FortiOS 5.4 and FortiGate NGFW Appliances

FIPS 140-2 and Common Criteria Technote

FORTINET DOCUMENT LIBRARY

http://docs.fortinet.com

FORTINET VIDEO GUIDE

http://video.fortinet.com

FORTINET BLOG

https://blog.fortinet.com

CUSTOMER SERVICE & SUPPORT

https://support.fortinet.com

http://cookbook.fortinet.com/how-to-work-with-fortinet-support/

FORTIGATE COOKBOOK

http://cookbook.fortinet.com

FORTINET TRAINING SERVICES

http://www.fortinet.com/training

FORTIGUARD CENTER

http://www.fortiguard.com

FORTICAST

http://forticast.fortinet.com

END USER LICENSE AGREEMENT

http://www.fortinet.com/doc/legal/EULA.pdf

FORTINET PRIVACY POLICY

https://www.fortinet.com/corporate/about-us/privacy.html

FEEDBACK

Email: techdocs@fortinet.com

Thursday, April 12, 2018

FIPS 140-2 and Common Criteria Technote for FortiOS 5.4 and FortiGate NGFW Appliances

01-544-416377-20170426

TABLE OF CONTENTS

Introduction

Fortinet performs FIPS 140-2 and Common Criteria certifications on specific FortiOS versions in combination with specific FortiGate family hardware models. At the publication date of this document, the latest CC certified version of FortiOS is 5.4.

The documentation set for FortiGate units operated in FIPS-CC mode consists of this document and the standard FortiOS 5.4 documentation set. This document covers Common Criteria specific installation instructions and explains the FortiOS FIPS-CC mode of operation.The standard documentation is available from the Fortinet Technical Documentation web site (http://docs.fortinet.com).

For detailed information on the FortiOS 5.4 Common Criteria certification, including the certified hardware models, refer to the FortiOS 5.4 Security Target. The Security Target can be found on the Fortinet Support web site in the FortiOS 5.4 FIPS-CC certified firmware download directory (http://support.fortinet.com).

References

Security Target: FortiGate NGFW Appliances running FortiOS 5.4, Version 1.0, 30 November 2017
FIPS 140-2 Security Policy: FortiOS 5.4, Version 2.8, March 28 2018
FortiOS Handbook - The Complete Guide to FortiOS
The FortiGate Cookbook 5.4
FortiOS 5.4.1 CLI Reference
FortiOS 5.4.4 Log Reference
Model specific Hardware Information Supplements

Certified Models

FG/FWF-50E	FG-100E	FG-500D	FG-3000D
FG/FWF-51E	FG-101E	FG-600D	FG-3100D
FG-52E	FG-200D	FG-800D	FG-3200D
FG/FWF-60E	FG-200E	FG-900D	FG-3700D
FG/FWF-61E	FG-201E	FG-1000D	FG-3810D

FG-60E-PoE	FG-240D	FG-1200D	FG-3815D
FG-80E	FG-240D-PoE	FG-1500D	FG-5001D
FG-81E	FG-300D	FG-2000E	FGT-VM/KVM
FG-81E-PoE	FG-400D	FG-2500E	

Installing the CC Certified Firmware

This section describes how to install the CC certified firmware on your FortiGate unit.

Verifying secure delivery

Before installing the FortiGate unit, you should take steps to ensure the unit has not been tampered with during transit. Perform the following checks to verify the integrity of the unit prior to installation.

- Courier - Fortinet only uses bonded couriers such as UPS, FedEx or DHL. Verify the shipment was received using a bonded courier.
- Shipping information - Verify the shipment information against the original purchase order or evaluation request. Verify the shipment has been received directly from Fortinet.
- External packaging - Verify the Fortinet branded packing tape sealing the packaging is intact and the packaging has not been cut or damaged to allow access to the unit.
- Internal packaging - Verify the unit is sealed in an undamaged, clear plastic bag for non-blade units. For blade units, verify the internal box packaging is intact.
- Warranty seal - For non-blade units, verify the unit's warranty seal is intact. The warranty seal is a small, grey sticker with the Fortinet logo and is normally placed over a chassis access screw. The chassis cannot be opened without destroying the warranty seal.

If you identify any concerns while verifying the integrity of the unit, contact your supplier immediately.

