Forcepoint

Next Generation Firewall

Hardware Version: 1101, 2101, 2105, 3305, and 6205
Firmware Version: 6.4.1.20056.fips.8

FIPS 140-2 Non-Proprietary Security Policy

FIPS Security Level: 2
Document Version: 0.7

Prepared for:

Forcepoint
10900-A Stonelake Blvd.
Suite 350
Austin, TX 78759
United States of America

Phone: +1 853 320 8000
www.forcepoint.com

Prepared by:

Corsec Security, Inc.
13921 Park Center Road
Suite 460
Herndon, VA 20171
United States of America

Phone: +1 703 267 6050
www.corsec.com

Table of Contents

List of Tables

List of Figures

1. Introduction

1.1 Purpose

This is a non-proprietary Cryptographic Module Security Policy for the Next Generation Firewall (Hardware Version: 1101, 2101, 2105, 3305, and 6205; firmware Version: 6.4.1.20056.fips.8) from Forcepoint. This Security Policy describes how the Next Generation Firewall appliances (referred as NGFW appliances) meet the security requirements of Federal Information Processing Standards (FIPS) Publication 140-2, which details the U.S[1]. and Canadian government requirements for cryptographic modules. More information about the FIPS 140-2 standard and validation program is available on the National Institute of Standards and Technology (NIST) and the Communications Security Establishment (CSE) Cryptographic Module Validation Program (CMVP) website at http://csrc.nist.gov/groups/STM/cmvp.

This document also describes how to run the modules in a secure FIPS-Approved mode of operation. This policy was prepared as part of the Level 2 FIPS 140-2 validation of the module. The Next Generation Firewall appliances are referred to in this document as the NGFW appliances, crypto modules, or modules.

1.2 References

This document deals only with operations and capabilities of the modules in the technical terms of a FIPS 140-2 cryptographic module security policy. More information is available on the modules from the following sources:

- The Forcepoint website (https://www.forcepoint.com/) contains information on the full line of products from Forcepoint.
- The CMVP website (http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/140val-all.htm) contains contact information for individuals to answer technical or sales-related questions for the module.

1.3 Document Organization

The Security Policy document is organized into two primary sections. Section 2 provides an overview of the validated modules. This includes a general description of the modules' capabilities and their use of cryptography as well as a presentation of the validation level achieved in each applicable functional area of the FIPS standard. It also provides high-level descriptions of how the modules meet FIPS requirements in each functional area. Section 3 documents the guidance needed for the secure use of the modules, including initial setup instructions, management methods, and applicable usage policies.

[1] U.S. – United States

2. NGFW

2.1 NGFW Overview

The NGFW appliances are high-performance network security appliances that add a broad range of built-in security features, including VPN[2], IPS[3], anti-evasion, TLS inspection, SD-WAN[4], 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 140-2 approved mode, the appliances are deployed in Firewall/VPN mode of operation, which provides access control and VPN connectivity. Each of these appliances run NGFW firmware version 6.4.1.20056.fips.8 based on the Debian 9 based operating system with Linux kernel version 4.9.76.

- The **NGFW 1101** (Figure 1 and Figure 2) is a 1U[5] rack-mounted design featuring modular connectivity. The NGFW 1101 is equipped with 8x GE[6] RJ[7]45 and 2x 10 Gbps[8] SFP+[9] fixed Ethernet ports, and includes one Network I/O[10] slot, allowing for additional connectivity. The appliance contains an integrated power supply that supports a wide range of voltages: 100 – 240 VAC[11] or -72 – -36 VDC[12]. The operating temperature range of the appliances is between 0°C to +40°C[13] (+32°F[14] to +104°F).

Figure 1 – NGFW 1101 (Front Panel)

[2] VPN – Virtual Private Network
[3] IPS – Intrusion Prevention System
[4] SD-WAN – Software-Defined Wide-Area Network
[5] U – Unit
[6] GE – Gigabit Ethernet
[7] RJ – Registered Jack
[8] Gbps – Gigabits per second
[9] SFP+ – Small Form-Factor Pluggable
[10] I/O – Input/Output
[11] VAC – Voltage Alternating Current
[12] VDC – Voltage Direct Current
[13] °C – Celsius
[14] °F – Fahrenheit

Figure 2 – NGFW 1101 (Rear Panel)

- The **NGFW 2101** (Figure 3 and Figure 4) and **NGFW 2105** (Figure 5 and Figure 6) appliances are 1U rack-mounted design featuring modular connectivity. Both NGFW 2101 and NGFW 2105 are equipped with 12x GE RJ45 and 2x 10 Gbps SFP+ fixed Ethernet ports, and includes two Network I/O slots, allowing for additional connectivity. The appliances contain an integrated, dual redundant (optional for NGFW 2101), 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 3 – NGFW 2101 (Front Panel)

Figure 4 – NGFW 2101 (Rear Panel)

Figure 5 – NGFW 2105 (Front Panel)

Figure 6 – NGFW 2105 (Rear Panel)

- The **NGFW 3305** (Figure 7 and Figure 8) is a 2U rack-mounted design featuring modular connectivity. The NGFW 3305 is equipped with 2x GE RJ45 and 1x 40 Gbps QSFP[15] fixed Ethernet ports, and includes four 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 7 – NGFW 3305 (Front Panel)

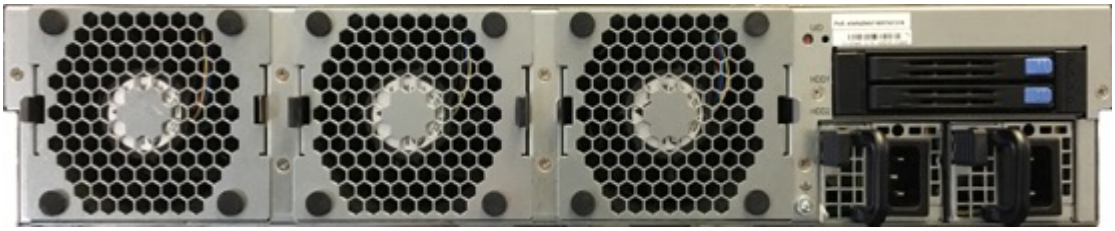

Figure 8 – NGFW 3305 (Rear Panel)

- The **NGFW 6205** (Figure 9 and Figure 10) is a 4U rack-mounted design featuring modular connectivity. The NGFW 6205 is equipped with 2x GE RJ45 and 1x 40 Gbps QSFP 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 +10°C to +40°C (+50°F to +104°F).

[15] QSFP – Quad Small Form-Factor Pluggable

Figure 9 – NGFW 6205 (Front Panel)

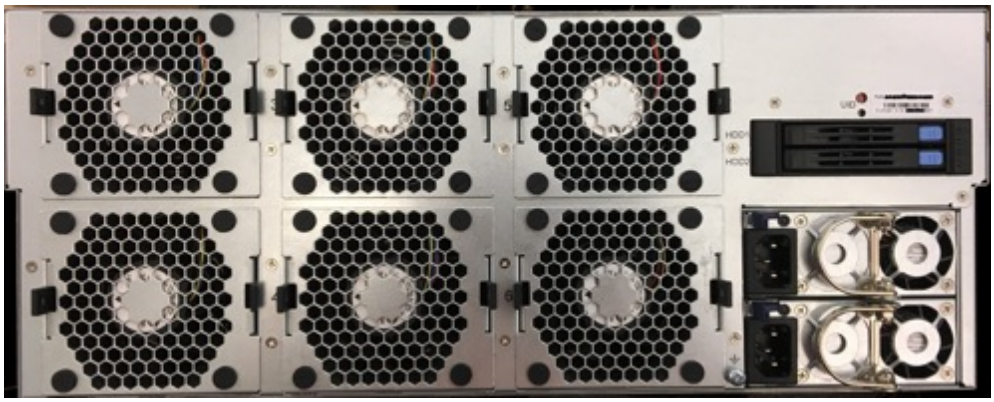

Figure 10 – NGFW 6205 (Rear Panel)

The NGFW appliances are validated at the FIPS 140-2 section levels shown in Table 1.

Table 1 – Security Level per FIPS 140-2 Section

Section	Section Title	Level
1	Cryptographic Module Specification	2
2	Cryptographic Module Ports and Interfaces	2
3	Roles, Services, and Authentication	2
4	Finite State Model	2
5	Physical Security	2
6	Operational Environment	N/A
7	Cryptographic Key Management	2
8	EMI/EMC[16]	2

[16] EMI/EMC – Electromagnetic Interference / Electromagnetic Compatibility

Section	Section Title	Level
9	Self-tests	2
10	Design Assurance	2
11	Mitigation of Other Attacks	N/A

2.2 Module Specification

The NGFW appliances are hardware cryptographic modules with a multiple-chip standalone embodiment. The overall security level of the modules is 2. The cryptographic modules consist of firmware and hardware components enclosed in a secure, industrially-hardened metal case. For all appliances, the cryptographic boundary is defined as the outer edge of the chassis (illustrated by the red-dotted line shown in

Figure 11 below).

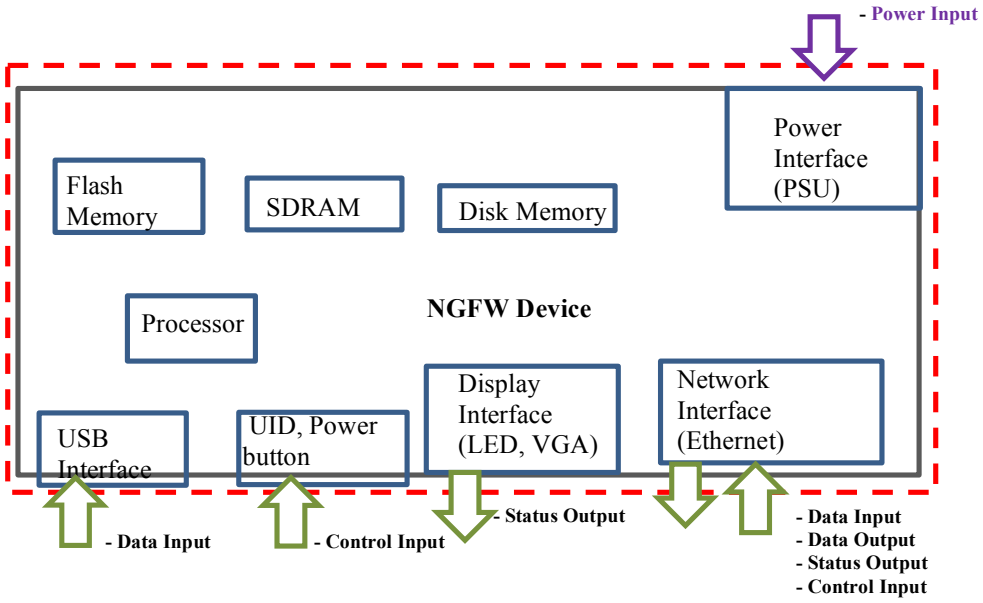

Figure 11 – NGFW Cryptographic Boundary

Each module is primarily composed of the following components:

- Processor
- SDRAM[17]
- Flash Memory
- Disk Memory
- Main Circuit Board
- Network Component(s)
- LEDs[18]
- Power Supply(s)

[17] SDRAM – Synchronous Dynamic Random Access Memory
[18] LED – Light Emitting Diode

