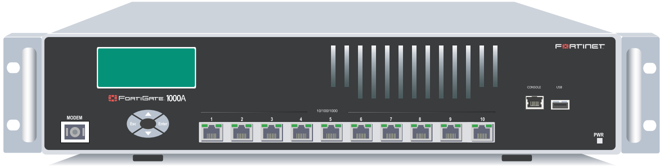
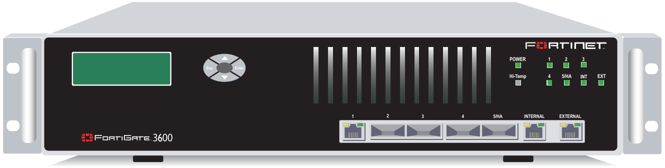
# FIPS 140-2 Security Policy

## FortiGate-1000A/3600





| *FortiGate-1000A/3600 FIPS 140-2 Security Policy* | |
|---|---|
| **Document Version:** | 2.1 |
| **Publication Date:** | June 25, 2007 |
| **Description:** | Documents FIPS 140-2 Security Policy issues, compliancy and requirements for FIPS compliant operation. |
| **Hardware Models:** | FortiGate-1000A (C4WA49)<br>FortiGate-3600 (C4KW75) |
| **Firmware Version:** | FortiOS 3.0, build8317, 061121 |

FORTINET™
www.fortinet.com

*FortiGate-1000A/3600 FIPS 140-2 Security Policy*
v2.1

June 25, 2007

01-00000-0382-20061201

**Trademarks**

**Regulatory compliance**

FCC Class A Part 15 CSA/CUS

⚠ **Caution:** If you install a battery that is not the correct type, it could explode. Dispose of used batteries according to local regulations.

# Contents

This document is a FIPS 140-2 Security Policy for Fortinet Incorporated's FortiGate-1000A and 3600 Multi-Threat Security Systems. This policy describes how the FortiGate-1000A and 3600 models (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:

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 FortiGuard Center of the Fortinet corporate website at http://www.fortinet.com/FortiGuardCenter.

## Security Level Summary

The Fortinet FortiGate-1000A and 3600 modules meet the overall requirements for a Level 2 FIPS 140-2 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 | N/A |
| Cryptographic Key Management | 3 |
| EMI/EMC | 2 |
| Self-Tests | 2 |
| Design Assurance | 3 |
| Mitigation of Other Attacks | 2 |

# FIPS-CC Mode of Operation

To operate the FortiGate modules in a FIPS compliant manner, the modules must be configured to run in the FIPS-CC mode of operation. Enabling the FIPS-CC mode of operation sets default values, disables some features and performs additional configuration procedures to meet the following requirements:

- FIPS 140-2 Level 2 as specified in Table 1.
- US Government Firewall Protection Profile for Medium Robustness Environments, Version 1.0, October 28, 2003

See "FIPS 140-2 Compliant Operation" on page 23 for complete details on configuring the modules in the FIPS-CC mode of operation.

# FortiGate Module Description

The FortiGate family spans the full range of network environments, from SOHO to service provider, offering cost effective systems for any size of 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 firewall protection, the FortiGate modules 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 Multi-Layered Security Systems 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 ICSA for firewall, IPSec VPN, SSL VPN, antivirus, and intrusion prevention functionality, the FortiGate modules deliver the highest level of security available. They provide 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, antispam 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. FortiGate modules also provide SSL VPN services.

This section contains the following information:

## 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, antispam, intrusion prevention, content filtering and traffic shaping capabilities. This FIPS 140-2 Security Policy specifically covers the firewall, IPSec and SSL-VPN capabilities of the modules.

The antivirus, antispam, intrusion prevention, 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 in order to support different network configurations:

- The FortiGate-1000A has 10 network interfaces with a status LED for each network interface (10 10/100/1000 Base-T)
- The FortiGate-3600 has 7 network interfaces with a status LED for each network interface (1 10/100 Base-T, 2 10/100/1000 Base-SX, 4 1000 Base-SC)

The modules have two x86 compatible CPUs.

The FortiGate-1000A and 3600 are 2u rackmount devices.

All of the modules have 4 external ventilation fans on the back panel of the chassis.

The FortiGate-3600 module has a fixed, internal hard drive. The FortiGate-1000A does has no hard drive.

# Cryptographic Module Ports and Interfaces

## FortiGate-1000A Module

### Figure 1: FortiGate-1000A Front and Rear Panels

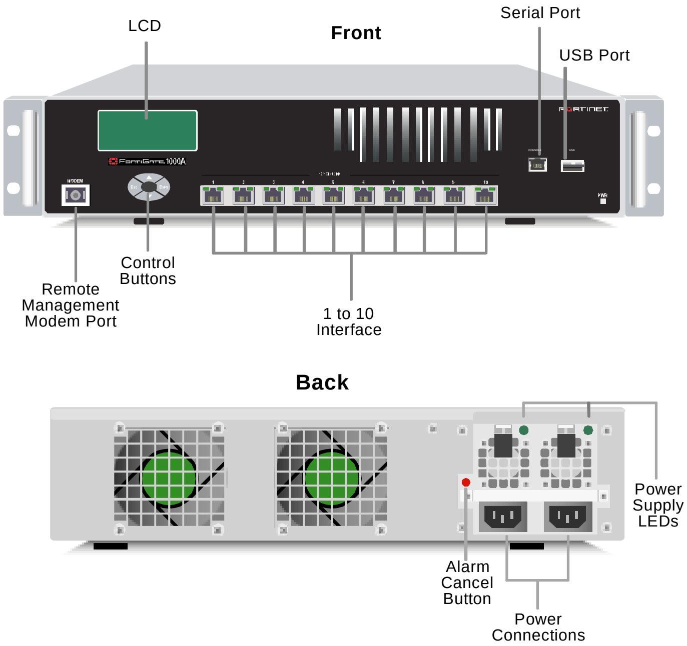


**Table 2: FortiGate-1000A Status LEDs**

| LED | State | Description |
|---|---|---|
| Power | Green | The Fortinet unit is powered on. |
| | Off | The Fortinet unit is powered off. |
| 1 to 10 Ports | Green | The correct cable is in use, and the connected equipment has power. |
| | Flashing green | Network activity at this interface. |
| | Off | No link established. |

**Table 3: FortiGate-1000A Front Panel Connectors and Ports**

| Connector | Type | Speed | Supported Logical Interfaces | Description |
|---|---|---|---|---|
| Ports 1 to 10 | RJ-45 | 1000Base-T | Data input, data output, control input and status output | Copper gigabit connection to 10/100/1000 copper networks. |
| Console Port | RJ-45 | 9600 bps | Control input, status output | Optional connection to the management computer. Provides access to the command line interface (CLI). |
| USB Port | USB | N/A | Key loading and archiving | Optional connection for FortiUSB token. |
| Modem Port | N/A | N/A | N/A | Future use. |

**Table 4: FortiGate-1000A Rear Panel Connectors and Ports**

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

## FortiGate-3600 Module

**Figure 2: FortiGate-3600 Front and Rear Panels**

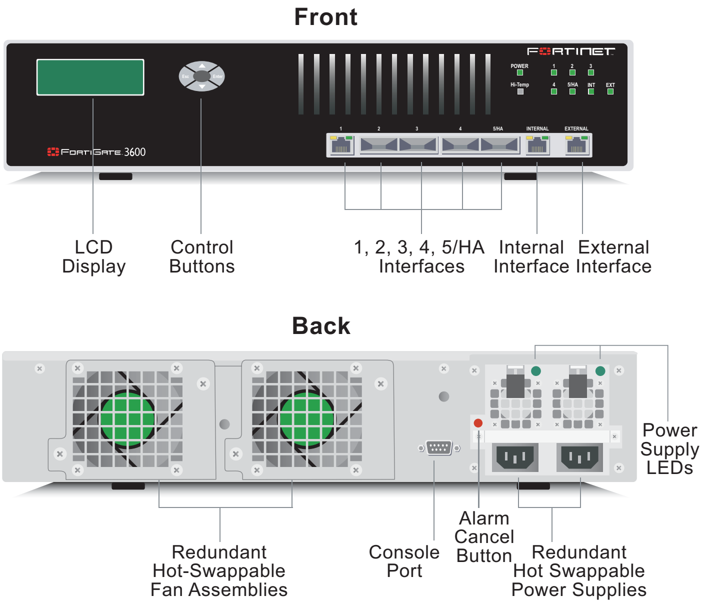


**Table 5: FortiGate-3600Status LEDs**

| LED | State | Description |
|---|---|---|
| Power | Green | The Fortinet unit is powered on. |
| | Off | The Fortinet unit is powered off. |
| 1, 2, 3, 4, 4/HA, 5/HA, INT, EXT | Green | The correct cable is in use, and the connected equipment has power. |
| | Flashing green | Network activity at this interface. |
| | Off | No link established. |
| 1, 2, 3 (Interfaces) (10/100 Interface) | Green | The correct cable is in use, and the connected equipment has power. |
| | Flashing Green | Network activity at this interface. |
| | Green | The interface is connected at 100 Mbps. |
| | Off | No link established. |
| Internal External (gigabit copper Interfaces) 4/HA (Interface) | Amber | The correct cable is in use, and the connected equipment has power. |
| | Flashing amber | Network activity at this interface. |
| | Green | The interface is connected at 1000 Mbps. |
| | Off | No link established. |

