FIPS 140-2 Security Policy

FortiGate-3000/3600

FortiGate-3000/3600 FIPS 140-2 Security Policy	
Document Version:	1.05
Publication Date:	July 14, 2004
Description:	Documents FIPS 140-2 Security Policy issues, compliancy and requirements for FIPS compliant operation.
Hardware Models:	FortiGate-3000 (build xx20), FortiGate-3600 (build xx20)
Firmware Version:	2.50,build219,040616

Fortinet Inc.

FortiGate-3000/3600 FIPS 140-2 Security Policy
v1.05
July 14, 2004

Regulatory Compliance
FCC Class A Part 15 CSA/CUS

Table of Contents

References 5

Security Level Summary 6

FortiGate Module Description 6

Cryptographic Module Description 7

Cryptographic Module Ports and Interfaces 8

Roles, Services and Authentication 12

Physical Security 15

Operational Environment 16

Cryptographic Key Management 16

Electromagnetic Interference/Electromagnetic Compatibility (EMI/EMC) 18

Mitigation of Other Attacks 19

NIDS Detection Component 20

NIDS Prevention Component 20

NIDS Attack Types 20

Antivirus Protection 22

Web Filtering 22

Email Filtering 23

FIPS 140-2 Compliant Operation 24

Secure Operation of the Modules 24

Initial Inspection of the Modules 24

Secure Remote Administration 24

Initial Configuration of the Modules 25

Verifying the Firmware Version 25

Enabling FIPS Compliant Mode 25

Self-Tests 26

Error Mode 27

Effects of FIPS Compliant Mode 28

Disabling FIPS Mode 28

Non-FIPS Approved Services 28

.... 28

This document is a FIPS 140-2 Security Policy for Fortinet Incorporated's FortiGate-3000 and 3600 Antivirus Firewalls. This policy describes how the FortiGate-3000 and 3600 (hereafter referred to as the 'module' or 'modules') meet the FIPS 140-2 security requirements and how to operate the modules in a FIPS compliant manner. This policy was created as part of the Level 2 FIPS 140-2 validation of the modules.

This document contains the following sections:

- Security Level Summary
- FortiGate Module Description
- Mitigation of Other Attacks
- FIPS 140-2 Compliant Operation

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/cryptval/.

References

This policy deals specifically with operation and implementation of the FortiGate modules in the technical terms of the FIPS 140-2 standard and the associated validation program. Additional information on the FortiGate modules and 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 FortiResponse Center of the Fortinet corporate website at http://www.fortinet.com/FortiResponseCenter.

Security Level Summary

The Fortinet FortiGate-3000 and 3600 modules meet 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	2
Roles, Services and Authentication	2
Finite State Model	2
Physical Security	2
Operational Environment	N/A
Cryptographic Key Management	2
EMI/EMC	2
Self-Tests	2
Design Assurance	2
Mitigation of Other Attacks	2

FortiGate Module Description

The FortiGate family spans the full range of network environments, from SOHO to service provider, offering cost effective systems for any 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 protection, the FortiGate modules deliver a full range of network-level services — firewall, VPN, intrusion detection and traffic shaping — in dedicated, easily managed platforms.

With models spanning SOHO to service providers, the FortiGate product family spans the full range of network environments and offers cost effective systems for any application. All FortiGate Antivirus Firewalls 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 the ICSA for antivirus, IPSec, firewall and intrusion detection functionality, the FortiGate modules deliver the highest level of security available. They add 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 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.

This section contains the following information:

- Cryptographic Module Description
- Cryptographic Module Ports and Interfaces
- Roles, Services and Authentication
- Physical Security
- Operational Environment
- Cryptographic Key Management
- Electromagnetic Interference/Electromagnetic Compatibility (EMI/EMC)

Cryptographic Module Description

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

The modules are Internet devices that provide integrated firewall, VPN, antivirus, intrusion detection, content filtering and traffic shaping capabilities. This FIPS 140-2 Security Policy specifically covers the firewall and VPN capabilities of the modules.

The intrusion detection, antivirus, content filtering and traffic shaping capabilities of the modules can be used without compromising the FIPS approved mode of operation.

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

- The FortiGate-3000 has 6 network interfaces with a status LED for each network interface (3 10/100BaseT, 1 1000BaseT and 2 1000Base-SX)
- The FortiGate-3600 has 7 network interfaces with a status LED for each network interface (1 10/100 BaseT, 2 1000BaseT and 4 1000Base-SX)

These differences are detailed in Figures 1 and 2 and Tables 2 to 7. Both the FortiGate-3000 and 3600 have fixed, internal hard drives.

