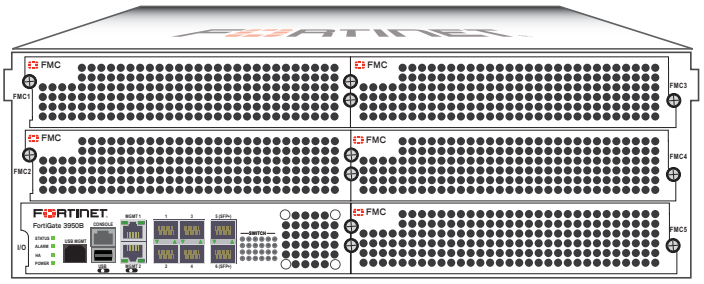
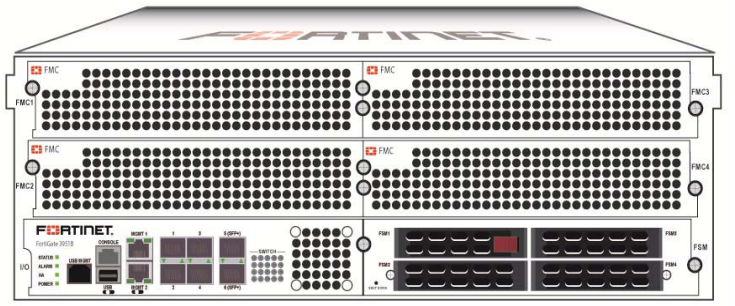
# FIPS 140-2 Security Policy

## FortiGate-3950B/3951B





| | | |
|---|---|---|
| *FortiGate-3950B/3951B FIPS 140-2 Security Policy* | | |
| **Document Version:** | 3.1 | |
| **Publication Date:** | May 20, 2014 | |
| **Description:** | Documents FIPS 140-2 Level 2 Security Policy issues, compliancy and requirements for FIPS compliant operation. | |
| **Firmware Version:** | FortiOS 4.0, build3830, 131223 | |
| **Hardware Version:** | FortiGate-3950B (C4DE23) | Blank Face Plate (P06698-02) |
| | FortiGate-3951B (C4EL37) | Fortinet Storage Module (PE4F79) |

***FortiGate-3950B/3951B FIPS 140-2 Security Policy***

01-436-176918-20120725

for FortiOS 4.0 MR3



**Trademarks**

# Contents

# Overview

This document is a FIPS 140-2 Security Policy for Fortinet Incorporated's FortiGate-3950B and 3951B Multi-Threat Security Systems. This policy describes how the FortiGate-3950B and 3951B (hereafter referred to as the '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:



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 modules 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 using TLS 1.0 in FIPS-CC mode.

# Security Level Summary

The modules meet 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 | 3 |
| Roles, Services and Authentication | 3 |
| Finite State Model | 2 |
| Physical Security | 2 |
| Operational Environment | 2 |
| Cryptographic Key Management | 2 |
| EMI/EMC | 2 |
| Self-Tests | 2 |
| Design Assurance | 3 |
| Mitigation of Other Attacks | 2 |

# Module Description

The FortiGate-3950B and 3951B 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 have 8 network interfaces with a status LED for each network interface (2 10GB SFP+, 4 1GB SFP, 2 10/100/1000 Base-T)

The modules have one, quad core, x86 compatible CPU.

The modules is are 3u rackmount devices.

The modules have external ventilation fans on the back panel of the chassis.

The FortiGate-3950B module supports up to 5 Fortinet Mezzanine Card (FMC) components. The FortiGate-3951B module supports up to 4 Fortinet Mezzanine Card (FMC) components. The FMC components provide additional input/output interfaces.

The FortiGate-3951B module has 4 Fortinet Storage Module (FSM) slots that support removable solid state drives (SSDs). One FSM is installed by default.

The FMC components are excluded from the scope of this FIPS 140-2 validation.

The validated firmware version is FortiOS 4.0, build3830, 131223.

Figure 1, Figure 2 and Figure 3 are representative of the modules tested.

