



FortiGate Logging in FortiOS 4.0™

Version 4.0.0

Technical Note

FortiGate Logging in FortiOS 4.0

Version 4.0.0

4 May 2009

01-400-82625-20090504

© Copyright 2009 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.

Trademarks

Dynamic Threat Prevention System (DTPS), APSecure, FortiASIC, FortiBIOS, FortiBridge, FortiClient, FortiGate®, FortiGate Unified Threat Management System, FortiGuard®, FortiGuard-Antispam, FortiGuard-Antivirus, FortiGuard-Intrusion, FortiGuard-Web, FortiLog, FortiAnalyzer, FortiManager, Fortinet®, FortiOS, FortiPartner, FortiProtect, FortiReporter, FortiResponse, FortiShield, FortiVoIP, and FortiWiFi are trademarks of Fortinet, Inc. in the United States and/or other countries. The names of actual companies and products mentioned herein may be the trademarks of their respective owners.

Contents

Introduction	5
Revision history	5
About logging in FortiOS 4.0	5
Fortinet documentation	6
Fortinet Tools and Documentation CD	6
Fortinet Knowledge Center	6
Comments on Fortinet technical documentation	6
Best practices for logging in FortiOS 4.0	7
About logging	7
Logging FortiGate features	8
Traffic logs	8
Virtual Domain (VDOM) logs	8
VPN logs	8
Data Leak Prevention (DLP) logs	8
Application Control logs	9
Content archiving	9
Log devices	9
System memory	9
Local disk or AMC disks	9
FortiAnalyzer unit	10
FortiGuard Analysis server	10
Syslog server	10
NetIQ WebTrends server	10
Backup solutions for logging	11
FortiGate units with hard disks and AMC hard disks	11
FortiAnalyzer unit	11
Syslog server	11
NetIQ WebTrends server backup solution	11
Storing logs	13
Configuring log devices	13
Logging to memory	13
Logging to a FortiAnalyzer unit	14
Testing the FortiAnalyzer configuration	14
Connecting to FortiAnalyzer unit using Automatic Discovery	14
Logging to a FortiGuard Analysis server	15
Logging to a Syslog server	15
Logging to a WebTrends server	16
Example	16

Logging to multiple FortiAnalyzer units or Syslog servers	16
Configuring multiple FortiAnalyzer units	16
Enabling multiple Syslog servers.....	17
Logging in FortiOS 4.0.....	19
FortiGate log types	19
Log severity levels.....	20
Enabling logging.....	20
Enabling firewall policy traffic logging	20
Enabling event logging	21
Enabling Data Leak Prevention log	22
Enabling application control logging	22
Enabling antivirus logging.....	22
Enabling Web Filter logging.....	23
Enabling attack logging.....	23
Enabling spam filter logging.....	23
Enabling IM and P2P logging	24
Enabling content archiving.....	24
Alert Email	25
Configuring alert email.....	26
FortiGate log messages	29
Log types and sub-types.....	29
Log messages explained.....	30
Traffic log messages.....	31
Event log messages	34
Content Archive logs.....	36
Antivirus log messages.....	37
WebFilter log messages	39
Attack log messages.....	41
AntiSpam log messages.....	43
Data Leak Prevention log message.....	44
Application control log message	46
IM/P2P log message.....	48
VoIP log messages.....	49

Introduction

This document introduces you to FortiGate logging in FortiOS 4.0 and includes information on where to enable logging of FortiGate features. It also includes explanations about each log message recorded in FortiOS 4.0.

FortiGate Logging in FortiOS 4.0 describes FortiGate logging, including how to log to multiple FortiAnalyzer units and Syslog servers. This chapter also includes how to configure and enable logging of various FortiGate features.

This section describes:

- [Revision history](#)
- [About logging in FortiOS 4.0](#)
- [Fortinet documentation](#)

Revision history

The following table provides information on the current version of the document, including the date it was published on, and the description of what changes occurred if any for the current release.

Table 1: Revision history of the FortiGate Logging in FortiOS 4.0

Version	Date	Description of changes
First Release	November 27, 2006	Initial release.
Second Release	June 21, 2007	Updated for FortiOS 3.0 MR5
Third Release	September 2, 2008	Updated for FortiOS 3.0 MR7 and includes logging to a FortiGuard Analysis server.
Fourth Release	May 4, 2009	Updated for FortiOS 4.0. Included the section on best practices.

About logging in FortiOS 4.0

Logging is an integral component of the FortiGate system. Logging allows you to view the activity and status of the traffic passing through your network, and monitor for anomalies.

FortiOS 4.0 logging provides you with a way to track down and pinpoint problems efficiently, by monitoring the many facets of network and Internet traffic. FortiOS can log network traffic, antivirus and web filtering action, email and IM conversations, including Spam activity.

FortiOS 4.0 can store logs in various locations, depending on your office environment and configuration. You can enable logging to the FortiGate system memory, hard disk (if available), a FortiAnalyzer unit, FortiGuard Analysis server, or Syslog server. You can also configure the FortiGate unit to log to multiple FortiAnalyzer units or Syslog servers.

If you require urgent action when certain events or severity levels are recorded, you can configure the FortiGate unit to send an alert email. An alert email notifies you whenever a specified event or events (or severity level) is logged in a given time period, allowing you to quickly respond to a potential problem or prevent a problem from occurring.

Customer service and technical support

Fortinet Technical Support provides services designed to make sure that your Fortinet products install quickly, configure easily, and operate reliably in your network.

To learn about the technical support services that Fortinet provides, visit the Fortinet Technical Support web site at <https://support.fortinet.com>.

Fortinet documentation

The Fortinet Technical Documentation web site, <http://docs.fortinet.com>, provides the most up-to-date versions of Fortinet publications, as well as additional technical documentation such as technical notes.

In addition to the Fortinet Technical Documentation web site, you can find Fortinet technical documentation on the Fortinet Tools and Documentation CD, and on the Fortinet Knowledge Center.

Fortinet Tools and Documentation CD

Many Fortinet publications are available on the Fortinet Tools and Documentation CD shipped with your Fortinet product. The documents on this CD are current at shipping time. For current versions of Fortinet documentation, visit the Fortinet Technical Documentation web site, <http://docs.fortinet.com>.

Fortinet Knowledge Center

The Fortinet Knowledge Center provides additional Fortinet technical documentation, such as troubleshooting and how-to-articles, examples, FAQs, technical notes, a glossary, and more. Visit the Fortinet Knowledge Center at <http://kc.fortinet.com>.

Comments on Fortinet technical documentation

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

Best practices for logging in FortiOS 4.0

This section contains valuable information about logging practices and what you need to consider before logging FortiGate features on your FortiGate unit. This section includes how logging affects system performance, what logging devices are appropriate for your logging setup, and solutions for ensuring that logs are not lost if a failure occurs with your logging device.

Fortinet recommends reading this section when one or more of the following applies:

- You are new to logging in general or new to logging using a FortiGate unit and log device.
- You are deciding on a log scenario for your network environment and need to know what log devices are available for the FortiGate unit, including what FortiGate features would be best suited for your network traffic.
- You want to upgrade your current log scenario which may mean a new log device (such as a FortiGuard Analysis server)
- You need to create a new log scenario because the current one no longer meets your network's means.

This section describes:

- [About logging](#)
- [Logging FortiGate features](#)
- [Log devices](#)
- [Backup solutions for logging](#)

About logging

Logging is a valuable tool, providing insight into how to better protect the network traffic against attacks, including misuse and abuse. This valuable tool requires a plan so that you can properly configure logging for your particular network's needs.

This plan should provide you with an outline of what log requirements your network needs. Your plan should cover:

- what FortiGate features you want logged
- the logging device best suited for your network
- if you want or are required to archive log files
- ensuring log files are not lost in the event a failure occurs (backup solution).

Your plan should also include the following:

- 1 The FortiGate features you want to log. For more information, see "[Logging FortiGate features](#)" on page 8.
- 2 The amount of storage space required to log the chosen FortiGate features. For example, traffic logs cannot be stored in the FortiGate system memory because they are large files. For more information, see "[Logging FortiGate features](#)" on page 8.

- 3 The type of device appropriate for logging the chosen FortiGate features. If your organization/company requires reports compiled from log data, a FortiAnalyzer unit may be a better solution since it can create reports at scheduled times. For more information, see [“Log devices” on page 8](#).
- 4 A backup solution in the event your logging device becomes unavailable. For more information, see [“Backup solutions for logging” on page 10](#).

Logging FortiGate features

When you are deciding which FortiGate features should be logged, it is important to know what types of features are best suited for your logging requirements. For example, you want to archive only spam email messages and log VoIP, IM/P2P, event, and traffic logs. You also need to know if your logging device accepts the types of FortiGate features that you want log. For example, a FortiGuard Analysis server accepts all content archive logs, but a Syslog server does not. The backup solution must also fit with what you want to log. For example, you have enabled traffic, event and content archiving to log to a FortiAnalyzer unit with a Syslog server as a backup solution: a power failure occurs with the FortiAnalyzer unit and only traffic and event logs are sent to the Syslog server because content archives are not supported.

