FortiGate Logging with FortiOS 3.0
Version 3.0

www.fortinet.com

FortiGate Logging with FortiOS 3.0 Technical Note
Version 3.0
08 September 2008
01-30000-0381-20080908

Trademarks

Regulatory compliance

FCC Class A Part 15 CSA/CUS

Contents

Introduction

This document introduces you to FortiGate logging in FortiOS 3.0 and includes information on where to enable logging of FortiGate features. It also includes explanations about each log message recorded in FortiOS 3.0.

FortiGate Logging in FortiOS 3.0 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 chapter contains the following topics:

- Revision history
- About logging in FortiOS 3.0
- Fortinet documentation
- Fortinet documentation
- Customer service and technical support

Revision history

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.

About logging in FortiOS 3.0

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

FortiOS 3.0 logging enables you 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 3.0 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, Syslog or WebTrends 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(s) or severity level is logged in a given time period, enabling you to quickly respond to a potential problem or prevent a problem from occurring.

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 Install 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*

  Describes how to use the FortiGate CLI and contains a reference to all FortiGate CLI commands.
- *FortiGate Log Message Reference*

  Available exclusively from the Fortinet Knowledge Center, the FortiGate Log Message Reference describes the structure of FortiGate log messages and provides information about the log messages that are generated by FortiGate units.
- *FortiGate High Availability User Guide*

  Contains in-depth information about the FortiGate high availability feature and the FortiGate clustering protocol.
- *FortiGate IPS User Guide*

  Describes how to configure the FortiGate Intrusion Prevention System settings and how the FortiGate IPS deals with some common attacks.
- *FortiGate IPSec VPN User Guide*

  Provides step-by-step instructions for configuring IPSec VPNs using the web-based manager.

- *FortiGate SSL VPN User Guide*

  Compares FortiGate IPSec VPN and FortiGate SSL VPN technology, and describes how to configure web-only mode and tunnel-mode SSL VPN access for remote users through the web-based manager.
- *FortiGate PPTP VPN User Guide*

  Explains how to configure a PPTP VPN using the web-based manager.
- *FortiGate Certificate Management User Guide*

  Contains procedures for managing digital certificates including generating certificate requests, installing signed certificates, importing CA root certificates and certificate revocation lists, and backing up and restoring installed certificates and private keys.
- *FortiGate VLANs and VDOMs User Guide*

  Describes how to configure VLANs and VDOMS in both NAT/Route and Transparent mode. Includes detailed examples.

Fortinet documentation CD

All Fortinet documentation is available from the Fortinet documentation CD shipped with your Fortinet product. The documents on this CD are current at shipping time. For up-to-date versions of Fortinet documentation see the Fortinet Knowledge Center.

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

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

Please visit the Fortinet Technical Support web site at http://support.fortinet.com to learn about the technical support services that Fortinet provides.

Logging in FortiOS 3.0

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 3.0.

If you require more information about FortiGate logging in FortiOS 3.0, see the *FortiGate Administration Guide* and the *FortiGate CLI Reference*.

The following topics are included in this section:

- FortiGate log types
- Log severity levels
- Enabling logging
- Alert Email

Note: The following procedures were updated to FortiOS 3.0 MR7.

In FortiOS 3.0 MR6, all FortiGate units can log to a FortiGuard Analysis server, if they have a subscription for FortiGuard Analysis and Management Service. For more information about this FortiGuard service, see the *FortiGuard Analysis and Management Service Administration Guide* and the *FortiGate Administration Guide*.

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 Filter	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.
IM/P2P	ilog.log	The IM and P2P log records the following: • instant message text • audio communications • file transfers attempted by users • time of a transmission attempt • type of IM applications used and the content of the transmission • VoIP SIMPLE block messages

VoIP	plog.log	The VoIP log records VoIP SCCP violations including SIP blocked.
Content	clog.log	The content log records all log messages, including most IM log messages as well as the following VoIP log messages: • 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 1: 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 1, 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 3.0, there are many different logs you can enable. Depending on what you choose to log, you need to enable the logging in various locations in 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: In FortiOS 3.0 MR7, enabling interface traffic logging is no longer available. If you want to log traffic, you can only log firewall policy traffic.

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 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 Edit 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 Edit 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 IM and P2P logging

The IM and P2P logs record instant message text, file transfers and audio communications, file transfers attempted by users, the time the transmission was attempted, the type of IM application used and the content of the transmission.

To enable IM and P2P 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 IM Activity.
5. Select Log P2P Activity.
6. Select OK.

