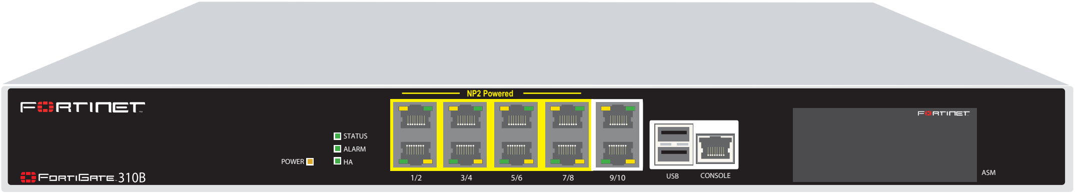
FIPS 140-2 Security Policy

FortiOS v4.0



FortiOS v4.0 FIPS 140-2 Security Policy	
Document Version:	1.0
Publication Date:	August 30, 2010
Description:	Documents FIPS 140-2 Level 1 Security Policy issues, compliancy and requirements for FIPS compliant operation.
Firmware Version:	FortiOS 4.0, build6341, 100617

www.fortinet.com

FortiOS v4.0 FIPS 140-2 Security Policy
v1.0

August 30, 2010

01-400-123278-20100413

Trademarks

Contents

This document is a FIPS 140-2 Security Policy for Fortinet Incorporated’s FortiOS 4.0 firmware, which runs on the FortiGate/FortiWiFi family of security appliances. This policy describes how the FortiOS 4.0 firmware (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 1 FIPS 140-2 validation of the module.

This document contains the following sections:

- Introduction
- Security Level Summary
- Module Description
- Mitigation of Other Attacks
- FIPS 140-2 Compliant Operation
- Self-Tests
- Non-FIPS Approved Services

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.

Security Level Summary

The module meets the overall requirements for a FIPS 140-2 Level 1 certification.

Table 1: Summary of FIPS security requirements and compliance levels

Security Requirement	**Compliance Level**
Cryptographic Module Specification	1
Cryptographic Module Ports and Interfaces	3
Roles, Services and Authentication	3
Finite State Model	1
Physical Security	1
Operational Environment	N/A
Cryptographic Key Management	1
EMI/EMC	1
Self-Tests	1
Design Assurance	3
Mitigation of Other Attacks	1

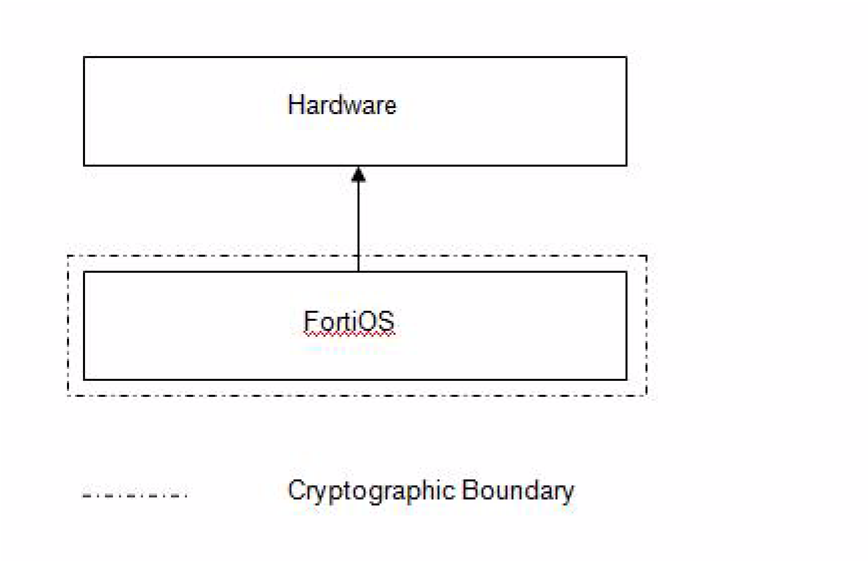
Module Description

The module is a firmware operating system that runs exclusively on Fortinet’s FortiGate/FortiWiFi product family (hereafter referred to as the FortiGate product family). FortiGate units are PC-based, purpose built appliances.

The module 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.

Figure 1: FortiOS Cryptographic Boundary



Module Interfaces

The module’s logical interfaces and physical ports are described in Table 2.

