport=<port_num> dst=<ip_address>
dstport=<port_num> service=http hostname=<url> status=blocked
msg="URL is blocked because it is in URL block/pattern list"
Meaning: The specified URL was blocked because it is in the URL blacklist.

Message ID: 93003
Severity: Info
Message: user=<user_id> src=<ip_address> srcport=<port_num> dst=<ip_address>
dstport=<port_num> service=http hostname=<url> status=passthrough
msg="Policy allows URLs when a rating error occurs"
Meaning: A rating error occurred and the policy allows URLs when a rating error occurs

Message ID: 93006
Severity: Critical
Message: hostname=<url> msg="gethostbyname() failed: <hostname>"
Meaning: Cannot resolve the name of the FortiGuard server.
Action: Check settings.

Message ID: 93007
Severity: Critical
Message: msg="calloc() failed: <hostname>"
Meaning: Insufficient resources.
Action: Delete logs to free some memory.

Message ID: 93009
Severity: Critical
Message: hostname=<url> msg="gethostbyname() failed: <hostname>"
Meaning: Cannot resolve the name of the FortiGuard server.
Action: Check settings.

Message ID:	93013
Severity:	Critical
Message:	Category block is enabled but no rating server is enabled.
Meaning:	Category block is enabled but no rating server is enabled.

Urlexempt

The following log messages are generated when a Web page is passed through because it is on the Web filter URL exempt list.

Message ID:	96002
Severity:	Info
Message:	hostname: <url> is found in the local exempt list\n
Meaning:	The specified host/domain name was allowed because it is in the URL exempt list.

Catblock

The following log messages are generated when category blocking is enabled and Web pages are being filtered.

Message ID:	99000 – 99500
Severity:	Information
Message:	hostname=<domain_name> ip=<ip_address> port=<port_num>, result=<string>, code=<value_rating_code>, msg=<string>
Meaning:	An error has occurred while retrieving a rating. The IP address and port number are those of the rating server. The message indicates what kind of error occurred.

Message ID:	99501
Severity:	Information
Message:	src=<ip_address> dst=<ip_address> src_int=<interface_name> dst_int=<interface_name> service=http status=<string> profile=<prot_profile> cat=<category_num> cat_desc=<string> url=http://<url_address> msg=<string>
Meaning:	A Web site was blocked by the Web category filtering service. The client and server addresses, the protection profile applied, and the category and URL that was blocked are listed in the log message.

Message ID:	99502
Severity:	Information
Message:	src=<ip_address> dst=<ip_address> src_int=<interface_name> dst_int=<interface_name> service=http status=<string> profile=<prot_profile> cat=<category_num> cat_desc=<string> url=<url> msg=<string>
Meaning:	A Web site was monitored by the Web category filtering service. The client and server addresses, the protection profile applied, and the category and URL that was monitored are listed in the log message.

Spam filter log messages

SMTP

The following log messages are generated when email messages in SMTP traffic are blocked by a component of the spam filter.

Message ID:	80000
Severity:	Notification
Message:	src=<ip_address> dst=<ip_address> src_int=<interface_name> dst_int=<interface_name> service=SMTP status=detected msg="from ip is in ip blacklist"
Meaning:	The email message from the specified source was blocked because the source IP address is marked as spam by the IP address list.

Message ID:	80001
Severity:	Notification
Message:	src=<ip_address> dst=<ip_address> src_int=<interface_name> dst_int=<interface_name> service=SMTP status=detected msg="from ip is in dnsbl/ordbl"
Meaning:	The email message from the specified source was blocked because the source IP address is on an DNSBL or an ORDBL.

Message ID:	80002
Severity:	Notification
Message:	src=<ip_address> dst=<ip_address> src_int=<interface_name> dst_int=<interface_name> service=SMTP status=detected msg="smtp helo/helo domain name DNS check failed."
Meaning:	The email message from the specified source was blocked because the source domain name in the SMTP HELO command did not match the Domain Name Server.

Message ID: 80003
Severity: Notification
Message: src=<ip_address> dst=<ip_address> src_int=<interface_name>
dst_int=<interface_name> service=SMTP status=detected msg="from email
address is in email blacklist."
Meaning: The email message from the specified source was blocked because the
source email address is marked as spam by the email address list.

Message ID: 80004
Severity: Notification
Message: src=<ip_address> dst=<ip_address> src_int=<interface_name>
dst_int=<interface_name> service=SMTP status=detected msg="the email
contains banned header"
Meaning: The email message from the specified source was blocked because the
MIME header contains a value marked as spam by the MIME headers list.