Enabling VoIP logging

You can log Voice over Internet Protocol (VoIP) calls. You can also configure VoIP rate limiting for Session Initiated Protocol (SIP) and Skinny Client Control Protocol (SCCP) or Skinny protocol. SIP and SCCP are two types of VoIP protocols.

Rate limiting is generally different between SCCP and SIP. For SIP, rate limiting is for that SIP traffic flowing through the FortiGate unit. For SCCP, the call setup rate is between the FortiGate unit and the clients because the call manager normally resides on the opposite side of the FortiGate unit from the clients.

To enable VoIP 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 VoIP Activity.
5. Select OK.

To configure VoIP activity

1. Go to **Firewall > Protection Profile**.
2. Select Edit beside the protection profile that you want.
3. Select the Expand Arrow beside VoIP to reveal the available options.
4. Select the SIP and SCCP check boxes/policy.
5. Enter a number for requests per second in the Limit REGISTER request (requests/sec/policy) (SIP only) field.
6. Enter a number for requests per second in the Limit INVITE request (requests/sec/policy) (SIP only field).
7. Enter a number for the maximum calls per minute in the Limit Call Setup (calls/min/client) (SCCP only) field.
8. Select OK.

Enabling content archive logging

If you want to archive log files, you require a FortiAnalyzer unit. The FortiAnalyzer unit will store email, FTP, web, instant messaging, and VoIP. You can only archive VoIP messages if you are running FortiGate 3.0 MR4 and higher.

To enable content archive logging

1. Go to **Firewall > Protection Profile**.
2. Select Edit beside the protection profile that you want.
3. Select the Expand Arrow beside Content Archive to reveal the available options.
4. Select the check boxes of the protocols that you require for “Display content meta-information on the system dashboard”.
5. Select one of the following in the Archive to FortiAnalyzer/FortiGuard list:

None	No logs will be archived to the log location.
Summary	Only a summary of the logs will be archived to the log location. The FortiGuard Analysis and Management Service provides only summary content archiving.
Full	The entire log will be archived to the log location. This option is only available for logging to a FortiAnalyzer unit.

6 Select Apply.

Alert Email

An alert email notifies you when the FortiGate unit records a log message at a specified severity level. If FortiOS 3.0 MR2 or higher is installed on the FortiGate unit, you can configure an alert email to notify you of either an event logged or a severity level logged. For example, if you require notification about an administrator logging in and out, you can configure the FortiGate unit to send an alert email whenever administrators logs in and out of the FortiGate unit.

Configuring Alert Email

The FortiGate unit uses the SMTP server name to connect to the mail server. When configuring an alert email, you must configure at least one DNS server if you are configuring an Fully Qualified Domain Name (FQDN); if not, you can specify a specific IP address.

The method of configuring an alert email varies slightly depending on the maintenance release.

To configure an alert email in FortiOS 3.0 MR1

1 Go to **Log&Report > Log Config > Alert Email**.

2 Enter the information for the following options:

SMTP Server	The name/address of the SMTP email server.
Email from	The SMTP user name.
Email to	Enter up to three email recipients for the alert email message.
Authentication Enable	Select to enable SMTP authentication.
SMTP user	Enter the user name for logging on to the SMTP server. You only need to do this if you have enabled the SMTP authentication.
Password	Enter the password for logging on to the SMTP server. You only need to do this if you selected SMTP authentication.

3 Select Test Connectivity to receive a test email message to the email account you configured.

4 Select the severity level for sending an alert email based on severity level.

5 Enter the number of minutes for each severity level.

6 Select Apply.

To configure an alert email in FortiOS 3.0 MR2 and higher

1 Go to **Log&Report > Log Config > Alert Email**.

2 Enter the information for the following options.

SMTP Server	The name/address of the SMTP email server.
Email from	The SMTP user name.
Email to	Enter up to three email recipients for the alert email message.
Authentication: [Enable]	Select the Enable check box to enable SMTP authentication.
SMTP user	Enter the user name for logging on to the SMTP server. You only need to do this if you have enabled the SMTP authentication.
Password	Enter the password for logging on to the SMTP server. You only need to do this if you selected SMTP authentication.

3 Select Test Connectivity to receive a test email message to the email address that you configured in the previous step.

4 Select “Send alert email for the following” if you require sending an email based on one or more of the following:

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 to send an alert email message based on intrusion detection.
Virus detected	Select to send an alert email message based on virus detection.
Web access blocked.	Select to send an alert email message based on blocked web sites that were accessed.
HA status changes	Select to send an alert email message based on HA status changes.
Violation traffic detected	Select to send an alert email message based on violated traffic your FortiGate unit detects.
Firewall authentication failure	Select to send an alert email message based on firewall authentication failures.
Administrator login/logout	Select to send an alert email message based on whether the administrator logs in and logs out.
IPSec tunnel errors	Select to send an alert email message based on where there is an error in the IPSec tunnel configuration.
Configuration changes	Select to send an alert email message based on any changes made to the FortiGate configuration.
FortiGuard license expiry time (1-9999 days)	Enter the number of days for notification of the FortiGuard license expiry time.
FortiGuard log quota usage	Select if you require an alert email message based on the FortiGuard Analysis server log disk quota getting full.

