FIPS 140-2 Security Policy

FortiGate-VM Virtual Appliances

Software Version 4.0 MR3
FortiGate-VM Virtual Appliances: FIPS 140-2 Security Policy
01-436-192877-20130104
for FortiOS 4.0 MR3
© Copyright 2014 Fortinet, Inc.
This document may be freely reproduced and distributed whole and intact including this copyright notice.

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

Overview .................................................. 2
References .................................................. 2
Introduction ............................................... 3
Security Level Summary ................................. 3
Module Description ....................................... 4
  Module Interfaces ...................................... 5
  Web-Based Manager ................................. 6
  Command Line Interface ......................... 6
Roles, Services and Authentication ............... 7
  Roles .................................................. 7
  FIPS Approved Services ......................... 7
  Authentication ....................................... 8
Physical Security ........................................ 9
Operational Environment ............................. 9
Cryptographic Key Management .................... 9
  Random Number Generation ...................... 9
  Key Zeroization .................................... 9
  Algorithms .......................................... 10
  Cryptographic Keys and Critical Security Parameters ............................................ 10
  Alternating Bypass Feature .................... 12
  Key Archiving .................................... 12
Mitigation of Other Attacks ......................... 13
FIPS 140-2 Compliant Operation .................... 13
  Enabling FIPS-CC mode ......................... 14
Self-Tests ............................................. 14
Non-FIPS Approved Services ....................... 15
Overview

This document is a FIPS 140-2 Security Policy for Fortinet Incorporated’s FortiGate-VM family of virtual appliances running FortiOS 4.0 MR3. This policy describes how the appliances (hereafter referred to as the ‘module’) meet the FIPS 140-2 security requirements and how to operate the module in a FIPS compliant manner. This policy was created as part of a FIPS 140-2 Level 1 validation of the module.

This document contains the following sections:

- Introduction
- Security Level Summary
- Module Description
- Mitigation of Other Attacks
- FIPS 140-2 Compliant Operation
- Self-Tests
- Non-FIPS Approved Services


References

This policy deals specifically with operation and implementation of the module in the technical terms of the FIPS 140-2 standard and the associated validation program. Other 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 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, both physical and virtual, 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. FortiGate appliances 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 appliances 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 the FIPS-CC mode of operation.

Security Level Summary

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

Table 1: Summary of FIPS security requirements and compliance levels

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

Module Description

The FortiGate-VM appliances are software modules designed to execute on a General Purpose Computer (GPC) hardware platform running the VMware hypervisor.
The validated software version is FortiGate-VM64 v4.0, build 3688, 130430.

**Module Interfaces**

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

<table>
<thead>
<tr>
<th>FIPS 140 Interface</th>
<th>Logical Interface</th>
<th>Physical Port</th>
</tr>
</thead>
<tbody>
<tr>
<td>Data Input</td>
<td>API input parameters</td>
<td>Network interface</td>
</tr>
<tr>
<td>Data Output</td>
<td>API output parameters</td>
<td>Network interface</td>
</tr>
<tr>
<td>Control Input</td>
<td>API function calls</td>
<td>Network interface, serial interface</td>
</tr>
<tr>
<td>Status Output</td>
<td>API return values</td>
<td>Network interface, serial interface</td>
</tr>
<tr>
<td>Power Input</td>
<td>N/A</td>
<td>The power supply is the power interface</td>
</tr>
</tbody>
</table>
Web-Based Manager

The FortiGate-VM web-based manager provides GUI based access to the module and is the primary tool for configuring the module. The manager requires a web browser on the management computer and an Ethernet connection between the FortiGate-VM unit and the management computer.

A web-browser that supports Transport Layer Security (TLS) 1.0 is required for remote access to the web-based manager when the module is operating in FIPS-CC mode. HTTP access to the web-based manager is not allowed in FIPS-CC mode and is disabled.

