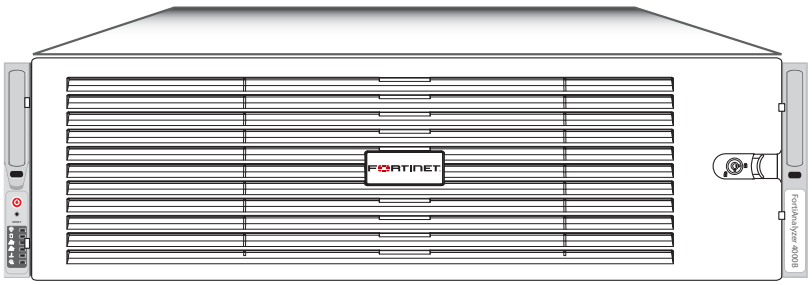
FIPS 140-2 Security Policy

FortiAnalyzer-4000B



FortiAnalyzer-4000B FIPS 140-2 Security Policy	
Document Version:	2.7
Publication Date:	March 6, 2014
Description:	Documents FIPS 140-2 Level 2 Security Policy issues, compliancy and requirements for FIPS compliant operation.
Hardware Model:	C4EQ87
Firmware Version:	FortiAnalyzer v4.0,build3059,130918

FortiAnalyzer-4000B FIPS 140-2 Security Policy

05-430-143702 -201100502

for FortiAnalyzer 4.0 MR3

© Copyright 2014 Fortinet, Inc.

This document may be freely reproduced and distributed whole and intact including this copyright notice.

Trademarks

Dynamic Threat Prevention System (DTPS), APSecure, FortiASIC, FortiBIOS, FortiBridge, FortiClient, FortiGate®, FortiGate Unified Threat Management System, FortiGuard®, FortiGuard-Antispam, FortiGuard-Antivirus, FortiGuard-Intrusion, FortiGuard-Web, FortiLog, FortiAnalyzer, FortiManager, Fortinet®, FortiAnalyzer, FortiPartner, FortiProtect, FortiReporter, FortiResponse, FortiShield, FortiVoIP, and FortiWiFi are trademarks of Fortinet, Inc. in the United States and/or other countries. The names of actual companies and products mentioned herein may be the trademarks of their respective owners.

Contents

Overview

This document is a FIPS 140-2 Security Policy for Fortinet Incorporated's FortiAnalyzer-4000B Centralized Reporting appliance. This policy describes how the FortiAnalyzer-4000B (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 FIPS 140-2 Level 2 validation of the module.

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 FortiAnalyzer 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 FortiAnalyzer 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 FortiAnalyzer family of logging, analyzing, and reporting appliances securely aggregate log data from Fortinet devices and other syslog-compatible devices. Using a comprehensive suite of customizable reports, users can filter and review records, including traffic, event, virus, attack, Web content, and email data.

A typical deployment architecture for a FortiAnalyzer appliance is shown in Figure 1.

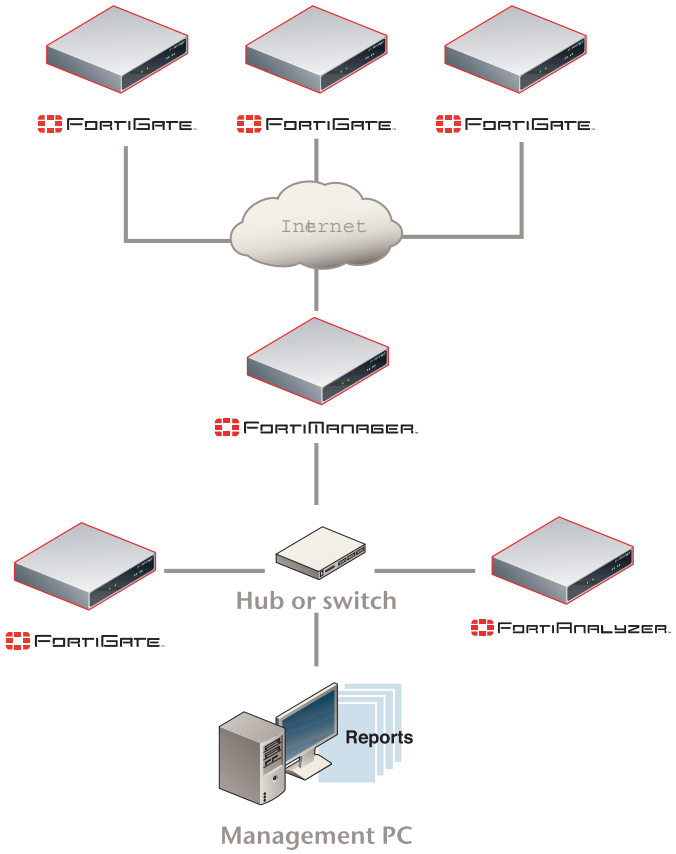


Figure 1: A typical FortiAnalyzer deployment architecture

Security Level Summary

The module meets 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	2
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	N/A