Cryptographic Module Ports and Interfaces

FortiGate-3000 Module

Figure 1: FortiGate-3000 Front and Rear Panels

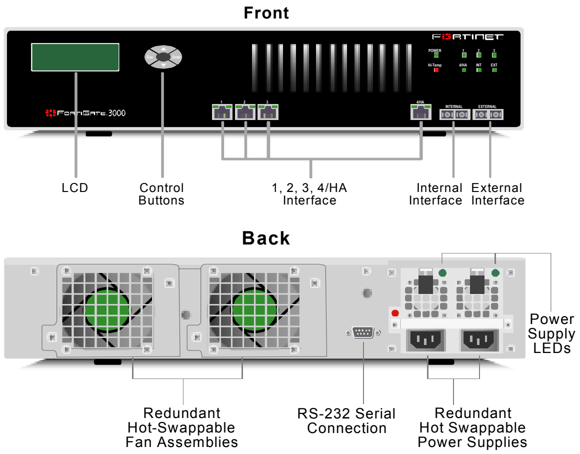


Table 2: FortiGate-3000 Status LEDs

LED	State	Description
Power	Green	The FortiGate-3000 module is powered on.
	Off	The FortiGate-3000 module is powered off.
Display LEDs: 1, 2, 3, 4, INT, EXT	Green	Link established.
	Flashing Green	Network activity at this interface.
	Off	No link established.
Left Interface LED: 1, 2, 3, 4/HA	Green	The interface is connected at 100 Mbps.
	Off	The interface is connected at 10Mbps or the equipment does not have power.
Right Interface LED: 1, 2, 3, 4/HA	Amber or Green	Link established.
	Flashing Amber or Green	Network activity at this interface.
	Off	No link established.
Hi-Temp	N/A	Not in use.

Table 3: FortiGate-3000 Front Panel Connectors and Ports

Connector	Type	Speed	Supported Logical Interfaces	Description

Table 3: FortiGate-3000 Front Panel Connectors and Ports

1, 2, 3	RJ-45	10/100Base-T	Data input, data output, control input and status output	Optional connection to other networks.
4/HA	RJ-45	1000Base-T	Data input, data output, control input and status output	Optional copper gigabit connection to another network or other FortiGate-3000s for HA.
INTERNAL	SC	1000Base-SX	Data input, data output, control input and status output	Multimode fiber optic connection to the internal network.
EXTERNAL	SC	1000Base-SX	Data input, data output, control input and status output	Multimode fiber optic connection to the Internet.

Table 4: FortiGate-3000 Rear Panel Connectors and Ports

Connector	Type	Speed	Supported Logical Interfaces	Description
CONSOLE	DB-9	9600 bps	Control input and status output	Provides access to the command line interface (CLI).
POWER	N/A	N/A	Power	120/240VAC power connection.

FortiGate-3600 Module

Figure 2: FortiGate-3600 Front and Rear Panels

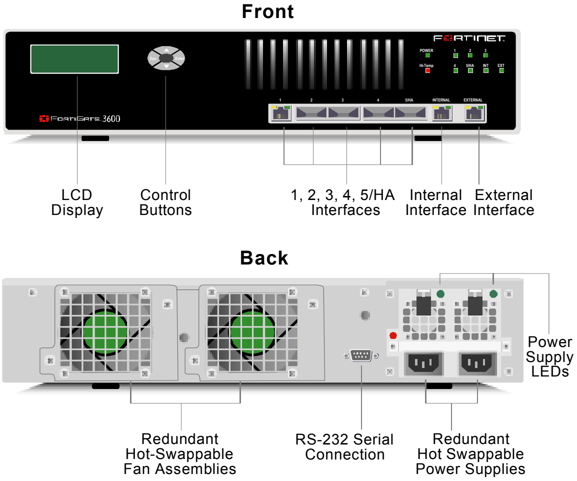


Table 5: FortiGate-3600 Status LEDs

LED	State	Description
Power	Green	The FortiGate-3600 module is powered on.
	Off	The FortiGate-3600 module is powered off.
Display LEDs: **1, 2, 3, 4, 5/HA, INT, EXT**	Green	Link established.
	Flashing Green	Network activity at this interface.
	Off	No link established.

Table 5: FortiGate-3600 Status LEDs

Left Interface LED: **1, Internal, External**	Green	The interface is connected at 100 Mbps.
	Off	The interface is connected at 10Mbps or the equipment does not have power.
Right Interface LED: **1, Internal, External**	Amber or Green	Link established.
	Flashing Amber or Green	Network activity at this interface.
	Off	No link established.
Hi-Temp	N/A	Not in use.

Table 6: FortiGate-3600 Front Panel Connectors and Ports

Connector	Type	Speed	Supported Logical Interfaces	Description
1	RJ-45	10/100Base-T	Data input, data output, control input and status output	Optional connection to other networks.
2, 3, 4	SC	1000Base-SX	Data input, data output, control input and status output	Optional multimode fiber connection to other networks.
5/HA	SC	1000Base-SX	Data input, data output, control input and status output	Optional copper gigabit connection to another network or other FortiGate-3000s for HA.
INTERNAL	RJ-45	1000Base-T	Data input, data output, control input and status output	Copper gigabit connection to the internal network.
EXTERNAL	RJ-45	1000Base-T	Data input, data output, control input and status output	Copper gigabit connection to the internal network.

Table 7: FortiGate-3600 Rear Panel Connectors and Ports

Connector	Type	Speed	Supported Logical Interfaces	Description
CONSOLE	DB-9	9600 bps	Control input and status output	Provides access to the command line interface (CLI).
POWER	N/A	N/A	Power	120/240VAC power connection.

