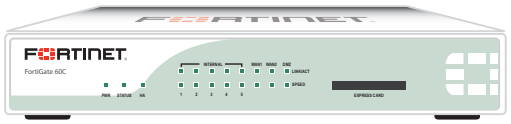
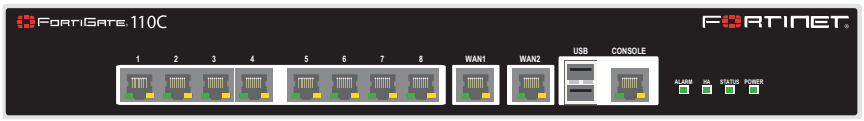
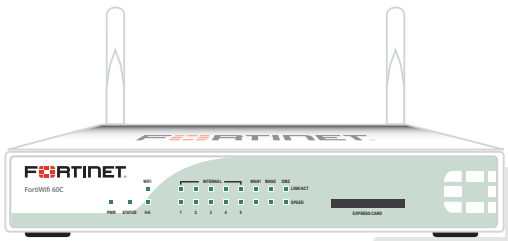
FIPS 140-2 Security Policy

FortiGate-60C/80C/110C and FortiWiFi-60C







FortiGate-60C/80C/110C and FortiWiFi-60C FIPS 140-2 Security Policy			
Document Version:	2.9		
Publication Date:	May 20, 2014		
Description:	Documents FIPS 140-2 Level 2 Security Policy issues, compliancy and requirements for FIPS compliant operation.		
Firmware Version:	FortiOS 4.0, build3830, 131223		
Hardware Version:	FortiGate-60C (C4DM93)	FortiGate-110C (C4HA15)	
	FortiGate-80C (C4BC61)	FortiWiFi-60C (C4DM95)	

FortiGate-60C/80C/110C and FortiWiFi-60C: FIPS 140-2 Security Policy

01-436-175479-20120710

for FortiOS 4.0 MR3

Trademarks

Contents

Overview

This document is a FIPS 140-2 Security Policy for Fortinet Incorporated's FortiGate-60C, 80C, 110C and FortiWiFi-60C Multi-Threat Security Systems. This policy describes how the FortiGate-60C, 80C, 110C and FortiWiFi-60C (hereafter referred to as the 'modules') meet the FIPS 140-2 security requirements and how to operate the modules in a FIPS compliant manner. This policy was created as part of the Level 2 FIPS 140-2 validation of the modules.

This document contains the following sections:

The Federal Information Processing Standards Publication 140-2 - *Security Requirements for Cryptographic Modules* (FIPS 140-2) details the United States Federal Government requirements for cryptographic modules. Detailed information about the FIPS 140-2 standard and validation program is available on the NIST (National Institute of Standards and Technology) website at http://csrc.nist.gov/groups/STM/cmvp/index.html.

References

This policy deals specifically with operation and implementation of the module in the technical terms of the FIPS 140-2 standard and the associated validation program. Other Fortinet product manuals, guides and technical notes can be found at the Fortinet technical documentation website at http://docs.forticare.com.

Additional information on the entire Fortinet product line can be obtained from the following sources:

- Find general product information in the product section of the Fortinet corporate website at http://www.fortinet.com/products.
- Find on-line product support for registered products in the technical support section of the Fortinet corporate website at http://www.fortinet.com/support
- Find contact information for technical or sales related questions in the contacts section of the Fortinet corporate website at http://www.fortinet.com/contact.
- Find security information and bulletins in the FortiGuard Center of the Fortinet corporate website at http://www.fortinet.com/FortiGuardCenter.

Introduction

The FortiGate product family spans the full range of network environments, from SOHO to service provider, offering cost effective systems for any size of application. FortiGate appliances detect and eliminate the most damaging, content-based threats from email and Web traffic such as viruses, worms, intrusions, inappropriate Web content and more in real time — without degrading network performance. In addition to providing application level firewall protection, FortiGate appliances deliver a full range of network-level services — VPN, intrusion prevention, web filtering, antivirus, antispam and traffic shaping — in dedicated, easily managed platforms.

All FortiGate appliances employ Fortinet's unique FortiASIC™ content processing chip and the powerful, secure, FortiOS™ firmware achieve breakthrough price/performance. The unique, ASIC-based architecture analyzes content and behavior in real time, enabling key applications to be deployed right at the network edge where they are most effective at protecting enterprise networks. They can be easily configured to provide antivirus protection, antispam protection and content filtering in conjunction with existing firewall, VPN, and related devices, or as complete network protection systems. The modules support High Availability (HA) in both Active-Active (AA) and Active-Passive (AP) configurations.

FortiGate appliances support the IPSec industry standard for VPN, allowing VPNs to be configured between a FortiGate appliance and any client or gateway/firewall that supports IPSec VPN. FortiGate appliances also provide SSL VPN services using TLS 1.0 in the FIPS-CC mode of operation.

Security Level Summary

The modules meet the overall requirements for a FIPS 140-2 Level 2 validation.

Table 1: Summary of FIPS security requirements and compliance levels

Security Requirement	Compliance Level
Cryptographic Module Specification	2
Cryptographic Module Ports and Interfaces	3
Roles, Services and Authentication	3
Finite State Model	2
Physical Security	2
Operational Environment	2
Cryptographic Key Management	2
EMI/EMC	2
Self-Tests	2
Design Assurance	3
Mitigation of Other Attacks	2

Module Description

The FortiGate-60C, 80C, 110C and FortiWiFi-60C are multiple chip, standalone cryptographic modules consisting of production grade components contained in a physically protected enclosure in accordance with FIPS 140-2 Level 2 requirements.

The modules have a similar appearance and perform the same functions, but have different numbers and types of network interfaces in order to support different network configurations:

- The FortiGate-60C has 8 network interfaces with a status LED for each network interface (8x 10/100/1000 Base-T).
- The FortiGate-80C has 9 network interfaces with a status LED for each network interface (6x 10/100 BaseT, 3x 10/100/1000 BaseT)
- The FortiGate-110C has 10 network interfaces with a status LED for each network interface (8x 10/100 BaseT, 2x 10/100/1000 BaseT)

- The FortiWiFi-60C has 8 network interfaces with a status LED for each network interface (8x 10/100/1000 Base-T). The FortiWiFi-60C also includes an IEEE 802.11a/b/g/n compliant WiFi interface with a separate status LED.

The FortiGate-60C and FortiWiFi-60C each have one ARM compatible CPU.

The FortiGate-80C and 110C each have one x86 compatible CPU.

The modules are 1u desktop devices. The modules have optional rackmount adapters that allow installation in standard 19” equipment racks.

The modules do not have external ventilation fans.

The validated firmware version is FortiOS 4.0, build3830, 131223.

Figure 1, Figure 2, Figure 3 and Figure 4, are representative of the modules tested.