Module Description

The FortiAnalyzer-4000B is a 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 module has 4network interfaces with a status LED for each network interface (2 10/100/1000 Base-T, 2 SFP).

The module has 2 quad core, x86 compatible CPUs.

The module is a 4u rackmount device.

The module has 3 internal and 4 external ventilation fans.

The evaluated configuration of the module includes 6 1TB hard disk drives. The module supports up to 24 hard disk drives.

The module includes several components that are not supported by the FortiAnalyzer firmware and are excluded from the evaluated configuration:

- VGA port
- Keyboard port
- Mouse port

The validated firmware version is FortiAnalyzer 4.0, build3059, 130918.

Cryptographic Module Ports and Interfaces

FortiAnalyzer-4000B Module

Figure 2: FortiAnalyzer-4000B Front and Rear Panels

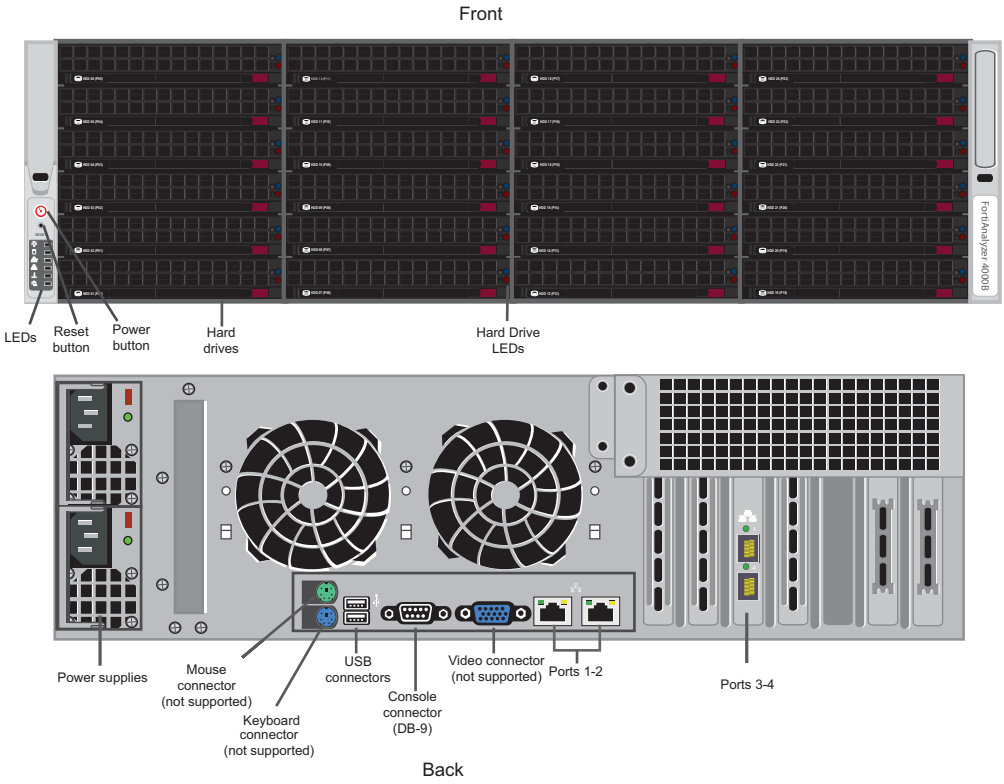


Table 2: FortiAnalyzer-4000B Status LEDs

LED		State	Description
Power		Green	The module is powered on.
		Off	The module is powered off.
Ports 1 to 2	Link	Green	Port is connected at 1000 Mbps.
		Amber	Port is connected at 10/100 Mbps.
		Off	Port is disconnected or down.
	Activity	Blinking	Port is receiving or sending data.
		Off	Port may be on, but is not receiving or sending data.
Ports 3 to 4		Green	Port is online.
		Off	Port is disconnected or down.
Hard Disk	Activity	Blinking	Disk read/write activity.
		Off	No disk activity.
	Status	Green	Drive online.
		Green, blinking slowly	Drive rebuilding RAID.