## Cryptographic Module Ports and Interfaces

### FortiGate-3950B/3951B Chassis Module

**Figure 1: FortiGate-3950B Front Panel**

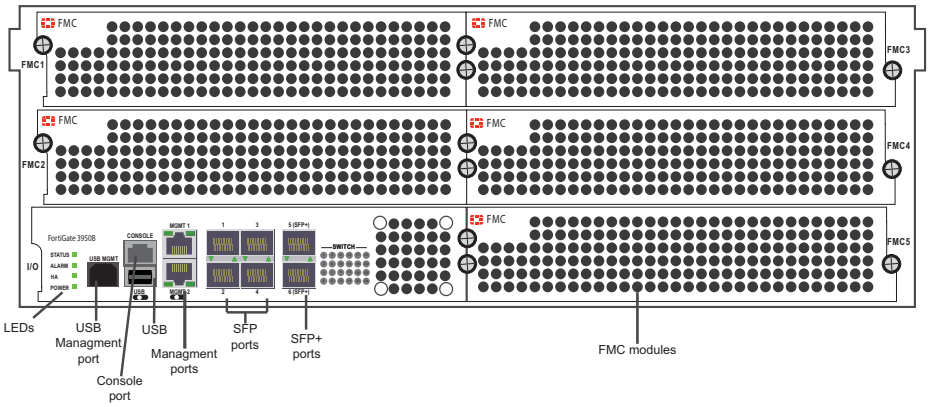



**Figure 2: FortiGate-3951B Front Panel**

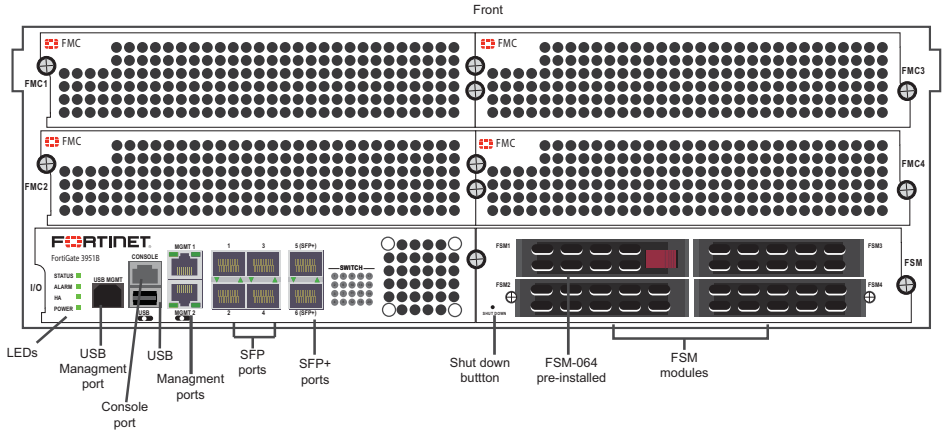


**Figure 3: FortiGate-3950B/3951B Rear Panel**

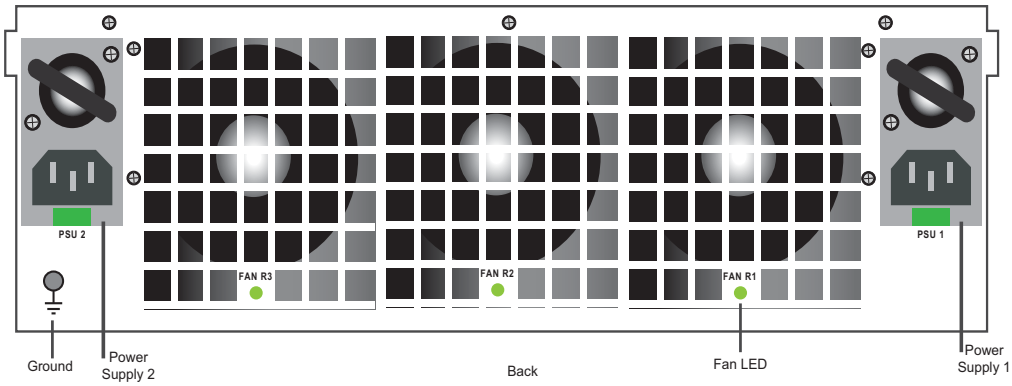



**Table 2: FortiGate-3950 and 3951B Status LEDs**

| LED | | State | Description |
|---|---|---|---|
| Power | | Green | The module is powered on. |
| | | Off | The module is powered off. |
| Status | | Flashing Green | The module is starting up. |
| | | Green | The module is running normally. |
| | | Off | The module is powered off. |
| HA | | Green | HA is enabled and in normal mode. |
| | | Red | HA is enabled but in failover mode. |
| | | Off | The unit is in stand-alone mode. |
| Alarm | | N/A | Future use. |
| Ports 1 to 6 | Link | Green | Port is online. |
| | | Off | Port is offline. |
| | Activity | Flashing Green | Port is receiving or sending data. |
| | | Off | Port may be on, but is not receiving or sending data. |
| Management Ports 1 and 2 | Link | Green | Port is online. |
| | | Flashing Green | Port is receiving or sending data. |
| | Activity | Green | Connected at 1000 Mbps. |
| | | Amber | Connected at 100 Mbps. |
| | | Off | Connected at 10Mbps. |
| AC Power | | Green | AC power is connected and has power. |
| | | Amber | AC power is not connected. |
| Fan | | Green | The fan is running and within the speed range. |
