Operating FortiGate Units in Common Criteria Mode

FortiOS v2.80 MR5

FortiOS v2.80 MR5 Operating FortiGate Units in Common Criteria Mode	
Document Version:	2.2
Publication Date:	February 11, 2005
Description:	This document describes how to configure and operate FortiGate Antivirus Firewall in compliance with Common Criteria Evaluation Assurance Level (EAL) 4 as defined in *Security Target for the Fortinet FortiGate-50A, 60, 100A, 200A, 300A, 800, 3000, 3600, 5001 Antivirus Firewalls and FortiOS 2.80 CC Compliant Firmware: EAL 4+*, Version 0.90, 2 February 2005.
Document Number:	01-28005-0107-20050211
Hardware Models:	FortiGate models 50A, 60, 100A, 200A, 300A, 800, 3000, 3600, 5001
Firmware Version:	2.80,build275,050127

Fortinet Inc.

FortiOS v2.80 MR5 Operating FortiGate Units in Common Criteria Mode

February 11, 2005
01-28005-0107-20050211

Regulatory Compliance
FCC Class A Part 15 CSA/CUS

Table of Contents

Introduction

Common Criteria mode is an enhanced security option for some FortiGate Antivirus Firewall models. It requires the installation of Common Criteria certified firmware on validated versions of FortiGate unit hardware.

Security level summary

Fortinet Antivirus Firewalls meet the overall requirements of a CC EAL 4+ certification as defined in *Security Target for the Fortinet FortiGate-50A, 60, 100A, 200A, 300A, 800, 3000, 3600, 5001 Antivirus Firewalls and FortiOS 2.80 CC Compliant Firmware: EAL 4+*, Version 0.90, 2 February 2005. Fortinet Antivirus Firewalls also meet the U.S. Government *Traffic-Filter Firewall Protection Profile for Low-Risk Environments*, Version 1.1, April 1999 (TFFWLR PP).

Common Criteria security concerns

The following security issues are not addressed in the standard documentation set.

TSF domain separation

FortiOS maintains an isolated security domain for its own execution. Specifically:

- No unrelated applications are allowed to run on the FortiGate unit.
- No unrelated applications can be loaded onto the FortiGate unit.
- Administrators have no access to the operating system or the file system.
- All security and configuration data are stored in segregated configuration files.

Subset residual data protection

FortiOS ensures that no residual data from previous packets passing through a FortiGate unit is reused in any way. Any residual information in any resource is over-written or otherwise destroyed so that it cannot be reused or otherwise accessed either inadvertently or deliberately.

Restrictive default values

Enabling the CC mode of operation changes the configuration of the FortiGate unit to restrictive default values. For more information, see “Effects of CC-compliant mode” on page 12. The administrator can override the default values.

Reliable time stamps

The FortiGate unit provides reliable timestamps using an internal clock that the administrator can set manually or synchronize to an external time server using the NTP protocol.

Documentation

The documentation for FortiGate units operated in Common Criteria mode consists of this technical note and the following documents that comprise the standard FortiOS version 2.80 MR5 documentation set for FortiGate units:

- *FortiGate QuickStart Guide*

  Each *QuickStart Guide* provides the basic information required to connect and install a FortiGate model.
- *FortiGate Installation Guide*

  Each *Installation Guide* provides detailed information required to install a FortiGate model. Includes hardware reference, default configuration, installation procedures, connection procedures, and basic configuration procedures.
- *FortiGate Administration Guide*

  Each *Administration Guide* describes how to configure a FortiGate model. Configuration information includes how to use FortiGate firewall policies to control traffic flow through the FortiGate unit and how to configure VPN, IPS, antivirus, web filtering, spam filtering. The administration guide also describes how to use protection profiles to apply intrusion prevention, antivirus protection, web content filtering, and spam filtering to traffic passing through the FortiGate unit.
- *FortiGate CLI Reference Guide*

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

  Describes the structure of FortiGate log messages and provides information on all log messages generated by the FortiGate unit.
- *FortiGate High Availability Guide*

  Contains in-depth information about FortiGate High Availability and the FortiGate Clustering Protocol (FGCP).
- *FortiGate VPN Guide*

  Explains how to configure VPNs using the web-based manager.