Cryptographic Module Ports and Interfaces

FortiGate-60C

Figure 1: FortiGate-60C Front and Rear Panels

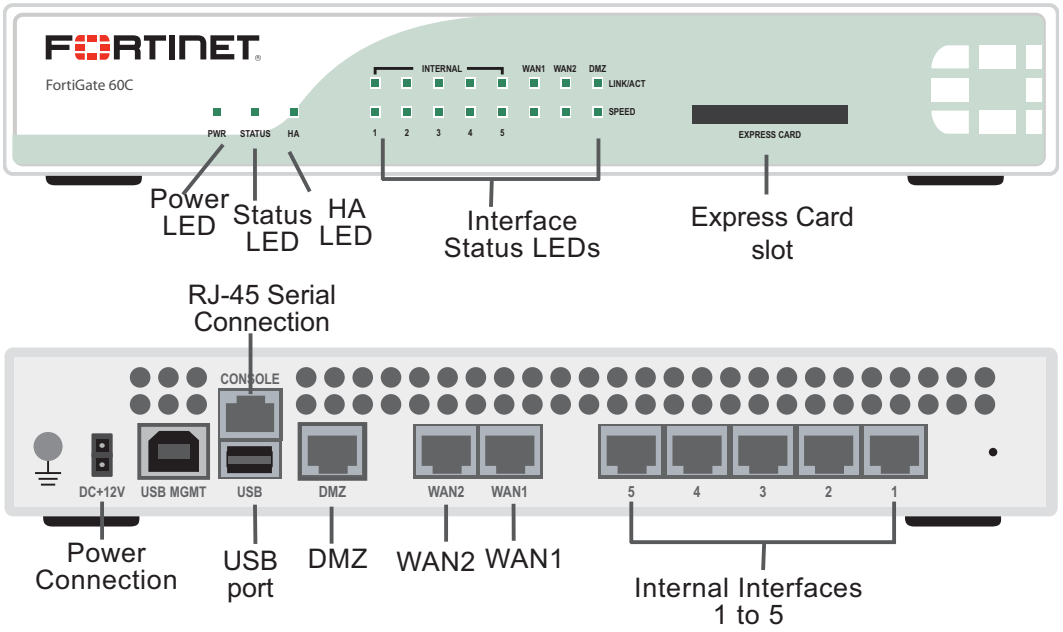


Table 2: FortiGate-60C Status LEDs

LED	State	Description
Power	Green	The module is powered on.
	Off	The module is powered off.
Status	Flashing	The module is starting up.
	Green	The module is running normally.
	Off	The module is powered off.
HA	Green	HA is enabled.
	Off	The unit is in stand-alone mode.

WAN1, WAN2, DMZ, Ports 1 to 5	Link/ACT	Green	Port is online.
		Flashing	Port is sending/receiving data.
		Off	Port is offline.
	Speed	Green	Connected at 1000 Mbps.
		Amber	Connected at 100 Mbps.
		Off	Connected at 10Mbps.

Table 3: FortiGate-60C Rear Panel Connectors and Ports

Connector	Type	Speed	Supported Logical Interfaces	Description
WAN1, WAN2, DMZ, Ports 1 to 5	RJ-45	10/100/1000 Base-T	Data input, data output, control input and status output	Copper gigabit connection to 10/100/1000 copper networks.
CONSOLE	RJ-45	9600 bps	Control input, status output	Optional connection to the management computer. Provides access to the command line interface (CLI).
USB	USB	N/A	Key loading and archiving, configuration backup and restore	Optional connection for USB token.

FortiGate-80C Module

Figure 2: FortiGate-80C Front and Rear Panels

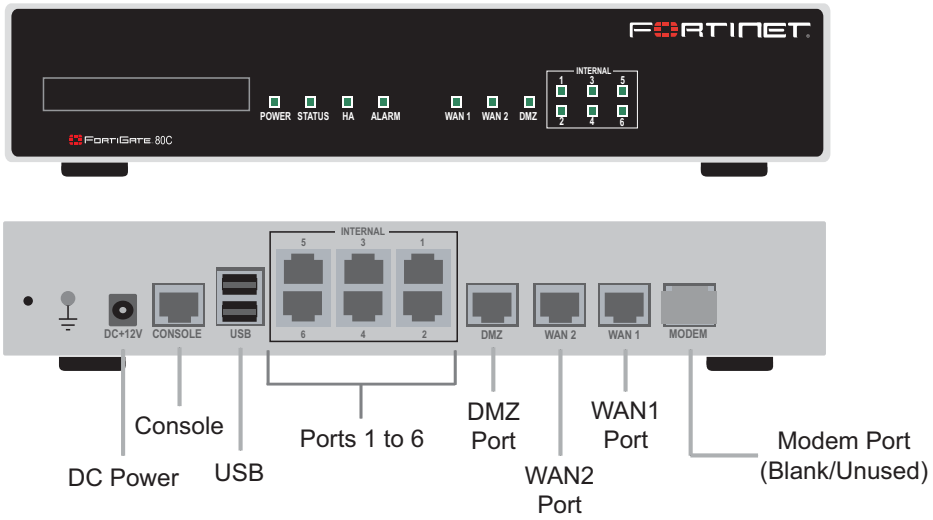


Table 4: FortiGate-80C Status LEDs

LED		State	Description
Power		Green	The module is powered on.
		Off	The module is powered off.
Status		Flashing Green	The module is starting up.
		Green	The module is running normally.
HA		Green	The module is part of an HA cluster.
Alarm		Red	A critical error has occurred.
		Amber	A minor error has occurred.
		Off	No errors detected.
Internal, WAN1, WAN2, DMZ		Green	The correct cable is in use and the connected equipment has power.
		Flashing Green	Network activity at this interface.
		Off	No link established.

Table 5: FortiGate-80C Connectors and Ports

Connector	Type	Speed	Supported Logical Interfaces	Description
Internal	RJ-45	10/100 BaseT	Data input, data output, control input and status output	Connection to internal network.
WAN1, WAN2	RJ-45	10/100/1000 BaseT	Data input, data output, control input and status output	Connection to the Internet.
DMZ	RJ-45	10/100 BaseT	Data input, data output, control input and status output	Connection to DMZ network.
Console	RJ-45	9600 bps	Control input, status output	Optional connection to the management computer. Provides access to the command line interface (CLI).
USB Ports	USB	N/A	Key loading and archiving	Optional USB token.
POWER	N/A	N/A	Power	+12VDC power connection.

