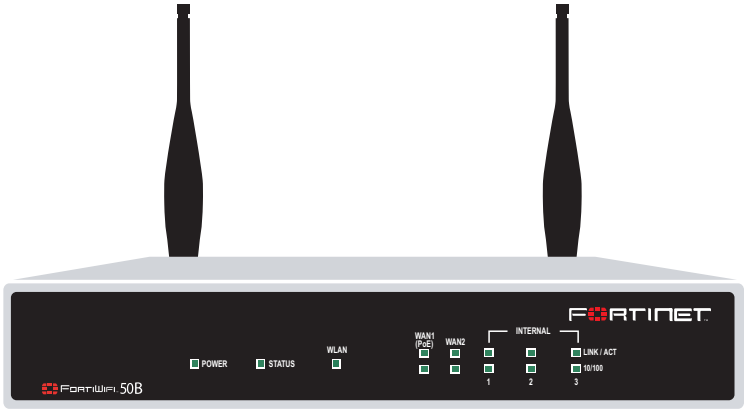
FIPS 140-2 Security Policy

FortiWiFi-50B



FortiWiFi-50B FIPS 140-2 Security Policy	
Document Version:	2.7
Publication Date:	February 4, 2009
Description:	Documents FIPS 140-2 Security Policy issues, compliancy and requirements for FIPS compliant operation.
Hardware Models:	FortiWiFi-50B (C5WF27)
Firmware Version:	FortiOS 3.00,build8802,080626

FortiWiFi-50B FIPS 140-2 Security Policy

v2.7

February 4, 2009

01-00000-0388-20080704

Trademarks

Contents

This document is a FIPS 140-2 Security Policy for Fortinet Incorporated's FortiWiFi-50B Multi-Threat Security System. This policy describes how the FortiWiFi-50B (hereafter referred to as the 'module') meets the FIPS 140-2 security requirements and how to operate the module in a FIPS compliant manner. This policy was created as part of the Level 2 FIPS 140-2 validation of the module.

Note that the FortiWiFi-50B is considered part of Fortinet's FortiGate family of products. General documentation and references related to the FortiGate product in this Security Policy also apply to the FortiWiFi product.

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 FortiGate module in the technical terms of the FIPS 140-2 standard and the associated validation program. This policy also provides information on the differences between the normal FortiGate mode of operation and the FIPS-CC mode of operation. Other FortiGate 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 FortiGate 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.

Security Level Summary

The Fortinet FortiWiFi-50B module meets the overall requirements for a Level 2 FIPS 140-2 certification.

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	N/A
Cryptographic Key Management	2
EMI/EMC	2
Self-Tests	2
Design Assurance	3
Mitigation of Other Attacks	2

FIPS-CC Mode of Operation

To operate the FortiGate modules in a FIPS compliant manner, the modules must be configured to run in the FIPS-CC mode of operation. Enabling the FIPS-CC mode of operation sets default values, disables some features and performs additional configuration procedures. See “FIPS 140-2 Compliant Operation” on page 21 for complete details on configuring the modules in the FIPS-CC mode of operation.

FortiGate Module Description

The FortiGate family spans the full range of network environments, from SOHO to service provider, offering cost effective systems for any size of application. They 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, the FortiGate module 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 Multi-Layered Security Systems employ Fortinet’s unique FortiASIC™ content processing chip and the powerful, secure, FortiOS™ operating system to 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. As the only systems in the world that are certified by ICSA for firewall, IPSec VPN, SSL VPN, antivirus, and intrusion

prevention functionality, the FortiGate modules deliver the highest level of security available. They provide a critical layer of real-time, network-based antivirus protection that complements host-based antivirus software and supports “defense-in-depth” strategies without compromising performance or cost. 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.

FortiGate modules support the IPSec industry standard for VPN, allowing VPNs to be configured between a FortiGate module and any client or gateway/firewall that supports IPSec VPN. FortiGate modules also provide SSL VPN services.

This section contains the following information:

Cryptographic Module Description

The FortiWiFi-50B is a multiple chip, standalone cryptographic module consisting of production grade components contained in a physically protected enclosure in accordance with FIPS 140-2 Level 2 requirements.

The module is an Internet device that provides integrated firewall, VPN, antivirus, antispam, intrusion prevention, content filtering and traffic shaping and HA capabilities. This FIPS 140-2 Security Policy specifically covers the firewall, IPSec and SSL-VPN capabilities of the module.

The antivirus, antispam, intrusion prevention, content filtering and traffic shaping capabilities of the module can be used without compromising the FIPS-CC mode of operation.

The FortiWiFi-50B has 5 network interfaces with a status LED for each network interface (3 10/100 BaseT (switched), 2 10/100 Base T). The FortiWiFi-50B also includes an IEEE 802.11b and 802.11g compliant WiFi interface with a separate status LED.

The module has a single x86 compatible CPU.

The module is a 1u desktop device.

The module has no internal hard drive.