5 If you want to send an alert based on a log severity level, select Send an alert based on severity.

This enables the FortiGate unit to send an alert email message whenever a specific log level appears in the log.

6 Select the Minimum severity level from the list.

7 Select Apply.

Note: The default minimum severity level is Alert. If the FortiGate unit collects more than one log message before an interval is reached, the FortiGate unit combines the messages and sends one alert email. For more information about log messages and log severity levels, see the *FortiGate Log Message Reference* and "Log severity levels" on page 10.

Storing logs

The FortiGate unit can log to several different destinations, providing greater flexibility when storing log files. The FortiGate unit can log to a FortiAnalyzer unit, Syslog server, WebTrends server, the FortiGate system memory, or hard disk if available.

By default, the FortiGate unit logs to memory or hard disk if available. The FortiGate system memory has a limited capacity and when full, the FortiGate unit overwrites the oldest log messages. The FortiGate system memory is able to store most log entries, except Traffic and Content logs, because of their size and frequent entries. The FortiGate hard disk, if available, stores logs similar to the FortiGate system memory but contains more space than system memory.

The FortiAnalyzer unit is a Fortinet network appliance that provides integrated log collection analysis tools and data storage. The FortiAnalyzer unit also provides current historical analysis of network activity to help identify security issues and reduce network misuse and abuse.

In FortiOS 3.0 MR6 and higher, all FortiGate units can log to a FortiGuard Analysis server when you subscribe to FortiGuard Analysis and Management Service. The FortiGuard Analysis and Management Service is a subscription-based service that provides logging, reporting and remote management features. Fortinet recommends reviewing the *FortiGuard Analysis and Management Administration Guide* because of its detailed information about this FortiGuard service.

The Syslog server is a remote computer running syslog software. Syslog is a standard for forwarding log messages in an IP network. The Syslog server is both convenient and flexible since any computer, either Linux or Unix systems, can run syslog software.

WebTrends is a remote computer running a NetIQ WebTrends firewall reporting server and is similar to a Syslog server. FortiGate log formats comply to WebTrends log formats. WebTrends is a traffic analysis tool, mainly used for gathering and analyzing data on web traffic.

The following provides information on configuring these four devices.

- Logging to memory
- Logging to a FortiAnalyzer unit
- Connecting to FortiAnalyzer using Automatic Discovery
- Logging to a FortiGuard Analysis server
- Logging to a Syslog server
- Logging to a WebTrends server
- 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.

The following topics also include logging to the FortiGuard Analysis server. This option is available only when subscribed to the FortiGuard Analysis and Management Service Fortinet recommends reviewing the *FortiGuard Analysis and Management Service Administration Guide* because of its detailed information about this FortiGuard service.

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 10.

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

Logging to a FortiAnalyzer unit

The Automatic Discovery feature is another way to connect to a FortiAnalyzer unit in FortiOS 3.0. In FortiOS 3.0, you can connect to a FortiAnalyzer unit either by using the Automatic Discovery feature or by going to **Log&Report > Log Config**.

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.

Connecting to FortiAnalyzer using Automatic Discovery

Automatic Discovery is a method of establishing a connection to a FortiAnalyzer unit. 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.

Note: FortiAnalyzer 3.0 MR2 and higher is required when using the Automatic Discovery feature on the FortiGate unit. The Automatic Discovery is enabled only when FortiAnalyzer is selected under Remote Logging.

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.

Testing the FortiAnalyzer configuration

After configuring FortiAnalyzer settings, you can test the connection between the FortiGate 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

1. Go to **Log&Report > Log Config > Log Settings**.
2. Select Test Connectivity.

Logging to a FortiGuard Analysis server

You can configure logging to a FortiGuard Analysis server after registering for the FortiGuard Analysis and Management Service on the Fortinet support web site. Fortinet recommends verifying that the connections between the FortiGuard Analysis and Management Service and the FortiGate unit are working properly before configuring logging to a FortiGuard Analysis server.

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 FortiGate 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 10.

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 FortiGate units.