		Amber, blinking 4x/sec	Drive failure.
		Amber, blinking 2x/sec	Identify drive, prepare for removal.
		Blinking, green, amber, off	Drive failure predicted.
		Off	Drive ready for removal.
AC Power		Green	AC power is connected and has power.
		Amber	Power supply problem.
		Blinking, green, amber	Power supply mismatch with 2nd power supply.
		Off	AC power is not connected.

Table 3: FortiAnalyzer-4000B Rear Panel Connectors and Ports

Connector	Type	Speed	Supported Logical Interfaces	Description
Ports 1 to 2	RJ-45	10/100/1000 BaseT	Data input, data output, control input and status output	Multimode fiber optic connections to gigabit optical networks.
Ports 3 to 4	SFP	1Gbps	Data input, data output, control input and status output	Copper gigabit connection to 10/100/1000 copper networks.
CONSOLE	DB-9	9600 bps	Control input, status output	Optional connection to the management computer. Provides access to the command line interface (CLI).
VGA	DB-15	N/A	N/A	Not supported.
Keyboard	PS/2	N/A	N/A	Not supported.
Mouse	PS/2	N/A	N/A	Not supported.
USB	USB	N/A	Key loading and archiving, configuration backup and restore	Optional connection for USB token.
POWER	N/A	N/A	Power	120/240VAC power connection.

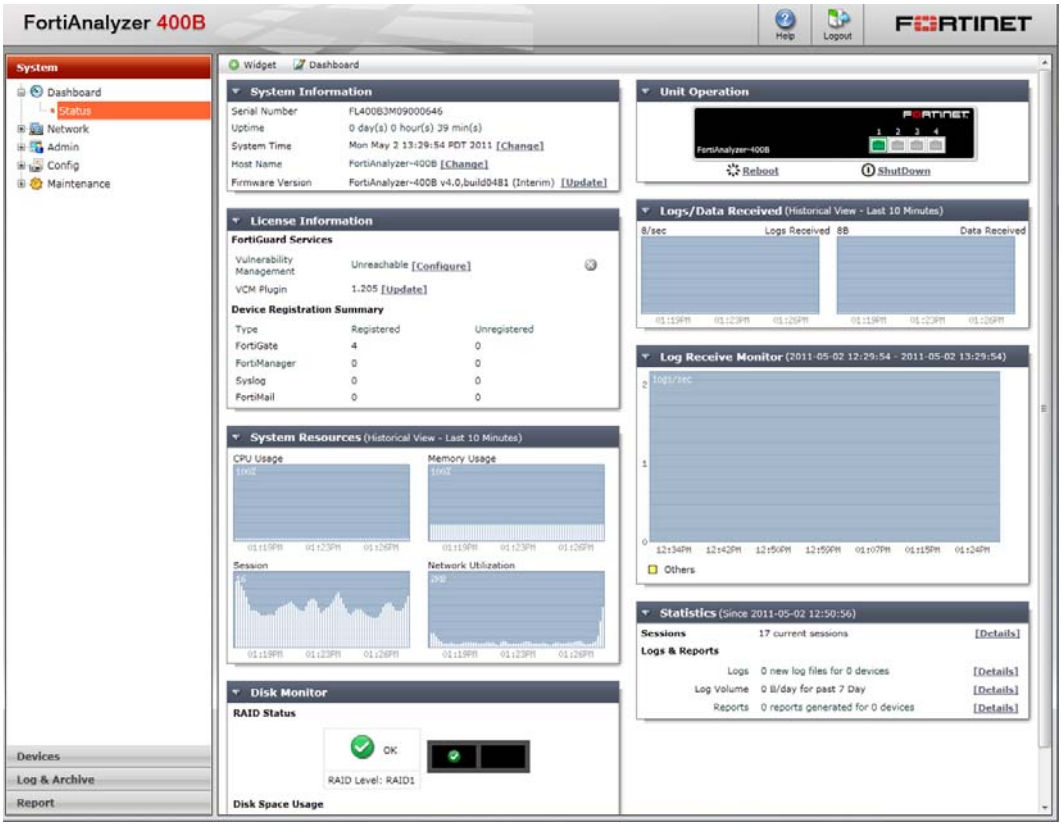
Web-Based Manager

The FortiAnalyzer 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 FortiAnalyzer 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 mode. HTTP access to the web-based manager is not allowed in FIPS mode and is disabled.