The FortiGate unit can log eleven types of features. These types are:

- traffic
- event
- Data Leak Prevention (DLP)
- application control
- antivirus
- web filtering
- attack (IPS)
- spam filtering
- content archiving (available only on FortiAnalyzer units)

If you have enabled and configured VDOMs on your FortiGate unit, you can enable logging of FortiGate features within each VDOM. The log message, whether recorded in a VDOM or not, provides what VDOM that log message was recorded in. For example, an event log recorded user_1 editing administrative profiles for user_23 in the vdom_hq. This type of detail provides you with additional help in tracking down and taking action against such things as misuse and abuse or attacks.

Log devices

Log devices provide a secure place to store and view generated log files; however, some these devices can also provide much more. For example, a FortiAnalyzer unit provides both archiving and reporting features.

The following explains each of the supported log devices, including why that logging device may be a good idea for your network.

System memory

The system memory on the FortiGate unit logs the following features:

- Event log

- Attack log
- Antivirus log
- Webfilter log
- Spam log
- Data Leak Prevention log
- Application Control log
- IM/P2P log
- VoIP log

System memory is limited; the system memory cannot log traffic or content archive logs because of their file size and occurrence; however, if you have a local disk, it can log traffic or content archive logs.

If you configured system memory logging, these logs display in *Log&Report > Log Access > Memory*. System memory is a good log device when you only require logging a few FortiGate features or for small networks, such as a home business.

Local disk or AMC disks

If you configured local disk logging, these logs display in *Log&Report > Log Access > Disk*. This option is available only on FortiGate units with hard disks.

If you have an AMC disk, you can enable uploading of log files to a FortiAnalyzer unit using the CLI.

FortiAnalyzer unit

The FortiAnalyzer unit logs all FortiGate features and can also archive logs. If you also require creating reports from log data, the FortiAnalyzer unit provides a wide variety of reports. Reports contain log information that is presented in both graphical and tabular formats. Reports are a useful tool for reviewing what has occurred on your network in a daily, weekly, or monthly time period.

Logs are accessed from either the web-based manager of the FortiAnalyzer unit or the web-based manager of the FortiGate unit (*Log&Report > Log Access > Remote*).

You can configure up to three FortiAnalyzer units for logging FortiGate features; however, this is more of a redundant option than a back up solution.

The FortiAnalyzer unit is perfect for large networks that require content archiving and reports. The FortiAnalyzer unit can also be considered when

FortiGuard Analysis server

You can also configure logging to a FortiGuard Analysis server. The FortiGuard Analysis Service provides a server which you can configure a FortiGate unit to log FortiGate features to. The FortiGuard Analysis Service is a subscription-based service that provides logging and reporting capabilities previously only found on a FortiAnalyzer unit. You can log to a FortiGuard Analysis server if your FortiGate unit is running FortiOS 4.0 and higher.

The FortiGuard Analysis server can log all FortiGate features including traffic logs, as well as full content archiving of all archival FortiGate features, such as email messages and FTP. You can also generate reports from the log data stored on the FortiGuard Analysis server.

FortiGuard Analysis servers provide all the features of a FortiAnalyzer unit, but without having an actual, physical FortiAnalyzer unit. This service provides an easy, maintenance-free environment for logging and is best for those networks that are growing or administrators who may not have a lot of experience with logging with a FortiGate unit. The FortiGuard Analysis server can be used in all types of networks, large or small.



Note: If you have not already upgraded to FortiOS 4.0, you can still subscribe to the FortiGuard Analysis and Management Service so that you can configure your FortiGate unit to log to a FortiGuard Analysis server; however, certain FortiOS 3.0 maintenance releases do not contain all the available features that the current FortiGuard Analysis and Management Service version supports.

Syslog server

The Syslog server can log all FortiGate features, including content logs and VoIP logs. You can also configure up to three Syslog servers to log all FortiGate features. Configuring three Syslog servers is more of a redundant solution, than a back up solution.

Syslog servers are useful in any network setup, large or small.

If you require reports (which are generated from log data), you need to log to a FortiAnalyzer unit or FortiGuard Analysis server.

NetIQ WebTrends server

The NetIQ WebTrends server logs all FortiGate features, except content archive. You can configure only one NetIQ WebTrends server to log FortiGate features. A NetIQ WebTrends server is useful in any network setup, large or small.

Backup solutions for logging

You need to have a backup solution, or backup plan, in the event the logging device becomes unavailable. If you decide not to include a backup solution when you begin logging, log files may be lost if the logging device becomes unavailable.

The following are backup solutions for various logging devices.

The FortiGuard Analysis Service has several secondary FortiGuard Analysis servers configured as backup servers in the event the FortiGuard Analysis server that is storing your log files becomes unavailable. The FortiGuard Analysis service does not require a backup solution because the secondary servers provide the backup solution you may need if the FortiGuard Analysis server your FortiGate unit is logging to becomes unavailable.

FortiGate units with hard disks and AMC hard disks

You can use the hard disk, if available, to log to a FortiAnalyzer unit with buffering to the hard disk by the configuring this in the CLI. For more information, see the *FortiGate CLI Reference*.

You can configure the AMC hard disk on the FortiGate unit, if available, to store logs including content archives and then upload these logs to a FortiAnalyzer unit on a daily basis. You can also schedule when to upload these logs from the AMC disk to the FortiAnalyzer unit.

FortiAnalyzer unit

A backup solution to a FortiAnalyzer unit may be a Syslog server or NetIQ WebTrends server. You cannot configure a FortiGuard Analysis server to be a backup logging device when logging to a FortiAnalyzer unit because you cannot log to both.

Syslog server

You can configure up to three Syslog servers for ensuring logs are not lost when a failure occurs. When the FortiGate unit logs to all three Syslog servers, all three Syslog servers receive the same logs. This ensures logs are available at all times.

NetIQ WebTrends server backup solution

You can log to the FortiGate system memory or hard disk, as a backup solution when logging FortiGate features to a NetIQ WebTrends server.

Storing logs

The FortiGate unit supports logging to a variety of log devices, including the FortiGuard Analysis server. This provides greater flexibility when logging requirements change. The log devices that the FortiGate unit supports are:

- FortiGate system memory
- Hard disk or AMC
- FortiAnalyzer unit
- FortiGuard Analysis server (part of the FortiGuard Analysis and Management Service)
- Syslog server
- NetIQ WebTrends server

The following topics explain how to configure each type of logging device, including how to configure multiple FortiAnalyzer units or Syslog servers or logging to a FortiGate Analysis server. This option is available only when subscribed to the FortiGuard Analysis and Management Service.

This section describes:

- [Configuring log devices](#)
- [Logging to multiple FortiAnalyzer units or Syslog servers](#)



Note: All log entries are cleared from the FortiGate unit system memory when the FortiGate unit restarts.

Configuring log devices

In your log plan, you specified a log device (or devices) that meets your logging requirements. The following explains how to configure your chosen log device to communicate and send logs from your FortiGate unit. If you need to configure multiple FortiAnalyzer units or Syslog servers, proceed to [“Logging to multiple FortiAnalyzer units or Syslog servers” on page 16](#) to configure these devices.

Logging to memory

The FortiGate system memory has a limited capacity for log messages. The system memory displays recent log entries and stores most log types except traffic and content logs. The FortiGate system memory cannot store traffic and content logs because of their size and frequency of log entries. When the system memory is full, the FortiGate unit overwrites the oldest messages. All log entries stored in system memory are cleared when the FortiGate unit restarts.

To configure the FortiGate unit to save logs in memory

- 1 Go to *Log&Report > Log Config > Log Setting*.
- 2 Select the check box beside *Memory*.
- 3 Select the Expand Arrow beside the check box to reveal the available options.
- 4 Select the severity level.

- 5 Select *OK*.

The FortiGate unit logs all messages at and above the logging severity level you select. For more information on log severity levels, see [“Log severity levels” on page 20](#).

You can log to the FortiGate hard disk, if available from the CLI. For more information, see the *FortiGate CLI Reference*.

Logging to a FortiAnalyzer unit

A FortiAnalyzer unit can log all FortiGate features that are available for logging, including content archiving. The following procedure assumes that you have only one FortiAnalyzer unit to configure. If you are configuring more than one, you must configure the other FortiAnalyzer units in the CLI. Use the procedures in [“Configuring multiple FortiAnalyzer units” on page 16](#) to configure multiple FortiAnalyzer units.

To send logs to a FortiAnalyzer unit

- 1 Go to *Log&Report > Log Config > Log Setting*.
- 2 Select the Expand Arrow beside *Remote Logging* to reveal the available options.
- 3 Select *FortiAnalyzer*.
- 4 Select the level of the log messages to send to the FortiAnalyzer unit.
- 5 Enter the server IP address of the FortiAnalyzer unit.
- 6 Select *Apply*.

Testing the FortiAnalyzer configuration

After configuring FortiAnalyzer settings, you can test the connection between the Fortinet unit and the FortiAnalyzer unit to ensure the connection is working properly. This enables you to view the connection settings between the FortiGate unit and the FortiAnalyzer unit.