Table 2: FortiOS logical interfaces and physical ports

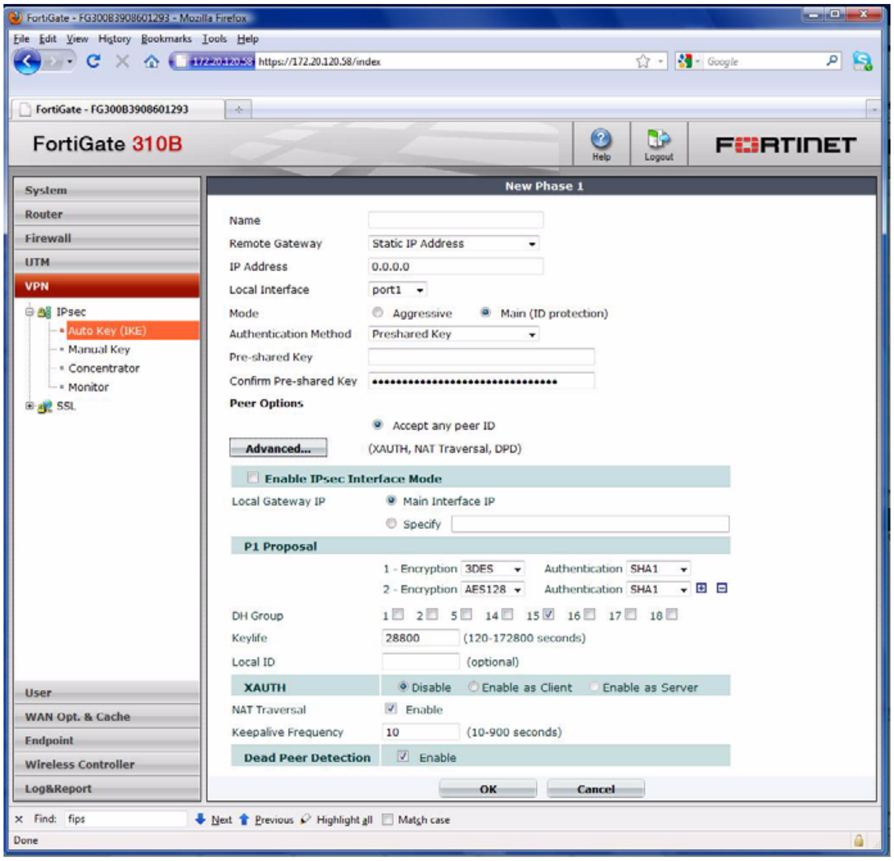
FIPS 140 Interface	Logical Interface	Physical Port
Data Input	API input parameters	Network interface
Data Output	API output parameters	Network interface
Control Input	API function calls	Network interface, serial interface
Status Output	API return values	Network interface, serial interface
Power Input	N/A	The power supply is the power interface

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 2: The FortiGate web-based manager



New Phase 1

Name
Remote Gateway: Static IP Address
IP Address: 0.0.0.0
Local Interface: port1
Mode: ○ Aggressive ● Main (ID protection)
Authentication Method: Preshared Key
Pre-shared Key
Confirm Pre-shared Key: ••••••••••••••••••••••••••••••

Peer Options
● Accept any peer ID
(XAUTH, NAT Traversal, DPD)

□ Enable IPsec Interface Mode
Local Gateway IP: ● Main Interface IP ○ Specify

P1 Proposal
1 - Encryption 3DES Authentication SHA1
2 - Encryption AES128 Authentication SHA1
DH Group: 1 □ 2 □ 5 □ 14 □ 15 ☑ 16 □ 17 □ 18 □
Keylife: 28800 (120-172800 seconds)
Local ID: (optional)
XAUTH: ● Disable ○ Enable as Client ○ Enable as Server
NAT Traversal: ☑ Enable
Keepalive Frequency: 10 (10-900 seconds)
Dead Peer Detection: ☑ Enable

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).

Roles, Services and Authentication

Roles

When configured in FIPS-CC mode, the module provides 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 module 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 module, including resetting or shutting down the module. 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 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.

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

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:

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 3: Services available to Crypto Officers