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

Figure 3: The FortiAnalyzer web-based manager



Command Line Interface

The FortiAnalyzer 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 FortiAnalyzer 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 mode).

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

Roles, Services and Authentication

Roles

When configured in FIPS mode, the module provides a Crypto Officer role and a Network User role.

The Crypto Officer role is initially assigned to the default ‘admin’ operator account. The Crypto Officer role has read-write access to the module’s administrative services. Crypto Officer access to the services can be customized using access profiles. A Crypto Officer with sufficient permissions can create or modify access profiles to limit access to the administrative services. When operator accounts are created, the Crypto Officer specifies an access profile for that operator.

The module provides a **Network User** role for remote IT entities. Network users can make use of the encrypt/decrypt services for the purpose of transferring log/content data to the module, 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 CSPs they affect.

The role names are abbreviated as follows:

Crypto Officer	CO
Network User	NU

The access types are abbreviated as follows:

Read Access	R
Write Access	W
Execute Access	E

Table 4: Services available to Crypto Officers

Service	Access	Key/CSP
authenticate to module	WE	Operator Password, Operator Public Key, Diffie-Hellman Key, Server/Host Key, HTTPS/TLS Keys, SSH Keys, RNG Seed and RNG AES Key
show system status	N/A	N/A
show FIPS mode enabled/disabled (console only)	N/A	N/A
enable FIPS mode of operation (console only)	WE	N/A
execute factory reset (zeroize keys, disable FIPS mode)	WE	See “Key Zeroization” on page 11
execute FIPS on-demand self-tests (console only)	N/A	Configuration Integrity Key, Firmware Integrity Key
add/delete operators and network users	RWE	Operator Password, Network User Password
set/reset operator and network user passwords	WE	Operator Password, Network User Password

Table 4: Services available to Crypto Officers

Service	Access	Key/CSP
backup configuration file	WE	Configuration Backup Key, Configuration Encryption Key, all keys stored in configuration file
read/set/delete/modify module configuration	N/A	N/A
read/set/delete/modify IPSec VPN configuration	RWE	IKE Pre-Shared Key
enable/disable alternating bypass mode	N/A	N/A
execute firmware update	WE	Firmware Update Public Key
read log data	R	N/A
delete log data	WE	N/A
execute a report	RE	N/A
execute remote system scan	E	N/A

Table 5: Services available to Network Users

Service/CSP	Access	Key/CSP
IPSec VPN log/content data transfer	E	Diffie-Hellman Key, IKE and IPSec Keys, RNG Seed and RNG AES Key
SSL VPN log/content data transfer	E	Diffie-Hellman Key, Server/Host Key, HTTPS/TLS Keys, RNG Seed and RNG AES Key

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. The password entry feedback mechanism does not provide information that could be used to guess or determine the authentication data.

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 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 15.

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 red wax/plastic with white lettering that reads “Fortinet Inc. Security Seal”. The seals are serialized.

The tamper seals are not applied at the factory prior to shipping. It is the responsibility of the Security Administrator to apply the seals before use to ensure full FIPS 140-2 compliance. Once the seals have been applied, the Security Administrator 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 Security Administrator 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. The seals require a curing time of 24 hours to ensure proper adhesion.

Additional seals can be ordered through your Fortinet sales contact. Reference the SKU FIPS-SEAL-RED when ordering and specify the number of seals required.

The FortiAnalyzer-4000B uses 5 seals to secure:

- the top panel (one seal, see Figure 4)
- the front cover plate (one seal, see Figure 4)
- the power supplies (two seals, see Figure 5)
- the rear access panel (one seal, see Figure 5)