| | | Off | The fan is not running or is over the speed range. |
| Switch LEDS | | Green | The FMC module is inserted properly and the interfaces are online. |
| | | Off | The FMC module is unavailable, offline, or there is an interface problem. |

**Table 3: FortiGate-3950 and 3951B Front Panel Connectors and Ports**

| Connector | Type | Speed | Supported Logical Interfaces | Description |
|---|---|---|---|---|
| Ports 1 to 4 | SFP | 1 Gbps | Data input, data output, control input and status output | Multimode fiber optic connections to gigabit optical networks. |
| Ports 5 and 6 | SFP+ | 10Gbps | Data input, data output, control input and status output | Multimode fiber optic connections to gigabit optical networks. |
| Management 1 and 2 | RJ-45 | 10/100/1000 Base-T | Data input, data output, control input and status output | Copper gigabit connection to 10/100/1000 copper networks. |
| CONSOLE | RJ-45 | 9600 bps | Control input, status output | Optional connection to the management computer. Provides access to the command line interface (CLI). |
| USB | USB | N/A | Key loading and archiving, configuration backup and restore | Optional connection for USB token. |

**Table 4: FortiGate-3950 and 3951B Rear Panel Connectors and Ports**

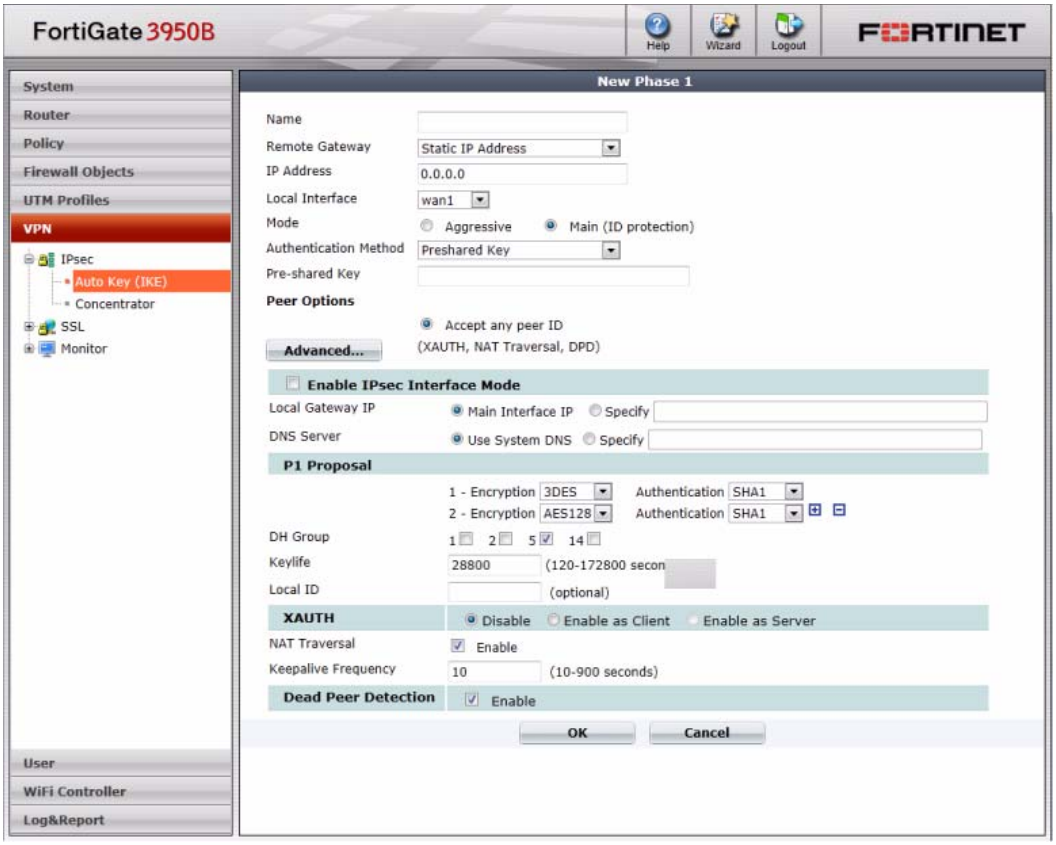
| Connector | Type | Speed | Supported Logical Interfaces | Description |
|---|---|---|---|---|
| POWER | N/A | N/A | Power | 120/240VAC power connection. |