Cryptographic Module Ports and Interfaces

FortiWiFi-50B Module

Figure 1: FortiWiFi-50B Front and Rear Panels

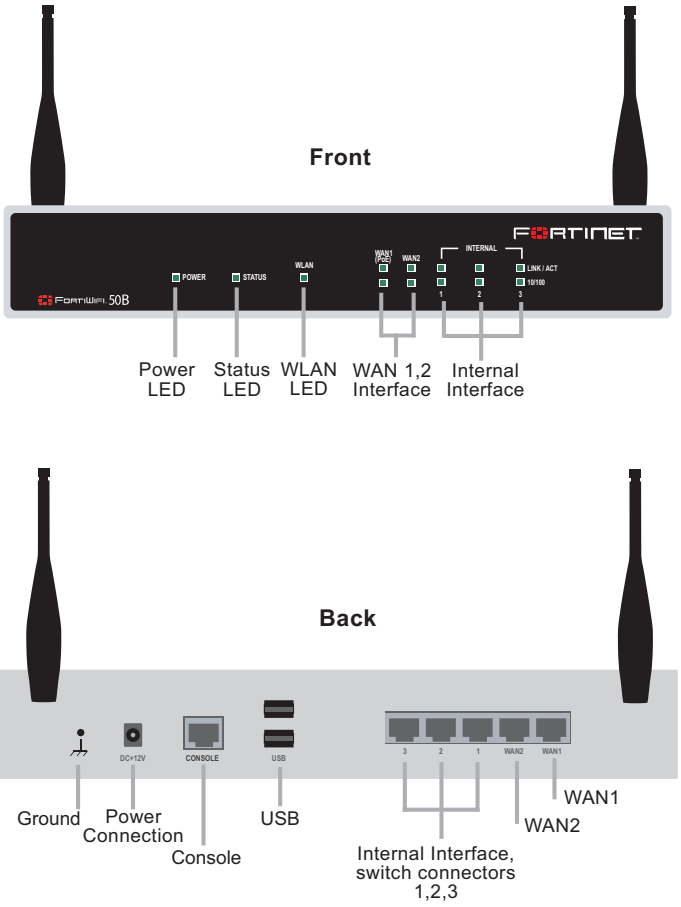


Table 2: FortiWiFi-50B Status LEDs

LED	State	Description
Power	Green	The FortiWiFi unit is powered on.
	Off	The FortiWiFi unit is powered off.
Status	Flashing	Flashing occurs during start up or reboot.
	Off	Normal operation.
WLAN	Green	The WLAN interface is enabled.
	Off	The WLAN interface is disabled.
Link/Activity	Green	The correct cable is in use and the connected equipment has power.
	Flashing Green	Network activity at this interface.
	Off	No link established.
10/100	Green	The interface is connected at 100 Mbps.

Table 3: FortiWiFi-50B Rear Panel Connectors and Ports

Connector	Type	Speed	Supported Logical Interfaces	Description
Internal	RJ-45	10/100Base_T	Data input, data output, control input and status output	Default connection to the internal network. 3 port switched interface.
WAN1 and 2	RJ-45	10/100Base_T	Data input, data output, control input and status output	Redundant connections to the Internet.
WLAN	Antennae	Up to 54Mbps	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	Optional connection for FortiUSB token.
POWER	N/A	N/A	Power	120/240VAC power connection.

