Forcepoint Next Generation Firewall

LEVEL 2 NON-PROPRIETARY SECURITY POLICY

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

Revision History

Revision	Date	Reason
A	March 9, 2022	Initial release.
B	February 22, 2024	CMVP Comment Responses

Trademarks, Copyrights, and Third-Party Software

Preface

This is a non-proprietary Cryptographic Module Security Policy for the Next Generation Firewall (Hardware Version: 2201, 2205, 2210, 3401 and 3410; firmware Version: 6.10.3.26158) from Forcepoint. This Security Policy describes how the Next Generation Firewall appliances (referred as NGFW appliances, modules, firewalls) 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 modules in a secure Approved mode of operation. This policy was prepared as part of the Level 2 FIPS 140-3 validation of the module. The Next Generation Firewall appliances are referred to in this document as the NGFW appliances, crypto modules, or modules.

Table of Contents

List of Figures

List of Tables

1. General

1.1 Security Level

The Forcepoint Next Generation Firewall meets all level 2 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	2
2	Cryptographic Module Specification	2
3	Cryptographic Module Interfaces	2
4	Roles, Services, and Authentication	2
5	Software/Firmware Security	2
6	Operational Environment	N/A
7	Physical Security	2
8	Non-Invasive Security	N/A
9	Sensitive Security Parameter Management	2
10	Self-Tests	2
11	Life-Cycle Assurance	2
12	Mitigation of Other Attacks	N/A

2. Cryptographic Module Specification

2.1 Module Overview

The NGFW appliances are high-performance network security appliances that add a broad range of built-in security features, including VPN, IPS, anti-evasion, TLS inspection, SD-WAN, and mission-critical application proxies, to a traditional firewall and provides end-to-end protection across the entire enterprise network. All appliances can be

deployed as either a Layer 2 or Layer 3 firewall or a next generation IPS. However, in the FIPS 140-3 approved mode, the appliances are deployed in Firewall/VPN mode of operation, which provides access control and VPN connectivity. Each of the appliances run NGFW firmware version 6.10.3.26158 based on the NGFW OS 10 operating system with Linux kernel version 4.19.

2.2 Module Description

The cryptographic module is a **hardware module** of type **multi-chip standalone**. The cryptographic boundary of the module is shown in the figures below. The cryptographic boundary is defined as the outer edge of the chassis.

The NGFW 2201, 2205, and 2210 appliances are a 1U rack-mounted design featuring modular connectivity. All the units are equipped with 9x GE RJ45 and 4x (2201) or 8x (2205, 2210) 10 Gbps SFP+ fixed Ethernet ports, and include an interface module slot, allowing for additional connectivity. The appliances contain an integrated, dual redundant (on the 2210), power supply that supports a wide range of voltages: 100 – 240 VAC or -72 – -36 VDC. The operating temperature range of the appliances is between +5°C to +40°C (+41°F to +104°F).

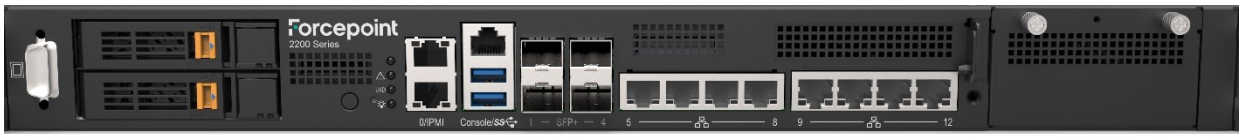

FIGURE 1: 2201 FRONT PANEL

FIGURE 2: 2201/2205 REAR PANEL

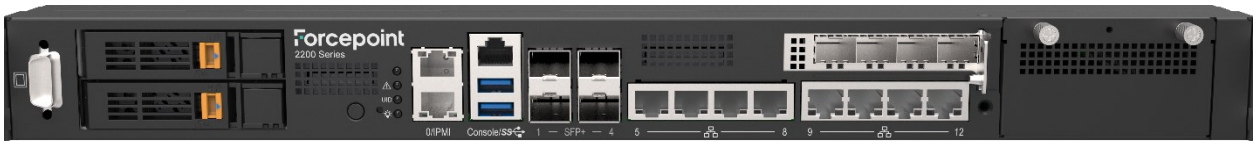

FIGURE 3: 2205/2210 FRONT PANEL

FIGURE 4: 2210 REAR PANEL

The NGFW 3401 and 3410 are a 2U rack-mounted design featuring modular connectivity. The NGFW 3400 series is equipped with 1x GE RJ45 and 2x 10 Gbps SFP+ fixed Ethernet ports, and includes eight Network I/O slots, allowing for additional connectivity. The appliance contains an integrated, dual redundant, power supply that supports a wide range of voltages: 100 – 240 VAC or -72 – -36 VDC. The operating temperature range of the appliances is between +5°C to +40°C (+41°F to +104°F).

FIGURE 5: 3400 SERIES FRONT PANEL

FIGURE 6: 3400 SERIES REAR PANEL

2.3 Test Configuration

The following tested configurations are covered in this security policy:

TABLE 2: CRYPTOGRAPHIC MODULE TESTED CONFIGURATION

Model	Hardware [Part Number and Version]	Firmware Version	Distinguishing Features
NGFW 2201	2201	Firmware: 6.10.3.26158	1U • Intel Xeon D-2123IT Skylake Processor • 1 Power Supply Unit • 2 x 16 GB DDR4 RAM
NGFW 2205	2205	Firmware: 6.10.3.26158	1U • Intel Xeon D-2145NT Skylake Processor • 1 Power Supply Unit • 4 x 10GE PCIe card • 2 x 16 GB DDR4 RAM
NGFW 2210	2210	Firmware: 6.10.3.26158	1U • Intel Xeon D-2177NT Skylake Processor • 2 Power Supply Units • 4 x 10GE PCIe card • 2 x 16 GB DDR4 RAM

Model	Hardware [Part Number and Version]	Firmware Version	Distinguishing Features
NGFW 3401	3401	Firmware: 6.10.3.26158	2U • Intel Xeon 4210 Cascade Lake Processor • 2 Power Supply Units • 8 Port Gigabit Ethernet RJ45 Module • 8 x 8GB RDIMM D4 RAM
NGFW 3410	3410	Firmware: 6.10.3.26158	2U • Intel Xeon 6230N Cascade Lake Processor • 2 Power Supply Units • 8 Port Gigabit Ethernet RJ45 Module • 12 x 16GB RDIMM D4 RAM

2.4 Cryptographic Algorithms

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

- **Forcepoint NGFW FIPS Cryptographic Module** (Cert. #A2155)
- **Forcepoint NGFW FIPS Library** (Cert. #A2209)
- **Forcepoint NGFW Cryptographic Kernel Module** (Cert. #A2166)
- **Forcepoint NGFW Entropy Library** (Cert. #A2167)

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. Note that the referenced algorithm certificates may contain more tested options than are utilized by the module, and that only those listed in the table below are implemented and used.

TABLE 3: APPROVED ALGORITHMS

CAVP Cert	Algorithm and Standard	Mode / Method	Description / Key Size(s) / Key Strength(s)	Use / Function
Forcepoint NGFW FIPS Cryptographic Module				
#A2155	AES FIPS 197, SP 800-38A, SP 800-38D, SP 800-38F	AES-CBC, AES-ECB, AES-GCM, AES-KWP	Direction: Encrypt, Decrypt Key Length: 128, 192, 256	Used for confidentiality of configuration files, logs, and monitoring data, management connections and services, peer connections, VPN, HTTPS, and TLS connections
Vendor Affirmed	CKG SP 800-133rev2[1]	RSA, EC, and FFC key pairs per FIPS 186-4 and SP 800-56Arev3 using the unmodified output of the DRBG for seeds. Symmetric keys using the unmodified output of the DRBG	RSA 2048, 3072 bits EC P-224, P-256, P-384, P-521 curves FFC 2048-8192 bits	Key generation for all module services that utilize internal generation
#A2155	CVL SP 800-135rev1	IKEv1 KDF, IKEv2 KDF, TLS 1.2 KDF[2]	IKE with SHA-1, SHA2-256, SHA2-384, SHA2-512 TLS with SHA2-256, SHA2-384, SHA2-512	TLS and IPsec connections

[1] The module complies with Section 6.1, 5, and Section 4 (Bullet 1) of SP 800-133rev2.

[2] No parts of the IKEv1, IKEv2, or TLS protocol, other than the approved cryptographic algorithms and the KDFs, have been tested by the CAVP and CMVP

CAVP Cert	Algorithm and Standard	Mode / Method	Description / Key Size(s) / Key Strength(s)	Use / Function
#A2155	DRBG SP 800-90A	AES-256-CTR	Prediction Resistance: No Supports Reseed Capabilities: Derivation Function Enabled: Yes Additional Input: 0-256 bits Entropy Input: 512-1024 bits Nonce: 256 bits Personalization String Length: 0-256 bits	All random number generation and key generation within the module
#A2155	ECDSA FIPS 186-4	Key Pair Generation, Signature Generation, Signature Verification, Public Key Validation	P-224, P-256, P-384 and P-521 curves SHA2-224, SHA2-256, SHA2-384, SHA2-512	Used in TLS and VPN connections for digital signatures
#A2155	HMAC FIPS 198-1	SHA-1, SHA2-224, SHA2-256, SHA2-384, SHA2-512	> 256 bit keys	Used for authentication of configuration files, logs, and monitoring data, management connections and services, peer connections, VPN, HTTPS, TLS connections and SNMP monitoring.

CAVP Cert	Algorithm and Standard	Mode / Method	Description / Key Size(s) / Key Strength(s)	Use / Function
#A2155	KAS SP 800-56Arev3	KAS-ECC-SSC with CVL (IKEv1 KDF)[3]	See KAS-ECC-SSC and CVL entries	Establishing session keys for VPN connections
		KAS-ECC-SSC with CVL (IKEv2 KDF)[3]	See KAS-ECC-SSC and CVL entries	Establishing session keys for VPN connections
		KAS-FFC-SSC with CVL (IKEv1 KDF)[4]	See KAS-FFC-SSC and CVL entries	Establishing session keys for VPN connections
		KAS-FFC-SSC with CVL (IKEv2 KDF)[4]	See KAS-FFC-SSC and CVL entries	Establishing session keys for VPN connections
#A2155	KAS SP 800-56Arev3	KAS-ECC-SSC with CVL (TLS 1.2 KDF)[3]	See KAS-ECC-SSC and CVL entries	Establishing session keys for TLS connections
		KAS-FFC-SSC with CVL (TLS 1.2 KDF)[3]	See KAS-FFC-SSC and CVL entries	Establishing session keys for TLS connections
#A2155	KAS-ECC-SSC SP 800-56Arev3	ephemeralUnified KAS Role: initiator, responder	Domain Parameter Generation Methods: P-224, P-256, P-384, P-521	Establishing shared secrets for TLS and VPN connections

[3] Key establishment methodology provides between 112 and 256 bits of encryption strength.

[4] Key establishment methodology provides between 112 and 202 bits of encryption strength.

CAVP Cert	Algorithm and Standard	Mode / Method	Description / Key Size(s) / Key Strength(s)	Use / Function
#A2155	KAS-FFC-SSC SP 800-56Arev3	dhEphem KAS Role: initiator, responder	Domain Parameter Generation Methods: ffdhe2048, ffdhe3072, ffdhe4096, ffdhe6144, ffdhe8192, MODP-2048, MODP-3072, MODP-4096, MODP-6144, MODP-8192	Establishing shared secrets for TLS and VPN connections
#A2155	KTS[5] SP 800-38F	AES-CBC HMAC	AES-128, AES-256 HMAC-SHA-1 with 160-bit keys HMAC-SHA2-256 with 256-bit keys HMAC-SHA2-384 with 384-bit keys	TLS and IPsec connections
#A2155	KTS[5] SP 800-38F	AES-GCM	AES-128, AES-256	TLS and IPsec connections
#A2155	KTS[6] SP 800-38F	AES-KWP	AES-256	Used in VPN connections

[5] Key establishment methodology provides 128 and 256 bits of encryption strength.

[6] Key establishment methodology provides 256 bits of encryption strength.

