FIPS 140-2 Non-Proprietary Security Policy

FortiManager™ 5.2

FortiManager™ 5.2 FIPS 140-2 Non-Proprietary Security Policy	
Document Version:	2.0
Publication Date:	December 23, 2015
Description:	Documents FIPS 140-2 Level 1 Security Policy issues, compliancy and requirements for FIPS compliant operation.
Firmware Version:	v5.2.4-build0738 150923 (GA)

FortiManager™ 5.2: FIPS 140-2 Non-Proprietary Security Policy

02-524-256726-20151001

for FortiManager™ 5.2

Contents

Overview

This document is a FIPS 140-2 Security Policy for Fortinet Incorporated's FortiManager 5.2 firmware, which runs on the FortiManager family of security appliances. This policy describes how the FortiManager 5.2 firmware (hereafter referred to as the 'Module') meets the FIPS 140-2 security requirements and how to operate the Module in a FIPS compliant manner. This policy was created as part of the FIPS 140-2 Level 1 validation of the Module.

This document contains the following sections:

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

The Federal Information Processing Standards Publication 140-2 - *Security Requirements for Cryptographic Modules* (FIPS 140-2) details the United States Federal Government requirements for cryptographic modules. Detailed information about the FIPS 140-2 standard and validation program is available on the NIST (National Institute of Standards and Technology) website at http://csrc.nist.gov/groups/STM/cmvp/index.html.

References

This policy deals specifically with operation and implementation of the Module in the technical terms of the FIPS 140-2 standard and the associated validation program. Other Fortinet product manuals, guides and technical notes can be found at the Fortinet technical documentation website at http://docs.fortinet.com.

Additional information on the entire Fortinet product line can be obtained from the following sources:

- Find general product information in the product section of the Fortinet corporate website at http://www.fortinet.com/products.
- Find on-line product support for registered products in the technical support section of the Fortinet corporate website at http://www.fortinet.com/support
- Find contact information for technical or sales related questions in the contacts section of the Fortinet corporate website at http://www.fortinet.com/contact.
- Find security information and bulletins in the FortiGuard Center of the Fortinet corporate website at http://www.fortinet.com/FortiGuardCenter.

Introduction

FortiManager Network Security Management Appliances were designed to provide security management for large enterprise organizations and service providers. They enable you to centrally manage Fortinet devices, including FortiGate, FortiWiFi, and FortiCarrier. FortiManager provides the high performance and scalability you need to efficiently apply policies and distribute content security/firmware updates, regardless of the size of your network. FortiManager is one of several versatile Fortinet Management Products that provide a diversity of deployment types, growth flexibility, advanced customization through APIs and simple licensing.

Security Level Summary

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

Table 1: Summary of FIPS security requirements and compliance levels

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

Module Description

The Module is a firmware operating system that runs exclusively on Fortinet's FortiManager product family. FortiManager units are PC-based, purpose built appliances.

The FortiManager units are multiple chip, standalone cryptographic modules consisting of production grade components contained in a physically protected enclosure.

Figure 1: FortiManager Physical Cryptographic Boundary

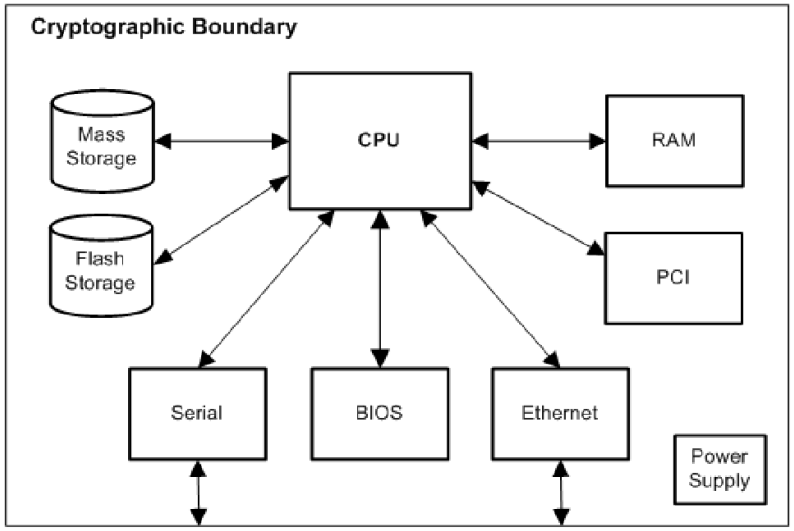
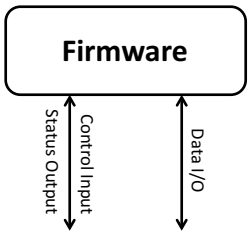


Figure 2: FortiManager Logical Cryptographic Boundary



For the purposes of FIPS 140-2 conformance testing, the Module was tested on a FortiManager-4000D unit and used a Fortinet entropy token (part number FTR-ENT-1) as the entropy source.