Registering the unit

Register your product in order to access firmware builds, customer support, etc. You can register your FortiGate unit through the Fortinet Support Website. Refer to the Fortinet Support Website User Guide for details on registering your product.

Installation Requirements

Common Criteria compliant operation requires that you use the FortiGate unit in its FIPS-CC mode of operation and that you follow secure procedures for installation and operation of the 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.
- A Fortinet entropy token is used to seed the RBG (for models other than the FortiGate-2000E and 25005 - see the Entopy Section for details) and the Fortinet entropy token remains in the USB port during operation (to allow for periodic reseeding of the RBG).

Installing the unit

The documentation shipped with your unit includes a FortiGate/FortiWiFi WiFi QuickStart Guide and a model specific Hardware Supplement. The FortiOS Handbook includes a Getting Started chapter that provides additional installation and configuration details. These documents 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).

Downloading the FIPS-CC certified firmware and MD5 check sums

To download the firmware and MD5 check sums

1. With your web browser, go to https://support.fortinet.com/ and log in using the name and password you received when you registered your unit with Fortinet Support.
2. Navigate to the FortiGate 5.4. FIPS-CC Certified download page. Download the firmware build for your specific hardware model. Save the file on the management computer or on your network where it is accessible from the FortiGate unit.
3. Download the md5sum.txt file from the same directory as the firmware. This file contains MD5 check sums for the firmware builds.

Note that upgrading a FortiGate unit running a FortiOS 5.0 (or earlier) certified build in FIPS-CC mode to FortiOS 5.4 is not officially supported. Back up your configuration and contact Fortinet Support before starting.

Verifying the integrity of the firmware build

Use a hashing utility to create an MD5 hash of the firmware build you downloaded. Compare the resulting hash to the corresponding hash from the `md5sum.txt` file. If the hashes match, the downloaded build is uncorrupted and unmodified.

Installing the FIPS-CC firmware build

Install the FIPS-CC firmware build on your FortiGate unit. There are several methods to do this. Refer to the FortiGate Cookbook, FortiGate Handbook or FortiGate CLI Guide for more information.

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. For example:

```
Version: FortiGate-300D v5.4.4,build9791,170925
```

Verify in the relevant security target or security policy document that your firmware version, build number and date are correct.

Potential Firmware issues

If the unit is not booting correctly and power cycling the unit does not clear the problem, then it may be necessary to reinstall the firmware. The firmware can be reinstalled using the FortiGate BIOS boot menu and a remote tftp server. The BIOS can also be used to format the boot device prior to reinstalling the firmware to ensure a clean installation.

Refer to the following Cookbook recipe for more details: Navigating the FortiGate BIOS

You may want to contact Fortinet's technical support group before attempting to use the FortiGate BIOS tools. You can open a support ticket on the support website.

Potential Hardware issues

If the unit fails any of the startup hardware checks or displays a hardware fault during operation, contact Fortinet technical support.

Entropy

Generation of strong encryption keys requires a strong source of random data, also referred to as entropy. FortiOS 5.4 makes use of two different strong entropy sources, depending on the model: the FortiASIC CP9 and the Fortinet Entropy Token. FortiOS also includes a basic, software based entropy source that is used if the model does not yet support the CP9 entropy source, does not include a CP9 chip, the entropy token is not installed or the entropyt token is installed, but not enabled.

The FortiASIC CP9

The CP9 entropy source is supported by the following models when running the FortiOS 5.4.4 CC certified build:

- FortiGate-2000E
- FortiGate-2500E

These models use the CP9 by default as the FortiOS entropy source - no configuration changes are required.

The Fortinet Entropy Token

Based on a wide band, Gaussian white noise generator, the Fortinet Entropy Token provides users with a simple, FIPS 140-2 and NDPP CC validated source of entropy.

The Fortinet Entropy Token is compatible with FortiOS 5.0.10 or higher.

Installing the entropy token

Plug the entropy token into an available USB port on the FortiGate unit. Note that the entropy token requires a USB-A port.

