FortiOS 6.4 and FortiGate NGFW Appliances

FIPS 140-2 and NDcPP 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://www.fortinet.com/support/contact.html

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: techdoc@fortinet.com

Friday, March 3, 2023

FIPS 140-2 and NDcPP Technote for FortiOS 6.4 and FortiGate NGFW Appliances

01-649-0773518-20230303

TABLE OF CONTENTS

Introduction

Fortinet performs FIPS 140-2 and NDcPP Common Criteria certifications on specific FortiOS versions in combination with specific FortiGate family hardware models. At the publication date of this document, the latest NDcPP CC certified version of FortiOS is 6.4.

The documentation set for FortiGate units operated in FIPS-CC mode consists of this document and the standard FortiOS 6.4 documentation set. This document covers NDcPP 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 6.4 NDcPP Common Criteria certification, including the certified hardware models, refer to the FortiOS 6.4 NDcPP Security Target. The Security Target can be found on the Fortinet Support web site in the FortiOS 6.4 FIPS-CC certified firmware download directory (http://support.fortinet.com).

References

Security Target: FortiGate/FortiOS 6.4
FIPS 140-2 Security Policy: FortiOS 6.4 and 7.0
FortiOS 6.4.9 Administration Guide
FortiOS 6.4.9 CLI Reference
FortiOS 6.4.9 Log Message Reference
FortiOS 6.4 and FortiGate NGFW Appliances NDcPP Common Criteria Logging Addendum
Model specific Hardware Information Supplements

NDcPP Certified Models

FG-VM	FG-81F-2R	FG-201F	FG-2000E	FG-4201F
FG-61E	FG-81F-PoE	FG-301E	FG-2201E	FG-4201F-DC
FG-61F	FG-81F-2R-3G4G-PoE	FG-401E	FG-2500E	FG-4401F
FWF-61E	FG-81F-2R-PoE	FG-401E-DC	FG-2601F	FG-4401F-DC

FWF-61F	FG-90E	FG-501E	FG-2601F-DC	FG-5001E1
FG-81E	FG-91E	FG-601E	FG-3301E	FG-6300F
FG-81E-PoE	FG-101E	FG-1101E	FG-3401E	FG-6301F
FG-81F	FG-101F	FG-1801F	FG-3401E-DC	FG-6500F
	FG-201E	FG-1801F-DC	FG-3601E	FG-6501F

For FIPS 140-2 certified models, refer to the relevant FIPS 140-2 Security Policy documents.

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.
- An Araneus Alea I or II entropy token is used to seed the RBG, if required, and the token remains in the USB port during operation (to allow for periodic reseeding of the RBG). See the Entropy Section for details on which models require an entropy token as a strong entropy source.

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

The FortiOS 6.4 FIPS-CC certified firmware builds are identified using a higher level identifer instead of the build number. The validated firmware version is FortiOS 6.2.9 (FIPS-CC-64-6), where FIPS-CC-64-6 is the higher level identifiers. The higher level identifiers may map to more than one build number for each certified release.

To download the firmware

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 FortiOS 6.4 FIPS-CC Certified folder. Download the firmware build for your specific hardware model or software build for your specific VM version. Save the file on the management computer or on your network where it is accessible from the FortiGate unit or FortiGate-VM.

Verifying the integrity of the firmware build

Download the model specific FIPS validated firmware image and checksum from the Fortinet Support site at https://support.fortinet.com/. Both MD5 and SHA-512 checksums are provided. Use a hashing utility on the downloaded firmware image to compare and verify the output against the result from the checksum listing. If the hashes match, the downloaded build is uncorrupted and unmodified.

Installing the FIPS-CC firmware build

Starting with FortiOS 6.4, FIPS-CC certified builds are identified with a higher-level build identifier.