To test the connection between your FortiGate unit and the FortiAnalyzer unit, go to *Log&Report > Log Config > Log Settings*, and then select *Test Connectivity*.

Connecting to FortiAnalyzer unit using Automatic Discovery

Automatic Discovery is a method of establishing a connection to a FortiAnalyzer unit by using the FortiGate unit to find a FortiAnalyzer unit on the network. The Fortinet Discovery Protocol (FDP) is used to locate the FortiAnalyzer unit. Both units must be on the same subnet to use FDP, and they must also be able to connect using UDP.

When you select Automatic Discovery, the FortiGate unit uses HELLO packets to locate any FortiAnalyzer units that are available on the network within the same subnet. When the FortiGate unit discovers the FortiAnalyzer unit, the FortiGate unit automatically enables logging to the FortiAnalyzer unit and begins sending log data.

To connect to a FortiAnalyzer unit using Automatic Discovery

- 1 Go to *Log&Report > Log Config > Log Settings*.
- 2 Select *Automatic Discovery*.
- 3 If in Transparent mode, select an interface from the Interface list.
- 4 If available, select a FortiAnalyzer unit from the *Connect To* list when a FortiAnalyzer unit is discovered.
- 5 Select *Discover*.

- 6 When you select Discover in Transparent mode, a warning displays. Select OK to continue.

If your FortiGate unit is in Transparent mode, the interface using the automatic discovery feature will not carry traffic. For more information about how to enable the interface to also carry traffic when using the automatic discovery feature, see the Fortinet Knowledge Center article, [Fortinet Discovery Protocol in Transparent mode](#).



Note: The FortiGate unit searches within the same subnet for a response from any available FortiAnalyzer units.

Logging to a FortiGuard Analysis server

You can configure logging to a FortiGuard Analysis server after registering for the FortiGuard Analysis and Management Service. The following procedure assumes that you have already configured the service account ID in *System > Maintenance > FortiGuard*.

To log to a FortiGuard Analysis server

- 1 Go to *Log&Report > Log Config*.
- 2 Select the Expand Arrow beside *Remote Logging* to reveal the available options.
- 3 Select *FortiGuard Analysis Service*.
- 4 Enter the account ID in the *Account ID* field.
- 5 Select one of the following:

Overwrite oldest logs	Deletes the oldest log entry and continues logging when the maximum log disk space is reached.
Do not log	Stops log messages going to the FortiGuard Analysis server when the maximum log disk space is reached.
- 6 Select a severity level.
- 7 Select *Apply*.

Logging to a Syslog server

The Syslog server is a remote computer running syslog software. Syslog is a standard for forwarding log messages in an IP network. Syslog servers capture log information provided by network devices.

To send logs to a syslog server

- 1 Go to *Log&Report > Log Config > Log Setting*.
- 2 Select the check box beside *Syslog*.
- 3 Select the Expand Arrow beside the check box to reveal the available options.
- 4 Enter the appropriate information for the following:

Name/IP	Enter the domain name or IP address of the syslog server.
Port	Enter the port number for communication with the syslog server, usually port 514.
Level	Select a log level the Fortinet unit will log all messages at and above that logging severity level. For more information about log severity levels, see " Log severity levels " on page 20.

Facility	Facility indicates to the syslog server the source of a log message. By default, the FortiGate reports facility as local7. You can change the Facility if you want to distinguish log messages from different Fortinet units.
Enable CSV Format	Select to have logs formatted in CSV format. When you enable CSV format, the Fortinet unit produces the log in Comma Separated Value (CSV) format. If you do not enable CSV format, the Fortinet unit produces plain text files.

5 Select *Apply*.

Logging to a WebTrends server

A WebTrends server is a remote computer, similar to a Syslog server, running NetIQ WebTrends firewall reporting server. FortiGate log formats comply with WebTrends Enhanced Log Format (WELF) and are compatible with NetIQ WebTrends Security Reporting Center and Firewall Suite 4.1.

To send logs to a WebTrends server, log in to the CLI and enter the following commands:

```
config log webtrends setting
  set server <address_ip4>
  set status {disable | enable}
end
```

Example

This example shows how to enable logging to and set an IP address for a remote NetIQ WebTrends server.

```
config log webtrends settings
  set status enable
  set server 172.25.82.145
end
```

Logging to multiple FortiAnalyzer units or Syslog servers

FortiOS 4.0 allows you to send log messages to multiple FortiAnalyzer units or multiple Syslog servers, which provides additional redundant log storage. By logging to multiple FortiAnalyzer units, or Syslog servers, you can ensure that all logs are not lost in the event one of them fails.

You can configure multiple FortiAnalyzer units or Syslog servers within the CLI. You should review the *FortiGate CLI Reference* before proceeding because the reference document provides detailed explanations on all the CLI commands used in the following procedures.

Configuring multiple FortiAnalyzer units

Before proceeding, make sure the FortiAnalyzer unit configured in [“Logging to a FortiAnalyzer unit” on page 14](#) is properly connected. You need to configure one of the FortiAnalyzer units before configuring the others because of the way commands are enabled/disabled for configuring multiple FortiAnalyzer units. Review the *FortiGate CLI Reference* for more information.

Fortinet recommends that you contact a FortiAnalyzer administrator first, to verify that the IP addresses of the FortiAnalyzer units you want to send logs to are correct, and that all FortiAnalyzer units are currently installed with FortiAnalyzer 4.0 firmware.

You must configure multiple FortiAnalyzer units in `config system` to configure all FortiAnalyzer settings. The command, `config log`, only enables logging to multiple FortiAnalyzer units. All filter settings are enabled by default.

The following procedure does not contain how to enable logging of FortiGate features within the CLI. Use the *FortiGate CLI Reference* (the `config log` chapter) to enable which FortiGate features you want to enable.

To enable logging to multiple FortiAnalyzer units

- 1 Configure the first FortiAnalyzer unit using the procedure “[To send logs to a FortiAnalyzer unit](#)” on page 14. If already configured, go to step 2.

- 2 Log in to the CLI.

- 3 Enter the following commands:

```
config system fortianalyzer2 setting
  set status {disable | enable}
  set server <fortianalyzer_ipv4>
  set encrypt {disable | enable}
  set localid <identifier>
  set psksecret <pre-shared_key>
  set ver-1 {disable | enable}
end
```

- 4 Enter the following commands:

```
config system fortianalyzer3 settings
  set status {disable | enable}
  set server <fortianalyzer_ipv4>
  set encrypt {disable | enable}
  set localid <identifier>
  set psksecret <pre-shared_key>
  set ver-1 {disable | enable}
end
```

- 5 Enter the following commands to enable logging to each FortiAnalyzer unit:

```
config log fortianalyzer2 setting
  set status enable
end
config log fortianalyzer3 setting
  set status enable
end
```

Enabling multiple Syslog servers

Before proceeding, make sure the Syslog server configured in “[Logging to a Syslog server](#)” on page 15 is properly connected.

The following procedure does not contain how to enable logging of FortiGate features within the CLI. Use the *FortiGate CLI Reference* (the `config log` chapter) to enable which FortiGate features you want to enable.

To enable logging to multiple Syslog servers

- 1 Configure the first Syslog server using the procedure “[To send logs to a syslog server](#)” on page 15. If already configured, go to step 2.

- 2 Log in to the CLI.

- 3 Enter the following commands:

```
config log syslogd2 setting
  set csv {disable | enable}
  set facility <facility_name>
  set port <port_integer>
  set server <ip_address>
  set status {disable | enable}
end
```

4 Enter the following commands to configure a third Syslog server:

```
config log syslogd3 setting
  set csv {disable | enable}
  set facility <facility_name>
  set port <port_integer>
  set server <ip_address>
  set status {disable | enable}
end
```

Logging in FortiOS 4.0

This section introduces you to the types of logs the FortiGate unit records, log severity levels, and where to enable logging of FortiGate features in FortiOS 4.0.

If you require more information about FortiGate logging in FortiOS 4.0, see the *FortiGate Administration Guide* and the *FortiGate CLI Reference*.

This section describes:

- [FortiGate log types](#)
- [Log severity levels](#)
- [Enabling logging](#)
- [Alert Email](#)

FortiGate log types

The FortiGate unit can record the following log types based on the network traffic.

