Forcepoint NGFW Cryptographic Kernel Module

LEVEL 1 NON-PROPRIETARY SECURITY POLICY

10900-A Stonelake Blvd, Ste. 350,
Austin, TX 78759, USA
www.forcepoint.com

Revision History

Revision	Date	Reason
A	April 29, 2022	Initial release.
B	April 29, 2024	CMVP comment responses.
C	September 30, 2024	CMVP comment responses.

Trademarks, Copyrights, and Third-Party Software

© 2024 Forcepoint. This document may be freely reproduced and distributed whole and intact including this copyright notice.

Contents

Acronyms and Abbreviations

Term	Definition
AES	Advanced Encryption Standard
ANSI	American National Standards Institute
API	Application Programming Interface
CBC	Cipher Block Chaining
CFB	Cipher FeedBack
CMVP	Cryptographic Module Validation Program
CO	Crypto Officer
CSP	Critical Security Parameter
ECB	Electronic Code Book
FIPS	Federal Information Processing Standard
GCM	Galois Counter Mode
HMAC	Keyed-Hash Message Authentication Code
IG	Implementation Guidance
ISO/IEC	International Organization for Standardization / International Electrotechnical Commission
I/O	Input/Output
IV	Initialization Vector
KAT	Known Answer Test
MAC	Message Authentication Code
NIST	National Institute of Science and Technology
N/A	Not Applicable

Term	Definition
OFB	Output FeedBack
POST	Power-on Self-Test
SHA	Secure Hash Algorithm
SSP	Sensitive Security Parameter

Preface

This is a non-proprietary Cryptographic Module Security Policy for the Forcepoint NGFW Cryptographic Kernel Module (Software Version: 3.0) from Forcepoint. This Security Policy describes how the Forcepoint NGFW Cryptographic Kernel Module (referred as crypto module, module, library) meet the security requirements of Federal Information Processing Standards (FIPS) Publication 140-3, which details the U.S. and Canadian government requirements for cryptographic modules. More information about the FIPS 140-3 standard and validation program is available on the National Institute of Standards and Technology (NIST) and the Canadian Centre for Cyber Security (CCCS) Cryptographic Module Validation Program (CMVP) website at https://csrc.nist.gov/projects/cryptographic-module-validation-program

This document also describes how to run the module in a secure Approved mode of operation. This policy was prepared as part of the Level 1 FIPS 140-3 validation of the module.

1. General

1.1. Security Level

The Forcepoint NGFW Cryptographic Kernel Module meets overall level 1 security requirements for FIPS 140-3 as summarized in the table below:

TABLE 1: SECURITY LEVELS

ISO/IEC 24759 Section 6 [Number Below]	FIPS 140-3 Section Title	Security Level
1	General	1
2	Cryptographic Module Specification	1
3	Cryptographic Module Interfaces	1
4	Roles, Services, and Authentication	1
5	Software/Firmware Security	1
6	Operational Environment	1
7	Physical Security	N/A
8	Non-Invasive Security	N/A
9	Sensitive Security Parameter Management	1

Rev.C, Copyright © 2024 Forcepoint

ISO/IEC 24759 Section 6 [Number Below]	FIPS 140-3 Section Title	Security Level
10	Self-Tests	1
11	Life-Cycle Assurance	1
12	Mitigation of Other Attacks	N/A

2. Cryptographic Module Specification

2.1. Module Overview

The Forcepoint NGFW Cryptographic Kernel Module is a module that provides general-purpose cryptographic algorithms for Forcepoint applications. The binary of the module and the integrity check file are **qcl_fips.ko** and **checksums.fips**. Assembly language optimizations are used in the cryptographic module implementation. The module contains the following cryptographic functionality:

- Cryptographic hash functions
- Message authentication code functions
- Symmetric key encryption and decryption

2.2. Approved Mode

The cryptographic module supports only an approved mode. The cryptographic module is initialized and set in the approved mode when the kernel module is loaded.

The calling application can call the ssh_crypto_get_certification_mode function to confirm the current mode of operation. It returns SSH_CRYPTO_CERTIFICATION_FIPS_140_2 to indicate that the module is indeed in the approved mode.

Rev.C, Copyright © 2024 Forcepoint

The module supports the following approved functions:

- AES: ECB, CBC, OFB, CFB128 and GCM modes
- SHS: hashing
- HMAC: message integrity

2.3.Module Description

The cryptographic module is a **software module** of type **multi-chip standalone**. This cryptographic module performs cryptographic operations for the Forcepoint Next Generation Firewall kernel. The cryptographic boundary of the module is the compiled, binary code of the module itself. The Tested Operational Environment's Physical Perimeter (TOEPP) of the module is the edges of the enclosure of the appliance that the module is running on. Figure 1 and Figure 2 provide an illustration of the description above.