## 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 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 modules is operating in FIPS-CC mode. HTTP access to the web-based manager is not allowed in FIPS-CC mode and is disabled.

**Figure 4: The FortiGate web-based manager**




## Command Line Interface

The FortiGate Command Line Interface (CLI) is a full-featured, text based management tool for the 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 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). Telnet access to the CLI is not allowed in FIPS-CC mode and is disabled.

## Roles, Services and Authentication

### Roles

When configured in FIPS-CC mode, the modules provide the following roles:

- Crypto Officer
- Network User

The Crypto Officer role is initially assigned to the default ‘admin’ operator account. The Crypto Officer role has read-write access to all of the modules’ administrative services. The initial Crypto Officer can create additional operator accounts. These additional accounts are assigned the Crypto Officer role and can be assigned a range of read/write or read only access permissions including the ability to create operator accounts.

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

The modules do not provide a Maintenance role.

## FIPS Approved Services

The following tables detail the types of FIPS approved services available to each role, the types of access for each role and the Keys or CSPs they affect.

The role names are abbreviated as follows:

| | |
|---|---|
| **Crypto Officer** | CO |
| **User** | U |

The access types are abbreviated as follows:

| | |
|---|---|
| **Read Access** | R |
| **Write Access** | W |
| **Execute Access** | E |

**Table 5: Services available to Crypto Officers**

| Service | Access | Key/CSP |
|---|---|---|
| authenticate to module | WE | Operator Password, Diffie-Hellman Key, HTTP/TLS and SSH Server/Host Keys, HTTPS/TLS and SSH Session Authentication Keys, and HTTPS/TLS Session Encryption Keys, RNG Seed, RNG AES Key |
| show system status | WE | N/A |
| show FIPS-CC mode enabled/disabled (console/CLI only) | WE | N/A |
| enable FIPS-CC mode (console only) | WE | Configuration Integrity Key |
| execute factory reset (zeroize keys, disable FIPS mode, console/CLI only) | E | See “Key Zeroization” on page 13 |
| execute FIPS-CC on-demand self-tests (console only) | E | Configuration Integrity Key, Firmware Integrity Key |
| add/delete operators and network users | WE | Operator Password, Network User Password |
| set/reset operator and network user passwords | WE | Operator Password, Network User Password |
| backup/restore configuration file | WE | Configuration Encryption Key, Configuration Backup Key |
| read/set/delete/modify module configuration | WE | N/A |
| enable/disable alternating bypass mode | WE | N/A |