Enable CSV Format Select to have logs formatted in CSV format. When you enable CSV format, the FortiGate unit produces the log in Comma Separated Value (CSV) format. If you do not enable CSV format, the FortiGate 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

1 Log into the CLI.

2 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 WebTrends server.

```
config log webtrends settings
    set status enable
    set server 220.210.200.190
  end
```

Logging to multiple FortiAnalyzer units or Syslog servers

FortiOS 3.0 enables you to send log messages to multiple FortiAnalyzer units or multiple Syslog servers, providing additional redundant log storage.

Use the CLI to configure logging to multiple destinations.

Note: Before proceeding, review the relevant CLI commands for this feature in the *FortiGate CLI Reference*.

Configuring multiple FortiAnalyzer units

Before proceeding, make sure the FortiAnalyzer unit configured in “Logging to a FortiAnalyzer unit” on page 20 is properly connected.

It is recommended to contact a FortiAnalyzer administrator 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 3.0 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.

To enable logging to multiple FortiAnalyzer units

1 Log into the CLI.

2 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
```

3 Enter the following commands to configure logging FortiGate features to the FortiAnalyzer unit:

```
config log fortianalyzer2 filter
    set traffic {enable | disable}
    set web {enable | disable}
    set url-filter {enable | disable}
  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 configure logging FortiGate features to the FortiAnalyzer unit:

```
config log fortianalyzer3 filter
    set traffic {enable | disable}
    set web {enable | disable}
    set url-filter {enable | disable}
  end
```

6 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 22 is properly connected. All filter settings are enabled by default.

To enable logging to multiple Syslog servers

1 Log into the CLI.

2 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
```

3 Enter the following commands to configure logging FortiGate features to the Syslog server:

```
config log syslogd2 filter
    set traffic {enable | disable}
    set web {enable | disable}
    set url-filter {enable | disable}
  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
```

5 Enter the following commands to configure logging FortiGate features to the Syslog server:

```
config log syslogd3 filter
    set traffic {enable | disable}
    set web {enable | disable}
    set url-filter {enable | disable}
  end
```

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, informing 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 3.0.

Log file names generated in FortiOS 3.0 MR3 and higher have a specific naming convention that identifies the log type, FortiGate unit, VDOM, along with the date and time that the log file was rolled.

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.

Note: The following log messages are updated to FortiOS 3.0 MR7. Log messages recorded in FortiOS 3.0 MR7, contain two additional fields in the log header: devname (device name) and device_id (device serial number).

Log types and sub-types

The following table provides an explanation of the log types and sub-types in FortiOS 3.0.

Table 2: 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 event	34
		his-performance – performance statistics	43
		vip ssl – VIP SSL events	45
		ldb-monitor – LDB monitor events	46

Table 2: Log types and subtypes

content archive (Content Archive Log)	06	HTTP – Virus infected FTP – FTP content metadata SMTP – SMTP content metadata POP3 – POP3 content metadata IMAP – IMAP content metadata	24 25 26 27 28
virus (Antivirus Log)	02	infected – Virus infected filename – Filename blocked oversize – File oversized	11 12 13
webfilter (Web Filter Log)	03	content – content block urlfilter – URL filter FortiGuard block FortiGuard allowed FortiGuard error ActiveX script filter Cookie script filter Applet script filter	14 15 16 17 18 35 36 37
ids (Attack Log)	04	signature – Attack signature anomaly – Attack anomaly	19 20
emailfilter (Spam Filter Log)	05	SMTP POP3 IMAP	08 09 10
im (Instant Messaging)	07	IM – Instant Messaging activity	31
voip (Voice Over Internet Protocol)	08	sip – VoIP activity	40

Content Archive logs are only available on FortiGate units running FortiOS 3.0 MR3 and higher. Voice over Internet Protocol (VoIP) logs are only available on FortiGate units running FortiOS 3.0 MR4 or higher.

Traffic log messages

The Traffic log message records all traffic to and through the interfaces on the FortiGate unit.

```
2008-06-21 06:38:49 devname=FGT-60_125 device_id=FGT-
602803030702 log_id=0021010001 type=traffic subtype=allowed
pri=notice vd=root SN=2371 duration=144 user=N/A group=N/A
policyid=1 proto=6 service=443/tcp app_type=N/A
status=accept src=172.16.135.42 srcname=172.16.135.42
dst=172.24.120.193 dstname=172.24.120.193 src_int=internal
dst_int=external sent=3073 rcvd=14452 sent_pkt=17
rcvd_pkt=19 src_port=1156 dst_port=443 vpn=N/A
tran_ip=0.0.0.0 tran_port=0 dir_disp=org tran_disp=noop
```

The first half of a log message is called the log header. For example, in the above traffic log message the log header is:

```
2008-06-21 06:38:49 devname=FGT-60_125 device_id=FGT-
602803030702 log_id=0021010001 type=traffic subtype=allowed
pri=notice vd=root SN=2371
```

The rest of a log message is called the log body.

The following is a detailed explanation of the above example of a traffic log message.

date=(2007-03-05)	The year, month and day of when the event occurred in yyyy-mm-dd format.
time=(06:38:49)	The hour, minute and second of when the event occurred in the format hh:mm:ss.
devname=(FGT-60_125)	The default name of the FortiGate unit in short form with the last three digits of its internal IP address.
device_id=(FGT-602803030702)	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. The log types are traffic, event, attack, antivirus, webfilter, and spam filter.
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 10.
vd=(root)	The virtual domain where the traffic was logged. In this example, it is the root virtual domain.
SN=(2371)	The session number only appears in traffic log messages.
duration=(144)	This represents the value in seconds.
user=(N/A)	The name of the user creating the traffic.
group=(N/A)	The name of the group creating the traffic.
policy_id=(1)	The ID number of the firewall policy that applies to the session or packet.

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=(443/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: • 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=(172.16.135.42)	The source IP address.
srcname= (172.16.135.42)	The source name or the IP address.
dst=(172.24.120.193)	The destination IP address.
dstname= (172.24.120.193)	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=(external)	The interface where the through traffic goes to the public or Internet. For incoming traffic to the firewall, it is "unknown".
sent=(3073)	The total number of bytes sent.
rcvd=(14452)	The total number of bytes received.
sent_ pckt=(17)	The total number of packets sent during the session.
rcvd_pckt=(19)	The total number of packets received during the session.
src_ port=(1156)	The source port of the TCP or UDP traffic. The source protocol is zero for other types of traffic.
dst_ port=(443)	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.

```
2008-03-26 07:42:02 devname=FGT-60_125 device_id=FGT-
602803030702 log_id=0104032126 type=event subtype=admin
pri=notice vd=root user=”admin” ui=GUI(172.16.100.5) seq=4
sintf=”dmz” dintf=”internal” saddr=”all” daddr=”all”
schd=”always” svr=”ANY” act=accept nat=no log=no msg=”User
admin added firewall policy 4 from GUI(172.16.100.5)”
```

date=(2007-03-01)	The year, month and day of when the event occurred in yyyy-mm-dd format.
time=(07:42:02)	The hour, minute and second of when the event occurred in the format hh:mm:ss.
devname=(FGT-60_125)	The default name of the FortiGate unit in short form with the last three digits of its internal IP address.
device_id= (FGT-602803030702)	The serial number of the FortiGate unit.
log_id=(0104032126)	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. The log types are traffic, event, attack, antivirus, webfilter, and spam filter.
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 10.
vd=(root)	The virtual domain where the traffic was logged.
user=(“admin”)	The user’s admin profile, usually an administration user. In this example, the admin administrator changed the banned word.
ui=[GUI (172.16.100.5)]	The interface where this particular event occurred, along with the IP address of that interface. The ui includes GUI, CLI, console, and LCD.
seq=(4)	The sequence order of the firewall policies. In this example, the firewall policy was fourth when added to the Policy list.
sint=(“dmz”)	The name of the source interface specified in the firewall policy.
dintf=(“internal”)	The name of the destination interface specified in the firewall policy.
saddr=(“all”)	The source IP address specified in the firewall policy.
daddr=(“all”)	The destination IP address specified in the firewall policy.
schd=(“always”)	The type of schedule specified in the firewall policy.
svr=(“ANY”)	The type of service or service group specified in the firewall policy.
act=(“accept”)	The action the FortiGate unit should take for that firewall policy.
nat=(“no”)	The firewall policy has NAT selected or not selected NAT. If the FortiGate unit is in Transparent mode, `nat` will always be `“no”`.

log=(“no”)	The firewall policy has either logging enabled or disabled.
msg=(“User admin added firewall policy 4 from GUI (172.16.100.5)”	Explains the activity or event that the FortiGate unit recorded. In this example, an administrator added a fourth firewall policy from the IP address, 172.20.120.24

Content Archive logs

The Content Archive log message provides information concerning logs that are archived on the FortiAnalyzer unit. FortiOS 3.0 MR2 or higher is required to view Content Archive log messages on the FortiGate unit.

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