**Table 6: FortiGate-3600 Front Panel Connectors and Ports**

| Connector | Type | Speed | Supported Logical Interfaces | Description |
|---|---|---|---|---|
| Internal | SC | 1000Base-SX | Data input, data output, control input and status output | Copper gigabit connection to the internal network. |
| External | SC | 1000Base-SX | Data input, data output, control input and status output | Copper gigabit connection to the internet. |
| Port 1 | RJ-45 | 10/100Base-T | Data input, data output, control input and status output | Optional connection to a 10/100Base-T network. |
| Port 2, 3, 4 | SC | 1000 Base-SC | Data input, data output, control input and status output | Optional multimode fiber optic connections to other networks. |
| Port 5/HA | SC | 1000 Base-SC | Data input, data output, control input and status output | Optional multimode fiber optic connection to another network, or to other FortiGate-3600 units for high availability (HA). |

**Table 7: FortiGate-3600 Rear Panel Connectors and Ports**

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

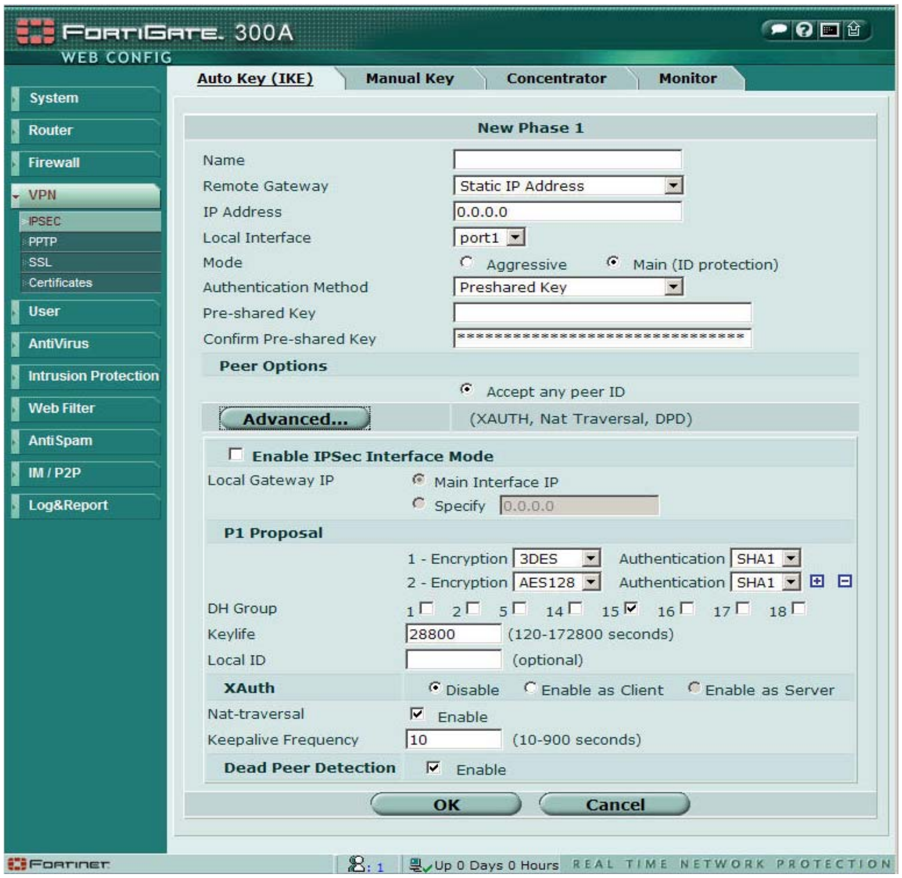
## Web-Based Manager

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

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

**Figure 3: The FortiGate web-based manager**



New Phase 1

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

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

□ Enable IPSec Interface Mode
Local Gateway IP: ● Main Interface IP ○ Specify 0.0.0.0

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

### Command Line Interface

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

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

### Control Panel and LCD

The front panel of the modules provides a control panel and an LCD. The control panel has 4 buttons. The buttons and LCD can be used to configure basic parameters such as the network 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 panel is disabled in the FIPS-CC mode of operation.

## Roles, Services and Authentication

### Roles

When configured in FIPS-CC mode, the modules provide three roles for Crypto Officers (hereafter referred to as operators): **Security Administrator**, **Crypto Administrator** and **Audit Administrator**. These roles, or combinations of these roles, are assumed by an operator after authenticating to the module remotely or through the console connection using a username/password combination.

An operator assuming the Security Administrator role has read/write access to all of the administrative functions and services of the module, including resetting or shutting down the module. An operator with the Security Administrator role can also create accounts for additional operators and assign roles to those operators. However, the Security Administrator role has read only access to crypto and audit related functions and services.

An operator assuming the Crypto Administrator role has read/write access to crypto related functions and services and read only access to all other functions and services.

An operator assuming the Audit Administrator role has read/write access to audit related functions and services and read only access to all other functions and services.

Operators can be assigned more than one role. An operator that assumes all three administrative roles has complete administrative access to the module. Multiple operator accounts can be created. Operator accounts are differentiated by the username during authentication. More than one operator can be connected to the modules at any given time, however each operator session is authenticated separately.

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.

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

The module does not provide a Maintenance role.

## FIPS Approved Services

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

The role names are abbreviated as follows:

| | |
|---|---|
| **Security Administrator** | SA |
| **Crypto Administrator** | CA |
| **Audit Administrator** | AA |
| **Network User** | NU |

**Table 8: FIPS approved services available by role via the CLI**

| Service/CSP | SA | CA | AA |
|---|---|---|---|
| authenticate to module | E | E | E |
| show system status | R | R | R |
| show FIPS mode enabled/disabled | R | R | R |
| enable/disable FIPS mode of operation | WE | N/A | N/A |
| set/reset operator passwords | WE | N/A | N/A |
| zeroize keys (execute factory reset) | E | N/A | N/A |
| execute FIPS-CC on-demand self-tests | E | N/A | N/A |
| add/delete operators | RWE | N/A | N/A |
| set/reset own password | WE | N/A | N/A |
| execute firmware download | E | N/A | N/A |
| execute system reboot | E | N/A | N/A |
| execute system shutdown | E | N/A | N/A |
| execute system diagnostics | E | N/A | N/A |
| change system time | WE | N/A | N/A |
| read/set/delete/modify system/network configuration | RWE | N/A | N/A |
| read/set/delete/modify firewall policies. enable/disable alternating bypass mode | RWE | N/A | N/A |
| read/set/delete/modify AV configuration | RWE | N/A | N/A |
| read/set/delete/modify AS configuration | RWE | N/A | N/A |
| read/set/delete/modify Web Filter configuration | RWE | N/A | N/A |
| read/set/delete/modify IM/P2P configuration | RWE | N/A | N/A |
| read/set/delete/modify VPN configuration | R | RWE | N/A |
| read/set/delete/modify IPS configuration | RWE | N/A | N/A |
| read/set/delete/modify logging/reporting configuration | R | N/A | RWE |
| manual AV/IPS signature download/update | E | N/A | N/A |

**Table 9: FIPS approved services available by role via the web-manager**

| Service/CSP | SA | CA | AA |
|---|---|---|---|
| authenticate to module | E | E | E |
| show system status | R | R | R |
| zeroize keys (execute factory reset) | E | N/A | N/A |
| add/delete operators | RWE | N/A | N/A |
| set/reset operator passwords | WE | N/A | N/A |
| execute firmware download | E | N/A | N/A |
| execute system reboot | E | N/A | N/A |
| execute system shutdown | E | N/A | N/A |
| create and download backup configuration file | WE | N/A | N/A |
| restore system configuration from backup | RWE | N/A | N/A |
| change system time | WE | N/A | N/A |
| set/reset own password | WE | N/A | N/A |
| read/set/delete/modify system/network configuration | RWE | R | R |
| read/set/delete/modify firewall policies. enable/disable alternating bypass mode | RWE | R | R |
| read/set/delete/modify AV configuration | RWE | R | R |
| read/set/delete/modify AS configuration | RWE | R | R |
| read/set/delete/modify Web Filter configuration | RWE | R | R |
| read/set/delete/modify IM/P2P configuration | RWE | R | R |
| read/set/delete/modify VPN configuration | R | RWE | R |
| read/set/delete/modify NIPS configuration | RWE | R | R |
| read/set/delete/modify logging/reporting configuration | R | R | RWE |
| manual AV/IPS signature download/update | E | N/A | N/A |

**Table 10: VPN Cryptographic Services available to Network Users**

| Service/CSP | NU |
|---|---|
| authenticate to module | RWE |
| encrypt/decrypt controlled by firewall policies | E |

## Authentication

Operators must authenticate with a user-id and password combination to access the module remotely or via the console. Remote operator authentication is done over HTTPS or SSH.