Rev.C, Copyright © 2024 Forcepoint

The following block diagram provides an illustration of the following Operational environments:

- NGFW OS 10 on Linux 4.19 running on NGFW 3410 with Intel Xeon Gold 6230N with PAA;
- NGFW OS 10 on Linux 4.19 running on NGFW N120W with Intel Atom C3338 with PAA;
- NGFW OS 10 on Linux 4.19 running on NGFW N120W with Intel Atom C3338 without PAA

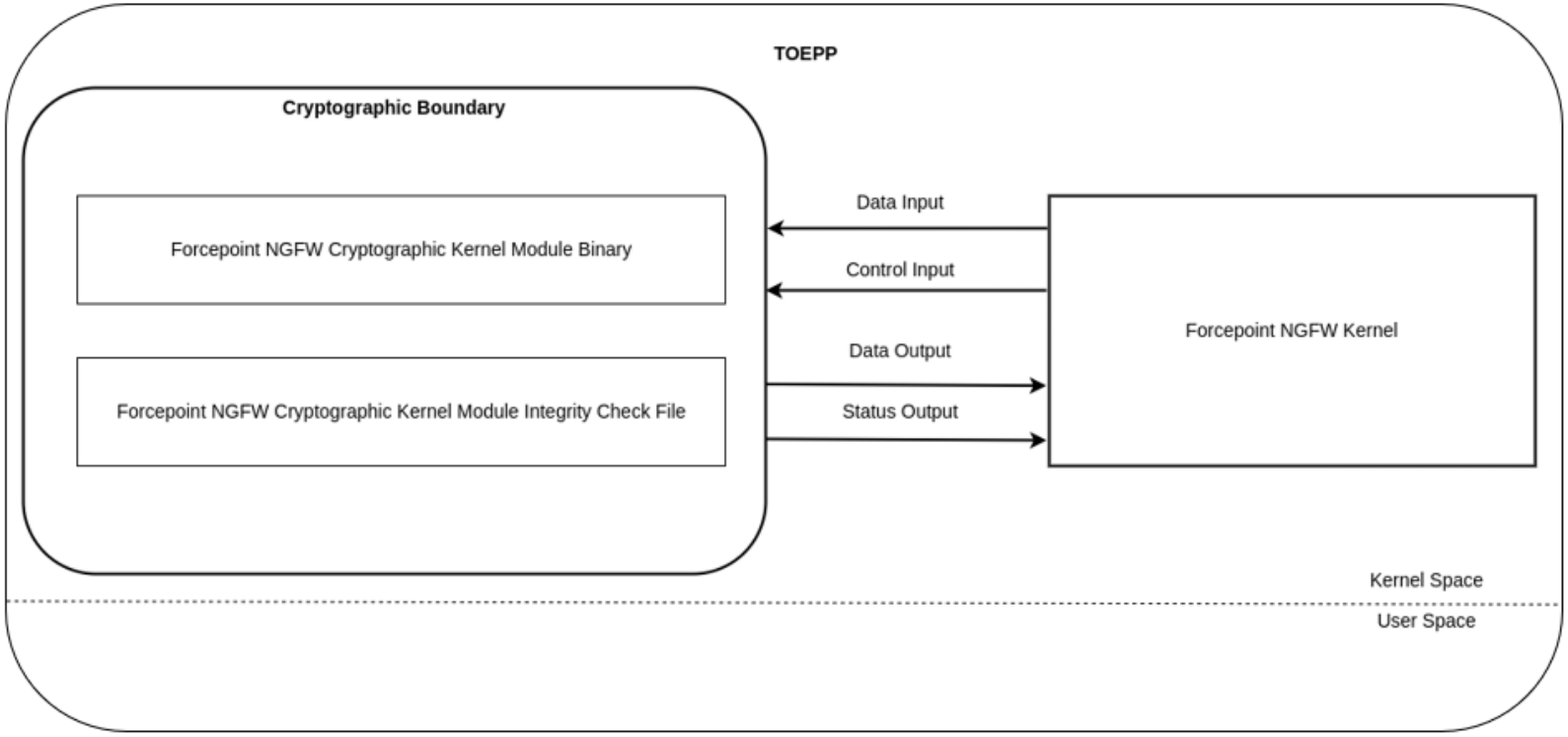

FIGURE 1: SOFTWARE BLOCK DIAGRAM 1

Rev.C, Copyright © 2024 Forcepoint

The following block diagram provides an illustration of the following Operational environment:

- NGFW OS 10 on Linux 4.19 on ESXi 7.0 running on Dell PowerEdge R440 with Intel Xeon Silver 4208 with PAA