```
2008-07-24 21:28:05 devname=FGT-60_125 device_id=FGT-
602803030702 log_id=0627000000 type=contentlog subtype=POP3
pri=information vd=root user=”N/A” group=”N/A”
3:1647209140:1:10.10.20.10 <-> 192.168.20.101:clean:8412:
f/t=abbcc@xyz.com/ccaabb@xyz.com:0:Finance Meeting Today
```

date=2006-07-24	The year, month and day of when the event occurred in yyyy-mm-dd format.
time (21:28:05)	The hour, minute and second of when the content archive logged the email event.
devname=(FGT-60_125)	The default name of the FortiGate unit in short form with the last three digits of its internal IP address.
device_id= (FGT-602803030702)	The serial number of the FortiGate unit.
log_id= (0627000000)	A number identifying the log message. In the above example, 06 identifies the log as the content archive log and 27 identifies the content archive log as a POP3, indicating its about email.
log_type= (contentlog)	The type of log. The log types are traffic, event, attack, antivirus, web filter, and spam filter.
sub_type=(POP3)	The subtype of the content archive. In this example, it is email because the subtype is POP3.
pri=(information)	The severity or priority level of the event. For more information, see “Log severity levels” on page 10.
vd=(root)	The virtual domain where the traffic was logged.
user=(“N/A”)	The name of the user creating the traffic.
group=(“N/A”)	The name of the group creating the traffic.
content log version: (3)	The content log version number.
session number: (164729140)	The session number of the content archive log.
clientP:(10.10.20.4)	The IP address of the client server.
serverIP: (192.168.20.101)	The IP address of the server where the mail came from.
infectionstatus: (clean)	Indicates whether the email is infected with a virus or is clean.
size sent: (8412)	The size of the email sent.
ft=(abbcc@xyn.com/ ccaabb@xyn.com)	Indicates the sender and receiver of the email message.
attachment=(0)	Indicates whether there was an attachment or not with the email message.
subject=(Finance Meeting Today)	The subject line of the email message.

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.

```
2008-03-15 07:47:28 devname=FGT-60_125 device_id=FGT-
602803030702 log_id=0213066000 type=virus subtype=oversize
pri=notice vd=root serial=1630 user=”N/A” group=”N/A”
src=172.16.130.25 sport=1344 src_int=”internal”
dst=172.16.10.133 dport=80 dst_int=”external” service=”http”
status=passthrough file=”upgrade”
url=”http:///system/config/upgrade” ref=”N/A” msg=”File
exceeds size limit.”
```

date=(2007-02-19)	The year, month and day of when the event occurred in yyyy-mm-dd format.
time=(07:47:28)	The hour, minute and second of when the event occurred in the format hh:mm:ss.
devname=(FGT-60_125)	The default name of the FortiGate unit in short form with the last three digits of its internal IP address.
device_id=(FGT-602803030702)	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. The log types are traffic, event, attack, antivirus, webfilter, and spam filter.
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 10.
vd=(root)	The virtual domain where the event originated from.
serial=(1630)	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=(1344)	The source port of where the traffic is originating from.
src_int=”internal”	The interface of the source. In this example, the source interface is the internal interface of the FortiGate unit.
dst=(172.16.10.133)	The destination IP address.
dport=(80)	The destination port of where the traffic is going to.
dst_int=(“external”)	The interface of the destination. In this example, the destination interface is the external interface of the FortiGate unit.
service=http	The service used. It is always HTTP.
status=(passthrough)	The action the FortiGate unit took when the event occurred.
file=(“upgrade”)	The name of the file containing a virus or that appears suspicious to the FortiGate unit.
url=(“http:///system/config/upgrade”)	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, a reference URL address is given for more information about the suspicious virus.

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.

```
2008-02-26 12:52:44 devname=FGT-60_125 device_id=FGT-
602803030702 log_id=0315093003 type=webfilter
subtype=urlfilter pri=information vd=root serial=76914
user=”N/A” group=”N/A” src=172.16.130.25 sport=1576
src_int=”internal” dst=192.168.24.16 dport=80
dst_int=”external” service=”http” hostname=”www.chc.ca”
status=exempted url=”/includes/css/homepage.css” msg=”URL
was exempted because it is in the URL filter list”
```

date=(2007-02-26)	The year, month and day of when the event occurred in yyyy-mm-dd format.
time=(12:52:44)	The hour, minute and second of when the event occurred in the format hh:mm:ss.
devname=(FGT-60_125)	The default name of the FortiGate unit in short form with the last three digits of its internal IP address.
device_id= (FGT-602803030702)	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. The log types are traffic, event, attack, antivirus, webfilter, and spam filter.
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 10.
vd=(root)	The virtual domain where the event was logged.
serial=(76914)	The serial number of the log ID.
user=(“N/A”)	The name of the user creating the traffic.
group=(“N/A”)	The group name of the user creating the traffic.
src=(172.16.130.25)	The source IP address.
sport=(1576)	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=(192.168.24.16)	The destination IP address.
dport=(80)	The destination port number.
dst_int=(“external”)	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=(“www.chc.ca”)	The name of the website accessed.
status=(exempted)	The status of the action taken when the event occurred. In this example, the URL was exempted.

url=(”/includes/css/homepage.css”)	The URL of the website.
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. The following is an example of an attack log message.