**Table 5: Services available to Crypto Officers**

| Service | Access | Key/CSP |
|---|---|---|
| read/set/delete/modify IPSec/SSL VPN configuration | N/A | IPSec: IPSec Manual Authentication Key, IPSec Manual Encryption Key, IKE Pre-Shared Key, IKE RSA Key<br>SSL: HTTPS/TLS Server/Host Key, HTTPS/TLS Session Authentication Key, HTTPS/TLS SSH Session Encryption Key |
| read/set/modify HA configuration | WE | HA Password,<br>HA Encryption Key |
| execute firmware update | E | Firmware Update Key |
| read log data | WE | N/A |
| delete log data (console/CLI only) | N/A | N/A |
| execute system diagnostics (console/CLI only) | WE | N/A |

**Table 6: Services available to Network Users**

| Service/CSP | Access | Key/CSP |
|---|---|---|
| authenticate to module | E | Network User Password, Diffie-Hellman Key, HTTPS/TLS Server/Host Key, HTTPS/TLS Session Authentication Key, HTTPS/TLS Session Encryption Key, RNG Seed, RNG AES Key |
| IPSec VPN controlled by firewall policies | E | Diffie-Hellman Key, IKE and IPSec Keys, RNG Seed, RNG AES Key |
| SSL VPN controlled by firewall policies | E | Network User Password, Diffie-Hellman Key, HTTPS/TLS Server/Host Key, HTTPS/TLS Session Authentication Key, HTTPS/TLS Session Encryption Key, RNG Seed, 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.

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). 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 18.

For Network Users invoking the IPSec VPN encrypt/decrypt services, the modules act 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 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 serialized red wax/plastic with black lettering that reads "Fortinet Security Seal".

The tamper seals are not applied at the factory prior to shipping. It is the responsibility of the Crypto Officer to apply the seals before use to ensure full FIPS 140-2 compliance. Once the seals have been applied, the Crypto Officer must 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 Crypto Officer 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 following SKU when ordering: FIPS-SEAL-RED. Specify the number of seals required based on the specific module as described below.

The FortiGate-3950B uses 10 seals to secure:

- the FMC slots on the front panel (seals 1 to 5 of 10, see Figure 5)
- the power supplies on the rear panel (seals 6 and 7 of 10, see Figure 5)
- the fan access panels (seals 8 and 9 of 10, see Figure 7)
- the external enclosure (seal 10 of 10, see Figure 8)

The FortiGate-3951B uses 9seals to secure:

- the FMC slots on the front panel (seals 1 to 4 of 9, see Figure 6)
- the power supplies on the rear panel (seals 5 and 6 of 9, see Figure 6)

- the fan access panels (seals 7 and 8 of 9, see Figure 7)
- the external enclosure (seal 9 of 9, see Figure 8)