The validated firmware version is FortiManager v5.2.4-build0738 150923 (GA).

The Module can also be executed on any of the following FortiManager units and remain vendor affirmed FIPS-compliant:

- FortiManager-100C
- FortiManager-200D
- FortiManager-1000C
- FortiManager-1000D
- FortiManager-3000C
- FortiManager-3900E
- FortiManager-4000E

The CMVP makes no statement as to the correct operation of the Module or the security strength of the generated keys when so ported if the specific operational environment is not listed on the validation certificate.

Module Interfaces

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

Table 2: FortiManager logical interfaces and physical ports

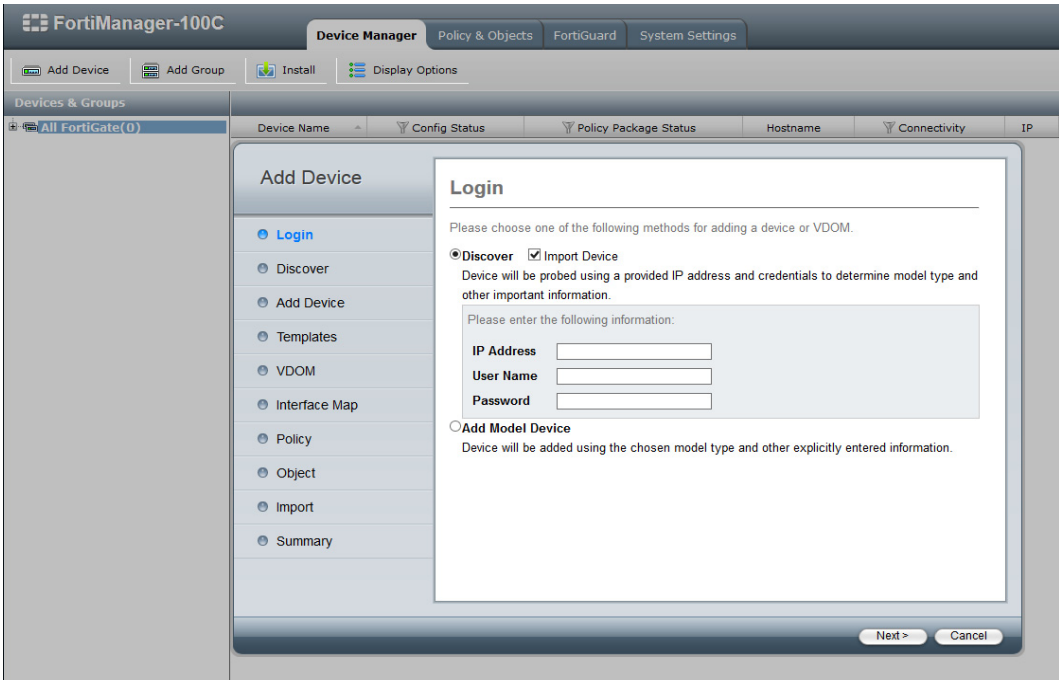
FIPS 140 Interface	Logical Interface	Physical Port
Data Input	API input parameters	Network interface, USB interface (Entropy token)
Data Output	API output parameters	Network interface
Control Input	API function calls	Network interface, serial interface, USB interface (Entropy token)
Status Output	API return values	Network interface, serial interface
Power Input	N/A	The power supply is the power interface

Web-Based Manager

The FortiManager 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 FortiManager unit and the management computer.

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

Figure 3: The FortiManager web-based manager



Command Line Interface

The FortiManager 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 FortiManager unit and the management computer. The console connection is a direct serial connection. Terminal emulation software is required on the management computer using either method. For network access, a Telnet or SSH client that supports the SSH v2.0 protocol is required (SSH v1.0 is not supported in FIPS mode). Telnet access to the CLI is not allowed in FIPS mode and is disabled.