Install the FIPS-CC firmware build on your FortiGate unit. There are several methods to do this. Refer to the FortiOS Administration Guide or FortiGate CLI Reference 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 and build number. For example:

```
Version: FortiGate-60F v6.4.7,build8695,211216 (FIPS-CC-64-2)
```

Verify in the relevant security target or security policy document that your firmware version and identifier are correct. Note that YYMMDD is the build date, but the date is not relevant for verifying the firmware version. The build number is also not relevant. The identifier (e.g. FIPS-CC-64-3) is the higher level identifier used to identify the certified builds.

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.

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 6.4 makes use of four different strong entropy sources in the FIPS-CC mode of operation, depending on the model: the Fortinet SoC3 or SoC4, the Fortinet CP9 Security Processor or the Araneus Alea II entropy token. The Araneus Alea II entropy token is only required for FortiGate-VM deployments. Refer to the Security Policies for specific model and entropy source information.

The Araneus Alea II entropy token

Based on a wide band, Gaussian white noise generator, the Alea token provide users with a FIPS 140-2/3 and cPP CC validated source of entropy for FortiGate models that do not have an internal strong entropy source.

The Alea II token is compatible with FortiOS 5.0.10 or higher. The Alea token is generically referred to as the entropy token.

Installing the token

Plug the token into an available USB port on the FortiGate unit or the VMware ESXi host.

Configuring the entropy token settings

Use of the token is required for FIPS 140-2/3 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.

RBG Seeding and Reseed Interval

The RBG is seeded 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 physical USB port the token is using must first be mapped to the FortiGate-VM instance. The following steps show how to do this on the Linux KVM hypervisor . Other hypervisors will have equivalent commands.