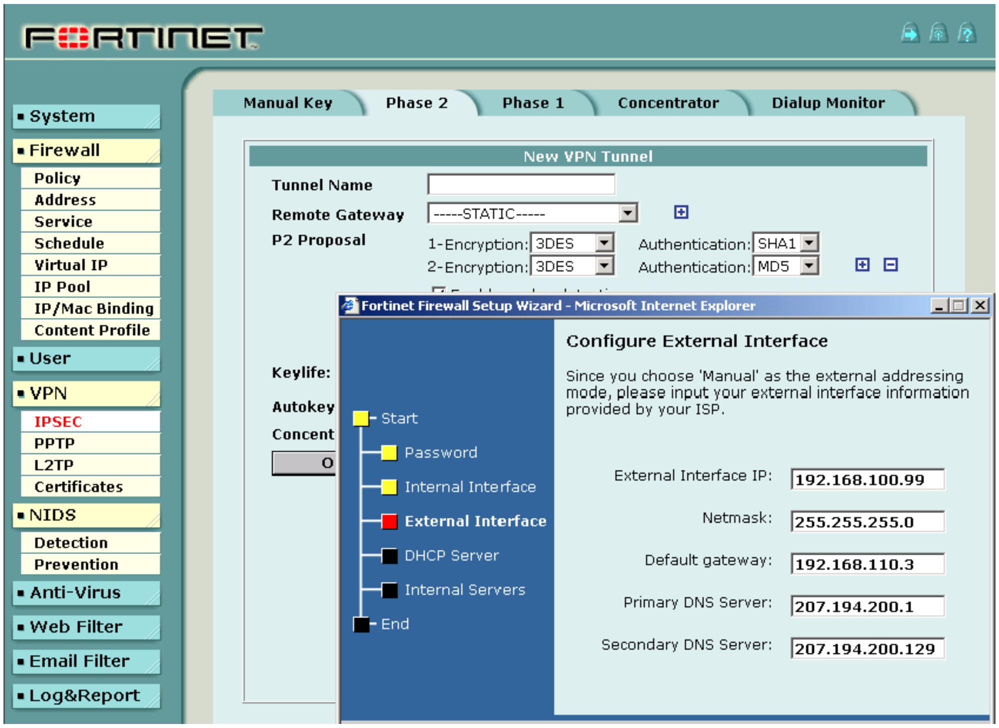
Web-Based Manager

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 module and the management computer.

The web-based manager uses Transport Layer Security (TLS) for connection security in FIPS mode.

The web-based manager is not part of the validated module boundaries.

Figure 3: The FortiGate web-based manager



New VPN Tunnel

Tunnel Name

Remote Gateway -----STATIC-----

P2 Proposal 1-Encryption: 3DES Authentication: SHA1

2-Encryption: 3DES Authentication: MD5

Keylife:

Autokey

Concent

Fortinet Firewall Setup Wizard - Microsoft Internet Explorer

Configure External Interface

Since you choose 'Manual' as the external addressing mode, please input your external interface information provided by your ISP.

External Interface IP: 192.168.100.99

Netmask: 255.255.255.0

Default gateway: 192.168.110.3

Primary DNS Server: 207.194.200.1

Secondary DNS Server: 207.194.200.129

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 is required.

A FIPS 140-2 validated SSH client is recommended for SSH access to the CLI when the modules are operating in FIPS mode. Telnet access to the CLI is not allowed in FIPS mode and is disabled. The Telnet or SSH client is not part of the validated module boundaries.

Control Buttons and LCD

The front panel of the modules provides 4 control buttons and an LCD. The front panel buttons and LCD can be used to configure basic parameters such as the internal, external and DMZ/HA interface addresses, and the default gateway address. To access advanced services and configurations the operator must use the web-based manager or the CLI.

Use of the control buttons can be restricted through the use of a 6 digit PIN. Use of the PIN to access the control buttons is mandatory in FIPS mode.

Roles, Services and Authentication

Roles

The modules provides four roles for operators: **Crypto Officer**, **Junior Crypto Officer, User** and **Local Crypto Officer**. The Crypto Officer, Junior Crypto Office and User roles are assumed by operators authenticating to the module remotely or through the console connection. An operator assuming the Crypto Officer role has complete access to all of the administrative functions and services of the module, including resetting or shutting down the module. An operator assuming the Junior Crypto Officer role has read/write access to most of the module functions and services. An operator assuming the User role has read only access to the module functions and services.

The Local Crypto Officer role is assumed when an operator authenticates to module using the control panel and LCD on the front panel of the module. An operator assuming the Local Crypto Office role has read/write access to a limited set of configuration functions for the module.

The modules also provide a **Network User** role for end-users. Network users can make use of the encrypt/decrypt services, but cannot access the administrative functions and services.