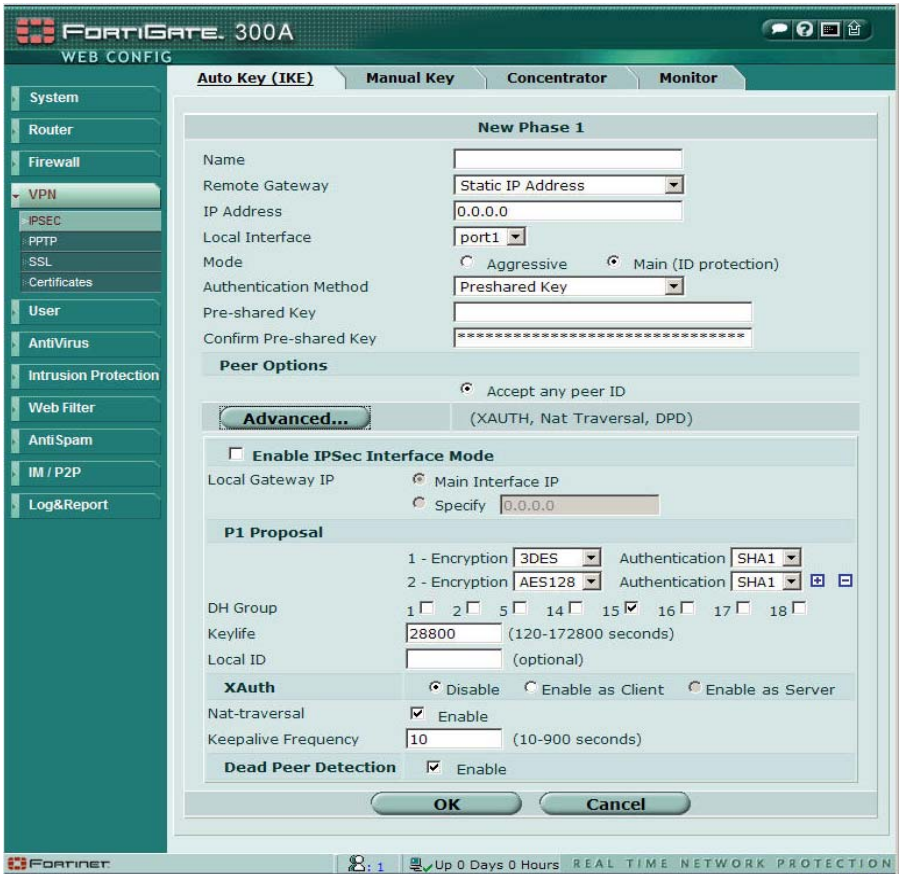
Web-Based Manager

The FortiGate web-based manager provides GUI based access to the modules and is the primary tool for configuring the modules. The manager requires a web browser on the management computer and an Ethernet connection between the FortiGate modules 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 modules are operating in FIPS-CC mode. HTTP access to the web-based manager is not allowed in FIPS-CC mode and is disabled.

The web browser is not part of the validated module boundary.

Figure 2: The FortiGate web-based manager



Command Line Interface

The FortiGate Command Line Interface (CLI) is a full-featured, text based management tool for the FortiGate modules. The CLI provides access to all of the possible services and configuration options in the modules. The CLI uses a console connection or a network (Ethernet) connection between the FortiGate module 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).

The Telnet or SSH client is not part of the validated module boundaries.

Roles, Services and Authentication

Roles

When configured in FIPS-CC mode, the modules provide three roles for Crypto Officers (hereafter referred to as operators): **Security Administrator**, **Crypto Administrator** and **Audit Administrator**. These roles, or combinations of these roles, are assumed by an operator after authenticating to the modules remotely or through the console connection using a username/password combination.

An operator assuming the Security Administrator role has read/write access to all of the administrative functions and services of the modules, including resetting or shutting down the modules. An operator with the Security Administrator role can also create accounts for additional operators and assign roles to those operators. However, the Security Administrator role has read only access to crypto and audit related functions and services.

An operator assuming the Crypto Administrator role has read/write access to crypto related functions and services and read only access to all other functions and services.

An operator assuming the Audit Administrator role has read/write access to audit related functions and services and read only access to all other functions and services.

Operators can be assigned more than one role. An operator that assumes all three administrative roles has complete administrative access to the module. Multiple operator accounts can be created. Operator accounts are differentiated by the username during authentication. More than one operator can be connected to the module at any given time, however each operator session is authenticated separately.

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

Refer to the next section on Services for detailed information on what functions and services each role has access to.

The modules do 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:

Security Administrator	SA
Crypto Administrator	CA
Audit Administrator	AA
Network User	NU

The access types are abbreviated as follows:

Read Access	R
Write Access	W
Execute Access	E

Table 4: FIPS approved services available by role via the CLI (console or SSH)

Service	SA	CA	AA	Key/CSP
authenticate to module	E	E	E	Operator Username, Operator Password
show system status	R	N/A	N/A	N/A
show FIPS-CC mode enabled/disabled	R	N/A	N/A	N/A
enable FIPS-CC mode of operation (console only)	WE	N/A	N/A	FIPS-CC Mode Key
set/reset operator passwords	WE	N/A	N/A	Operator Password
execute factory reset (zeroize keys, disable FIPS-CC mode)	E	N/A	N/A	All keys stored in Flash RAM
execute FIPS-CC on-demand self-tests (console only)	E	E	E	N/A
add/delete operators	RWE	N/A	N/A	Operator Username, Operator Password
set/reset own password	WE	N/A	N/A	Operator Password
execute firmware download	E	N/A	N/A	N/A
execute system reboot	E	N/A	N/A	N/A
execute system shutdown	E	N/A	N/A	N/A
backup configuration file	WE	N/A	N/A	All keys stored in Flash RAM
restore system configuration	RWE	N/A	N/A	All keys stored in Flash RAM
execute system diagnostics	E	E	E	N/A
change system time	WE	N/A	N/A	N/A
read/set/delete/modify system/network configuration	RWE	N/A	N/A	N/A
read/set/delete/modify firewall policies. enable/disable alternating bypass mode	RWE	N/A	N/A	N/A
read/set/delete/modify AV configuration	RWE	N/A	N/A	N/A
read/set/delete/modify AS configuration	RWE	N/A	N/A	N/A
read/set/delete/modify Web Filter configuration	RWE	N/A	N/A	N/A
read/set/delete/modify IM/P2P configuration	RWE	N/A	N/A	N/A
read/set/delete/modify VPN configuration	N/A	RWE	N/A	IPSec Manual Authentication Key, IPSec Manual Encryption Key, IKE Pre-Shared Key, IKE RSA Key
read/set/delete/modify IPS configuration	RWE	N/A	N/A	N/A
read/set/delete/modify logging configuration	RWE	N/A	N/A	N/A
read log data	R	R	R	N/A
delete log data	N/A	N/A	WE	N/A