The FortiGate online help also contains procedures for using the FortiGate web-based manager to configure and manage the FortiGate unit. For a complete list of FortiGate documentation visit Fortinet Technical Support at http://support.fortinet.com.

Fortinet Knowledge Center

The most recent Fortinet technical documentation is available from the Fortinet Knowledge Center. The knowledge center contains short how-to articles, FAQs, technical notes, product and feature guides, and much more. Visit the Fortinet Knowledge Center at http://kc.forticare.com.

Comments on Fortinet technical documentation

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

About this document

This technical note describes how to install Common Criteria (CC) compliant firmware on a FortiGate Antivirus Firewall unit and how to operate the unit in CC compliant mode. It provides information that is not included in the standard documentation provided with your FortiGate unit.

This document was created as part of the Common Criteria EAL 4+ validation of FortiGate Antivirus Firewalls and applies only to the models named in the security target document.

This technical note contains the following sections:

This document is intended to be used by a system administrator.

Secure operation of FortiGate units

Common Criteria operation requires both that you use the FortiGate Antivirus Firewall in its Common Criteria compliant mode and that you follow secure procedures for installation and operation of the FortiGate unit. You must ensure that:

- The FortiGate unit is installed in a secure physical location.
- Physical access to the FortiGate unit is restricted to authorized operators.
- LCD PIN codes are six digits long and not an easily-guessed sequence such as 123456.
- Administrative passwords are at least 8 characters long.
- Administrative passwords are changed regularly.
- Procedurally, the Administrator is also required to choose a password with the following characteristics:
  - One (or more) of the characters should be capitalized.
  - One (or more) of the characters should be numeric.
  - One (or more) of the characters should be non alpha-numeric (e.g. punctuation mark).
- Administration of the FortiGate unit is permitted using only certified administrative methods. These are:
  - Console connection
  - Directly connected web-based manager
  - Directly connected command line interface (CLI) access

- The FortiGate unit can be used in either of its two operation modes: NAT/Route or Transparent. NAT/route mode applies security features between two or more different networks (for example, between a private network and the Internet). Transparent mode applies security features at any point in a network. The current operation mode is displayed on the web-based manager Status page and in the output of the `get system status` CLI command. Also, on LCD-equipped units, Transparent mode is indicated by “CC-TP” or “CC-TB” on the LCD display.

Initial configuration of the FortiGate unit

This section describes how to upgrade your standard FortiGate firmware to CC-compliant firmware and configure the unit in the Common Criteria mode of operation. Proceed as follows:

- Verify the hardware version of your FortiGate unit.
- Install the unit following the procedures in the documentation.
- Register your FortiGate unit with Fortinet.
- Determine the appropriate CC-compliant firmware version for your unit and download it from Fortinet.
- Install the CC firmware.
- Verify the firmware version of your FortiGate unit.
- Set the administrator password.
- Enable Common Criteria compliant mode.
- Optionally, set the LCD PIN.

Verifying the hardware version of the unit

Check the label on the back of the unit to determine the hardware revision number. CC-validated hardware revisions are listed in Table 1.

Table 1: CC EAL4 certified FortiGate models and hardware versions

FortiGate Model	Hardware Version
FG-50A	C-5FA27-01-AA-0000
FG-60	C-4AN27-03-AA-0000
FG-100A	C-4DZ47-01-AA-0000
FG-200A	C-4AY89-01-AA-0000
FG-300A	C-4FK88-01-AA-0000
FG-800	C-4UT39-01-AA-0000
FG-3000	C-4JE25-02-AA-0000
FG-3600	C-4KW75-02-AA-0000
FG-5001	P-4CF76-01-AA-0000

Installing the unit

Both the *Quick Start Guide* and the Getting Started section of the *Installation Guide* for your FortiGate unit provide instructions on the physical installation and initial configuration of your unit. When you have completed these procedures you will be able to access both the web-based manager and Command Line Interface (CLI).

Registering the unit

For information about registering your FortiGate unit, see “Registering a FortiGate unit” in the System Maintenance chapter of the *Administration Guide* for your unit. You need the user name and password Fortinet provides to you to download the CC compliant firmware.