Message ID: 80005
Severity: Notification
Message: src=<ip_address> dst=<ip_address> src_int=<interface_name>
dst_int=<interface_name> service=SMTP status=detected msg="smtp
helo/ehlo domain name DNS check failed."
Meaning: The email message from the specified source was blocked because the
domain name of the reply-to or from address does not have an A or MX
record on the DNS server.

Message ID: 80006
Severity: Notification
Message: src=<ip_address> dst=<ip_address> src_int=<interface_name>
dst_int=<interface_name> service=SMTP status=detected msg="The email
contains banned word(s)."
Meaning: The email message from the specified source was blocked because it
contains a word from the banned word list.

POP3

The following log messages are generated when email messages in POP3 traffic are blocked by a component of the spam filter.

Message ID: 83000
Severity: Notification
Message: src=<ip_address> dst=<ip_address> src_int=<interface_name>
dst_int=<interface_name> service=POP3 status=detected msg="from ip is
in ip blacklist"
Meaning: The email message from the specified source was blocked because the
source IP address is marked as spam by the IP address list.

Message ID: 83001
Severity: Notification
Message: src=<ip_address> dst=<ip_address> src_int=<interface_name>
dst_int=<interface_name> service=POP3 status=detected msg="from ip is
in dnsbl/ordbl"
Meaning: The email message from the specified source was blocked because the
source IP address is on an DNSBL or an ORDBL.

Message ID: 83002
Severity: Notification
Message: src=<ip_address> dst=<ip_address> src_int=<interface_name>
dst_int=<interface_name> service=POP3 status=detected msg="smtp
helo/ehlo domain name DNS check failed."
Meaning: The email message from the specified source was blocked because the
source domain name in the SMTP HELO command did not match the
Domain Name Server.

Message ID: 83003
Severity: Notification
Message: src=<ip_address> dst=<ip_address> src_int=<interface_name>
dst_int=<interface_name> service=POP3 status=detected msg="from email
address is in email blacklist."
Meaning: The email message from the specified source was blocked because the
source email address is marked as spam by the email address list.

Message ID: 83004
Severity: Notification
Message: src=<ip_address> dst=<ip_address> src_int=<interface_name>
dst_int=<interface_name> service=POP3 status=detected msg="the email
contains banned header"
Meaning: The email message from the specified source was blocked because the
MIME header contains a value marked as spam by the MIME headers list.

Message ID: 83005
Severity: Notification
Message: src=<ip_address> dst=<ip_address> src_int=<interface_name> dst_int=<interface_name> service=POP3 status=detected msg="smtp helo/ehlo domain name DNS check failed."
Meaning: The email message from the specified source was blocked because the domain name of the reply-to or from address does not have an A or MX record on the DNS server.

Message ID: 83006
Severity: Notification
Message: src=<ip_address> dst=<ip_address> src_int=<interface_name> dst_int=<interface_name> service=POP3 status=detected msg="The email contains banned word(s)."
Meaning: The email message from the specified source was blocked because it contains a word from the banned word list.

IMAP

The following log messages are generated when email messages in IMAP traffic are blocked by a component of the spam filter.

Message ID: 86000
Severity: Notification
Message: src=<ip_address> dst=<ip_address> src_int=<interface_name> dst_int=<interface_name> service=IMAP status=detected msg="from ip is in ip blacklist"
Meaning: The email message from the specified source was blocked because the source IP address is marked as spam by the IP address list.

Message ID: 86001
Severity: Notification
Message: src=<ip_address> dst=<ip_address> src_int=<interface_name> dst_int=<interface_name> service=IMAP status=detected msg="from ip is in dnsbl/ordbl"
Meaning: The email message from the specified source was blocked because the source IP address is on an DNSBL or an ORDBL.

Message ID: 86002
Severity: Notification
Message: src=<ip_address> dst=<ip_address> src_int=<interface_name> dst_int=<interface_name> service=IMAP status=detected msg="smtp helo/ehlo domain name DNS check failed."
Meaning: The email message from the specified source was blocked because the source domain name in the SMTP HELO command did not match the Domain Name Server.

Message ID: 86003
Severity: Notification
Message: src=<ip_address> dst=<ip_address> src_int=<interface_name>
dst_int=<interface_name> service=IMAP status=detected msg="from email
address is in email blacklist."
Meaning: The email message from the specified source was blocked because the
source email address is marked as spam by the email address list.

Message ID: 86004
Severity: Notification
Message: src=<ip_address> dst=<ip_address> src_int=<interface_name>
dst_int=<interface_name> service=IMAP status=detected msg="the email
contains banned header"
Meaning: The email message from the specified source was blocked because the
MIME header contains a value marked as spam by the MIME headers list.