Table 2 – NGFW Hardware Components

Appliance	Component	Quantity
1101	Intel Pentium D Processor	1
	16 GB[19] DDR4[20] RAM[21]	2
	BMC AST 2300	1
	1U, PCIE[22] G3, Network Component	1
	CFast[23] Card	1
	Flash System BIOS[24]	1
	TPM[25] Header	1
	Power Supply Unit	1
2101	Intel Xeon D Processor	1
	16 GB DDR4 RAM	2
	PCH Intel C612 chipset	1
	1U, PCIE G3, Network Component	2
	CFast Card	1
	Flash System BIOS	1
	TPM Header	1
	Power Supply Unit	1
2105	Intel Xeon D Processor	1
	16 GB DDR4 RAM	2
	PCH Intel C612 chipset	1
	1U, PCIE G3, Network Component	2
	CFast Card	1
	Flash System BIOS	1
	TPM Header	1
	Power Supply Unit	2
3305	Intel Xeon E5 Processors	2
	16 GB DDR4 RAM	8
	PCH Intel C612 chipset	1
	1U, PCIE G3, Network Component	4
	SSD[26], 2.5",480GB HAGIWARA SERIES XFD25S	1

[19] GB – Gigabyte
[20] DDR4 – Double Data Rate
[21] RAM – Random Access Memory
[22] PCIE – Peripheral Component Interconnect Express
[23] CFast – Compact Fast
[24] BIOS – Basic Input/Output System
[25] TPM – Trusted Platform Module
[26] SSD – Solid State Drive

Appliance	Component	Quantity
	Flash System BIOS	1
	TPM Header	1
	Power Supply Unit	2
6205	Intel Xeon E5 Processors	2
	16 GB DDR4 RAM	8
	PCH Intel C612 chipset	1
	1U, PCIE G3, Network Component	8
	SSD, 2.5",480GB HAGIWARA SERIES XFD25S	1
	Flash System BIOS	1
	TPM Header	1
	Power Supply Unit	2

In addition to the primary components listed above, the appliances feature a modular design that makes them highly configurable. Because of the modular design, the appliances have numerous combinations of interfaces and networking capabilities. However, these customer-orderable components do not provide any additional cryptography-related services or logic. Instead, these components provide options for flexible network connectivity. Each available slot must be filled with a Network Component when in FIPS-Approved mode of operation. The selection and configuration of components has no impact on the FIPS-related behavior of the modules. Validation testing was performed on the specific configuration(s) of each appliance as listed in Table 3 below.

Table 3 – NGFW Tested Configurations

Model	Slots	Network Component Configuration	Network Component Description
NGFW 1101	1	MOD-GE-SFP-4	4 Port Gigabit Ethernet SFP[27] component
NGFW 2101	2	MOD-GE-8	8 Port Gigabit Ethernet RJ45[28] component
		MOD-EM2-10G-SFP-4	4 Port 10 Gigabit Ethernet SFP+ component
NGFW 2105	2	MOD-GE-8	8 Port Gigabit Ethernet RJ45 component
		MOD-40G-2	2 Port 40 Gigabit Ethernet QSFP[29] component
NGFW 3305	4	MOD-GE-8	8 Port Gigabit Ethernet RJ45 component
		MOD-40G-2	2 Port 40 Gigabit Ethernet QSFP component
		MOD-EM2-10G-SFP-4	4 Port 10 Gigabit Ethernet SFP+ component
		MOD-GE-SFP-4	4 Port Gigabit Ethernet SFP component
NGFW 6205	8	2x MOD-GE-8	8 Port Gigabit Ethernet RJ45 component
		2x MOD-40G-2	2 Port 40 Gigabit Ethernet QSFP component

[27] SFP – Small Form-Factor Pluggable
[28] RJ45 – Registered Jack 45
[29] QSFP – Quad Small Form-Factor Pluggable

Model	Slots	Network Component Configuration	Network Component Description
		2x MOD-EM2-10G-SFP-4	4 Port 10 Gigabit Ethernet SFP+ component
		2x MOD-GE-SFP-4	4 Port Gigabit Ethernet SFP component

The module contains the following cryptographic firmware components:

- OpenSSL FIPS Object Module 2.0.14 SE (referred to as OpenSSL Library) built in FIPS-capable OpenSSL 1.0.2. The cryptographic implementations from this library are used by the Linux based operating system for TLS[30] communication and TLS key/certificate management.

- Forcepoint NGFW Cryptographic Library (referred to as NGFW Library) built based on a VPN Crypto Library. The NGFW Library is a shared library that provides cryptographic algorithms and services in NGFW firmware user space. The cryptographic implementations from this library are used for IKE[31] in VPN, VPN key/certificate management, RSA[32] key generation for TLS, and certification validation.

- Forcepoint NGFW Cryptographic Kernel component (referred to as NGFW Kernel) is a loadable kernel component that provides cryptographic algorithms and services in NGFW firmware kernel space. The NGFW Kernel is a subset of the VPN Crypto Library linked to a loadable kernel component. The cryptographic implementations from NGFW Kernel are used for IPsec[33].

In addition, the module implements TLS KDFs[34] and PBKDF2 in Linux OS user space and IKE v1, IKE v2 KDFs in NGFW firmware user space.

The following section lists the FIPS-Approved cryptographic algorithms, FIPS-Allowed cryptographic algorithms, and KDFs in Table 4, Table 5, and Table 6, respectively.

Table 4 – FIPS-Approved Algorithm Implementations[35]

Algorithm	CSP[36]	Standard	Certificate Number								
			NGFW 1101			NGFW 2101 and 2105			NGFW 3305 and 6205		
			Intel Pentium D Processor			Intel Xeon D Processor			Intel Xeon E5 Processor		
			OpenSSL Library	NGFW Library	NGFW Kernel	OpenSSL Library	NGFW Library	NGFW Kernel	OpenSSL Library	NGFW Library	NGFW Kernel
AES[37] CBC[38] encryption/decryption	128 and 256-bit keys	FIPS 197	5168	5511	5514	5168	5512	5515	5168	5513	5516
AES ECB[39] encryption/decryption	128 and 256-bit keys	FIPS 197	5168	5511	-	5168	5512	-	5168	5513	-

[30] TLS – Transport Layer Security
[31] IKE – Internet Key Exchange
[32] RSA – Rivest, Shamir, Adleman
[33] IPsec – Internet Protocol Security
[34] KDF – Key Derivate Function
[35] This table only contains algorithms with modes and block sizes included in the FIPS validated module described in this Security Policy. Additional algorithms with mode and block sizes have been validated by CAVP but are not used in the FIPS validated module.
[36] CSP – Critical Security Parameter
[37] AES – Advance Encryption Service
[38] CBC – Cipher Block Chaining
[39] ECB – Electronic Code Book

Algorithm	CSP[36]	Standard	Certificate Number								
			NGFW 1101			NGFW 2101 and 2105			NGFW 3305 and 6205		
			Intel Pentium D Processor			Intel Xeon D Processor			Intel Xeon E5 Processor		
			OpenSSL Library	NGFW Library	NGFW Kernel	OpenSSL Library	NGFW Library	NGFW Kernel	OpenSSL Library	NGFW Library	NGFW Kernel
AES CFB128[40] encryption/decryption	128-bit keys	FIPS 197	5168	-	-	5168	-	-	5168	-	-
AES-GCM[41] authenticated encryption and decryption	128-bit keys	NIST SP[42] 800-38D	5168	-	5514	5168	-	5515	5168	-	5516
	256-bit keys		5168	-	5514	5168	-	5515	5168	-	5516
AES key wrapping	256-bit keys	SP 800-38F	-	5511	-	-	5512	-	-	5513	-
Triple-DES[43] CBC encryption and decryption	168-bit keys	NIST SP 800-67	2632	2774	2777	2632	2775	2778	2632	2776	2779
Triple-DES[44] ECB encryption and decryption	168-bit keys	NIST SP 800-67	2632	-	-	2632	-	-	2632	-	-
RSA key-pair generation	2048, 3072 bits modulus size. Public key value 65537.	FIPS 186-4	-	2957	-	-	2958	-	-	2959	-
RSA signature generation (PKCS[45]#1 v1.5)	2048, 3072-bit modulus	FIPS 186-4	2777	2957	-	2777	2958	-	2777	2959	-
RSA signature generation (PSS)	2048-bit modulus	FIPS 186-4	2777	-	-	2777	-	-	2777	-	-
RSA signature verification (PKCS#1 v1.5)	1024, 2048, 3072-bit modulus	FIPS 186-4	2777	2957	-	2777	2958	-	2777	2959	-
RSA signature verification (PSS)	2048-bit modulus	FIPS 186-4	2777	-	-	2777	-	-	2777	-	-
ECDSA[46] key-pair generation	P-224, P-256, P-384, P-521	FIPS 186-4	1339	1480	-	1339	1481	-	1339	1482	-
ECDSA signature generation	P-224, P-256, P-384, P-521	FIPS 186-4	1339	1480	-	1339	1481	-	1339	1482	-
ECDSA signature verification	P-192, P-224, P-256, P-384, P-521	FIPS 186-4	1339	1480	-	1339	1481	-	1339	1482	-

[40] CFB – Cipher Feedback
[41] GCM – Galois/Counter
[42] SP – Special Publication
[43] DES – Data Encryption Standard
[44] DES – Data Encryption Standard
[45] PKCS – Public Key Cryptography Standard
[46] ECDSA – Elliptic Curve Digital Signature Algorithm

Algorithm	CSP[36]	Standard	Certificate Number								
			NGFW 1101			NGFW 2101 and 2105			NGFW 3305 and 6205		
			Intel Pentium D Processor			Intel Xeon D Processor			Intel Xeon E5 Processor		
			OpenSSL Library	NGFW Library	NGFW Kernel	OpenSSL Library	NGFW Library	NGFW Kernel	OpenSSL Library	NGFW Library	NGFW Kernel
SHS[47] Message Digest	SHA[48]-1 SHA-224 SHA-256 SHA-384 SHA-512	FIPS 180-4	4175	4422	4425	4175	4423	4426	4175	4424	4427
HMAC[49]-SHA-1 HMAC-SHA-224 HMAC-SHA-256 HMAC-SHA-384 HMAC-SHA-512	At least 112 bits HMAC key	FIPS 198-1	3429	3667	3670	3429	3668	3671	3429	3669	3672
EC[50] Diffie-Hellman shared secret computation	P-224, P-256, P-384, P-521	NIST SP 800-56A	CVL 1676	CVL 1957	-	CVL 1676	CVL 1959	-	CVL 1676	CVL 1961	-
SP 800-90A CTR_DRBG[51]	AES 256 ECB Mode	NIST SP 800-90A	1946	2179	-	1946	2180	-	1946	2181	-

Table 5 – FIPS-Allowed Algorithm Implementations

Algorithm[52]	Use	Library
Diffie-Hellman (DH)	Used for key agreement during TLS and IKE (2048-bit keys)	OpenSSL Library NGFW Library
EC Diffie-Hellman (ECDH)	Used for key agreement during TLS and IKE (P-224, P-256, P-384, P-521 curves)	OpenSSL Library NGFW Library
RSA	Used for key establishment during TLS (2048-bit and 3072-bit keys)	OpenSSL Library
Non-Deterministic Random Number Generator (NDRNG)	The NDRNG is used for seeding the DRBGs. It is based on non-deterministic entropy from Linux kernel Random Number Generator (LKRNG) which in turn uses jitterentropy-rngd as the entropy source. The module meets the scenario 1a) of IG 7.14 where the NDRNG is inside the module's boundary and the NDRNG provides 256 bits of entropy.	Jitterentropy-rngd – NGFW Firmware User Space /dev/random – Linux Kernel