Configuring the entropy token settings

Use of the entropy token is required for FIPS 140-2 and Common Criteria compliance. It is possible to disable the use of the token in FIPS-CC mode, but doing so means the unit is not operating in a FIPS or CC compliant manner. There are three options for the entropy token setting:

- `enable` — token required
- `disable` — token is not required and is not used even if present
- `dynamic` — token is not required, but is used if present

To enable FIPS-CC mode with use of the entropy token enter the following commands from the FortiGate console.

```
config system fips-cc
   set status enable
   set entropy-token enable
```

```
end
```

See the FIPS-CC Mode of Operation section for complete details on enabling the FIPS-CC mode of operation.

The FIPS-CC mode of operation can only be enabled from the FortiGate console.

RBG Seeding and Reseed Interval

The RBG is seeded from the entropy token or CP9 during the boot process and then reseeded periodically. The default reseed period is once every 24 hours (1440 minutes) and is configurable using the `self-test-period` CLI command.

To set the reseed interval to 60 minutes, enter the following commands from the FortiGate CLI.

```
config system fips-cc
   set self-test-period 60
end
```

The entropy token must be present to allow the RNG to seed or reseed from the token.

When FortiGate is configured in FIPS-CC mode with the entropy token enabled, if the token is not present at boot time or the reseed interval, the boot process will pause until the token is inserted. The following message is displayed on the console:

```
Please insert entropy-token to complete RNG seeding
```

The message is repeated until the token is inserted.

If the entropy token is set to dynamic and the token is not present at boot time or the scheduled reseed interval, the unit will use the default, internal FortiOS seed method instead.

Using the Entropy Token with FortiGate-VM

In order to use the entropy token with FortiGate-VM running on a hypervisor, the USB port the token is using must first be mapped to the FortiGate-VM instance. To do this on a FortiHypervisor appliance, use the following steps:

1. Determine determine the USB bus and device ID by running the `diagnose hardware lsusb` command and looking for the entropy token VID:PID string (22a7:3001). On a FortiHypervisor-500D, the result will look similar to the following. In this example the entropy token is device 2 on bus 6.

```
diagnose hardware lsusb
   Bus 006 Device 002 22a7:3001
   Bus 001 Device 001 1d6b:0002 Linux Foundation 2.0 root hub
   Bus 002 Device 001 1d6b:0002 Linux Foundation 2.0 root hub
   Bus 003 Device 001 1d6b:0001 Linux Foundation 1.1 root hub
   Bus 004 Device 001 1d6b:0001 Linux Foundation 1.1 root hub
```

```
Bus 005 Device 001 1d6b:0001 Linux Foundation 1.1 root hub
Bus 006 Device 001 1d6b:0001 Linux Foundation 1.1 root hub
Bus 007 Device 001 1d6b:0001 Linux Foundation 1.1 root hub
Bus 008 Device 001 1d6b:0001 Linux Foundation 1.1 root hub
Bus 009 Device 001 1d6b:0001 Linux Foundation 1.1 root hub
```

2. Assign the entropy token to the FortiGate-VM using the following commands on the FortiHypervisor console. This example assumes the FortiGate-VM is instance 1 on the FortiHypervisor:

```
config vm instance
   edit 1
      config usb
         edit 1
            set bus 6
            set device 2
         end
end
```

3. Enable the entropy token on the FortiGate-VM.

The FIPS-CC Mode of Operation

If you have verified the firmware version, you are ready to enable FIPS-CC mode.

When you enable FIPS-CC mode, the existing configuration is cleared and restrictive default settings are implemented.

You must use a console connection to enable FIPS-CC mode. Enabling FIP-CC mode is not supported via the GUI or SSH in FortiOS.

The new password must be at least 8 characters long and must contain at least one each of:

- upper-case-letter
- lower-case-letter
- numeral
- non-alphanumeric character

Enabling FIPS-CC mode

Use the following steps to enable FIPS-CC mode:

1. If required, plug the entropy token into a USB port on the FortiGate unit.
2. Log in to the CLI through the console port. Use the default admin account or another account with a super_admin access profile. Enter the following commands.

```
config system fips-cc
   set status enable
   set entropy-token [enable|disable|dynamic]
   set self-test-period [1 to 1440]
end
```

3. In response to the following prompt, enter the new password for the administrator:

```
Please enter administrator password:
```

4. When prompted, re-enter the administrator password. The CLI displays the following message:

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

5. Enter `y`. The FortiGate unit restarts and is now running in FIPS-CC mode.
6. Verify FIPS mode is enabled. The `get system status` CLI command output should include “FIPS-CC mode: enable”.