Message ID: 86005
Severity: Notification
Message: src=<ip_address> dst=<ip_address> src_int=<interface_name>
dst_int=<interface_name> service=IMAP status=detected msg="smtp
helo/ehlo domain name DNS check failed."
Meaning: The email message from the specified source was blocked because the
domain name of the reply-to or from address does not have an A or MX
record on the DNS server.

Message ID: 86006
Severity: Notification
Message: src=<ip_address> dst=<ip_address> src_int=<interface_name>
dst_int=<interface_name> service=IMAP status=detected msg="The email
contains banned word(s)."
Meaning: The email message from the specified source was blocked because it
contains a word from the banned word list.

Content archive messages

The FortiGate unit archives content meta-data for web and email traffic content.

HTTP

The following message is generated when archiving HTTP meta-data.

Message ID: 06250
Severity: Information
Message: <ContLogVersionNo>:<SessionNo>:<clientIP><-><serverIP>:
 <infectionStatus>:<RequestSize>/<ResponseSize>:<HTTPrequest>

Meaning:

FTP

The following message is generated when archiving FTP meta-data.

Message ID: 06260
Severity: Information
Message: <ContLogVersionNo>:<SessionNo>:<clientIP><-><serverIP>:
 <infectionStatus>:<RequestSize>/<ResponseSize>:<FTPcommand>

SMTP

The following message is generated when archiving SMTP meta-data.

Message ID: 06270
Severity: Information
Message: <ContLogVersionNo>:<SessionNo>:
 <clientIP><-><serverIP>:<infectionStatus>:
 <SizeSent>:f/t=<from/to>:<attachment(1=yes, 0=no)>

POP3

The following message is generated when archiving POP3 meta-data.

Message ID: 06280
Severity: Information
Message: <ContLogVersionNo>:<SessionNo>:
 <clientIP><-><serverIP>:<infectionStatus>:
 <SizeSent>:f/t=<from/to>:<attachment(1=yes, 0=no)>

IMAP

The following message is generated when archiving IMAP meta-data.

Message ID: 06290
Severity: Information
Message: <ContLogVersionNo>:<SessionNo>:
<clientIP><-><serverIP>:<infectionStatus>:
<SizeSent>:f/t=<from/to>:<attachment (1=yes, 0=no)>

Glossary

Connection: A link between machines, applications, processes, and so on that can be logical, physical, or both.

DMZ, Demilitarized Zone: Used to host Internet services without allowing unauthorized access to an internal (private) network. Typically, the DMZ contains servers accessible to Internet traffic, such as Web (HTTP) servers, FTP servers, SMTP (email) servers and DNS servers.

DMZ interface: The FortiGate interface that is connected to a DMZ network.

DNS, Domain Name Service: A service that converts symbolic node names to IP addresses.

Ethernet: A local-area network (LAN) architecture that uses a bus or star topology and supports data transfer rates of 10 Mbps. Ethernet is one of the most widely implemented LAN standards. A newer version of Ethernet, called 100 Base-T (or Fast Ethernet), supports data transfer rates of 100 Mbps. And the newest version, Gigabit Ethernet, supports data rates of 1 gigabit (1,000 megabits) per second.

External interface: The FortiGate interface that is connected to the Internet.

FTP, File transfer Protocol: An application and TCP/IP protocol used to upload or download files.

Gateway: A combination of hardware and software that links different networks. Gateways between TCP/IP networks, for example, can link different subnetworks.

HTTP, Hyper Text Transfer Protocol: The protocol used by the World Wide Web. HTTP defines how messages are formatted and transmitted, and what actions Web servers and browsers should take in response to various commands.

HTTPS: The SSL protocol for transmitting private documents over the Internet using a Web browser.

Internal interface: The FortiGate interface that is connected to an internal (private) network.

Internet: A collection of networks connected together that span the entire globe using the NFSNET as their backbone. As a generic term, it refers to any collection of interdependent networks.

ICMP, Internet Control Message Protocol: Part of the Internet Protocol (IP) that allows for the generation of error messages, test packets, and information messages relating to IP. This is the protocol used by the ping function when sending ICMP Echo Requests to a network host.

IKE, Internet Key Exchange: A method of automatically exchanging authentication and encryption keys between two secure servers.

IMAP, Internet Message Access Protocol: An Internet email protocol that allows access to your email from any IMAP compatible browser. With IMAP, your mail resides on the server.

IP, Internet Protocol: The component of TCP/IP that handles routing.

IP Address: An identifier for a computer or device on a TCP/IP network. An IP address is a 32-bit numeric address written as four numbers separated by periods. Each number can be zero to 255.