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). 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 hypervisor console. This example assumes the FortiGate-VM is instance 1 on the hypervisor:

```
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 using the CLI.

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 FIPS-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

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

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 using 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.

Functionality Excluded from the Evaluated Configuration

Excluded Features

The following TOE features are excluded from the scope of this evaluation:

- The TOE’s antispam, content filtering and traffic shaping features
- SMTP, SNMP, LDAP, Windows AD, NTP, and RADIUS
- FortiGuard-Antispam, Firmware, Endpoint Control, and FortiSandbox services

- The TOE's DHCP, DDNS, or DNS server capabilities
- Centralized management of the TOE by FortiManager servers
- Traffic offloading to the FortiASIC NPx network processors
- Routing protocols (RIP, OSPF, BGP)
- Use of the USB interface for anything other than an Entropy Token
- Diagnostics interface
- FortiAnalyzer, Syslog

Disabled Features

The following TOE Features are disabled by default and are excluded from the scope of this evaluation:

- HTTP GUI
- The TOE acting as a Telnet client or server
- The FortiGate REST API
- The TOE acting as a TFTP client

Non-Supported Protocols

The TOE does not support use of the UDP-Lite protocol for IPv4 or IPv6.

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 Administration Guide for details on how to configure trusted hosts.

Disabling NPU support

The encryption algorithms used in the Fortinet FortiASIC NP4, NP6, and NP7 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 FortiOS 6.4 Hardware Acceleration manual for details on disabling specific capabilities of the processors or the entire processor, if desired.

Administration

This section describes administration specific changes to the way FortiOS functions in the FIPS-CC mode of operation and addresses general administration related issues.

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.

Note that the Administrator's credentials (private keys) used to access the TOE must be protected on any other platform on which they reside (e.g. management computers used to remotely access the TOE).

Configuration and use of approved cryptographic algorithms

The FIPS-CC mode of operation enforces the use of approved cryptographic algorithms and key sizes. The cipher suites and/or algorithms used for HTTPS, SSH, and TLS are hard coded and not exposed to (or modifiable by) the administrator. For IPSec VPN, the Phase 1 and Phase 2 algorithms are configurable by the administrator. The available algorithms are:

Phase 1:

- AES CBC 128/256
- HMAC/SHA 256/384/512

Phase 2:

- AES CBC 128/256 with HMAC/SHA 256/384/512
- AES-GCM 128/256

Where the block sizes and output lengths (in bytes) of the HMAC algorithm are:

- 64/32 for HMAC 256
- 128/48 for HMAC 384
- 128/64 for HMAC 512

Loading custom certificates

Note that the CLI command tree used for loading all custom certificates in the evaluated configuration is "config vpn certificate". The "config certificate" CLI command tree is only available if VDOMs are enabled and is used to load certificates for the global VDOM.

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 1.1 or 1.2
- One of the following TLS cipher suites:
  - TLS_DHE_RSA_WITH_AES_128_CBC_SHA
  - TLS_DHE_RSA_WITH_AES_256_CBC_SHA
  - TLS_DHE_RSA_WITH_AES_128_CBC_SHA256
  - TLS_DHE_RSA_WITH_AES_256_CBC_SHA256
  - TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA
  - TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA2
  - TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA
  - TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA
  - TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256
  - TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
  - TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
  - TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384

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 “Using the GUI” in the *FortiGate 6.0 Handbook*

Trusted hosts

Trusted hosts for adminstrator remote access should configured. Trusted hosts can be configured through the web-based manager or the CLI. Refer to the FortiOS Administration Guide for more information.

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 FortiOS 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 6.4 & 7.0 FIPS 140-2 Level 1 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.

SSH server key regeneration

FortiOS 6.4.9 regenerates SSH server keys on a reboot. This means that an administrator using SSH to connect to the TOE for administration purposes will have to accept a new server key after a reboot of the TOE. Administrators need to be aware of when the TOE has been rebooted so as not to mistake the new server key for an attempted MitM attack. Conversely, if a reboot has not occurred and a new server key is being offered, it could be an attempted MitM attack and administrators should investigate further.

Logging out from the GUI and CLI

To log out from the FortiOS Web-Based Manager, click on your username in the top right of the window and select "logout".

To logout from the CLI, enter "exit" from the top level of the CLI tree.

Disable NTP

NTP is not claimed in the Security Target. NTP should be disabled to be compliant with the Security Target. Use the following CLI commands to disable NTP.

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

FortiGuard Labs PSIRT Security Advisories

The administrator is encouraged to keep up to date on security advisories from FortiGuard Labs Product Security Incident Response Team (PSIRT) https://fortiguard.com/psirt and apply fixes where available.

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 server 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.
- In the System settings, under Feature Visibility, ensure that "IPv6" is enabled.
- In the Policy & Objects setttings, under Firewall Policy, ensure "IPv4 + IPv6" is selected.
- Edit the "Implicit Deny Policy" and ensure that "Log IPv4 Violation Traffic" and "Log IPv6 Violation Traffic" selections are enabled.

VM Security

Ensure VMware ESXi is fully patched and the ESXi web-console is on a separate network with limited access.

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 select the toggle at the bottom of the policy editing page to enable the policy. 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
```

Additional default Firewall policies

Several firewall policies are required for CC compliance. FIPS-CC mode creates default policies 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.

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. For example, to bring up the ssl.root interface:

  ```
  config system interface
     edit ssl.root
     set status up
  end
  ```

- 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 certificate 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. Since FIPS-CC mode does not enforce this requirement by default, to ensure you are operating the unit in a CC compliant manner, the administrator must manually change the configuration by use of the CLI or GUI to configure the IPSec VPN tunnels. For example, 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.

Note that when changing the IKE version, the proposal will change. For example, use of "set ike-version 1" will result in a proposal change to "set proposal aes-128-sha256 aes256-sha256"

Use of the FortiGate Web-Manager

The FortiGate Web-Based Manager (GUI) must be used to import, export, create, delete and assign certificates.

CAs and CRLs

All applicable CAs and CRLs should be imported to the FortiGate unit.

Preshared keys

Note that the FortiGate Administration Guide specifies that FortiOS supports a preshared key lengths of 16-128 characters. This is incorrect for FortiOS 6.4.9. The correct supported length is 6-128 characters.