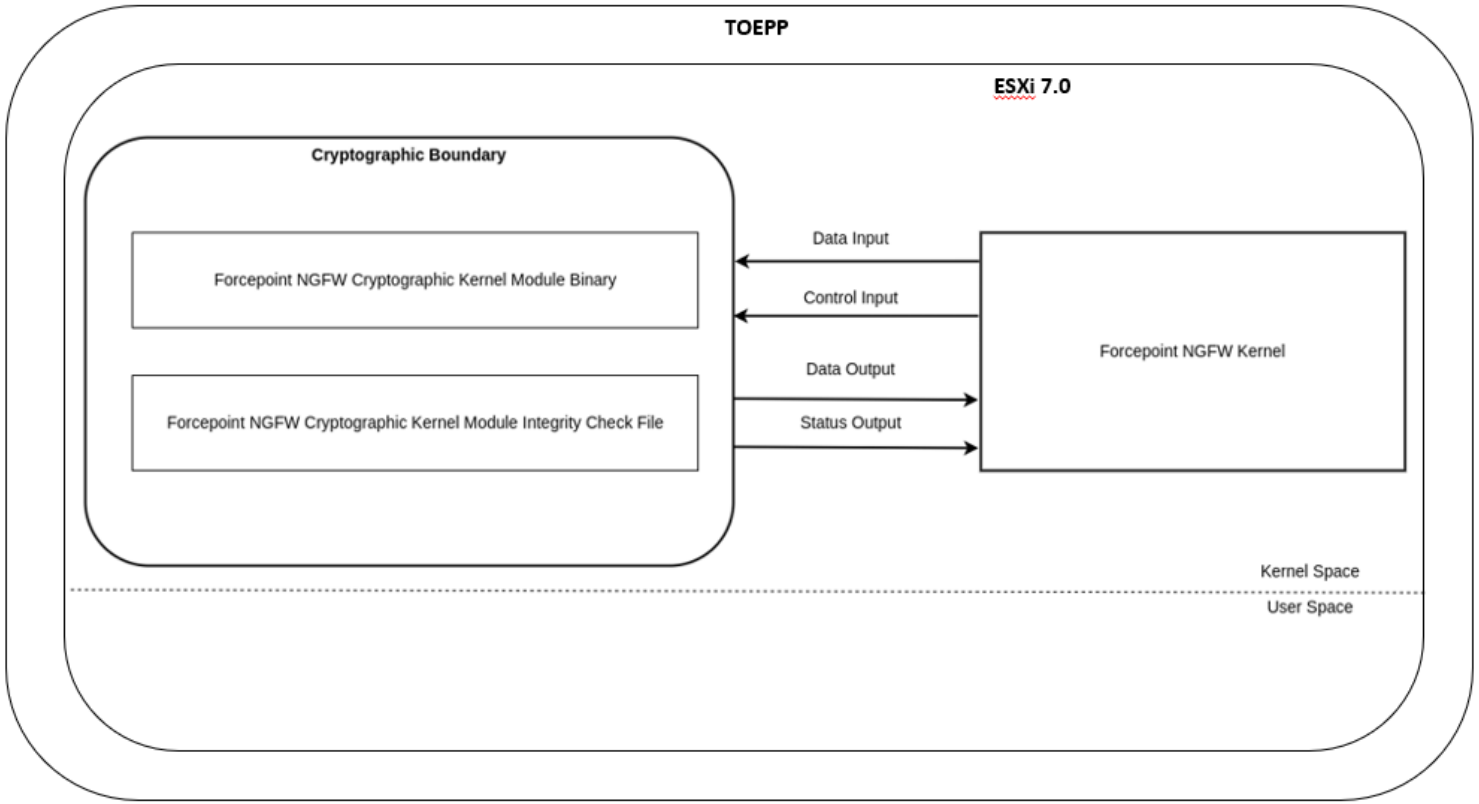

FIGURE 2. SOFTWARE BLOCK DIAGRAM 2

Rev.C, Copyright © 2024 Forcepoint

2.4.Test Configuration

The following tested configurations are covered in this security policy:

TABLE 2: TESTED OPERATIONAL ENVIRONMENTS

#	Operating System	Hardware Platform	Processor	PAA/Acceleration
1	NGFW OS 10 on Linux 4.19 on ESXi 7.0	Dell PowerEdge R440	Intel Xeon Silver 4208	AES-NI
2	NGFW OS 10 on Linux 4.19	NGFW 3410	Intel Xeon Gold 6230N	AES-NI
3	NGFW OS 10 on Linux 4.19	NGFW N120W	Intel Atom C3338	AES-NI
4	NGFW OS 10 on Linux 4.19	NGFW N120W	Intel Atom C3338	None

Rev.C, Copyright © 2024 Forcepoint

TABLE 3: VENDOR AFFIRMED OPERATIONAL ENVIRONMENTS

#	Operating System	Hardware Platform
1	NGFW OS 10 on Linux 4.19	NGFW 3401
2	NGFW OS 10 on Linux 4.19	NGFW 2210
3	NGFW OS 10 on Linux 4.19	NGFW 2205
4	NGFW OS 10 on Linux 4.19	NGFW 2201
5	NGFW OS 10 on Linux 4.19	NGFW N120
6	NGFW OS 10 on Linux 4.19	NGFW N60

Note: The CMVP makes no statement as to the correct operation of the module or the security strengths of the generated keys when the module is ported to the vendor affirmed platforms that are not listed on the validation certificate.

Rev.C, Copyright © 2024 Forcepoint

2.5.Approved Algorithms

The following associated CAVP certificates are used by the cryptographic module:

> **Forcepoint NGFW Cryptographic Kernel Module** (Cert. #A2166)

The approved algorithms implemented by the module alongside their mapping to the certificates above alongside algorithms use by services are listed in the table below.

TABLE 4: APPROVED ALGORITHMS

CAVP Cert	Algorithm and Standard	Mode / Method	Description / Key Size(s) / Key Strength(s)	Use / Function
Symmetric Encryption/Decryption				
#A2166	AES-CBC, AES-CFB128, AES-ECB, AES-GCM, AES-OFB FIPS 197, SP 800-38A, SP 800-38D	AES-CBC, AES-CFB128, AES-ECB, AES-GCM, AES-OFB	Direction: Encrypt, Decrypt Key Length: 128, 192, 256	Used for encryption and decryption services