Downloading the CC-compliant firmware

There is a specific firmware version for each CC-validated FortiGate model, as listed in Table 2.

Table 2: CC EAL4 certified FortiGate models and firmware download files

FortiGate Model	Firmware Version
FG-50A	FGT_50A-v280-build028-cc.out
FG-60	FGT_60-v280-build028-cc.out
FG-100A	FGT_100A-v280-build028-cc.out
FG-200A	FGT_200A-v280-build028-cc.out
FG-300A	FGT_300A-v280-build028-cc.out
FG-800	FGT_800-v280-build028-cc.out
FG-3000	FGT_3000-v280-build028-cc.out
FG-3600	FGT_3600-v280-build028-cc.out
FG-5001	FGT_5000-v280-build028-cc.out

To download the firmware

1. Determine the appropriate firmware version from Table 2.
2. With your web browser, go to https://support.fortinet.com and log in using the name and password you received when you registered with Fortinet Support.
3. Navigate to the version 2.80 FortiOS Images and Notes page. Select Download Page for the CC-compliant firmware build you need. Save the file on the management computer or on your network where it is accessible from the FortiGate unit.

Installing the CC firmware

You install the CC-compliant firmware as an upgrade from the standard firmware.

To install the CC firmware

1. Using the management computer, connect to the unit's web-based manager. See the the *Quick Start Guide* or the *Installation Guide* for information.
2. Type admin in the name field. If you have assigned a password, type it in the Password field. Select Login.
3. Go to **System > Status**.
4. Under Unit Information > Firmware version, select Update.
5. Type the path and filename of the firmware image file, or select Browse and locate the file.
6. Select OK.
   The unit uploads the firmware image file, upgrades to the new firmware version, restarts, and displays the Login page. This process takes a few minutes.

Verifying the firmware version of the unit

Execute the following command from the command line:

```
get system status
```

The version line of the status display shows the FortiGate model number, firmware version, build number and date:

```
Version:Fortigate-800 2.80,build275,050127
```

Verify that your firmware version, build number and date match those in Table 3.

Table 3: CC EAL4 certified FortiGate models and firmware versions

FortiGate Model	Firmware Version
FG-50A	Fortigate-50A 2.80,build275,050127
FG-60	Fortigate-60 2.80,build275,050127
FG-100A	Fortigate-100A 2.80,build275,050127
FG-200A	Fortigate-200A 2.80,build275,050127
FG-300A	Fortigate-300A 2.80,build275,050127
FG-800	Fortigate-800 2.80,build275,050127
FG-3000	Fortigate-3000 2.80,build275,050127
FG-3600	Fortigate-3600 2.80,build275,050127
FG-5001	Fortigate-5000 2.80,build275,050127

Setting the administrator password

The default administrator account, admin, has a blank password. You cannot enable CC-compliant mode until you set a password of at least eight characters.

To set the admin password using the web-based manager

1. Go to **System > Admin > Administrators**.
2. Select the Change Password icon for the admin account.
3. Type the password in the New Password field, type it again in the Confirm Password field, and select OK.
4. Select the Log out icon.

To set the admin password using the CLI

```
config system admin
  edit admin
    set password <password>
  end
```

Enabling Common Criteria mode

If you have verified the firmware version and set the administrator password, you are ready to enable common criteria compliant mode. You must use a console connection to enable CC mode. If you try to use another type of connection, a “check permission failed” error occurs.

Note: When you enable CC mode, all of the configuration except the administrator password is lost.

To enable CC mode

1. Log in to the CLI and enter the following commands:

```
config system global
  set CC-mode enable
end
```

Note: If the CLI displays a message that the current image does not have a valid CC signature, you need to repeat the CC firmware installation procedure. This occurs because of signature differences between the CC build and the previously loaded build. After upgrading the CC firmware a second time, you can enable CC mode.