FortiGate-110C module

Figure 3: FortiGate-110C Front and Rear Panels

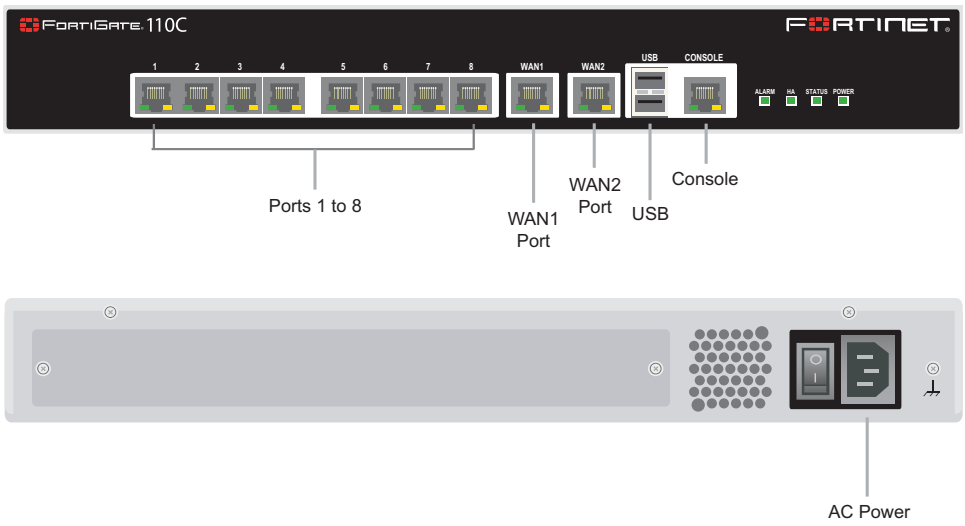


Table 6: FortiGate-110C Status LEDs

LED	State	Description
Power	Green	The FortiGate unit is powered on.
	Off	The FortiGate unit is powered off.
Status	Flashing Green	The module is starting up.
	Green	The module is running normally.
HA	Green	The module is part of an HA cluster.
Alarm	N/A	Future use.
Ports 1 to 8, WAN1, WAN2	Amber (Left LED)	The correct cable is in use and the connected equipment has power on ports.
	Flashing Amber (Left LED)	Network activity at this interface.
	Green (Right LED)	The interface is connected at 100 Mbps.
	Amber (Right LED)	The interface is connected at 1000 Mbps.
	Off	No link established. (Left LED) Connection is at 10Mbps. (Right LED)

Table 7: FortiGate-110C Rear Panel Connectors and Ports

Connector	Type	Speed	Supported Logical Interfaces	Description
Ports 1 to 8	RJ-45	10/100 Base_T	Data input, data output, control input and status output	Switched ports, connection to internal network.
WAN1, WAN2	RJ-45	10/100/1000 Base_T	Data input, data output, control input and status output	Connection to the Internet.
Console Port	RJ-45	9600 bps	Control input, status output	Optional connection to the management computer. Provides access to the command line interface (CLI).
USB Ports	USB	N/A	Key loading and archiving	Optional USB token.
POWER	N/A	N/A	Power	120/240VAC power connection.

FortiWiFi-60C

Figure 4: FortiWiFi-60C Front and Rear Panels

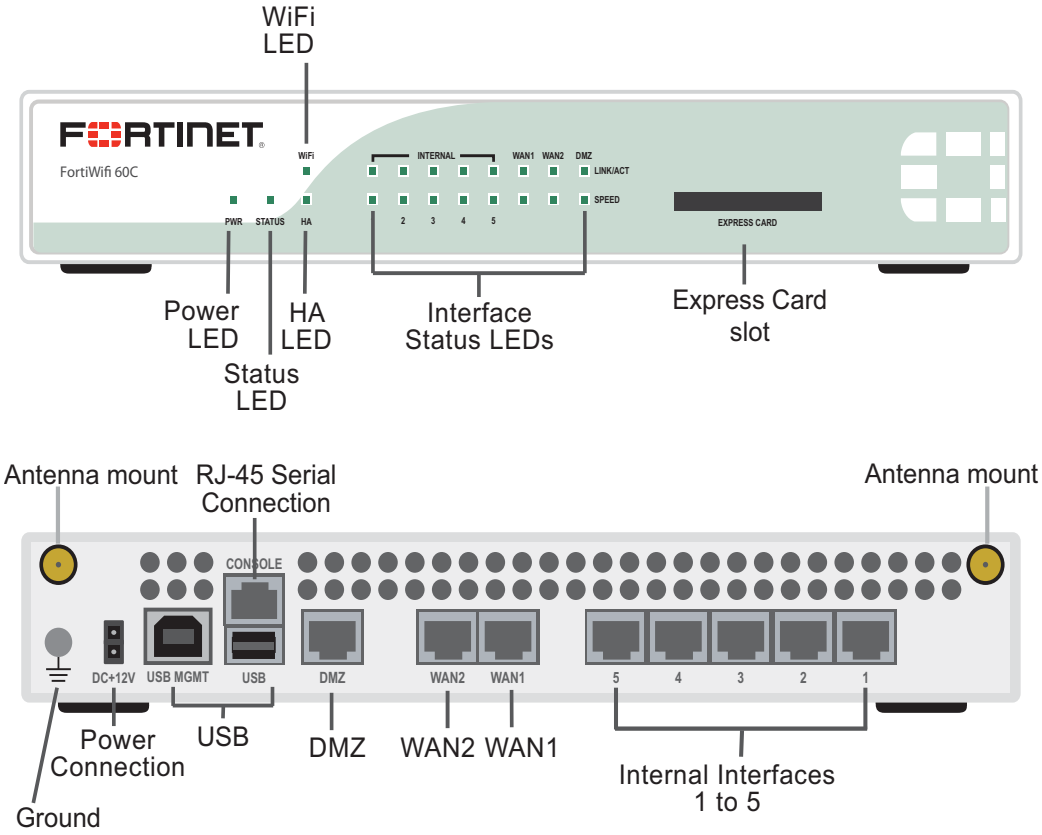


Table 8: FortiWiFi-60C Status LEDs

LED		State	Description
Power		Green	The module is powered on.
		Off	The module is powered off.
Status		Flashing	The module is starting up.
		Green	The module is running normally.
		Off	The module is powered off.
HA		Green	HA is enabled.
		Off	The unit is in stand-alone mode.
WAN1, WAN2, DMZ, Ports 1 to 5	Link/ACT	Green	Port is online.
		Flashing	Port is sending/receiving data.
		Off	Port is offline.
	Speed	Green	Connected at 1000 Mbps.
		Amber	Connected at 100 Mbps.
		Off	Connected at 10Mbps.
WiFi		Flashing	Wireless interface is active.
		Off	Wireless interface is inactive.