Table 5: FIPS approved services available by role via the web-manager

Service	SA	CA	AA	Key/CSP
authenticate to module	E	E	E	Operator Username, Operator Password
show system status	R	N/A	N/A	N/A
set/reset operator passwords	WE	N/A	N/A	Operator Password
execute factory reset (zeroize keys, disable FIPS-CC mode)	E	N/A	N/A	All keys stored in Flash RAM
add/delete operators	RWE	N/A	N/A	Operator Username, Operator Password
set/reset own password	WE	N/A	N/A	Operator Password
execute firmware download	E	N/A	N/A	N/A
execute system reboot	E	N/A	N/A	N/A
execute system shutdown	E	N/A	N/A	N/A
backup configuration file	WE	N/A	N/A	All keys stored in Flash RAM
restore system configuration	RWE	N/A	N/A	All keys stored in Flash RAM
change system time	WE	N/A	N/A	N/A
read/set/delete/modify system/network configuration	RWE	N/A	N/A	N/A
read/set/delete/modify firewall policies. enable/disable alternating bypass mode	RWE	N/A	N/A	N/A
read/set/delete/modify AV configuration	RWE	N/A	N/A	N/A
read/set/delete/modify AS configuration	RWE	N/A	N/A	N/A
read/set/delete/modify Web Filter configuration	RWE	N/A	N/A	N/A
read/set/delete/modify IM/P2P configuration	RWE	N/A	N/A	N/A
read/set/delete/modify VPN configuration	N/A	RWE	N/A	IPSec Manual Authentication Key, IPSec Manual Encryption Key, IKE Pre-Shared Key, IKE RSA Key
read/set/delete/modify IPS configuration	RWE	N/A	N/A	N/A
read/set/delete/modify logging configuration	RWE	N/A	N/A	N/A
read log data	R	R	R	N/A
manual AV/IPS signature download/update	E	N/A	N/A	N/A

Table 6: VPN Cryptographic Services available to Network Users

Service	NU	Key/CSP
authenticate to module	WE	Network User Username, Network User Password
encrypt/decrypt controlled by firewall policies	E	N/A

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 or SSH.

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 for operator authentication using the Web-based manager 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. Using a strong password policy, where operator and network user passwords are at least 8 characters in length and use a mix of alphanumeric (printable) characters from the ASCII character set, the odds of guessing a password are 1 in 94^8.

For Network Users invoking the IPSec 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 Preshared 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 Preshared key.

For Network Users invoking the wireless WPA2 encrypt/decrypt services, the module acts on behalf of the Network User and negotiates a wireless connection with a remote computer running a wireless client. The strength of authentication for wireless services is based on the preshared key defined in the module's wireless interface configuration. The preshared key is effectively a password used to access the WPA2 encrypt/decrypt services.

The minimum wireless preshared key length is 8 characters when in FIPS-CC mode. Using a strong password policy, where the preshared key is at least 8 characters in length and use a mix of alphanumeric (printable) characters from the ASCII character set, the odds of guessing the wireless preshared key are 1 in 94^8.

Physical Security

The module 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 a tamper-evident seal to secure the overall enclosure.

The seal is blue wax/plastic with white lettering that reads “Fortinet Inc. Security Seal”.

The tamper seal is not applied at the factory prior to shipping. The seal to secure each module is included in the product packaging. It is the responsibility of the customer to apply the seal before use to ensure full FIPS compliance. Once the seal has been applied, the customer must develop an inspection schedule to verify that the external enclosure of the module and the tamper seal has not been damaged or tampered with in any way.

The FortiWiFi-50B uses 1 seal to secure the external enclosure as shown in Figure 3.

Figure 3: FortiWiFi-50B security seal placement

Operational Environment

This section is not applicable to the module. The module utilizes a firmware based, proprietary and non-modifiable operating system that does not provide a programming environment.

Cryptographic Key Management

Random Number Generation

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

Key Zeroization

All keys and CSPs except the ANSI X9.31 RNG AES Key are zeroized when the operator executes a factory reset via the web-manager, CLI or console and when enabling or disabling the FIPS-CC mode of operation via the console. The ANSI X9.31 RNG AES Key is zeroized by executing a factory reset followed by a firmware update. See Table 9 on page 17 for a complete list of keys and CSPs.

Algorithms

Table 7: FIPS Approved or Allowed Algorithms

Algorithm	NIST Certificate Number
RNG (ANSI X9.31 Appendix A)	345
Triple-DES	489, 583, 584
AES	475, 613, 614, 758
SHA-1	543, 661, 662
HMAC SHA-1	232, 316, 317
Diffie-Hellman (key agreement; key establishment methodology provides between 80 and 201 bits of encryption strength; non-compliant less than 80-bits of encryption strength)	
RSA ANSI X9.31 (key generation, signature generation/verification)	285
RSA PKCS1 (digital signature creation and verification, key wrapping; key establishment method provides 112 bits of encryption strength - only 2048 bit certificates are supported)	285

Table 8: 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)

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 9: FIPS Approved Cryptographic Keys and Critical Security Parameters