Disabling FIPS-CC mode

To disable the FIPS-CC mode of operation, reset the unit to the factory default configuration using the following CLI command:

```
execute factoryreset
```

Disabling FIPS-CC mode erases the current configuration and zeroizes most keys and critical security parameters. To completely zeroize the unit, refer to the instructions in the next section.

Key Zeroization

All keys and CSPs are zeroized by erasing the unit's boot device and then power cycling the unit. To erase the boot device, execute the following command from the CLI:

```
execute erase-disk <boot device>
```

The boot device ID may vary depending on the FortiGate module. The following command will output a list of the available internal disks:

```
execute erase-disk ?
```

Erasing the unit's boot device will leave the unit unbootable. The firmware can be reinstalled used the FortiGate BIOS boot menu tools and a tftp server.

Common Criteria compliant operation

Use of non-CC evaluated features

FIPS-CC mode does not prevent you from using features that were not part of the evaluated configuration. However, if you use these features, you may not be operating the FortiGate unit in strict compliance with the Security Target. Refer to the Security Target for more information.

Install Updated Certificates

By default, FortiGate units use a certificate signed by a Fortinet Certificate Authority (CA). Administrators should install a new, signed certificate from a trusted CA for the unit itself and optionally a second certificate for use in VPN connections. Consult the FortiGate Administration Guide for additional information on replacing the default certificate.

Trusted Hosts

Trusted hosts should be configured for Administrators to improve security. FortiWeb supports up to three trusted hosts per Administrator account. Refer to the FortiOS Handbook for details on how to configure trusted hosts.

Disabling NPU support

The encryption algorithms used in the Fortinet FortiASIC NP4 and NP6 network processors are not FIPS validated and using them for packet level encryption is not compliant with the evaluated configuration as described in the Common Criteria Security Target. Refer to the unit's datasheet, available from http://www.fortinet.com, to determine if your unit includes network processors, which type and on which ports. Refer to the Hardware Acceleration section of the FortiOS Handbook for details on disabling specific capabilities of the processors or the entire processor if desired.

Administration Specific Changes

This section describes administration specific changes to the way FortiOS functions in the FIPS-CC mode of operation.

Remote access requirements

In FIPS-CC mode, remote administration via HTTP or Telnet is disabled. HTTPS, SSH or the console should be used. The FIPS-CC mode of operation restricts the cipher suites used by HTTPS and SSH to a subset of the NDcPP compliant suites. Refer to the Security Target for additional information. The administrator does not need to take any specific actions to ensure compliance when using HTTPS or SSH as long as the FIPS-CC mode of operation has been enabled.

Web browser requirements

To use the web-based manager in FIPS-CC mode, your web browser application must meet the following requirements:

- Authentication algorithm: PKCS1 RSA
- Connection security: TLS 1.1 or 1.2

Enabling administrative access

In FIPS-CC mode, remote administrative access is disabled by default. You can enable use of the web-based manager using CLI commands on the console. This example adds HTTPS and SSH administrative access on the port1 interface:

```
config system interface
   edit port1
      set allowaccess https ssh
end
```

For detailed information about accessing the web-based manager, see “Connecting to the GUI” in the *FortiGate 5.4 Administration Guide*.

Configuration backup

Configuration backup files created in FIPS-CC mode are not compatible with backup files created in non-FIPS-CC mode. A FIPS-CC mode configuration backup cannot be restored in non-FIPS-CC mode and vice-versa.

You can create FIPS-CC configuration backup files to use for disaster recovery. They are valid on a replacement FortiGate unit or to restore configuration after you exit and then re-enter FIPS-CC mode.

Refer to the FortiGate Administration Guide for detailed information about creating configuration backup files.

Admin access disclaimer

In order to meet NDcPP (Network Device Protection Profile) compliance, a pre-login disclaimer banner must be enabled.