Table 9: FortiWiFi-60C Rear Panel Connectors and Ports

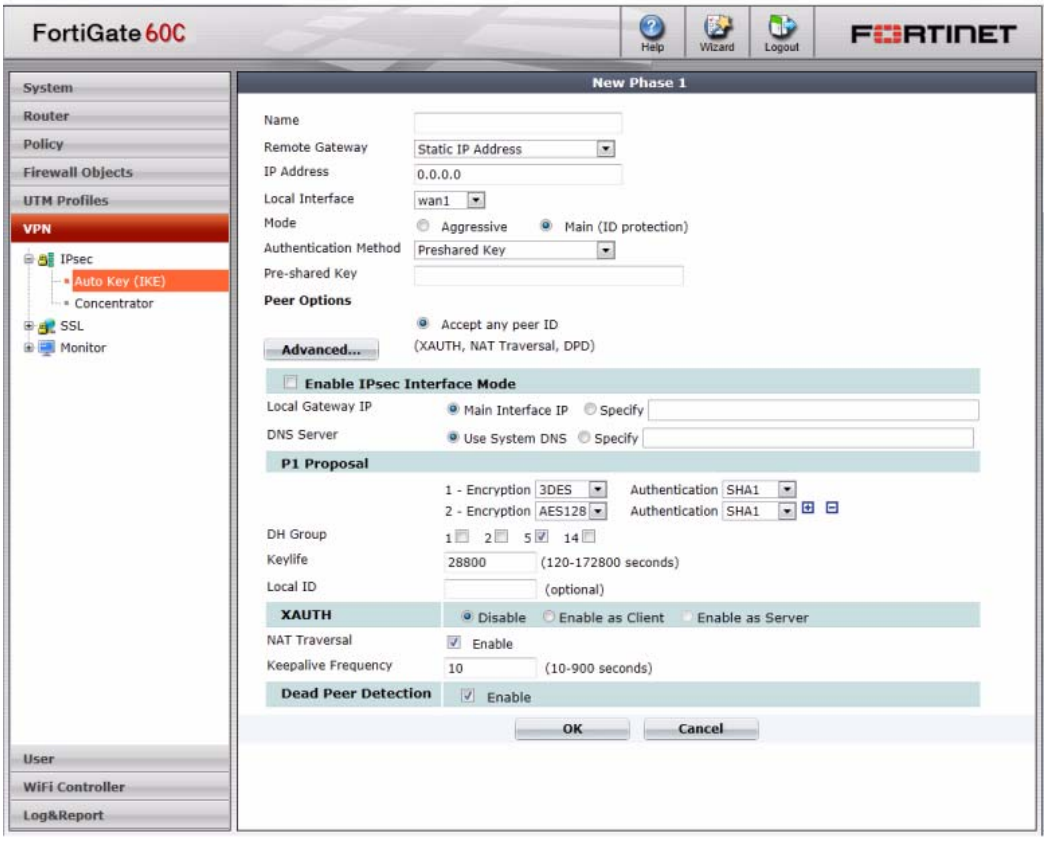
Connector	Type	Speed	Supported Logical Interfaces	Description
WAN1, WAN2, DMZ, Ports 1 to 5	RJ-45	10/100/1000 Base-T	Data input, data output, control input and status output	Copper gigabit connection to 10/100/1000 copper networks.
WiFi	Antennae	Up to 72 Mbps	Data input, data output, control input and status output	Wireless LAN connection.
CONSOLE	RJ-45	9600 bps	Control input, status output	Optional connection to the management computer. Provides access to the command line interface (CLI).
USB	USB	N/A	Key loading and archiving, configuration backup and restore	Optional connection for USB token.

Web-Based Manager

The FortiGate web-based manager provides GUI based access to the module and is the primary tool for configuring the module. The manager requires a web browser on the management computer and an Ethernet connection between the FortiGate unit and the management computer.

A web-browser that supports Transport Layer Security (TLS) 1.0 is required for remote access to the web-based manager when the module is operating in FIPS-CC mode. HTTP access to the web-based manager is not allowed in FIPS-CC mode and is disabled.

Figure 5: The FortiGate web-based manager



Command Line Interface

The FortiGate Command Line Interface (CLI) is a full-featured, text based management tool for the module. The CLI provides access to all of the possible services and configuration options in the module. The CLI uses a console connection or a network (Ethernet) connection between the FortiGate unit and the management computer. The console connection is a direct serial connection. Terminal emulation software is required on the management computer using either method. For network access, a Telnet or SSH client that supports the SSH v2.0 protocol is required (SSH v1.0 is not supported in FIPS-CC mode). Telnet access to the CLI is not allowed in FIPS-CC mode and is disabled.

Roles, Services and Authentication

Roles

When configured in FIPS-CC mode, the module provides the following roles:

- Crypto Officer
- Network User

The Crypto Officer role is initially assigned to the default ‘admin’ operator account. The Crypto Officer role has read-write access to all of the module’s administrative services. The initial Crypto Officer can create additional operator accounts. These additional accounts are assigned the Crypto Officer role and can be assigned a range of read/write or read only access permissions including the ability to create operator accounts.

The module provides a **Network User** role for end-users (Users). Network users can make use of the encrypt/decrypt services, but cannot access the module for administrative purposes.

The module does not provide a Maintenance role.

FIPS Approved Services

The following tables detail the types of FIPS approved services available to each role, the types of access for each role and the Keys or CSPs they affect.

The role names are abbreviated as follows:

Crypto Officer	CO
User	U

The access types are abbreviated as follows:

Read Access	R
Write Access	W
Execute Access	E

Table 10: Services available to Crypto Officers

Service	Access	Key/CSP
authenticate to module	WE	Operator Password, Diffie-Hellman Key, HTTP/TLS and SSH Server/Host Keys, HTTPS/TLS and SSH Session Authentication Keys, and HTTPS/TLS Session Encryption Keys, RNG Keys
show system status	WE	N/A
show FIPS-CC mode enabled/disabled (console/CLI only)	WE	N/A
enable FIPS-CC mode of operation (console only)	WE	Configuration Integrity Key
execute factory reset (zeroize keys, disable FIPS mode, console/CLI only)	E	See “Key Zeroization” on page 17
execute FIPS-CC on-demand self-tests (console only)	E	Configuration Integrity Key, Firmware Integrity Key
add/delete operators and network users	WE	Operator Password, Network User Password
set/reset operator and network user passwords	WE	Operator Password, Network User Password
backup configuration file	WE	Configuration Encryption Key, Configuration Backup Key
read/set/delete/modify module configuration	WE	N/A
enable/disable alternating bypass mode	WE	N/A

Table 10: Services available to Crypto Officers

Service	Access	Key/CSP
read/set/delete/modify IPSec/SSL VPN configuration	N/A	IPSec: IPSec Manual Authentication Key, IPSec Manual Encryption Key, IKE Pre-Shared Key, IKE RSA Key SSL: HTTPS/TLS Server/Host Key, HTTPS/TLS Session Authentication Key, HTTPS/TLS SSH Session Encryption Key
read/set/delete/modify HA configuration	WE	HA Password, HA Encryption Key
execute firmware update	E	Firmware Update Key
read log data	WE	N/A
delete log data (console/CLI only)	N/A	N/A
execute system diagnostics (console/CLI only)	WE	N/A