CAVP Cert	Algorithm and Standard	Mode / Method	Description / Key Size(s) / Key Strength(s)	Use / Function
#A2155	RSA FIPS 186-4	Key Pair Generation, Signature Generation, Signature Verification PKCS #1 v1.5 and PSS	1024 (verification only), 2048, 3072, 4096 bits SHA2-224, SHA2-256, SHA2-384, SHA2-512	Used in TLS and VPN connections for digital signatures
#A2155	Safe Primes Key Generation Safe Primes Key Verification SP 800-56Arev3	FFC key pairs per SP 800-56Arev3 using the unmodified output of the DRBG for seeds	Safe Prime Groups: ffdhe2048, ffdhe3072, ffdhe4096, ffdhe6144, ffdhe8192, MODP-2048, MODP-3072, MODP-4096, MODP-6144, MODP-8192	Key generation for all module services that utilize KAS-FFC-SSC
#A2155	SHS FIPS 180-4	SHA-1, SHA2-224, SHA2-256, SHA2-384, SHA2-512	BYTE only	Used in HTTPS user authentication and as a prerequisite for higher-level algorithms
Forcepoint NGFW FIPS Library				
#A2209	AES FIPS 197, SP 800-38A, SP 800-38C	AES-ECB, AES-CFB128	Direction: Encrypt, Decrypt Key Length: 128, 192, 256	Used in peer connections, SNMP monitoring
#A2209	KBKDF SP 800-108	SHA2-256 Counter and Feedback Mode	> 112 bit keys	Key Derivation

CAVP Cert	Algorithm and Standard	Mode / Method	Description / Key Size(s) / Key Strength(s)	Use / Function
#A2209	PBKDF SP 800-132	SHA-1, SHA2-256	128, 256-bit keys	Key Encryption, Key Derivation
Forcepoint NGFW Cryptographic Kernel Module				
#A2166	AES FIPS 197, SP 800-38A, SP 800-38D	AES-CBC, AES-GCM	Direction: Encrypt, Decrypt Key Length: 128, 192, 256	Used in VPN connections
#A2166	HMAC FIPS 198-1	SHA-1, SHA2-224, SHA2-256, SHA2-384, SHA2-512	> 112 bit keys	Used in VPN connections
#A2166	SHS FIPS 180-4	SHA-1, SHA2-224, SHA2-256, SHA2-384, SHA2-512	BYTE only	Used as a prerequisite for higher-level algorithms (HMAC)
Forcepoint NGFW Entropy Library				
N/A	ENT (NP) SP 800-90B	Non-physical RNG based on CPU timing jitter	Entropy source expected to provide full entropy in its outputs due to the vetted conditioning component. Raw noise expected to provide at least 1/3 bits of min-entropy per 64-bit sample.	Used to seed the module's DRBG
#A2167	SHA-3 FIPS 202	SHA3-256	BYTE only	Conditioning within the entropy source

TABLE 4: NON-APPROVED ALGORITHMS ALLOWED IN THE APPROVED MODE OF OPERATION WITH NO SECURITY CLAIMED

Algorithm	Caveat	Use / Function
Triple-DES-CBC	Use of a non-approved cryptographic algorithm to "obfuscate" a CSP allowed as per IG 2.4.A Scenario 1.	Used to obfuscate/de-obfuscate private keys stored on disk
SHA-1	Use of a non-approved cryptographic algorithm to "obfuscate" a CSP allowed as per IG 2.4.A Scenario 1.	Used to derive the key pair obfuscation and integrity protection keys

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
VGA port	Status output	Used for external connections to monitors, which can be used for status monitoring
SSD port (x2)	N/A	None
SSD port LEDs (x4)	Status output	Used to indicate whether an SSD is in the bay and SSD activity (reads and writes)
Interface module slot (x1 on 2200 series, x8 on 3400 series)	Data input, Data output, Control input, Control output, Status output	Network traffic

Physical port	Logical interfaces	Data that passes over port/interface
Interface module slot LEDs	Status output	Used to indicate link status and network activity
Power button	Control input	Used to turn on and turn off the module
Power LEDs (x3)	Status output	Used to indicate whether the module is running, in a standby state, or powered down
IPMI port	Disabled in the validated configuration	None
IPMI port LEDs (x2)	Status output	Used to indicate link status and network activity
Fixed Gb ethernet port (x9 on 2200 series, x1 on 3400 series)	Data input, Data output, Control input, Control output, Status output	Network traffic
Fixed ethernet port LEDs (x18 on 2200 series, x2 on 3400 series)	Status output	Used to indicate link status and network activity
Fixed SFP+ ports (x2 on 3400 series, x4 on 2201, x8 on 2205, 2210)	Data input, Data output, Control input, Control output, Status output	Network traffic
Fixed SFP+ port LEDs (x4 on 3400 series, x8 on 2201, x16 on 2205, 2210)	Status output	Used to indicate link status and network activity
Console port	Status output	Used for external connections to console monitors, which can be used for status monitoring
Console port LEDs (x2)	Status output	Used to indicate link status and console activity

Physical port	Logical interfaces	Data that passes over port/interface
USB ports (x2)	Control input, disabled after initialization	Can be used to input initial configuration from SMC
Power input (x1 on 2201, 2205, x2 on 2210, 3400 series)	Power input	Used to input power to the module
Power input LEDs (x2)	Status output	Used to indicate power input status
Fan LEDs (x3)	Status output	Used to indicate fan status

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, SERVICES, INPUT AND OUTPUT

Role	Service	Input	Output
Crypto officer	Initialize module	NA	NA
Crypto officer	Shut down the module	NA	NA
Crypto officer	Zeroize keys	NA	NA
Crypto officer	Display versioning information	NA	Module version information
Crypto officer	Show status	NA	Module status
Crypto officer	Perform self-tests	NA	NA
Crypto officer	Management Connection Service	Configuration commands	Configuration status

Role	Service	Input	Output
Crypto officer	Peer Connection Service	NA	Heartbeat, state synchronization data, and data synchronization data
Crypto officer	Key pair management service	Key pair request	NA
Crypto officer	User management service	Password hashes	NA
Crypto officer	Modify and apply configuration	Configuration commands	Configuration status
User	IPsec VPN Service	IKE key negotiation IPsec traffic	IKE key negotiation IPsec traffic
User	Mobile VPN Service	IKE key negotiation IPsec traffic	IKE key negotiation IPsec traffic
User	HTTPS User Authentication Service	TLS data	TLS data
User	TLS Inspection Service	TLS data	TLS data
User	HTTPS Proxy Service	TLS data	TLS data
Crypto officer	Export Logs and Monitoring Data Service	NA	Logs and monitoring data
User	SNMP Monitoring Service	SNMP requests	SNMP responses

4.2 Roles and Authentication

The module supports role-based authentication within the module, where all roles must authenticate to the module by providing their authentication data.

The module does not implement a limit on consecutive authentication attempts, as described in section 5.2.2 of SP 800-63B. However, this is mitigated by the two-second delay for failed user password attempts and by a conservative argument about network session rate for the other authenticators. The success probability for random attempts during a one-minute period, as shown in the third column of the below table, shows that the module is well protected against password guessing attacks for all authenticators.

Note: The strength of HMAC SHA-1 is estimated at 80 bits of strength in the analysis, below. NIST SP 800-107 states that the strength is somewhat less than 80 bits but does not specify a value. For simplicity, 80 bits are used in the analysis below. This does not change the conclusion if the actual strength is somewhat less than 80 bits.

TABLE 7: ROLES AND REQUIRED IDENTIFICATION AND AUTHENTICATION

Role	Authentication Method	Authentication Strength
Crypto Officer (SMC, Peer NGFW, Log Server)	Single factor cryptographic software (ECDSA Digital Signature, HMAC-SHA-1)	The public key used for authentication is ECDSA, yielding at least 112 bits of strength, assuming the smallest curve size P-224. The chance of a random authentication attempt falsely succeeding is 1 / (2^{112}). Assuming 1 attempt per microsecond, there can be 60,000,000 attempts in a one-minute period. This means that at worst case an attacker has the probability of breaking the authentication in one minute as 60,000,000 / (2^{112}).
User (SNMP)	Single factor cryptographic software (HMAC-SHA-1)	The SNMP key is the output of the SNMP KDF as described in NIST SP 800-135. The key is a 160-bit SHA-1 hash value. The chance of a random attempt falsely succeeding is 1 / (2^{80}). Assuming 1 attempt per microsecond, there can be 60,000,000 attempts in a one-minute period. This means that in the worst case, an attacker has the probability of guessing the key in one minute as 60,000,000/ (2^{80}).
User (HTTPS, Mobile VPN)	Memorized secret (SHA2-512)	Once properly configured, the

Role	Authentication Method	Authentication Strength
		minimum length of the password is 10 characters, with 94 different case-sensitive alphanumeric characters and symbols possible for usage. Assuming a minimum password length of 10 characters, the chance of a random attempt falsely succeeding is 1 / (94^{10}). The module adds a two-second delay between each login attempt. Therefore, the maximum number of login attempts is limited to 30 per minute. This means that in the worst case, an attacker has the probability of guessing the password in one minute as 30 / (94^{10}).
User (IPsec VPN)	Single factor cryptographic software (RSA or ECDSA Digital Signature) Memorized secret (HMAC-SHA-1)	PSK: The minimum PSK length is 14 characters. Therefore, assuming a minimum length password of 14 characters, the probability to guess every character successfully is 1 / (94^{14}). Assuming 1 attempt per microsecond, there can be 60,000,000 attempts in a one-minute period. This means that in the worst case, an attacker has the probability of guessing the key in one minute as 60,000,000 / (94^{14}). Digital Signature: The public key used for authentication can be either ECDSA or RSA, yielding at least 112 bits of strength, assuming

Role	Authentication Method	Authentication Strength
		the smallest curve size P-224 or modulus size 2048 bit. The chance of a random authentication attempt falsely succeeding is 1 / (2^{112}). Assuming 1 attempt per microsecond, there can be 60,000,000 attempts in a one-minute period. This means that at worst case an attacker has the probability of breaking the authentication in one minute as 60,000,000 / (2^{112}).

4.3 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 Cryptographic Algorithms.

Notes on the content of Table 8: Module 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 SSP Management.

TABLE 8: MODULE SERVICES

Service	Description	Approved Security Functions	Key and/or SSPs	Roles	Access Rights to Keys and/or SSPs	Indicator
Initialize module	Set up the module using NGFW Initial Configuration Wizard. The setup process includes mandatory firmware upgrade, applying initial configuration and enabling the Approved Mode of operation.	DRBG	Configuration File Protection Key Configuration File Protection Passphrase	Crypto officer	G, R,W,E	**Log field** Started in FIPS 140 operating mode.

Service	Description	Approved Security Functions	Key and/or SSPs	Roles	Access Rights to Keys and/or SSPs	Indicator
Shut down the module	Terminate module operations in preparation for powering off.	None	Ephemeral SSPs[7]	Crypto officer	Z	**Power LED** A shut down module is indicated by an unlit power LED.

[7] The designation of 'Ephemeral SSPs' encompasses any keys noted to be stored solely in the module's SDRAM in Table 10: Summary of SSPs

Service	Description	Approved Security Functions	Key and/or SSPs	Roles	Access Rights to Keys and/or SSPs	Indicator
Zeroize keys	The module will overwrite all CSPs. Zeroization of keys can be invoked by performing a factory reset exercising commands. The zeroization occurs while the module is still in the Approved mode, and the module is restored to a factory state.	DRBG	All CSPs	Crypto officer	E,Z	**Console output** System zeroization complete following reboot. Factory default settings restored.
Display versioning information	Display the module name and version information.	None	None	Crypto officer	N/A	**Console output**: Forcepoint NGFW version <version> **SMC monitoring interface**: version displayed in SMC monitoring window.