Command Line Interface

The FortiGate-VM Command Line Interface (CLI) is a full-featured, text based management tool for the module. The CLI provides access to all of the possible services and configuration options in the module. The CLI uses a console connection or a network (Ethernet) connection between the FortiGate-VM 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 module provides 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 module’s 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 module provides a Network User role for end-users (Users). Network users can make use of the encrypt/decrypt services, but cannot access the module for administrative purposes.

The module does not provide a Maintenance role.

FIPS Approved Services

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

The role names are abbreviated as follows:

<table>
<thead>
<tr>
<th>Role</th>
<th>Abbreviation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Crypto Officer</td>
<td>CO</td>
</tr>
<tr>
<td>User</td>
<td>U</td>
</tr>
</tbody>
</table>

The access types are abbreviated as follows:

<table>
<thead>
<tr>
<th>Access Type</th>
<th>Abbreviation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Read Access</td>
<td>R</td>
</tr>
<tr>
<td>Write Access</td>
<td>W</td>
</tr>
<tr>
<td>Execute Access</td>
<td>E</td>
</tr>
</tbody>
</table>

Table 3: Services available to Crypto Officers - FIPS-CC mode of operation

<table>
<thead>
<tr>
<th>Service</th>
<th>Access</th>
<th>Key/CSP</th>
</tr>
</thead>
<tbody>
<tr>
<td>authenticate to module</td>
<td>WE</td>
<td>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</td>
</tr>
<tr>
<td>show system status</td>
<td>WE</td>
<td>N/A</td>
</tr>
<tr>
<td>show FIPS-CC mode enabled/disabled (console/CLI only)</td>
<td>WE</td>
<td>N/A</td>
</tr>
<tr>
<td>enable FIPS-CC mode of operation (console only)</td>
<td>WE</td>
<td>Configuration Integrity Key</td>
</tr>
<tr>
<td>execute factory reset (zeroize keys, disable FIPS mode, console/CLI only)</td>
<td>E</td>
<td>See “Key Zeroization” on page 8</td>
</tr>
<tr>
<td>execute FIPS-CC on-demand self-tests (console only)</td>
<td>E</td>
<td>Configuration Integrity Key, Firmware Integrity Key</td>
</tr>
<tr>
<td>add/delete operators and network users</td>
<td>WE</td>
<td>Operator Password, Network User Password</td>
</tr>
</tbody>
</table>
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 12.

For Network Users invoking the IPSec VPN 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: 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 $1640$ 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 FortiGate-VM family of virtual appliances are software modules and are defined as multi-chip, standalone cryptographic modules. As software modules the FIPS 140-2 physical requirements are not applicable.

**Operational Environment**

The operational environment for the module consists of the FortiGate-VM software and the VMware hypervisor. The module was tested as meeting level 1 with the FortiGate-VM firmware on VMWare ESXi 5.0.0 Update 1 running on a Dell PowerEdge R410.

**Cryptographic Key Management**

**Random Number Generation**

The modules use a software 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 key (estimated strength 128 bits) and 64 bytes of entropy (estimated strength 60 bits) gathered from a combination of system data and internal resources such as time, memory addresses, kernel ticks, and module identifiers. As the module's ANSIX 9.31 RNG implementation only generates random values of size 16 bytes (128 bits), it would take multiple calls to form a 32 byte (256 bit) key. The total estimated strength for the two calls required to form a 32 byte (256 bit) key is 188 bits.

**Key Zeroization**

All keys except the following are zeroized by executing a factory reset:
• ANSI X9.31 RNG AES Key
• Firmware Update Key
• Firmware Integrity Key
• Configuration Integrity Key
• Configuration Backup Key
• SSH Server/Host Key
• HTTPS/TLS Server/Host Key

All keys and CSPs are zeroized by deleting the FortiGate-VM appliance from the VMWare server.