Roles, Services and Authentication

Roles

When configured in FIPS 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 also provides a Network User role. Network Users have read/write access to a restricted set of the Module’s administrative services. Network User accounts are created by Crypto Officers with the necessary permissions.

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 in each mode of operation, the types of access for each role and the Keys or CSPs they affect.

The access types are abbreviated as follows:

Read Access	R
Write Access	W
Execute Access	E

Table 3: Services available to Crypto Officers

Service	Access	Key/CSP
authenticate to Module	WE	Crypto Officer Password, Diffie-Hellman Key, HTTP/TLS and SSH Server/Host Keys, HTTPS/TLS and SSH Session Authentication Keys, and HTTPS/TLS Session Encryption Keys, DRBG Output, DRBG Seed, DRBG Input String
show system status	WE	N/A
show FIPS mode enabled/disabled (console/CLI only)	WE	N/A
enable FIPS mode of operation (console only)	WE	Configuration Integrity Key

Table 3: Services available to Crypto Officers

Service	Access	Key/CSP
key zeroization (console/CLI only)	WE	All keys. (See “Key Zeroization” on page 9)
execute factory reset (disable FIPS mode, console/CLI only)	WE	All keys except firmware update key, configuration integrity key, configuration backup key
execute FIPS on-demand self-tests (console only)	E	Configuration Integrity Key, Firmware Integrity Key
add/delete operators and network users	WE	Crypto Officer Password, Network User Password
set/reset operator and Network User Password passwords	WE	Crypto Officer Password, Network User Password
backup/restore configuration file	WE	Configuration Encryption Key, Configuration Backup Key
read/set/delete/modify Module configuration	WE	N/A
execute firmware update	E	Firmware Update Key
read log data	WE	N/A
delete log data (console/CLI only)	WE	N/A
execute system diagnostics (console/CLI only)	WE	N/A

Table 4: Services available to Network Users

Service/CSP	Access	Key/CSP
authenticate to Module	WE	Crypto Officer Password, Diffie-Hellman Key, HTTP/TLS and SSH Server/Host Keys, HTTPS/TLS and SSH Session Authentication Keys, and HTTPS/TLS Session Encryption Keys, DRBG Output, DRBG Seed, DRBG Input String
read/set/delete/modify FortiGate web filter profile, IPS profile and application sensors	E	Diffie-Hellman Key, HTTPS/TLS Server/Host Key, HTTPS/TLS Session Authentication Key, HTTPS/TLS Session Encryption Key, DRBG Output, DRBG Seed, DRBG Input String
show system status (console only)	WE	N/A
execute FIPS on-demand self-tests (console only)	E	Configuration Integrity Key, Firmware Integrity Key
show FIPS mode enabled/disabled (console/CLI only)	WE	N/A

Non-FIPS Approved Services

The Module also provides the following non-FIPS approved services:

- Configuration backups using password protection
- LLTP and PPTP VPN

- All services specified in Table 3 and Table 4 are considered non-approved when using the following algorithms:
  - Non-compliant-strength Diffie-Hellman
  - Non-compliant-strength RSA key wrapping
  - DES
  - HMAC-MD5

The above services shall not be used in the FIPS approved mode of operation.

Authentication

The Module implements identity based authentication. Operators must authenticate with a user-id and password combination to access the Module 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.

The minimum password length is 8 characters when in FIPS mode (maximum password length is 32 characters). The password may contain any combination of upper- and lowercase letters, numbers, and printable symbols; allowing for 94 possible characters. The odds of correctly guessing a password are $1/94^8$ 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.

Note that operator authentication over HTTPS/SSH and using the console is subject to a limit of 3 failed authentication attempts in 1 minute; thus, the maximum number of attempts in one minute is 3. Therefore, the probability of a success with multiple consecutive attempts in a one-minute period is $3/94^8$ which is less than 1/100,000.

Physical Security

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

Operational Environment

The Module constitutes the entire firmware operating system for a FortiManager unit and can only be installed and run on a FortiManager unit. The Module provides a proprietary and non-modifiable operating system and does not provide a programming environment.

For the purposes of FIPS 140-2 conformance testing, the Module was tested on the FortiManager-4000D unit.

Cryptographic Key Management

Random Number Generation

The Module uses a firmware based, deterministic random bit generator (DRBG) that conforms to NIST Special Publication 800-90A. The Module generates cryptographic keys whose strengths are modified by available entropy. There is no assurance of the minimum strength of generated keys.