Rev.C, Copyright © 2024 Forcepoint

CAVP Cert	Algorithm and Standard	Mode / Method	Description / Key Size(s) / Key Strength(s)	Use / Function
Hashing				
#A2166	SHA-1, SHA2-224, SHA2-256, SHA2-384, SHA2-512 FIPS 180-4	SHA-1, SHA2-224, SHA2-256, SHA2-384, SHA2-512	BYTE only	Used for secure hashing services
Message Authentication Code				
#A2166	HMAC-SHA-1, HMAC-SHA2-224, HMAC-SHA2-256, HMAC-SHA2-384, HMAC-SHA2-512 FIPS 198-1	SHA-1, SHA2-224, SHA2-256, SHA2-384, SHA2-512	HMAC-SHA-1 (96, 160 bit MAC; > 112 bit keys) HMAC-SHA2-224 (128, 224 bit MAC; > 112 bit keys) HMAC-SHA2-256 (96, 128, 256 bit MAC; > 112 bit keys) HMAC-SHA2-384 (128, 192, 384 bit MAC; > 112 bit keys) HMAC-SHA2-512 (128, 256, 512 bit MAC; > 112 bit keys)	Used for message authentication services and module integrity

Rev.C, Copyright © 2024 Forcepoint

The module does not implement any non-approved algorithms allowed in the approved mode of operation. The module does not implement any non-approved algorithms allowed in the approved mode of operation with no security claimed.

3. Cryptographic Module Interfaces

3.1. Ports and Interface Overview

The figures in section Module Description identify the physical interfaces to the cryptographic module. The following table maps the physical interface to logical interfaces and supported data.

TABLE 5: PORTS AND INTERFACES

Physical port	Logical interfaces	Data that passes over port/interface
N/A	Data Input, Data Output, Control Input, Status Output	API Input Parameters, API Output Parameters and Return Values, API Functions, Console, Kernel Ring Buffer
N/A	Data Input, Data Output, Control Input, Status Output	API Input Parameters, API Output Parameters and Return Values, API Functions, Console, Kernel Ring Buffer
N/A	Data Input, Data Output, Control Input, Status Output	API Input Parameters, API Output Parameters and Return Values, API Functions, Console, Kernel Ring Buffer
N/A	Status Output	API Return Values, Console, Kernel Ring Buffer
N/A	Power Input	N/A

Rev. B, Copyright © 2024 Forcepoint

4. Roles, Services, and Authentication

4.1. Roles

The mapping of the cryptographic module's roles services is in the table below:

TABLE 6: ROLES, SERVICE COMMANDS, INPUT AND OUTPUT

Role	Service	Input	Output
Crypto officer	Initialize module	NA	NA
Crypto officer	Uninitialize module	NA	NA
User	Show status	NA	Status
User	Perform self-tests	NA	Indicator of success or failure
User	Perform zeroization	State record	NA
User	Show module versioning information	NA	Version
User	Perform encryption and decryption (AES)	Key and data to process	Encrypted or decrypted data
User	Perform authenticated encryption and decryption (AES-GCM)	Key and data to process	Encrypted or decrypted data
User	Perform secure hash (SHS)	Data to process	Message digest
User	Perform message authentication (HMAC)	Key and data to process	Message authentication code

Rev. B, Copyright © 2024 Forcepoint

Roles and Authentication

All roles are assumed implicitly based on the API that is currently being executed.

TABLE 7: ROLES AND AUTHENTICATION

Role	Authentication Method	Authentication Strength
Crypto Officer	Implicitly assumed when the APIs associated with the 'Crypto Officer' services are being exercised.	N/A
User	Implicitly assumed when the APIs associated with the 'User' services are being exercised.	N/A

4.2.Services

All services listed in the table below can be accessed in approved mode and when in this mode exclusively use the security functions listed in Approved Algorithms.

Notes on the content of Table 8: Approved Services:

> In the 'Access Rights to Keys and/or SSPs' column:

- G = Generate: The module generates or derives the SSP.
- R = Read: The SSP is read from the module (e.g., the SSP is output).
- W = Write: The SSP is updated, imported, or written to the module.
- E = Execute: The module uses the SSP in performing a cryptographic operation.
- Z = Zeroize: The module zeroizes the SSP.

In the 'Keys and/or SSPs' column:

For a complete description of SSP referenced from the table, see section Sensitive Security Parameter Management.

Rev. B, Copyright © 2024 Forcepoint

TABLE 8: APPROVED SERVICES

Service	Description	Approved Security Functions	Key and/or SSPs	Roles	Access Rights to Keys and/or SSPs	Indicator
Initialize module	Prepare the module for operation **API Functions:** • ssh_crypto_library_initialize • ssh_crypto_register_error_callback • ssh_crypto_get_certification_mode • ssh_crypto_set_certification_mode	N/A	N/A	Crypto Officer	N/A	SSH_CRYPTO_OK (0) from associated API Functions
Uninitialize module	Take the module out of operation **API Functions:** • ssh_crypto_free • ssh_crypto_library_uninitialize	N/A	N/A	Crypto Officer	N/A	SSH_CRYPTO_OK (0) from associated API Functions
Show status	Query the status of the module **API Functions:** • ssh_crypto_library_get_status • ssh_crypto_status_message	N/A	N/A	User	N/A	SSH_CRYPTO_OK (0) from associated API Functions

Rev. B, Copyright © 2024 Forcepoint.