Refer to the next section on Services for detailed information on what cryptographic 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, and the CSPs they affect, available to each role and the type of access for each role. The role names are abbreviated as follows:

Crypto Officer	CO
Junior Crypto Officer	JCO
User	U
Local Crypto Officer	LCO
Network User	NU

Table 8: VPN Cryptographic Services available by role via the CLI

Roles	Service/CSP	Access
CO, JCO, U	authenticate to module	E
	show status	R
CO	enable/disable FIPS mode of operation	WE
	set/reset operator passwords	WE

Table 8: VPN Cryptographic Services available by role via the CLI

Roles	Service/CSP	Access
CO, JCO	zeroize keys (execute factory reset)	E
	execute FIPS self-tests	E
	add/delete operators	RWE
	set/reset own password	WE
	execute firmware download	E
	execute system reboot	E
	execute system shutdown	E
	enable/disable debug mode	WE
	execute system diagnostics	E
	change system time	WE
CO, JCO	read/set/delete/modify system/network configuration	RWE
	read/set/delete/modify firewall policies	RWE
	read/set/delete/modify VPN configuration	RWE
	read/set/delete/modify NIDS configuration	RWE
	read/set/delete/modify logging/reporting configuration	RWE

Table 9: VPN Cryptographic Services available by role via the web-manager

Roles	Service/CSP	Access
CO, JCO, U	authenticate to module	E
	show status	R
CO	zeroize keys (execute factory reset)	E
	add/delete operators	RWE
	set/reset operator passwords	WE
	execute firmware download	E
	execute system reboot	E
	execute system shutdown	E
	create and download backup configuration file	WE
	restore system configuration from backup	RWE

Table 9: VPN Cryptographic Services available by role via the web-manager

Roles	Service/CSP	Access
CO, JCO	change system time	WE
	set/reset own password	WE
	read/set/delete/modify system/network configuration	RWE
	read/set/delete/modify firewall policies	RWE
	read/set/delete/modify VPN configuration	RWE
	read/set/delete/modify NIDS configuration	RWE
	read/set/delete/modify logging/reporting configuration	RWE

Table 10: VPN Cryptographic Services available by role via the control panel

Roles	Service/CSP	Access
LCO	read/set/modify network configuration	RWE
	zeroize keys (execute factory reset)	E
	change console baud rate	RWE

Table 11: VPN Cryptographic Services available to Network Users

Roles	Service/CSP	Access
NU	authenticate to module based on ip or MAC address	E
	encrypt/decrypt controlled by firewall policies	E

Authentication

The modules support role based authentication. Operators must authenticate with a user-id and password combination to access the module remotely or via the console. Operators must authenticate with a 6 digit PIN to access the front panel control panel.

Authenticated users assume a specific role. To assume the Crypto Officer role the operator must be authenticated by using the appropriate user-id and password combination to access the **admin** account. To assume a Junior Crypto Officer role the operator must be authenticated by using the appropriate user-id and password combination to access an **Administrator** account with read/write privileges that has been created by the Crypto Officer. To assume a User role the operator must be authenticated by using the appropriate user-id and password combination to access an **Administrator** account with read only privileges that has been created by the Crypto Officer. To assume the Local Crypto Officer role the operator must enter the correct PIN using the front control panel.

The minimum password length must be 8 characters when in FIPS mode. 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 an operator password are 1 in 96^8.

The odds of guessing the PIN are 1 in 10^6.

For Network Users invoking the VPN encryption/decryption services, the module acts on behalf of the Network User and negotiates a VPN connection with a remote module. The strength of authentication for VPN services is based on the authentication method defined in a specific firewall policy: either manual key, pre-shared key or RSA certificate.

The minimum permitted manual key size in FIPS mode is 128 bits, pre-shared key authentication uses Diffie-Hellman with a minimum modulus of 768 bits and certificate based authentication uses 1024 bit keys. Therefore the odds of guessing a VPN authentication key are at least 1 in $2^{128.}$

Physical Security

The modules meet FIPS 140-2 Security Level 2 requirements by using production grade components with passivation coating (where applicable) and an opaque, sealed enclosure. Access to the enclosure is restricted through the use of a tamper-evident seals to secure the overall enclosure. The seals are applied at the factory prior to shipping.

The FortiGate-3000 and 3600 use five seals to secure:

- the external enclosure
- the removable fans assemblies (two)
- the removable power supplies
- the bottom side access panel