Service	Description	Approved Security Functions	Key and/or SSPs	Roles	Access Rights to Keys and/or SSPs	Indicator
Show status	Report the status of the module.	None	None	Crypto officer	N/A	**SMC monitoring interface** SMC: Approved mode displayed in SMC monitoring window
Perform self-tests	Perform all power-on self-tests.	See section Self-Tests	Firmware Integrity Check Public Key	Crypto officer	R,E	**Console output**: FIPS power-up tests succeeded. **Log field**: Cryptographic self-tests succeeded

Service	Description	Approved Security Functions	Key and/or SSPs	Roles	Access Rights to Keys and/or SSPs	Indicator
Management Connection Service	SMC establishes secure management connections to the module over TLS. After initializing the module and initial contact with SMC, all post-installation configuration and modification of initial configuration is secured using TLS connections from SMC.	AES, DRBG, ECDSA, HMAC, KAS-ECC-SSC, SHA, TLS KDF	TLS SSPs[8] DRBG SSPs[9]	Crypto officer	G,R,W,E	**Log field** Management; TLS: Connection established

[8] The designation of 'TLS SSPs' encompasses the TLS Encryption Key, TLS Authentication Key, TLS Pre-Master Secret, TLS Master Secret, TLS ECDSA Private Key, TLS ECDSA Public Key, TLS ECDH Private Key, TLS ECDH Public Key, TLS Trusted Certificates

[9] The designation of 'DRBG SSPs' encompasses the 256-bit DRBG Entropy Input, 256-bit DRBG Seed, 128-bit DRBG 'V' Value, and 256-bit DRBG 'Key' Value

Peer Connection Service	Peer NGFW modules establish secure network connection within a cluster.	AES, DRBG, ECDSA, HMAC, KAS-ECC-SSC, KAS-FFC-SSC, RSA, SHA, TLS KDF	Cluster Protocol Key, State Synchronization Key, HTTPS RSA Private Key, HTTPS RSA Public Key, IKE Encryption Key, IKE Authentication Key, SKEYID, SKEYID_d, SKEYSEED, SK_d, SK_pi, SK_pr, IPsec Encryption Key, IPsec Authentication Key, VPN RSA Private Key, VPN RSA Public Key, VPN ECDSA Private Key, VPN ECDSA Public Key, VPN DH Public Key, VPN ECDH Public Key TLS SSPs[8] DRBG SSPs[9]	Crypto officer	G,R,W,E	**Log field** **dsd**: FIPS: starting in FIPS compliant mode **ssd**: FIPS: starting in FIPS compliant mode **sendlogd**: FIPS: starting in FIPS compliant mode

Service	Description	Approved Security Functions	Key and/or SSPs	Roles	Access Rights to Keys and/or SSPs	Indicator
Key pair management service	SMC using the management communication protocol requests engine to generate key pair and certificate signing request.	AES, DRBG, ECDSA, HMAC, KAS-ECC-SSC, KBKDF, RSA, SHA, TLS KDF	VPN RSA Private Key, VPN RSA Public Key, VPN ECDSA Private Key, VPN ECDSA Public Key, HTTPS RSA Private Key, HTTPS RSA Public Key, Configuration File Encryption Key, Configuration File Authentication Key TLS SSPs[8] DRBG SSPs[9]	Crypto officer	G,R,W,E	**Log field** Private key <filename> has been created
User management service	SMC enters the user password hashes using LDAPS.	AES, DRBG, ECDSA, HMAC, KAS-ECC-SSC, SHA, TLS KDF	User Password TLS SSPs[8] DRBG SSPs[9]	Crypto officer	G,R,W,E	**Log field** slapd: FIPS: running in FIPS compliant mode

Modify and apply configuration	Verify and apply the configuration changes to the modules securely including configuration of client protection and server protection certificate authority and TLS credentials.	AES, HMAC, KBKDF, PBKDF	Configuration file encryption key, Configuration file authentication key, Key Encryption Passphrase, Key Encryption Key, VPN Pre-Shared Key, Client Protection CA RSA Private Key, Client Protection IM CA RSA Private Key, Client Protection IM CA ECDSA Private Key, Client Protection RSA Private Key, Client Protection ECDSA Private Key, SNMP Encryption Key, SNMP Authentication Key, Cluster Protocol Key	Crypto officer	G,R,W,E	**Log field** **Inspection**: System Policy-Loaded **Inspection**: System Policy-Applied

Service	Description	Approved Security Functions	Key and/or SSPs	Roles	Access Rights to Keys and/or SSPs	Indicator
IPsec VPN Service	VPN tunneling clients establish secure IPsec VPN connections to the module.	AES, DRBG, ECDSA, HMAC, IKE KDF, KAS-ECC-SSC, KAS-FFC-SSC, RSA, SHA	User Password, IKE Encryption Key, IKE Authentication Key, SKEYID, SKEYID_d, SKEYSEED,SK_d,SK_pi,SK_pr, IPsec Encryption Key, IPsec Authentication Key, VPN Trusted Certificates VPN SSPs[10] DRBG SSPs[9]	User	G,R,W,E	**Log field** IPsec VPN: IPsec SA initiator done IPsec VPN: IPsec SA responder done

[10] The designation of 'VPN SSPs' encompasses the VPN RSA Private Key, VPN ECDSA Private Key, VPN Pre-Shared Key, VPN DH Private Key, VPN DH Shared Secret, VPN ECDH Private Key, VPN ECDH Shared Secret, VPN Key Wrapping Key, VPN RSA Public Key, VPN ECDSA Public Key, VPN DH Public Key, VPN ECDH Public Key

Service	Description	Approved Security Functions	Key and/or SSPs	Roles	Access Rights to Keys and/or SSPs	Indicator
Mobile VPN Service	VPN tunneling clients establish secure IPsec VPN connections to the module.	AES, DRBG, ECDSA, HMAC, IKE KDF, KAS-ECC-SSC, KAS-FFC-SSC, RSA, SHA, TLS KDF	User Password, IKE Encryption Key, IKE Authentication Key, SKEYID, SKEYID_d, SKEYSEED,SK_d,SK_pi,SK_pr, IPsec Encryption Key, IPsec Authentication Key, VPN Trusted Certificates TLS SSPs[8] VPN SSPs[10] DRBG SSPs[9]	User	G,R,W,E	**Log field** IPsec VPN: Mobile session created IPsec VPN: Mobile session closed

Service	Description	Approved Security Functions	Key and/or SSPs	Roles	Access Rights to Keys and/or SSPs	Indicator
HTTPS User Authentication Service	End user's authentication to the module via web browser.	AES, DRBG, ECDSA, HMAC, KAS-ECC-SSC, KAS-FFC-SSC, RSA, SHA, TLS KDF	User Password HTTPS SSPs[11] DRBG SSPs[9]	User	G,R,W,E	**Log field** New user has been authorized User has been reauthorized

[11] The designation of 'HTTPS SSPs' encompasses the HTTPS Encryption Key, HTTPS Authentication Key, HTTPS Pre-Master Secret, HTTPS Master Secret, HTTPS RSA Private Key, HTTPS DH Private Key, HTTPS ECDH Private Key, HTTPS RSA Public Key, HTTPS DH Public Key, HTTPS ECDH Public Key

Service	Description	Approved Security Functions	Key and/or SSPs	Roles	Access Rights to Keys and/or SSPs	Indicator
TLS Inspection Service	Perform TLS inspection on HTTPS network traffic.	AES, DRBG, ECDSA, HMAC, KAS-ECC-SSC, KAS-FFC-SSC, RSA, SHA, TLS KDF	Trusted Internet Certificates Inspection SSPs[12] Client Protection SSPs[13] Server Protection SSPs[14] DRBG SSPs[9]	User	G,R,W,E	**Log field** Inspection; TLS Decrypted=true

[12] The designation of 'Inspection SSPs' encompasses the Inspection DH Private Key, Inspection ECDH Private Key, Inspection Encryption Key, Inspection Authentication Key, Inspection Pre-Master Secret, Inspection Master Secret, Inspection DH Public Key, Inspection ECDH Public Key

[13] The designation of 'Client Protection SSPs' encompasses the Client Protection CA RSA Private Key, Client Protection IM CA RSA Private Key, Client Protection IM CA ECDSA Private Key, Client Protection RSA Private Key, Client Protection ECDSA Private Key, Client Protection CA RSA Public Key, Client Protection IM CA RSA Public Key, Client Protection IM CA ECDSA Public Key, Client Protection ECDSA Public Key, and Client Protection ECDSA Public Key, Client Protection RSA Public Key

[14] The designation of 'Server Protection SSPs' encompasses the Server Protection RSA Private Key, Server Protection ECDSA Private Key, Server Protection RSA Public Key, and Server Protection ECDSA Public Key

Service	Description	Approved Security Functions	Key and/or SSPs	Roles	Access Rights to Keys and/or SSPs	Indicator
HTTPS Proxy Service	Sidewinder proxy used for outbound traffic.	AES, DRBG, ECDSA, HMAC, KAS-ECC-SSC, KAS-FFC-SSC, PBKDF, RSA, SHA. TLS KDF	Key Encryption Key, Trusted Internet Certificates SSM SSPs[15] DRBG SSPs[9]	User	G,R,W,E	**Log field** SSM Proxy; TLS Decrypted=true
Export Logs and Monitoring Data Service	Traffic logs and monitoring data are exported to Log Server securely.	AES, DRBG, ECDSA, HMAC, KAS-ECC-SSC, KAS-FFC-SSC, RSA, SHA, TLS KDF	TLS SSPs[8] DRBG SSPs[9]	Crypto officer	G,R,W,E	**Log field** entries are received by the log server. **SMC Monitoring** data shown in the SMC monitoring window

[15] The designation 'SSM SSPs' encompasses the SSM HTTPS DH Private Key, SSM HTTPS DH Public Key, SSM HTTPS ECDH Private Key, SSM HTTPS ECDH Public Key, SSM HTTPS Encryption Key, SSM HTTPS Authentication Key, SSM HTTPS Pre-Master Secret, SSM HTTPS Master Secret, SSM Client Protection RSA Private Key, SSM Client Protection ECDSA Private Key, SSM Client Protection RSA Public Key, and SSM Client Protection ECDSA Public Key

Service	Description	Approved Security Functions	Key and/or SSPs	Roles	Access Rights to Keys and/or SSPs	Indicator
SNMP Monitoring Service	SNMP manager receives network management information and traps.	AES, HMAC	SNMP Encryption Key, SNMP Authentication Key	User	R,E	**Log field** smonitd: FIPS starting in FIPS compliant mode

4.4 Alternating Bypass Feature

The module operates in an alternating bypass mode according to the policies set. The enabling and disabling of the bypass capability is performed via 'Modify and apply configuration' service allocated to the CO role. The module implements the following forms of alternating bypass:

VPN network traffic:

For policy-based VPN traffic, the module operates with bypass deactivated if the module action is set to IPsec VPN, where the module is operating to provide VPN service for the specified source/destination addresses. The module will encrypt/decrypt network traffic according to the policy. The module operates with bypass activated if the module action is set to allow in Access rules for network traffic, where the module is accepting/sending plaintext data for the specified source/destination addresses. For route-based VPN traffic, the module operates with bypass deactivated when network traffic is routed to module interfaces that are designated as endpoints for a VPN tunnel and is sent into the VPN tunnel. If Access rules allow the traffic, traffic is automatically sent through the tunnel to the endpoint. The module operates with bypass activated when network traffic is routed to module interfaces that accept plaintext data. Based on the Access rule (allow/discard), the traffic is either forwarded to the endpoint or dropped. In both cases, to activate the bypass feature, two independent actions must be taken by a CO. The CO must create the firewall policy allowing the bypass feature and apply the policy to the module to enable it.

Firewall network traffic:

The default action for network traffic in firewall Access rules is discard. For firewall traffic, the module operates with bypass deactivated if the traffic from the endpoint is sent/received using HTTPS, and the module action is set to allow. If traffic from the endpoint is passed directly to the module using HTTP, and the module action is set to allow, then the module is operating with bypass activated. For incoming traffic, if the HTTPS option is selected, the module connections with the endpoint are encrypted using TLS (bypass deactivated). If the HTTP option is selected, the module accepts connections in plaintext (bypass activated). For Outgoing traffic, If HTTPS is selected, web traffic will be re-encrypted using TLS (bypass deactivated). If HTTP is configured, web traffic is sent in plaintext (bypass activated). Two independent actions must be taken by a CO. The CO must create the firewall policy allowing bypass and apply to the module to enable it.

The rules in the policy that is currently applied to the module specify whether the module allows the encrypted or plaintext traffic. The status information for the bypass activation and deactivation can be viewed via established management connection from SMC as indicated below:

Bypass – When bypass is activated, the Situation field in the Logs view shows "Connection Allowed" and the TLS decrypted field in the Connections view is blank.

IPSEC VPN/HTTPS – The Situation field in the Logs view indicates the respective operations performed by these services. For example, "IPsec-SA-Responder-Done".

TLS inspection – For this service the Situation field in the Logs view shows “Connection_Allowed” and the TLS decrypted field in Connections view is "true".

4.5 Self-Initiated Cryptographic Output Capability

The Export Logs and Monitoring Data Service and the Peer Connection Service are self-initiated cryptographic output capabilities supported by the module. In both cases, these services are triggered by the module itself without a specific request to perform the service.

The **Export Logs and Monitoring Data Service** is enabled on the first policy push from the SMC where the Log Server address is specified. This is configured through two independent steps: adding the Log Server and activating the policy.

The **Peer Connection Service** is enabled when the module is joined to a cluster. While the module is in a cluster, this communication happens, and it stops when module is removed from the cluster. This is also configured through two independent steps:

- Installing the new engine (module) and performing the initial configuration after adding the engine to the Firewall Cluster element’s properties and defining the node-specific IP addresses of the new node.
- Refreshing the security policy of the Firewall Cluster.