[47] SHS – Secure Hash Standard
[48] SHA – Secure Hash Algorithm
[49] HMAC – Hash-based Message Authentication Code
[50] EC – Elliptical Curve
[51] DRBG – Deterministic Random Bit Generator
[52] Please section 2.7 for the encryption strength of all the key establishment schemes

Table 6 – KDF Algorithm Certificate Numbers

KDF	Standard	Library	Certificate Number		
			NGFW 1101	NGFW 2101 and 2105	NGFW 3305 and 6205
			Intel Pentium D Processor	Intel Xeon D Processor	Intel Xeon E5 Processor
TLS v1.0/1.1 TLS v1.2 KDF	SP 800-135	/usr/lib/x86_64-linux-gnu/libssl.so.1.0.2	CVL 1958	CVL 1960	CVL 1962
IKE v1 IKE v2 KDF	SP 800-135	/usr/lib/libqskdf.so.1	CVL 1958	CVL 1960	CVL 1962
KBKDF[53]	SP 800-108	/usr/lib/libsgcommon.so.1	230	231	232
PBKDF2[54]	SP 800-132	/usr/lib/x86_64-linux-gnu/libssl.so.1.0.2	Vendor Affirmed	Vendor Affirmed	Vendor Affirmed

2.3 Module Interfaces

The modules' physical ports can be categorized into the following logical interfaces defined by FIPS 140-2:

- Data Input Interface
- Data Output Interface
- Control Input Interface
- Status Output Interface

Table 7 lists the physical ports/interfaces available in the NGFW appliances and also provides the mapping from the physical ports/interfaces to logical interfaces as defined by FIPS 140-2. For additional information on modules' ports and interfaces refer to the following Hardware Guides:

- *Forcepoint Next Generation Firewall Hardware Guide Models 1101, 2101, 2105 Revision C*
- *Forcepoint Next Generation Firewall Hardware Guide Models 3305 Revision F*
- *Forcepoint Next Generation Firewall Hardware Guide Models 6205 Revision B*

Table 7 – FIPS 140-2 Logical Interface Mappings

Module	Physical Port/Interface	Quantity	FIPS 140-2 Logical Interface
1101	VGA[55] port	1	Status Output
	Ethernet port (1 Gbps[56])	8	Data Input, Data Output, Control Input, Status Output
	Ethernet port (1 Gbps) LEDs[57]	16	Status Output
	Ethernet port (10 Gbps)	2	Data Input, Data Output, Control Input, Status Output
	Ethernet port (10 Gbps) LEDs	4	Status Output

[53] KBKDF – Key Based Key Derivation Function
[54] PBKDF2 – Password Based Key Derivation Function
[55] VGA – Video Graphics Array
[56] Gbps – Gigabits per second
[57] LEDs – Light Emitting Diodes

Module	Physical Port/Interface	Quantity	FIPS 140-2 Logical Interface
	IPMI[58] port	1	Disabled in the validated configuration
	Power button	1	Control Input
	Power button LED	1	Status Output
	Indicator LEDs	4	Status Output
	UID[59] button (1 front and 1 rear)	2	Control Input
	UID LEDs (1 front, 1 rear)	2	Status Output
	Network Component slot (Ethernet ports) *	1	Data Input, Data Output, Control Input, Status Output
	Console port	1	Disabled in the validated configuration
	USB[60] ports	3	Data Input
	Power supply port	1	Power Input
2101	VGA port	1	Status Output
	Ethernet port (1 Gbps)	12	Data Input, Data Output, Control Input, Status Output
	Ethernet port (1 Gbps) LEDs	24	Status Output
	Ethernet port (10 Gbps)	2	Data Input, Data Output, Control Input, Status Output
	Ethernet port (10 Gbps) LEDs	4	Status Output
	IPMI port	1	Disabled in the validated configuration
	Power button	1	Control Input
	Power button LED	1	Status Output
	Indicator LEDs	4	Status Output
	UID button (1 front, 1 rear)	2	Control Input
	UID LEDs (1 front, 1 rear)	2	Status Output
	Network Component slot (Ethernet ports)*	2	Data Input, Data Output, Control Input, Status Output
	Console port	1	Disabled in the validated configuration
	USB ports	3	Data Input
	Power supply port	1	Power Input
2105	VGA port	1	Status Output
	Ethernet port (1 Gbps)	12	Data Input, Data Output, Control Input, Status Output
	Ethernet port (1 Gbps) LEDs	24	Status Output
	Ethernet port (10 Gbps)	2	Data Input, Data Output, Control Input, Status Output
	Ethernet port (1 Gbps) LEDs	4	Status Output
	IPMI port	1	Disabled in the validated configuration
	Power button	1	Control Input
	Power button LED	1	Status Output

[58] IPMI – Intelligent Platform Management Interface
[59] UID – Unit Identification
[60] USB – Universal Serial Bus

Module	Physical Port/Interface	Quantity	FIPS 140-2 Logical Interface
	Indicator LEDs	4	Status Output
	UID button (1 front and 1 rear)	2	Control Input
	UID LEDs (1 front, 1 rear)	2	Status Output
	Network Component slot (Ethernet ports)*	2	Data Input, Data Output, Control Input, Status Output
	Console port	1	Disabled in the validated configuration
	USB ports	3	Data Input
	Power supply port	2	Power Input
3305	VGA port	1	Status Output
	Ethernet port (1 Gbps)	2	Data Input, Data Output, Control Input, Status Output
	Ethernet port (1 Gbps) LEDs	4	Status Output
	Ethernet port (40 Gbps)	1	Data Input, Data Output, Control Input, Status Output
	Ethernet port (40 Gbps) LEDs	2	Status Output
	IPMI port	1	Disabled in the validated configuration
	Power button	1	Control Input
	Indicator LEDs	4	Status Output
	UID button (1 front and 1 rear)	2	Control Input
	UID LED (1 rear)	1	Status Output
	Network Component slot (Ethernet ports)*	4	Data Input, Data Output, Control Input, Status Output
	Console port	1	Disabled in the validated configuration
	USB ports	4	Data Input
	Power supply port	2	Power Input
	SSD LEDs	4	Status Output
6205	VGA port	1	Status Output
	Ethernet port (1 Gbps)	2	Data Input, Data Output, Control Input, Status Output
	Ethernet port (1 Gbps) LEDs	4	Status Output
	Ethernet port (40 Gbps)	1	Data Input, Data Output, Control Input, Status Output
	Ethernet port (40 Gbps) LEDs	2	Status Output
	IPMI port	1	Disabled in the validated configuration
	Power button	1	Control Input
	Indicator LEDs	4	Status Output
	UID button (1 front and 1 rear)	2	Control Input
	UID LEDs (1 rear)	1	Status Output
	Network Component slot (Ethernet ports)*	8	Data Input, Data Output, Control Input, Status Output
	Console port	1	Disabled in the validated configuration
	USB ports (2 2.0 ports, 3 3.0 ports)	5	Data Input
	Power supply port	1	Power Input

Module	Physical Port/Interface	Quantity	FIPS 140-2 Logical Interface
	SSD LEDs	4	Status Output

*See Table 3 for information on ports on Network Components and the tested configurations.

As described above, the modules have a number of LEDs that indicate various states and conditions. The descriptions for the LEDs are listed in Table 8 below.

Table 8 – Module LED Descriptions

Module	LED	State	Description
1101 2101 2105	Power button LED	Green	The module is in a running state.
		Red	The module is in a standby state.
		Off	The module is powered down.
	Indicator LED (Warning)	Red (Steady)	Overheating or general system failure.
		Red (Flashing)	Fan failure.
		Off	The module is powered down.
	Indicator LED (Disk Activity)	Green (Flashing)	Indicates CFast card activity.
		Off	Indicates no CFast card activity.
	Indicator LED (Firmware Status)	Amber (Flashing)	Initial contact is established but the module is offline.
		Green	The module is online.
		Off	The module is powered down.
	Indicator LED (Management connectivity)	Green	Connection between the module and the Management Server has been established.
		Off	The module is powered down or connection loss with SMC
	UID LED	Blue	The UID indicator has been switched on. When the UID button is pressed, the UID indicators on the front and rear panel turn on until the UID button is pressed again.
	Ethernet Port (1 Gbps) LED (Activity/Link Indicator)	Green (Steady)	Link OK.
		Green (Flashing)	Link activity.
		Off	No link detected.
	Ethernet Port (1 Gbps) LED (Link Speed Indicator)	Unlit	10 Mbps[61] link or no link detected
		Amber	100 Mbps link.
		Green	1 Gbps link.
	Ethernet Port (10 Gbps) LED (Link Status Indicator)	Blue	Link OK.
		Off	No link detected.
	Ethernet Port (10 Gbps) LED (Link Speed Indicator)	Green	10 Gbps
		Off	No link detected.

[61] Mbps – Megabits per second

3305	Indicator LED (Power)	Green	The module is in a running state.
		Red	The module is in a standby state.
		Off	The module is powered down.
	Indicator LED (Warning)	Red (Steady)	Overheating or general system failure.
		Red (Flashing)	Fan failure.
		Off	The module is powered down.
	Indicator LED (Disk Activity)	Amber	Indicates SSD activity.
		Off	Indicates no SSD activity.
	Indicator LED (UID)	Blue	The UID indicator has been switched on. When the UID button is pressed, the UID indicators on the front and rear panel turns on until the UID button is pressed again.
	UID LED (rear)	Blue	The UID indicator has been switched on. When the UID button is pressed, the UID indicators on the front and rear panel turn on until the UID button is pressed again.
	Ethernet Port (1 Gbps) LED (Activity Indicator)	Amber (Steady)	Link OK.
		Amber (Flashing)	Link activity.
	Ethernet Port (1 Gbps) LED (Link Speed Indicator)	Unlit	No link.
		Orange	100 Mbps link.
		Green	1 Gbps link.
	Ethernet Port (40 Gbps) LED (Activity Indicator)	Amber (Steady)	Link OK.
		Amber (Flashing)	Link activity.
	Ethernet Port (40 Gbps) LED (Link Speed Indicator)	Unlit	No link.
		Green	40 Gbps link.
	SSD LED (Power Indicator)	Blue	An SSD is in the bay.
	SSD LED (Disk Indicator)	Unlit	This indicator is not used.
6205	Indicator LED (Power)	Green	The module is in a running state.
		Red	The module is in a standby state.
		Off	The module is powered down.
	Indicator LED (Warning)	Red (Steady)	Overheating or general system failure.
		Red (Flashing)	Fan failure.
		Off	The module is powered down.
	Indicator LED (Disk Activity)	Amber	Indicates SSD activity.
		Off	Indicates no SSD activity.
	Indicator LED (UID)	Blue	The UID indicator has been switched on. When the UID button is pressed, the UID indicators on the front and rear panel turn on until the UID button is pressed again.
	UID LED (rear)	Blue	The UID indicator has been switched on. When the UID button is pressed, the UID indicators on the front and rear panel turn on until the UID button is pressed again.