Service	Description	Approved Security Functions	Key and/or SSPs	Roles	Access Rights to Keys and/or SSPs	Indicator
Perform self-tests	Re-run pre-operational and conditional self-tests **API Functions:** • ssh_crypto_library_self_tests	AES-CBC, AES-CFB128, AES-ECB, AES-OFB, AES-GCM, SHA-1, SHA2-256, SHA2-512, HMAC-SHA-1, HMAC-SHA2-256, HMAC-SHA2-512	HMAC Key for Module Integrity Check	User	E	SSH_CRYPTO_OK (0) from associated API Functions

Service	Description	Approved Security Functions	Key and/or SSPs	Roles	Access Rights to Keys and/or SSPs	Indicator
Perform zeroization	Zeroize keys by freeing crypto operation state records **API Functions:** • ssh_cipher_free • ssh_mac_free	N/A	AES Symmetric Keys HMAC Keys	User	Z	SSH_CRYPTO_OK (0) from associated API Functions
Show module versioning information	Query the version of the module **API Functions:** • ssh_crypto_library_get_version	N/A	N/A	User	N/A	SSH_CRYPTO_OK (0) from associated API Functions

Rev. B, Copyright © 2024 Forcepoint.

Perform encryption and decryption (AES)	Perform cryptography **API Functions:** • ssh_cipher_allocate • ssh_cipher_get_block_length • ssh_cipher_get_iv • ssh_cipher_get_iv_length • ssh_cipher_get_key_length • ssh_cipher_get_max_key_length • ssh_cipher_get_min_key_length • ssh_cipher_get_supported • ssh_cipher_has_fixed_key_length • ssh_cipher_is_fips_approved • ssh_cipher_name • ssh_cipher_set_iv • ssh_cipher_supported • ssh_cipher_transform • ssh_cipher_transform_remaining • ssh_cipher_transform_with_iv • ssh_cipher_get_block_len • ssh_cipher_auth_reset • ssh_cipher_auth_update • ssh_cipher_auth_final • ssh_cipher_auth_digest_length • ssh_cipher_is_auth • ssh_cipher_generate_iv_ctr • ssh_cipher_auth_digest_len	AES-CBC, AES-CFB128, AES-ECB, AES-GCM, AES-OFB	AES Symmetric Keys	User	W, E	SSH_CRYPTO_OK (0) from associated API Functions

Rev. B, Copyright © 2024 Forcepoint.

Service	Description	Approved Security Functions	Key and/or SSPs	Roles	Access Rights to Keys and/or SSPs	Indicator
Perform authenticated encryption and decryption (AES-GCM)	Perform cryptography **API Functions:** See 'Perform encryption and decryption (AES)'	AES-GCM	AES Symmetric Keys	User	W, E	SSH_CRYPTO_OK (0) from associated API Functions
Perform secure hash (SHS)	Perform cryptography **API Functions:** • ssh_hash_allocate • ssh_hash_digest_length • ssh_hash_final • ssh_hash_free • ssh_hash_get_supported • ssh_hash_input_block_size • ssh_hash_is_fips_approved • ssh_hash_name • ssh_hash_reset • ssh_hash_supported • ssh_hash_update	SHA-1, SHA2-224, SHA2-256, SHA2-384, SHA2-512	N/A	User	N/A	SSH_CRYPTO_OK (0) from associated API Functions

Rev. B, Copyright © 2024 Forcepoint.

Service	Description	Approved Security Functions	Key and/or SSPs	Roles	Access Rights to Keys and/or SSPs	Indicator
Perform message authentication (HMAC)	Perform cryptography **API Functions:** • ssh_mac_allocate • ssh_mac_final • ssh_mac_get_block_length • ssh_mac_get_max_key_length • ssh_mac_get_min_key_length • ssh_mac_get_supported • ssh_mac_is_fips_approved • ssh_mac_length • ssh_mac_name • ssh_mac_reset • ssh_mac_supported • ssh_mac_update	HMAC-SHA-1, HMAC-SHA2-224, HMAC-SHA2-256, HMAC-SHA2-384, HMAC-SHA2-512	HMAC Keys	User	W, E	SSH_CRYPTO_OK (0) from associated API Functions

5. Software/Firmware Security

5.1. Software Integrity

The Forcepoint NGFW Cryptographic Kernel Module's software integrity is checked on startup as described in section Self-Tests. The module runs the self-test functions to check the software integrity as well as the cryptographic algorithms used. Any failures during these tests will result in the module entering an error state where it will provide an error indicator.

The module is stored along with a 'checksums.fips' file which contains an HMAC-SHA-256 MAC of the module binary. The module checks its own integrity upon every load, and the operator can trigger an on-demand check of the module by either re-loading the module or executing the dedicated API function 'ssh_crypto_library_run_self_tests'.

6. Operational Environment

The module supports a **modifiable operating environment** as defined in ISO/IEC 19790:2012. The module operates on the NGFW OS 10 operating system, which is a hardened operating system based on GNU/Linux 4.19.

7. Physical Security

The module was tested on a Dell PowerEdge R440, the Forcepoint NGFW 3410, and NGFW 120W appliances. These appliances consist of production-grade components with standard passivation and a production-grade enclosure.

8. Non-Invasive Security

N/A: Section 8, Non-invasive security is non-Applicable as there are currently no requirement in SP 800-140F.

9. Sensitive Security Parameter Management

9.1. Sensitive Security Parameters

The following table lists Sensitive Security Parameters (SSP) used to perform approved security function supported by the cryptographic module.