L2TP, Layer Two (2) Tunneling Protocol: An extension to the PPTP protocol that enables ISPs to operate Virtual Private Networks (VPNs). L2TP merges PPTP from Microsoft and L2F from Cisco Systems. To create an L2TP VPN, your ISP's routers must support L2TP.

IPSec, Internet Protocol Security: A set of protocols that support secure exchange of packets at the IP layer. IPSec is most often used to support VPNs.

LAN, Local Area Network: A computer network that spans a relatively small area. Most LANs connect workstations and personal computers. Each computer on a LAN is able to access data and devices anywhere on the LAN. This means that many users can share data as well as physical resources such as printers.

MAC address, Media Access Control address: A hardware address that uniquely identifies each node of a network.

MIB, Management Information Base: A database of objects that can be monitored by an SNMP network manager.

Modem: A device that converts digital signals into analog signals and back again for transmission over telephone lines.

MTU, Maximum Transmission Unit: The largest physical packet size, measured in bytes, that a network can transmit. Any packets larger than the MTU are divided into smaller packets before being sent. Ideally, you want the MTU your network produces to be the same as the smallest MTU of all the networks between your machine and a message's final destination. If your messages are larger than one of the intervening MTUs, they get broken up (fragmented), which slows down transmission speeds.

Netmask: Also called subnet mask. A set of rules for omitting parts of a complete IP address to reach a target destination without using a broadcast message. It can indicate a subnetwork portion of a larger network in TCP/IP. Sometimes referred to as an Address Mask.

NTP, Network Time Protocol: Used to synchronize the time of a computer to an NTP server. NTP provides accuracies to within tens of milliseconds across the Internet relative to Coordinated Universal Time (UTC).

Packet: A piece of a message transmitted over a packet-switching network. One of the key features of a packet is that it contains the destination address in addition to the data. In IP networks, packets are often called datagrams.

Ping, Packet Internet Grouper: A utility used to determine whether a specific IP address is accessible. It works by sending a packet to the specified address and waiting for a reply.

POP3, Post Office Protocol: A protocol used to transfer email from a mail server to a mail client across the Internet. Most email clients use POP.

PPP, Point-to-Point Protocol: A TCP/IP protocol that provides host-to-network and router-to-router connections.

PPTP, Point-to-Point Tunneling Protocol: A Windows-based technology for creating VPNs. PPTP is supported by Windows 98, 2000, and XP. To create a PPTP VPN, your ISP's routers must support PPTP.

Port: In TCP/IP and UDP networks, a port is an endpoint to a logical connection. The port number identifies what type of port it is. For example, port 80 is used for HTTP traffic.

Protocol: An agreed-upon format for transmitting data between two devices. The protocol determines the type of error checking to be used, the data compression method (if any), how the sending device indicates that it has finished sending a message, and how the receiving device indicates that it has received a message.

RADIUS, Remote Authentication Dial-In User Service: An authentication and accounting system used by many Internet Service Providers (ISPs). When users dial into an ISP they enter a user name and password. This information is passed to a RADIUS server, which checks that the information is correct, and then authorizes access to the ISP system.

Router: A device that connects LANs into an internal network and routes traffic between them.

Routing: The process of determining a path to use to send data to its destination.

Routing table: A list of valid paths through which data can be transmitted.

Server: An application that answers requests from other devices (clients). Used as a generic term for any device that provides services to the rest of the network such as printing, high capacity storage, and network access.

SMTP, Simple Mail Transfer Protocol: In TCP/IP networks, this is an application for providing mail delivery services.

SNMP, Simple Network Management Protocol: A set of protocols for managing networks. SNMP works by sending messages to different parts of a network. SNMP-compliant devices, called agents, store data about themselves in Management Information Bases (MIBs) and return this data to the SNMP requesters.

SSH, Secure shell: A secure Telnet replacement that you can use to log into another computer over a network and run commands. SSH provides strong secure authentication and secure communications over insecure channels.

Subnet: A portion of a network that shares a common address component. On TCP/IP networks, subnets are defined as all devices whose IP addresses have the same prefix. For example, all devices with IP addresses that start with 100.100.100. would be part of the same subnet. Dividing a network into subnets is useful for both security and performance reasons. IP networks are divided using a subnet mask.

Subnet Address: The part of the IP address that identifies the subnetwork.

TCP, Transmission Control Protocol: One of the main protocols in TCP/IP networks. TCP guarantees delivery of data and also guarantees that packets will be delivered in the same order in which they were sent.

UDP, User Datagram Protocol: A connectionless protocol that, like TCP, runs on top of IP networks. Unlike TCP, UDP provides very few error recovery services, offering instead a direct way to send and receive datagrams over an IP network. It is used primarily for broadcasting messages over a network.