Entropy Token

The Module uses an entropy token (part number FTR-ENT-1 or part number FTR-ENT-2) to seed the DRBG during the Module's boot process and to periodically reseed the DRBG. The entropy token is not included in the boundary of the Module and therefore no assurance can be made for the correct operation of the entropy token nor is there a guarantee of stated entropy.

The default reseed period is once every 24 hours (1440 minutes). The token must be installed to complete the boot process and to reseed of the DRBG. The entropy token is responsible for loading a minimum of 256 bits of entropy.

Key Zeroization

The zeroization process must be performed under the direct control of the operator. The operator must be present to observe that the zeroization method has completed successfully.

All keys and CSPs are zeroized by erasing the Module's flash memory and then power cycling the FortiManager unit. To erase the flash memory, execute the following command from the CLI:

```
execute erase-disk flash <erase-times>
```

Algorithms

Table 5: FIPS Approved Algorithms

Algorithm	NIST Certificate Number
CTR DRBG (NIST SP 800-90A) with 256-bits	929
Triple-DES in CBC mode with 192-bits	2001
AES in CBC mode (128-, 192-, 256-bits)	3594
SHA-1	2956
SHA-256	2956
HMAC SHA-1	2291
HMAC SHA-256	2291
RSA PKCS1 -Signature Generation: 2048 and 3072-bit -Signature Verification: 1024, 2048 and 3072-bit -For legacy use, the module supports 1024-bit RSA keys and SHA-1 for signature verification	1848
CVL (SSH) - with TDES-192 bit-CBC, AES 128 bit-, AES 256 bit -CBC (using SHA1, SHA256 and SHA512)	616
CVL (TLS) - TLS1.0/1.1	616

Table 6: FIPS Allowed Algorithms

Algorithm
RSA (key wrapping; key establishment methodology provides 112 or 128 bits of encryption strength)
Diffie-Hellman (key agreement; key establishment methodology provides between 112 and 201 bits of encryption strength)
NDRNG (Entropy Token) - please refer to the "Entropy Token" on page 9 for additional information.

Table 7: Non-FIPS Approved Algorithms

Algorithm
DES (disabled in FIPS mode)
MD5 (disabled in FIPS mode)
HMAC MD5 (disabled in FIPS mode)
RSA is non-compliant when keys less than 2048 bits are used, since such keys do not provide the minimum required 112 bits of encryption strength.
Diffie-Hellman is non-compliant when keys less than 2048 bits are used, since such keys do not provide the minimum required 112 bits of encryption strength.

Note that the SSH and TLS protocols have not been tested by the CMVP or CAVP.

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 tabl

Key or CSP The key or CSP description.

Storage Where and how the keys are stored

Usage How the keys are used

Zeroization The key zeroization method

Table 8: Cryptographic Keys and Critical Security Parameters used in FIPS Mode

Key or CSP	Generation	Storage	Usage	Zeroization
Diffie-Hellman Keys	Automatic	SDRAM Plaintext	Key agreement and key establishment	By erasing the flash memory and power cycling the FortiManager unit
NDRNG output string	Automatic	Flash RAM Plain-text	Input string for the entropy pool	By erasing the flash memory and power cycling the FortiManager unit
DRBG seed	Automatic	Flash RAM Plain-text	Seed used by the DRBG (output from NDRNG)	By erasing the flash memory and power cycling the FortiManager unit
DRBG output	Automatic	Flash RAM Plain-text	Random numbers used in cryptographic algorithms	By erasing the flash memory and power cycling the FortiManager unit
DRBG v and key values	Automatic	Flash Ram Plain-text	Internal state values for the DRBG	By erasing the flash memory and power cycling the FortiManager unit
Firmware Update Key	Preconfigured	Flash RAM Plain-text	Verification of firmware integrity when updating to new firmware versions using RSA public key (firmware load test)	By erasing the flash memory and power cycling the FortiManager unit