Figure 4: FortiAnalyzer-4000B top panel and front faceplate seals, top

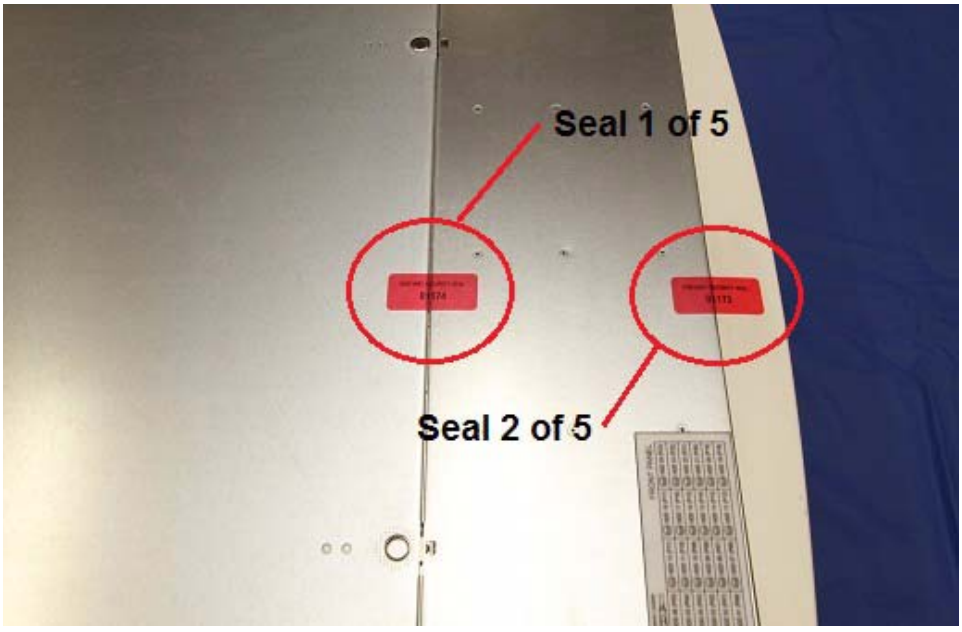
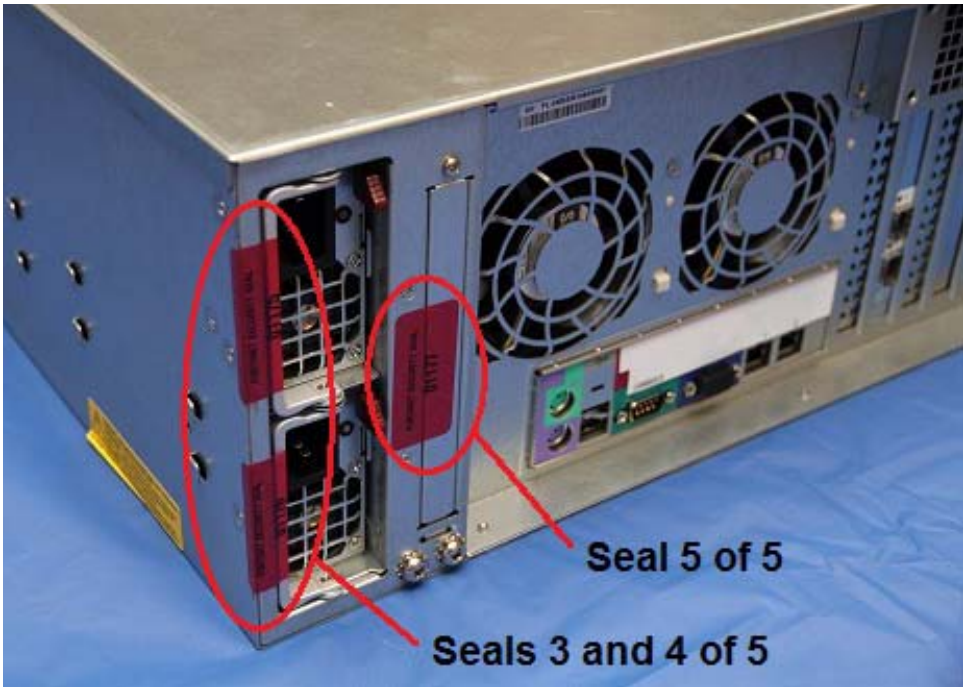


Figure 5: FortiAnalyzer-4000B rear access panel and power supply seals, rear



Operational Environment

The module consists of the combination of the FortiAnalyzer operating system and the FortiAnalyzer appliance. The FortiAnalyzer operating system can only be installed, and run, on a FortiAnalyzer appliance. The FortiAnalyzer 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 6: FIPS Approved Algorithms