The following notes should be observed when reading the table:

- When reading the 'strength' column, the listed security strength is calculated using methods in FIPS 140-3 IG D.B, 'Strength of SSP Establishment Methods'.
- When reading the 'Security Function and Cert Number' column, this is the security function that will consume the SSP.
- When reading the 'Use and Related Keys' column, this will contain the other SSPs that are either established via the SSP, other SSPs that are used to establish the SSP, or if it is a key pair the associated public or private component will be listed as well.

Rev. B, Copyright © 2024 Forcepoint

TABLE 9: SSPS

Key / SSP Name / Type	Strength	Security Function and Cert Number	Generation	Import/ Export	Establishment	Storage	Zeroisation	Use and Related Keys
AES Symmetric Keys	128-256 bits	AES-CBC, AES-CFB128, AES-ECB, AES-GCM, AES-OFB Cert. #A2166	N/A	Plaintext Electronic Entry from App	N/A	Plaintext in RAM	Zeroization API or Power Off	AES keys used for general encryption and decryption services **Related SSPs**: None
HMAC Keys	112-256 bits	HMAC-SHA-1, HMAC-SHA2-224, HMAC-SHA2-256, HMAC-SHA2-384, HMAC-SHA2-512 Cert. #A2166	N/A	Plaintext Electronic Entry from App	N/A	Plaintext in RAM	Zeroization API or Power Off	HMAC keys used for general message authentication services **Related SSPs**: None

Key / SSP Name / Type	Strength	Security Function and Cert Number	Generation	Import/ Export	Establishment	Storage	Zeroisation	Use and Related Keys
HMAC Key for Module Integrity Check	256 bits	HMAC-SHA2-256 Cert. # A2166	Pre-loaded (hard coded in module binary)	N/A	N/A	Plaintext in Persistent Storage	Not Required per ISO 19780:2012 section 7.9.7, as it's used solely for self-test purposes	HMAC key used for integrity check **Related SSPs**: None **Note:** Per ISO/IEC19790:2012 section 7.5, this key is only used for the approved integrity technique, and as such is not considered an SSP. However, it has been included in this table for completeness.

10. Self-Tests

10.1. Pre-Operational Tests

The pre-operational self-tests are run automatically when the module is loaded to confirm the software integrity, and to check the continued correct operation of each of the implemented cryptographic algorithms used in support of the integrity checks. User may initiate the on-demand pre-operational self-tests by calling the API function ssh_crypto_library_self_tests.

While the module is running these self-tests, all data output interfaces are disabled until the successful completion of the self-tests. If one of the pre-operational self-tests fails or a conditional self-test fails, the module enters an error state. Error indicators are output on the status output interface specifying which self-test failed within the module. In this state, all cryptographic functions and data output via the module's data output interfaces is inhibited. If the module is re-loaded, it will rerun all self-tests. Successful completion of the self-tests will clear the error state, and the module will return to the approved mode of operation. For any consecutive failure of the self-tests during reload, the module will remain in an error state. If the problem persists, CO intervention is required to either perform a restore to factory default settings and reinstall, or power-off the Forcepoint NGFW and contact Forcepoint Customer Support.

TABLE 10: PRE-OPERATIONAL SELF-TESTS

Test	Operations Performed	Indicator
Kernel Module Integrity Test	HMAC-SHA2-256 Verify	**SSH_CRYPTO_TEST_INTEG_DIGEST** or **SSH_CRYPTO_TEST_INTEG_INVALID** and error state entry

10.2. Conditional Tests

The module automatically performs conditional self-tests based on the module operation. These self-tests do not require operator input to initiate. Implemented conditional tests are in one of the following forms:

- Known Answer Test (KAT)

All KATs are performed immediately following the pre-operational self-tests when the module is loaded, and can be performed on-demand by the User by calling the API function ssh_crypto_library_self_tests.

TABLE 11: CONDITIONAL SELF-TESTS (SOFTWARE)

Test	Cryptographic Mechanism Tested	Location	When Performed	Operations Performed	Indicator
KAT test for AES encryption	AES-CBC, AES-CFB128, AES-ECB, AES-OFB 128, 192, 256	Cert. #A2166	Upon Library Load	Encryption	**SSH_CRYPTO_TEST_CIPHER** and error state entry
KAT test for AES decryption	AES-CBC, AES-CFB128, AES-ECB, AES-OFB 128, 192, 256	Cert. #A2166	Upon Library Load	Decryption	**SSH_CRYPTO_TEST_CIPHER** and error state entry

Test	Cryptographic Mechanism Tested	Location	When Performed	Operations Performed	Indicator
KAT test for AES-GCM authenticated encryption	AES-GCM 128	Cert. #A2166	Upon Library Load	Encryption	**SSH_CRYPTO_TEST_CIPHER** and error state entry
KAT test for AES-GCM authenticated decryption	AES-GCM 128	Cert. #A2166	Upon Library Load	Decryption	**SSH_CRYPTO_TEST_CIPHER** and error state entry
KAT test for SHA	SHA-1, SHA2-256, SHA2-512	Cert. #A2166	Upon Library Load	Hashing	**SSH_CRYPTO_TEST_HASH** and error state entry
KAT test for HMAC	HMAC-SHA-1, HMAC-SHA2-256, HMAC-SHA2-512	Cert. #A2166	Upon Library Load	MAC Generation, Verification	**SSH_CRYPTO_TEST_MAC** and error state entry

11. Life-Cycle Assurance

11.1. Installation

The cryptographic module is delivered as part of the Forcepoint NGFW firmware for appliances and Forcepoint NGFW software installation package for virtualization platforms. The FIPS 140-3 validated Forcepoint NGFW Cryptographic Kernel Module version 3.0 is included in Forcepoint NGFW firmware and software installation package version 6.10.3.26158.