Table 11: Services available to Network Users

Service/CSP	Access	Key/CSP
authenticate to module	E	Network User Password, Diffie-Hellman Key, HTTPS/TLS Server/Host Key, HTTPS/TLS Session Authentication Key, HTTPS/TLS Session Encryption Key, RNG Keys
IPSec VPN controlled by firewall policies	E	Diffie-Hellman Key, IKE and IPSec Keys, RNG Keys
SSL VPN controlled by firewall policies	E	Network User Password, Diffie-Hellman Key, HTTPS/TLS Server/Host Key, HTTPS/TLS Session Authentication Key, HTTPS/TLS Session Encryption Key, RNG Keys

Authentication

The modules implement identity based authentication. Operators must authenticate with a user-id and password combination to access the modules remotely or locally via the console. Remote operator authentication is done over HTTPS (TLS) or SSH. Password entry is obfuscated using asterisks and the module does not provide feedback on the authentication process - i.e. the module does not indicate if the password or the user/operator account is incorrect for a failed authentication attempt.

By default, Network User access to the modules is based on firewall policy and authentication by IP address or fully qualified domain names. Network Users can optionally be forced to authenticate to the modules using a username/password combination to enable use of the IPSec VPN encrypt/decrypt or bypass services. For Network Users invoking the SSL-VPN encrypt/decrypt services, the modules support authentication with a user-id/password combination. Network User authentication is done over HTTPS and does not allow access to the modules for administrative purposes.

Note that operator authentication over HTTPS/SSH and Network User authentication over HTTPS are subject to a limit of 3 failed authentication attempts in 1 minute. Operator authentication using the console is not subject to a failed authentication limit, but the number of authentication attempts per minute is limited by the bandwidth available over the serial connection.

The minimum password length is 8 characters when in FIPS-CC mode (maximum password length is 32 characters). The password may contain any combination of upper- and lower-case letters, numbers, and printable symbols; allowing for 94 possible characters. The odds of guessing a password are 1 in 94^8 which is significantly lower than one in a million. Recommended procedures to increase the password strength are explained in "FIPS 140-2 Compliant Operation" on page 22.

For Network Users invoking the IPSec VPN encrypt/decrypt services, the module acts on behalf of the Network User and negotiates a VPN connection with a remote module. The strength of authentication for IPSec services is based on the authentication method defined in the specific firewall policy: IPSec manual authentication key, IKE pre-shared key or IKE RSA key (RSA certificate). The odds of guessing the authentication key for each IPSec method is:

- 1 in 16^{40} for the IPSec Manual Authentication key (based on a 40 digit, hexadecimal key)
- 1 in 94^{8} for the IKE Pre-shared Key (based on an 8 character, ASCII printable key)
- 1 in 2^{1024} for the IKE RSA Key (based on a 1024bit RSA key size)

Therefore the minimum odds of guessing the authentication key for IPSec is 1 in 94^{8}, based on the IKE Pre-shared key.

Physical Security

The modules meet FIPS 140-2 Security Level 2 requirements by using production grade components and an opaque, sealed enclosure. Access to the enclosure is restricted through the use of tamper-evident seals to secure the overall enclosure.

The seals are either blue wax/plastic with white lettering that reads "Fortinet Inc. Security Seal" (FortiGate-80C and 110C) or serialized red wax/plastic with black lettering that reads "Fortinet Security Seal" (FortiGate-60C and FortiWiFi-60C).

The tamper seals are not applied at the factory prior to shipping. It is the responsibility of the Crypto Officer to apply the seals before use to ensure full FIPS 140-2 compliance. Once the seals have been applied, the Crypto Officer must develop an inspection schedule to verify that the external enclosure of the module and the tamper seals have not been damaged or tampered with in any way. The Crypto Officer is also responsible for securing and controlling any unused seals.

The surfaces should be cleaned with 99% Isopropyl alcohol to remove dirt and oil before applying the seals. Ensure the surface is completely clean and dry before applying the seals. If a seal needs to be re-applied, completely remove the old seal and clean the surface with an adhesive remover before following the instructions for applying a new seal.

Additional seals can be requested through your Fortinet sales contact. Reference the following SKUs when ordering: FIPS-SEAL-RED or FIPS-SEAL-BLUE. Specify the type and number of seals required based on the specific module as described below:

The FortiGate-60C and FortiWiFi-60C use 1 red seal to secure the external enclosure (see Figure 6)

The FortiGate-80C uses two blue seals to secure:

- the external enclosure (two seals, see Figure 7 and Figure 8)

The FortiGate-110C uses three blue seals to secure:

- the external enclosure (two seals, see Figure 9 and Figure 10)
- the rear cover plate (one seal, see Figure 11)

Figure 6: FortiGate-60C and FortiWiFi-60C external enclosure seal, bottom, right side