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

Figure 4: FortiGate-3000 and 3600 tamper seal placement

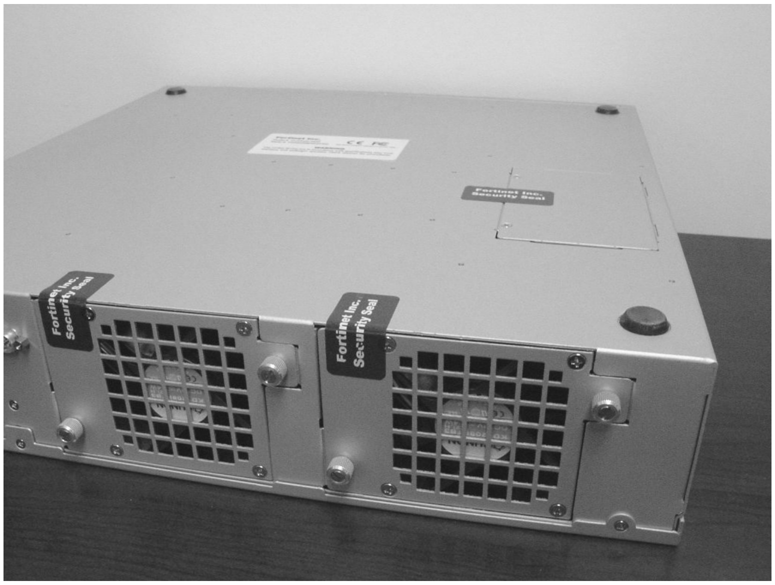
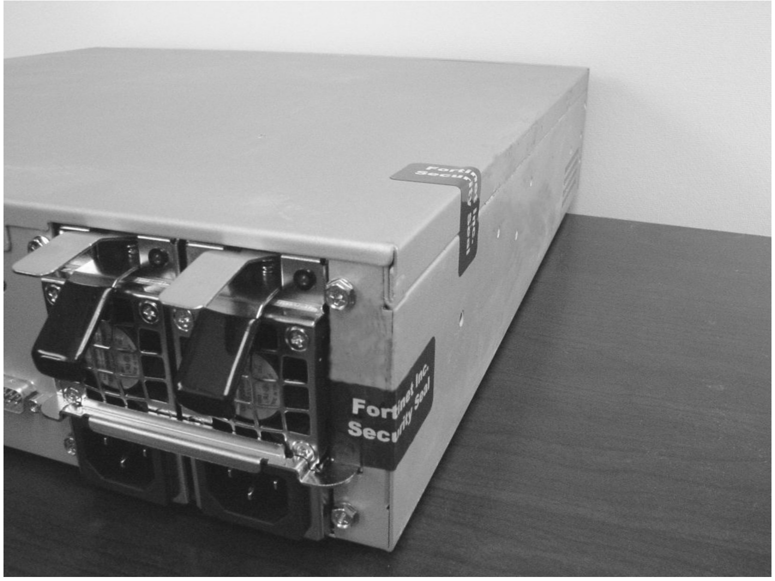

Fortinet Inc. Security Seal
Fortinet Inc. Security Seal
Fortinet Inc. Security Seal

Figure 5: FortiGate-3000 and 3600 tamper seal placement



The Crypto Officer should develop an inspection schedule to verify that the external enclosure of the modules and the tamper seals have not been damaged or tampered with in any way.

The modules do not provide any environmental failure protection features.

Operational Environment

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

Cryptographic Key Management

Random Number Generation

The modules use a firmware based, deterministic random number generator that conforms to the FIPS 186-2 standard, Appendix 3.1, modified as per Change Notice 1.

Key Zeroization

Key zeroization occurs when the Crypto Officer executes a factory reset via the web-manager or the CLI. A factory reset returns the module to the default configuration parameters. All non-preconfigured keys, critical security parameters are zeroized during a factory reset. See table 14 for details on which keys and CSPs are not preconfigured. A factory reset also clears all firewall, VPN and other module configuration parameters.

Algorithms

Table 12: FIPS Approved Algorithms

Algorithm	NIST Certificate Number
3DES	237
AES	128
SHA-1	213
HMAC SHA-1	213 (Vendor Affirmed)
RSA PKCS1 (digital signature creation and verification, key wrapping)	Vendor Affirmed

Table 13: Non-FIPS Approved Algorithms

Algorithm
DES (disabled in FIPS mode)
Diffie Hellman (key agreement)
MD5 (disabled in FIPS mode)
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 modules. The following definitions apply to the table:

Key or CSP Lists the key description.

Storage Where the keys are stored and how they are protected.

Usage How the keys are used

Table 14: FIPS Approved Crytographic Keys and Critical Security Parameters

Key or CSP	Storage	Usage
IPSEC Manual Encryption Key	Flash RAM AES encrypted	VPN traffic encryption/decryption using 3DES or AES
IPSEC Session Encryption Key	SDRAM Plain-text	VPN traffic encryption/decryption using 3DES or AES
IKE Pre-Shared Key	Flash RAM AES encrypted	Seed used to generate IKE session key and authentication key
IKE Authentication Key	SDRAM Plain-text	IKE peer-to-peer authentication using HMAC SHA-1 (SKEYID_A)
IKE Key Generation Key	SDRAM Plain-text	Deriving IPSEC SA keying material (SKEYID_D)
IKE Session Encryption Key	SDRAM Plain-text	Encryption of IKE peer-to-peer key negotiation using 3DES or AES (SKEYID_E)
IKE RSA Key	Flash Ram Plain text	IKE peer-to-peer authentication using X.509 certificates