	Ethernet Port (1 Gbps) LED (Activity Indicator)	Yellow (Steady)	Link OK.
		Yellow (Flashing)	Link activity.
	Ethernet Port (1 Gbps) LED (Link Speed Indicator)	Unlit	No link.
		Amber	100 Mbps link.
		Green	1 Gbps link.
	Ethernet Port (40 Gbps) LED (Activity Indicator)	Amber (Steady)	Link OK.
		Amber (Flashing)	Link activity.
	Ethernet Port 410 Gbps) LED (Link Speed Indicator)	Unlit	No link.
		Green	10 Gbps link.
	SSD LED (Power Indicator)	Blue	An SSD is in the bay.
	SSD LED (Disk Indicator)	Blue (Flashing)	Indicates SSD activity.

2.4 Roles, Services, and Authentication

The sections below describe the modules' roles and services and define the authentication methods employed.

2.4.1 Authorized Roles

There are two authorized roles that module operators may assume: Crypto Officer (CO) role or a User role.

- CO role - The Security Management Center (SMC) is the only calling management entity of the NGFW modules and acts as the CO role. The SMC establishes secure management connections to the module over TLS. Once the initial contact has been established, the module receives a X.509 certificate from the SMC, which is used for authentication. The X.509 certificates use ECDSA P-521. After initializing the module and initial contact with the SMC, all post-installation configuration and modification of initial configuration is secured using TLS connections from the SMC. If the X.509 certificate is expired or is deleted, the initial contact process with the SMC specified in section 3.2 needs to be repeated.
- User role - The HTTPS user, SSL VPN and IPsec VPN tunneling clients, SNMP manager, peer NGFW modules in a cluster, and Log Server assume the role of users. The operators assuming the role of a User can make use of services but cannot access the modules for administrative purposes. The HTTPS, SSL VPN portal, and SNMP users are authenticated using username and password, and the modules can store user accounts in internal databases or can be integrated with external directory servers. The SSL VPN and IPsec VPN tunneling clients, peer NGFW modules in a cluster, and Log Server establish secure sessions with the module using TLS or IPsec and are authenticated using certificates with RSA/ECDSA signature verification or a pre-shared key in case of IPsec VPN.

The module does not provide a Maintenance role. The module supports concurrent operators belonging to different roles: one CO and one User role, which creates two different authenticated sessions, achieving the separation between the concurrent operators.

2.4.2 Operator Services

Table 9 below provides a list of services offered by the modules, authorized role per service, and indicates the type of access required. The following notation is used for indicating access type:

- R – Read: The plaintext CSP is read by the service.
- W – Write: The CSP is established, generated, modified, or zeroized by the service.
- X – Execute: The CSP is used within an Approved or Allowed security function

Table 9 – FIPS-Approved Mode Services

Service	Operator		Access	CSP	Description
	CO	User			
Initialize the module	✓	-	WRX	Firmware Update Verification Key Configuration File Protection Key	Set up the module using the NGFW Initial Configuration Wizard. The setup process includes mandatory firmware upgrade, applying initial configuration, and enabling FIPS 140-2 Approved-mode. For more information, see section 3.
Establish secure management connection	✓	-	WRX	TL Key set[62]	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.
Key pair management service	✓	-	WRX	VPN RSA Private Key VPN ECDSA Private Key HTTPS RSA Private Key VPN DRBG Entropy Input VPN DRBG V, key TLS key set	SMC using the management communication protocol requests the NGFW Engine to generate key pair and certificate signing request.
User management service	✓	-	WRX	User password TLS Key set	SMC enters the user password hashes using LDAPS.
Modify and apply configuration	✓	-	WRX	Configuration file encryption key Configuration file authentication key Key Encryption Passphrase VPN Pre-Shared Key RWP RSA Private RWP ECDSA Private Key	Verify and apply the configuration changes to the modules securely, including configuration of client protection and server protection certificate authority and TLS credentials.

[62] TLS Key Set implies the following CSPs - TLS Encryption Key, TLS Authentication Key, TLS Pre-Master Secret, TLS Master Secret, NGFW ECDSA Private Key, TLS ECDH Private Key, TLS DRBG Entropy Input, TLS DRBG V, key

Service	Operator		Access	CSP	Description
	CO	User			
				RWP Cookie Protection Master Key1 RWP Cookie Protection Master Key2 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 Server Protection RSA Private Key Server Protection ECDSA Private Key SNMP encryption key SNMP authentication key Cluster Protocol Key	
Establish IPsec VPN connections	-	✓	WRX	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 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 DRBG Entropy Input VPN DRBG, V, key	VPN tunneling clients establish secure IPsec VPN connections to the module.
Establish SSL VPN connections	-	✓	WRX	User Password RWP[63] Encryption Key RWP Authentication Key RWP Pre-master Secret RWP Master Secret RWP Cookie Protection Master Key1 RWP Cookie Protection Master Key2 RWP Cookie Protection User Key1 RWP Cookie Protection User Key2 RWP RSA Private RWP ECDSA Private Key RWP DH Private Key RWP DH Shared Secret RWP ECDH Private Key RWP ECDH Shared Secret	VPN tunneling clients establish secure SSL VPN connections to the module using a web portal or a client application.

63 Reverse Web Proxy (RWP) is the alternate name for the SSL VPN Portal

Service	Operator		Access	CSP	Description
	CO	User			
Establish Mobile IPsec/ SSL VPN connections	-	✓	WRX	User Password SSL VPN encryption Key SSL VPN authentication Key SSL VPN Pre-master Secret SSL VPN Master Secret SSL VPN ECDH Private Key SSL VPN ECDH Shared Secret SSL VPN DH Private Key SSL VPN DH Shared Secret SSL VPN IV VPN RSA Private Key VPN ECDSA Private Key IKE Encryption Key IKE Authentication Key SKEYID, SKEYID_d SKEYSEED, SK_d, SK_pi, SK_pr IPsec Encryption Key IPsec Authentication Key VPN Pre-Shared Key VPN DH Private Key VPN DH Shared Secret VPN ECDH Private Key TLS DRBG Entropy Input TLS DRBG V, key VPN ECDH Shared Secret VPN DRBG Entropy Input VPN DRBG, V, key	Mobile VPN tunneling clients establish secure IPsec/SSL VPN connections to the module.
Establish secure peer connections	-	✓	WRX	Cluster Protocol Key State Synchronization Key VPN RSA Private Key HTTPS RSA Private Key RWP Cookie Protection Master Key1 RWP Cookie Protection Master Key2 TLS Key Set VPN Key Encryption Key	Peer NGFW modules establish secure network connection within a cluster.
HTTPS user authentication	-	✓	WRX	User Password HTTPS Encryption Key HTTPS Authentication Key HTTPS Pre-master Secret HTTPS Master Secret HTTPS RSA Private Key HTTPS DH Private Key HTTPS DH Shared Secret HTTPS ECDH Private Key HTTPS ECDH Shared Secret TLS DRBG Entropy Input TLS DRBG V, key	End user's authentication to the module via web browser.

Service	Operator		Access	CSP	Description
	CO	User			
Inspect TLS traffic	-	✓	WRX	Inspection DH Shared Secret Inspection DH Private Key Inspection ECDH Shared Secret Inspection ECDH Private Key Inspection Encryption Key Inspection Authentication Key Inspection Pre-master Secret Inspection Master Secret TLS DRBG Entropy Input TLS DRBG, V, key	Perform TLS inspection on HTTPS network traffic.
HTTPS proxy	-	✓	WRX	SSM[64] HTTPS DH Shared Secret SSM HTTPS DH Private Key SSM HTTPS ECDH Shared Secret SSM HTTPS ECDH Private Key SSM HTTPS Encryption Key SSM HTTPS Authentication Key SSM HTTPS Pre-master Secret SSM HTTPS Master Secret TLS DRBG Entropy Input TLS DRBG, V, key	Sidewinder proxy used for outbound traffic.
Export logs and monitoring data	-	✓	WRX	TLS Key Set	Traffic logs and monitoring data are exported to Log Server securely.
SNMP[65] encryption & authentication	-	✓	RX	SNMP encryption key SNMP authentication key	SNMP manager receives network management information and traps

2.4.3 Additional Services

The modules provide a limited number of services for which the operator is not required to assume an authorized role. Table 10 lists the services for which the operator is not required to assume an authorized role. None of the services listed in the table modify, disclose, or substitute cryptographic keys and CSPs or otherwise affect the security of the modules.

Table 10 – Additional Services

Service	Access	CSP	Description
Show status	-	None	View status of the module via the LEDs (see section 2.3), the error message displayed via VGA port.
Execute self-tests (restart the module)	W	All keys and CSPs stored in SDRAM. For more information, see section 2.7.	Perform power up self-tests on demand by power cycling the module.
	WRX	Root File System Integrity Test HMAC Key	
Shutdown the module	W	All keys and CSPs stored in SDRAM. For more information, see section 2.7.	Shutdown the module by removing the power.

[64] SSM Source-specific multicast
[65] The module does not implement SNMP KDF. The derived key enters from outside of the module.

Service	Access	CSP	Description
Zeroize keys (reset to factory state)	W	All Keys and CSPs stored in SDRAM and on disk. For more information, see section 2.7.	The module will overwrite all CSPs. Zeroization of keys can be invoked by restarting the module or performing a factory reset. For more information, see section 3.2.4.

2.4.4 Authentication

The modules support role-based authentication. Role assumption is explicit and is based on the authentication credential employed. The module does not maintain authenticated sessions upon power cycling. When power cycling the module, any active authenticated session is terminated and upon restart a new session needs to be initiated requiring the authentication credentials to be re-entered. There is no visible display of the authentication data. The authentication data is protected by the OS and restricting physical access to the internal storage media.

For signature verification based authentication with certificates, either RSA or ECDSA is used with a minimum key size of 2048 bits or a P-224 curve, providing 112-bit security strength. For pre-shared key (PSK), the minimum length is 14 characters. For user passwords, hashed values of the passwords are entered electronically to NGFW modules from SMC over TLS channel. The passwords are stored protected within the module via a hash mechanism using SHA-512. Table 11 provides the strength of the authentication mechanisms used by the modules.

Table 11 – Authentication Mechanism Used by the Modules

Authentication Type	Strength
Signature Verification	The public key used for authentication can either be ECDSA or RSA, yielding at least 112 bits of strength, assuming the smallest curve size P-224 or modulus size 2048 bit. The chance of a random authentication attempt falsely succeeding is: $1/(2^{112})$ which is less than 1:1,000,000 as required by FIPS 140-2. Assuming the scenario of 1 attempt per microsecond, there can be 60000000 attempts in a one minute period. This means that at worst case an attacker has the probability of guessing the password in one minute as 60000000/2^112 which is less than the requirement of 1/100,000.
User password	Once properly configured, the minimum length of the password is 8 characters, with 94 different case-sensitive alphanumeric characters and symbols possible for usage. Assuming a minimum password length of 8 characters, assuming the worst-case scenario where all 8 characters are digits, the chance of a random attempt falsely succeeding is: $1/(10^{8})$ which is less than 1:1,000,000 as required by FIPS 140-2. The module adds a two second delay between each login attempt. So, 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 30/10^8 which is less than the requirement of 1/100,000.