The CLI displays the following message:

```
Warning: most configuration will be lost,
do you want to continue? (y/n)
```

2. Type `y`.
   The CLI displays the following message:

```
Please enter admin password:
```

3. Type the Admin password.
   The FortiGate unit restarts and runs in CC-compliant mode.

CC mode status indicators

There are two status indicators that show whether the FortiGate unit is running in the Common Criteria compliant mode of operation:

Table 4: CC mode status indicators

Location	Indication
Front panel LCD	Common Criteria Mode
Output of `get system global` command	CC-mode: enable

Effects of CC-compliant mode

The following list describes, not necessarily in order, the effects of enabling CC mode with respect to the normal mode of operation.

- All previous configuration settings except the Administrator password are lost.
- The FortiGate unit front panel LCD displays “Common Criteria Mode”.
- The `get system global` CLI command display includes “CC-mode: enable”.
- Only one administrator at a time can access the FortiGate unit through any of the interfaces.
- Disk logging is enabled if the unit contains a hard disk drive. Otherwise, logging to memory is enabled for all log types including traffic logs.
- Reaching 95% of the log device storage capacity results in the FortiGate unit entering an error mode that shuts down all of the interfaces until the administrator intervenes.
- Anomaly detection and protection is applied to traffic addressed to the FortiGate unit.
- Logging is enabled for failed connection attempts to the FortiGate unit using TCP/IP ports other than 22 (ssh), 23 (telnet), 80 (HTTP), and 443 (HTTPS).
- All firewall policies are removed.

Setting the LCD PIN

In CC mode, the LCD front panel (available on some models) is disabled unless you set a PIN for it. Enter the following commands in the CLI:

```
config system global
   set lcdprotection enable
   set lcdpin <pin_integer>
   end
```

Use of non-CC compliant features

CC mode does not prevent you from re-enabling non-CC compliant features, but if you do so, you are not operating the FortiGate unit in strict CC compliance according to the Security Target.

Administration via the web-based manager

In CC-mode, the network interfaces by default do not allow administrative access, preventing you from using the web-based manager. You can re-enable use of the web-based manager using CLI commands on the console. This example enables HTTPS administrative access on the Internal interface to allow use of the web-based manager:

```
config system interface
  edit internal
     set allowaccess https
  end
```

To be CC compliant, the administration computer must be connected directly to the interface.

For detailed information about accessing the web-based manager, see “Connecting to the web-based manager“ in the *Installation Guide* for your unit.

Disabling Common Criteria mode

To return the FortiGate unit to the normal mode of operation, enter the following CLI command:

```
config system global
     set CC-mode disable
  end
```

Disabling CC mode erases the current configuration except for the administrator password.

Logging

The Common Criteria protection profile requires logging of all traffic and system events. The severity threshold for logging is set to the lowest level: information. This ensures that the maximum amount of information is logged.

By default, logs are written to local hard disk. If there is no hard disk, logs are written to memory. Models 50A, 60, 100A, 200A and 5001 do not have hard disks. To check for a hard disk, execute the following command from the command line:

```
get system status
```

The output includes a line that indicates “Log hard disk:Available” or “Log hard disk:Not Available”.

The FortiGate unit generates warning log entries when the disk or memory allocated for logging is filled to 75%, then 90% and finally 95% of capacity. When logs exceed 95% of capacity, the default action is to block further traffic and switch to Error mode. See “Clearing Error mode” on page 18 for more information.

Logging to external devices is disabled due to the security requirements of Common Criteria operation, except for downloading of logs to the management computer. See “Backing up log messages” on page 17.

Table 5 and Table 6 list the disk and memory logging settings required for CC-mode. If you change the following options from the default, the operation of your FortiGate unit is no longer common criteria-compliant.