Algorithms

Table 5: FIPS Approved Algorithms

<table>
<thead>
<tr>
<th>Algorithm</th>
<th>NIST Certificate Number</th>
</tr>
</thead>
<tbody>
<tr>
<td>RNG (ANSI X9.31 Appendix A)</td>
<td>1192</td>
</tr>
<tr>
<td>Triple-DES</td>
<td>1503, 1504</td>
</tr>
<tr>
<td>AES</td>
<td>2414, 2415</td>
</tr>
<tr>
<td>SHA-1</td>
<td>2071, 2072</td>
</tr>
<tr>
<td>SHA-256</td>
<td>2071, 2072</td>
</tr>
<tr>
<td>HMAC SHA-1</td>
<td>1500, 1501</td>
</tr>
<tr>
<td>HMAC SHA-256</td>
<td>1500, 1501</td>
</tr>
<tr>
<td>RSA PKCS1 (digital signature creation and verification)</td>
<td>1248</td>
</tr>
</tbody>
</table>

Table 6: FIPS Allowed Algorithms

<table>
<thead>
<tr>
<th>Algorithm</th>
</tr>
</thead>
<tbody>
<tr>
<td>RSA (key establishment methodology provides 112 bits of encryption strength; non-compliant less than 112-bits of encryption strength)</td>
</tr>
<tr>
<td>Diffie-Hellman (key agreement; key establishment methodology provides between 112 and 188 bits of encryption strength; non-compliant less than 112-bits of encryption strength)</td>
</tr>
</tbody>
</table>

Table 7: Non-FIPS Approved Algorithms

<table>
<thead>
<tr>
<th>Algorithm</th>
</tr>
</thead>
<tbody>
<tr>
<td>RSA PKCS1 (digital signature creation with 1024 or 1536 bit keys)</td>
</tr>
<tr>
<td>DES (disabled in FIPS-CC mode)</td>
</tr>
<tr>
<td>MD5 (disabled in FIPS-CC mode except for use in the TLS protocol)</td>
</tr>
<tr>
<td>HMAC MD5 (disabled in FIPS-CC mode)</td>
</tr>
</tbody>
</table>

Some algorithms may be classified as deprecated, restricted, or legacy-use. Please consult NIST SP 800-131A for details.
The vendor makes no conformance claims to any key derivation function specified in SP 800-135rev1. 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 module. The following definitions apply to the table:

<table>
<thead>
<tr>
<th>Key or CSP</th>
<th>Storage</th>
<th>Usage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Diffie-Hellman Keys</td>
<td>SDRAM</td>
<td>Key agreement and key establishment</td>
</tr>
<tr>
<td>IPSec Manual Authentication Key</td>
<td>Flash RAM AES encrypted</td>
<td>Used as IPSec Session Authentication Key</td>
</tr>
<tr>
<td>IPSec Manual Encryption Key</td>
<td>Flash RAM AES encrypted</td>
<td>Used as IPSec Session Encryption Key</td>
</tr>
<tr>
<td>IPSec Session Authentication Key</td>
<td>SDRAM</td>
<td>IPSec peer-to-peer authentication using HMAC SHA-1</td>
</tr>
<tr>
<td>IPSec Session Encryption Key</td>
<td>SDRAM</td>
<td>VPN traffic encryption/decryption using Triple-DES or AES</td>
</tr>
<tr>
<td>IKE Pre-Shared Key</td>
<td>Flash RAM AES encrypted</td>
<td>Used to generate IKE protocol keys</td>
</tr>
<tr>
<td>IKE Authentication Key</td>
<td>SDRAM</td>
<td>IKE peer-to-peer authentication using HMAC SHA-1 (SKEYID_A)</td>
</tr>
<tr>
<td>IKE Key Generation Key</td>
<td>SDRAM</td>
<td>IPSec SA keying material (SKEYID_D)</td>
</tr>
<tr>
<td>IKE Session Encryption Key</td>
<td>SDRAM</td>
<td>Encryption of IKE peer-to-peer key negotiation using Triple-DES or AES (SKEYID_E)</td>
</tr>
<tr>
<td>IKE RSA Key</td>
<td>Flash Ram Plain text</td>
<td>Used to generate IKE protocol keys</td>
</tr>
<tr>
<td>RNG Seed (ANSI X9.31 Appendix A.2.4)</td>
<td>Flash RAM Plain text</td>
<td>Seed used for initializing the RNG</td>
</tr>
<tr>
<td>RNG AES Key (ANSI X9.31 Appendix A.2.4)</td>
<td>Flash RAM Plain text</td>
<td>AES Seed key used with the RNG</td>
</tr>
<tr>
<td>Firmware Update Key</td>
<td>Flash RAM Plain text</td>
<td>Verification of firmware integrity when updating to new firmware versions using RSA public key</td>
</tr>
<tr>
<td>Firmware Integrity Key</td>
<td>Flash RAM Plain text</td>
<td>Verification of firmware integrity in the firmware integrity test using RSA public key</td>
</tr>
<tr>
<td>HTTPS/TLS Server/Host Key</td>
<td>Flash RAM Plain text</td>
<td>RSA private key used in the HTTPS/TLS protocols</td>
</tr>
</tbody>
</table>
Alternating Bypass Feature