Log Type	File name	Description
Traffic	tlog.log	The traffic log records all traffic to and through the FortiGate interface.
Event	elog.log	The event log records management and activity events. For example, when an administrator logs in or logs out of the web-based manager.
Antivirus	vlog.log	The antivirus log records virus incidents in Web, FTP, and email traffic.
Web	wlog.log	The web filter log records HTTP FortiGate log rating errors including web content blocking actions that the FortiGate unit performs.
Attack	alog.log	The attack log records attacks that are detected and prevented by the FortiGate unit.
Spam Filter	slog.log	The spam filter log records blocking of email address patterns and content in SMTP, IMAP, and POP3 traffic.
Data Leak Prevention	dlog.log	The Data Leak Prevention log records log data that is considered sensitive and that should not be made public. This log also records data that a company does not want entering their network.
Application Control	rlog.log	The application control log records data detected by the FortiGate unit and the action taken against the network traffic depending on the application that is generating the traffic, for example, instant messaging software, such as MSN Messenger.
Content	clog.log	The content log records all log messages, including most IM log messages as well as the following VoIP log messages: <ul style="list-style-type: none"> • SIP start and end call • SCCP phone registration • SCCP call info (end of call) • SIMPLE log message

Log severity levels

You can define what severity level the FortiGate unit records logs at when configuring the logging location. The FortiGate unit logs all message 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: Log severity levels

Levels	Description
0 - Emergency	The system has become unstable.
1 - Alert	Immediate action is required.
2 - Critical	Functionality is affected.
3 - Error	An error condition exists and functionality could be affected.
4 - Warning	Functionality could be affected.
5 - Notification	Information about normal events.
6 - Information	General information about system operations.

The Debug severity level, not shown in [Table 2](#), is rarely used. It is the lowest log severity level and usually contains some firmware status information that is useful when the FortiGate unit is not functioning properly. Debug log messages are only generated if the log severity level is set to Debug. Debug log messages are generated by all types of FortiGate features.

Enabling logging

Within FortiOS 4.0, there are many different logs you can enable. Depending on what you choose to log, you need to enable them in various locations within the web-based manager. This section describes where you enable logging for each log type.

Enabling firewall policy traffic logging

Firewall policy traffic logging records the traffic, both permitted and denied by the firewall policy, based on the protection profile. Firewall policy traffic logging records packets that match the policy. This method of traffic logging is preferred because it reduces system load on the FortiGate unit.



Note: You need to set the logging severity level to Notification when configuring a logging location to record traffic log messages.

To enable firewall policy traffic logging

- 1 Go to *Firewall > Policy*.
- 2 Select the Expand Arrow to view the policy list for a policy.
- 3 Select *Edit* beside the policy that you want.

If required, create a new firewall policy by selecting Create New. For more information about firewall policies, see the *FortiGate Administration Guide*.

- 4 Select *Log Allowed Traffic*.
- 5 Select *OK*.

Enabling event logging

The event log records management and activity events, such as when a configuration has changed, admin login, or high availability (HA) events occur.

When you are logged in to VDOMs, certain options may not be available, such as VIP ssl event or CPU and memory usage events. You can enable event logs only when you are logged in to a VDOM; you cannot enable event logs in the root VDOM.

To enable the event logs

1 Go to *Log&Report > Log Config > Event Log*.

2 Select the *Enable* check box.

3 Select one or more of the following logs:

System activity event	All system-related events, such as ping server failure and gateway status.
IPSec negotiation event	All IPSec negotiation events, such as process and error reports.
DHCP service event	All DHCP-events, such as the request and response log.
L2TP/PPTP/PPPoE service event	All protocol-related events, such as manager and socket create processes.
Admin event	All administrative events, such as user logins, resets, and configuration updates.
HA activity event	All high availability events, such as link, member, and stat information.
Firewall authentication event	All firewall-related events, such as user authentication.
Pattern update event	All pattern update events, such as antivirus and IPS pattern updates and update failure.
SSL VPN user authentication event	All administrator events related to SSL VPN, such as SSL configuration and CA certificate loading and removal.
SSL VPN administration event	All administration events related to SSL VPN, such as SSL configuration and CA certificate loading and removal.
SSL VPN session event	All session activity such as application launches and blocks, timeouts, verifications and so on.
VIP ssl event	All server-load balancing events that are happening during SSL session, especially details about handshaking.
VIP server health monitor event	All related VIP server health monitor events that occur when the VIP health monitor is configured, such as an interface failure.
CPU & memory usage (every 5 min)	Real-time CPU and memory events only, at 5-minute intervals.

4 Select *Apply*.

Enabling Data Leak Prevention logging

Data Leak Prevention (DLP) provides additional information for administrators that can better analyze and detect data leaks. You can enable logging of your configured settings for DLP within the DLP sensor.

Before enabling logging of DLP events, verify that you have the correct DLP sensor for what you want logged.

To enable logging of DLP events

- 1 Go to *Firewall > Protection Profile*.
- 2 Select the Expand Arrow to view the policy list for a policy.
- 3 Select *Edit* beside the policy that you want.
- 4 Select the Expand Arrow to view the *Data Leak Prevention* options.
- 5 Select the check box next to the sensor list.
- 6 Select a sensor from the list.
- 7 Select the Expand Arrow to view the *Logging* options.
- 8 Select the *Data Leak Prevention Log DLP* check box.

Enabling application control logging

This log file includes IPS, IM/P2P and VoIP events that the FortiGate unit records. The application control log also includes some IPS activities.

Before enabling logging of Application Control events, verify that the correct application control list is available for what you want to log. An application control list is required for logging application control events.

To enable logging of application control settings

- 1 Go to *Firewall > Protection Profile*.
- 2 Select *Edit* beside the protection profile that you want.
- 3 Select the Expand Arrow to expand *Application Control*.
- 4 Select the check box beside the application control list.
- 5 Select a list from the application control list.
- 6 Select the Expand Arrow to expand the *Logging* options.
- 7 Select the *Log Application Control* check box.

Enabling antivirus logging

The Antivirus logs record virus incidents in Web, FTP and email traffic. For example, when the FortiGate unit detects an infected file, blocks a file type, or blocks an oversized file or email. You can also apply filters to customize what the FortiGate unit logs, which are:

- **Viruses** – The FortiGate unit logs all virus infections
- **Blocked Files** – The FortiGate unit logs all instances of blocked files.
- **Oversized Files/Emails** – The FortiGate unit logs all instances of files and email messages exceeding defined thresholds.
- **AV Monitor** – The FortiGate unit logs all instances of viruses, blocked files, and oversized files and email. This applies to HTTP, FTP, IMAP, POP3, SMTP, and IM traffic.

To enable antivirus logs

- 1 Go to *Firewall > Protection Profile*.
- 2 Select the *Edit* icon beside the protection profile that you want.
- 3 Select the Expand Arrow beside *Logging* to reveal the available options.
- 4 Under *Antivirus*, select what antivirus events you want logged.
- 5 Select *OK*.

Enabling Web Filter logging

Web Filter logs record HTTP, FortiGuard log rating errors including web content blocking actions.

To enable web filter logs

- 1 Go to *Firewall > Protection Profile*.
- 2 Select the *Edit* icon beside the protection profile that you want.
- 3 Select the Expand Arrow beside *Logging* to reveal the available options.
- 4 Under *Web Filtering*, select the web filtering events to log.
- 5 Select the *FortiGuard Web Filtering Rating Errors (HTTP only)* to log FortiGuard filtering.
- 6 Select *OK*.

Enabling attack logging

The Attack log records attacks detected and prevented by the FortiGate unit. The FortiGate unit will log attack signatures and attack anomalies.

To enable the attack logs

- 1 Go to *Firewall > Protection Profile*.
- 2 Select *Edit* beside the protection profile that you want.
- 3 Select the Expand Arrow beside *Logging* to reveal the available options.
- 4 Select *Log Intrusions*.
- 5 Select *OK*.

Enabling spam filter logging

Spam Filter logs record blocking of email address patterns and content in SMTP, IMAP, and POP3 traffic.

To enable the spam log

- 1 Go to *Firewall > Protection Profile*.
- 2 Select *Edit* beside the protection profile that you want.
- 3 Select the Expand Arrow beside *Logging* to reveal the available options.
- 4 Select *Log Spam*.
- 5 Select *OK*.

Enabling content archiving

You can content archive FTP, Email, IM, and Web (including HTTPS and all other secure protocols), using DLP rules and sensors. You need to first configure a DLP sensor before you can archive log files. For information about how to configure a DLP sensor, see the FortiGate Administration Guide. When configuring content archiving, you can associate only one DLP sensor for a protection profile.

Configuring content archiving is enabled within the DLP sensor; however, VoIP and spam email messages are configured differently. VoIP content archiving is configured in the CLI. You also need to configure an application control list that contains the SIP, SIMPLE and SCCP protocols. Content archiving of spam email messages is configured only in the protection profile. For information about how to configure application control lists, see the FortiGate Administration Guide.

You can use the default DLP sensors that are available in *UTM > Data Leak Prevention > Sensor*. The two default DLP sensors, *Content_Archive* and *Content_Summary*, are dedicated to content archiving. *Content_Archive* provides full content archiving, while *Content_Summary* provides summary content archiving. For more information, see the FortiGate Administration Guide.

The following procedures explain how to configure content archiving of spam email messages and VoIP content archiving.

To enable content archiving of spam email messages

- 1 Go to *Firewall > Protection Profile*.
- 2 Select *Edit* for a protection profile.
- 3 Select the Expand Arrow to view the *Data Leak Prevention Sensor* option.
- 4 Select the DLP sensor for content archiving from the list.
- 5 Select the check boxes for the email protocol or protocols you want to archive beside *Archive SPAMed email to FortiAnalyzer/FortiGuard*.
- 6 Select *OK*.