The Crypto officer can make usage of the module’s Show status service to determine if the self-initiated cryptographic output capability is active by observing the ‘Status’ tab on the SMC Web GUI:

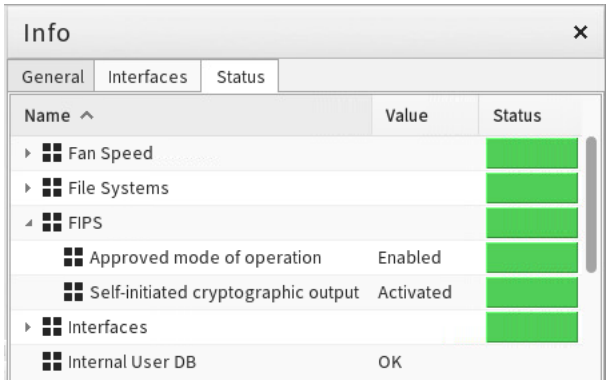

FIGURE 7: SELF-INITIATED CRYPTOGRAPHIC OUTPUT CAPABILITY STATUS ON SMC WEB GUI

5. Software/Firmware Security

5.1 Firmware Integrity

The Forcepoint Next Generation Firewall's firmware integrity is checked on startup as described in section Self-Tests. The module runs the self-test functions to check the firmware integrity as well as the cryptographic algorithms used. Any failures during these tests will result in a module halt in which an error message is output, the module reboots and data output is inhibited.

The images are stored as signed binaries using the "Firmware Integrity Check Public Key" which uses ECDSA with P-521 and SHA2-512. The operator can trigger an on-demand check of the module firmware by rebooting the module.

6. Operational Environment

Per Section 7.5 of the FIPS 140-3 Management Manual, this section is not-applicable. The module supports a **non-modifiable operating environment** as defined by ISO/IEC 19790:2012 and meets the Level 2 Physical Security requirements.

7. Physical Security

7.1 Module Construction

The module is enclosed in a strong metal (steel) enclosure that provides tamper-evidence. Any tampering that might compromise a module's security is detectable by visual inspection of the physical integrity of a module. The Crypto Officer should perform a visual inspection of the module at regular intervals.

The module's enclosure is opaque to resist visual inspection of the device design, physical probing of the device and attempts to access sensitive data on individual components of the device.

7.2 Tamper-Evident Labels

The following table depicts the number of tamper evident labels required for each hardware module:

Hardware Module	Number of Tamper Evident Labels Required
NGFW 2201	2
NGFW 2205	3
NGFW 2210	4
NGFW 3400	14

Each shipment of the Forcepoint NGFW FIPS Kit includes 25 tamper labels. Additional tamper labels can be purchased in single boxes of 25 (SKU: ACFIPS3) from Forcepoint.

In addition to the strong metal enclosure, the module employs uniquely numbered tamper-evident labels. The following images depict the tested, Approved TEL configurations for the modules:

FIGURE 8: 2205/2210 FRONT TEL PLACEMENTS

FIGURE 9: 2210 REAR TEL PLACEMENTS

FIGURE 10: 2201 FRONT TEL PLACEMENT

FIGURE 11: 2201/2205 REAR TEL PLACEMENT

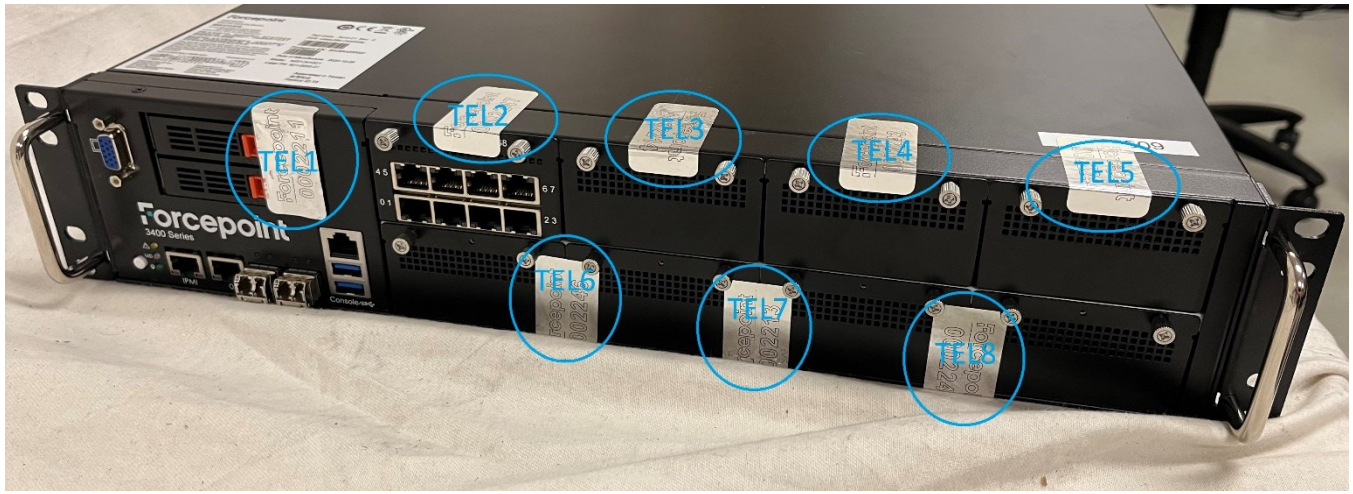

FIGURE 12: 3400 SERIES FRONT TEL PLACEMENTS

FIGURE 13: 3400 SERIES RIGHT SIDE TEL PLACEMENT

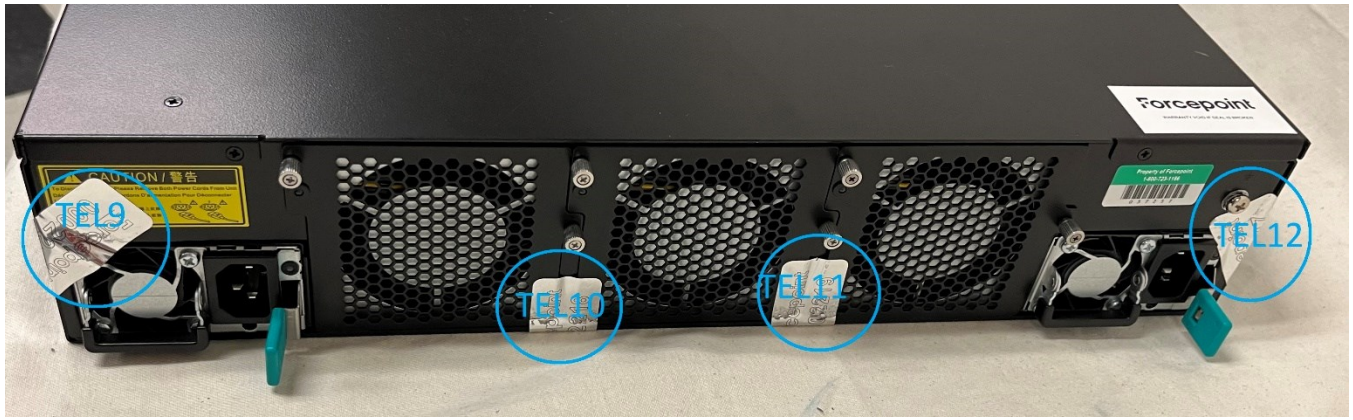

FIGURE 14: 3400 SERIES REAR TEL PLACEMENTS

FIGURE 15: 3400 SERIES LEFT SIDE TEL PLACEMENT

7.3 Internal Baffles

The module also employs internal baffles to deter visual observation of the internal components of the modules through vents. The following image depicts a vent that is protected by a baffle:

FIGURE 16: DEPICTION OF VENT PROTECTED BY INTERNAL BAFFLE

7.4 Module Inspection

The following routine inspections are recommended.

TABLE 9: PHYSICAL SECURITY INSPECTION GUIDELINES

Physical Security Mechanism	Recommended Frequency of Inspection/Test	Inspection/Test Guidance Details
Physical inspection of enclosure surfaces and tamper-evident seals for signs of tamper.	On receipt of module following transport. At any point following any un-authorized access to the environment hosting the module. Following any extended periods of unattended storage for the module.	<see below>.

Any attempts to remove the covers will result in tamper evidence.

Example (but not exhaustive) pictures of potential attempts to tamper a module are shown below:

If any evidence of tampering is observed on the module enclosures or tamper-evident seals, the modules shall be considered in a non-compliant state. Upon such discovery, the CO shall immediately take the module out of operation and contact Forcepoint Customer Support.

8. Non-Invasive Security

N/A: Section 8, Non-Invasive Security is Not-Applicable as there are currently no requirements in SP 800-140F.

9. SSP Management

9.1 Sensitive Security Parameter

The following table lists Sensitive Security Parameters (SSP) used to perform approved security functions 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.

TABLE 10: SUMMARY OF SSPS

Key / SSP Name / Type	Strength	Security Function and Cert Number	Generation	Import/ Export	Establishment	Storage	Zeroisation	Use and Related Keys
TLS Encryption Key	256 bits	AES Cert. #A2155	N/A	N/A	Derived using TLS 1.2 KDF	Plaintext in SDRAM	Automatically at the expiration of the session or Power off	Data encryption key used in TLS. Related SSPs: TLS Master Secret
TLS Authentication Key	256 bits	HMAC Cert. #A2155	N/A	N/A	Derived using TLS 1.2 KDF	Plaintext in SDRAM	Automatically at the expiration of the session or Power off	Authentication key used in TLS. Related SSPs: TLS Master Secret
TLS Pre-Master Secret	112-256 bits	KDF TLS Cert. #A2155	N/A	N/A	Established through Elliptical Curve Diffie-Hellman agreement using NIST SP 800-56Arev3	Plaintext in SDRAM	Automatically at the expiration of the session or Power off	Shared secret generated or established for a TLS session. Related SSPs: TLS ECDH Private Key, TLS ECDH Public Key, TLS Master Secret
TLS Master Secret	112-256 bits	KDF TLS Cert. #A2155	N/A	N/A	Derived using TLS 1.2 KDF	Plaintext in SDRAM	Automatically at the expiration of the session or Power off	Value calculated during TLS handshake. Related SSPs: TLS Pre-Master Secret, TLS Encryption Key, TLS Authentication Key
TLS ECDSA Private Key	112-256 bits	ECDSA Cert. #A2155	FIPS 186-4, Testing Candidates	N/A	Generated	Obfuscated (equivalent to Plaintext) on disk	Disk erasure	Private key used in TLS signature. Related SSPs: TLS ECDSA Public Key

Key / SSP Name / Type	Strength	Security Function and Cert Number	Generation	Import/ Export	Establishment	Storage	Zeroisation	Use and Related Keys
TLS ECDH Private Key	112-256 bits	KAS-ECC-SSC Cert. #A2155	SP 800-56Ar3, Testing Candidates	N/A	Generated	Plaintext in SDRAM	Automatically at the expiration of the session or Power off	Private ephemeral key agreement key used in TLS. Related SSPs: TLS Pre-Master Secret, TLS ECDH Public Key
IKE Encryption Key	128, 256 bits	AES Cert. #A2155	N/A	Input and Output Encrypted via TLS (KTS)	Derived using IKEv1 or IKEv2 KDF	Plaintext in SDRAM	Automatically at the expiration of the session or Power off	Data encryption key used in IKE negotiations. Related SSPs: SKEYID, SKEYID_d, SKEYSEED, SK_d, SK_pi, SK_pr
IKE Authentication Key	128-256 bits	HMAC Cert #A2155	N/A	Input and Output Encrypted via TLS (KTS)	Derived using IKEv1 or IKEv2 KDF	Plaintext in SDRAM	Automatically at the expiration of the session or Power off	Authentication key used in IKE negotiations. Related SSPs: SKEYID, SKEYID_d, SKEYSEED, SK_d, SK_pi, SK_pr
SKEYID, SKEYID_d	112-256 bits	KDF IKE Cert. #A2155	N/A	Input and Output Encrypted via TLS (KTS)	Derived using IKEv1 KDF	Plaintext in SDRAM	Automatically at the expiration of the session or Power off	Values calculated during IKE v1 negotiation. Related SSPs: VPN DH Shared Secret, VPN ECDH Shared Secret, VPN Pre-Shared Key, IKE Encryption Key, IKE Authentication Key, IPsec Encryption Key, IPsec Authentication Key