To enable the disclaimer, log in to the CLI using the default admin account or another account with a super_ admin access profile. Enter the following commands:

```
config system global
   set pre-login-banner enable
end
```

Please note that a post-login disclaimer banner is enabled by default. If desired, this disclaimer can be disabled by entering the following command:

```
config system global
   set post-login-banner disable
   end
```

Self-tests

The FIPS-CC mode of operation includes a set of startup and conditional self-tests. The tests include algorithm known answer tests (KATs), a firmware integrity test and a configuration bypass test. Refer to the FortiOS 5.4 Security Policy for a complete list of the self-tests.

The administrator can run self-tests manually at any time. To run all of the tests, enter the following CLI command:

```
execute fips kat all
```

To run an individual test, enter `execute fips kat <test_name>`. To see the list of valid test names, enter `execute fips kat ?`

FIPS Error Mode

If one or more of the self-tests fail, the FortiGate unit switches to FIPS Error mode. The unit shuts down all interfaces including the console and blocks traffic. To resume normal FIPS-CC mode operation, power cycle the unit. If the self-tests pass after the reboot, the unit will resume normal FIPS-CC operation. If a self-test continues to fail after rebooting, there is likely a serious firmware or hardware problem and the unit should be removed from the network until the problem is solved.

Miscellaneous administration related changes

- By default, after three failed attempts to log on to an administrator account, the account is locked out for one hour. You can change the number of attempts permitted and the length of the lockout.
- On a CLI session, when an administrator logs out or the session times out, the FortiGate unit sends 300 carriage return characters to clear the screen. Note: if your terminal buffer is large, not all information from the session may be cleared.
- When configuring passwords or keys, the FortiGate unit requires you to enter the password or key a second time as confirmation.
- The `maintainer` account, which allows you to reset the admin password, is disabled.
- The local FortiGate TFTP servers is disabled by default. TFTP can be re-enabled using the tftp keyword in the `config system global` CLI command, but this is not FIPS-CC compliant operation.
- USB auto-install options are disabled.
- The fnsysctl command, which provides some access to the underlying operating system in the default mode of operation, is not available.
- Virus attack reporting to FortiGuard Distribution Service (FDS) is disabled.

Firewall Specific Changes

This section describes firewall rule specific changes to the way FortiOS functions by default or should be configured in the FIPS-CC mode of operation.

Enabling Firewall policies

When you create a security policy in FIPS-CC mode, by default the policy is not enabled. You must explicitly enable it. In the web-based manager, after creating the policy, select the checkbox at the beginning of the policy entry on the Policy > Policy page. In the CLI, enable a policy by setting its status to enable. You can do this when you create the policy or later:

```
config firewall policy
   edit 2
      set status enable
end
```

Required Firewall policies

Several firewall policies are required for CC compliance. Policies are required to:

- Block local link traffic (address block 169.254.1.0 through 169.254.254.255).
- Block Class E traffic (240.0.0.0/4).
- Restrict the IPv6 address space to the allocated global unicast space.

These policies are not created by default.

Blocking local link traffic

To block local link traffic, create a local link firewall address and then create policies for the interfaces you want to protect. The example below blocks local link source/destination traffic from the WAN to Internal interfaces:

```
config firewall address
   edit "Local-Link"
      set subnet 169.254.1.0 255.255.0.0
end
config firewall policy
   edit 1
      set srcintf "wan"
      set dstintf "internal"
      set srcaddr "Local-Link"
      set dstaddr "all"
      set action deny
      set status enable
      set schedule "always"
      set service "ALL"
   next
   edit 2
      set srcintf "wan"
      set dstintf "internal"
```

```
      set srcaddr "all"
      set dstaddr "Local-Link"
      set action deny
      set status enable
      set schedule "always"
      set service "ALL"
   next
end
```

Blocking Class E traffic

To block Class E traffic, create a Class E firewall address and then create policies for the interfaces you want to protect. The example below blocks Class E source/destination traffic from the WAN to Internal interfaces:

```
config firewall address
   edit "Class-E"
      set subnet 240.0.0.0 240.0.0.0
end
config firewall policy
   edit 3
      set srcintf "internal"
      set dstintf "wan"
      set srcaddr "Class-E"
      set dstaddr "all"
      set action deny
      set status enable
      set schedule "always"
      set service "ALL"
   next
   edit 4
      set srcintf "wan"
      set dstintf "internal"
      set srcaddr "all"
      set dstaddr "Class-E"
      set action deny
      set status enable
      set schedule "always"
      set service "ALL"
   next
end
```

