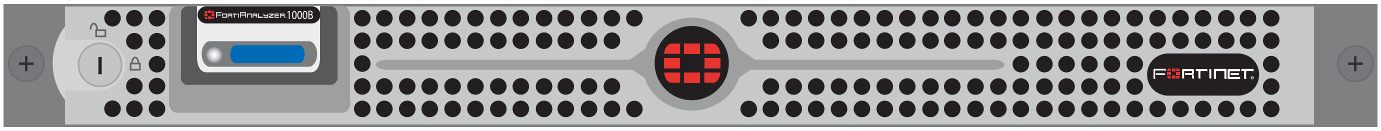
FortiAnalyzer

v4.0.0



FortiAnalyzer v4.0.0 FIPS 140-2 Security Policy	
Document Version:	2.1
Publication Date:	August 26, 2010
Description:	Documents FIPS 140-2 Security Policy issues, compliancy and requirements for FIPS compliant operation.
Firmware Version:	v4.0.0,build6087,091105

FortiAnalyzer v4.0.0 FIPS 140-2 Security Policy
v2.1

August 26, 2010

05-400-96351-20090812

Trademarks

Contents

This document is a FIPS 140-2 Security Policy for Fortinet Incorporated's FortiAnalyzer v4.0.0 firmware for the FortiAnalyzer line of security appliances. This policy describes how the FortiAnalyzer v4.0.0 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 FIPS 140-2 Level 1 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.

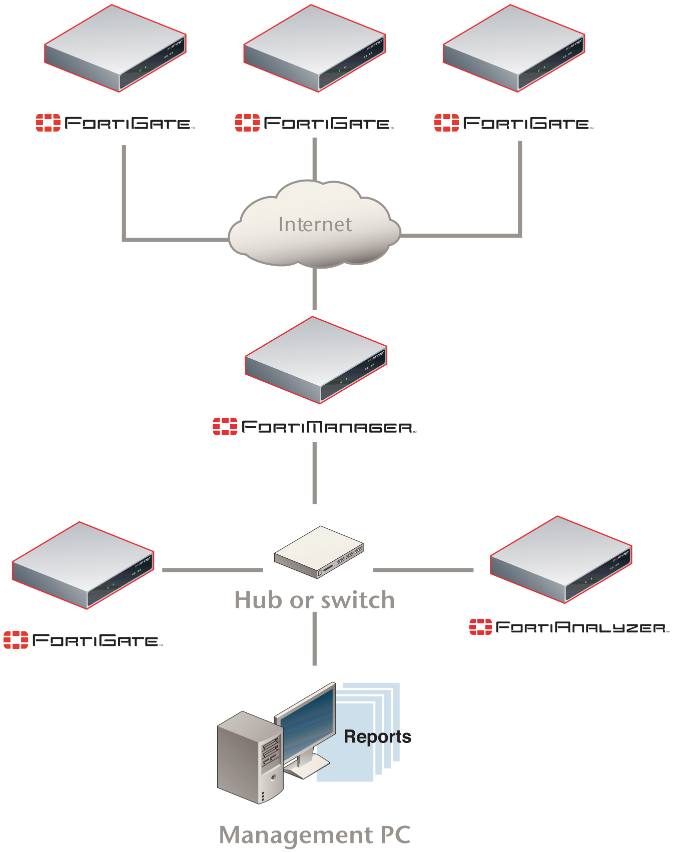


Figure 1: A typical FortiAnalyzer deployment architecture

Security Level Summary

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

Table 1: Summary of FIPS Security Requirements and Compliance Levels

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

Module Description

The module is a firmware based operating system that runs exclusively on Fortinet’s FortiAnalyzer product family. FortiAnalyzer units are PC-based, purpose built appliances. The module constitutes the entire firmware based operating system for a FortiAnalyzer appliance and can only be installed and run on a FortiAnalyzer appliance. The module provides a proprietary and non-modifiable operating system and does not provide a programming environment.