The Forcepoint NGFW component providing the firewall and VPN capabilities on a Linux-based operating system is referred to as NGFW Engine. When NGFW Engine is initialized in approved mode of operation, the Forcepoint NGFW Cryptographic Kernel Module is loaded. Once loaded, the Forcepoint NGFW Cryptographic Kernel Module supports only the approved mode of operation.

The following sections detail how to ensure that the validated version of the module is installed and being utilized by the Forcepoint NGFW.

11.1.1. Downloading the Forcepoint NGFW Cryptographic Kernel Module

Forcepoint NGFW appliances are delivered in an operational state with the most recent firmware preinstalled. The NGFW firmware must be upgraded to a NGFW firmware version containing the FIPS 140-3 validated Forcepoint NGFW Cryptographic Kernel Module version 3.0 to be placed in the approved mode of operation.

Note: Upgrading an appliance to a Forcepoint NGFW firmware version is necessary even if the same version was installed previously. This is required because the file system checksum is stored during the upgrade process. A method to update the firmware image with a SHA2-512 checksum signed with ECDSA P-521 is provided. Prior to installing the new image, its associated checksum is checked. If the signature check fails, the new firmware is ignored, and the current firmware remains loaded. If the signature check passes, the new image will be installed and executed after the appliance is restarted. Failure to follow this will result in the module operating in a non-compliant state.

Rev. B, Copyright © 2024 Forcepoint

Forcepoint NGFW may also be installed on supported virtualization platforms. An existing virtual machine must be upgraded to a Forcepoint NGFW software version containing the FIPS 140-3 validated Forcepoint NGFW Cryptographic Kernel Module version 3.0 to be placed in the approved mode of operation by reinstalling the Forcepoint NGFW software.

The installation file is downloaded as follows:

1. Login to the Forcepoint Support https://support.forcepoint.com
2. Proceed to the **Forcepoint NGFW downloads** section.
3. Download the installation file
    a. For upgrading the NGFW appliance firmware, download the .zip file
    b. For installing the NGFW software on a virtual machine, download the .iso file
4. Verify the SHA checksum

Note: The correct checksums are shown on the download page and can also be found in the release notes.

11.1.2. Upgrading on a Forcepoint NGFW Appliance

After downloading the firmware, the operator can upgrade the NGFW appliance to a version containing the validated module:

1. Save the NGFW firmware version upgrade .zip file to the root directory of a USB drive. **Note** – The firmware upgrade .zip file must be in the root directory of the media.
2. Connect to the appliance using a monitor and keyboard.
3. Power on the appliance and start the NGFW Configuration Wizard.
4. Select the Firewall/VPN option.
5. Select **Upgrade**. The Select Source Media dialog opens.
6. Select the appropriate media type and select **OK**. The firmware update signature is verified.
7. Select **OK**. The upgrade starts.
8. Select **Set kernel in FIPS mode** after restart. Select **OK**.
9. The NGFW appliance restarts and displays the upgraded version.
10. Verify the NGFW firmware version to ensure that the correct NGFW firmware version is loaded.

This process also results in the NGFW appliance being configured to load the Forcepoint NGFW Cryptographic Kernel Module.

11.1.3. Installing on a Virtual Machine

After downloading the installation package, the operator can install the NGFW software containing the validated module on a virtual machine:

1. Connect the DVD drive of the virtual machine to the .iso file.
2. Restart the virtual machine. The License Agreement appears.
3. Type **YES**, then press Enter to accept the license agreement and continue with the configuration.
4. Select the type of installation:
    a. Type **1** for the normal Full Install.
    b. Type **2** for the Full Install in expert mode if you want to partition the hard disk manually
5. Enter the number of processors:
    a. For a uniprocessor system, type **1**, then press Enter.

Rev. B, Copyright © 2024 Forcepoint

   b. For a multiprocessor system, type **2**, then press Enter.
6. Continue in one of the following ways:
   a. If you selected Full Install, type **YES**, then press Enter to accept automatic hard disk partitioning.
   b. If you selected Full Install in expert mode, install the engine in expert mode.
7. The installation process starts. When the installation is ready press Enter to reboot.
8. The virtual machine restarts and displays the installed version.
9. Verify the NGFW software version to ensure that the correct NGFW software version is loaded.

11.2. Setting up a FIPS-Compatible Configuration on the Engine

To configure the NGFW Engine:

1. Start the NGFW Configuration Wizard as instructed in the **Configuring the Engine in the Engine Configuration Wizard** section of the NGFW Installation Guide.
2. Configure the Operating System settings as instructed in the **Configuring the Operating System Settings** section of the NGFW Installation Guide. Select **Restricted FIPS-compatible operating mode**. The SSH daemon and root password options are automatically disabled in the Engine Configuration Wizard. Select **FIPS 140-3 compatible mode** as well.
3. Configure the network interfaces according to your environment as instructed in the **Configuring the Network Interfaces** section of the NGFW Installation Guide.
4. Contact the Management Server as instructed in the **Contacting the Management Server** section of the NGFW Installation Guide. Enter node IP address manually is selected by default and other IP address options are disabled when FIPS-compatible operating mode is enabled. The engine restarts.