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 derive 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	X.509 certificate used to derive IKE protocol keys
RNG Seed (ANSI X9.31 Appendix A.2.4)	SDRAM Plain-text	Seed used for initializing the RNG
RNG AES Key (ANSI X9.31 Appendix A.2.4)	SDRAM Plain-text	AES Seed key used with the RNG
Firmware Download Public Key	Flash RAM Plain-text	Verification of firmware integrity for download of new firmware versions using RSA public key
TLS/SSH/SSL-VPN Server/Host Key	Flash RAM Plain-text	Remote Web manager and CLI authentication using HMAC SHA-1. Also used for encrypting TLS session key using RSA method.
HTTPS Session Key	SDRAM Plain-text	Remote Web manager session encryption and authentication using AES or Triple-DES
SSH Session Key	SDRAM Plain-text	Remote CLI session encryption and authentication using AES or Triple-DES
SSL-VPN Session Key	SDRAM Plain-text	SSL-VPN session encryption and authentication using AES or Triple-DES
Operator Username	Flash RAM Plain-text	Used during operator authentication to identify and assign roles to operators
Operator Password	Flash RAM SHA-1 hash	Used to authenticate operator access to the module
FIPS-CC Mode Key	Flash RAM Plain-text	HMAC SHA-1 key used for configuration, firmware and VPN integrity (bypass) test
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)

Table 9: FIPS Approved Cryptographic Keys and Critical Security Parameters

Key or CSP	Storage	Usage
Configuration Backup Key	Flash RAM Plain-text	HMAC SHA-1 key used to encrypt operator passwords in the backup configuration file
Network User Name	Flash RAM Plaintext	Used during network user authentication
Network User Password	Flash RAM SHA-1 hash	Used during network user authentication
Wireless (WPA2) Pre-Shared Key	Flash Ram AES Encrypted	Peer-to-Peer authentication
Wireless (WPA2) Encryption Key	SDRAM Plain-text	Wireless traffic encryption/decryption

Alternating Bypass Feature

The primary cryptographic function of the FortiGate modules is as a firewall and VPN device. Encrypt/decrypt operations are performed on outgoing/incoming traffic based on firewall policies. 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 accordingly. Firewall policies with an action of allow mean that the firewall is accepting/sending plaintext data for the specified source/destination addresses.

The FortiGate implements an alternating bypass feature that is based on the firewall policies. A firewall policy with an action of accept means that the modules are operating in a bypass state for that policy. A firewall policy with an action of IPSec or SSL-VPN means that the modules are operating in a non-bypass state for that policy.

Two independent actions must be taken by an SA to create bypass firewall policies: the SA must create the bypass policy and then specifically enable that policy.

Key Archiving

The modules support 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. By default, the configuration file is stored in plain text, but keys in the configuration file are either AES encrypted with the configuration encryption key or stored as a SHA-1 hash. Note that while the modules also support encrypting the entire configuration file using AES, doing so is considered a non-FIPS Approved service.

Electromagnetic Interference/Electromagnetic Compatibility (EMI/EMC)

The module complies with EMI/EMC requirements for Class A (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 module.

Table 10: FCC Report Information

Module	Lab Information	FCC Report Number
FortiWiFi-50B	Bay Area Compliance Laboratory Corp (Shenzen) 6/F, Wanli Industrial Building, 3rd Phase Shihua Road, FuTian Free Trade Zone Shenzen, Guandong, China 86-755-33320018	RBJ07032151

Mitigation of Other Attacks

The FortiWiFi-50B module includes a real-time Network Intrusion Prevention System (NIPS) as well as antivirus protection, antispam and content filtering. Use of these capabilities is optional.

The FortiGate IPS has two components: a signature based component for detecting attacks passing through the FortiGate modules 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.

FortiGate 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. FortiGate 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.

FortiGate 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.

FortiGate web filtering can be configured to provide web (HTTP) content filtering. FortiGate 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.

The rest of this section provides additional information on the IPS, antivirus, antispam and web and email filtering capabilities of the FortiGate module and the FortiGuard Service. For complete information refer to the FortiGate Installation Guide for the specific module in question, the FortiGate Administration Guide, and the FortiGate IPS Guide.

This section contains the following information:

- Antispam Protection
- Web Filtering
- FortiGuard Services

IPS Signature Protection

The FortiGate IPS can detect a wide variety of suspicious network traffic and network-based attacks aimed at systems behind the FortiGate modules. Attack signatures are the core of the FortiGate IPS signature protection component. Signatures are transmission patterns and other codes that indicate that a system might be under attack. Functionally, signatures are similar to virus signatures, with each signature designed to detect a particular type of attack.

The FortiGate modules can be configured to automatically check for and download updated IPS packages from the FortiGuard servers, or they can be downloaded manually by the operator. Verification of the IPS download package is done using RSA. The IPS package is signed with the FortiGuard server's private key and verified by the FortiGuard module using the FortiGuard server's public key.

User defined attack signatures are also supported.

IPS Attack Protection

The FortiGate IPS can also protect the modules themselves from direct attacks, such as TCP, ICMP, UDP, and IP attacks. Access is denied or packets are dropped when an attack is detected. Attack parameters can be modified by the operator to ensure that normal network traffic is not considered an attack.