Restrict the IPv6 address space to the allocated global unicast space

To restrict the IPv6 address space to the allocated global unicast space, create an IPv6 firewall address and then create policies for the interfaces you want to protect. The example below blocks global unicast source/destination traffic from the WAN to Internal interfaces:

```
config firewall address6
   edit "IPv6-Global-Unicast"
      set ip6 2000::/3
   next
end
config firewall policy6
   edit 1
      set srcintf "wan"
      set dstintf "internal"
```

```
        set srcaddr "IPv6-Global-Unicast"
        set dstaddr "all"
        set action deny
        set status enable
        set schedule "always"
        set service "ALL"
        set srcaddr-negate enable
    next
    edit 2
        set srcintf "wan"
        set dstintf "internal"
        set srcaddr "all"
        set dstaddr "IPv6-Global-Unicast"
        set action deny
        set status enable
        set schedule "always"
        set service "ALL"
        set dstaddr-negate enable
    next
end
```

Note that this example covers the entire global unicast range and will block special ranges which could be legitimate, including all IPv6 Multicast (ff00::/8) as well as reserved addresses for 6to4 and ipv4-mapped addresses (::ffff:0:0/96, 64:ff9b::/96).

Firewall authentication

In FIPS-CC mode, user passwords must be 8 characters or more. FTP and Telnet mechanisms for Proxy User Authentication are not allowed, and SSL redirection must be enabled for the HTTP mechanism.

Additional settings

The following settings are required to maintain CC compliance:

```
config system global
    set anti-replay strict
    set check-protocol-header strict
    set check-reset-range strict
end
config system settings
    set ses-denied-traffic enable
    set strict-src-check enable
end
config system interface
    edit <interface>
        set drop-overlapped-fragment enable
end
```

Enabling strict header checking disables all hardware acceleration by NPx, SPx and CPx processors, since strict header checking requires processing by the main CPU(s).

Interfaces and Routing

- Immediately after switching to FIPS-CC mode, all network interfaces are down and have no IP address assigned. This includes virtual interfaces such as the SSL VPN interface. Configure interfaces as needed. Use the CLI to view a complete list of interfaces including virtual interfaces.
- By default, admin access is disabled and must be enabled on a per-interface basis.
- Network interfaces, including virtual interfaces, cannot be configured to allow HTTP or Telnet administrative access.
- Immediately after switching to FIPS-CC mode, no DNS addresses are configured.
- Immediately after switching to FIPS-CC mode, no default route is configured.

VPN Specific Settings

This section describes VPN policy specific changes to the way FortiOS functions by default or should be configured in the FIPS-CC mode of operation.

Phase 1/Phase2 encryption strength

The NDcPP VPN Extended Package includes a requirement that the IPSec Phase 2 encryption strength not exceed the IKE Phase 1 encryption strength. In FIPS-CC mode the the FortiOS CLI enforces this requirement. If you want to ensure you are operating the unit in a CC compliant manner, use the CLI to configure your IPSec VPN tunnels. Alternatively, you can use the GUI and manually ensure the Phase 2 encryption strength does not exceed the Phase 1 encryption strength - e.g. if AES-128 is configured for Phase 1, then Phase 2 must also use a 128 bit encryption algorithm. If AES-256 is configured for Phase 1, then Phase 2 could use a 128 or 256 bit encryption algorithm.

Miscellaneous VPN related changes

- The DES, 3DES and MD5 algorithms are not available.
- Diffie-Hellman groups 1 through 5, and 14 through 18 are available to VPN configurations. Group 15 is the default. DH groups 15 through 18 use 3072 to 8192-bit keys. Fortinet recommends using group 15 or higher between FortiGate units.

Log Specific Settings

This section describes logging specific changes to the way FortiOS functions in the FIPS-CC mode of operation.

Logging to external devices

Offloading logs to a remote server over a secure connection is required to maintain CC compliance. For information on how to offload logs to a FortiAnalyzer device over SSL, see the Logging and Reporting chapter of the FortiOS Handbook.