**Figure 5: FortiGate-3950B Front and Rear Panel Seals**

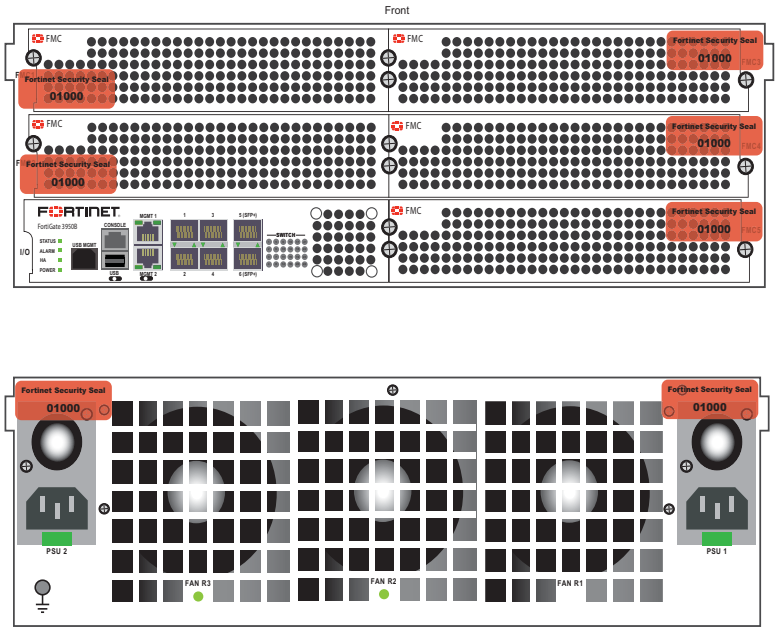



**Figure 6: FortiGate-3951B Front and Rear Panel Seals**

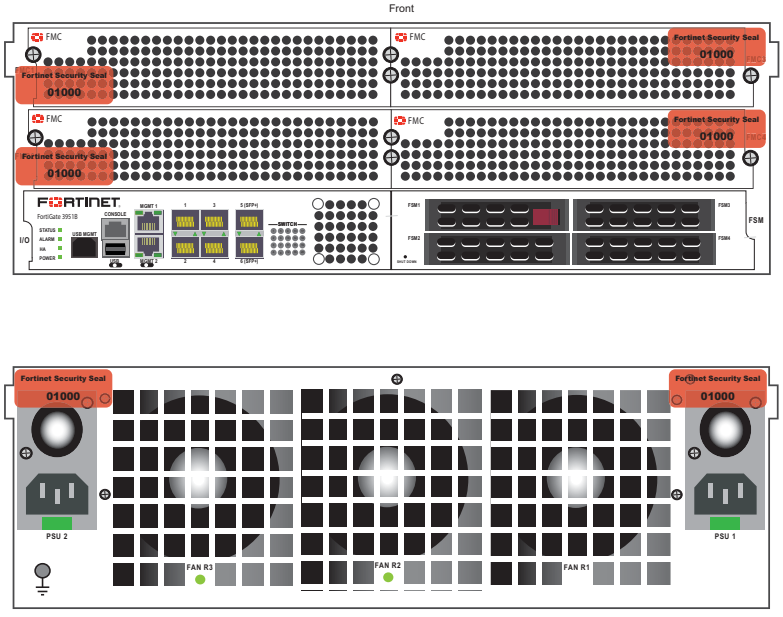


**Figure 7: FortiGate-3950B/3951B Fan Access Panel Seals, top**

**Figure 8: FortiGate-3950B/3951B External Enclosure Seal, top, left side**


## Operational Environment

The module consists of the combination of the FortiOS operating system and the FortiGate appliances. The FortiOS operating system can only be installed, and run, on a FortiGate appliance. The FortiOS 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.

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
- 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 7: FIPS Approved Algorithms**

| Algorithm | NIST Certificate Number |
|---|---|
| RNG (ANSI X9.31 Appendix A) | 1234 |
| Triple-DES | 1425, 1572, 1573 |
| AES | 2278, 2607, 2608 |
| SHA-1 | 1959, 2191, 2192 |
| SHA-256 | 1959, 2191, 2192 |
| HMAC SHA-1 | 1396, 1615, 1616 |
| HMAC SHA-256 | 1396, 1615, 1616 |
| RSA PKCS1 (digital signature verification) | 1169, 1334 |

**Table 8: 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) |
| Diffie-Hellman (key agreement; key establishment methodology provides between 112 and 201 bits of encryption strength; non-compliant less than 112 bits of encryption strength) |
| NDRNG |

**Table 9: 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) |

Note that algorithms may have deprecated encryption strengths, please see NIST SP 800-131A for details.

The vendor makes no conformance claims to any key derivation function specified in SP 800-135rev1. References to the key derivation functions addressed in SP 800-135rev1 including IKE, SSH, and TLS are only listed to clarify the key types supported by the module. Keys related to IKE, SSH, and TLS are only used in the Approved mode under the general umbrella of a non-Approved Diffie-Hellman scheme, with no assurance claims to the underlying key derivation functions."

## 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** | The key or CSP description. |
| **Storage** | Where and how the keys are stored |
| **Usage** | How the keys are used |

**Table 10: Cryptographic Keys and Critical Parameters used in FIPS-CC 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 or HMAC SHA-256 |
| 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) | Flash RAM 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 (key establishment) |
| 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 modules |
| Configuration Integrity Key | Flash RAM Plain-text | SHA-1 hash used for configuration/VPN bypass test |