Table 14: FIPS Approved Crytographic Keys and Critical Security Parameters

Key or CSP	Storage	Usage
HA Encryption Key	Flash RAM AES encrypted	Encryption of traffic between modules in a HA cluster using AES
Firmware Integrity Key	Flash RAM Plain-text	Verify integrity of firmware during self-test using HMAC SHA-1
VPN Bypass Key	Flash RAM Plain-text	Verify integrity of VPN table during self-tests (bypass test) using HMAC SHA-1
RNG Seed	SDRAM Plain-text	Random number generation
Firmware Download Public Key	Flash RAM Plain-text	Verification of firmware integrity for download of new firmware versions using RSA public key
TLS Server/Host Key	Flash RAM Plain-text Preconfigured	Remote Web manager authentication using HMAC SHA-1
TLS Session Key	SDRAM Plain-text	Remote Web manager session encryption and authentication using AES
SSH Server/Host Key	Flash RAM Plain-text	Remote CLI authentication using HMAC SHA-1
SSH Session Key	SDRAM Plain-text	Remote CLI session encryption and authentication using AES
Operator Username	Flash RAM Plain-text	Used during operator authentication to differentiate between Crypto Officers, Junior Crypto Officer and Users
Operator Password	Flash RAM AES	Used to authenticate operator access to the module
FIPS Mode Seed Key	Flash RAM Plain-text	Static key used as a seed key to: • generate an AES encryption key used to encrypt CSPs stored on the flash card. • calculate the HMAC SHA-1 used in the self-tests. • generate a PKCS12 public/private key pair used to key wrap any RSA private keys in the backup configuration file.

Electromagnetic Interference/Electromagnetic Compatibility (EMI/EMC)

The modules comply with EMI/EMC requirements as specified by part 15 of the FCC rules. The following table lists the specific lab and FCC report information for the modules.

Table 15: FCC Report Information

Module	Lab Information	FCC Report Number
FortiGate-3000	C&C Laboratory Co. #B1, first Floor, Universal Center No. 183, Sec. 1, Tatung Road, Hsi Chih Taipei Hsien, Taiwan, R.O.C. 011-886-2-8642-2071	021422-F-1
FortiGate-3600	BACL Corp 230 Commercial Street Sunnyvale, CA 94085 (408) 732-9162	R0309152

Mitigation of Other Attacks

The FortiGate modules include real-time a Network Intrusion Detection System (NIDS) as well as antivirus protection and content filtering. Use of these capabilities is optional.

The FortiGate NIDS has two components: an attack detection component and an attack prevention component. Both components use attack signatures to both detect and prevent a wide variety of suspicious network traffic and direct network-based attacks. Functionally, signatures are similar to virus definitions, with each signature designed to detect a particular type of attack. The FortiGate NIDS uses over 1,000 attack signatures.

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 module. FortiGate antivirus protection also controls the blocking of oversized files and email and the exemption of fragmented email from blocking.

FortiGate content filtering can be configured to provide both web (HTTP) and email (POP3, IMAP, and SMTP) filtering. FortiGate web filtering is based on banned words, URL block/exempt lists, and script filtering. FortiGate email filtering is based on banned words and email address block/exempt lists.

Whenever a NIDS, antivirus or filtering event occurs, the module can record the event in the log and/or send an alert email to the Crypto Officer or other user.

The rest of this section provides a summary of the NIDS, antivirus and content filtering capabilities of the FortiGate modules. For complete information refer to the FortiGate Installation and Configuration Guide for the specific module in question, the FortiGate NIDS Guide, and the FortiGate Content Protection Guide.

This section contains the following information:

- NIDS Detection Component
- NIDS Prevention Component
- NIDS Attack Types
- Antivirus Protection
- Web Filtering
- Email Filtering

NIDS Detection Component

The FortiGate NIDS can detect a wide variety of suspicious network traffic and network-based attacks. Attack signatures are the core of the FortiGate NIDS Detection module. Signatures are transmission patterns and other codes that indicate that a system might be under attack. Functionally, signatures are similar to virus definitions, with each signature designed to detect a particular type of attack.

The FortiGate modules can be configured to automatically check for and download updated attack definitions from the Fortinet signature download server, or they can be manually downloaded manually by the Crypto Officer.

Downloading updated attack signatures makes no changes to the firmware, configuration or basic operation of the modules.

User defined attack signatures are also supported.

NIDS Prevention Component

The FortiGate NIDS can prevent common TCP, ICMP, UDP, and IP attacks from disrupting network operations. When the NIDS detects an intrusion which matches a definition, access is denied or packets are dropped thereby avoiding costly network disruptions.

Like the NIDS detection component, the NIDS prevention component uses signatures to detect attacks and generates attack messages which can be logged or emailed. However, although the NIDS prevention component and the NIDS detection component operate similarly, they use unique signatures and generate unique messages.

The signatures listed in the NIDS prevention component are updated when the FortiGate module receives a firmware upgrade. New prevention signatures cannot be downloaded from Fortinet.