Note: Infected files are clearly indicated in the Content Archive menu so that you know which content archives are infected and which are not.

To configure VoIP content archiving

- 1 Verify that you have the correct application control list for VoIP content archiving.
- 2 Verify that logging is enabled for that application control VoIP list .
- 3 Log in to the CLI.
- 4 Enter the following to access the application control VoIP list and the entries:

```
config application list
  edit <name>
    config entries
      edit <entry_identification>
```
- 5 Enter one of the following to enable content archiving for the entry you chose in step 5:

```
set sip-archive-summary enable
set sccp-archive-summary enable
set simple-archive-summary enable
```
- 6 If you want to enable full content archiving of SIMPLE, enter the following:

```
set simple-archive-full enable
```

Alert Email

You can use the Alert Email feature to monitor logs for log messages, and to send email notification about a specific activity or event logged. For example, if you require notification about administrators logging in and out, you can configure an alert email that is sent whenever an administrator logs in and out.

You can also base alert email messages on the severity levels of the logs.

Figure 1: Alert Email options

SMTP Server	The name/address of the SMTP email server.
Email from	The SMTP user name.
Email to	Enter up to three email address recipients for the alert email message.
Authentication	Select the authentication <i>Enable</i> check box to enable SMTP authentication.
SMTP user	Enter the user name for logging on to the SMTP server to send alert email messages. You need to do this only if you have enabled the SMTP authentication.
Password	Enter the password for logging on to the SMTP server to send alert email. You need to do this only if you selected SMTP authentication.
Send alert email for the following	Select to have the alert email sent for one or multiple events that occur, such as an administrator logging in and out.
Interval Time (1-9999 minutes)	Enter the minimum time interval between consecutive alert emails. Use this to rate-limit the volume of alert emails.
Intrusion detected	Select if you require an alert email message based on attempted intrusion detection.

Virus detected	Select if you require an alert email message based on virus detection.
Web access blocked	Select if you require an alert email message based on blocked web sites that were accessed.
HA status changes	Select if you require an alert email message based on HA status changes.
Violation traffic detected	Select if you require an alert email message based on violated traffic that is detected by the Fortinet unit.
Firewall authentication failure	Select if you require an alert email message based on firewall authentication failures.
SSL VPN login failure	Select if you require an alert email message based on any SSL VPN logins that failed.
Administrator login/logout	Select if you require an alert email message based on whether administrators log in or out.
IPSec tunnel errors	Select if you require an alert email message based on whether there is an error in the IPSec tunnel configuration.
L2TP/PPTP/PPPoE errors	Select if you require an alert email message based on errors that occurred in L2TP, PPTP, or PPPoE.
Configuration changes	Select if you require an alert email message based on any changes made to the FortiGate configuration.
FortiGuard license expiry time (1-100 days)	Enter the number of days before the FortiGuard license expiry time notification is sent.
FortiGuard log quota usage	Select if you require an alert email message based on the FortiGuard Analysis server log disk quota getting full.
Send alert email for logs based on severity	Select if you want to send an alert email that is based on a specified log severity, such as warning.
Minimum log level	Select a log severity from the list. For more information about log severity levels, see “Log severity levels” on page 20 .

Configuring alert email

Before configuring alert email, you must configure at least one DNS server if you are configuring with an Fully Qualified Domain Server (FQDN). The FortiGate unit uses the SMTP server name to connect to the mail server, and must look up this name on your DNS server. You can also specify an IP address.

To configure alert email

- 1 Go to *Log&Report > Log Config > Alert E-mail*.
- 2 Enter the information for the SMTP server and select *Apply*.
- 3 Select *Test Connectivity* to send a test email message to the email account you configured in the above step.
- 4 Select *Send alert email for the following* if you require sending an email based and then select the alert options you want.
- 5 Select *Send an alert based on severity* if you require sending an alert email based on log severity level.
- 6 Select the minimum severity level in the *Minimum severity level* list if you are sending an alert based on severity.
- 7 Select *Apply*.



Note: The default minimum log severity level is Alert. If the Fortinet unit collects more than one log message before an interval is reached, the Fortinet unit combines the messages and sends out one alert email.

FortiGate log messages

FortiGate log messages present detailed accounts of an event or activity that happened on your network recorded by the FortiGate unit. These log messages provide valuable information about your network that inform you about attacks, misuse and abuse, and traffic activity.

The following information provides explanations for log types and sub-types, including log messages in FortiOS 4.0.

If you require more information about FortiGate log messages than this technical note provides, see the *FortiGate Log Message Reference* on the Fortinet Knowledge Center.

This section describes:

- [Log types and sub-types](#)
- [Log messages explained](#)

Log types and sub-types

The following table provides an explanation of the log types and sub-types in FortiOS 4.0.

Table 3: Log types and subtypes

Log Type	Category Number	Sub-Type	Sub-Type Number
traffic (Traffic Log)	00	allowed – Policy allowed traffic	21
		violation – Policy violation traffic	22
		Other	38
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
		alertemail – Alert email notifications	23
		chassis – FortiGate-4000 and FortiGate-5000 series chassis event	29
		sslvpn-user – SSL VPN user event	32
		sslvpn-admin – SSL VPN administration event	33
		sslvpn-session – SSL VPN session even	34
		his-performance – performance statistics	43
vipssl – VIP SSL events	45		
ldb-monitor – LDB monitor events	46		
dlp (Data Leak Prevention)	09	dlp – Data Leak Prevention	54
app-crtl (Application Control Log)	10	app-crtl-all – All application control	59

Table 3: (Continued)Log types and subtypes

content archive (Content Archive Log)	06	HTTP – Virus infected	24
		FTP – FTP content metadata	25
		SMTP – SMTP content metadata	26
		POP3 – POP3 content metadata	27
		IMAP – IMAP content metadata	28
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
		urfilter – URL filter	15
		FortiGuard block	16
		FortiGuard allowed	17
		FortiGuard error	18
		ActiveX script filter	35
		Cookie script filter	36
Applet script filter	37		
ids (Attack Log)	04	signature – Attack signature	19
		anomaly – Attack anomaly	20
emailfilter (Spam Filter Log)	05	SMTP	08
		POP3	09
		IMAP	10

Log messages explained

The following log messages are explained in detail and are all recorded in FortiOS 4.0. Each field of each log message is clearly outlined and explained. If you need additional information about specific log messages, see the *FortiGate Log Message Reference*.

Before proceeding, you should be aware of the two parts that make up a log message: the header and the body. The header is the beginning part of a log message and includes key information about that specific log message, such as the date and time of when it was recorded.

The following is an example of a log header:

```
2009-03-10 12:24:36 devname=FGT50B3G06500085
device_id=FGT50B3G06500085 log_id=0021010001 type=traffic
subtype=allowed pri=notice vd=root fwver=040000
```

The rest of the log message is the log body, which includes the log message. The log message body contains specific information for that specific log type and subtype.

This topic contains the following:

- [Traffic log messages](#)
- [Event log messages](#)
- [Content Archive logs](#)
- [Antivirus log messages](#)
- [WebFilter log messages](#)
- [Attack log messages](#)
- [Antispam log messages](#)
- [Data Leak Prevention log message](#)
- [Application control log message](#)

Traffic log messages

The Traffic log message records all traffic to and through the interfaces on the FortiGate unit. The following is an example of a traffic log message.

```
2009-03-10 12:24:36 devname=FGT50B3G06500085
device_id=FGT50B3G06500085 log_id=0021010001 type=traffic
subtype=allowed pri=notice vd=root fwver=040000 SN=613874
duration=120 carrier_ep=N/A user=admin1 group=admingroup
policyid=1 proto=6 service=80/tcp app_type=N/A status=accept
src=172.16.135.25 srcname=172.16.135.25 dst=172.16.25.125
dstname=172.16.25.125 src_int="internal" dst_int="wan1"
sent=825 rcvd=4451 sent_pkt=8 rcvd_pkt=6 src_port=2504
dst_port=80 vpn="N/A" tran_ip=0.0.0.0 tran_port=0 dir_disp=org
tran_disp=noop
```

date=(2009-03-10)	The year, month and day of when the event occurred in yyyy-mm-dd format.
time=(12:24:36)	The hour, minute and second of when the event occurred in the format hh:mm:ss.
devname=(FGT50B3G06500085)	The name of the FortiGate unit. The name is either the default name (FGT<serial_number>) or the name given by an administrator. The name that appears in this field is the name that appears in Host Name in <i>System > Status</i> in the System Information widget.
device_id=(FGT50B3G06500085)	The serial number of the FortiGate unit.
log_id=(0021010001)	A ten-digit number. The first two digits represent the log type and the following two digits represent the log subtype. The last five digits are the message id.
type=(traffic)	The section of system where the event occurred.
subtype=(allowed)	The subtype of the log message. This represents a policy applied to the FortiGate feature in the firewall policy.
pri=(notice)	The severity level of the event. There are six severity levels to specify. For more information, see "Log severity levels" on page 20 .
vd=(root)	The virtual domain where the traffic was logged. In this example, it is the root virtual domain.
fwver=(04000)	The firmware version that was running when the log message was recorded.
SN=(613874)	The session number of the log message.
duration=(120)	This represents the value in seconds.
carrier_ep=(N/A)	The FortiOS Carrier end-point identification. For example, it would display the MSISDN of the phone that sent the MMS message. If you do not have FortiOS Carrier, this field always displays N/A.
user=(admin1)	The name of the user creating the traffic.
group=(admingroup)	The name of the group creating the traffic.
policyid=(1)	The ID number of the firewall policy that applies to the session or packet. Any policy that is automatically added by the FortiGate will have an index number of zero. For more information, see the Fortinet Knowledge Center article, Firewall policy with ID number of zero .
proto=(6)	The protocol that applies to the session or packet. The protocol number in the packet header that identifies the next level protocol. Protocol numbers are assigned by the Internet Assigned Number Authority (IANA).