Authentication Type	Strength
Pre-Shared key	The minimum PSK length is 14 characters. So, assuming the worst-case scenario where all the 14 characters are digits, the probability to guess every character successfully is $1/(10^{14})$ which is less than 1:1,000,000. Assuming the scenario of 1 attempt per microsecond, there can be 60000000 attempts in a one minute period. This means that in the worst case, an attacker has the probability of guessing the password in one minute as 60000000/10^14 which is less than the requirement of 1/100,000.

2.4.5 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 or SSL 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, in order 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.

SSL/IPSEC VPN/SSL Portal/HTTPS – The Situation field in the Logs view indicates the respective operations performed by these services. For example, “IPsec-SA-Responder-Done”, “SSL-VPN-webservice-access-granted”.

TLS inspection – For this service the Situation field in the Logs view shows “Connection_Allowed” and the TLS decrypted field in Connections[66] view is "true".

2.5 Physical Security

Each of the NGFW appliances consists of production-grade components that include standard passivation techniques. Each appliance is encased in a hard metal enclosure made of galvanized steel.

There are a limited set of ventilation holes provided in the module enclosures. Internal baffles cover the ventilation holes, which makes it impossible to view the internal components of the module. Tamper-evident seals are applied to the enclosures to provide physical evidence of unauthorized attempts to open the enclosure or remove module components. The tamper-evident seals must be inspected every 96 hours for signs of tampering. The placement of the tamper-evident seals can be found in the Secure Operation section 3 of this document.

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

2.6 Operational Environment

The modules employ a non-modifiable operating environment. The modules do not provide a general-purpose operating system to module operators. The modules’ processors (Intel Pentium D Processor, Intel Xeon D Processor, and Intel Xeon E5 Processors) run Forcepoint NGFW firmware based on a Debian Linux hardened operating system in a non-modifiable operational environment.

[66] The connection monitoring view may need to be reopened to refresh the status information of the recently established connection.

2.7 Cryptographic Key Management

Table 12 below describes the keys and CSPs supported by the modules. In accordance with FIPS 140-2 IG D.12, the cryptographic module performs Cryptographic Key Generation (CKG) as per SP 800-133 (vendor affirmed). For generation of RSA and EC keys, the module implements asymmetric key generation services compliant with FIPS 186-4, and using DRBG compliant with SP 800-90A. A seed (i.e. the random value) used in asymmetric key generation is obtained from SP 800-90A CTR_DRBG. The symmetric keys used are either derived from a shared secret by applying SP 800-135 as part of the TLS/IPsec protocol or they are derived from another key using SP 800-108 KBKDF or derived from a password using SP 800-108 PBKDF. The keys derived from SP 800-135 KDF map to the section 7.3 symmetric keys generated using the Key agreement scheme of the SP 800-133. The keys derived from SP 800-108/SP 800-132 KDF map to section 4.1 of SP 800-133 as indirect generation from DRBG. The Diffie-Hellman key generation based on safe primes is allowed according to IG D.13. The module does not support manual key entry or intermediate key generation output.

The module provides the following key establishment schemes:

- SP 800-38F AES key wrapping provides 256 bits of encryption strength
- RSA key wrapping provides 112 or 128 bits of encryption strength
- EC Diffie-Hellman provides between 112 and 256 bits of encryption strength
- Diffie-Hellman provides 112 bits of encryption strength
- SP 800-38F key wrapping using approved authenticated encryption mode i.e. AES GCM provides 128 or 256 bits of encryption strength
- SP 800-38F key wrapping using a combination of approved AES encryption and HMAC authentication method provides 128 or 256 bits of encryption strength
- SP 800-38F key wrapping using a combination of approved Triple-DES encryption and HMAC authentication method provides 112 bits of encryption strength

Table 12 – Cryptographic Keys, Cryptographic Key Components, and CSPs

Key/CSP	Key/CSP Type	Generation / Input	Output	Storage	Zeroization	Use
NGFW ECDSA Private Key	Private Key	Generation using FIPS 186-4	N/A	Plaintext on disk	Disk erasure	Private authentication key used in remote management
TLS Encryption Key	AES or TDES Symmetric Key	Derived using TLS 1.2 KDF	N/A	Plaintext in SDRAM	Automatically at the expiration of the session or Power off	Data encryption key used in TLS

Key/CSP	Key/CSP Type	Generation / Input	Output	Storage	Zeroization	Use
TLS Authentication Key	HMAC key	Derived using TLS 1.2 KDF	N/A	Plaintext in SDRAM	Automatically at the expiration of the session or Power off	Authentication key used in TLS
TLS Pre-Master Secret	Shared Secret	Generated through Diffie-Hellman /Elliptical Curve Diffie-Hellman agreement	N/A	Plaintext in SDRAM	Automatically at the expiration of the session or Power off	Shared secret generated or established for a TLS session
TLS Master Secret	Master Secret	Derived using TLS 1.2 KDF	N/A	Plaintext in SDRAM	Automatically at the expiration of the session or Power off	Value calculated during TLS handshake
TLS ECDSA Private Key	ECDSA Private Key	Generation using FIPS 186-4	N/A	Plaintext on disk	Disk erasure	Private key used in TLS signature
TLS ECDH Private Key	Private Key	Generation using FIPS 186-4	N/A	Plaintext in SDRAM	Automatically at the expiration of the session or Power off	Private ephemeral key agreement key used in TLS
TLS DH Private Key	Private Key	Safe prime generation (allowed according to IG D.13)	N/A	Plaintext in SDRAM	Automatically at the expiration of the session or Power off	Private ephemeral key agreement key used in TLS
TLS DRBG Entropy Input	Entropy Input	Obtained from NDRNG	N/A	Plaintext in SDRAM	Automatically after use or Power off	Entropy input for DRBG used in TLS
TLS DRBG V, key	V, Key	Derived from entropy string as defined by SP800-90A	N/A	Plaintext in SDRAM	Automatically after use or Power off	V, Key for DRBG used in TLS
IKE Encryption Key	AES or TDES Symmetric Key	Derived using IKEv1/IKEv2 KDF	Distributed in NGFW cluster using state synchronization[67]	Plaintext in SDRAM	Automatically at the expiration or Power off	Data encryption key used in IKE negotiations
IKE Authentication Key	HMAC Key	Derived using IKEv1/IKEv2 KDF	Distributed in NGFW cluster using state synchronization	Plaintext in SDRAM	Automatically at the expiration or Power off	Authentication key used in IKE negotiations

[67] State Synchronization – secure method to synchronize state tables within an NGFW cluster. The key is output encrypted using SP 800-38F AES key wrapping.

Key/CSP	Key/CSP Type	Generation / Input	Output	Storage	Zeroization	Use
SKEYID, SKEYID_d	Derived key	Derived using IKEv1 KDF	Distributed in NGFW cluster using state synchronization	Plaintext in SDRAM	Automatically at the expiration or Power off	Values calculated during IKE v1 negotiation
SKEYSEED, SK_d, SK_pi, SK_pr	Derived key	Derived using IKEv2 KDF	Distributed in NGFW cluster using state synchronization	Plaintext in SDRAM	Automatically at the expiration or Power off	Values calculated during IKEv2 negotiation
IPsec Encryption Key	AES or TDES Symmetric Key	Derived using IKEv1/IKEv2 KDF	Distributed in NGFW cluster using state synchronization	Plaintext in SDRAM	Automatically at the expiration or Power off	Data encryption key used in IPsec negotiations
IPsec Authentication Key	HMAC Key	Derived using IKEv1/IKEv2 KDF	Distributed in NGFW cluster using state synchronization	Plaintext in SDRAM	Automatically at the expiration or Power off	Authentication key used in IPsec negotiations
VPN RSA Private Key	Private Key	Generation using FIPS 186-4	Distributed in NGFW cluster using data synchronization	Encrypted on disk	Disk erasure	Private authentication key used in IKE and SSL VPN
VPN ECDSA Private Key	Private Key	Generation using FIPS 186-4	Distributed in NGFW cluster using data synchronization	Encrypted on disk	Disk erasure	Private authentication key used in IKE and SSL VPN
VPN Pre-Shared Key	Shared Secret	External/Encrypted electronic entry[68]	N/A	Plaintext or encrypted on disk[69]	Disk erasure	Shared secret used in IKE
VPN DH Private Key	Private Key	Safe prime generation (allowed according to IG D.13)	N/A	Plaintext in SDRAM	Automatically after use or Power off	Private ephemeral key agreement key used in IKE
VPN DH Shared Secret	Shared Secret	Safe prime generation (Allowed per IG D.13)	N/A	Plaintext in SDRAM	Automatically after use or Power off	Diffie-Hellman shared secret in IKE

[68] Refers to the keys entering from outside of the module over TLS channel.
[69] Storage for the VPN Pre-Shared Key is a checkbox configurable in the **SMC Engine Editor -> Advanced Settings -> Encrypt Configuration Data**. This option is checked, encrypted on disk, by default.

Key/CSP	Key/CSP Type	Generation / Input	Output	Storage	Zeroization	Use
VPN ECDH Private Key	Private Key	Generation using FIPS 186-4	N/A	Plaintext in SDRAM	Automatically after use or Power off	Private ephemeral key agreement key used in IKE
VPN ECDH Shared Secret	Shared Secret	Generated through Elliptical Curve Diffie-Hellman agreement	N/A	Plaintext in SDRAM	Automatically after use or Power off	Elliptical curve Diffie-Hellman shared secret in IKE
VPN Key Wrapping Key	AES Symmetric Key	Derived using SP 800-108 KBKDF	N/A	Plaintext in SDRAM	Automatically after use or Power off	IKE and IPsec key and key wrapping material
VPN DRBG Entropy Input	Entropy Input	Obtained from NDRNG	N/A	Plaintext in SDRAM	Automatically after use or Power off	Entropy input for DRBG used in VPN
VPN DRBG V, key	V, Key	Derived from entropy string as defined by SP800-90A	N/A	Plaintext in SDRAM	Automatically after use or Power off	V, Key for DRBG used in VPN
RWP Encryption Key	AES or Triple-DES Symmetric Key	Derived using TLS 1.0/1.1 or TLS 1.2 KDF	N/A	Plaintext in SDRAM	Automatically at the expiration or Power off	Data encryption key used in TLS
RWP Authentication Key	HMAC Key	Derived using TLS 1.0/1.1 or TLS 1.2 KDF	N/A	Plaintext in SDRAM	Automatically at the expiration or Power off	Authentication key used in TLS
RWP Pre-master Secret	Shared Secret	Generated internally using DRBG for RSA key wrapping or established through Diffie-Hellman /Elliptical Curve Diffie-Hellman agreement	Output encrypted with RSA key wrapping when using the RSA key exchange with TLS.	Plaintext in SDRAM	Automatically at the expiration or Power off	Shared secret generated or established for a TLS session
RWP Master Secret	Master Secret	Derived using TLS 1.2 KDF	N/A	Plaintext in SDRAM	Automatically at the expiration	Value calculated during TLS handshake
RWP Cookie Protection Master Key1	HMAC Key	Generated internally using DRBG	Distributed in NGFW cluster using data synchronization	Plaintext in SDRAM	Power off	Authentication key used to create RWP cookie protection user key1
RWP Cookie Protection Master Key2	HMAC Key	Generated internally using DRBG	Distributed in NGFW cluster using data synchronization	Plaintext in SDRAM	Power off	Authentication key used to create RWP cookie protection user key2