Module Interfaces

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

Table 2: FortiAnalyzer Crypto Module physical ports and logical interfaces

I/O	Logical Interface	Physical Port
Data Input	Network I/O	Network interface
Data Output	Network I/O	Network interface
Control Input	Web Manager, CLI, Console	Network interface, serial interface
Status Output	Web Manager, CLI, Console	Network interface, serial interface
Power Input	N/A	The power supply is the power interface

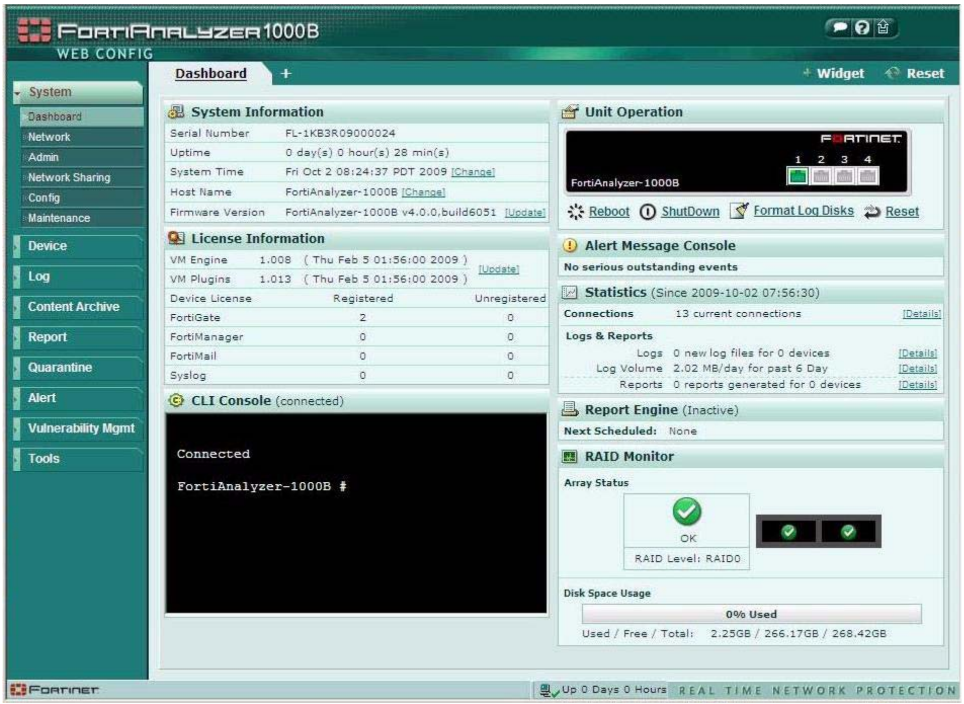
Web-Based Manager

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 2: The FortiAnalyzer web-based manager



System Information

Serial Number	FL-1KB3R09000024
Uptime	0 day(s) 0 hour(s) 28 min(s)
System Time	Fri Oct 2 08:24:37 PDT 2009 [Change]
Host Name	FortiAnalyzer-1000B [Change]
Firmware Version	FortiAnalyzer-1000B v4.0.0,build6051 [Update]

License Information

VM Engine	1.008 (Thu Feb 5 01:56:00 2009)	[Update]
VM Plugins	1.013 (Thu Feb 5 01:56:00 2009)	
Device License	Registered	Unregistered
FortiGate	2	0
FortiManager	0	0
FortiMail	0	0
Syslog	0	0

CLI Console (connected)

```
Connected

FortiAnalyzer-1000B #
```

Unit Operation

FortiAnalyzer-1000B

Alert Message Console

No serious outstanding events

Statistics (Since 2009-10-02 07:56:30)

Connections	13 current connections	[Details]
Logs & Reports		
Logs	0 new log files for 0 devices	[Details]
Log Volume	2.02 MB/day for past 6 Day	[Details]
Reports	0 reports generated for 0 devices	[Details]

Report Engine (Inactive)

Next Scheduled: None

RAID Monitor

Array Status

OK

RAID Level: RAID0

Disk Space Usage

0% Used

Used / Free / Total: 2.25GB / 266.17GB / 268.42GB

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 two roles (hereafter referred to as operators): **Crypto Officer** and **User**.

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

Operators assigned the User role have read-only access to the module’s administrative services.

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
User	U

The access types are abbreviated as follows:

Read Access	R
Write Access	W
Execute Access	E

Table 3: Authenticated Services

Service	**CO**	**U**	**Key/CSP**
authenticate to module	WE	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	N/A
show FIPS mode enabled/disabled (console only)	N/A	N/A	N/A
enable FIPS mode of operation (console only)	WE	N/A	N/A
execute factory reset (zeroize keys, disable FIPS mode)	WE	N/A	See “Key Zeroization” on page 9
execute FIPS on-demand self-tests (console only)	N/A	N/A	Configuration Integrity Key, Firmware Integrity Key
add/delete operators	RWE	N/A	N/A
set/reset operator password	WE	N/A	Operator Password,
backup configuration file	WE	N/A	Configuration Backup Key, Configuration Encryption Key, all keys stored in configuration file
read/set/delete/modify module configuration	N/A	N/A	N/A
read/set/delete/modify IPSec VPN configuration	RWE	N/A	IKE Pre-Shared Key
enable/disable alternating bypass mode	N/A	N/A	N/A
execute firmware update	WE	N/A	Firmware Update Public Key