The primary cryptographic function of the module is as a firewall and VPN device. The module implements 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 module is 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.

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 interface, the module is operating in a bypass state. When traffic is routed over the virtual interface, the module is 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 module supports key archiving to a management computer or USB token as part of a module configuration file backup. Operator entered keys are archived as part of the module configuration file. The configuration file is stored in plain text, but keys in the configuration file are either AES encrypted using the Configuration Encryption Key or stored as a keyed hash using HMAC-SHA-1 using the Configuration Backup Key.

### Mitigation of Other Attacks

The module includes 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-VM 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-VM appliance. 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.

### FIPS 140-2 Compliant Operation

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

- The FortiGate-VM unit is configured in the FIPS-CC mode of operation.
- The VMWare server and FortiGate-VM appliance are installed in a secure physical location.
- Physical access to the VMWare server and FortiGate-VM appliance unit are restricted to authorized operators.
Self-Tests

- Administrative passwords are at least 8 characters long.
- Administrative passwords are changed regularly.
- Administrator account passwords must have the following characteristics:
  - One (or more) of the characters must be capitalized
  - One (or more) of the characters must be numeric
  - One (or more) of the characters must be non alpha-numeric (e.g. punctuation mark)
- Administration of the module is permitted using only validated administrative methods. These are:
  - Console connection
  - Web-based manager via HTTPS
  - 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 2048 bit or greater key sizes.
- LDAP based authentication must use secure LDAP (LDAPS).
- Only approved and allowed algorithms are used (see “Algorithms” on page 9).

The module 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 the FIPS 140-2 compliant mode of operation, 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 module will execute self-tests to ensure the correct initialization of the module’s cryptographic functions.

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

```
get system status
```

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

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

Note that enabling/disabling the FIPS-CC mode of operation 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:
Non-FIPS Approved Services

- Firmware integrity test using RSA signatures
- Configuration/VPN bypass test using HMAC SHA-1
- Triple-DES, CBC mode, encrypt known answer test
- Triple-DES, CBC mode, decrypt known answer test
- AES, CBC mode, encrypt known answer test
- AES, CBC mode, decrypt known answer test
- HMAC SHA-1 known answer test
- SHA-1 known answer test (test as part of HMAC SHA-1 known answer test)
- HMAC SHA-256 known answer test
- SHA-256 known answer test (test as part of HMAC SHA-256 known answer test)
- RSA signature generation known answer test
- RSA signature verification known answer test
- RNG known answer test

The results of the startup self-tests are displayed on the console during the startup process. The startup self-tests can also be initiated on demand using the CLI command `execute fips kat all` (to initiate all self-tests) or `execute fips kat <test>` (to initiate a specific self-test).

When the self-tests are run, each implementation of an algorithm is tested - e.g. when the AES self-test is run, all AES implementations are tested.

The module executes the following conditional tests when the related service is invoked:
- Continuous RNG test
- 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 module enters 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 module also provides the following non-FIPS approved services:
- Configuration backups using password protection
- LLTP and PPTP VPN

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