service=(80/tcp)	The IP network service that applies to the session or packet. The services displayed correspond to the services configured in the firewall policy.
app_type=(N/A)	The application or program used. If there was no program used to create the traffic, then it is empty and displays N/A. The following are application types: <ul style="list-style-type: none"> • BitTorrent • eDonkey • Gnutella • KaZaa • Skype • WinNY • AIM • ICQ • MSN • Yahoo!
status=(accept)	The status can be either deny or accept depending on the applicable firewall policy.
src=(172.16.135.25)	The source IP address.
srcname=(172.16.135.25)	The source name or the IP address.
dst=(172.16.25.125)	The destination IP address.
dstname=(172.16.25.125)	The destination name or IP address.
src_int=(internal)	The interface where the through traffic comes in. For outgoing traffic originating from the firewall, it is "unknown".
dst_int=(wan1)	The interface where the through traffic goes to the public or Internet. For incoming traffic to the firewall, it is "unknown".
sent=(825)	The total number of bytes sent.
rcvd=(4451)	The total number of bytes received.
sent_pckt=(8)	The total number of packets sent during the session.
rcvd_pckt=(6)	The total number of packets received during the session.
src_port=(2504)	The source port of the TCP or UDP traffic. The source protocol is zero for other types of traffic.
dst_port=(80)	The destination port number of the TCP or UDP traffic. The destination port is zero for other types of traffic.
vpn=(N/A)	The name of the VPN tunnel used by the traffic.
tran_ip=(0.0.0.0)	The translated IP in NAT mode. For transparent mode, it is "0.0.0.0".
tran_port=(0)	The translated port number in NAT mode. For transparent mode, it is zero (0).
dir_disp=(org)	The direction of the sessions. Org displays if a session is not a child session or the child session originated in the same direction as the master session. Reply displays if a different direction is taken from the master session.
tran_disp=(noop)	The packet is source NAT translated or destination NAT translated.

Event log messages

The Event log message records all event activity. The following is an example of an event log message that recorded an admin user adding a firewall policy.

```
2009-03-18 04:36:30 devname=devname=FGT50B3G06500085
device_id=FGT50B3G06500085 log_id=0104032120 type=event
subtype=admin pri=notice vd=root fwver=040000 user=admin
ui=GUI(172.16.24.144) name="admin" msg="Administrator admin
edited the settings of administrator admin from
GUI(172.16.24.144) "
```

date=(2009-03-18)	The year, month and day of when the event occurred in yyyy-mm-dd format.
time=(04:36:30)	The hour, minute and second of when the event occurred in the format hh:mm:ss.
devname=(FGT50B3G06500085)	The name of the FortiGate unit. The name is either the default name (FGT<serial_number>) or the name given by an administrator. The name that appears in this field is the name that appears in Host Name in <i>System > Status</i> in the System Information widget.
device_id=(FGT50B3G06500085)	The serial number of the FortiGate unit.
log_id=(0104032120)	A ten-digit number. The first two digits represent the log type and the following two digits represent the log subtype. The last five digits are the message id.
type=(event)	The section of system where the event occurred.
subtype=(admin)	The subtype of the log message. This represents a policy applied to the FortiGate feature in the firewall policy.
pri=(notice)	The severity level of the event. There are six severity levels to specify. For more information, see "Log severity levels" on page 20 .
vd=(root)	The virtual domain where the traffic was logged.
fwver=(04000)	The firmware version that was running when the log message was recorded.
user=("admin")	The user's admin profile, usually an administration user. In this example, the admin administrator changed the banned word.
ui=[GUI (172.16. 34.144)]	The interface where this particular event occurred, along with the IP address of that interface. The ui field includes GUI, CLI, console, and LCD.
name=("admin")	The user who created the traffic.
msg=("Administrator admin edited the settings of administrator admin from GUI (172.16.24.144)")	Explains the activity or event that the FortiGate unit recorded. In this example, an administrator edited the settings of the administrator admin from the web-based manager.

Content Archive logs

The Content Archive log message provides information concerning logs that are archived on the FortiAnalyzer unit.

The following is an example of a content archive web log message:

```
2009-03-10 12:22:36 devname=FGT50B3G06500085
device_id=FGT50B3G06500085 log_id=0624000000 type=contentlog
subtype=HTTP pri=information vd=root fwver=040000 SN=613874
user=user1 group=usergroup carrier_ep=N/A cat=N/A cat_desc=N/A
3:240060590:0:172.16.25.142<->172.25.124.133:clean:401/4203:
GET 172.25.124.133/favicon.ico
```

date=(2009-03-10)	The year, month and day of when the event occurred in yyyy-mm-dd format.
time (12:22:36)	The hour, minute and second of when the content archive logged the email event.
devname=(FGT50B3G06500085)	The name of the FortiGate unit. The name is either the default name (FGT<serial_number>) or the name given by an administrator. The name that appears in this field is the name that appears in Host Name in <i>System > Status</i> in the System Information widget.
device_id=(FGT50B3G06500085)	The serial number of the FortiGate unit.
log_id=(0624000000)	A number identifying the log message. In the above example, 06 identifies the log as the content archive log and 24 identifies the content archive log as a web archive log message.
log_type=(contentlog)	The type of log. The log types are traffic, event, attack, antivirus, web filter, and spam filter.
subtype=(HTTP)	The subtype of the content archive. In this example, it is web because the subtype is HTTP.
pri=(information)	The severity or priority level of the event. For more information, see “Log severity levels” on page 20 .
vd=(root)	The virtual domain where the traffic was logged.
fwver=(040000)	The firmware version that was running when the log message was recorded.
SN=(613874)	The session number of the log message.
user=(“user1”)	The name of the user creating the traffic.
group=(“usergroup”)	The name of the group creating the traffic.
carrier_ep=(N/A)	The FortiOS Carrier end-point identification. For example, it displays the MSISDN of the phone that sent the MMS message. If you do not have FortiOS Carrier, this field always display N/A.
cat=(N/A)	The FortiGuard web site category number.
cat_desc=(N/A)	The name of the FortiGuard web site category.
content log version: (3)	The content log version number.
timestamp: (240060590)	The time of the recorded content archive log.
serial number: (0)	The session number of the content archive log.
client IP:(172.16.25.142)	The IP address of the client server.
server IP: (172.25.124.133)	The IP address of the server where the mail came from.

HTTP status: (clean)	Indicates the status of the HTTP content. This can be any one of the following: <ul style="list-style-type: none">• clean• infected• heuristic• banned_word• blocked• exempt• oversize
number of bytes from client: (401)	The number of bytes that were received from the client.
number of bytes from server: (4203)	The number of bytes that were received from the server.
HTTP command: (GET)	The type of HTTP command used. In this example, it was the GET command.
url= (172.25.124.133/favicon.ico)	The URL address of the web site that was accessed.