Key/CSP	Key/CSP Type	Generation / Input	Output	Storage	Zeroization	Use
RWP Cookie Protection User Key1	HMAC Key	Derived using SP 800-108 KBKDF	N/A	Plaintext in SDRAM	Automatically at the session expiration or Power off	Authentication key used to create RWP cookie
RWP Cookie Protection User Key2	HMAC Key	Derived using SP 800-108 KBKDF	N/A	Plaintext in SDRAM	Automatically at the session expiration or Power off	Authentication key used to create RWP cookie
RWP RSA Private key	Private Key	External/Encrypted electronic entry	N/A	Plaintext or encrypted on disk	Disk erasure	Private authentication key used in TLS
RWP ECDSA Private Key	Private Key	External/Encrypted electronic entry	N/A	Plaintext or encrypted on disk	Disk erasure	Private authentication key used in TLS
RWP DH Private Key	Private Key	Safe prime generation (allowed as per IG D.13)	N/A	Plaintext in SDRAM	Automatically after use or Power off	Private ephemeral key agreement key used in TLS
RWP ECDH Private Key	Private Key	Generated through FIPS 186-4	N/A	Plaintext in SDRAM	Automatically after use or Power off	Private ephemeral key agreement key used in TLS
SSL VPN encryption Key	AES or Triple-DES Symmetric Key	Derived using TLS 1.2 KDF	N/A	Plaintext in SDRAM	Automatically at the session expiration or Power off	Data encryption key used in TLS
SSL VPN authentication Key	HMAC Key	Derived using TLS 1.2 KDF	N/A	Plaintext in SDRAM	Automatically at the session expiration or Power off	Authentication key used in TLS
SSL VPN Pre-master Secret	Shared Secret	Generated through Elliptical Curve Diffie-Hellman agreement, or RSA key wrapping	N/A	Plaintext in SDRAM	Automatically at the session expiration or Power off	Shared secret generated or established for a TLS session
SSL VPN Master Secret	Master Secret	Derived using TLS 1.2 KDF	N/A	Plaintext in SDRAM	Automatically at the session expiration or Power off	Value calculated during TLS handshake

Key/CSP	Key/CSP Type	Generation / Input	Output	Storage	Zeroization	Use
SSL VPN DH Private Key	Private Key	Safe prime generation (allowed as per IG D.13)	N/A	Plaintext in SDRAM	Automatically after use or Power off	Private ephemeral key agreement key used in TLS
SSL VPN ECDH Private Key	Private Key	Generated using FIPS 186-4	N/A	Plaintext in SDRAM	Automatically after use or Power off	Private ephemeral key agreement key used in TLS
Cluster Protocol Key	HMAC Key	External/Encrypted electronic entry	N/A	Plaintext or encrypted on disk	Disk erasure	Authentication key used in Cluster Protocol
State Synchronization Key	AES Symmetric Key HMAC Key	Generated internally using DRBG	Distributed in NGFW cluster using key exchange interface[70]	Plaintext in SDRAM	Power off	Data encryption and authentication key used in State Synchronization
Configuration File Protection Key	HMAC key	Generated internally using DRBG	N/A	Plaintext on disk	Disk erasure	Master key used in configuration file protection
Configuration file encryption key	AES Symmetric key	Derived using SP 800-132 KBKDF	N/A	Plaintext in SDRAM	Power off	Data encryption key used in configuration file protection
Configuration file authentication key	HMAC key	Derived using SP 800-132 KBKDF	N/A	Plaintext in SDRAM	Power off	Authentication key used in configuration file protection
HTTPS Encryption Key	AES or TDES Symmetric key	Derived using TLS 1.0/1.1 or TLS 1.2 KDF	N/A	Plaintext in SDRAM	Automatically at the session expiration or Power off	Data encryption key used in TLS
HTTPS Authentication Key	HMAC Key	Derived using TLS 1.0/1.1 or TLS 1.2 KDF	N/A	Plaintext in SDRAM	Automatically at the session expiration or Power off	Authentication key used in TLS
HTTPS Pre-master Secret	Shared Secret	Generated through Diffie-Hellman protocol, Elliptical Curve Diffie-Hellman agreement, or RSA key wrapping	N/A	Plaintext in SDRAM	Automatically at the session expiration or Power off	Shared secret generated or established for a TLS session

[70] Key exchange interface – secure method used to synchronize protocol keys within an NGFW cluster. The key is sent over TLS channel.

Key/CSP	Key/CSP Type	Generation / Input	Output	Storage	Zeroization	Use
HTTPS Master Secret	Master secret	Derived using TLS 1.0/1.1 or TLS 1.2 KDF	N/A	Plaintext in SDRAM	Automatically at the session expiration Power off	Value calculated during TLS handshake
HTTPS RSA Private Key	Private Key	Generated internally using FIPS 186-4	Distributed in NGFW cluster using data synchronization	Plaintext on disk	Disk erasure	Private authentication key used in HTTPS user authentication
HTTPS DH Private Key	Private Key	Safe prime generation (allowed as per IG D.13)	N/A	Plaintext in SDRAM	Automatically after use or Power off	Private ephemeral key agreement key used in TLS
HTTPS ECDH Private Key	Private Key	Generated using FIPS 186-4	N/A	Plaintext in SDRAM	Automatically after use or Power off	Private ephemeral key agreement key used in TLS
Client Protection CA RSA Private Key	Private Key	External/Encrypted electronic entry	N/A	Encrypted on disk	Disk erasure	Private signature key used in TLS inspection CA
Client Protection IM CA RSA Private Key	Private Key	Generated internally using FIPS 186-4	N/A	Plaintext in SDRAM	Power off	Private authentication key used in TLS inspection
Client Protection IM CA ECDSA Private Key	Private Key	Generated using FIPS 186-4	N/A	Plaintext in SDRAM	Power off	Private authentication key used in TLS inspection
Client Protection RSA Private Key	Private Key	Generated using FIPS 186-4	N/A	Plaintext in SDRAM	Power off	Private authentication key used in TLS inspection
Server Protection RSA Private Key	Private Key	External/Encrypted electronic entry	N/A	Encrypted on disk	Disk erasure	Private authentication key used in TLS inspection
Client Protection ECDSA Private Key	Private Key	Generated using FIPS 186-4	N/A	Plaintext in SDRAM	Power off	Private authentication key used in TLS inspection
Server Protection ECDSA Private Key	Private Key	External/Encrypted electronic entry	N/A	Encrypted on disk	Disk erasure	Private authentication key used in TLS inspection

Key/CSP	Key/CSP Type	Generation / Input	Output	Storage	Zeroization	Use
Inspection DH Private Key	Private Key	Safe prime generation (allowed as per IG D.13)	N/A	Plaintext in SDRAM	Automatically after use	Private ephemeral key agreement key used in TLS inspection
Inspection ECDH Private Key	Private Key	Generated using FIPS 186-4	N/A	Plaintext in SDRAM	Automatically after use	Private ephemeral key agreement key used in TLS inspection
Inspection Encryption Key	AES or Triple-DES Symmetric Key	Derived using TLS 1.0/1.1 or TLS 1.2 KDF	N/A	Plaintext in SDRAM	Automatically at the expiration of the session	Data encryption key used in TLS inspection
Inspection Authentication Key	HMAC Key	Derived using TLS 1.0/1.1 or TLS 1.2 KDF	N/A	Plaintext in SDRAM	Automatically at the expiration	Authentication key used in TLS inspection
Inspection Pre-Master Secret	Shared Secret	Generated through Diffie-Hellman protocol, Elliptical Curve Diffie-Hellman protocol, or RSA key wrapping	N/A	Plaintext in SDRAM	Automatically at the expiration	Shared secret generated or established for TLS inspection
Inspection Master Secret	Master Secret	Derived using TLS 1.0/1.1 or TLS 1.2 KDF	N/A	Plaintext in SDRAM	Automatically at the expiration	Value calculated during TLS inspection
SSM HTTPS DH Private Key	Private Key	Safe Prime generation (allowed as per IG D.13)	N/A	Plaintext in SDRAM	Automatically after use	Private ephemeral key agreement key used in HTTPS inspection
SSM HTTPS ECDH Private Key	Private Key	Generated through FIPS 186-4	N/A	Plaintext in SDRAM	Automatically after use	Private ephemeral key agreement key used in HTTPS inspection
SSM HTTPS Encryption Key	AES or Triple-DES Symmetric Key	Derived using TLS 1.0/1.1 or TLS 1.2 KDF	N/A	Plaintext in SDRAM	Automatically at the expiration of the session	Data encryption key used in HTTPS inspection
SSM HTTPS Authentication Key	HMAC Key	Derived using TLS 1.0/1.1 or TLS 1.2 KDF	N/A	Plaintext in SDRAM	Automatically at the expiration	Authentication key used in HTTPS inspection

Key/CSP	Key/CSP Type	Generation / Input	Output	Storage	Zeroization	Use
SSM HTTPS Pre-Master Secret	Shared Secret	Generated through Diffie-Hellman protocol, Elliptical Curve Diffie-Hellman protocol, or RSA key wrapping	N/A	Plaintext in SDRAM	Automatically at the expiration	Shared secret generated or established for HTTPS inspection
SSM HTTPS Master Secret	Master Secret	Derived using TLS 1.0/1.1 or TLS 1.2 KDF	N/A	Plaintext in SDRAM	Automatically at the expiration	Value calculated during HTTPS inspection
User Password	Password	External/Encrypted electronic entry	N/A	SHA-512 digest on disk	Disk erasure	User authentication password that can be used in HTTPS authentication or mobile VPN
SNMP encryption key	AES Symmetric Key	External/Encrypted electronic entry	N/A	Plaintext or encrypted on disk	Disk erasure	Data encryption key used in SNMPv3
SNMP authentication key	HMAC Key	External/Encrypted electronic entry	N/A	Plaintext or encrypted on disk	Disk erasure	Authentication key used in SNMPv3
Passphrase used in PBKDF	Passphrase	External/ Encrypted electronic entry	N/A	Plaintext or encrypted on disk[71]	Disk erasure	Passphrase used to derive Key encryption key
Key Encryption Key	Derived key	Derived using SP 800-132 PBKDF	N/A	Plaintext in SDRAM	Automatically after use or power off	Key encryption key to encrypt private keys[72] stored on the disk

[71] Storage for the passphase is a checkbox configurable in the **SMC Engine Editor -> Advanced Settings -> Encrypt Configuration Data**. This option is checked, encrypted on disk, by default.
[72] Refers to all private leys in this table where the storage column indicates 'encrypted on disk'.

2.8 EMI / EMC

The NGFW appliances were tested and found conformant to the EMI/EMC requirements specified by 47 Code of Federal Regulations, Part 15, Subpart B, Unintentional Radiators, Digital Appliances, Class A (business use).

2.9 Self-Tests

Cryptographic self-tests are performed automatically (without operator intervention) by each module during the boot sequence (at power-up, upon restarts, and after power cycles) and during runtime as certain conditions exist. While the module is in a self-test condition, all data output via the module's data output interfaces is inhibited.

The following sections list the self-tests performed by the modules, their expected error status, and error state recovery.

2.9.1 Power-Up Self-Tests

The NGFW performs the following self-tests at power-up. When all tests have passed, a message indicating success is displayed on the status output interface. If any one of the self-test fails, module enters an error state.