VPN, Virtual Private Network: A network that links private networks over the Internet. VPNs use encryption and other security mechanisms to ensure that only authorized users can access the network and that data cannot be intercepted.

Virus: A computer program that attaches itself to other programs, spreading itself through computers or networks by this mechanism usually with harmful intent.

Worm: A program or algorithm that replicates itself over a computer network, usually through email, and performs malicious actions, such as using up the computer's resources and possibly shutting the system down.

Index

A

- access 13
- accessing
 - messages on the disk 13
- admin event log messages 44
- alert email
 - configuring 11
 - options 10
- alert, logging severity level 19
- allowed traffic log messages 25
- anomaly attack log messages 61
- antivirus log
 - body format 22
 - sub-types 18
- antivirus log messages 60
 - infected 60
- attack log
 - body format 22
 - sub-types 18
- attack log messages 61
 - anomaly 61
 - signature 61
- auth event log messages 57

B

- body
 - antivirus log 22
 - attack log 22
 - event log 21
 - spam filter log 23
 - traffic log 20
 - web filter log 22
- body, log format 20

C

- comments, documentation 8
- configuring alert email 11
- critical, logging severity level 19
- customer service 8

D

- DHCP event log messages 41

- disk
 - log access 13
- DMZ interface
 - definition 71
- document conventions 6
- documentation
 - commenting on 8
 - FortiGate 7

E

- email alert
 - configuring 11
 - options 10
- email filter
 - sub-types 18
- emergency, logging severity level 19
- enabling traffic logging 12
- error, logging severity level 19
- Event 26
- event log
 - body format 21
 - messages 25
 - sub-types 18
- event log messages 26
 - admin 44
 - auth 57
 - DHCP 41
 - HA 56
 - IPSec 39
 - PPP 41
 - system 26

F

- format
 - local disk log header 19
 - log body 20
 - log header 17, 18
 - log messages 17
 - memory buffer log header 19
 - remote syslog log header 19
 - WebTrends log header 19
- FortiGate documentation 7
 - commenting on 8
- Fortinet customer service 8
- Fortinet Knowledge Center 7

H

HA event log messages 56
header format 17, 18
HTTPS 71

I

ICMP 71
ID
 log ID, message ID 17
ids
 log sub-types 18
IKE 71
IMAP 71
 spam filter log messages 67
infected antivirus log messages 60
information, logging severity level 19
Internet key exchange 71
introduction 5
 FortiGate documentation 7
IPSec 71
IPSec event log messages 39

L

L2TP 71
local disk
 log header format 19
local disk or memory buffer log header format 19
log access 13
 disk 13
log body 20
log body format
 antivirus 22
 attack 22
 event 21
 spam filter 23
 traffic 20
 web filter 22
log formats 17
log header format variations 19
log messages 25
log setting 9
 options 9
log types and sub-types 18
logging
 configuring 9
 event log 25
 introduction 5
logging configuration overview 9
logging severity levels 19

M

MAC address 72
memory buffer
 log header format 19
message ID 17, 25

messages
 antivirus log 60
 attack log 61
 event log 25, 26
 format 17
 log header format 17, 18
 severity level 17, 19
 spam filter log 64
 traffic log 25
 web filter log 61
MTU size
 definition 72

N

notification, severity level 19
NTP 72

P

POP3 72
 spam filter log messages 66
PPP event log messages 41
PPTP 72

R

RADIUS
 definition 72
remote syslog log header format 19
routing
 definition 72
routing table
 definition 72

S

severity level
 log messages 17, 19
signature attack log messages 61
SMTP
 definition 72
 spam filter log messages 64
SNMP
 definition 72
spam filter log 18
 body format 23
Spam filter log messages
 IMAP 67
 POP3 66
 SMTP 64
spam filter log messages 64
SSH
 definition 73
SSL
 definition 71
subnet
 definition 73
subnet address
 definition 73

- sub-types 18
- sub-types, log 18
- syslog server
 - log header format 19
- system event log messages 26

T

- technical support 8
- traffic log
 - body format 20
 - enabling 12
 - sub-types 18
- traffic log messages 25
 - allowed 25
 - violation 26

U

- urlblock web filter log messages 61

- urlxempt web filter log messages 63

V

- variations, log header formats 19
- viewing log messages 13
- violation traffic log messages 26
- virus log
 - sub-types 18

W

- warning, logging severity level 19
- web filter log
 - body format 22
 - sub-types 18
- web filter log messages 61
 - urlblock 61
 - urlxempt 63
- WebTrends log header format 19