Antivirus log messages

The Antivirus log records virus incidents in Web, FTP, and email traffic. The following is an example of an antivirus log message.

```
2009-02-26 05:52:42 devname=FGT50B3G06500085
device_id=FGT50B06500085 log_id=0213066000 type=virus
subtype=oversize pri=notice vd=root fwver=040000 policyid=1
serial=110961 user="user23" group="admingroup"
src=172.16.22.122 sport=1254 src_int="port1" dst=10.10.25.1
dport=80 dst_int="wan1" profile="Profile_Office" service="http"
agent="n/a" status="passthrough"
url="http://172.16.25.124/finance/finance_headquarters/headqua
rters_pic1.png" ref="n/a" msg="File exceeds size limit."
```

date=(2009-02-26)	The year, month and day of when the event occurred in yyyy-mm-dd format.
time=(05:52:42)	The hour, minute and second of when the event occurred in the format hh:mm:ss.
devname=(FGT50B3G06500085)	The name of the FortiGate unit. The name is either the default name (FGT<serial_number>) or the name given by an administrator. The name that appears in this field is the name that appears in Host Name in <i>System > Status</i> in the System Information widget.
device_id=(FGT50B3G06500085)	The serial number of the FortiGate unit.
log_id=(0213066000)	A ten-digit number. The first two digits represent the log type and the following two digits represents the log subtype. The last five digits are the message ID.
type=(virus)	The section of system where the event occurred.
subtype=(oversize)	The subtype of the log message. This represents a policy applied to the FortiGate feature in the firewall policy.
pri=(notice)	The severity level of the event. For more information, see "Log severity levels" on page 20 .
vd=(root)	The virtual domain where the event originated from.
fwver=(0400)	The firmware version that was running when the log message was recorded.
policyid=(1)	The firewall policy identification number.
serial=(110961)	The serial number of the log.
user=("user23")	The name of the user creating the traffic.
group=("admingroup")	The name of the group creating the traffic.
src=(172.16.22.122)	The source IP address.
sport=(1254)	The source port of where the traffic is originating from.
src_int=("port1")	The interface of the source. In this example, the source interface is the internal interface of the FortiGate unit.
dst=(10.10.25.1)	The destination IP address.
dport=(80)	The destination port of where the traffic is going to.
dst_int=("wan1")	The interface of the destination. In this example, the destination interface is the external interface of the FortiGate unit.
profile=("Profile_Office")	The protection profile associated with the firewall policy that traffic used when the log message was recorded.

service= ("http")	The service of where the activity or event occurred, whether it was on a web page using HTTP or HTTPS. The service field can have the protocols HTTP, FTP or SMTP.
agent= ("n/a")	This field is for FortiGate units running FortiOS Carrier. If you do not have FortiOS Carrier running on your FortiGate unit, this field always displays N/A.
status= ("passthrough")	The action the FortiGate unit took when the event occurred.
url= ("http://172.16.25.127/finance/finance_headquarters/headquarters_pic1.png")	The URL address of where the file was acquired.
ref= ("n/a")	The URL reference that gives more information about the virus. If you enter the URL in your web browser's address bar, the URL directs you to the specific page that contains information about the virus.
msg= ("File exceeds size limit.")	Explains the activity or event that the FortiGate unit recorded. In this example, the file that was downloaded from the web site exceeded the specified size limit.

WebFilter log messages

The Webfilter log messages record HTTP FortiGate log rating errors, including web content blocking actions that the FortiGate unit performs. The following is an example of a Web filter log message.

```
2009-03-10 11:56:04 devname=FGT50B3G06500085
device_id=FGT50B3G06500085 log_id=0315093003 type=webfilter
subtype=urlfilter pri=information vd=root fwver=0400000
policyid=4 serial=613044 user="user23" group="admingroup"
src=172.16.22.122 sport=2364 src_int="internal"
dst="10.10.30.120" dport=80 dst_int="wan2" service="http"
hostname="a.example.com" profile="ProtectionProfile_1"
status=exempted req_type="referral" url="example1.example.com"
msg="URL was exempted because it is in the URL filter list"
```

date=(2009-03-10)	The year, month and day of when the event occurred in yyyy-mm-dd format.
time=(11:56:04)	The hour, minute and second of when the event occurred in the format hh:mm:ss.
devname=(FGT50B3G06500085)	The name of the FortiGate unit. The name is either the default name (FGT<serial_number>) or the name given by an administrator. The name that appears in this field is the name that appears in Host Name in <i>System > Status</i> in the System Information widget.
device_id=(FGT50B3G06500085)	The serial number of the FortiGate unit.
log_id=(0315093003)	A ten-digit number. The first two digits represent the log type and the following two digits represent the log subtype. The last five digits are the message ID.
type=(webfilter)	The section of system where the event occurred.
subtype=(urlfilter)	The subtype of the log message. This represents a policy applied to the FortiGate feature in the firewall policy.
pri=(information)	The severity level of the event. For more information, see "Log severity levels" on page 20 .
vd=(root)	The virtual domain where the event was logged.
fwver=(04000)	The firmware version that was running when the log message was recorded.
policyid=(4)	The firewall policy identification number.
serial=(613044)	The serial number of the log ID.
user=("user23")	The name of the user creating the traffic.
group=("admingroup")	The group name of the user creating the traffic.
src=(172.16.22.122)	The source IP address.
sport=(2364)	The source port number.
src_int=("internal")	The name of the source interface. In this example, the source interface is the internal interface of the FortiGate unit.
dst=(10.10.30.120)	The destination IP address.
dport=(80)	The destination port number.
dst_int=("wan2")	The name of the destination interface. In this example, the destination interface is the external interface of the FortiGate unit.
service=("http")	The service of where the event or activity occurred.

hostname= ("a.example.com")	The name of the web site accessed.
profile= ("ProtectionProfile_1")	The protection profile that was used with the firewall policy.
status=(exempted)	The status of the action taken when the event occurred. In this example, the URL was exempted.
req_type=("referral")	The type of request, which can be one of the following: <ul style="list-style-type: none">• referral – If the HTTP transaction is requested from a parent web site such as selecting a link on a web page.• direct – a direct connection to a web page, such as typing in the URL address manually.
url= ("example1.example.com")	The URL of the web site.
msg=("URL was exempted because it is in the URL filter list.")	Explains the activity or event that the FortiGate unit recorded. In this example, the URL is exempted since that URL is specified as exempt in the URL filter list.

Attack log messages

The Attack log messages record all attacks that occur against your network. These log messages also contain links to the Fortinet Vulnerability Encyclopedia where you can better assess the attack. When viewing these log messages from *Log&Report > Remote*, you can view the packet log that is associated with an attack log message.

The following is an example of an attack log message.

```
2009-03-09 15:02:40 dev_name=FGT50B3G06500085
device_id=FGT50B3G06500085 log_id=0419070000 type=ips
subtype=signature pri=alert vd=root fwver=040000 policyid=2
serial=581265 attack_id=13707 severity=high carrier_ep=N/A
profile=N/A sensor="all_default_pass" src=172.16.22.122
dst=10.10.20.10 src_port=52903 dst_port=139 src_int="wan1"
dst_int="internal" status=detected proto=6 service=139/tcp
user=user55 group=usergroup_1
ref="http://www.fortinet.com/ids/VID13707" count=1
incident_serialno=86324148 msg="netbios:
MS.Network.Share.Provider.Unchecked.Buffer.DoS"
```

date=(2009-03-09)	The year, month and day of when the event occurred in yyyy-mm-dd format.
time=(15:02:40)	The hour, minute and second of when the event occurred in the format hh:mm:ss.
devname=(FGT50B3G06500085)	The name of the FortiGate unit. The name is either the default name (FGT<serial_number>) or the name given by an administrator. The name that appears in this field is the name that appears in Host Name in <i>System > Status</i> in the System Information widget.
device_id=(FGT50B3G06500085)	The serial number of the FortiGate unit.
log_id=(0419070000)	A ten-digit number. The first two digits represent the log type and the following two digits represent the log subtype. The last five digits are the message ID.
type=(ips)	The part of the system where the event occurred.
subtype=(signature)	The subtype of the log message.
pri=(alert)	The severity level of the event. For more information, see "Log severity levels" on page 20 .
vd=(root)	The virtual domain where the event was logged.
fwver=(04000)	The firmware version that was running when the log message was recorded.
policyid=(2)	The firewall policy identification number.
serial=(581265)	The serial number of the log message.
attack_id=(12707)	The identification number of the attack log message.
severity=(high)	The specified severity level of the attack.
carrier_ep=(N/A)	The FortiOS Carrier end-point identification. For example, it would display the MSISDN of the phone that sent the MMS message. If you do not have FortiOS Carrier, this field always display N/A.
profile=(N/A)	The protection profile associated with the firewall policy that traffic used when the log message was recorded.
sensor=("all_default_pass")	The DLP sensor that was used.
src=(172.16.22.122)	The source IP address.
dst=(10.10.20.10)	The destination IP address.

src_port=(52903)	The source port number.
dst_port=(139)	The destination port number.
src_int=("wan1")	The name of the source interface.
dst_int=("internal")	The name of the destination interface.
status=(detected)	The status of the action the FortiGate unit took when the event occurred. In this example, the FortiGate unit detected an attack.
proto=(6)	The protocol of the event.
service=(139/tcp)	The service of where the event or activity occurred.
user=(user55)	The name of the user creating the traffic.
group=(usergroup_1)	The name of the group creating the traffic.
ref=("http://www.fortinet.com/ids/VID13707")	The reference URL of where to find more information about the attack.
count=(1)	The number of times that attack was detected within a short period of time. This is useful when the attacks are DoS attacks.
incident_serialno=(86324148)	The unique ID for this attack. This number is used for cross-referencing IPS packet logs.
msg= ("netbios:MS.Network.Share.Provider.Unchecked.Buffer.DoS")	Explains the activity or event that the FortiGate unit recorded. In this example, an attack occurred that could have caused a system crash.