Antivirus Protection

FortiGate antivirus protection scans for infected files in the protocols for which antivirus protection as been enabled. Supported protocols include HTTP, FTP, SMTP, POP3, IMAP, and IM. If a file is found to contain a virus it is removed from the content stream and replaced with a replacement message.

FortiGate antivirus protection can also be configured to quarantine infected files. The quarantined files are stored on the module's hard disk. An operator can delete quarantined files from the hard disk or download them. Downloaded quarantine files can be submitted to Fortinet as virus samples for analysis. FortiGate antivirus protection is transparent to the end user.

The FortiGate modules can be configured to automatically check for and download updated AV packages from the FortiGuard servers, or they can be downloaded manually by the operator. Verification of the AV download package is done using RSA. The AV package is signed with the FortiGuard server's private key and verified by the FortiGuard module using the FortiGuard server's public key.

FortiGate antivirus protection also detects and removes grayware such as adware, spyware, etc.

Antispam Protection

FortiGuard antispam protection can detect spam in SMTP, POP3 or IMAP traffic. Spam email is tagged or discarded. Spam detection methods include banned words, black/white lists, return email DNS check and the FortiGuard antispam service. The FortiGuard Antispam Service provides IP checking, URI address checking and email checksum analysis.

To prevent unintentional tagging of email from legitimate senders, an operator can add sender address patterns to an exempt list that overrides the email block and banned word lists.

Web Filtering

FortiGate web filtering can be configured to scan HTTP protocol streams for banned URLs or web page content. Web filtering methods include banned words, URLs and the FortiGuard web filtering service. The FortiGuard web filtering service is a managed service that uses a database of URLs to block access to banned web sites and URLs based on content categories. If a match is found between a URL in the URL block list, the FortiGuard web filtering service, or if a web page is found to contain a word or phrase in the content block list, the FortiGate module blocks the web page. The blocked web page is replaced with a message that an operator can edit using the web-based manager.

An operator can configure URL blocking to block all or just some of the pages on a specific web site. This feature can be used to deny access to parts of a web site without denying access to it completely. To prevent unintentional blocking of legitimate web pages, an operator can add URLs to an Exempt List that overrides the URL blocking and content blocking.

Web content filtering also includes a script filter feature that can be configured to block insecure web content such as Java Applets, Cookies, and ActiveX.

FortiGuard Services

The FortiGuard services are a family of managed services available to Fortinet customers. The FortiGuard services include:

- IPS signature and engine updates
- AV signature and engine updates
- A managed antispam service
- A managed web filtering service
- Firmware updates

Customers can purchase FortiGuard services for their FortiGate modules on a yearly basis. Use of the FortiGuard services is optional, but recommended.

Communication between the FortiGate module and the FortiGuard servers is protected using TLS.

FIPS 140-2 Compliant Operation

To operate a FortiGate module in a FIPS compliant manner, organizations must follow the procedures explained in this section of the Security Policy.

This section contains the following information:

Overview of FIPS 140-2 compliant operation

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

- The FortiGate module is installed in a secure physical location.
- Physical access to the FortiGate module 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 FortiGate module is permitted using only validated administrative methods. These are:
  - Console connection
  - Web-based manager via HTTPS
  - Command line interface (CLI) access via SSH
- Web browsers are configured to use TLS 1.0 only for use with the SSL VPN functionality (SSL v3.0 support must be disabled in the browser).
- Diffie-Hellman key sizes of less than less than 1024 bits (Group 5) are not used.
- If the wireless interface is enabled:
  - WPA2 must be selected as the security mode (which forces the use of AES CCM as the encryption method).
  - The wireless preshared key must use the same password policy as described previously for administrative passwords.

The FortiGate 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.

Initial Inspection of the Modules

The SO must inspect a module before installation to verify that it has not been tampered with during shipment. The packaging and external enclosure must be inspected for visible signs of damage or tampering. If a module displays signs of damage or tampering, the SO must contact Fortinet to obtain a replacement module.

Applying the Security Seals

After completing the initial inspection of the module the SO must apply the security seals as explained in the section "Physical Security" on page 15 to ensure full compliance with the FIPS 140-2 standard.

Initial configuration of the FortiGate module

This section describes how to configure your FortiGate module in the FIPS-CC mode of operation. Proceed as follows:

- Install the module following the procedures in the documentation.
- Register your FortiGate module with Fortinet.
- If you are upgrading an existing FortiGate module to FIPS-CC firmware, download the appropriate firmware from Fortinet and install it on your module.
- Verify the firmware version of your FortiGate module.
- Enable FIPS-CC mode.

Verifying the hardware version of the module

Check the label on the back or underside of the module to determine the hardware version. Match the first 6 characters of the hardware version to the FIPS validated hardware versions listed in Table 11.

Table 11: FIPS 140-2 validated hardware versions

FortiGate Model	Hardware Version
FWF-50B	C5WF27

Installing the module

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

Registering the module

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

Downloading and installing FIPS-CC compliant firmware

Unless you purchased a FortiGate module with FIPS-CC firmware pre-installed, you need to download and install the appropriate firmware for your FortiGate module. The firmware can be obtained from the Fortinet support site after registering your module. The validated firmware build for the module is listed in Table 12.