Administrators must ensure that preshared keys meet strong password security rules - i.e. preshared keys must be be at least 8 characters in length and include at least 1 uppercase character, 1 lowercase character, 1 numeric character, and 1 special character (e.g. “!”, “@”, “#”, “$”, “%”, “^”, “&”, “*”, “(“, and “)”).

Miscellaneous

- The DES, 3DES and MD5 algorithms are not available.
- Diffie-Hellman group 15 is the default setting in FIPS-CC mode. IKE should be configured to use one of DH Groups 14 (2048-bit MODP), 19 (256-bit Random ECP) or 20 (384-bit Random ECP) to match the evaluated configuration.
- SANs are not supported in IPSec VPN peer authentication certificates.
- SANs are supported in the certificates when acting as a TLS client.
- RSA and ECDSA keys that are generated during a Certificate Signing Request operation are stored on the boot device of the FortiGate.
- The FortiGate willl validate the extendedKeyUsage field according to the following rules:
    - Certificates used for trusted updates and executable code integrity verification will have the Code Signing purpose (id-kp 3 with OID 1.3.6.1.5.5.7.3.3) in the extendedKeyUsage field.
    - Server certificates presented for TLS will have the Server Authentication purpose (id-kp 1 with OID 1.3.6.1.5.5.7.3.1) in the extendedKeyUsage field.
    - Client certificates presented for TLS will have the Client Authentication purpose (id-kp 2 with OID 1.3.6.1.5.5.7.3.2) in the extendedKeyUsage field.
    - OCSP certificates presented for OCSP responses will have the OCSP Signing purpose (id-kp 9 with OID 1.3.6.1.5.5.7.3.9) in the extendedKeyUsage field.

Log Specific Settings

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

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 FortiGate device. To configure the FortiAnalyzer device connection, use the following CLI commands. Note that the CLI must be used for the FortiAnalyzer configuration.

```
config log fortianalyzer setting
   set status enable
   set server "192.168.10.1"
   set certificate "faz_certificate"
   set certificate-verification disable
   set upload-option realtime
   set reliable enable
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. The FortiAnalyzer certificate must be an RSA certificate.

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.

Logging Local SSL Connections

Local SSL connection logging must be specifically enabled. To enable local SSL connection logging, use the following CLI commands.

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

Logging Invalid Packets

Invalid packet logging must be specifically enabled. To enable invalid packet logging, use the following CLI commands.

```
config log setting
   set log-invalid-packet enable
end
```

FortiGate logs packets that do not match an established TCP session and does a best effort to provide details identifying the reason for rejecting the problem. Problems may be:

- no session matched

- syned but no ack, suspicious
- replay packet(seq_check), suspicious

Depending on the timing and sequence of packets, FortiGate may group logs packets not matching an established TCP session into a single log message.

Log entries for invalid packets can contain a "sentpkt=" field such as "sentpkt=1". This is a zero based counter that indicates the number of packets received.

Logging Dropped Packets Due to Exceeding the Traffic Processing Capability

In order to log dropped packets due to an interface processing traffic beyond its maximum capability, the administrator should set interface limits to a value lower than the capability. For example, for a 2048 mbps physically capable network interface, the admistrator could choose to set the value to 1024 kbps such as the below. This would result in packets received over the 1024 kbps mark being dropped and being logged.