Antispam log messages

The antispam log messages record blocking of email address patterns and content in SMTP, IMAP and POP3 traffic. The following is an example of an antispam log message.

```
2009-03-20 09:19:04 devname=FGT50B3G06500085
device_id=FGT50B3G06500085 log_id=0509083003 type=emailfilter
subtype=pop3 pri=notice vd=root fwver=04000 policyid=1
serial=511989 user="N/A" group="N/A" src=172.16.130.25
sport=1874 src_int="internal" dst=192.168.39.8 dport=110
dst_int="wan2" service="pop3" profile="Profile_1"
status="detected" from="admin1@example.com"
to="user23@example.com" msg="from email address is in email
blacklist.(no.4 pattern matched)"
```

date=(2009-03-20)	The year, month and day of when the event occurred in yyyy-mm-dd format.
time=(09:19:04)	The hour, minute and second of when the event occurred in the format hh:mm:ss.
devname=(FGT50B3G06500085)	The name of the FortiGate unit. The name is either the default name (FGT<serial_number>) or the name given by an administrator. The name that appears in this field is the name that appears in Host Name in <i>System > Status</i> in the System Information widget.
device_id=(FGT50B3G06500085)	The serial number of the FortiGate unit.
log_id=(0509083003)	A ten-digit number. The first two digits represent the log type and the following two digits represent the log subtype. The last five digits are the message id.
type=(emailfilter)	The section of system where the event occurred.
subtype=(pop3)	The subtype of the log message. This represents a policy applied to the FortiGate feature in the firewall policy.
pri=(notice)	The severity level of the event. For more information, see "Log severity levels" on page 20 .
vd=(root)	The virtual domain where the event was logged.
fwver=(04000)	The firmware version that was running when the log message was recorded.
policyid=(1)	The firewall policy identification number.
serial=(511989)	The serial number of the log.
user=("N/A")	The name of the user creating the traffic.
group=("N/A")	The name of the group creating the traffic.
src=(172.16.130.25)	The source IP address.
sport=(1874)	The source port.
src_int=("internal")	The name of the source interface.
dst=(192.168.39.8)	The destination IP address.
dport=("110")	The destination port.
dst_int=("wan2")	The name of the destination interface.
service=("pop3")	The service of where the event or activity occurred.
profile=("Profile_1")	The protection profile associated with the firewall policy that traffic used when the log message was recorded.
status=("detected")	The action the FortiGate unit took when the attack occurred.

from= ("admin1@example.com")	The sender's email address.
to= ("user23@example.com")	The receiver's email address.
msg=["from email address is in email blacklist. (no.4 pattern matched)"]	Explains the activity or event that the FortiGate unit recorded. In this example, the sender's email address is in the blacklist and matches the fourth email address in that list.

Data Leak Prevention log message

The Data Leak Prevention log messages record events that may be either leaking out from or entering your network.

The following is an example of a data leak prevention log message.

```
2009-03-10 12:22:36 devname=FGT50B3G06500085
device_id=FGT50B3G06500085 log_id=0954110000 type=dlp
subtype=dlp pri=notice vd=root fwver=040000 policyid=1
serial=613874 user="user1" group="admingroup" src=172.16.20.144
sport=2504 src_int="internal" dst=172.16.152.255 dport=80
dst_int="wan2" service="http" status="detected"
hostname="172.16.152.255" url="/favicon.ico"
from="user22@example.com" to="user55@example.com" msg="data
leak detected(Data Leak Prevention Rule matched)"
rulename="All-HTTP" action="log-only"
```

date=(2009-03-10)	The year, month and day of when the event occurred in yyyy-mm-dd format.
time=(12:22:36)	The hour, minute and second of when the event occurred in the format hh:mm:ss.
devname=(FGT50B3G06500085)	The name of the FortiGate unit. The name is either the default name (FGT<serial_number>) or the name given by an administrator. The name that appears in this field is the name that appears in Host Name in <i>System > Status</i> in the System Information widget.
device_id=(FGT50B3G06500085)	The serial number of the FortiGate unit.
log_id=(095411000)	A ten-digit number. The first two digits represent the log type and the following two digits represent the log subtype. The last five digits are the message id.
type=(dlp)	The section of system where the event occurred.
subtype=(dlp)	The subtype of the log message.
pri=(notice)	The severity level of the event. For more information, see "Log severity levels" on page 20 .
vd=(root)	The virtual domain where the event was logged.
fwver=(04000)	The firmware version that was running when the log message was recorded.
policyid=(1)	The firewall policy identification number.
serial=(613874)	The serial number of the log.
user=("user1")	The name of the user creating the traffic.
group=("admingroup")	The name of the user group creating the traffic.
src=(172.16.20.144)	The source IP address.
sport=(2504)	The source port.
src_int=("internal")	The name of the source interface.
dst=(172.16.152.255)	The destination IP address.
dport=(80)	The destination port.
dst_int=("wan2")	The name of the destination interface.
service=("http")	The service of where the event or activity occurred.
status=("detected")	The action the FortiGate unit took when the attack occurred.
hostname=("172.16.152.255")	The host name. In this example it is an IP address.

from= ("user22@example.com")	The sender's email address.
to= ("user55@example.com")	The receiver's email address.
msg= [("data leak detected (Data Leak Prevention Rule matched")]	Explains the activity or event that the FortiGate unit recorded. In this example, the data leak that was detected match the rule, All-HTTP, in the DLP sensor.
rulename= ("All-HTTP")	The name of the rule within the DLP sensor.
action= ("log-only")	The action that was specified within the rule. In some rules within sensors, you can specify content archiving. If no log type is specified, this field displays log-only.

Application control log message

The application control log messages records IM, P2P and VoIP activity. This log file also records some IPS activities.

The following is an example of an application control log message.

```
2009-03-10 12:24:23 devname=FGT50B3G06500085
device_id=FGT50B3G06500085 log_id=1059116020 type=app-crt1
subtyp=app-crt1-all pri=notice vd=root fwver=0400000
user="user23" group="admingroup" carrier_ep="N/A" kind=N/A
profile="N/A" dir=N/A src=172.16.23.99 src_port=443
src_int="wan1" dst=10.10.20.1 dst_port=2524 dst_int="internal"
src_name="172.16.23.99" dst_name="10.10.20.1" proto=6
service="2524/tcp" policyid=1 serial=613935 app_list="App_1"
app_type="N/A" app="Unknown Application" action=pass count=1
msg=":Unknown Application"
```

date=(2009-03-10)	The year, month and day of when the event occurred in yyyy-mm-dd format.
time=(12:24:23)	The hour, minute and second of when the event occurred in the format hh:mm:ss.
devname=(FGT50B3G06500085)	The name of the FortiGate unit. The name is either the default name (FGT<serial_number>) or the name given by an administrator. The name that appears in this field is the name that appears in Host Name in <i>System > Status</i> in the System Information widget.
device_id=(FGT50B3G06500085)	The serial number of the FortiGate unit.
log_id=(1059116020)	A ten-digit number. The first two digits represent the log type and the following two digits represent the log subtype. The last five digits are the message id.
type=(app-crt1)	The section of system where the event occurred.
subtype=(app-crt1-all)	The subtype of the log message. This represents a policy applied to the FortiGate feature in the firewall policy.
pri=(notice)	The severity level of the event. For more information, see "Log severity levels" on page 20 .
vd=(root)	The virtual domain where the event was logged.
fwver=(0400000)	The firmware version that was running when the log message was recorded.
user=("user23")	The name of the user creating the traffic.
group=("admingroup")	The name of the group creating the traffic.
carrier_ep=("N/A")	The FortiOS Carrier end-point identification. For example, it would display the MSISDN of the phone that sent the MMS message. If you do not have FortiOS Carrier, this field always display N/A.

kind=(N/A)	The type of operation which triggered the action. This can be any one of the following: <ul style="list-style-type: none"> • login • chat • file • photo • audio • call • regist • unregister • call-block • request • response
profile=(“N/A”)	The protection profile associated with the firewall policy that traffic used when the log message was recorded.
dir=(N/A)	The direction of the traffic that triggered the action, which can be incoming, outgoing, N/A, or unknown.
src=(172.16.23.99)	The source IP address.
sport=(443)	The source port.
src_int=(“wan1”)	The name of the source interface.
dst=(10.10.20.1)	The destination IP address.
dport=(2524)	The destination port.
dst_int=(“internal”)	The name of the destination interface.
proto=(6)	The protocol that applies to the session or packet. The protocol number in the packet header that identifies the next level protocol. Protocol number's are assigned by the Internet Assigned Number Authority (IANA).
service=(“2524/tcp”)	The service of where the event or activity occurred.
policyid=(1)	The firewall policy identification number.
serial=(613935)	The session number of the application control log message. same as dlp
app_list=(“App_1”)	The name of the application control list that triggered the action.
app_type=(“N/A”)	The type of application that triggered the action within the control list.
app=(“Unknown Application”)	The name of the application that triggered the action within the control list.
action=(pass)	The action that was taken by the application control engine. This can be any one of the following: <ul style="list-style-type: none"> • pass • block • monitor • kickout • encrypt-kickout • reject • unknown
count=(1)	The number of times the same event was detected within a short period of time.
msg=(:Unknown Application”)	Explains the activity or event that the FortiGate unit recorded. In this example, the application control list App_1 detected an unknown application.

FORTINET®

www.fortinet.com

FORTINET®

www.fortinet.com