```
2008-04-26 11:41:45 devname=FGT-60_125 device_id=FGT-
602803030702 log_id=0419070000 type=ips subtype=signature
pri=alert vd=root serial=75732 attack_id=0101947272
severity=high src=172.16.130.25 dst=192.168.24.16
src_port=1499 dst_port=443 src_int=internal dst_int=external
status=detected proto=6 service=https user=N/A group=N/A
ref="http://www.fortinet.com/ids/IDIo1974272"
msg="applications:OpenSSL.ASN.1.Double.Free"
```

date=(2007-02-26)	The year, month and day of when the event occurred in yyyy-mm-dd format.
time=(11:41:45)	The hour, minute and second of when the event occurred in the format hh:mm:ss.
devname=(FGT-60_125)	The default name of the FortiGate unit in short form with the last three digits of its internal IP address.
device_id=(FGT-602803030702)	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. The log types are traffic, event, attack, antivirus, webfilter, and spam filter.
subtype=(signature)	The subtype of the log message. This represents a policy applied to the FortiGate feature in the firewall policy.
pri=(alert)	The severity level of the event. For more information, see "Log severity levels" on page 10.
vd=(root)	The virtual domain where the event was logged.
serial=(75732)	The serial number of the log message.
attack_id=(0101947272)	The identification number of the attack log message.
severity=(high)	The specified severity level of the attack.
src=(172.16.130.25)	The source IP address.
dst=(192.168.24.16)	The destination IP address.
src_port=(1499)	The source port number.
dst_port=(443)	The destination port number.
src_int=(internal)	The name of the source interface.
dst_int=(external)	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=(https)	The service of where the event or activity occurred.
user=(N/A)	The name of the user creating the traffic.
group=(N/A)	The name of the group creating the traffic.

ref=("http://www.fortinet.com/ids/ID101974272")	The reference URL of where to find more information about the attack.
msg=("applications:OpenSSL.ASN.1.Double.Free")	Explains the activity or event that the FortiGate unit recorded.

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.

```
2008-05-28 07:25:14 devname=FGT-60_125 device_id=FGT-60-
2803030702 log_id=0509083003 type=emailfilter subtype=pop3
pri=notice vd=root serial=318 user=”N/A” group=”N/A”
src=172.16.130.25 sport=1303 src_int=”internal”
dst=192.168.39.8 dport=110 dst_int=”external” service=”pop3”
status=”detected” from=”trx@xyncompany.com”
to=”sdf@edncompany.com” msg=”from email address is in email
blacklist.(no.1 pattern matched)”
```

Note: In FortiOS 3.0 MR6, the banned word is included in the message field of the AntiSpam log message (83006).

date=(2007-03-05)	The year, month and day of when the event occurred in yyyy-mm-dd format.
time=(07:25:14)	The hour, minute and second of when the event occurred in the format hh:mm:ss.
devname=(FGT-60_125)	The default name of the FortiGate unit in short form with the last three digits of its internal IP address.
device_id= (FGT-602803030702)	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. The log types are traffic, event, attack, antivirus, webfilter, and spam filter.
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 10.
vd=(root)	The virtual domain where the event was logged.
serial=(318)	The serial number of the log.
user=(“N/A”)	The name of the user creating the traffic.
src=(172.16.130.25)	The source IP address.
sport=(1303)	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=(“external”	The name of the destination interface.
service=(“pop3)	The service of where the event or activity occurred.
status=(“detected”)	The action the FortiGate unit took when the attack occurred.
from= (“trx@xyncompany.com”)	The sender’s email address.

to= (“sdf@edncompany.com”)	The receiver’s email address.
msg=[“from email address is in email blacklist. (no.1 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 first email address in that list.

IM/P2P log messages

The IM/P2P feature records all instant messaging programs, including file transfers. The following is an example of an IM log message the FortiGate unit may record in FortiOS 3.0.