Table 5: config log {disk | memory} filter command keywords and variables

Keywords and variables	Description	Default	Availability
`admin {disable | enable}`	Enable or disable logging all administrative events, such as user logins, resets, and configuration updates in the event log.	`enable`	All models. `event enable` only.
`allowed {disable | enable}`	Enable or disable logging all traffic that is allowed according to the firewall policy settings in the traffic log.	`enable`	All models. `traffic enable` only.
`auth {disable | enable}`	Enable or disable logging all firewall-related events, such as user authentication in the event log.	`enable`	All models. `event enable` only.
`event {disable | enable}`	Enable or disable the event log.	`enable`	All models.
`severity {alert | critical | debug | emergency | error | information | notification | warning}`	Select the logging severity level. The FortiGate unit logs all messages at and above the logging severity level you select. For example, if you select `error`, the unit logs `error`, `critical`, `alert` and `emergency` level messages. `emergency` - The system is unusable. `alert` - Immediate action is required. `critical` - Functionality is affected. `error` - An erroneous condition exists and functionality is probably affected. `warning` - Functionality might be affected. `notification` - Information about normal events. `information` - General information about system operations. `debug` - Information used for diagnosing or debugging the FotiGate unit.	`information`	All models.
`system {disable | enable}`	Enable or disable logging of all system-related events, such as ping server failure and gateway status, in the event log.	`enable`	All models. `event enable` only.
`traffic {disable | enable}`	Enable or disable the traffic log.	`enable`	All models.
`violation {disable | enable}`	Enable or disable logging of all traffic that violates the firewall policy settings in the traffic log.	`enable`	All models. `trafic enable` only.

Table 6: config log {disk | memory} setting command keywords and variables

Keywords and variables	Description	Default	Availability
`diskfull {blocktraffic | nolog | overwrite}`	Enter the action to take when the log memory is full.	`blocktraffic`	All models.
`status {disable | enable}`	Enter `enable` to enable logging to the FortiGate system memory.	`enable`	All models.

Viewing log messages from the CLI

You can view and clear log messages from the CLI. Before viewing logs, you must set filter options to select the logs that you want to view. You can view one log category on one device at a time. Optionally, you can filter the listing to show only specified date ranges or severities of log messages. For traffic logs, you can filter log messages by source or destination IP address.

Setting filtering for log messages

You set up log message filtering using the `execute log filter` command. Commands are cumulative. If you omit a required variable, the command displays the current setting.

```
execute log filter <keyword> <variable>
```

Table 7: execute log filter command keywords and variables

Keywords and variables	Description	Default	Availability
`category {event | ids | spam | traffic | virus | webfilter | list }`	Type of log, except `list`, which displays the current setting.	`event`	All models.
`device {disk | memory | list}`	Device where the logs are stored, except `list`, which displays the current setting.	`disk`	Models numbered 300 and higher with hard disk.
`dst_ip <ipv4_str>`	Destination IP for traffic logs.	No default.	All models.
`dst_ip_range <ipv4_str>-<ipv4_str>`	Destination IP range for traffic logs.	No default.	All models.
`end_day <integer>`	Latest day of date range.	`1`	All models.
`end_level {alert | critical | debug | emergency | error | info | notice | warning | list}`	Log severity - end level `list` displays the current setting.	`emergency`	All models.
`end_month <integer>`	Latest month of date range.	`1`	All models.
`end_time <time_str>`	Latest time of date range.	`00:00:00`	All models.
`end_year <integer>`	Latest year of date range.	`9999`	All models.
`keyword <string>`	Word or part of word to match in log message. Case sensitive.	None	All models.
`list`	Display current filter settings.	No default.	All models.
`number <integer>`	Number of log entries displayed per page.	`10`	All models.

Table 7: execute log filter command keywords and variables (Continued)

Keywords and variables	Description	Default	Availability
`src_ip <ipv4_str>`	Source IP for traffic logs.	No default.	All models.
`src_ip_range <ipv4_str>-<ipv4_str>`	Source IP range for traffic logs.	No default.	All models.
`start_day <integer>`	Earliest day of date range.	`1`	All models.
`start_index <integer>`	Position in filtered logs from which to begin display. 1 starts from beginning of filtered logs.	`1`	All models.
`start_level {alert | critical | debug | emergency | error | info | notice | warning | list}`	Log severity - start level `list` displays the current setting.	information	All models.
`start_month <integer>`	Earliest month of date range.	1	All models.
`start_time <time_str>`	Earliest time of date range.	`00:00:00`	All models.
`start_year <integer>`	Earliest year of date range.	0000	All models.