Key / SSP Name / Type	Strength	Security Function and Cert Number	Generation	Import/ Export	Establishment	Storage	Zeroisation	Use and Related Keys
SKEYSEED, SK_d, SK_pi, SK_pr	112-256 bits	KDF IKE Cert. #A2155	N/A	Input and Output Encrypted via TLS (KTS)	Derived using IKEv2 KDF	Plaintext in SDRAM	Automatically at the expiration of the session or Power off	Values calculated during IKEv2 negotiation. Related SSPs: VPN DH Shared Secret, VPN ECDH Shared Secret, VPN Pre-Shared Key, IKE Encryption Key, IKE Authentication Key, IPsec Encryption Key, IPsec Authentication Key
IPsec Encryption Key	128, 256 bits	AES Cert. #A2166	N/A	Input and Output Encrypted via TLS (KTS)	Derived using IKEv1 or IKEv2 KDF	Plaintext in SDRAM	Automatically at the expiration of the session or Power off	Data encryption key used in IPsec negotiations. Related SSPs: SKEYID, SKEYID_d, SKEYSEED, SK_d, SK_pi, SK_pr
IPsec Authentication Key	128-256 bits	HMAC Cert #A2166	N/A	Input and Output Encrypted via TLS (KTS)	Derived using IKEv1 or IKEv2 KDF	Plaintext in SDRAM	Automatically at the expiration of the session or Power off	Authentication key used in IPsec negotiations. Related SSPs: SKEYID, SKEYID_d, SKEYSEED, SK_d, SK_pi, SK_pr
VPN RSA Private Key	112-150 bits	RSA Cert. #A2155	FIPS 186-4, B.3.6	Input and Output Encrypted via TLS (KTS)	Generated	Encrypted on disk	Disk erasure	Private authentication key used in IKE. Related SSPs: VPN RSA Public Key
VPN ECDSA Private Key	112-256 bits	ECDSA Cert. #A2155	FIPS 186-4, Testing Candidates	Input and Output Encrypted via TLS (KTS)	Generated	Encrypted on disk	Disk erasure	Private authentication key used in IKE. Related SSPs: VPN ECDSA Public Key
VPN Pre-Shared Key	112-256 bits	KDF IKE Cert. #A2155	N/A	Input Encrypted via TLS (KTS)	Input	Plaintext or encrypted on disk	Disk erasure	Shared secret used in IKE. Related SSPs: SKEYID, SKEYID_d, SKEYSEED, SK_d, SK_pi, SK_pr

Key / SSP Name / Type	Strength	Security Function and Cert Number	Generation	Import/ Export	Establishment	Storage	Zeroisation	Use and Related Keys
VPN DH Private Key	112-202 bits	KAS-FFC-SSC Cert. #A2155	SP 800-56Ar3, Testing Candidates	N/A	Generated	Plaintext in SDRAM	Automatically after use or Power off	Private ephemeral key agreement key used in IKE. Related SSPs: VPN DH Public Key, VPN DH Shared Secret
VPN DH Shared Secret	112-202 bits	KDF IKE Cert. #A2155	N/A	N/A	Established via KAS-FFC-SSC Key Agreement	Plaintext in SDRAM	Automatically after use or Power off	Diffie-Hellman shared secret in IKE Related SSPs: VPN DH Private Key, VPN DH Public Key
VPN ECDH Private Key	112-256 bits	KAS-ECC-SSC Cert. #A2155	SP 800-56Ar3, Testing Candidates	N/A	Generated	Plaintext in SDRAM	Automatically after use or Power off	Private ephemeral key agreement key used in IKE. Related SSPs: VPN ECDH Public Key, VPN ECDH Shared Secret
VPN ECDH Shared Secret	112-256 bits	KDF IKE Cert. #A2155	N/A	N/A	Established via KAS-ECC-SSC Key Agreement	Plaintext in SDRAM	Automatically after use or Power off	Elliptical curve Diffie-Hellman shared secret in IKE Related SSPs: VPN ECDH Private Key, VPN ECDH Public Key
VPN Key Wrapping Key	256 bits	AES Cert. #A2155	N/A	N/A	Derived via KBKDF	Plaintext in SDRAM	Power off	IKE and IPsec key and key wrapping material Related SSPs: Cluster Protocol Key
HTTPS Encryption Key	128, 256 bits	AES Cert. #A2155	N/A	N/A	Derived using TLS 1.2 KDF	Plaintext in SDRAM	Automatically at the expiration of the session or Power off	Data encryption key used in TLS. Related SSPs: HTTPS Master Secret
HTTPS Authentication Key	256 bits	HMAC Cert. #A2155	N/A	N/A	Derived using TLS 1.2 KDF	Plaintext in SDRAM	Automatically at the expiration of the session or Power off	Authentication key used in TLS. Related SSPs: HTTPS Master Secret

Key / SSP Name / Type	Strength	Security Function and Cert Number	Generation	Import/ Export	Establishment	Storage	Zeroisation	Use and Related Keys
HTTPS Pre-Master Secret	112-256 bits	KDF TLS Cert. #A2155	N/A	N/A	Established through Diffie-Hellman agreement or Elliptical Curve Diffie-Hellman agreement using NIST SP 800-56Arev3	Plaintext in SDRAM	Automatically at the expiration of the session or Power off	Shared secret generated or established for a TLS session. Related SSPs: HTTPS DH Private Key, HTTPS DH Public Key, HTTPS ECDH Private Key, HTTPS ECDH Public Key, HTTPS Master Secret
HTTPS Master Secret	112-256 bits	KDF TLS Cert. #A2155	N/A	N/A	Derived using TLS 1.2 KDF	Plaintext in SDRAM	Automatically at the expiration of the session or Power off	Value calculated during TLS handshake. Related SSPs: HTTPS Pre-master Secret, HTTPS Encryption Key, HTTPS Authentication Key
HTTPS RSA Private Key	112-150 bits	RSA Cert. #A2155	FIPS 186-4, B.3.6	Input and Output Encrypted via TLS (KTS)	Generated	Obfuscated (equivalent to Plaintext) on disk	Disk erasure	Private authentication key used in HTTPS user authentication. Related SSPs: HTTPS RSA Public Key
HTTPS DH Private Key	112-202 bits	KAS-FFC-SSC Cert. #A2155	SP 800-56Ar3, Testing Candidates	N/A	Generated	Plaintext in SDRAM	Automatically after use or Power off	Private ephemeral key agreement key used in TLS. Related SSPs: HTTPS DH Public Key, HTTPS Pre-master Secret
HTTPS ECDH Private Key	112-256 bits	KAS-ECC-SSC Cert. #A2155	SP 800-56Ar3, Testing Candidates	N/A	Generated	Plaintext in SDRAM	Automatically after use or Power off	Private ephemeral key agreement key used in TLS. Related SSPs: HTTPS ECDH Public Key, HTTPS Pre-master Secret

Key / SSP Name / Type	Strength	Security Function and Cert Number	Generation	Import/ Export	Establishment	Storage	Zeroisation	Use and Related Keys
Client Protection CA RSA Private Key	112-150 bits	RSA Cert. #A2155	N/A	Input Encrypted via TLS (KTS)	Input	Encrypted on disk	Disk erasure	Private signature key used in TLS inspection CA. Related SSPs: Client Protection CA RSA Public Key
Client Protection IM CA RSA Private Key	112-150 bits	RSA Cert. #A2155	FIPS 186-4, B.3.6	N/A	Generated	Plaintext in SDRAM	Power off	Private authentication key used in TLS inspection. Related SSPs: Client Protection IM CA RSA Public Key
Client Protection IM CA ECDSA Private Key	112-256 bits	ECDSA Cert. #A2155	FIPS 186-4, Testing Candidates	N/A	Generated	Plaintext in SDRAM	Power off	Private authentication key used in TLS inspection. Related SSPs: Client Protection IM CA ECDSA Public Key
Client Protection RSA Private Key	112-150 bits	RSA Cert. #A2155	FIPS 186-4, B.3.6	N/A	Generated	Plaintext in SDRAM	Power off	Private authentication key used in TLS inspection. Related SSPs: Client Protection RSA Public Key
Server Protection RSA Private Key	112-150 bits	RSA Cert. #A2155	N/A	Input Encrypted via TLS (KTS)	Input	Encrypted on disk	Disk erasure	Private authentication key used in TLS inspection. Related SSPs: Server Protection RSA Public Key
Client Protection ECDSA Private Key	112-256 bits	ECDSA Cert. #A2155	FIPS 186-4, Testing Candidates	N/A	Generated	Plaintext in SDRAM	Power off	Private authentication key used in TLS inspection. Related SSPs: Client Protection ECDSA Public Key
Server Protection ECDSA Private Key	112-256 bits	ECDSA Cert. #A2155	N/A	Input Encrypted via TLS (KTS)	Input	Encrypted on disk	Disk erasure	Private authentication key used in TLS inspection. Related SSPs: Server Protection ECDSA Public Key

Key / SSP Name / Type	Strength	Security Function and Cert Number	Generation	Import/ Export	Establishment	Storage	Zeroisation	Use and Related Keys
Inspection DH Private Key	112-202 bits	KAS-FFC-SSC Cert. #A2155	SP 800-56Ar3, Testing Candidates	N/A	Generated	Plaintext in SDRAM	Automatically after use or Power off	Private ephemeral key agreement key used in TLS inspection. Related SSPs: Inspection DH Public Key, Inspection Pre-Master Secret
Inspection ECDH Private Key	112-256 bits	KAS-ECC-SSC Cert. #A2155	SP 800-56Ar3, Testing Candidates	N/A	Generated	Plaintext in SDRAM	Automatically after use or Power off	Private ephemeral key agreement key used in TLS inspection. Related SSPs: Inspection ECDH Public Key, Inspection Pre-Master Secret
Inspection Encryption Key	128, 256 bits	AES Cert. #A2155	N/A	N/A	Derived using TLS 1.2 KDF	Plaintext in SDRAM	Automatically at the expiration of the session or Power off	Data encryption key used in TLS inspection. Related SSPs: Inspection Master Secret
Inspection Authentication Key	256 bits	HMAC Cert. #A2155	N/A	N/A	Derived using TLS 1.2 KDF	Plaintext in SDRAM	Automatically at the expiration of the session or Power off	Authentication key used in TLS inspection. Related SSPs: Inspection Master Secret
Inspection Pre-Master Secret	112-256 bits	KDF TLS Cert. #A2155	N/A	N/A	Established through Diffie-Hellman agreement or Elliptical Curve Diffie-Hellman agreement using NIST SP 800-56Arev3	Plaintext in SDRAM	Automatically at the expiration of the session or Power off	Shared secret generated or established for TLS inspection. Related SSPs: Inspection ECDH Private Key, Inspection ECDH Public Key, Inspection DH Private Key, Inspection DH Public Key, Inspection Master Secret

Key / SSP Name / Type	Strength	Security Function and Cert Number	Generation	Import/ Export	Establishment	Storage	Zeroisation	Use and Related Keys
Inspection Master Secret	112-256 bits	KDF TLS Cert. #A2155	N/A	N/A	Derived using TLS 1.2 KDF	Plaintext in SDRAM	Automatically at the expiration of the session or Power off	Value calculated during TLS inspection. Related SSPs: Inspection Pre-Master Secret, Inspection Encryption Key, Inspection Authentication Key
SSM HTTPS DH Private Key	112-202 bits	KAS-FFC-SSC Cert. #A2155	SP 800-56Ar3, Testing Candidates	N/A	Generated	Plaintext in SDRAM	Automatically after use or Power off	Private ephemeral key agreement key used in HTTPS inspection. Related SSPs: SSM HTTPS DH Public Key, SSM HTTPS Pre-Master Secret
SSM HTTPS ECDH Private Key	112-256 bits	KAS-ECC-SSC Cert. #A2155	SP 800-56Ar3, Testing Candidates	N/A	Generated	Plaintext in SDRAM	Automatically after use or Power off	Private ephemeral key agreement key used in HTTPS inspection. Related SSPs: SSM HTTPS ECDH Public Key, SSM HTTPS Pre-Master Secret
SSM HTTPS Encryption Key	128, 256 bits	AES Cert. #A2155	N/A	N/A	Derived using TLS 1.2 KDF	Plaintext in SDRAM	Automatically at the expiration of the session or Power off	Data encryption key used in HTTPS inspection. Related SSPs: SSM HTTPS Master Secret
SSM HTTPS Authentication Key	256 bits	HMAC Cert. #A2155	N/A	N/A	Derived using TLS 1.2 KDF	Plaintext in SDRAM	Automatically at the expiration of the session or Power off	Authentication key used in HTTPS inspection. Related SSPs: SSM HTTPS Master Secret