```
2008-08-14 11:45:49 devname=FGT-60_125 device_id=FGT-
602803030702 log_id=0731100004 type=im subtype=im-all
pri=information vd=root user=”N/A” group=”N/A” proto=msn
kind=login action=permit laddr=172.16.130.25
local=”aabbcc@ourcompany.com”
```

date=(2007-05-01)	The year, month and day of when the event occurred in yyyy-mm-dd format.
time=(11:45:49)	The hour, minute and second of when the event occurred in the format hh:mm:ss.
devname=(FGT-60_125)	The default name of the FortiGate unit in short form with the last three digits of its internal IP address.
device_id=(FGT-602803030702)	The serial number of the FortiGate unit.
log_id=(0731100004)	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=(im)	The section of system where the event occurred. The log types are traffic, event, attack, antivirus, webfilter, and spam filter.
subtype=(im-all)	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. There are six severity levels to specify. For more information, see “Log severity levels” on page 10.
vd=(root)	The virtual domain where the event was logged.
user=(“N/A”)	The name of the user creating the traffic.
group=(“N/A”)	The name of the group creating the traffic.
proto=(msn)	The protocol of the program that was used. The protocols are BitTorrent, eDonkey, Gnutella, Kazaa, Skype, or Winny.
kind=(login)	The type of action taken by the user who is creating the traffic.
action=(permit)	The action the FortiGate unit took when the program occurred.
laddr=(172.16.130.25)	The user’s local address.
local=(“aabbcc@ourcompany.com”)	The user’s login user name for logging into the instant messaging program.

VoIP log messages

The VoIP log messages records SIP, SCCP, and SIMPLE. The main VoIP log file is plog. The plog file logs violations with the exception of the SIMPLE protocol violations. SIMPLE protocol violations are logged to the IM log file, or ilog. VoIP log messages are generated from permitted VoIP traffic that is sent to the content log or clog.

VoIP log messages are separated into three types of log files, clog, plog, and the ilog. The ilog is the instant messaging log. The following shows the VoIP log message types that are associated with each VoIP log file type:

Message Type	Log file
SIP start call	clog
SIP end call	clog
SIP blocked	plog
SCCP phone registration	clog
SCCP call info (end of call)	clog
SCCP blocked	plog
SIMPLE log message	clog
SIMPLE block message	ilog

The following is an example of a violation VoIP log message (plog.log) that a FortiGate unit may generate:

```
2008-07-04 12:37:01 devname=FGT-60_125 device_id=FGT-
602803030702 log_id=08040106001 type=voip subtype=VOIP
pri=notice vd=root serial=15 user=”N/A” group=”N/A”
proto=sip kind=response action=block reason=unrecognized-
form req=REGISTER src=172.16.130.25 dst=192.168.110.68
from=” “ to=” “ repeat=1
```

date=(2007-02-21)	The year, month and day of when the event occurred in yyyy-mm-dd format.
time=(12:37:01)	The hour, minute and second of when the event occurred in the format hh:mm:ss.
devname= (FGT-60_125)	The default name of the FortiGate unit in short form with the last three digits of its internal IP address.
device_id= (FGT-602803030702)	The serial number of the FortiGate unit.
log_id=(08040106001)	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=voip	The section of system where the event occurred. The log types are traffic, event, attack, antivirus, webfilter, and spam filter.
subtype=(VOIP)	The subtype of the log message.
pri=(notice)	The severity level of the event. For more information, see “Log severity levels” on page 10.
vd=(root)	The virtual domain where the log file was generated from.
serial=(15)	The serial number of the log message.

user=("N/A")	The name of the user creating the traffic.
group=("N/A")	The name of the user group creating the traffic.
proto=(sip)	The protocol the telephone call used. In this example, it is the SIP protocol that was used for the telephone call.
kind=(response)	The type of VoIP message recorded by plog. In this example, the type is a response to a previous SIP request. Kind can also be
action=(block)	The action the FortiGate unit took when the telephone call occurred.
reason= (unrecognized-form)	The reason why the action was taken. In this example, the FortiGate unit did not recognize the SIP message and so the SIP message was dropped.
req=(REGISTER)	The type of request of the call. The type can be any SIP request type as defined by SIP RFCs, including the following: • ACK • REGISTER • CANCEL • INFO • INVITE • MESSAGE • NOTIFY • OPTIONS • PRAK • PUBLISH • REFER • SUBSCRIBE • UDPATE • UNKNOWN
src=(172.16.130.25)	The source IP address.
dst=(192.168.110.68)	The destination IP address.
from=(" ")	The person that is calling.
to=(" ")	The person that is receiving the call.
repeat=(1)	This indicates how many times the same action was detected or blocked in a period of 30 seconds. If a program is set to block and the user repeatedly tries to connect, instead of logging every single attempt, all attempts are logged in the 30 second period and logged as a single entry that indicates how many attempts the user made.

FORTINET™

www.fortinet.com

FORTINET™

www.fortinet.com