By default, Network User access to the modules is based on authentication by IP address for FQDN. Network Users can optionally be forced to authenticate to the module using a username/password combination to enable use of the encrypt/decrypt or bypass services. Network User authentication is done over HTTPS and does not allow access to the modules for administrative purposes. For Network Users invoking the SSL-VPN encrypt/decrypt services, the module supports authentication with a user-id/password combination or an RSA certificate.

The minimum password length is 8 characters when in FIPS-CC mode. Using a strong password policy, where operator or network user passwords are at least 8 characters in length and use a mix of alphanumeric (printable) characters from the ASCII character set, the odds of guessing a password are 1 in $96^8$.

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

The minimum permitted IPSec manual key size in FIPS-CC 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 an IPSec authentication key are at least 1 in $2^{128.}$ Note that a minimum modulus of 1024 bits must be used in order to operate the modules in a FIPS compliant manner.

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

The tamper seals are not applied at the factory prior to shipping. The required number of seals to secure each unit are included in the product packaging. It is the responsibility of the customer to apply the seals before use to ensure full FIPS compliance. Once the seals have been applied, the customer 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 FortiGate-1000A uses four seals to secure:

- the external enclosure
- the removable fans assemblies (two)
- the removable power supplies

The FortiGate-3600 uses 5 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-1000A and 3600 external enclosure and power supply seals**

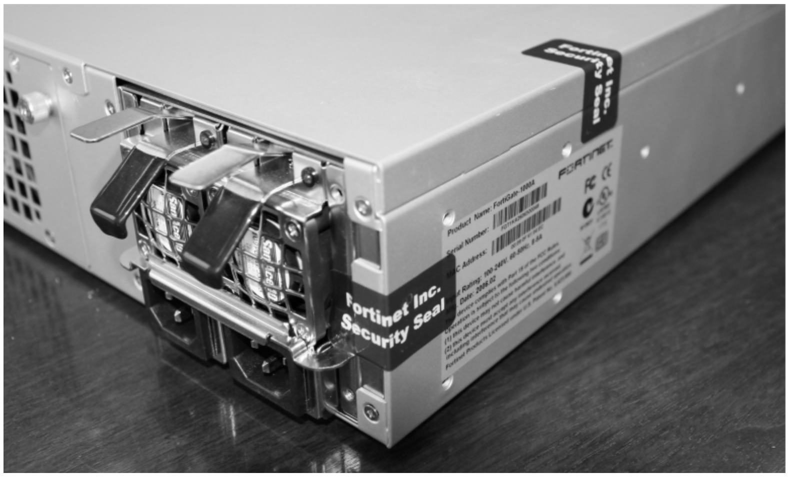

Fortinet Inc. Security Seal
Fortinet Inc. Security Seal
FORTINET
Product Name: FortiGate-1000A
Serial Number:
MAC Address:

**Figure 5: FortiGate-1000A and 3600 fan assembly seals**

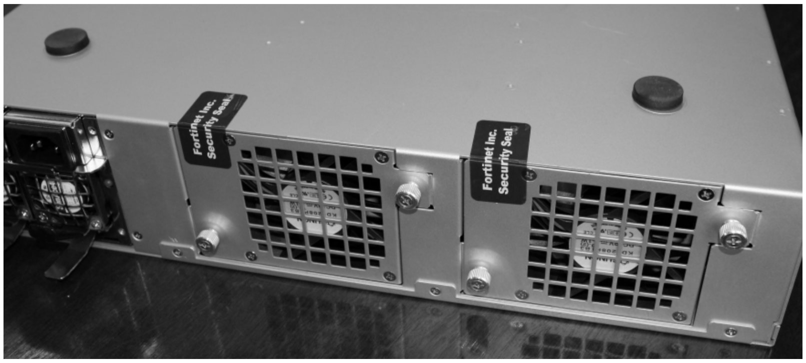
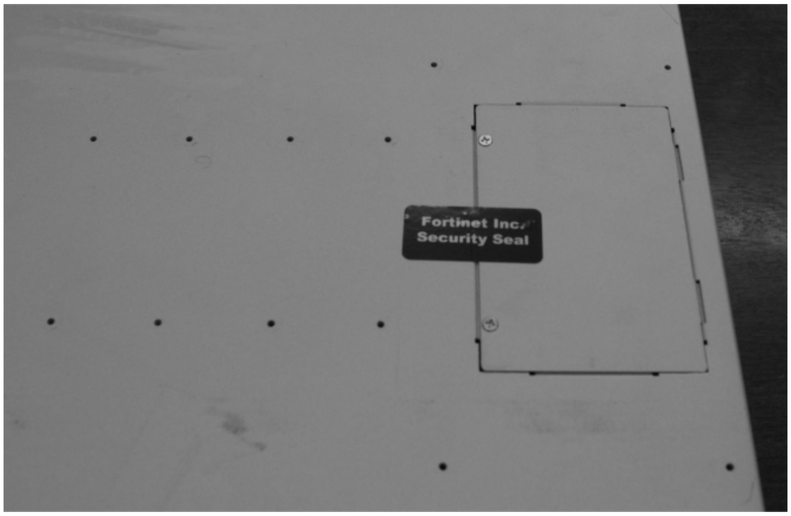


**Figure 6: FortiGate-3600 access panel seal**



## 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 ANSI X9.31 Appendix A.2.4.

### Key Zeroization

All keys and CSPs except the ANSI X9.31 RNG AES Key are zeroized when the operator executes a factory reset via the web-manager, CLI or console and when enabling or disabling the FIPS-CC mode of operation via the console. The ANSI X9.31 RNG AES Key is zeroized by executing a factory reset followed by a firmware update. See Table 13 on page 19 for a complete list of keys and CSPs.

### Algorithms

**Table 11: FIPS Approved or Allowed Algorithms**

| Algorithm | NIST Certificate Number |
|---|---|
| RNG (ANSI X9.31 Appendix A) | 251 |
| Triple-DES | 486, 487, 489, 490 |
| AES | 471, 472, 475, 476 |
| SHA-1 | 539, 540, 543, 544 |
| HMAC SHA-1 | 229, 228, 232, 233 |
| Diffie-Hellman (key agreement; key establishment methodology provides between 80 and 201 bits of encryption strength; non-compliant less than 80-bits of encryption strength) | |
| RSA ANSI X9.31 (key generation, signature generation/verification) | 193 |
| RSA PKCS1 (digital signature creation and verification, key wrapping; key establishment method provides 110 bits of encryption strength - only 2048 bit certificates are supported) | 193 |

**Table 12: Non-FIPS Approved Algorithms**

| Algorithm |
|---|
| DES (disabled in FIPS mode) |
| 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** | The key or CSP description. |
| **Storage** | Where and how the keys are stored |
| **Usage** | How the keys are used |