Table 8: Cryptographic Keys and Critical Security Parameters used in FIPS Mode

Key or CSP	Generation	Storage	Usage	Zeroization
Firmware Integrity Key	Preconfigured	Flash RAM Plain-text	Verification of firmware integrity in the firmware integrity test using RSA public key (firmware integrity test)	By erasing the flash memory and power cycling the FortiManager unit
HTTPS/TLS Server/Host Key	Preconfigured	Flash RAM Plain-text	RSA private key used in the HTTPS/TLS protocols (key establishment)	By erasing the flash memory and power cycling the FortiManager unit
HTTPS/TLS Session Authentication Key	Automatic	SDRAM Plain-text	HMAC SHA-1 or HMAC SHA-256 key used for HTTPS/TLS session authentication	By erasing the flash memory and power cycling the FortiManager unit
HTTPS/TLS Session Encryption Key	Automatic	SDRAM Plain-text	AES or Triple-DES key used for HTTPS/TLS session encryption	By erasing the flash memory and power cycling the FortiManager unit
SSH Server/Host Key	Preconfigured	Flash RAM Plain-text	RSA private key used in the SSH protocol (key establishment)	By erasing the flash memory and power cycling the FortiManager unit
SSH Session Authentication Key	Automatic	SDRAM Plain-text	HMAC SHA-1 or HMAC SHA-256 key used for SSH session authentication	By erasing the flash memory and power cycling the FortiManager unit
SSH Session Encryption Key	Automatic	SDRAM Plain-text	AES or Triple-DES key used for SSH session encryption	By erasing the flash memory and power cycling the FortiManager unit
Crypto Officer Password	Manual	Flash RAM SHA-1 hash	Used to authenticate operator access to the Module	By erasing the flash memory and power cycling the FortiManager unit
Configuration Integrity Key	Preconfigured	Flash RAM Plain-text	HMAC SHA-256 hash used for configuration integrity test	By erasing the flash memory and power cycling the FortiManager unit
Configuration Encryption Key	Automatic	Flash RAM Plain-text	AES key used to encrypt CSPs on the flash RAM and in the backup configuration file (except for crypto officer passwords in the backup configuration file)	By erasing the flash memory and power cycling the FortiManager unit

Table 8: Cryptographic Keys and Critical Security Parameters used in FIPS Mode

Key or CSP	Generation	Storage	Usage	Zeroization
Configuration Backup Key	Automatic	Flash RAM Plain-text	HMAC SHA-256 key used to encrypt crypto officer passwords in the backup configuration file	By erasing the flash memory and power cycling the FortiManager unit
Network User Password	Manual	Flash RAM SHA-1 hash	Used to authenticate network access to the Module	By erasing the flash memory and power cycling the FortiManager unit

Note: The Generation column lists all of the keys/CSPs and their entry/generation methods. Manual entered keys are entered by the operator electronically (as defined by FIPS) using the console or a management computer. Pre-configured keys are set as part of the firmware (hardcoded) and are not operator modifiable. Automatic keys are generated as part of the associated protocol.

Key Archiving

The Module supports key archiving to a management computer as part of the Module configuration file backup. Operator entered keys are archived as part of the Module configuration file. The configuration file is stored in plain text, but keys in the configuration file are either AES encrypted using the Configuration Encryption Key or stored as a keyed hash using HMAC SHA-1 using the Configuration Backup Key.

Mitigation of Other Attacks

The Module does not mitigate against any other attacks.

FIPS 140-2 Compliant Operation

FIPS 140-2 compliant operation requires both that you use the Module in its FIPS mode of operation and that you follow secure procedures for installation and operation of the FortiManager unit. You must ensure that:

- The FortiManager unit is configured in the FIPS mode of operation.
- The FortiManager unit is installed in a secure physical location.
- Physical access to the FortiManager unit is restricted to authorized operators.
- A USB entropy token is used to seed the DRBG.
- The token remains in the USB port during operation
- 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 2048 bits are not used.
- Client side RSA certificates must use 2048 bit or greater key sizes.
- 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 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 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 mode by executing the following command from the CLI:

```
get system status
```

If the Module is running in FIPS mode, the system status output will display the line:

```
FIPS mode: enable
```

Note: Enabling/disabling the FIPS mode of operation will automatically invoke the key zeroization service. The key zeroization is performed immediately after FIPS mode is enabled/disabled. Additionally, certain non-FIPS approved services may still be available, but they shall not be used in the FIPS approved mode of operation.

Self-Tests

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

- Firmware integrity test using RSA signatures
- Configuration integrity 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
- DRBG 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 NDRNG test
- Continuous DRBG test
- RSA pairwise consistency test
- Configuration integrity test using HMAC SHA-256
- 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:

```
FIPS error: <Alg> test failed
Entering error mode...
```

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