**Table 10: Cryptographic Keys and Critical Parameters used in FIPS-CC Mode**

| Key or CSP | Storage | Usage |
|---|---|---|
| Configuration Encryption Key | Flash RAM<br>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<br>Plain-text | HMAC SHA-1 key used to encrypt operator passwords in the backup configuration file |
| Network User Password | Flash RAM<br>AES encrypted | Used during network user authentication |
| HA Password | Flash RAM<br>AES encrypted | Used to authenticate FortiGate units in an HA cluster |
| HA Encryption Key | Flash RAM<br>AES encrypted | Encryption of traffic between units in an HA cluster using AES |

## Alternating Bypass Feature

The primary cryptographic function of the modules is as a firewall and VPN device. The modules implement two forms of alternating bypass for VPN traffic: policy based (for IPSec and SSL VPN) and interface based (for IPSec VPN only).

### Policy Based VPN

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 according to the policy. Firewall policies with an action of allow mean that the firewall is accepting/sending plaintext data for the specified source/destination addresses.

A firewall policy with an action of accept means that the modules are operating in a bypass state for that policy. A firewall policy with an action of IPSec or SSL-VPN means that the modules are operating in a non-bypass state for that policy.

### Interface Based VPN

Interface based VPN is supported for IPSec only. A virtual interface is created and any traffic routed to the virtual interface is encrypted and sent to the VPN peer. Traffic received from the peer is decrypted. Traffic through the virtual interface is controlled using firewall policies. However, unlike policy based VPN, the action is restricted to Accept or Deny and all traffic controlled by the policy is encrypted/decrypted.

When traffic is routed over the non-virtual interfaced, the modules are operating in a bypass state. When traffic is routed over the virtual interface, the modules are operating in a non-bypass state.

In both cases, two independent actions must be taken by a CO to create bypass firewall policies: the CO must create the bypass policy and then specifically enable that policy.

## Key Archiving

The modules support key archiving to a management computer or USB token as part of a modules' configuration file backup. Operator entered keys are archived as part of the modules' 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 modules.

**Table 11: FCC Report Information**

| Module | Lab Information | FCC Report Number |
|---|---|---|
| FG-3950B | Bay Area Compliance Laboratories Corp.<br>1274 Anvilwood Ave.<br>Sunnyvale, CA 94089<br>408-732-9162<br>408-732-9164 | R10031911A |
| FG-3951B | Bay Area Compliance Laboratories Corp.<br>1274 Anvilwood Ave.<br>Sunnyvale, CA 94089<br>408-732-9162<br>408-732-9164 | R10031911A |

## Mitigation of Other Attacks

The modules include 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 modules in FIPS-CC mode and that you follow secure procedures for installation and operation of the FortiGate unit. You must ensure that:

- The FortiGate unit is configured in FIPS-CC mode.
- 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 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 modules 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 2048 bits (Group 14) are not used.
- Client side RSA certificates must use 1024 bit or greater key sizes.
- LDAP based authentication must use secure LDAP (LDAPS).
- Only approved and allowed algorithms are used (see “Algorithms” on page 14).
- The tamper evident seals are applied (see “Physical Security” on page 10).

The modules 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.

## Enabling FIPS-CC mode

To enable FIPS-CC mode, the operator must execute the following command from the Local Console:

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

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-CC mode.

Upon restart, the modules will execute self-tests to ensure the correct initialization of the modules’ cryptographic functions.

After restarting, the Crypto Officer can confirm that the modules are running in FIPS-CC mode by executing the following command from the CLI:

```
get system status
```

If the modules are running in FIPS-CC mode, the system status output will display the line:

```
FIPS-CC mode: enable
```

Note that enabling/disabling FIPS-CC mode will automatically invoke the key zeroization service. The key zeroization is performed immediately after FIPS-CC 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 modules execute the following conditional tests when the related service is invoked:

- Continuous RNG test
- Continuous NDRNG test
- RSA pairwise consistency test
- Configuration/VPN bypass test using HMAC SHA-1
- Firmware load test using RSA signatures

If any of the self-tests or conditional tests fail, the modules enter an error state as shown by the console output below:

```
Self-tests failed
Entering error mode...
The system is going down NOW !!
The system is halted.
```

All data output and cryptographic services are inhibited in the error state.

# Non-FIPS Approved Services

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

- Configuration backups using password protection
- LLTP and PPTP VPN

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