**Table 13: FIPS Approved Cryptographic Keys and Critical Security Parameters**

| Key or CSP | Storage | Usage |
|---|---|---|
| Diffie-Hellman Keys | SDRAM<br>Plaintext | Key agreement and key establishment |
| IPSEC Encryption Key | Flash RAM<br>AES encrypted | VPN traffic encryption/decryption using Triple-DES or AES |
| IPSEC Authentication Key | Flash RAM<br>AES encrypted | Peer-to-Peer authentication using manually entered electronic keys |
| IPSEC Session Encryption Key | SDRAM<br>Plain-text | VPN traffic encryption/decryption using Triple-DES or AES |
| IKE Pre-Shared Key | Flash RAM<br>AES encrypted | Used to generate IKE session encryption key and authentication key |
| IKE Authentication Key | SDRAM<br>Plain-text | IKE peer-to-peer authentication using HMAC SHA-1 (SKEYID_A) |
| IKE Key Generation Key | SDRAM<br>Plain-text | IPSEC SA keying material (SKEYID_D) |
| IKE Session Encryption Key | SDRAM<br>Plain-text | Encryption of IKE peer-to-peer key negotiation using Triple-DES or AES (SKEYID_E) |
| IKE RSA Key | Flash Ram<br>Plain text | IKE peer-to-peer authentication using X.509 certificates |
| HA Password | Flash RAM<br>SHA-1 hash | Used to authenticate FortiGate units in an HA cluster |
| HA Encryption Key | Flash RAM<br>AES encrypted | Encryption of traffic between modules in an HA cluster using AES |
| Firmware Integrity Key | Flash RAM<br>Plain-text | Verify integrity of firmware during self-test using HMAC SHA-1 |
| VPN Bypass Key | Flash RAM<br>Plain-text | Verify integrity of VPN table during self-tests (bypass test) using HMAC SHA-1 |
| ANSI X9.31 RNG AES Key | Flash RAM<br>Plain-text | Static AES key used with ANSI X9.31 RNG |
| Firmware Download Public Key | Flash RAM<br>Plain-text | Verification of firmware integrity for download of new firmware versions using RSA public key |
| TLS/SSH/SSL-VPN Server/Host Key | Flash RAM<br>Plain-text | Remote Web manager and CLI authentication using HMAC SHA-1. Also used for encrypting TLS session key using RSA method. |
| TLS Session Key | SDRAM<br>Plain-text | Remote Web manager session encryption and authentication using AES or Triple-DES |

**Table 13: FIPS Approved Cryptographic Keys and Critical Security Parameters**

| Key or CSP | Storage | Usage |
|---|---|---|
| SSH Session Key | SDRAM<br>Plain-text | Remote CLI session encryption and authentication using AES or Triple-DES |
| SSL-VPN Session Key | SDRAM<br>Plain-text | SSL-VPN session encryption and authentication using AES or Triple-DES |
| Operator Username | Flash RAM<br>Plain-text | Used during operator authentication to identify and assign roles to operators |
| Operator Password | Flash RAM<br>SHA-1 hash | Used to authenticate operator access to the module |
| FIPS-CC Mode Key | Flash RAM<br>AES encrypted | AES key used to encrypt key CSPs stored on flash card |
| Backup Configuration Password | Flash RAM<br>AES encrypted | Used as seed to generate configuration file encryption key |
| Configuration File Encryption key | Flash RAM<br>AES encrypted | AES key used to encrypt backup configuration file |

## Alternating Bypass Feature

The primary cryptographic function of the FortiGate modules is as a firewall and VPN device. Encrypt/decrypt operations are performed on outgoing/incoming traffic based on firewall policies. Firewall policies with an action of IPSec or SSL-VPN mean that the firewall is functioning as a VPN start/end point for the specified source/destination addresses and will encrypt/decrypt traffic accordingly. Firewall policies with an action of allow mean that the firewall is accepting/sending plaintext data for the specified source/destination addresses.

The FortiGate implements an alternating bypass feature that is based on the firewall policies. A firewall policy with an action of accept is means that the module operating in a bypass state for that policy. A firewall policy with an action of IPSec or SSL-VPN means that the module is operating in a non-bypass state for that policy.

Two independent actions must be taken by an operator to create bypass firewall policies: the operator must create the bypass policy and then specifically enable that policy.

## Key Archiving

The module supports key archiving to a management computer or USB token as part of a module configuration file backup. Operator entered keys are archived as part of the module configuration file. By default, the configuration file is stored in plain text, but any keys in the configuration file keys are AES encrypted. The modules also support encrypting the entire configuration file using AES.

## Electromagnetic Interference/Electromagnetic Compatibility (EMI/EMC)

The modules comply with EMI/EMC requirements 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 14: FCC Report Information**

| Module | Lab Information | FCC Report Number |
|---|---|---|
| FG-1000A | Compliance Certification Services Inc.<br>Hsintien Lab<br>No. 165, Chunghsen Road, Hsintien City<br>Taipei Hsien, Taiwan<br>(02) 2217-0894 | 51118201-F |
| FG-3600 | BACL Corp<br>230 Commercial Street<br>Sunnyvale, CA 94085<br>(408) 732-9162 | R0309152 |

## Mitigation of Other Attacks

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

The FortiGate NIPS has two components: a signature based component for detecting attacks passing through the FortiGate module 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.

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 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.

FortiGate 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.

FortiGate web filtering can be configured to provide web (HTTP) content filtering. FortiGate web filtering uses methods such as banned words, address block/exempt lists, and the FortiGuard managed content service.

Whenever a NIPS, antivirus, antispam or filtering event occurs, the module can record the event in the log and/or send an alert email to an operator.

The rest of this section provides additional information on the NIPS, antivirus, antispam and web and email filtering capabilities of the FortiGate modules and the FortiGuard Service. For complete information refer to the FortiGate Installation Guide for the specific module in question, the FortiGate Administration Guide, and the FortiGate IPS Guide.

This section contains the following information:

## NIPS Signature Protection

The FortiGate NIPS can detect a wide variety of suspicious network traffic and network-based attacks aimed at systems behind the FortiGate module. Attack signatures are the core of the FortiGate NIPS signature protection component. 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 FortiGuard server, or they can be downloaded manually by the operator.

Downloading updated IPS signatures or an updated IPS engine makes no changes to the configuration or basic operation of the modules. Verification of the IPS download package is done using RSA. The IPS package is signed with the FortiGuard server's private key and verified by the FortiGuard module using the FortiGuard server's private key.

User defined attack signatures are also supported.

## NIPS Attack Protection

The FortiGate NIPS can also protect the module itself from direct attacks, such as TCP, ICMP, UDP, and IP attacks. Access is denied or packets are dropped when an attack is detected. Attack parameters can be modified by the operator to ensure that normal network traffic is not considered an attack.

## Antivirus Protection

FortiGate antivirus protection scans for infected files in the protocols for which antivirus protection as been enabled. Supported protocols include HTTP, FTP, SMTP, POP3, IMAP, and IM. 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 also be configured to quarantine blocked or infected files. The quarantined files are stored on the module's hard disk. An operator can delete quarantined files from the hard disk or download them. Downloaded quarantine files can be submitted to the FortiGuard Center as a virus sample. FortiGate antivirus protection is transparent to the end user.

Downloading updated AV signatures or an updated AV engine makes no changes to the configuration or basic operation of the modules. Verification of the AV download package is done using RSA. The AV package is signed with the FortiGuard server's private key and verified by the FortiGuard module using the FortiGuard server's private key.

FortiGate antivirus protection also detects and removes grayware such as adware, spyware, etc.

## Antispam Protection

FortiGuard antispam protection can detect spam in SMTP, POP3 or IMAP traffic. Spam email is tagged or discarded. Spam detection methods include banned words, black/white lists, return email DNS check and the FortiGuard antispam service. The FortiGuard Antispam Service provides IP checking, URI address checking and email checksum analysis.

To prevent unintentional tagging of email from legitimate senders, an operator can add sender address patterns to an exempt list that overrides the email block and banned word lists.

## Web Filtering

FortiGate web filtering can be configured to scan HTTP protocol streams for banned URLs or web page content. Web filtering methods include banned words, URLs and the FortiGuard web filtering service. The FortiGuard web filtering service is a managed service that uses a database of URLs to block access to banned web sites and URLs based on content categories. If a match is found between a URL in the URL block list, the FortiGuard web filtering service, or if a web page is found to contain a word or phrase in the content block list, the FortiGate module blocks the web page. The blocked web page is replaced with a message that an operator can edit using the web-based manager.

An operator 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, an operator can add URLs to an Exempt List that overrides the URL blocking and content blocking.

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.

## FortiGuard Services

The FortiGuard services are a family of managed services available to Fortinet customers. The FortiGuard services include:

- IPS signature and engine updates
- AV signature and engine updates
- A managed antispam service
- A managed web filtering service
- Firmware updates

Customers can purchase FortiGuard services for their FortiGate units on a yearly basis. Use of the FortiGuard services is optional, but recommended.