Log messages are cached on the local Fortinet unit before being offloaded to the remote FortiAnalyzer device. The log messages are cached on the local disk or in system memory if the unit does not have disk storage. The log message cache is separate and distinct from local log storage.

If the SSL connection with the FortiAnalyzer is interrupted, one (or both) of the following log messages will be displayed:

```
SSL write to <ip address> has failed.

SSL connection to <ip address> is successfully closed.
```

Please re-establish the SSL connection between the devices to maintain CC compliance.

FortiAnalyzer configuration

Connections to a FortiAnalyzer device in the FIPS-CC mode of operation require the FortiAnalyzer's X.509 certificate be loaded onto the FortiGate device. To configure the FortiAnalyzer device connection, use the following CLI commands.

```
config log fortianalyzer setting
   set status enable
   set server "192.168.10.1"
   set certificate "faz_certificate"
   set upload-option realtime
end
```

This example assumes the address of the FortiAnalyzer device is 192.168.10.1 and the certificate name is faz_certificate. Note that the server address can use either ip-address or FQDN to set the reference identifier. Refer to the FortiGate Handbook for instructions on how to load the FortiAnalyzer certificate on to the FortiGate unit.

To verify the connection to the FortiAnalyzer unit, use the following CLI command:

```
execute log fortianalyzer test-connectivity
```

If the connection is successful, you will see output similar to the following:

```
FortiAnalyzer Host Name: FAZVM64
FortiGate Device ID: FG300D3G16200001
Registration: registered
Connection: allow
Disk Space (Used/Allocated): 47/Unlimited MB
Total Free Space: 77516 MB
Log: Tx & Rx (log not received)
IPS Packet Log: Tx & Rx
Content Archive: Tx & Rx
Quarantine: Tx & Rx
```

If the connection is unsuccessful, you will see output similar to the following:

```
Failed to get FAZ's status. SSL error. (-3)
```

Reconnecting to FortiAnalyzer

Should communications to the FortiAnalyzer be interrupted, the FortiGate is no longer considered to be operating in a CC compliant manner. If an interruption occurs in the communications path between the FortiGate and FortiAnalyzer units, the administrator can attempt to re-establish the connection manually by sending a ping to the FortiAnalyzer via the FortiGate CLI. This can be done in the evaluated configuration by logging in to the GUI via HTTPS and launching the console. Once the console is launched, the administrator may execute the following command:

```
exec ping <FortiAnalyzer IP address>
```

If the ping is successful, the FortiAnalyzer and the FortiGate should re-establish communication and logs should resume flowing to the FortiAnalyzer.

If a manual ping does not re-establish the connection, there may be a more serious network problem or problem with the FortiAnalyzer unit itself. Contact Fortinet support, if necessary, to resolve the problem.

The “Test Connectivity” feature is not supported in FIPS-CC mode.

Local logging

Logs are written to the FortiGate unit's hard disk if the unit contains one before. Models that do not contain a hard disk log to system memory. The default log setting is to overwrite the oldest log entries once the local log capacity is reached.

The System Event Log contains log entries for when:

- Local log files are rolled (new log file created)
- Local log files are deleted (old log files are overwritten)

Clearing local logs

The local logs can be cleared from the GUI or the CLI. Clearing the local logs does not affect cached logs - i.e. logs cached for offloading to a remote FortiAnalyzer unit.

Miscellaneous Logging

- The Common Criteria protection profile requires logging of all traffic and logging of system events, including startup and shutdown of functional components. Logging is enabled by default for:
  - new security policies
  - interfaces where administrative access is enabled
  - attempts to gain administration access on network interfaces where administrative access is not enabled
  - failed connection attempts to the FortiGate unit using TCP/IP ports other than 22 (ssh), 23 (telnet), 80 (HTTP), and 443 (HTTPS).
  - all configuration changes
  - configuration failures
  - remote IP lockout due to reaching maximum number of failed login attempts
  - log viewing
  - interface going up or down
  - other traffic: dropped ICMP packets, dropped invalid IP packets, session start and session deletion
- Logging is enabled for all event types at the information severity level.
- Memory logging is enabled on units that do not contain a hard disk. Logging includes traffic logging and all event types. Note that traffic logging to memory is available only in FIPS-CC mode and the log capacity is restricted by the available memory in the unit.
- The diskfull action is set to overwrite.