FortiProxy 1.0

FIPS 140-2 and Common Criteria Technote

FORTINET DOCUMENT LIBRARY

https://docs.fortinet.com

FORTINET VIDEO GUIDE

https://video.fortinet.com

FORTINET KNOWLEDGE BASE

http://kb.fortinet.com

FORTINET BLOG

https://blog.fortinet.com

CUSTOMER SERVICE & SUPPORT

https://support.fortinet.com

FORTINET COOKBOOK

http://cookbook.fortinet.com

FORTINET NSE INSTITUTE (TRAINING)

https://training.fortinet.com/

FORTIGUARD CENTER

https://fortiguard.com

FORTICAST

http://forticast.fortinet.com

END USER LICENSE AGREEMENT AND PRIVACY POLICY

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

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

FEEDBACK

Email: techdocs@fortinet.com

Monday, April 15, 2019

FIPS 140-2 and Common Criteria Technote for FortiProxy 1.0

45-100-528378-20181210

TABLE OF CONTENTS

Introduction

Fortinet performs FIPS 140-2 and Common Criteria certifications on specific FortiProxy OS versions in combination with specific FortiProxy hardware models. At the publication date of this document, the latest CC certified version of FortiProxy is 1.0.

The documentation set for FortiProxy units operated in FIPS-CC mode consists of this document and the standard FortiProxy documentation set. This document covers Common Criteria specific installation instructions and explains the FortiProxyFIPS-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 FortiProxy 1.0 Common Criteria certification, including the certified hardware models, refer to the FortiProxy 1.0 Security Target. The Security Target can be found on the Fortinet Support web site in the FortiProxy 1.0.5 firmware download directory (http://support.fortinet.com).

References

Security Target: FortiProxy 1.0, Version TBD, Date TBD
FIPS 140-2 Security Policy: FortProxy-400E/2000E/4000E, Version TBD, Date TBD
FortiProxy Administration Guide
FortiProxy 1.0 CLI Reference
FortiProxy 1.0 Log Reference
Model specific Hardware Information Supplements

Certified Models

FortiProxy-400E	FortiProxy-2000E	FortiProxy-4000E

Installing the CC Certified Firmware

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

Operating Environment

The following table list the Common Criteria Operating Environment assumptions and the specific product details. Note that TOE refers to the Common Criteria Target of Evaluation - i.e. the FortiProxy appliance.

Identifier	Description	Detail
OE.PHYSICAL	Physical security, commensurate with the value of the TOE and the data it contains, is provided by the environment.	The administrator is responsible for ensuring the physical security of the TOE. The TOE should be deployed in a secure location where access is restricted to trusted administrators.
OE.NO_GENERAL_PURPOSE	There are no general-purpose computing capabilities (e.g., compilers or user applications) available on the TOE, other than those services necessary for the operation, administration and support of the TOE.	The TOE does not provide operating system level access. All access is through the Web-Manager GUI or CLI. Third party applications cannot be loaded onto the TOE.
OE.NO.THRU.PROTECTION	The TOE does not provide any protection of traffic that traverses it. It is assumed that protection of this traffic will be covered by other security and assurance measures in the operational environment.	The administrator is responsible for ensuring the through traffic is protected by other devices in the operational environment.
OE.TRUSTED.ADMIN	Security Administrators are trusted to follow and apply all guidance documentation in a trusted manner.	The administrator is responsible for reading the relevant product documentation and deploying the TOE in compliance with the documentation and best practices.

OE.UPDATES	The TOE firmware and software is updated by an Administrator on a regular basis in response to the release of product updates due to known vulnerabilities.	The adminstrator is responsible for using the trusted update capability of TOE's FIPS-CC mode of operation to update the firmware as necessary.
OE.ADMIN_CREDENTIALS_SECURE	The Administrator's credentials (private key) used to access the TOE must be protected on any other platform on which they reside.	The administrator is responsible for ensuring the protection of their credentials (private key) on any system used to access the TOE remotely or used to host/back up the credentials.
OE.RESIDUAL_INFORMATION	The Security Administrator ensures that there is no unauthorized access possible for sensitive residual information (e.g. cryptographic keys, keying material, PINs, passwords etc.) on networking equipment when the equipment is discarded or removed from its operational environment.	The TOE provides tools for zeroizing keys and overwriting the TOE's persistent storage device(s). The administator is responsible for using the tools to destroy any residual information prior to removing the TOE from the secure operating environment.

Verifying secure delivery

Before installing the FortiProxy 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 - 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 FortiProxy 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 FortiProxy 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 FortiProxy unit is installed in a secure physical location.
- Physical access to the FortiProxy unit is restricted to authorized operators.