Key / SSP Name / Type	Strength	Security Function and Cert Number	Generation	Import/ Export	Establishment	Storage	Zeroisation	Use and Related Keys
SSM HTTPS Pre-Master Secret	112-256 bits	KDF TLS Cert. #A2155	N/A	N/A	Established through Diffie-Hellman agreement or Elliptical Curve Diffie-Hellman agreement using NIST SP 800-56Arev3	Plaintext in SDRAM	Automatically at the expiration of the session or Power off	Shared secret generated or established for HTTPS inspection. Related SSPs: SSM HTTPS DH Private Key, SSM HTTPS DH Public Key, SSM HTTPS ECDH Private Key, SSM HTTPS ECDH Public Key, SSM HTTPS Master Secret
SSM HTTPS Master Secret	112-256 bits	KDF TLS Cert. #A2155	N/A	N/A	Derived using TLS 1.2 KDF	Plaintext in SDRAM	Automatically at the expiration of the session or Power off	Value calculated during HTTPS inspection. Related SSPs: SSM HTTPS Pre-Master Secret, SSM HTTPS Encryption Key, SSM HTTPS Authentication Key
SSM Client Protection RSA Private Key	112-150 bits	RSA Cert. #A2155	FIPS 186-4, B.3.6	N/A	Generated	Plaintext in SDRAM	Power off	Used to identify the module in the SSM Proxy Service Related SSPs: SSM Client Protection RSA Public Key
SSM Client Protection ECDSA Private Key	112-256 bits	ECDSA Cert. #A2155	FIPS 186-4, Testing Candidates	N/A	Generated	Plaintext in SDRAM	Power off	Used to identify the module in the SSM Proxy Service Related SSPs: SSM Client Protection ECDSA Public Key
SSM Client Protection RSA Public Key	112-150 bits	RSA Cert. #A2155	FIPS 186-4, B.3.6	Output in Plaintext as part of TLS protocol	Generated	Plaintext in SDRAM	Power off	Used to identify the module in the SSM Proxy Service Related SSPs: SSM Client Protection RSA Private Key

Key / SSP Name / Type	Strength	Security Function and Cert Number	Generation	Import/ Export	Establishment	Storage	Zeroisation	Use and Related Keys
SSM Client Protection ECDSA Public Key	112-256 bits	ECDSA Cert. #A2155	FIPS 186-4, Testing Candidates	Output in Plaintext as part of TLS protocol	Generated	Plaintext in SDRAM	Power off	Used to identify the module in the SSM Proxy Service Related SSPs: SSM Client Protection ECDSA Private Key
SNMP Encryption Key	128, 256 bits	AES Cert. #A2155	N/A	Input Encrypted via TLS (KTS)	Input	Plaintext or encrypted on disk	Disk erasure	Data encryption key used in SNMPv3. Related SSPs: None
SNMP Authentication Key	256 bits	HMAC Cert. #A2155	N/A	Input Encrypted via TLS (KTS)	Input	Plaintext or encrypted on disk	Disk erasure	Authentication key used in SNMPv3. Related SSPs: None
TLS ECDSA Public Key	112-256 bits	ECDSA Cert. #A2155	FIPS 186-4, Testing Candidates	Output in Plaintext as part of TLS protocol	Generated	Plaintext on disk	Disk erasure	Public key used in TLS signature. Related SSPs: TLS ECDSA Private Key
TLS ECDH Public Key	112-256 bits	KAS-ECC-SSC Cert. #A2155	SP 800-56Ar3, Testing Candidates	Input and Output in Plaintext as part of TLS protocol	Generated, Input	Plaintext in SDRAM	Automatically at the expiration of the session or Power off	Public ephemeral key agreement key used in TLS. Related SSPs: TLS ECDH Private Key, TLS Pre-Master Secret
VPN RSA Public Key	112-150 bits	RSA Cert. #A2155	FIPS 186-4, B.3.6	Input and Output in Plaintext as part of TLS/IKE protocols	Generated, Input	Encrypted on disk	Disk erasure	Public authentication key used in IKE. Related SSPs: VPN RSA Private Key

Key / SSP Name / Type	Strength	Security Function and Cert Number	Generation	Import/ Export	Establishment	Storage	Zeroisation	Use and Related Keys
VPN ECDSA Public Key	112-256 bits	ECDSA Cert. #A2155	FIPS 186-4, Testing Candidates	Input and Output in Plaintext as part of TLS/IKE protocols	Generated, Input	Encrypted on disk	Disk erasure	Public authentication key used in IKE. Related SSPs: VPN ECDSA Private Key
VPN DH Public Key	112-202 bits	KAS-FFC-SSC Cert. #A2155	SP 800-56Ar3, Testing Candidates	Input and Output in Plaintext as part of IKE protocol	Generated, Input	Plaintext in SDRAM	Automatically after use or Power off	Public ephemeral key agreement key used in IKE. Related SSPs: VPN DH Private Key, VPN DH Shared Secret
VPN ECDH Public Key	112-256 bits	KAS-ECC-SSC Cert. #A2155	SP 800-56Ar3, Testing Candidates	Input and Output in Plaintext as part of IKE protocol	Generated, Input	Plaintext in SDRAM	Automatically after use or Power off	Public ephemeral key agreement key used in IKE. Related SSPs: VPN ECDH Private Key, VPN ECDH Shared Secret
HTTPS RSA Public Key	112-150 bits	RSA Cert. #A2155	FIPS 186-4, B.3.6	Input and Output in Plaintext as part of TLS protocols	Generated, Input	Plaintext on disk	Disk erasure	Public authentication key used in HTTPS user authentication. Related SSPs: HTTPS RSA Private Key
HTTPS DH Public Key	112-202 bits	KAS-FFC-SSC Cert. #A2155	SP 800-56Ar3, Testing Candidates	Input and Output in Plaintext as part of TLS protocol	Generated, Input	Plaintext in SDRAM	Automatically after use or Power off	Public ephemeral key agreement key used in TLS. Related SSPs: HTTPS DH Private Key, HTTPS Pre-master Secret

Key / SSP Name / Type	Strength	Security Function and Cert Number	Generation	Import/ Export	Establishment	Storage	Zeroisation	Use and Related Keys
HTTPS ECDH Public Key	112-256 bits	KAS-ECC-SSC Cert. #A2155	SP 800-56Ar3, Testing Candidates	Input and Output in Plaintext as part of TLS protocol	Generated, Input	Plaintext in SDRAM	Automatically after use or Power off	Public ephemeral key agreement key used in TLS. Related SSPs: HTTPS ECDH Private Key, HTTPS Pre-master Secret
Client Protection CA RSA Public Key	112-150 bits	RSA Cert. #A2155	N/A	Input Encrypted via TLS (KTS)	Input	Encrypted on disk	Disk erasure	Public signature key used in TLS inspection CA. Related SSPs: Client Protection CA RSA Private Key
Client Protection IM CA RSA Public Key	112-150 bits	RSA Cert. #A2155	FIPS 186-4, B.3.6	N/A	Generated	Plaintext in SDRAM	Power off	Public authentication key used in TLS inspection. Related SSPs: Client Protection IM CA RSA Private Key
Client Protection IM CA ECDSA Public Key	112-256 bits	ECDSA Cert. #A2155	FIPS 186-4, Testing Candidates	N/A	Generated	Plaintext in SDRAM	Power off	Public authentication key used in TLS inspection. Related SSPs: Client Protection IM CA ECDSA Private Key
Client Protection RSA Public Key	112-150 bits	RSA Cert. #A2155	FIPS 186-4, B.3.6	Output in Plaintext as part of TLS protocol	Generated	Plaintext in SDRAM	Power off	Public authentication key used in TLS inspection. Related SSPs: Client Protection RSA Private Key
Server Protection RSA Public Key	112-150 bits	RSA Cert. #A2155	N/A	Input Encrypted via TLS (KTS)	Input	Encrypted on disk	Disk erasure	Public authentication key used in TLS inspection. Related SSPs: Server Protection RSA Private Key
Client Protection ECDSA Public Key	112-256 bits	ECDSA Cert. #A2155	FIPS 186-4, Testing Candidates	Output in Plaintext as part of TLS protocol	Generated	Plaintext in SDRAM	Power off	Public authentication key used in TLS inspection. Related SSPs: Client Protection ECDSA Private Key

Key / SSP Name / Type	Strength	Security Function and Cert Number	Generation	Import/ Export	Establishment	Storage	Zeroisation	Use and Related Keys
Server Protection ECDSA Public Key	112-256 bits	ECDSA Cert. #A2155	N/A	Input Encrypted via TLS (KTS)	Input	Encrypted on disk	Disk erasure	Public authentication key used in TLS inspection.
Inspection DH Public Key	112-202 bits	KAS-FFC-SSC Cert. #A2155	SP 800-56Ar3, Testing Candidates	Input and Output in Plaintext as part of TLS protocol	Generated, Input	Plaintext in SDRAM	Automatically after use or Power off	Public ephemeral key agreement key used in TLS inspection. Related SSPs: Inspection DH Private Key, Inspection Pre-Master Secret
Inspection ECDH Public Key	112-256 bits	KAS-ECC-SSC Cert. #A2155	SP 800-56Ar3, Testing Candidates	Input and Output in Plaintext as part of TLS protocol	Generated, Input	Plaintext in SDRAM	Automatically after use or Power off	Public ephemeral key agreement key used in TLS inspection. Related SSPs: Inspection ECDH Private Key, Inspection Pre-Master Secret
SSM HTTPS DH Public Key	112-202 bits	KAS-FFC-SSC Cert. #A2155	SP 800-56Ar3, Testing Candidates	Input and Output in Plaintext as part of TLS protocol	Generated, Input	Plaintext in SDRAM	Automatically after use or Power off	Public ephemeral key agreement key used in HTTPS inspection. Related SSPs: SSM HTTPS DH Private Key, SSM HTTPS Pre-Master Secret
SSM HTTPS ECDH Public Key	112-256 bits	KAS-ECC-SSC Cert. #A2155	SP 800-56Ar3, Testing Candidates	Input and Output in Plaintext as part of TLS protocol	Generated, Input	Plaintext in SDRAM	Automatically after use or Power off	Public ephemeral key agreement key used in HTTPS inspection. Related SSPs: SSM HTTPS ECDH Private Key, SSM HTTPS Pre-Master Secret

Key / SSP Name / Type	Strength	Security Function and Cert Number	Generation	Import/ Export	Establishment	Storage	Zeroisation	Use and Related Keys
TLS Trusted Certificates	112-256 bits	RSA Cert. #A2155 ECDSA Cert. #A2155	N/A	Input Encrypted via TLS (KTS)	Input	Plaintext in SDRAM	Disk erasure	Trusted certificates for use in TLS Related SSPs: None
Trusted Internet Certificates	112-256 bits	RSA Cert. #A2155 ECDSA Cert. #A2155	N/A	Input Encrypted via TLS (KTS)	Input	Plaintext in SDRAM	Disk erasure	Trusted certificates for authenticating internet servers Related SSPs: None
VPN Trusted Certificates	112-256 bits	RSA Cert. #A2155 ECDSA Cert. #A2155	N/A	Input Encrypted via TLS (KTS)	Input	Plaintext on disk	Disk erasure	Trusted certificates for use in VPNs Related SSPs: None
256-bit DRBG Entropy Input	256	DRBG Cert. #A2155	ENT (NP)	N/A	Generated	Plaintext in SDRAM	Automatically after use or Power off	Entropy input for 256-bit DRBG Related SSPs: 128-bit DRBG 'V' Value, 256-bit DRBG 'Key' Value, 256-bit DRBG Seed
128-bit DRBG 'V' Value	128	DRBG Cert. #A2155	SP 800-90A	N/A	Derived via SP 800-90A mechanisms based on entropy input	Plaintext in SDRAM	Automatically after use or Power off	V (128 bits) for 256-bit DRBG Related SSPs: 256-bit DRBG Entropy Input, 256-bit DRBG Seed
256-bit DRBG 'Key' Value	256	DRBG Cert. #A2155	SP 800-90A	N/A	Derived via SP 800-90A mechanisms based on entropy input	Plaintext in SDRAM	Automatically after use or Power off	Key (256 bits) for 256-bit DRBG Related SSPs: 256-bit DRBG Entropy Input, 256-bit DRBG Seed