Table 13 - List of Power-Up Self-Tests

Power-Up Self-Test	OpenSSL Library	NGFW Library	NGFW Kernel
Firmware Integrity Test HMAC-SHA-256 (Root File System)	N/A	N/A	N/A
AES encryption and decryption KAT[73]	✓AES-ECB	✓AES-CBC	✓AES-CBC
Triple-DES encryption and decryption KAT	✓3DES-ECB	✓3DES-CBC	✓3DES-CBC
HMAC KAT with SHA-1, SHA-256, and SHA-512*	✓	✓	✓
SP 800-90A CTR_DRBG KAT	✓	✓	N/A
RSA signature generation and verification KAT	(PSS)	(PKCS#1)	N/A
ECDSA PCT[74]	✓	✓	N/A
Diffie-Hellman primitive Z computation KAT**	N/A	✓	N/A
EC Diffie-Hellman primitive Z computation KAT	✓	✓	N/A

***Note:** SHA KATs are covered by HMAC-SHA KATs. ****Note:** Diffie-Hellman is an allowed algorithm with KAT implemented for NGFW only.

2.9.2 Conditional Self-Tests

The modules perform the following conditional self-tests. If the bypass test fails, module enters the 'Bypass Error' state. For any other conditional test failure, module enters the 'Error' state.

Table 14 – List of Conditional Self-Tests

[73] KAT – Known Answer Test
[74] PCT – Pairwise Consistency Test

Conditional Self-Test	OpenSSL Library	NGFW Library
Repetition count test for NDRNG	N/A	N/A
Continuous Random Number Generator Test for DRBG	✓	✓
RSA PCT	N/A	✓
ECDSA PCT	✓	✓
Configuration Bypass Test	✓	N/A

2.9.3 DRBG Health Checks

The DRBG Instantiate, Generate, Reseed, and Uninstantiate tests are performed as described in Section 11.3 of NIST SP 800-90A.

Table 15 – List of DRBG Health Checks

Health Tests	OpenSSL Library	NGFW Library
SP 800-90A CTR_DRBG Instantiate Test	✓	✓
SP 800-90A CTR_DRBG Generate Test	✓	✓
SP 800-90A CTR_DRBG Reseed Test	✓	✓
SP 800-90A CTR_DRBG Uninstantiate Test	✓	✓

2.9.4 Self-Test Error Behavior and Recovery

If one of the power-up self-test fails or a conditional self-test (except bypass test) fails, the module enters the '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 power-up self-tests. Successful completion of the self-test will clear the error state, and the module will return to the FIPS-Approved mode of operation. For any consecutive failure of the power-up 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.

The bypass test is run at each power-up and whenever a new configuration is applied to the device. If the bypass test fails, the module enters the 'Bypass Error' state. An error message is output on the status output interface and a default initial configuration is applied to the device. In this state, no crypto operations are allowed. The CO needs to perform two independent actions consisting of 1) configure the policy for the module 2) apply the policy to the module which performs the bypass test on the new configuration policy. Successful application of the policy to the device clears the error.

2.10 Mitigation of Other Attacks

This section is not applicable. The modules do not claim to mitigate any attacks beyond the FIPS 140-2 Level 2 requirements for this validation.

3. Secure Operation

The NGFW meets Level 2 requirements for FIPS 140-2. The sections below describe how to set up and keep the modules in the FIPS-Approved mode of operation.

3.1 Initial Setup

This section discusses hardware setup, downloading a FIPS 140-2 Validated NGFW firmware version, upgrading to a FIPS 140-2 Validated NGFW firmware version, enabling Restricted FIPS-Compatible Operating Mode, and verifying that the module is in FIPS-Approved mode of operation.

3.1.1 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 the following number of labels to each module:

- NGFW 1101: **7**
- NGFW 2101: **10**
- NGFW 2105: **11**
- NGFW 3305: **13**
- NGFW 6205: **19**

The CO shall apply the proper number of tamper-evident seals as shown for each module in Figure 12 below through Figure 26 below for each module:

Figure 12 – Labels Front (NGFW 1101)

Figure 13 – Labels Rear (NGFW 1101)

Figure 14 – Labels Front (NGFW 2101)

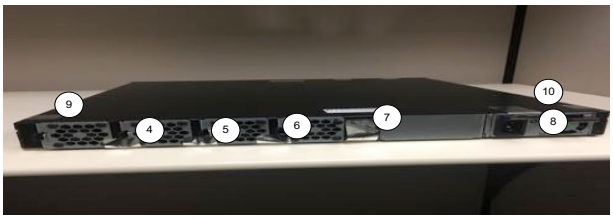

Figure 15- Labels Rear (NGFW 2101)

Figure 16 - Labels Side (NGFW 2101)

Figure 17 – Labels Front (NGFW 2105)

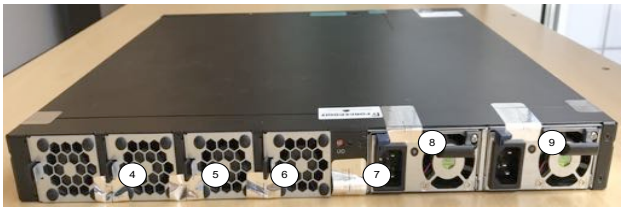

Figure 18- Labels Rear (NGFW 2105)

Figure 19 - Labels Side (NGFW 2105)

Figure 20 - Labels Front (NGFW 3305)

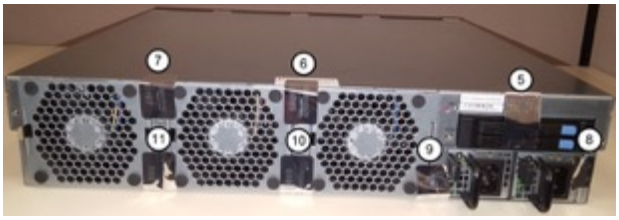

Figure 21 - Labels Rear (NGFW 3305)

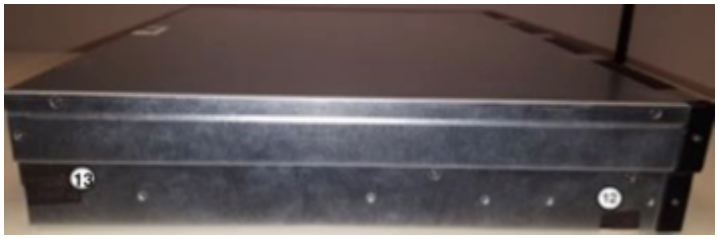

Figure 22 - Labels Side 1 (NGFW 3305)

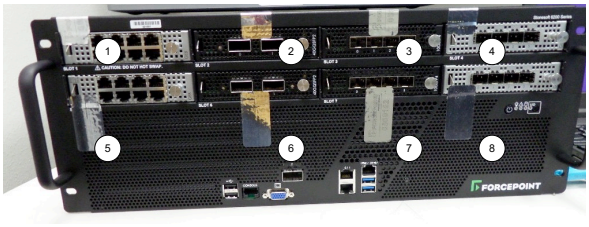

Figure 23 – Labels Front (NGFW 6205)

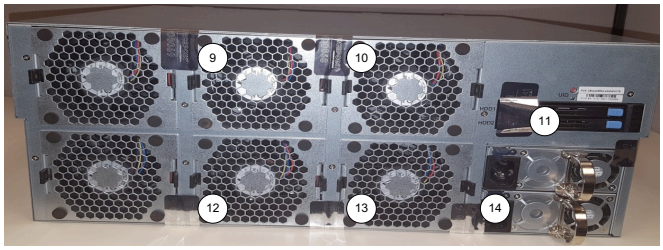

Figure 24 - Rear (NGFW 6205)

Figure 25 – Side 1 (NGFW 6205)

Figure 26 – Side 2 (NGFW 6205)

The tamper-evident seals are shipped as part of the Forcepoint NGFW FIPS Kit with the Stock Keeping Unit ACFIPS3. It is up to the CO to ensure proper placement of the tamper-evident seals using the following steps (the CO must wear gloves to ensure proper cleaning and installation of the seals):

1. The CO shall apply the adhesive at room temperature – the adhesive will not form a solid bond if applied at temperatures below 50° F.
2. The CO must ensure that the surface is dry and free of dirt, oil, and grease, including finger oils. Alcohol pads or a 99% isopropyl alcohol solution can be used to clean the surface. The surface should be dried with a clean cloth before application of the labels.
3. Once the seal is placed, the CO shall rub a thumb over it to ensure complete adhesion.

4. The CO must wait 24 hours until the tamper-evident seals are completely adhesive. This will ensure that all tamper-evident features of the seals can be activated.

3.1.2 Creating a Configuration for the NGFW Engine

The administration of the NGFW modules is done through the SMC, which provides centralized administrative functionality 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 FIPS-Approved Mode of Operation.

1. To use HTTPS User Authentication, TLS Inspection for Client Protection or Server Protection, SSL VPN Portal, or SSL VPN Tunneling, create a TLS Cryptography Suite Set element. Select only FIPS-Approved and FIPS-Allowed algorithms and TLS cipher suites. Refer to Table 4 above for a list of algorithms implemented. For more information, see the *Select SSL cryptographic algorithms for the SSL VPN* topic in the *Configuring VPNs* chapter of the *Forcepoint Next Generation Firewall Product Guide*.
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 FIPS-Approved signature algorithm. For more information, see the *Create Trusted Certificate Authority elements* topic in the *Setting up TLS Inspection* chapter of the *Forcepoint Next Generation Firewall Product Guide*.
3. To use HTTPS User Authentication, SSL VPN Portal, or SSL VPN Tunneling, 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 in the *Configuring system communications chapter* of the *Forcepoint Next Generation Firewall 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.
    - To use HTTPS User Authentication, browse to Add-Ons | User Authentication, then enable HTTPS and select the TLS Profile element. Use 2048 as the Key Length when creating a certificate signing request in HTTPS Settings. For more information, see the *Enable browser-based user authentication* topic in the *Setting up user authentication* chapter of the *Forcepoint Next Generation Firewall 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 FIPS-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 *Activate TLS inspection on engines* topics in the *Setting up TLS Inspection* chapter of the *Forcepoint Next Generation Firewall 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 *Activate TLS inspection on engines* topic in the *Setting up TLS Inspection* chapter of the *Forcepoint Next Generation Firewall 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 DHE:ECDHE:RSA:-NULL@STRENGTH on the HTTP tab. For more information, see the *Advanced settings for Sidewinder Proxies* topic in the *Sidewinder Proxies* chapter of the *Forcepoint Next Generation Firewall Product Guide*.
- To use the SSL VPN Portal, browse to VPN | SSL VPN Portal, then select the TLS Cryptography Suite and select the allowed SSL or TLS versions. For more information, see the *Edit the engine-specific SSL VPN Portal settings* topic in the *Configuring VPNs* chapter of the *Forcepoint Next Generation Firewall Product Guide*.
- When using IPsec or SSL VPN Tunneling, disable Automated RSA Certificate Management. Browse to VPN | Certificates, then deselect Automated RSA Certificate Management.
- When using SSL VPN Tunneling, browse to VPN | VPN Client, then select the TLS Cryptography Suite Set. For more information, see the *Define VPN client settings for Forcepoint NGFW* topic in the *Configuring VPNs* chapter of the *Forcepoint Next Generation Firewall Product Guide*.
- To use an IPsec or SSL VPN, right-click the Gateway element, then select Tools | Generate Certificate to create a certificate signing request. Select RSA with 2048 or 3072 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 Next Generation Firewall Product Guide*.