Algorithm	NIST Certificate Number
RNG (ANSI X9.31 Appendix A)	1251
Triple-DES	1608, 1609
AES	2681
SHA-1	2251, 2252
SHA-256	2251, 2252
HMAC SHA-1	1667, 1668
HMAC SHA-256	1667, 1668
RSA PKCS1 (digital signature verification)	1030

Table 7: FIPS Allowed Algorithms

Algorithm
RSA (key wrapping; key establishment methodology provides 112 bits of encryption strength; non-compliant less than 112 bits of encryption strength)
NDRNG

Table 8: Non-FIPS Approved Algorithms

Algorithm
DES (disabled in FIPS mode)
MD5 (disabled in FIPS mode except for use in the TLS protocol)
HMAC MD5 (disabled in FIPS mode)
Diffie-Hellman (non-compliant)

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.

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: Cryptographic Keys and Critical Security Parameters Used in FIPS Mode

Key or CSP	Storage	Description/Usage
Diffie-Hellman Key	SDRAM Plaintext	Key agreement and key establishment
IPSec Session Authentication Key	SDRAM Plain-text	IPSec peer-to-peer authentication using HMAC SHA-1 or HMAC SHA-256
IPSec Session Encryption Key	SDRAM Plain-text	VPN traffic encryption/decryption using Triple-DES
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
IKE Encryption Key	SDRAM Plain-text	Encryption of IKE peer-to-peer key negotiation using Triple-DES
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 (signature verification)
Firmware Integrity Key	Flash RAM Plain-text	Verification of firmware integrity in the firmware integrity test using RSA public key (signature verification)
HTTPS/TLS Server/Host Key	Flash RAM Plain-text	RSA private key used in the HTTPS/TLS protocols (key establishment)

Table 9: Cryptographic Keys and Critical Security Parameters Used in FIPS Mode

Key or CSP	Storage	Description/Usage
HTTPS/TLS Session Authentication Key	SDRAM Plain-text	HMAC SHA-1 or or HMAC SHA-256 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 (key establishment)
SSH Session Authentication Key	SDRAM Plain-text	HMAC SHA-1 or or HMAC SHA-256 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-256 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
Operator Password	Flash RAM SHA-1 hash	Used during operator authentication
Operator Public Key	Flash RAM, Plain-text	RSA public key used for operator authentication (signature verification)

Alternating Bypass Feature

The primary function of the module is as a log and content aggregation device. Remote devices send log/content data to the FortiAnalyzer unit. Encrypt/decrypt operations are performed on incoming/outgoing traffic based on the configuration. Remote devices can be configured to send log/content data over a plain-text connection, an encrypted IPSec tunnel or an SSL encrypted connection using TLS 1.0.

A remote device configured to send log/content data using an IPSec tunnel or SSL connection means that the module is operating in a non-bypass state for communications with the device. A remote device configured to send log/content data using a plain-text connection means that the module is operating in a bypass state for communications with the device.

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 (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
FAZ-4000B	Bay Area Compliance Laboratories Corp. 1274 Anvilwood Ave. Sunnyvale, CA, 94089 Tel (408) 732-9162 Fax (408) 732-9164	R1006282A

Mitigation of Other Attacks

The module does not mitigate against any other attacks.

FIPS 140-2 Compliant Operation

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

- The FIPS mode of operation is enabled
- The FortiAnalyzer unit is installed in a secure physical location.
- Physical access to the FortiAnalyzer 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 must be capitalized
  - One (or more) of the characters must be numeric
  - One (or more) of the characters must 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 (TLS v1.0)
  - Command line interface (CLI) access via SSH (v2.0)
- Only approved and allowed algorithms are used (see “Algorithms” on page 12).
- The tamper evident seals are applied (see “Physical Security” on page 9).

Enabling FIPS mode

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

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

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 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 mode by executing the following command from the CLI:

```
get system status
```

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

```
FIPS mode: enabled
```

Note that enabling/disabling the FIPS mode of operation will automatically invoke the key zeroization service. The key zeroization is performed immediately after FIPS 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 integrity test using HMAC SHA-
- Firmware load test using RSA signatures

If any of the self-tests or conditional tests fail, the module enters a FIPS error mode. For example, if the AES self-test fails, the following would be displayed on the console:

```
Entering FIPS Error Mode because of the following issues:
1. SELF_TEST_AES_Failed

You must power cycle the unit to recover.

The system is going down NOW !!
Pasuing log daemons...
Stopping RAID ...

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 service:

- Configuration backups using password protection

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