Table 12: Firmware builds for validated FortiGate models

FortiGate Model	Firmware Build
FWF-50B	FWF_50B-v300-build8802-mr4_fips_cc_lr.out

To download the firmware

1. Determine the appropriate firmware build from Table 12.
2. With your web browser, go to https://support.fortinet.com and log in using the name and password you received when you registered with Fortinet Support.
3. Navigate to the version 3.00 FortiOS Images and Notes page. Select Download Page for the FIPS-CC compliant firmware build you need. Save the file on the management computer or on your network where it is accessible from the FortiGate module.

Installing the FIPS-CC firmware

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

To install the FIPS-CC firmware

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

   When the module attempts to load the new firmware build, the firmware load test is performed and verifies the integrity of the new firmware using a digital signature. If the load test fails, the firmware update is rejected and the message "File is not an update file" is displayed. If the firmware load test passes, the module uploads the new firmware image file, upgrades to the new firmware version, restarts, and displays the Login page. This process takes a few minutes.

Verifying the firmware version of the module

Execute the following command from the command line:

```
get system status
```

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

```
Version: FortiWiFi-50B 3.00,build8802,080626
```

Verify that your firmware version, build number and date match those shown above for your specific model.

Enabling FIPS-CC mode

If you have verified the firmware version, you are ready to enable FIPS-CC mode. As part of enabling FIPS-CC mode, you must define administrator account names and passwords. The default admin account is not available in FIPS-CC mode. You must use a console connection to enable FIPS-CC mode. If you try to use another type of connection, a “check permission failed” occurs.

Note: When you enable FIPS-CC mode, all of the existing configuration is lost.

To enable FIPS-CC mode

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

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

2. In response to the following prompt, enter the account name for the Security Administrator:

```
Please enter SECURITY administrator name:
```

3. In response to the following prompt, enter the password for the Security Administrator:

```
Please enter SECURITY administrator password:
```

4. When prompted, re-enter the Security Administrator password.
5. In response to the following prompt, enter the account name for the Audit Administrator:

```
Please enter AUDIT administrator name:
```

If you want the Security Administrator to also act as the Audit Administrator, enter the Security Administrator account name you defined in step 2. There will be no prompt for a password. (Skip step 6.)

6. In response to the following prompt, enter the password for the Audit Administrator:

```
Please enter AUDIT administrator password:
```

7. When prompted, re-enter the Audit Administrator password.
8. In response to the following prompt, enter the account name for the Crypto Administrator:

```
Please enter CRYPTO administrator name:CryptoAdmin
```

If you want the Security Administrator to also act as the Crypto Administrator, enter the Security Administrator account name you defined in step 2. There will be no prompt for a password. (Skip step 9.)

9. In response to the following prompt, enter the password for the Cryptographic Administrator:

```
Please enter CRYPTO administrator password:
```

10 When prompted, re-enter the Crypto Administrator password.

The CLI displays the following message:

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

11 Enter y.

The FortiGate module restarts and runs in FIPS-CC compliant mode.

FIPS-CC mode status indicators

There is one status indicator that shows whether the FortiGate module is running in the FIPS 140-2 and Common Criteria compliant mode of operation:

Table 13: FIPS-CC mode status indicators

Location	Indication
Output of `get system status` command	FIPS-CC mode: enable

Self-Tests

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

- Firmware integrity test using HMAC SHA-1
- VPN bypass test using HMAC SHA-1 (VPN table integrity test)
- Triple-DES, CBC mode, encrypt/decrypt known answer test
- AES, CBC mode, encrypt/decrypt known answer test
- AES-CCM, using AES ECB mode, encrypt/decrypt known answer test
- HMAC SHA-1 known answer test
- RSA signature generation/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).

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

- Continuous RNG test
- RSA pairwise consistency test
- VPN bypass test using HMAC SHA-1 (VPN table integrity test)
- Firmware download integrity test using RSA public/private keys

Self-Test Status Indicators

There are two types of self-test status indicators: the startup indicators and the on-demand indicators. The startup self-test status indicators are output through the console connection during the startup process. The on-demand self-test status indicators are output as a the result of a **execute fips kat <test>** CLI command.

The following output shows the successful completion of the startup self-tests:

```
Initializing firewall...
System is started.

FIPS-CC mode: Starting self-tests.
Running AES test...                              passed
Running 3DES test...                             passed
Running SHA1 HMAC test...                        passed
Running RSA test...                              passed
Running Firmware/VPN config integrity test... passed
Running RNG test...                              passed
Self-tests passed
```

The following output shows the successful completion of the on-demand self-tests for all of the algorithm known answer tests:

```
FortiWiFi-50B # execute fips kat all
Starting self-tests
Running AES test...       passed
Running 3DES test...      passed
Running SHA1 HMAC test... passed
Running RSA test...       passed
Running RNG test...       passed
Self-tests passed
```

Effects of FIPS-CC compliant mode

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

- All previous configuration settings are lost (cleared or reset to defaults) except for the SA, AA and CA accounts created when enabling FIPS-CC mode.
- All network interfaces are down by default.
- The `get system status` CLI command display includes “FIPS-CC mode: enable”.
- Memory logging is enabled by default (including traffic logs).
- Reaching 95% of the log storage capacity results in the FortiGate module entering a CC Error mode that shuts down all of the interfaces until the administrator intervenes. See “CC Error Mode” on page 30.
- Failure of a self-test results in the FortiGate module entering a FIPS Error mode that halts the module until the administrator intervenes. See “FIPS Error Mode” on page 29.
- Anomaly detection and protection is applied to traffic addressed to the FortiGate module.
- TFTP communication is not permitted.
- SNMP services are disabled.
- Remote access clients must meet security requirements. See “Remote access requirements” on page 28.
- All administrators must accept a disclaimer statement at logon. This disclaimer is configured in the Post Login replacement message.