# FIPS 140-2 Compliant Operation

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

This section contains the following information:

## Overview of FIPS 140-2 compliant operation

FIPS 140-2 compliant operation requires both that you use the FortiGate Multi-Threat Security System in its 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 installed in a secure physical location.
- Physical access to the FortiGate unit is restricted to authorized operators.
- Administrative passwords are at least 8 characters long.
- Administrative passwords are changed regularly.
- Administrator account passwords must have the following characteristics:
  - One (or more) of the characters should be capitalized.
  - One (or more) of the characters should be numeric.
  - One (or more) of the characters should be non alpha-numeric (e.g. punctuation mark).
- Administration of the FortiGate unit is permitted using only certified administrative methods. These are:
  - console connection
  - web-based manager via HTTPS
  - command line interface (CLI) access via SSH
- The FortiGate unit can be used in either of its two operation modes: NAT/Route or Transparent. NAT/Route mode applies security features between two or more different networks (for example, between a private network and the Internet). Transparent mode applies security features at any point in a network. The current operation mode is displayed on the web-based manager Status page and in the output of the `get system status` CLI command. Also, on LCD-equipped units, Transparent mode is indicated by “FIPS-CC-TP” and NAT/Route by “FIPS-CC-NAT” on the LCD display.

### Initial Inspection of the Modules

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

### Applying the Security Seals

After completing the initial inspection of the modules the SO must apply the security seals as explained in the section “Physical Security” on page 16 to ensure full compliance with the FIPS 140-2 standard.

## Initial configuration of the FortiGate unit

This section describes how to configure your FortiGate unit in the FIPS-CC mode of operation. Proceed as follows:

- Install the unit following the procedures in the documentation.
- Register your FortiGate unit with Fortinet.
- If you are upgrading an existing FortiGate unit to FIPS-CC firmware, download the appropriate firmware from Fortinet and install it on your unit.
- Verify the firmware version of your FortiGate unit.
- Enable FIPS-CC mode.

### Verifying the hardware version of the unit

Check the label on the back or underside of the unit to determine the hardware version. Match the first 6 characters of the hardware version to the FIPS validated hardware versions listed in Table 15.

**Table 15: FIPS 140-2 validated hardware versions**

| FortiGate Model | Hardware Version |
|---|---|
| FG-1000A | C4WA49 |
| FG-3600 | C4KW75 |

### Installing the unit

Both the *Quick Start Guide* and the Getting Started section of the *Installation Guide* for your FortiGate unit provide instructions on the physical installation and initial configuration of your unit. When you have completed these procedures you will be able to access both the web-based manager and Command Line Interface (CLI).

### Registering the unit

For information about registering your FortiGate unit, see “Registering a FortiGate unit” in the System Maintenance chapter of the *Administration Guide* for your unit. You need the user name and password Fortinet provides to you to download the FIPS-CC compliant firmware.

### Downloading and installing FIPS-CC compliant firmware

Unless you received a FortiGate unit with FIPS-CC firmware pre-installed, you need to download and install the appropriate firmware for your FortiGate unit. The firmware files can be obtained from the Fortinet support site after registering your unit. The firmware build information and firmware files for each model are listed in Table 16 and Table 17. Note that the chassis component of the modules do not require firmware.

**Table 16: Firmware builds for validated FortiGate models**

| FortiGate Model | Firmware Build |
|---|---|
| FG-1000A | FortiOS 3.0, build8317, 061121 |
| FG-3600 | FortiOS 3.0, build8317, 061121 |

**Table 17: Firmware files for validated FortiGate models**

| FortiGate Model | Firmware File |
|---|---|
| FG-1000A | FGT_1000A-v300-build8317-fips_cc_lr.out |
| FG-3600 | FGT_3600-v300-build8317-fips_cc_lr.out |

#### To download the firmware

1. Determine the appropriate firmware version from Table 16.
2. Determine the appropriate firmware file from Table 17.
3. With your web browser, go to https://support.fortinet.com and log in using the name and password you received when you registered with Fortinet Support.
4. Navigate to the v3.00 FIPS-CC certified firmware page for the FortiGate product. Select the firmware build(s) you need and save the file on the management computer or on your network where it is accessible from the FortiGate unit.

## Installing the FIPS-CC firmware

You install the FIPS-CC compliant firmware as an upgrade from the standard firmware.

#### To install the FIPS-CC firmware

1. Using the management computer, connect to the unit’s web-based manager. See the *Quick Start Guide* or the *Installation Guide* for information.
2. Type admin in the name field. If you have assigned a password, type it in the Password field. Select Login.
3. Go to **System > Status**.
4. Under System Information > Firmware version, select Update.
5. Type the path and filename of the firmware image file, or select Browse and locate the file.
6. Select OK.

   The unit uploads the firmware image file, upgrades to the new firmware version, restarts, and displays the Login page. This process takes a few minutes.

## Verifying the firmware version of the unit

Execute the following command from the command line:

```
get system status
```

The version line of the status display shows the FortiGate model number, firmware version, build number and date:

```
Version:Fortigate-1000A 3.00,build8317,061121
```

Verify that your firmware version, build number and date match those shown above for your specific model.

## Enabling FIPS-CC mode

If you have verified the firmware version, you are ready to enable FIPS-CC mode. As part of enabling FIPS-CC mode, you must define administrator account names and passwords. The default admin account is not available in FIPS-CC mode. You must use a console connection to enable FIPS-CC mode. If you try to use another type of connection, a “check permission failed” error occurs.

**Note:** When you enable FIPS-CC mode, all of the existing configuration is lost.

To enable FIPS-CC mode

1 Log in to the CLI and enter the following commands:

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

2 In response to the following prompt, enter the account name for the Security Administrator:

```
Please enter SECURITY administrator name:
```

3 In response to the following prompt, enter the password for the Security Administrator:

```
Please enter SECURITY administrator password:
```

4 When prompted, re-enter the Security Administrator password.

5 In response to the following prompt, enter the account name for the Audit Administrator:

```
Please enter AUDIT administrator name:
```

If you want the Security Administrator to also act as the Audit Administrator, enter the Security Administrator account name you defined in step 2. There will be no prompt for a password. (Skip step 6.)

6 In response to the following prompt, enter the password for the Audit Administrator:

```
Please enter AUDIT administrator password:
```

7 When prompted, re-enter the Audit Administrator password.

8 In response to the following prompt, enter the account name for the Crypto Administrator:

```
Please enter CRYPTO administrator name:CryptoAdmin
```

If you want the Security Administrator to also act as the Crypto Administrator, enter the Security Administrator account name you defined in step 2. There will be no prompt for a password. (Skip step 9.)

9 In response to the following prompt, enter the password for the Cryptographic Administrator:

```
Please enter CRYPTO administrator password:
```

10 When prompted, re-enter the Crypto Administrator password.

The CLI displays the following message:

```
Warning: most configuration will be lost,
do you want to continue? (y/n)
```

**11** Enter y.

The FortiGate unit restarts and runs in FIPS-CC compliant mode.

### FIPS-CC mode status indicators

There are two status indicators that show whether the FortiGate unit is running in the FIPS 140-2 and Common Criteria compliant mode of operation:

**Table 18: FIPS-CC mode status indicators**

| Location | Indication |
|---|---|
| Front panel LCD | FIPS-CC-NAT or FIPS-CC-TP |
| Output of `get system status` command | FIPS-CC mode: enable |

## 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)
- 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 modules execute the following conditional tests when the related service is invoked:

- Continuous RNG test
- RSA pairwise consistency 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 **execute fips <test>** CLI command.

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

```
Initializing firewall...

System is started.
```

```
FIPS-CC mode: Starting self-tests.
Running AES test...                           passed
Running 3DES test...                          passed
Running SHA1 HMAC test...                     passed
Running RSA 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-1000A # execute fips kat all
Starting self-tests
Running AEStest...       passed
Running 3DES test...      passed
Running SHA1 HMAC test... passed
Running RSA test...       passed
Running RNG test...       passed
Self-tests passed
```

## Effects of FIPS-CC compliant mode

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

- All previous configuration settings except the network interface settings are lost. If HTTP or Telnet administrative access was enabled on any interfaces, it is disabled.
- The FortiGate unit front panel LCD displays “FIPS-CC-” followed by the operation mode, “NAT” or “TP”. You might have to press an LCD panel key to see this display.
- The `get system status` CLI command display includes “FIPS-CC mode: enable”.
- Logging is enabled by default for:
  - new firewall policies
  - interfaces where administrative access is enabled
  - failed connection attempts to the FortiGate unit using TCP/IP ports other than 22 (ssh), 23 (telnet), 80 (HTTP), and 443 (HTTPS).
  - all configuration changes
  - configuration failures
  - remote IP lockout due to reaching maximum number of failed login attempts
  - log viewing
  - interface going up or down
- Disk logging is enabled.
- Reaching 95% of the log disk storage capacity results in the FortiGate unit entering an error mode that shuts down all of the interfaces until the administrator intervenes.
- Anomaly detection and protection is applied to traffic addressed to the FortiGate unit.