Figure 7: FortiGate-80C external enclosure seal, bottom, left side

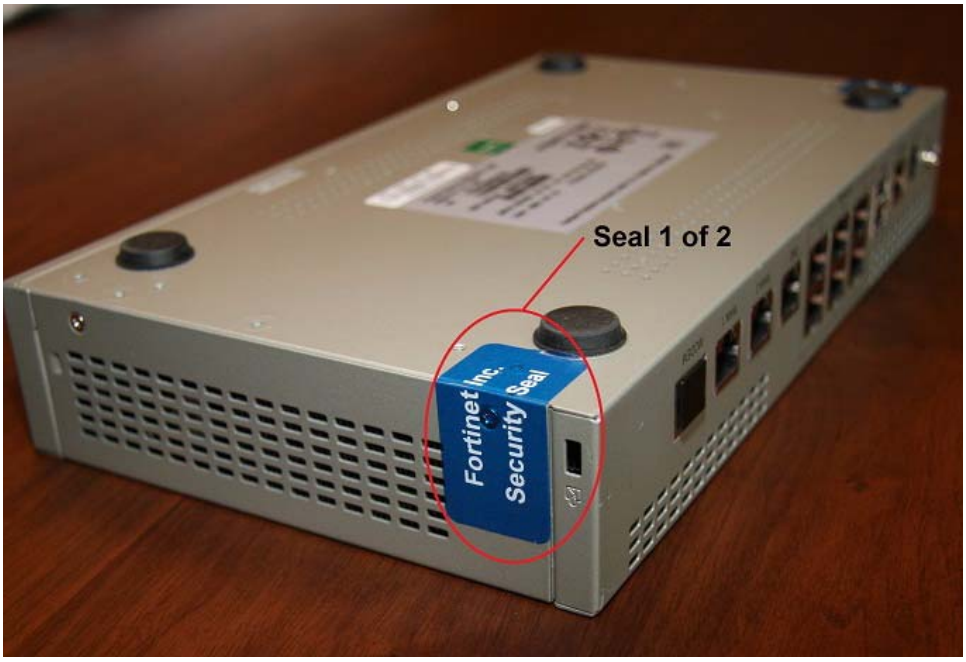


Figure 8: FortiGate-80C external enclosure seal, bottom, right side

Figure 9: FortiGate-110C external enclosure seal, bottom, left side

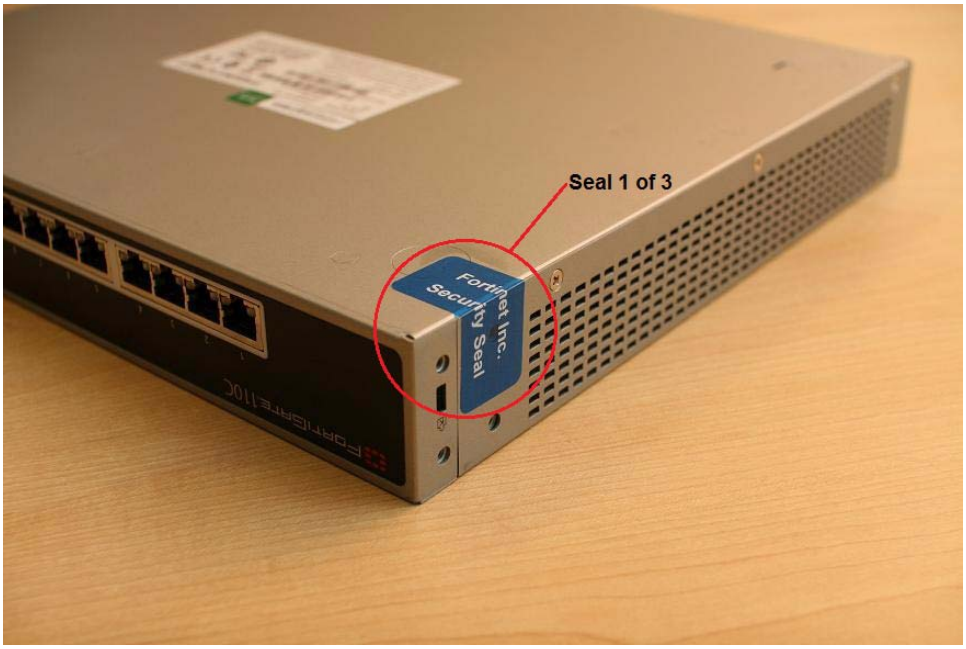


Figure 10: FortiGate-110C external enclosure seal, bottom, right side

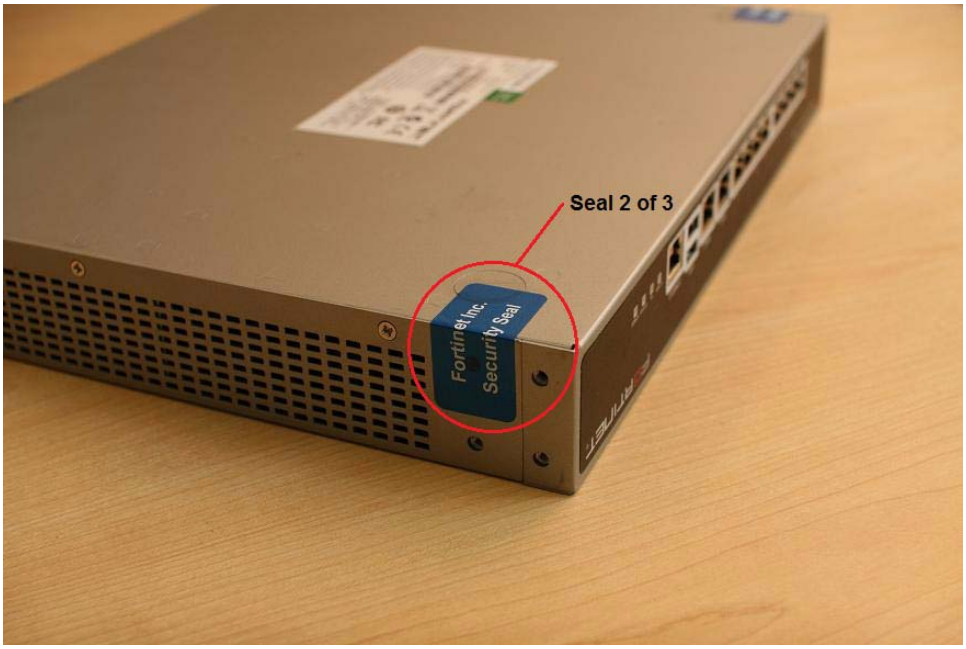


Figure 11: FortiGate-110C cover plate seal

Operational Environment

The module consists of the combination of the FortiOS operating system and the FortiGate appliances. The FortiOS operating system can only be installed, and run, on a FortiGate appliance. The FortiOS operating system provides a proprietary and non-modifiable operating system.

Cryptographic Key Management

Random Number Generation

The modules use a firmware based, deterministic random number generator that conforms to ANSI X9.31 Appendix A.2.4.

The ANSI X9.31 RNG is seeded using a 128-bit AES seed key generated external to the module (estimated entropy 128 bits) and 256 bits of seed (estimated entropy 60 bits) gathered from a random pool filled with 64 bytes of system data and internal resources such as time, memory addresses, kernel ticks, and module identifiers. As the module's ANSI X9.31 RNG implementation only generates random values of size 128 bits, it would take multiple calls to form a 256-bit key. Each time a key is generated with a bit length of more than 128 bits, the key is refreshed with an additional 12 bits of entropy. The total estimated strength for the two calls required to form a 256 bit key would be at theoretical best 200 bits.

Key Zeroization

The zeroization process must performed under the direct control of the operator. The operator must be present to observe that the zeroization method has completed successfully.