Service	SA	CA	AA	Key/CSP
authenticate to module	WE	WE	WE	Operator Password, Diffie-Hellman Key, Server/Host Key, HTTPS/TLS Session Authentication Key, HTTPS/TLS Session Encryption Key, RNG Keys
show system status	WE	N/A	N/A	N/A
show FIPS-CC mode enabled/disabled (console/CLI only)	WE	N/A	N/A	N/A
enable FIPS-CC mode of operation (console only)	WE	N/A	N/A	Configuration Integrity Key
execute factory reset (zeroize keys, disable FIPS mode, console/CLI only)	E	N/A	N/A	See “Key Zeroization” on page 11
execute FIPS-CC on-demand self-tests (console only)	E	E	E	Configuration Integrity Key, Firmware Integrity Key
add/delete operators and network users	WE	N/A	N/A	N/A
set/reset operator and network user passwords	WE	N/A	N/A	Operator Password, Network User Password
backup configuration file	WE	N/A	N/A	See “Key Archiving” on page 13
read/set/delete/modify module configuration	WE	N/A	N/A	N/A
enable/disable alternating bypass mode	WE	N/A	N/A	N/A
read/set/delete/modify IPSec/SSL VPN configuration	N/A	WE	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 Session Encryption Key
read/set/delete/modify HA configuration	WE	N/A	N/A	HA Password, HA Encryption Key
execute firmware update	E	N/A	N/A	Firmware Update Key
read log data	WE	WE	WE	N/A
delete log data (console/CLI only)	N/A	N/A	WE	N/A
execute system diagnostics (console/CLI only)	WE	WE	WE	N/A

Table 4: Services available to Network Users

Service/CSP	NU	Key/CSP
authenticate to module	E	Network User Password, Diffie-Hellman Key, 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, Server/Host Key, HTTPS/TLS Session Authentication Key, HTTPS/TLS Session Encryption Key, RNG Keys

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.

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). 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 96^8.

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 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 physical security for the module is provided by the FortiGate hardware which uses production grade components and an opaque enclosure.

Operational Environment

The module constitutes the entire firmware operating system for a FortiGate unit and can only be installed and run on a FortiGate appliance. The module provides a proprietary and non-modifiable operating system and does not provide a programming environment.

For the purposes of FIPS 140-2 conformance testing, the module was tested on the following FortiGate/FortiWiFi appliances:

- FortiGate-80C
- FortiGate-200B
- FortiGate-310B
- FortiGate-620B
- FortiGate-800
- FortiGate-1240B
- FortiGate-3016B
- FortiGate-3600A
- FortiGate-3810A-E4
- FortiGate-5001A-DW

The module can also be executed on any of the following FortiGate appliances, or any other FortiGate appliance running the same processors as the appliances listed above, and remain vendor affirmed FIPS-compliant:

- FortiGate-80CM
- FortiGate-100A
- FortiGate-110C
- FortiGate-111C
- FortiGate-224B
- FortiGate-200A
- FortiGate-300A
- FortiGate-311B
- FortiGate-621B
- FortiGate-800F
- FortiGate-3000
- FortiGate-3600
- FortiGate-1000A
- FortiGate-1000AFA2
- FortiGate-5001SX
- FortiGate-5001A-SW
- FortiGate-5001FA2
- FortiGate-5005FA2
- FortiWiFi-80CM
- FortiWiFi-81CM

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.

Key Zeroization

The following keys are zeroized by executing a factory reset followed by a firmware update.

- ANSI X9.31 RNG AES Key
- Firmware Update Key
- Firmware Integrity Key
- Configuration Integrity Key
- Configuration Backup Key

All other keys and CSPs are zeroized when the operator executes a factory reset or when enabling or disabling the FIPS-CC mode of operation.

See Table 7 on page 12 for a complete list of keys and CSPs.

Algorithms

Table 5: FIPS Approved or Allowed Algorithms

Algorithm	NIST Certificate Number
RNG (ANSI X9.31 Appendix A)	770
Triple-DES	957, 962
AES	1404, 1409
SHA-1	1274, 1279
HMAC SHA-1	825, 830
RSA ANSI X9.31 (key generation, signature generation and verification)	686
RSA PKCS1 (digital signature creation and verification)	686

Table 6: 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)
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 PKCS1 (key wrapping; key establishment method provides between 80 and 112 bits of encryption strength - 1024 to 2048 bit certificates are supported)
SHA-256
HMAC SHA-256

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 7: Cryptographic Keys and Critical Parameters used in FIPS 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)	SDRAM 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 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

Table 7: Cryptographic Keys and Critical Parameters used in FIPS Mode

Key or CSP	Storage	Usage
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
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. 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 module implements an alternating bypass feature that is based on the firewall policies. 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.

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 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.

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).

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-CC mode of operation:

1 Log in to the FortiGate unit using the console connection and the default administrator account.

2 Enable the FIPS-CC mode of operation and when prompted enter an administrator account name and password for each of the administrator roles (Security Administrator, Crypto Administrator and Audit Administrator).

3 Verify FIPS-CC mode is enabled after the unit reboots by checking the results of the `get system status` CLI command.

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/decrypt known answer test
- AES, CBC 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

- Configuration/VPN bypass test using HMAC SHA-1
- Firmware load test using RSA signatures

Non-FIPS Approved Services

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

- Encrypted configuration backups using the backup configuration password
- 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.