Note: To migrate from FIPS-compatible operating mode to FIPS 140-3 compatible mode, the engine must be reset to factory default settings and reinstalled.

11.3. Verifying Activation of FIPS 140-3 Compatible Operating Mode

Restricted FIPS 140-3 compatible operating mode must be enabled during the initial configuration of the engine. The following steps describe how to verify that FIPS 140-3 compatible operating mode has been activated.

To verify activation of FIPS 140-3 compatible operating mode:

1. Verify that the following messages are displayed on the console when the engine restarts:

   FIPS: rootfs integrity check OK

   (Displayed after the root file system integrity test has been executed successfully)

   FIPS power-up tests succeeded

   (Displayed after the FIPS 140 power-up tests have been executed successfully)

2. Continue as instructed in the **After Successful Management Server Contact** section of the NGFW Installation Guide.

Note: If the engine does not enter FIPS-compatible operating mode even though it is configured to do so, or if the power-up tests fail (a power-up test error message is displayed or the success message is not displayed), the engine must be reset to factory default settings and reinstalled.

Rev. B, Copyright © 2024 Forcepoint

11.4. Secure Initialization

The cryptographic module is initialized by loading the kernel module before any cryptographic functionality is available. The kernel module is loaded as follows:

 # modprobe qcl_fips.ko

- qcl_fips.ko is the name of the kernel module

The operation is performed automatically by the Forcepoint NGFW engine when configured to operate in the approved mode.

11.5. Secure Sanitization

The stored keys and CSPs are zeroized when the application calls the appropriate API function: ssh_cipher_free and ssh_mac_free. It is the calling application's responsibility to call the zeroization API function to zeroize the keys and CSPs. Temporary key material is zeroized automatically by the module when no longer needed. All keys and CSPs can be zeroized by powering off the platform where the module is running.

11.6. Guidance

11.6.1. Identifying the Module Version

The version of the module (3.0) is stored within the module binary itself (qcl_fips.ko), and is made available to a calling application via the API call ssh_crypto_library_get_version.

11.6.2. Non-Approved Mode of Operation

The module does not support a non-approved mode of operation.

11.6.3. Resetting the Engine to Factory Default Settings

Resetting the engine to factory default settings is not part of the normal installation procedure. There is no need to reset the engine to factory default settings before starting to use it for the first time. These instructions can be used to reset the engine to factory default settings when necessary, such as when initial configuration has been completed without enabling the Restricted FIPS-compatible operating mode, during use, or when the engine is being removed from use.

To reset the engine to factory default settings:

1. Reboot the engine and select **System restore options** from the boot menu. Forcepoint NGFW System Restore starts.
2. Enter 2 for **Advanced data removal options**.
3. Enter one of the following options:
   - 1 for **1 pass overwrite**
   - 8 for a **Custom** number of overwrite passes

If you selected **Custom**, enter the number of overwrite passes. A larger number of overwrites is more secure, but it may take a considerable amount of time depending on the engine storage capacity.

11.6.4. Recovering from a FIPS 140 Self-test Failure

If the FIPS 140 power-up self-tests fail, or the engine does not enter FIPS-compatible operating mode, the engine must be reset to factory default settings and reinstalled according to these instructions. Begin by Resetting the engine to factory default settings.

To recover from a FIPS 140 self-test failure:

1. Reset the engine to factory default settings as instructed in Error! Reference source not found.
2. Repeat the engine version installation/upgrade as instructed in sections **11.1.1, 11.1.2** and **11.1.3** of this document.
   Note: The firmware upgrade step from **Section 11.1.2** is only applicable to hardware engines.

3. Configure the firewall engine and enable FIPS-compatible operating mode as instructed in **Setting up a FIPS-Compatible Configuration on the Engine**
4. Verify that FIPS-compatible operating mode is activated as instructed in **Verifying Activation of FIPS 140-3 Compatible Operating Mode**

11.6.5. User Guidance

The notes below provide additional guidance and policies that must be followed by module operators:

- **Use of AES GCM**:
  - The module complies with Scenario 3 from FIPS 140-3 IG C.H via the module's ssh_cipher_generate_iv_ctr API. The module maintains a deterministic 64-bit non-repetitive counter that increments by 1 any time the API is called. The API will return 'SSH_CRYPTO_INVALID_OPERATION' and fail if the 64-bit counter has wrapped around. The IV's total length is 96 bits, with 32 of the bits being the 'name' and 64 bits being the described deterministic non-repetitive counter.
  - If the module's power is lost and then restored, the key used for the AES GCM encryption/decryption shall be redistributed.
- **Zeroization**: When a cryptographic key is no longer used, the key must be zeroized and freed using the ssh_cipher_free and ssh_mac_free functions for symmetric key encryption/decryption and message authentication keys, respectively.

11.6.6. External Guidance Documents

Forcepoint NGFW Installation Guide:

https://help.forcepoint.com/docs/ngfw/v610/install/ngfw_6100_ig_a_en-us.pdf

Forcepoint NGFW Product Guide:

https://help.forcepoint.com/docs/ngfw/v610/mgmt/ngfw_6100_pg_a_en-us.pdf

12. Mitigation of Other Attacks

This section is not applicable. The modules do not claim to mitigate any attacks beyond the FIPS 140-3 Level 1 requirements for this validation.