All keys except the following are zeroized by executing a factory reset:

- ANSI X9.31 RNG AES Key
- Firmware Update Key
- Firmware Integrity Key
- Configuration Integrity Key
- Configuration Backup Key
- SSH Server/Host Key
- HTTPS/TLS Server/Host Key

All keys and CSPs are zeroized by formatting the modules' flash memory storage. To format the flash memory, connect a computer to the modules' console port and reboot the module. Access the configuration menu by pressing any key when prompted (see example below). Select "F" to format the flash memory (boot device).

```
Press any key to display configuration menu...

[G]:  Get firmware image from TFTP server.
[F]:  Format boot device.
[B]:  Boot with backup firmware and set as default.
[I]:  Configuration and information.
[Q]:  Quit menu and continue to boot with default firmware.
[H]:  Display this list of options.

Enter G,F,B,I,Q,or H:
```

Algorithms

Table 12: FIPS Approved Algorithms

Algorithm	NIST Certificate Numbers
RNG (ANSI X9.31 Appendix A)	1234
Triple-DES	1424, 1572, 1573
AES	2277, 2607, 2608
SHA-1	1958, 2191, 2192
SHA-256	1958, 2191, 2192
HMAC SHA-1	1395, 1615, 1616
HMAC SHA-256	1395, 1615, 1616
RSA PKCS1 (digital signature creation and verification)	1168, 1334

Table 13: FIPS Allowed Algorithms

Algorithm
RSA (key establishment methodology provides 80 or 112 bits of encryption strength)
Diffie-Hellman (key agreement; key establishment methodology provides between 80 and 201bits of encryption strength; non-compliant less than 80-bits of encryption strength)
NDRNG

Table 14: Non-FIPS Approved Algorithms

Algorithm
DES (disabled in FIPS-CC mode)
MD5 (disabled in FIPS-CC mode except for use in the TLS protocol)
HMAC MD5 (disabled in FIPS-CC mode)
AES-CCM (non-compliant, FortiWiFi-60C only)

Note that some algorithms may be classified as deprecated, restricted, or legacy-use. Please consult NIST SP 800-131A for details.

The vendor makes no conformance claims to any key derivation function specified in SP 800-135rev1. References to the key derivation functions addressed in SP 800-135rev1 including IKE, SSH, and TLS are only listed to clarify the key types supported by the module. Keys related to IKE, SSH, and TLS are only used in the Approved mode under the general umbrella of a non-Approved Diffie-Hellman scheme, with no assurance claims to the underlying key derivation functions.

Cryptographic Keys and Critical Security Parameters

The following table lists all of the cryptographic keys and critical security parameters used by the module. The following definitions apply to the table:

Key or CSP The key or CSP description.

Storage Where and how the keys are stored

Usage How the keys are used

Table 15: Cryptographic Keys and Critical Parameters used in FIPS-CC Mode

Key or CSP	Storage	Usage
Diffie-Hellman Keys	SDRAM Plaintext	Key agreement and key establishment
IPSec Manual Authentication Key	Flash RAM AES encrypted	Used as IPSec Session Authentication Key
IPSec Manual Encryption Key	Flash RAM AES encrypted	Used as IPSec Session Encryption Key
IPSec Session Authentication Key	SDRAM Plain-text	IPSec peer-to-peer authentication using HMAC SHA-1
IPSec Session Encryption Key	SDRAM Plain-text	VPN traffic encryption/decryption using Triple-DES or AES
IKE Pre-Shared Key	Flash RAM AES encrypted	Used to generate IKE protocol keys
IKE Authentication Key	SDRAM Plain-text	IKE peer-to-peer authentication using HMAC SHA-1 (SKEYID_A)
IKE Key Generation Key	SDRAM Plain-text	IPSec SA keying material (SKEYID_D)
IKE Session Encryption Key	SDRAM Plain-text	Encryption of IKE peer-to-peer key negotiation using Triple-DES or AES (SKEYID_E)
IKE RSA Key	Flash Ram Plain text	Used to generate IKE protocol keys
RNG Seed (ANSI X9.31 Appendix A.2.4)	Flash RAM Plain-text	Seed used for initializing the RNG
RNG AES Key (ANSI X9.31 Appendix A.2.4)	Flash RAM Plain-text	AES Seed key used with the RNG
Firmware Update Key	Flash RAM Plain-text	Verification of firmware integrity when updating to new firmware versions using RSA public key. Firmware update can only be performed when in the FIPS-approved mode of operation.
Firmware Integrity Key	Flash RAM Plain-text	Verification of firmware integrity in the firmware integrity test using RSA public key
HTTPS/TLS Server/Host Key	Flash RAM Plain-text	RSA private key used in the HTTPS/TLS protocols
HTTPS/TLS Session Authentication Key	SDRAM Plain-text	HMAC SHA-1 key used for HTTPS/TLS session authentication
HTTPS/TLS Session Encryption Key	SDRAM Plain-text	AES or Triple-DES key used for HTTPS/TLS session encryption
SSH Server/Host Key	Flash RAM Plain-text	RSA private key used in the SSH protocol
SSH Session Authentication Key	SDRAM Plain-text	HMAC SHA-1 key used for SSH session authentication
SSH Session Encryption Key	SDRAM Plain-text	AES or Triple-DES key used for SSH session encryption
Operator Password	Flash RAM SHA-1 hash	Used to authenticate operator access to the module
Configuration Integrity Key	Flash RAM Plain-text	SHA-1 hash used for configuration/VPN bypass test

Table 15: Cryptographic Keys and Critical Parameters used in FIPS-CC Mode

Key or CSP	Storage	Usage
Configuration Encryption Key	Flash RAM Plain-text	AES key used to encrypt CSPs on the flash RAM and in the backup configuration file (except for operator passwords in the backup configuration file)
Configuration Backup Key	Flash RAM Plain-text	HMAC SHA-1 key used to encrypt operator passwords in the backup configuration file
Network User Password	Flash RAM AES encrypted	Used during network user authentication
HA Password	Flash RAM AES encrypted	Used to authenticate FortiGate units in an HA cluster
HA Encryption Key	Flash RAM AES encrypted	Encryption of traffic between units in an HA cluster using AES

Alternating Bypass Feature

The primary cryptographic function of the module is as a firewall and VPN device. The module implements two forms of alternating bypass for VPN traffic: policy based (for IPSec and SSL VPN) and interface based (for IPSec VPN only).

Policy Based VPN

Firewall policies with an action of IPSec or SSL-VPN mean that the firewall is functioning as a VPN start/end point for the specified source/destination addresses and will encrypt/decrypt traffic according to the policy. Firewall policies with an action of allow mean that the firewall is accepting/sending plaintext data for the specified source/destination addresses.

A firewall policy with an action of accept means that the module is operating in a bypass state for that policy. A firewall policy with an action of IPSec or SSL-VPN means that the module is operating in a non-bypass state for that policy.

Interface Based VPN

Interface based VPN is supported for IPSec only. A virtual interface is created and any traffic routed to the virtual interface is encrypted and sent to the VPN peer. Traffic received from the peer is decrypted. Traffic through the virtual interface is controlled using firewall policies. However, unlike policy based VPN, the action is restricted to Accept or Deny and all traffic controlled by the policy is encrypted/decrypted.

When traffic is routed over the non-virtual interfaced, the module is operating in a bypass state. When traffic is routed over the virtual interface, the module is operating in a non-bypass state.

In both cases, two independent actions must be taken by a CO to create bypass firewall policies: the CO must create the bypass policy and then specifically enable that policy.