```
config system interface
   edit "to_swan"
   set inbandwidth 1024
   set outbandwidth 1024
end
```

Different FortiGate models have different maximum processing capacity capabilities for various interfaces. The administrator should refer to the product Datasheets currently available at https://www.fortinet.com/products/next-generation-firewall.

The Specifications section and the end of the Datasheet shows the maximum capabilities for all items, such as "IPS Throughput", "IPsec VPN Throughput", and "SSL-VPN Throughput" (SSL-VPN is an unevaluated function). The administrator can use these values and others listed to determine the maximum threshold the value should be set at. The number of ports in use, number of IPSec VPNs, and the number of interfaces with IPS or firewall rules configured should be considered.

Local Logging

On FortiGate models with internal disks, logs are written to the disks. On models that do not have internal disks local logs are written 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:

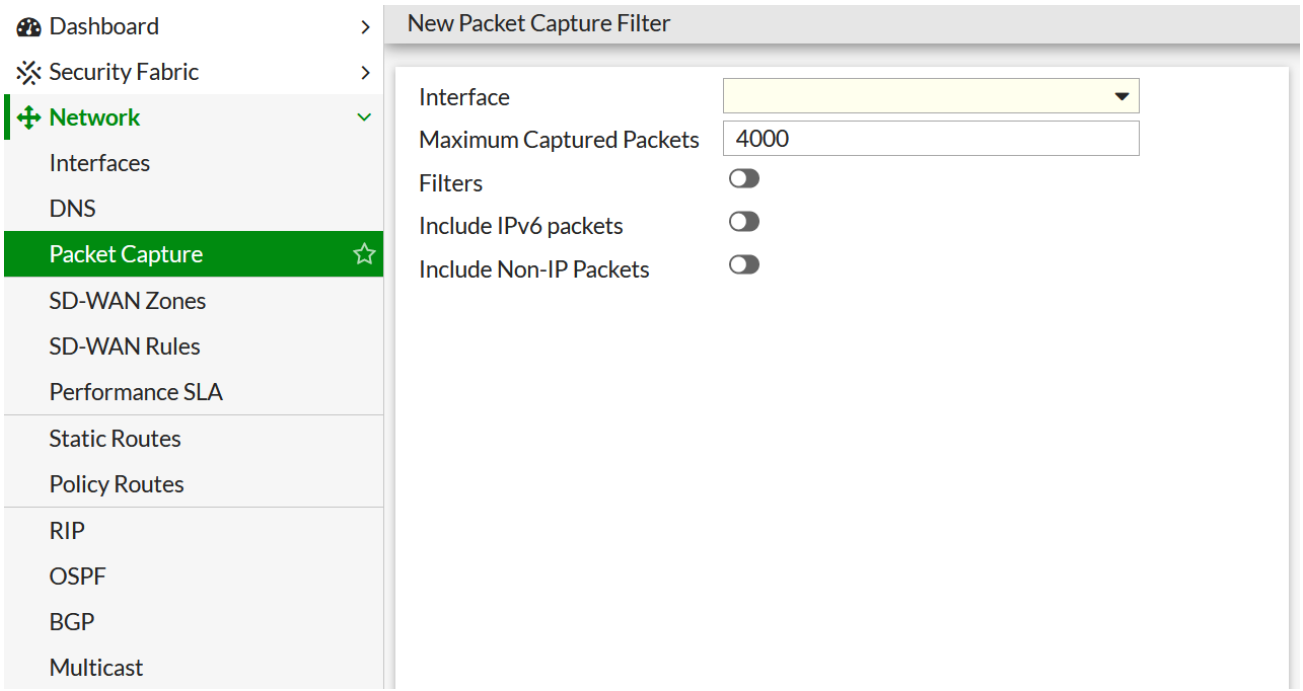
- Local log files are rolled (new log file created)
- Local log files are deleted (old log files are overwritten)

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.

Packet Capture

FortiOS provides a built-in packet capbility. Packets are captured to a file on the FortiGate unit and can be downloaded for review in an application such as Wireshark. To configure a packet capture, navigate to Network>Packet Capture in the FortiOS GUI and select "Create New".



Once you have configured the packet capture parameters, click "Ok" to save the filter. To start the capture, right-click on the filter and select the "Start" option. The capture will stop automatically it reaches the maximum number of captured packets. Once the capture is complete, download the capture file to the management computer to view the contents.

Miscellaneous Logging

- 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.