NIDS Attack Types

The Foritgate NIDS can be configured to detect and prevent the following types of attacks:

- Denial of Service (DoS)
- Reconnaissance
- Exploits
- NIDS evasion

Denial of Service (DoS) attacks

Denial of Service attacks attempt to deny access to a service or a computer by overloading network links, overloading the CPU, or filling up disks. The attacker is not trying to gain information, but to interfere with access to network resources. The FortiGate NIDS detects the following common DoS attacks:

- Packet floods, including Smurf flood, TCP SYN flood, UDP flood, and ICMP flood
- Incorrectly formed packets, including Ping of Death, Chargen, Tear drop, land, and WinNuke

Reconnaissance

Reconnaissance attacks attempt to gain information about a computer network in preparation for an attempt to break into it. Using the information gained, an attacker can identify and attack specific vulnerabilities. The FortiGate NIDS detects the following common reconnaissance attacks:

- Fingerprinting
- Ping sweeps
- Port scans
- Buffer overflows, including SMTP, FTP and POP3
- Account scans
- OS identification

Exploits

Exploits are attempts to take advantage of features or bugs to gain unauthorized access to a computer or network. The FortiGate NIDS detects the following common exploits:

- Brute Force attack
- CGI Scripts, including Phf, EWS, info2www, TextCounter, GuestBook, Count.cgi, handler, webdist.cgi,php.cgi, files.pl, nph-test-cgi, nph-publish, AnyForm, and FormMail
- Web Server attacks
- Web Browser attacks, including URL, HTTP, HTML, JavaScript, Frames, Java, and ActiveX
- SMTP (SendMail) attack
- IMAP/POP attack
- Buffer overflow
- DNS attacks, including BIND and Cache
- IP spoofing
- Trojan Horse attacks, including BackOrifice 2K, IniKiller, Netbus, NetSpy, Priority, Ripper, Striker, and SubSeven

NIDS evasion

As attackers become more sophisticated, they are developing techniques to evade NIDS systems. The FortiGate NIDS detects the following NIDS evasion techniques:

- Signature spoofing
- Signature encoding
- IP fragmentation
- TCP/UDP disassembly

Antivirus Protection

Virus scanning intercepts most files (including files compressed with up to 12 layers of compression using zip, rar, gzip, tar, upx, and OLE) in the content streams for which antivirus protection as been enabled. Each file is tested to determine the file type and to determine the most effective method of scanning the file for viruses. For example, binary files are scanned using binary virus scanning and Microsoft Office files containing macros are scanned for macro viruses. 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 be configured to quarantine blocked or infected files. The quarantined files are stored on the module’s hard disk. A Crypto Officer can delete quarantined files from the hard disk or download them. Downloaded quarantine files can be submitted to the FortiResponse Center as a virus sample. FortiGate antivirus protection is transparent to the end user.

FortiGate virus definitions provide protection from all viruses on the current WildList virus list as well as from many legacy viruses. The WildList is an authoritative list of viruses known to be in active circulation. For more information, see the WildList web site at www.wildlist.org. Legacy viruses are only very rarely encountered but are included to protect legacy software and hardware running on protected networks.

Web Filtering

FortiGate web filtering can be configured to scan all HTTP content protocol streams for URLs or for web page content. If a match is found between a URL on the URL block list, or if a web page is found to contain a word or phrase in the content block list, the FortiGate blocks the web page. The blocked web page is replaced with a message that a Crypto Officer can edit using the web-based manager.

A Crypto Officer can configure URL blocking to block all or just some of the pages on a 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, a Crypto Officer can add URLs to an Exempt List that overrides the URL blocking and content blocking lists.

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.

Email Filtering

FortiGate email filtering can be configured to scan all IMAP and POP3 protocol traffic for unwanted senders or for unwanted content. If a match is found in a sender address pattern on the email block list, or if an email is found to contain a word or phrase in the banned word list, the FortiGate adds a tag to the subject line of the email. Receivers can then use their mail client software to filter messages based on the tag.

A Crypto Officer can configure email blocking to tag emails from all or some senders within organizations that are known to send unwanted emails. To prevent unintentional tagging of email from legitimate senders, a Crypto Officer can add sender address patterns to an exempt list that overrides the email block and banned word lists.

FIPS 140-2 Compliant Operation

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

This section contains the following information:

- Secure Operation of the Modules
- Initial Inspection of the Modules
- Secure Remote Administration
- Initial Configuration of the Modules
- Verifying the Firmware Version
- Enabling FIPS Compliant Mode
- Self-Tests
- Error Mode
- Effects of FIPS Compliant Mode
- Disabling FIPS Mode
- Non-FIPS Approved Services

Secure Operation of the Modules

The organization must assign a Crypto Officer for the modules.

The Crypto Officer must ensure that:

- modules are installed in a secure physical location,
- physical access to a module is restricted to authorized operators,
- modules are regularly inspected for damage or tampering.

The Crypto officer must enforce a strong password policy, where operator passwords are at least 8 characters in length and use a mix of alphanumeric characters. Operator passwords must also be changed on a regular basis.

If the Crypto Officer is going to allow remote administration of a module, it is recommended that trusted hosts are defined for each operator.

Initial Inspection of the Modules

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

Secure Remote Administration

Remote administration of a module is supported in FIPS mode. A web browser that supports transport layer security (TLS) 1.0 is required to access the web-based manager. A FIPS 140-2 validated SSH client is recommended for remote access to the CLI. The SSH client must be configured to use HMAC SHA-1 and AES128.