Key Archiving

The module supports key archiving to a management computer or USB token as part of a module configuration file backup. Operator entered keys are archived as part of the module configuration file. The configuration file is stored in plain text, but keys in the configuration file are either AES encrypted using the Configuration Encryption Key or stored as a keyed hash using HMAC-SHA-1 using the Configuration Backup Key.

Electromagnetic Interference/Electromagnetic Compatibility (EMI/EMC)

The modules comply with EMI/EMC requirements for Class A or B (business use) devices as specified by Part 15, Subpart B, of the FCC rules. The following table lists the specific lab and FCC report information for the modules.

Table 16: FCC Report Information

Module	Lab Information	FCC Report Number
FG-60C	Bay Area Compliance Laboratories Corp 1274 Anvilwood Avenue Sunnyvale, CA 94089, USA 408-732-9162 408-732-9164	R1004167
FG-80C	Spectrum Research and Testing Laboratory, Inc No. 101-10, Ling 8 Shan-Tong Li Chung-Li City Taoyuan, Taiwan 03-498-7684 03-498-6528	FCBA10030506
FG-110C	Bay Area Compliance Laboratories Corp 6/F, WanLi industrial Building, 3rd Phase ShiHua Road, FuTian Free Trade Zone Shenzhen, Guandong, China 86-755-33320018 86-755-33320008	RBJA09040751

The FortiWiFi-60C module is declared to conform with EMI/EMC requirements for Class B (business use) devices as specified by Part 15, Subpart B, of the FCC rules.

Mitigation of Other Attacks

The module includes a real-time Intrusion Prevention System (IPS) as well as antivirus protection, antispam and content filtering. Use of these capabilities is optional.

The FortiOS IPS has two components: a signature based component for detecting attacks passing through the FortiGate appliance and a local attack detection component that protects the firewall from direct attacks. Functionally, signatures are similar to virus definitions, with each signature designed to detect a particular type of attack. The IPS signatures are updated through the FortiGuard IPS service. The IPS engine can also be updated through the FortiGuard IPS service.

FortiOS antivirus protection removes and optionally quarantines files infected by viruses from web (HTTP), file transfer (FTP), and email (POP3, IMAP, and SMTP) content as it passes through the FortiGate modules. FortiOS antivirus protection also controls the blocking of oversized files and supports blocking by file extension. Virus signatures are updated through the FortiGuard antivirus service. The antivirus engine can also be updated through the FortiGuard antivirus service.

FortiOS antispam protection tags (SMTP, IMAP, POP3) or discards (SMTP only) email messages determined to be spam. Multiple spam detection methods are supported including the FortiGuard managed antispam service.

FortiOS web filtering can be configured to provide web (HTTP) content filtering. FortiOS web filtering uses methods such as banned words, address block/exempt lists, and the FortiGuard managed content service.

Whenever a IPS, antivirus, antispam or filtering event occurs, the modules can record the event in the log and/or send an alert email to an operator.

For complete information refer to the FortiGate Installation Guide for the specific module in question, the FortiGate Administration Guide and the FortiGate IPS Guide.

FIPS 140-2 Compliant Operation

FIPS 140-2 compliant operation requires both that you use the module in its FIPS-CC mode of operation and that you follow secure procedures for installation and operation of the FortiGate unit. You must ensure that:

- The FortiGate unit is configured in the FIPS-CC mode of operation.
- The FortiGate unit is installed in a secure physical location.
- Physical access to the FortiGate unit is restricted to authorized operators.
- Administrative passwords are at least 8 characters long.
- Administrative passwords are changed regularly.
- Administrator account passwords must have the following characteristics:
  - One (or more) of the characters should be capitalized
  - One (or more) of the characters should be numeric
  - One (or more) of the characters should be non alpha-numeric (e.g. punctuation mark)
- Administration of the module is permitted using only validated administrative methods. These are:
  - Console connection
  - Web-based manager via HTTPS
  - Command line interface (CLI) access via SSH
- Diffie-Hellman groups of less than less than 1024 bits (Group 5) are not used.
- Client side RSA certificates must use 1024 bit or greater key sizes.
- LDAP based authentication must use secure LDAP (LDAPS).
- Only approved and allowed algorithms are used (see “Algorithms” on page 18).
- The tamper evident seals are applied (see “Physical Security” on page 13).

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

Enabling FIPS-CC mode

To enable the FIPS 140-2 compliant mode of operation, the operator must execute the following command from the Local Console:

```
config system fips
  set status enable
end
```

The Operator is required to supply a password for the admin account which will be assigned to the Crypto Officer role.

The supplied password must be at least 8 characters long and correctly verified before the system will restart in FIPS-CC mode.

Upon restart, the module will execute self-tests to ensure the correct initialization of the module's cryptographic functions.

After restarting, the Crypto Officer can confirm that the module is running in FIPS-CC mode by executing the following command from the CLI:

```
get system status
```

If the module is running in FIPS-CC mode, the system status output will display the line:

```
FIPS-CC mode: enable
```

Note that enabling/disabling the FIPS-CC mode of operation will automatically invoke the key zeroization service. The key zeroization is performed immediately after FIPS-CC mode is enabled/disabled.

Self-Tests

The module executes the following self-tests during startup and initialization:

- Firmware integrity test using RSA signatures
- Configuration/VPN bypass test using HMAC SHA-1
- Triple-DES, CBC mode, encrypt known answer test
- Triple-DES, CBC mode, decrypt known answer test
- AES, CBC mode, encrypt known answer test
- AES, CBC mode, decrypt known answer test
- HMAC SHA-1 known answer test
- SHA-1 known answer test (test as part of HMAC SHA-1 known answer test)
- HMAC SHA-256 known answer test
- SHA-256 known answer test (test as part of HMAC SHA-256 known answer test)
- RSA signature generation known answer test
- RSA signature verification known answer test
- RNG known answer test

The results of the startup self-tests are displayed on the console during the startup process. The startup self-tests can also be initiated on demand using the CLI command **execute fips kat all** (to initiate all self-tests) or **execute fips kat <test>** (to initiate a specific self-test).

When the self-tests are run, each implementation of an algorithm is tested - e.g. when the AES self-test is run, all AES implementations are tested.

The module executes the following conditional tests when the related service is invoked:

- Continuous RNG test
- Continuous NDRNG test
- RSA pairwise consistency test
- Configuration/VPN bypass test using HMAC SHA-1
- Firmware load test using RSA signatures

If any of the self-tests or conditional tests fail, the module enters an error state as shown by the console output below:

```
Self-tests failed
Entering error mode...
The system is going down NOW !!
The system is halted.
```

All data output and cryptographic services are inhibited in the error state.

Non-FIPS Approved Services

The module also provides the following non-FIPS approved services:

- Configuration backups using password protection
- WiFi encryption using AES-CCM (FortiWiFi-60C only)
- LLTP and PPTP VPN

If the above services are used, the module is not considered to be operating in the FIPS approved mode of operation.