- TFTP communication is not permitted. It is not secure. In non-FIPS-CC operation this can be used for remote configuration backup.
- SNMP services are disabled.
- Remote access clients must meet security requirements. See "Remote access requirements" on page 30.
- All firewall policies are removed.
- All administrators must accept a disclaimer statement at logon. This disclaimer is configured in the Post Login replacement message.
- The FortiGate unit performs self-tests at startup. Also, the administrator can run some self-tests at any time. If any of these tests fail, the unit goes into error mode and shuts down.
- There is an alarm capability. See "Alarms" on page 41.
- The DES and MD5 algorithms are not available for VPN configurations.
- Diffie-Hellman groups 14 through 18 are available to VPN configurations and group 15 is the default. DH groups 15 through 18 use 3072 to 8192-bit keys. You should use these groups for FIPS-CC complaint VPNs between FortiGate units. Current versions of the FortiClient Host Security application support only DH groups 1, 2 and 5.
- ANSI X9.31 RSA signature is an optional authentication method for IPSec VPNs. This method is supported only on FortiGate units in FIPS-CC mode.
- When configuring passwords, the FortiGate unit requires you to enter the password a second time as confirmation.
- Configuration backups use Triple-DES encryption with a HMAC-SHA1 checksum and a user-defined password. It is not possible to use a FIPS-CC backup file if you take the FortiGate unit out of FIPS-CC mode. If you re-enable FIPS-CC mode, the seed key used in the encryption changes.
- In HA mode, HA heartbeat data is encrypted.
- Blocking of spoofed TCP RST packets is enabled by default.
- On a CLI session, when an administrator logs out or the session times out, the FortiGate unit sends 100 carriage return characters to clear the screen.

## Remote access requirements

In FIPS-CC mode, remote administration is not allowed via HTTP or Telnet, which are not secure. SSH and HTTPS access are permitted but must meet certain security requirements.

### Setting minimum DH primes size

By default, in FIPS-CC mode the FortiGate unit requires values at least 3072 bits long to be used in the Diffie-Hellman key exchange when an HTTPS session begins. Using the CLI, you can set this minimum to any of the safe standard values specified in RFC 3526: 1024, 1536, 2048, 3072, 4096, 6144 or 8192 bits. For example, to use commercially available browsers, you might need to set the key size to 1024, as follows:

```
config system global
    set dh-params 1024
  end
```

### SSH client requirements

To access the CLI through network interfaces in FIPS-CC mode, your SSH client must support the following:

Authentication:

- HMAC SHA-1

Encryption:

- AES256

### Web browser requirements

To use the web-based manager in FIPS-CC mode, your web browser application must meet the following requirements:

- Authentication algorithm:
  - RSA X9.31
  - PKCS1 RSA
- Connection security:
  - TLS 1.0

#### Enabling administrative access

In FIPS-CC mode, the network interfaces by default do not allow administrative access, preventing you from using the web-based manager. You can re-enable use of the web-based manager using CLI commands on the console. This example enables HTTPS administrative access on the Internal interface to allow use of the web-based manager:

```
config system interface
  edit internal
    set allowaccess https
  end
```

For detailed information about accessing the web-based manager, see “Connecting to the web-based manager” in the *Installation Guide* for your unit.

## Disabling FIPS-CC mode

The only way that you can return the FortiGate unit to the normal mode of operation is to restore the factory default configuration. Enter the following CLI command:

```
execute factoryreset
```

Disabling FIPS-CC mode erases the current configuration.

# Administration

FIPS-CC mode enforces predefined administrator roles instead of the more granular selection access permissions allowed in the non-FIPS-CC mode of operation. Also, by default, administrator logon requires acceptance of a disclaimer statement.

This section contains the following information:

## Administrator roles

In FIPS-CC mode, access profiles for administrators are configured only in terms of administrator roles. There are three administrator roles. All have read access to the entire configuration. They can modify the configuration as follows:

| **Administrator role** | **can modify** |
|---|---|
| **Security administrator** | all except VPN settings and log data (cannot delete logs) |
| **Audit administrator** | log data (can delete logs) but cannot change log settings |
| **Crypto administrator** | VPN settings |

## Administrator accounts and profiles

When you invoke FIPS-CC mode for the first time, the FortiGate unit prompts you for a name and password to create an administrator account for each role. You can, as an alternative, assign the Security administrator account all three roles.

After the initial configuration of administrators when you enable FIPS-CC mode, you can modify administrators and administrator profiles through the web-based manager or the CLI.

In FIPS-CC mode, the FortiGate unit has three preconfigured access profiles, that you can edit, but not delete:

**Table 19: Default administrator access profiles**

| Access profile | Default administrator role |
|---|---|
| def_prof_SA | Security Administrator Role |
| def_prof_AA | Audit Administrator Role |
| def_prof_CA | Crypto Administrator Role |
| def_prof_SA_AA | Security/Audit Administrator Role |
| def_prof_SA_CA | Security/Crypto Administrator Role |
| def_prof_AA_CA | Audit/Crypto Administrator Role |
| def_prof_SA_AA_CA | Security/Audit/Crypto Administrator Role |

You can create additional access profiles and enable one or more administrator roles for them. You can create additional administrators and assign them to any of the access profiles.

If, when enabling FIPS-CC mode, you chose to use the SA account name for the AA and/or CA account names, only the applicable default profiles will be created. For example, if you used the SA account name for both the AA and CA account names, only the def_prof_SA_AA_CA access profile will be created.

## Enabling multiple virtual domain configuration

The FortiGate unit can operate multiple virtual domains (VDOMs). VDOMs enable a FortiGate unit to function as multiple independent units. For more information, see the “Using virtual domains” chapter of the *FortiGate Administration Guide*.

Before you can enable virtual domain operation, you must make at least one of your administrators a VDOM administrator using the CLI. For example, to make the “SecAdmin” administrator a VDOM admin, enter the following command:

```
config sys admin
  edit cc_admin
    set is-admin 1
end
```

To enable multiple VDOM operation in the web-based manager, go to System > Admin > Settings, select Virtual Domain Configuration, and then select Apply. To enable multiple VDOM operation using the CLI, enter the following command:

```
config system global
  set vdom-admin enable
end
```

## Disclaimer access banner

By default, in FIPS-CC mode, each time you log on as an administrator, you see a warning statement that usage is monitored and that unauthorized usage can result in disciplinary or legal action. You must accept the statement to continue. If you decline the statement, you are immediately logged out. Logs record response to the disclaimer at each logon.

You can disable the disclaimer in the CLI as follows:

```
config system global
  set access-banner disable
end
```

Similarly, you can enable the disclaimer, like this:

```
config system global
  set access-banner enable
end
```

You can modify the disclaimer to meet the requirements of your organization. The disclaimer is an editable replacement message called “Post login”. See “Replacement messages” in the System Config chapter of the FortiGate Administration Guide.

## Using custom administrator access keys (certificates)

You can upload VPN certificates to use as custom RSA keys to authenticate administrators. To do this, you must upload the signed public certificate to the FortiGate unit. If the private key was not generated on the FortiGate unit, it also must be uploaded. Certificates must have a modulus of at least 2048 bits.

### Importing the custom RSA key

In FIPS-CC mode, you cannot import certificates using TFTP. You must use a USB storage device instead. Put the files you want to upload on the device and connect the device to the FortiGate unit. Use one of the following commands to import the files:

If you have a PKCS12 format key-certificate file,

```
execute vpn certificate local import pkcs12 <file_name>
  <password>
```

If you have separate certificate and key files,

```
execute vpn certificate local import cert <cert_file_name>
  <key_file_name><password_for_key_file>
```

Each command is a single line.

### Enabling the custom RSA key

To enable the custom RSA key you imported, use the following CLI command:

```
config system global
  set admin-server-cert admin-cert
end
```

This applies to both HTTPS and SSH connections.

### Enabling RSA X9.31 signatures

By default, ANSI X9.31 signatures are required for administrative access. This requires the administrator to use a web browser or SSH client that supports this feature. To use a browser or SSH client that does not support X9.31 signatures, disable the X9.31 support as follows:

```
config system global
  set rsa-x931 disable
end
```

Disabling X9.31 support means that the modules will use PKCS1 instead.