Initial Configuration of the Modules

The modules are shipped with the FIPS compliant version of the firmware already installed on the modules. The Crypto Officer must complete an initial setup and configuration of each module as explained in the module's Installation and Configuration Guide. As a minimum, the Crypto Officer must configure console access to the CLI and set the Crypto Officer (admin) password.

Verifying the Firmware Version

The Crypto Officer must verify that a module is running a FIPS compliant firmware version before completing the setup and configuration. There is a specific firmware version for each FortiGate model. The firmware version can be verified using the web-manager or the CLI.

To view the firmware version using the web-manager, go to the **System > Status** page. To view the firmware version using the CLI, enter the command **get system status**.

Table 16 lists the FIPS 140-2 validated FortiGate models and the corresponding firmware version.

Table 16: FIPS 140-2 certified FortiGate models and firmware versions

FortiGate Model	Firmware Version
FortiGate-300	2.50,build219,040616
FortiGate-400	2.50,build219,040616
FortiGate-500	2.50,build219,040616
FortiGate-800	2.50,build219,040616
FortiGate-3000	2.50,build219,040616
FortiGate-3600	2.50,build219,040616

Enabling FIPS Compliant Mode

To enable the FIPS compliant mode of operation the Crypto Officer must perform the following steps.

To enable FIPS mode

1. Set the Admin (Crypto Officer) password from the web-based manager or the CLI.
2. Log in to the CLI and enter the command **set system fips enable**.
3. Enter a FIPS mode seed key.

   Entering a FIPS mode seed key is not mandatory. If a seed key is not entered, the system will generate a 512 bit random number to use as the seed key.

   Once the seed key is entered (or generated) the Crypto officer is logged out of the CLI, the self-tests are executed, and the module switches to the FIPS compliant mode of operation. Enabling FIPS mode will zeroize any previously entered cryptographic keys, CSPs and configuration information.

4 Verify the LCD displays “FIPS Mode”.

The module is now running in FIPS compliant mode.

5 Configure VPN parameters.

Refer to the *FortiGate Installation and Configuration Guide* and the *FortiGate VPN Guide* for complete information on configuring VPN parameters.

6 Configure firewall security policies.

Refer to the *FortiGate Installation and Configuration Guide* for complete information on configuring security policies.

No encrypt/decrypt services can occur until VPN has been configured with an associated firewall security policy that has an action of “encrypt”.

FIPS Mode Status Indicators

There are two status indicators that show whether a module is running in the FIPS compliant mode of operation: the front panel LCD and the results of a **get system status** CLI command. If a module is in FIPS mode, the front panel LCD will display “FIPS Mode” and the results of a **get system status** will include the text “FIPS Mode: enabled”.

Self-Tests

The modules execute 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)
- 3DES, 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
- Continuous RNG 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 **diagnose fips all** (to initiate all self-tests) or **diagnose fips <test>** (to initiate a specific self-test).

The modules execute the following conditional tests when the related service is invoked:

- Continuous RNG 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 **diagnose fips <test>** CLI command.

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

```
Initializing firewall...
FIPS mode: Starting self-tests.
Running aes test...                          passed
Running 3des test...                         passed
Running sha1 hmac test...                    passed
Running rsa test...                          passed
Running hw 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:

```
Fortigate-300 # diagnose fips all
Starting self-tests
Running aes test...       passed
Running 3des test...      passed
Running sha1 hmac test... passed
Running rsa test...       passed
Running hw test...        passed
Running rng test...       passed
Self-tests passed
```

Error Mode

If any of the self or conditional tests fail, the modules switch to an error mode. In error mode all system interfaces are disabled and the status indicator “Error Mode” is displayed on the front LCD panel of the module. The Crypto Officer can attempt to clear the error condition by power cycling the module. If power cycling the module does not clear the error condition, the Crypto Officer must contact a Fortinet technical support representative.

Effects of FIPS Compliant Mode

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

- **admin** (Crypto Officer) password cannot be blank
- “FIPS Mode” is displayed on the front panel LCD of the modules
- “FIPS Mode: Enabled” is displayed by the **get system status** CLI command
- HTTP and Telnet remote administration of the module is disabled
- TFTP is disabled
- SNMP services are disabled
- Remote access to the web-manager requires a web browser that supports TLS 1.0
- Remote access to the CLI requires an SSH client configured to use HMAC SHA-1 and AES128
- Only one operator at a time may access the module through any of the control/status interfaces
- Remote logging is disabled
- Disk logging is enabled
- Startup, conditional and manual self-tests are enabled
- Failure of the self or conditional tests results in the module entering an error mode that shuts down all of the interfaces until operator intervention
- MD5 algorithm is disabled
- DES algorithm is disabled
- Modules cannot be operated in bridge mode

Disabling FIPS Mode

The Crypto Officer can return a module to the normal mode of operation by entering the CLI command **set system fips disable**. Disabling FIPS mode will zeroize the cryptographic keys, CSPs and system configuration. The admin (Crypto Officer) password is not reset by disabling FIPS mode.

Non-FIPS Approved Services

The modules also provide the following non-FIPS approved services:

- NTP synchronization
- Configuration backup and recovery