Key / SSP Name / Type	Strength	Security Function and Cert Number	Generation	Import/ Export	Establishment	Storage	Zeroisation	Use and Related Keys
256-bit DRBG Seed	256	DRBG Cert. #A2155	SP 800-90A	N/A	Derived via SP 800-90A mechanisms based on entropy input	Plaintext in SDRAM	Automatically after use or Power off	Seeding material for the DRBG Related SSPs: 256-bit DRBG Entropy Input, 128-bit DRBG 'V' Value, 256-bit DRBG 'Key' Value
Cluster Protocol Key	256	HMAC Cert. #A2155	N/A	Input Encrypted via TLS (KTS)	Input	Plaintext or encrypted on disk	Disk erasure	Used for authentication within the cluster protocol. Related SSPs: None
State Synchronization Key	128	AES Cert. #A2155 HMAC Cert. #A2155	CKG using unmodified DRBG output	Input and Output Encrypted via TLS (KTS)	Generated, Input	Plaintext in SDRAM	Power off	Used for encryption and authentication in the state synchronization protocol. Related SSPs: None
Configuration File Protection Key	256	KBKDF Cert. #A2209	CKG using unmodified DRBG output	N/A	Generated	Plaintext on disk	Disk erasure	Used to derive the configuration file encryption and authentication keys. Related SSPs: Configuration File Encryption Key, Configuration File Authentication Key
Configuration File Protection Passphrase	256	PBKDF Cert. #A2209	CKG using unmodified DRBG output	N/A	Generated	Plaintext on disk	Disk erasure	Used to derive the key pair obfuscation and integrity protection keys. Related SSPs: None
Configuration File Encryption Key	256	AES Cert. #A2155	N/A	N/A	Derived via KBKDF	Plaintext in SDRAM	Automatically after use or Power off	Used to encrypt configuration files on disk. Related SSPs: Configuration file protection Key

Key / SSP Name / Type	Strength	Security Function and Cert Number	Generation	Import/ Export	Establishment	Storage	Zeroisation	Use and Related Keys
Configuration File Authentication Key	256	HMAC Cert. #A2155	N/A	N/A	Derived via KBKDF	Plaintext in SDRAM	Automatically after use or Power off	Used to authenticate configuration files on disk. Related SSPs: Configuration file protection Key
User Password	>65 bits	N/A	N/A	Input hashed (SHA2-512) and salted	Input	SHA2-512 digest on disk	Disk erasure	Identify users in HTTPS authentication and Mobile VPN. Related SSPs: None
Key Encryption Passphrase	256	PBKDF Cert. #A2209	N/A	Input Encrypted via TLS (KTS)	Input	Plaintext on disk	Disk erasure	Derive the key encryption key used to protect private keys stored on disk. Related SSPs: Key Encryption Key
Key Encryption Key	128	AES Cert. #A2155	N/A	N/A	Derived via PBKDF	Plaintext in SDRAM	Automatically after use or Power off	Used to encrypt/decrypt private keys stored on disk. Related SSPs: Key Encryption Passphrase
Firmware Integrity Check Public Key [16]	256	ECDSA Cert. #A2155	N/A	N/A	Pre-loaded by the manufacturer	Plaintext on disk	Disk erasure	Used for firmware integrity check. Related SSPs: None

[16] The key “Firmware Integrity Check Public Key” is not considered to be an SSP, but otherwise included for completeness.

9.2 Non-Deterministic Random Number Generation Specification

The module includes a non-deterministic Random Number Generator (RNG) within the module boundary.

The non-deterministic RNG is used exclusively to feed an approved SHA-3 conditioning function where in-turn the output of the conditioning function is used to seed the DRBG.

The Non-Deterministic RNG complies with SP 800-90B and has been certified using FIPS 140-3 IG D.J with guidance set out in FIPS 140-3 IG D.K.

TABLE 11: NON-DETERMINISTIC RANDOM NUMBER GENERATION SPECIFICATION

Entropy sources	Minimum number of bits of entropy	Details
CPU timing jitter	Full-entropy output	SP 800-90B compliant Non-Deterministic RNG using a software-based noise source internal to the module boundary. Output from the noise source is fed through an approved conditioning function based on SHA3-256. Raw noise is generated based on non-deterministic jitter inherent in CPUs from factors such as CPU instruction pipelines, CPU clock cycles being different from memory bus clock speeds, CPU frequency scaling, CPU power management, instruction and data cache states, CPU topology, different CPU cache technologies, CPU branch prediction, hardware interrupts, etc. The module achieves full entropy from the output of the conditioning function where every 512-bits used to seed the DRBG includes 512-bits of entropy. All outputs from the noise source are subjected to health testing ahead of being fed to the conditioning function.

10. Self-Tests

10.1 Pre-Operational Tests

The module performs the pre-operational self-tests upon power-up to confirm the firmware integrity, and to check the continued correct operation of the random number generator and each of the implemented cryptographic algorithms used in support of the integrity checks.

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. An error message is output on the status output interface specifying the library within the module that failed the self-test. In this state, all data output via the module's data output interfaces is inhibited. The module proceeds to reboot and reruns 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 restart, the appliance continues to restart. If the problem persists, CO intervention is required to either perform a restore to factory defaults settings and reinstall, or power-off and contact Forcepoint Customer Support.

TABLE 12: PRE-OPERATIONAL SELF-TESTS

Test	Operations Performed	Indicator
Root Filesystem Integrity Test (ECDSA with P-521 and SHA2-512)	Verify	Error output and module reboot.
Pre-operational Bypass Test	Bypass	Error output and module reboot.

10.2 Conditional Self-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)
- Pair-Wise Consistency Test (PCT)
- Health tests
- Bypass tests

All KATs alongside health testing of the noise source are performed immediately following the pre-operational self-tests at module power-on

TABLE 13: CONDITIONAL CRYPTOGRAPHIC ALGORITHM SELF-TESTS

Test	Cryptographic Mechanism Tested	Location	When Performed	Operations Performed	Indicator
Forcepoint NGFW FIPS Cryptographic Module					
KAT test for AES encryption and decryption	AES-CBC-128	Cert. #A2155	Upon Library Load	Encryption, Decryption	Error output and module reboot.
KAT test for AES GCM encryption and decryption	AES-GCM-128	Cert. #A2155	Upon Library Load	Encryption, Decryption	Error output and module reboot.
Health test for AES-CTR-256 DRBG	AES-256 CTR_DRBG	Cert. #A2155	Upon Library Load	Instantiate, Reseed, Generate	Error output and module reboot.
KAT test for AES-CTR-256 DRBG	AES-256 CTR_DRBG	Cert. #A2155	Upon Library Load	Prediction Resistance: No Derivation Function Enabled: Yes	Error output and module reboot.
KAT for Diffie-Hellman (KAS-FFC-SSC)	KAS-FFC-SSC (2048, 224)	Cert. #A2155	Upon Library Load	Shared Secret Computation	Error output and module reboot.

Test	Cryptographic Mechanism Tested	Location	When Performed	Operations Performed	Indicator
KAT for EC Diffie-Hellman (KAS-ECC-SSC)	KAS-ECC-SSC w/ P-224	Cert. #A2155	Upon Library Load	Shared Secret Computation	Error output and module reboot.
KAT for ECDSA verification	ECDSA P-224 w/ SHA2-224	Cert. #A2155	Upon Library Load	Verify	Error output and module reboot.
KAT for ECDSA signing	ECDSA P-224 w/ SHA2-224	Cert. #A2155	Upon Library Load	Sign	Error output and module reboot.
KAT for HMAC	HMAC-SHA2-256	Cert. #A2155	Upon Library Load	MAC Generation, Verification	Error output and module reboot.
Configuration Bypass Test	HMAC	Cert. #A2155	New Policy Files Received	MAC Verification	Error output and module reboot.
KAT for RSA verification	RSA 2048 w/ SHA2-256 PKCS#1v1.5	Cert. #A2155	Upon Library Load	Verify	Error output and module reboot.
KAT for RSA signing	RSA 2048 w/ SHA2-256 PKCS#1v1.5	Cert. #A2155	Upon Library Load	Sign	Error output and module reboot.
KAT test for SHA	SHA-1, SHA2-512	Cert. #A2155	Upon Library Load	Hashing	Error output and module reboot.
KAT for IKEv1 and IKEv2 KDF	IKEv1 and IKEv2 KDFs	Cert. #A2155	Upon Library Load	Key Derivation	Error output and module reboot.
KAT for TLSv1.2 KDF	TLSv1.2 KDF	Cert. #A2155	Upon Library Load	Key Derivation	Error output and module reboot.
Forcepoint NGFW FIPS Library					
KAT test for AES encryption and decryption	AES-CCM-192 *AES-CCM can only be used for self-testing purposes.*	Cert. #A2209	Upon Library Load	Encryption, Decryption	Error output and module reboot.
KAT test for AES encryption end decryption	AES-ECB-128	Cert. #A2209	Upon Library Load	Encryption, Decryption	Error output and module reboot.
KAT test for PBKDF2	PBKDF w/ SHA2-256	Cert. #A2209	Upon Library Load	Key Derivation	Error output and module reboot.
KAT test for KBKDF	KBKDF w/ HMAC-SHA2-256	Cert. #A2209	Upon Library Load	Key Derivation	Error output and module reboot.
Forcepoint NGFW Cryptographic Kernel Module					
KAT test for AES encryption and decryption	AES-CBC, CFB, ECB, OFB 128, 192, 256	Cert. #A2166	Upon Library Load	Encryption, Decryption	Error output and module reboot.

Test	Cryptographic Mechanism Tested	Location	When Performed	Operations Performed	Indicator
KAT test for AES-GCM authenticated encryption and decryption	AES-GCM-128	Cert. #A2166	Upon Library Load	Encryption, Decryption	Error output and module reboot.
KAT test for SHA	SHA-1, SHA2-256, SHA2-512	Cert. #A2166	Upon Library Load	Hashing	Error output and module reboot.
KAT test for HMAC	HMAC-SHA-1, SHA2-256, SHA2-512	Cert. #A2166	Upon Library Load	MAC Generation, Verification	Error output and module reboot.
Forcepoint NGFW Entropy Library					
KAT for SHA3-256	SHA3-256	Cert. #A2167	Upon Library Load	Hashing	Error output and module reboot.
Repetition Count Test	ENT (NP)	N/A	At Startup and Upon Entropy Generation	Comparison of Subsequent Entropy Samples	Error output and module reboot.
Adaptive Proportion Test	ENT (NP)	N/A	At Startup and Upon Entropy Generation	Comparison of Samples within Window	Error output and module reboot.

TABLE 14: CONDITIONAL PAIR-WISE CONSISTENCY TESTS

Test	Cryptographic Mechanism Tested	Location	When Performed	Operations Performed	Indicator
PCT for RSA key pairs created for digital signature purposes	RSA w/ PKCS#1v1.5	Cert. #A2155	Upon RSA Key Generation	Sign, Verify	Error output and module reboot.
PCT for ECDSA key pairs created for digital signature purposes	ECDSA	Cert. #A2155	Upon ECDSA Key Generation	Sign, Verify	Error output and module reboot.
PCT for DH key pairs created for key agreement purposes	KAS-FFC-SSC	Cert. #A2155	Upon DH Key Generation	Public Key Recalculation	Error output and module reboot.
PCT for ECDH key pairs created for key agreement purposes	KAS-ECC-FFC	Cert. #A2155	Upon ECDH Key Generation	Public Key Recalculation	Error output and module reboot.

11. Life-Cycle Assurance

Operating the module without following the guidance below will result in non-compliant behavior and is outside the scope of this Security Policy.

11.1 Performing Secure Initialization of the Module

11.1.1 Hardware Setup

Upon receiving the NGFW hardware, the CO shall check that the appliance is not damaged and that all required parts and instructions are included. If the Network Components are not installed in the appliance, the CO must insert them by performing the following:

Note: Read all safety instructions before installing the Network Components. Do not install any Network Components while the appliance is on. Fasten a grounding strip from the wrist to the appliance.

1. Locate the Network Component slots on the front of the appliance.
2. If the appliance was shipped with the Network Component slot(s) covered by a plate, remove the thumbscrew and plate from the appliance. Store the thumbscrew and plate in case the Network Component is eventually removed.
3. Push the Network Component into the slot. The Network Component is properly installed when the front of the Network Component is flush with the front of the appliance.

The NGFW uses tamper-evident seals to protect against unauthorized access to the internal components of the chassis through removable covers. The CO shall apply labels to the module as depicted in section Tamper-Evident Labels.

11.1.2 Creating a Configuration for the Approved Mode of Operation

The administration of the NGFW modules is done through the SMC, which provides centralized administrative functionalities for all the managed NGFW modules. The SMC can be shipped preinstalled on its own Forcepoint hardware appliance, installed as a virtual machine on a virtualization platform, or installed on a third-party Windows or Linux platform. The SMC can be accessed by an administrator via a Java-based Management Client running on the administrator's workstation.

Using the Management Client, create a configuration for the NGFW Engine in the Approved Mode of Operation.