## Configuration backup

Configuration backup files created in FIPS-CC mode are not compatible with backup files created in non-FIPS-CC mode. Also, a FIPS-CC backup file is not usable after you exit and then re-enter FIPS-CC mode because its checksum is based on a seed value calculated when you start FIPS-CC mode.

# Logging

The FIPS-CC mode of operation enforces logging of all traffic and system events. The severity threshold for logging is set to the lowest level: debug. This ensures that the maximum amount of information is logged.

This section contains the following information:

- Default log settings
- Excluding specific logs

- Viewing log messages from the web-based manager
- Viewing log messages from the CLI
- Backing up log messages
- Viewing log file information
- Deleting filtered log messages
- Deleting rolled log files

## Default log settings

Logs are written to the FortiGate unit hard disk. The FortiGate unit generates warning log entries when the disk space allocated for logging is filled to 75%, then 90% and finally 95% of capacity. When logs exceed 95% of capacity, the default action is to block further traffic and switch to Error mode. See “Clearing Error mode” on page 43 for more information.

Logging to external devices is disabled due to the security requirements of FIPS-CC operation, except for downloading of logs to the management computer. See “Backing up log messages” on page 39.

Table 21 lists the disk logging settings required for FIPS-CC mode. If you change these options from the default, the operation of your FortiGate unit is no longer FIPS-CC compliant.

**Table 20: config log disk filter command keywords and variables**

| Keywords and variables | Description | Default |
|---|---|---|
| `admin {disable \| enable}` | Enable or disable logging all administrative events, such as user logins, resets, and configuration updates in the event log. This is available only if `event` is set to `enable`. | `enable` |
| `allowed {disable \| enable}` | Enable or disable logging all traffic that is allowed according to the firewall policy settings in the traffic log. This is available only if `traffic` is set to `enable`. | `enable` |
| `auth {disable \| enable}` | Enable or disable logging all firewall-related events, such as user authentication in the event log. This is available only if `event` is set to `enable`. | `enable` |
| `event {disable \| enable}` | Enable or disable the event log. | `enable` |
| `severity {alert \| critical \| debug \| emergency \| error \| information \| notification \| warning}` | Select the logging severity level. The FortiGate unit logs all messages at and above the logging severity level you select. For example, if you select `error`, the unit logs `error`, `critical`, `alert` and `emergency` level messages.<br>`emergency` - The system is unusable.<br>`alert` - Immediate action is required.<br>`critical` - Functionality is affected.<br>`error` - An erroneous condition exists and functionality is probably affected.<br>`warning` - Functionality might be affected.<br>`notification` - Information about normal events.<br>`information` - General information about system operations.<br>`debug` - Information used for diagnosing or debugging the FotiGate unit. | `debug` |
| `system {disable \| enable}` | Enable or disable logging of all system-related events, such as ping server failure and gateway status, in the event log. This is available only if `event` is set to `enable`. | `enable` |
| `traffic {disable \| enable}` | Enable or disable the traffic log. | `enable` |
| `violation {disable \| enable}` | Enable or disable logging of all traffic that violates the firewall policy settings in the traffic log. This is available only if `traffic` is set to `enable`. | `enable` |

**Table 21: config log disk setting command keywords and variables**

| Keywords and variables | Description | Default |
|---|---|---|
| `diskfull {blocktraffic \| nolog \| overwrite}` | Enter the action to take when the log disk is full. | blocktraffic |

## Excluding specific logs

Use the exclude-list option of the log filtering command to define log entries that will not be recorded:

```
config log disk filter
  config exclude-list
    edit <number>
      set category <category>
      config fields
        edit <field_name>
          set args <argvalue>
          set negate {enable | disable}
        end
      end
    end
  end
end
```

**Table 22: log filter exclude-list command keywords and variables**

| Keywords and variables | Description | Default |
|---|---|---|
| `category <category>` | `category` is one of:<br>`attack`, `content`, `event`, `im`, `spam`, `traffic`, `virus`, `webfilter` | No default. |
| `edit <field_name>` | Enter the name of the field on which to base exclusion. Available `field_name` values depend on the category setting. If you enter an invalid field name, valid field names are listed. | No default. |
| `args <argvalue>` | Enter the field value to match. | No default. |
| `negate {enable \| disable}` | Enable to exclude logs where the value of the `<field_name>` field does not match `<argvalue>`.<br>Disable to exclude logs where the value of the `<field_name>` field matches `<argvalue>`. | disable |

## Viewing log messages from the web-based manager

To view log messages from the web-based manager, go to Log & Report > Log Access. For detailed instructions about viewing the logs, consult the online Help system or see the Log & Report chapter of the *FortiGate Administration Guide*.

## Viewing log messages from the CLI

You can view and clear log messages from the CLI. Before viewing logs, you must set filter options to select the logs that you want to view. You can view one log category on one device at a time. Optionally, you can filter the listing to show only specified date ranges or severities of log messages. For traffic logs, you can filter log messages by source or destination IP address.

### Setting filtering for log messages

Use `execute log filter` commands to select which logs to display with the `execute log display` command. Commands are cumulative. Enter `execute log filter list` to see the current settings. For more information about log filtering, see the FortiGate CLI Reference.

The command syntax is:

```
execute log filter <keyword> <variable>
```

**Table 23: execute log filter command keywords and variables**

| Keywords and variables | Description | Default |
|---|---|---|
| `category {event \| ids \| spam \| traffic \| virus \| webfilter \| list }` | Type of log, except `list`, which displays the current setting. | `event` |
| `device {disk \| memory \| list}` | Device where the logs are stored, except `list`, which displays the current setting. | `disk` |
| `field <field_name>` | Filter on log field. Use ? as `field_name` to see a list of valid fields. | No default. |
| `lines-per-view <number>` | Set lines per view. Range: 5 to 1000 | 10 |
| `list` | Display current filter settings. | No default. |
| `reset` | Reset filter settings. | No default. |
| `rolled-number <number>` | Select logs from rolled log files. 0 selects current log file. | 0 |
| `sortby` | Set display order. See "Sorting log messages" on page 38. | No default. |
| `start_line <integer>` | Select first line of logs to display. | 1 |

Use as many `execute log filter` commands as you need to define the log messages that you want to view. For example, to select the memory event logs from 10-14 July 2006, you use the following commands:

```
execute log filter category event
execute log filter device memory
execute log filter field date 2006-07-10 2006-07-14
```

## Sorting log messages

In addition to selecting logs to display, the `execute log filter` command can sort logs by field.

```
execute log filter sortby <field_name>
```

Enter the command without a field name to see a list of valid field names.

## Viewing log messages

After you have selected the log messages that you want to view using the `execute log filter` command, you can display them with the following command:

```
execute log display
```

The console displays the first 10 log messages. To view more messages, run the command again. You can do this until you have seen all of the selected log messages. To restart viewing the list from the beginning, use the commands

```
execute log filter start_line 1
execute log display
```

## Resetting log filters

You can restore the log filters to their default values using the command

```
execute log reset
```

## Backing up log messages

You can back up log messages to your Administrative computer or other computer on the network.

### Backing up log messages using the web-based manager

The FortiGate unit downloads log files to the Administrative computer using HTTPS.

1. Go to **Log & Report > Log Access**.
2. Select either the Disk or Memory tab as appropriate.
3. From the Log Type list, select the type of log you want to back up.
4. Select the download icon for the log file you want to back up.
5. Select either Download file in the normal format or Download file in CSV format, as appropriate.
6. Follow your browser's procedure for saving the downloaded file.

### Backing up log messages using the CLI

You can back up logs from the CLI only if you re-enable TFTP communication which is disabled by default in FIPS-CC mode. Enter the following command:

```
config system global
  set tftp enable
end
```

Using the CLI, you can back up selected log types or perform an all-logs backup that includes logs that have rolled over.

**To back up log messages using the CLI**

1. Install a TFTP server on the computer in the directory where you want to receive the log files.
2. Use a crossover cable to connect the computer to the appropriate network interface. On models 800 and below, connect to the Internal interface; on other models, connect to port 1.
3. Start the TFTP server.
4. Connect to the CLI interface.
5. To back up all log messages, execute the following command:

   ```
   execute backup alllogs <tftp_server_ip_address>
   ```

   To back up only a specific log type, execute the following command:

   ```
   execute backup log <tftp_server_ip_address> <log_type>
   ```

   `<log_type>` can be one of: `traffic`, `event`, `ids`, `virus`, `webfilter` or `spam`.