- The FortiGate module performs self-tests at startup. Also, the administrator can run some self-tests at any time. If any of these tests fail, the module goes into error mode and shuts down.
- There is an alarm capability.
- The DES and MD5 algorithms are not available for VPN configurations.
- Use of the AES or Triple-DES algorithms is enforced for IPSec and SSL VPN configurations.
- The use of TLS is enforced for remote administration over HTTPS.
- Support for large Diffie-Hellman groups 14 through 18 is added to IPSec VPN configurations and group 15 is the default. DH groups 15 through 18 use 3072 to 8192-bit keys.
- ANSI X9.31 RSA signature is an optional authentication method for IPSec VPNs. This method is supported only on FortiGate modules in FIPS-CC mode.
- When configuring passwords, the FortiGate module requires you to enter the password a second time as confirmation.
- Blocking of spoofed TCP RST packets is enabled by default.
- On a CLI session, when an administrator logs out or the session times out, the FortiGate module sends 100 carriage return characters to clear the screen.
- WEP and WPA are not available for wireless configurations.

Remote access requirements

In FIPS-CC mode, remote administration is not allowed via HTTP or Telnet, which are not secure. SSH and HTTPS access are permitted but must meet certain security requirements.

Setting minimum DH primes size

By default, in FIPS-CC mode the FortiGate module requires values at least 3072 bits long to be used in the Diffie-Hellman key exchange when an HTTPS session begins. Using the CLI, you can set this minimum to one of the following safe standard values specified in RFC 3526: 1024, 1536, 2048, 3072, 4096, 6144 or 8192 bits. For example, to use commercially available browsers, you might need to set the key size to 1024, as follows:

```
config system global
    set dh-params 1024
  end
```

SSH client requirements

To access the CLI through network interfaces in FIPS-CC mode, your SSH client must support the following:

Authentication:

- HMAC SHA-1

Encryption:

- AES128, AES192, AES256 or Triple-DES

Note that only SSH v2 is supported.

Web browser requirements

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

- Authentication algorithm (one of the following, in descending order of preference):
  - RSA X9.31
  - PKCS1 RSA
- Connection security:
  - TLS 1.0

Enabling administrative access

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

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

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

Disabling FIPS-CC mode

The only way that you can return the FortiGate module to the normal mode of operation is to restore the factory default configuration. Enter the following CLI command:

```
execute factoryreset
```

Disabling FIPS-CC mode erases the current configuration.

Error mode

In FIPS-CC mode, there are two specific error modes: FIPS Error mode and CC Error mode.

FIPS Error Mode

The FortiGate module switches to FIPS Error mode when one or more of the self-tests fail. On entering FIPS Error mode the FortiGate module shuts down all interfaces (including the console) and blocks traffic.

The module indicates FIPS Error mode by outputting an error message to the console. For example, if the startup AES self-test fails, the following error message would be displayed on the console:

```
FIPS error: AES self-test failed
Entering error mode...
```

```
The system is going down NOW !!


The system is halted.
```

To resume normal FIPS-CC mode operation, first attempt a reboot of the FortiGate module by power cycling the module. If the self-tests pass after the reboot, the module will resume normal FIPS-CC compliant operation. If a self-test continues to fail after rebooting, there is likely a serious firmware or hardware problem and the module should be removed from the network until the problem is solved.

If the self-test failure persists across reboots, you can attempt to reload the firmware after resetting the module to the factory default configuration. If the self-test failure persists after reloading the firmware and re-enabling the FIPS-CC mode of operation, contact Fortinet technical support.

CC Error Mode

The FortiGate module switches to CC Error mode when the current and rolled log files consume more than 95% (the default setting) of log device capacity. On entering CC Error mode the FortiGate module shuts down the network interfaces and blocks traffic. Administrator access is restricted to the console when the module is in CC Error mode.

The FortiGate module indicates CC Error mode by prepending “CC-ERR” to the console prompt:

```
CC-ERR FortWifi-50B$
```

To resume normal FIPS-CC mode operation, you must first reduce the logs to below 95% of the disk capacity. Only an Administrator with the Audit Administrator role can do this. Ideally you should reduce the logs to 50% or less of the device capacity.

Once you have cleared space on the log device, use the following console command to clear error mode:

```
execute error-mode exit
```

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

Non-FIPS Approved Services

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

- Encrypted configuration backups using the backup configuration password
- High Availability (HA) in both Active-Active (AA) and Active-Passive (AP) configurations

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