Table 3: Authenticated Services

Service	CO	U	Key/CSP
read log data	N/A	N/A	N/A
delete log data	N/A	N/A	N/A
execute remote system scan	N/A	N/A	N/A

Table 4: Unauthenticated services

Service/CSP	NU	Key/CSP
Access to log data	N/A	N/A
Content archiving	N/A	N/A
Centralized quarantine	N/A	N/A
Samba file sharing	N/A	N/A
NFS file sharing	N/A	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.

Note that operator authentication over HTTPS/SSH over HTTPS is 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.

Using a strong password policy, where operator 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.

Using client side certificates, where operators are authenticated using an RSA certificate, the strength of authentication is based on the RSA key size. Using an RSA cerificate with a key of at least 1024 bits, the odds of guessing the authentication key are 1 in 2^{1024}.

Physical Security

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

Operational Environment

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

- FortiAnalyzer-1000B

The module can also be executed on any of the following FortiAnalyzer appliances and remain vendor affirmed FIPS-compliant:

- FortiAnalyzer-100B
- FortiAnalyzer-800

- FortiAnalyzer-800B
- FortiAnalyzer-2000
- FortiAnalyzer-2000A
- FortiAnalyzer-4000
- FortiAnalyzer-4000A

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 Public 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 10 for a complete list of keys and CSPs.

Algorithms

Table 5: FIPS Approved or Allowed Algorithms

Algorithm	CAVP Validation Number
RNG (ANSI X9.31 Appendix A)	667
Triple-DES (168 bit keys)	870, 874
AES (128, 192 and 256 bit keys)	1206, 1213
SHA-1	1109, 1117
HMAC SHA-1	701, 707
Diffie-Hellman (key agreement; key establishment methodology provides between 80 and 96 bits of encryption strength; non-compliant less than 80-bits of encryption strength)	
RSA PKCS1 (digital signature verification, key wrapping; key establishment method provides 80 or 112 bits of encryption strength - 1024 and 2048 bit certificates are supported)	584

Table 6: 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)

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 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
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
HTTPS/SSL Server/Host Key	Flash RAM Plain-text	RSA private key used in the HTTPS/TLS protocols
HTTPS/TLS Session Authentication Key	SDRAM Plain-text	HMAC SHA-1 key used for HTTPS/TLS session authentication
HTTPS/TLS Session Encryption Key	SDRAM Plain-text	AES or Triple-DES key used for HTTPS/TLS session encryption
SSH Server/Host Key	Flash RAM Plain-text	RSA private key used in the SSH protocol
SSH Session Authentication Key	SDRAM Plain-text	HMAC SHA-1 key used for SSH session authentication
SSH Session Encryption Key	SDRAM Plain-text	AES or Triple-DES key used for SSH session encryption
Firmware Update Public Key	Flash RAM Plain-text	Verification of firmware integrity during firmware load test using RSA public key
Firmware Integrity Key	Flash RAM Plain-text	Verification of firmware integrity during firmware integrity test using RSA public key
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 the operator passwords)

Table 7: Cryptographic Keys and Critical Security Parameters Used in FIPS Mode

Key or CSP	Storage	Description/Usage
Configuration Backup Key	Flash RAM Plain-text	HMAC SHA-1 key used to hash 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

Alternating Bypass Feature

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

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

Three independent actions must be taken by the CO or User to configure a device to communicate with the module in a non-bypass state.

- Enable secure connectivity for the device
- Set the pre-shared key for the IPSec tunnel
- Set the local identifier for the remote 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.

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 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 (TLS v1.0)
  - Command line interface (CLI) access via SSH (v2.0)
- Diffie-Hellman key sizes of less than1024 bits (Group 5) are not used.
- Client side RSA certificates for administrator authentication use a minimum key size of 1024 bits.

The module can be configured in either gateway or transparent mode. Server mode is not supported.

Self-Tests

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

- Firmware integrity test using RSA signatures
- Configuration integrity test using SHA-1 hash
- 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 integrity test using SHA-1 hash
- Firmware load test using RSA signatures

Non-FIPS Approved Services

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

- RADIUS support for operator authentication

If the above service isused, the module is not considered to be operating in the FIPS approved mode of operation.