1. To use HTTPS User Authentication and TLS Inspection for Client Protection or Server Protection, create a TLS Cryptography Suite Set element. Select only the Approved and Allowed algorithms and TLS cipher suites. The Management Connection Service, Peer Connection Service, Key Pair Management Service, and User Management Service utilize the TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 cipher suite. Refer to Table 3: Approved Algorithms above for a list of algorithms implemented. For more information, see the "Create TLS Cryptographic Suite Set elements" topic of the Forcepoint NGFW Product Guide.
    - In accordance with the NGFW Product user guide, the following TLS Cipher Suites are utilized within the module:
        - TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256
        - TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384
        - TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256

- TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256
- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384
- TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
- TLS_DHE_RSA_WITH_AES_128_CBC_SHA256
- TLS_DHE_RSA_WITH_AES_256_CBC_SHA256
- TLS_DHE_RSA_WITH_AES_128_GCM_SHA256
- TLS_DHE_RSA_WITH_AES_256_GCM_SHA384

2. To use certificates signed by a Certificate Authority (CA) that is not one of the default Trusted Certificate Authority elements, create a Trusted Certificate Authority element. Import only a certificate signed using a Approved signature algorithm. For more information, see the “Create Trusted Certificate Authority elements” topic of the Forcepoint NGFW Product Guide.
3. To use HTTPS User Authentication, create a TLS Profile element. Select the TLS Cryptography Suite Set element, the Trusted Certificate Authority, and the minimum TLS version. For more information, see the “Create TLS Profile elements” topic of the Forcepoint NGFW Product Guide.
4. Create the NGFW Engine Element by defining the properties in the Engine Editor.
    - Browse to Advanced Settings, then select FIPS-Compatible Operating Mode.
    - Select “FIPS-Disable Remote Engine Upgrades” for the NGFW to prevent firmware load attempts from the SMC.
    - To use HTTPS User Authentication, browse to Add-Ons | User Authentication, then enable HTTPS and select the TLS Profile element. Use 2048 or greater as the Key Length when creating a certificate signing request in HTTPS Settings. For more information, see the “Enable browser-based user authentication” topic of the Forcepoint NGFW Product Guide.
    - To use TLS Inspection for Client Protection, create a Client Protection Certificate Authority element and import the private key and the certificate used to issue certificates in TLS Inspection. Use only the Approved algorithms and key size for the key pair and certificate. In the Engine Editor, browse to Add-Ons | TLS Inspection, then select the Cryptography Suite Set. For more information, see the “Configure TLS inspection for client protection” and “Activating TLS inspection” topics in the “Setting up TLS Inspection” chapter of the Forcepoint NGFW Product Guide.
    - To use TLS Inspection for Server Protection, browse to Add-Ons | TLS Inspection, then select the Cryptography Suite Set. For more information, see the “Activating TLS inspection” topic in the “Setting up TLS Inspection” chapter of the Forcepoint NGFW Product Guide.
    - When using TLS Inspection or Sidewinder HTTPS proxy, create a Firewall Policy that has an Access rule that allows the TLS connection and create an Inspection Policy that has an Inspection rule that terminates connections that match the TLS_Certificate-Verify-Failed Situation. On the Inspection tab of the Firewall Policy, you must select the Inspection Policy that you created.
    - To use Sidewinder HTTP and HTTPS proxies, browse to Add-Ons | Sidewinder Proxy, click Advanced, then set the value of the tls_cipher_override property to **TLSv1.2+ECDHE+AES!AESCCM:TLSv1.2+DHE+AES!AESCCM!DSS** on the HTTP tab. For more information, see the “Advanced settings for Sidewinder Proxies” topic in the “Sidewinder Proxies” chapter of the Forcepoint NGFW Product Guide.

- When using IPsec, disable Automated RSA Certificate Management. Browse to VPN | Certificates, then deselect Automated RSA Certificate Management.
- To use IPsec, right-click the Gateway element, then select Tools | Generate Certificate to create a certificate signing request. Select RSA with 2048 or greater key size, or ECDSA as the Public Key Algorithm. For more information, see the "Create a VPN certificate or certificate request for a VPN Gateway element" topic in the "Managing VPN certificates" chapter of the Forcepoint NGFW Product Guide.

5. To use an IPsec VPN, create a VPN Profile element. Use only the Approved and Allowed algorithms and key sizes in the profile. Refer to Table 3: Approved Algorithms above for a list of algorithms implemented. Additionally, in the profile element, the IPsec Tunnel Lifetime should be set to less than 2^{32} bytes. Select the VPN Profile element. For more information, see the "Create VPN Profile elements" topic in the "VPNs in Forcepoint NGFW" chapter of the Forcepoint NGFW Product Guide.
6. Create Access Rules to configure the Alternating Bypass Feature.
7. Save the initial configuration for the NGFW Engine. Make a note of the one-time password, which is required for initial contact with the SMC.

See section "Setting up the Approved Configuration" for setting up the device configurations.

11.1.3 Downloading and Upgrading to an Approved Firmware Version

The NGFW appliances are delivered in an operational state with the most recent firmware preinstalled. The NGFW firmware must be upgraded to the FIPS 140-3 validated NGFW firmware version to be placed in the Approved mode of operation.

Note: The upgrade to the FIPS 140-3 validated 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. Any firmware loaded into the module other than version 6.10.3.26158 is out of the scope of this validation and will mean that the module is not operating in the approved mode of operation.

A FIPS 140-3 Validated NGFW firmware version is downloaded as follows:

1. Login to the Forcepoint Support https://support.forcepoint.com/Login
2. Proceed to the Forcepoint NGFW downloads section.
3. Download the firmware version 6.10.3.26158 installation file (sg_engine_6.10.3.26158_x86-64-small.zip).
4. Verify the SHA checksum.

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

After downloading the firmware, the operator can upgrade to a FIPS 140-3 validated firmware version:

1. Save the FIPS 140-3 validated 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 FIPS validated NGFW firmware version is loaded.

11.1.4 Setting up the Approved Configuration

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 network interfaces according to your environment as instructed in the Configuring the Network Interfaces section of the NGFW Installation Guide.
    a. Configure the operating system settings according to the "Configuring the Operating System Settings" section of the NGFW Installation Guide.
    b. Select both:
        - "Restricted FIPS-compatible operating mode" (This automatically disables the SSH daemon and root password options in the Engine Configuration Wizard).
        - "FIPS 140-3 compatible mode" (This setting ensures the module uses only FIPS 140-3 approved algorithms and security functions).
3. 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 the “Restricted FIPS-compatible operating mode” setting is enabled. The engine restarts.
4. To verify the “FIPS 140-3 compatible operating mode” setting is activated:
    a. 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)
    b. Continue as instructed in the “After Successful Management Server Contact” section of the NGFW Installation Guide.

Note: If the engine does not enter the “Restricted 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 appliance must be reset to factory settings and reinstalled.

Note: The “FIPS 140-3 compatible operating mode” and “Restricted FIPS-compatible operating mode” settings must be enabled during the initial configuration of the appliance.

11.1.5 Resetting the Module to Factory Settings (Sanitization)

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

To reset the appliance to factory settings:

1. Reboot the appliance and select System restore options from the boot menu. 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 appliance storage capacity

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 2 requirements for this validation.

13. Guidance

13.1 Identifying the Module Version

1. At the Home screen of the SMC that is being used to manage the module, click on the firewall.
2. On the right-hand column, under “Info”, the firewall version (and update package) will be in the “General” tab

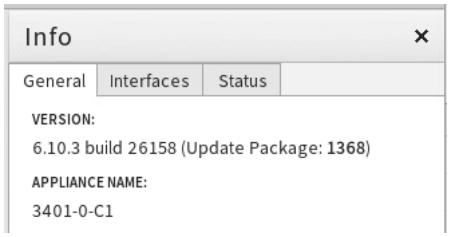

FIGURE 17: DEPICTION OF THE MODULE VERSION DISPLAYED IN THE SMC GUI

13.2 Non-Approved Mode of Operation

When configured according to the guidance in this Security Policy, the modules do not support a Non-Approved mode of operation.

13.3 Additional Guidance and Usage Policies

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

- **Use of AES GCM**: The module generates AES GCM IV in accordance with SP 800-38D in compliance with IG C.H scenario 1. The GCM IV generation in the TLS context follows RFC 5288 and SP 800-52rev2 section 3.3.1 and shall only be used for the TLS protocol version 1.2. The GCM IV generation in the IPsec context follows RFC 4106 and RFC 7296 and shall only be used with IPsec and IKEv2 to be compliant with IG C.H. The implementation of the 64-bit nonce_explicit part of the IV is deterministic and management logic is inside the module. By the design of the module and by virtue of the data size limit (see above section Creating a Configuration for the Approved Mode of Operation) set, the maximum number possible value of 2^64 for nonce_explicit part of the IV is never reached. In case the module’s power is lost and then restored, the key used for the AES GCM encryption or decryption shall be re-distributed.
- **Use of PBKDF**: The module implements key derivation through the SP 800-132 PBKDF2. The module supports option 1a from Section 5.4 of SP 800-132, whereby the MK is used directly as the DPK. Keys derived from passwords or passphrases are only used for data at rest. The length of the salt should be at least 128 bits and the length of the password or passphrase should be at least 10 characters, which provides the probability of guessing this password or passphrase to be $(1/94)^{10}$. The caller shall observe all requirements and should consider all recommendations specified in SP 800-132 with respect to the strength of the generated key, including the quality of the password and the quality of the salt. Keys derived from passwords, as shown in SP 800-132, may only be used in storage applications. For encrypted private key entry as part of the configuration, the PBKDF2 iteration count must be between

1000 and 10000 to allow the recommended minimum in SP 800-132 while keeping performance the impact small, and the passphrase must be at least 14 characters.

- **Use of insecure protocols** – The following insecure protocols are disabled by default: SSH, Console Access, and WIFI Interfaces. The root password option is automatically disabled. To maintain compliance with FIPS requirements, these protocols and services shall not be enabled.
- **Network Component replacement** – As noted earlier, the NGFW appliances are modular by design. The Network Components are field-replaceable. Operators in the field can order the desired Network Components directly from Forcepoint Customer Support using the appropriate part numbers. The CO must install the Network Components as described in section Hardware Setup above.

  Because these Network Components play a role in maintaining the module's physical security, they are secured in place using tamper-evident labels. Thus, replacing a Network Component necessitates the replacement of any tamper-evident label affixed to the Network Component as well. When a CO orders Network Components, they must also order a Forcepoint NGFW FIPS kit with the Stock Keeping Unit ACFIPS3. The FIPS kit is delivered with the number of tamper-evident labels required for proper installation (see details per NGFW appliance in section Tamper-Evident Labels). Module operators must follow the guidance below to ensure continued compliance with FIPS requirements:

  1. Zeroize all keys and CSPs on the module.

  2. Remove power from the module.

  3. Remove the Network Component to be replaced.

  4. Remove any remaining bits of the now-broken tamper-evident label from the module chassis.

  5. Install the replacement Network Component in the open slot.

  6. Using a 99% isopropyl alcohol solution, clean the chassis surface in the area where the replacement tamper-evident label will be placed.

  7. Affix the replacement tamper-evident label to the chassis (refer to section Tamper-Evident Labels for placements). Allow 24 hours for the seal to fully cure.

  8. Apply power to the module

13.4 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

Appendix A. Acronyms and Abbreviations

Term	Definition
AES	Advanced Encryption Standard
ANSI	American National Standards Institute
API	Application Programming Interface
CBC	Cipher Block Chaining
CKG	Cryptographic Key Generation
CFB	Cipher Feedback
CMVP	Cryptographic Module Validation Program
CO	Crypto Officer
CSP	Critical Security Parameter
CTR	Counter
CVL	Component Validation List
DH	Diffie-Hellman
DRBG	Deterministic Random Bit Generator
ECB	Electronic Code Book
ECC	Elliptic Curve Cryptography
ECDH	Elliptic Curve Diffie-Hellman
ECDSA	Elliptic Curve Digital Signature Algorithm
FFC	Finite Field Cryptography
FIPS	Federal Information Processing Standard
GCM	Galois Counter Mode
HMAC	Keyed-Hash Message Authentication Code
IG	Implementation Guidance

Term	Definition
ISO/IEC	International Organization for Standardization / International Electrotechnical Commission
I/O	Input/Output
IV	Initialization Vector
KAS	Key Agreement Scheme
KAT	Known Answer Test
KBKDF	Key-Based Key Derivation Function
KDF	Key Derivation Function
KTS	Key Transport Scheme
LED	Light Emitting Diode
MAC	Message Authentication Code
Mbps	Megabits per second
NIST	National Institute of Science and Technology
N/A	Not Applicable
OFB	Output Feedback
PBKDF	Password Based Key Derivation Function
PCT	Pair-Wise Consistency Test
PKCS	Public-Key Cryptography Standards
POST	Power-on Self-Test
RNG	Random Number Generator
RSA	Rivest Shamir Adleman
SHA	Secure Hash Algorithm
SSC	Shared Secret Computation
SSP	Sensitive Security Parameter

Term	Definition
USB	Universal Serial Bus