Use as many `execute log filter` commands as you need to define the log messages that you want to view. For example, to select the memory event logs from 12-16 July 2004, you use the following commands:

```
execute log filter category event
execute log filter device memory
execute log filter start-year 2004
execute log filter end-year 2004
execute log filter start-month 07
execute log filter end-month 07
execute log filter start-day 12
execute log filter end-day 16
execute log filter start-time 00:00:00
execute log filter end-time 23:59:59
execute log filter keyword invalid
```

Viewing log messages

After you have selected the log messages that you want to view using the `execute log filter` command, you can display them with the following command:

```
execute log display
```

The console displays the first 10 log messages. To view more messages, run the command again. You can do this until you have seen all of the selected log messages. To restart viewing the list from the beginning, use the commands

```
execute log filter start_index 1
execute log display
```

Resetting log filters

You can restore the log filters to their default values using the command

```
execute log reset
```

Backing up log messages

You can back up log messages to your Administrative computer or other computer directly connected to the appropriate network interface. The backup includes logs that have rolled over.

To back up log messages

1. Install a TFTP server on the computer in the directory where you want to receive the log files.
2. Use a crossover cable to connect the computer to the appropriate network interface. On models 800 and below, connect to the Internal interface; on other models, connect to port 1.
3. Start the TFTP server.
4. Connect to the CLI interface.
5. To back up all log messages, execute the following command:

   ```
   execute backup alllogs <tftp_server_ip_address>
   ```

   To back up only a specific log type, execute the following command:

   ```
   execute backup log <tftp_server_ip_address> <log_type>
   ```

   `<log_type>` can be one of: `traffic`, `event`, `ids`, `virus`, `webfilter` or `spam`.

   The FortiGate unit reports each transferred file as follows:

   ```
   Connect to tftp server 192.168.1.1 ...
   Please wait...
   ##Sent log file /var/log/tlog to tftp server as
   tlog_20041014_080007 OK.
   ```

Viewing log file information

You can view the list of current and rolled log files on the console. The list shows the file name, size and timestamp. The CLI command is as follows:

```
execute log list <category>
```

`<category>` must be one of: `event`, `ids`, `spam`, `traffic`, `virus` or `webfilter`.

The output looks like this:

```
elog                 8704    Fri Jan 28 14:24:35 2005
elog.1               1536    Thu Jan 27 18:02:51 2005
elog.2              35840    Wed Jan 26 22:22:47 2005
```

At the end of the list the total number of files in the category is displayed. For example:

```
501 event log file(s) found.
```

Deleting filtered log messages

You can select log messages with the `execute log filter` command and then delete them with the command:

```
execute log delete-filtered
```

For example, to delete all the traffic logs, enter the following commands:

```
execute log filter category traffic
execute log delete-filtered
```

For information about the `execute log filter` command, see "Setting filtering for log messages" on page 15.

Deleting rolled log files

You can delete rolled log files using the `execute log delete-rolled` command:

```
execute log delete-rolled <category> <start> [<end>]
```

`<category>` must be one of: `event`, `ids`, `spam`, `traffic`, `virus` or `webfilter`. The `<start>` and `<end>` values represent the range of log files to delete. If `<end>` is not specified, only the log number specified by `<start>` is deleted.

For example, to delete all of the rolled traffic log files, enter the following command:

```
execute log delete-rolled traffic 1 9999
```

Clearing Error mode

The FortiGate unit switches to Error mode, shuts down network interfaces and blocks traffic when:

- logging to memory consumes more than 95% of allocated memory

or

- current and rolled log files consume more than 95% of disk capacity

The FortiGate unit indicates Error mode as follows:

- The console displays "CC error:", the cause of the failure, and "Entering ERROR mode."
- The CLI prompt has "CC-ERR" appended to it, `FortiGate-800 CC-ERR #`, for example.

To resume normal CC mode operation, you must reduce the logs to below 95% of device capacity. Then you can exit Error mode. On units with a hard disk, delete rolled log files. On units that log to memory, delete filtered log file entries. Ideally you should reduce logs to 50% or less of device capacity. For information on how to delete logs, see "Deleting filtered log messages" on page 18. To disable error mode, enter the following CLI command:

```
execute errormode exit
```

The FortiGate unit resumes normal CC compliant operation unless there is still too little free space on the log device.