5. To use an IPsec VPN, create a VPN Profile element. Use only FIPS-Approved and FIPS-Allowed algorithms and key sizes in the profile. Refer to Table 4 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 *Configuring VPNs* chapter of the *Forcepoint Next Generation Firewall 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 3.1.5 for setting up FIPS-compatible device configuration.

3.1.3 Downloading a FIPS 140-2 Validated NGFW 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 140-2 validated NGFW firmware version to be placed in the FIPS-Approved mode of operation.

Note: The upgrade to the FIPS 140-2 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 SHA-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 6.4.1.20056.fips.8 is out of the scope of this validation and will mean that the module is not operating in a validated mode of operation.

A FIPS 140-2 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 6.4.1.20056.fips.8 installation file (sg_engine_6.4.1.20056.fips.8_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.

3.1.4 Upgrading to a FIPS 140-2 Validated NGFW Firmware Version

Upgrade to a FIPS 140-2 validated NGFW firmware version as follows:

1. Save the FIPS 140-2 Validated NGFW firmware version upgrade .zip file to the root directory of a USB drive or CD media.
2. Connect to the appliance using a monitor and keyboard.
3. Power on the appliance and start the NGFW Initial Configuration Wizard.
4. Select Firewall/VPN option of the module.
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. (When upgrading from NGFW Engine versions lower than 5.10) Select Calculate to verify the checksum. The file system checksum is calculated and displayed. Verify that the calculated checksum is identical to the checksum from the .zip file.
8. Select OK. The upgrade starts and the NGFW appliance restarts.
9. Select Set Kernel in FIPS mode after restart. Select OK.
10. The NGFW restarts and displays the upgraded version.
11. Verify the NGFW firmware version to ensure that the FIPS 140-2 Validated NGFW firmware version is loaded.

3.1.5 Setting up a FIPS-Compatible Device Configuration

The CO shall perform the following steps for device configuration and use the *Forcepoint Next Generation Firewall Installation Guide 6.4* for the referenced sections:

1. Use the Management Client to create the configuration for the NGFW Engine according to section 3.1.2 in this document. (Refer to *Installing the SMC* for the SMC and Management Client installation.)
2. Connect to the appliance using a monitor and keyboard, and start the NGFW Initial Configuration Wizard.
3. Configure the general settings, and select FIPS-Compatible Operating Mode. (Refer to *Configure general settings*.)
4. Configure the network interfaces for the appliance according to your environment. (Refer to *Configure network interfaces*.)
5. Contact the Management Server (refer to *Contact the Management Server* section). The NGFW Engine restarts and the initial configuration is applied. Command line login and the NGFW Initial Configuration Wizard are disabled.
6. Use the Management Client to apply the configuration created in step 1 to the NGFW appliance. (Refer to *NGFW Engine post-installation tasks*.)

3.1.6 Verifying FIPS-Approved mode of operation

Upon restart, the module operates in the FIPS-Approved mode of operation. Verify that the following messages are displayed on the console when the NGFW appliance restarts:

```
FIPS: rootfs integrity check OK
```
Note: This confirms that the module's integrity test has been executed successfully

```
FIPS power-up tests succeeded
```
Note: This implies that the FIPS 140-2 power-up self-tests have been executed successfully.

Note: If the power-up tests fail, a power-up test error message is displayed, and the module restarts. See section 2.9 above for information on recovering from a FIPS 140-2 power-up self-test failure.

3.2 Crypto Officer Guidance

The entity in charge of receiving and installing the module is responsible for creating the CO role. The entity uses a proof-of-serial (POS) code delivered with the module and one-time password generated by the Security Management Center (SMC) for establishing initial contact between the SMC and the module. The SMC is the only calling management entity of the NGFW modules and acts as the CO role. Once the initial contact has been established, the module receives a X.509 certificate from the SMC, which is used for authentication.

The CO shall be in charge of initializing and maintaining the NGFW module. The CO should follow the steps in section 3.1.5 to enable the FIPS mode for the module. When configured accordingly, the modules only run in the FIPS-Approved mode of operation. The CO should follow section 3.1.2 for configuration of the NGFW engine. During this configuration, the CO should create the passwords for users requiring password authentication. The passwords must be at least eight characters long. The passwords should not be based on personal information such as names, birthdays, social security numbers, phone numbers, street names, or registration plate numbers.

The CO shall power cycle the module if the module has encountered a critical error and becomes non-operational. If power cycling the module does not correct the error condition, the module is considered to be compromised or malfunctioning, and the CO should perform a reset to factory default settings and reinstall, or contact Forcepoint Customer Service to return the module for replacement or repair.

3.2.1 Monitoring Status

The CO shall be responsible for regularly monitoring the modules' status. The module's operational status is indicated with LEDs as described in Table 8 above. A CO can view the operational status on the remote terminal window via SMC.

3.2.2 Physical Inspection

For the modules to operate in their FIPS validated mode, the tamper-evident labels must be in place as specified in section 3.1. Per FIPS 140-2 Implementation Guidance (IG) 14.4, the CO is also responsible for the following:

- Direct control and observation of any changes to the module where the tamper-evident labels are removed or applied to ensure that the security of the module is maintained during such changes and that the module is returned to its Approved state

The CO is also required to periodically inspect the modules for evidence of tampering at intervals specified per end-user policy (96-hour interval is recommended). The CO must visually inspect the tamper-evident seals for tears, rips, dissolved adhesive, and other signs of tampering. If evidence of tampering is found during periodic inspection, the CO must zeroize the keys and contact Forcepoint Customer Service to return the module for replacement or repair.

The CO shall maintain control of any additional tamper-evident seals. The module must be under the direct control and observation of the CO. If the tamper evident seals are removed, the modules are not in a validated mode of operation. To return the modules to the validated mode of operation, all tamper-evident seals must be properly secured or installed.

3.2.3 On-Demand Self-Test Execution

Although power-up self-tests are performed automatically during module power up, they can also be manually launched on demand. Self-tests can be executed by power-cycling the modules or using the reset button (on appliances so equipped). If one of the power-up self-tests fails, the appliances will exhibit the behavior described in section 2.9 above.

3.2.4 CSP Zeroization

The keys and CSPs in the NGFW appliances can be destroyed or zeroized in the following ways depending on the type of the key and the storage location:

- All symmetric and ephemeral asymmetric keys are destroyed automatically after use or at the end of the crypto-period.
- All keys and CSPs in memory can be destroyed by powering the device off.
- All keys and CSPs on disk can be destroyed by first powering the appliances off and then erasing the disks. For the NGFW appliances, the disks and partitions can be overwritten by selecting Factory Reset from the boot menu.

3.3 User Guidance

While the CO is responsible for ensuring that the modules' physical security mechanisms are in place and that the appliances are running in their FIPS-Approved mode of operation, Users should also monitor the appliance status. Any changes in the status of the appliances should immediately be reported to the CO.

3.4 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 to SP 800-38D in compliance with IG A.5 scenario 1. The GCM IV generation in the TLS context is in compliance with RFC 5288 and shall only be

used for the TLS protocol version 1.2. The GCM IV generation in the IPsec context is in compliance with RFC 4106 and shall only be used with IPsec and IKEv2 to be compliant with IG A.5. 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 3.1.2 bullet 5) 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 Triple-DES: According to IG A.13, the same Triple-DES key shall not be used to encrypt more than 2^{16} 64-bit blocks of data.

- Use of PBKDF: The module implements key derivation through the SP 800-132 PBKDF2 vendor affirmed algorithm. 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 20 characters, which provides the probability of guessing this password or passphrase to be $(1/10)^{20}$ assuming a scenario where all characters are digits. 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.

- 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 3.1 above with the configuration stated in Table 3.

  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 3.1.1). 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 Figure 12 through Figure 26 for label locations). Allow 24 hours for the seal to fully cure.
  8. Apply power to the module.

3.5 Non-FIPS-Approved Mode

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

4. Acronyms

Table 16 provides definitions for the acronyms used in this document.

Table 16 – Acronyms

Acronym	Definition
AES	Advanced Encryption System
API	Application Programming Interface
BIOS	Basic Input/Output System
°C	Celsius
CBC	Cipher Block Chaining
CFast	Compact Fast
CFB	Ciphertext Feedback
CMVP	Cryptographic Module Validation Program
CO	Crypto Officer
CSE	Communications Security Establishment
CSP	Critical Security Parameter
CTR	Counter
DDR	Double Data Rate
DES	Data Encryption Standard
DH	Diffie-Hellman
DRBG	Deterministic Random Bit Generator
DSA	Digital Signature Algorithm
E	Execute
EC	Elliptic Curve
ECB	Electronic Code Book
ECDH	Elliptic Curve Diffie-Hellman
ECDSA	Elliptical Curve Digital Signature Algorithm
EMC	Electromagnetic Compatibility
EMI	Electromagnetic Interference
°F	Fahrenheit
FIPS PUB	Federal Information Processing Standards Publications
GB	Gigabyte
Gbps	Gigabits per second
GCM	Galois Counter Mode
GE	Gigabit Ethernet
HMAC	(keyed-) Hash Message Authentication Code

Acronym	Definition
I/O	Input/Output
IKE	Internet Key Exchange
IPMI	Intelligent Platform Management Interface
IPS	Intrusion Prevention System
IPsec	Internet Protocol System
KBKDF	Key Based Key Derivation Function
KDF	Key Derivation Function
LED	Light Emitting Diode
LKRNG	Linux kernel Random Number Generator
Mbps	Megabits per second
NDRNG	Non-Deterministic Random Number Generator
NGFW	Next Generation Firewall
NIST	National Institute of Standards and Technology
NPTRNG	Non-physical True Random Number Generator
OFB	Output Feedback
OS	Operating System
PBKDF2	Password Based Key Derivation Function
PCIE	Peripheral Component Interconnect Express
PCH	Platform Controller Hub
PCT	Pairwise Consistency Test
PKCS	Public Key Cryptography Standard
PSU	Power Supply Unit
QSFP	Quad Small Form-Factor Pluggable
R	Read
RAM	Random Access Memory
RJ	Registered Jack
RNG	Random Number Generator
RSA	Rivest, Shamir, Adleman
SAS	Serial Attached SCSI (Small Computer System Interface)
SDRAM	Synchronous Dynamic Random Access Memory
SD-WAN	Software-Defined Wide-Area Network
SFP	Small Form-Factor Pluggable
SHA	Secure Hash Algorithm
SHS	Secure Hash Standard
SMC	Forcepoint NGFW Security Management Center
SNMP	Simple Network Management Protocol

Acronym	Definition
SP	Special Publication
SSD	Solid State Drive
SSH	Secure Shell
TLS	Transport Layer Security
U	Unit
UID	Unique Identifier
USB	Universal Serial Bus
VAC	Voltage Alternating Current
VDC	Voltage Direct Current
VGA	Video Graphics Array
VPN	Virtual Private Network
W	Write

Prepared by:

Corsec Security, Inc.

13921 Park Center Road, Suite 460
Herndon, VA 20171
United States of America

Phone: +1 703 267 6050
Email: info@corsec.com
http://www.corsec.com