Installing the unit

The documentation shipped with your unit includes a FortiProxy QuickStart Guide and a model specific Hardware Supplement. The FortiProxy Administration Guide 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 FortiProxy 1.0.5 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 FortiProxy unit.
3. Download the md5sum.txt file from the same directory as the firmware. This file contains MD5 check sums for the firmware builds.

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 FortiProxy unit. There are several methods to do this. Refer to the FortiProxy Administration 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 FortiProxy model number, firmware version, build number and date. For example:

```
Version: FortiProxy-2000E v1.0.5,build9999,YYMMDD
```

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 FortiProxy 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. Although the document is titled "Navigating the FortiGate BIOS", the content is equally applicable to FortiProxy.

You may want to contact Fortinet's technical support group before attempting to use the FortiProxy 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. FortiProxy units use the FortiASIC CP9 as a strong entropy source. FortiProxy models use the CP9 by default in the FIPS-CC mode of operation - no configuration changes are required.

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 FortiProxy.

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. 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
```

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

```
Please enter administrator password:
```

3. 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)
```

4. Enter `y`. The FortiProxy unit restarts and is now running in FIPS-CC mode.
5. 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 FortiProxy 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 FortiProxy 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 FortiProxy unit in strict compliance with the Security Target. Refer to the Security Target for more information.

Install Updated Certificates

By default, FortiProxy units use a certificate signed by a Fortinet Certificate Authority (CA). Administrators should install a new, signed certificates from a trusted CA. Consult the FortiProxy 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 FortiProxy Administration Guide for details on how to configure trusted hosts.

Administration

This section describes administration specific issues and changes to the way FortiProxy 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:

- Connection security: TLS 1.2
- One of the following TLS cipher suites:
  - TLS_DHE_RSA_WITH_AES_128_CBC_SHA as defined in RFC 3268
  - TLS_DHE_RSA_WITH_AES_256_CBC_SHA as defined in RFC 3268
  - TLS_DHE_RSA_WITH_AES_128_CBC_ SHA256 as defined in RFC 5246
  - TLS_DHE_RSA_WITH_AES_256_CBC_ SHA256 as defined in RFC 5246
  - TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA as defined in RFC 4492
  - TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA as defined in RFC 4492
  - TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256 as defined in RFC 5289
  - TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 as defined in RFC 5289

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
```

The Diffie-Hellman group should be set to Group 14 (2048-bit modulus) as per the evaluated configuration:

```
config system global
```

```
    set dh-params 2048
end
```

For detailed information about accessing the web-based manager, see “Connecting to the GUI” in the *FortiProxy 1.0 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 FortiProxy unit or to restore configuration after you exit and then re-enter FIPS-CC mode.

Refer to the FortiProxy 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 FortiProxy 1.0 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 ?`

Trusted Updates

The FIPS-CC mode of operation uses 2048 bit RSA signatures to verify the integrity of firmware update files. The firmware images are signed with a Fortinet private key and the appliance will verify the integrity of the firmware image before starting the update procedure.

If the signature is verfied, the following message is displayed on the console and the update proceeds normally:

```
Firmware image verified.
```

If the signature fails verification, the following message is displayed and the update procedure will terminate:

```
Image upgrade failed.
```

FIPS Error Mode

If one or more of the FIPS self-tests fail, the FortiProxy 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.

Disabling NTP

NTP should be disabled to match the evaluated configuration. NTP can be disabled with the following CLI command:

```
config system ntp
   set ntpsync disable
end
```

Terminating Local and Remote Administration Sessions

Local console and remote CLI adminstration sessions are terminated (i.e. the administrator can log out) by entering "exit" at the top level of the CLI.

Remote Web-Manager administration sessions are terminated by clicking on your username in the top right-hand corner of the Web-Manager and then selecting "Logout".

Miscellaneous administration related changes

- By default, after three failed attempts to log on to an administrator account, the account is locked out for 5 minutes. 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 FortiProxy 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 FortiProxy 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 FortiProxy 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.

Logging

This section describes logging specific issues and changes to the way FortiProxy 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 FortiProxyAdministration Guide.

Log messages are cached on the local FortiProxy 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.

Logging SSL/TLS connections

Log messages for SSL/TLS connections must be enabled to match the evaluated configuration. Enable SSL/TLS connection logging as follows:

```
config system global
   set log-ssl-connection enable
end
```

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.

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

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 FortiProxydevice. 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 FortiProxy 1.0 Administration Guide for instructions on how to load the FortiAnalyzer certificate on to the FortiProxy 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 FortiProxy is no longer considered to be operating in a CC compliant manner. If an interruption occurs in the communications path between the FortiProxy and FortiAnalyzer units, the administrator can attempt to re-establish the connection manually by sending a ping to the FortiAnalyzer via the FortiProxy 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 FortiProxy 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.

Local logging

Logs are written to the FortiProxy unit's hard disk. 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 FortiProxy 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.