   The FortiGate unit reports each transferred file as follows:

```
Connect to tftp server 192.168.1.1 ...
Please wait...
##Sent log file /var/log/tlog to tftp server as
tlog_20041014_080007 OK.
```

## Viewing log file information

You can view the list of current and rolled log files on the console. The list shows the file name, size and timestamp. The CLI command is as follows:

```
execute log list <category>
```

`<category>` must be one of: `event`, `ids`, `spam`, `traffic`, `virus` or `webfilter`.

The output looks like this:

```
elog                     8704    Fri Jan 28 14:24:35 2005
elog.1                   1536    Thu Jan 27 18:02:51 2005
elog.2                  35840    Wed Jan 26 22:22:47 2005
```

At the end of the list the total number of files in the category is displayed. For example:

```
501 event log file(s) found.
```

## Deleting filtered log messages

You can select log messages with the `execute log filter` command and then delete them with the command:

```
execute log delete-filtered
```

For example, to delete all the traffic logs, enter the following commands:

```
execute log filter category traffic
```

```
execute log delete-filtered
```

For information about the `execute log filter` command, see "Setting filtering for log messages" on page 37.

## Deleting rolled log files

You can delete rolled log files using the `execute log delete-rolled` command:

execute log delete-rolled <category> <start> [<end>]

`<category>` must be one of: `event`, `ids`, `spam`, `traffic`, `virus` or `webfilter`. The `<start>` and `<end>` values represent the range of log files to delete. If `<end>` is not specified, only the log number specified by `<start>` is deleted.

For example, to delete all of the rolled traffic log files, enter the following command:

```
execute log delete-rolled traffic 1 9999
```

# Alarms

In FIPS-CC mode, the FortiGate unit can raise alarms for the following types of events:

- failed administrator authentication
- packet replay attempts (IPS?)
- bootup self-test failure
- cryptographic failure
- firewall policy violation (blocked sessions)

Alarms for all of these events are based on logs that report these events. For firewall events, traffic violation logs are used.This section contains the following information:

- Configuring alarms
- Alarm notifications
- Acknowledging alarms

## Configuring alarms

An alarm consists of one or more trigger events that occur a specified number of times in a particular time period. For example, you could configure the FortiGate unit to raise an alarm if there are three unsuccessful administrative login attempts in the same minute.

You can configure alarms only in the CLI. Each alarm is defined as an “alarm group”. There are separate alarm groups for each virtual domain (VDOM). You can select whether the alarms in each VDOM are audible. Within each alarm group, you specify:

- the threshold for each triggering event, 0 for events that will not trigger the alarm
- the period over which the number of triggering events is counted, 0 to count from startup

If you include more than one trigger event, the threshold for all the trigger events must be met to trigger the alarm. Firewall policy violations are configured together.

Alarm notification messages appear on the web-based manager, in SSH administrator sessions and on the console. The messages repeat until the administrator acknowledges the alarm.

### Alarm CLI configuration

The `system alarm` command syntax is as follows:

```
config system alarm
  set status {enable | disable}
  set audible {enable | disable}
  config groups
    edit <group_id>
      set admin-auth-failure-threshold <integer>
      set crypto-failure-threshold <integer>
      set period <integer>
      set replay-attempt-threshold <integer>
      set self-test-failure-threshold <integer>
```

```
        config fw-policy-violations
          edit <count>
            dst-port <dport_number>
            dst-ip <dst_ip>
            src-port <sport_number>
            src-ip <src_ip>
            threshold <integer>
          end
        end
      end
```

The keywords and variables are:

**Table 24: system alarm keywords and variables**

| Keywords and variables | Description | Default |
|---|---|---|
| `audible {enable \| disable}` | If enabled, the console beeps when the alarm notification appears. | `disable` |
| `status {enable \| disable}` | Enable or disable all alarms. | `disable` |
| **Alarm group keywords and variables** | | |
| `edit <group_id>` | `<group_id>` is the group identifier. Use 0 to automatically assign the next available number. | No default. |
| `admin-auth-failure-threshold <integer>` | Enter threshold for administrator authentication failures. Use 0 to disregard in this alarm group. | 0 |
| `crypto-failure-threshold <integer>` | Enter threshold for cryptographic failure. Use 0 to disregard in this alarm group. | 0 |
| `period <integer>` | Enter the period over which triggering events are counted. Use 0 for no limit (events are counted from start-up). | 0 |
| `replay-attempt-threshold <integer>` | Enter threshold for packet replay attempts.<br>Use 0 to disregard in this alarm group. | 0 |
| `self-test-failure-threshold <integer>` | Enter threshold for failure of startup integrity tests. Use 0 to disregard in this alarm group.<br>A self-test failure alarm is visible only after you recover from Error mode. | 0 |
| **`fw-policy-violations` keywords and variables** | | |
| `edit <violation_id>` | `<violation_id>` is the identifier for this trigger. Use 0 to automatically assign the next available number. | No default. |
| `dst-port <dport_number>` | Enter the destination port number to match in the traffic violation log. | 0 |
| `dst-ip <dst_ip>` | Enter the destination IP or subnet address to match in the traffic violation log. | 0 |
| `src-port <sport_number>` | Enter the source port number to match in the traffic violation log. | 0 |
| `src-ip <src_ip>` | Enter the source IP or subnet address to match in the traffic violation log. | 0 |

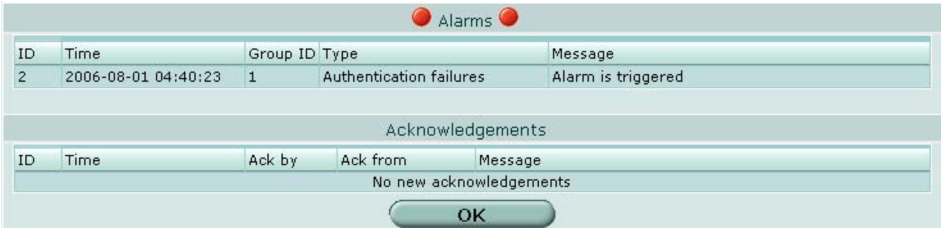
## Alarm notifications

Alarm notifications appear on both the CLI console and the web-based manager. On the CLI console alarm notifications look like this:

```
******************* !!! A L A R M !!! *******************
* ID: 1                    Time: Tue Sep 5 09:39:55 2006
* Group ID: 1              VD: root
* Type: Authentication failures
* Message: Alarm is triggered
*********************************************************
```

On the web-based manager, alarm notifications appear in a separate browser window and look like this:

**Figure 7: Alarm notification - web-based manager**



Alarms

| ID | Time | Group ID | Type | Message |
|---|---|---|---|---|
| 2 | 2006-08-01 04:40:23 | 1 | Authentication failures | Alarm is triggered |

Acknowledgements

| ID | Time | Ack by | Ack from | Message |
|---|---|---|---|---|
| No new acknowledgements | | | | |

The notification clearly shows the time, virtual domain, alarm group and type. Alarm notifications repeat until you acknowledge them. On the CLI console, the notification repeats every time you use the Enter key. In the web-based manager, you can close the alarm notification window, but the alarm will reappear in a few seconds.

## Acknowledging alarms

To acknowledge an alarm in the web-based manager, you simply select OK in the alarm notification window. On the CLI console, you acknowledge alarms using one of the following commands:

### To acknowledge a single alarm

```
execute ack-alarm <alarm-ID>
```

### To acknowledge all alarms

```
execute ack-alarm all
```

# Clearing Error mode

The FortiGate unit switches to Error mode, shuts down network interfaces and blocks traffic when current and rolled log files consume more than 95% of disk capacity.

The FortiGate unit indicates Error mode as follows:

- The console displays “FIPS-CC-ERR”. You might have to press an LCD panel key to see this display.

- "FIPS-CC-ERR" is prepended to the CLI prompt, `FIPS-CC-ERR FortiGate-1000A$`, for example.

To resume normal FIPS-CC mode operation, you first must reduce the logs to below 95% of device capacity. Only an administrator with the Audit Administrator role can do this. From the console, do any of the following:

- Delete rolled log files using the command `execute log delete-rolled`.
- Delete all current log entries using the command `execute log delete-all`.

Ideally you should reduce logs to 50% or less of device capacity. For information on how to delete logs, see "Deleting filtered log messages" on page 40. To disable error mode, enter the following CLI command:

```
execute error-mode exit
```

The FortiGate unit resumes normal FIPS-CC compliant operation unless there is still too little free space on the log device.

## Non-FIPS Approved Services

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

- NTP synchronization
- DHCP server
- Configuration backup and recovery